

AXIS OS Portal | AXIS OS Release Notes | AXIS OS YouTube playlist| AXIS OS Hardening Guide | Security Advisories

About

About

Welcome to the AXIS OS Knowledge base, a comprehensive repository designed to be the go-to resource for technical information about AXIS OS. *AXIS OS* is the Linux-based operating system used in most of your Axis network devices. It is purpose-built to live up to the most important criteria for network devices: high standards for cybersecurity, ease of integration, quality, and long-term value.

Cybersecurity

Cybersecurity

Security advisories

We now have a Security Advisories page which lists all known vulnerabilities in Axis products. Please visit to stay informed.

Device hardening

For information on how to harden AXIS OS devices, visit AXIS OS Hardening Guide. The hardening guide is written for, and can be applied to, all AXIS OS devices running an AXIS OS LTS or active track. Legacy products running version 4.xx and 5.xx are also in scope.

Identity and access management

Summary

Identity and Access Management comprises policies for safeguarding that individuals and applications have access to system resources in the right context. For example, individuals should only interact with applications, and only applications access devices. IAM ensures integrity over time, for example, that passwords are not leaked, and that accesses are revoked when no longer needed.

Axis recommends to use Axis' device management applications, AXIS Device Manager or AXIS Device Manager Extend, to set up and manage unique service accounts for applications accessing devices. The following sections further detail Axis' recommendations for identity and access management in video surveillance systems.

Introduction

Identity and Access Management (IAM) systems are responsible for managing identities, permissions, and access control within an organization. IAM makes sure that the right individuals and applications have the right level of access to the right system resources. This is a fundamental cybersecurity measure for preventing unauthorized access. One of the main challenges is maintaining integrity over time. This includes ensuring that passwords and other secrets have not been leaked, and that individuals and applications that should no longer have access indeed have their access revoked.

Identity and access management typically involves authentication, authorization, and privileges.

- Authentication. Verifying that an entity is who or what it states to be.
- Authorization. Controlling which entities are allowed to perform specific functions.
- Privileges. Grouping of entities based on what they are authorized to do. Axis defines privileges as roles.

Throughout the document, the terms user account and service account are used. Both are registered and governed through IAM.

- User account. A user account is an account used by a person to access applications.
- Service account. A service account is a non-human account used by an application to access devices. Service accounts are used in machine-to-machine communication or when an application needs to access devices in a trusted and automated manner.

Best practices when working with service accounts

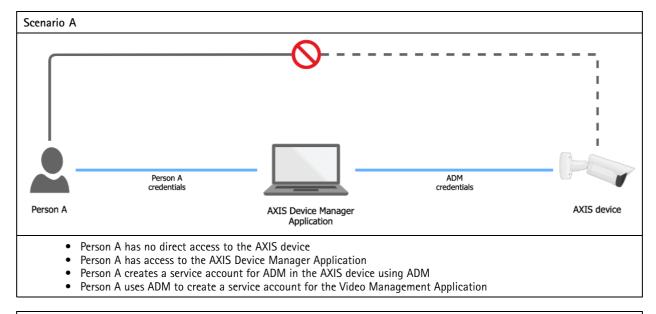
For maintaining integrity over time the following best practices of service account management are recommended.

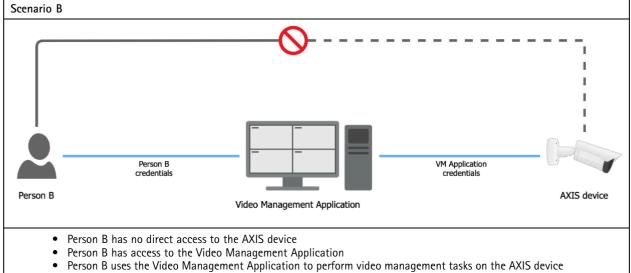
- Use Axis' device management applications, AXIS Device Manager or AXIS Device Manager Extend, for service account management.
- Set up unique service accounts for each application accessing devices, as recommended in the AXIS OS Hardening Guide.
- Select appropriate privilege to each service account.
- Remove service accounts that are no longer in use.

Cybersecurity

- Avoid persons accessing devices directly (if it is absolutely necessary, use a unique and temporary service account), the web-interface can be disabled as recommended in the AXIS OS Hardening Guide.
- Ensure high password complexity is given to avoid account leakage, see recommendations from the AXIS OS Hardening Guide.

The below diagrams visualize the best practices of access management in the device.





The device is exposed to following risks when using user accounts in the device:

- unauthorized personell accessing devices
- wrong level of authorization in different devices
- reuse of user account credentials leads to no audit traceability
- poor scalability with increasing number of devices

Cybersecurity

Different sites and organizations can have different policies, including password policies. The setup of the system should accommodate these policies. Typically, each application should have its own credentials to devices. If the password is reused in devices, Axis recommends to rotate the password frequently.

Authorization and account privileges

Axis devices support the roles Administrator, Operator, and Viewer, with different authorization levels. Axis recommends to set up an administrator account for management application that has access to the devices. This account should be unique for each application and not shared. Ideally, the password for this account should be generated by the management application itself and remain unknown to all individuals.

If direct access to devices is needed

Some configurations may not be natively supported by the application and may need to be done through the devices web interface. Axis recommends to access the Axis device web interface through the seamless access provided by Axis' device management applications.

If there are strong reasons for allowing direct access to devices, Axis recommends to use temporary service account impersonalization with limited access. A new service account should be created on the device with the appropriate role for what needs to be done. Once the direct access is no longer needed, this service account should be deleted.

Device access

Legacy access procedure (default user with default password)

Historically, Axis devices in their factory defaulted state have had their VAPIX and ONVIF interfaces activated for quick and easy out-of-the-box access on the network for clients connecting to them. This means that a client, such as an application or video management system, can access the Axis network device via anonymous ONVIF calls as well as the default VAPIX user "root" with the default password "pass", prior to having configured anything on the Axis network device itself.

Updated access procedure (default user with no default password)

The VAPIX and ONVIF interfaces have been disabled and the "root" VAPIX user password is no longer set in factory default state. This means that it's no longer possible for a client to access or configure the device out-of-the-box without setting a password for the VAPIX user "root".

The new access procedure has been implemented in the following AXIS OS releases:

- Version 5.51.6
- Version 6.50.4 (2016 LTS)
- Version 8.40.3 (2018 LTS)
- Version 9.40.1 and higher

Furthermore, the new updated procedure has been rolled out on individual product releases that are located outside of the above platform releases, such as:

- 1.65.x
- 1.8x.x
- 5.75.x
- 6.53.x
- 6.55.x
- 7.15.x

Cybersecurity

Welcome.	
Set a password for the root account.	
root	
Password 💿	
Repeat password	
Password strength: Blank. Type a password.	
English	
Share data with developers Share non-personal browser data with Axis Communications AB. This helps us improve the application and user experience. Learn more.	
Create login	
	1º

Modern access procedure (no default user)

With AXIS OS 11.6 and higher, the default VAPIX user "root" has been removed from the Axis device in their factory default state and it is now possible to create a custom named VAPIX user instead during factory default state.

Cybersecurity

	0 🖙 🛈		
AXIS P1375 Network Camera			
Account			
New password			
Repeat password			
		Ó)	
 I accept the end user license agreement. Share non-personal browser data with Axis Communications AB. This helps us improve the application and your user experience. Learn more. 			
Add account		AXIS OS version: 11.11.2 Serial number: ACCC8EC3E923	

Anonymous interface calls

Interface calls that do not require authentication (=anonymous) are still allowed for device identification purposes. An Axis device can be identified in its factory default state by its HTTP response header which is set to "AXIS-Setup:vapix" when an VAPIX or ONVIF API call is made, as illustrated below:

```
HTTP/1.1 401
Unauthorized Date: Thu, 19 Sep 2019 18:15:20 GMT
Server: Apache/2.4.39 (Unix) OpenSSL/1.1.1c
Axis-Setup: vapix
```

Activate VAPIX and/or ONVIF interfaces

The VAPIX and/or ONVIF interfaces in the Axis device can be activated using the following methods:

- The VAPIX interface is activated when an initial VAPIX user password is set, either via VAPIX System Settings API, as described in the or by using the Axis device's web interface during the installation wizard process.
- The ONVIF interface can only be activated after the VAPIX interface has been activated. After that, the ONVIF interface can be activated by creating an ONVIF user via the device's web interface.

Cybersecurity

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

• In addition, an ONVIF user can also be created using the . An example of the API call to create an ONVIF user is described below:

```
POST /vapix/services HTTP/1.1
<SOAP-ENV:Envelope xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:tds="http://www.onvif.org/ver10/device/wsdl"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:onvif="http://www.onvif.org/ver10/schema"
xmlns:tt="http://www.onvif.org/ver10/schema"
xmlns:SOAP-ENV="http://www.w3.org/2003/05/soap-envelope">
<SOAP-ENV:Body>
<tds:CreateUsers xmlns="http://www.onvif.org/ver10/device/wsdl">
<User>
<tt:Username>admintt:Username>admin>
<tt:Password>admintt:Password>admin>
<tt:UserLevel>Administratortt:UserLevel>Administrator>
</User>
</tds:CreateUsers>
</SOAP-ENV:Body></SOAP-ENV:Envelope>
```

Password strength indicator

Axis devices with AXIS OS 7.20 or higher support a password strength indicator which is visible when creating or modifying a user account password through the web interface. It indicates if the strength of the chosen password is considered weak, medium or strong and also provides advice on how to strengthen the password. The indicator follows the . More information about setting the device password is available in the *AXIS OS Hardening Guide*.



I forgot my password, what to do?

There is no possibility to recover lost or forgotten access credentials to an Axis device. The Axis device needs to be reset to its factory default settings in order to reconfigure it with new access credentials.

Device access logging

In this section you can read about how successful and unsuccessful login attempts are logged in the Axis device's log system depending on the network protocol that is used. At all times, it is recommend to configure a remote syslog server where the Axis

Cybersecurity

device can send its syslogs. This will ensure that the logs can be kept and reviewed for a suitable time and not get erased after e.g. a reboot or factory default of the device itself.

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	<pre>[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]</pre>

FTP

Successful	<pre>[INFO] vftpd[18263]: Accepted request from 172.27.0.3 50333 [INFO] vftpd[18263]: User root logged in.</pre>
Unsuccessful	<pre>[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.</pre>

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.

IP filtering***

Cybersecurity

Unsuccessful	IP_FILTER: IN=eth0 OUT= MAC=ff:ff:f-
	f: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:f-
	f: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.

User management configuration

From AXIS OS 10.9 and onwards, user configuration related changes are logged in the system log and can therefore 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 below table illustrates what log messages to expect when certain changes to the user management configuration are done:

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

Cybersecurity

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

Brute force delay protection

AXIS OS 7.30 or higher

Axis devices running AXIS OS 7.30 and higher can be configured to automatically block HTTP/HTTPS requests coming from a client in the network (IP address). For a certain amount of time, a defined number of authentications fail. This feature can help in avoiding and to protect the Axis device from brute-force attacks, or from network clients that unintentionally imitate a similar behavior. The brute force delay protection can be configured in **Plain config > System**.

AXIS OS 11.5 or higher

With AXIS OS 11.5 or higher, Brute Force delay protection is enabled by default using the configuration example 1 below.

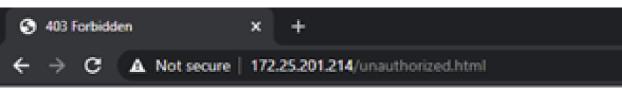
Generally the lower the allowed page/site count is, the more secure the protection. Using Brute force delay protection increases the time to guess a password tremendously. Some indications can be found below. Note that configuring a strong password *is always recommend*.

Condition	Total Brute Force time without delay protection enabled – 720 requests/sec*	Total Brute Force time configuration example 1	Total Brute Force time configuration example 2
4 characters with only lower case letters	+- 11 minutes	+- 6 hours	+- 13 hours
4 characters with upper and lower case letters, and 0 to 9	+- 6 hours	+- 205 hours	+- 410 hours
5 characters with only lower case letters	+- 5 hours	+- 7 days	+- 14 days
5 characters with upper and lower case letters, and 0 to 9	+- 14 days (+- 2 weeks)	+- 1.5 years	+- 3 years

*Actual rate may vary and is depending on product performance.

Trying to access the web interface from the network client that was previously identified as a threat would result in a HTTP 403 Forbidden response.

Cybersecurity



Forbidden

You don't have permission to access this resource.

Furthermore, the Axis device would log the following internally in the system log:

AXIS OS 11.5 and lower	2021-08-16T12:17:35.119+02:00 axis-accc8ed910b9 [WARNING] httpd[592]: [evasive20:warn] [client 172.25.201.116:41972] Blacklisting address 172.25.201.116: possible DoS attack.
AXIS OS 11.6 and higher	2021-08-16T12:17:35.119+02:00 axis-accc8ed910b9 [WARNING] httpd[592]: [evasive20:warn] [client 172.25.201.116:41972] Blocklisting address 172.25.201.116: possible DoS attack.

Parameter Description

Parameter	Description
DOSBlockingPeriod	The blocking period is the amount of time (in seconds) a client will be blocked if they are added to the blocking list. During this time, all subsequent requests from the client will result in a 403 (Forbidden).
DOSPageCount	This is the threshold for the number of requests for the same page (or URI) per page interval. Once the threshold for that interval has been exceeded, the IP address of the client will be added to the blocking list. A page is considered http://ip-address/system/plainconfig.
DOSPageInterval	The interval for the page count threshold; defaults to 1 second intervals.
DOSSiteCount	This is the threshold for the total number of requests for any object by the same client on the same listener per site interval. Once the threshold for that interval has been exceeded, the IP address of the client will be added to the blocking list. A site is considered http://ip-address/
DOSSiteInterval	The interval for the site count threshold; defaults to 1 second intervals.

Cybersecurity

Configuration examples

- Example 1: After 20 failed login attempts within one second, the client IP address gets blocked for 10 seconds. This configuration is the default configuration and offers flexible security where, to some extent, failed login attempts from good-known authorized clients are taken into account.
- Example 2: After 10 failed login attempts within one second, the client IP address gets blocked for 10 seconds. This configuration is recommended for very strict and high security systems where already a few failed login attempts will block a client.

Setting	Example 1	Example 2
Activate Password Throttling	On	On
DoS Blocking Period(sec)	10	10
DoS Page Count(req/DoSPageInterval)	20	10
DoS Page Interval(sec)	1	1
DOS Site Count(req/DoSSiteInterval)	20	10
DoS Site Interval(sec)	1	1

Signed OS

About signed OS

Signed \overline{OS} is a feature that was introduced to ensure that only verified and trusted software is uploaded and used in Axis devices. In this section you can read about technical details that will ensure that the correct update and downgrade paths are selected to avoid issues. For general information about the signed OS feature, see the *Cybersecurity features in Axis products* white paper.

Axis started to sign its software from AXIS OS 8.30.1. Until the release of AXIS OS 9.20.1, devices would still accept both unsigned and signed for backwards compatibility. After the release of AXIS OS 9.20.1, signed OS was fully activated and Axis devices would then only accept software signed by Axis. This means it is not possible to perform a rollback or downgrade to a version below AXIS OS 8.30.1, which is the version where Axis initially started to sign the device software.

- Question: My device runs AXIS OS 9.10.1 and I want to downgrade to AXIS OS 8.40 LTS. Does this work? Answer: Yes, this will work.
- Question: My device runs AXIS OS 9.20.1 and I want to downgrade to AXIS OS 8.20.1 or lower as my VMS requires me this to keep backwards compatibility. Does this work?
 Answer: The downgrade will fail. The unsigned version will be rejected by the device and it will continue to run AXIS 9.20.1. In order to perform such a downgrade, you need to downgrade in two steps using AXIS OS 8.30.1 as a gateway. So first from 9.20.1 -> 8.30.1 -> 8.20.1 or further below. Note that Axis does not encourage downgrades to older, unsupported AXIS OS versions in general.

Signed OS key lifecycle

Signature key pairs are generated on a dedicated offline key generation device. After generation the private key is encrypted with two different asymmetric keys. One for secure import into a cluster of Thales Luna HSMs and another key for long-term offline backup outside the HSM in at two separate secure locations.

The private key is provisioned into the HSM using an administrative role of the HSM that requires M of N authentication. At no point is the private key exposed in plain text during the import.

When Axis signs a AXIS OS image with said key, the signing request is processed by an application server that guards access to the HSM and audits use of the signing key. The application server can only be accessed from inside the Axis network and requires a signing-authorized account.

Revoking of a AXIS OS signing key entails issuing a bootloader update for all Axis devices using that key. As part of the update, the device's anti-rollback mechanism is updated to block older bootloaders which are still accepting the revoked AXIS OS signing keys. Secure destruction of signing keys requires physical destruction of the master backup key that exist in two copies.

Cybersecurity

Troubleshooting

How can you identify that an upgrade did not work because of an unsigned OS? If a user tries to upload an unsigned version, one of the following messages is displayed in the log files of the camera when a device software upgrade fails due to signed OS:

[ERR] fwmgr: Unknown firmware domain [ERR] fwmgr: Image has no signature. [ERR] fwmgr: No custom firmware certificate for camera group 'xxx'.

Signed ACAP applications

Axis takes proactive steps to implement ACAP application signing, aligning with industry best practices for secure software delivery. Additionally, it anticipates potential future enforcement through legislation, including the E.U. Cybersecurity Resilience Act, E.U. Radio Equipment Directive, and Executive Order 14028. Therefore, starting from AXIS OS 12.0 customers will only be able to install signed ACAP applications on Axis devices by default. Installation of unsigned ACAP applications will be possible only and only if a device is actively configured to accept unsigned ACAP applications. Configuring a device to accept unsigned ACAP applications will lower the device's security, but it can be useful during development or if you develop and run your own ACAP application. Running unsigned ACAP applications is not recommended.

What are the benefits for end customers?

A signed ACAP indicates that Axis has a TIP-relationship with the partner who has developed the ACAP. By inspecting the ACAP, the end customer can see who the TIP-partner is. The partner name under the vendor tag is equivalent to the company name in Axis CRM records. Therefore, the signing process ensures the validation of the partner, traceability and accountability. This process enables the end customers to validate their ACAP applications.

What are the benefits in terms of cybersecurity?

The signing process ensures that the ACAP will only require Axis-approved access-rights and privileges when running on the Axis device. An ACAP that went through the signing process, will only run with limited, approved access rights on an Axis device. Furthermore, by signing the ACAP application, it is ensured that the content of the application is not tampered with from release to installation, hence it enables the secure software delivery.

Is Axis vetting the software quality, secure development practices or performing QA-testing on Signed ACAPs?

No, Axis does not take any responsibility for whether a TIP-partner ACAP that went through the signing process is QA-tested, or has been developed according to industry best-practices secure development processes. This responsibility lies entirely on the TIP-partner that is providing an ACAP application.

Who do we allow to have their ACAPs signed?

Only TIP partners are allowed to do so. This indicates that Axis has conducted a vetting process for its partners.

Will Axis provide ACAP signing capabilities for non-TIP partners as well?

For non-TIP partners that require signing capabilities, we will also perform a vetting process. Please use this link to request access.

How does the ACAP signing technically work?

During the ACAP application signing process, a cryptographic signature is added at the end of the application package. The signature is verified by the Axis device when installing the ACAP application as part of the overall secure software delivery architecture.

When will Axis enforce mandatory ACAP signing?

In alignment with secure software delivery practices, Axis will accept only and only Signed ACAP applications without the possibility to disable this security control on its devices. Axis aims to achieve this is the next generation of the AXIS OS operating system which is planned to be *AXIS OS 13.0* in H2 2026 and onwards.

Cryptographic support

A secure keystore is generally referred to as a dedicated hardware crypto computing module that offers protection of cryptographic operations, certificates, and keys. Axis products that support *AXIS Edge Vault* feature up to two secure keystores with corresponding security certification, either Common Criteria CC EAL6+ and/or CC EAL4+ / FIPS 140-2 level 2 certification according to the Federal

Cybersecurity

Information Processing Standard, which could be a regulatory requirement for certain customers and use cases. Both secure keystores offer the same level of protection in terms of cryptographic operations, certificates, and keys. Additionally, some system-on-chips include a so-called Trusted Execution Environment (TEE). Depending on the installation requirements, the TEE might be a good choice due to lower latency for cryptographic operations.

The table below provides an overview of the cryptographic features of keystores found in Axis devices.

Cryptographic feature	Trusted Platform Mod- ule 2.0 (CC EAL4+, FIPS 140-2 level 2)	Secure element (CC EAL6+, FIPS 140-3 level 3)	Trusted Execution En- vironment (SoC TEE)	Software ⁽¹⁾
Dedicated hardware protection of cryptographic operations, certificates and keys	\checkmark	\checkmark	V	
Strongest security	\checkmark	\checkmark		
Fastest performance			\checkmark	\checkmark
Recommended for long-lived keys/certificate	V	V		
Recommended for short-lived keys/certificates			V	V
X.509 certificates in format .PEM, .DER, .CER and .CRT with PKCS#1 formatted private keys	\checkmark	\checkmark	✓	V
PKCS#12 certificate/private key container in .p12 or .pfx format ⁽²⁾	V	V	\checkmark	V
RSA-cryptographic support	V	V	V	V
ECC-cryptographic support	√ ⁽³⁾	√ ⁽⁴⁾	√ ⁽⁴⁾	√ ⁽⁴⁾
Hash algorithms SHA-224/256/384/512	SHA-224/256	SHA-224/256/384/512	SHA-224/256/384/512	SHA-224/256/384/512
Max RSA-crypto private key size uploadable	2048	4096 ⁽⁵⁾	4096	4096
Max ECC-crypto private key size uploadable	ECC NIST P-256	ECC NIST P-256, ECC NIST P-384, ECC NIST P-521	ECC NIST P-256, ECC NIST P-384, ECC NIST P-521	ECC NIST P-256, ECC NIST P-384, ECC NIST P-521
RSA-crypto private key size for self-signed certificate or certificate signing request ⁽⁶⁾	2048	4096	4096	4096
ECC-crypto private key size for self-signed certificate or certificate signing request ⁽⁷⁾	ECC NIST P-256	ECC NIST P-256, ECC NIST P-384, ECC NIST P-521	ECC NIST P-256, ECC NIST P-384, ECC NIST P-521	ECC NIST P-256, ECC NIST P-384, ECC NIST P-521

1. Legacy for products without any hardware protected secure keystore.

Cybersecurity

- 2. Support from AXIS OS 5.50 and higher, Max size of .PFX and .P12 certificate/private key container are limited to 102400 bytes except for devices running AXIS OS 9.20 and lower where only a maximum file size of 10240 bytes is supported.
- 3. The support for ECC was added in AXIS OS 10.10 excluding the following products which need to receive an software update manually: HWID 79C: AXIS Q3527-LVE, HWID 7DA: AXIS Q6074, HWID 7D9: AXIS Q6074-E, HWID 7B1: AXIS Q6075, HWID 7B0: AXIS Q6075-E, HWID 7B2: AXIS Q6075-C, HWID 7B3: AXIS Q6075-S, HWID 7FA: AXIS Q6075-SE and HWID 7C7: AXIS Q9216-SLV.
- 4. ECC cryptography support for Axis devices without TPM module has been added from AXIS OS 10.1 and higher.
- 5. RSA 3072 key length is not supported.
- 6. Max key bit size of private key generated by the Axis device when creating a self-signed certificate (SSC) or issuing a certificate signing request (CSR). During the very first boot, the Axis device will generate a self-signed certificate automatically, which prior to AXIS OS 10.1 had a private key bit size of 1536-bit. Starting with AXIS OS 10.1 and higher, the size is 2048-bit.
- 7. Support from AXIS OS 11.6 or higher.

Certificate management

Default device certificate

Axis devices contain a certificate to allow for encrypted HTTPS and other secure connections in order to provide the possibility to access the device securely and proceed with the initial configuration of the device. Depending on the hardware capabilities of the Axis product and which AXIS OS version it is running, different default configuration applies.

Self-Signed Certificate

Axis products with support for TPM module or Software keystore only generate a self-signed certificate during first-boot up. Axis devices come with a pre-installed self-signed certificate in order to provide the possibility to access the device via encrypted HTTPS connection and proceed with the initial setup of the device. Since the first-boot certificate is self-signed by the device, it is not suitable for providing authentication or authenticity against networks and applications. Therefore, Axis recommends removing the self-signed certificate from the device and replace it with a server certificate that is trusted in your organization when HTTPS connection is the preferred type of connection to the device.

Axis device ID (IEEE 802.1AR)

Axis devices equipped with Axis Edge Vault are provisioned with an Axis device ID. The Axis device ID conforms with the IEEE 802.1AR standard and can be verified using the Axis device ID certificate chain. ou can download and find more information about the Axis device ID certificate chain in our *Public Key Infrastructure Repository*. Remember to verify the downloaded certificates against the provided sha256 hash before using the Axis device ID CA certificates as a trust anchor.

Axis root certificate	Integrity checksum SHA256
Axis device ID Root CA ECC	32ca2dc3230764f2d638b54d2826c050613266162932a2d7e7 66f81a51e3aa60
Axis device ID Intermediate CA ECC 1	e7a2fe5d9eb7af9d2ad45a432621389fc50362b62e482c0396 9ca5e3e3c114a4
Axis device ID Intermediate CA ECC 2	2df287bda13db287f6e177a0ac666e3087de9c39e93d4dafb0 74e0ca944b0d45
Axis device ID Root CA RSA	fc1a8b0d6585dc74215bcc4e87e852af9258637062d0fc4c41 7554a6f1b5a85e
Axis device ID Intermediate CA RSA 1	6b5da02ed3feb18ab787c3dfe2a32a311cf93852733e6ebe46 3f3ec33d45a89d
Axis device ID Intermediate CA RSA 2	c02a61b0448ab245994d7d81b5ae50253424a4cd930426172e- 5f0d89598b69a6

CA certificates

CA certificates are certificates used by the Axis device to validate/verify the authenticity of other servers in the network. This means that CA certificates that are going to be uploaded in the CA certificate section of the Axis device need to fulfill one of the following:

Cybersecurity

- X509v3 CA certificate with basicConstraints extension CA:TRUE*
- X509 v1 self-signed certificate
- The keyUsage attribute extension with bit keyCertSign set but without basicConstraints
- Netscape Certificate Type extension saying that it is CA certificate

*The CA:TRUE or CA:FALSE attribute also decides whether the CA certificate is allowed to sign other certificates.

Note

Installing a concatenate certificate file that contains the whole certificate chain is not currently supported. You should install the intermediate CA certificate and CA certificate separately.

Certificate signing request (CSR)

A certificate signing request (CSR) can be created from an already existing certificate in the Axis device. The certificate request in PEM format can be sent to a certificate authority (CA) for signing/verifying. After the signed certificate is returned from the CA, it needs to be uploaded on the Axis device and be compared/verified with the original certificate request. If all information is correct, the certificate upload will end successfully. However, if system changes occur between the time the CSR was issued and the certificate was uploaded, the process can be interrupted. Possible reasons why a certificate upload would fail are:

- The Axis device has been factory defaulted in the meantime
- The certificate used for the signing request has been removed or changed in the Axis device

Default HTTP(S) headers

AXIS OS by default has the following most common security-related HTTP(S) headers enabled to increase overall minimum cybersecurity in factory defaulted state. The custom HTTP header VAPIX API can be used to configure further HTTP(S) headers. For more information, see the *Vapix Library*.

AXIS OS 10.1 and higher

With AXIS OS 10.1 or higher, the below default HTTP(S) headers have been introduced to increase overall minimum cybersecurity level:

Header	Values	Description
X-Frame-Options	SAMEORIGIN	This specifies that the page can only be embedded in a frame on the same domain as the page itself.
X-Content-Type-Options	nosniff	This value instructs the browser to not interpret files with an unknown MIME type as a different content type. For example, if a server sends an HTML file with a .jpg extension, the browser will not treat it as an image but instead will display it as text.
X-XSS-Protection	1; mode=block	This value instructs the browser to enable its built-in XSS protection feature.

AXIS OS 11.5 - 11.11

With AXIS OS 11.5 – 11.11, a Content-Security-Policy (CSP) HTTP(S) response header is added in addition to specify a policy that tells the browser which sources of content can be trusted for the Axis device. This header can be used to protect against various types of attacks, including cross-site scripting (XSS) and data injection attacks.

When a browser receives a web page, it checks the CSP header to determine which sources of content are allowed to be loaded for that page. If any content is attempted to be loaded from a source that is not on the list, the browser will block it.

Directive	Values	Description
default-src	'self'	This specifies the default sources from which resources are allowed to be loaded if not explicitly specified.

Cybersecurity

frame-ancestors	'self'	This specifies the sources from which frames or iframes can be loaded on the page.		
connect-src	'self' https://*.google-analytics.com https://*.analytics.google.com https://*.googletagmanager.com https://*.axis.com mediastream: blob:	This specifies the sources to which the page can make network requests.		
script-src	'self' 'unsafe-inline' 'unsafe-eval' https://www.googletagmanager.com https://*.google-analytics.com https://ssl.google-analytics.com https://*.axis.com	This specifies the sources from which JavaScript code can be loaded and executed on the page.		
style-src	'self" 'unsafe-inline'	This specifies the sources from which styles can be loaded and applied on the page.		
img-src	'self' https://*.analytics.google.com https://www.googletagmanager.com https://*.axis.com data: blob:	This directive guards the loading of images (for example using the HTML tag).		
media-src	'self' mediastream: blob:	This specifies the sources from which audio and video can be loaded on the page		
object-src	'none'	This specifies valid sources for the <i><object></object></i> , <i><embed/></i> , and <i><applet></applet></i> elements.		

In addition to the CSP, a Referrer-Policy header is added. HTTP requests may include the optional Referrer header, which indicates the origin or web page URL the request was made from. The Referrer-Policy header defines what data is made available in the Referrer header.

Header	Values	Description	
Referrer-Policy	strict-origin-when-cross-origin	With this policy, only the origin is sent in th be accessible from other parts of the full U	

AXIS OS 12.0 and higher With AXIS OS 12.0 and higher, the default Content-Security-Policy (CSP) HTTP(S) response header has been updated.

Directive	Values	Description
default-src	'self'	This specifies the default sources from which resources are allowed to be loaded if not explicitly specified.
frame-ancestors	'self'	This specifies the sources from which frames or iframes can be loaded on the page.

Cybersecurity

connect-src	'self' https://*.google-analytics.com https://*.analytics.google.com https://*.googletagmanager.com https://*.axis.com mediastream: blob:	This specifies the sources to which the page can make network requests.
script-src	'self' https://www.googletagmanager.com https://*.google-analytics.com https://ssl.google-analytics.com https://*.axis.com	This specifies the sources from which JavaScript code can be loaded and executed on the page.
style-src	'self' 'unsafe-inline'	This specifies the sources from which styles can be loaded and applied on the page.
img-src	'self' https://*.analytics.google.com https://www.googletagmanager.com https://*.axis.com data: blob:	This directive guards the loading of images (for example using the HTML tag).
media-src	'self' mediastream: blob:	This specifies the sources from which audio and video can be loaded on the page
object-src	'none'	This specifies valid sources for the <i><object></object></i> , <i><embed/></i> , and <i><applet></applet></i> elements.

Decommissioning

When decommissioning an Axis device, a factory default should be performed. After the factory default, most data is erased by overwriting/sanitization. For more information, go to AXIS OS Hardening Guide.

Media streaming

Media streaming

Video streaming in Axis products

The purpose of this section is to encourage and enable partners, system integrators and end users to consider their individual setup when configuring general video streaming settings in Axis devices in order to ensure optimal performance and user experience.

General considerations

Axis video capable devices deliver a video stream according to the desired requirements of the system it is used in and according to the specifications of the Axis device itself. The following information provides a foundation and understanding of how video streaming in Axis devices works and what settings to consider.

About video streaming clients

The Axis device as such recognizes several types of clients that it encodes and distributes video streams to. The clients can be categorized as *internal* and *external*, and they are served with video streams as they are requested. See examples below for each category:

Internal clients

- Action rule for (S)FTP/HTTP(S) MJPEG image upload
- Action rule for (S)FTP/HTTP(S) video clip upload
- Action rule for recording videos to SD card and network share
- Continuous recording to SD card or network share
- (Analytics) ACAPs that request video stream or MJPEG images

External clients

- Viewing video in web interface
- Viewing video via secure remote access
- Live view and recording to AXIS Companion
- Live view and recording to AXIS Camera Station
- Live view and recording to 3rd party video management system

Unique encoded streams

The number of unique encoded streams tells us how many different video streams an Axis device is encoding. This information can be obtained in the server report of devices with version 5.70 or higher in the section **Snapshot of the current (caching) streams**. For devices with AXIS OS version 10.7 or higher, this information is available in the section **Snapshot of all running streams**. The number of unique encoded streams are affected by stream properties, as will be shown in the examples below. Note that the illustrations are taken from a graphical user interface to better illustrate the use case.

Example 1: In this example, the Axis device is encoding a total number of three unique encoded video streams. The video streams differ in one stream property – resolution – and since the resolution is different, the Axis device needs to encode each video stream separately.

Туре	Resolution	FPS	Compression	VideoKeyFrameInterval	VideoZStrength	Rotation
Stream 1: video/x-h264	1920x1080	30	30	62	10	0
Stream 2: video/x-h264	1280x720	30	30	62	10	0
Stream 3: video/x-h264	800x600	30	30	62	10	0

Media streaming

Example 2: In this example, the Axis device is encoding a total number of two unique encoded video streams. The video streams differ in one stream property – frame rate (fps) – and since the frame rate is different, the Axis device needs to encode each video stream separately.

Туре	Resolution	FPS	Compression	VideoKeyFrameInterval	VideoZStrength	Rotation
Stream 1: video/x-h264	1920x1080	30	30	62	10	0
Stream 2: video/x-h264	1920x1080	15	30	62	10	0

<u>Conclusion</u>: Axis devices need to encode video streams according to their stream properties. If stream properties, such as fps, compression, VideoKeyFrameInterval (GOP), etc. differ from one requested video stream to another, the Axis device is forced to encode separate video streams. This may have an impact on video streaming performance and generally it is recommended to optimize the setup towards the least amount of video streams possible.

<u>Note</u>: From AXIS OS 10.8 and onwards a single unique encoded video stream can be distributed to a maximum of eight physical network clients at the same time. If more physical network clients need to pull the same video stream, we suggest implementing multicast video streaming instead, or to have additional clients request another unique encoded video stream.

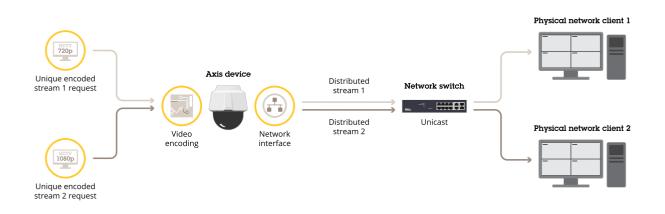
Distributed streams

The number of distributed video streams refers to the number of actual physical network clients in the network and the number of video streams that they are requesting. For example, it would be possible to video stream from AXIS Camera Station and from the web interface of the Axis device from the same physical network client.

This information can be obtained in the server report of devices with version 9.80 and higher in the section **Snapshots of the current outgoing RTP streams**. This section lists the number of distributed streams in relation to their destination IP address. The distributed stream is declared as a ratio of *Number of video streams:Number of physical network clients*.

Example 1: In this example, the number of distributed streams is 2:2 because the Axis device streams in total two video streams to two physical network clients.

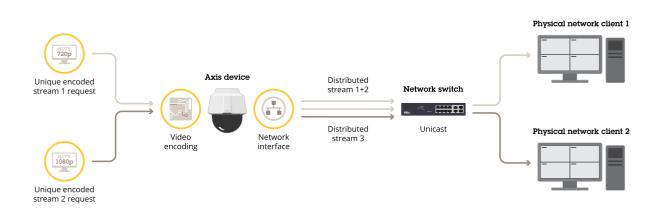
↑ ID	# Mime	Source	Destination	Transport	Stream	Media	State	Construction in the second	# Multicast
8	video/x-h264	172.25.201.154:64322	172.25.201.201:50000	UDP	RTP	VIDEO	PLAYING	No	No
9	video/x-h264	172.25.201.154:62832	172.25.201.202:50002	UDP	RTP	VIDEO	PLAYING	No	No



Media streaming

<u>Example 2</u>: In this example, the number of distributed streams is 3:2 because the Axis device streams in total three video streams to two physical network clients. Observe that the **Physical network client 1** is requesting the **Unique encoded stream 1** twice.

↑ ID	# Mime	Source	Destination	Transport	Stream	Media	State	Encrypted	# Multicast
8	video/x-h264	172.25.201.154:64322	172.25.201.201:50000	UDP	RTP	VIDEO	PLAYING	No	No
9	video/x-h264	172.25.201.154:62832	172.25.201.202:50002	UDP	RTP	VIDEO	PLAYING	No	No
10	video/x-h264	172.25.201.154:54324	172.25.201.202:50004	UDP	RTP	VIDEO	PLAYING	No	No



<u>Conclusion</u>: An Axis device can stream a single or many video streams to either the same or many physical network clients. A physical network client is defined by the number of video streams it is requesting and its destination IP address in the network.

<u>Note</u>: From AXIS OS 10.8 and onwards a single unique encoded video stream can be distributed to a maximum of eight physical network clients at the same time. If more physical network clients need to pull the same video stream, we suggest implementing multicast video streaming instead, or to have additional clients request another unique encoded video stream.

Unique encoded streams and distributed streams

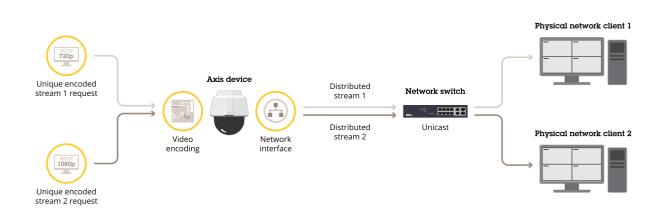
With the information above, we can now explain the relation between the number of unique encoded streams in relation to the number of distributed streams to physical network clients.

Example 1: In this example, two physical network clients are requesting a unique encoded stream each. This results in a distributed stream to each physical network client.

Туре	Resolution	FPS	Compression	VideoKeyFrameInterval	VideoZStrength	Rotation
Stream 1: video/x-h264	1920x1080	30	30	62	10	0
Stream 2: video/x-h264	1920x1080	15	30	62	10	0

↑ ID	# Mime	Source	Destination	Transport	Stream	Media	State	Encrypted	# Multicast
8	video/x-h264	172.25.201.154:64322	172.25.201.201:50000	UDP	RTP	VIDEO	PLAYING	No	No
9	video/x-h264	172.25.201.154:62832	172.25.201.202:50002	UDP	RTP	VIDEO	PLAYING	No	No

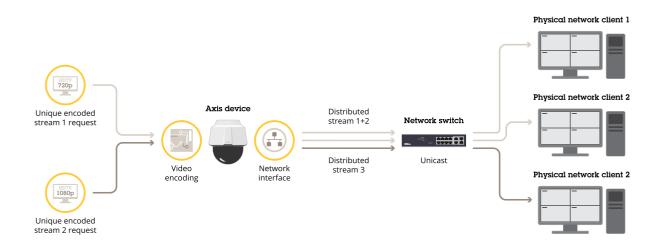
Media streaming



Example 2: In this example, the Axis device is encoding two unique streams and distributes them to three physical network clients.

Туре	Resolution	FPS	Compression	VideoKeyFrameInterval	VideoZStrength	Rotation
Stream 1: video/x-h264	1920x1080	30	30	62	10	0
Stream 2: video/x-h264	1920x1080	15	30	62	10	0

<mark>↑</mark> ID	# Mime	Source	Destination	Transport	Stream	Media	State	Encrypted	# Multicast
8	video/x-h264	172.25.201.154:64322	172.25.201.201:50000	UDP	RTP	VIDEO	PLAYING	No	No
9	video/x-h264	172.25.201.154:62832	172.25.201.202:50002	UDP	RTP	VIDEO	PLAYING	No	No
10	video/x-h264	172.25.201.154:54324	172.25.201.203:50004	UDP	RTP	VIDEO	PLAYING	No	No



Media streaming

Example 3: In this example, the Axis device is encoding a single unique stream and distributes it to two physical network clients via multicast. Observe that this setup would result in a single distributed stream only as the two physical network clients will receive the stream from the multicast address. So, multicast has the advantage of consuming less network bandwidth compared to example 4 below.

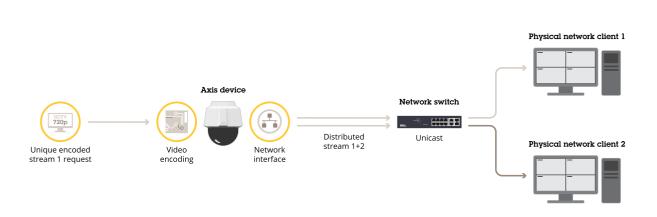
Туре		Resolution	FPS	Compre	ssion	VideoKey	FrameInter	al Vide	oZStrength	Rotation
Stream 1: video	o/x-h264	1920x1080	30	30	(62		10		0
▲ ID		≎ Des	tination	1	Transp	ort 😄 Stre	am 💠 Media	≑ State	Encrypted	≑ Multicast
8 video/x-h264	172.25.20	1.154:0 239.20	8.128.2	35:50000	UDP	RTP	VIDEO	PLAYING	No	Yes
Unique encoded stream 1 request		Axis o Video encoding		Network interface	Distril strea		Network switch			etwork client 1

Example 4: In this example, the Axis device is encoding a single unique stream and distributes it to two physical network clients via unicast instead. Compared to example 3, this setup would require the Axis device to consume more network bandwidth as the unique stream has to be distributed twice.

Туре	Resolution	FPS	Compression	VideoKeyFrameInterval	VideoZStrength	Rotation
Stream 1: video/x-h264	1920x1080	30	30	62	10	0

↑ ID	# Mime	Source	Destination	Transport	Stream	Media	State	Encrypted	# Multicast
8	video/x-h264	172.25.201.154:64322	172.25.201.201:50000	UDP	RTP	VIDEO	PLAYING	No	No
9	video/x-h264	172.25.201.154:62832	172.25.201.202:50002	UDP	RTP	VIDEO	PLAYING	No	No

Media streaming



Maximum number of clients

Another important setting is the maximum number of clients (=viewers) that can receive a video stream. The number is set to 10 or 20 in all Axis devices and is depending on the configuration and performance capabilities of the device.

This means that either the Axis device is delivering a single video stream to 10 or 20 different physical clients in the network, or the Axis device is delivering 10 or 20 different video streams to one client in the network. The number of receiving video clients (physical and software instances) is the main limit. This configuration can be obtained by reading out the following VAPIX parameter: https://ip-address/axis-cgi/param.cgi?action=list&group=Image.MaxViewers

In practice, the maximum number should never be reached at any point. If an increasing number of clients need to access the video stream, it is recommended to make use of e.g. multicast.

Video, audio and metadata

In *Maximum number of clients on page 26*, we learned that there is a limit to how many video streams a device can deliver as a maximum, and we explained this with the number of video streams. In addition to video streams, Axis devices can also deliver audio and metadata streams. While the purpose of video and audio streams is self-explanatory, the purpose of metadata might not be. With a metadata stream, an application or VMS can listen to the Axis device's event stream and both react on it and create its own events and actions in return.

Below is an example of an Axis device that is currently streaming one of each stream type to a single physical network client. Observe which stream type is streamed under Media.

<mark>↑</mark> ID	\$ Mime	Source	Destination	Transport	\$ Stream	# Media	\$\$ State	Encrypted	# Multicast
24	video/x-h264	172.25.201.190:0	172.25.201.50:64959	TCP	RTP	VIDEO	PLAYING	No	No
25	audio/mpeg	172.25.201.190:0	172.25.201.50:64959	TCP	RTP	AUDIO	PLAYING	No	No
26	application/x-onvif-metadata+xml	172.25.201.190:0	172.25.201.50:64959	TCP	RTP	METADATA	PLAYING	No	No

To summarize, the maximum number of clients is applied to video, audio and metadata streams separately, meaning that if the parameter **MaxViewers** is configured to 20, the Axis device can deliver 20 x video, 20 x audio and 20 x metadata streams in total.

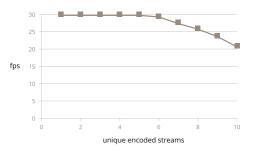
Performance considerations and maximum bitrate

Performance considerations

While it's possible for an Axis device to encode multiple video streams simultaneously, this will at some point have an impact on the performance if "too many" unique video streams are encoded. In the example illustration below, you can observe that the Axis device can deliver five unique video streams in full frame rate of 30 fps. In case a sixth unique video stream needs to be encoded, the performance of the product will be exceeded, causing the Axis device to deliver all of the requested video streams equally in reduced

Media streaming

frame rate. In case of exceeding the performance of the product, the Axis device will not prioritize any of the video streams to be delivered in full fps, instead it will distribute the performance bottleneck across all video streams.



Note that the above example is an oversimplified illustration and the number of concurrent video streams an Axis device can deliver in full frame rate is heavily dependent on a lot of factors, such as requested frame rate, resolution, compression, bitrate and many more. It's recommended to test the device against the desired behavior in an environment that is exact, or close to, the environment the device is installed in.

Maximum video stream bitrate

A typical H.264 video stream in 1080p and 30 fps will have a bitrate of approximately 1 Mbit/s to 10 Mbit/s depending on scene, lighting conditions, movement and many other factors. In order to avoid network bottlenecks and congestion of the underlying network infrastructure which the Axis device is connected to, the maximum bitrate of a video stream is hard-capped and cannot exceed 50 Mbit/s per video stream in total.

Video source buffer configuration

In addition to the above information, the below listed Axis devices have additional video buffer configurations that must be considered. These devices have a limited number of statically configured so called *video source buffers*. The number of video source buffers depends on the device.

For single-sensor products the video source buffer can deliver at least one unique video stream, and for multi-sensor products the video source buffer can deliver at least four unique video streams. So, Axis devices containing video source buffer configurations are limited by the amount of unique video streams they can provide.

Products released before 2022

In Axis devices released before 2022, there are a maximum of four video source buffers.

- Main source buffer: The main source buffer is statically configured to the device's maximum default resolution and can only deliver a unique video stream in that specific resolution. This is indicated by the "fixed" term.
- **2nd source buffer**: The 2nd source buffer is a low resolution video buffer suitable for applications that rely on a lower sized resolution, such as (analytics) ACAP's or motion jpeg image. This buffer provides variations of possible resolutions.
- **3rd source buffer**: The 3rd source buffer is a high resolution video buffer providing either the device's maximum resolution, or a resolution close to it. In addition to that, HDMI capable devices allocate the 3rd source buffer HDMI video streaming when enabled. This buffer provides variations of possible resolutions.
- **4th source buffer**: The 4th source buffer is a high resolution buffer providing either the device's maximum resolution or a resolution close to it. This buffer provides variations of possible resolutions.

Products released in 2022 and onwards

In Axis devices released in 2022 and onwards, there are at least four video source buffers available for encoded video such as H26X and MJPEG. HDMI will not affect the available number of source buffers for encoded video. ACAPs (typically analytics applications) that fetches YUV will not affect the available number of source buffers for encoded video.

• Fixed source buffer (Main): The fixed source buffer is statically configured to the device's maximum default resolution and can only deliver a unique video stream in that specific resolution. This is indicated by the "fixed" term.

Media streaming

- **2nd source buffer**: The 2nd source buffer is a low resolution video buffer suitable for applications that rely on a lower sized resolution motion JPEG image. This buffer provides variations of possible resolutions.
- Nth source buffer: The Nth source buffer is a high resolution video buffer. This buffer provides variations of possible resolutions.

Example illustration

Axis device	Main source buffer	2nd source buffer	3rd source buffer	4th source buffer
AXIS Q6125-LE	Fixed 1920x1080	320x240 to 720x576	320x240 to 1920x1080	320x240 to 1280x960

In summary, this device can deliver 2 x unique video streams in max 1920×1080 resolution — one in max 1280×960 and one in 720×576 . As described in *Unique encoded streams on page 21*, the information in the server report can help identifying which of the video source buffers that are already used and saturated, and which are still available.

<u>Example 1</u>: In this example, the Axis device is delivering the following unique video streams which means the Main, 3rd and 4th video source buffers are in use. Requesting e.g. another unique video stream in 1920x1080 resolution with fps = 15 would fail because no video source buffer is available to deliver this request.

Туре	Resolution	FPS	Compression	VideoKeyFrameInterval	VideoZStrength	Rotation
Stream 1: video/x-h264	1920x1080	30	30	62	10	0
Stream 2: video/x-h264	1280x720	30	30	62	10	0
Stream 3: video/x-h264	800x600	30	30	62	10	0

<u>Example 2</u>: In this example, the Axis device is delivering the following unique video streams which means the Main and 3rd video source buffer are in use. Requesting e.g. another unique video stream in 1920x1080 resolution with fps = 15 would fail because no video source buffer is available to deliver this request. Requesting a unique video stream buffer in 800x600 resolution can however be delivered by the 4th source buffer.

Туре	Resolution	FPS	Compression	VideoKeyFrameInterval	VideoZStrength	Rotation
Stream 1: video/x-h264	1920x1080	30	30	62	10	0
Stream 2: video/x-h264	1920x1080	15	30	62	10	0

Axis device specifics

Below are all Axis devices and their video source buffer configurations listed:

Axis device	Main source buffer	2nd source buffer	3rd source buffer	4th source buffer
AXIS 18116-E	Fixed 2592x1944	320x240 to 640x480 ^{*****}	320x240 to 1920x1080 ^{*****}	320x240 to 1920x1080 ^{*****}
AXIS M1025 AXIS M3005-V AXIS M3025-VE	Fixed 1920x1080	320x240 to 720x576	320x240 to 1920x1080	320x240 to 1280x720
AXIS M1004-W AXIS M1014 AXIS M1034-W AXIS M3004-V AXIS M3024-LVE	Fixed 1280x800	320x240 to 720x576	320x240 to 1440x900	320x240 to 1280x720

Media streaming

AXIS M1013 AXIS M1033-W AXIS M1143-L	Fixed 800x600	320x240 to 720x576	320x240 to 800x600	320x240 to 800x600
AXIS M3046-V 2.4 mm	Fixed 2688x1520 Fixed 2560x1440	320x240 to 720x576	HDMI: 1080p 320x240 to 1920x1080	320x240 to 1280x720
AXIS M1045-LW AXIS M1065-L/-LW AXIS M3045-V/-WV	Fixed 1920x1080	320x240 to 720x576	HDMI: 1080p 320x240 to 1920x1080	320x240 to 1280x720
AXIS M3044-V/-WV	Fixed 1280x720	320x240 to 720x576	<i>No HDMI</i> 320x240 to 1280x720	320x240 to 1280x720
AXIS M2026-LE AXIS M2026-LE Mk II AXIS M3106-L/-LVE AXIS M3106-L/-LVE Mk II	Fixed 2688x1520	320x240 to 720x576	<i>No HDMI</i> 320x240 to 1920x1080	320x240 to 1280x960
AXIS M3046-V 1.8 mm	Fixed 2304x1296 (16:9) Fixed 2016x1512 (4:3)	320x240 to 720x576	HDMI: 1080p 320x240 to 1920x1080	320x240 to 1280x960
AXIS M4206-V/-LV	Fixed 2048x1536	320x240 to 720x576	HDMI: 1080p 320x240 to 1920x1080	320x240 to 1280x960
AXIS M4215-V/-LV	Fixed 1920x1080	320x240 to 640x360*****	320x240 to 1920x1080*****	320x240 to 1920x1080*****
AXIS M4216-V/-LV	Fixed 2304x1728 (4:3)	320x240 to 640x480*****	320x240 to 1920x1080*****	320x240 to 1920x1080*****
	Fixed 2304x1296 (16:9)	320x240 to 640x360*****	320x240 to 1920x1080*****	320x240 to 1920x1080*****
AXIS M3016 AXIS M3066-V AXIS M3206-LVE	Fixed 2304x1728 Fixed 2304x1296	320x240 to 720x576	HDMI: 1080p 320x240 to 1920x1080	320x240 to 1280x960
AXIS M3015 AXIS M3065-V AXIS M3075-V AXIS M3205-LVE AXIS Q9216-SLVE	Fixed 1920x1080	320x240 to 720x576	HDMI: 1080p 320x240 to 1920x1080	320x240 to 1280x960
AXIS M3064-V	Fixed 1280x720	320x240 to 720x576	<i>No HDMI</i> 320x240 to 1280x720	320x240 to 1280x720
AXIS M3047-P*	Fixed 2048x2048	480x480 to 720x720	HDMI: 720p 480x480 to 2048x2048	480x480 to 720x720
AXIS M3048-P*	Fixed 2880x2880	480x480 to 720x720	HDMI: 720p 480x480 to 2880x2880	480x480 to 720x720
AXIS Q6125-LE	Fixed 1920x1080	320x240 to 720x576	320x240 to 1920x1080	320x240 to 1280x960
AXIS P1428-E** AXIS Q6128-E**	Fixed 3840x2160	240x135 to 640x480	480x270 to 1280x720	240x135 to 1920x1080
AXIS Q6010-E*** AXIS Q6100-E***	Fixed 2592x1944	320x240 to 1280x960	320x240 to 1920x1080	Not available
AXIS P3719-PLE****	Fixed 2560x1440	Fixed 640x360	640x360 to 1920x1080	Fixed 2560x1440
AXIS M2035-LE	Fixed 1920x1080	320x240 to 640x360*****	320x240 to 1920x1080*****	320x240 to 1920x1080*****

Media streaming

AXIS M2036-LE	Fixed 2304x1728 (4:3)	320x240 to 640x480 ^{*****}	320x240 to 1600x1200*****	320x240 to 1600x1200*****
	Fixed 2688x1512 (16:9)	320x240 to 640x360*****	320x240 to 1920x1080*****	320x240 to 1920x1080*****
AXIS M3085-V	Fixed 1920x1080	320x240 to 640x360*****	320x240 to 1920x1080*****	320x240 to 1920x1080*****
AXIS M3086-V	Fixed 2688x1512 (16:9)	320x240 to 640x360*****	320x240 to 1920x1080***	**320x240 to 1920x1080***
	Fixed 2304x1728 (4:3)	320x240 to 640x360*****	320x240 to 1920x1080*****	320x240 to 1920x1080*****
AXIS M3088-V	Fixed 3840x2160	320x240 to 640x360*****	320x240 to 1920x1080*****	320x240 to 1920x1080*****
AXIS M1055-L	Fixed 1920x1080	320x240 to 640x360*****	320x240 to 1920x1080*****	320x240 to 1920x1080*****
AXIS M1075-L	Fixed 1920x1080	320x240 to 640x360*****	320x240 to 1920x1080*****	320x240 to 1920x1080*****
AXIS P3905-R Mk III	Fixed 1920x1080 Fixed 1280x720	320x240 to 720x576	320x240 to 1920x1080 320x240 to 1280x720	320x240 to 1280x960 320x240 to 1280x720
AXIS M3905-R	Fixed 1920x1080 Fixed 1280x720	320x240 to 720x576	320x240 to 1920x1080 320x240 to 1280x720	320x240 to 1280x960 320x240 to 1280x720

* The resolutions are only for fisheye overview and differ for other dewarped view modes. When pulling view area 1 & 2 with the same resolution on AXIS M3047-P and AXIS M3048-P, this will work either by using the highest resolution (1920x1440) or with lower resolutions like 640x480 and 480x360.

** Each source buffer can deliver two video streams in the corresponding resolution. Example: either 4x1080p in total with 2x1080p delivered from the main source buffer and 2x1080p delivered from the 4th source buffer, or 2x4K delivered from the main source buffer and 2x1080p delivered from the 4th source buffer.

*** The device is a multi-sensor device with 4 physical sensors, which translates to each buffer being able to deliver one video stream per physical sensor. Example: 1 x video stream in 2592x1944 resolution per sensor on AXIS Q6010-E makes it a total of 4 video streams on the main source buffer.

**** The 4th source buffer is allocated for quad-view only, so this means that the 4th source buffer cannot be utilized further even if quad-view is not used.

 $\star\star\star\star\star$ These video source buffers are capable of providing two unique video streams per buffer instead of just a single one.

Troubleshooting

You may refer to each device's release notes for all the supported resolutions. You will also notice the following line in the release notes for devices with hardware limitations: "5.40.5:L35026 Number of different configured video streams are limited by hardware".

A typical first hand indication that the Axis device cannot provide additional unique video streams as the video source buffers are already exceeded is the "503 Service Unavailable" error message in the web interface of the Axis device.

Other applications, like AXIS Companion or AXIS Camera Station, would show the user a "Camera error". The Server report and included log messages of Axis devices are an excellent tool to debug this kind of scenarios.

Below you can find a list of some common log messages that would appear in case the video source buffer is saturated and the Axis device is not being able to deliver a requested unique video stream

<u>Troubleshooting example 1</u>: In this example, requesting a unique video stream has failed due to there simply not being any video source buffer available to facilitate another unique 1024x768 video stream. The log messages indicate which source buffer is already occupied and which is still available to use at the time when the new unique video stream is requested.

```
<INFO> Jan 4 11:22:03 axis-00408cdc12b7 /usr/bin/ambad[960]: Unable to find available
stream configuration for resolution 1024x768
<INFO> Jan 4 11:22:03 axis-00408cdc12b7 /usr/bin/ambad[960]: buffer[0]: fixed
1920x1080, current 1920x1080
<INFO> Jan 4 11:22:03 axis-00408cdc12b7 /usr/bin/ambad[960]: buffer[1]: max 720x576,
```

Media streaming

current 0x0
<INFO> Jan 4 11:22:03 axis-00408cdc12b7 /usr/bin/ambad[960]: buffer[2]: max
1920x1080, current 1280x960
<INFO> Jan 4 11:22:03 axis-00408cdc12b7 /usr/bin/ambad[960]: buffer[3]: max
1280x720, current 0x0
<INFO> Jan 4 11:22:03 axis-00408cdc12b7 /usr/bin/ambad[960]: Failed to allocate a
source buffer

<u>Troubleshooting example 2</u>: Like in the example above, requesting a unique video stream has failed due to there not being any video source buffer available to facilitate another unique 800x600 video stream.

```
<INFO> Jan 4 11:22:03 axis-0040 /usr/bin/ambad[960]: Unable to find available stream
configuration for resolution 800x600
<INFO> Dec 30 21:15:36 axis408 /usr/bin/ambad[1051]: buffer[0]: fixed 800x600,
current 800x600
<INFO> Dec 30 21:15:36 axis408 /usr/bin/ambad[1051]: buffer[1]: max 720x576, current
0x0
<INFO> Dec 30 21:15:36 axis408 /usr/bin/ambad[1051]: buffer[2]: max 800x600, current
800x600
<INFO> Dec 30 21:15:36 axis408 /usr/bin/ambad[1051]: buffer[3]: max 800x600, current
800x600
<INFO> Dec 30 21:15:36 axis408 /usr/bin/ambad[1051]: buffer[3]: max 800x600, current
800x600
<INFO> Dec 30 21:15:36 axis408 /usr/bin/ambad[1051]: Failed to allocate a source
buffer
```

<u>Troubleshooting example 3</u>: Axis devices with newer AXIS OS versions print their log message in a slightly different manner, as seen in this example.

```
[ INFO ] /usr/bin/ambad[1035]: Failed to allocate a source buffer (1280x720, channel
1): No matching buffer available
[ INFO ] /usr/bin/ambad[1035]: stream[1]: encoding [ 1920x1080, 25/1 fps, buffer_id
2, state active, channel 1 ]
[ INFO ] /usr/bin/ambad[1035]: stream[2]: encoding [ 640x480, 25/1 fps, buffer_id 3,
state active, channel 1 ]
[ INFO ] /usr/bin/ambad[1035]: stream[3]: encoding [ 320x240, 25/1 fps, buffer_id 1,
state active, channel 1 ]
[ WARNING ] monolith: Failed to allocate 1280x720 H264 stream on channel 1: Failed
to allocate stream resources: Failed to add stream
[ ERR ] monolith[925]: Could not set caching pipeline to playing.
```

Recommendations

The following general recommendations can be given to reduce complexity, configuration time and to optimize the video streaming setup of Axis devices:

- Make use of stream profiles to package streams and their configuration in a simple way to optimize stream and configuration handling
- · Action rules that upload MJPEG images or video clips should utilize user-configured stream profiles
- Use the same stream settings (=stream profile) for live view and recording if possible
- Have in mind that action rules allocate a video source buffer once the action rule is activated. This means that even though the Axis device is supposed to send an image to an FTP server once a day, it will result in the video source buffer being allocated for the entire day
- Have in mind that (Analytics) ACAPs such as AXIS Video Motion Detection or 3rd party ACAPs may consume a low resolution buffer for detection, such as 320x240
- Have in mind that the "Adaptive Resolution/Streaming" feature enabled per default when accessing the Axis device's web interface will request a unique video stream tailored to the actual resolution size of the physical display of the user. This might consume a video source buffer by itself

Media streaming

- Avoid having anonymous viewers enabled. Besides the aspect of cybersecurity, having anonymous viewers enabled allows the uncontrolled access to an Axis device and may exceed the video source buffer configurations
- Avoid questionable setups such as requesting two unique video streams in the same resolution, framerate but with different compression, like 30 and 35. The difference in image quality is negligible compared to the cost of consuming a video source buffer

Video latency

The time from an actual event happens until it's displayed on the client's screen is called latency. The latency includes processing of the image in the camera, transmission over the network, and decompression on the client. More information about latency can be found *here*. In some circumstances, it is desired to keep this latency as low as possible. To reduce the processing time on the camera, there are a few possibilities. Note that these settings will affect all video streams.

- Choose a capture mode with higher frame rate. In high frame rate capture modes, the processing is usually performed faster than in low frame rate capture modes.
- Enable LowLatencyMode (Settings > Plain config > Select group: ImageSource > ImageSource / IO / Sensor > Low latency mode: on). In this mode, the amount of image processing is reduced to lower the latency. The drawback is that the images will become noisier, especially in low light conditions and around moving object. This will reduce the latency up to 30 - 200 milliseconds depending on camera model and settings. Depending on the Axis device, this feature is available on AXIS OS 9.80.1 or higher.

Multicast video streaming

Streaming video using multicast allows different video clients located in the network to access a single video stream which the Axis device distributes to a specific multicast address and port. One of the benefits of using multicast as a transport method for video streaming is that the Axis device keeps its system and resource consumption low by only sending a single or dual video stream to a specific address in the network. It is also an efficient way of using the network infrastructure since many different video clients can retrieve the video stream from the multicast address instead of each video client pulling a separate video stream from the Axis device. The way multicast is served, distributed and received in the network can actually minimize the bandwidth consumption of the network infrastructure and all its involved clients as such. Just imagine the difference this can make in a system with more than 5.000 Axis devices in operation.

Axis devices support a variety of ways to stream video in a multicast scenario. In the following sections we will go through multicast from a streaming perspective and not take into account the general mechanics of multicast and how it is routed through the network, or the basics of the different forms of multicast.

Any-source multicast (ASM)

Independently of the desired transport method – i.e. multicast or unicast – the initial RTSP protocol communication that is required to properly initialize the video client and Axis device is very similar, except that the video client in multicast-mode specifies this instead of the unicast scenario.

We will go through the details of a typical RTSP build-up step-by-step below. For more details, see the actual network traces in *Multicast in detail on page 40.*

Step 1: video client

The video client initiates the RTSP DESCRIBE and signals to the Axis device to prepare video streaming with the specified streaming parameters given in the RTSP URL and to share its corresponding Session Description Protocol (SDP) file, which includes information about how to decode the video stream.

```
DESCRIBE rtsp://172.25.201.100:554/axis-media/media.amp?videocodec=h265&audio=0
&resolution=1920x1080&camera=1&compression=30&fps=30 RTSP/1.0
CSeq: 2
User-Agent: OmnicastRTSPClient/1.0
Accept: application/sdp
Authorization: Digest username="root", realm="AXIS_ACCC8ED910B9",
nonce="00000450Y2804646c4d9f7d3175fa496417b9c4e7aa39a2",
```

Media streaming

```
uri="rtsp://172.25.201.100:554/axis-media/media.amp?videocodec=h265
&audio=0&resolution=1920x1080&camera=1&compression=30&fps=30",
response="7a2e2dcad7618b36479ec76e252bc1c3"
Step 2: Axis device
The Axis device validates the request and shares the corresponding SDP file with the video client. Note that in any-source multicast
mode, no multicast-specific network parameters are shared. In source-specific multicast mode (SSM), this is different.
RTSP/1.0 200 OK
CSeq: 2
Content-Type: application/sdp
Content-Base: rtsp://172.25.201.100:554/axis-media/media.amp/
Server: GStreamer RTSP server
Date: Thu, 11 Feb 2021 06:51:12 GMT
Content-Length: 1063
v=0
o=- 17136744296195211872 1 IN IP4 172.25.201.100
s=Session streamed with GStreamer
i=rtsp-server
t=0 0
a=tool:GStreamer
a=type:broadcast
a=range:npt=now-
a=control:rtsp://172.25.201.100:554/axis-media/media.amp?videocodec=h265&audio=0
&resolution=1920x1080&camera=1&compression=30&fps=30
m=video 0 RTP/AVP 96
c=IN IP4 0.0.0.0
b=AS:50000
a=rtpmap:96 H265/90000
a=framerate:30
a=fmtp:96 sprop-vps=QAEMAf//AUAAAAMAgAAAAwAAAwCcEJAk;sprop-
sps=QqEBAUAAAAMAqAAAAwAAAwCcoAPAqBEHy55CbkSq8quTqoKC8IAAAAMAqAAAAwKE; sprop-
pps=RAHANzwEbJA=
a=ts-refclk:local
a=mediaclk:sender
a=recvonly
a=control:rtsp://172.25.201.100:554/axis-media/media.amp/stream=0?videocodec=h265
&adui=0&resolution=1920x1080&camera=1&compression=30&fps=30
a=transform:1.000000,0.000000,0.000000;0.000000,1.000000,0.000000;0.000000,0.000000,1.000000
```

Step 3: video client

The video client then goes ahead and defines the appropriate transport method as multicast, the multicast IP address, streaming ports and the TTL. This is the important step in the RTSP build-up where the video client actually can specify the desired transport method. Note that in order for the Axis device to accept video client-specific multicast network parameters, the VAPIX parameter **RTSP Allow Client Transport Settings** in **Plain Config > Network** has to be enabled. If this parameter is not set, the Axis device might ignore these parameters and offer their own configuration set in **Plain Config > Network** > **RO**.

```
SETUP rtsp://172.25.201.100:554/axis-media/media.amp/stream=0?videocodec=h265&audio=0
&resolution=1920x1080&camera=1&compression=30&fps=30 RTSP/1.0
CSeq: 3
User-Agent: OmnicastRTSPClient/1.0
Transport: RTP/AVP;multicast;destination=224.16.17.51;port=47806-47807;ttl=64
Authorization: Digest username="root", realm="AXIS_ACCC8ED910B9",
nonce="00000450Y2804646c4d9f7d3175fa496417b9c4e7aa39a2",
uri="rtsp://172.25.201.100:554/axis-media/media.amp/stream=0?videocodec=h265
&audio=0&resolution=1920x1080&camera=1&compression=30&fps=30",
response="48cf0f723aca20f6530e79ecb966ec0a"
```

Media streaming

Step 4: Axis device

The Axis device in return validates the request and if successful, it answers with the exact same network parameters back to the video client to prepare the upcoming session.

```
RTSP/1.0 200 OK
CSeq: 3
Transport: RTP/AVP;multicast;destination=224.16.17.51;ttl=64;port=47806-
47807;mode="PLAY"
Server: GStreamer RTSP server
Session: f2imQtCHhuoH2FbW;timeout=60
Date: Thu, 11 Feb 2021 06:51:12 GMT
```

Step 5: video client

The video client then finally signals to the Axis device via RTSP PLAY to start video streaming as agreed based on the network and video streaming parameters that have been handshaked previously.

```
PLAY rtsp://172.25.201.100:554/axis-media/media.amp?videocodec=h265&audio=0
&resolution=1920x1080&camera=1&compression=30&fps=30 RTSP/1.0
CSeq: 4
Session: f2imQtCHhuoH2FbW
User-Agent: OmnicastRTSPClient/1.0
Range: npt=0.000-
Authorization: Digest username="root", realm="AXIS_ACCC8ED910B9",
nonce="00000450Y2804646c4d9f7d3175fa496417b9c4e7aa39a2",
uri="rtsp://172.25.201.100:554/axis-media/media.amp?videocodec=h265
&audio=0&resolution=1920x1080&camera=1&compression=30&fps=30",
response="d015b378a8a1000c964d6c48d1883d1f"
```

Step 6: Axis device

The Axis device acknowledges the request by sending an RTSP OK and provides the video client with information about how the video stream will be momentarily available at the defined multicast network parameters. In order to signal the start of the video stream to the video client, the Axis device specifies the sequence number of the first RTP package and the initial RTP timestamp so that the client expects and processes the correct start of the video stream.

```
RTSP/1.0 200 OK
CSeq: 4
RTP-Info: url=rtsp://172.25.201.100:554/axis-media/media.amp/stream=0?videocodec=h265
&audio=0&resolution=1920x1080&camera=1&compression=30
&fps=30;seq=24067;rtptime=417717697
Range: npt=now-
Server: GStreamer RTSP server
Session: f2imQtCHhuoH2FbW;timeout=60
Date: Thu, 11 Feb 2021 06:51:12 GMT
```

Optional client transport setting handling

In case the video client would not specify all the necessary network transport parameters accordingly, the Axis device will fallback and offer the default multicast parameter set in **Plain Config > Network > RO** as illustrated in the following example. We can observe here that the video client's request for video streaming specifies multicast as transport method and the port to be used for multicast streaming, but misses to specify the multicast IP address. The Axis device treats this as a non-complete request and offers instead its configuration set in RO, which the video client either can agree on or simply close the connection. Another reason why the Axis device would disregard the video client's desired settings is when the VAPIX parameter **RTSP Allow Client Transport Settings in Plain Config > Network** is unchecked.**Step 3: video client**

```
SETUP rtsp://172.25.201.100:554/axis-media/media.amp/stream=0 RTSP/1.0
CSeq: 5
Authorization: Digest username="root", realm="AXIS_ACCC8ED910B9",
nonce="0003628fY51859629beb31964cb09d13947338e39266e77",
uri="rtsp://172.25.201.100:554/axis-media/media.amp/",
response="78be3d448c752bda36df4b82baf4ecf9"
User-Agent: LibVLC/3.0.11 (LIVE555 Streaming Media v2016.11.28)
Transport: RTP/AVP;multicast;port=55810-55811
```

Media streaming

Step 4: Axis device

```
RTSP/1.0 200 OK
CSeq: 5
Transport: RTP/AVP;multicast;destination=224.225.226.227;ttl=5;port=50000-
50001;mode="PLAY"
Server: GStreamer RTSP server
Session: xvIhEhZ3W5QpueEZ;timeout=60
Date: Thu, 11 Feb 2021 06:28:05 GMT
```

Source-specific multicast (SSM)

While in any-source multicast (ASM) the multicast network parameters are handshaked after sharing the Session Description Protocol (SDP) file during the initial RTSP build-up, this is not the case in the source-specific multicast mode. In SSM, the multicast network parameters are pre-configured in the Axis device and shared with the requesting video client when the SDP file is shared. The benefit of this is that the requesting video client can join a multicast group and only filter for the multicast traffic the video client is interested in. This can be done by applying a source-specific filter when joining the multicast group.

A typical scenario where SSM would be beneficial is when multiple Axis devices would stream video to the same multicast address but would use different ports. A video client connecting via any-source multicast would receive the multicast traffic from all streaming devices, while a video client requesting source-specific multicast would be able to filter out unwanted traffic. On top of that, SSM allows for reliable planning of multicast routing/path-forwarding since it is known how multicast is switched and routed through the network.

Source-specific multicast requires pre-configuration on the Axis device to configure the desired multicast network parameters. You can find information on how to configure an Axis device for source-specific multicast in *the VAPIX Library* but is also illustrated below. There is no specific setting to enable or disable source-specific multicast as such, but the source-specific multicast network parameters that need to be defined in advance can be configured from **Plain Config > Network** for each individual video source. Below is a typical example configuration:

R0					
Always multicast audio					
Always multicast profile					
videocodeo=h264					
Always multicast video					
Audio address					
239.216.121.37					
Audio port 0					
ΠL					
5 [1255]					
Video address					
225.226.227.228					
Video port 60000					

Media streaming

Step 1: video client

Compared to the any-source multicast mode, SSM mode requires a different streaming URL for signaling to the Axis device that source-specific multicast is wanted.

```
DESCRIBE rtsp://172.25.201.100:554/axis-media/ssm/media.amp?camera=1 RTSP/1.0
CSeq: 4
Authorization: Digest username="root", realm="AXIS_ACCC8ED910B9",
nonce="000006c7Y356087c783187c3a95be0ca315f5fa0cd57ddc",
uri="rtsp://172.25.201.100:554/axis-media/ssm/media.amp?camera=1",
response="3226806a8c988f0d473df291e8c7ffb8"
User-Agent: LibVLC/3.0.11 (LIVE555 Streaming Media v2016.11.28)
Accept: application/sdp
```

Step 2: Axis device

The SDP file that is shared between the Axis device and the requesting video client includes the source-specific multicast network parameters which the video client has to learn in order to join the multicast group accordingly and filter for the correct traffic.

```
RTSP/1.0 200 OK
CSeq: 4
Content-Type: application/sdp
Content-Base: rtsp://172.25.201.100:554/axis-media/ssm/media.amp/
Server: GStreamer RTSP server
Date: Thu, 11 Feb 2021 07:01:42 GMT
Content-Length:
                749
v=0
o=- 9871677480407248934 1 IN IP4 172.25.201.100
s=Session streamed with GStreamer
i=rtsp-server
c=IN IP4 225.226.227.228/5
t=0 0
a=tool:GStreamer
a=type:broadcast
a=range:npt=now-
a=control:rtsp://172.25.201.100:554/axis-media/ssm/media.amp?camera=1
a=source-filter: incl IN IP4 225.226.227.228 172.25.201.100
m=video 60000 RTP/AVP 96
b=AS:50000
a=rtpmap:96 H264/90000
a=fmtp:96 packetization-mode=1;profile-level-id=640029;sprop-parameter-
sets=Z2QAKa0AxSAeAIn5ZuAgIDSDxIio,a048sA==
a=ts-refclk:local
a=mediaclk:sender
a=recvonly
a=control:rtsp://172.25.201.100:554/axis-media/ssm/media.amp/stream=0?camera=1
a=framerate:30.000000
a=transform:1.000000,0.000000,0.000000;0.000000,1.000000,0.000000;0.000000,0.000000,1.000000
```

Step 3: video client

Since the video client knows the multicast network parameters that will be used in advance, the client can include them in the RTSP SETUP request.

```
SETUP rtsp://172.25.201.100:554/axis-media/ssm/media.amp/stream=0?camera=1 RTSP/1.0
CSeq: 5
Authorization: Digest username="root", realm="AXIS_ACCC8ED910B9",
nonce="000006c7Y356087c783187c3a95be0ca315f5fa0cd57ddc",
uri="rtsp://172.25.201.100:554/axis-media/ssm/media.amp/",
response="89e1cf3338144d096723df0b10864cab"
User-Agent: LibVLC/3.0.11 (LIVE555 Streaming Media v2016.11.28)
Transport: RTP/AVP;multicast;port=60000-60001
```

Step 4: Axis device

The Axis device validates and responds with the correct multicast network parameter according to the pre-configuration done in R0.

Media streaming

```
RTSP/1.0 200 OK
CSeq: 5
Transport: RTP/AVP;multicast;destination=225.226.227.228;ttl=5;port=60000-
60001;mode="PLAY"
Server: GStreamer RTSP server
Session: 06yirClN7xQCtW8q;timeout=60
Date: Thu, 11 Feb 2021 07:01:42 GMT
```

Step 5: video client

The requesting video client then signals to the Axis device to start video streaming to the agreed streaming and network parameters.

```
PLAY rtsp://172.25.201.100:554/axis-media/ssm/media.amp?camera=1 RTSP/1.0
CSeq: 6
Authorization: Digest username="root", realm="AXIS_ACCC8ED910B9",
nonce="000006c7Y356087c783187c3a95be0ca315f5fa0cd57ddc",
uri="rtsp://172.25.201.100:554/axis-media/ssm/media.amp/",
response="c19526013f73f3db72cd4fca98ec1c40"
User-Agent: LibVLc/3.0.11 (LIVE555 Streaming Media v2016.11.28)
Session: 06yirClN7xQctW8q
Range: npt=0.000-
```

Step 6: Axis device

The Axis device acknowledges the request by sending an RTSP OK and provides the video client with info on how the video stream will be momentarily available at the defined multicast network parameters. In order to signal the start of the video stream to the video client, the Axis device specifies the sequence number of the first RTP package and the initial rtp timestamp so that the client expects and processes the correct start of the video stream.

```
RTSP/1.0 200 OK
CSeq: 6
RTP-Info: url=rtsp://172.25.201.100:554/axis-
media/ssm/media.amp/stream=0?camera=1;seq=21707;rtptime=3563678630
Range: npt=now-
Server: GStreamer RTSP server
Session: 06yirClN7xQCtW8q;timeout=60
Date: Thu, 11 Feb 2021 07:01:42 GMT
```

Always multicast

Always multicast is not a network multicast mode but a specific adaption to video clients that are not capable of performing a proper RTSP and/or multicast setup in either of the ways described previously (i.e. via ASM or SSM). In always multicast mode, the Axis device is statically configured to stream video to a specific multicast address and port, and also to start streaming to it directly, regardless if there are video clients in the network that are actually requesting video from that particular Axis device or not. On top of that, RTSP is not used to connect, instead the requesting video client will make a HTTP call to retrieve the Session Description Protocol (SDP) file in order to understand and make the connection to the multicast address and port where the video stream is connected. Always multicast can be configured in Axis devices in Plain Config > Network for each individual video source.

Example 1: The device will only stream video to the multicast address 224.225.226.227 and video port 50000. If video port 0 would be entered here, the Axis device would select the next possible port which has been defined in the RTP > End Port and Start Port configuration.

Media streaming

R0
Always multicast audio
Always multicast profile
videocodeo=h264
Always multicast video
Audio address
239.216.121.37
Audio port 0
ΠL
5 [1255]
Video address
224.225.228.227
Video port 50000

<u>Example 2</u>: The device will stream video to the multicast address 224.225.226.227 to port 50000, and audio to multicast address 239.216.121.37 to port 51000. Observe that it is also possible to adjust the video streaming parameters in the always multicast profile. If other streaming parameters should be used, e.g. a framerate of 15 frames per second and compression of 15, then the field can be adjusted in the following way: *videocodec=h264&tfps=15&tcompression=15*. Otherwise the current configured default stream settings will be used.

~	Always multicast audio
Alwa	ys multicast profile
	leocodeo=h264&fps=15&compression=15
	Always multicast video
	o address 9.218.121.37
23	5.210.121.57
Audi	o port
	51000
ΠL	
	5 [1255]
Vide	o address
22	4.225.226.227
Vide	o port
	50000

Media streaming

Once the above settings are saved, the Axis device will start streaming to the configured multicast address and port immediately regardless if there are clients requesting the video stream or not. The client can access this multicast stream via the SDP file, which determines the video stream settings so that the video client learns how to play the video. The SDP file can be accessed using *http://ip-address/axis-cgi/alwaysmulti.sdp?camera=1* where camera=1 is mapped to R0. An example of such an SDP file can be found via *alwaysmulti.sdp*. Below is a network trace example illustrating the procedure.

Step 1: video client

The video client has requested the SDP file from the Axis device. Observe that no streaming parameters or multicast network parameters are mentioned by the client, hence this configuration must be performed on the Axis device prior to making the request as described in the previous examples.

```
GET /axis-cgi/alwaysmulti.sdp?camera=1 HTTP/1.1
Host: 172.25.201.100
Accept: */*
Accept-Language: en_US
Authorization: Basic cm9vdDpwYXNz
User-Agent: VLC/3.0.11 LibVLC/3.0.11
Range: bytes=0-
```

Step 2: Axis device

The Axis device looks up the current configuration in R0 and then initializes and sends the SDP file to the requesting video client. This is done in order to pass on the required information so that the video client can access the already ongoing multicast stream at the pre-configured multicast address and port. No further unicast communication is exchanged at this point, the video client will switch over to the specified multicast network parameters in order to access the stream.

```
HTTP/1.1 200 OK
Date: Thu, 11 Feb 2021 06:14:25 GMT
Server: Apache/2.4.46 (Unix) OpenSSL/1.1.1g
Cache-Control: no-cache, no-store, max-age=0
Pragma: no-cache
Expires: Thu, 01 Dec 1994 16:00:00 GMT
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Transfer-Encoding: chunked
Content-Type: application/sdp
v=0
o=- 1188340656180883 1 IN IP4 172.25.201.100
s=Session streamed with GStreamer
i=rtsp-server
t = 0 \quad 0
a=tool:GStreamer
a=type:broadcast
a=control:*
a=range:npt=now-
m=video 50000 RTP/AVP 96
c=IN IP4 224.225.226.227/5
b=AS:50000
a=rtpmap:96 H264/90000
a=fmtp:96 packetization-mode=1;profile-level-id=640029;sprop-parameter-
sets=Z2QAKa0AxSAeAIn5ZuAgIDSDxIio,a048sA==
a=control:stream=0
a=ts-refclk:local
a=mediaclk:sender
a=framerate:30.000000
```

Media streaming

Multicast in detail

Example network trace	Multicast address	Multicast port	Video client	Video client IP address	Axis device IP address
FFMPEG_Any_Source	_ 11 41£725\$\$27&2977g	50000	FFMPEG	172.25.201.50	172.25.201.100
VLC_Any-Source_Mu	12265225022950229	50000	VLC*	172.25.201.50	172.25.201.100
Genetec_Any_Source	_ 2/2/ AltiGast. F tapng	47806	Genetec	172.25.201.51	172.25.201.100
Milestone_Any_Sour	c@_2\41.û1&i& d s\$5.1pcapng	47806	Milestone	172.25.201.52	172.25.201.100
VLC_Source_Specific	_MATA2652,}70,000g	60000	VLC	172.25.201.50	172.25.201.100
FFMPEG_Always_Mu	16226458_2153i26266_25207P_Fi	le <u>5</u> ØФФФсарпд	FFMPEG**	172.25.201.50	172.25.201.100
VLC_Always_Multica	st <u>2</u> 29ii <i>1</i> 2225.23DP2_1271e_Pi	a ‰@@@ @ng	VLC**	172.25.201.50	172.25.201.100
VLC_Always_Multica	s&_214TTP_5_\$2016_P2d7y.pcd	1/550g000	VLC***	172.25.201.50	172.25.201.100

*In VLC, you may need to enable "Force multicast RTP via RTSP" in the RTP/RTSP/SDP demuxer settings under Advanced Preferences.

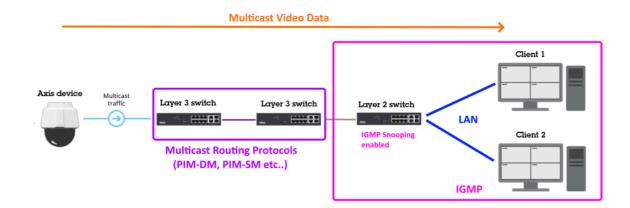
**In order for FFMPEG and VLC to access and retrieve the SDP file via HTTP-authentication, the HTTP-basic authentication has to be configured in Plain Config > Network > Authentication policy.

***These examples illustrate how a video client is capable of connecting to the multicast stream just by using the file SDP alone without making any further connection to the Axis device. Assuming that no configuration change is made on the Axis device, the user is only required to download the SDP file once and then one could use the SDP to start playing the video. VLC and FFMPEG are examples of clients that are capable of doing so.

Multicast network overview

A typical multicast scenario consists of three parts: the source, the multicast network infrastructure, and the receivers.

The Axis device is the source which sends out the streams to the multicast address. The multicast address is agreed between the clients and the device during the negotiation. The network infrastructure must be configured by network professionals. A multicast routing protocol (like PIM) needs to be running between the routers, and the IGMP protocol needs to be running between the last-hop router and the receiving clients. Additionally, IGMP snooping needs to be enabled on the layer 2 switches to avoid multicast traffic being flooded.

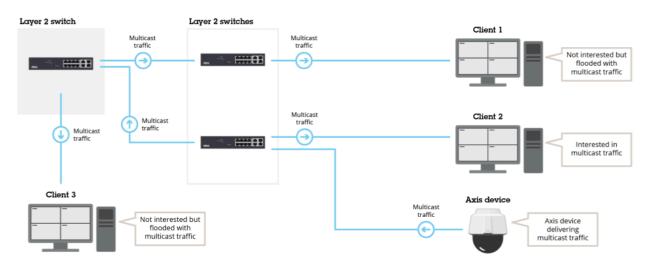


Multicast in a switched network

A network where traffic is served within a certain VLAN and IP address network is called a switched network since no layer-3 IP routing is needed. Let's start with the basic setup and assume that the network switches have not been configured properly for handling multicast traffic. What you would see is similar to the illustration below, a switched network consisting of a handful of

Media streaming

switches with client computers and Axis devices. From all of the clients, only **Client 2** is interested and requests a multicast video stream from the Axis device. Since the network switches are not configured properly at this point, the multicast traffic, which is only supposed to flow from the Axis device over the traversing switches to **Client 2**, will be flooded to all switches and clients in the network, regardless if they are interested in receiving the traffic or not.

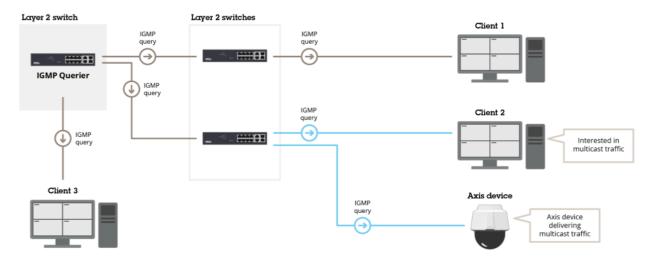


Let's look at the same network when properly configured with IGMP (Internet Group Management Protocol) enabled. IGMP is a protocol that helps the network infrastructure learn and understand who is delivering multicast traffic to which destination in order to avoid multicast flooding to non-interested clients. To configure the network to avoid multicast flooding, it is enough to configure the main switch – i.e. Layer 2 switch – for IGMP in the following example configuration:

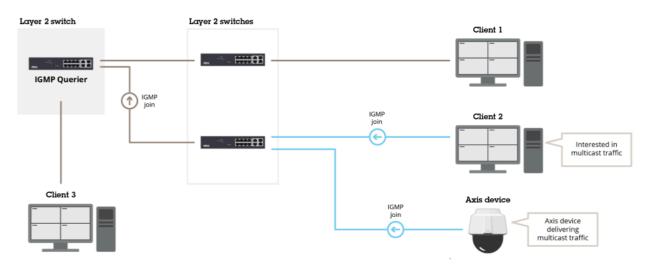
Global configuration

ip igmp snooping querier address 172.25.201.10 ip igmp snooping querier query-interval 15 ip igmp snooping querier

By doing this, the Layer 2 switch will be sending out IGMP queries to the connected network devices in order to find out which ones are interested in receiving and sending multicast packages.

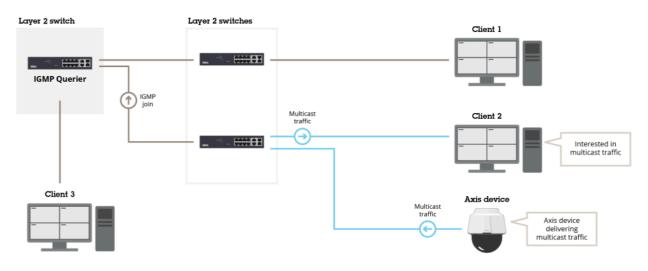


Media streaming



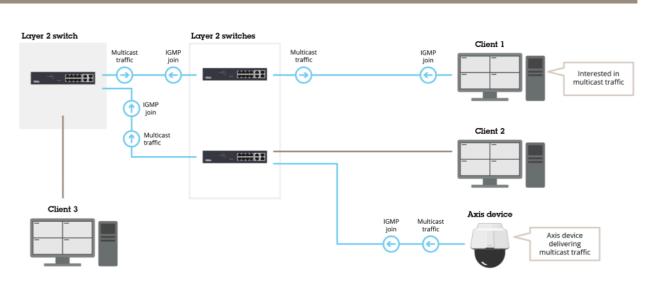
The network devices will respond with "join" messages in order to signal their participation in multicast-related traffic.

The network switches will listen and learn from this traffic in order to properly switch network packages to their appropriate destinations. In the illustration below, only **Client 2** is requesting video from the Axis device via multicast.



With the correct configuration in place, the network switches are now capable of switching packages as well across switches. In the illustration below, we have switched the clients, so that **Client 1** requests a multicast video stream from the same Axis device that previously served **Client 2**. The result will be proper switched network traffic across the network to the correct destination.

Media streaming

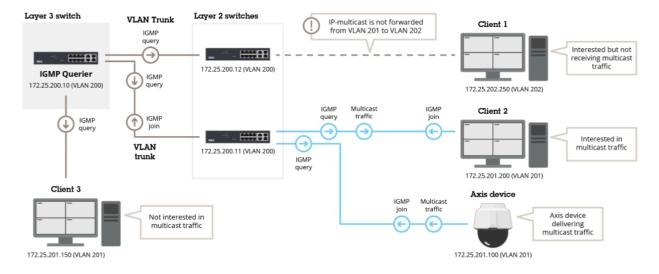


Multicast in a routed network

Multicast in a routed network does not differ essentially from a switched scenario in regards to how multicast traffic is handled. A network where clients exchange network traffic across different VLANs and IP networks is called a routed network since layer-3 IP routing techniques are needed to deliver the network traffic across. Let's re-use the same network topology as we did in the switched network scenario. The only - but important - difference is that Client 1 is placed in a different VLAN and IP address network compared to Client 2 and 3 as well as the Axis device. We assume that we have already performed the same IGMP configuration as mentioned earlier. For reference, see below:

Global configuration

ip igmp snooping querier address 172.25.201.10 ip igmp snooping querier query-interval 15 ip igmp snooping querier



As you can see, **Client 2** is already requesting video from the Axis device using multicast and since we have applied the correct IGMP configuration to the Layer 3 switch, this setup works flawlessly. But **Client 1** from the other IP network also wants to

Media streaming

receive a video via multicast, which is <u>not</u> working since multicast is not routed across different IP networks by design. So in order to allow multicast traffic to be routed across layer-3 networks we have to enable IP-multicast routing and use a protocol such as Protocol Independent Multicast (PIM). The most basic and simple use case would be to make use of the passive mode of PIM, as illustrated below in the suggested configuration:

Global configuration *ip multicast-routing*

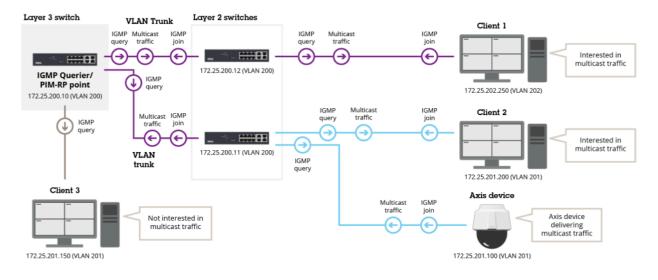
Configuration VLAN 201

interface Vlan201 description LAN1 clients ip address 172.25.201.10 255.255.255.0 ip pim passive !

Configuration VLAN 202

interface Vlan202 description LAN2 clients ip address 172.25.202.10 255.255.255.0 ip pim passive

With this configuration applied, multicast is properly routed across different networks. From the **Axis device** located in VLAN 201 to **Client 1** that is located in VLAN 202.



Video streaming rotation

In this section we will take a closer look at the VAPIX and ONVIF image rotation configuration when it comes to video streaming, which is handled differently depending on AXIS OS version.

AXIS OS 8.50 and higher

After support for ONVIF Profile T was added, the handling of image rotation in Axis devices has been completely separated between VAPIX and ONVIF. This means that both protocols have dedicated parameters for image rotation configuration, and that the image rotation parameter for one protocol does not affect the other and vice-versa. For VAPIX this is configured via the image rotation parameter **Image.IO.Appearance.Rotation**, either in the image settings in the web interface, or directly via VAPIX HTTP request. For ONVIF it's configured in the ONVIF media stream profiles in the web interface, or directly via the script editor for legacy devices in the configuration file: **/etc/ws/onvif/media/media.conf**.

Media streaming

Exception: The above is not true for Axis devices with support for ImageSource.IO.SourceRotation=yes. On these devices, the image rotation parameter is set globally via VAPIX and ONVIF will adapt to it accordingly.

AXIS OS 8.40 and lower

Configuring the image rotation parameter Image.IO.Appearance.Rotation via the image settings in the web interface or directly via VAPIX HTTP request will affect both VAPIX and ONVIF video streams. ONVIF video streams will adapt to the same image rotation configured via VAPIX, unless specified otherwise in the ONVIF stream profile settings.

Example configurations

VAPIX configuration of image rotation from the device web interface:

Image	Stream	Overlay	PTZ	Audio	Privacy mask	View area	Apps	System			
	Appeara					Sharpness 0	5		100 50	Orientation	
	Saturation		0-		100 50	Focus				Rotate Auto 0* 90* 180* 270* Zoom	
	Contrast				100 50	Sho	ow AF area	3	Autofocus	Wide Tel	e
	Brightness				100 50	Near			Far		
										•••••	

ONVIF configuration of image rotation from the device web interface:

AXIS M1065-L Network Camera	
ONVIF media profiles	
profile_1 h264 Profile token: profile_1_h264 Profile name	î
Video source Select a configuration user0 w	î
General Source token: 0	
Orientation Rotate image	
	ONVIF media profiles profile_1 h264 Profile token: profile_1_h264 Profile name profile_1 h264 Video source Select a configuration user0 General Source token: 0 Orientation

Media streaming

ONVIF configuration of the image rotation via script editor:



Streaming timestamps

In this section you can read about different ways to receive timestamp information when streaming video and downloading single images from Axis devices. This metadata information can be used for processing in business applications, e.g. when receiving metadata about how many persons in a store went through a certain area. It can also be used in other use cases where time-synchronisation towards 3rd party video clients is needed

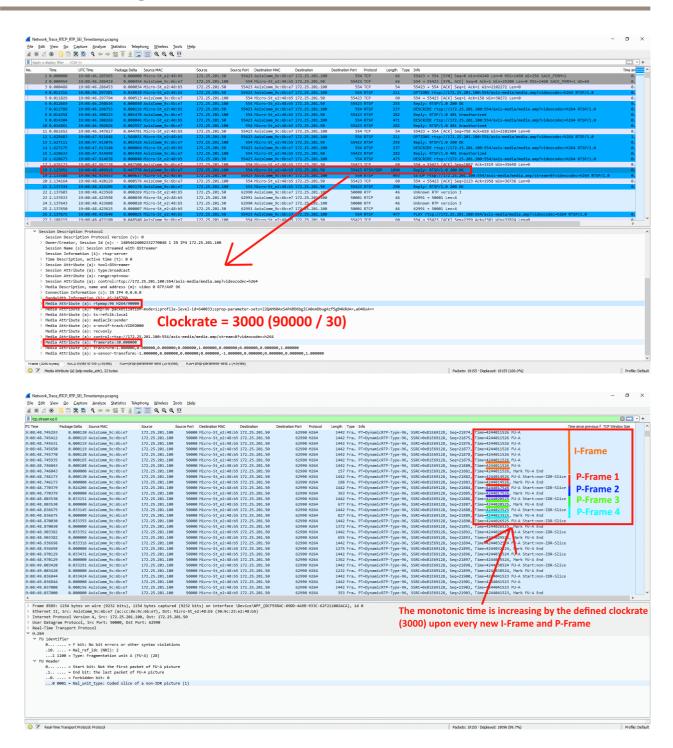
H.264/MJPEG and RTP timestamps

The following network trace can be used for testing what is described below.

RTP timestamps can be found in the payload of RTP packages and function as a monotonic timestamp that can be used to identify a specific frame of the video stream. Based on the clock rate that is computed during the video stream build-up, the RTP timestamp is expected to increase incrementally from one frame to another.

The clock rate depends on the image frequency of the video stream. In this example, the video stream consists of 30 frames per second, which means the computed clock rate will be 3000. This in turn means that the monotonic RTP timestamp will increase by 3000 upon every new I-Frame or P-Frame as you can see in the following two screenshots.

Media streaming



When the video stream starts, the Axis device will let the external video client know about the initial RTP timestamp of the first frame (I-Frame), as you can see below. This allows the receiving video client to identify e.g. missing frames and can be used for RTP timestamp drift measurement while the video stream is ongoing.

Media streaming

lisplay filter <cb< th=""><th>ป-/></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></cb<>	ป-/>							
Time		Package Delta Source MAC		ource Port Destination MAC Destination	Destination Port Protocol	Length Typ		Tim
2.137643	19:08:48.423608 19:08:48.423615	0.000010 Micro-St_e2:48:b5 0.000007 Micro-St_e2:48:b5	172.25.201.50 172.25.201.50	62990 AxisComm_9c:6b:e7 172.25.201.100 62991 AxisComm_9c:6b:e7 172.25.201.100	50000 RTP 50001 RTCP	46 46	Unknown RTP version 3 62991 → 50001 Len=4	
2.137675	19:08:48.423640	0.000025 Micro-St_e2:48:55	172.25.201.50	55423 AxisComm_9c:6b:e7 172.25.201.100	554 RTSP	477	PLAY rtsp://172.25.201.100:554/axis-media/media.amp?videocodec=h264 RTSP/1.0	
2.186215	19:08:48.472180	0.048540 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St e2:48:b5 172.25.201.50	55423 TCP	60	554 → 55423 [ACK] Seq=2359 Ack=2381 Win=37824 Len=0	
2.422826	19:08:48.708791	0.236611 AxisComm_9c:6b:e7	172.25.201.100	554 Micro-St_e2:48:b5 172.25.201.50	55423 RTSP	321	Reply: RTSP/1.0 200 OK	
2.424153 2.428593	19:08:48.710118 19:08:48.714558	0.001327 AxisComm_9c:6b:e7 0.004440 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:55 172.25.201.50 50000 Micro-St e2:48:55 172.25.201.50	62990 H264 62990 H264		L. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21615, Time=4244011526 SEI a. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21616, Time=4244011526 FU-A Start:IDR-Slice	
2.428595	19:08:48.714558	0.000140 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:05 172.25.201.50 50000 Micro-St e2:48:05 172.25.201.50	62990 H264		 a. PI=DynamickIP-Type-96, SSRC=0x01c09128, Seq=21616, Imme=4244011526 FU-A Start:1DK-SIICe a. PT=DynamickIP-Type-96, SSRC=0x01c69128, Seq=21617, Time=4244011526 FU-A 	
2.428843	19:08:48.714808	0.000110 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:b5 172.25.201.50	62990 H264		a. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21618, Time=4244011526	
2.428951	19:08:48.714916	0.000108 AxisComm_9c:6b:e7	172.25 201.100	50000 Micro-St_e2:48:b5 172.25.201.50	62990 H264		a. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21619, Time=4244011546 FU-A	
2.429059	19:08:48.715024	0.000108 AxisComm_9c:6b:e7	172.29.201.100	50000 Micro-St_e2:48:b5 172.25.201.50	62990 H264		a PT=DynamicRTP-Type-96, SSRC=0xB1E69128, Seq=21620, Time=4244011526 FV-A	
2.429172	19:08:48.715137	0.000113 AxisComm_9c:6b:e7	172.75.201.100	50000 Micro-St_e2:48:b5 172.25.201.50	62990 H264		a. PT=DynamicRTP-Type-96, SSRC=0xB1E69128, Seq=21621, Time=4244011526 FD-A	
2.429267	19:08:48.715232 19:08:48.715370	0.000095 AxisComm_9c:6b:e7 0.000138 AxisComm 9c:6b:e7	172 25.201.100	50000 Micro-St_e2:48:b5 172.25.201.50 50000 Micro-St e2:48:b5 172.25.201.50	62990 H264 62990 H264		a. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21622, Time=4244011526 8U-A a. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21623, Time=4244011526 4U-A	
2.429524	19:08:48.715489	0.000119 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:b5 172.25.201.50	62990 H264		a. PT-DynamicRTP-Type-96, SSRC-0x81E69128, Seq=21624, Time=424401126 FU-A	
2.429644	19:08:48.715609	0.000120 AxisComm_9c:6b:e7	12.25.201.100	50000 Micro-St_e2:48:b5 172.25.201.50	62990 H264		a. PT=DynamicRTP-Type-96, SSRC=0xB1E69128, Seq=21625, Time=4244011529 FU-A	
2.429769	19:08:48.715734	0.000125 AxisComm_9c:6b:e7	72.25.201.100	50000 Micro-St_e2:48:b5 172.25.201.50	62990 H264		a PT=DynamicRTP-Type-96, SSRC=0xB1E69128, Seq=21626, Time=4244011526 FU-A	
2.429860	19:08:48.715825	0.000091 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.201.50	62990 H264		a PT=DynamicRTP-Type-96, SSRC=0xB1E69128, Seq=21627, Time=4244011526 FU-A	
2.430008	19:08:48.715973 19:08:48.716086	0.000148 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.201.50	62990 H264 62990 H264		a PT=DynamicRTP-Type-96, SSRC=0xB1E69128, Seq=21628, Time=424401526 FU-A a PT=DynamicRTP-Type-96, SSRC=0xB1E69128, Seq=21629, Time=424401526 FU-A	
2,430121 2,430262	19:08:48.716227	0.000113 AxisComm_9c:6b:e7 0.000141 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.201.50 50000 Micro-St e2:48:b5 172.25.201.50	62990 H264		a PI=DynamickIP-Type-96, SSRC=0x81E69128, Seq=21629, Time=4244421526 FU-A a PT=DynamickTP-Type-96, SSRC=0x81E69128, Seq=21630, Time=4244011526 FU-A	
2.430377	19:08:48.716342	0.000115 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:b5 172.25.201.50	62990 H264		a. PT=DynamicRTP-Type-96, SSRC=0xB1E69128, Seq=21631, Time=444011526 FU-A	
2.438498	19:08:48.716463	0.000121 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:b5 172.25.201.50	62990 H264		a. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21632, Tip=4244011526 FU-A	
D 470614	10.00.40 710070	a againe Aviacame Garchia	172 26 201 100	E0000 Mires C+ 23.40.6E 173 3E 301 E0	60000 UDEA	1443 6-	- 07_0	
ission Contro ime Streaming ponse: RTSP/1 q: 9\r\n	ol Protocol, Src P g Protocol 1.0 200 OK\r\n csp://172.25.201.10	2.25.201.100, Dst: 172.25/201.50 ort: 554, Dst Port: 5542, Seq: 2 200:554/axis-media/media.amp/strea						

An I-Frame and/or P-Frame can consist of several RTP packages. As you can see, all packages that belong to the same I-Frame have the same unique timestamp, while each of the following P-Frames have their own timestamp corresponding to the clock rate. So for each unique I-Frame or P-Frame, the RTP timestamp increases incrementally.

The UTC The Pedago Das Source Mode Source Mode Destination MC Destination MC Destination MC Lingth Type: 16 22.12759 1998144.42016 0.000000 TRLors-5; 22:4016 122.32.321.00 59901 Atticame_price 172.32.321.00 59901 TRTP 46 UNDOWN TRLors-5; 22:4016 122.32.321.00 59901 Atticame_price 172.32.321.00 59901 TRTP 46 UNDOWN TRLors-5; 22:4016 122.32.321.00 59901 Atticame_price 172.32.321.00 59901 TRTP 46 UNDOWN TRLors-5; 22:4016 122.32.321.00 59901 Atticame_price 172.32.321.00 59901 TRTP 46 UNDOWN TRLORS-5; 22:4016 122.32.321.00 59901 Atticame_price 172.32.321.00 59901 TRTP 46 UNDOWN TRLORS<5; 22:401.00 59901 TRTP 46 UNDOWN TRLORS<5; 22:401.00 59901 TRTP 46 UNDOWN TRLORS<5; 22:401.00 120.42233 120.42234 120.42243 <			₮ ½ 🚍 🗏 @ @ @ ₩						
3: 1,1750 19:88:44,2233 0.000007 MICro-5* (2:44:80) 72:2.52:81:00 5981 AliXione (10:77:72:2.52:10:0) 5981 AliXione (10:77:72:2.52:10:0) 5981 TPC 4 74	Time		adkage Delta Source MAC	Source	Source Port Destination MAC Destination	Destination Port Protocol	Length Type	Info	Time sin
5:1:7769 19:08:14.42435 0.00007 Mirco-5************************************	24 2.137643	19:08:48.423608	0.000010 Micro-St e2:48:b5	172.25.201.50	62990 AxisComm 9c:6b:e7 172,25,201,100	50000 RTP	46	Unknown RTP version 3	
37 1.10005 1989.84.4.2048 0.40008 Microsofe gradesis 77.2.201.00 594 78.20 78	25 2.137650	19:08:48.423615		172.25.201.50		50001 RTCP	46	62991 > 50001 Len=4	
32 2.0283 0.000141.700710 0.23021 Autom (retains) 0.2322 Autom (retains) 0.232 Autom (retains) 0.232 Autom (retains) 0.232 Autom (retains) 0.2322 Autom (retains) 0.00132 Autom (retains) 0.0013 Autom (26 2.137675	19:08:48.423640	0.000025 Micro-St e2:48:b5	172.25.201.50		554 RTSP	477	PLAY rtsp://172.25.201.100:554/axis-media/media.amp?videocodec=h264 RTSP/1.0	Θ.
2 2	27 2.186215	19:08:48.472180	0.048540 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St e2:48:b5 172.25.201.50	55423 TCP	60	554 → 55423 [ACK] Seg=2359 Ack=2381 Win=37824 Len=0	0.
39 2:42839 19:18:43.7.4638 0:40444 A 44:1000 (1:0000) 122:25:281.10 56000 Micros 5:2:44:155 172.5:281.10 56000 Micros 5:2:44:155 172.5:281.10 1444 rp. 17:0000000(1:0000) 1444 rp. 17:000000(1:0000) 1444 rp. 17:000000(1:0000) 1444 rp. 17:000000(1:0000000000000000000000000000	28 2.422826	19:08:48.708791	0.236611 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St e2:48:b5 172.25.201.50	55423 RTSP	321	Reply: RTSP/1.0 200 0K	0.
13 1 2 42243 13 9484.47.14049 0.00014 Actions (science 17, 22, 23, 20, 10) 5000 Micross (science 17, 23, 23, 23, 20, 10) 5000 Micross (science 17, 23, 23, 23, 20, 10) 5000 Micross (science 17, 23, 23, 23, 20, 10) 5000 Micross (science 17, 23, 23, 23, 20, 10) 5000 Micross (science 17, 23, 23, 23, 20, 10) 5000 Micross (science 17, 23, 23, 23, 20, 10) 5000 Micross (science 17, 23, 23, 23, 20, 10) 5000 Micross (science 17, 23, 23, 23, 20, 10) 5000 Micross (science 17, 23, 23, 23, 20, 20) 5000 Micross (science 17, 23, 23, 23, 20, 20) 5000 Micross (science 17, 23, 23, 23, 20, 20) 5000 Micross (science 17, 23, 23, 23, 23, 23, 23, 23, 23, 23, 23	29 2.424153	19:08:48.710118	0.001327 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:b5 172.25.201.50	62990 H264	104 NAL.	_ PT=DvnamicRTP-Tvpe-96, SSRC=0x81E69128, Seg=21615, Time=4244011526 SEI	
13 12 22 23 <td< td=""><td>30 2,428593</td><td>19:08:48.714558</td><td>0.004440 AxisComm 9c:6b:e7</td><td>172.25.201.100</td><td>50000 Micro-St e2:48:b5 172,25,201,50</td><td>62990 H264</td><td>1442 Fra.</td><td>PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seg=21616, Time=4244011526 FU-A Start:IDR-Slice</td><td></td></td<>	30 2,428593	19:08:48.714558	0.004440 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:b5 172,25,201,50	62990 H264	1442 Fra.	PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seg=21616, Time=4244011526 FU-A Start:IDR-Slice	
31 2.42843 3.9864.3.7.4889 0.000018 Attackom (science 7) 172.2.5.28.1.89 5000 Micro St, 2.4455 772.5.29.1.0 2200 0124 1442 rn. 174.07main(HT-T)rgs-46, SSK-0hol10123, Seq-2103, Tim=-244011250 UV.A Start 51 51 52.2.2253 51.000 Micro St, 2.24165 772.5.29.1.89 5000 Micro St, 2.4455 772.5.29.1.90 5200 0124 1442 rn. 174.07main(HT-T)rgs-46, SSK-0hol10123, Seq-2103, Tim=-244011250 UV.A Start 51 52.2.2253 51.000 Micro St, 2.24165 772.5.29.1.90 5200 0124 1424 rn. 174.07main(HT-T)rgs-46, SSK-0hol10123, Seq-2103, Tim=-244011250 UV.A Start 51.000 Micro St, 2.24165 772.5.29.1.00 5200 0124 1424 rn. 174.07main(HT-T)rgs-46, SSK-0hol10123, Seq-2103, Tim=-244011250 UV.A of an 32.242845 3.9864.7.15849 0.000018 Attackom (science 7) 172.5.28.100 B000 Micro St, 2.24165 772.5.28.100 B0000 Micro St, 2.24165 772.5.28.100 B000 Micro St, 2.24165 772.5.28.100 B0000 Micro St, 2.24165 772.5.28.100 B000 Micr	31 2,428733	19:08:48.714698	0.000140 AxisComm 9c:6b:e7			62990 H264			
31 2.4393 13 384:4.7.1942 0.400018 Attaicum (science 7) 172.37.201.00 5000 Micro 51, 224:455 77.25.201.00 5200 Micro 51, 224:455 77.25.201.00 <t< td=""><td>32 2.428843</td><td>19:08:48.714808</td><td>0.000110 AxisComm 9c:6b:e7</td><td>172.25.201.100</td><td></td><td>62990 H264</td><td></td><td>PT=DvnamicRTP-Tvpe-96, SSRC=0x81E69128, Seg=21618, Time=4244011526 FU-A</td><td></td></t<>	32 2.428843	19:08:48.714808	0.000110 AxisComm 9c:6b:e7	172.25.201.100		62990 H264		PT=DvnamicRTP-Tvpe-96, SSRC=0x81E69128, Seg=21618, Time=4244011526 FU-A	
3 2.42221 19.18(4.7.1327) 0.40013 Actionm Science 7 122.23.281.100 56000 Micros 52.24465 372.5.29.10 2200 1024 1442 rn. Projment(HT-Type-4), SIX-00011028, Sep21021, Time-44401128 UVA of an 3 2.42227 19.88(4.7.1327) 0.40013 Actionm Science 7 127.25.281.100 56000 Micros 52.24455 372.5.29.10 5200 1024 1442 rn. Projment(HT-Type-4), SIX-00011028, SiX-00110218, SiX-001110118, SiX-00110218, SiX-001118, SiX-00110218,	33 2.428951	19:08:48.714916		172.25.201.100		62990 H264		PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21619, Time=4244011526 FU-A Start	
32 2-22927 19:88:47.73528 0.000033 AxisCom Sciebs? 122.53.20:1.00 5000 Pilce 55;22:23.10:1.0 5000 Pilce 55;22:23.10:1.0 5000 Pilce 51;22:23.20:1.00 5000 Pilce 51;22:23:20:1.00 5000 Pilce 51;	34 2.429059	19:08:48.715024	0.000108 AxisComm 9c:6b:e7	172.25.201.100		62990 H264			
30 2.42927 19.804.47.0578 0.000015 Actionm (crimer, crimer, crimar, crimer, crimar, crimer, crimer, crimar,	35 2.429172	19:08:48.715137	0.000113 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:b5 172.25.201.50	62990 H264	1442 Fra.	PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21621, Time=4244011526 FU-A of an	
38 2.42542 10.808-4.7.15409 0.400013 AxisCom_Erclibro (10.90012) 56000 Micro-52, 42.4165 172.5.20.100 5000 Micro-52, 52.4161 126 Micro-52,	36 2.429267	19:08:48.715232	0.000095 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:b5 172.25.201.50	62990 H264	1442 Fra.	PT-DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21622, Time=4244011526 FU-A	
30 242434 1018184.71539 0.00013 Akticum_Prime 172.25.201.100 5000 11201	37 2.429405	19:08:48.715370	0.000138 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:b5 172.25.201.50	62990 H264	1442 Fra.	PT-DynamicRTP-Type-96, SSRC-0x81E69128, Seq-21623, Time-4244011526 FU-A	
40 2.4290 10:80:4.7.1574 0.400215 Attaicum (c:0):0:0:0 122.32.30:1.00 5000 Micro:d; 2:4165 172.5:30:1.00 5000 Micro:d;	38 2.429524	19:08:48.715489	0.000119 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:b5 172.25.201.50	62990 H264	1442 Fra.	PT-DynamicRTP-Type-96, SSRC-0x81E69128, Seq-21624, Time-4244011526 FU-A	-
49 2.429 10:88:47.73274 0.400125 AutiCom_Science 71 172.25.281.100 5000 MPL(ros5, qc:24:85 127.25.30.10) 5000 MPL(ros5, qc:	39 2.429644	19:08:48.715609	0.000120 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:b5 172.25.201.50	62990 H264	1442 Fra.	PT-DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21625, Time=4244011526 FU-A	
41 2.4280 13.881-8.7373 0.400014 AutsCom_Scribtr 71 172.25.201.10 5000 P01(ro-55_c2.43615 372.5.23.0.10 6200 P1244 1442 Fra. PTO_MMAIGHTP-Type-50_S SSC+006102125, 5eg-21627, Time-244011256 FU-A 42 2.4800 13.881-8.7373 0.60013 AutsCom_Scribtr 72 172.25.201.100 5000 P01(ro-55_c2.43615 372.5.23.0.100 6200 P1244 1442 Fra. PTO_MMAIGHTP-Type-50_S SSC+006102125, 5eg-21627, Time-244011256 FU-A 43 2.4800 13.881-8.7373 0.60013 AutsCom_Scribtr 72 172.25.201.100 5000 P1(ro-55_c2.43615 372.5.23.0.00 6220 P1244 1442 Fra. PTO_MMAIGHTP-Type-50_S SSC+006102125, 5eg-21627, Time-244011526 FU-A Mathematication of the segment of the segmen	40 2.429769	19:08:48.715734	0.000125 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:b5 172.25.201.50	62990 H264			
42 2.4380 1948144.73973 0.4002144 AutsCom_Stelster 172.25.201.00 5000 MUICo-52_c2146155 72.25.201.00 5000 MUICo-52_c214615 72.25.201.00 5000 MUICO-52_c2146120 MUICO-52_c214612									
43 2.4212 19.88:47.7168 0.40013 AutoCom_Brither 172.57.201.100 50000 Micro-5(e2146):5172.75.201.30 62090 H24 1442 Fra. Projmanic/RP-Type-96, 53RC+00160128, 5ee-21629, Time-424011525 FU-A as 30.142 bytes on wine (1036 bits), 1443 bytes optioned (1036 bits), 1444 bytes optioned (1036 bits), 1444 bytes optioned (10									
<pre>abii 1442 bytes on wire (11536 bits), 1442 bytes appured (11536 bits) on interface \Device\WF_[DC7558AC-8800-4498-93XC-827211892ACA), id 0 ennet II, Src: AsixCom_Erclosof (accelests(bits)), Dit: Filteruste_Erclosof (abies), Dit: Filteruste</pre>									
erret TI, Sri AsiZem Britisher (arcicle Strickshor), bit: Nicro-Strickishis) meth Potscol Pues P Dategrame Protocol, src Port: SB000, Dit Port: 62990 1-Tiser Transport Protocol 64 70 Julient Time 71 Julie			0.000113 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.201.50	62990 H264	1442 Fra.		
.11	43 2.430121 ne 30: 1442 byt	19:08:48.716086 tes on wire (11536 b	- its), 1442 bytes captured (11536	i bits) on interfa	- ce \Device\NPF_{DCF558AC-89DD-4A9B-933C-62F		1442 Fra.		,
1 1100 = Type: Fragmentation unit A (FU-A) (28) Filesder 1 = Start bit: the first packet of FU-A picture Ae Start bit: the the last packet of FU-A picture Start = Start =	43 2.430121 me 30: 1442 byt ernet II, Src: Datagram Protocol -Time Transpo 54 U identifier	19:08:48.716086 tes on wire (11536 b AxisComm_9C:6b:e7 (Version 4, Src: 172 tocol, Src Port: 500 rt Protocol	- its), 1442 bytes captured (11536 ac:cc:08:9c:06:e7), Dxt: Nicro-5 .25.201.100, Dxt: 172.25.201.50 00, Dxt Port: 62990	i bits) on interfa	- ce \Device\NPF_{DCF558AC-89DD-4A9B-933C-62F		1442 Fra.		,
VU Header VU Header VU Header Start bit: the first packet of FU-A picture .0 = find bit: hick the last packet of FU-A picture .0	43 2.430121 me 30: 1442 byternet II, Src: ernet Protocol Datagram Proto L-Time Transpor 54 U identifier 0	19:08:48.716086 tes on wire (11536 b AxisComm_9c:06:e7 (Version 4, Src: 172 tocol, Src Port: 500 rt Protocol F bit: No bit error:	- its), 1442 bytes captured (11536 acicc:8e:9c:6b:e7), Dist: Nicro-5 25.801.00, Dist: 172.35.201.50 00, Dist Port: 62990 s or other syntax violations	i bits) on interfa	- ce \Device\NPF_{DCF558AC-89DD-4A9B-933C-62F		1442 Fra.		,
1 = Start bit: the first packet of FU-A picture = find bit: Not the last packet of FU-A picture 	43 2.430121 me 30: 1442 byt ernet II, Src: ernet Protocol - Datagram Prot - Datagram Prot - Time Transpor 54 U identifier 0	19:08:48.716086 tes on wire (11536 b AxisComm_9c:6b:e7 (Version 4, Src: 172 tocol, Src Port: 500 rt Protocol F bit: No bit error: Nal_ref_idc (NRI): :	- its), 1442 bytes captured (11538 actor8te:95(-65); Dst: NErco-5 .25,201.100; Dst: 172.25.201.50 00; Dst Port: 62990 s or other syntax violations 3	i bits) on interfa	- ce \Device\NPF_{DCF558AC-89DD-4A9B-933C-62F		1442 Fra.		,
.0 = find bit: Not the last packet of fU-A picture .0	43 2.430121 me 30: 1442 by ernet II, Src: ernet Protocol Datagram Prot Julian Protocol 4 U identifier 0	19:08:48.716086 tes on wire (11536 b AxisComm_9c:6b:e7 (Version 4, Src: 172 tocol, Src Port: 500 rt Protocol F bit: No bit error: Nal_ref_idc (NRI): :	- its), 1442 bytes captured (11538 actor8te:95(-65); Dst: NErco-5 .25,201.100; Dst: 172.25.201.50 00; Dst Port: 62990 s or other syntax violations 3	i bits) on interfa	- ce \Device\NPF_{DCF558AC-89DD-4A9B-933C-62F		1442 Fra.		,
e = forbidden bit: 0 0 0101 = Hal_unit_type: Coded slice of an IDR picture (5) COM ANL Unit Fayricad	43 2.430121 me 30: 1442 byt rrnet II, Src: rrnet Protocol batagram Prot 44 U identifier 0	19:08:48.716086 tes on wire (11536 b AxisComm_9c:6b:e7 (Version 4, Src: 172 tecol, Src Port: 500 rt Protocol F bit: No bit error Nal_ref_idc (NRI): : Type: Fragmentation		i bits) on interfa	- ce \Device\NPF_{DCF558AC-89DD-4A9B-933C-62F		1442 Fra.		>
0 810 = Hal_unit_type: Coded slice of an IDR picture (5) ECA MAL Unit Fungicant	43 2.430121 me 30: 1442 byt ernet II, Src: ernet Protocol - Datagram Prot L-Time Transpor 54 U identifier 0	19:08:48.716086 tes on wire (11536 b AxisComm_9c:6b:67 (Version 4, Src: 172 tocol, Src Port: 500 rt Protocol F bit: No bit error Nal_ref_idc (NRJ): Type: Fragmentation Start bit: the firs		i bits) on interfa	- ce \Device\NPF_{DCF558AC-89DD-4A9B-933C-62F		1442 Fra.		,
H264 NAL Unit Payload	43 2.430121 me 30: 1442 by rmet II, Src: rmet Protocol - Time Transpos - Datagram Prot - U identifier 0	19:08:48.716086 tes on wire (11536 b AxisComm_9c:6b:e7 (Version 4, Src: 172 tocol, Src Port: S00 rt Protocol F bit: No bit error Nal_ref_idc (NRI): : Type: Fragmentation Start bit: the firs End bit: Not the la		i bits) on interfa	- ce \Device\NPF_{DCF558AC-89DD-4A9B-933C-62F		1442 Fra.		
	43 2.430121 me 30: 1442 byf ernet II, Src: ernet Protocol - Datagram Prot - Ditagram Prot - Time Transpoo 54 U identifier 0	19:08:48.716086 tes on wire (11536 b AxisComm_9c:6b:e7 (Version 4, Src: 172 tocol, Src Port: 500 rt Protocol F bit: No bit error Nal_ref_idc (NRT): : Type: Fragmentation Start bit: he firs: End bit: Not the la Forbidden bit: 0	(1153) ist), L442 bytes captured (1153) exect (0.68)(0.017), Dirt (licer-5 2.7.20.21.00, Dirt (172.3.201.00 00, Dirt Port: 6.2990 is or other syntax violations of unit A (\overline{r} U-A) (28) to packet of FU-A picture ts packet of FU-A picture	i bits) on interfa	- ce \Device\NPF_{DCF558AC-89DD-4A9B-933C-62F		1442 Fra.		>
	43 2.430121 me 30: 1442 byt ernet II, Src: ernet Protocol - Datagram Proto- - Datagram Proto- - U identifier 0	19:08:48.716086 tes on wire (11536 b AxisComm_9c:06:17 (Version 4, Src: 172 tocol, Src Port: 500 rt Protocol F bit: No bit error Nal_ref_idc (NRI): : Type: Fragmentation Start bit: the firs' End bit: Not the la Forbidden bit: 0 Nal_unit_type: Code	(1153) ist), L442 bytes captured (1153) executes(science)) bit (lice-5 2.2.3.2.1.3.00, 0.5.1172, 3.5.20.1.50 80, Dit Port: 6.2990 is or other syntax violations of unit A ($70-A$) (28) to packet of $70-A$ picture ts packet of $70-A$ picture	i bits) on interfa	- ce \Device\NPF_{DCF558AC-89DD-4A9B-933C-62F		1442 Fra.		>
1 = first_mb_in_slice: 0	43 2.430121 me 30: 1442 byt srnet II, Src: srnet Protocol - Datagram Prot - Datagram Prot - L-Time Transpos 	19:88:48.716086 tes on wire (11536 b ArisComm Sreber?) Version 4, src: 172 tocol, src Port: 500 rt Protocol F bit: No bit error Nal_ref_idc (NRI): : Type: Fragments End bit: No the large Start bit: to firs End bit: No the Start Start bit: 0 Nal_unit_type: Code Reglad		i bits) on interfa	- ce \Device\NPF_{DCF558AC-89DD-4A9B-933C-62F		1442 Fra.		,
.011 = slice_type: I (I slice) (2)	43 2.430121 me 30: 1442 byn srnet II, Src: srnet Protocol - Time Transpor 44 0	19:08:48.716086 tes on wire (11536 b AxisComm SciBior () Version 4, Src: 172 tocol, Src Port: 500 rt Protocol F bit: No bit error Nal_ref_idc (NRI): Type: Fragmentation Start bit: the firs Tobit: Not the la Forbidden bit: 0 Nal_unit_type: Code Payload first_mbin_slice:	iti), 1442 bytes ceptured (1153 accccles(6)(b)(2)), btt; Hicro's 22:20:31.080, 06:1722:52:301.90 000, Dst Port: 52290 a or other syntax violations a unit A (FU-A) (28) c packet of FU-A picture t packet of FU-A picture d slice of sn IDR picture (5) 0	i bits) on interfa	- ce \Device\NPF_{DCF558AC-89DD-4A9B-933C-62F		1442 Fra.		
1 = pic_parameter_set_id: 0	43 2.430121 ac 30: 1442 by srnet II, Src: srnet Protocol - Datagram Prot - Datagram Prot - Uidentifier 0	19:08:48.716086 tes on wire (11536 b AxisComm Sci0bird) Version 4, Scien 122 totool, Scie Port: 180 the Portson F bit: No bit error Nal_ref_idc (NRT): Type: Fragmentation Start bit: Not frain Forbidden bit: 0 Nal_unit_type: Code Payload first_b_in_slice: I (I al Science I (I al)	<pre>int). 1442 bytes.coptured (11358 exists). 1442 bytes.coptured (11358 exists). 2819(20). Ditt. Nicro-5 25.2.931.80, Bott Firz.52.291.80 B0, Dit Port: 62998 is or other syntax violations on int A (FU-A) (28) b packet of FU-A picture is packet of FU-A picture d slice of an IDR picture (5) Dices) (2)</pre>	i bits) on interfa	- ce \Device\NPF_{DCF558AC-89DD-4A9B-933C-62F		1442 Fra.		,
Y [Not decoded yet]	43 2.430121 == 30: 1442 byternet II, Src: rmet Protocol = Datagram Protocol = Datagram Protocol = Datagram Protocol = 0	19:08:48.716086 tas on wine (11358 b statics on setting of the statics of the set of the	<pre>int). 1442 bytes.coptured (11358 exists). 1442 bytes.coptured (11358 exists). 2819(20). Ditt. Nicro-5 25.2.931.80, Bott Firz.52.291.80 B0, Dit Port: 62998 is or other syntax violations on int A (FU-A) (28) b packet of FU-A picture is packet of FU-A picture d slice of an IDR picture (5) Dices) (2)</pre>	i bits) on interfa	- ce \Device\NPF_{DCF558AC-89DD-4A9B-933C-62F		1442 Fra.		
V [Expert Info (Warning/Undecoded): [Not decoded yet]] [[Inter decoded yet]]	43 2.430121 me 30: 1442 byt srmet II, Src: rmet Protocol Datagram Protocol Datagram Protocol U dentifier U dentifier U dendet I U dendet I U dendet U U d	19:08:48.716086 tes on wire (11536 b AxisComm SciBoir () Version 4, Scie 122 totool, Scie Port: 180 f bit: No bit arror Nal_ref Jdc (WRI): Type: Fragmentation Start bit: No frist Forbidden bit: 0 Nal_unit_type: Code Payload first_bd_Inslice: (I slice_type: I (slice) pic_parameter_set_i yet]	<pre>iti). 1442 bytes captured (1133 beccc.18/95/0b)e7). Ditt Nicro-5 25:2031.080, Dott 172.25:201.80 000, Dit Port: 62990 in or other syntax violations out: A (FU-A) (28) b packet of FU-A picture st packet of FU-A picture d slice of an IDR picture (3) a lice) (2).</pre>	i bits) on interfa	- ce \Device\NPF_{DCF558AC-89DD-4A9B-933C-62F		1442 Fra.		

Media streaming

282 2.458613	UTC Time Pade	age Delta Source MAC		Port Destination MAC Destination	Destination Port Protocol	Length Type Info	Time
283 2.458733	19:08:48.744578 19:08:48.744698	0.000119 AxisComm_9c:6b:e7 0.000120 AxisComm_9c:6b:e7		50000 Micro-St_e2:48:b5 172.25.20 50000 Micro-St_e2:48:b5 172.25.20		1442 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21868, Time=4244011526 FU-A 1442 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21869, Time=4244011526 FU-A	
284 2.458852	19:08:48.744817	0.000119 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264	1442 Fra. PT=DynamicRTP-Type-96, SSRC=0xB1E69128, Seq=21870, Time=4244011526 FU-A	
185 2.458985 186 2.459089	19:08:48.745054	0.000133 AxisComm_9c:6b:e7 0.000104 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20 50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264	1442 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21871, Time=4244011526 FU-A 1442 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21872, Time=4244011526 FU-A	End of
87 2.459208 88 2.459328	19:08:48.745173 19:08:48.745293	0.000119 AxisComm_9c:6b:e7 0.000120 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20 50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264	1442 Fra. PT=DynamicRTP-Type-96, SSRC=0xB1E69128, Seq=21873, Time=4244011526 FU-A	
89 2.459447 90 2.459566	19:08:48.745412	0.000119 AxisComm_9c:6b:e7 0.000119 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20 50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264	1442 Fra. PT=DynamicRTP-Type-96, SSRC=0xB1E69128, Seq=21875, Time=4244011526 FU-A	-Frame
91 2.459685	19:08:48.745650	0.000119 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264	1442 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21877, Time=4244011526 FU-A	
92 2.459805 93 2.459970	19:08:48.745770 19:08:48.745935	0.000120 AxisComm_9c:6b:e7 0.000165 AxisComm_9c:6b:e7	172.25.201.100 172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20 50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264 .50 62990 H264	1442 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21878, Time=4244011526 FU-A 1442 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21879, Time=4244011526 FU-A	
94 2.460078 95 2.460078	19:08:48.746043 19:08:48.746043	0.000108 AxisComm_9c:6b:e7 0.000000 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20 50000 Micro-St e2:48:b5 172.25.20	.50 62990 H264	1442 Fra. PT-DynamicRTP-Type-96, SSRC-0x81E69128, Seq=21880, Time=4244011526 FU-A 157 Fra. PT-DynamicRTP-Type-96, SSRC-0x81E69128, Seq=21881, Time=4244011526, Mark FU-	-A Fod
96 2.460208 97 2.460208	19:08:48.746173	0.000130 AxisComm_9c:6b:e7 0.000000 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:b5 172.25.20	.50 62990 H264	1442 Fra. PT-DynamicRTP-Type-96, SSRC=0xB1E69128, Seq=21882, Time=4244014526 FU-A Star	rt:non-IDR-Slice
98 2.477453	19:08:48.746173 19:08:48.763418	0.017245 Micro-St_e2:48:b5	172.25.201.50	50000 Micro-St_e2:48:b5 172.25.20 55423 AxisComm_9c:6b:e7 172.25.20	.100 554 TCP	188 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21883, Time=4244014526, Mark FU- 54 55423 → 554 [ACK] Seq=2381 Ack=2626 Win=2101760 Len=0	
99 2.484414 00 2.484414	19:08:48.770379 19:08:48.770379	0.006961 AxisComm_9c:6b:e7 0.000000 AxisComm 9c:6b:e7	172.25.201.100 172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20 50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264 .50 62990 H264	1442 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21884, Time=4244017526 FU-A Star 363 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21885, Time=4244017526, Mark FU-	rt:non-IDR-Slice -A End
01 2.517565 02 2.517565	19:08:48.803530 19:08:48.803530	0.033151 AxisComm_9c:6b:e7 0.000000 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20 50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264	1442 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21886, Time=4244020525 FU-A Star 677 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21887, Time=4244020525, Mark FU-	rt:non-IDR-Slice
03 2.550710	19:08:48.836675	0.033145 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264	1442 Fra. PT=DvnamicRTP-Tvpe-96, SSRC=0x81E69128, Seg=21888, Time=4244023525 FU-A Star	rt:non-IDR-Slice
04 2.550710 05 2.584065	19:08:48.836675 19:08:48.870030	0.000000 AxisComm_9c:6b:e7 0.033355 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20 50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264	827 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21889, Time=4244023525, Mark FU- 1442 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21890, Time=4244026525 FU-A Star	rt:non-IDR-Slice
06 2.584065 07 2.617417	19:08:48.870030 19:08:48.903382	0.000000 AxisComm_9c:6b:e7 0.033352 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20 50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264	1372 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21891, Time=4244026525, Mark FU- 1442 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21892, Time=4244029525 FU-A Star	-A End rt:non-IDR-Slice
08 2.617417 09 2.650733	19:08:48.903382 19:08:48.936698	0.000000 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264	655 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21893, Time=4244029525, Mark FU-	-A End
0 2.650733	19:08:48.936698	0.033316 AxisComm_9c:6b:e7 0.000000 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20 50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264	1442 Fra. PT-DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21894, Time=4244032524 FU-A Star 1275 Fra. PT-DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21895, Time=4244032524, Mark FU	-A End
11 2.684164 12 2.684164	19:08:48.970129 19:08:48.970129	0.033431 AxisComm_9c:6b:e7 0.000000 AxisComm_9c:6b:e7	172.25.201.100 172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20 50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264 .50 62990 H264	1442 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21896, Time=4244035524 FU-A Star 1362 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21897, Time=4244035524, Mark FU-	rt:non-IDR-Slice -A End
13 2.717455	19:08:49.003420 19:08:49.003420	0.033291 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264	1442 Fra. PT=DynamicRTP-Type-96, SSR=0x81E69128, Seq=21898, Time=4244938524 FU-A Star 1232 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21899, Time=4244938524, Mark FU-	rt:non-IDR-Slice
15 2.750879	19:08:49.036844	0.000000 AxisComm_9c:6b:e7 0.033424 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20 50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264	1442 Fra. PT=DynamicRTP-Type-96, SSRC=0xB1E69128, Seq=21900, Time=4244041523 FU-A Star	rt:non-IDR-Slice
16 2.750879 17 2.751035	19:08:49.036844 19:08:49.037000	0.000000 AxisComm_9c:6b:e7 0.000156 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20 50000 Micro-St_e2:48:b5 172.25.20	.50 62990 H264	1442 Fra PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21901, Time=4244041523 FU-A 1442 Fra PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21902, Time=4244041523 FU-A	
L8 2.751035 L9 2.784077	19:08:49.037000	0.000000 AxisComm_9c:6b:e7 0.033042 AxisComm 9c:6b:e7	172.25.201.100 172.25.201.100	50000 Micro-St_e2:48:b5 172.25.20 50000 Micro-St e2:48:b5 172.25.20	.50 62990 H264 .50 62990 H264	353 Fra. PT=DynamicRTP-Type-96, SSRC=0x81E69128, Seq=21903, Time=4244041523, Mark FU- 1442 Fra. PT=DynamicRTP-Type-96. SSRC=0x81E69128. Seg=21904. Time=4244044523 FU-A Star	-A End
0= .11= 1 1100 = Header 0= .1=	End bit: the last pac	nit A (FU-A) (28) st packet of FU-A picture				Packets: 19155 - Displayed: 19155 (100.0%)	Pro
.11 = 1 1100 = U Header 0 = .1 = Text item (text), : ork_Trace_RICP_RT	Nal_ref_idc (NRI): 3 Type: Fragmentation un Start bit: Not the fi End bit: the last pack Ibyte PP_SE_Timestamps.pcapng	nit A (FU-A) (28) "st packet of FU-A picture set of FU-A picture				Packets: 19155 - Displayed: 19155 (100.0%)	- 0
0 = 1100 1100	Nal_ref_idc (NRI): 3 Type: Fragmentation un Start bit: Not the fii End bit: the last pack Ibyte P_SELTimestampsprapng Capture Analyze Statist X C Q & m M S	hit A (FU-A) (28) "st packet of FU-A picture tet of FU-A picture ics Telephony Wireles Jook F ▲ □ □ ● Q Q Q					- 0
0 = 1 1100 I Header = 0 = I Header = = Text item (text), : wrk_Trace_RTCP_RT it Yiew Go Image: Second Go (Second Go	Nal_ref_idc (NRI): 3 Type: Fragmentation un Start bit: Not the fi End bit: the last pack Ibyte P_SELTemestamps.pcapng Capture Analyze Statist	tit A (FV-A) (28) The packet of FU-A picture tet of FU-A picture Sector FU-A picture The appendix Sector Sect	ce Port Destination MAC 1 50000 Micro-St_e2:48:55		1442 Fra. PT=Dynami	The Store - SSRCBudit69128, Seq-21874, Time-4244011526 FU-A	- 0
0 =	Nal_ref_ide (NRI): 3 Type: fragmentation w Start bit: Not the fi End bit: the last and hype: Sel_Timestamp:pcaping Cepture Analyze Subst Cepture Analyze Subst Debas Source NAC Debas Source NAC Debas Source MAC BODI2A Axiscom Scribb BODI2A Axiscom Scribb	tit A (FV-A) (28) → packet of FV-A picture tet of FV-A picture → Display by the size of FV-A	ce Port Destination MAC 59000 Micro-St_e2:48:b5 50000 Micro-St_e2:48:b5 50000 Micro-St_e2:48:b5	172.25.201.50 62990 H26 172.25.201.50 62990 H26 172.25.201.50 62990 H26 172.25.201.50 62990 H26	1442 Fra PT=Dynami 1442 Fra PT=Dynami 1442 Fra PT=Dynami	CRTP-Type-96, 536C-0x01269120, 5ee-21874, Time-6244011526 FU-A CRTP-Type-96, 536C-0x01269120, 5ee-21875, Time-4244011526 FU-A CRTP-Type-96, 556C-0x01269120, 5ee-21875, Time-4244011526 FU-A	- 0
0 =	Nal_ref_ide (NRI): 3 Type: Fragmentation with End bit: the last and bit: the last and provide the state of the provide state of the Capture Analyse Statist Capture Analyse St	tit A (FU-A) (28) "st packet of FU-A picture et of FU-A picture TU-A	Destination MAC Destination MAC 50000 Micro-St_e2:48:b5 50000 Micro-St_e2:48:b5 50000 Micro-St_e2:48:b5 50000 Micro-St_e2:48:b5	172.25.201.50 62990 H26	1442 Fra PT=Dynami 1442 Fra PT=Dynami 1442 Fra PT=Dynami 1442 Fra PT=Dynami	CETP-Type-96, 5587-0-00159130, 5ex-11274, Time-044011356 FU-A CETP-Type-96, 5587-0-00159030, 5ex-21275, Time-044011356 FU-A CETP-Type-96, 5587-0-00159030, 5ex-21275, Time-044011356 FU-A CETP-Type-96, 5587-0-00159030, 5ex-21277, Time-044011356 FU-A	- 0
θ	Nal_ref_ide (NRI): a Start bit: Not the fil End bit: the last acc link bit: the last acc link P.SI.Imestamps.pcapg Capture Analyse Subst Capture Analyse Subst	tit A (FU-A) (28) The packet of FU-A picture at of FU-A picture t of FU-A picture T = 1 = 0, eq. (1) (1) = 1, (2)	Destination MAC Destination MAC 50000 Hicro-St_e2:48:b5 50000 Hicro-St_e2:48:b5 50000 Micro-St_e2:48:b5 50000 Micro-St_e2:48:b5 50000 Hicro-St_e2:48:b5 50000 Hicro-St_e2:48:b5	172.25.201.50 62990 H26	 1442 Fra PT-Dynami. 	CRTP-Type-96, SSRC-9x81E69128, Seq-21874, Tise-4244911536 FU-A GRTP-Type-96, SSRC-9x81E69128, Seq-21875, Tise-4244911536 FU-A GRTP-Type-96, SSRC-9x81E9128, Seq-21875, Tise-4244911536 FU-A GRTP-Type-96, SSRC-9x81E9128, Seq-21879, Tise-4244911526 FU-A GRTP-Type-96, SSRC-9x81E9128, Seq-21879, Tise-4244911526 FU-A	- 0
θ	Nal_ref_ide (NRI): a Start bit: Not the fil find bit: the last act info bit: the last act bits P.50; Imestamps.pcapa Capture Analyse Statut Capture Analyse Stat	tit A (FU-A) (28) t packet of FU-A picture et of FU-A picture store and fU	ce Port Destination MAC 50000 Micro-St_02:48:15	172. 25. 201. 50 62990 H26	1442 Fra. PT-Dynami 1442 Fra. PT-Dynami 1442 Fra. PT-Dynami 1442 Fra. PT-Dynami 1442 Fra. PT-Dynami 1442 Fra. PT-Dynami 1442 Fra. PT-Dynami 157 Fra. PT-Dynami	CRTP-Type-96, SSRC-0x01609128, Seq-21874, Time-4244011526 FU-A CRTP-Type-96, SSRC-0x01609128, Seq-21875, Time-4244011526 FU-A CRTP-Type-96, SSRC-0x016109128, Seq-21877, Time-4244011526 FU-A CRTP-Type-96, SSRC-0x016109128, Seq-21877, Time-4244011526 FU-A CRTP-Type-96, SSRC-0x016109128, Seq-21877, Time-4244011526 FU-A CRTP-Type-96, SSRC-0x016109128, Seq-21878, Time-524011526 FU-A CRTP-Type-96, SSRC-0x01640000, Seq-21878, Time-524011526 FU-A CRTP-Type-96, SSRC-0x0164000, Seq-21878, Time-524011526 FU-A CRTP-Type-96, SSRC-0x016400, Seq-21878, Time-524011526 FU-A CRTP-Type-96, SSRC-0x016400, Seq-21878, Time-524011526 FU-A CRTP-Type-96, SSRC-0x016400, Seq-2188, Seq-21878, Time-524011526 FU-A CRTP-Type-96, SSRC-0x016400, Seq-2188, Seq-21878, Time-524011526 FU-A CRTP-Type-96, SSRC-0x016400, Seq-2188, Seq-21878, Seq-21878, Time-524011526 FU-A FU-A FU-A FU-A FU-A FU-A FU-A FU-A	- 0 previous f TOP Window Size rame
0	Nal_ref_ide (NRI): 3 Vipe: Fragmentation un Start bit: Not the fit ind bit: Not the fit ind bit: Not the fit ind bit: Not the fit Defa Source MAC Bit Add Sourc	tit A (FU-A) (28) "t packet of FU-A picture et of FU-A picture by the second secon	ce Port Destination MAC 500000 Micro-St_02448:b5	172.55.201.50 62990 H26 172.52.201.50 62990 H26 172.25.201.50 62990 H26	1442 Fra. PT-Oynami. 1442 Fra. PT-Oynami. 1442 Fra. PT-Oynami. 1442 Fra. PT-Oynami. 1442 Fra. PT-Oynami. 1442 Fra. PT-Oynami. 1442 Fra. PT-Oynami. 157 Fra. PT-Oynami. 1442 Fra. PT-Oynami. 188 Fra. PT-Oynami.	CRTP-Type-96, SSGC=001169128, Sep-21874, Time=4244911526 FU-A Tme:smcr CRTP-Type-96, SSGC=001169128, Sep-21874, Time=4244911526 FU-A CRTP-Type-96, SSGC=001169128, Sep-21877, Time=4244911526 FU-A CRTP-Type-96, SSGC=001169128, Sep-21877, Time=4244911526 FU-A CRTP-Type-96, SSGC=001169128, Sep-21877, Time=4244911526 FU-A CRTP-Type-96, SSGC=001169128, Sep-21877, Time=4244911526 FU-A CRTP-Type-96, SSGC=001169128, Sep-21877, Time=4244911526 FU-A CRTP-Type-96, SSGC=001169128, Sep-21877, Time=4244911527, FU-A Startmon-128-Starter CRTP-Type-96, SSGC=001169128, Sep-21893, Time=424491257, FU-A Startmon-128-Starter CRTP-Type-96, SSGC=001169128, Sep-21893, Time=424491257, FU-A Startmon-128-Starter CRTP-Type-96, SSGC=001169128, Sep-21893, Time=424491257, FU-A Startmon-128-Starter	- o revious 1 TCP Window Size rame Frame 1
9	Nal_ref_ide (NBI): 3 Start bit: Not the fi Ind bit: the last motion P.5E.Timestampip.caps Capture Amyles Suisti Capture Amyles Suis	tit A (FU-A) (28) 	cs Port Destination MAC 500000 Hitcro-St_g2148135	172.15.201.50 6.2990 H26	1442 Fra., PT-Qynail. 1442 Fra., PT-Qynail.	cttp-Type-46, 5564-060150105, 5eq-11574, Time-244011516 FU-A The short cttp-Type-46, 5564-060150105, 5eq-21175, Time-244011516 FU-A Cttp-Type-46, 5564-060150105, 5eq-21175, Time-244011556 FU-A cttp-Type-46, 5564-060150105, 5eq-21175, Time-244011556 FU-A Cttp-Type-46, 5564-060150105, 5eq-21175, Time-244011556 FU-A cttp-Type-46, 5564-060150105, 5eq-21175, Time-244011556 FU-A Cttp-Type-46, 5564-060150105, 5eq-21175, Time-244011556 FU-A cttp-Type-46, 5564-060150105, 5eq-21175, Time-244011556 FU-A Cttp-Type-46, 5564-060150105, 5eq-21175, Time-244011556, FU-A cttp-Type-46, 5564-060150105, 5eq-21175, Time-244011556, FU-A Cttp-Type-46, 5564-060150105, 5eq-21185, Time-244011556, FU-A cttp-Type-46, 5564-060150105, 5eq-21180, Time-244011557, FU-A Cttp-Type-46, 5564-060150105, 5eq-21186, Time-244011557, FU-A cttp-Type-46, 5564-060150105, 5eq-21180, Time-244011557, FU-A FU-A cttp-Type-46, 5564-060150105, 5eq-21180, Time-244011557, FU-A FU-A cttp-Type-46, 5564-060150105, 5eq-21180, Time-244011557, FU-A FU-A cttp-Type-46, 5564-060150105, 5eq-21180, Time-244011576, FU-A FU-A	- 0 previous f TOP Window Size rame
9	Nal_ref_ide (NRI): 3 Vipe: Fragmentation un Start bit: Not the fit ind bit: bel ast. and ind bit: bel ast. and Della Source MAC MOIIS A ALICOM 2 (1) Della Source MAC MOIIS A ALICOM 2 (1) MOIIS A ALICOM 2 (1) MO	tit A (FU-A) (28) t packet of FU-A picture et of FU-A picture t picture	ce Port Destination MAC 500000 Micros 51; e2148155	172.152.201.50 62999 126 172.152.201.50 62999 126 172.152.201.50 62999 126 172.152.201.50 62999 126 172.152.201.50 62999 126 172.152.201.50 62999 126 172.152.201.50 62999 126 172.152.201.50 62999 126 172.152.201.50 62999 126 172.152.201.50 62999 126 172.152.201.50 62999 126 172.152.201.50 62999 126 172.152.201.50 62999 126 172.152.201.50 62999 126 172.152.201.50 62999 126 172.152.201.50 62999 126	1442 Fra., PT-Qynail. 1442 Fra., PT-Qynail.	GTP-Type-66, 558C-0x81609128, 5eq-21174, T1se-4244011536 FU-A GTP-Type-66, 558C-0x81609128, 5eq-21174, T1se-4244011536 FU-A GTP-Type-66, 558C-0x816190128, 5eq-21177, T1se-4244011536 FU-A GTP-Type-66, 558C-0x816190128, 5eq-21177, T1se-4244011536 FU-A GTP-Type-66, 558C-0x816190128, 5eq-21179, T1se-4244011536 FU-A GTP-Type-66, 558C-0x816190128, 5eq-21179, T1se-4244011536 FU-A GTP-Type-66, 558C-0x816190128, 5eq-21189, T1se-324011757, FU-A tot GTP-Type-66, 558C-0x816190128, 5eq-21189, T1se-324011757, FU-A tot GTP-Type-66, 558C-0x816190128, 5eq-21188, T1se-32401757, FU-A tot GTP-Type-66, 558C-0x8169128, 5eq-21188, T1se-32401757, FU-A tot GTP-Type-66, 558C-0x8169128, 5eq-21188, T1se-32401757, FU-A tot GTP-Type-66, 558C-0x8169128, 5eq-21188, T1se-32401757, FU-A tot GTD-Type-66, 558C-0x8169128, 5eq-21188, T1se-32401757, FU-A	- o revious 1 TCP Window Size rame Frame 1
9	Nal_ref_ide (NRI): 3 Start bit: Not the fit ind bit: Not the fit ind bit: Not the fit ind bit: Not the fit problem and the start of the start problem and the start of the start Defa Source MAC BODITA Acidems Scieb BODITA Acidems Scie	tit A (FU-A) (28) "t packet of FU-A picture et of FU-A picture tot of FU-A picture Source 7 172,25,201,100 7 172,25,201,000 7 172,25,201,000 7 172,25,201,000 7 17	ce.Port Destination MAC 50000 Micro-St, e2148155	172, 155, 201, 96 0.0990 465 172, 155, 201, 96 0.2990 465 172, 155, 201, 96 0.2990 465 172, 155, 201, 96 0.2990 465 172, 155, 201, 96 0.2990 465 172, 155, 201, 96 0.2990 465 172, 155, 201, 96 0.2990 465 172, 155, 201, 96 0.2990 465 172, 155, 201, 96 0.2990 465 172, 155, 201, 96 0.2990 465 172, 155, 201, 96 0.2990 465 172, 155, 201, 96 0.2990 465 172, 155, 201, 96 0.2990 465 172, 155, 201, 96 0.2990 465 172, 155, 201, 96 0.2990 456 172, 155, 201, 96 0.2990 456 172, 155, 201, 96 0.2990 456 172, 155, 201, 96 0.2990 456 172, 155, 201, 96 0.2990 456 172, 155, 201, 96 0.2990 456 172, 152, 201, 96 0.2990 </td <td>1442 Fra. PT-Qynail 1442 Fra. PT-Qynail 1443 Fra. PT-Qynail 1444 Fra. PT-Qynail 1444 Fra. PT-Qynail 1444 Fra. PT-Qynail</td> <td>cdPP-Type-96, SSC-000169128, Seq-21874, Time-2244911526 FU-A cdPP-Type-96, SSC-000169128, Seq-21875, Time-244811526 FU-A cdPP-Type-96, SSC-000169128, Seq-2188, Time-244811526, FU-A cdPP-Type-96, SSC-000169128, Seq-2188, Time-244811527, FU-A cdPP-Type-96, SSCC-000169128, Seq-2188, Time-244811527, FU-A cdPP-Type-96, SSC-000169128, Seq-2188, Time-244811527, FU-A cdPP-Type-96, SSC-000169128, Seq-2188, Time-244811527, FU-A cdPP-Type-96, SSC-000169128,</td> <td>- a previoual TCP Window Save rame Frame 1 Frame 1 Frame 2 Frame 3</td>	1442 Fra. PT-Qynail 1442 Fra. PT-Qynail 1443 Fra. PT-Qynail 1444 Fra. PT-Qynail 1444 Fra. PT-Qynail 1444 Fra. PT-Qynail	cdPP-Type-96, SSC-000169128, Seq-21874, Time-2244911526 FU-A cdPP-Type-96, SSC-000169128, Seq-21875, Time-244811526 FU-A cdPP-Type-96, SSC-000169128, Seq-2188, Time-244811526, FU-A cdPP-Type-96, SSC-000169128, Seq-2188, Time-244811527, FU-A cdPP-Type-96, SSCC-000169128, Seq-2188, Time-244811527, FU-A cdPP-Type-96, SSC-000169128, Seq-2188, Time-244811527, FU-A cdPP-Type-96, SSC-000169128, Seq-2188, Time-244811527, FU-A cdPP-Type-96, SSC-000169128,	- a previoual TCP Window Save rame Frame 1 Frame 1 Frame 2 Frame 3
0	Nal_ref_ide (NBI): 3 Start bit: Not the fil Ind bit	tit A (19-A) (28) "It packet of FU-A picture et of FU-A picture T-A picture Source Source T-27, 25, 201, 100 T-27, 25,	Control Destination MAC Seeten Hitroro 54, 22, 488, 355 Seeten Hitroro 54, 248, 485, 356 Seeten Hitroro 54, 248, 485, 356	172, 155, 201, 96 COPMO R65 172, 155, 201, 96 COPMO R65 <t< td=""><td>1442 Fra. PT-Oynai. 1442 Fra. PT-Oynai. 1442 Fra. PT-Oynai. 1442 Fra. PT-Oynai. 1442 Fra. PT-Oynai. 1442 Fra. PT-Oynai. 1442 Fra. PT-Oynai. 1457 Fra. PT-Oynai.</td><td>cftP-Type-95, 553C-000169128, 5eq-21874, Time-4244011355 FU-A cftP-Type-96, 553C-000169128, 5eq-21875, Time-4244011355 FU-A cftP-Type-96, 553C-000169128, 5eq-21875, Time-4244011355 FU-A cftP-Type-96, 553C-000169128, 5eq-21875, Time-4244011355 FU-A cftP-Type-96, 553C-000169128, 5eq-21875, Time-4244011355 FU-A cftP-Type-96, 553C-000169128, 5eq-21875, Time-4244011355 FU-A cftP-Type-96, 553C-000169128, 5eq-21875, Time-4244011357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-4244011357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-4244011357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-4244011357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-4244011357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-4244011357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-4244011357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-424401357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-424401357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-424401357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-424401357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-424401357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-42440157, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-424401525, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2189, Time-424405255, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2189, Time-42</td><td>- σ revisual 1 TO Window Sze rame Frame 1 Frame 2</td></t<>	1442 Fra. PT-Oynai. 1442 Fra. PT-Oynai. 1442 Fra. PT-Oynai. 1442 Fra. PT-Oynai. 1442 Fra. PT-Oynai. 1442 Fra. PT-Oynai. 1442 Fra. PT-Oynai. 1457 Fra. PT-Oynai.	cftP-Type-95, 553C-000169128, 5eq-21874, Time-4244011355 FU-A cftP-Type-96, 553C-000169128, 5eq-21875, Time-4244011355 FU-A cftP-Type-96, 553C-000169128, 5eq-21875, Time-4244011355 FU-A cftP-Type-96, 553C-000169128, 5eq-21875, Time-4244011355 FU-A cftP-Type-96, 553C-000169128, 5eq-21875, Time-4244011355 FU-A cftP-Type-96, 553C-000169128, 5eq-21875, Time-4244011355 FU-A cftP-Type-96, 553C-000169128, 5eq-21875, Time-4244011357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-4244011357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-4244011357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-4244011357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-4244011357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-4244011357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-4244011357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-424401357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-424401357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-424401357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-424401357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-424401357, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-42440157, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2188, Time-424401525, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2189, Time-424405255, Next FU-A for cftP-Type-96, 553C-000169128, 5eq-2189, Time-42	- σ revisual 1 TO Window Sze rame Frame 1 Frame 2
0	Nal_ref_ide (NRI): 3 Start bit: Not the fit ind bit: Not the fit ind bit: Not the fit ind bit: Not the fit ind bit: Not the fit Diffe Control Cont	tit A (FU-A) (28) t packet of FU-A picture et of FU-A picture t of FU-A picture 5 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	setup Destination MAC setup Incrost_e14835 setup Incrost_e24835 setup Incrost_e248355 setup Incrost_e24835 setup	172, 155, 201, 90 COPPIe Fac	1442 Fra. PT-Oynai 1442 Fra. PT-Oynai 1442 Fra. PT-Oynai 1442 Fra. PT-Oynai 1442 Fra. PT-Oynai 1442 Fra. PT-Oynai 1452 Fra. PT-Oynai	cdff7-7yg=46, 558c+08150120, 5eq-1157, Tim=-24401135 (FU.A The short cdf77-7yg=46, 558c+08150120, 5eq-21175, Tim=-24401135 (FU.A Control (Control (Contro) (Contro) (Control (Control (Control (Control (Control (Contro	- a previoual TCP Window Save rame Frame 1 Frame 1 Frame 2 Frame 3
0	Nal_ref_ide (NRI): 3 Start bit: Not the fil Ind bit: Not the fil Not the fil	tit A (FU-A) (28) "t packet of FU-A picture est of FU-A picture Source 0	Seeter Destination MAC Seeter IncrosSt_p2148155 <	17.1 55. 201.9 19.9 19.9 17.2 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19.9 19.9 17.1 55. 201.9 19.9 19	1441 Fra. PT-Oynai 1442 Fra. PT-Oynai 1442 Fra. PT-Oynai 1442 Fra. PT-Oynai 1442 Fra. PT-Oynai 1442 Fra. PT-Oynai 1442 Fra. PT-Oynai 1447 Fra. PT-Oynai	cfP-Type-96, SSC-000109128, Sep-2107A, Time-244011526 FU-A cfP-Type-96, SSC-000109128, Sep-2107A, Time-244011526 FU-A cfP-Type-96, SSC-000109128, Sep-2107A, Time-244011526 FU-A cfP-Type-96, SSC-000109128, Sep-2107A, Time-244011526 FU-A cfP-Type-96, SSC-000109128, Sep-2107A, Time-244011526 FU-A cfP-Type-96, SSC-000109128, Sep-2107A, Time-244011526 FU-A cfP-Type-96, SSC-000109128, Sep-2107A, Time-244011526 FU-A cfP-Type-96, SSC-000109128, Sep-2107A, Time-244011526 FU-A cfP-Type-96, SSC-000109128, Sep-2107A, Time-244011527, FU-A cfP-Type-96, SSC-000109128, Sep-2107A, Time-244011527, FU-A cfP-Type-96, SSC-000109128, Sep-2108, Time-244011527, FU-A cfP-Type-96, SSC-000109128, Sep-2108, Time-24401257, FU-A dime-100-5104 cfP-Type-96, SSC-000109128, Sep-2108, Time-24401257, FU-A dime-100-5104 p- cfP-Type-96, SSC-000109128, Sep-2108, Time-24401257, FU-A dime-100-5104 p- cfP-Type-96, SSC-000109128, Sep-2108, Time-2440257, FU-A true dime-5104 p-	- a previoual TCP Window Save rame Frame 1 Frame 1 Frame 2 Frame 3
9	Nal_ref_ide (NBI): 3 Start bit: Not the fil Ind bit: the last and list in the last and list i	tit A (FU-A) (28) 12: packet of FU-A picture ext of FU-A picture 5: Telephony Workes Jook 5: Telephony Workes Jook 6: Telephony Workes Jook 7: Telephony	ce. Port Destination MAC S00000 Inicros 5::;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;	172, 155, 201, 90 CC990 R65 172, 155, 201, 90 CC990 R65 </td <td>1447 Fra. PT-Oynai 1447 Fra. PT-Oynai 1457 Fra. PT-Oynai</td> <td>cftP-Type-95, 55C-000169120, 5eq-21074, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21075, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011326 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011326, FU-A cftP-Type-96, 55C-000169120, 5eq-2108, Time-4244011326, FU-A cftP-Type-96, 55C-000169120, 5eq-2108, Time-4244011326, FU-A cftP-Type-96, 55C-000169120, 5eq-2108, Time-424401257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2108, Time-424401257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2108, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2108, Time-424402157, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2108, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2108, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2109, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2109, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2109, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2109, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2109, Time-42440257, FU-A fdf</td> <td>- a previoual TCP Window Save rame Frame 1 Frame 1 Frame 2 Frame 3</td>	1447 Fra. PT-Oynai 1447 Fra. PT-Oynai 1457 Fra. PT-Oynai	cftP-Type-95, 55C-000169120, 5eq-21074, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21075, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011326 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011326, FU-A cftP-Type-96, 55C-000169120, 5eq-2108, Time-4244011326, FU-A cftP-Type-96, 55C-000169120, 5eq-2108, Time-4244011326, FU-A cftP-Type-96, 55C-000169120, 5eq-2108, Time-424401257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2108, Time-424401257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2108, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2108, Time-424402157, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2108, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2108, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2109, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2109, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2109, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2109, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2109, Time-42440257, FU-A fdf	- a previoual TCP Window Save rame Frame 1 Frame 1 Frame 2 Frame 3
0	Nal_ref_ide (NR1): 3 Start bit: Not the fit ind hit: the last add ind hit: the last add	tit A (FU-A) (28) t packet of FU-A picture et of FU-A picture t of FU-A picture 5 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	cr.htt Destination MAC Seebell Historo St. e2148135	172, 155, 201, 90 COPPO Factor 172, 15	1447 Fra. PT-Oynai 1447 Fra. PT-Oynai 1457 Fra. PT-Oynai	cftP-Type-95, 55C-000169120, 5eq-21074, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21075, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011325 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011326 FU-A cftP-Type-96, 55C-000169120, 5eq-21076, Time-4244011326, FU-A cftP-Type-96, 55C-000169120, 5eq-2108, Time-4244011326, FU-A cftP-Type-96, 55C-000169120, 5eq-2108, Time-4244011326, FU-A cftP-Type-96, 55C-000169120, 5eq-2108, Time-424401257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2108, Time-424401257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2108, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2108, Time-424402157, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2108, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2108, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2109, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2109, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2109, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2109, Time-42440257, FU-A fdf cftP-Type-96, 55C-000169120, 5eq-2109, Time-42440257, FU-A fdf	- a previoual TCP Window Save rame Frame 1 Frame 1 Frame 2 Frame 3
9	Nal_ref_ide (NRI): 3 Start bit: Not the fil Ind bit: Not the fil Ind bit: Not the fil Ind bit: Not the fil Delse and the second second Capture and the second second Capture and the second second Second Second Second Second Second Second Second Second Second Second Second Second Second Second	tit A (FU-A) (28) "t packet of FU-A picture et of FU-A picture tot of FU-A picture Source of 2 122,25,281,180 (7 122,2	Sector Destination MAC Sector Bitcro-St_e2148155	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	1447 Fra. PT-Oynai 1447 Fra. PT-Oynai 1457 Fra. PT-Oynai	cdP7-Type=6; SSC=001169123; Seq=21174; Tim==24401155; FU-A cdP7-Type=6; SSC=001169123; Seq=21175; Tim==24401155; FU-A cdP7-Type=6; SSC=001169123; Seq=21185; Tim==24401155; FU-A cdP7-Type=6; SSC=001169123; Seq=2118; Tim==24401155; FU-A cdP7-Type=6; SSC=001169123; Seq=2118; Tim==24401155; FU-A cdP7-Type=6; SSC=001169123; Seq=2118; Tim==24401155; FU-A Tim==24401155; cdP7-Type=6; SSC=001169123; Seq=2118; Tim==24401253; FU-A Tim=FU-A Tim==24401164; <t< td=""><td>- a previoual TCP Window Save rame Frame 1 Frame 1 Frame 2 Frame 3</td></t<>	- a previoual TCP Window Save rame Frame 1 Frame 1 Frame 2 Frame 3
0	Nal_ref_ide (NRI): 3 Start bit: Not the fil Ind bit: Not the fil Ind bit: Not the fil Capture anyoes beaution Capture anyoes b	<pre>stit A (FU-A) (28) "st packet of FU-A picture st of FU-A picture</pre>	Sector Destination MAC Sector IncrosSt_0148155 Sector <t< td=""><td>$\begin{array}{cccccccccccccccccccccccccccccccccccc$</td><td>1447 Fra. PT-Oynai 1447 Fra. PT-Oynai</td><td>cffP-Type-95, 55G-0b0169128, 5eq-2187A, Time-244011356 FU-A cffP-Type-96, 55G-0b0169128, 5eq-2187S, Time-244011356 FU-A cffP-Type-96, 55G-0b0169128, 5eq-2188, Time-244011357, FU-A cffP-Type-96, 55G-0b0169128, 5eq-2188, Time-24401257, FU-A cffP-Type-96, 55G-0b0169128, 5eq-2189, Time-24402525, FU-A cffP-Type-96, 55G-0b0169128, 5eq-2189, Time-24402525, FU-A fort contained to the top top top top top top top top top top</td><td>- a previoual TCP Window Save rame Frame 1 Frame 1 Frame 2 Frame 3</td></t<>	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	1447 Fra. PT-Oynai 1447 Fra. PT-Oynai	cffP-Type-95, 55G-0b0169128, 5eq-2187A, Time-244011356 FU-A cffP-Type-96, 55G-0b0169128, 5eq-2187S, Time-244011356 FU-A cffP-Type-96, 55G-0b0169128, 5eq-2188, Time-244011357, FU-A cffP-Type-96, 55G-0b0169128, 5eq-2188, Time-24401257, FU-A cffP-Type-96, 55G-0b0169128, 5eq-2189, Time-24402525, FU-A cffP-Type-96, 55G-0b0169128, 5eq-2189, Time-24402525, FU-A fort contained to the top	- a previoual TCP Window Save rame Frame 1 Frame 1 Frame 2 Frame 3
0	Nal_ref_ide (NR1): 3 Start bit: Not the fit ind hit: Not the fit Debis Source MAC Month Start Start Start Debis Source MAC MONTH ALL Start Start Debis Source MAC MONTH ALL Start Start Month Start Start Start Month Start Mo	tit A (FU-A) (28)	cs hort Destination MAC seeme Hisroro St. e2148135 seeme His	172, 155, 201, 90 COPPO PAS 172, 157, 201, 90 COPPO PAS <t< th=""><th>1444 Fra. PT-Oynai 144 Fra. PT-Oynai 144 Fra. PT-Oynai 144 Fra. PT-Oynai 144 Fra. PT-Oynai 144 Fra. PT-Oynai 145 Fra. PT-Oynai 146 Fra. PT-Oynai 146 Fra. PT-Oynai 146 Fra. PT-Oynai 147 Fra. PT-Oynai 148 Fra. PT-Oynai 148 Fra. PT-Oynai 148 Fra. PT-Oynai 148 Fra. PT-Oynai 149 Fra. PT-Oynai 149 Fra. PT-Oynai 140 Fra. PT-Oynai</th><th>cdfP-Type-Ms, SSG-me8169123, 5eq-1175, Time-d4481135 FU-A Fme short, cdfP-Type-Ms, SSG-me8169123, 5eq-2177, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2177, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2177, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2177, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2177, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2177, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2187, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2187, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2188, Time-d44811357, FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2188, Time-d44811357, FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2188, Time-d44811357, FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2188, Time-d44811357, FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2188, Time-d44811357, FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2188, Time-d4481237, FU-A Startinon, TMP-S11ce cdfP-Type-Ms, SSG-me8169123, 5eq-2188, Time-d4481235, FU-A Startinon, TMP-S11ce p- cdfP-Type-Ms, SSG-me8169123, 5eq-2189, Time-d4482535, FU-A Startinon, TMP-S11ce p- cdfP-T</th><th>- a previoual TCP Window Save rame Frame 1 Frame 1 Frame 2 Frame 3</th></t<>	1444 Fra. PT-Oynai 144 Fra. PT-Oynai 144 Fra. PT-Oynai 144 Fra. PT-Oynai 144 Fra. PT-Oynai 144 Fra. PT-Oynai 145 Fra. PT-Oynai 146 Fra. PT-Oynai 146 Fra. PT-Oynai 146 Fra. PT-Oynai 147 Fra. PT-Oynai 148 Fra. PT-Oynai 148 Fra. PT-Oynai 148 Fra. PT-Oynai 148 Fra. PT-Oynai 149 Fra. PT-Oynai 149 Fra. PT-Oynai 140 Fra. PT-Oynai	cdfP-Type-Ms, SSG-me8169123, 5eq-1175, Time-d4481135 FU-A Fme short, cdfP-Type-Ms, SSG-me8169123, 5eq-2177, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2177, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2177, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2177, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2177, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2177, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2187, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2187, Time-d4481135 FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2188, Time-d44811357, FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2188, Time-d44811357, FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2188, Time-d44811357, FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2188, Time-d44811357, FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2188, Time-d44811357, FU-A cdfP-Type-Ms, SSG-me8169123, 5eq-2188, Time-d4481237, FU-A Startinon, TMP-S11ce cdfP-Type-Ms, SSG-me8169123, 5eq-2188, Time-d4481235, FU-A Startinon, TMP-S11ce p- cdfP-Type-Ms, SSG-me8169123, 5eq-2189, Time-d4482535, FU-A Startinon, TMP-S11ce p- cdfP-T	- a previoual TCP Window Save rame Frame 1 Frame 1 Frame 2 Frame 3
0	Nal_ref_ide (NRI): 3 Start bit: Not the fil Ind bit: Not the fil Ind bit: Not the fil Capture anyoes beaution Capture anyoes b	tit A (19-A) (28) Tit packet of FU-A picture et of FU-A picture to FU-A picture TI (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	Sector Destination MAC Sector IncrosSt_0148155 Sector <t< td=""><td>$\begin{array}{cccccccccccccccccccccccccccccccccccc$</td><td>1447 Fra. PT-Oynai 1447 Fra. PT-Oynai</td><td>cffP-Type-95, 55G-0b0169128, 5eq-2187A, Time-244011356 FU-A cffP-Type-96, 55G-0b0169128, 5eq-2187S, Time-244011356 FU-A cffP-Type-96, 55G-0b0169128, 5eq-2188, Time-244011357, FU-A cffP-Type-96, 55G-0b0169128, 5eq-2188, Time-24401257, FU-A cffP-Type-96, 55G-0b0169128, 5eq-2189, Time-24402525, FU-A cffP-Type-96, 55G-0b0169128, 5eq-2189, Time-24402525, FU-A fort contained to the top top top top top top top top top top</td><td>- a previoual TCP Window Save rame Frame 1 Frame 1 Frame 2 Frame 3</td></t<>	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	1447 Fra. PT-Oynai 1447 Fra. PT-Oynai	cffP-Type-95, 55G-0b0169128, 5eq-2187A, Time-244011356 FU-A cffP-Type-96, 55G-0b0169128, 5eq-2187S, Time-244011356 FU-A cffP-Type-96, 55G-0b0169128, 5eq-2188, Time-244011357, FU-A cffP-Type-96, 55G-0b0169128, 5eq-2188, Time-24401257, FU-A cffP-Type-96, 55G-0b0169128, 5eq-2189, Time-24402525, FU-A cffP-Type-96, 55G-0b0169128, 5eq-2189, Time-24402525, FU-A fort contained to the top	- a previoual TCP Window Save rame Frame 1 Frame 1 Frame 2 Frame 3
0	Nal_ref_ide (NRI): 3 Start bit: Not the fit ind bit: Not the fit Not the fit	<pre>stat A (FU-A) (28) " tat packet of FU-A picture et of FU-A picture stat of FU-A picture</pre>	chyt Destination MAC Seeden Hicro-St_e2148155 Seeden Hicro-St_e2148155	172, 152, 103 153 154 159 159 159 159 150 <th150< th=""> <t< td=""><td>144 Fra. PT-Oynaii 144 Fra. PT-Oynaii 146 Fra. PT-Oynaii 146 Fra. PT-Oynaii 146 Fra. PT-Oynaii 146 Fra. PT-Oynaii 147 Fra. PT-Oynaii 148 Fra. PT-Oynaii 148 Fra. PT-Oynaii 148 Fra. PT-Oynaii 149 Fra. PT-Oynaii 149 Fra. PT-Oynaii 149 Fra. PT-Oynaii 149 Fra. PT-Oynaii 140 Fra. PT-Oynaii</td><td>ctr: y=96 \$SG-eb0169123 Seq=21874 Time=4244011556 TU-A ctr: y=96 \$SG-eb0169123 Seq=21874 Time=4244011526 TU-A ctr: y=96 \$SG-eb01691235 Seq=21874 Time=4244011526 TU-A ctr: y=96 \$SG-eb01691235 Seq=21875 Time=4244011526 TU-A ctr: y=96 \$SG-eb0169123 Seq=21875 Time=4244011526 TU-A ctr: y=96 \$SG-eb0169123 Seq=21875 Time=4244011526 TU-A ctr: y=97 \$SG-eb0169123 Seq=21875 Time=4244011256 TU-A ctr: y=97 \$SG-eb0169123 Seq=2188 Time=4244011257 TU-A TU-A ctr: y=97 \$SG-eb0169123 Seq=2188 Time=424401257 TU-A TU-A ctr: y=97 \$SG-eb0169123 Seq=2188 Time=424401257 TU-A TU-A ctr: y=97 \$SG-eb0169123 Seq=2188 Time=424491257 TU-A Tu-A TU-A</td><td>- a arented 1 TO2 Window See rame Frame 1 Frame 2 Frame 3 Frame 3 Frame 4</td></t<></th150<>	144 Fra. PT-Oynaii 144 Fra. PT-Oynaii 146 Fra. PT-Oynaii 146 Fra. PT-Oynaii 146 Fra. PT-Oynaii 146 Fra. PT-Oynaii 147 Fra. PT-Oynaii 148 Fra. PT-Oynaii 148 Fra. PT-Oynaii 148 Fra. PT-Oynaii 149 Fra. PT-Oynaii 149 Fra. PT-Oynaii 149 Fra. PT-Oynaii 149 Fra. PT-Oynaii 140 Fra. PT-Oynaii	ctr: y=96 \$SG-eb0169123 Seq=21874 Time=4244011556 TU-A ctr: y=96 \$SG-eb0169123 Seq=21874 Time=4244011526 TU-A ctr: y=96 \$SG-eb01691235 Seq=21874 Time=4244011526 TU-A ctr: y=96 \$SG-eb01691235 Seq=21875 Time=4244011526 TU-A ctr: y=96 \$SG-eb0169123 Seq=21875 Time=4244011526 TU-A ctr: y=96 \$SG-eb0169123 Seq=21875 Time=4244011526 TU-A ctr: y=97 \$SG-eb0169123 Seq=21875 Time=4244011256 TU-A ctr: y=97 \$SG-eb0169123 Seq=2188 Time=4244011257 TU-A TU-A ctr: y=97 \$SG-eb0169123 Seq=2188 Time=424401257 TU-A TU-A ctr: y=97 \$SG-eb0169123 Seq=2188 Time=424401257 TU-A TU-A ctr: y=97 \$SG-eb0169123 Seq=2188 Time=424491257 TU-A Tu-A TU-A	- a arented 1 TO2 Window See rame Frame 1 Frame 2 Frame 3 Frame 3 Frame 4

RTCP NTP timestamps

The following network trace can be used for testing what is described below.

If RTCP communication takes place between an Axis device and a video client, so called RTCP sender and receiver reports are exchanged. These reports include important information about the clock-sync within an ongoing RTSP/RTP stream. The Axis device,

Media streaming

being the sender of the video, sends the *RTCP sender report* where the current RTP stream time and the current NTP timestamp in UTC are included.

Metwork_Trace_RTCP_RT	P_SEI_Timestamps.pcapng	3								- 0	×
<u>File Edit View Go</u>	⊆apture <u>A</u> nalyze <u>S</u> tat	tistics Telephony Wireless Tools	Help								
🖌 🔳 🧔 💿 📙 🛅	🎗 🖸 🤇 🗢 🔿 🕾	T 🜆 🗖 🖉 🍯 🖉 🍕 🖉 🖉									
rtop											
No. Time	UTC Time Pa	ackage Delta Source MAC	Source	Source Port Destination MAC	Destination	Destination Port Protocol	Length Typ	e Info		Time	sin
966 4.759974	19:08:51.045939	0.000000 Micro-St_e2:48:b5	172.25.201.50	62991 AxisComm_9c:6b:		50001 RTCP	94		Source description		
1000 5.239011	19:08:51.524976	0.479037 AxisComm_9c:6b:e7	172.25.201.100			62991 RTCP	122		Source description		
2611 9.964093	19:08:56.250058	4.725082 Micro-St_e2:48:b5	172.25.201.50	62991 AxisComm_9c:6b:			94		Source description		
2666 10.760037	19:08:57.046002	0.795944 AxisComm_9c:6b:e7	172.25.201.100			62991 RTCP	122		Source description		
4288 15.662264	19:09:01.948229	4.902227 AxisComm_9c:6b:e7	172.25.201.100			62991 RTCP	122 94		Source description		
	19:09:02.391288 19:09:06.554236	0.443059 Micro-St_e2:48:b5 4.162948 AxisComm 9c:6b:e7	172.25.201.50 172.25.201.100	62991 AxisComm_9c:6b: 50001 Micro-St e2:48:		50001 RTCP 62991 RTCP	122		Source description Source description		
5963 21.379869	19:09:07.665834	1.111598 Micro-St e2:48:b5	172.25.201.100	62991 AxisComm_9c:6b:			94		Source description		
	19:09:11.516070	3.850236 AxisComm 9c:6b:e7	172.25.201.100			62991 RTCP	122		Source description		
7927 27,519313		2.289208 Micro-St e2:48:b5	172.25.201.50	62991 AxisComm 9c;6b;			94		Source description		
		2.166234 AxisComm 9c:6b:e7	172.25.201.100				122		Source description		
9272 32.129829	19:09:18.415794	2.444282 Micro-St_e2:48:b5	172.25.201.50	62991 AxisComm_9c:6b	e7 172.25.201.100	50001 RTCP	94	Receiver Report	Source description		
10552 35.794149	19:09:22.080114	3.664320 AxisComm_9c:6b:e7	172.25.201.100	50001 Micro-St_e2:00	b5 172.25.201.50	62991 RTCP	122	Sender Report	Source description		
<				/							>
) User Dotzgram Prot Real time Transport) (Stream Setup 0 10.0	occl, src Port: 1980 y MTSP (frame 21) bin: RC 1080 Versi splin: regot count net report count bedials (2046/7767 20	(Sender Report) ion (2) 2) 2) 2335) 2331) 15, 2021 19:09:15.970979999 UT 16, 2021 19:09:15.970979999 UT 10 (Source description) 10 20 20 20 20 20 20 20 20 20 2	K	Sender Rep	ort of the	Axis device					
🔘 🎽 Real-time Transpo	rt Control Protocol (rtcp), 28	8 bytes							Packets: 19155 ' Displayed: 27 (0.1%)	Pro	file: Def

The receiving video client on the other hand exchanges the so called *RTCP receiver report* with the Axis device to reply to the information previously sent, and to allow for mutual time-synchronisation checks and compensation for time drift between the Axis device and the video client itself. RTCP sender and receiver reports are exchanged every couple of seconds of an ongoing video stream.

Media streaming

2 🛛 🗌 🖓 🎽									× 🗆 -
Time	UTC Time Pa	ckage Delta Source MAC	Source 5	ource Port Destination MAC Destination	Destination Port Protocol	Length Typ	a Tafa		Time sin
966 4.759974	19:08:51.045939	0.000000 Micro-St e2:48:b5	172.25.201.50	62991 AxisComm 9c:6b:e7 172.25.201.100	50001 RTCP	94		Source description	Title Sit
800 5.239011	19:08:51.524976	0.479037 AxisComm 9c:6b:e7	172.25.201.100	50001 Micro-St e2:48:b5 172.25.201.50	62991 RTCP	122		Source description	
611 9.964093	19:08:56.250058	4.725082 Micro-St_e2:48:b5	172.25.201.50	62991 AxisComm_9c:6b:e7 172.25.201.100	50001 RTCP	94		Source description	
666 10.760037	19:08:57.046002	0.795944 AxisComm_9c:6b:e7	172.25.201.100	50001 Micro-St_e2:48:b5 172.25.201.50	62991 RTCP	122	Sender Report	Source description	
	19:09:01.948229	4.902227 AxisComm_9c:6b:e7	172.25.201.100	50001 Micro-St_e2:48:b5 172.25.201.50	62991 RTCP	122		Source description	
	19:09:02.391288	0.443059 Micro-St_e2:48:b5	172.25.201.50	62991 AxisComm_9c:6b:e7 172.25.201.100	50001 RTCP	94		Source description	
	19:09:06.554236	4.162948 AxisComm_9c:6b:e7	172.25.201.100	50001 Micro-St_e2:48:b5 172.25.201.50	62991 RTCP	122		Source description	
	19:09:07.665834	1.111598 Micro-St_e2:48:b5	172.25.201.50	62991 AxisComm_9c:6b:e7 172.25.201.100	50001 RTCP	94		Source description	
257 25.230105 927 27.519313	19:09:11.516070 19:09:13.805278	3.850236 AxisComm_9c:6b:e7	172.25.201.100	50001 Micro-St_e2:48:b5 172.25.201.50	62991 RTCP 50001 RTCP	122 94		Source description	
	19:09:13.805278	2.289208 Micro-St_e2:48:b5 2.166234 AxisComm 9c:6b:e7	172.25.201.50	62991 AxisComm_9c:6b:e7 172.25.201.100 50001 Micro-St_e2:48:b5 172.25.201.50	50001 RTCP 62991 RTCP	94		Source description	
	19:09:18.415794	2.444282 Micro-St e2:48:b5	172.25.201.50	62991 AxisComm 9c:6b:e7 172.25.201.100	50001 RTCP	94		Source description	
		3.664320 AX15COMM 9C:60:67	172.25.201.100	50001 MICCO-51 02:48:05 172.25.201.50	62991 KICP	122		Source description	
				/					,
net Protocol V Datagram Proto -time Transport	Version 4, Src: 172. ocol, Src Port: 6299 t Control Protocol (sion: RFC 1889 Versi	Receiver Report)	alacionies (acreci	Receiver report of the					

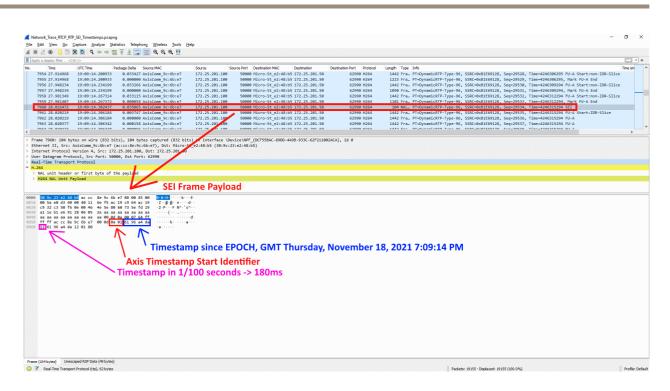
SEI timestamps

The following network trace can be used for testing what is described below.

The so called SEI frame is available when this VAPIX parameter is enabled: Image.IO.MPEG.UserDataEnabled=yes. Here Image.IO corresponds to the default video source, and if multiple video sources are available, the parameter needs to be enabled for each video source.

SEI frames are sent from the Axis device right before every I-Frame and include useful timestamp information. As described in the VAPIX library, SEI frames include timestamp information in Linux Epoch time down to 1/100ms accuracy in HEX format.

Media streaming



For debugging purposes we recommend using the following online converters:

- https://www.epochconverter.com/hex
- https://www.rapidtables.com/convert/number/hex-to-decimal.html

Image timestamps

A single image can be downloaded from the Axis device using the following VAPIX request: http://ip-address/axis-cgi/jpg/image.cgi. The received JPEG image from the Axis device provides valuable timestamp information from either the JPEG header itself or from the EXIF header data, depending on the AXIS OS version of the Axis device.

AXIS OS 8.40 and higher

From AXIS OS 8.40, the EXIF header data can be used to obtain timestamp information as you can see in the screenshot below. For debugging purposes, a simple windows application such as JPEGSnoop or EXIF in Linux OS can be used to obtain the information provided from the EXIF header. Go to the following source for more information about JPEG and EXIF timestamp header information: *Exif 2 specification*.

Media streaming



AXIS OS 6.50 and lower

Since the EXIF header data is not available in older AXIS OS versions, the plain JPEG comment header can be used to receive timestamp information. An application such as the HxD editor can be used to obtain the timestamp information in HEX-format, which in turn can be converted to human readable time format using a Linux EPOCH time converter, e.g. *https://www.epochconverter.com/hex.* For the 1/100 seconds information, a simple Hex to decimal converter can be used, e.g. *https://www.rapidtables.com/convert/number/hex-to-decimal.html.*

Image: Set Sumble View Analysis Table: V
Pr0:/Lenget_Intendemy_AM5_05.65.83pr Social effort
Cfract(i) Col 0
$ \begin{array}{ c c c c c c c c c c c c c$
000000000000000000000000000000000000
00000000 97 57 68 67 77
cococcel 0 to
00000000 10 15 16 15 16 16 15 16
000000000000000000000000000000000000
$ \begin{array}{c} $
000000000000000000000000000000000000
10 10 <td< th=""></td<>
10 10 <td< th=""></td<>
000000000000000000000000000000000000
000000000000000000000000000000000000
000000000000000000000000000000000000
0000010 10 00
0000010 00
00000110 12 13 14 16 13 14 14 16 14 14 16 14 14 16 14 14 16 14 14 16 14 14 16 14 14 16 14
0000110 10
0000010 15 14 14 15
0000010 15 15 14 46 66 67 76 76 76 77
00001010 70 70 80 80 60 70 80 80 60 70 80 80 60 70 80 80 60 70 80 80 60 70 80 80 60 70 80 80 60 70 80 80 80 70 80 80 70 80 80 70 80 70 80 70 80 80 70 80 80 70 80
0000010 00
00001010 10 000010 10
00001120 12 17
00000100 00
00000100 00 1.0 2.0 0.0 <
0000010 11 0<
00000100 71 00 01 01 00 01 01 00 01 01 00 01 01 01 00 01 01 01 00 01 01 01 01 01 01 00 00 01
00000210 10 64 10 15 64 10 <
00002210 26 27 28 29 28 35 46 37 38 39 38 41 44 45 44 71 41 15-567951CCEPG 00002220 46 94 53 554 55 56 57 58 55 58 56 56 56 56 56 56 56 56 56 56 56 56 56
0000220 4 9 9 4 3 5 4 5 5 6 5 7 8 9 5 5 4 6 4 6 4 6 7 Hij3TUYMKT2defg 0000220 4 9 6 4 7 7 8 7 7 7 8 7 7 8 6 4 7 8 9 7 7 8 7 7 8 7 8 7 8 9
0000220 68 66 A7 74 75 F6 77 78 79 7A 82 83 64 85 86 hijsturwary, f.,-t 00002210 68 69 80 82 63 64 55 65 95 69 59 69 50 84 123 A4 145 ² ***-*********************************
0000224 87 88 89 8A 92 93 94 95 96 97 96 99 9A A2 A3 A4 4*Å3***
00000260 C3 C4 C5 C6 C7 C8 C9 CA D2 D3 D4 D5 D6 D7 D8 D9 AAAzzźźźźóóóóo-e0
00000270 DA E2 E3 E4 E5 E6 E7 E8 E9 EA F2 F3 F4 F5 F6 F7 Údákámyéééőőőőő:
0000230 F8 F9 FA FF TA 00 CC 30 10 00 21 10 03 F mahyfr
00000250 00 57 02 59 10 DM 73 10 30 AS CO 71 0K 03 10 50,7,805HT=04037.« 00000250 C 77 E BS 04 A7 19 A9 89 80 37 D1 C - U-M, 67,307A
000002B0 A9 19 56 79 32 6B 2A F2 4C 72 2A FC EF D7 9A C6 0.VV2*0Lr*01*8E
000002C0 BD 7C 29 FS AA 15 96 E6 5D E3 EE 62 72 79 EB 54 %[)3*m]BibryeT
000002D0 FE F7 4E 95 2C CE 0B EE FD 2A 16 27 6E 3F 95 55 p+N+,1.19*.'n?+U
000002E0 \$3 34 50 00 7A 13 4E 75 C7 42 29 00 05 60 38 E9 "4]Ex.N5(E),.184 000002E7 0 25 55 10 6C 00 60 66 94 FD C0 13 A 4C 05 63 AdvD1; 17405.5Ac
00000270 D2 5C 55 D0 6C 00 60 65 94 FC DC 01 84 4C E0 63 0 60001.1"T00.5Lab 00000300 D7 75 A1 F3 01 E 94 AC 71 C3 A1 8A 9A 56 94 57 D0 *YA0."
00000300 DF AS 1E 30 LE 54 AU 1 1 L 54 AL 9 AD 5 55 DF /00 AFLO, T.T.T.BARTO 00000310 DF 23 JE 87 AB 66 65 CE 23 AD 12 D 11 39 24 8 0 44,tete23. ¹
00000320 D6 80 82 03 A7 4A 85 AC 62 DA 17 70 C6 39 38 AC 0*.534-b0.pgs9-
00000330 8D 3E 3E 57 1D 7A D7 45 64 98 70 7D 78 AF 2E 6F .>>W.z×Edxp)xT.o
00000340 5D 4E 19 1A 50 2E 0F 1D 0D 5E 40 08 E3 8A A9 14]N.P
0000350 78 02 AE C6 59 E8 00 62 A3 0C C7 TA E8 38 84 60 x, ABT#A.biTi4X.
0000360 0C 72 64 0 38 91 C5 35 40 C5 49 33 82 95 B4 000) 73 45 \$45 \$42 35 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

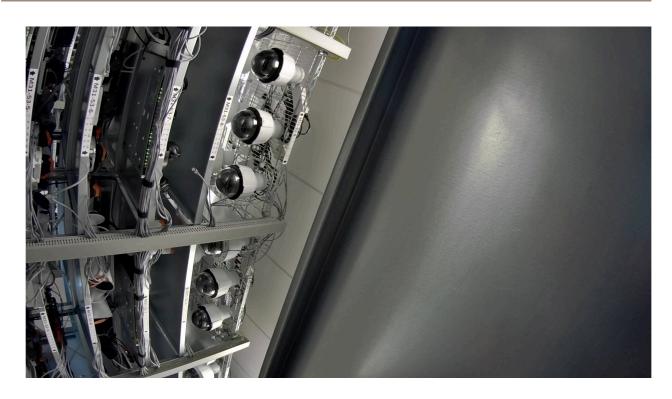
Media streaming

These sample images can be used for testing:





Media streaming



Metadata via RTSP

Generally speaking, metadata in Axis devices consists of three different types: event, PTZ and analytics metadata. The metadata is encapsulated in an RTP/TCP stream that can be requested from the Axis device. Let's take a closer look at the different types of available metadata.

Event and PTZ metadata

Starting from AXIS OS 5.40, Axis devices have been capable of sending event and PTZ metadata to a receiving 3rd party application, such as a video management system. The event and PTZ metadata is sent only when the state of the Axis device changes, meaning that no constant stream is being sent. Some common examples of event metadata are the manual trigger, virtual inputs, and storage related triggers. For mechanical PTZ cameras, the metadata includes positioning data as well as information on when a PTZ preset is reached or when the Axis device is moving.

Analytics metadata

Analytics-related metadata is available from AXIS OS 9.50 and later. Unlike the event and PTZ metadata stream described above, analytics metadata is streamed constantly from the Axis device to receiving clients, even if nothing happens in the scene. Typical examples of analytics metadata are motion or object detection coming from Axis analytics applications (ACAPs), such as AXIS Video Motion Detection. In AXIS OS 10.10 device software, AXIS Object Analytics changes from using the Axis Object Analytics engine to AXIS Analytics Scene Description. For more information on this, click *here*. You can also find out more about AXIS Object Analytics *here*.

A sample network trace that illustrates how metadata information is transferred can be downloaded *here*. By using Wireshark it's possible to search and find specific metadata events within the RTP/TCP stream, as illustrated in the screenshot below.

Media streaming

								Metadata	_Stream_On	ly.pcapng						-	8
				ony Wireless Tools	Help												
	r <ctil-></ctil->	९ २	🗢 🕾 Ŧ 🛓 🗔	<u> </u>												Exp	
a display fit Packet byter		rrow & Wide	e ∨ □ Case s	ensitive String	√ In	au)									12	Find	Cano
Real Ti Ti			Source MAC	Source IP	Source Port	Destination MAC	Destination IP	Destination Port	Destand Los	ngth Info					[22	rino	Cano
201 6			AxisComm 35:4a:3		554	Micro-St e2:48:b5	172 25.201.50	52500			e-98, SSRC=0x2E11CBE,	Seq=4809,	Time=2491593683	Mark			
			AxisComm_35:4a:3		554	Micro-St_e2:48:b5	177.25.201.50	52500			e-98, SSRC=0x2E11CBE,						
				4 172.25.201.200 4 172.25.201.200	554 554	Micro-St_e2:48:b5 Micro-St e2:48:b5	12.25.201.50 72.25.201.50	52500 52500		996 PT=DynamicRTP-Typ 1514 PT=DynamicRTP-Typ	e-98, SSRC=0x2E11CBE, e-98 SSRC=0x2E11CBE						
				4 172.25.201.200	554	Micro-St e2:48:b5	172.25.201.50	52500			e-98, SSRC=0x2E11CBE,						
			AxisComm_35:4a:3		554	Micro-St_e2:48:b5	172.25.201.50	52500		1514 PT=DynamicRTP-Typ							
201				4 172.25.201.200 4 172.25.201.200	554	Micro-St_e2:48:b5 Micro-St_e2:48:b5	172.25.201.50	52500 52500			e-98, SSRC=0x2E11CBE, e-98, SSRC=0x2E11CBE,						
				4 172.25.201.200	554	Micro-St_e2:48:b5	172.25.201.50	52500		514 PT=DynamicRTP-Typ							
	.796221 (0.000480	AxisComm_35:4a:3	4 172.25.201.200	554	Micro-St_e2:48:b5	172.25.201.50	52500		525 PT=DynamicRTP-Typ							
				4 172.25.201.200	554	Micro-St_e2:48:15	172.25.201.50	52500			e-98, SSRC=0x2E11CBE,						
				4 172.25.201.200 4 172.25.201.200	554 554	Micro-St_e2:48.05 Micro-St e2:44:b5	172.25.201.50 172.25.201.50	52500 52500		1514 PT=DynamicRTP-Typ 500 PT=DynamicRTP-Typ							
				4 172.25.201.200	554	Micro-St e2: 8:b5	172.25.201.50	52500		1514 PT=DynamicRTP-Typ							
				4 172.25.201.200	554	Micro-St_e2.48:b5	172.25.201.50	52500		490 PT=DynamicRTP-Typ							
				4 172.25.201.200 4 172.25.201.200	554 554	Micro-St_02:48:b5 Micro-St_02:48:b5	172.25.201.50	52500 52500		987 PT=DynamicRTP-Typ 1514 PT=DynamicRTP-Typ							
				4 172.25.201.200 4 172.25.201.200	554	Micro-St e2:48:b5 Micro-St e2:48:b5	172.25.201.50	52500		483 PT=DynamicRTP-Typ							
				4 172.25.201.200	554	Micro-it_e2:48:b5	172.25.201.50	52500	RTP 1	514 PT=DynamicRTP-Typ	e-98, SSRC=0x2E11CBE,	Seq=4827,	Time=2491639044	Mark,			
				4 172.25.201.200	554	Micro St_e2:48:b5	172.25.201.50	52500		527 PT=DynamicRTP-Typ							
201 7	.050327 (0.023121	AxisComm_35:4a:3	4 172.25.201.200	554	Micro-St_e2:48:b5	172.25.201.50	52500	RTP 1	1514 PT=DynamicRTP-Typ	e-98, SSRC=0x2E11CBE,	Seq=4829,	fine=2491640592	, Mark,			
net Prot mission Interle: Time Tra	ocol Versi Control Pr ved Frame, nsport Pro - Version:	ion 4, Sro rotocol, 9 Channel: otocol RFC 1889	c: 172.25.201.200	, Dst: 172.25.201.5 t Port: 52500, Seq:	0	o5 (30:9c:23:e2:48:b5) 1965, Len: 1460											
net Prot mission Interlea Time Tra 	ocol Versi Control Pr ved Frame, nsport Pro - Version: = Padding: = Extensio = Contribu = Narker: pe: Dynami umber: 481	ion 4, Sro rotocol, S Channel: btocol RFC 1885 False tring sour True cRTP-Type 4	c: 172.25.201.200 Src Port: 554, Dst : 0x00, 937 bytes 9 Version (2) rce identifiers co	, Dst: 172.25.201.5 t Port: 52500, Seq:	0												
et Prot ission interlea ime Tra 0 0 0000 ione ty uence r estamp	ocol Versi Control Pr ved Frame, nsport Pro = Version: = Padding: = Extensio = Contribu = Marker: pe: Dynami umber: 481 249160702	ion 4, Sro rotocol, 5 . Channel: otocol RFC 1885 False on: False sting sour True cRTP-Type .4	c: 172.25.201.200 Src Port: 554, Dst : 0x00, 937 bytes 9 Version (2) rce identifiers co	, Dst: 172.25.201.5 t Port: 52500, Seq: bunt: 0	0												
net Prot mission Interlea Time Tra 0 0000 yload ty quence r mestamp: nchroni:	ocol Versi Control Pr ved Frame, nsport Pro = Version: = Padding: = Extensio = Contribu = Narker: pe: Dynami umber: 481 249160702 ation Sour	ion 4, Sro rotocol, 5 . Channel: otocol RFC 1885 False on: False sting sour True ccRTP-Type 4 .7 rce identi	<pre>c: 172.25.201.200, Src Port: 554, Dst : 0x00, 937 bytes 9 Version (2) rce identifiers cc e-98 (98)</pre>	, Dzt: 172.25.201.5 t Port: 52500, Seq: punt: 0 (48307390)	0												
net Prof mission Interlea Time Tro. 0 0 0000 yload ty yload ty yload ty yload ty yload si yload: 2 06 04 2 06 04 2 06 07 2 06 03 2 06 000 0 0000000000000000000000000000	ocol Versi Control Pr version: = Padding: = Version: = Padding: = Extensio = Contribue = Narker: 249160702 4916070000000000000000	ion 4, Src protocol, 5 , Channell, 5 , Channell, 5 RFC 1885 False mn: False tring sour True .cRTP-Type 4 7 cc identi 3076657277 cc identi 3076657277 cc identi 3076657277 cc identi 3076657277 cc identi 3076657277 cc identi 3076657277 cc identi 3076657277 cc identi 3076657277 cc identi 30766777 cc identi 307667777 cc identi 307667777 cc identi 3076777 cc identi 3076777 cc identi 30767777 cc identi 30767777 cc identi 307677777 cc identi 3076777777 cc identi 3076777777 cc identi 30767777777 cc identi 3076777777777 cc identi 307677777777777777777777777777777777777	<pre>c: 122.25.201.200 src Part: 554, 055 sr Part: 554, 055 sr Part: 554, 057 sr Par</pre>	, DET: 172.25.201.5 POTT: 52500, Seq: Sunt: 0 (48307390) (4830	e 6561, Ack bc/ws smt19 ence ess30 64-b6 9-997 (Aust feren feren feren												
Let Profesission riterial control of the second se	ocol Versi Control Pr ved Frame, nsport Prc - Version: - Padding: - Extensio - Contribu - Narker: pe: Dynami usber: 481 249106702 - Marker: - Narker: - Nark	ion 4, Src otocol, 8 (Channel: tocol RFC 1885 False in: False tring sour True ceridenti trig cer	<pre>c: 172.25.201.200 srcPort: 554, 051 srcPort</pre>	Det: 12.25.201.01	e 5561, Ack 6561, Ack 5670, Ack												

In the following sections you can read more about how to get started and perform further testing.

Receiving metadata via RTSP

Metadata information can be received from an Axis device by opening an RTSP stream that uses the TCP transport protocol. The self-developed AXIS Metadata Monitor can be used as a simple test tool to request metadata from an Axis device. You can download AXIS Metadata Monitor *here* and install it on a computer in order to connect to an Axis device in your network. Below is a sample list of RTSP requests for receiving metadata events from the Axis device.

RTSP request	Description
rtsp://ip-address/axis-media/media.amp?event=on&tvideo=0	Event metadata excluding video stream
rtsp://ip-address/axis-media/media.amp?event=on&analyt- ics=polygon&tvideo=0	Event and video analytics metadata excluding video stream
rtsp://ip-address/axis-media/media.amp?event=on&analyt- ics=polygon&tptz=all&tvideo=0	Event, video analytics and PTZ metadata excluding video stream
rtsp://ip-address/axis-media/media.amp?event=on	Event metadata including video stream
rtsp://ip-address/axis-media/me- dia.amp?event=on&video=1&taudio=1	Event metadata including video and audio stream
rtsp://ip-address/axis-media/me- dia.amp?event=on&video=0&taudio=1	Event metadata excluding video but including audio stream

Media streaming

RTSP request	Description
rtsp://ip-address/axis-media/me- dia.amp?event=on&video=0&eventtopic=axis:CameraApplica- tionPlatform/VMD/Camera1ProfileANY	Event metadata excluding video and filtering only for AXIS Video Motion Detection (VMD) alarms
rtsp://ip-address/axis-media/me- dia.amp?event=on&video=0&eventtopic=onvif:De- vice/axis:10/VirtualPort	Event metadata excluding video and filtering only for the manual trigger event

Additional parameters such as camera=2 to camera=9 can be added to the above requests to e.g. receive metadata events from a different video channel. This is useful when the Axis device supports more than one video source or if different view areas are configured. In the example below we use AXIS Metadata Monitor to connect to an Axis device by using one of the RTSP requests above together with the IP address of the Axis device and its access credentials.

AXIS Metadata Monitor

			?event=on&ptz=all&video=0	
ter:			Apply Clear Autoscroll	
Seq#	Timestamp (UTC)	Category	Event Topic Tree	Info
121	12:07:08.282	Event	Device/IO/VirtualInput	[INIT] port = 40; active = 0;
122	12:07:07.426	Event	Device/HardwareFailure/PowerSupplyFailure/PTZPowerFailure	[INIT] Token = 1; Failed = 0;
123	12:07:13.773	Event	PTZController/ControlQueue	[INIT] PTZConfigurationToken = 1; queue_owner = ;
124	08:50:11.363	Event	Video Source/Live Stream Accessed	[INIT] accessed = 1;
125	12:07:12.015	Event	Video Source/DayNight Vision	[INIT] VideoSourceConfigurationToken = 1; day = 1;
126	12:07:08.041	Event	Device/I0/VirtualInput	[INIT] port = 17; active = 0;
127	12:07:08.290	Event	Device/IO/VirtualInput	[INIT] port = 52; active = 0;
128	12:07:07.428	Event	PTZController/PTZReady	[INIT] channel = 6; ready = 0;
129	12:07:07.815	Event	Device/HardwareFailure/PowerSupplyFailure/PTZPowerFailure	[INIT] Token = 6; Failed = 0;
130	12:07:58.406	Event	Device/Status/SystemReady	[INIT] ready = 1;
131	12:07:08.067	Event	Device/IO/VirtualInput	[INIT] port = 29; active = 0;
132	12:07:07.849	Event	Device/I0/VirtualInput	[INIT] port = 6; active = 0;
133	10:25:21.899	Event	Device/Status/Temperature/Below	[INIT] sensor_level = 0;
134	12:07:13.551	Event	PTZController/PTZReady	[INIT] channel = 1; ready = 1;
135	12:07:10.361	Event	MediaClip/Playing	[INIT] AudioOutput = 0; Playing = 0;
136	12:07:08.431	Event	Device/IO/VirtualInput	[INIT] port = 64; active = 0;
137	12:07:07.734	Event	Device/HardwareFailure/PowerSupplyFailure/PTZPowerFailure	[INIT] Token = 8; Failed = 0;
138	12:07:10.233	Event	Device/MQTT/ClientStatus	[INIT] active = 0; connected = 0;

-<tt:MetadataStream>

-<tt:Event>

-<wsnt:NotificationMessage>
</wsnt:Topic Dialect="http://docs.oasis-open.org/wsn/t-1/TopicExpression/Simple">tns1:Device/tnsaxis:IO/VirtualInput</wsnt:Topic> -<wsnt:ProducerReference

</wsa5:Address>uri://7c34806f-fcbe-4566-9f85-ca5478121fac/ProducerReference</wsa5:Address> </wsnt:ProducerReference>

```
- <wsnt:Message>
```

-<tt:Message UtcTime="2022-01-28T12:07:08.067482Z"PropertyOperation="Initialized">

-<tt:Source> <tt:SimpleItem Name="port"Value="29"/>

- </tt:Source>
- <tt:Key/>
- -<tt:Data> <tt:SimpleItem Name="active"Value="0"/>
- </tt:Data>
- </tt:Message>
- </wsnt:Message>

```
</wsnt:NotificationMessage>
</tt:Event>
```

```
</tt:MetadataStream>
```

As you can see, the Axis device is responding to the RTSP request with all its currently available metadata information and states. A simple way of testing incoming metadata events is to toggle the manual triggers in the web interface.

Media streaming

	//172.25.201.100/axis-m	edia/media.amj	p?event=on&ptz=all&video=0									
_			Apply Clear Autoscroll									
Seq#	Timestamp (UTC)	Category	Event Topic Tree	Info								
125	12:07:12.015	Event	Video Source/DayNight Vision	[INIT] VideoSourceConfigurationToken = 1; day = 1;								
126	12:07:08.041	Event	Device/IO/VirtualInput	[INIT] port = 17; active = 0;								
127	12:07:08.290	Event	Device/IO/VirtualInput	[INIT] port = 52; active = 0;		AXIS P1375 Events	×	+		~	-	
128	12:07:07.428	Event	PTZController/PTZReady	[INIT] channel = 6; ready = 0;	•	And The Presents						
129	12:07:07.815	Event	Device/HardwareFailure/PowerSupplyFailure/PTZPowerFailure	[INIT] Token = 6; Failed = 0;	I ←	> C A M	lot secure 172	.25.201.100/aca/in	dex.html#settings	s/system/t 🖻	☆ 🛸	×.
130	12:07:58.406	Event	Device/Status/SystemReady	[INIT] ready = 1;	1						-	
131	12:07:08.067	Event	Device/IO/VirtualInput	[INIT] port = 29; active = 0;	A	XIS		AXIS F	21375		-	0 (
132	12:07:07.849	Event	Device/I0/VirtualInput	[INIT] port = 6; active = 0;								
133	10:25:21.899	Event	Device/Status/Temperature/Below	[INIT] sensor_level = 0;								
134	12:07:13.551	Event	PTZController/PTZReady	[INIT] channel = 1; ready = 1;			Device ev	vents MQTT ever	its			
135	12:07:10.361	Event	MediaClip/Plaving	[INIT] AudioOutput = 0; Playing = 0;								
136	12:07:08.431	Event	Device/IO/VirtualInput	[INIT] port = 64; active = 0;			Rules So	chedules Recipie	ents Manual trig	gers		
137	12:07:07.734	Event	Device/HardwareFailure/PowerSupplyFailure/PTZPowerFailure	[INIT] Token = 8; Failed = 0;								
138	12:07:10.233	Event	Device/MQTT/ClientStatus	[INIT] active = 0: connected = 0:	1		Manual	triggers				
139	10:26:09.876	Event	Device/IO/VirtualPort	port = 1; state = 1;	1		View are	a 1				
140	10:26:12.066	Event	Device/IO/VirtualPort	port = 1: state = 0:	1		Active/In	active (On/Off)				
141	10:26:13.041	Event	Device/I0/VitualPort	port = 2: state = 1:			View are					
142	10:26:13.750	Event	Device/IO/VirtualPort	port = 2; state = 0;				active (On/Off)				
<tt:eve - <wsn <w - <w< th=""><th>t:NotificationMessa snt:Topic Dialect="I snt:ProducerRefere</th><th>http://doc nce></th><th>s.oasis-open.org/wsn/t-1/TopicExpression/Simp f-fcbe-4566-9f85-ca5478121fac/ProducerReferen</th><th>le*>tns1:Device/tnsaxis:IO/VirtualInput</th><th></th><th>Image Stream</th><th>Overlay PTZ</th><th>Audio Privacy</th><th>mask View area</th><th>Apps System</th><th></th><th></th></w<></w </wsn </tt:eve 	t:NotificationMessa snt:Topic Dialect="I snt:ProducerRefere	http://doc nce>	s.oasis-open.org/wsn/t-1/TopicExpression/Simp f-fcbe-4566-9f85-ca5478121fac/ProducerReferen	le*>tns1:Device/tnsaxis:IO/VirtualInput		Image Stream	Overlay PTZ	Audio Privacy	mask View area	Apps System		
	vsnt:ProducerRefere					e	Pinta I	38		_	-	
	snt:Message>					4		20	±	<u>Quur</u>	SNMP	
	tt:Message UtcTim - <tt:source></tt:source>	e='2022-01	-28T12:07:08.067482Z'PropertyOperation='Initializ	ed">		Language	Date and time	Orientation	Users	ONVIF	SNMP	
	<tt:simpleitem n<="" td=""><td>lame="port"</td><td>Value="29"/></td><td></td><td>17</td><td></td><td>~</td><td>•</td><td>-</td><td>- 100 -</td><td>-</td><td></td></tt:simpleitem>	lame="port"	Value="29"/>		17		~	•	-	- 100 -	-	
						8	P	Ø	1	i i i i i i i i i i i i i i i i i i i	2	
	<tt:key></tt:key> - <tt:data></tt:data>					тсрлр	03C	Security	Storage	I/O ports	MQTT	
	<tt:simpleitem n<br=""></tt:simpleitem>	lame='activ	e'Value="0"/>									

Another option would be to use one of the pre-installed Axis analytics applications (ACAPs), such as AXIS Video Motion Detection, to trigger a test alarm or motion in front of the Axis device in order to get motion detection/analytics based metadata events.

			Apply Clear Autoscroll				
Seq#	Timestamp (UTC)	Category	Event Topic Tree	Info			
142	12:07:07.734	Event	Device/HardwareFailure/PowerSupplyFailure/PTZPowerFailure	[INIT] Token = 8; Failed = 0;			
143	12:07:10.233	Event	Device/MQTT/ClientStatus	[INIT] active = 0: connected = 0:			
144	11:25:55.627	Event	CameraApplicationPlatform/VMD/xinternal_data	svgframe = <svg><desc></desc>;</svg>			✓ - □ >
145	11:25:57.061	Event	CameraApplicationPlatform/VMD/Camera1Profile1	active = 1;	AXIS Video Motion Detection	on 4 × +	
146	11:25:57.061	Event	CameraApplicationPlatform/VMD/Camera1ProfileANY	active = 1;	← → C A Not sec	cure 172.25.201.100/local/vmd/index.html#	P 🕁 🗯 👔
147	11:25:57.061	Event	RuleEngine/VMD3/vmd3_video_1	areaid = 0; active = 1;	C -> C A NOT SEC	ure 172.25.201.100/local/vmd/index.ntmi#	ਾ ਮ 🖪 🚛
48	11:25:57.061	Event	Video Source/MotionAlarm	Source = 0; State = 1;		AXIS Video Motion Detection 4	Help ?
49	11:25:57.061	Event	RuleEngine/MotionRegionDetector/Motion	VideoSource = 0; RuleName = Profile 1; State = 1;	CONNUNICATIONS		(Treated for
150	11:25:57.061	Event	CameraApplicationPlatform/VMD/xinternal_data	svgframe =			

wsnt:Message>
vtt:Message>
vtt:Message UtcTime='2022-01-28T12:07:10.361345Z'PropertyOperation='Initialized'>
-vtt:Source>
vtt:SimpleItem Name='AudioOutput'Value='0'>
vtt:SimpleItem Name='AudioOutput'Value='0'>
vtt:Source>
vtt:Source>

<tt:Sourcester

Media streaming

Examples of metadata events

Further down you will find a (non-complete) table of common metadata and device events available in Axis devices. The type and amount of events that are available depend on the hardware/software capabilities of the Axis device, some of which are:

- Mechanical and/or digital PTZ
- Mechanical and/or digital I/O
- Audio in and audio out capabilities
- Axis analytics applications (ACAPs) such as AXIS Video Motion Detection, AXIS Object Analytics etc.
- 3rd party applications

Metadata/event category	Торіс	Possible states
PTZ	PTZController/PTZPresets/Channel1	on_preset=0/1
PTZ	PTZController/Move/Channel1	is_moving=0/1
PTZ	PTZController/PTZReady	ready=0/1
PTZ	PTZController/ControlQueue	queue_owner=userx
1/0	Device/IO/VirtualInput	actve=0/1
1/0	Device/IO/Port	state=0/1
1/0	Device/Trigger/DigitalInput	state=0/1
Temperature	Device/Status/Temperature/Above	sensorlevel=0/1
Temperature	Device/Status/Temperature/Below	sensorlevel=0/1
Temperature	Device/Status/Temperature/Inside	sensorlevel=0/1
Temperature	Device/Status/Tempera- ture/Above_and_Below	sensorlevel=0/1
Temperature	Device/Heater/Status	running=0/1
System	Device/Status/SystemReady	ready=0/1
Hardware	Device/Sensor/PIR	state=0/1
Audio	Device/RingPowerLimitExceeded	limit_exceeded=0/1
Hardware	Device/Network/Lost	lost=0/1
Hardware	Device/Network/BlockedIP	address = x.x.x.x
Hardware	Device/Casing/Open	open=0/1
Storage	Storage/Disruption	disruption=0/1
Storage	Storage/Recording	recording=0/1
Hardware	Device/HardwareFailure/StorageFailure	disruption=0/1
Hardware	Device/HardwareFailure/FanFailure	failure=0/1
Hardware	LightControl/LightStatusChanged/Status	state=off/on
Video	VideoSource/LiveStreamAccessed	day=0/1
Video	VideoSource/DayNightVision	accessed=0/1

Media streaming

Metadata/event category	Торіс	Possible states
Video	VideoSource/ABR	abr_error=0/1
Audio	AudioSource/TriggerLevel	triggered=0/1
Audio	AudioControl/DigitalSignalStatus	signal_status=signal/no signal
Video	VideoEncoder/Connections	connected=0/1
Video	VideoSource/Connections	connected=0/1
Analytics	VideoAnalytics/Tampering	active=0/1
Analytics	VideoAnalytics/MotionDetection	motion=0/1
Analytics	CameraApplicationPlatform/VMD	active=0/1
Analytics	CameraApplicationPlatform/Mo- tionGuard	active=0/1
Analytics	CameraApplicationPlatform/Loitering- Guard	active=0/1
Analytics	CameraApplicationPlatform/FenceGuard	active=0/1

Axis analytics metadata configuration

From AXIS OS 10.11 and onwards, it's possible to choose dedicated analytics producers within the Axis device or to have multiple analytics metadata producers enabled simultaneously. In the backend, the Axis device can either be configured to produce analytics metadata by using the "Axis video motion tracker", which is the commonly known producer used since AXIS OS 9.50, or by using the newer "Axis object analytics" producer. The "Axis object analytics" producer offers some valuable extensions and more information with regards to analytics data, such as more detailed object classification (human faces, license plate numbers, etc.) that are useful in forensic search scenarios.

	AXIS P1375 N	letwork Camera
2		
	Metadata producers	
1.	Producer	– Channel 1
սի.	Axis video motion tracker o Shape	
REC	Analytics Scene Description	✓
*	 Classification Human, Human face, License plate, Vehicle 	
敬	ShapeVehicle information	
۹.		

Media streaming

Metadata via WebSocket

From AXIS OS 10.11 and onwards it's possible to subscribe to the metadata stream using the (secure) WebSocket protocol. For more general information about Axis metadata streaming, see *Metadata via RTSP on page 55*.

In the below example we're using the *WebSocket King extension* for the Google Chrome browser, however there are many other clients available supporting WebSocket communication.

Step 1: Login to your Axis device using the browser the extension has been installed to.

Step 2: In the WebSocket King extension, connect to:

- HTTP: ws://IP/vapix/ws-data-stream?sources=events
- HTTPS: wss://IP/vapix/ws-data-stream?sources=events

Note that if you're using HTTPS in step 1, you will need to use the same for the connection in the WebSocket King extension.

WebSocket King client A testing X +		~ - σ ×
$\eqref{eq:constraint} \leftrightarrow \eqref{eq:constraint}$ WebSocket King Client chrome-extension://cbcbl	khalmedgiunpalt/ht/addpompil.torv/index.html	8 x * 0 2 i
	совысноки 🖪 +	🛄 WebSocket King
Untitled Project	4 n wsz/172.25.201.250/uppiv/ws/data-tream/bources-events	O Disconnect = ×
	UNTITLED 1	
NO BUILD PATLADAS To de ore or un tre "To de de faither or a convector Core	PUID1 Prime	
🛋 😌 ⊌ 🧕 📾 <u>4</u> 🗵		^ 12 SWT 2022-02-11 1

Step 3: Send the following request to receive all events:

```
{
"apiVersion": "1.0",
"method": "events:configure",
"params": {
"eventFilterList":[
{
"topicFilter":""
}
]
```

Media streaming

<pre>} } Middate Cog dee A tento; x +</pre>	v – σ × 2 ± ★ □ ↓ : • endower tog
	2 x * 1 & 1
	2 x * 1 & 1
	2 x * 1 & 1
	2 x * 1 & 1
	2 x * 1 & 1
	2 x * 1 & 1
$e^{-3} \otimes e^{-3}$ WeisSock King Getel I otrome extension//dxtabhamsgjanpathdaddynongrlow/indxt/tent	WebSocket King
П П сомисноя ст +	
Unitide Project 4 a statistical statistica	O Disconnect – ×
Fiber UNITILD1	
SAVID PARLANDS +	
"notiversity" (* 1.a.") "nethod": "vevents configure", "powers : (
"eventFilterList":	
{ "uppictIter":"	*
Seed	
OUTPUT 01:59 21:39 O Connected to uss://172.55.201.250/vsg5u/us-deta-stream/sources-events	0
minut and the connected to assi//art.com/active/mpl/arts-artem/connected-events	
NO SAVIED PARTICADS	
Create one or use the "Sare Ac" button on a connection.	
Cone	
	^ 1000 1000 1000 1000

It's also possible to subscribe to a specific *topicFilter*, for example: "topicFilter":"tns1:Device/tnsaxis:IO/VirtualInput". Go to *Examples of metadata events on page 59* for more topic examples. Furthermore it's possible to subscribe to a specific port. Below you can see an example of virtual input port 47.

```
{
"apiVersion": "1.0",
"method": "events:configure",
"params": {
"eventFilterList":[
{
"topicFilter":"tns1:Device/tnsaxis:IO/VirtualInput",
"contentFilter":"boolean(//SimpleItem[@Name=\"port\" and @Value=\"47\"])"
}
}
```



Media streaming

→ C * WebSocket King Client chrome-extension://cbcbkhdmec		
	gianpaifchdaddpningniony/index.html	요 ☆ 🐐 🖬 😩
	CONNECTIONS 1 +	WebSocket Ki
itled Project d	wss//172.25.201.250/vapix/ws-data-stream?sources=events	O Disconnect –
	UNTITLED 1	
D PHILLINGS +	(
NO SAVED PAYLOADS Create one or use the "Sav AC" human on a servention. Create	<pre>server lime tool + {</pre>	

Step 5: Below is an example of toggling the manual trigger on the Axis device, which is reflected in the metadata stream.

AXIS P1448-LE Network	Camera × +	•	✓ - □ ×	WebSocket King client: A testing X +		✓ - □ ×
← → C ▲ Not	secure 172.25.	201.250/camera/index.html#/system/events/manualtriggers	8 x * 1 & 1	← → C * WebSocket King Client ch	hrome-extension://cbcbkhdmedgianpaifchdaddpnmgnknn/index.html	@ 🖈 角 🚨 E
AXISA		AXIS P1448-LE Network Camera	0 🕾 0 🖪 :		CONNECTIONS +	WebSocket King
🗟 Status				Untitled Project 🖉	ws://172.25.201.250/vapix/ws-data-stream?sources=events	Obsconnect = x
D Video	~	Rules Recipients Schedules Manual triggers		Filter	UNTITLED 1	
⊕ PTZ		II View Area 1		SAVED PAYLOADS +	"eventFilterList":[
🛦 Audio	~				"topicFilter":"")	
Recordings					3	I
🗱 Apps					3 Send Save As	
System	^				OUTFUT	c
図 Date and time					10:50 10.77 4 {	1
Network					"apiVersion": "1.8", "method": "events:notify",	
Ø Security					"params": { "notification": {	
⊥ Users	_				"topic": "tnsi:Device/tnsaxis:IO/VirtualPort", "timestamp": 1644573490757,	
Events					"message": { "source": {	
MQTT					"port": "1"), "key": (),	
Bo Storage					Key : {}; "dats": { "state": "1"	
De Stream profiles)	
ONVIF				NO SAVED PAYLOADS)'	
🖭 Metadata				Create one or use the "Save As" button on a connection.		
⊗ Detectors				Create	10:58 05.31 ↓ { "apiVersion": "1.0",	
E Logs					"method": "events:notify", "params": { "notification": {	
Plain config					"topic": "tns1:Device/tnsaxis:IO/VirtualPort", "timestarp": 1644571485206,	
Maintenance					"message": { "source": {	
- mantenance					"port": "1"),	
					"key": {}. "data": {	
					"state": "0"	
)	
					, ¹	
					18:58 81.88 { "apiversion": "1.8",	
					"method: "events:notify", "params": {	
					<pre>params : { "notification": { "topic": "tnsi:Device/tnsaxis:IO/VirtualPort", "topic": "tnsi:Device/tnsaxis:IO/VirtualPort",</pre>	
					<pre>timestamp": 1644573483867, "messamp": 1644573483867,</pre>	
	=×				message : { "source": {	
🛋 🤮 ڬ 🛛	🦻 📖					^ 10.58 10.58 2022-02-11 10

Network protocols

Network protocols

Commonly used network ports

In this section you can read about commonly used network ports used by an Axis device for different services over the network.

Enabled by default

Protocol	Port	Transport	Comments
802.1X	N/A**	EAP	IEEE 802.1X network authentication
Bonjour	5353	UDP	Used by 3rd party applications to discover the Axis device via mDNS discovery protocol (Bonjour)
CDP	N/A**	CDP	Used by network infrastructure to identify the Axis device or to provide PoE negotation capabilities.
HTTP	80	ТСР	General HTTP traffic such as web interface access, VAPIX and ONVIF API interface or Edge-to-edge communication.
HTTPS	443	ТСР	General HTTPS traffic such as web interface access, VAPIX and ONVIF API interface or Edge-to-edge communication.
LLDP	N/A**	LLDP	Used by network infrastructure to identify the Axis device or to provide PoE negotation capabilities.
RTP	Ephemeral port range*	UDP	Used by the Axis device for video/audio streaming
RTSP	554	UDP	Used by the Axis device for video/audio streaming
UPnP	49152	ТСР	Used by 3rd party applications to discover the Axis device via UPnP discovery protocol
SSDP	1900	UDP	Used by 3rd party applications to discover the Axis device via SSDP (UPnP)
WS-Discovery	3702	UDP	Used by 3rd party applications to discover the Axis device via WS-Discovery protocol (ONVIF)

Configuration dependent

Protocol	Port	Transport	Comments
ICMP/PING	N/A**	ICMP	General OSI layer 3 communication

Network protocols

FTP	21	ТСР	FTP access to Axis device
SSH	22	TCP	SSH access to Axis device
Telnet	23	TCP	Telnet access to Axis device
DNS	53	UDP	Used by the Axis device to resolve IP address to hostnames
NTP	123	UDP	Used by the Axis device to synchronize time
NTS	4460	ТСР	Used by the Axis device to synchronize time. From AXIS OS 11.1
SNMP	161	UDP/TCP	Used by the Axis device to send SNMP communication
SNMP (Traps)	162	UDP/TCP	Used by the Axis device to send SNMP communication
Syslog	514	UDP	Used by the Axis device to send log messages to a remote syslog
Syslog	601	ТСР	Used by the Axis device to send log messages to a remote syslog
Syslog	6514	ТСР	Used by the Axis device to send log messages to a remote syslog via SSL/TLS
ΜΩΤΤ	1883	ТСР	Used by the Axis device to send device events to a MQTT broker
ΜΩΤΤ	8883	ТСР	Used by the Axis device to send device events to a MQTT broker via websockets
RTSPS	322	UDP	Used by the Axis device for encrypted video streaming (RTSPS/SRTP)
SMB	445	ТСР	Used by the Axis device for edge recording to a remote network storage
03C	3128	ТСР	Used by the Axis device for O3C-related cloud communication
SOCKS	1080	ТСР	Used by the Axis device for SOCKS-proxy network communication
SFTP	22	ТСР	Used by the Axis device to send data via SFTP in an event rule
Action rule: email	Ephemeral port range*	ТСР	Used by the Axis device to send images/videos via mail notification in an event rule

Network protocols

Action rule: TCP notification	Ephemeral port range*	ТСР	Used by the Axis device to send notifications via TCP in an event rule
Action rule: image/video upload	Ephemeral port range*	ТСР	Used by the Axis device to send images/videos via HTTP(S) in an event rule
SIP	5060	UDP/TCP	Used by the Axis device to send SIP communication
SIP	5061	UDP/TCP	Used by the Axis device to send SIP communication via TLS

*Allocated automatically within a predefined range of port numbers according to RFC 6056. More information can be found here. **There is no TCP or UDP port number associated with this network traffic as these are associated with the transport layer above.

***IEEE 802.1X is only enabled by default on Axis Device ID capable devices.

To find out which Axis product that support Axis Device ID, please go to Axis product selector and select Axis device ID under Cybersecurity.

NTP and NTS (Network Time Sync)

Network Time Protocol (NTP)

Network Time Protocol is used to synchronize computer clocks on the Internet or in local networks. Version 4 (NTPv4) is the current version and is described by RFC 5904. It's fully compatible with NTPv3 and all previous versions and is designed to support the IPv6 protocol and dynamic server discovery. NTP is utilizing UDP as a transport protocol via port 123, which means that package delivery cannot be guaranteed.

Axis devices use two implementations as their current platform, depending on the AXIS OS version.

AXIS OS	Implementation
< 11.0	OpenNTPD
≥ 11.0	Chrony

Chrony is a newer implementation of the Network Time Protocol compared with OpenNTPD. It can perform well in challenging situations where the network is congested or the network connection is intermittent. Chrony can synchronize the system faster and quickly adapt to sudden clock rate changes. Additionally, Chrony supports Network Time Security (NTS) (RFC 8915) so that the time the device gets comes from a trusted source. You can find more information about Chrony *here*.

NTP uses a hierarchical structure where several NTP servers operating on different levels and accuracy (=stratum) are synced against each other to provide accurate time syncs to network devices. To do so, an NTP server in the network that provides time to local network devices should always sync to one or more NTP servers higher up in the hierarchy to avoid time-fluctuation and increased time accuracy. However, it's possible to operate an NTP server locally in a network in a standalone mode if no other NTP servers are available. More information about how the NTP protocol works can be obtained from public sources such as *Wikipedia*.

Network Time Security (NTS)

Axis devices with AXIS OS 11.1 or higher support Network Time Security. NTS allows the devices to get time from a trusted source. NTS is a mechanism for using Transport Layer Security (TLS) and Authenticated Encryption with Associated Data (AEAD) to provide cryptographic security for the client-server mode of the NTP.

NTS consists of 2 protocols:

1. NTS Key Exchange (KE): Exchange the necessary keys between the NTP client and server via Transport Layer Security (TLS). Once key exchanges are done, the TLS channel will be closed. The NTP client also knows which NTP server to query.

Network protocols

2. NTP Authentication: The NTP client queries the time to the NTP server. Both parties authenticate NTP time synchronization packets using the results of the TLS handshake.

More public information about NTS can be found here.

Sync process

OpenNTPD

The following sections illustrate the steps taken during a complete NTP synchronization while using OpenNTPD. *This network trace* can be used as a reference for below steps and shows a complete NTP synchronization from the first phase until the Axis device is in full NTP sync with the configured NTP server.

- Phase 1: It starts with the initial time query. The very first time-sync from an Axis device to an NTP server is a "universal sync" which means that any time provided by the NTP server will be taken by the Axis device as system time. Phase 1 is usually initiated when configuring the Axis device to sync against an NTP server (enable NTP), when the Axis device is restarted or when an upgrade is initiated that also results in a restart of the Axis device.
- Phase 2: After phase 1 follows a consolidation phase, where a number of time-sync requests from the Axis device against the NTP server are performed in between a 6 s – 60 s interval + 10 % randomization apart in order to align further with the NTP server to assure a close time-sync. The number of time-syncs vary depending on accuracy and trust according to the NTP protocol, but 5-15 time-syncs are usually needed.

NTP sync		
NTP servers:	172.25.201.104	
Synced:	No	
Due for next sync:	6 sec	
Time offset:	-	

NTP sync

NTP servers:	172.25.201.104
Synced:	No
Due for next sync:	33 sec
Time offset:	
Refresh information	1

Network protocols

• Phase 3: Phase 3 is considered the usual operation mode. The query interval will stabilize after phase 2 between 30 – 1500 s + 10 % randomization apart. In case the time difference increases during normal operation mode, the device will shorten the interval to sync more often in order to compensate for this. And if the time drift is very small, the intervals between two syncs will be larger. Note that the sync state is changing to "Yes", which indicates that the Axis device is in good time-sync with the configured NTP server.

NTP sync

NTP servers:	172.25.201.104
Synced:	Yes
Due for next sync:	32 sec
Time offset:	0.002 ms
Refresh information	

NTP sync

NTP servers:	172.25.201.104
Synced:	Yes
Due for next sync:	1328 sec
Time offset:	0.026 ms
Refresh information	n

Network protocols

Chrony

The following sections illustrate the steps taken during a complete NTP synchronization while using Chrony.

• Phase 1: Phase 1 starts with the initial time query. Chronyd will begin with a burst of 4-8 requests to make the clock's first update sooner. Once it gets the reply from the NTP server, it calculates the time difference between the current system time against the timestamp from the NTP server. In our implementation, we set the Chrony to step the system clock if the adjustment is larger than 0.1 seconds, but only in the first clock update since chrony was started. If the time difference is less than 0.1s, the Chrony will enter slew mode. The max rate that Chrony allowed to slew the time is set to 83333.333ppm (1/12s). Once the time is synchronized, you will see "yes" on the webpage.

Time sync status

```
Time servers 172.25.201.104
Synchronized Yes
Next sync: 59 sec
Time offset: 0.001 ms
```

Phase 2: Phase 2 is considered the usual operation mode. Once the time is synchronized, the general query polling interval to the NTP server is set to 64 seconds.Most of the Axis devices have a built-in real-time clock (RTC). The system will copy the clock from the RTC on the boot. To maintain the accuracy of the RTC, we enabled chronyd to copy the system time to the RTC every 11 minutes. Please be aware that chronyd will not track RTC drift.One of the main activities of the chronyd program is to work out the rate at which the system clock gains or loses time relative to real time. Whenever chronyd computes a new value of the gain or loss rate, it will record the value at /var/lib/chrony/drift. This can also help stabilize the initial synchronization on the next start.

NTS Sync process

To configure NTS, go to System > Date and time, and select Automatic date and time (manual NTS KE servers). You can either input the IP address of the NTP KE servers or the hostname (make sure the DNS server is properly configured). Here is an example of successful time sync via NTS:

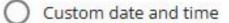
Network protocols

Synchronization

Automatic date and time (manual NTS KE servers) 0

Automatic date and time (NTP servers using DHCP)

Automatic date and time (manual NTP servers)



Manual NTS KE servers

sth1.nts.netnod.se

sth2.nts.netnod.se

Time zone

Europe/Stockholm

Time sync status

Time serverssth1.nts.netnod.se, sth2.nts.netnod.seSynchronizedYesNext sync:60 secTime offset:0.262 ms

The behaviors of the time sync process are almost identical to those we mentioned in the above Chrony sync process. Here we mainly focus on the key exchange and secure part.

• Phase 1

The Chrony client starts communicating with the KE server by establishing a TLS channel. That follows the key exchange. In the key exchange process, the client receives secret keys and cookies to be used later. The cookies contain secret keys only understood by the NTP server. The KE server also notifies the client which NTP server to query. Once the exchange is done, the TLS channel will be terminated.

• Phase 2

The Chrony client directly contacts the NTP server. It encrypts the query by the key it gets from phase 1. In that query, a cookie is also included. Once the server receives the query, it knows how to read the query. The server will respond to the client with a signed query. The client validates the signature in the incoming packet and then sets the time knowing it was sent from the correct server.

Network protocols

Common log messages

The following common log messages from Axis devices can be seen during NTP/NTS time-sync operations as well as during certain error conditions, e.g. if the NTP/NTS server is not operating correctly or cannot be reached. The log messages and their explanations provide a great detail of information on how the NTP/NTS protocol is working in practice. Plus, it's good to get an understanding of the log messages when troubleshooting NTP/NTS protocol related issues.

Situation	Clock	NTP log message	Explanation
Sync	NTPd Linux system clock	ntpd[21696]: reply from 192.168.255.29: offset -0.879648 delay 0.000313, next query 32s	This is a common log message indicating the offset, delay and when the next time-sync is going to be performed. • The delay in an NTP server describes the round-trip delay or latency of a timing message passed from client to server and back again. The delay is important so that network delays can be calculated and accounted for by the NTPd process of the Axis device. • The offset in ms indicates the actual time difference between the NTPd process of the Axis device and the NTP server time it's syncing to. • The next query is the time it takes for the Axis device's NTPd process to sync again to the NTP Server. When the "clock is in sync state" (more information below), the query interval is set to larger sync-intervalls that can be seen during the initial time-sync. • The jitter associated with a timing reference indicates the

Network protocols

			magnitude of variance, or dispersion, of the signal. Different timing references have different amounts of jitter. The more accurate a timing reference, the lower the jitter value.
No reply	NTPd Linux system clock	ntpd[21696]: no reply from 192.168.255.29 received in time, next query 30s	The Axis device's NTPd process could not reach the NTP server on the network layer 2 and/or 3.
No reply	NTPd Linux system clock	ntpd[21696]: no reply from 192.168.255.29 received in time, retransmit query 32s	The Axis device's NTPd process could not reach the NTP server on the network layer 2 and/or 3.
Negative delay	NTPd Linux system clock	ntpd[21696]: reply from 192.168.255.29: negative delay -0.000471s, next query 3213s	A state where the Axis device's NTPd process considers the NTP server in an erroneous state. Most likely the time has drifted significantly between the two network interfaces of the Axis device and the NTP server under a very short period of time and the "delay" can no longer be calculated correctly. No sync will take place for a longer period of time.
NTP server denies sync	NTPd Linux system clock	ntpd[21696]: reply from 192.168.255.29: not synced (alarm), next query 3196s	The log message indicates that the NTP server itself denies to synchronize the NTPd process of the Axis device because it considers itself not synchronized to its (lower stratum) NTP server. It's a message that is sent from the NTP server. No sync will take place for a longer period of time.
System clock synced	NTPd Linux system clock	ntpd[21696]: clock is now synced	The log message means that the NTPd process of the Axis device considers itself synced to the NTP server. This will cause the time-sync interval to be set to larger sync intervals since less syncs are needed. Directly after the sync state is reached, the RTC clock of the Axis device can be updated by the NTPd process.

Network protocols

System clock unsynced	NTPd Linux system clock	ntpd[21696]: clock is now unsynced	The log message means that the NTPd process of the Axis device is not considering itself in sync with the NTP server. This state should not last long. When in this state, no RTC clock updates can be performed. If the logs indicate that the camera is in an unsynced state for many hours or days, it means that the NTP server is drifting faster than the Axis device's NTPd process can account and compensate for.
NTP server reachable	NTPd Linux system clock	ntpd[21696]: peer 172.27.0.41 now valid	The log message indicates that the NTPd process of the Axis device could successfully verify the NTP server(s) integrity it's supposed to sync to.
NTPd drift file	NTPd Linux system clock	1323.2313	This value is in ppm (=mi- croseconds) and indicates the amount of drift of the Linux system time that needs to be considered and compen- sated for by the Axis device's NTPd process. Note that this has nothing to do with the time drift that can occur on the RTC clock. Can be obtained via /var/lib/open- ntpd/db/ntpd.drift.
RTC clock is set	RTC clock	ntpd[21696]: set local clock to Tue May 29 08:34:21 CEST 2018 (offset 0.000168s)	The log message indicates that the NTPd process of the Axis device is updating the RTC clock for the first time after it considered itself in good NTP sync towards the NTP server.
RTC clock is updated	RTC clock	ntpd[21696]: adjusting local clock. The current time diff is now –76.421369s	When the NTPd process of the Axis device is in "Clock is now in sync" state, the RTC clock receives updates. The "current time diff" represents the time difference between NTPd Linux system clock and RTC clock.
Sync	Chronyd Linux system clock	chronyd[19610]: chronyd version 4.2 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP -SCFILTER -SIGND +ASYNCDNS +NTS -SECHASH +IPV6 +DEBUG)	The log message indicates that the chronyd process of the Axis device is up and running. This log can be seen when you set the devices to sync the time with NTP server.
Sync	Chronyd Linux system clock	chronyd[19610]: Selected source 194.58.207.79 (sth1.nts.netnod.se) chronyd[18836]: Selected source 172.20.45.119	The log message means that the chronyd process of the Axis device successfully verifies the NTP server and selects the NTP server as the time source.

Network protocols

Sync	Chronyd Linux system clock	chronyd[17156]: System clock wrong by 250.930199 seconds chronyd[17156]: System clock was stepped by 250.930199 seconds scheduled[900]: Time was manipulated!	This log can be seen when the chronyd process of the Axis device gets the time from the NTP server and adjust its time to the correct one.
Chronyd drift file	Chronyd Linux system clock	chronyd[19610]: Frequency 1.637 +/- 13.841 ppm read from /var/lib/chrony/drift	The log message can be seen when chronyd process just started. When chronyd computes a new value of the rate at which the system clock gains or loses time relative to real time, it records it here /var/lib/chrony/drift. This allows chronyd to begin compensating the system clock at that rate whenever it is restarted. The first is the rate at which the system clock gains or loses time, expressed in parts per million, with gains positive. The second is an estimate of the error bound around the first value in which the true rate actually lies.
System clock unsynced	Chronyd Linux system clock	chronyd[2235]: Can't synchronise: no selectable sources	This log can be seen when the chronyd process of the Axis device gets a new update from the NTP server. However, the time varies too much and therefore the Axis device decide not to trust it. In the device's webpage, you will see the "Synchronized" status becomes No.
System clock unsynced	Chronyd Linux system clock	time-service: No request received, starting termination process systemd[1]: systemd-timedated.service: Deactivated successfully. systemd[1]: time.service: Deactivated successfully.	This log will show when the chronyd process of the Axis device doesn't get a reply from the NTP server.
NTS	Chronyd Linux system clock	Source 194.58.207.69 changed to 194.58.207.79 (sth1.nts.netnod.se)	This log will show when the chronyd process of the Axis device is redirecting itself from a KE server to an NTP server.
NTS Key Exchange	S Key Exchange Chronyd Linux system clock		This log will show when using NTS. The system doesn't trust the KE Server. Please ensure the KE server's CA certificate is uploaded into the Axis device.

Network protocols

NTS Key Exchange	Chronyd Linux system clock	chronyd[29971]: NTS-KE session with 194.58.207.10:4460 (194.58.207.10) timed out	This log indicates that the chronyd process of the Axis device cannot establish an NTS-KE session with the servers. Please check the configuration and network settings to see if anything is blocked.
NTS Key Exchange	Chronyd Linux system clock	ntpconfd: No NTS servers available!	This log indicates that the NTS server is not set correctly in the device webpage.
Stop NTP	Chronyd Linux system clock	systemd[1]: Stopping NTP client/server systemd[1]: Started Time & Date Service. chronyd[12200]: chronyd exiting systemd[1]: chronyd.service: Deactivated successfully. systemd[1]: Stopped NTP client/server.	This log will be shown when you switch to manual date and time instead of NTP.

Multiple time servers

With AXIS OS 9.40.1 or higher it's possible to configure a secondary NTP server in the web interface as well as up to five NTP servers via the VAPIX Time API. The device tries to synchronize with all servers that are configured. With the VAPIX Time API it's possible to configure up to 5 NTP server URLs. Additionally, one NTP server URL can resolve to many addresses, but only one "valid" server per URL is used for synchronization. So if you configure...

pool.ntp.axis.com AND 0.ntp.com where pool.ntp.axis.com resolves as three addresses [146.76.54.5, 146.76.54.56, 146.76.54.5] and 0.ntp.com resolves to 45.32.76.99

...the actual NTP servers that will be used are ONE valid and reachable address of the first URL and ONE valid and reachable address of the second URL:

(146.76.54.5 OR 146.76.54.56 OR 146.76.54.5) AND 45.32.76.99

The NTP algorithm determines which NTP server to use from the first pool.

With AXIS OS 11.0 or higher, when setting multiple NTP sources, Chrony tries to select the most accurate and stable sources for the synchronization of the system clock. This also applies when setting multiple NTS servers.

External time servers

Axis public NTP server

Axis public NTP server is *ntp.axis.com*, to which cameras connected to the internet can sync its time.

Meinberg NTP server

Meinberg has its own standalone NTP server software that can be installed on Microsoft Windows OS with the possibility to sync against other NTP servers. It also has a standalone operation mode, ideal and simple for standalone environments without network connection to the outside.

Netnod NTS server

Netnod's NTP service, funded by the PTS, is available for free to anyone. Netnod currently provides the following NTS servers.

- nts.netnod.se
- sth1.nts.netnod.se
- sth2.nts.netnod.se

Windows NTP server

By following *these steps*, it's possible to configure your local Windows system as an NTP server.

Network protocols

Note that Windows by default will have a lower NTP time accuracy as well as larger sync intervals, which may not be optimal for good time accuracy.

For Chrony, a common issue with Windows NTP servers is that they report a very large root dispersion (e.g., three seconds or more), which causes chronyd to ignore the server for being too inaccurate.

It's recommended to configure the Windows NTP server with more strict and accurate time accuracy and sync intervals. See the following guides for more information on this:

- Windows high accuracy time
- Windows high accuracy time configuration guide

If you use Windows as the NTP server for an offline installation, the Windows NTP server may use the local CMOS clock time. By default, it will report a root dispersion of 10 seconds. See the following guides for more information on how to change this value:

LocalClockDispersion Entry

Windows Time service tools and settings

Troubleshooting

Peer clock stratum unspecified or invalid (0)

Implementation	Explanation
OpenNTPD	The Axis device will not accept timestamps if the local NTP server is not synced with high layer NTP servers (<i>Higher NTP hierarchy</i>) as no reliable timestamps are provided.
Chrony	The chronyd process of the Axis device will only synchronize with an NTP server at Stratum 15 or above.

What time is the Axis device sending?

While debugging NTP-related network issues, it can be observed that the Axis device is transmitting a random 64-bit time to the NTP server in order to mitigate the risk of cybersecurity attacks. This does not have any impact on the performance or quality of the NTP time sync itself since the NTP server will still respond with a valid time stamp which the Axis device will apply to its time.

Maximum time difference

Implementation	Explanation
OpenNTPD	Time differences between the Axis device and the NTP server that are larger than 2.145 s (35.75 min / 0.5 h) will result in there being no more time syncs. The reason is that the Axis device will assume that the time coming from the NTP server has changed too drastically and therefore considers the NTP server unreliable. It's recommended to check if the NTP server is functioning correctly and to reconfigure the Axis device to sync with the NTP server again to initiate a new time sync procedure.

Counteract clock drifting

If the system clock has a significant drift, the Axis device's clock will never achieve a close enough offset to the NTP server. However, the system clock should not drift at a rate of that magnitude.

Implementation	Explanation
OpenNTPD	The NTP client can adjust the system clock to 500 ppm (part per million) at most. It can counteract a clock drift of 1.8 seconds per hour.
Chrony	The Chrony client can adjust the system clock to 83333.333 ppm (part per million) at most. In theory, it can, counteract a clock drift of 300 seconds per hour.

Network protocols

QoS (Quality of Service)

QoS provides the means to guarantee a certain level of a specified resource to selected traffic on a network. Quality can be defined as e.g. a maintained level of bandwidth, low latency, no packet losses, etc. The main benefits of a QoS aware network can be summarized as:

- The ability to prioritize traffic and thus allow critical flows to be served before flows with lesser priority
- Greater reliability in the network, thanks to the control of the amount of bandwidth an application may use, and thus control over bandwidth races between applications

To use QoS in a network with Axis video products the following requirements need to be met:

- All network switches and routers must include support for QoS. This is important to achieve end-to-end QoS functionality
- The Axis video products used must be QoS enabled

Imagine that the network in Figure 1 is an ordinary (non-QoS aware) network. In this example, PC1 is watching two surveillance video streams from cameras Cam1 and Cam2, with each camera streaming at 2.5 Mbps. Suddenly, PC2 starts a file transfer from PC3. In this scenario the file transfer will try to use the full 10 Mbps capacity between the routers R1 and R2, whilst the video streams will try to maintain their total of 5 Mbps. We can no longer guarantee the amount of bandwidth given to the surveillance system and the video frame rate will probably be reduced. At worst, the FTP traffic will consume all the available bandwidth.

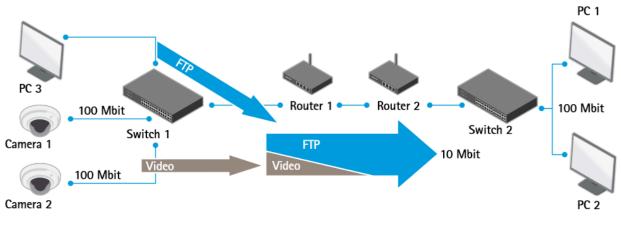
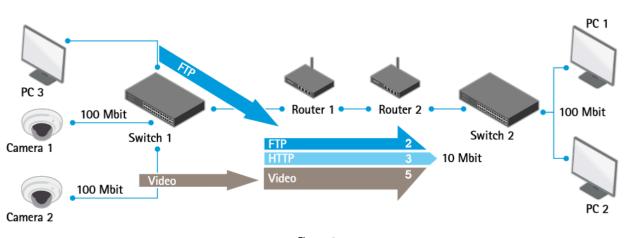


Figure 1

Now, suppose the network in Figure 2 is Ω oS-aware and uses the DiffServ model (see below). The router R1 has been configured to devote up to 5 Mbps of the available 10 Mbps for streaming video. FTP traffic is allowed to use 2 Mbps, and HTTP and all other traffic can use a maximum of 3 Mbps. Using this division, video streams will always have the necessary bandwidth available. File transfers are considered less important and get less bandwidth, but there will still be bandwidth available for web browsing and other traffic. Note that these maximums only apply when there is congestion on the network. If there is unused bandwidth available, this can be used by any type of traffic. By using QoS we allow the network applications to co-exist on the same network, without consuming each other's bandwidth.

Network protocols





Further reading

For further reading and more detailed documentation about the Quality of Service standard, see the following links:

- RFC 2475 An Architecture for Differentiated Services
- RFC 2597 Assured Forwarding PHB Group
- RFC 2598 An Expedited Forwarding PHB
- RFC 3168 The Addition of Explicit Congestion Notification (ECN) to IP
- RFC 1633 Integrated Services in the Internet Architecture: an Overview

QoS models

There are several different ways (models) of implementing QoS. Axis products use the DiffServ model, for greater scalability and flexibility. See below for more information.

The IntServ model

The IntServ model, or Integrated Services model uses a protocol called RSVP (Reservation Setup Protocol), which is used to reserve a certain traffic quality in the network. Prior to use, each application in an IntServ QoS network reserves its own resources and the router either grants or denies the request. When a reservation request is received, the routers need to find a path that can support the IntServ request and also the route that offers the best services. The major problem with this model is scalability. As the network increases in size, the connections database will grow to enormous proportions and it will be both difficult and ineffective to keep track of all reservations. Another drawback is the model's inflexibility – the maximum amount of the resource in question that each type of traffic will ever receive is the maximum specified in the model, even if there are other unused resources available.

The DiffServ model

The Differentiated Services (DiffServ) model was introduced in 1998. It is based on two major components:

- Packet marking
- Router queuing disciplines

The applications in a DiffServ network mark their traffic so the router knows which service to apply to the packet. The marking is done in the IP header, by setting a field called the DSCP (Differentiated Services Codepoint). This is a 6-bit field that provides 64 different class IDs. Each DSCP value represents a QoS class, also known as a behavior aggregate. Thus, different applications can mark their own traffic with the same DSCP value. The intelligence of a DiffServ network is setup in the routers, where a particular DSCP value is mapped to a particular routing behavior. This behavior is referred to as a Per-Hop Behavior (PHB) and is implemented in the router using different queuing disciplines.

Network protocols

The DiffServ model abandons the concept of states as used in IntServ, and routers operate in a connectionless mode. This adds scalability to the system, since each router works independently, unaware of the network size and complexity. This model is also more flexible, as the classes of service are not strictly defined. Resources over and above the value specified as the maximum when resources are limited can be freely exploited whenever available. The main benefit of using this model in Axis products is that the products mark their own traffic, instead of letting the boundary nodes of the DiffServ domain do so. The conditioning algorithms in the boundary node cannot, for example, distinguish video over HTTP from audio over HTTP – they will only see HTTP, and probably provide a much lower level of service than actually required. To allow a node outside the DS domain to classify its own traffic:

- The boundary router must be correctly configured
- The camera must be set up as a trusted node

Per-Hop Behaviors (PHBs) define the router's forwarding treatment for a certain class of traffic. Classes of traffic are also known as Behavior Aggregates (BA). Members of the BA are marked with the same DSCP value. There are four recommended PHBs defined, each mapped to one or more DSCP value.

<u>The Default PHB</u>: The default PHB provides the traditional best-effort service. It is represented by DSCP value 000000 (NOTE: 6-bits set to 0) and it must be available at any DiffServ router. This is the forwarding treatment applied to all non-DiffServ aware applications.

<u>The Class-Selector PHB</u>: To preserve backward compatibility with the old TOS field definition, the class-selector PHB defines a DSCP value of the form xxx000. The three bits represent the IP Precedence defined by a Type of Service aware network. The Class-Selector PHB ensures that DiffServ compliant nodes can coexist with IP Precedence-based nodes.

Expedited Forwarding: The Expedited Forwarding (EF) PHB provides a low loss, low latency, low jitter and guaranteed bandwidth service and can be considered the top priority behavior. Applications such as VoIP require this kind of robust service. The recommended DSCP value for EF is 101110.

<u>Assured Forwarding</u>: With Assured Forwarding (AF) traffic can be divided into four different classes. Each class is usually assigned a specific amount of bandwidth.

Within each class it is possible to specify three different drop precedence values. This value denotes the order in which packets will be dropped when there is congestion. A packet with a higher drop precedence will be dropped first. This gives us an AF matrix, and hence AF is often denoted AFxy, where x is the class number and y is the drop precedence. The table below shows the DSCP values recommended for the AF PHB. This gives us an AF matrix, and hence AF is often denoted AFxy, where x is the class number and y is the drop precedence. Table 1.1 shows the DSCP values recommended for the AF PHB.

Drop precedence	Class 1	Class 2	Class 3	Class 4
Low dP (1)	001010	010010	011010	100010
Medium dP (2)	001100	010100	011100	100100
High dP (3)	001110	010110	011110	100110

Table 1

DiffServ domain

A DiffServ domain (DS-domain) is a network that has been set up according to a particular DiffServ specification, and which has a set of DSCP values mapped to certain PHBs. As each router in a DiffServ domain forwards traffic based on DSCP value mapping, we can only guarantee that we get the correct forwarding treatment within our own DS-domain. As soon as a packet leaves the domain we can no longer guarantee how other routers will map our DSCP values. The same goes for incoming traffic - we must reclassify incoming traffic to match our rules. This means we must mark the traffic with a DSCP value valid in our domain. This is usually done by looking at the packet header and setting a new DSCP value based on the source address, port numbers, etc. The marking process is called traffic conditioning and is done at the boundary nodes of the DS domain.

VLAN 802.1P model

IEEE 802.1P defines a QoS model at OSI Layer 2 (L2, Data Link). This is called CoS, Class of Service, and adds an extra 3-bit field (called user-priority) to the VLAN MAC header. This splits traffic into 8 different classes. Priority is set up in the switches, which then use different queuing disciplines to forward the packets correctly. Although the 802.1P CoS works well, it lacks scalability and cannot

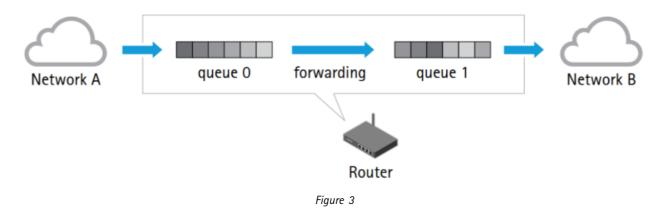
Network protocols

provide end-to-end guarantees. We cannot assume the L2 protocol to be constant on a larger network or on the Internet. Therefore, most of today's high-end switches implement mapping from L3 (IP DSCP) QoS to L2 CoS.

Routers

The DiffServ implementation in routers

Routers handle the forwarding of network traffic from one network to another. All packets entering from one network (see Figure 3) are queued before being processed, to determine which network they should be forwarded to. The DiffServ implementation in routers is a way of providing forwarding treatment based on the DSCP of an incoming packet. This is done by using queuing disciplines and prioritizing of packets. Note that router configuration is brand dependent and is not covered by this document.



Queue disciplines

To be able to provide the mechanism desired by DiffServ the routers implement different ways of handling its queues. These different techniques are known as queuing disciplines and are algorithms designed to provide different service guarantees. To exemplify the use of different queuing disciplines we will briefly explain FIFO queues and priority queues.

FIFO is the simplest queuing discipline and is usually the default setting in network routers. FIFO describes the simple First-In-First-Out behavior of the queue. The below image shows a FIFO queue where packets enter from the left and exit to the right. The first packet entering will be the first packet sent out on the port. Other packets will be placed at the end of the queue and must wait their turn. This discipline is too basic to provide any QoS service.

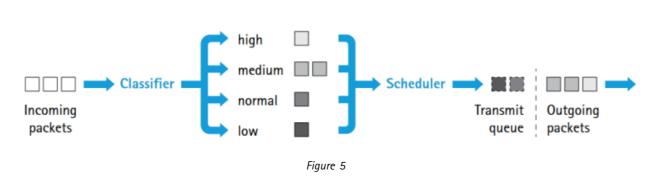




Priority queuing

Priority queuing is a relatively simple way of implementing differentiated service classes in a router. Instead of using one FIFO queue only, several are used, and each is assigned a different priority. A classifier determines which queue to put the incoming packet in, and the scheduler puts the packets out onto the network. The classifier parses the header of incoming packets and decides which priority queue to put the packetin. In a DiffServ network this decision is based on the DSCP value of the incoming packet. The scheduler ensures that the high priority queue gets served first, the medium priority queue next, and so on. This discipline allows the traffic to be prioritized.

Network protocols



AXIS OS

Axis has opted to use the DiffServ model, to provide greater scalability and flexibility. This is implemented by:

- Marking network traffic
- Classifying network applications in QoS classes
- Providing a user interface

AXIS OS QoS classes

AXIS OS uses four QoS classes. The members of a class all mark their traffic with the same DSCP value and thus receive the same forwarding treatment from routers:

- Live video This class consists of applications that stream Motion JPEG video streams over HTTP, and MPEG-4 video streams over RTP, RTP/RTSP and RTP/RTSP/HTTP.
- Live audio This class consists of applications that generate audio flows, and is only present in products that supportaudio.
- Event/Alarm This class consists of applications that generate event and alarm traffic. The class handles FTP, HTTP, SMTP and TCP events.
- Management This class consists of applications that generate management traffic. The class can handle FTP, HTTP, HTTPS and SNMP management traffic.

AXIS OS QoS configuration

The image below shows an example of a screenshot of the HTTP user interface for QoS in Axis devices using AXIS OS 6.5X and lower. It shows the different QoS classes supported by the product and lets the user specify the DSCP (DiffServ Codepoint) value for each class. The default DSCP value is 0, which is the same as the default PHB and which can be interpreted as QoS disabled.

Network protocols

AXIS A	XIS F34 Network	Camera	Live View Se	erup i Help
Basic Setup	QoS Settings			0
	QoS DSCP Settings			
Video	Live Video DSCP:	þ	[063]	
Live View Config	Event/Alarm DSCP:	0	[063]	
Detectors	Management DSCP:	0	[063]	
Detectors	Metadata DSCP:	0	[063]	
Applications		Save	Reset	
Events		and the second second second second		
Recordings				
Languages				
 System Options Security Date & Time Network TCP/IP SOCKS QoS SNMP UPnP™ RTP Bonjour Storage Ports & Devices Maintenance Support Advanced 				
About				

Figure 6

In Axis devices running AXIS OS 7.10 and higher the Plain Config in Settings > System > Plain Config > Network is used to perform QoS related configuration.

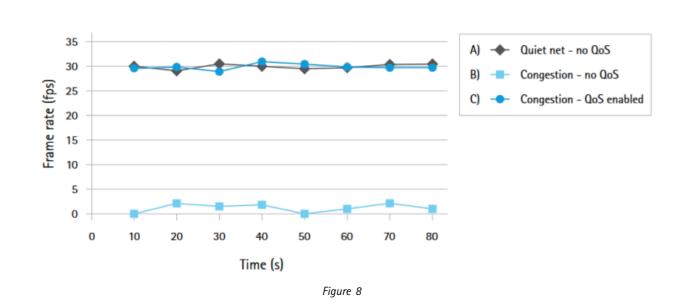
Network protocols

			AXIS P137	'5 Netwo	ork Camera			•	٥	0	
					ISCP 0	[063]					^
				c	Class2						
					Desc						
					AxisLiveAud						
					0	[063]					
					Class3						
					AxisEventAla						
					SCP	_					
					0	[063]					
				c	lass4						
					AxisManager						
					SCP	_					
					0	[063]					
				c	lass5						
					AxisRemoteS						
					SCP						~
Image Stream (Overlay PTZ	Audio Privacy mask	View area	Apps	System					~	
	.	Cinir	SNUP		Ö	٢	ع				
	Users	ONVIF	SNMP		Events	Detectors	Maintenance				
(\sim		9						
	Storage	VO ports	MQTT		Plain confi	9					
				igure	7						

Performance improvements

The graph below illustrates a possible scenario in which performance is maintained/improved on a QoS enabled network.

- Video is first streamed over a quiet, non-QoS network, where the frame rate can be assumed to be approximately 30 frames per second. This is illustrated by line A.
- Network congestion is then simulated by, e.g., adding a non-responsive UDP stream. The frame rate drops sharply, to a practically unusable level, as shown by line B.
- Video is then streamed over a DiffServ-enabled network, with the same congestion also added here. The video traffic is unaffected by the congestion and the frame rate is maintained, as shown by line C.



Network protocols

TCP ECN

ECN is an acronym for Explicit Congestion Notification and is an improvement of the congestion control i n T C P. The basic idea is for TCP to report that congestion is about to occur, before the queue actually overflows. The router does this by marking a field in the IP header called CE (Congestion Experienced). When the sender receives this signal the flow is slowed down. The traditional method of indicating congestion is for routers to drop packets that lead to the re-transmission of packets.

The ECN model will only be used when both communication end-points support it. This is achieved by negotiating at TCP connection initialization time. By introducing ECN support re-transmission over the network is minimized, which leads to higher throughput and less delay. TCP ECN is enabled by default in Axis video products and can be disabled in **Plain Config > Network > TCP ECN**.

IPv6

IPv6 (Internet Protocol version 6) was initially designed by the IETF to replace the current IP version 4 (IPv4). The most likely scenario now is that IPv4 will remain even after IPv6 enters the arena. One of the main reasons for the introduction of IPv6 is the growing shortage of IPv4 addresses. Additionally, IPv6 also adds improvements in areas such as routing and network auto-configuration. Some general information about IPv6 addresses and configuration is provided in the following sections, and the complete IPv6 specifications can be found in the *RFC 2460 specifications*.

IPv6 addresses

The IPv6 address is written in hexadecimal form, and consists of eight double-bytes separated by colons. To make the address representation as short as possible, a number of consecutive zeros may be abbreviated to a double colon, which is allowed once in any single IPv6 address. Instead of using a subnet mask as in IPv4, IPv6 simply uses a network prefix length. The prefix length is appended to the address.

Example: fe80::250:daff:fe4d:7592/64

The prefix length specifies how many bits of the address will be considered part of the prefix. In the example above, the first 64 bits specify the network address, while the final 64 bits specify the host address. IPv6 addresses can be assigned in different ways:

- A link-local IPv6 address is automatically configured.
- A DHCPv6 server can be used to assign IPv6 addresses.
- Router advertisements can be used to assign auto-configured addresses.

Auto-configured link-local address

A device that supports IPv6 will get an auto-configured link-local address that starts with fe80. The remainder of the address is usually

Network protocols

built on a so-called EUI64 address. The EUI64 address is constructed by taking the Ethernet MAC address of the network interface, and filling it with two specific bytes (fffe) in the middle, to get a 64-bit address (see the example address in the previous section.)

Auto-configuration using router advertisements

In an IPv6 network, network devices may be auto-configured by listening to advertisements sent by routers in the network. These advertisements will then define how the network devices should be configured in order to be able to be routable. A routable IPv6 address can be derived by using the information in the router advertisements. This auto-configured address is derived using the EUI64 address, together with the address of the router and the network prefix. The router advertisements may instruct the network device to use DHCPv6, and if so, at which level.

DHCPv6 configuration

Just as an IPv4 network may use a DHCP server to assign IP configuration, an IPv6 network may use a DHCPv6 server. DHCPv6 can be used at different levels:

- In stateless mode the DHCPv6 server will designate the network servers to use, e.g., DNS servers and NTP servers, but it will not assign IPv6 addresses for network devices. This must be done using some other method.
- In stateful mode, the DHCPv6 server will also assign IPv6 addresses to the network devices, as well as assigning the network servers as in stateless mode.

Accessing IPv6 devices

Most programs accept host names and will automatically look up the IPv6 address. This is the preferred way of passing addresses to programs. If the name maps to an IPv4 address, IPv4 will be used. If the name maps to an IPv6 address, IPv6 will be used. If there are both IPv4 and IPv6 mappings, the operating system will decide which to try first. To pass IPv6 literal addresses to a program, there are a few points to consider. When passing an URL, brackets must be used. To pass IPv6 literal addresses to a program, there are a few points to consider. When passing an URL, brackets must be used. For example:

Example	Comment
http://[2001:5c0:84d9:2:240:8cff:fe6b:3cb9]	Accessing an Axis device using http
http://[2001:5c0:84d9:2:240:8cff:fe6b:3cb9]:8080	Accessing an Axis device using http and custom httpport
https://[2001:5c0:84d9:2:240:8cff:fe6b:3cb9]	Accessing an Axis device using https
http://root:pass@[2001:5c0:84d9:2:240:8cff:fe6b:3cb9]	Accessing an Axis device using http and pre-entered access credentials
http://[fe80::2:240:8cff:fe6b:3cb9%eth0]	Accessing an Axis device using the link-local address. Note that the network interface is specified after the IPv6 address. This is because the link-local prefix fe80::/10 has multi-path routes, i.e., one route per interface. The routing system has no way of knowing which interface the device you are trying to contact is located on.

Most programs (e.g., FTP, Telnet, etc) will accept the IPv6 address in its literal form such as *ftp 2001:5c0:84d9:2:240:8cff:fe6b:3cb9* or *ftp fe80::2:240:8cff:fe6b:3cb9%4*. Some programs may take the interface identifier in a non-standard way. An example of this is the ping6 tool usually distributed with linux. It expects to be run like this *ping6 -I eth1 fe80::2:240:8cff:fe6b:3cb9*. On Windows you can see the identifier of each adapter by running 'ipconfig' and finding the IPv6 link-local address of that interface. It may look something like this:

Network protocols

Windows IP Configuration Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : testnetwork.com				
IP Address:	192.168.2.22			
Subnet Mask:	255.255.255.0			
IP Address:	fe80::204:75ff:fec2:3a79%4			
Default Gateway:	192.168.2.1			
	fe80::213:20ff:fe11:d2ee%4			

Running ping6 on Windows: ping6 fe80::2:240:8cff:fe6b:3cb9%4

Common IPv6 addresses and ranges

IPv6 address	Explanation
0:0:0:0:0:0:0	Equals IPv4 0.0.0.0 and is the source address of a host before it receives an IP address from DHCP
0:0:0:0:0:0:1	Equals ::1 and is the equivalent of IPv4 127.0.0.1
0:0:0:0:0:0:192.168.100.1	This is how an IPv4 address would be written in a dual-stack mixed IPv4-IPv6 environment
2000:::/3	The global unicast address range
FC00::/7	The unique local unicast range
FE80::/10	The link-local unicast range
FF00::/8	The multicast range
3FFF:FFFF::/32	Reserved for examples and documentation
2001:0DB8::/32	Reserved for examples and documentation
2002::/16	Used for IPv6 to IPv4 tunneling and used as a transition system which allows IPv6 packets to be transported over an IPv4 network without the need to configure an explicit tunnel.

IPv6: AXIS OS configuration

Web interface

The IP configuration of the Axis video product is usually made from the TCP/IP settings (see section 2.1) pages in the embedded web interface. In addition to this, you can list the parameters directly in the **Plain Config** page. From here you can customize the IPv6 configuration, by changing parameters that are not available from the TCP/IP settings page. On the TCP/IP settings page, it is possible to enable or disable the use of IPv4 and/or IPv6.

Network protocols

	AXIS P1435-E Network Camera	± 0
	тсрир	
	IPv4 Automatic IP (DHCP) and DNS (DHCP) Save	
	Friendly name Use Borjour™ Use Riters Use Riters	
	Bonjour name Policy AXIS P1435-E - ACCC8E54045D 	
	AXIS P1435-E - ACCC8E54045D	
	Current network settings IPv4 address: 172 27.56.194 Subnet mask: 255.256.128.0 IPv4 addresse: fe80.iseo:Beff:fe84.456 IPv4 addresse: fe80.iseo:Deff:fe84.456 IPv4 addresse:	
	IPV6 default route: Domain ame: labnet; md.axis.com se.axis.com axis.com axis.se Primary DNS server: 172.27.0.41 Secondary DNS server: Primary NTP server: Secondary NTP server: DHCP NTP server: DHCP NTP server: 172.27.0.41	
Image Stream Overlay PTZ Privacy mask View	area Apps System	
Emp Language D. 🚫	te and time Orientation Users ONVIF SNMP Detectors Maintena	

The user is prohibited from disabling both IPv4 and IPv6, since this will render the Axis device inaccessible. It is however, still possible to disable both IPv4 and IPv6 from the Plain Config page. If this happens, the Axis device will override the configuration and start IPv4 according to the IPv4 configuration.

Use of IPv4 is enabled by default. When IPv4 is disabled no IPv4 configuration will be made on the device. The device will then only be accessible via IPv6. Note that when IPv4 is disabled, a link-local IPv4 address will not be assigned, even if the use of a link-local IPv4 address is enabled on the Advanced TCP/IP Settings page.

Use of IPv6 is disabled by default. When IPv6 is enabled, the Axis device will assign a link-local IPv6 address. By default, the device will also listen to router advertisements and assign IPv6 addresses accordingly. It is possible to change the IPv6 configuration behavior using the plain configuration interface found in the Advanced System Options menu. For further descriptions of the advanced IPv6 settings.

Plain Config

The IPv6 configuration is by default set to accept router advertisements and to use DHCPv6 according to the router advertisements. In different environments it may be necessary to change the IPv6 configuration. To do this, go to the Plain Config page and select the Network parameter group. By altering the parameters in the Network.IPv6 parameter group, the behavior of the IPv6 configuration is changed. The group consists of five parameters:

Parameter	Comment
Network.IPv6.Enabled	This parameter is used to enable or disable IPv6 network configuration.

Network protocols

Network.IPv6.AcceptRA	The Accept router advertisements parameter is used to enable or disable the said functionality. If this parameter is set to yes, the Axis device will listen to router advertisements on the network and perform IPv6 configuration according to it.
Network.IPv6.DHCPv6	 This parameter is used to configure either of the four DHCPv6 client settings auto – The use of DHCPv6 is determined by the router advertisements stateless – DHCPv6 is used to set DNS servers and NTP servers etc, but not to set IPv6 addresses stateful – DHCPv6 is used to set IPv6 addresses as well as DNS servers, etc. off – DHCPv6 is disabled
Network.IPv6.IPAddress	The IP Address parameter is used to manually set an IPv6 address. This address will be used in parallel with other IPv6 addresses that may be set by DHCPv6 or by router advertisements. If a specific prefix length is requested the prefix length is defined last in the address, like this: 2001:5c0:84d9:2::1:3b/128. If no prefix length is defined, the default length 64 will be used.
Network.IPv6.DefaultRouter	The Default router parameter is used to manually set an IPv6 default router. This address will be set in parallel with other IPv6 addresses that may be set by DHCPv6 or by router advertisements.
Additional Information	The IPv6 addresses currently in use are read from the IP address parameter In the Network. <interface>.IPv6 group, where <<i>interface></i> is the name of the interface (e.g. eth0, eth1 etc). This parameter lists all IPv6 addresses, separated by space characters.</interface>

IPv6	
 Accept router advertisements 	
Default router	
DHCPv6	
auto	
IPv6 Enabled	
IP address	

IEEE 802.1X

There are different levels of security for a network's infrastructure and the devices connected to it. The first level is authentication and authorization. The user or device identifies itself to the network and the remote end by a username and password, which are then verified before the device is allowed into the system. Added security can be achieved by encrypting the data to prevent others from using or reading the data. Common methods are HTTPS (also known as SSL/ TLS), VPN, and WEP or WPA in wireless networks. IEEE 802.1X is an authentication and authorization technique. Axis network video products support IEEE 802.1X as a security feature. This section presents the background of IEEE 802.1X, as well as its working principle. It also describes how IEEE 802.1X should be used in Axis devices, and how the RADIUS (remote authentication dial-in user service) servers and switches need to be configured. The intended audience of this document is technical personnel and system integrators.

Network protocols

IEEE 802.1X is an IEEE standard for port-based network access control ("port" means the physical connection to the LAN infrastructure). It is part of the IEEE 802.1 group of networking protocols and provides an authentication mechanism for devices to connect to a LAN, either establishing a connection or preventing the connection if authentication fails. IEEE 802.1X prevents what is called "port hi-jacking", that is, when an unauthorized computer gets access to a network through a network jack inside or outside a building. IEEE 802.1X is useful in network video applications since their devices are often located in public spaces where a network jack can pose a security risk. In modern enterprise networks, IEEE 802.1X is becoming a basic requirement for anything that is connected to a network.

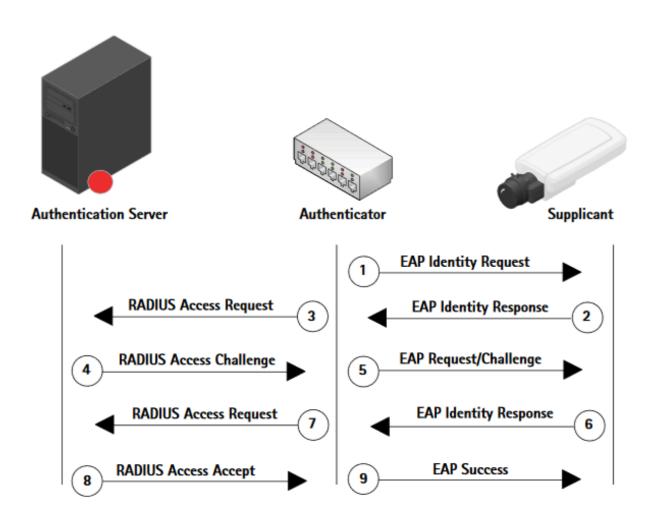
Working principle

There are three basic terms in IEEE 802.1X. The user or client that wants to be authenticated is called a supplicant. The actual server doing the authentication, typically a RADIUS server, is called the authentication server. And the device in between, such as a switch, is called the authenticator. The protocol used in IEEE 802.1X is EAPOL (Extensible authentication protocol encapsulation over LANs). There are several modes of operation, but the most common case is described here:

- The authenticator sends an "EAP-Request/Identity" packet to the supplicant as soon as it detects that the network link is active (this could be because the supplicant, for example a specific Axis device in a network video system, is connected to the switch).
- The supplicant sends an "EAP-Response/Identity" packet to the authenticator.
- The "EAP-Response/Identity" packet is then passed on to the authentication (RADIUS) server by the authenticator.
- The authentication server sends back a challenge to the authenticator, such as with a token password system.
- The authenticator unpacks this from IP and repackages it into EAPOL and sends it to the supplicant. Different authentication methods will vary this message and the total number of messages. EAP supports client-only authentication and strong mutual authentication.
- The supplicant responds to the challenge by the authenticator.
- The authenticator passes the response to the challenge onto the authentication server.
- If the supplicant provides proper identity, the authentication server responds with a success message to the authenticator.

The success message is then passed onto the supplicant by the authenticator. The authenticator now allows access of the supplicant to the LAN, possibly restricted based on attributes that came back from the authentication server. For example, the authenticator might switch the supplicant to a particular virtual LAN or install a set of firewall rules.

Network protocols



It should be noted that setting up and configuring IEEE 802.1X is a fairly complex procedure, and it is important that RADIUS servers, switches, and clients (such as Axis devices) are set up correctly.

IEEE 802.1X: AXIS OS configuration

Web interface

To gain access to a protected network, the Axis device must have a CA certificate, a client certificate, and a client private key. These should be created by the servers and uploaded via a web interface. When the Axis device is connected to the network switch, the device will present its certificate to the switch. If the certificate is approved, the switch allows the device access on a preconfigured port. As pointed out previously, in order to use port-based authentication, the network must be equipped with a RADIUS server and a network switch with support for IEEE 802.1X. You may also need to contact your network administrator for information on certificates, user IDs and passwords depending on the type of RADIUS server that is used.

The settings here enable the Axis device to access a network protected by IEEE 802.1X/EAPOL (Extensible Authentication Protocol over LAN). There are many EAP methods available to gain access to a network. Before AXIS OS 11.6, the protocol used by Axis is EAP-TLS (EAP-Transport Layer Security) for wired and wireless IEEE 802.1X network authentication, as well as EAP-PEAP/MSCHAPv2 for wireless IEEE 802.1 network authentication.

Network protocols

Client certificate	
none	*
CA certificate	
none	v
EAP Identity	
EAPOL Version 0 1	
Use IEEE 802.1x	

Excerpt of the web interface of AXIS M1065-LW with wired IEEE 802.1X settings

Network protocols

Wireless networks	~
No network selected	
Add another network	^
SSID name	
Use WPA ^{TU}	
Use Enterprise	
WPA-Enterprise protocol	
EAP-TLS	
EAP-PEAP/MSCHAPv2	
Identity	
EAPOL version	
1	,
CA certificate	
None	
Client certificate	
None	

Excerpt of the web interface of AXIS M1065-LW with wireless IEEE 802.1X settings (System tab > Wireless).

The client and the RADIUS server authenticate each other using digital certificates provided by a PKI (public key infrastructure) signed by a certification authority. Note that to ensure successful certificate validation, time synchronization should be performed on all clients and servers prior to configuration. Further configuration of Axis devices should be performed on a safe network to avoid MITM (man in the middle) attacks. Terms used in the web interface are described as follows:

- CA certificate The CA certificate is created by the certification authority for the purpose of validating itself and the Axis device needs it to check the server's identity. Select the correct certificate that was uploaded previously in the security tab under CA certificates. From AXIS OS 10.1 and onwards, selecting no CA certificate (none) means the Axis device will skip doing any validation of the server's identity.
- **Client certificate** The Axis device must also authenticate itself using a client certificate. Select the correct certificate that was uploaded previously in the security tab under client certificates.
- EAPOL version Select the EAPOL version (1 or 2) used in your network switch.
- EAP identity Enter the user identity associated with your certificate. A maximum of 16 characters can be used.

Network protocols

With AXIS OS 11.6 and later, we added support for EAP-PEAP/MSCHAv2 for wired connection. With AXIS OS 11.8 and later, customers can configure EAP-PEAP/MSCHAPv2 through the web interface.

Vse IEEE 802.1x

Network protocols

Authentication method		
EAP-PEAP/MSCHAPv2		
Client certificate		
Axis device ID ECC-P256 (802.1AR)		,
CA certificates		
r2d2 ×	×	•
EAP Identity		
dotxmschap		
EAPOL Version		
O 1 🦲 2 🔘 3		
Password		

Peap version		
● PEAPv0 ○ PEAPv1		
Label		
1 O 2		

Network protocols

- Client certificate This is not needed for this authentication mode.
- CA certificate Optional. The CA certificate is created by the certification authority for the purpose of validating the server's identity by the Axis devices. No CA certificate (none) means the Axis device will skip doing any validation of the server's identity.
- EAP identity The username for MSCHAPv2 authentication.
- EAPOL version Select version 2.
- **Password** The password for MSCHAPv2 authentication.
- Peap version Select PEAPv0.
- Label Select 1.

IEEE 802.1AE

With AXIS OS 11.8 and later, IEEE 802.1AE MACsec capabilities were added to AXIS OS-based devices.

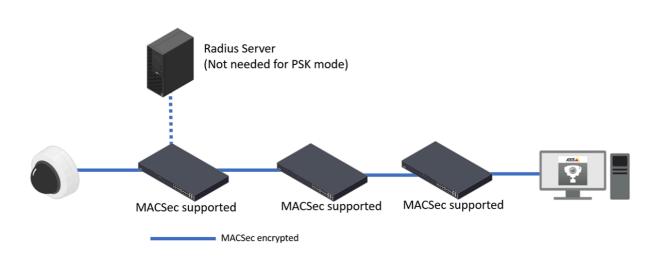
IEEE 802.1AE MACsec (Media Access Control Security) is a well-defined network protocol that cryptographically secures point-to-point ethernet links on network layer 2 ensuring the confidentiality and integrity of data transmissions between two hosts.

OSI Layer	Unencrypted Network Protocols	Encrypted Network Protocols
Layer 7 – Application*	UPnP, DHCP, DNS, HTTP, SNMPv1/v2, FTP, NTP, RTP, RTSP, SMPT, MQTT, Syslog, SIP	HTTPS, SNMPv3, NTS, SSH, SRTP
Layer 6 – Presentation*		TLS/SSL
Layer 5 – Session*	RTCP, SMB	
Layer 4 – Transport*	TCP/UDP	
Layer 3 – Network*	IP, ICMP, ARP, IGMP	
Layer 2 – Data Link*	CDP, LLDP	802.1X EAP-TLS, 802.1AE MACsec
Layer 1 – Physical*		

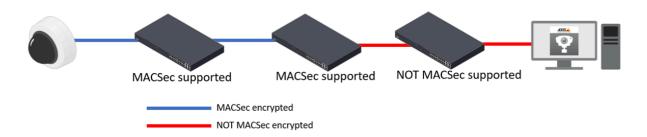
* List of example network protocols used by Axis devices that are protected by IEEE 802.1AE MACsec. MACsec adds protection to network protocols without native security capabilities and adds an additional layer of protection as well to network protocols with built-in security.

Unlike protocols such as IPSec which operates at Layer 3 as an end-to-end technology, MACsec encrypts each frame that leaves the Ethernet LAN and decrypts the frames as it enters the Ethernet LAN. In order to achieve end-to-end network encryption using MACsec, all links/hops in between source and destination need to have MACsec enabled to ensure traffic traversing across a network is MACsec protected.

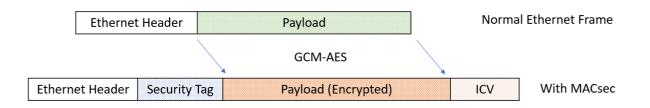
Network protocols



A single link/hop that does not support MACsec will therefore leave network traffic unencrypted from that link/hop to the next.



Not only does MACsec prevent unauthorized access to network data streams through strong encryption but also prevents man-in-the-middle attack scenarios. Because MACsec operates at the low layer 2 of the network stack, it adds an additional layer of security to network protocols that do not offer native encryption capabilities (ARP, NTP, DHCP, LLDP, CDP...) as well as ones that do offer it alike (HTTPS, TLS). The illustration below outlines the MACsec frame.



A Security Tag (SecTAG) containing MACsec parameters is inserted immediately after the source mac address in the Ethernet Header. The Integrity Check Value(ICV) is calculated via an agreed algorithm by the sender and attached to the frame. When the receiver receives the frame, it will use the same algorithm to calculate the ICV again and compare it with the one attached to the packet. The integrity is confirmed if the two ICV values are identical which means the packet is not tampered.

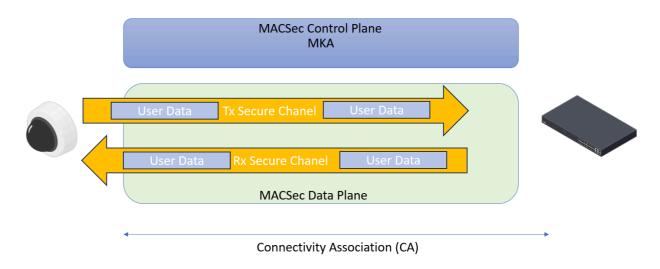
Terminologies

Network protocols

Acronym	Terminology	Description
CA	secure Connectivity Association	A security relationship, established and subset of the service access points in s supported by MACsec
САК	Connectivity Association Key	This key is used to derive the actual key via 802.1x authentication.
CKN	Connectivity Association Key Name	The name of the CAK.
МКА	MACsec Key Agreement	The protocol used to negotiate the key
SC	Secure Chanel	A security relationship used to provide Connectivity Association (CA) to the ot
SAK	Secure Association Key	It is derived from a CAK using a specifi

The MACsec Key Agreement (MKA)

When implementing MACsec between two devices, the MACsec Key Agreement(MKA) protocol provides and manages the session keys. The MKA protocol relies on the EAP framework to establish the communication. The two devices establish a unique connectivity association. Within the CA, there are two secure channels, one for inbound traffic, and the other one for outbound traffic. The two devices use the same cipher suite for data encryption.



MACsec Ciphers

To protect the confidentiality of the data traveling through the MACsec Secure Channel, the packets are encrypted by the industrial standard GCM-AES-128 or GCM-AES-256 cipher suites. There are another two cipher suites GCM-AES-XPN-128 and GCM-AES-XPN-256. XPN standards for Extended Packet Numbering, these two ciphers are generally used on high-speed links.

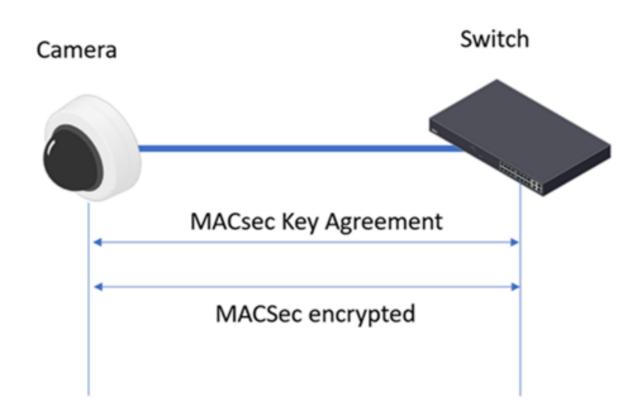
In the current implementation, AXIS OS supports GCM-AES-128 cipher suite only. Additional cipher suites can be added on demand.

MACsec modes

The IEEE 802.1AE MACsec standard describes two modes of operation, a manually configurable Pre-Shared Key (PSK)/Static CAK mode and an automatic Master Session/Dynamic CAK mode using IEEE 802.1X EAP-TLS sessions. The Pre-Shared Key mode is recommended to be used when the connecting network switch is not capable of supporting auto-negotiation through IEEE 802.1X EAP TLS.

Since IEEE 802.1X EAP-TLS is enabled by default and through that, MACsec Master Session/Dynamic CAK mode is also automatically enabled. When plugging in a factory defaulted Axis device, IEEE 802.1X network authentication will be tried and when successful, MACsec Dynamic CAK mode will be tried as well. If the connected switch does not support IEEE 802.1X EAP TLS and/or MACsec Dynamic CAK, then the Axis device will simply connect anyway without further enforced security mechanisms.

Network protocols



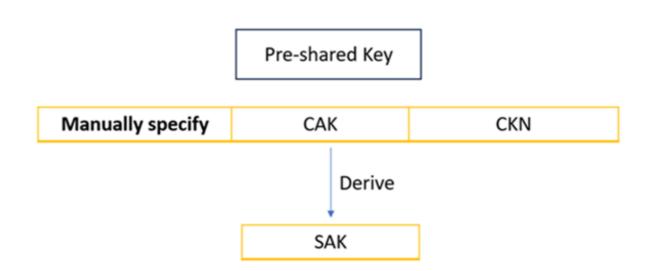
Pre-shared Keys (PSK), Static CAK mode

In pre-shared key(PSK) mode, also known as static CAK mode, the MACsec implementation is comprised of three phases: PSK configuration, MKA key negotiation and MACsec data encryption and decryption.

This mode requires the user to configure the to-be-used pre-shared key on both devices, the Axis device and the network switch. Every PSK consists of two fields: a connectivity association key name (CKN) and a connectivity association key (CAK). The CKN and CAK must match on both ends of the ethernet link.

Once the pre-shared key is verified, the MKA protocol is enabled to maintain the MACsec session on the link. One participant on the link will be elected as the key server and its primary responsibility is to generate, distribute and refresh the Secure Association Key(SAK). The SAK is the actual key used for encrypting the data. The MKA protocol limits the number of frames that can be protected with a single SAK. When the Packet Numbers (PNs) in an SA are exhausted, the corresponding SAK will be refreshed.

Network protocols



Axis device configuration

To configure the MACsec PSK in AXIS OS devices, go to System > Security > IEEE 802.1ae MACsec > Mode, select "Static CAK / Pre-Shared Key(PSK)" mode.

IEEE 802.1ae MACsec

Secured

Mode

Static CAK / Pre-Shared Key (PSK)

Key agreement connectivity association key name

001122334455667711111111111111111

Key agreement connectivity association key

The CAK must be either 16 bytes (32 hexadecimal characters) or 32 bytes (64 hexadecimal characters). The CKN must be 1 to 32 bytes (2 to 64 and divisible by 2) hexadecimal characters.

At the time of writing this article, please also check the box to enable IEEE 802.1x before saving the configuration. When MACsec is secured, the status of IEEE 802.1x will show "authorized". We are in the process of optimize this as MACsec PSK mode doesn't work in conjunction with 802.1x.

Network protocols

Switch configuration

The below configuration example is outlined using the Aruba CX switch series.

1. Configure the MACsec policy

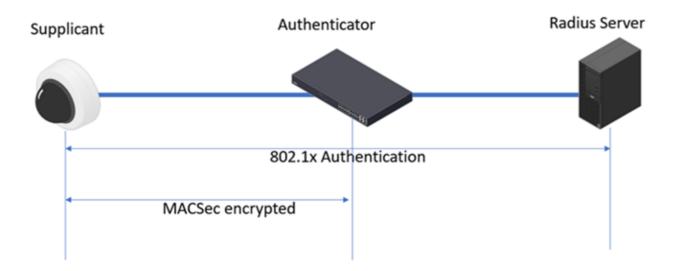
```
switch(config)# macsec policy axis_ms_policy
switch(config-macsec-policy)# cipher-suite gcm-aes-128
switch(config-macsec-policy)# replay-protection window-size 100
switch(config-macsec-policy)# exit
switch(config)#
```

2. Configure the MKA policy

3. Apply the MAC on the switch port

```
switch(config)# interface 1/1/28
switch(config-if)# apply macsec policy axis_ms_policy
switch(config-if)# apply mka policy axis_ms_policy
switch(config-if)# exit
switch(config)#
```

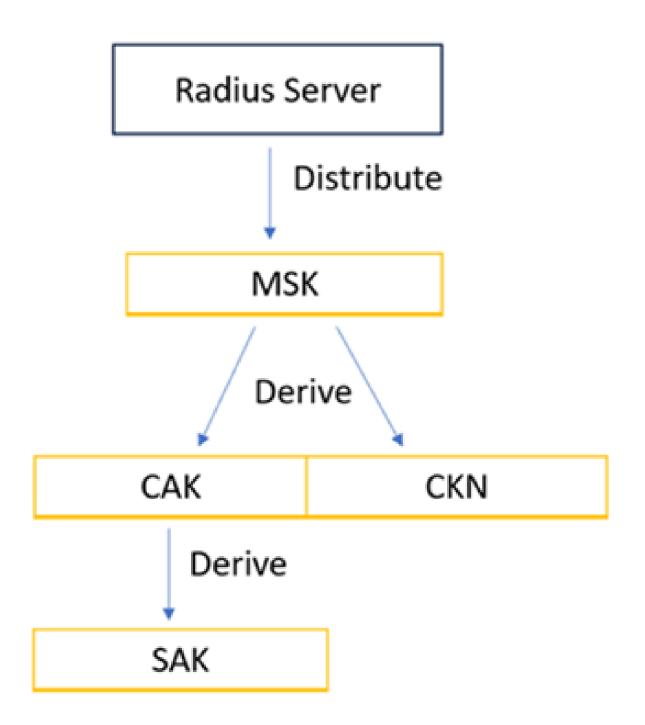
Master Session Key (802.1x, EAP-TLS), Dynamic CAK mode



When implementing MACsec in conjunction with EAP-TLS, the Authenticator or the access switch performs the 802.1x authentication against the devices first. Once authentication is successful, the Radius server sends the master session key (MSK) to the switch and the device. The CAK and CKN will be derived from the MSK by both parties.

Following that, the MKA protocol is enabled on both parties on the link to start the MACsec session. Same as the PSK mode, one of the parties will be elected as the key server to manage the SAK keys. Once the SAK key is exchanged between the parties, the MACsec encryption and decryption starts.

Network protocols



Axis device configuration

Since AXIS OS 10.1 (September 2020), IEEE 802.1X is enabled in the factory default state using the IEEE 802.1AR-compliant Axis device ID certificate. The Axis device will automatically try to authenticate against an IEEE 802.1X-enabled network. For manual IEEE 802.1X configuration, please refer to the *AXIS OS Knowledge base*. To use 802.1x port-based authentication, the network must be

Network protocols

equipped with a RADIUS server and a network switch with support for IEEE 802.1X and IEEE 802.1AE MACsec. You may also need to contact your network administrator for information on certificates and further configuration of the RADIUS server.

Once the 802.1x authentication is done, if the switch supports MACsec, the MACsec talk will happen accordingly.

Freeradius Server configuration

Once the Freeradius server is up and running, there is just one additional step needed to enable the usage of MACsec through the Freeradius server side. The FreeRADIUS server in this case needs to send the EAP-KEY-NAME attribute for the switch to derive the Session-ID used in creating the CKN and CAK for MKA.

To enable FreeRADIUS to send the EAP-Session-ID in Access-Accept frames, please uncomment the following lines inside:

```
/etc/freeradius/sites-enabled/default for FreeRADIUS 2.x
```

or

/etc/freeradius/3.0/sites-enabled/default in case of FreeRADIUS 3.x

	# #	MacSEC requires the use of EAP-Key-Name. However, we don't want to send it for all EAP sessions. Therefore, the EAP modules put required data into the EAP-Session-Id attribute.
	#	This attribute is never put into a request or reply packet.
	#	Uncomment the next few lines to copy the required data into
	#	the EAP-Key-Name attribute
#	if	(&reply:EAP-Session-Id) {
#		update reply {
#		EAP-Key-Name := &reply:EAP-Session-Id
#		}
#	}	

In this document, we are using the Aruba CX switch series that requires a User-Role after the 802.1x authentication to trigger the MACsec. The "Aruba-User-Role" is a vendor-specific-value sent from the FreeRadius server to the Aruba switch based on the EAP-identity configured in the AXIS OS devices. To do that, please add below to the file /etc/freeradius/3.0/users.

Network protocols

```
#steve cleartext-Password := "testing"
# Service-Type = Framed-User,
# Framed-Protocol = PPP,
# Framed-IP-Address = 172.16.3.33,
# Framed-IP-Netmask = 255.255.255.0,
# Framed-Routing = Broadcast-Listen,
# Framed-Filter-Id = "std.ppp",
# Framed-Filter-Id = "std.ppp",
# Framed-MTU = 1500,
# Framed-Compression = Van-Jacobsen-TCP-IP
```

Aruba ClearPass Policy Manager configuration

Please follow the instructions *here* to securely onboard the Axis devices into Aruba networks. The integration guide outlines example configurations in great detail using IEEE 802.1AR and 802.AE MACsec for secure zero trust network integration of Axis devices into Aruba networks. The "Aruba-user-Role" attribute must also be dispatched from the ClearPass Policy Manager to the switch.

Aruba switch configuration

1. Configure the MACsec policy

```
switch(config)# macsec policy macsec-eap
switch(config-macsec-policy)# cipher-suite gcm-aes-128
switch(config-macsec-policy)# replay-protection window-size 100
switch(config-macsec-policy)# exit
switch(config)#
```

2. Configure the port-access role

```
switch(config)# port-access role axiscamera
switch(config-pa-role)# associate macsec-policy macsec-eap
switch(config-pa-role)# auth-mode client-mode
```

3. enable MACsec on the port

```
switch(config-if)# aaa authentication port-access dot1x authenticator
switch(config-if-dot1x-auth)# macsec
```

Network protocols

switch(config-if-dot1x-auth) # mka cak-length 16

The cak-length should be configured to 16 bytes for the dot1x authentication mode in our current implementation.

Verify the MACsec status on the AXIS OS devices:

IEEE 802.1x Authorized	IEEE 802.1ae MACsec Secured
Authentication method	Mode
EAP-TLS 💌	Dynamic CAK / EAP-TLS 🔹
Client certificate 🕠	
Axis device ID RSA-2048 (802.1AR)	
CA certificates	
No CA certificate selected	
EAP Identity	
axis-b8a44f0d8672	
EAPOL Version	
O 1 O 2 🖲 3	
Vse IEEE 802.1x	

Below is what the MACsec frames look like when doing a packet trace from the camera directly. Go to System > Logs > Network trace.

Save

	Time		Source	Destination	Protocol	Length	Info
11	5802 2023-10-05	15:04:04,371476	AxisComm_d9:c8:5f	IntelCor_6f:bc:6a	MACSEC	1514	MACsec frame
11	5804 2023-10-05	15:04:04,371604	AxisComm_d9:c8:5f	IntelCor_6f:bc:6a	MACSEC	1514	MACsec frame
11	5806 2023-10-05	15:04:04,371710	AxisComm_d9:c8:5f	IntelCor_6f:bc:6a	MACSEC	1514	MACsec frame
11	5808 2023-10-05	15:04:04,371836	AxisComm_d9:c8:5f	IntelCor_6f:bc:6a	MACSEC	1514	MACsec frame
11	5810 2023-10-05	15:04:04,371943	AxisComm_d9:c8:5f	IntelCor_6f:bc:6a	MACSEC	1514	MACsec frame
11	5812 2023-10-05	15:04:04,372239	AxisComm_d9:c8:5f	IntelCor_6f:bc:6a	MACSEC	1514	MACsec frame
11	5814 2023-10-05	15:04:04,372283	AxisComm_d9:c8:5f	IntelCor_6f:bc:6a	MACSEC	1514	MACsec frame
11	5816 2023-10-05	15:04:04,372323	AxisComm_d9:c8:5f	IntelCor_6f:bc:6a	MACSEC	1514	MACsec frame
11	5818 2023-10-05	15:04:04,372456	AxisComm_d9:c8:5f	IntelCor_6f:bc:6a	MACSEC	1514	MACsec frame
11	5820 2023-10-05	15:04:04,372585	AxisComm_d9:c8:5f	IntelCor_6f:bc:6a	MACSEC	1514	MACsec frame
11	5822 2023-10-05	15:04:04,372695	AxisComm_d9:c8:5f	IntelCor_6f:bc:6a	MACSEC	1514	MACsec frame
11	5824 2023-10-05	15-04-04 372838	AvisComm d9:c8:5f	IntelCor 6f:bc:6a	MACSEC	1514	MACser frame
Ether	net II, Src: Ax	isComm_d9:c8:5f		captured (12288 bits) st: IntelCor_6f:bc:6a (b0:3c:dc:6	F:bc:6a)		
Ether > De > So	net II, Src: Ax stination: Inte	isComm_d9:c8:5f lCor_6f:bc:6a (b d9:c8:5f (ac:cc:	(ac:cc:8e:d9:c8:5f), D 0:3c:dc:6f:bc:6a)		f:bc:6a)		
Ether > De > So Ty	net II, Src: Ax stination: Inte urce: AxisComm_	isComm_d9:c8:5f lCor_6f:bc:6a (b d9:c8:5f (ac:cc: Csec) (0x88e5)	(ac:cc:8e:d9:c8:5f), D 0:3c:dc:6f:bc:6a)		f:bc:6a)		
Ether > De > So Ty 802.1 > 00	net II, Src: Ax stination: Inte urce: AxisComm_ pe: 802.1AE (MA AE Security tag 10 11 = TCI: 00 = AN: 0	isComm_d9:c8:5f lCor_6f:bc:6a (t d9:c8:5f (ac:cc: Csec) (0x88e5) 0x0b, VER: 0x0,	(ac:cc:8e:d9:c8:5f), D 0:3c:dc:6f:bc:6a) 8e:d9:c8:5f)		F:bc:6a)		
Ether > De > So Ty 802.1 > 00 	net II, Src: Ax stination: Inte uurce: AxisComm_ pe: 802.1AE (MA AE Security tag 10 11 = TCI: 00 = AN: 0 nort length: 0	isComm_d9:c8:5f lCor_6f:bc:6a (t d9:c8:5f (ac:cc: Csec) (0x88e5) 0x0b, VER: 0x0, x0	(ac:cc:8e:d9:c8:5f), D 0:3c:dc:6f:bc:6a) 8e:d9:c8:5f)		f:bc:6a)		
Ether > De > So Ty 802.1 > 00 Sh Pa	<pre>net II, Src: Ax stination: Inte uurce: AxisComm_ pe: 802.1AE (MA AE Security tag 10 11 = TCI: 00 = AN: 0 oort length: 0 ucket number: 14</pre>	isComm_d9:c8:5f lCor_6f:bc:6a (t d9:c8:5f (ac:cc: Csec) (0x88e5) 0x0b, VER: 0x0, x0 3677	(ac:cc:8e:d9:c8:5f), D 00:3c:dc:6f:bc:6a) 8e:d9:c8:5f) SC, E, C	st: IntelCor_6f:bc:6a (b0:3c:dc:6	F:bc:6a)		
Ether > De > So Ty 802.1 > 00 Sh Pa Sy	<pre>nnet II, Src: Ax stination: Inte urce: AxisCom- pe: 802.1AE (MA AE Security tag 10 11 = TCI: 00 = AN: 0 oort length: 0 cote length: 0 stem Identifier</pre>	15Comm_d9:c8:5f 1Cor_6f:bc:6a (t d9:c8:5f (ac:cc: Csec) (0x88e5) 0x0b, VER: 0x0, x0 3677 : AxisComm_d9:c8	(ac:cc:8e:d9:c8:5f), D 0:3c:dc:6f:bc:6a) 8e:d9:c8:5f)	st: IntelCor_6f:bc:6a (b0:3c:dc:6	F:bc:6a)		_
Ether > De > So Ty 802.1 > 00 Sh Pa Sy Po	net II, Src: Ax stination: Inte pe: 802.1AE (MA AE Security tag 10 11. = TCI: 00 = AN: 0 oort length: 0 cket number: 14 stem Identifier ri Identifier:	isComm_d9:c8:5f lCor_6f:bc:6a (t d9:c8:5f (ac:cc: Csec) (0x88865) 0x0b, VER: 0x0, x0 3677 : AxisComm_d9:c8 1	(ac:cc:8e:d9:c8:5f), D 00:3c:dc:6f:bc:6a) 8e:d9:c8:5f) SC, E, C SSC, E, C SSC (ac:cc:8e:d9:c8:5f)	st: IntelCor_6f:bc:6a (b0:3c:dc:6	f:bc:6a)		_
Ether > De > So Ty 802.1 > 00 Sh Pa Sy Po IC	<pre>met II, Src: Ax stination: Inte uurce: AxisComm_ pe: 802.1AE (MA AE Security tag 10 11 = TCI: 0 ort length: 0 icket number: 14 stem Identifier V: 6f637465742d</pre>	15Comm_d9:c8:5f 1Cor_6f:bc:6a (t d9:c8:5f (ac:cc: Csec) (0x88e5) 0x0b, VER: 0x0, x0 3677 : AxisComm_d9:c8	(ac:cc:8e:d9:c8:5f), D 00:3c:dc:6f:bc:6a) 8e:d9:c8:5f) SC, E, C SSC, E, C SSC (ac:cc:8e:d9:c8:5f)	st: IntelCor_6f:bc:6a (b0:3c:dc:6	F:bc:6a)		_
Ether > De > So Ty 802.1 > 00 Sh Pa Sy Po IC Data	net II, Src: Ax stination: Inte unce: AxisComm_ pe: 802.1AE (MA AE Security tag 10 11 = TCI: 00 = AN: 0 oort length: 0 toket number: 14 stem Identifier rt Identifier: V: 6f637465742d (1492 bytes)	isComm_d9:c8:Sf lCor_6f:bc:6a (t 09:c8:Sf (ac:cc: Csec) (0x88e5) 0x00, VER: 0x0, x0 3677 : AxisComm_d9:c8 1 73747265616d0d0a	(ac:cc:8e:d9:c8:5f), D M9:3c:dc:6f:bc:6a) 8e:d9:c8:5f) SC, E, C N:5f (ac:cc:8e:d9:c8:5f)	st: IntelCor_6f:bc:6a (b0:3c:dc:6	F:bc:6a)		

Verify the MACsec status on the Aruba Switch:

Network protocols

```
switch# show macsec status
MACsec Protocol Status
Interface Port ID Policy Protection Status State
                                       _____ ____
_____
_____
1/1/27 1 macsec-eap IC, Conf, Offset 0 Up Retire
1/1/28 1 axis_ms_policy IC, Conf, Offset 0 Up Retire
SW23# show mka policy
MKA Policy Details
_____
Policy Name: MKA Auth 1/1/27 b8a44f4645f4
                                  -----
   _____
Mode : EAP-TLS
CKN : b0d80475242fbcd5c97ece50670e4dfe
CAK (encrypted) : AQBapQh5tkM/wWCQLE4jp0G/Iu6If0+QutBMu8gFBKf...
Key-server Priority : 0
Transmit Interval : 2 seconds
Policy Name: axis-mka policy
                               _____
Mode : Pre-shared key
CKN : 001122334455667711111111111111111
```

```
CAK (encrypted) : AQBapcO5rGnurI1zhrDB3JVwhbLmJhcgQkiRWgiJtfK...
Key-server Priority : 5
Transmit Interval : 2 seconds
```

WS-Discovery (Web Services Dynamic Discovery Protocol)

The Web Services Dynamic Discovery protocol utilizes UDP Port 3702 and defines itself as a multicast discovery protocol that is used to detect other devices and services on the network. ONVIF is relying on this protocol in order to detect other capable devices, so Axis devices support WS-Discovery for initial on-boarding and configuration. It's recommended to disable the WS-Discovery after usage since it is vulnerable to attacks as described in this *security advisory*. See instructions below on how to disable WS-Discovery.

AXIS OS > 9.70

Disable the service by disabling the parameter Enable WS-Discovery discoverable mode in Settings > System > Plain config > WebService > DiscoveryMode > Enable WS-Discovery. For multiple device configuration in AXIS Device Manager, the corresponding VAPIX parameter is called DiscoveryMode.Discoverable.

AXIS OS 5.70 - 9.60

- Enable SSH in Plain config > Network > SSH and connect to the Axis device via Putty
- Type the following commands, each followed by pressing ENTER
 - systemctl mask wsdd
 - systemctl mask wsd
 - systemctl mask wsd.socket
 - systemctl stop wsdd
- Disable SSH again from Plain Config and restart the device

AXIS OS 5.60

Network protocols

- Enable SSH in Plain Config > Network > SSH and connect to the Axis device via Putty
- Type the following commands, each followed by pressing ENTER
 - rm /etc/rc3.d/S92wsdd
 - /etc/init.d/wsdd stop
- Disable SSH again from Plain Config and restart the device

AXIS OS < 5.50

- Enable Telnet and connect to the Axis device via command-line tool. Go to Telnet access on page 327.
- Type the following commands, each followed by pressing ENTER
 - rm /etc/rc3.d/S92wsdd
 - /etc/init.d/wsdd stop
- Disable Telnet again and restart the device

Bonjour

Bonjour is Apple's implementation for zero-configuration networking. A method that helps the users to find services on a local network. By using mDNS and DNS-SD protocols, Bonjour covers three major areas:

- Addressing Bonjour self-assigns a link-local address if no DHCP server is present in the network. For IPv4, randomly selected from 169.254.0.0/16. For IPv6, the address is assigned from fe80::/10.
- 2. Hostname to IP address translation Bonjour uses multicast DNS (mDNS) in the local network to resolve a hostname.
- Service Discovery Bonjour discovers the available services in the local network via DNS service records.

The mDNS protocol resolves the hostname to the IP address without relying on a conventional unicast-based DNS server in a local network. The mDNS messages are sent through multicast (IPv4: 224.0.0.251 or IPv6: ff02::fb) to UDP port 5353. The Axis device will select a domain name with the prefix ".local", which only works with mDNS within the local network. An example domain name is "AXIS P1375.local".

To discover a service and use that service in the network by a client, several DNS records are used in the process:

Туре	Name	Purpose	Convention	
А	A Record	Resolve a hostname to an IPv4 address		
АААА	AAAA Record	Resolve a hostname to an IPv6 address		
SRV	Service Record	Maps the service instance to the hostname and port number	<instance name="">.<service td="" type:<=""><td>>.<domain></domain></td></service></instance>	>. <domain></domain>

Network protocols

PTR	Pointer Record	Maps the service type to the specific instance of that service	<service type="">.<domain></domain></service>
TXT	Text Record	The text field normally describes additional information about the service	Key=value

Axis Bonjour implementation

Prior to AXIS OS 11.4, AXIS OS products used Bonjour to announce their presence in the network. Starting from AXIS OS 11.4, we added new service names - *vapix-http* and *vapix-https* - to simplify the discovery of Axis devices and better comply with the RFC 6763 specification. In the table below, you can see some examples of service names used on AXIS OS devices.

Service name	Default instance name		Transport	Port	TXT	Remark
	< 11.4	≥ 11.4	protocol	(default port number)		
axis-video	AXIS <model> - mac/serial number**</model>		TCP	http port If http (and http re-direct) is disabled, it will not be advertised.	macaddress	Camera and audio products
axis-bwsc			TCP		macaddress	Body Worn SCU
axis-nvr			TCP		macaddress	Recorders
http	AXIS <model> - mac/serial number**</model>		TCP	80		
https			TCP	443		
rtsp			TCP	554	path, camera	
vapix-http* vapix-https*	N/A	AXIS <model>***</model>	ТСР	The HTTP or HTTPS port of the service. By default 80 or 443.	 sn=< serial num- ber> txtve- rs=1 ep=para tags= ***** 	Added from AXIS OS 11.4. m,apidisc,decaf****

*VAPIX is Axis own open API (Application Programming Interface) to our products, using standard protocols that enable integration into a wide range of solutions on different platforms.

** Example: AXIS P1375 - B8A44F42B4C6

*** Example: AXIS P1375. If you add a second device of the same model, the second one will be named AXIS P1375 (2) and so on.

**** param stands for param.cgi, apidisc stands for apidiscovery, and decaf stands for device configuration framework. Decaf was added in AXIS OS 11.11 and is included in all subsequent versions.

***** This field is used by services to indicate temporary roles.

AXIS OS < 11.4

In the below example, an Axis P1375 camera is running on the AXIS OS version earlier than 11.4. We use AXIS IP Utility to discover an Axis device. AXIS IP Utility sends a query message including PTR record. Querying a service instance called "_axis-video._tcp.local".

Network protocols

8066 2022-12-30 11:04:39,046881 192.168.0.4 224.0.0.251 MDNS 82 Standard query 0x0000 PTR _axis-video._tcp.local, "QM" question > Frame 8066: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{F98F2CB5-C9CD-400E-AE88-D374F6472ADC}, id 0
> Ethernet II, Src: HP_c6:a1:f1 (84:69:93:c6:a1:f1), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
> Internet Protocol Version 4, Src: 192.168.0.4, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353 Multicast Domain Name System (query) Transaction ID: 0x0000 > Flags: 0x0000 Standard query
Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0

- ✓ Queries

> _axis-video._tcp.local: type PTR, class IN, "QM" question

Once the Axis device receives the query message, it will respond with a mDNS query response containing the PTR record and additional records.

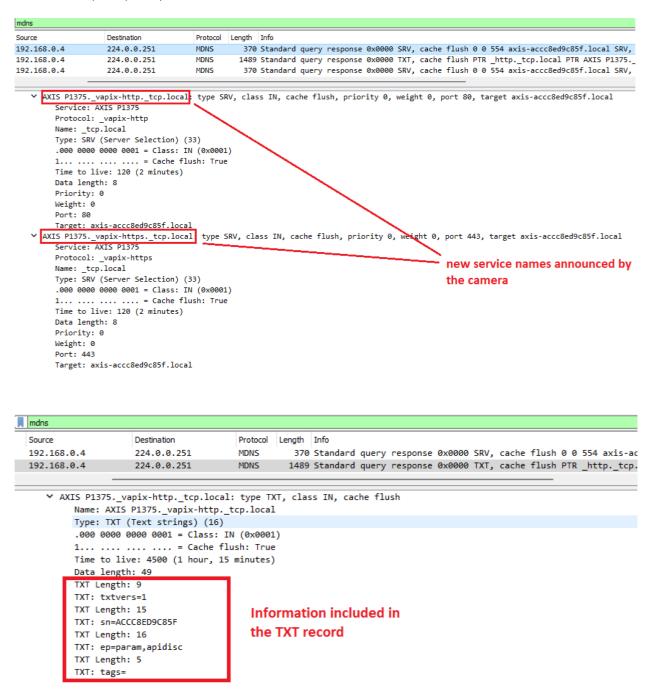
8072 2022-12-30 11:04:39,117633	192.168.0.3 224.0.0.251	MDNS 260 Standa	ard query response 0x0000 PTR AXIS P1375 - B8A44F42B4C6z	xis-videotcp.local TXT,
Frame 8072: 260 bytes on wire (2080 bits)	. 260 bytes captured (2080 bits)	on interface \Device\NPE	{F98F2CB5-C9CD-400E-AE88-D374F6472ADC}, id 0	
Ethernet II, Src: AxisComm_42:b4:c6 (b8:a				
Internet Protocol Version 4, Src: 192.168		(01100100100100100)		
User Datagram Protocol, Src Port: 5353, D				
Multicast Domain Name System (response)	50.00.00 5555			
Transaction ID: 0x0000				
> Flags: 0x8400 Standard query response,	No eccor			
Ouestions: 0				
Answer RRs: 1				
Authority RRs: 0				
Additional RRs: 6				
✓ Answers				
<pre>v axis-video. tcp.local: type PTR, c</pre>	1244 TN AVIS 01275 - PRAMAEA3PAC	6 pric video ten local	PTR	
Name: _axis-videotcp.local	1855 IN, AXIS F1575 - D0A44(4204C	oaxis-videoccp.iocai	T IK	
Type: PTR (domain name PoinTeR)	(12)			
.000 0000 0000 0001 = Class: IN				
0 = Cache flush				
Time to live: 4500 (1 hour, 15 m:	inutes)			
Data length: 28				
Domain Name: AXIS P1375 - B8A44F4	4284C6axis-Videotcp.local			
 Additional records 		T	VT	
✓ AXIS P1375 - B8A44F42B4C6axis-vid		, cache tlush	XT	
Name: AXIS P1375 - B8A44F42B4C6.	_axis-videotcp.local			
Type: TXT (Text strings) (16)	·			
.000 0000 0000 0001 = Class: IN				
1 = Cache flus				
Time to live: 4500 (1 hour, 15 m:	inutes)			
Data length: 24				
TXT Length: 23	ner and the tax and the			
	TXT contains information a		S	
✓ axis-b8a44f42b4c6.local: type A, cl	ass IN, cache flush, addr 192.168	.0.3		
Name: axis-b8a44f42b4c6.local				
Type: A (Host Address) (1)				
.000 0000 0000 0001 = Class: IN				
1 = Cache flus	1: True			
Time to live: 120 (2 minutes)				
Data length: 4				
	e IP address fo the device			
> axis-b8a44f42b4c6.local: type A, cl				
		, cache flush, priority 0	, weight 0, port 80, target axis-b8a44f42b4c6.local	SRV
Service: AXIS P1375 - B8A44F42B40	26			
Protocol: _axis-video				
Name: _tcp.local				
Type: SRV (Server Selection) (33))			
.000 0000 0000 0001 = Class: IN	(0x0001)			
1 = Cache flus	h: True			
Time to live: 120 (2 minutes)				
Data length: 8				
Priority: 0				
Weight: 0				
Port: 80				
Target: axis-b8a44f42b4c6.local				
	eo. tcp.local: type NSEC, class I	N, cache flush, next domai	in name AXIS P1375 - B8A44F42B4C6. axis-video. tcp.local	
> axis-b8a44f42b4c6.local: type NSEC,				
cype note;	,,,,,,			

"AXIS P1375 - B8A44F42B4C6" is the service instance name. "_axis-video._tcp" is the service type that identifies what the service does and its transport protocol. In this example, the Axis device announces itself by providing the "_axis-video" service through TCP. The TXT record contains the mac address information of the Axis device.

Network protocols

AXIS OS ≥ 11.4

Below is another example that the same Axis P1375 camera running on version 11.4. The camera announces the service instance as "AXIS P1375_vapix-http(s)._tcp.local". In the TXT records, additional information has been included there.



The devices are still announcing all the previous service names at the same time for the time being. So the VMSs and other clients should still be able to discover the Axis Devices, see below.

Network protocols

Time	Source	Destination	Protocol	Length Info
129 2023-02-15 17:47:44,154001	192.168.0.4	224.0.0.251	MDNS	1489 Standard query response 0x0000 TXT, cache flush PTR _httptcp.local PTR AXIS P1375httptcp.loca
rame 129: 1489 bytes on wire (11	.912 bits), 1489 b	ytes captured (11912	bits) on in	terface \Device\NPF_{F98F2CB5-C9CD-400E-AE88-D374F6472ADC}, id 0
thernet II, Src: AxisComm_d9:c8:			_fb (01:00:	5e:00:00:fb)
nternet Protocol Version 4, Src:				
lser Datagram Protocol, Src Port:		5353		
Nulticast Domain Name System (res	ponse)			
Transaction ID: 0x0000				
 Flags: 0x8400 Standard query r Ouestions: 0 	esponse, No error			
Answer RRs: 40				
Authority RRs: 0				
Additional RRs: 0				
Answers				
> AXIS P1375. http. tcp.local	: type TXT, class	TN, cache flush		
> services. dns-sd. udp.loca			1	
> http. tcp.local: type PTR,				
> AXIS P1375httpstcp.loca	1: type TXT, clas	s IN, cache flush		
> _servicesdns-sdudp.loca	l: type PTR, clas	s IN, _httpstcp.loc	al	
> _httpstcp.local: type PTR	, class IN, AXIS	P1375httpstcp.loc	əl	
> AXIS P1375 - ACCC8ED9C85F.				flush
> _servicesdns-sdudp.loca				
> _axis-videotcp.local: typ				videotcp.local
> AXIS P1375 H.264 1rtspt				
> _servicesdns-sdudp.loca				
<pre>> _rtsptcp.local: type PTR, > AXIS P1375 H.264 2. rtsp. t</pre>				
<pre>> rtsp. tcp.local: type PTR,</pre>				
> AXIS P1375 H.264 3rtspt				
<pre>> rtsp. tcp.local: type PTR,</pre>				
> AXIS P1375 H.264 4. rtsp. t				
> rtsp. tcp.local: type PTR,	class IN, AXIS P	1375 H.264 4. rtsp. t	cp.local	
> AXIS P1375 H.264 5. rtsp. t	cp.local: type TX	T, class IN, cache fl	ush	
> _rtsptcp.local: type PTR,	class IN, AXIS P	1375 H.264 5rtspt	cp.local	
> AXIS P1375 H.264 6rtspt	cp.local: type TX	T, class IN, cache fl	ush	
> _rtsptcp.local: type PTR,				
> AXIS P1375 H.264 7rtspt				
> _rtsptcp.local: type PTR,				
> AXIS P1375 H.264 8rtspt				
<pre>> _rtsptcp.local: type PTR,</pre>				
> AXIS P1375vapix-httptcp				
<pre>> _servicesdns-sdudp.loca > vapix-http. tcp.local: typ</pre>				
<pre>> AXIS P1375. vapix-https. to</pre>				1
<pre>> services. dns-sd. udp.loca</pre>				
<pre>> vapix-https. tcp.local: ty</pre>				cal
				ight 0, port 80, target axis-accc8ed9c85f.local
> axis-accc8ed9c85f.local: ty				
> axis-accc8ed9c85f.local: ty				
				eight 0, port 443, target axis-accc8ed9c85f.local
				flush, priority 0, weight 0, port 80, target axis-accc8ed9c85f.local
				ty 0, weight 0, port 554, target axis-accc8ed9c85f.local
	cp.local: type SR	V, class IN, cache fl	ush, priori	ty 0, weight 0, port 554, target axis-accc8ed9c85f.local ty 0, weight 0, port 554, target axis-accc8ed9c85f.local

The default instance name (in the webpage, we call "Bonjour name" or "Friendly name") can be changed when needed:

AXIS OS version	Web interface configuration path
< 7.10	Setup > System Options > Network > Bonjour
≥ 7.10	Settings > System > TCP/IP > Friendly name
≥ 10.9	System > Network > Network discovery protocols

After changing the friendly name, it will apply to all services.

SNMP (Simple Network Management Protocol)

This section describes how to use Axis Video SNMP MIB. It's assumed that you are familiar with the Simple Network Management Protocol (SNMP) already.

SNMP/MIBs allow network management operators to use standard SNMP tools to monitor the status of Axis products. The Axis Management Information Base (MIB) for video hardware enables monitoring of hardware-related issues that may need administrative attention. This applies to devices with AXIS OS 5.60 and higher. Note that new functionality may be added in later releases. For detailed information, read the MIB file.

Some products will not have all the hardware as specified below and there will only be one MIB defined for all hardware. In case the agent requests the status of hardware that is not included in the product, the device will return "noSuchObject". Which hardware is supported is handled at run time, meaning there is no need for product specific configuration. All Axis devices support the Axis Video MIB from AXIS OS 5.60 and higher except for AXIS Companion Line devices, however it's recommended to update to the latest version. These MIBs are required to use Axis Video MIB:

Network protocols

- SNMPv2–TC
- SNMPv2-SMI
- SNMPv2-CONF
- AXIS-ROOT-MIB
- AXIS-VIDEO-MIB

Enable SNMP

To use this functionality, SNMP must be enabled in the cameras and encoders on the network. SNMP in Axis devices can be enabled as below:

AXIS OS 6.5X and lower

SNMP can be enabled from the web interface using Setup > System Options > Network > SNMP.

AXIS OS 7.10 and higher

SNMP can be enabled from the web interface using Settings > System > SNMP.

To use SNMPv3, HTTPS has to be enabled. For information about how to enable HTTPS, see the user manual for the device.

You can use AXIS Device Manager to enable SNMP on multiple devices. AXIS Device Manager is available for download from *www.axis.com*.

SNMPv3 access

To enable SNMPv3 in Axis devices, a password must be set in the web interface for the default SNMP user *initial*. Once SNMPv3 is enabled, the following default privacy and authentication modes are pre-configured:

AXIS OS	Privacy	Authentication
> 11.0	AES-128	SHA-256
≥ 10.7	AES-128	SHA-1
< 10.6	DES	MD5

Note that it's currently not possible for the user to change the default privacy and authentication modes in an easy way.

SNMP trap configuration

All Axis devices support the default SNMP MIB-II traps (Cold start, Warm start, Link up, Authentication failed). In addition, Axis devices support a number of feature and product specific traps that are included in Axis Video MIB (described in *Axis Video MIB traps on page 112*). Depending on your SNMP version, different configurations are required/available for using SNMP traps.

SNMPv1/v2c trap configuration

When SNMPv1 and SNMPv2c are used, all Axis Video MIB traps documented in *Axis Video MIB traps on page 112* will be enabled and sent when SNMP traps are enabled. The default MIB-II SNMP traps can be configured and enabled/disabled individually:

- Cold start sent when SNMP has been started and the configuration and MIB have changed
- Warm start sent when SNMP has been started and the configuration has changed, but not the MIB
- Link up sent when the network link changed from down to up
- Authentication failed sent when snmp-authentication attempt failed

SNMPv3 trap configuration

For SNMPv3, both the default MIB-II SNMP traps as well as the Axis Video MIB traps need to be configured and enabled manually. This is done using the SNMP-TARGET-MIB and SNMP-NOTIFICATION-MIB modules, defined in RFC 3413. So in order to configure the Axis device to send out SNMP traps, the following tables need to be configured accordingly:

Network protocols

- snmpNotifyTable
- snmpTargetAddrTable
- snmpTargetParamsTable
- snmpNotifyFilterProfileTable
- snmpNotifyFilterTable

Axis Video MIB

Axis Video MIB (Message Information Base) extends the way to monitor Axis devices over SNMP. The Video MIB enables network administrators to monitor status information and a number of new notifications. To make use of the Axis Video MIB, download the MIB files *here* and import them in your SNMP network monitoring application. The Axis Video MIB is supported by Axis network devices from AXIS OS 5.60 and higher.

Axis Video MIB traps

There are only three kinds of traps that can be generated by a video product. These three kinds are defined in the Axis Video MIB and they should cover all the future needs of traps and thus they are defined in general terms. The trap types are described below:

- alarmNew This trap is sent to warn about a status change. Additional parameters include a unique trap ID (alarmID), a
 text string identifying the event (alarmName) and an additional string (alarmText) that specifies more detailed information
 about the event, for instance the unique identifier of the hardware or its status. This new state is valid until it is cleared by
 an alarmCleared trap. In general the state can be obtained through an SNMP get command as well.
- alarmCleared This trap is sent to indicate that some hardware has gone back to its normal state. The *alarmID* specifies the ID of a previous *alarmNew* trap that is cleared by this trap. Additional parameters include the same *alarmName* and *alarmText* that was sent by the *alarmNew* trap.
- alarmSingle This trap is sent to warn about a certain event. Additional parameters include a unique trap ID (*alarmID*), a text string identifying the event (*alarmName*) and an additional string (*alarmText*) that specifies more detailed information about the event, for instance the unique identifier of the hardware or its status. The difference from the *alarmNew* trap is that this trap refers to a stateless event. For this reason there is no *alarmCleared* and hence several traps indicating the same event might follow each other. Since this is a stateless event it is impossible to get any related information through SNMP get command.

Trap name/use case	Trap type	Alarm name	Alarm cleared event*	Supported products
(Multiple) Power Supply Failure	alarmNew	powerSupplyAlert	 	AXIS Q7900 Rack and AXIS Q7920 Video Encoder Chassis
(Multiple) Fan Failure	alarmNew	fanAlert	 Image: A state of the state of	AXIS Q7900 Rack and AXIS Q7920 Video Encoder Chassis
(High or Low) Temperature Limit Reached Alert	alarmNew	temperatureAlert	✓	All Axis devices
(Multiple) Analog Video S	galantolstew	videoSignalAlert	 	Axis video encoders, with AXIS OS 5.60 – 6.50
(Multiple) Audio Input Signal Lost	alarmNew	audioSignalAlert	Ý	All Axis audio-capable devices with external audio input
Product Casing Opened Alert	alarmNew	openCasingAlert	 	All Axis devices connected with AXIS T93F door switch / intrusion alarm

Network protocols

Mechanical PTZ Error Alert	alarmSingle	PTZAlert	\checkmark	All Axis mechanical PTZ devices
Edge Storage Alert	alarmNew	storageMediaAlert	V	All Axis devices featuring SD cards and mounted network share
Camera Tampering Alert	alarmSingle	tamperingAlert		All Axis tampering- capable devices (does not apply to AXIS Image Health Analytics)
General Trap	alarmNew or alarmSingle**	Custom AlarmText		All Axis devices

*The *alarm cleared event* is sent automatically. E.g. if the Axis device detects an issue with the storage devices, it will send out an alarm, and if the issue resolved itself, it will send another alarm notifying that the issue is resolved.

**Depending on whether the event is stateless or stateful the trap is of type *alarmNew* or *alarmSingle*

Axis Video MIB OIDs

The status operations that are available in the AXIS SNMP MIB are listed below. All statuses are read-only objects. If a set operation is requested on the OID it will return 17, notWritable (or 2,nosSuchName, for protocol version 1). A status operation can have one or more OIDs depending on the product. As an example, .1.3.6.1.4.1.368.4.1.1.1.3.x can be .1.3.6.1.4.1.368.4.1.1.1.3.1 Temperature Sensor 1, .1.3.6.1.4.1.368.4.1.1.1.3.2 Temperature Sensor 2, .1.3.6.1.4.1.368.4.1.1.1.3.3 Temperature Sensor 3, and so on.

OID Name	OID	Possible OID States	Supported products
Get Power Supply Status	.1.3.6.1.4.1.368.4.1.1.1.3.x	OK;Failure	AXIS Q7900 Rack and AXIS Q7920 Video Encoder Chassis
Get Fan Status	.1.3.6.1.4.1.368.4.1.2.1.3.1.x	OK;Failure	AXIS Q7900 Rack and AXIS Q7920 Video Encoder Chassis
Get Temperature Sensor Value	.1.3.6.1.4.1.368.4.1.3.1.4.1.x	Temperature in degree celsius	All Axis devices
Get Temperature Sensor Status	.1.3.6.1.4.1.368.4.1.3.1.3.1.x	OK;Failure;OutOfBoundary	All Axis devices
Get Video Signal Status	.1.3.6.1.4.1.368.4.1.4.1.2.x	SignalOK;NoSignal	All Axis video encoders
Get Audio Signal Status	.1.3.6.1.4.1.368.4.1.5.1.2.x	SignalOK;NoSignal	All Axis audio-capable devices
Get Casing Status	.1.3.6.1.4.1.368.4.1.6.1.3.x	Open;Closed	All Axis devices connected with AXIS T93F door switch / intrusion alarm
Get Storage Disruption Status	.1.3.6.1.4.1.368.4.1.8.1.3.x	Yes;No	All Axis devices

Network protocols

axis(1.3.6.1.4.1.368) - products(1) videoBased(1) video(4) videoObjects(1) powerSupplyTable(1) powerSupplyEntry(1) [powerSupplyType,powerSupplyId] Enumeration powerSupplyType(1) - Unsigned32 powerSupplyId(2) Enumeration powerSupplyStatus(3) fanTable(2) fanEntry(1) [fanType,fanId] - Enumeration fanType(1) - Unsigned32 fanId(2) - Enumeration fanStatus(3) tempSensorTable(3) tempSensorEntry(1) [tempSensorType,tempSensorId] Enumeration tempSensorType(1) Unsigned32 tempSensorId(2) Enumeration tempSensorStatus(3) Integer32 tempSensorValue(4) videoChannelTable(4) videoChannelEntry(1) [videoChannelId] — Unsigned32 videoChannelId(1) Enumeration videoSignalStatus(2) audioChannelTable(5) – audioChannelEntry(1) [audioChannelId] — Unsigned32 audioChannelId(1) Enumeration audioSignalStatus(2) casingTable(6) casingEntry(1) [casingId] – Unsigned32 casingld(1) – DisplayString casingName(2) Enumeration casingStatus(3) storageTable(8) storageEntry(1) [storageId] Unsigned32 storageld(1) DisplayString storageName(2) - Enumeration storageDisruptionDetected(3) videoNotifications(2) videoNotificationPrefix(0) alarmNew(1) [alarmID,alarmName,alarmText] alarmCleared(2) [alarmID,alarmName,alarmText] — alarmSingle(3) [alarmID,alarmName,alarmText] Unsigned32 alarmID(1) DisplayString alarmName(2) DisplayString alarmText(3) videoConformance(3) videoGroups(1) - videoObjectGroup(1) videoNotificationGroup(2) videoCompliances(2) videoCompliance(1) axisAgents(16) axisVideoCapabilities(1)

Axis Video MIB Tree

Import Axis Video MIB files using iReasoning MIB Browser

The screenshots below illustrates how to import Axis Video MIB on page 112 files into the iReasoning MIB Browser.

Network protocols

Concession 100 fear one					
Reasoning MB Browser File Edit Operations Tools Bookmarks Help					
Load MIBs Cal+L • Advanced. OID 1.3					 Operations: Get Next
UnLoad MBs MB Modules	Result Table				
Open Sention ab-2		Name/OID		Value	Type IP.Port 🥥
Sare Session					8
Exet					2
					بی ب م
					\$
Name					
Nane OID MIB					
MB Souther					
Syntex Access					
Status DefVal					
Indexes					
🚯 🥝 🗒 🗕 🜍 🔤 🚳					⁵⁷ - 4e 56 10 2021-11-09
· Second Million					C_ 1.4 cm
Record Mill brane					0 0 0
					• Operations (Get Num •) 🏟 Go
Lok k 🔒 M8 - O 🕽 🕨 🔤 -	Result Table				• Operations Get Next • 🕐 Go
	Result Table	HanarOID	I	Value	• Operations Get Next • 🕐 Go
	Result Table	Manarotid	I	Value	• Operations Get Next • 🕐 Go
	Rendi Table	Mean COD		Value	• Operations Get Next • 🕐 Go
	Prodi Tale	Mener OD		Value	• Operations Get Next • 🕐 Go
	Result Table	Nexe(VD)	I	Value	• Operations Get Next • 🕐 Go
	Rendt Table	Heast OID		Value	
Lower Conceptor	Rendi Table	Yearst		Valer	• Operations Get Next • 🕐 Go
Lower Conceptor	Renti Table	Nexe(VD)		Value	• Operations Get Next • 🕐 Go
	Rendi Table	NewOD		Value	• Operations Get Next • 🕐 Go
Lower Conceptor	Rendi Table	Yeane CED		Value	• Operations Get Next • 🕐 Go
Lower Conceptor	Result Table	Nexe(VD)		Value	• Operations Get Next • 🕐 Go
Lower Conceptor	Pendi Tale	Hear OD		Value	• Operations Get Next • 🕐 Go
Lower Conceptor	Renali Table	Yeane CED		Valar	• Operations Get Next • 🕐 Go
Lower Conceptor	Rendi Take	Neter(VD)		Value	• Operations Get Next • 🕐 Go
Lower Conceptor	Prodi Tale	MenerOID		Valer	• Operations Get Next • 🕐 Go
Lower Conceptor	Renal Table	Nexe#CED		Valar	• Operations Get Next • 🕐 Go
Lower Conceptor	Rendi Table	MenrOD		Value	• Operations Get Next • 🕐 Go
Lower Conceptor	Real Tale	YeareOD		Valer	• Operations Get Next • 🕐 Go
Lower Conceptor	Renali Table	Neue/OD		Value	• Operations Get Next • 🕐 Go
Lower Conceptor	Peroli Tale	Hear(OD		Value	• Operations Get Next • 🕐 Go
Lower Conceptor	Real Tale	YeartOD		Value	• Operations Get Next • 🕐 Go
Careford Control (Careford) Control (Careford) Careford Carefo	Rendi Take	MenrOD		Value	• Operations Get Next • 🕐 Go
Careford Control (Careford) Control (Careford) Careford Carefo	Proli Tale	Mene OID		Valer	• Operations Get Next • 🕐 Go
Careford Control (Careford) Control (Careford) Careford Carefo	Real Tabe	Yeard OD		Valar	• Operations Get Next • 🕐 Go
Careford Control (Careford) Control (Careford) Careford Carefo	Rendi Table	HenrOD		Valar	• Operations Get Next • 🕐 Go
Careford Control (Careford) Control (Careford) Careford Carefo	Proli Tale	Mene OID		Van	• Operations Get Next • 🕐 Go
Careford Control (Careford) Control (Careford) Careford Carefo	Real Tab	Years CED		Valar	• Operations Get Next • 🕐 Go
	Perdi Tale	NewOD		Value	• Operations Get Next • 🕐 Go
		Mene OD		Vaa	• Operations Get Next • 🕐 Go
	Prod Tale	MentCD		Valar	• Operations Get Next • 🕐 Go
		NewOD		Vale	• Operations Get Next • 🕐 Go
		Year		Vale	• Operations Get Next • 🕐 Go
	Perdi Tale	HearOD		Value	• Operations Get Next • 🕐 Go
Control 2 Million Addressed		MenrOD		Van	• Operations Get Next • 🕐 Go
		Year		Valar	• Operations Get Next • 🕐 Go
		HearOD		Valar	• Operations Get Next • 🕐 Go

SNMP walk using iReasoning MIB Browser

The screenshots below illustrate how to do an SNMP walk on an Axis device. Note that SNMP needs to be enabled.

SNMPv1/2

Network protocols

Edit Operations Tools Bookmarks Help ss. 172.25.151.148 • Advanced. OID: 1.3.6.1			a Orientina (With
# 172.25.151.148 • Advanced OED 1.3.6.1	Result Table		Operations: Walk.
Tree s ogg di d internet	Name/OID	Value	Type IP-P-
nego si anteresti mgrat geirate			
private enterprises			
🕀 🌲 exts			
soducts			
E Judeo	Advanced Properties of SIAMP Agent		
19 🔒 videoObjects 10 🔒 videoNottiications	Address 172.25.151.148		
# 3 videoConformance	Port 161		
	Read Community public		
	Write Community write SNIMP Version 2		
	OTVAL VEDION &		
	Ok Cancel		
istemet 1.3.6.1	î		
ning MB Preser Ar Constants Taols Rockmarks Heb.			
fit Operations Tools Bookmarks Help 172.25.151.148 • Advanced. OID: 1.3.6.14.1.368.4.1.8.1.3.2			
fit Operations Tools Bookmarks Help 172.25.151.148 • Advanced. OID: 13.6.14.1368.4.18.1.3.2 MIBs	Renit Take		Operations: Walk
Correction: Tools: Bookmarks: Help OED 136.14.1368.418.13.2 172.25:151.148 • Advanced. OED 136.14.1368.418.13.2 Office: • Office: • Office: • Office:	Name/OID	0.0 0.0	Operations Walk Type IP-Port
Correction: Tools: Bookmarks: Help OED 136.14.1368.418.13.2 172.25:151.148 • Advanced. OED 136.14.1368.418.13.2 Office: • Office: • Office: • Office:	Name/OED #Specific 1 #Specific 2	0.0	Operation: Wulk Type IP-Port OID 172.25 OID 172.25
de Cyentoma Turbe Bookanako Hitoj 1722215114 • Advanced. [OCD.]136141368418132 MDB Thr ment pende pende pende	Name/OD #Specific 1 #Specific 2 \$K cover dang 0	0.0 0.0 not-forwarding (2)	Operations: Walk Type IP Port OID 172.25 OID 172.25 Innee: 172.75
(k: Operators Tools Bookmando Holp) 172.25 1511.46 • Advanced. ODD 13.614.1368.41.813.2 Other	NumerODD diponds 1 diponds 2 pironestage pironestage pironestage pironestage pironestage pironestage pironestage pironestage	0.0 0.0 not-forwarding (2) 64 2	Coperations Widt Type BParce OD 122.25 OD 122.25 Manager 122.25
ik Operators Tools Boolsmalls Rab 122 S15114 • Advanced. ODD 13.614.1368.418.13.2 The ment sensense sense sense sense sense sense sense se	Name/OD dSpecific 1 dSpecific 2 pSPrever date 0 pSP-instantTL 0 1.3.6.12.14.25.0 1.3.6.12.14.26.0	0.0 0.0 0.6 Fernending (2) 64 2 2 4	 Operations Walk Type IP-Port ODD 172:25 Banger 172:25 Banger 172:25 Banger 172:25 Banger 172:25 Banger 172:25
té Cyenton Touls Bolomarko Hab 17222151191 • Advanced. OCD 136141366418132 Other transmission prontor pron	NumerCOD direction 1 direction 2 vpression 2 vpressin 2 vpression 2	0.0 0.0 not-forwarding (2) 64 2	Cyrrenting: [Vide] Type Di-Peter ODD 172.25 ODD 172.25 Damegre 172.25
ta Cyentom Touls Bodemakh Hab 17222151114 • Advanced. GDD 136141368418132 GDD 136141368418 GDD 136141368418 GDD 136141368418 GDD 136141368418 GDD 136141368418 GDD 136141368418 GDD 1361418418 GDD 1361418418 GDD 1361418418 GDD 1361418 GDD 1361418 GDD 1361418 GDD 1361418 GDD 1361488 GDD 13614888 GDD 1361488888 GDD 1361488888 GDD 136148888	Near/OD dPprefix 1 dPprefix 2 dPprefix 3 dPrefix 40 114121420 114121420 114121420 114121420 114121420 114121420 mapOrDE00 mapOrDE00 mapOrDE00	0.0 0.0 16.0 Forwarding (2) 64 2 64 64 649	Operations [Vid.
is Operators Tools Solomated Tools is Operators Tools Solomated Tools is Operators in the solution of the solu	Near/OD d/profile 1 d/profile 2	0 0 0 0 0 0 0 64 2 4 4 4 4 90 40 5	Operations Web Type 19 Jun Operations Operations Operation Op
te Operatore Tode Socientifică (DED 136141366418132) CED 122515114 • Advenced. OED 136141366418132 CED 122515140 CED 122515140 CED 122515140 CED 1236141366418132 CED 12361418 CED 12361418 CED 12361418 CED 1236148 CED 123614	NumerCOD dipende 1 dipende 2 pit new role (0 pit new role (0 pit new role (0 13.612.14.25.0 13.612.14.25.0 13.612.04.25.0 mapi-Order 0 mapi-Order 0 mapi-Order 0 mapi-Order 0 mapi-Order 0 mapi-Order 0	0 0 0 0 0 0 0 64 2 4 4 49 6 4 5 5 0 0 0 0 7 3 3 0 0 0 0 0 0 0 0 0 0 0 0 0	Cyperations [Vide] Type DPvent OD 712 25 OD 712 25 Danger
i Cynnow Todi Sodawid Tab i Cynnow Todi Sodawid Tab I 22 515114 Advaced. ODD 13 6141360418132 D o o o o o o o o o o o o	NumerCOD different 1 different 2 pir www.dag 0 spir dearter 10 13.61.21.42.0 13.61.21.42.0 13.61.21.42.0 map/Dath 0 map/Dath 0 map/Dath 0 map/Dath 70*man 0 map/Dath 70*man 0 map/Dath 70*man 0 map/Dath 70	0 0 00 molecular (2) 64 0 2	Cyrrations Watk Type Drawn Dia Type Dia Dia Type Dia Dia Type Dia Dia Type Dia Dia Dia Type Dia Dia
i Cynnow Todi Sodawid Tab i Cynnow Todi Sodawid Tab I 22 515114 Advaced. ODD 13 6141360418132 D o o o o o o o o o o o o	NeuroCOD dipends 1 dipends 2 splowerdug 0 plotairTL 0 134131420 134131420 mapQuBMCProst0 mapQuBMCProst0 mapQuBMCProst0 mapQuBMCProst0 mapQuBMCProst0 mapQuBMCProst0 mapQuBMCProst0 mapQuBMCPLand	0 0 0.0 0.0 Forwarding (2) 64 64 64 65 65 75 75 75 75 75 75 75 75 75 7	Type 12 June 000 172 55 1000
© Cynethode Toble Bookanada Help T22 553114 ▲ Advanced. ODD 136141364418132 T25 551144 ▲ T25 551144 T25 551144 ▲ T25 551144 T25 55114	Name/OD dipends 1 dipends 2 ipPowordug 0 ipOntarTT.0 13.612.14.25.0 13.612.14.25.0 mapData for results mapDatafore for results	00 00 00 externeting (2) 64 64 64 65 66 67 76 76 76 76 76 76 76 76 76 76 76	Type ID-Inter 000 172.55 0000 172.55 00000 172.55 000000 172.55 000000 172.55 000000 172.55 0000000 172.55 00000000 172.55 00000000 172.55 00000000 172.55 000000000 172.55 000000000 172.55 0000000000000 172.55 000000000000000000000000000000000000
i Cynnow Todi Sodawid Tab i Cynnow Todi Sodawid Tab I 22 515114 Advaced. ODD 13 6141360418132 D o o o o o o o o o o o o	NearODD dipend:1 dipend:2 up forwarding 0 umup/OBTR:0	00 00 00 conversing (2) 64 00 00 00 00 00 00 00 00 00 00 00 00 00	Operations With Part 100 17.35 000 17.35 000 17.25 000 17.25 000 17.25 000 17.25 000 17.25 000 17.25 000 17.25 0000 17.25 0000 17.25 00000 17.25 00000 17.25 000000 17.25 000000 17.25 000000 17.25 000000 17.25 000000 17.25 000000 17.25 000000 17.25 000000 17.25 000000 17.25 000000 17.25 000000 17.25 0000000 17.25 000000 17.25 0000000 17.25 000000 17.25 0000000 17.25 000000 17.25 00000000 17.25 000000 17.25 0000000000000 17.25 0000000 17.25 0000000000000000000000000000000
i Cynnow Todi Sodawid Tab i Cynnow Todi Sodawid Tab I 22 515114 Advaced. ODD 13 6141360418132 D o o o o o o o o o o o o	NumeCOD dipend:1 dipend:2 pirowardug 0 mapOddiration mapOddiration 0	00 00 00 externeting (2) 64 64 64 65 66 67 76 76 76 76 76 76 76 76 76 76 76	Cyrentine Web: Type Difference Differe
i Cynnow Todi Sodawid Tab i Cynnow Todi Sodawid Tab I 22 515114 Advaced. ODD 13 6141360418132 D o o o o o o o o o o o o	NumerCOD different 1 different 2 pir www.drag 0 pir dearth 2 pir www.drag 0 pir dearth 2 pir dearth 2 <td>00 00 00 conversing (2) 04 04 05 05 05 05 04 05 05 05 05 05 05 05 05 05 05 05 05 05</td> <td>• Operations With • • • • • • • • • • • • • • • • • • •</td>	00 00 00 conversing (2) 04 04 05 05 05 05 04 05 05 05 05 05 05 05 05 05 05 05 05 05	• Operations With • • • • • • • • • • • • • • • • • • •
i Cynnow Todi Sodawid Tab i Cynnow Todi Sodawid Tab I 22 515114 Advaced. ODD 13 6141360418132 D o o o o o o o o o o o o	NumerCOD dipend:1 dipend:2 updread:2 up	0 0.0 0.0 0.0 0.0 0.0 0.1 0.2 0.3 0.4 0.4 0.4 0.7 0.1 0.1 0.2 0.3 0.4	Type IP Int 000 172 55 1000
© Cynethode Toble Bookanada Help T22 553114 ▲ Advanced. ODD 136141364418132 T25 551144 ▲ T25 551144 T25 551144 ▲ T25 551144 T25 55114	Name/COD dipende 1 dipende 2 up? over dag 0 up? dipende 2 up? over dag 0 up? dipende 2 up? over dag 0 up? dipende 2	00 00 00 conversing (2) 04 04 05 05 05 05 04 05 05 05 05 05 05 05 05 05 05 05 05 05	Type ID-Integration 000 172.52 0000 172.52 Design 172.52 Design 172.52 Design 172.52 Design 172.52 Design 172.52 Outst22 172.52
i Cynnow Todi Sodawid Tab i Cynnow Todi Sodawid Tab I 22 515114 Advaced. ODD 13 6141360418132 D o o o o o o o o o o o o	Numericity Africanic 1 Africanic 2 Africani	00 00 00 conversing (2) 04 04 05 05 05 05 04 05 05 05 05 05 05 05 05 05 05 05 05 05	Operation West In red 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 000 012.5 0000 012.5 000<
i Cynnow Todi Sodawid Tab i Cynnow Todi Sodawid Tab I 22 515114 Advaced. ODD 13 6141360418132 D o o o o o o o o o o o o	NeurOD dipend:1 dipend:2 update:1	00 00 00 conversing (2) 04 04 05 05 05 05 04 05 05 05 05 05 05 05 05 05 05 05 05 05	Operation Mode Description 000 012 01 </td
© Cynethode Toble Bookanada Help T22 553114 ▲ Advanced. ODD 136141364418132 T25 551144 ▲ T25 551144 T25 551144 ▲ T25 551144 T25 55114	Mean-COD dipend:1 dipend:2 spl-owerdag 0 spl-distrift.0 1.14.12.42.0 impol/dipend impol/dipend <	00 00 00 conversing (2) 04 04 05 05 05 05 04 05 05 05 05 05 05 05 05 05 05 05 05 05	Operation With 1 Processor Processor 000 17.23 Processor
i Cynnow Todi Sodawid Tab i Cynnow Todi Sodawid Tab I 22 515114 Advaced. ODD 13 6141360418132 D o o o o o o o o o o o o	Numericity Africania Africania <t< td=""><td>0 0.0 <t< td=""><td>• Operations With:</td></t<></td></t<>	0 0.0 <t< td=""><td>• Operations With:</td></t<>	• Operations With:
te Operatore Tode Socientifică (DED 136141366418132) CED 122515114 • Advenced. OED 136141366418132 CED 122515140 CED 122515140 CED 122515140 CED 1236141366418132 CED 12361418 CED 12361418 CED 12361418 CED 1236148 CED 123614	NumerCOD dipend:1 dipend:2 ipProvedug 0 ipCreduit1 ipProvedug 0 ipCreduit1 ipProvedug 0 ipCreduit1 ipProvedug 0	0 0.0 <t< td=""><td>Operation With 00 72.33 000 72.33 000 72.33 000 72.33 000 72.33 000 72.33 000 72.33 000 72.33 0000 72.33 00000 72.33 00000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 0000000 72.33 00000000 72.33 0</td></t<>	Operation With 00 72.33 000 72.33 000 72.33 000 72.33 000 72.33 000 72.33 000 72.33 000 72.33 0000 72.33 00000 72.33 00000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 000000 72.33 0000000 72.33 00000000 72.33 0
i Cynnow Todi Sodawid Tab i Cynnow Todi Sodawid Tab I 22 515114 Advaced. ODD 13 6141360418132 D o o o o o o o o o o o o	Mean-OID dipend: 1 dipend: 2 ipPowordug 0 impowordug 0 </td <td>0 0.0 <t< td=""><td>Operation With 100 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 0000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 000000 17.35 000000 17.35 000000 17.35 000000 17.35 000000 17.35 000000 17.35 000000 17.35 0000000</td></t<></td>	0 0.0 <t< td=""><td>Operation With 100 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 0000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 000000 17.35 000000 17.35 000000 17.35 000000 17.35 000000 17.35 000000 17.35 000000 17.35 0000000</td></t<>	Operation With 100 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 0000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 000000 17.35 000000 17.35 000000 17.35 000000 17.35 000000 17.35 000000 17.35 000000 17.35 0000000
i Cynnow Todi Sodawid Tab i Cynnow Todi Sodawid Tab I 22 515114 Advaced. ODD 13 6141360418132 D o o o o o o o o o o o o	Mean-COD dipend:1 dipend:2 update:1 update:2 update:2 <t< td=""><td>0 0.0 0.0 0.0 0.0 0.0 0.0 0.1 <t< td=""><td>• Operations With:</td></t<></td></t<>	0 0.0 0.0 0.0 0.0 0.0 0.0 0.1 <t< td=""><td>• Operations With:</td></t<>	• Operations With:
te Operatore Tode Socientifică (DED 136141366418132) CED 122515114 • Advenced. OED 136141366418132 CED 122515140 CED 122515140 CED 122515140 CED 1236141366418132 CED 12361418 CED 12361418 CED 12361418 CED 1236148 CED 123614	Mean-COD dipend:1 dipend:2 dipend:2 dipend:2 </td <td>0 0.0 0.0 0.0 0.0 0.0 0.1 <t< td=""><td>Typ DPstr 000 172.55 barger 172.55 barger 172.55 barger 172.55 barger 172.55 barger 172.55 Control 2 172.55 Control 2</td></t<></td>	0 0.0 0.0 0.0 0.0 0.0 0.1 <t< td=""><td>Typ DPstr 000 172.55 barger 172.55 barger 172.55 barger 172.55 barger 172.55 barger 172.55 Control 2 172.55 Control 2</td></t<>	Typ DPstr 000 172.55 barger 172.55 barger 172.55 barger 172.55 barger 172.55 barger 172.55 Control 2
te Operatore Tode Socientifică (DED 136141366418132) CED 122515114 • Advenced. OED 136141366418132 CED 122515140 CED 122515140 CED 122515140 CED 1236141366418132 CED 12361418 CED 12361418 CED 12361418 CED 1236148 CED 123614	NumeCOD dipend:1 dipend:2 pirowardug 0 mapOddiration mapOddiration <td< td=""><td>θ θ b</td><td>Operation With 00 00 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000</td></td<>	θ θ b	Operation With 00 00 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000 02.03 000
te Operatore Tode Socientifică (DED 136141366418132) CED 122515114 • Advenced. OED 136141366418132 CED 122515140 CED 122515140 CED 122515140 CED 1236141366418132 CED 12361418 CED 12361418 CED 12361418 CED 1236148 CED 123614	Mean-COD dipend: 1 dipend: 2	00 00 00 00 00 00 01 02 03 04 05 05 01 02 03 04 05 04 05 04 05 04 05 04 05	Operation Mode 000 17.23 000 17.23 000 17.23 000 17.23 000 17.23 000 17.23 0000 17.23 0000 17.23 0000 17.23 0000 17.23 00000 <t< td=""></t<>
is Contract. Tools Booleands Hab T222515114 • Advanced. OCD 13.614.1364.418.132 Without and the second se	Mass/CID dipend:1 dipend:2 ipPowerkeg 0 impoliation impoliat	00 00 00 00 00 00 01 02 03 04 05 05 01 02 03 04 05 04 05 04 05 04 05 04 05	Operation With 100 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 000 17.35 0000 17.35 0000 17.35 0000 17.35 0000 17.35 0000 17.35 0000 17.35 0000 17.35 0000 17.35 0000 17.35 0000 17.35 0000 17.35 0000 17.35 0000 17.35 0000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 00000 17.35 <
ta Cyentom Touls Bodemakh Hab 17222151114 • Advanced. GDD 136141368418132 GDD 136141368418 GDD 136141368418 GDD 136141368418 GDD 136141368418 GDD 136141368418 GDD 136141368418 GDD 1361418418 GDD 1361418418 GDD 1361418418 GDD 1361418 GDD 1361418 GDD 1361418 GDD 1361418 GDD 1361488 GDD 13614888 GDD 13614888 GDD	Mean-OID dipend:1 dipend:2 gipend:2 gipend:2 <t< td=""><td>00 00 00 00 00 00 00 01 02 03 04 05 05 01 02 03 04 05 04 05 04 05 04 05</td><td>Operation With 100 17.25 000 17.25 000 17.25 000 17.25 000 17.25 000 17.25 000 17.25 000 17.25 000 17.25 0000 17.25 0000 17.25 000000 1</td></t<>	00 00 00 00 00 00 00 01 02 03 04 05 05 01 02 03 04 05 04 05 04 05 04 05	Operation With 100 17.25 000 17.25 000 17.25 000 17.25 000 17.25 000 17.25 000 17.25 000 17.25 000 17.25 0000 17.25 0000 17.25 000000 1
<pre>it Cyrent Trub Booleands Unity it Cyrent Trub Booleands Unity it Cyrent Cy</pre>	Mean/OD dipend:1 dipend:2 dipend:1 dipend:2 gipend:2 gipend:2 <td< td=""><td>00 00 00 00 00 00 00 01</td><td>Operation Mode Disc 000 12.33 000 12.33 000 12.33 000 12.33 000 12.33 000 12.33 0000 <</td></td<>	00 00 00 00 00 00 00 01	Operation Mode Disc 000 12.33 000 12.33 000 12.33 000 12.33 000 12.33 000 12.33 0000 <
State Interest	Mean/OD dipend:1 dipend:2 dipend:2 <td< td=""><td>00 00 00 00 00 00 01 02 03 04 05 05 01 02 03 04 05 04 05 04 05 04 05 04 05</td><td>• Operation With</td></td<>	00 00 00 00 00 00 01 02 03 04 05 05 01 02 03 04 05 04 05 04 05 04 05 04 05	• Operation With
KRT: To To T	Mean-OD dipend: 1 dipend: 2 maph2nt/date: 0	00 00 00 00 00 00 00 01 02 03	• Operation With
State Interest	Mass/CID dipend: 1 dipend: 2	00 00 00 00 00 00 01 02 03 04 05 05 01 02 03 04 05 04 05 04 05 04 05 04 05	Operation Math 00 19.54 00 19.52
site Contractor The Societarial State VIT Adversed. CDD 13.6.1.4.1.366.4.1.8.16.2 With Societarial State With Societaria Wit	Mass/CID dipute 1 dipute 2 gipute 2 <t< td=""><td>00 00 00 00 00 00 00 01 01 01 01 02 03 01 01 01 01 01 02 03 04 05 04 05 05 05 04 05</td><td>Operation Math 00 19.54 00 19.52</td></t<>	00 00 00 00 00 00 00 01 01 01 01 02 03 01 01 01 01 01 02 03 04 05 04 05 05 05 04 05	Operation Math 00 19.54 00 19.52
it Cyrentor Trols Booleands Italy (T22315114) Advanced. (CD) Italian	Mean/OD dipend:1 dipend:2 dipend:1 dipend:1 dipend:2 gipend:2 gipend:2 gipend:2 gipend:2 gipend:2 gipend:2 gipend:2 gipend:2 gipend:2 maphaff maphaff <t< td=""><td>00 00 00 00 00 00 01 02 03 04 05 05 01 02 03 04 05 04 05 04 05 04 05</td><td>• Operation With</td></t<>	00 00 00 00 00 00 01 02 03 04 05 05 01 02 03 04 05 04 05 04 05 04 05	• Operation With

SNMPv3

Network protocols

Edit Operations Tools Bookmarks Help deress + 172.25.151.148 Advanced OID: 1.3.6.1	1		 Operations: Walk
MIBs	Result Table Name OID	Value	Type IP.Port
o.org.dod.internet mgrat			
private sampV2			
	& Advanced Progeties of SIMP Agent X		
	Address 172.25.151.148 Port 161		
	Read Community		
	SNMP Version 3		
	SNMP version 5		
	USM User inhial Security Level auth, priv		
	Security Level anth, prov Anth Algorithm SHA		
	Auth Password		
	Privacy Algorithm AES Privacy Password *******		
	Context Name		
	Engine ID 0x 80 00 1F 88 03 AC CC 8E CA 32 5D		
	Localized Auth Key 0x 6E 13 10 43 7B 42 F6 66 13 1B E4 0E 31 29 8F 28 A5		
	Localized Priv Key (0x 6E 13 10 43 7B 42 F6 66 13 1B E4 0E 31 29 8F 28 AS		
	Ok Cancel		
interact			
1.3.6.1			
e 😸 💩 🗰 💁			
Ade larment Ade larment Amount	Result Table		 σ Operation: Walk
Image: Second	Nume OID Nume OID 13.6.1.6.3.16.1.5.2.1.5.4.98.97.115.101.8.1.3.6.1.2.1.88.1 4	Valee	Operations: Walk Operations: Walk Type IPPort Integer 172.25.1.
Image: Second	Name OID Name OID 1.3.6.1.6.3.5.1.5.4.9.897.115.101.8.1.3.6.1.2.1.88.1 4 1.3.6.1.6.1.6.1.5.2.1.5.5.997.100.1026.95.1.0 4	Valer	Operation: Walt: Operation: Walt: Type IP-Port Integer 1722.5. Integer 1722.5.
Image: Second	Num OD Num OD 13561615151690711010813612381 4 13561615155997108108951 4 135615155997108108951 4 135615155997108108951 4	Valer	Operation: Wait: Operation: Wait: Type UPPert Integer 172241. Integer 172241. Integer 172251. Integer 172251.
e image: second se	Num Num <od< th=""> 13.64.65.64.61.44.64.60.7116.016.61.06.21.84.1 4 13.64.65.61.61.21.65.97.100.1008.61.1 4 13.64.65.91.61.52.15.85.97.100.1008.61.1 4 13.64.65.91.65.91.65.97.100.1008.61.2 4 13.64.65.91.65.91.65.97.100.1009.61.1 4 13.64.65.91.65.97.100.1009.01.0 4</od<>	Valer	- 5 • Operations Walk • 6 Type IP-944 Integer 172.24.1 Integer 172.24.1 Integer 172.24.1 Integer 172.24.1 Integer 172.24.1 Integer 172.24.1 Integer 172.24.1 Integer 172.24.1 Integer 172.24.1 Integer 172.24.1
e image: second se	Num Num Old 1.5.4.6.5.16.1.5.2.1.5.4.98.97.115.101.8.1.3.6.1.2.1.8.1 4 1.5.6.6.5.16.1.5.2.1.5.99.77.010.100.01.6 4 1.5.6.6.5.16.5.2.1.5.99.77.010.100.01.6 4 1.5.6.6.5.16.5.2.1.6.99.11.01.11.00.01.91.0 4 1.5.6.6.5.16.5.2.1.6.99.11.01.11.00.01.91.0 4 1.5.6.6.5.6.5.5.15.6.99.11.01.11.00.01.90.12 4 1.5.6.6.5.6.5.5.15.91.11.01.00.09.01.2 4 1.5.6.6.5.6.5.5.15.91.11.01.00.09.01.2 4	Valer	- 0 • Operations Walk • 1 Type PP-ext larger 172:241. larger 172:241.
e image: second se	Num<70D Num<70D 1.3.6.6.3.16.1.5.1.2.4.498.97.115.101.8.1.3.6.1.2.1.88.1 4 1.3.6.6.3.16.1.5.2.1.4.498.97.110.100.96.1.0 4 1.3.6.6.3.16.1.5.2.1.4.5.2.1.458.1 4 1.3.6.6.3.16.1.5.2.1.4.6.7 11.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1	Valer	- 0
Image: Second	Num CDD Num CDD 1.5.6.1.5.1.6.1.5.2.1.5.4.98.971151018.1.3.6.1.2.1.88.1 4 1.3.6.6.1.6.1.5.2.1.5.9.9771010108.91.0 4 1.3.6.6.1.6.1.5.2.1.5.9.977101010891.0 4 1.3.6.6.1.6.1.6.2.1.5.9.1.5.997101010891.0 4 1.3.6.6.1.6.1.6.1.5.1.5.9.97101010891.0 4 1.3.6.6.1.6.1.6.1.5.1.5.9.97101010109.91.0 4 1.3.6.6.1.6.1.6.1.5.1.6.98110111110109.951.0 4 1.3.6.6.1.6.1.5.1.5.1.6.98110111110109.951.0 4 1.3.6.6.1.6.1.5.5.1.6.98110111110109.951.0 4 1.3.6.6.1.6.1.5.5.1.6.98110111110109.951.0 4 1.3.6.6.1.6.1.5.5.1.6.98110111110109.951.0 4 1.3.6.6.1.6.1.5.5.1.6.1.6.911101010110119.1.5.1.6.1.2.1.4.31 4 1.3.6.6.1.6.5.5.1.6.1.6.1.81110100190119.1.5.4.2.2.4.33 4 1.3.6.6.1.6.5.5.1.6.1.6.1.811.1.0.100190113.1.5.1.6.2.1.4.31 4	Valer	 Operation: Wak Type PPert langer 172.24.1. langer 172.24.1.
Image: Second	Num CBD Num CBD 1.5.6.5.3.1.5.2.1.5.4.98.971151018.1.5.6.12.18.81 4 1.3.6.6.3.16.1.5.2.1.5.99.071010109511 4 1.3.6.6.3.16.5.2.1.5.99.071010109511 4 1.3.6.6.3.16.5.2.1.5.99.071010109512 4 1.3.6.6.3.16.5.2.1.5.99.071010109513 4 1.3.6.6.3.16.5.2.1.5.99.071011101019513 4 1.3.6.6.3.16.5.2.1.5.99.110111101019513 4 1.3.6.6.3.16.5.2.1.5.99.110111101019513 4 1.3.6.6.3.16.5.2.1.5.99.110111101019513 4 1.3.6.6.3.16.5.2.1.5.91.1111101019513 4 1.3.6.6.3.16.5.2.1.6.1111101019513 4 1.3.6.6.3.16.5.2.1.6.1111101019513 4 1.3.6.6.3.16.5.2.1.6.11111010195119101 4 1.3.6.6.3.16.5.2.1.6.11111010195119101 4 1.3.6.6.3.16.5.2.1.6.11111010195119101 4 1.3.6.6.3.16.5.5.2.1.6.111101019101191191.3.6.2.1.4.23 4 1.3.6.6.3.16.5.5.2.1.6.1111101019101191131.3.6.2.1.4.23 4 1.3.6.6.3.16.5.5.2.1.6.11111101019101191.3.6.2.1.4.23 4 1.3.6.6.3.16.5.5.2.1.6.11111101019101101191.3.6.2.1.4.23 4 1.3.6.6.3.16.5.5.2.1.6.11111110101910111111111111111111111	Value	 Operations: Walk Type Type<
Image: Second	Nume COD Nume COD 13.8.6.8.16.8.16.8.16.8.16.8.16.8.17.8.8.1 4 13.8.6.8.16.8.16.8.16.8.17.8.8.17.8.17.8.1	Valer	 Operations: Walk Type Type<
Image: Second	Num Num <td>Valer</td> <td>- 0 • Opensione Walk • Opensione Walk • Type • PPen sampe • 122.41. barger • 122.</td>	Valer	- 0 • Opensione Walk • Opensione Walk • Type • PPen sampe • 122.41. barger • 122.
Image: Second	Num Num <td>Vale</td> <td>- 0 • Opension: Walk • Opension: Walk • Tape • Piper • 222.1 • Integer • 122.2 • Integer • 122.2 • Integer • Integer • Integer • Integer • Integer • Integer • Intege</td>	Vale	- 0 • Opension: Walk • Opension: Walk • Tape • Piper • 222.1 • Integer • 122.2 • Integer • 122.2 • Integer • Integer • Integer • Integer • Integer • Integer • Intege
Image: Second	Num Num <td>Valer</td> <td>- 0 • Operations Walk • Operations • Operations • Operations • Operations • Operations • Operations • Operations • Operations • Operations • Operations • Operations • Operations • Operations • Op</td>	Valer	- 0 • Operations Walk • Operations • Operations • Operations • Operations • Operations • Operations • Operations • Operations • Operations • Operations • Operations • Operations • Operations • Op
Image: Second	Num Num Old 13.6.4.5.16.4.5.17.4.6.8.97115.101.8.1.3.6.12.1.8.1 4 13.6.4.5.16.4.5.2.1.4.6.8.97115.101.8.1.3.6.12.1.8.1 4 13.6.4.5.16.4.5.2.1.4.6.8.97115.101.8.1.5.1.2.1.8.1 4 13.6.4.5.16.7.5.1.6.9.97118.101.9.0.971.0 4 13.6.4.5.16.5.2.1.6.9.97118.1010.971.0 4 13.6.4.5.16.5.2.1.6.9.110.111.100.0971.0 4 13.6.4.5.16.5.2.1.6.9.110.111.100.0971.0 4 13.6.4.5.16.5.2.1.6.9.110.111.100.0971.0 4 13.6.4.5.16.5.2.1.6.9.110.111.100.0971.0 4 13.6.4.5.16.5.2.1.6.9.110.111.100.0971.0 4 13.6.4.5.16.5.2.1.6.9.111.101.00.971.0 4 13.6.6.5.16.5.2.1.6.9.111.101.00.971.0 4 13.6.6.6.16.5.2.1.6.4.114.5.11.100.01.101.13.6.12.14.31 4 13.6.6.6.16.5.2.1.6.4.114.5.11.100.01.101.13.6.12.14.31 4 13.6.6.6.16.5.2.1.6.4.114.5.11.100.01.101.13.6.12.14.31 4 13.6.6.6.16.5.2.1.6.4.114.5.11.100.01.01.13.6.12.14.31 4 13.6.6.6.16.5.2.1.6.4.114.5.11.100.01.01.13.6.12.14.31 4 13.6.6.6.16.5.2.1.6.4.114.5.11.100.01.01.01.13.6.12.14.31 4 13.6.6.16.5.5.1.5.6.114.5.11.100.01.01.01.13.6.12.14.31 4	Vas	- 0 • Operations Walk • • Dependence Walk • • Operations Walk • • Operations Walk • • • • • • • • • • • •
Image: Second	Num Num <td>Valer</td> <td> Operations Walk Type PPert Integra 122241. Integra 12241.</td>	Valer	 Operations Walk Type PPert Integra 122241. Integra 12241.
Image: Second	Num Num <td>Vater</td> <td>- 0 • Opension: Walk • Type PPen samper 12:24.1 anger 12:24.1</td>	Vater	- 0 • Opension: Walk • Type PPen samper 12:24.1 anger 12:24.1
Image: Second	Num Num Num 1.5.4.5.5.1.5.1.5.4.8.9711101105.1.5.6.1.1.8.1 4 1.5.4.6.5.1.5.1.5.9.9711001095.1.1 4 1.5.4.6.5.1.5.1.5.9.9711001095.1.1 4 1.5.4.6.5.1.6.5.1.5.9.9711001095.1.1 4 1.5.4.6.5.1.6.5.1.5.9.9711001095.1.1 4 1.5.4.6.5.1.6.5.2.1.5.99710010095.1.0 4 1.5.4.6.5.1.6.5.2.1.5.99710010095.1.0 4 1.5.4.6.5.1.6.5.2.1.5.99710010095.1.0 4 1.5.4.6.5.1.6.5.2.1.5.99710010095.1.0 4 1.5.4.6.5.1.6.5.2.1.5.991101111001095111 4 1.5.4.6.5.1.6.5.2.1.5.91110101010910111 4 1.5.4.6.5.1.6.5.2.1.5.9111010101010111.1 4 1.5.4.6.5.1.6.5.2.1.5.91110101010111.1 4 1.5.4.6.5.1.6.5.2.1.5.91110101010111.1 4 1.5.4.6.5.1.6.5.2.1.5.9111011010101111011.3.1.5.3.2.1.4.2.2 4 1.5.4.6.5.1.6.5.2.1.5.1.5.1.5.1.5.1.5.1.5.1.5.1.5.1.5	Valer	 Opentions Wak Type PPont Marger Type PPont Marger Type PPont Marger Type PPont Marger Type Provide Marger Type Network Network<
Image: Second	Num Num <td>Valer</td> <td>- 9 • Operations Walk • Operations • Oper</td>	Valer	- 9 • Operations Walk • Operations • Oper
e image: second se	Num Num <td>Vate</td> <td>− 0 • Openform Wait • image 722.81. • image 722.81.<</td>	Vate	− 0 • Openform Wait • image 722.81. • image 722.81.<
e imp M8 Revue 8 Operation Tools Rockmarks Help: xx -(12.25 151144) xx	Num Num Num 113.64.51.05.12.14.489.71110103.11.61.21.181.1 4 13.64.61.05.12.14.489.7110103.11.61.21.181.1 4 13.64.61.05.12.14.59.97.10010095.11 4 13.64.61.05.12.14.59.97.10010095.11 4 13.64.61.05.12.14.69.70.1011001095.10 4 13.64.61.05.21.14.69.101111001095.10 4 13.64.61.05.21.14.69.101111001095.10 4 13.64.61.05.21.14.69.101111001095.10 4 13.64.61.05.21.14.69.101111001095.11 4 13.64.61.05.21.54.11.55.11.05.01.05.11.61.14.14.21.14.11 4 13.64.61.05.21.54.11.55.11.05.01.05.11.61.14.14.21.14.11 4 13.64.61.05.21.54.11.55.11.05.01.05.11.61.14.14.21.14.11 4 13.64.61.05.21.54.11.55.11.05.01.05.11.61.21.4.22.14.12 4 13.64.61.05.51.54.11.55.11.05.01.05.11.61.21.4.23.14.22.14.12 4 13.64.61.05.51.54.11.05.11.05.01.01.15.61.21.4.23.14.22.14.12 4 13.64.61.05.51.54.11.05.11.05.01.01.05.11.61.21.4.23.14.22.14.14 4 13.64.61.05.51.54.11.05.11.05.01.01.05.11.61.21.61.23.14.23.14.23.14.23.14.24.14.24.24.24.24.24.24.24.24.24.24.24.24.24	Vair	Opentione Wait Type PPentione Wait Type PPentint T
Image: Second	Num Num <td>Valer</td> <td>- σ • Opension: Wak • Type Per issue • Opension: Wak • Type Per issue • Type Per • Type Per</td>	Valer	- σ • Opension: Wak • Type Per issue • Opension: Wak • Type Per issue • Type Per
e image: second se	Nume OB Nume OB 1354.63.16.21.44.89.79.11.01.01.21.62.21.81.1 4 1354.63.16.21.44.89.79.11.01.01.21.62.21.81.1 4 1354.63.16.21.44.89.79.11.01.01.05.91.12 4 1354.63.16.21.44.89.79.11.01.02.09.11.2 4 1354.63.16.21.44.89.79.11.01.02.09.11.2 4 1354.63.16.21.45.93.14.89.10.01.01.09.11.2 4 1354.63.16.21.45.91.11.01.00.09.11.2 4 1354.63.16.21.45.91.11.01.00.09.11.2 4 1354.63.16.21.45.91.11.01.00.09.11.2 4 1354.63.16.52.14.89.10.01.11.00.09.11.2 4 1354.63.16.52.14.69.10.01.11.00.09.11.2 4 1354.63.16.52.14.69.10.01.11.00.13.154.12.14.20 4 1354.63.16.52.14.61.11.01.00.09.11.01.13.42.12.14.20 4 1354.63.15.52.14.61.11.01.00.09.10.01.13.62.12.14.20 4 1354.63.15.52.14.61.15.11.00.09.10.01.13.62.12.14.20 4 1354.63.15.52.14.61.11.00.09.10.01.13.62.12.14.20 4 1354.63.15.52.14.61.11.00.09.10.01.13.62.12.14.20 4 1354.63.15.52.14.61.11.00.09.10.01.13.62.12.14.20 4 1354.63.15.52.14.61.11.00.09.10.01.13.62.12.14.20 4 1354.63.15.52.14.61.14.00.01.00.01.00.13.62.12.14.20 <td>Vater</td> <td>- 0 • Opentione Wak • Type PPon for P221 arger 72221 arger 72221</td>	Vater	- 0 • Opentione Wak • Type PPon for P221 arger 72221
Image: Provide State Stat	Num Num Num 13.4.6.2.16.2.1.4.4.97.971.101.0.10.1.6.2.1.8.1 4 13.6.4.2.16.2.1.4.4.97.971.0.101.0.1.6.2.1.8.1 4 13.6.4.2.16.2.1.4.4.97.971.0.101.0.971.1 4 13.6.4.2.16.2.1.4.9.977.101.0.007.971.2 4 13.6.4.2.16.2.1.4.9.977.101.0.007.971.2 4 13.6.4.2.16.2.1.4.9.977.101.0.007.971.2 4 13.6.4.2.16.2.2.1.4.9.971.0.01.0.071.1 4 13.6.6.2.1.6.5.2.1.4.9.971.0.01.0.071.1 4 13.6.6.2.1.6.5.2.1.4.9.971.0.01.0.071.1 4 13.6.6.2.1.6.5.2.1.4.9.971.0.01.0.071.1 4 13.6.6.2.1.6.5.2.1.4.9.971.0.01.0.071.1.0.01.2.1.0.1.0.01.0.01.0	Valer	- 0 • Opension: Wait. • Type: Piece • Opension: Wait. • Opension: Wait. • Opens
Person Person 24 Person 24 Person 24 Person 25 Person 25 Person 25 Person 25 Person 25 Person 26 Person 27 Person 28 Person 29 Person 29 Person 20 13414316152164115116101101101 20 13414316152164115116101101101 20 13414316152164115116101101101 20 13414316152164115116101101101 20 234141 20 234141	Number Number 1.0.4.0.10.1.1.4.4.0.971101100.1.1.5.1.1.1.8.1 4 1.0.4.0.10.1.1.5.1.5.9.971001100.0.1.5.1.1.1.8.1 4 1.0.4.0.10.1.1.5.9.971001100.0.911.0 4 1.0.4.0.10.1.1.5.9.971001100.0.911.0 4 1.0.4.0.10.1.5.1.5.9.971001100.0.911.0 4 1.0.4.0.10.1.5.9.1.5.991101110.00.9911.0 4 1.0.4.0.10.5.9.1.5.911.0.00.9911.0 4 1.0.4.0.10.5.911.5.911.0.00.9911.0 4 1.0.4.0.10.5.911.5.911.0.00.9911.0 4 1.0.4.0.10.5.911.5.911.0.00.9911.0 4 1.0.4.0.10.5.911.5.911.0.00.9911.0 4 1.0.4.0.10.5.911.5.911.0.00.9911.0 4 1.0.4.0.10.5.911.6.911.0.00.9911.0.1.1.4.0.1.0.0 4 1.0.4.0.10.5.911.6.911.0.00.9911.0.1.1.4.0.1.0.0 4 1.0.4.0.10.5.911.6.911.0.00.911.0.0.1.1.4.0.1.0.0 4 1.0.4.0.10.5.911.6.911.0.00.911.0.0.1.1.4.0.0.0 4 1.0.4.0.4.0.5.911.6.911.0.00.911.0.0.1.1.4.0.0.0 4 1.0.4.0.4.0.5.911.6.911.0.00.911.0.0.1.1.4.0.0.0 4 1.0.4.0.4.0.911.5.0.011.0.0.0.0.00.00.00.00.00.00.00.00.0	Vate	- 0 • Opension Wait • Type Prevent integra 72251. integra
Image: Provide State Stat	Nume OD Nume OD Nume OD 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Vas	- 0 Opension: Wak Type Ty
Image: Second comparison of the intervention of t	Number Number Number 13.84.83.18.18.11.84.89.71.81.01.84.23.18.1 4 13.84.83.18.18.12.14.88.97.11.01.01.84.23.18.1 4 13.84.83.18.12.14.88.97.11.01.01.89.11.01 4 13.84.83.18.12.14.88.97.11.01.01.01.91.11 4 13.84.83.18.12.14.88.97.11.01.01.01.91.10 4 13.84.83.18.52.14.88.97.10.01.01.01.01.91.10 4 13.84.83.18.52.14.88.97.10.01.01.01.01.91.10 4 13.84.83.18.52.14.88.91.01.01.01.01.91.11 4 13.84.83.18.52.14.88.91.01.01.01.01.91.13 4 13.84.83.18.52.14.84.91.01.01.01.01.91.13 4 13.84.83.18.52.14.84.18.11.01.00.01.01.01.13.14.14.14.23 4 13.84.83.18.52.14.84.18.11.01.00.01.01.01.13.84.14.14.23 4 13.84.83.18.52.14.84.18.11.01.00.01.01.01.13.84.14.14.23 4 13.84.83.18.52.14.84.11.01.01.00.01.01.01.13.84.14.14.23 4 13.84.83.18.52.14.84.18.11.01.00.01.01.01.13.84.12.14.33 4 13.84.83.18.52.14.84.18.11.01.00.01.01.01.13.84.12.14.33 4 13.84.83.18.52.14.84.18.11.01.00.01.01.01.13.84.12.14.33 4 13.84.83.18.52.14.84.07.01.01.14.14.12.13.11 4 13.84.84.84.97.01.01.14.14.14.23.13.11 4	Vate	– Ø Vjernice Wik Typ PPen Name 722.1. Barge 722.1.
Image: Second	Numerical Numerical 13.64.63.16.21.44.84.97.110.10.11.64.23.84.1 4 13.64.63.16.21.44.84.97.110.10.11.64.23.84.1 4 13.64.63.16.21.44.84.97.110.10.10.16.23.84.1 4 13.64.63.16.21.44.84.97.110.10.10.10.84.1 4 13.64.63.16.21.44.84.97.110.10.10.10.97.10 4 13.64.63.16.23.14.85.71.16.97.10.10.10.97.11 4 13.64.63.16.23.14.87.110.10.10.97.12 4 13.64.63.16.23.14.87.110.10.10.97.12 4 13.64.63.16.23.14.87.110.10.10.97.12 4 13.64.63.16.23.14.87.110.10.10.97.12 4 13.64.63.16.23.14.87.110.10.10.97.12 4 13.64.63.16.23.14.118.11.10.10.97.11.34.12.14.23 4 13.64.63.16.23.14.61.11.10.10.19.13.14.12.14.23 4 13.64.63.16.23.14.61.11.10.10.19.13.14.12.14.23 4 13.64.63.16.23.14.61.11.10.10.19.13.14.12.14.23 4 13.64.63.16.23.14.61.11.10.10.19.13.14.12.14.23 4 13.64.63.16.23.14.61.11.10.10.19.13.14.12.14.23 4 13.64.63.16.23.14.67.11.10.11.16.12.14.23 4 13.64.63.16.23.14.67.11.10.11.16.12.14.23 4 13.64.63.16.23.14.67.11.10.10.15.14.12.14.23 4	Valer	- 0 Opension: Wak Type Ty

Receiving SNMP traps using iReasoning MIB Browser

The screenshots below illustrate how to receive an SNMP trap from an Axis device. Note that SNMP traps need to be enabled.

Network protocols

01111448-Lt Simp x + → C ▲ Inte saker 172,25.151.148/sca/index/html#settings/system/hetwork/smrp					teli t
(15🔺		AXIS P1448-LE Network Camera			1
		SNMP			
		SNMP V1 and V2s T			
		Read community			
		public Write community			
		virta Activala trapa			
		Trap address 172.25.201.105			
		Trap community public			
		Traps			
		Vibre start			
		Link up Authentication failed			
		Save			
image Steam Overlay PTZ Audio Privacy/mask View-area Apps Dystem					
	9 8 X	1 = <mark>-</mark>	i ©	٩	
	Language Date and time Crientation		Events Detectors	Maintenance	
	😵 😰 🦁 109.19 000 Security	Storage I/O pofs M01T	ඒ 🎐 Accessories Plain config		
VERMed there x +					
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		ANSP 148.11 Entronk Convex			lei *
VEI/H441 fore X +		AMS PH48.LT Website Cansera			lei *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Device events MOTT events			lei t
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Device events MOTT events Rules Schedules Recipients Manual triggers			 lei t
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Davice events MOTT events Rules Schedules Recipients Manual triggers			لما *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Device events MOTT events Rules Schedules Recipients Manual triggers Page trap Tomporting Sen Bloop tag message Content of			لما *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Device events MOTT events Rules Schedules Recipients Manual triggers South Tage South Tage Constants [South Tag message South Tage South Tage			لما *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Device events MOTT events Rules Schedules Recipients Manual triggers Page trap Tomporting Sen Bloop tag message Content of			لما *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Cradia Cadia Cadia Cadia Condition Condition Condition Condition Condition Condition Condition			لما *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Everice events: MOTT events: Evers Excludes: Recipients: Manual triggers Every State (Section 2018) Events Every State (Section 2018) Events Candina Events Even			لما *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Device events: MOTT events: Refer Schedules: Receivent: Manual triggers • Stepping Text Diab Yaa nessage • Internet • Internet • Candian • Candian			لما *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Everice events: MOTT events: Evers Excludes: Recipients: Manual triggers Every State (Section 2018) Events Every State (Section 2018) Events Candina Events Even			lei t
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Device events: MOTT events: Refer Schedules: Receivent: Manual triggers • Stepping Text Diab Yaa nessage • Internet • Internet • Candian • Candian			lei t
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Device events: MOTT events: Tutes Schedules Receiverts: Manual biggers • Staff tige Tutes from the Charlenge of the Staff tige Part of the Staff tige Part of the Staff tige of the Staff tige of the Staff tige Part of the Staff tige of			lei *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Device events, MOTT events; Telas Schedules Receivents, Manual biggers • Staff tipe Tela france New Part (See Child Flag message New Part (See Child Flag message Condition on Staff) (See Child Flag message New Part (See New Part			lei *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti					lei *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Caddia Control (2013)			lei *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Cradie Control (2019) Cradie Control (2019) Control			lei *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Caddia Control (2013)			lei *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Cradie Control (2019) Cradie Control (2019) Control			lei *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Cradie Control (2019) Cradie Control (2019) Control			lei *
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Cradie Control (2019) Cradie Control (2019) Control			lei t
MILHAALIbee: x + ⇒ C A be cale 1223/SB148/sub4es/heimetrogutyten/haldowett SSA		Cradie Control (2019) Cradie Control (2019) Control			lei t
METERS/Livers x ↓ → C A los siler 1728/IS148/ac/des/bis/Hetting/system/tool/wenti		Device events: MOTT events: Rules: Schodules: Receivents: Manual Utgerse Subject Data fage Subject			لما *
MITHAAItoo: x + ⇒ C A ba cale 1223/SB148/out-backback/bin/Hittings/system/batkbaventi SSA		Land reader HOT events: Table Schedules Respirate. Manual tragents Subject Schedules Respirate. Manual tragents Subject Schedules Respirate. Schedules Respirate. Subject Schedules Respirate. Schedules Respirate. Subject Schedules Respirate. Schedules Respirate. Subject Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate.	€ ⊗		loli *
MITHAAItoo: x + ⇒ C A ba cale 1223/SB148/out-backback/bin/Hittings/system/batkbaventi SSA	Language Date and time Crientation	Period sector MOT events Ture to head use 2000 Period (sector 2000) Period (sector 2			
MITHAAItoo: x + ⇒ C A ba cale 1223/SB148/out-backback/bin/Hittings/system/batkbaventi SSA	Language Date and time Crientation	Land reader HOT events: Table Schedules Respirate. Manual tragents Subject Schedules Respirate. Manual tragents Subject Schedules Respirate. Schedules Respirate. Subject Schedules Respirate. Schedules Respirate. Subject Schedules Respirate. Schedules Respirate. Subject Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate. Schedules Respirate.	€ ⊗	Maritenance	loli *

Network protocols

Reserving M8 Browser File Edit Operations Tools Bookmanks Help						-	a ×
Address: * Trap Receiver Cat+1 OID, 1.3						 Operations: Get Next 	~ 🏟 Go
SNMP MIBs Trap Sender	Result Table						
MIB Tree Ping inc.org.dod.internet Trace Route		Name/OID			lahae	Type IP	
Add to Watches Ctrl+D							1
Watches Ctrt+O							2
Run Script							
Network Discovery Manage SNMPv3 USM Users							-
Compare Devices							
Port View							
Switch Port Mapper Device Snapshot							
Cisco Device Snapshot							
Log Window							
Options							
Name	_						
Name OID							
MIB Syntax							
Access							
Status DefVal							
Indexes Descr							
Dec							
<u>,</u>							
Parsoning MB Browne File SER Operations Tools Bookanacks Help Advance 000 13							σ ×
File Edit Operations Tools Bookmarks Help Address: * V Advanced OED: 1.3 SNOP Mills	Result Table Trap Receiver -						o × ≤ ♠ Go
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Result Table Trap Receiver × Operations Tools Database						
File Edit Operations Tools Bookmarks Help Address: * V Advanced OED: 1.3 SNOP Mills	Operations Tools Database					Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations Tools Database		Source 172,25,151,148	Time 2021-11-09 105433			
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations Tools Database		Source 172 25 151 148 172 25 151 148 172 25 151 148	Tee 2001-11-09-105433 2002-11-09-105433 2002-11-09-105433		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations Tools Database		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations Tools Database		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations Tools Database		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations Tools Database		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations Tools Database		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations Tools Database		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations Tools Database		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations Tools Database		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNADP MIB: MIB: MIB: MIB: MIB: MIB: MID: MI	Operations Tools Database		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations Tools Database		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations Tools Database		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNADP MIB: MIB: MIB: MIB: MIB: MIB: MID: MI	Operations Tools Database		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: +	Operations Tools Database		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations Tools Database		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: +	Operations Tools Database		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations: Tool: Database ♥ ● ♥ ♥ ♥ ♥ ↑ Decorption: damNew: damNew: 11616311151		172.25.151.148	2021-11-09 10:54:33		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations: Tool: Database Tool: Tool: To	12251914	172.25.151.148	2021-11-09 10:54:33	SNP Version:	Coperations Get Next :	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations: Tool: Database ♥ ● ♥ ♥ ♥ ♥ ↑ Decorption: damNew: damNew: 11616311151	1722581146 13451431133	172 25 1148 172 25 111 48 172 25 111 48	2021-11-09-016433 2021-14-09-016433 2021-14-09-0164-23		Operations: Get Next	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations Tool Dealers		172 25 1148 172 25 111 48 172 25 111 48	2021-11-09-016433 2021-14-09-016433 2021-14-09-0164-23	SNP Version:	Coperations Get Next :	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations: Tool: Database	sysUpTime.0 [TimeTicks] 230 milliseconds (23)	172 25 1148 172 25 111 48 172 25 111 48	2021-11-09-016433 2021-14-09-016433 2021-14-09-0164-23	SNP Version:	Coperations Get Next :	
File Edit Operations Tools Bookmarks Help Address: Advanced OID 1.3 SNAP MID: MDB Tre	Operations: Tool: Database	sysUpTime.0 [TimeTicks] 230 millisecends (23) snrtpTrapOID [OID] 1.3.6.1.6.3.1.1.5.1	172 25 1148 172 25 111 48 172 25 111 48	2021-11-09-016433 2021-14-09-016433 2021-14-09-0164-23	SNP Version:	Coperations Get Next :	
Te Edr Qverden Todi Bokanka Hdp Adhene * Adhened. OD 13 SARTMik * In org dolammet	Opennius Tool Dadens	sysUpTime.0 [TimeTicks] 230 miliseconds (23) sempTrapOID [OID] 1.3.6.1.6.3.1.1.5.1 1.3.6.1.6.3.1.1.4.3.0	172 25 1148 172 25 111 48 172 25 111 48	2021-11-09-016433 2021-14-09-016433 2021-14-09-0164-23	SNP Version:	Coperations Get Next :	
Te Edr Qverden Todi Bokanka Hdp Adhene * Adhened. OD 13 SARTMik * In org dolammet	Operations: Tool: Database	sysUpTime.0 [TimeTicks] 230 millisecends (23) snrtpTrapOID [OID] 1.3.6.1.6.3.1.1.5.1	172 25 1148 172 25 111 48 172 25 111 48	2021-11-09-016433 2021-14-09-016433 2021-14-09-0164-23	SNP Version:	Coperations Get Next :	
Nate: Advaced. OD 13 NAT:: Advaced. OD 13 NaT:: * to org dolament	Operation Tool Deduce Image: Complete Image: Complete Image: Complete Image: Complete Image: Complete Image: Complete Verter: Neare: Complete Verter: Verter: Complete	sysUpTime.0 [TimeTicks] 230 miliseconds (23) sempTrapOID [OID] 1.3.6.1.6.3.1.1.5.1 1.3.6.1.6.3.1.1.4.3.0	172 25 1148 172 25 111 48 172 25 111 48	2021-11-09-016433 2021-14-09-016433 2021-14-09-0164-23	SNP Version:	Coperations Get Next :	
Nate: Advaced. OD 13 NAT:: Advaced. OD 13 NaT:: * to org dolament	Operation Tool Deduce Image: Complete Image: Complete Image: Complete Image: Complete Image: Complete Image: Complete Verter: Neare: Complete Verter: Verter: Complete	sysUpTime.0 [TimeTicks] 230 miliseconds (23) sempTrapOID [OID] 1.3.6.1.6.3.1.1.5.1 1.3.6.1.6.3.1.1.4.3.0	172 25 1148 172 25 111 48 172 25 111 48	2021-11-09-016433 2021-14-09-016433 2021-14-09-0164-23	SNP Version:	Coperations Get Next :	
Name Image: Comparison of the Declaration of the Declaratio	Operation Tool Deduce Image: Complete Image: Complete Image: Complete Image: Complete Image: Complete Image: Complete Verter: Neare: Complete Verter: Verter: Complete	sysUpTime.0 [TimeTicks] 230 miliseconds (23) sempTrapOID [OID] 1.3.6.1.6.3.1.1.5.1 1.3.6.1.6.3.1.1.4.3.0	172 25 1148 172 25 111 48 172 25 111 48	2021-11-09-016433 2021-14-09-016433 2021-14-09-0164-23	SNP Version:	Coperations Get Next :	
The Edit Quention Tools Blockmarks Help Address * • Address * • Main • WMIT Tree • It to eng dod ammet	Operation Tool Deduce Image: Complete Image: Complete Image: Complete Image: Complete Image: Complete Image: Complete Verter: Neare: Complete Verter: Verter: Complete	sysUpTime.0 [TimeTicks] 230 miliseconds (23) sempTrapOID [OID] 1.3.6.1.6.3.1.1.5.1 1.3.6.1.6.3.1.1.4.3.0	172 25 1148 172 25 111 48 172 25 111 48	2021-11-09-016433 2021-14-09-016433 2021-14-09-0164-23	SNP Version:	Coperations Get Next :	
Tel: Edit Operation Table Bookands Help Address AdvancedODD_13 SNAP Mith Particular State * Tel: Tel: * Tel: Tel:	Operation Tool Deduce Image: Complete Image: Complete Image: Complete Image: Complete Image: Complete Image: Complete Verter: Neare: Complete Verter: Verter: Complete	sysUpTime.0 [TimeTicks] 230 miliseconds (23) sempTrapOID [OID] 1.3.6.1.6.3.1.1.5.1 1.3.6.1.6.3.1.1.4.3.0	172 25 1148 172 25 111 48 172 25 111 48	2021-11-09-016433 2021-14-09-016433 2021-14-09-0164-23	SNP Version:	Coperations Get Next :	
Name Image: Comparison of the point of t	Operation Tool Deduce Image: Complete Image: Complete Image: Complete Image: Complete Image: Complete Image: Complete Verter: Neare: Complete Verter: Verter: Complete	sysUpTime.0 [TimeTicks] 230 miliseconds (23) sempTrapOID [OID] 1.3.6.1.6.3.1.1.5.1 1.3.6.1.6.3.1.1.4.3.0	172 25 1148 172 25 111 48 172 25 111 48	2021-11-09-016433 2021-14-09-016433 2021-14-09-0164-23	SNP Version:	Coperations Get Next :	

LLDP (Link Layer Discovery Protocol)

All Axis devices with AXIS OS 7.10 and higher are utilizing LLDP (Link Layer Discovery Protocol) to neighbor-announce their identity and capabilities information using the TLV-encoding scheme (Type-Length-Value) in the network. When sending out LLDP announcements, it is possible to configure certain information such as system description and name of the device. In order to configure specific LLDP settings, you can access the device via SSH, SSH is disabled per default and can be enabled in Settings

Network protocols

> System > Plain config > Network. Once SSH access is established, type "Ildpcli". See the *following instructions* for further commands that can be used in the LLDPCLI.

In addition to neighbor announcements, LLDP can also be used for software-based PoE negotiation. IEEE 802.3at (30 W PoE+) capable devices support software-based PoE negotiations, and IEEE 802.3af (15.4 W) capable devices running AXIS OS 9.20 and higher support the LLDP allocation of max-power towards the connected PoE-switch. When enabled, the Axis device will notify the PoE-switch about its max PoE consumption so that the PoE-switch can perform a better PoE-management and allocate less PoE to the network port. LLDP allocation for max-power can be enabled in Settings > System > Plain config > Network > LLDP POE > LLDP Send Max PoE. Both methods utilize the LLDP Dot3 PoE-MDI TLV.

When LLDP allocation for max-power is enabled in the Axis device, and the network switch is configured properly in regards to LLDP- and PoE-mode according to vendor documentation, the network switch should be able to reserve the exact amount of max PoE wattage that the Axis device would need. The example below illustrates the behavior of LLDP allocation for max-power being enabled and disabled in an Axis device.

sw03#show power inline gigabitEthernet 1/0/1 detail
Interface: Gi1/0/1
Inline Power Mode: auto
Operational status: on
Device Detected: yes
Device Type: Ieee PD
IEEE Class: 3
Discovery mechanism used/configured: Unknown
Police: off
Power Allocated
Admin Value: 15.4
Power drawn from the source: 15.4
Power available to the device: 15.4
Actual consumption
Measured at the port: 4.0
Maximum Power drawn by the device since powered on: 4.5
Absent Counter: 0
Over Current Counter: 0
Short Current Counter: 0
Invalid Signature Counter: 0
Power Denied Counter: 0
Power Negotiation Used: None
LLDP Power NegotiationSent to PDRcvd from PD
Power Type:
Power Source:
Power Priority:
Requested Power(W):
Allocated Power(W):

Disabled

Network protocols

```
w03#show power inline gigabitEthernet 1/0/2 detail
Interface: Gi1/0/2
Inline Power Mode: auto
Operational status: on
Device Detected: yes
Device Type: Ieee PD
IEEE Class: 3
Discovery mechanism used/configured: Unknown
Police: off
Power Allocated
Admin Value: 15.4
Power drawn from the source: 11.3
Power available to the device: 11.3
Actual consumption
Measured at the port: 4.0
Maximum Power drawn by the device since powered on: 4.7
Absent Counter: 0
Over Current Counter: 0
Short Current Counter: 1
Invalid Signature Counter: 0
Power Denied Counter: 0
Power Negotiation Used: IEEE 802.3at LLDP
LLDP Power Negotiation --Sent to PD--
                                            --Rcvd from PD--
                       Type 2 PSE
                                             Type 1 PD
  Power Type:
  Power Source:
                       Primary
                                             PSE
  Power Priority:
                                             high
                       low
  Requested Power(W):
                       9.6
                                             9.6
  Allocated Power(W):
                       9.6
                                             9.6
```

Enabled

When LLDP allocation for max-power is *disabled*, the network switch will reserve the full amount of 15.4 W PoE according to IEEE 802.3af with no savings gained. Compare this with having the LLDP allocation for max-power *enabled*, which will result in the network switch reserving in total 11.3 W PoE instead, where 9.6 W results from the needs of the Axis device and the additional 1.7 W is a margin for power loss due to cable length. This improved PoE management results in saving 4.1 W PoE that can be used on a different network port on the same network switch.

Media Endpoint Discovery (LLDP-MED)

LLDP-MED (Media Endpoint Device Extension) is an extension on top of the LLDP protocol stack that allows devices to include more information (TLVs) during LLDP exchange with network neighbors. At the time of writing (December 2020), Axis devices do not support LLDP-MED extensions and therefore do not support e.g. the LLDP-MED POE-MDI TLV for PoE power negotiation.

Fabric Attach

Fabric Attach (FA) is a technology developed by Extreme Networks. It comes with an Autonomic Edge capability which simplifies the addition of new devices to the network. Axis devices with AXIS OS 12.1 or later have the Basic Fabric Attach client capability, which reduces the time and cost to deploy them in Extreme Networks with "Zero-Touch". For a complete list of products supporting Fabric Attach, please refer to *Products on active track* in AXIS OS Release notes.

Fabric Attach uses the Link Layer Discovery Protocol (LLDP) with custom organizational Type-Length-Values (TLVs) to automate the onboarding process for network devices onto different networks or services. As a Basic Fabric Attach client, Axis devices generate a Fabric Attach Element TLV which includes the following properties:

Network protocols

- Fabric Attach Element type
- A System ID with the device's MAC Address

The screenshot below provides a closer look at the LLDP packet structure for an Axis device.

>	Etl	nernet II, Src: AxisCommunic_28:25:d1 (b8:a4:4f:28:25:d1), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
~	Li	nk Layer Discovery Protocol
	>	Chassis Subtype = MAC address, Id: b8:a4:4f:28:25:d1
	>	Port Subtype = MAC address, Id: b8:a4:4f:28:25:d1
	>	Time To Live = 120 sec
	>	System Name = axis-b8a44f2825d1
	>	System Description = AXIS P3265-LV Dome Camera 12.1.31
	>	Capabilities
		Management Address
		Port Description = eth0
		Ieee 802.3 - Link Aggregation
	>	Ieee 802.3 - MAC/PHY Configuration/Status
	>	Ieee 802.3 - Power Via MDI
	~	Avaya Inc - Extreme Fabric Attach Element TLV
		1111 111 = TLV Type: Organization Specific (127)
		0 0011 0010 = TLV Length: 50
		Organization Unique Code: 00:04:0d (Avaya Inc)
		Subtype: Extreme Fabric Attach Element TLV (11)
		HMAC-SHA Digest: 000000000000000000000000000000000000
		0010 11 = Element Type: 11
		0000 0000 0000 = Mgmt VLAN: 0
		Reserved: 0
		System ID: b8:a4:4f:28:25:d1:00:00:00
	>	End of LLDPDU

The following applies for all Axis devices:

- Fabric Attach Element Type is always set to 11 (IP camera).
- System ID contains your device's unique MAC address.
- LLDP is enabled by default.
- The FA Element TLV is included in every outgoing LLDP packet.

Extreme Networks has four FA client variants. Axis devices act as Basic FA clients with minimal implementation, which allows you to bypass authentication for the FA Element TLV. As a result, the HMAC-SHA digest value is always zero.

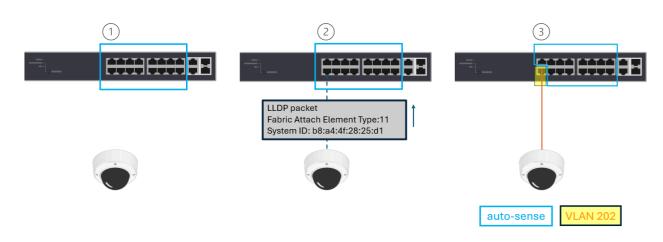
Example setup

In this scenario, the customer has a dedicated network segment, VLAN 202.

Previously, to onboard a camera, the customer would connect it to a physical switch port and then manually assign that port to VLAN 202. Fabric Attach simplifies the onboarding process.

- 1. By default, all ports on the Extreme Networks Fabric Engine switch are set for auto-sense.
- 2. The customer connects the Axis device to Port 2, which has Fabric Attach enabled. Once the device is powered on, it starts sending LLDP packets.
- 3. Using the FA Element TLV, the switch identifies the device as an IP Camera and automatically moves Port 2 to VLAN 202 with no manual intervention required.

Network protocols



To verify the Fabric Attach status on the Extreme Network switch:

SW24.15 **# show fabric attach assignments** Fabric Attach Mode: Standalone Proxy Port VLAN VLAN Name Type ISID/NSI Status

202 VLAN_0202 Static N/A Active 2 202 VLAN_0202 ZTC N/A Active

The type ZTC stands for Zero Touch Client. The minimal configurations of Fabric Attach have been included below for reference.

configure fabric attach uplink 24 configure fabric attach zero-touch-client camera vlan VLAN_0202 nsi 12345 configure fabric attach zero-touch-client camera enable configure vlan VLAN 0202 add nsi 12345

CDP (Cisco Discovery Protocol)

All Axis devices with AXIS OS 8.50.1 and higher are utilizing the CDP (Cisco Discovery Protocol) protocol to announce their identity and capabilities in the network. Compared to the LLDP protocol, no CDP traffic is sent out from the Axis device by default unless the network switch initiates CDP communication first.

CDP is also used for power negotiation in IEEE 802.3at (30W PoE+) capable devices. By default, the Axis device is capable of power negotiating IEEE 802.3at (30W PoE+) either using CDP or LLDP. Which one of these protocols is used depends on the network switch configuration.

In a situation where both protocols are being enabled and used by the network switch, the Axis device will respond to the protocol that arrives first (first come, first served). Note that Cisco 60W UPoE power negotiations are not supported regardless if they are hardware- or software-based.

Syslog

Syslog is a standard for message logging in IT devices. It is increasingly required in IT business applications and governance to facilitate, store, monitor and analyze audit logs from IT devices. The syslog standard is based on RFC 3164 and the newer RFC 5424.

Network protocols

Axis devices are compliant with both standards in order to allow for an easy and simple integration towards 3rd party syslog servers such as Nagios, PRTG, Syslog-NG- or Rsyslog-based syslog servers. The common term used for edge devices sending their log messages to a syslog server is referred to as "remote logging" or "remote syslogging". When it comes to syslog, there are two different types of devices in a network working together:

- Edge device: An edge device with support for syslog generates log messages which are sent to a centralized server. The edge device in itself, however, may have limited amount of system resources to keep log messages long enough, or the messages may be overwritten or erased automatically upon reboot. Axis devices are examples of edge devices.
- Syslog server: The syslog server is a centralized entity in the network that receives syslog messages from edge devices and facilitates and stores them in a manner that allows for real-time analysis and/or auditing. Different types of syslog servers are available and range from simple servers that "just" store incoming syslog messages up to fully-fledged enterprise-class syslog servers providing all means for real-time analysis as well as auditing with notification backend.

In order to send log messages to the syslog server, the edge device and server need to communicate using the same protocol/port. The edge device also needs to be configured so that it sends log messages with the desired severity.

- **Protocol/ports**: The syslog standard is based on RFC 3164 and the newer RFC 5424. The default ports that are used are UDP port 514 and TCP port 601 as well as encrypted transport via SSL/TLS port 6514. With AXIS OS 11.6 and later, we introduced our own proprietary format called "Axis" format that is mainly for our internal use. It's the same format that we currently using in our server report logs. Please be noted that Axis may change this format without prior notice.
- Log message severity: Log messages are categorized in severities based on importance, from low to high. In newer AXIS
 OS versions, it is possible to define from which severity level the Axis device will send log messages to a remote syslog
 sever. See log message severities for Axis devices below:
 DEBUG INFO NOTICE WARNING ERROR CRITICAL ALERT EMERGENCY

Examples of log messages from an Axis device

RFC 3164

<8>Aug 23 16:32:18.000 axis-b8a44f18d105 remote-syslogd:	remote-syslogd-test:	This
is Emergency message		
<9>Aug 23 16:32:18.000 axis-b8a44f18d105 remote-syslogd:	remote-syslogd-test:	This
is Alert message		
<10>Aug 23 16:32:18.000 axis-b8a44f18d105 remote-syslogd:	: remote-syslogd-test:	This
is Critical message		
<11>Aug 23 16:32:18.000 axis-b8a44f18d105 remote-syslogd:	: remote-syslogd-test:	This
is Error message		
<12>Aug 23 16:32:18.000 axis-b8a44f18d105 remote-syslogd:	: remote-syslogd-test:	This
is Warning message		

RFC 5424

<8>1 2023-08-23T16:34:23.000+02:00 axis-b8a44f42b8b0 remote-syslogd - - remote-syslogd-test: This is Emergency message
<9>1 2023-08-23T16:34:23.000+02:00 axis-b8a44f42b8b0 remote-syslogd - - remote-syslogd-test: This is Alert message
<10>1 2023-08-23T16:34:23.000+02:00 axis-b8a44f42b8b0 remote-syslogd - - remote-syslogd-test: This is Critical message
<11>1 2023-08-23T16:34:23.000+02:00 axis-b8a44f42b8b0 remote-syslogd - - remote-syslogd-test: This is Error message
<12>1 2023-08-23T16:34:23.000+02:00 axis-b8a44f42b8b0 remote-syslogd - - remote-syslogd-test: This is Error message
<12>1 2023-08-23T16:34:23.000+02:00 axis-b8a44f42b8b0 remote-syslogd - - remote-syslogd-test: This is Error message
<12>1 2023-08-23T16:34:23.000+02:00 axis-b8a44f42b8b0 remote-syslogd - - remote-syslogd-test: This is Error message
<12>1 2023-08-23T16:34:23.000+02:00 axis-b8a44f42b8b0 remote-syslogd - - -

Axis format

2023-08-23T16:30:14.998+02:00 axis-b8a44f4645f4 [EMERG] remote-syslogd[209665]: remote-syslogd-test: This is Emergency message 2023-08-23T16:30:14.998+02:00 axis-b8a44f4645f4 [ALERT] remote-syslogd[209665]: remote-syslogd-test: This is Alert message 2023-08-23T16:30:14.998+02:00 axis-b8a44f4645f4 [CRIT] remote-syslogd[209665]: remote-syslogd-test: This is Critical message

Network protocols

2023-08-23T16:30:14.998+02:00 axis-b8a44f4645f4 [ERR] remote-syslogd[209665]: remote-syslogd-test: This is Error message 2023-08-23T16:30:14.998+02:00 axis-b8a44f4645f4 [WARNING] remote-syslogd[209665]: remote-syslogd-test: This is Warning message

Syslog in Axis devices

Axis devices have been compliant with the syslog standard since its implementation in the 2000s. As such, Axis devices have throughout the years been supporting syslog in various ways in order to adapt, always using the newest implementation:

Implementation	SYSKLOGD	RSYSLOG	SYSLOG-NG MK I	SYSLOG-NG MK II
Supported versions	≤ 5.55	5.60 - 6.50	7.10 - 10.0	10.1 ≥
Script editor configuration	V	\checkmark	V	
Web interface configuration				V
VAPIX API configuration				\checkmark
SD card or network share storage*	V	\checkmark		
Transport protocol	UDP	TCP/UDP	TCP/UDP	TCP/UDP/TLS
Primary & secondary remote syslog server**				V
Send log messages test button***				\checkmark
Log severity configuration****				V

* Optional support for saving syslog messages to the local SD card or network share.

** Possibility to configure a primary and secondary remote syslog server. When both are configured, the Axis device will send its log messages simultaneously to both servers. Observe that this is not a failover-configuration.

*** Possibility to send test messages to the remote syslog server in order to verify correct configuration.

**** Possibility to configure the Axis device to send log messages with a specific severity and higher only.

The coming sections will show example configurations that can be accomplished illustrated with the different syslog implementations that Axis devices have supported throughout the years.

Syslog configuration in AXIS OS 10.1

Web interface

Devices with AXIS OS version 10.1 and higher have a graphical user interface for syslog configuration. This can be found via the web interface of the device, under Settings > System > TCP/IP.

Network protocols

Remote syslog Use remote syslog Server Host 192.168.0.100
Server ^
Host
402 469 0 400
192.100.0.100
Format
RFC 3164 RFC 5424
Protocol
TCP
Port
601
Severity
Alert or higher (1)
X
+
CA certificates ~
Test

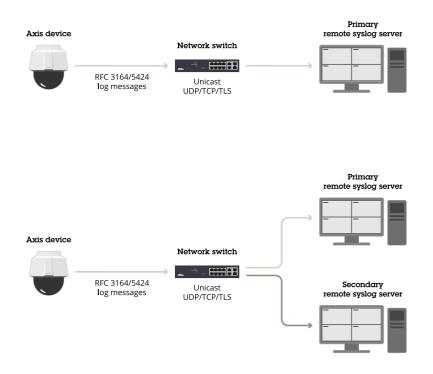
Network protocols

Remote syslog		Remote syslog	
Use remote syslog 🚺 🔵		Use remote syslog 1	
Server	^	Server	
Host		Host	
192.168.0.100		192.168.0.100	
Format		Format	
RFC 3164 RFC 5424		RFC 3164 RFC 5424	
Protocol		Protocol	
TLS	•	TLS	
Port		Port	
6514		6514	
Severity		Severity	
Alert or higher (1)	▼	Alert or higher (1)	
X		X	
+		Server	
CA certificates	~	Host	
		192.168.0.101	
Cybertrust Global Root	* ×	Format	
+		RFC 3164 RFC 5424	
		Protocol	
		TLS	
Test	Save	Port	
		6514	
		Severity	
		Warning or higher (4)	
		X	
		CA certificates	
		Cybertrust Global Root 🛛 🔻	X
		DigiCert Assured ID Root CA	

Network protocols

* For the TLS mode you need to specify a CA certificate that will be used by the Axis device to verify the remote syslog server. This CA certificate is generated and provided during the configuration of the 3rd party remote syslog server. ** When a primary and secondary syslog server is configured, the Axis device will always send its log messages simultaneously to both servers independently regardless if the primary, secondary, or both servers are available.

See the sample illustrations below of an Axis device streaming its syslog messages to either a primary server only, or a primary/secondary server in parallel.



VAPIX interface (VAPIX API)

Devices with AXIS OS version 10.1 and higher also support the Remote Syslog API VAPIX interface that allows for mass-configuration of Axis devices e.g. using AXIS Device Manager. For more information, go to the VAPIX library.

AXIS Device Manager

With the introduction of the new Remote Syslog API, it's also possible to configure remote syslog settings for multiple Axis devices simultaneously.

Network protocols

	0 🚣 🐻 🛈	9 🎝 🛛	₿ 5				
es, 1 selected MAC address Status	Address Hostnam	e Model	Firmware	DHCP	HTTPS	Server	
ACCC8ED9C85F OK	172.25.201.163	AXIS P1375	CVP-20.32.4	Yes	Disabled (multiple server.	VMS05	
			Configure devices				? _ D ×
Which settings do you w	ant to apply?						
Parameters Action R	,						
Action R	Muuruonai Setung	p			Type to search	×	Use configuration from:
Name	Value					^	Device
APLRemoteSyslog1						•	Configuration File
Enabled	false						X Address: 172.25.201.163
API.RemoteSyslog1.Server1			_				MAC Address: ACCC8ED9C85F Model: AXIS P1375
Address							Firmware: CVP-20.32.4
Port		An integer					
Protocol	TLS						
Severity	Warning						
Syslog format	RFC5424						
API.RemoteSyslog1.Server2			-				
Address							
Port		An integer	_				
Protocol	TLS						
Severity	Warning						
Syslog format	RFC5424					¥	
Select / Deselect all							
						Help	< Back Next > Cancel

Syslog configuration in AXIS OS 7.10 - 10.0

Script editor

In order to configure remote syslog server, the script editor needs to be enabled. This can be done via the web interface of the Axis device, under Settings > System > Plain config > System > Enable the script editor (editcgi).

To configure syslog, open the following link in the browser, replace the IP adress placeholder ("ip_of_cam") with the real IP address of the Axis device: http://ip_of_cam/admin-bin/editcgi.cgi?file=/etc/syslog-ng.d/remote.conf

Add IP address, transport method and port as you see in the below example configuration. Click Save file once done and restart the device.

Network protocols



Note

Make sure that no code line is out commented by a hash symbol ("#") like in the example configuration above.

Syslog configuration in AXIS OS 5.60 - 6.50

In order to configure syslog, open the following link in the browser and replace the IP address placeholder (i.e. "ip-address") with the real IP address of the Axis device: http://ip-address/admin-bin/editcgi.cgi?file=/etc/rsyslog.d/40-remote_log.conf

Remote syslog server

Add * . * @ip-address at the bottom of the configuration file and specify the real IP address of the remote syslog server instead. Click Save file once done and restart the device.

Network protocols

/e as: /etc/rsyslog.d/40-remote_log.conf	Mode: 0100644	Convert CRLF to LF: 🗹
	Save file	
Remote logging configuration !!! INPORTANT: !!! This file will be replaced on firmwar !!! Add your additions to a new file and !!! in /etc/ <u>rsyslog.d</u> /	iii e upgrade iii	
nplate(name=" <u>sysklogd</u> " type="string" string="<%	PRI%>%TIMESTANP% % <u>syslogtag</u> %% <u>msg</u> %\"")	
TEMPLATES There are several templates available to speci RSYSLOG Forwardformat A new high-precision forwarding format very one, but with high-precision timestamps and Recommended to be used when sending messages RSYSLOG TraditionalForwardfFormat The traditional forwarding format with low-p Most useful if you send messages to other <u>sy</u> below version 3.12.5. <u>sysklogd</u> <u>sysklogd</u> does not support RFC 3164 format. A <u>duplicate hostnames</u> if <u>rsyslog</u> is the sender Specify <u>sysklogd</u> as your template if you run <u>AvisFormat</u> The default format used in local log files of	<pre>similar to the traditional timezone information. to <u>rsyslog</u> 3.12.5 or above. recision timestamps. <u>slogd's</u> or <u>rsyslogd</u> s such, you will experience and <u>sysklogd</u> is the receiver. into this problem.</pre>	
EXANPLE To send messages from all facilities and all <u>RSYSLOG ForwardFormat</u> via <u>UDP</u> to a server wi 55555, use the following line: ".* action(type=" <u>omfud</u> " template=" <u>RSYSLOG Forwa</u>	. <u>severties</u> in th <u>ip</u> 192.168.0.1 on port <u>rdFormat</u> " Target="192.168.0.1" Port="55555" Proto	col=" <u>udp</u> ")
See the following link for more information abo h <u>ttp://www.rsyslog.com</u> /doc/ <u>v8</u> -stable/configurat * @192.168.0.100		

SD card Start by mounting an SD card in the Axis device. Then add *.* /var/spool/storage/SD_DISK/logs.txt at the bottom of the configuration file. Click Save file once done and restart the device.

Network protocols

/e as: /etc/rsyslog.d/40-remote_log.conf	Mode: 0100644	Convert CRLF to LF:
	Save file	
Remote logging configuration		
<pre>III IMPORTANT: !!! This file will be replaced on firm !!! Add your additions to a new file ar !!! in /etc/<u>rsyslog.d</u>/</pre>		
<pre>splate(name="sysklogd" type="string" string='</pre>	<%PRI%>%TIMESTAMP% %syslogtag%%msg%\"")	
TEMPLATES There are several templates available to spo <u>RSYSLOG ForwardFormat</u> A new high-precision forwarding format ver one, but with high-precision timestamps are Recommended to be used when sending messag	y similar to the traditional d timezone information.	
RSYSLOG TraditionalForwardFormat The traditional forwarding format with low Most useful if you send messages to other below version 3.12.5.		
sysklogd sysklogd duplicate <u>hostnames</u> if <u>rsyslog</u> is the sent Specify <u>sysklogd</u> as your template if you r AxisFormat The default format used in local log files	fer and <u>sysklogd</u> is the receiver. 'un into this problem.	
EXANPLE To send messages from all facilities and a <u>RSYSLOG ForwardFormat</u> via UDP to a server 55555, use the following line: *.* action(type=" <u>omfwd</u> " template=" <u>RSYSLOG For</u>		tocol=" <u>udp</u> ")
See the following link for more information : http://www.rsyslog.com/doc/v8-stable/configur * /var/spool/storage/SD_DISK/logs.txt		
/ver/spost/storage/su_oisk/adgs.txt		

Network share

Start by mounting a network share on the Axis device. Add *.* /var/spool/storage/NetworkShare/logs.txt at the bottom of the configuration file. Click Save file once done and restart the device.

Network protocols

ve as: /etc/rsyslog.d/40-remote_log.conf	Mode: 0100644	Convert CRLF to LF: 🗹
	Save file	
Remote logging configuration !!! IMPORTANT: !!! This file will be replaced on firmwa !!! Add your additions to a new file and !!! in /etc/rsyslog.d/	III re upgrade III	
mplate(name=" <u>sysklogd</u> " type="string" string="<	<pre>SPRI%>%TIMESTAMP% %syslogtag%%msg%\"")</pre>	
 TEMPLATES There are several templates available to spec RSYSLOG ForwardFormat A new high-precision forwarding format very one, but with high-precision timestamps and Recommended to be used when sending message 	similar to the traditional timezone information.	
RSYSLOG TraditionalForwardFormat The traditional forwarding format with low- Most useful if you send messages to other <u>s</u> below version 3.12.5. sysklogd	<u>yslogd's</u> or <u>rsyslogd</u>	
sysklogd does not support RFC 3164 format. duplicate hostnames if rsyslog is the sende Specify sysklogd as your template if you ru <u>AxisFormat</u> The default format used in local log files	r and <u>sysklogd</u> is the receiver. n into this problem.	
EXAMPLE To send messages from all facilities and al <u>RSYSLOG ForwardFormat</u> via <u>UDP</u> to a server w 55555, use the following line: *.* action(type=" <u>omfwd</u> " template=" <u>RSYSLOG Forw</u>		cocol=" <u>udp</u> ")
See the following link for more information ab http://www.rsyslog.com/doc/ <u>v8</u> -stable/configura * /var/spool/storage/NetworkShare/logs.txt		

Syslog configuration in AXIS OS 5.55 and below

In order to configure syslog, open the following link in the browser, replace the IP address placeholder (i.e. "ip-address") with the real IP address of the Axis device: http://ip-address/admin-bin/editcgi.cgi?file=/etc/syslog.conf.

Remote syslog server

Start by adding * . * @ip-address at the bottom of the configuration file and specify the real IP address of the remote syslog server instead. Click Save file once done and restart the Axis device.

Network protocols

File: /etc/syslog.conf Length: 795 bytes [Select new file] Save as: /etc/syslog.conf	Mode: 0100644	Convert CRLF to LF:
Save as: reichsysiog.com	Save file	Convert CRLF to LF:
# An <u>autogenerated</u> default /etc/ <u>syslog.conf</u> . *.info;*.lwarning; <u>authpriv.none;kern.none</u> *.info;*.lwarning;mail.none; <u>authpriv.none;kern.none</u>	//var/log/info_log_pipe //var/log/info_mld_pipe	
*.=warning; <u>authpriv.none;kern.none</u> *.=warning;mail.none; <u>authpriv.none;kern.none</u>	/var/log/warning_log_pipe /var/log/warning_mld_pipe	
*.err; <u>authpriv.none</u> *.err;mail.none; <u>authpriv.none</u>	/var/log/crit_log_pipe /var/log/crit_mld_pipe	
authpriv.warning;kern.=warning;authpriv.!crit authpriv.warning;authpriv.!crit authpriv.crit authpriv.crit	//var/log/authpriv_warn_log_pipe //var/log/warning_mld_pipe //var/log/authpriv_crit_log_pipe //var/log/crit_mld_pipe	
<pre>#kern.debug #*.debug;authpriv.none;kern.none *.debug;authpriv.none</pre>	/var/log/ <u>kern_</u> logs / <u>dev</u> /console / <u>dev</u> /console	
. @192.168.0.100		
	Save file	

SD card

Start by mounting an SD card in the Axis device. Then add *.* /var/spool/storage/SD_DISK/logs.txt at the bottom of the configuration file. Click Save file once done and restart the Axis device.

Network protocols

File: /etc/syslog.conf Length: 795 bytes [Select new file]		
Save as: /etc/syslog.conf	Mode: 0100644	Convert CRLF to LF:
	Save file	
<pre>Save as: //eto/systog.conf # An autogenerated default /stc/systog.conf. *.info;*.lwarning;authpriv.none;kern.none *.info;*.lwarning;authpriv.none;kern.none *.ewarning;authpriv.none;kern.none *.ewarning;mail.none;authpriv.none;kern.none *.ewarning;mail.none;authpriv.none authpriv.warning;authpriv.none authpriv.warning;authpriv.lcrit authpriv.crit #kern.debug #*.debug;authpriv.none;kern.none *.debug;authpriv.none *.* /var/spool/storage/SD_DISK/logs.txt</pre>		Convert CRLF to LF:
L	Save file	

Network share

Start by mounting a network share on the Axis device. Then add *.* /var/spool/storage/NetworkShare/logs.txt at the bottom of the configuration file. Click Save file once done and restart the Axis device.

Network protocols

ile: /etc/syslog.conf Length: 795 bytes [Select new file]		
ave as: /etc/syslog.conf	Mode: 0100644	Convert CRLF to LF: Z
	Save file	
An autogenerated default /etc/syslog.conf. .info;".lwarning;authpriv.none;kern.none .info;".lwarning;mail.none;authpriv.none;kern.none	/var/log/info_log_pipe /var/log/info_mld_pipe	
.=warning; <u>authpriv.none;kern.none</u> .=warning;mail.none; <u>authpriv.none;kern.none</u>	/var/log/warning_log_pipe /var/log/warning_mld_pipe	
.err; <u>authpriv.none</u> .err;mail.none; <u>authpriv.none</u>	/var/log/ <u>crit_log_pipe</u> /var/log/ <u>crit_mld_</u> pipe	
authpriv.warning;kern.=warning;authpriv.!crit authpriv.warning;authpriv.!crit authpriv.crit authpriv.crit	/var/log/authpriv_warn_log_pipe /var/log/warning_mld_pipe /var/log/authpriv_crit_log_pipe /var/log/ <u>crit_mld_p</u> ipe	
# <u>kern.debug</u> #*.debug; <u>authpriv.none;kern.none</u> *.debug; <u>authpriv.none</u>	/var/log/ <u>kern</u> logs / <u>dev</u> /console / <u>dev</u> /console	
. /var/spool/storage/NetworkShare/logs.txt		
	Save file	

About syslog server support

Axis devices are compliant with the syslog standard that is based on RFC 3164 and the newer RFC 5424, so the transmission of syslogs to a server should work out-of-the-box when configured correctly. Axis devices are tested regularly with different syslog servers such as syslog-ng, rsyslog as well as PRTG Paessler, Nagios, QNAP and Synology.

Below is a sample image of an Axis device sending log messages to a Nagios syslog server.

Network protocols

Dashboard - Neglos Log Se	and the second														-	
→ C ① Inte săli	oer 172.25.201.10	8/hagioslogserver	/dashboard#/das	/hboard/ela	isticsearch///WoRgiYS	IKJDEWCMBIQ									Q,	*
gios' <mark>LS</mark>	Home Dashbo	ards Alerting	Help				Z						Search logs	•	≜ psadmi	in Ol
Main Dashboard	×											Aug 14, 20	120 06:39:20 to Aug 14, 2020 06:53		s •	*
																۹.
ed +	• LiAlert • 2	Critical = 3:Emp	a 🛛 🗧 4/Warning	School	ice 6.1nformation	al 7:Debug										_
ni e muste na se	A See suit : 6-M : grants free : 7000-00 i 6- : 7000-00 i	4104 20 20.4001. 1-14134 314:39:39:39:01. A X	* 													
ENTS OVER TIME											0	0 + x	SYSLOG TYPES		0 0	•
• 2008 Out • * (207) IS	ourit per 184 (207 Mil)															
															× .	
						_										
						_										
														109%		
86-40-00	06-10-38	06:42:08	06-43-00	86-44:00	86-43-80	04-44-00	06:47:00	86+48:00	86-49-00	24,51,62	00.51-00	06-52-98				
L EVENTS														A support as to		• •
(14) / Current (14)								0 to 50 of 20	? available for paging					*		
e to filler	Otimestamp>		< host >		emessage											ctions
		52:03.764+02:00			<30>1 2020-08-1410						se time 600				9	Q *
These fields have been	2020-08-14T06	:52:01.725+02:00			<30>1 2020-08-1470											a .
These fields have been ceed from your mapping. It fields may be available		:51:05.169+02:00	172.25.201.157	golaya /	<30>1 2020-08-14T0	6:50:59.000+02:00	anis-accolled9c857	systemd 1 remote	e-syslogd.service: 5a	ucceeded.					9	۹. ۴
These fields have been check from your mapping, it fields may be available or source decument.							and accellant of the	remote-systend	D-Bus com aals Ren	noteSyslog1 released					0	q +
These fields have been ched from your megging, if fields may be available or source document.	2020-08-54705	:51:05.159+02:00	172.25.201.153	golaya 7	<14>1 2020-08-14T0	5:50:59.000+02:00	BRIN BOARDANSER									
These fields have been cad from your mapping, if fields may be available or equate document.	2020-08-14T05 2020-08-54T05	:51:05.159+02:00 :51:05.153+02:00			<14>1 2020-08-14T0				No request received	L starting termination	process				9	۹.
These fields have been med from your mapping, it freids may be available or docut discussed. If optimised the field optimised of the field optimised optimised field field field optimised field field field field field field field field field field field field field field field field field field field f	2020-08-14700 2020-08-54700 2020-08-14706			7 syslog		6:50:59.000+82:08	aais-accc8ed9c85f	remote-syslogd			process					а + а +
These fields have been code floors your mapping, if fields may be available or should adsounded. T gittmestamp T gittmestamp T gotting, jabel T facility_label T facility_label T facility_label T gotting_label g gotting	2020-08-54T05 2020-08-54T05 2020-08-54T05 2020-08-54T05	:51:05.153+02:00	172.25.201.157 172.25.201.157	7 syskop 7 syskop	<14>1 2020-08-1470 <30>1 2020-08-1470	6:50:59.000+82:88 6:50:40.000+82:88	awis-accolled9c85f awis-accolled9c85f	remote-syslogd systemd 1 usage	statistics.service: S	ucceeded.					9	
These fields have been send from your mapping, and the ray to available our about discussed.	2020-08-54T05 2020-08-54T05 2020-08-54T05 2020-08-54T05 2020-08-54T05 2020-08-54T06	:51:05:153+02:00 :50:46:213+02:00	172.25.201.157 172.25.201.157 172.25.201.157	7 syskop 7 syskop 7 syskop	<14>1 2020-08-1470	6:50:59.000+02:00 6:50:40.000+02:00 0:50:40.000+02:00	axis-accciled9c85f axis-accciled9c85f axis-accciled9c85f axis-accciled9c85f	remate-suslogd systemd 1 usage usage-statistics 181	statistics.service: Bi I No request rece	ucceeded. rived, starting termine	flon precess				9	۹. ۲

Contact

Contact Axis Technical Services for further assistance and additional requests: https://www.axis.com/support

MQTT

MQTT is a machine-to-machine (M2M)/Internet of things (IoT) connectivity protocol. It was designed as an extremely lightweight publish/subscribe messaging transport and is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium.

MQTT is quickly becoming the standard communication protocol for implementing IoT solutions due to its lightweight and bandwidth-efficient characteristics. You can read more about benefits and usecases in the whitepaper *Device integration with MQTT* or keep on reading to learn more about configuring MQTT, starting with the most important components.

Client

Any publisher or subscriber that connects to a centralized server/broker over a network is a client. Both publishers and subscribers are called clients since they connect to a centralized service. Clients can be persistent or transient. Persistent clients maintain a session with the server/ broker while transient clients are not tracked by the server/ broker. Clients often connect to the server/ broker through libraries and SDKs.

Server/broker

The server/broker is the software that receives all the messages from the publishing clients and sends them to the subscribing clients. It holds the connection to persistent clients. Since the server/broker can become a bottleneck or result in a single point of failure, it is often clustered for scalability and reliability. It is up to the implementor to decide how to create a scalable server/broker infrastructure. Some of the commercial implementations of MQTT brokers include HiveMQ, Xively, AWS IoT and Loop.

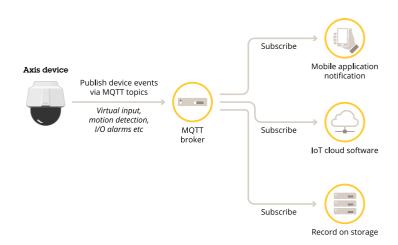
Topic

A topic in MQTT is an endpoint information that a client (publisher) can share, and another client (subscriber) can connect to. Topics are simple, hierarchical strings, encoded in UTF-8, delimited by a forward slash. For example, "building1/room1/temperature" and "building1/room1/humidity" are valid topic names.

Network protocols

Connection

MQTT can be utilized by clients based on TCP/IP. The standard port exposed by servers/brokers is 1883, which is not a secure port. Servers/brokers that support TLS/SSL typically use port 8883. For secure communication, the clients and the server/broker rely on digital certificates.



Functionality overview

Axis devices with AXIS OS version 9.80 and above support the MQTT protocol to allow customers and the market to deepen the integration of their business and system applications. In the table you can see the functionality that is currently supported as well as upcoming functionality.

Functionality	AXIS OS version
Generic MQTT event publishing	AXIS OS 9.80.1
Custom MQTT event publishing	AXIS OS 10.4.0
Custom MQTT event subscription	AXIS OS 10.6. Added to web interface in AXIS OS 10.7
MQTT web interface support	AXIS OS 10.1
MQTT over TCP	AXIS OS 9.80.1
MQTT over SSL	AXIS OS 9.80.1
MQTT over WebSocket	AXIS OS 9.80.1
MQTT over WebSocket (SSL)	AXIS OS 9.80.1
ΜΩΤΤ VAPIX API	AXIS OS 9.80.1
MQTT ALPN support (Application-Layer Protocol Negotiation)	AXIS OS 10.9.0
MQTT Overlay Support	AXIS OS 11.4

In the following sections you can read more about configuring a device via the web interface.

Server

These examples show you how to configure an Axis device to connect to an MQTT server/broker in the web interface. To connect, the user must specify the server's/broker's IP address or hostname, the transport protocol and port, as well as credentials (i.e.

Network protocols

username and password). The MQTT server/broker connection configurations can be found under Settings > System > MQTT in the web interface.

ple configuration: MQTT over TCP		Example configuration: MQTT over SSL*	
MQTT		MQTT	
Client		Client	
Connect		Connect	
Status: Connected		Status: Connected	
Server	^	Server	^
Host		Host	
172.25.201.102		172.25.201.102	
Protocol		Protocol	
MQTT over TCP	Ŧ	MQTT over SSL	
Port		Port	
1883		8883	
Username		Username	
mqtt_1		mqtt_1	
Password		Vse password	
•••••		Password	
		•••••	
Policies	~		
Last will testament	~	Certificates	^
Connect message	~	Client certificate	
		Default (self-signed)	
	Save	CA certificate	
		Baltimore CyberTrust Root 🖤	
		Validate server certificate	
		Policies	~
		Last will testament	~
		Connect message	~
			Save

*For the MQIT over SSL connection to be successful the CA and client certificate must be available under Settings > System > Security so that they can be selected in the MQIT configuration.

Network protocols

Policies

The connection policies help the user define general MQTT connection behavior of the Axis device towards the MQTT server/broker it connects to. Below you will find a more detailed description of the individual settings of the policies.

Client	
Connect	
Status: Connected	
Server	~
Policies	^
Client id	
AXIS-M1137	
Keep alive interval	
60	
Timeout	
60	
 Reconnect automatically 	
Clean session	
Last will testament	~
Connect message	~

- Client id: nice/nick name that is used by the Axis device to identify itself towards the MQTT server/broker.
- Keep alive interval: defines the maximum time in seconds that can pass without communication between the Axis device and the MQTT server/broker. The Axis device will send a keep alive message within the defined interval to ensure connection. Note that this will affect the last will testament settings.
- **Timeout**: defines the maximum time in seconds for a connection to complete successfully. If the connection attempt exceeds the defined value, the connection will not be accomplished.
- **Reconnect automatically**: when enabled, the Axis device will try to reconnect to the MQTT server/broker upon unintentional connection loss.
- Clean session: controls the client state persistency on the broker side and defines how a connecting client should be treated upon connection. When enabled, no state is kept on the broker. When disabled, the MQTT broker will keep the subscriptions alive and queue QoS 1/2 messages for delivery after a reconnect. This field has no impact on publishing only clients.

Network protocols

MQTT QoS settings

Each distinct message - i.e. the connect message, the last will testament message and the individual event filtering/topics - allows for dedicated QoS settings to be configured. Below the general QoS behavior and the level of service upon message delivery is described.

Level 0 is the lowest service level and provides no guarantee of message delivery.

- > Frame 972: 317 bytes on wire (2536 bits), 317 bytes captured (2536 bits)
- Ethernet II, Src: AxisComm_d9:c8:5f (ac:cc:8e:d9:c8:5f), Dst: VMware_85:93:68 (00:0c:29:85:93:68)
- Internet Protocol Version 4, Src: 172.25.201.156, Dst: 172.25.201.102
- > Transmission Control Protocol, Src Port: 49936, Dst Port: 1883, Seq: 18028, Ack: 545, Len: 251
- MQ Telemetry Transport Protocol, Publish Message

```
Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
Msg Len: 248
Topic Length: 74
Topic: ACCC8ED9C85F/event/tns:onvif/Device/tns:axis/IO/VirtualPort/$source/port/1
Message: 7b2274696d657374616d70223a2031353937333030353330...
```

Level 1 guarantees message delivery at least once to the broker with the possibility of receiving the same message multiple times before acknowledgement.

- Frame 581: 319 bytes on wire (2552 bits), 319 bytes captured (2552 bits)
- Ethernet II, Src: AxisComm_d9:c8:5f (ac:cc:8e:d9:c8:5f), Dst: VMware_85:93:68 (00:0c:29:85:93:68)
- Internet Protocol Version 4, Src: 172.25.201.156, Dst: 172.25.201.102
- > Transmission Control Protocol, Src Port: 49936, Dst Port: 1883, Seq: 1, Ack: 1, Len: 253
- MQ Telemetry Transport Protocol, Publish Message

Header Flags: 0x32, Message Type: Publish Message, QoS Level: At least once delivery (Acknowledged deliver) Msg Len: 250 Topic Length: 74 Topic: ACCC8ED9C85F/event/tns:onvif/Device/tns:axis/IO/VirtualPort/\$source/port/1 Message Identifier: 66 Message: 7b2274696d657374616d70223a2031353937333030353234...

Level 2 is the highest service level providing a four-way handshake to ensure that each message is delivered exactly once to the broker. Frame 633: 319 bytes on wire (2552 bits), 319 bytes captured (2552 bits)

- › Ethernet II, Src: AxisComm_d9:c8:5f (ac:cc:8e:d9:c8:5f), Dst: VMware_85:93:68 (00:0c:29:85:93:68)
- Internet Protocol Version 4, Src: 172.25.201.156, Dst: 172.25.201.102
- > Transmission Control Protocol, Src Port: 49936, Dst Port: 1883, Seq: 507, Ack: 9, Len: 253
- MQ Telemetry Transport Protocol, Publish Message
- Header Flags: 0x34, Message Type: Publish Message, QoS Level: Exactly once delivery (Assured Delivery) Msg Len: 250 Topic Length: 74 Topic: ACCC8ED9C85F/event/tns:onvif/Device/tns:axis/IO/VirtualPort/\$source/port/1

```
Message Identifier: 68
```

Message: 7b2274696d657374616d70223a2031353937333030353235...

Axis topic expressions

To determine which topics are supported by an Axis device, you can use the following API calls in VAPIX or ONVIF. Although it's possible to run these commands within the SSH console from the camera, we recommend using a tool like CURL or POSTMAN instead. This approach doesn't require enabling SSH access to the device.

If you prefer to use SSH, go to Plain config > Network > SSH and log in directly to the AXIS device.

For more information about Postman and CURL, see VAPIX on page 297.

Network protocols

VAPIX interface

Make a GetEventInstances request to VAPIX web services as in the example below, but replace the username, password and IP address with the actual configured settings:

```
curl --noproxy "*" --user <username>:<password> --digest --request POST
'http://<device-address>/vapix/services' \
    --header 'Content-Type: application/soap+xml;
action=http://www.axis.com/vapix/ws/event1/GetEventInstances; Charset=UTF-8' \
    --data-raw '<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://www.w3.org/2003/05/soap-
envelope" xmlns:SOAP-ENC="http://www.w3.org/2003/05/soap-encoding"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<SOAP-ENV:Body>
<m:GetEventInstances xmlns:m="http://www.axis.com/vapix/ws/event1"/>
</SOAP-ENV:Body>
</soAP-ENV:Body>
</soAP-ENV:Body>
</soAP-ENV:Envelope>'
```

ONVIF interface

Make a GetEventProperties request to ONVIF event services as in the example below, but replace the username, password and IP address with the actual configured settings:

```
curl --noproxy "*" --user <username>:<password> --digest --request POST
'http://<device-address>/onvif/services'
--header 'Content-Type: application/xml' \
--data-raw '<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://www.w3.org/2003/05/soap-envelope"
xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:tet="http://www.onvif.org/ver10/events/wsdl">
<SOAP-ENV:Header>
<wsa:Action>
http://www.onvif.org/ver10/events/wsdl/EventPortType/GetEventPropertiesRequest
</wsa:Action>
</SOAP-ENV:Header>
<SOAP-ENV:Body>
<tet:GetEventProperties>
</tet:GetEventProperties>
</SOAP-ENV:Body>
</SOAP-ENV:Envlope>'
```

Output examples

```
onvif:Device/axis:Status/SystemReady
onvif:Device/axis:IO//.
onvif:RuleEngine/MotionRegionDetector/Motion
axis:CameraApplicationPlatform/VMD/CameralProfileANY
```

Last will testament

The last will testament settings define the behavior of the Axis device towards the MQTT server/broker after ungraceful disconnection, i.e. without the Axis device sending out a *disconnect* message. This could happen due to bad network connection, power disconnect, etc.

Network protocols

When the last will testament is enabled, the MQTT server/broker will announce the defined message in case the Axis device disconnects ungracefully. Below you will find a more detailed description of the individual settings of the last will testament and an example of a customized last will testament message.

Connect	
Status: Disconnected	
Server	~
Policies	~
Last will testament	^
Send messages 👔 🔵	
Use default o	
Торіс	
Message	
Keep	
QoS	
0 🔻	
Connect message	~

- Use default: use predefined default settings.
- **Topic**: a customized topic that will be used by the MQTT broker for disconnection announcements, i.e. to announce to subscribed MQTT clients that the Axis device has disconnected ungracefully.
- Message: a customized message to be used by the MQTT broker for disconnection announcements. See below example.
- Keep: also known as *retain*. Defines if the broker should retain the last will testament message in the broker's cache so that new subscribers will receive the message directly after subscribing.
- QoS: defines the level of service upon message delivery. Go to MQTT QoS settings on page 141 for more information.

In the example below we have configured a customized last will testament (LWT) announcing the message "Axis device LWT message" in case the device disconnects ungracefully.

Network protocols

Client		=	MQTT Explorer	Q Search
Connect		▼ ACC	201.102 : (48 topics, 1719 messages) C8ED9C85F nt (59 topics, 59 messages)	
Server	~	Last_	Will_Testament = Axis device	e LVV I message
Policies	~			
Last will testament	^			
Send messages 1 Use default Topic ACCC8ED9C85F/Last_Will_Testament Message Axis device LWI message Keep QoS 0				
Connect message Send messages	^			

Connect message

The connect message can be used to let the Axis device announce its connection state to the MQTT broker and other subscribed MQTT clients. Below you will find a more detailed description of the individual settings of the connect message.

Network protocols

Client	
Connect	
Status: Connected	
Server	~
Policies	v
Last will testament	~
Connect message	^
Send messages 🚺	
Use default o	
Торіс	
Topic Message	
Message	
Message	

- Use default: use predefined default settings.
- Topic: a customized topic to be used for announcements upon connection to an MQTT broker.
- Message: a customized message to be used for announcements upon connection to an MQTT broker.
- Keep: also known as *retain*. Defines if the broker should retain the connection announcement message in the brokers cache so that new subscribers will get this message directly after subscribing.
- QoS: defines the level of service upon message delivery. Go to MOTT QoS settings on page 141 for more information

Configuration example with a default connect message

Network protocols

Client			MQTT Explorer	Q Search
Connect 1 Status: Connected		▼ 172.25.201 ► \$\$Y\$ (48	. 102 3 topics, 309 messages)	
Server	~	► event (62 topics, 62 messages)	
Policies	~			
Last will testament	~			
Connect message	^			
Send messages				
Use default				
Message				
	4			
Кеер				
QoS				
0				

Configuration example with a customized connect message

Network protocols

Client		=	MQTT Explorer	Q Search
Connect				
Status: Connected		V ACCC	(48 topics, 1062 messages) 8ED9C85F	
Server	~	► even	e_Connection = AXIS device nt (59 topics, 59 messages)	ce is connected now.
Policies	~			
Last will testament	~			
Connect message	^			
Send messages				
ACCC8ED9C85F/Device_Connection				
Message				
AXIS device is connected now.				
Keep				
QoS				
0 🔻				

Generic MQTT event publishing

After connecting to an MQTT broker, the user must specify event and event filtering related configurations, which can be found under Settings > System > Events > MQTT events.

The below MQTT configuration shows a typical setup where the Axis device will be configured to send specific events to the MQTT broker, in this example by using **manual trigger** and **virtual input**.

Note

If a specific option is missing in the list of conditions, you may need to enable the functionality and then reboot the device for the condition to appear.

Example: If "Shock detected" is missing, go to **Settings > System > Detectors** and enable shock detection, and then reboot the device. Performing this step will add "Shock detected" to the list of conditions.

The examples in this section are illustrated using an *Eclipse Mosquitto* broker and an MQTT client such as *MQTT Explorer*, which has a graphical user interface.

Network protocols

Publish	
Ise default condition prefix	
Custom condition prefix	
Include condition name	
Include condition namespaces	
Include serial number in payload	
vent filter list	~
Manual trigger	^
Condition	
Manual trigger	
QoS	
0 🔻	
Keep	
None 🔻	
	×
Virtual input	~
Condition	
Virtual input	
QoS	
0 🔻	
Keep	
None 🔻	
	X
+	

Note that if no event is added, the Axis device will not send any events to the MQTT broker. Furthermore, it's only possible to select **virtual input** as an event topic. The virtual input trigger usually consists of 32–64 virtual inputs, and if **virtual input** is selected as an event topic, all available virtual inputs are considered.

Network protocols

-

- Keep: also known as *retain*. Defines if the broker should retain the last state of this message in the brokers cache so that new MQTT subscribers will get the actual state of the event directly after subscription. This setting affects stateful and stateless events of an Axis device. Go to the *Event and action services section* in the VAPIX library for information about if particular events are stateful or stateless.
 - None: all events are sent as non-retained, regardless if they are stateful or stateless events.
 - **Property:** only stateful events are sent as non-retained, regardless if they are stateful or stateless events.
 - All: all stateful and stateless events are sent as retained messages.
- **QoS**: defines the level of service upon message delivery. For more information, see *MQTT QoS settings on page 141*.

To exemplify we have configured the manual trigger as an event to be published to the MQTT broker. The manual trigger is a stateful event, meaning that the manual trigger at all times is in either one of two states; 0 or 1. In the two configurations below we compare two possible scenarios.

- 1. We do not want the broker to keep the last known event state of the manual trigger to be available for newly subscribed MQTT clients.
- 2. We do want the broker to keep the last known event state of the manual trigger to be available for newly subscribed MQIT clients.

Scenario 1

Scenario 2

Network protocols

Publish		Publish	
Use default condition prefix		Use default condition prefix	
Custom condition prefix		Custom condition prefix	
Include condition name		Include condition name	
Include condition namespaces		Include condition namespaces	
Include serial number in payload		✓ Include serial number in payload	
Event filter list	^	Event filter list	
Manual trigger	^	Manual trigger	^
Condition		Condition	
Manual trigger	Ŧ	Manual trigger	
Topic: onvif:Device/axis:IO/VirtualPort		Topic: onvif:Device/axis:IO/VirtualPort	
QoS		QoS	
0 🔻		0 🔻	
Retain		Retain	
None 🔻		Property 🔻	
	×		Х
+		+	

Let's assume that the manual trigger was triggered, and that we have been connected to a broker in order to subscribe to it. As you can see below, we would see the actual MQTT message because we were connected and subscribed to the broker at the same time the

Network protocols

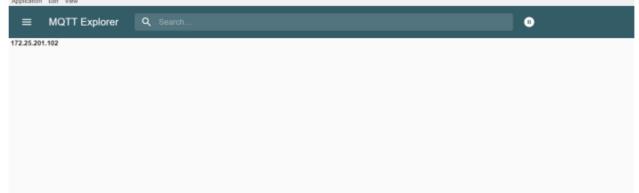
manual trigger triggered.

Application	Edit View			
=	MQTT Explorer	Q Search	•	
▼eve ▼tn	i8ED910B9 nt s:onwif Device ▼ Instaxis ▼ IO ▼ VirtualPort ▼ Source ▼ port	04564763907, "topic": "onvihDevice/axis XOA/IntualPort",	"serial": "ACCC8ED91089", "message": ("source": ("port": "1"). "key": (). "data": ("state": "0"))	19

In case we would not have been connected to the broker with our MQTT client and would have connected at a later point in time, we would still see the last state of the manual trigger event if we had configured the event as "Retain=Property", as can be seen below:



If we had configured the manual trigger event as "Retain=Off", we would not see the last message of the manual trigger and would only receive newly triggered events after we had been connected to the broker in question. Reasonably, no events would be listed: MQTT Explorer Application Edit View

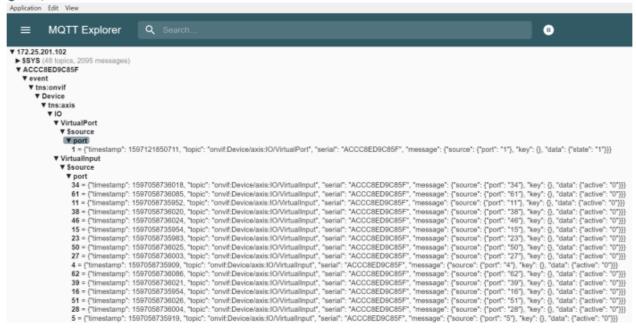


Network protocols

After successful configuration we can see that the Axis device is publishing events for the manual trigger (=VirtualPort) and the 64 virtual inputs.



By expanding the tree structure further, we can see the status of each individual virtual input, identified by the **port** argument.



Include condition name

Enable Include condition name to include the entire event topic name tree instead of just the raw event itself.

Enabled

Network protocols

Publish Use default condition prefix		■ MQTT Explorer Q Search ▼ 172.25.201.102
Custom condition prefix		 ▶ \$SYS (48 topics, 3751 messages) ▼ ACCC8ED9C85F ▼ event ▼ tns:onvif
 Include condition name Include condition namespaces 		▼ Device ▼ tns:axis ▼ IO ▶ VirtualPort (1 topic, 1 message)
Include serial number in payload Event filter list	^	► VirtualInput (64 topics, 64 messages)
Manual trigger	~	
Virtual input	~	
+		

Disabled

Network protocols

Include condition name Include condition namespaces Include serial number in payload	event = {"timesta	E mp": 1597135492122, "topic": "onvif:Device/a
Event filter list	~	
Manual trigger		
Virtual input		

Include condition namespaces Enable Include condition namespaces if the ONVIF topic namespaces should be included.

Enabled

Network protocols

Publish Use default condition prefix		\equiv MQTT Explorer Q Search
Custom condition prefix		▼ 172.25.201.102 ► \$SYS (48 topics, 2986 messages) ▼ ACCC8ED9C85F
 Include condition name Include condition namespaces 		▼ event ▼ tns:onvif ▼ Device ▼ tns:axis
Include serial number in payload		 ▼ IO ▶ VirtualPort (1 topic, 1 message) ▶ VirtualInput (64 topics, 64 messages)
Event filter list	^	
Manual trigger	~	
Virtual input	~	
+		

Disabled

Network protocols

Publish Use default condition prefix Use default condition prefix Custom condition prefix Include condition name Include condition namespaces Include serial number in payload		▼ ACCC: ▼ even ▼ De	48 topics, 3429 messages) 8 ED9C85F t vice	ssage)
Event filter list	^			
Manual trigger	~			
Virtual input	~			
+				

Include serial number in payload Enable Include serial number in payload to include the serial number of the Axis device in the MQTT payload message. This could be used as additional information to identify the sending device.

Enabled

Network protocols

Publish Use default condition prefix Custom condition prefix Custom condition prefix Include condition name Include condition namespaces		▼ 172.25.201.102 > \$\$Y3 (46 logics, 1623 messages) ▼ ACCC6ED9C6SF ▼ vent ▼ trasconvif ♥ trasconvif ♥ trasconvif ♥ 100	
 Include serial number in payload Event filter list 	^		
Manual trigger	~		
Virtual input	~		
+			

Disabled

Network protocols

Publish Use default condition prefix Use default condition prefix Custom condition prefix Include condition name Include condition namespaces Include serial number in payload		<pre>▼ 172.25.201.102</pre>
Event filter list	^	
Manual trigger	~	
Virtual input	~	
+		

Custom MQTT event publishing

In addition to the generic MQTT events that come with predefined topics and payloads, the **Publish MQTT** action rule can be triggered by any of the available device events and send a message with a custom topic and payload.

In the below example the Axis device is publishing a message to the topic "P1375/ManualTrigger/Custom/Topics/" carrying the payload "Manual Trigger is activated". The topic can include up to 1024 characters and the payload's limit is set to 8192 characters.

Network protocols

Rules Schedules Recipients Manual tr	riggers	■ MQTT Exp ▼ 172:25:201.102 ▼ P1375	lorer Q Search	
MQTT_Publish Manual trigger Publish MQTT	^	▼ P1375 ▼ ManualTrigger ▼ Custom ▼ Topics ≅ Manual Trigger i	activated)	
Vse this rule				
Name				
MQTT_Publish				
Wait between actions (max 23:59:59) 00:00:00				
Condition Manual trigger	~			
+				
Action	^			
Publish MQTT	Ŧ			
Торіс				
P1375/ManualTrigger/Custom/Topics/				
Payload	_			
Manual Trigger is activated	.4			
QoS 0 🔻				
Retained				
Save				

This video illustrates how the action rule is set up:

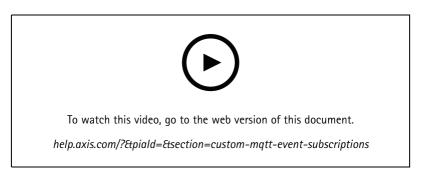
Network protocols



Custom MQTT event subscription

Custom MQTT event subscription is available from AXIS OS 10.7 and onwards and makes it possible for the Axis device to subscribe to a topic when connecting to the MQTT broker. Once subscribed, the Axis device will listen to new incoming messages and will be able to act on it, e.g. by configuration of an action rule in the built-in event system.

See how it's configured in this video:



MQTT subscription data as overlays

With AXIS OS 11.4 and subsequent versions, you can overlay MQTT subscription data onto the video stream. In this section, we guide you through the process of implementing this feature.

First, make sure the device can successfully publish MQTT messages to the broker. In the screenshot below, we have a door monitor that can publish the door status among other information to the broker.



In the Axis device web interface, go to System > MQTT > MQTT client and fill in the necessary information for the MQTT broker based on your setup. Once finished, you should be able to see the MQTT connection status has changed to Connected.

Network protocols

MQTT client				
Connect Connected				
Broker				^
Host	Client ID			
172.25.201.102	client_B8A44F28254E			
Protocol	Clean session			
MQTT over TCP 🔹	LITTO prove			
Port	HTTP proxy			
1883				
Username	HTTPS proxy			
psadmin				
Password	Keep alive interval		Timeout	
	60	s	60	S
	Reconnect automaticall	y		
	Device topic prefix			
	axis/B8A44F28254E			
Connect message				~
Last Will and Testament message				~
				Save
				Save

After that, you can create MQTT overlays in the Axis device. Go to System > MQTT > MQTT overlays and click Add overlay modifier. There are two types of modifiers:

- #XMP: The payload tag. The overlay modifier with #XMP form contains the entire payload of a published MQTT message.
- **#XMD**: The data tag. The overlay modifier with **#XMD** form contains the JSON value of a key in the payload of a published MQTT message.

Let's take a second look at the door monitor. In the published message, there's a section called "announce":

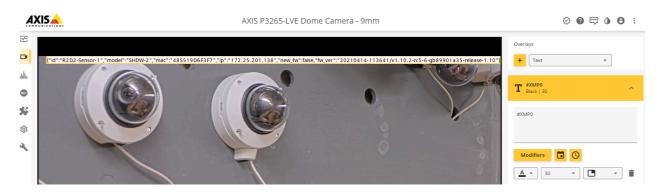
▼ shellies
► R2D2-Sensor-1 (11 topics, 21 messages)
(announce = {"id":"R2D2-Sensor-1","model":"SHDW-2","mac":"485519D6F3F7","p":"172.25.201.138","new fw":false,"fw ver":"20210414-113641/v1.10.2-rc5-6-gb89901a35-release-1.10"})

Enter shellies/announce in the Topic filter. Click Save to subscribe to this topic and use it as an overlay.

Network protocols

,	Add overlay modifier								
	Topic filter								
	shellies/announce								
	Data field								
			Cancel	Save					
This	will generate a modifier called #XM F	20.							
-	+ Add overlay modifier			Go to Overlays					
То	pic filter	Data field	Modifier						
sh	ellies/announce		#XMP0						

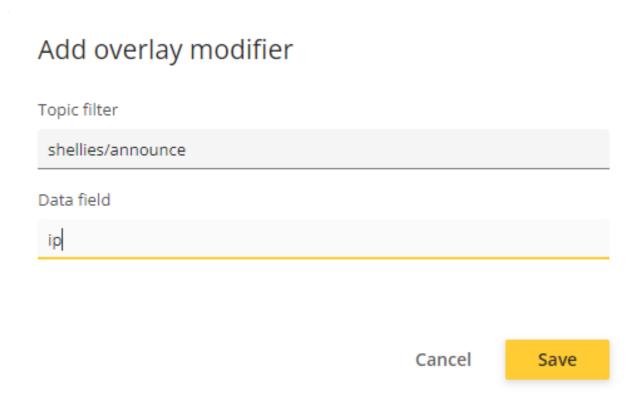
On the same page, click **Overlays**. On the Overlays page, you can see the entire payload of the message as an overlay in the live view.



You can also choose to only overlay a specific part of the message, such as the IP address of the door monitor. That's what the #XMD modifier is used for.

Network protocols

Go to System > MQTT > MQTT overlays and click Add overlay modifier. Enter shellies/announce in the Topic filter and ip in the Data field. Finally, click Save.

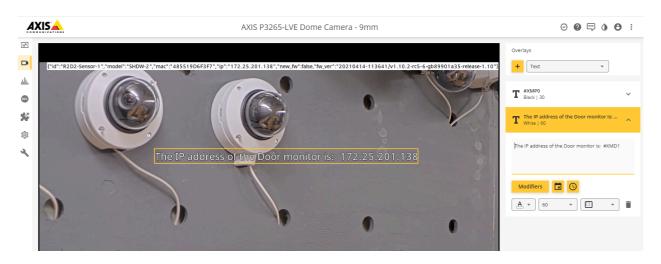


You should now see a new overlay modifier in the list:

+ Add overlay modifier			Go to Overlays
Topic filter	Data field	Modifier	
shellies/announce		#XMP0	
shellies/announce	ip	#XMP1, #XMD1	

On the same page, click **Overlays**. On the Overlays page, create a new text overlay with **#XMD1** in the string. For example, **The IP** address of the door monitor is: **#XMD1**. In the overlay, **#XMD1** will be replaced by the door monitor's IP address.

Network protocols



In some scenarios, subscribed messages include a lot of information in JSON format. Objects might also be nested within other objects, as in the example below.

{

```
"topic": "axis:CameraApplicationPlatform/ObjectAnalytics/Device1Scenario2",
"timestamp": 1710240482163,
"message": {
"source": {},
"key": {},
"data": {
"bike": "0",
"human": "0",
"bus": "0".
"total": "0",
"otherVehicle": "0",
"scenario": "Scenario 2",
"car": "0",
"truck": "0"
}
}
}
```

To overlay the number of humans, for instance, you would enter message.data.human in the overlay modifier Data field.

With AXIS OS 11.8 and later, the MQTT graph overlay feature has been added to ARTPEC- 8 products as well (except the fisheye and panoramic cameras). The steps to create the MQTT overlays are the same aside from the final step to add the overlays in the video stream. Instead of overlaying the MQTT data in text format, it's displayed in graphs.

In the following example, we'll use the MQTT graph overlay to display the room temperature and the battery level, drawn from the door monitor data below:

Network protocols

▼ shellies
▼ R2D2-Sensor-1
online = false
announce = {"id":"R2D2-Sensor-1","model":"SHDW-2","mac":"485519D6F3F7","ip":"172.25.201.138","new_fw":false,"fw_ver":"20210414-113641/v1.10.2-rc5-6-gb89901a35-release-1.10"}
▼ sensor
state = close
tilt = -1
vibration = 0
temperature = 23.00
lux = 104
illumination = twilight
battery = 94
error = 0
act reasons = ["sensor"]

Go to System > MQTT > MQTT overlays and click Add overlay modifier . Create one for the door monitor's room temperature and another for the door monitor's battery level.

Add overlay modifier

Topic filter

shellies/R2D2-Sensor-1/sensor/temperature

Data field

Cancel Save

Network protocols

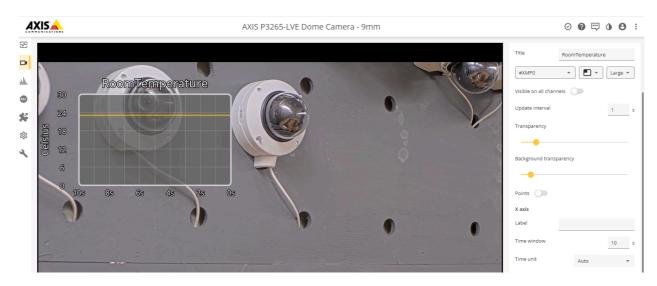
	Add overlay modifier								
	Topic filter								
	shellies/R2D2-Sensor								
	Data field								
			Cancel	Save					
Once	created, both overlay modifiers shou	Id be visible on the list.							
+	- Add overlay modifier			Go to Overlays					
Тор	oic filter	Data field	Modifier						
she	ellies/R2D2-Sensor-1/sensor/temperature		#XMP0						
she	ellies/R2D2-Sensor-1/sensor/battery		#XMP1						

On the same page, click **Overlays**. On the Overlays page, create a new Widget: Linegraph overlay.

Network protocols

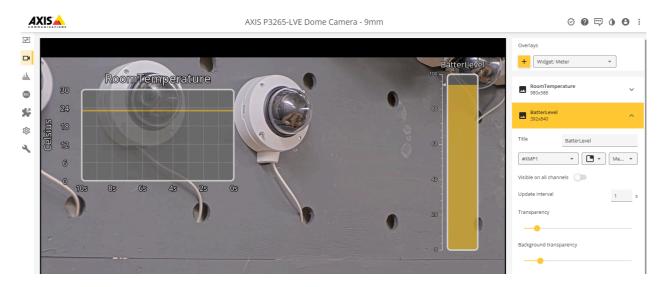
Overla	ys		
+	Text	•	
	Text		
	Image		
	Streaming indicator		
	Widget: Linegraph		
	Widget: Meter		

Select **##XMPO** as the overlay modifier.



Network protocols

Create another graph overlay for the battery level of the door monitor. This time, use Widget: Meter instead. Select #XMP1 as the overlay modifier.



Eclipse Mosquitto

In this section you can read about the configuration steps required to connect an Axis device to an Eclipse Mosquitto MQTT broker in order to publish topics.

Important

The below steps illustrate basic integration and use-cases within a test lab environment. Axis strongly recommends following the provider's guidelines for an integration that maximizes the handling of certificates, tokens, user-credentials and overall cybersecurity in a production environment.

Step 1: Eclipse Mosquitto configuration

For a common Mosquitto MQTT broker configuration based on Linux Ubuntu 18.04, see *this guide*. The steps below cover the configuration in TCP and SSL/TLS mode only.

Network protocols

psadmin@app02: ~ File Edit View Search Terminal Help /etc/mosquitto/mosquitto.conf GNU nano 2.9.3 Place your local configuration in /etc/mosquitto/conf.d/ # A full description of the configuration file is at # /usr/share/doc/mosquitto/examples/mosquitto.conf.example pid_file /var/run/mosquitto.pid persistence true persistence_location /var/lib/mosquitto/ log_dest file /var/log/mosquitto/mosquitto.log log type all include dir /etc/mosquitto/conf.d allow anonymous false #MQTT Server (Login Credentials Required) listener 1883 #MQTT Server (SSL/TLS Encryption w/o certificate) #listener 8883 #protocol mqtt #require_certificate false #MQTT Server (SSL/TLS Encryption) listener 8884 cafile /etc/mosquitto/ca certificates/R2D2MQTTRootCA.crt certfile /etc/mosquitto/certs/R2D2MQTTClient.crt keyfile /etc/mosquitto/certs/R2D2MQTTClient.key #Microsoft Azure Connections #listener 9155 #protocol websockets #Microsoft Azure Connections (SSL/TLS Encryption) #listener 9156 #protocol websockets #cafile /etc/mosquitto/ca_certificates/R2D2MQTTRootCA.crt #certfile /etc/mosquitto/certs/R2D2MQTTClient.crt #keyfile /etc/mosquitto/certs/R2D2MQTTClient.key

Step 2: Axis device configuration

Server configuration

MQTT over TCP

MQTT over SSL

Network protocols

Client		Client	
Connect 🔲		Connect	
Status: Connected		Status: Connected	
Server	^	Server	^
Host		Host	
172.25.201.102		172.25.201.102	
Protocol		Protocol	
MQTT over TCP	▼	MQTT over SSL	Ŧ
Port		Validate server certificate	
1883		Port	
Username		8884	
mqtt_1		Username	
Password		mqtt_1	
•••••		Password	
		•••••	
Policies	~		
Last will testament	~	Policies	~
Connect message	~	Last will testament	~
	-	Connect message	~

Policies configuration

Network protocols

Client	
Connect	
Status: Connected	
Server	```
Policies	
Client id	
AXIS-M1137	
Keep alive interval	
60	
Timeout	
60	
Reconnect automatically	
Clean session	
Last will testament	```
Connect message	

Microsoft Azure (SAS token)

In this section you can read about the configuration steps required to connect an Axis device to an MQTT broker in order to publish topics. For further reading, go to https://docs.microsoft.com/en-us/azure/iot-hub/quickstart-send-telemetry-cli and https://docs.microsoft.com/en-us/azure/iot-hub/ngtt-support.

Important

The below steps illustrate basic integration and use-cases within a test lab environment. Axis strongly recommends following the provider's guidelines for an integration that maximizes the handling of certificates, tokens, user-credentials and overall cybersecurity in a production environment.

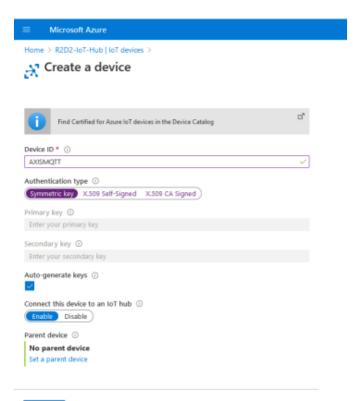
Step 1: Create an IoT device

In order to get started, an IoT device must be created in Microsoft Azure. Follow the steps below in order to proceed.

Network protocols

Microsoft Azure					P Search resources,	services, and docs (G+/)
fome >						
R2D2-IoT-Hub Io	T devices	\$				
P Search (Ctrl+/) «	+ New 🕚	Refresh 🗐 Delete				
X Overview	`					
Activity log	View, create	, delete, and update devices in your IoT Hub	1			
R Access control (IAM)		Field		Operator	Value	
Tags	+ ×	select or enter a property name	~	=	✓ specify constraint value	
Diagnose and solve problems	+ Add a ne	w clause				
Events	Query devic	*				Switch to query editor
ettings						
Shared access policies						
ldentity	DEVIC	ID STATUS	LAST S	TATUS UPDATE (UTC)	AUTHENTICATION TYPE	CLOUD TO DEVICE MESSAGE COUN
Pricing and scale						
Networking						
Certificates						
Built-in endpoints						
- Failover						
Properties						
Locks						
Export template						
xplorers						
Query explorer						
IoT devices						

Network protocols



Save

Network protocols

=	Microsoft Azure						₽ Search resources,	services, and docs (G+/)
Но	me >							
	R2D2-IoT-Hub	loT dev	vices 🖉	>				
٩	Search (Ctrl+/)	« +	New 🕐 R	lefresh 间 Delete				
R	Overview	^						
	Activity log		View, create, d	delete, and update devices in your IoT H	ub.			
ඉ	Access control (IAM)			Field		Operator	Value	
۲	Tags	1.1	+ ×	select or enter a property name	~	• · ·	specify constraint value	
Ð	Diagnose and solve problems		+ Add a new	clause				
۶	Events	1.1	Query devices					Switch to query editor
Set	tings	1.7						
+	Shared access policies							
8	Identity		DEVICE ID	D STATUS	LAST	STATUS UPDATE (UTC)	NUTHENTICATION TYPE	CLOUD TO DEVICE MESSAGE COUNT
0	Pricing and scale		AXISMO	Enabled		S	as	0
٠	Networking							
A	Certificates							
	Built-in endpoints							
- 1	Failover							
部	Properties							
A	Locks							
2	Export template							
Exp	plorers							
,D	Query explorer							
	IoT devices							

After creating a device, obtain the hostname of your Microsoft Azure entity. This can be looked up in the hub overview.

Microsoft Azure		∠P Search resources, services, and docs (G+/)
Home > R2D2-IoT-Hub *		
Search (Ctrl+/) «	\rightarrow Move i Delete O Refresh	
🕅 Overview 🄶	Resource group (change) : R2D2	Hostname : R2D2-IoT-Hubazure-devices.net
Activity log	Status : Active	Pricing and scale tier : S1 - Standard
Access control (IAM)	Current location : North Europe	Number of IoT Hub units : 1
Tags	Subscription (change) : Pay-As-You-Go	Device streams (preview) : https://db-002.northeurope-001.streams.azure-devices.net
Diagnose and solve problems	Subscription ID : ea99bb18-6b15-48fd-ae8a-3511ac491e34	Device streams documentation
	Tags (change) : Click here to add tags	
🗲 Events		۸

Step 2: Generate SAS token

The SAS token can be generated using the Cloud Shell console in Microsoft Azure. In the following example, the password is generated and valid for 3600 seconds. This SAS token is used later on to connect the Axis device to the Microsoft Azure MOTT broker.

Cloud Shell command: az iot hub generate-sas-token -d AXISMQTT -n R2D2-IoT-Hub --du 3600

Network protocols

Microsoft Azure		${\cal P}$ -Search resources, services, and docs (G+/)			
Home >					
R2D2-IoT-Hub 🖉					
P Search (Ctrl+/) «	\rightarrow Move 📋 Delete 🕐 Refresh				
🕅 Overview 🏠	Resource group (change) : R2D2		Hostname :	R2D2-IoT-Hub.azure-devices.net	
Activity log	Status : Active		Pricing and scale tier :	S1 - Standard	
Access control (IAM)	Current location : North Europe		Number of IoT Hub units :		
Tags	Subscription (change) : Pay-As-You-Go Subscription ID : ea99bb18-6b15-48fd-ae8a-3511ac491e34			https://db-002.northeurope-001.streams.azure-devices.net Device streams documentation	
Diagnose and solve problems	Subscription ID : ea99bb18-6b15-48fd-ae8a-3511ao491e34 Tags (change) : Click here to add tags				
🗲 Events	rags (change) . Crocknere to add tags		8		
Settings					
Shared access policies					
💲 identity		Need a way to provision millions of devices?	Need a way to monitor and secure your IoT solution?	Want to learn more about IoT Hub? Check out IoT Hub documentation. Learn how to	
Pricing and scale		IoT Hub Device Provisioning Service enables zero- touch, just-in-time provisioning to the right IoT	Azure Security for IoT (ASC for IoT) is a unified security management service. It provides end-to-	use IoT Hub to connect, monitor, and control billions of Internet of Things assets.	
斜 Networking		hub without requiring human intervention.	end threat analysis and protection across hybrid cloud workloads and your Azure IoT solution.	-	
🔎 Certificates			cloud nonoolas and your Adarc for Solation		
8 Built-in endpoints					
- Failover		We'd love your feedback!	Need to simulate IoT Devices?		
Se Properties		Your valuable feedback will help us to better understand your requirements in order to	development using simulated devices to help		
🔒 Locks		improve IoT Hub.	build and test your project throughout the development lifecycle.		
Export template					
Explorers					
Query explorer		Show	data for last: 1 Hour 6 Hours 12 Hours 10 Day 7 Days	30 Dars	
IoT devices					
Automatic Device Management					
🚔 IoT Edge		loT Hub Usage	Number of messages used	Device to cloud messages	
🕺 IoT device configuration			- 40		
Messaging		Messages used today: 69	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	-70	
File upload					
Bash ∨ © ? © [Ĵ [
Requesting a Cloud Shell.Suo Connecting terminal	ceeded.				
andre@Azure:~\$ az iot hub ge	nerate-sas-token -d AXISMQTT -n R2D2-IoT-Hubdu 3600				
(ure sr=R2D2-IoT-Hub.azure-devices.net%2Fdevices%2FAXISMQ79	4sig=107c0R3%2Bc3mN62BF9R2KWq%2FYRzLaEV0Wcm8K	ithGitI%3Dase=1597150332"		
} andre@Azure:~\$					

Step 3: Axis device configuration With the information provided in Step 1 and Step 2 we can now connect the Axis device to the Microsoft Azure MQTT broker.

Note that the custom condition prefix, disabling the condition name and the custom basepath is mandatory for the Axis device to publish messages.

Network protocols

Client	Publish
Connect 1	Use default condition prefix
Status: Connected	
Status, Connecteu	Custom condition prefix
	devices/AXISMQTT/messages/events/
Server ^	Include condition name
Host	
R2D2-IoT-Hub.azure-devices.net	 Include condition namespaces
Protocol	Include serial number in payload
MQTT over WebSocket Secure	
	Event filter list
Validate server certificate	
Port	
443	Manual trigger
Basepath	Condition
\$iothub/websocket	Manual trigger 💌
Usemame	QoS
R2D2-IoT-Hub.azure-devices.net/AXISMQTT/?api-versior	0
Password	
•••••	Keep None
Policies	X
Policies ^	
Client id	Virtual input
AXISMQTT	Condition
Keep alive interval	Virtual input V
60	QoS
Timeout	0
60	Keep
Reconnect automatically	None V
Clean session	X
Last will testament	+
Connect message 🗸 🗸	

Network protocols

Step 4: Listen to MQTT events

Now we're ready to test our setup. Use the following command in Cloud Shell to listen to incoming MQTT events from the Axis device. The simplest way of testing is to use **manual trigger** in the Axis device.

Cloud Shell Command: az iot hub monitor-events --hub-name R2D2-IoT-Hub

				, services, and docs (G+/)
Home >				
R2D2-IoT-Hub IoT	devices 🖉			
P Search (Ctrl+/) «	🕂 New 🖒 Refresh 📋 Delete			
X Overview				
Activity log	View, create, delete, and update devices in y	our IoT Hub.		
^ዓ ዲ Access control (IAM)	Field	Operator	Value	
🔷 Tags	+ × select or enter a property ne	ime 🗸 📒	✓ specify constraint value	
Diagnose and solve problems	+ Add a new clause			
🗲 Events	Query devices			Switch to query editor
Settings				
Shared access policies				
💲 Identity	DEVICE ID STATU		AUTHENTICATION TYPE	CLOUD TO DEVICE MESSAGE COUNT
Pricing and scale	AXISMQTT Enabl	ed	Sas	0
🚱 Networking				
🔎 Certificates				
 Built-in endpoints 				
🗠 Failover				
2 Properties				
🔒 Locks				
Export template				
Explorers				
Query explorer				
IoT devices				
Automatic Device Management				
🔮 IoT Edge				
IoT device configuration				
Messaging				
File upload				
Bash ∨ ⊙ ? ⊚ [a C Requesting a Cloud Shell.Succe				
Connecting terminal				
andre@Azure:~\$ az iot hub gene	rate-sas-token -d AXISMQTT -n R2	D2-IoT-Hubdu 3600		
{ "sas": "SharedAccessSignatur	e sr=R2D2-IoT-Hub.azure-devices.	net%2Fdevices%2FAXISMQTT&sig=CR5t7	5eow9d9%2FAFAp%2FWA	384PUz33CKtj07reM0rpSoQ%3D&se=1597151275"
	tor-eventshub-name R2D2-IoT-H			
Starting event monitor, use ct	rl-c to stop			
<pre>{ "event": { "origin": "AXISMQTT", "navload": "{\"timesta</pre>	mp\": 1597147326867. \"topic\": `	\"onvif:Device/axis:TO/VirtualPort	\". \"serial\": \"A	۲۲۲۶₽۶۹٬۳۵۶۲٬ \"messapp\": (\"source\": (\"onrt\": \"\\"). \"kev\": (). \"data\": (\"state\": \"@\")))"

Microsoft Azure (certificate authentication)

In this section you can read about the configuration steps required to connect an Axis device to an MQTT broker in order to publish topics. For further reading, go to https://docs.microsoft.com/en-us/azure/iot-hub/quickstart-send-telemetry-cli and https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-mqtt-support.

Important

The below steps illustrate basic integration and use-cases within a test lab environment. Axis strongly recommends following the provider's guidelines for an integration that maximizes the handling of certificates, tokens, user-credentials and overall cybersecurity in a production environment.

Step 1: Certificate authority configuration

In order to configure certificate-based authentication in Microsoft Azure, a trusted root certificate is required, which is used to sign and verify clients and their certificates in return. The below process describes how to add a root certificate in Azure and how to apply the proof-of-possession method in order to prove to Azure that this root certificate should be verified and trusted.

Let's create a root certificate of our choice by running the following commands:

openssl genrsa -des3 -out R2D2AzureRootCA.key 2048 openssl req -new -x509 -days 36500 -key R2D2AzureRootCA.key -out R2D2AzureRootCA.pem

Network protocols

🔺 AXIS Q1659 Events 🛛 🗙 🥂	R2D2-IoT-Hub - Microsoft Azure × +			
← → C ☆ 🏻 portal.azure.com	m/#@axis365.onmicrosoft.com/resource/subscriptions/	ea99bb18-6b15-48fd-ae8a-3511ac491	e34/resourceGroups/R2D2/providers/Microsoft.Devices/IotHubs/R2D	2-IoT-Hub/Certificates
■ Microsoft Azure			✓ Search resources, services, and docs (G+/)	
Home >				
A2D2-IoT-Hub Cer	rtificates 🖈			
	+ Add 🕐 Refresh			
X Overview				
Activity log	You can use this tool to upload and manage your	certificates.		
Access control (IAM)	•			
🗳 Tags	Name	Status	Expiry	Su
Diagnose and solve problems	No results			
🗲 Events				
Settings				
Shared access policies				
💲 Identity				
O Pricing and scale				
🜮 Networking				
🔎 Certificates 🖕				
Bash ∨ © ? © [] [± {} C>			
Requesting a Cloud Shell.Succeede Connecting terminal	ed.			
Generating RSA private key, 2048	es3 -out R2D2AzureRootCA.key 2048 bit long modulus			
e is 65537 (0x10001) Enter pass phrase for R2D2AzureRc	ootCA key:			
Verifying - Enter pass phrase for	r R2D2AzureRootCA.key:			
Enter pass phrase for R2D2AzureRc		-out R2D2AzureRootCA.pem		
You are about to be asked to enter into your certificate request.	er information that will be incorporated			
	hat is called a Distinguished Name or a DN.			
For some fields there will be a d	default value,			
If you enter '.', the field will				
Country Name (2 letter code) [AU] State or Province Name (full name				
Locality Name (eg, city) []:Lund		ons AB		
Organizational Unit Name (eg, sec	ction) []:R2D2 Test Lab			
Common Name (e.g. server FQDN or Email Address []:	YOUR name) []:R2D2 Test Lab			
andre@Azure:~\$				

Download the certificate that was created in the PowerShell and upload the certificate in the certificate store as seen below.

Network protocols

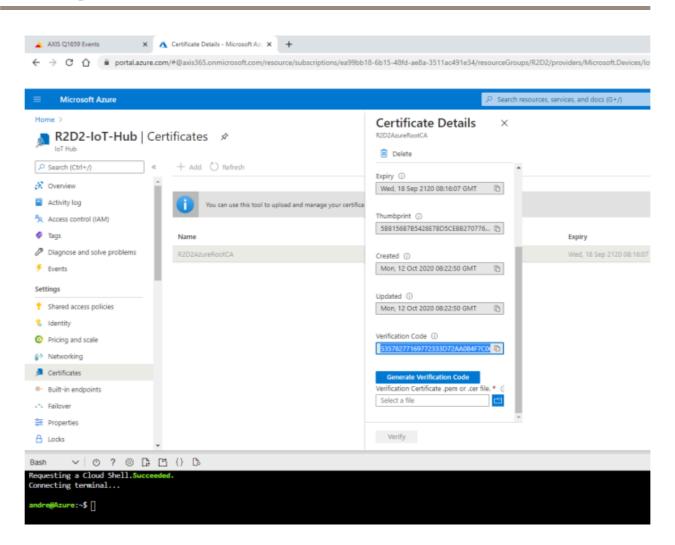
	_					
		- Microsoft Azure × +				
← → C ☆ ● portal.az	zure.com/#@axis365.c	onmicrosoft.com/resource/subscrip	tions/ea99bb18-6b15-48fd-ae8a-3511ac49	1e34/resourceGroups/R2D2/providers/Microsoft.Devices	lotHubs/R2D2-IoT-Hub/Certificates	
Microsoft Azure						
Home >						
AT HUD R2D2-IoT-Hub	Certificates	\$7				
P Search (Ctrl+/)	« + Add	🕐 Refresh				
🛪 Overview	A.					
Activity log	f Yo	ou can use this tool to upload and mana	ge your certificates.			
Access control (IAM)						
🗳 Tags	Name		Status	Expiry	Subject	
Diagnose and solve problems	No results					
🗲 Events						
Settings	1					
Shared access policies						
💲 Identity						
 Pricing and scale 						
🛟 Networking						
🔎 Certificates						
e- Built-in endpoints						
- Failover						
Properties						
🔒 Locks						
Explorers	• • • • • • •					
Bash ∨ 0 ? ⊗ Requesting a Cloud Shell.S						
Connecting terminal	Upload					
andre@Azure:~\$	Download					
	Manage file share	Ipload/Download files				
					Download a file	×
				Enter the fully qualified file	bownload a me bath. Only files persisted in your file share can be downloaded.	
					D2AzureRootCA.pem	
				Dor	vnload Quit	

Network protocols

Microsoft Azure	
Home > R2D2-IoT-Hub >	
Add Certificate	
Learn more about certificates.	
Certificate Name * 💿	
R2D2AzureRootCA 🗸	
Certificate .pem or .cer file. * ()	
"R2D2AzureRootCA.pem"	
Save	
Save	
Save ash ∨ © ? ⊗ []; [2] {} [];	

As you might have noticed, the status of the new root certificate is "Unverified", meaning that we need to prove to Azure that the uploading user is in real possession of the certificate and its authority. Therefore, Azure requires us to sign a new certificate from the root certificate that was uploaded, which includes the below verification code in the CN/Subject of the new certificate.

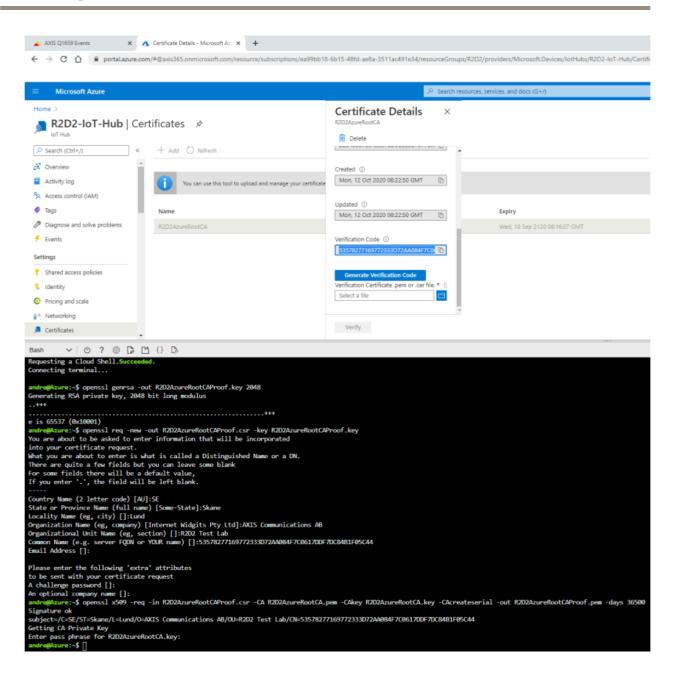
Network protocols



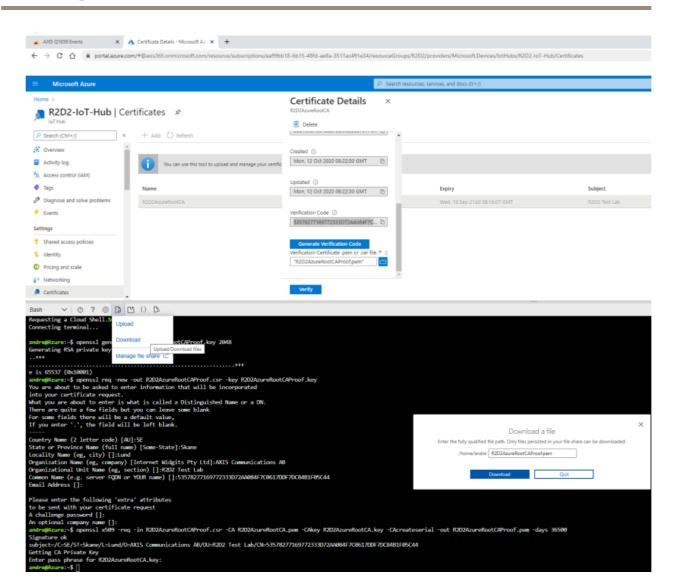
With the help of the below commands, a new certificate is created. Observe that the verification code must be used in the CN/Subject of the new certificate. Note that a challenge password during the certificate creation is not needed.

```
openssl genrsa -out R2D2AzureRootCAProof.key 2048
openssl req -new -out R2D2AzureRootCAProof.csr -key R2D2AzureRootCAProof.key
openssl x509 -req -in R2D2AzureRootCAProof.csr -CA R2D2AzureRootCA.pem -CAkey
R2D2AzureRootCA.key -CAcreateserial -out R2D2AzureRootCAProof.pem -days 36500
```

Network protocols



After the certificate has been successfully created, download it in order to upload it into the certification store to confirm the proof-of-possession. Upon successful verification, the certificate status should change to "Verified".



Network protocols

	R2D2-IoT-Hub - Microsoft Azure X	+ rcc/subscriptions/ea99bb18-6b15-48fd-ae8a-3511ac491e34/resou	rceGroups/R2D2/providers/Microsoft.Devices/lotHubs/F
= Microsoft Azure		<i>م</i>	Search resources, services, and docs (G+/)
Home >			
A R2D2-loT-Hub Cer	rtificates 🖈		
P Search (Ctrl+/) «	🕂 Add 🕐 Refresh		
🕺 Overview 🄶			
Activity log	You can use this tool to upl	oad and manage your certificates.	
R Access control (IAM)			
🔷 Tags	Name	Status	Expiry
Diagnose and solve problems	R2D2AzureRootCA	 Verified 	Wed, 18 Sep 2120 08:16:07 GMT
🗲 Events			
Settings			
Shared access policies			
🐒 Identity			
O Pricing and scale			
A Networking			
🔎 Certificates			

Step 2: Create an IoT device

In order to send MQTT messages from an Axis device to Microsoft Azure using certificate-based authentication, a new IoT device needs to be created with the appropriate authentication method.

Pricing and scale Networking	
Motified Control Control Image Disignose and solve problems View, create, delete, and update devices in your IoT Hub. Events Faild Shared access policies Image Shared access policies Image Pricing and scale Networking Deriver Events Built-in endpoints Failower Properties Device to Status Lost status Query explorer No devices found IoT devices X	
• Lot Hub 2 Search (Cht+/) • Tags • Dignose and solve problems Events tetings Shared access policies • Lentity • Pricing and scale • Networking • Deriver is • Lentity • Networking • Deriver is • Lentiticates • Luit-in endpoints • Failed • Deriver is • Outry devices • Deriver is • Outry devices • Outry devices • No devices found	
 Pags Diagnose and solve problems Events Events Field Operator View, create, delete, and update devices in your IoT Hub. Field Operator Value + × safeed or enter a property name x Select or enter a property name x X Create a device - Microsoft April × x Create a device - Microsoft April × 	
bigginges and solve problems Events tingg shared access policies identity Printing and scale Networking Certificates Built-in endpoints Failover Proparties Locks plorens Query explorer IoT devices AX05 Q1659 Events X View, create, delete, and update devices in your IoT Hub. Faild Operator Value + X select or enter a property name • Add a new clouse Outry devices • Add a new clouse • Device ID status Undry explorer IoT devices Auss Q1659 Events X Create a device - Microsoft Azer: X +	
Events Events shared access policies identity Pricing and scale Networking Cetificates Built-in endpoints Failover Properties Lods ptorers Query explorer Iot devices Adds Qu659 Events X Create a device - Microsoft Asur: X +	
Field Operator Value ttings salect ar enter a property name = gecify constraint value shared access policies i + Add a new clause i + Add a new clause i + Add a new clause Networking Image: Certificates Device ID Status i + Add a new clause Built-in endpoints Device ID Status LAST STATUS UPDATE (UTC) AutHENTIKATION TYPE CLOUD TO Built-in endpoints Failover No devices found No devices found No devices found Image: Certificates Auts Questioner Image: Certificates Image: Certificates Image: Certificates Image: Certificates No devices found Image: Certificates	
Shared access policies Identify Pricing and scale Networking Certificates Built-in endpoints Failover Properties Locks plorers Query explorer Iof devices XXS Q1659 Events X Create a device - Microsoft Acurr, X 4	
Identity Cuerry device: Pricing and scale Networking Certificates Built-in endpoints Failover No devices found Proparties Locks duery explorer Iof devices AX05 Q1659 Events X Create a device - Microsoft Azur: X	
Pricing and scale Networking Certificates Built-in endpoints Failover Proparties Locks doerers Query explorer Iof devices AX05 Q1659 Events X	
Networking Device ID STATUS LAST STATUS UPDATE (UTC) AUTHENTICATION TYPE CLOUD TO Built-in endpoints Failover No devices found No dev	witch to query editor
Certificates Bull-in endpoints Failover Proparties Locks Locks Locks Lot yepforer Int devices XX05 Q1659 Events X Create a device - Microsoft Azur: X +	
Built-in endpoints Failover Forparties Locks Loc	DEVICE MESSAGE COUNT
Failover No devices found Properties Locks	
Properties Locks Morers Query explorer ToT devices	
Locks Iorers Query explorer IoT devices AX05 Q1659 Events × Create a device - Microsoft Apur: × +	
Iorers Query explorer IoT devices AX05 Q1659 Events × Create a device - Microsoft Acure × +	
Query explorer LoT devices AX05 Q1659 Events × A Create a device - Microsoft Apure × +	
IoT devices AV05 Q1659 Events X 🔥 Create a device - Microsoft Apure X 🕂	
AVOS Q1659 Events X 🔥 Create a device - Microsoft Azuro X 🕂	
Microsoft Azure P Search resources, services, and doc	
	G (0+))
me > R2D2-loT-Hub > Create a device	
Find Certified for Azure IoT devices in the Device Catalog	
йсе Ю * ()	
CCC8E68C80A 🗸	
ccc8e68c80A ✓	

Network protocols

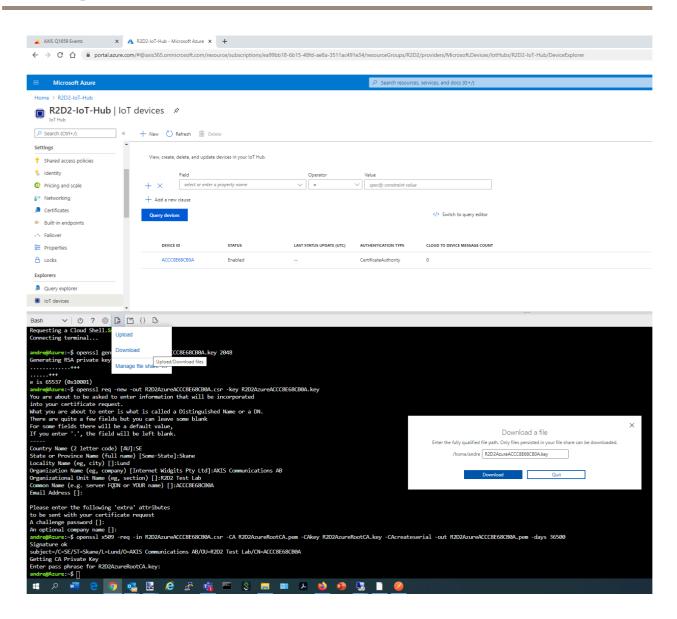
The Axis device must authenticate using a new client certificate that needs to be generated and signed from the root certificate that we uploaded in step 1. The below commands or similar are needed to do so:

openssl genrsa -out R2D2AzureACCC8E68CB0A.key 2048 openssl req -new -out R2D2AzureACCC8E68CB0A.csr -key R2D2AzureACCC8E68CB0A.key openssl x509 -req -in R2D2AzureACCC8E68CB0A.csr -CA R2D2AzureRootCA.pem -CAkey R2D2AzureRootCA.key -CAcreateserial -out R2D2AzureACCC8E68CB0A.pem -days 36500

Observe that the device ID must match the CN/Subject of the client certificate exactly, or the authentication will fail. Note that a challenge password during certificate creation is not needed.

🔺 AXIS Q1659 Events 🛛 🗙 🔥	R2D2-IoT-Hub - Microsoft Azure 🗙	+				
← → C ☆ 🔒 portal.azure.com/	#@axis365.onmicrosoft.com/resou	rce/subscriptions/ea99bb18-6b15-	-48fd-ae8a-3511ac491e3	4/resourceGroups/R2D2/p	providers/Microsoft.Devices/lotHubs/R2D2-loT-Hub/DeviceExplorer	
					services, and docs (G+/)	
Home > R2D2-IoT-Hub						
R2D2-IoT-Hub IoT c	devices 🖉					
	🕂 New 🖒 Refresh 🏢 Delete	2				
Settings						
Shared access policies	View, create, delete, and update de	evices in your IoT Hub.				
💲 Identity	Field		Operator	Value		
Pricing and scale	+ × select or enter a p	roperty name 🗸 🗸	= ~	specify constraint value		
🜮 Networking	+ Add a new clause					
🔎 Certificates	Query devices				Switch to query editor	
Built-in endpoints						
- Failover						
Se Properties	DEVICE ID	STATUS LAST	T STATUS UPDATE (UTC)	AUTHENTICATION TYPE	CLOUD TO DEVICE MESSAGE COUNT	
🔒 Locks	ACCC8E68CB0A	Enabled	c	CertificateAuthority	0	
Explorers						
🔎 Query explorer						
IoT devices						
Bash ∨ (Ů ? ⊚ []∓ 💾	() D					
Requesting a Cloud Shell.Succeeded Connecting terminal	•					
andre@Azure:~\$ openssl genrsa -out		2048				
Generating RSA private key, 2048 b:	it long modulus					
+++ e is 65537 (0x10001)						
andre@Azure:~\$ openssl req -new -ou			0A.key			
You are about to be asked to enter into your certificate request.	information that will be i	ncorporated				
What you are about to enter is what There are quite a few fields but yo		Name or a DN.				
For some fields there will be a det	fault value,					
If you enter '.', the field will be Country Name (2 letter code) [AU]:	SE					
State or Province Name (full name) Locality Name (eg, city) []:Lund						
Organization Name (eg, company) [In Organizational Unit Name (eg, sect		IS Communications AB				
Common Name (e.g. server FQDN or YO Email Address []:						
	attailutor					
Please enter the following 'extra' to be sent with your certificate re		Terminal conta	ainer button			
A challenge password []: An optional company name []:						
	in R2D2AzureACCC8E68CB0A.cs	r -CA R2D2AzureRootCA.pem	-CAkey R2D2AzureRoot	CA.key -CAcreateser	ial -out R2D2AzureACCC8E68CB0A.pem -days 36500	
subject=/C=SE/ST=Skane/L=Lund/0=AX	IS Communications AB/OU=R2D	2 Test Lab/CN=ACCC8E68CB0A				
Getting CA Private Key Enter pass phrase for R2D2AzureRoot	tCA.key:					
andre@Azure:~\$						

Network protocols



Step 3: Axis device configuration

In the last step, the previously created client certificate needs to be uploaded onto the Axis device, and be selected in the MQTT broker configuration. The rest of the configuration is well documented in the Microsoft Azure guidelines.

Security		
Certificates	HTTP and HTTPS	
Client certificates Default (self-signed)	Allow access through HTTP and HTTPS HTTP port HTTPS port 80 443	
+ 0 E	Certificate Default (self-signed)	
Battimore CyberTrust Root Cybertrust Global Root DigiCert Assured ID Root CA DigiCert Assured ID Root G2 DigiCert Global Root G2 DigiCert High Assurance EV Root CA	Save	Install a certificate Select a type of signing method Signing request Private key (PKCS#12)
IEEE 802.1x	Custom-signed firmware certificate	Separate private key Certificate R2D2AzureACCC8E68CB0A.pem
none		Private key Select file R2D2AzureACCC8E68CB0A.key
CA certificate none		Cancel
EAP Identity axis-accc8e68cb0a		
1 EAPOL Version 2 3		
Use IEEE 802.1x		
Save		

Network protocols

Client		
		Publish
Connect (Use default condition prefix
Status: Connected		
		Custom condition prefix
Server	^	devices/ACCC8E68CB0A/messages/events/
fost		Include condition name
R2D2-IoT-Hub.azure-devices.net		Include condition namespaces
Protocol	v	Include serial number in payload
MQTT over SSL		
Port		
8883		Event filter list
Jsername	Cami unersia	
R2D2-IoT-Hub.azure-devices.net/ACCC8E68CB0A/	rapi-versit	
Use password		Manual trigger
assword		Our film
1455		Condition
		Manual trigger 🔻
Certificates	~	QoS
		0 💌
Client certificate		Keep
R2D2AzureACCC8E68CB0A		None 💌
CA certificate		
Baltimore CyberTrust Root 🔻		×
Validate server certificate		
		+
Policies	^	
March Id		Save
ACCC8E68CB0A		2446
Keep alive interval		
60		
Timeout		
60		
Reconnect automatically		

Step 4: Listen to MQTT events

Now we're ready to test our setup. Use the following command in the Cloud Shell to listen to incoming MQTT events from the Axis device. The simplest way of testing is to use the **manual trigger** in the Axis device.

Cloud Shell command: az iot hub monitor-events --hub-name R2D2-IoT-Hub

Network protocols

Go to Microsoft Azure (SAS token) on page 171 and see the example in Step 4 for more information.

Amazon Web Services (AWS)

In this section you can read about the configuration steps required to connect an Axis device to an Amazon Web Services (AWS) MQTT broker in order to publish topics. For further reading, go to *https://docs.aws.amazon.com/iot/latest/developerguide/mqtt.html#mqtt-sdk*.

Important

The below steps illustrate basic integration and use-cases within a test lab environment. Axis strongly recommends following the provider's guidelines for an integration that maximizes the handling of certificates, tokens, user-credentials and overall cybersecurity in a production environment.

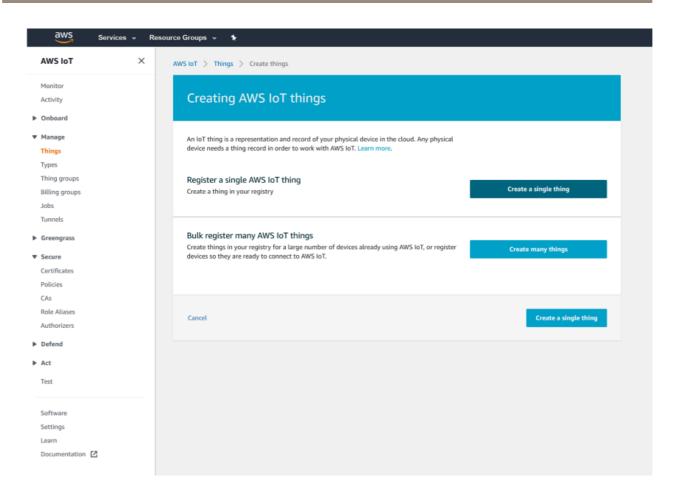
Step 1: Create a thing policy

Before we start creating a thing device in AWS, we want to configure the thing policy first. The thing policy is basically access and connection rights given to a device upon creation. The below example illustrates a policy that lets the Axis device connect and publish messages.

Network protocols

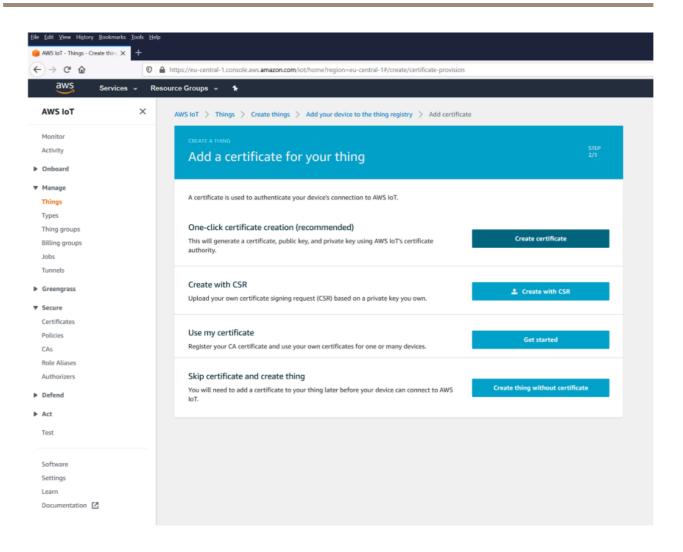
aws Services - Resourc	e Groups 🗸 🔥
AWS IoT ×	Create a policy
Monitor	
Activity	
Onboard	Create a policy to define a set of authorized actions. You can authorize actions on one or more resources (things, topics, topic filters). To learn more about IoT policies go to the AWS IoT Policies documentation page.
	Name
Manage	axismqttdevice
Things Types	
Thing groups	
Billing groups	Add statements
Jobs	Policy statements define the types of actions that can be performed by a resource. Advanced mode
Tunnels	
	Action
Greengrass	lot:Connect
Secure	Resource ARN
Certificates	arn:aws:iot:eu-central-1:148231931467:client/\${iot:Connection.Thing.ThingName}
Policies	ananzaolea en ar 11462 i 23 140 Adeny (foteometrona ingraing)
CAs	Effect
Role Aliases	Z Allow Deny
Authorizers	Kenove
Defend	Action
Act	iot:Publish
ACT	IOCPUDIISN
Test	Resource ARN
	arn:aws:iot:eu-central-1:148231931467:topic/*
Software	
Settings	Effect
Learn	Allow Deny Remove
Documentation 🖸	
	Add statement
	Create

Step 2: Create IoT device (thing) After creating the thing policy, it is time to create the actual device. AWS IoT Core is providing access via certificate-based authority rather than credential-based authentication. So, a certificate and a private key are generated during the process of creating a thing as well.



aws Services - Resource	se Groups 👻 🔭
AWS IoT \times ,	WS IoT > Things > Create things > Add your device to the thing registry
Monitor Activity IP Onboard	Add your device to the thing registry
Manage Things Types Thing groups Billing groups Jobs	This step creates an entry in the thing registry and a thing shadow for your device. Name axismqttdevice
Tunnels Greengrass Secure Certificates Policies	Apply a type to this thing Using a thing type simplifies device management by providing consistent registry data for things that share a type. Types provide things with a common set of attributes, which describe the identity and capabilities of your device, and a description. Thing Type axismqttgroup Create a type
CAs Role Aliases Authorizers Defend Act Test	Add this thing to a group Adding your thing to a group allows you to manage devices remotely using jobs. Thing Group Groups / Create group Change
Software Settings Learn Documentation 🔀	Set searchable thing attributes (optional) Enter a value for one or more of these attributes so that you can search for your things in the registry. This thing type does not have searchable attributes Set non-searchable thing attributes (optional)
	You can use thing attributes to describe the identity and capabilities of your device. Attribute key Value Provide an attribute key, e.g. Manufacturer Provide an attribute value, e.g. Acme-Corporation Add another Show thing shadow Cancel Back

Network protocols



Observe that the certificate and private key must be uploaded to the Axis device. If the Axis device should validate the AWS MQTT broker as well, the Amazon Root CA must be uploaded on the Axis device too. Furthermore, make sure that the certificates are activated by toggling the button as illustrated in the screenshot.

Network protocols

aws Services - Resourd	Groups 🗸 🛧	
AWS IoT ×		
Monitor	Contribute and all	
Activity	Certificate created!	
Onboard		
▼ Manage		
Things	Download these files and save them in a safe place. Certificates can be retrieved at any time, but the private and public keys cannot be retrieved at any time.	ved
Types	after you close this page.	
Thing groups	In order to connect a device, you need to download the following:	
Billing groups	A certificate for this	
Jobs Tunnels	thing Od653019e0.cert.pem Download	
	A public key 0d653019e0.public.key Download	
Greengrass	A private key 0d653019e0.private.key Download	
▼ Secure		
Certificates	You also need to download a root CA for AWS IoT:	
Policies	A root CA for AWS IoTDownload	
CAs Role Aliases	Deactivate	
Authorizers		
Defend		
▶ Act	Cancel Done Attach a polic	
Test	Uniter Done Attach a police	
Software		
Settings		
Learn		
Documentation		

Here we attached the policy that we created in Step 1 to the thing device we are creating. After doing this, the thing is ready and it is time to configure the Axis device.

Network protocols

<u>File Edit View History Bookmarks</u>	_		
😑 AWS IoT - Things - Create thing 🗙	+		
← → ୯ ŵ	0	https://eu-central-1.console.aws. amazon.com /iot/home?region=eu-central-1#/policy/attach	
aws Services	~ Res	ource Groups 🗸 🔥	
AWS IoT	×	AWS IoT $>$ Things $>$ Create things $>$ Add your device to the thing registry $>$ Add certificate $>$ Add authorization to certificate $>$ Add authorization t	rtificate
Monitor Activity		CREATE A THING Add a policy for your thing	STEP 3/3
Onboard			
▼ Manage			
Things		Select a policy to attach to this certificate:	
Types		Q. Search policies	
Thing groups			
Billing groups Jobs		axismqttdevice	View
Tunnels			
 Greengrass 		1 policy selected	Register Thing
▼ Secure			
Certificates			
Policies			
CAs			
Role Aliases			
Authorizers			

Step 3: Axis device configuration

With the information provided in step 1 and step 2 we can now connect the Axis device to the AWS MQTT broker.

Note that AWS IoT Core enforces a hard limit on the length of the topic expression so we simply started with only including the condition name to keep the topic short.

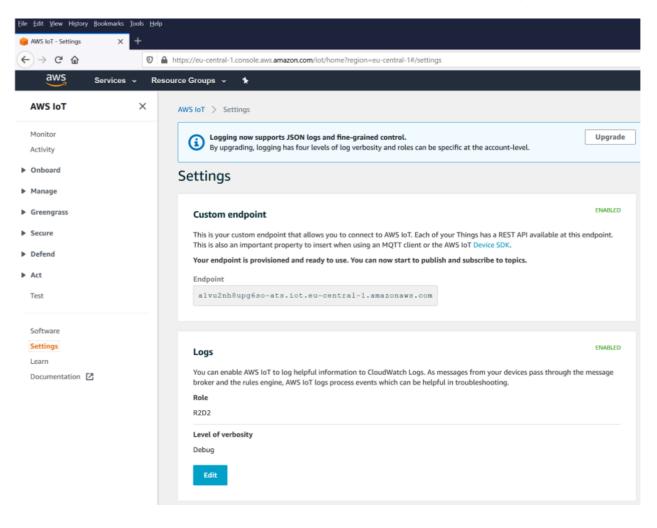
Client	1	Publish
Connect (I)		Use default condition prefix
Status: Connected		
		Custom condition prefix
Server	^	
		Include condition name
Host		Include condition namespaces
a1vu2nh8upg6so-ats.iot.eu-central-1.amazonaw	/s.com	Include serial number in payload
Protocol		
MQTT over SSL	*	Event filter list
Validate server certificate		Event litter list
Port		
8883		Manual trigger
Username		
		Condition
Password		Manual trigger 🛛 🔻
		QoS
		0 🔻
Certificates	~	Keep
		None 🔻
Client certificate		X
0d653019e0 🔻		
CA certificate		
		Virtual input
Validate server certificate		Condition
_		Virtual input 🔻
Policies	^	QoS
		0 🔻
Client id		Keep
axismqttdevice		None 💌
Keep alive interval		X
60		
Timeout		
60		+
Reconnect automatically		

Network protocols

Step 4: Listen to MQTT events

Now we are ready to test our setup. With the help of Amazon CloudWatch we can verify if the Axis device can send MQTT messages to the AWS cloud successfully.

First, make sure you have logging enabled. This will then result in the AWS cloud logging connection attempts.



By using the Amazon CloudWatch service, the AWSIoTlogs log group will reveal connection attempts and whether or not MQTT actions such as publishing or subscribing were successful.

Network protocols

t Yew History Bookmarks	+				
) С 6	0 6	https://eu-central-1.console.aws.amaz	cn.com/cloudswitch/home/region=eu-central-11logs/2/og-groups/log-groups/WSIoiLogs/log-events/1607560-cc25-4018-9009-8oe63e124484_148231931467_cf33FfitterPatternS3DE26startS3D-1800000	… 등 ☆	👱 lin, 🖽
aws Services	~ Res	source Groups 👻 🔸	ζ.	ADHIN/andrebt@axis.com @ 1.	. • Frankfurt • Support
fWatch	CloudW	Vatch > CloudWatch Logs > Log g	roups > AWSintLogs > 1e5075e0-ec25-4918-9009-fbe63e324e84_148231931467_0		Switch to the original inter
boards					
ам 🛛 🖸	Log	g events		C Actions	Create Metric Filter
IFFICIENT 0	Q	Filter events		Clear 1m 30m 1h	12h Custom 🖪 🤇
		Timestamp	Message		
roups			There are older events to load. Load more.		
	•	2020-08-21708128140-828+02100	2020-08-21 06128148.828 TMACID1F0656657-0870-f9ab-0904-61244408947 PRINCIPALID10F0713444405ee00760031a190a44d8e2302a90cf65200Ff0538cca50b065307 [INF0] EVENTINGTI Client Connect MESSAGEIconnect Status: SUCCESS		
		2020-08-21708:29:53.899+02:00	2020-08-21 06:29:53.099 TBACEDI:A1eb0bib-0b76-650a-9730-04005555dec29 PRINCIPALIDI:bic?134adatdstee00740031a190adadbc23b2a9bcfd520ffb53bcca5bb65307 [18F0] EV011:Publishivent T0PIGW#EACC68E06G85F/event PE55A6E:Publishin Statu	s: SUCCESS	
	•	2020-08-21708:29:53.966+02:00	2000-08-21 06120153.066 TBACEIDISCOSIABD-5073-1/BS-b179-4CAB5db76d1 MEINCIPALIDISbC713Addand5ee08760031a190adadBe2Db2009Cfd520ffb538cca5bb65307 [IBF0] EVRIT:Publiohevent T091DHWE:ACCCEB06035F/event MESSAGE:PublishIn Statu	s: SUCCESS	
	- F	2020-08-21708:29:53.966+02:00	2020-08-21 06:20:53.066 TBACEID:6c654806-5073-3FB6-bi79-4c805d8576d1 PRINCIPALID:8c7134a64a63ee08760031a100a4a48e025620876f530fFb538cca55865387 [INF0] EVRIT:PublishEvent MESSAGE: IpAddress: 85.235.16.11 SourcePort: 60614		
luses	•	2020-08-21708:29:53.967+02:00	2020-08-21 06:20:53.067 TRACED:bbf85730-f063-0f3b-d8x5-G1adic&ca8 PRINCIDALID:bbc?134ad4ad5ee0876a031a190a4ad8e23b2a0bcfd520ffb53acca5bb65307 [INFO] EVENT:PublishEvent T071CNME:ACCC8E09C85F/event MESSAGE:PublishIn Statu	s: SUCCESS	
Lens		2020-08-21708:29:53.967+02:00	2020-08-21 06:29:53.067 THACLED:bb/H5730-f063-0f3b-dBa5-631adicBccaB PRINCIPALID:bbc7313-484a0d5ee0874a031a190a4adBe23b2a0bc/d520ffb53Bcca5bb65307 [ENTO] ENTIT:bublishEvent MISSAGE: B5.275.10.11 SourcePort: 40614		
		2020-08-21708:29:53.967+02:00	2020-08-21 06:29:53.067 TBACED:9fbefa5e-9bae-a667-fbb+b7033554093b PRINCIPALID:bc71344a04see0074031a19ba4adbe23b2a05cfd520ffb53bcca5bb65307 [INFO] DVRNT:PublishEvent MISSAGE: B5.235.16.11 SourcePort: 40614		
Мар		2020-08-21708:29153.967+02:00	2020-06-21 06129153.067 TWACEEDIca251bba-d2ff-666a-5abd-22230d148545 PREMINITURALEDIb0c711444abd5ec0076a031a190a4ad0e23b2a9bc6d520ffb538cca5b685307 [EMF0] EVENTIVublishEvent T0P1CHWEIACCC08D9C085F/event MESSAGEIPublishEn Status	s: SUCCESS	
		2020-08-21708:29:53.967+02:00	2020-08-21 06129153.067 TBACELD1ca251bba-d2Ff-666a-5abd-22230d148545 PRIDCIDALID19b27134ad4a045ee0876a031a198a4a082202a9bcfd530fFb538cca50645307 [DXF0] EVENT1vbblishEvent MI554681: IpAddress: 85,235.16.11 SourcePort: 40514		
er Insights NW		2020-08-21708:29153.976+02:00	2020-08-21 06129153.976 TBACEED1200Fa890-19C3-7092-1603-4997a6640a82 PRINCIPALID130C7134ad4a9d5ee08740031a190a4a882302a90cfd520fFD538cca50b65307 [IXFO] EVENT FWD13hEvent T0P10MPE1ACC08E0FC85F/event PE55A6E(PublishIn Status	st SUCCESS	
085	•	2020-08-21708129153.976+02100	2020-08-21 06129153.976 TBACEED1200Fa090-19C3-7092-1603-4x97a6640a02 PRIDCIDALID130-C7134ad4a045ee0076a031a190a4a0822002a09C60520Ff0538cca50665307 [DRG] EVENT1/vb112hEvent ME55A6E1 1pAd0ress1 85,235-16-11 50urcePort1 40614		
nance Monitoring	- F	2020-08-21T08:29:53.978+02:00	2020-08-21 06:20:53.978 TRACED:2647e1f6-f6a4-3970-0443-923Bacd70c67 PRINCIPALD:10:7314ad4a045ee0074a031a190aadaBe23b2a0bcfd520ffb53bcca5bb65307 [INFO] DVENT:PublishEvent T0PICNAME:ACCC0800C035F/event MESSAGE:PublishIn Statu	s: SUCCESS	
ics www	•	2020-08-21708:29:53.978+02:00	2020-06-21 06129:53-978 TRACED:10321c8a-700a-63b3-6fe2-ff8dda64c367 PRIXCIDALID:10c7134ad4a045ee00746031a190a4ad0e23b2a9bcf6528ffb538cca5b665307 [INFO] EVENT:hvblishEvent T0P1CNWE:ACCC0809C85F/event MESSAGE:hvblishIn Status	s: SUCCESS	
es	•	2020-08-21708:29:53.978+02:00	2020-00-21 05:29:53.978 TBKETD:17faBB66-c559-09c2-7857-2fe1733bb279 PRINCIPALTD:09c7134a44a95ee00076a031a190a4adbc23b2a9bcfd520ffb530cca5bb5307 [IBF0] EVENT:PublishEvent MSSSAGE: IpAddress: 85.295.16.11 SourcePert: 40614		
utor Insights	•	2020-08-21708:29:53.978+02:00	2020-00-21 05:29:53.978 TBKEED:71e59996-b359-R2d7-b38-R2d7-b38-288485d896d3 PRINCIPALID:59c7134a44a95ee008760031a19ba4adBc23b2a9bcfd520ffb538cca5bb65397 [IBF0] EVHT:PublishEvent T0P1DNME:ACCC0ED9C087/event HESSAGE:PublishIn Statu	s: SUCCESS	
	•	2020-08-21708:29:53.978+02:00	2020-08-21 06:29:53.070 TINCED:0000073-f20b-2546-0d2d-00539a13066 PRINCIPALD:0bc7134ad4ad5e007A0331a190A4dBe23b2a05cfd530ffb530cca50665307 [DNF0] EVENTPublishEvent T091DHMELRCCEBBSCBSF(event MESSAGE:PublishEn Status	s: SUCCESS	
	•	2020-08-21708:29:53.979+02:00	2020-08-21 06:29:53.979 TBACED:5753092 TBACED:5753097 TBACED:57530972-0058-1fb:e9726-1f339a00fBac PRURCIPALD:b572134ad4ad5e007Au031a19bahadBac2b2a0bcfd520ffb538cca5bbc5307 [DRO] EVENT:PublishEvent T091DAME:ACCCBBDCBSF/event MESSAGE:PublishEn Status	s: SUCCESS	
es	- P	2020-08-21708:29153.979+02:00	2020-08-21 06/29153.979 TRACED157530672-0658-3Fbe-0726-1F33900FBac PRINCIPALD19bc7134ad4ad5ee0074a031a190A4aBe23b2a90cfd520fFb538cca50665307 [DRF0] EV0HTPublishEvent MESSAGE: IpAddress: 85.235.16.11 SourcePort: 40614		
	•	2020-08-21706:29:53.983+02:00	2020-08-21 061291531:003 TMACELDI-00301046-06ec-0154-0151-053005240f67 PEDICEPALEDI-052015464005ce0037600510310400408223020cf63200f765384cca58605387 [EMO] EVENTIVALISAEtroalDistribution		
	•	2020-08-21708:29:53.984+02:00	2020-08-21 06129153-084 TRACEID12797668-66cd-9951-9Mob-Fed3537adsfa PRINCIPALID106/213Madaad5ee08764031a39Mad8823b2a9bcfd538(f538(ca50b65307 [INF0] EVENTIVALISAEvent TOEICNWEIACCOE09605F/event PRESAME inabilishin Status	s: SUCCESS	
	•	2020-08-21708:30:54.807+02:00	2820-08-21 06130154.007 TMACEDD10961242-6C09-0230-9504-677/3332053 PRINCIPALID10F07134044095600760511a39044082302005105200715580530053007 [IMF0] EVENTIVAD130Event PRESSA0E: IpAddressi: 85.235.16.11 SourcePort: 40614		
		2020-08-21708:30:54.807+02:00	2420-08-21 06:30:54.007 TRACEDD:896f1742-6c09-a230-9dba-6c7c73d32a53 PRINCIPALID:30c713Mad4a9d5ee0076a031a390AndBe23b2a90cfd528ff5538cca65b65307 [INT0] EVENT:NublishEvent T001CNNE:ACCERE90C057/event/Device/ID/VirtualPort/By	source/port/1 MESSAGE:PublishIn Sta	itus: SUCCESS
		2020-00-21 06:30:54.007 TRACEID:a0	NFT/14-668-328-98a-6C72182337 PERCEPAED:00:723448648596887548311439844882952486-6529Ffb316cca5869387 [DW0] PUBLI-PublishEvent T097209E1ACCCEEDREPS/voont/Dwice/20/Virtual/PublishEvent/Source/port/1 PESAEE:PublishEvent/Source/port/1 PESAEE	SUCCESS	Copy
			No newer events at this moment. Auto retry obused. Resume		

IBM Watson

In this section you can read about the configuration steps required to connect an Axis device to an IBM Watson MQTT broker in order to publish topics. For further reading, go to *https://developer.ibm.com/articles/iot-mqtt-why-good-for-iot/*.

Important

The below steps illustrate basic integration and use-cases within a test lab environment. Axis strongly recommends following the provider's guidelines for an integration that maximizes the handling of certificates, tokens, user-credentials and overall cybersecurity in a production environment.

Step 1: Create IoT device Follow the steps below to create an IoT device.

φ BM Wats ← → C		a x
IBM Wats	n lof Plutform O 2009mit. Dis choya	(2)
	Brown Action Device Types Interfaces	
• •	Browse Devices	
A	Al Devices Elaginose	
® .7	This table shows a summary of all devices that have been added. It can be filtered, organized, and searched on using different oritoria. To get started, you can add devices by using the Add Device buttor, or by using APL.	
8	new Sealar State	
۲	Q Sanch by Device ID Device Timeser Version Hardware Version Handware Vers	
	٩ڦ٥	
	You don't have any devices. Grade a device.	

n IoT Platform										() a
Browse Action D	evice Types Interfaces									÷ ш
Add Device	•									
O Identity			Device Informati	on		Security			Summary	
	Select a device type	for the device that you are ad	ding and give the device a uniq	ue ID.						
	Device Type	AXIS								
	Device ID	P1375								
										Cancel
Browse D	ovicos									
All Devices	Diagnose									
		een added. It can be filtered, o ee Add Device button, or by us	rganized, and searched on usir ing API.	g different						
Q Search by Device II)									Device Simulator 💿 🛙
Device	ID Status	Device Type	Class ID	Date Added	Descriptive Location	Added By	Device Class	Firmware Version	Hardware Version	Manufacturer
						d₿b				
					You	don't have any devices.				

Add Device									
©								—0	
Identity			Device Information		Security			Summary	
			ore information about the device for identification						
	Serial Number	Enter Serial Number	Manufacturer	Enter Manufacturer					
	Model	Enter Model	Device Class	Enter Device Class					
	Description	Enter Description	Firmware Version	Enter Firmware Version					
	Hardware Version	Enter Hardware Version	Descriptive Location	Enter Descriptive Location					
	Add Metadata	0							
									Back
Drawaa D	ouiooo								
Browse D									
All Devices	Diagnose								
		een added. It can be filtered, organized, he Add Device button, or by using API.	, and searched on using different						
Q Search by Device II									Device Simulator (
Device									
	ID Status	Device Type	Class ID Date Added	Descriptive Location	Added By	Device Class	Firmware Version	Hardware Version	Manufacturer

a 42cyhjinternetofthings	sibmcloud.com/dashboard/devices/browse/add				() <i>ada</i> e
Browse Action Dev	ice Types Interfaces				U 1D: 42e
Add Device	There are two cetters for selecting a device author Auto-generated authentication toke (default) Allow de service to generate an authentication to be characters and products. The teken is more authentication of the second second second characters and products. The teken is more of the device registration process.	n Self-provide dauthentication token Provide your own authentication token for this device. The token must be between 8 and 36 characters and contain a mix numeric lowercase and uppercase letters, numbers, and symbols, which	ی Security	O Sutronary	
	Authentication Taken Rgs/PV/Smrs/Holdor/HKI Make a note of the generated taken. Lost aut tokens cannot be recovered, Takens are enc being stored. Authentication token are en	hentication			
					Back Nex

toT Platform × +					-
42cyhj.internetofthings.ibmcloud.com/d	ashboard/devices/browse/add				1
n IoT Platform					(2) 12d2@axis. (2) 1D: 42cytij
Browse Action Device Types Int	erfaces				
Add Device					
o <u> </u>				®	
Identity		vice Information	Security	Summary	
Verify the	t the following information is correct then select Done				
Device Typ AXIS	0				
AXIS Device ID					
P1375					
View	fetadata				
Security T	Aken				
RgvPVc5	mw3Hbdu6mK4x6				
					Back Finish

🕸 IBM Watson IoT	Platform × +			- ø ×
€ → C ■	42cyhj.internetofthings.ibmclo	oud.com/dashboard/devices/drilldown	n/AXISP1375/returnTo-/devices/browse	\$ 🙆 i
IBM Watson I	loT Platform			⑦ 12:d2@axis.com ⑧ 10:42:yhj ⑧
←	Back			
De De	evice Drilldown -	P1375		
A	vice Credentials	Device Credentials		
@ Con	nnection Information	You registered your device to t	the organization. Add these credentials to the device to connect it to the platform. After the device is connected, you can ravigate to view connection and event details.	
,√ Rec	cent Events			
Stat	ite	Organization ID	42c)hi	
Ø Dev	vice Information	Device Type	AXIS	
(\$ Met	tadata	Device ID	P175	
Dia	ignostics	Authentication Method		
Con	nnection Logs	Authentication Token	Rg/PVC5mv2Hbdu6mK4x6	
Dev	vice Actions			
		Authentication tokens	s are non-recoverable. If you misplace this token, you will need to re-register the device to generate a new authentication token.	
		Find out how to add these cre	selectisks to your desires 2	
		Connection Informati		
		Basic connection information a		
			P1375	
			AXIS	
			14 aug 2020 07:55	
			r2d2@axis.com	
		Connection Status	Disconnected	

Network protocols

Step 2: Axis device configuration With the information and settings provided by the IoT device creation in Step 1, we can now connect the Axis device to the IBM MQTT broker. Again, below is a typical example.

Note that the custom condition prefix in the MQTT events and the disabling of the condition name are mandatory for the Axis device to publish messages.

Client	Publish
Connect []	Use default condition prefix
Status: Connected	
olatas. comisciela	Custom condition prefix
-	iot-2/evt/event-id-1/fmt/json
Server ^	Include condition name
Host	
42cyhj.messaging.internetofthings.ibmcloud.com	Include condition namespaces
Protocol	Include serial number in payload
MQTT over SSL	
	Event filter list
Validate server certificate	
Port	
8883	Manual trigger
Usemame	Condition
use-token-auth	Manual trigger 💌
Password	QoS
Policies	Keep None
Client id	X
d:42cyhj:AXIS:P1375	
Keep alive interval	Virtual input
60	
Timeout	Condition Virtual input
60	Pirtue input
Reconnect automatically	QoS
	0 🔻
Clean session	Keep
	None 🔻
Last will testament 🗸 🗸	X
Connect message V	+

Network protocols

Step 3: Listen to MQTT events

IBM Watson Cloud does not possess a built-in MQTT client for subscribing to events in the cloud. We therefore use MQTT Explorer. In order for MQTT Explorer to connect to the IBM MQTT broker, it is necessary to first generate API keys to allow access. This is described in the following images.

	ashboard/apps/browse					
n IoT Platform					3 10 10	
Browse IBM Cloud Apps					+ Generate	
Browse API Keys	5				Type the app description to search for	
		ha filterad				
organized, and search on using different cri or by using the APL For more information a	that have been added for the organization. It can l eria. To get started, you can add API keys by clickin out adding API keys, see <u>API key connection</u> .	ng Generate API Key,				
Key C		Description 0	Role C	Expires 🗘		
			O results			
			00			
			0 est			
			There are no API Keys			
			Generate API Key			
IoT Platform × +						
A 42cyhj.internetofthings.ibmcloud.com/d	ashboard/apps/browse/add					
42cyhjintemetofthingsibmcloud.com/d	ashboard/apps/browse/add					
	ashboard/apps/browse/add				o in	
42cyhjintemetofthingsibmcloud.com/d	schboard/apps/browse/add				© ^a ir	
42cyhjintemetofthingsibmcloud.com/d n IoT Platform	achboand/apps/browse/add				© g	
42cyhjunternetotthings/bmcloud.com/d in IoT Platform Browse IBM Cloud Apps					© g	
42cyhjintemetofthingsibmcloud.com/d n IoT Platform	• <u> </u> 0				© a	
42cyhjunternetotthings/bmcloud.com/d in IoT Platform Browse IBM Cloud Apps	O Information Permissions				© a	
42cyhjunternetotthings/bmcloud.com/d in IoT Platform Browse IBM Cloud Apps	• <u> </u> 0				© =	
42cyhjunternetotthings/bmcloud.com/d in IoT Platform Browse IBM Cloud Apps	O Information Permissions				© =	
42cyhjunternetotthings/bmcloud.com/d in IoT Platform Browse IBM Cloud Apps	Orange O				© d	
42cyhjunternetotthings/bmcloud.com/d in IoT Platform Browse IBM Cloud Apps	Information Permissions Description MF to p tapice Or Or Or Or On				© =	
42cyhjunternetotthings/bmcloud.com/d in IoT Platform Browse IBM Cloud Apps	Orange O				© ª	
42cyhjunternetotthings/bmcloud.com/d in IoT Platform Browse IBM Cloud Apps	Information Permissions Description MF to p tapice Or Or Or Or On	5			© m	
42cyhjunternetotthings/bmcloud.com/d in IoT Platform Browse IBM Cloud Apps	Information Permissions Description MF to p tapice Or Or Or Or Or On					
42cyhjunternetotthings/bmcloud.com/d in IoT Platform Browse IBM Cloud Apps	Information Permissions Description MF to p tapice Or Or Or Or Or On				Cancel	
42cyhjunternetotthings/bmcloud.com/d in IoT Platform Browse IBM Cloud Apps	Information Permissions Description MF to p tapice Or Or Or Or Or On					
Opplannet/Megubinduation/stands In Carl Pratern Brease IM Cloud Ages Generate API Key	Permission Permissio				Caust	
Copy nemestime under dealers In of Peatern Terr Dealers In of Classif Ages Generate API Keys Browse API Keys	Permissions P					
Copy nemestime under dealers In of Peatern Terr Information Apps Generate API Key Browse API Keys	Permissions P				Canot	
Copy nemestime under dealers In of Peatern Terr Information Apps Generate API Key Browse API Keys	Permission Permissio				Canot	
Copy intermetching dendadations In of Pattern Inset Inset	Permissions P	he filtered, og Generate APJ Køy,			Concel Type the app description to search for	
Copy nemestime under dealers In of Peatern Terr Information Apps Generate API Key Browse API Keys	Permissions P			ppm ô	Canot	
Copy intermetching dendadations In of Pattern Inset Inset	Permissions P	he filtered, og Generate APJ Køy,	ne C Onto	Epres Q	Concel Type the app description to search for	
Copy intermetching dendadations In of Pattern Inset Inset	Permissions P	he filtered, og Generate APJ Køy,		Eater 0	Concel Type the app description to search for	
Copy intermetching dendadations In of Pattern Inset Inset	Permissions P	he filtered, og Generate APJ Koy,	0 results	Egén Ĉ	Concel Type the app description to search for	
Copy intermetching dendadations In of Pattern Inset Inset	Permissions P	he filtered, og Generate APJ Koy,	0 results	Epres Q	Concel Type the app description to search for	
Copy intermetching dendadations In of Pattern Inset Inset	Permissions P	he filtered, og Generate APJ Koy,		toire °	Concel Type the app description to search for	
Copy intermetching dendadations In of Pattern Inset Inset	Permissions P	he filtered, og Generate APJ Koy,	0 results	Egen û	Concel Type the app description to search for	

Network protocols

on IoT Platform					@ 10
Browse IBM Cloud Apps					
Generate API Key	⊚®				
	Information Permissions				
	The application will have access				
		uplication -			
	For more information about roles, see	User, application, and gateway roles.			
					Back Generate
Browse API Key					Type the app description to search for
This table shows a summary of the API ke organized, and search on using different of	ys that have been added for the organization. It o riteria. To get started, you can add API keys by cl about adding API keys, see <u>API key connection</u> .	can be filtered, icking Generate API Key,			
or by using the API. For more information	about adding API keys, see <u>API key connection</u> .				
Кеу С		Description	Role 🗘	Expires 🗘	
		Unscriptorin V	O results	Data A	
			0 mm b		
			0€0		
			There are no API Keys		
			There are no API Keys Generate API Key		
staf Fieldern × +					
hat Platform X 4 • 429/bj.interretofthings.bmcloud.com/	tanboard/appu/treess/add				
	dashboardrappe/browse/add				© ª
42cyhj.internetofthings.ibmcloud.com/	dashboardrappu/trowns/add				¢ ª
42cyhjinternetofthingsibmcloud.com/	stanikoanstrapper/treasas/add				© m
42cyhjinternetofthingsibmcloud.com/					t d
420yhjinternetothings.bmcloud.com 101 Platform Browse IBM Cloud Apps The API key has Authentication tokons are non-re	been added.	ed to re-register the AFI kay to			đ g
42xps interretoftlings benchaud conv in 1of Platform Browne IBM Cloud Ages The API key has Authentication tokens are non-re generate a new authentication to	been added. coverable. If you misplace this taken, you will ne				© a
2cp/janamentoffings binchod cons m fol Flatform Brews 104 Cloud Apps The API Key hass Anthenication bakes are non-re- generate a new attendication to Generated Details	been added. coverlab. If you mitigate this taken, you will ne keen. API Key J	Information			© å
Copy internet/Mings lands of one on Lof Plattern Brever Bit Cloud Ages The API key has Anthenisticiton bitmes are none-automationalitation Generated Details Antrey Copy	been added. Coverdate. If you mitigace this taken, you will ne taken. API Key J cover/housis @ Description M	Information NOTTExplorer			© d
Copy interventitings landed core An Lof Plattere Brown Ibit Cloud Ages The API key hass Anterinction taking an income Generated Details Arter = -0.007 Anterinstin Tax = -0.007	been added. coverdate. Type mitigkaon this taken, yee will ne know. APLKey J. Johd H. Gyael & Berefere M. Jaket H. Gyael & Berefere Status	Information IQTTExplorer Landard Application			© #
Copy interventitings landed core An Lof Plattere Brown Ibit Cloud Ages The API key hass Anterinction taking an income Generated Details Arter = -0.007 Anterinstin Tax = -0.007	been added. coverdate. Type mitigkaon this taken, yee will ne know. APLKey J. Johd H. Gyael & Berefere M. Jaket H. Gyael & Berefere Status	Information IQTTExplorer Landard Application			0 ²
Copy internet/Mings lands of one on Lof Plattern Brever Bit Cloud Ages The API key has Anthenisticiton bitmes are none-automationalitation Generated Details Antrey Copy	been added. coverdate. Type mitigkaon this taken, yee will ne know. APLKey J. Johd H. Gyael & Berefere M. Jaket H. Gyael & Berefere Status	Information IQTTExplorer Landard Application			© 2
Copylanteentottings benched core an Cof Plattere Brown IBSC Cloud Ages The API key hass Anterinction teams are noted automatication Generated Details Miter # 2000 Anterination Team	been added. coverdate. Type mitigkaon this taken, yee will ne know. APLKey J. Johd H. Gyael & Berefere M. Jaket H. Gyael & Berefere Status	Information IQTTExplorer Landard Application			
Copylanteentottings benched core an Cof Plattere Brown IBSC Cloud Ages The API key hass Anterinction teams are noted automatication Generated Details Miter # 2000 Anterination Team	been added. coverdate. Type mitigkaon this taken, yee will ne know. APLKey J. Johd H. Gyael & Berefere M. Jaket H. Gyael & Berefere Status	Information IQTTExplorer Landard Application			
Copy internet of they keed out on the Plattern Brown IBC Cool Ages The API key hass Anterfaciation taking as noted autority in the application taking as noted autority in the application taking as noted as noted the grant and a source of the grant and the take, year generative as our takes	been added. coverdate. If you mitigkator this taken, you will ne know. API Key J Johd H. Claw @ Bureform M Johd H. Claw @ Bureform M made analysis for a second seco	Information IQTTExplorer Landard Application			Yee APT Key Add Acuther 2
Copy interventifing landed core And La Plattere Interventification data Interventification Interventification Interventification Concernated Details Miler Miler Marka surver of theme means marka surver of theme marka marka surver of theme marka mark	been added. corentale. If you mitglace this taken, you will nee them. Autor 11, (good @ new result. Autor 11, (good @ new result. Autor 11, (good @ new result. Autor 11, (good @ new result. Martin exception the API to	Information 90TEstater Handradgetation ever			
Copy interventifing landed core And La Plattere Interventification data Interventification Interventification Interventification Concernated Details Miler Marken surventification Interventification Interve	been added. corentale. If you mitglace this taken, you will nee them. Autor 11, (good @ new result. Autor 11, (good @ new result. Autor 11, (good @ new result. Autor 11, (good @ new result. Martin exception the API to	Information 90TEstater Handradgetation ever			Yee APT Key Add Acuther 2
Copy interventifing landed core And La Plattere Interventification data Interventification Interventification Interventification Concernated Details Miler Marken surventification Interventification Interve	been added. coverdate. If you mitigkator this taken, you will ne know. API Key J Johd H. Claw @ Bureform M Johd H. Claw @ Bureform M made analysis for a second seco	Information 90TEstater Handradgetation ever			Yee APT Key Add Acuther 2
Copy interventifing landed core And La Plattere Interventification data Interventification Interventification Interventification Concernated Details Miler Marken surventification Interventification Interve	been added. corentale. If you mitglace this taken, you will nee them. Autor 11, (good @ new result. Autor 11, (good @ new result. Autor 11, (good @ new result. Autor 11, (good @ new result. Martin exception the API to	Information 90TEstater Handradgetation ever			Yee APT Key Add Acuther 2

With the newly generated API keys we can connect to the IBM MQTT broker. See example settings below.

Network protocols

+ Connections	MQTT Connection	mqtt://42cyhj.messaging.internetofthings.ibmo	loud.com:8
IBM Watson Cloud IoT mqtt.//42cyhj.messaging.internet	Name		-
test.mosquitto.org mqtt.//test.mosquitto.org:1883/	IBM Watson Cloud IoT	Validate certificate	Encryption (tls)
	Protocol Host mqtt:// 42cyhj.messa	ging.internetofthings.ibmcloud.com	Port 8883
	Username a-42cyhj-5ows7vouts	Password _+m357_NNzFH_(Ipw	d! ©
	DELETE 📋 🏟 ADV	ANCED	Осоллест

The below subscription topic is mandatory to configure, otherwise no events will be seen. The MQTT client ID must consist of your IBM cloud entity followed by a customizable string (e.g. "mqtt") that a user can define.

+ Connections	MQTT Connection mqtt://42cyhj.messaging.internetofthings.ibmcloud.com:8
IBM Watson Cloud IoT mqtt://42cyhj.messaging.internet	Subscription + ADD
test.mosquitto.org mqtt://test.mosquitto.org:1883/	iot-2/type/+/id/+/evt/+/fmt/+
	MQTT Client ID a:42cyhj:mqtt CERTIFICATES

Upon successful connection, events should be sent from the Axis device. The simplest way of testing this is to use the **manual** trigger in the Axis device.

Network protocols

4 MQTT Explorer	
Application Edit View	
■ MQTT Explorer Q Search	0
▼ 42cyhj.messaging.internetofthings.ibmcloud.com	
▼ iot-2	
▼ type	
▼ AXIS	
▼ id	
▼ P1375	
▼ evt	
▼ event-id-1	
▼ fmt	
(json = {"timestamp": 1597394187216, "topic": "onvif:Device/axis:IO/VirtualPort", "serial": "ACCC8ED9C85F", "message"	": {"source": {"port": "1"}, "key": {), "data": {"state": "0"})})

Google Cloud Platform (GCP)

In this section you can read about the configuration steps required to connect an Axis device to a Google Cloud Platform (GCP) MQTT broker in order to publish topics. For further reading, go to *https://cloud.google.com/iot/docs/how-tos/gateways/mqtt-bridge* and *https://cloud.google.com/iot/docs/how-tos/mqtt-bridge*.

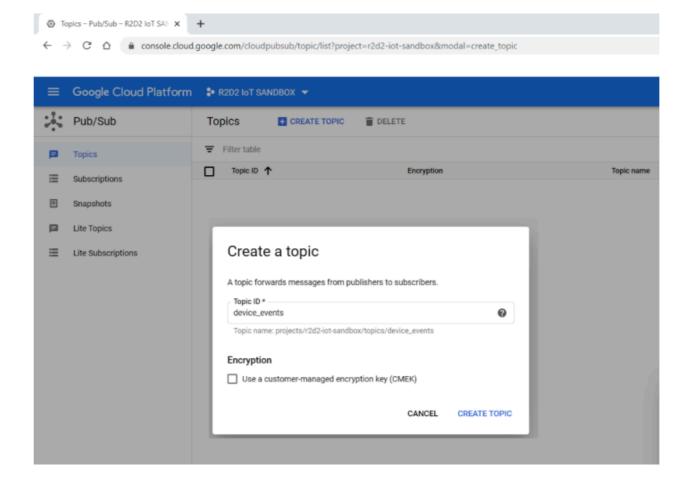
Important

The below steps illustrate basic integration and use-cases within a test lab environment. Axis strongly recommends following the provider's guidelines for an integration that maximizes the handling of certificates, tokens, user-credentials and overall cybersecurity in a production environment.

Step 1: Pub/Sub configuration

In the first step, we will use Google's Pub/Sub hub. Pub/Sub is used to create topics so that a device can publish its MQTT events to GCP. In addition, one can also subscribe directly to the topics.

• н	ome – R2D2 IoT SANDBOX – Go 🗙	+		
\leftarrow	C 🛆 🔒 console.clou	ud.google.com/home/dashboard?proj	ect=r2d2-iot-sandbox	
≡	Google Cloud Platform	n 🚦 R2D2 IoT SANDBOX 🔫		
A	Home	> DMMENDATIONS		
ŵ	IoT Core			
	Pub/Sub	COVID-19. Learn more		
:	1 45/545			
PROD	ucts 🔨		Project info	:
<u>کې</u>	Marketplace	î.	Project name R2D2 IoT SANDBOX	
50	Billing		Project ID r2d2-iot-sandbox	
RPI	APIs & Services	>	Project number 514219820656	
Ť	Support	>	ADD PEOPLE TO THIS PROJECT	
Θ	IAM & Admin	>	→ Go to project settings	
۲	Getting started			
۲	Security	>	Resources	:
\mathbb{A}	Anthos	>	This project has no resources	



© ™	© Topics - Pub/Sub - R2D2 IoT SAL ★						
$\leftarrow \neg$	← → C 🏠 🔹 console.cloud.google.com/cloudpubsub/topic/list?project=r2d2-iot-sandbox&cloudshell=false						
=	Google Cloud Platform	n 🔹 R2D2 IoT SANDBOX 👻 Q Search products and resources					
*	Pub/Sub	Topics 📑 СREATE ТОРІС 📑 DEI	LETE				
P	Topics	Filter table					
=	Subscriptions	Topic ID 1	Encryption	Topic name			
-		device_events	Google-managed	projects/r2d2-iot-sandbox/topics/device_events			
Ð	Snapshots						
	Lite Topics						
:=	Lite Subscriptions						

⊙ s	Subscriptions - Pub/Sub - R2D2 X +				
← -	← → C △ a console.cloud.google.com/cloudpubsub/subscription/list?project=r2d2-iot-sandbox				
≡	Google Cloud Platform	PR2D2 IoT SANDBOX	•		
÷.	Pub/Sub	Subscriptions	CREATE SUBSCRIPTION	DELETE	
₽	Topics	= Filter table			
=	Subscriptions	Subscription ID 1	Delivery ty	pe	Topic name
٥	Snapshots	No subscriptions to display			
	Lite Topics				
≡	Lite Subscriptions				
00	Create subscription – Pub/Sub – 🛛 🗙	+			
← -	→ C △ ê console.clo	ud.google.com/cloudpubsu	← → C 🏠 🔒 console.cloud.google.com/cloudpubsub/subscription/create?project=r2d2-iot-sandbox		

≡	Google Cloud Platform	🗣 R2D2 IoT SANDBOX 👻
:	Pub/Sub	← Create subscription
	Topics	A subscription directs messages on a topic to subscribers. Messages can be pushed to
≡	Subscriptions	subscribers immediately, or subscribers can pull messages as needed.
0	Snapshots	device_events
P	Lite Topics	Subscription name: projects/r2d2-iot-sandbox/subscriptions/device_events
≡	Lite Subscriptions	projects/r2d2-iot-sandbox/topics/device_events
		Delivery type
		If Pull, subscribers must request delivery. If Push, Pub/Sub delivers messages as soon as they are published.



Network protocols

O device_events - Pub/Sub - R2D2 × +						
← → C ☆ e console.cloud.google.com/cloudpubsub/subscription/detail/device_events?project=r2d2-iot-sandbox						
≡	Google Cloud Platform	🗣 R2D2 IoT SANDBOX 👻				
*	Pub/Sub	device_events	🖍 EDIT	• VIEW MESSAGES	CREATE SNAPSHOT	REPLAY MESSAGES
	Topics	Outranintian dataile				
=	Subscriptions	Subscription details				
		Subscription name		projects/r2d2-ic	t-sandbox/subscriptions/dev	rice_events 🖪
0	Snapshots	Topic name		projects/r2d2-lo	t-sandbox/topics/device_eve	ents 🗖
	Lite Topics					
≡	Lite Subscriptions					
		Unacked message count				
		6.05 6.10	6:15 6:20	6.25 6.30	6.35 6.40 6.	45 6.50 6.55
		Delivery type		Pull		
		Subscription expiry			pires in 31 days if there is no	activity.
		Acknowledgement deadline @		10 Seconds		
		Subscription filter		-		
		Message retention duration Retain acknowledged message	s	7 Days		
		Message ordering 🔞	-	Disabled		
		Dead lettering 🔞		Disabled		
		Retry policy 🔞		Retry immediate	ely	
		Labels		-		

Step 2: GCP MQTT bridge configuration In this step of the configuration we add a registry point so we can add devices that later on can publish topics. We will use the IoT Core tab for the configuration.

 Home - R2D2 IoT SANDBOX - G: x + ← → C △ ● console.cloud.google.com/home/dashboard?project=r2d2-iot-sandbox 						
≡	Google Cloud Platfor	m 🛟 R2D2 IoT SANDBOX 👻				
•	Home	> DMMENDATIONS				
ŵ	IoT Core					
4	Pub/Sub	> COVID-19. Learn more				
PROD	ucts 🔨		Project info	I		
È	Marketplace	-	Project name R2D2 IoT SANDBOX			
	Billing		Project ID			
RPI	APIs & Services	,	r2d2-iot-sandbox Project number			
*	Support		514219820656			
0	IAM & Admin		ADD PEOPLE TO THIS PROJECT			
*	Getting started		ightarrow Go to project settings			
j.	Security	,				
۵ ۵	Anthos	, ,	Resources This project has no resources	:		
	Anthos	, in the second se	тна ргојем наз но гезовноез			
0	Registries – IoT Core – R2					
÷	→ C ☆ 🇯 d	onsole.cloud.google.com/iot/registr	ies?project=r2d2-iot-sandbox			
≡	Google Cloud	Platform 💲 R2D2 IoT SANDE	30X 👻			
ណ្ណ	loT Core	Registries CREATE	REGISTRY			
Ŧ	= Filter registries					
	Registry ID 🕇			Region		
Nor	No registries to display					

Network protocols



≡	Google Cloud	d Plat	Form 💲 R2D2 IoT SANDBOX 🔫
M	IoT Core	÷	Create a registry

Define how devices in this registry will send data to Cloud IoT Core. After you create your registry, you can start adding devices to it. Learn more

Registry properties

Registry ID axis_device_registery
Permanent identifier for your registry. 3–255 characters. Start with a letter. You can also include numbers and the following characters: + . % ~
Region europe-west1

Determines where data is stored for devices in this registry. Choice is permanent.

Cloud Pub/Sub topics

Cloud IoT Core routes device messages to Cloud Pub/Sub for aggregation. You can route messages to different topics and subfolders in Cloud Pub/Sub based on the type of data in the messages. Learn more

```
    Select a Cloud Pub/Sub topic

    projects/r2d2-iot-sandbox/topics/device_events
```

Device telemetry events will be published to this topic by default.

```
+ ADD ADDITIONAL TOPIC
```

SHOW ADVANCED OPTIONS

CREATE CANCEL

213

Create a registry – IoT Core – R20 × +
← → C △ ▲ console.cloud.google.com/iot/registries/new?project=r2d2-iot-sandbox
≡ Google Cloud Platform 🗜 R2D2 IoT SANDBOX 👻
IoT Core Create a registry
projector zaz lot duration, topico, dettoe_evento
Device telemetry events will be published to this topic by default.
+ ADD ADDITIONAL TOPIC
Device state topic (optional)
Device state data will be published to your selected topic on a best-effort basis, as well
as to the default MQTT state topic (if your devices use MQTT protocol). Learn more
Select a Cloud Pub/Sub topic projects/r2d2-iot-sandbox/topics/device_events
projecta/r_cc_nor adirabox/ topica/ device_eventa
Protocols
Select the protocols that your devices will use to connect to Cloud IoT Core. Learn more
ЧТТН
Cloud Logging
Set the default logging for all devices in this registry. You can apply a different setting or debug at the device level. <u>Learn more</u>
O Disabled
No device data stored.
Captures device errors, such as failed connection attempts and failed publishes. Does not include authentication errors.
O Info
MQTT only. Captures device errors (except authentication errors) and includes all lifecycle events, such as device connections and disconnections.
Debug
Captures all device activity in a highly verbose log statement. Recommended for device troubleshooting.
CA certificate (optional)
Input method
Enter manually
O Upload
Certificate value
Certificate value
You can add more certificates after you've created this registry.
You can add more certificates after you ve created this registry. A HIDE ADVANCED OPTIONS
CREATE CANCEL

Network protocols

Registry details - IoT Core - R2D: × +							
← -	← → C 🏠 🌲 console.cloud.google.com/iot/locations/europe-west1/registries/axis_device_registery/overview?project=r2d2-iot-sandbox						
≡	Google Cloud Platform	R2D2 IoT SANDBOX 🔫					
ŵ	IoT Core	Registry details 🖍 EDIT REGISTRY 👕 DELETE REGISTRY					
	Registry details	Registry ID: axis_device_registery ~					
0	Devices	Region europe-west1					
	Gateways	Protocol MQTT					
_		Cloud Logging Debug View logs					
í í í	Monitoring						
		Debug logging is enabled for the entire registry.					
		Cloud Pub/Sub topics					
		A registry can have 1 or more topics for publishing device telemetry and state events. Add or edit topics					
		Pub/Sub topics					
		Topic name Topic type 🕐 Subfolder					
		projects/r2d2-iot-sandbox/topics/device_events Default telemetry -					
		- Device state -					
		CA certificates					
		A registry can have up to 10 CA certificates for device authentication. Learn more					
		ADD CERTIFICATE					
		Certificate value					
		No certificates added to the registry					
		▲ CA CERTIFICATES					

Step 3: GCP device configuration After creating the registry point, we can now bind devices to it. The devices will then be able to publish topics.

 O Devices - IoT Core - R2D2 IoT SA × + ← → C △ ● console.cloud.google.com/iot/locations/europe-west1/registries/axis_device_registery/devices?project=r2d2-iot-sandbox 				
≡	∃ Google Cloud Platform SANDBOX →			
f î,	IoT Core	Devices CREATE A DEVICE		
⊞	Registry details	Registry ID: axis_device_registery		
0	Devices	europe-west1		
	Gateways	Devices are things that connect to the Internet directly or through a gateway. Learn more		
<i>4</i>	Monitoring	= Enter exact device ID		
		Device ID		
		No devices to display in this registry		
		Cloud IoT Core documentation		

Network protocols

Create a device – IoT Core – R2	+ +
← → C △	le.cloud.google.com/iot/locations/europe-west1/registries/axis_device_registery/devices/new?project=r2d2-iot-sandbox
\equiv Google Cloud Plat	tform 🔹 R2D2 IoT SANDBOX 👻
စ္သံနဲ့ loT Core	← Create a device
Registry details	Device ID ACCC8E68CB0A
Devices	Enter a permanent ID that starts with a lowercase letter. Must end in a letter or number.
Gateways	You can also include the following characters: + . % ~
益 Monitoring	Device metadata (optional)
	You can set custom metadata, such as manufacturer, location, etc. for the device. These can be used to query devices in this registry. Learn more
	+ ADD ATTRIBUTE
	✓ COMMUNICATION, CLOUD LOGGING, AUTHENTICATION
	CREATE CANCEL

Network protocols

Google Cloud Platfo	rm 📑 R2D2 IoT SANDBOX 👻
loT Core	Create a device
 Registry details Devices 	Device metadata (optional) You can set custom metadata, such as manufacturer, location, etc. for the device. These
E Gateways	can be used to query devices in this registry. Learn more + ADD ATTRIBUTE
Monitoring	Device communication
	If blocked, all communications from the device will be rejected by Google Cloud. Blocking a device may be useful if it's defective or not configured. Allow
	O Block
	Choose a log setting for this device. Will override the registry default for this device only.
	Use registry default setting Disabled No device data stored.
	 Error Captures device errors, such as failed connection attempts and failed publishes. Does not include authentication errors. Info
	MQTT only. Captures device errors (except authentication errors) and includes all lifecycle events, such as device connections and disconnections. Debug Captures all device activity in a highly verbose log statement. Recommended for device troubleshooting.
	Authentication (optional) Specify the public key that will be used to authenticate this device. You can leave the key empty, but devices will not be able to connect to Google Cloud without a key. Learn more
	Input method Enter manually
	Upload Public key format RS256
	Public key value
	Public key expiry date (optional) Expires on:
	Date CET 💼

In order to authenticate a device in GCP, a JWT token needs to be used as password for each device, and GCP also needs to bind the public key to decrypt the traffic and authenticate the device correctly.

Network protocols

About the JWT token

The JWT token is generated at a later stage using the public and private key.

About the device public key

In order to create a device in GCP, a public key is needed to authenticate and decrypt traffic from the device. For a test environment, public and private keypairs can be generated in the GCP console directly.

openssl genpkey -algorithm RSA -out rsa_private.pem -pkeyopt rsa_keygen_bits:2048 openssl rsa -in rsa_private.pem -pubout -out rsa_public.pem

Read out the public and private key from the GCP console editor. Use the public key directly to create the device. The public key and the private key is also used later on to sign the JWT token.

Network protocols

00	Create a device – IoT Core – R2D 🗙 🕇	
←	→ C ☆ @ console.cloud.google.cr	com/iot/locations/europe-west1/registries/axis_device_registery/devices/new?project=r2d2-iot-sandbox&cloud
=	Google Cloud Platform	
đ		
999	IoT Core	Create a device
⊞	Registry details	Choose a log setting for this device. Will override the registry default for this device only. Learn more
0	Devices	Use registry default setting
æ	Gateways	O Disabled No device data stored.
ă	Monitoring	 Error Captures device errors, such as failed connection attempts and failed publishes. Does not include authentication errors.
		 Info MQTT only. Captures device errors (except authentication errors) and includes all lifecycle events, such as device connections and disconnections.
		Debug Captures all device activity in a highly verbose log statement. Recommended for device troubleshooting.
		Authentication (optional)
		Specify the public key that will be used to authenticate this device. You can leave the key empty, but devices will not be able to connect to Google Cloud without a key. Learn more
		Input method
		Enter manually Upload
		Public key format
		RS256
		Public key value
		Public key expiry date (optional) Expires on:
		Date CET 🛗
		COMMUNICATION, CLOUD LOGGING, AUTHENTICATION
		CREATE CANCEL
2	CLOUD SHELL Terminal (r2d2-iot-sandbox) ×	1 -
Your C	me to Cloud Shell! Type "help" to o Cloud Platform project in this seas	get started. sion is set to <u>r2d2-iot-sandbox</u> .
andreb	gcloud config set project [PROJECT bt@cloudshell:~ (r2d2-iot-sandbox) 	r ID]" to change to a different project. δ openssl genpkey -algorithm RSA -out rsa_private.pem -pkeyopt rsa_keygen_bits:2048
andreb		δ openssl rsa -in rsa_private.pem -pubout -out rsa_public.pem
	ng FSA Key bt@cloudsholl:~ (r2d2-iot-sandbox)@	5 I

Network protocols

© 0	reate a device - IoT Core - R2D: × +	
← -	C C C C console.cloud.google	$. com/iot/locations/europe-west1/registries/axis_device_registery/devices/new?project=r2d2-iot-sandbox \& cloudshow and the sandbox and the s$
≡	Google Cloud Platform	R2D2 IoT SANDBOX 👻
,	IoT Core	← Create a device
Ħ	Registry details	Choose a log setting for this device. Will override the registry default for this device only. Learn more
8	Devices	O Use registry default setting
۲	Gateways	O Disabled No device data stored.
<u> </u>	Monitoring	Error Captures device errors, such as failed connection attempts and failed publishes. Does not include authentication errors. Mono Info Mono
		Octug Captures all device activity in a highly verbose log statement. Recommended for device troubleshooting.
		Authentication (optional) Specify the public key that will be used to authenticate this device. You can leave the key empty, but devices will not be able to connect to Google Cloud without a key. Learn more Iput method Public key format Public key format Public key format Public key value Pub
2	CLOUD SHELL Editor (Built with Eclipse Theia)	CREATE CANCEL
	File Edit Selection View Go H	elp
0 ,0	EXPLORER ANDREDT C C	<pre>/ ra_public.pem x / ra_pu</pre>
004		7 k45+UI2100-ØSUDT/K7pLuDS6y6guW/Xb012nY0TV4-Th461x04+f5f620k+tvzyz m0210AA8 9END PUBLIC KEY

Network protocols

	Google Cloud Platform	R2D2 IoT SANDBOX 🔻
þ	IoT Core	Compare config and command the send comm
B	Registry details	Device ID: ACCC8E68CB0A
3	Devices	Device ID Registry Stackdriver Logging: Communication
8	Gateways	2821499520550893 axis_device_registery Debug View logs Allowed
	outenuya	DETAILS CONFIGURATION AND STATE AUTHENTICATION
	Monitoring	
		Latest activity
		Heartbeat (MQTT only) -
		Telemetry event received –
		Device state event received -
		Config sent –
		Config ACK (MQTT only) -
		Error -
		Device metadata
		Device metadata
		You can add or edit metadata in device settings. Edit device.

Step 4: JWT token claim

Google Cloud Platform uses JWT token-based authentication. To exemplify, we have used an *online tool* to generate the JWT token. Note that this is not recommended in a production environment.

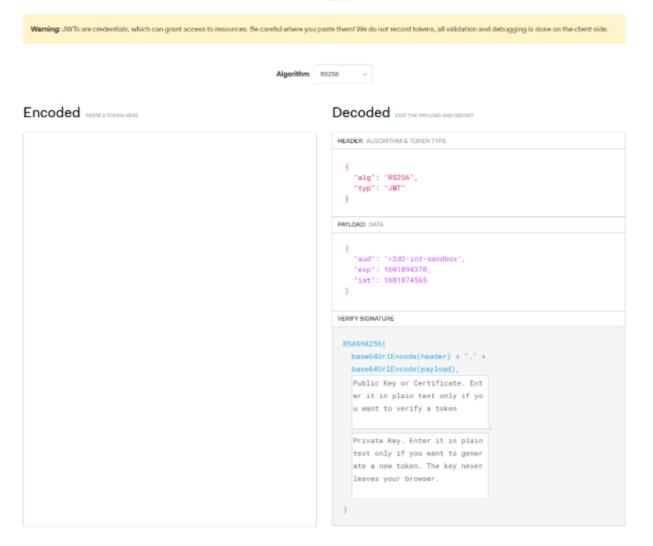
The JWT token itself needs the aud (audience), iat (issued-at) and exp (expiration) fields to be available in the JWT token. The iat and exp fields are defined as unix timestamps. These can be used e.g. using this *tool*. The aud field is defined by the project ID in Google Cloud Platform. When you are done with aud, iat and exp, paste the public and private keypair into the JWT claim in order to export the JWT token as a password for the Axis device.

Important: Google Cloud Platform will reject any authentication attempts with a JWT token that has a longer duration than 24 hours in total.

Network protocols

Thanks for using UnixTimeStamp.com Please tell your friends!	Timestamp Converter
	1601894370 Is equivalent to:
The Current Unix Timestamp	10/05/2020 @ 10:39am (UTC)
	2020-10-05T10:39:30+00:00 in 150 8601
1601874565 seconds since Jan 01 1970. (UTC)	Mon, 05 Oct 2020 10:39:30 +0000 in BFC 822, 1836, 1123, 2822
	Monday, 05-0ct-20 10:39:30 UTC in RFC 2222 2020-10-05T10:39:30+00:00 in RFC 2339
This epoch translates to:	
10/05/2020 @ 5:09am (UTC)	Make Another Conversion:
2020-10-05T05:09:25+00:00 In ISO 8601	Enter a Date & Time:
Mon, 05 Oct 2020 05:09:25 +0000 in RFC 822, 1036, 1123, 2822	YYYY - MI - DE @ 0 : 0 : 0 (24h:min:sec)
Monday, 05-Oct-20 05:09:25 UTC in RFC 2822 2020-10-05T05:09:25+00:00 in RFC 2839	Enter a Timestamp:
2020*10*00105:07:20*00:00 in INC 3559	1601894370

Debugger



Network protocols

	DUGGER
Algorithm Encoded PASTE A TOKEN HERE	RS256 V Decoded EDIT THE PAYLOAD AND SECRET
<pre>eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.ey JhdWQiOiJyMmQyLWlvdC1zYW5kYm94IiwiZXhwI joxNjAxODk0MzcwLCJpYXQiOjE2MDE4NzQ1NjV9 .H8q8Ngz9IFJWKDMjx2ruyxoRV4j2EV2FXKGRsG cKmFcBsw_zkNR8u4cY7pjMZ9Ex7kEQzfdSDv1j5 - EbAS9atB0WCnQCEFML1i0EiC_wo9oGn8jZFzgM8 Vxq2m6UGT6zR- 8kdZN2E5Vsp36FwoQkA8GMKZ3Dnwma26gtiqmvN tokI6AnKEfInpQNthu5Pjr1da1E0VvGFjKhosKj w5S-c_HWNZOyyQ0cFGlQrED5NonxsyMbhzx- Di2JzNR7yw-juBhP8Rt- Y1vlizJIpz0nJT2sheXIY2zq2HhRzpUauvpRNN6 J1T0Cn7Rp7NaEp93C_mHoH01ByzCcgEqlbgJXYA</pre>	<pre>HEADER: ALGORITHM & TOKEN TYPE { "alg": "RS256", "typ": "JWT" } PAVLOAD: DATA { { "aud": "r2d2-iot-sandbox", "exp": 1601894370, "iat": 1601874565 } VERFY SKGNATURE RSASHA256(base64UrlEncode(header) + "." + base64UrlEncode(payload), UW/Xb0iZnYOTVHrTh46ixMhfSfQ2 " Gkrtvzyz m0TDA0A8 END PUBLIC KEY ", Ylb5HAjBpkVBwmfTbvEALmkwsmS8 " VUON18 hotNq1/3RKLydaeggGZy6f25 END PRIVATE KEY ",) </pre>

Step 5: Axis device configuration

Below is the actual Axis device configuration for MQTT. Observe the settings required for a successful connection. The username is ignored/not respected in GCP. The client ID uses the following naming convention format, and the parts marked in bold are individual to your configuration illustrated previously:

projects/r2d2-iot-sandbox/locations/europe-west1/registries/axis_device_registery/devices/ACCC8E68CB0A

The password is the JWT token that has been generated previously. The custom condition prefix for event publication uses the following convention and depends on your previously made configuration:

/devices/ACCC8E68CB0A /events

Network protocols

Client	Publish
Connect 1	Use default condition prefix
Status: Connected	Custom condition prefix
Server	/devices/ACCC8E68CB0A/events
	Include condition name
Host	Include condition namespaces
mqtt.googleapis.com	Include serial number in payload
Protocol	
MQTT over SSL	Event filter list
Validate server certificate	
Port	Manual trigger 🗸 🗸
8883	
Usemame	+
ignored	
Password	Save
Policies	
Client id	
projects/r2d2-iot-sandbox/locations/europe-west1/registric	
45	
Timeout	
45	
Reconnect automatically	
Clean session	
Last will testament	

Step 6: listen to MQTT events

Google Cloud Platform has its own tools to listen to incoming MQTT events from devices either using the Pub/Sub hub or the GCP console directly by using the command below. Again, the part marked in bold is depending on your previous configuration.

gcloud pubsub subscriptions pull device_events

Network protocols

• н	ome – R2D2 IoT SANDBOX – Gc 🗙	+		
← -	C C C console.clou	d.google.com/home/dashboar	d?project=r2d2-iot-sandbox	
≡	Google Cloud Platform	R2D2 IoT SANDBOX		
A	Home	MMENDATIONS		
ŵ	IoT Core			
:	Pub/Sub	COVID-19. Learn more		
	100/000			
PROD	ucts 🔨		Project i	info I
Ŷ	Marketplace	^	Project nan R2D2 IoT S	
Face	Billing		Project ID r2d2-iot-sar	ndbox
API	APIs & Services	>	Project nun 514219820	
÷	Support	>	ADD PEOPI	LE TO THIS PROJECT
Θ	IAM & Admin	>		
۲	Getting started		→ Go to projec	ci serungs
0	Security	>	Resource Resource	es I
\mathbb{A}	Anthos	>	This project	t has no resources

© Scharpforn Medize Adv2 N										-	×
	-	tlevice_events/project+r2d2 ict sambox8anodal+pul					1		ŝ) * (9 ***)	, .
 Google Cloud Platform Pub/Sub 		🐵 V EN NESSASS 🔠 CREATE SUAPSIOT		 Beardy products PURSENNESSAGES 		T.	Messages				
p Tabas automptons	Subscription details	projecto; 2424 as socilare du bestitico y te	iaumera D				adiest enable bepulked at a	ACK messages and then d time. Click Pall again to refe	dy delay mesonya del ano in tati'n in norzhane da ala na tra tati de na songa ta permanya del proven mesonya del neg ta atter subserben neg menen norzhago fran i ta su delay. Na dina ostar mal seg a mandad tati anter na m Janmanago Al Balanti agen i na ster ellar ellastatare el tra ala seg atter delatare seneral degal	ta. Igaunia ha	
Createau Ute Topics Lite Sate proporte	Taponen	proportar 222 ac. aandloov/topets-toorce cor	ala 🖸				TOLL Double :	ек тилоро		8	
	Unadad maxage coart			10 10 18 14	G that una doctimes eage ag	•	Publishing = 0x02020, 0x16030 = 0x02020, 0x16030 = 0x22020, 0x16119 = 0x22020, 0x16119	Abibolyloga far odd far odd far odd	Nongelety Canochargi (1997) 2017 (2017) Apple Comfactionador (2017) 2017 (2019) 2017 (2017) 2017 (2017) 2017 (2017) 2017 (2017) 2017 (2019) 2017 (2017) 2017 (2017) 2017 (2017) 2017 (2017) 2017 (2017) (2017) 2017 (2017) 2017 (2017) 2017 (2017) 2017 (2017) 2017 (2017)	AUN	* * * *
	ain za vis	rða rið siða rös rös	vin vin zin	52 7 No ²	nia 200	236 Vis 7	5 05: 2020, 07:58:19 4	PAC WE	("Investorp": 1001072029931, "spire") www.hfs.wes.do.do.do.au.Eert", "new".	ASK	Ť,
	Inform Ison Scientific reach () Addressingeren staafte () Estantisker reach () Monage staafte sinder Schrift of Konstentingen Schrift of Konstenting () Herdersteig () Herdersteig () Herdersteig () Herdersteig ()	Sul Specific register is 3' republic to 4' I Science 7 April 1997 1997 1997 1997 1997 1997 1997 199	act #1y								

Network protocols

E - company and a second second	1 1 1 1 0 M 10 1 1									s :
 Selection - Put/Sel-2021 x ← → O O in consistent 		× + iption/dotail/dev/co_events?proj	oloct=r2d2 lot sand bes@cioudshell=tr	02						2 × 🙆 2004)
Google Cloud Flatform	🐤 вото ил замотох 👻								•	i 🗆 e 🔺 i 🙆
🙏 Pub/Sub	 device_events 		GAGES 🗄 CREATE SHAPSHOT	C REPLAY NESSAGES 🛛 🕀 PURSE ME	SSNGCS BCTVCH 🖀 CA	CLETC				LIDE NEO PANEL
E Topics	Subscription details								device_events	
a contributions									PERMISSIONS LABO	ELS ACTIVITY
Standarts	Bubscription same		ers/httblab-sandtrages/sectprines/device,						Ech or citize permissions bein	
	Topic name	[POL60	erselfelt-ko-kandrosofer rantas rajaserie	<u>× 0</u>					Rolt or celere petrolosione belo Rold Member lo grant nev	ALT ADD MEMORY
								These Ghours I day 7 days 20 days RESTIZION	Show inherited permitted permitte	issions
East Subscriptions					1					
	Bracked message os int				F Oldert unscheil message	A14				6
				/ 81				- 200.00#	Role-Herster 🕈	Interferrore
				/ 18				· · · · · · · · · · · · · · · · · · ·	E. Comer (8)	
	7.50 7.05	7/15 7/15 7/20	0 728 723 735 1	Dic Tid 720 725	700 700	5 2 0 2 1	727 725	as nas tás sie nie tás sis		
	164 East	En los cas	int the new r	24 00 ov os	100	1 238 104	- 1927 - 1-1-1	5 125 128 299 126 tor tore car		
	Deliverytype	21								
	Subscription only IB		soriation expires in St days if there is no act	childry.						
	Acknowledgement dead inc (0	10 500								
	Subscription filter O Message relation duration	- 7949								
	Message referition danation Referinschrowledged messages									
	Alexandre ontiering @	Couble	bled							
	Development (Direction Contraction								
c	Retry policy @ Labels	Setyl	ylmmediately							
	Cilico .									
Terminal 1202-in-south	* + × 0.041							2 op	er ed tor	
<pre>bloose to Cloud Shellf Type "hel bur Cloud Distions project in th be "polosi config set profest (nicobricionshel":- policions</pre>	<pre>dp* to get started. his persion is set to size s PROJECT TO!* to charge to a</pre>	ot pendbox. different project.								
ndrohtfisiendetal :- passessere	andien); palent reterin entern	listics of anno an	<u> </u>							
			IATA			SECOND 10	CORRECTION MET	e ATURIEUTES	CLEARNEY ATTENT	
The states to the states	the sets thread all warm for our	and the line in the second		Property front to 2011, Deeter		Laborate Services		discussed of ACCENDENTIAL		TRANSFORMER STREET, ST
14 JULI PERMINING DESCRIPTION OF THE OWNER OWNER OWNER OWNE	III. yikiyoyattarkari harabat	15V-125-01-025-151-0408-0308	2521 LIVINGSVHI VIKTAH SSREETIS DOO	Processing Products 2011, Despired medical and the comparison of the second statements of the se	ocapamento			aviventate=		
								projectidential int maniform		
undrehtficlindatell:- (2242-4ot-m	andbox) 5									

Contact

Contact Axis Technical Services for further assistance and additional requests: https://www.axis.com/support

OAuth 2.0 OpenID Connect

Using the OAuth 2.0 OpenID Connect protocol, AXIS OS devices running AXIS OS 11.6 or higher can be integrated into a IT-infrastructure controlled and centralized Identity and Access management (IAM) service allowing to use federated identities for authenticating to the Axis device. This removes the need of local device user management entirely. OpenID Connect is a standardized network protocol on top of OAuth 2.0 used for authentication and authorization of identities that can be used in various different Identity Provider or Active-Directory Federated System (ADFS) solutions such as Microsoft Active Directory, Microsoft Azure AD, Curity Identity Server and others.

For a complete list of OpenID Connect certified solutions, please go to the official *OpenID Connect* page. Depending on the feature set of the Identity Provider, the following security mechanism could be used to allow for further enhanced secure identity-based authentication towards the Axis device:

- Multi-Factor Authentication (MFA)
- Password Complexity Enforcement
- Password Rotation
- Time-limited authentication
- Centralized identity (user/service account) management

Network protocols



In this video, an operator logs into an Axis device using their corporate credentials, including a Multi-Factor Authentication.

Benefits

- Local Axis device account (e.g. root, user-created accounts) are disabled.
- HTTP(S) digest authentication is disabled.
- No local Axis device user and password management configuration or maintenance needed.
- Increased security by avoiding local device user account information leakage.
- Axis devices integrate seamlessly into IT-infrastructure supported secure Identity and Access Management (IAM).
- HTTP(S) web-interface access and tunneled video streaming is supported.
- IT enforced IAM security policies, traceability and security audit logging.

Limitations

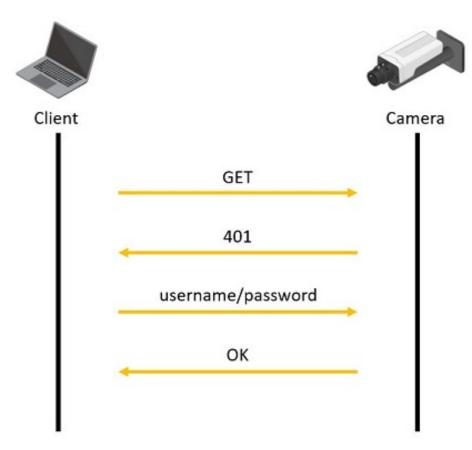
Please note that there are currently limitations/considerations that need to be taken into account when the Axis device is operated in OpenID connect mode:

- The Video or Device Management System that is connecting to the Axis device also needs to support OpenID Connect to interact with the Axis device. Please contact your 3rd party Video and Device-Management System vendor for further information.
- Video Streaming through RTSP-server authentication is not supported.
- AXIS Device Management solutions (ADM5, ADMX) as well as AXIS Companion and AXIS Camera Station are currently not supported.
- Access-Token according to OAuth 2.0 are not supported.

Function Overview

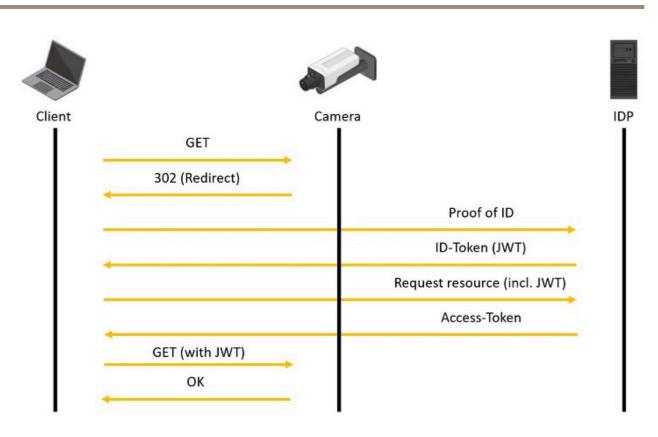
Classic Access Model

Network protocols



• OpenID connect

Network protocols



Curity Identity Server

In this section you can read about the configuration steps required to connect an Axis device to a Curity Identity Server. Please see the *Curity website* for further reading about the Curity Identity Server.

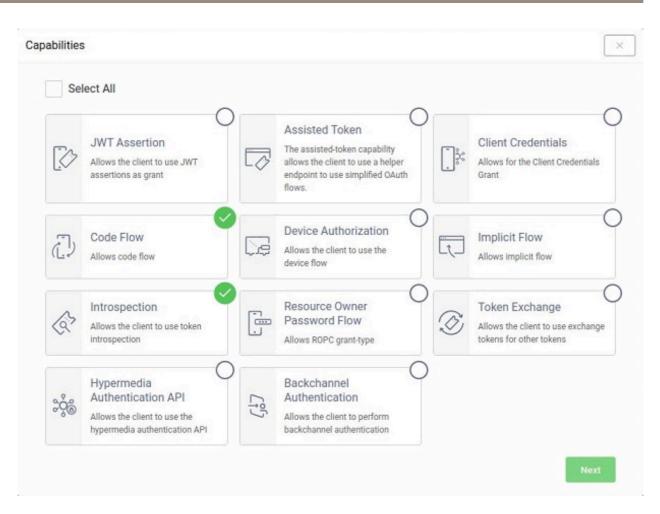
Important

The below steps illustrate basic integration and use-cases within a test lab environment. Axis strongly recommends following the provider's guidelines for an integration that maximizes the handling of certificates, tokens, user-credentials and overall cybersecurity in a production environment.

Curity Identity Server setup

- 1. Following the *getting started guide* described on the Curity website should supply you with a basic setup to integrate an Axis device into Curity Identity Server. Please note you should configure trusted certificates. Please refer to the Curity Identify Server documentation on how this is done.
- 2. Navigate to Token Service > Client and create a new client. Enter a client id and document it.
- 3. Add a new capability, choose Code Flow and Introspection.

Network protocols



4. Define a redirect URI. This should be device unique.

nt Application Details		
Redirect URIs		
	Add	🕸 OAuth.tools 🗸
ADDED VALUES (1)		
https://p1375.r2d2.lab/oidc/oauth2callback		

5. Define a client secret and document it.

Network protocols

Authentication Method	
secret	~
Secret	
	الله المعالم الم
A password used by the client	
Make sure to copy this value. You cannot get it later	٥

6. Define a user authentication method. During the getting started steps a default username-password page was created which we use in this example.

Filter authenticators	Select All	Select Authenticator Types \vee
username-		
password		

7. Add a scope and enter email, openid and profile.

Network protocols

Ceneral	Security A	User Authentication	Tokens [Application
Overview				
		Axis		
		Capabilities 2 Code Flow	Add Scopes	→ Scopes ×
		Introspection	Scope ID email	Action
			openid	
Client Authentication	User Authentication 1		A subset of the scopes define is allowed to request or all if a	d in the profile that this client

8. The overview now should look like this:

Network protocols

General	Security Security User Authent	tication 🔗 Toke	ens . Application
Overview			
	Axis	Q	
	Capabilities	2	
		le Flow	
		le Flow	<u>م</u>
Client Authentication		le Flow	Tokens

9. In the Security tab, under Origins and Validation, please add the hostname of your device.

Network protocols

Color Genera	Security	User Authentication		Tokens	Application
Origins and Validation					
Allowed Origins					
			Add	Add Test Origin	Add OAuth.tools
				Aud reat origin	
ADDED VALUES (1)					
https://p1375.r2d2.lab					
The optional list of URIs or URI-p	atterns that is allowed to emb	ed the rendered pages inside an ifra	ame, be a truste	d source or be used for	CORS.
The optional list of URIs or URI-p	Loopback Interfaces		ame, be a truste	d source or be used for	CORS.
The optional list of URIs or URI-p Validate Port on Whether the port should be va	Loopback Interfaces	ured to redirect	ame, be a truste	d source or be used for	CORS.
The optional list of URIs or URI-p	Loopback Interfaces Idated when a client is config rults to true for backwards co	ured to redirect mpatibility.	ame, be a truste	d source or be used for	CORS.
The optional list of URIs or URI-p Validate Port on Whether the port should be va to the loopback interface. Def	Loopback Interfaces Idated when a client is config iults to true for backwards co false because RFC-8252 (sec	ured to redirect mpatibility. 2. 3) says the	ime, be a truste	d source or be used for	CORS.
The optional list of URIs or URI-p Validate Port on Whether the port should be va to the loopback interface. Def Future versions may default to	Loopback Interfaces lidated when a client is config jults to true for backwards co false because RFC-8252 (see nd this does not generally redi	ured to redirect mpatibility. 2.3) says the uces the security	ime, be a truste	d source or be used for	CORS.

10. Under Changes in the menu, select to Commit your changes.

Network protocols

($m{\lambda}$ Recent Work $ imes $	U[®] Changes ∧	\gtrsim admin \sim
Edit Axis	Commit Validate Cancel Pending Changes History Upload	š: API 🛊 OAuth
Overview Axis Capabilities 2	Download	

Axis device parameters

Parameter	Value
OIDC_AuthzAdminClaim	Value of the issuer property from the ProviderMetadataURL. Example "issuer:https://curity_server/oauth/v2/oauth-anonymous"
OIDC_AuthzOperatorClaim	Value of the issuer property from the ProviderMetadataURL. Example "issuer:https://curity_server/oauth/v2/oauth-anonymous"
OIDC_AuthzViewerClaim	Value of the issuer property from the ProviderMetadataURL. Example "issuer:https://curity_server/oauth/v2/oauth-anonymous"
OIDC_ClientID	The client ID obtained during step 2.
OIDC_ClientSecret	The client secret obtained during step 10
OIDC_OutgoingProxy	Not used in this example but if required for your setup, specify here the outgoing proxy.
OIDC_ProviderMetadataURL	https://curity_server/oauth/v2/oauth-anonymous/.well-known/openid-configuration
OIDC_RemoteUserClaim	This is the value used by the web interface to display the logged in user. Possible values can be found in the ProviderMetadataURL > claims_supported. Example "sub"
OIDC_RequireClaim	Value of the issuer property from the ProviderMetadataURL. Example ""issuer:https://curity_server.com""
OIDC_AuthzScopes	Optional list of additional OIDC scopes.

Google Cloud Platform

In this section you can read about the configuration steps required to connect an Axis device to the Google Cloud Platform using OpenID Connect. For further reading, please review the *Google Identity documentation*.

Important

The below steps illustrate basic integration and use-cases within a test lab environment. Axis strongly recommends following the provider's guidelines for an integration that maximizes the handling of certificates, tokens, user-credentials and overall cybersecurity in a production environment.

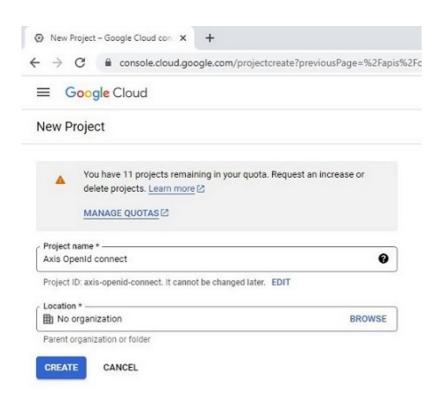
Network protocols

Google Cloud Platform setup

- 1. Setup a project in the Google API Console.
- 2. Click on Select project and select New project.

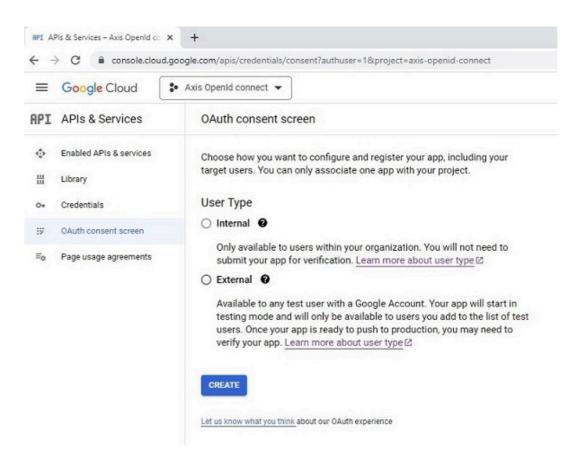
To view this page, select a proj	ject.			SELECT PROJECT CREATE P
Select a recent project	Select a pro	ject		NEW PROJECT
	Q. Search project			
Organization: No organization	RECENT	STARRED ALL		
Accessed 1 minute ago	Name		ID	
	☆ 3 •	0		
	\$\$ \$P	0		

3. Enter a Project name and click on Create.



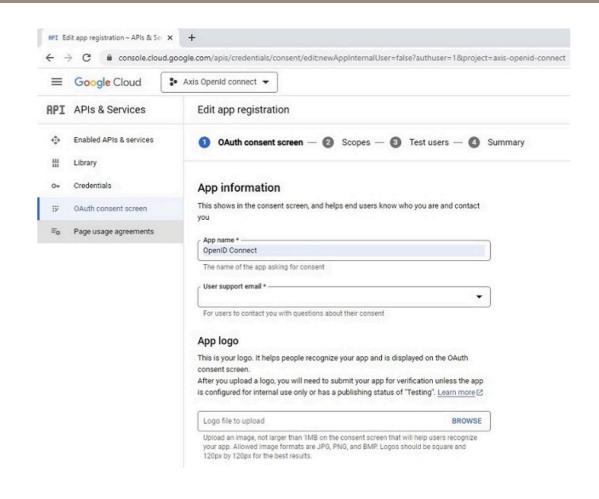
Network protocols

4. To setup OAuth 2.0, go to OAuth consent screen page and select user type.



5. Enter the required details.

Network protocols



6. Add the scopes: userinfo.email, userinfo.profile and openid.

Network protocols

≡	Google Cloud	Axis OpenId conne	ect 🕶					
IPI	APIs & Services	Edit app re	gistration					
¢	Enabled APIs & services	OAuth c	onsent screen —	2 Scopes — 3 Test users — 4	Summary			
Ш	Library							
0+	Credentials	tials sp and allow your project to access specific types of private user data						
IV.	OAuth consent screen	app and allow your project to access specific types of private user data from their Google Account. Learn more 🗠						
Ξo	Page usage agreements	ADD OR RE	ADD OR REMOVE SCOPES					
		Your nor	n-sensitive sco	opes				
		API 🛧	Scope	User-facing description				
			 ./auth/userinfo .email	See your primary Google Account 👘 🍵				
			 ./auth/userinfo .profile	See your personal info, including any personal info you've made publicly available				
			openid	Associate you with your personal 👘				
			Scope	es equest access to private user data. User-facing description				
			Scope	PES request access to highly sensitive user data. User-facing description				

7. Add authenticated users to the application.

Network protocols

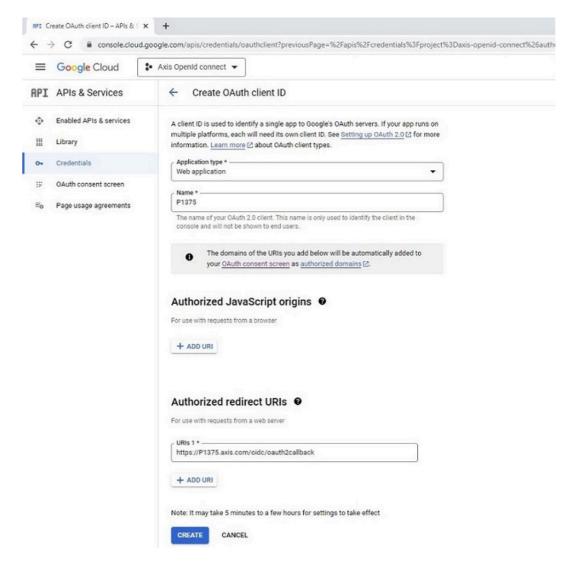
=	Google Cloud	• Axis OpenId connect 👻
PI	APIs & Services	Edit app registration
≎	Enabled APIs & services Library	🤣 OAuth consent screen — 🥑 Scopes — 3 Test users — 🔕 Summary
04	Credentials	Test users
iy	OAuth consent screen	While publishing status is set to "Testing", only test users are able to access the app. Allowed user cap prior to app verification is 100, and is counted over
Ξo	Page usage agreements	the entire lifetime of the app. <u>Learn more</u>
		Filter Enter property name or value
		User information

- 8. To obtain OAuth 2.0 credentials, go to the *Credentials page*.
- 9. Select Create credentials > OAuth client ID.

≡	Google Cloud	♣ Axis OpenId connect ▼		
API	APIs & Services	Credentials	+ CREATE CREDENTIALS 🝵 DELETE 🗠 RESTORE DELETED	CREDENTIALS
¢	Enabled APIs & services	Create credentials to ac	API key Identifies your project using a simple API key to check quota and access	
Ш	Library	API Keys	OAuth client ID Requests user consent so your app can access the user's data	
0-	Credentials	Name	Service account	n date 🗸
IJ	OAuth consent screen	No API keys to displa	Enables server-to-server, app-level authentication using robot accounts	
T ₀	Page usage agreements	OAuth 2.0 Client I	Help me choose Asks a few questions to help you decide which type of credential to use	
		Name -	(creation date
		No OAuth clients to dis	splay	
		Service Accounts		
		Email		
		No service accounts to	o display	

Network protocols

10. Select application type **Web application**, fill in a client name and configure authorized redirect URIs. Note that this the FQDN should end with *"/oidc/oauth2callback"*.



11. Document the Client ID and Client secret for further usage.

Network protocols

OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

	ess is restricted to the <u>test users</u> 🖄 listed on your asent screen
Client ID	965-
	n827n26j3bnd1c7mof7km1i1eqvfc2pm.ap
	ps.googleusercontent.com
Client secret	KOya6udLe8dxkiyr_h_5c-
	4 G
Creation date	May 30, 2023 at 10:49:29 AM GMT+2
Status	Enabled

Axis device parameters

Parameter	Value
OIDC_AuthzAdminClaim	https://accounts.google.com
OIDC_AuthzOperatorClaim	https://accounts.google.com
OIDC_AuthzViewerClaim	https://accounts.google.com
OIDC_ClientID	The <i>client ID</i> obtained during step 8.
OIDC_ClientSecret	The <i>client secret</i> obtained during step 8.
OIDC_OutgoingProxy	Not used in this example but if required for your setup, specify here the outgoing proxy.
OIDC_ProviderMetadataURL	https://accounts.google.com/.well-known/openid-configuration
OIDC_RemoteUserClaim	This is the value used by the web interface to display the logged in user. Possible values can be found in the ProviderMetadataURL > claims_supported. Example "sub"
OIDC_RequireClaim	Value of the issuer property from the ProviderMetadataURL. Example "iss:https://accounts.google.com"
OIDC_AuthzScopes	Optional list of additional OIDC scopes.

Microsoft Identity Platform (Azure)

In this section you can read about the configuration steps required to connect an Axis device to the Microsoft Identity Platform using OpenID Connect. For further reading, please review the *Microsoft Identity Platform documentation*.

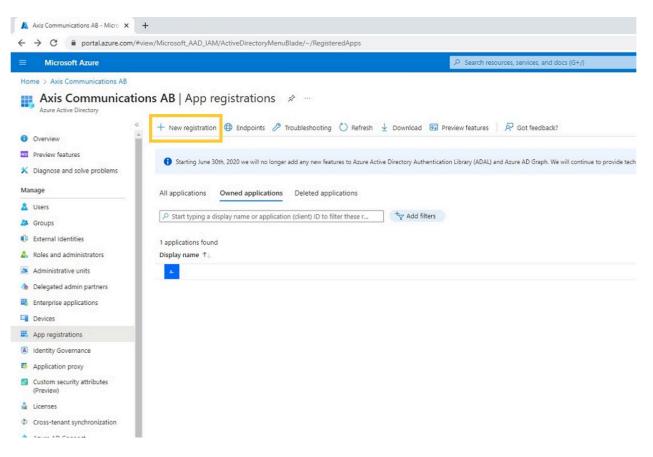
Important

The below steps illustrate basic integration and use-cases within a test lab environment. Axis strongly recommends following the provider's guidelines for an integration that maximizes the handling of certificates, tokens, user-credentials and overall cybersecurity in a production environment.

Microsoft Identity Platform setup

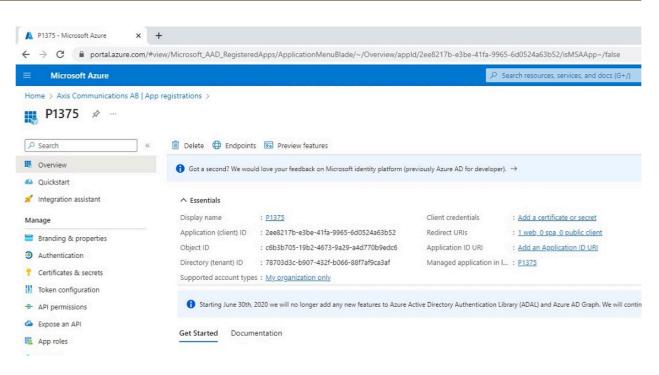
Network protocols

- 1. Setup an application in the Microsoft Azure Active Directory console.
- 2. Go to the App registrations page and select New registration.



 Fill in a display name and configure an authorized redirect URI. Note that this the FQDN should end with "/oidc/oauth2callback".
 Document the Application (client) ID.

Network protocols



- 4. To obtain a client secret, go to the Certificates & secrets page and select New client secret.
- 5. Fill in a description and expiry date and click Add. Document the Client secret.

R P1375 - Microsoft Azure X	+					
← → C 🔒 portal.azure.com/#\	view/Microsoft_AAD_RegisteredApps/Applicat	ionMenuBlade/~/Cre	dentials/appld/2ee8217	b-e3be-41fa-9965-6d0524a63b52/isMSA	App~/false	
■ Microsoft Azure				𝒫 Search resources, services, and 𝔅	nd docs (G+/)	
Home > Axis Communications AB Ap						
✓ Search «	Sot feedback?					
 Overview Quickstart 	Got a second to give us some feedback?	\rightarrow				×
Manage	Credentials enable confidential applications t scheme). For a higher level of assurance, we r				le location (using an HTTP	2S
 Branding & properties Authentication 	 Application registration certificates, secret 	ts and federated credent	ials can be found in the tabs	below.		×
Certificates & secrets Control Cont	Certificates (0) Client secrets (1) F A secret string that the application uses to p	ederated credentials prove its identity when		an be referred to as application password.		
App roles	+ New client secret					
A Owners	Description	Expires	Value 🕕	Secret ID		
 Roles and administrators Manifest 	secret	11/26/2023		MsG1wk 🗈	a32f-8ee0bcff67c0	0

6. Go to the Overview page and select Endpoints and document the shown endpoints.

Network protocols

Microsoft Azure		𝒫 Search resources, services, and docs (G+/)	
Home > Axis Communications AB A	pp registrations >	Endpoints	×
関 P1375 🖈 \cdots			
	* · · · · • • • • • • • • • • • • • • •	OAuth 2.0 authorization endpoint (v2)	
	📋 Delete 🌐 Endpoints 💀 Preview features	https://login.microsoftonline.com/78703d3c-b907-432f-b066-88f7af9ca3af/oauth2/v2.0/authorize	C
Overview	Got a second? We would love your feedback on Microsoft identity platform (previous)	OAuth 2.0 token endpoint (v2)	
🔒 Quickstart		https://login.microsoftonline.com/78703d3c-b907-432f-b066-88f7af9ca3af/oauth2/v2.0/token	Q
Integration assistant		OAuth 2.0 authorization endpoint (v1)	
lanage	Display name : P1375	https://login.microsoftonline.com/78703d3c-b907-432f-b066-88f7af9ca3af/oauth2/authorize	[
	Application (client) ID : 2ee8217b-e3be-41fa-9965-6d0524a63b52	OAuth 2.0 token endpoint (v1)	
Branding & properties	Object ID : c6b3b705-19b2-4673-9a29-a4d770b9edc6	https://login.microsoftonline.com/78703d3c-b907-432f-b066-88f7af9ca3af/oauth2/token	1
Authentication	Directory (tenant) ID : 78703d3c-b907-432f-b066-88f7af9ca3af	OpenID Connect metadata document	
Certificates & secrets	Supported account types : My organization only	https://login.microsoftonline.com/78703d3c-b907-432f-b066-88f7af9ca3af/v2.0/.well-known/openid-configuration	1
Token configuration		Microsoft Graph API endpoint	
API permissions	Starting June 30th, 2020 we will no longer add any new features to Azure Active F	https://graph.microsoft.com	1
Expose an API	and the second second	Federation metadata document	
App roles	Get Started Documentation	https://login.microsoftonline.com/78703d3c-b907-432f-b066-88f7af9ca3af/federationmetadata/2007-06/federationmetadata.xml	1
Owners		WS-Federation sign-on endpoint	
Roles and administrators		https://login.microsoftonline.com/78703d3c-b907-432f-b066-88f7af9ca3af/wsfed	[
Manifest	The Microsoft identity	SAML-P sign-on endpoint	
		https://login.microsoftonline.com/78703d3c-b907-432f-b066-88f7af9ca3af/saml2	1
upport + Troubleshooting		SAML-P sign-out endpoint	
Troubleshooting		https://iogin.microsoftonline.com/78703d3c-b907-432f-b066-88f7af9ca3af/saml2	1

Axis device parameters

Parameter	Value
OIDC_AuthzAdminClaim	Value of the issuer property from the ProviderMetadataURL. Example "iss:https://login.microsoftonline.com/78703d3c-b907-432f-b066-88f7af9ca3af/v2.0
OIDC_AuthzOperatorClaim	Value of the issuer property from the ProviderMetadataURL. Example "iss:https://login.microsoftonline.com/78703d3c-b907-432f-b066-88f7af9ca3af/v2.0
OIDC_AuthzViewerClaim	Value of the issuer property from the ProviderMetadataURL. Example "iss:https://login.microsoftonline.com/78703d3c-b907-432f-b066-88f7af9ca3af/v2.0
OIDC_ClientID	The <i>client ID</i> obtained during step 3.
OIDC_ClientSecret	The <i>client secret</i> obtained during step 5.
OIDC_OutgoingProxy	Not used in this example but if required for your setup, specify here the outgoing proxy.
OIDC_ProviderMetadataURL	OpenID Connect metadata document obtained during step 3.
OIDC_RemoteUserClaim	This is the value used by the web interface to display the logged in user. Possible values can be found in the ProviderMetadataURL > claims_supported. Example "sub"
OIDC_RequireClaim	Value of the issuer property from the ProviderMetadataURL. Example "iss:https://login.microsoftonline.com/78703d3c-b907-432f-b066-88f7af9ca3af/v2.0"
OIDC_AuthzScopes	Optional list of additional OIDC scopes.

Microsoft Windows AD FS

In this section you can read about the configuration steps required to connect an Axis device to Microsoft Windows Active Directory Federation Service (AD FS) using OpenID Connect. For further reading, please review the *Windows AD FS documentation*.

Important

The below steps illustrate basic integration and use-cases within a test lab environment. Axis strongly recommends following the provider's guidelines for an integration that maximizes the handling of certificates, tokens, user-credentials and overall cybersecurity in a production environment.

Network protocols

Windows AD FS setup

- 1. Install the Windows AD FS role as described *here*.
- 2. Configure the Windows AD FS role as described *here*.
- 3. Verify that Windows AD FS is working correctly be following the steps described here
- 4. From the Windows AD FS management console, add a new application group. Use the Server Application template.

Mad Application Group) Wizard	×
Welcome		
Steps	Name:	
Welcome	Axis ADFS	
 Server application Configure Application Credentials Summary 	Description:	
Complete	Template:	
Complete	Client-Server applications Native application accessing a web API Server application accessing a web API Web browser accessing a web application Standalone applications Native application Server application Web API	
	More information	
		< Previous Next > Cancel

5. Enter a Name, Client Identifier and Redirect URI. Document the Client Identifier. Note that the redirect URI is the FQDN of the Axis device and it should end with "/oidc/oauth2callback". Click Next.

Network protocols

Add Application Group		×
Steps	Name:	
Welcome	Axis ADFS - Server application	
Server application	Client Identifier:	
 Configure Application Credentials 	a69a5ecf-db9f-4d15-b431-aab6ea45eef0	
Summary	Redirect URI:	
Complete	Example: https://Contoso.com	Add
	https://FQDN/oidc/oauth2callback	Remove
	Description:	

6. Select Generate a shared secret. Document the shared secret. Click Next.

Network protocols

🙀 Add Application Group	p Wizard	×
Configure Application	on Credentials	
Steps Velcome Server application Configure Application Summary Complete	Generate a shared secret Segret: DJ-HVhL-eqUr08xGys_33-waOEqYMf-xB1lmfySG Copy and save the secret. You will not be able to view the secret after the application generated. You can reset the secret later if required.	elect

7. Complete the rest of the wizard.

Network protocols

🙀 Add Application Group	Wizard	×
Summary		
Steps • Welcome • Server application • Configure Application Credentials • Summary • Complete	Review the following settings and click 'Next' to create the application. Application Group Name: Axis ADFS Server application Name: Axis ADFS - Server application Identifier: a69a5ecf-db9f-4d15-b431-aab6ea45eef0 Redirect URIs: https://FQDN/oidc/oauth2callback Use client secret: True	
	< Previous Next >	Cancel

Axis device parameters

Parameter	Value
OIDC_AuthzAdminClaim	Value of the issuer property from the ProviderMetadataURL. Example "iss:https://ADFS_server/adfs/"
OIDC_AuthzOperator- Claim	Value of the issuer property from the ProviderMetadataURL. Example "iss:https://ADFS_server/adfs/"
OIDC_AuthzViewer- Claim	Value of the issuer property from the ProviderMetadataURL. Example "iss:https://ADFS_server/adfs/"
OIDC_ClientID	The client ID obtained during step 5.
OIDC_ClientSecret	The client secret obtained during step 6.
OIDC_OutgoingProxy	Not used in this example but if required for your setup, specify here the outgoing proxy.
OIDC_ProviderMeta- dataURL	https://ADFS_server/adfs/.well-known/openid-configuration
OIDC_RemoteUserClaim	This is the value used by the web interface to display the logged in user. Possible values can be found in the ProviderMetadataURL > claims_supported. Example "sub" or "unique_name".

Network protocols

OIDC_RequireClaim	Value of the issuer property from the ProviderMetadataURL. Example "iss:https://ADFS_server/adfs/"
OIDC_AuthzScopes	Optional list of additional OIDC scopes.

Axis device configuration

Important

Wrong parameter configuration can result in a non-accessible device due to other login methods (HTTP/HTTPS basic/digest) being disabled. For the initial configuration it is recommended to enable SSH access to allow access to the Axis device and being able to restore the configuration. Please contact Axis Technical Support for further assistance.

User roles

Axis devices know 3 different roles when using OIDC.

- Administrator
- Operator (with PTZ rights)
- Viewer (without PTZ rights)

The above identity provider setup examples result in providing all users with the administrator role. To illustrate a setup with different user roles the following security groups have been created in an Active Directory, each containing different users.

Active Directory Group Name	Group Members
Axis-Lund-admin	User1
Axis-Lund-operator	User2
Axis-Lund-viewer	User3

Depending on the identity provider a custom claim should be created. For the below example the claim "groups" has been configured.

In order to assign the Active Directory Groups to the Axis user roles, the following values should now be used during the Axis device parameter configuration.

Parameter	Value
OIDC_AuthzAdminClaim	groups:Axis-Lund-admin
OIDC_AuthzOperatorClaim	groups:Axis-Lund-admin
OIDC_AuthzViewerClaim	groups:Axis-Lund-viewer

This will result with the following user roles being assigned.

User	Role
User1	Administrator
User2	Operator with PTZ rights
User3	Viewer with PTZ rights

Configuration using the GUI

With AXIS OS 11.7 or higher, it is possible to configure OpenID in the web interface.

Network protocols

	AXIS P1375 Network Ca	amera	00 📼 00
🕻 Apps	Virtual hosts		
🕸 System 🗸	Add virtual host		
Time and location			
Network	Server name	Port	Туре
Security			
Accounts	OpenID Configuration		
Events	Client ID	Outgoing Proxy	
MQTT			
Storage	Admin claim	Provider URL	
Stream profiles	Operator claim	Require Claim	
ONVIF			
Analytics metadata	Viewer claim	Remote User	
Detectors			
Accessories	Scopes	Client secret	
Logs			
Plain config			
	1		Save

API Parameter	Web interface
OIDC_AuthzAdminClaim	Admin claim
OIDC_AuthzOperatorClaim	Operator claim
OIDC_AuthzViewerClaim	Viewer claim
OIDC_AuthzScopes	Scopes
OIDC_ClientID	Client ID
OIDC_ClientSecret	Client secret
OIDC_OutgoingProxy	Outgoing Proxy
OIDC_ProviderMetadataURL	Provider URL
OIDC_RemoteUserClaim	Remote user
OIDC_RequireClaim	Require Claim

Configuration using the API

While the above example shows the configuration using the built-in web interface, it is also possible to use the available VAPIX API to configure the required OpenID Connect parameters on an Axis device. Using *AXIS Device Manager*, the required settings can be pushed to multiple devices at once.

Login on the Axis device using OpenID Connect

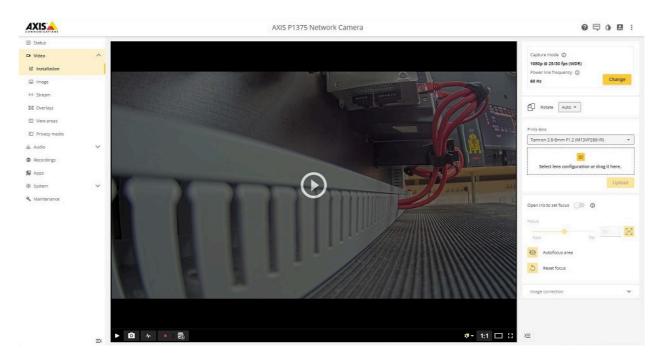
1. Browse to https://<hostname>/ of the Axis device. For example https://p1375.axis.com

Network protocols

2. The device should now redirect to the configured redirect URL of the Identity Provider. This example shows the redirect page of a Azure application.

Microsoft Sign in @axis.com	Microsoft Taking you to your organization's sign-in page	Axis Secure Token Service
Can't access your account?	Cancel	Sign in with your organizational account @axis.com Sign in
🔍 Sign-in options		

3. After providing the user identity to the identity provider, you are redirected back to the Axis device interface.



Virtual hosts

AXIS OS 11.11 and later versions support multiple virtual host authentication interfaces. This allows for hybrid setups where Digest/OAuth 2.0 OpenID Connect authentication schemes are used for centralized Identity Access Management (IAM) in active directory federated services (ADFS) and other identity provider (IDP) solutions.

Virtual hosts only support HTTPS.

By default, the HTTPS port configured on the Axis device supports all authentication schemes supported by the Axis device:

- Base
- Digest
- OAuth 2.0 OpenID Connect

Network protocols

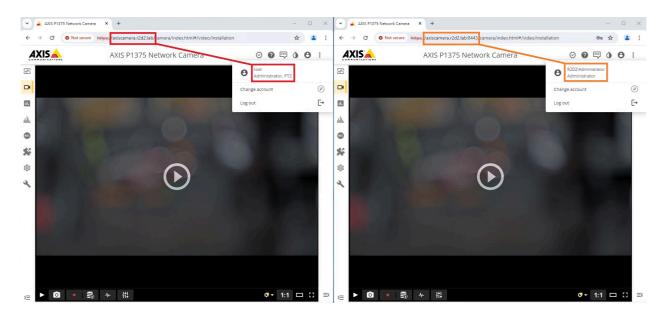
Example 1 - Authentication schemes on different ports

🗱 Apps		Virtual hosts			
鑗 System	^				
Time and location		+ Add virtual host			
Network		Server name	Port	Type	
Security		Enabled axiscamera.r2d2.lab	8443	OpenID	
Accounts					

Name	Port	Authentication scheme	Comment
Digest	443	Digest	Not added as host since digest is already accepted by default on the configured HTTPS port.
axiscamera.r2d2.lab	8443	OpenID	

The authentication scheme that the device accepts differs depending on which of the ports you attempt to access the Axis device from.

Address	Authentication scheme
https://axiscamera.r2d2.lab:443	Digest
https://axiscamera.r2d2.lab:8443	OAuth 2.0 OpenID Connect



Example 2 - Authentication schemes on the same port

Network protocols

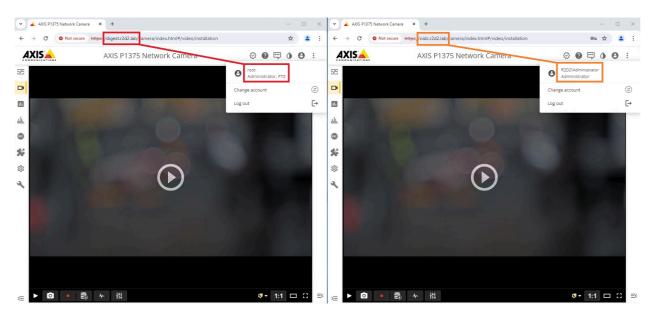
Apps			-			
🕅 System	^	Virtual ho	sts			
Time and location		+ Add	d virtual host			
Network			Server name	Port	Туре	
Security						
Accounts	1	Enabled	oidc.r2d2.lab	443	OpenID	
Events		Enabled	digest.r2d2.lab	443	Digest	
MQTT						

Name	Port	Authentication scheme
digest.r2d2.lab	443	Digest
oidc.r2d2.lab	443	OpenID

Because of the way virtual hosts work, the configured name will be used as the hostname to differentiate between the 2 above authentication schemes. In this example, we've chosen digest & oidc. The authentication scheme that the device accepts differs depending on which of the two hostnames you use to access the device.

Address	Authentication scheme
https://digest.r2d2.lab	Digest
https://oidc.r2d2.lab	OAuth 2.0 OpenID Connect

Note that this setup might require updates in your DNS infrastructure to ensure both hostnames are correctly accessible and resolved.



Network protocols

SFTP (SSH File Transfer Protocol)

Axis devices are capable of sending images and videos using the SFTP (SSH File Transfer Protocol) protocol to a remote server. SFTP is using the secure and encrypted SSH protocol to transfer data via FTP. This is not to be mistaken with FTPS (FTP over SSL), which is another secure method of transferring data securely, however not supported by Axis devices.

3rd party SFTP server

Depending on the environment and selected 3rd party SFTP server, the configuration may differ. In this tutorial we are going to have a look at the commonly used OpenSSH server for Linux operating systems.

Important

The below steps illustrate basic integration and use cases within a test lab environment. Axis strongly recommends following the provider's guidelines for an integration that maximizes the handling of certificates, tokens, user-credentials and overall cybersecurity in a production environment.

OpenSSH server configuration

The SFTP implementation of Axis devices is based on the open-source software component Curl. Out of the *many authentication methods that Curl supports*, Axis devices currently only support the so called **CURLSSH_AUTH_PASSWORD**. Therefore you need to make sure that the SFTP server being used supports this method as well.

This guide can be used as a reference to install OpenSSH, which then allows for the Axis device to transfer data using SFTP. Once the OpenSSH server is installed, it should be possible to test that the connections work, e.g. by using *Putty (SSH client)*. Enter the server IP address as well as the login credentials from your Linux operating system to connect.

Network protocols

🕵 PuTTY Configuration		? ×
Category:		
Session Logging Terminal Keyboard Bell Features Window	Basic options for your PuTTY ses Specify the destination you want to connect Host <u>N</u> ame (or IP address) 172.25.201.102 Connection type: O Raw O Telnet O Rlogin • SSH	t to <u>P</u> ort 22
Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH	Load, save or delete a stored session Saved Sessions	Load Sa <u>v</u> e Delete
About Help	Close window on e <u>x</u> it: Always Never Only on cle	ean exit Cancel

Network protocols

🧬 psadmin@app02: ~

```
login as: psadmin
psadmin@172.25.201.102's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-50-generic x86 64)
 * Documentation: https://help.ubuntu.com
  Management:
                  https://landscape.canonical.com
  Support:
                  https://ubuntu.com/advantage
 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
    https://ubuntu.com/livepatch
525 packages can be updated.
400 updates are security updates.
New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
Last login: Fri Feb 21 10:28:52 2020 from 10.86.129.251
psadmin@app02:~$
```

 \times

SFTP uses public key authentication in order to allow for secure data transfer, which is why it's recommended to *create dedicated key pairs* for this purpose. In AXIS OS, SSH-2 with RSA, DSA, ECDSA and ED25519 host keys are supported. AXIS OS 11.1 or higher includes a new OpenSSH version which removes depreciated authentication methods of using RSA keys. We recommend using the SFTP server's ECDSA or ED25519 host keys instead. By using the following commands, private/public host key pairs can be created in the OpenSSH server. The private key is exclusively used by the OpenSSH server while the public key will be used by the Axis device in form of a hashed MD5 or SHA-256 key that is generated from the public key.

Command	Description
sudo ssh-keygen -t dsa	Creates a private/public DSA host key pair
sudo ssh-keygen -t rsa	Creates a private/public RSA host key pair
sudo ssh-keygen -t ed25519	Creates a private/public ed25519 host key pair
sudo ssh-keygen -t ecdsa	Creates a private/public ecdsa host key pair

Network protocols

psadmin@app02: /etc/ssh

```
File Edit View Search Terminal Help
psadmin@app02:/etc/ssh$ sudo ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id rsa): Test Key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in Test_Key.
Your public key has been saved in Test_Key.pub.
The key fingerprint is:
SHA256:gUYVTq8MVXMaf/TPoJS+/5M9iPt+tGDciHPIp0HvUuA root@app02
The key's randomart image is:
+---[RSA 2048]----+
      ..=0+ . .
      . = . * o . |
      + 0 0 + 0 .
      . 0 0 = 0 0.
         S + 0 o o|
           E @ 0
             8 + +
           + + *.
            .=00.+|
+----[SHA256]----+
psadmin@app02:/etc/ssh$
```

psadmin@app02: /etc/ssh
File Edit View Search Terminal Help
<pre>psadmin@app02:/etc/ssh\$ ls -l</pre>
total 596
-rw-rr 1 root root 553122 Feb 10 2018 moduli
-rw-rr 1 root root 1580 Feb 10 2018 ssh_config
-rw-rr l root root 3264 Mar 4 2019 sshd_config
-rw 1 root root 672 Sep 3 2019 ssh_host_dsa_key
-rw-rr 1 root root 600 Sep 3 2019 ssh_host_dsa_key.pub
-rw 1 root root 227 Aug 6 2019 ssh_host_ecdsa_key
-rw-rr 1 root root 172 Aug 6 2019 ssh_host_ecdsa_key.pub
-rw 1 root root 399 Aug 6 2019 ssh_host_ed25519_key
-rw-rr 1 root root 92 Aug 6 2019 ssh_host_ed25519_key.pub
-rw 1 root root 1679 Aug 6 2019 ssh_host_rsa_key
-rw-rr 1 root root 392 Aug 6 2019 ssh_host_rsa_key.pub
-rw-rr 1 root root 338 Aug 6 2019 ssh_import_id
-rw 1 root root 1766 Jan 14 09:02 Test_Key
-rw-rr 1 root root _ 392 Jan 14 09:02 Test_Key.pub
<pre>psadmin@app02:/etc/ssh\$</pre>

Following the creation of the private/public key pair, we can use the following commands to generate the MD5 and/or SHA-256 hash keys that need to be used in the SFTP recipient configuration in the Axis device (see *Axis device configuration on page 260*). Note that it's possible to create both an MD5 and/or SHA-256 hash key from either of the generated public host keys above. In the below example, we generate an MD5 or a SHA-256 hash key from the different public host keys.

Network protocols

Command	Example output	Description
sudo ssh-keygen -I -E md5 -f ssh_host_rsa_key.pub	b800c8958b8679a7bd66c13669051466	Generates an MD5 hash from RSA public key
sudo ssh-keygen -I -E sha256 -f ssh_host_rsa_key.pub	gUYVTq8MVXMaf/TPoJS+/5M9iPt+tGD- ciHPIpOHvUuA	Generates a SHA-256 hash from RSA public key
sudo ssh-keygen -l -E sha256 -f ssh_host_ecdsa_key	xSUNCp2sUM0fvUE- JFDq7PWtRoBQej/t5NgwS7NMLI2k	Generates a SHA-256 hash from ECDSA public key
sudo ssh-keygen -l -E sha256 -f ssh_host_ed25519_key	21NFP8emqsMLejiG3Nxco2D64lZhd- MiseDmpXiSaTj0	Generates a SHA-256 hash from ED25519 public key

psadmin@app02: /etc/ssh

```
File Edit View Search Terminal Help
psadmin@app02:/etc/ssh$ sudo ssh-keygen -l -E md5 -f Test_Key.pub
2048 MD5:b8:00:c8:95:8b:86:79:a7:bd:66:c1:36:69:05:14:66 root@app02 (RSA)
psadmin@app02:/etc/ssh$ sudo ssh-keygen -l -E sha256 -f Test_Key.pub
2048 SHA256:gUYVTq8MVXMaf/TPoJS+/5M9iPt+tGDciHPIp0HvUuA root@app02 (RSA)
psadmin@app02:/etc/ssh$
```

While the Axis device supports both MD5 and SHA-256 hash keys, it's recommended to use SHA-256 due to stronger security over MD5.

Axis device configuration

When creating a new SFTP recipient, please make sure to enter the right MD5 or SHA256 fingerprint of the host key that is used by your SFTP server. Based on the public/private key we created previously and the MD5 or SHA-256 hash keys we generated from the public host key (see *3rd party SFTP server on page 256*), the SFTP recipient in the Axis device would look as below:

Network protocols

Add recipient				
Name				
SFTP Server Test				
Туре				
SFTP •				
Host				
172.25.201.102				
Port				
22				
Folder				
Username				
psadmin				
Password				
				0
SSH host public key type				
MD5				
O SHA256				
SSH host public key (32 byte Hex)				
b800c8958b8679a7bd66c13669051466				
Use temporary file name				
Test	Cano	el.	Sav	e

Network protocols

Add recipient		
Name		
SFTP Server Test		
Туре		
SFTP 👻		
Host		
172.25.201.102		
Port		
22		
Folder		
Username		
psadmin		
Password		
		Ø
SSH host public key type		
MD5		
SHA256		
SSH host public key (Base64)		
gUYVTq8MVXMaf/TPoJS+/5M9iPt+tGD	ciHPIp0HvUuA	
Use temporary file name		
Test	Cancel	Save

After the SFTP recipient has been created, action rules for image and/or video clip transfer can be created.

Network protocols

Add rule		
Action		
Send images through SFTP		-
Recipient		
SFTP Server		-
Create folder		
Filename		
image%y-%m-%d_%H-%M-%S-%f_#s.jpg		
Maximum sequence number (0 = ∞)		
0		
Camera		
View Area 1		
Stream profile		
None		-
Custom image frequency		
Prebuffer		
03 seconds		
Postbuffer		
00:05 MM:SS		
Maximum images (0 = ∞)		
1		
	Cancel	Save

Network protocols

Add rule			
Action			
Send video clip th	rough SFTP		•
Recipient			
SFTP Server			-
Create folder			
Filename			
video%y-%m-%d_%	6H-%M-%S-%f_#s.mk	v	
Camera View Area 1			_]
			•
Stream profile			
None			•
Prebuffer			
03	seconds		
Postbuffer			
00:05	MM:SS		
		Cancel	Save

IPv4 compliant mode

Since long ago, the default IP address of Axis devices has been 192.168.0.90 in case of no DHCP server being available on the network. The link-local address (169.254.0.0/16) has also always been on by default. In other words, the camera's interface has a routable address and an IPv4 link-local address configured simultaneously. However, this is not recommended by the RFC document.

Secondly, If an Axis device is configured with a static IPv4 address, it will use it regardless of whether anyone on the same network segment uses it. However, this will cause service interruptions for the other devices.

Network protocols

IP AXIS IP Utility		- 0	×
File View Tools Help			
😤 🎲 🗲		Type to filter	×
Name	IP Address	Serial Number	
AXIS P1375 - B8A44F42B8B0	192.168.0.90	B8A44F42B8B0	
AXIS P1375 - B8A44F42B4C6	192.168.0.90	B8A44F42B4C6	
AXIS Q3527-LVE - ACCC8EB05E83	192.168.0.90	ACCC8EB05E83	
192.168.0.90/24 169.254.217.205/16 192.168.0.90/24 169.254.72.129/16		NO DHC	CP server

For the aforementioned reasons, we decided to make changes to IPv4 addressing:

- To be completely RFC IPv4 compliant
- Disable link-local address when it is not used
- Better user experience for our customers, when multiple factory-defaulted Axis devices, are placed on the same network simultaneously
- Address conflict detection and resolution

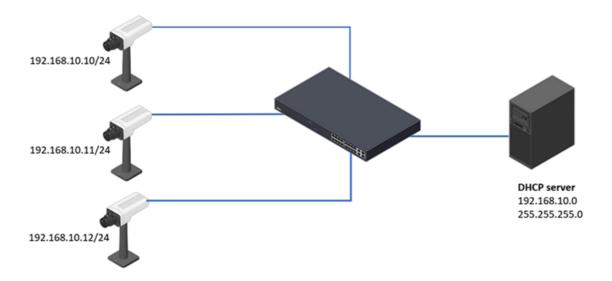
With AXIS OS 11.7 and later, we add:

- 1. A new "Auto Link-local mode" will be triggered if there is an address conflict on the static address or, a valid DHCP offer is unavailable on the network.
- 2. Address conflict detection for a static address. If conflict is detected, the Axis devices will not take any IP addresses used by other devices. It will fall back to the link-local address (in auto link-local mode).

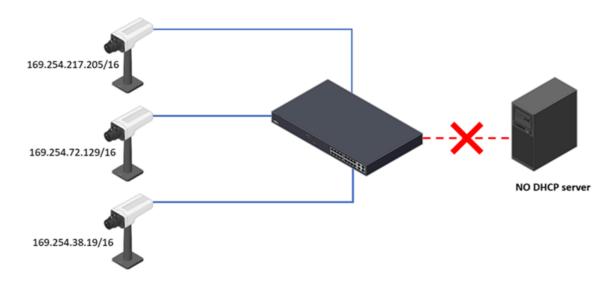
Network protocols

What do these changes mean to you?

1. If you have a DHCPv4 server in your network, the factory-defaulted Axis devices will take the offer from the DHCP server. The Axis device will only have one IPv4 address configured and the link-local address will not be available.

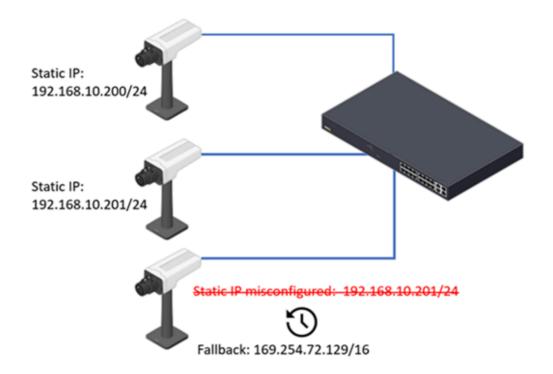


2. If you don't have a DHCPv4 server in your network, a factory default Axis device will no longer use 192.168.0.90/24 as the default IP address. Instead, a link-local address(169.254.0.0./16) will be configured.

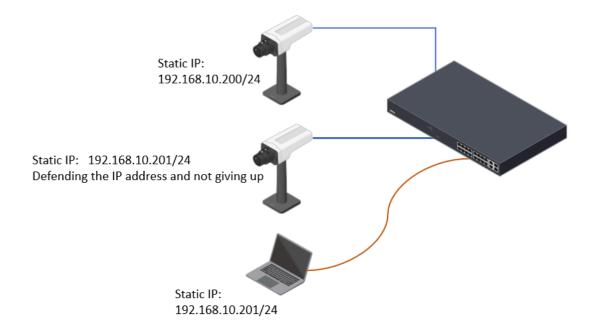


3. If you manually configured static IP addresses for multiple Axis devices. However, one IP address has been misconfigured on more than one unit. Only the first unit will use that specific IP address when you connect those devices to your network. The second and later units will fall back to the link-local address.

Network protocols



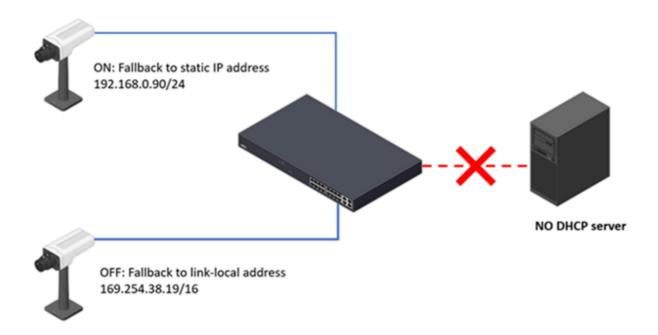
4. If an Axis device is running with a static IP address, another device with the same IP address is later connected to the network. In line with RFC recommendations, the Axis device will defend the current IP address and keep the IP address under any circumstances.



Network protocols

By default, the camera will fall back to the link-local address when no DHCP server is not available in your network. To make the transition smoother, we have added a setting (System > Network > IPv4) allowing customers to select fallback to the static IP address or link-local address when the DHCPv4 offer is unavailable.

- ON. When DHCP fails to obtain a lease, the static address is configured.
- OFF. When DHCP fails to obtain a lease, the link-local address is configured.



How to find those devices if the Axis devices fall back to the link-local address?

Find the network interface card on your computer connecting to the same LAN where the Axis devices sit. The network interface card of the PC should also have a link-local address configured. To configure a link-local address, follow the steps of one of the following three options.

- OPTION 1: Automatically assign link-local address when the DHCP server is not available
 - 1. Right-click the network interface, select **Properties**, select **Internet Protocol Version 4 (TCP/IPv4)**, then click on **Properties**.

Network protocols

	Ethernet Properties Networking Authentication Sharing	×
Contraction of the second seco	Connect using:	
Ethernet	Intel(R) Ethemet Connection (14) I219-V	
	Configure This connection uses the following items:	
	 Npcap Packet Driver (NPCAP) QoS Packet Scheduler Bridge Driver Internet Protocol Version 4 (TCP/IPv4) Microsoft Network Adapter Multiplexor Protocol Microsoft LLDP Protocol Driver Internet Protocol Version 6 (TCP/IPv6) 	
	wide area network protocol that provides communication across diverse interconnected networks.	

2. Select Obtain an IP address automatically and click OK.

Network protocols

Internet Protocol Version 4 (TCP/IPv4) Properties	\times
General Alternate Configuration	
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.	
Obtain an IP address automatically	
O Use the following IP address:	- 1
IP address:	
Subnet mask:	
Default gateway:	
 Obtain DNS server address automatically 	
OUse the following DNS server addresses:	1
Preferred DNS server:	
Alternate DNS server:	
Validate settings upon exit	
OK Cancel	

3. The Windows PC will automatically assign a link-local address to the network interface card.

Network protocols

```
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . : fe80::bdb2:adb3:cfd5:ad76%22
Autoconfiguration IPv4 Address. . : 169.254.178.84
Subnet Mask . . . . . . . . . : 255.255.0.0
Default Gateway . . . . . . . :
```

4. Now the IP Utility can discover devices that fall back to link-local address.

			C Q	
	Name	IP address	Serial number	
	AXIS Q3527-LVE	169.254.65.163	ACCC8EB05E83	
	IPv4	ACCC8EB05E83	Network connection 169.3 IPv6 IPv6 (link-local)	254.178.84 🗍
	😢 IP settings	Device web (2	
\Box	AXIS P1375	169.254.1.223	B8A44F42B8AB	
\Box	AXIS P1375	169.254.168.20	B8A44F42B4C6	
<				2
Showin	g 3 of 3 devices			→ Export

• OPTION 2: Manually assign a link-local address when the DHCP server is not available

Network protocols

1. Right-click the network interface, select **Properties**, select **Internet Protocol Version 4 (TCP/IPv4)**, then click on **Properties**.

	Ethernet Properties	<
	Networking Authentication Sharing	
	Connect using:	
Ethernet	Intel(R) Ethemet Connection (14) I219-V	
	Configure	
	This connection uses the following items:	
	 Ppcap Packet Driver (NPCAP) QoS Packet Scheduler 	
	Bridge Driver	
	Internet Protocol Version 4 (TCP/IPv4) Internet Protocol Version 4 (TCP/IPv4) Internet Protocol Inter	
	Microsoft LLDP Protocol Driver	
	✓ Internet Protocol Version 6 (TCP/IPv6)	
	Install Uninstall Properties	
	Description	
	Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.	
	OK Cancel)

2. Manually assign a link-local address. You can use any unused IP address within the 169.254.0.0/16 range, with the exception of 169.254.0.0 and 169.254.255.255.

Network protocols

Internet Protocol Version 4 (TCP/IPv4)	Properties	\times
General		
You can get IP settings assigned autor this capability. Otherwise, you need to for the appropriate IP settings.		
Obtain an IP address automatical	ly	
O Use the following IP address:		
IP address:	169 . 254 . 0 . 90	
Subnet mask:	255.255.0.0	
Default gateway:		
Obtain DNS server address auton	natically	
O Use the following DNS server add	resses:	
Preferred DNS server:		
Alternate DNS server:		
Validate settings upon exit	Advanced	
	OK Cancel	

3. Now the IP Utility can discover devices that fall back to link-local address.

Network protocols

IP Ut	tility				_		>
				C Q			
(Name	IP address	Serial number			
(AXIS Q3527-LVE	169.254.65.163	ACCC8EB05E83			
		Serial number IPv4	ACCC8EB05E83	Network connection	169.254.0.90	0	
		IPv4 (link-local)	169.254.65.163 🗌	IРvб (link-local)			
		🔞 IP settings	Device web [3			
(AXIS P1375	169.254.168.20	B8A44F42B4C6			
(AXIS P1375	169.254.1.223	B8A44F42B8AB			
<						\rightarrow	
Sh	owing	g 3 of 3 devices			$\mid \rightarrow$	Export	

- OPTION 3: Add link-local address to the network interface card when a routable address is configured
 - 1. Right-click the network interface, select **Properties**, select **Internet Protocol Version 4 (TCP/IPv4)**, then click on **Properties**.

Network protocols

	Ethernet Properties Networking Authentication Sharing	×
	Connect using:	
Ethernet	Intel(R) Ethernet Connection (14) I219-V	
	Configure This connection uses the following items:	
	 Npcap Packet Driver (NPCAP) QoS Packet Scheduler Bridge Driver Internet Protocol Version 4 (TCP/IPv4) Microsoft Network Adapter Multiplexor Protocol Microsoft LLDP Protocol Driver Internet Protocol Version 6 (TCP/IPv6) 	
	Install Uninstall Properties Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.	
	OK Cancel	

2. The network interface card already has an IP address 192.168.0.120/24 configured. Click Advanced to add an additional link-local address.

Network protocols

Internet Protocol Version 4 (TCP/IPv4)	Properties	×
General		
You can get IP settings assigned autom this capability. Otherwise, you need to for the appropriate IP settings.		
Obtain an IP address automatical	у	
O Use the following IP address:		
IP address:	192.168.0.120	
Subnet mask:	255 . 255 . 255 . 0	
Default gateway:		
Obtain DNS server address autom	natically	
 Use the following DNS server address 	resses:	
Preferred DNS server:		
Alternate DNS server:		
Validate settings upon exit	Advanced	
	OK Cancel	

3. Click Add under IP addresses to add the link-local address. You can use any unused IP address within the 169.254.0.0/16 range, with the exception of 169.254.0.0 and 169.254.255.255.

Network protocols

Advanced TCP/IP Settings	\times
IP Settings DNS WINS	
IP addresses	
IP address	Subnet mask
192.168.0.120	255.255.255.0
169.254.0.90	255.255.0.0
Add	Edit Remove
Default gateways:	
Gateway	Metric
Add	Edit Remove
Add	Edit Remove
Automatic metric	
Interface metric:	
	OK Cancel

4. The Network Interface card should now have two IP addresses configured.

Network protocols

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . : fe80::bdb2:adb3:cfd5:ad76%22

IPv4 Address. . . . . . . . : 192.168.0.120

Subnet Mask . . . . . . . . : 255.255.255.0

IPv4 Address. . . . . . . . : 169.254.0.90

Subnet Mask . . . . . . . . : 255.255.0.0

Default Gateway . . . . . . . :
```

5. Now the IP Utility can discover devices that fall back to link-local address.

Network protocols

IP Utility				—		
			C Q			
	Name	IP address	Serial number			
	AXIS Q3527-LVE	169.254.65.163	ACCC8EB05E83			
	Serial number IPv4	ACCC8EB05E83	Network connection	169.254.0.90	0	
		169.254.65.163 🗌				
	🔞 IP settings	Device web (2			
\Box	AXIS P1375	169.254.168.20	B8A44F42B4C6			
\Box	AXIS P1375	169.254.1.223	B8A44F42B8AB			
<					\rightarrow	
Showir	ng 3 of 3 devices			$ \rightarrow$	Export	

When will this new IPv4 compliant mode enabled by default and how to test it?

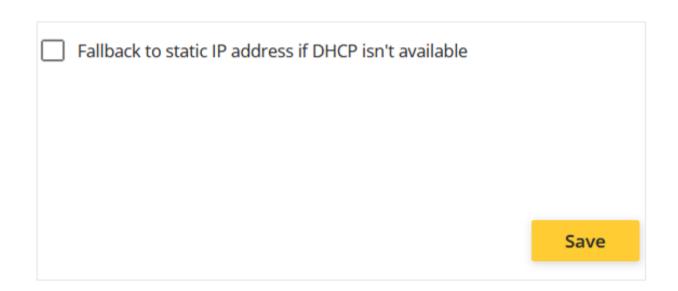
With AXIS OS 11.7 and later, the new IPv4 compliant mode has been implemented but it is disabled in the factory defaulted state. The current plan is to make it enabled by default in AXIS OS 12.0, which will be released in September 2024.

To try the IPv4 compliant mode, it can be enabled by changing the following parameters:

Step 1

Go to system----Network, uncheck "Fallback to static IP address if DHCP isn't available" and save.

Network protocols



Step 2

Go to System-Plain config-Network-Network/ZeroConf, check "Fallback" and save.

Network / ZeroConf
Enabled
✓ Fallback
IP address
169.254.253.240
Subnet mask
255.255.0.0

O3C (one-click cloud connection)

O3C (one-click cloud connection) is a protocol that allows an Axis device to connect via secure connection to a cloud video management system, such as Genetec Stratocast. In order to connect an Axis device, the so called OAK (owner authentication key) is needed. See instructions for how to look up the OAK below.

With each Axis device, you receive a piece of paper with the OAK printed on it. As mentioned, you need the OAK to verify ownership when you register the device with an O3C-based service. Keep this document in a safe place – it's a certificate that should not

Network protocols

be discarded or disclosed to third parties. If you have lost your OAK, you can retrieve it by logging in to the device as an admin user. Follow one of the paths below, depending on the AXIS OS version of your device.

Note

This requires that the device runs AXIS OS 5.51.7, 6.50.5.2, 8.40.4, 9.80.2, 10.0.0 or higher. Please upgrade if your device is running a lower version. Axis cannot assist in retrieving the OAK for you. For the external retrieval, an outgoing HTTPS (TCP port 443) connection to "oakcgi.o3c.axis.com" needs to be available.

AXIS OS 5.51 & LTS 216 (AXIS OS 6.50) Go to Setup > Options > Support > System Overview.

Basic Setup	System	Overv	iew				
basic Setup	Firmware vers	ion:			Serial number:		
Video					OAK:		
	IP address:				Date & Time	2022-01-24	07:55:31
Live View Config	Connected cl	lents: 0 Vid	ieo <u>(Vie</u> v	v log)	Uptime: 242 da	ys, 23:36	
PTZ	Recently used	bandwidth:	0.05 Mbit/s		Time mode: NT	P	
F12	Security						
Detectors	Defined users	2 Anonymo	us access:	Disabled	HTTPS: No	IP address	filter: Off
	Optional Ne	twork Serv	vices				
Applications	Service			Enabled	Proto	col	Server port
Events	FTP			Yes	TCF	,	21
Lycinta	RTSP			Yes	TCF	,	554
Recordings	Bonjour			Yes	UDI	P	5353
-	HTTPS			No	TCF	>	443
Languages	SNMP			No	UDI	P	161
Custom Ontions	<u>UPnP™</u>			Yes	UDI		1900
System Options Security					TCF)	49152 (auto)
Date & Time	ARP/Ping IF	<u>address se</u>	tting	Yes	-		-
Network	Link-local ad	<u>idress</u>		Yes	-		-
Storage	NAT travers	al		No	-		-
Ports & Devices	SOCKS			No	-		
Maintenance	AXIS Intern		DNS	No	-		-
- Support	IP address f	ilter		No	-		-
Support Overview	Event Setting	<u>js</u>					
System Overview Logs & Reports	Rules defined:	3	Rules enab	led: 1			
Advanced	Image Setti	ings					
		Res.	Comp.	Rot	. Color	Overlay	Source
About	Camera	4CIF	30	0	Yes	None	PAL

LTS 2018 (AXIS OS 8.40) & LTS 2020 (AXIS OS 9.80) Go to System > AVHS and click on Get key.

Network protocols

AVHS

Allow AVH				r authentication key	(OAK)	
Proxy se				t key		
Host		Port 3128		ure the device is conne a firewall or proxy.	ected to the internet	
Login						
Password						
Authentica	ation method					
Basic			r			
		Save				
Apps Sy	rstem					
	38		-		а	ŕ.
Date and time	Orientation	Users	ONVIF	SNMP	Maintenance	Plain co
		53613			Mantonarios	T laint de
AVHS	Security	Storage	Events	Detectors		

AXIS OS 10.0 or higher Go to System > O3C and click on Get key.

Network protocols

One-click cloud connect

Aller	w O3C		Ownor	authentication key	(04K)	
	e-click	Ψ.	Owner	authentication key	(OAR)	
Pro		Port 3128			nnected to the internet	
A-0-0.0	sword entication method sic					
		Save				
ivacy mask	View area Apps	System				
	38	÷	Citvu	SNMP		¢
Date and tim	e Orientation	Users	ONVIF	SNMP	Events	Dete
æ	•			\mathcal{I}	ť	9
O3C	Security	Storage	I/O ports	MQTT	Accessories	Plain

AXIS OS 10.9 or higher

Go to System > Network and click on Get key. Note that this applies to devices with support for the new web interface introduced in AXIS OS 10.9. For products that don't support the new web interface yet, follow the above instructions for AXIS OS 10.0.

🖌 Apps							
Image: System Owner authentication key (OAK)							
🛗 Date and time		Get key					
😵 Network		Make sure the device is connected to the internet without a firewall or proxy.					
Security							
💄 Users		CNIMD					

Web interface

Web interface

Browser support

AXIS OS 7.10 and higher

Video products with AXIS OS 7.10 or higher include the new web interface, which comes with an overall improved and simplified graphical user interface and focuses on camera installation, configuration, and troubleshooting. The web interface is tested and optimized for Chrome[™] and Firefox[®] browsers. It is platform-independent and works with Windows[®] (versions 7 through 10) as well as Linux[®] and OS X[®]. If you use other browsers, you could experience limitations in functionality and support. You can find more information about the latest AXIS OS version of your Axis product *here*.

You can use the device with the following browsers:

	Chrome TM	Firefox®	Edge™	Safari®
Windows®	recommended	recommended	\checkmark	
macOS®	recommended	recommended	\checkmark	\checkmark
Linux®	recommended	recommended	\checkmark	
Other operating systems	\checkmark	\checkmark	\checkmark	√*

*To use AXIS OS web interface with iOS 15 or iPadOS 15, go to **Settings > Safari > Advanced > Experimental Features** and disable NSURLSession Websocket.

To find out more about how to use the device, see the user manual available at axis.com.

If you need more information about recommended browsers, go to AXIS OS Portal.

Highlights

- Recommended browser: Latest Chrome and Firefox
- Supported browser: Latest Chrome, Firefox, Edge and Safari
- Platform-independent with latest Linux, OS X and Windows 7 through Windows 10
- Support for tablet and mobile devices
- 12 pre-installed languages and automatic language detection

Known limitations

- Edge: 1-second video delay when streaming H.264
- Safari, Chrome, Firefox: No support for H.264 video streaming in Apple mobile (iOS) devices
- Audio: No support for sending audio to the camera through the browser (i.e. through a computer microphone)
- Video: Some browser plugins are known to cause problems with live streaming. Try uninstalling plugins if the video does not play as it should.
- Video: H.265 video streaming is currently not supported in any browser
- Because the setting for NSURLSession Websocket can no longer be toggled off in iOS and IpadOS 17.0 and higher, anonymous viewers are required to be able to sign in via a web browser on iOS or IpadOS 17.0 or higher.

Video streaming

AXIS Media Control is no longer required for video streaming H.264 or RTSP. Displaying H.264 and RTSP video streams in the web interface (e.g. live view or when setting up analytics) requires that the browser can connect over WebSockets. Support for RTSP video streams over WebSockets requires an updated browser and that the network and proxy settings are configured to allow WebSockets.

Web interface

The viewing experience depends on the performance of the computer, the browser, and its encoding capabilities. If a video stream is lagging, the web interface either notifies the user or restarts the video stream automatically in case it lags a lot. If the user experiences continuous lagging, they should adapt to the computer's performance by lowering the resolution of the video stream stepwise. When viewing video streams in higher resolutions than 1080 pixels, they should use a computer with a powerful CPU and graphics card.*

*Tested and verified with the following configuration: Google Chrome[™] (latest version) on Windows[®] 10 or Linux, Intel[®] Core[™] i7-4770 Processor 3.40 Ghz with NVIDIA[®] GeForce[®] GTX[™] 950 or Intel[™] HD Graphics 4600.

Note

On some Linux systems, the web page might flicker when MJPEG is used. This can be resolved by turning off hardware acceleration in the browser.

AXIS OS 6.5X or lower

Video products with AXIS OS 6.5X or lower are tested and optimized for the latest version of Internet Explorer*, Windows, and AXIS Media Control (AMC). Although you can use other browsers, versions and operating systems, you might experience limitations in functionality and support. You can find more information about the latest AXIS OS version of your Axis product *here*.

Highlights

- Recommended browser: Internet Explorer* with AXIS Media Control
- Recommended for Windows operating system

Known limitations

- QuickTime player introduces a 3-second video delay when streaming
- Java applet-based clients only support one-way audio, and the audio quality, as well as the frame rate, might be reduced
- When using video products with AXIS OS 5.50 or lower and IE10, compatibility mode is recommended

Video streaming

AXIS Media Control and Internet Explorer* is required for video streaming H.264 over HTTP/RTSP/RTP. MJPEG video streaming is supported by Chrome, Firefox and Safari.

* Read more about Internet Explorer limitations in Internet Explorer mode in Edge on page 285.

Internet Explorer mode in Edge

Internet Explorer was previously used to view H.264 using AXIS Media Control and to configure the legacy embedded Video Motion Detection. Since Internet Explorer is outdated and unsupported, Microsoft Edge can be used for this purpose instead if set to *Internet Explorer mode*. Simply follow the steps below.

Note

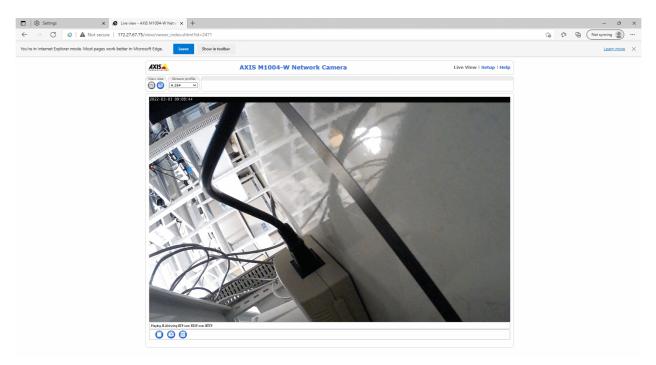
If using Windows 11 and the error message "Internet Explorer can't be found. you need to re-install or re-enable Internet Explorer" appears, first follow the steps in *this guide*.

- Go to Settings > Default browser.
- Set Allow sites to be reloaded in Internet Explorer mode to "Allow".
- Click "Add" next to Internet Explorer mode pages and enter the IP address of the Axis device.

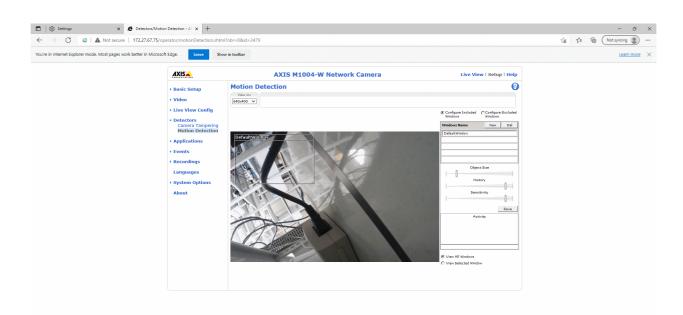
Web interface

ettings	Default browser					
Q. Search settings	Make Microsoft Edge your default browser		Make	default		
Profiles						
Privacy, search, and services						
③ Appearance	Internet Explorer compatibility					
Start, home, and new tabs	Let Internet Explorer open sites in Microsoft Edge 💿	Incompatible	e sites only (Recommender	0 ~		
Share, copy and paste	When browsing in Internet Explorer you can choose to automatically		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			
Cookies and site permissions	Microsoft Edge					
Default browser						
Downloads	Allow sites to be reloaded in Internet Explorer mode 📀			N ~		
Family safety	When browsing in Microsoft Edge, if a site requires Internet Explore Explorer mode	r for compatibility, you can choose to relo	ad it in Internet			
Languages						
Printers	Internet Explorer mode pages These pages will open in Internet Explorer mode for 30 days from th	ne date you add the page. You have 1 pag	e that'll automatically open in	Add		
! System	Internet Explorer mode.					
Reset settings	Page	Date added	Expires			
Phone and other devices	http://172.27.67.75/	03/03/2022	02/04/2022	Û		
Accessibility						
About Microsoft Edge						

When done, Edge will work the same way as Internet Explorer for that particular device.



Web interface



Configuration tips

How to use HTTP POST notifications in action rules
How to publish an MQTT message with an event rule action
How to add MQTT subscriptions
How to set SD card wear level
Automatic rollback verification
How to add polygon privacy masks
How to set privacy mask properties
How to perform a rollback
How to display live view stream statistics
Password security confirmation check
How to enable SD card encryption
How to enable Opus audio codecs

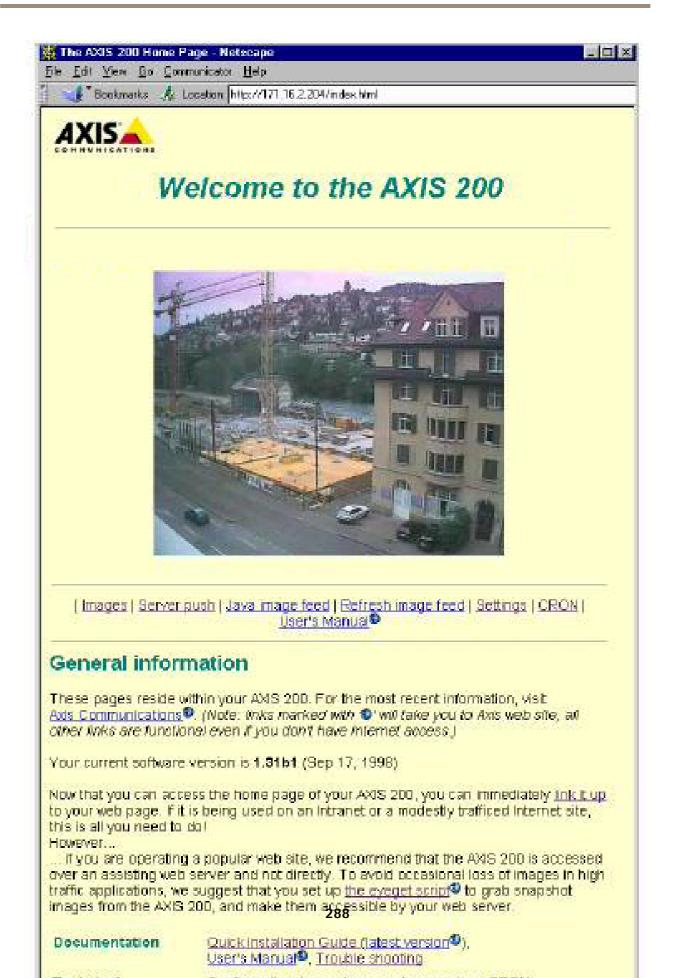
Web user interface versions

When discussing various features and problems, it can sometimes be important to clarify which version of the web user interface is used. Axis devices have had several different user interfaces throughout the years.

Axis released the first network camera, AXIS Neteye 200, in 1996. The web interface in may seem quite rudimentary by today's standards but was very much on par with everything else on the world wide web back then. (It can be noted that NCSA Mosaic, one of the first widely available and popular web browsers was released only three years prior, so Axis was in the game very early on.)

AXIS 200:

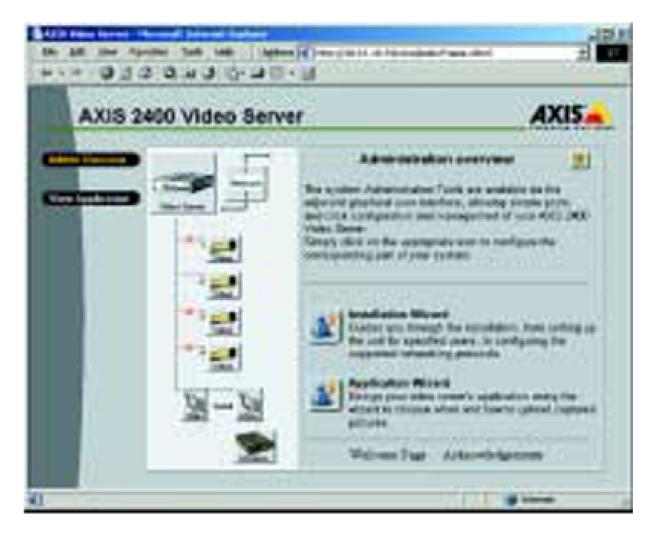
Web interface



Web interface

Only a couple of years later, Axis released their first encoders, or "video servers" as they were called back then; Axis 2400/2401. The web interface in these products had graphical representations of what was connected. It was also possible to control Pan-Tilt-Zoom on connected cameras directly from this web interface.

AXIS 2400:



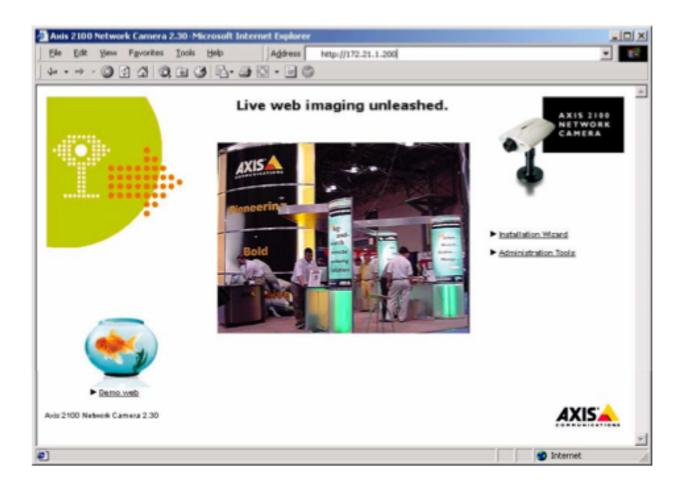
Web interface



In 1999, Axis released the first Linux based network camera, AXIS 2100. And with that, once again a brand new web interface. Unlike the gray interface in AXIS 2400/2410 that was intended for the conservative surveillance market, this interface targeted the younger web generation and thus was brighter and shinier.

AXIS 2100:

Web interface

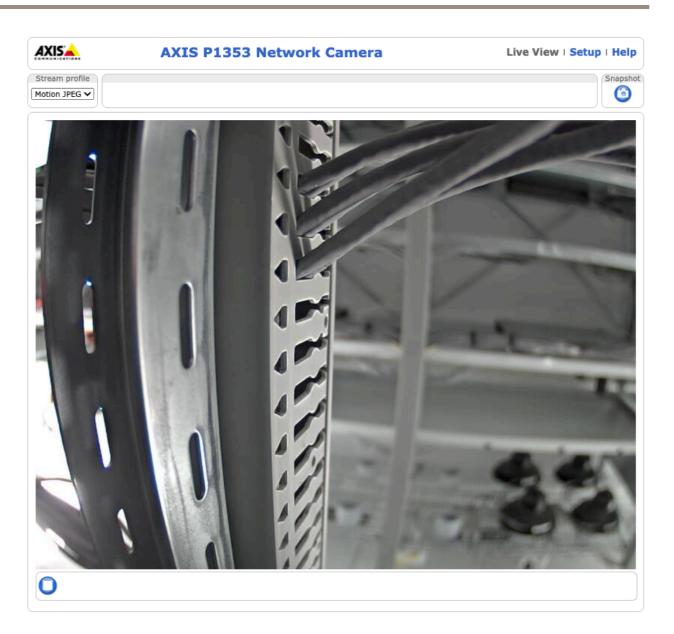


The two separate web interfaces for encoders and cameras lived side by side for a few years, but by 2003, the time had come to introduce a web interface that worked for both cameras and encoders. This interface version lived on all the way until 2016 (in different iterations) and has become what we sometime refer to as "Classic". We will continue to refer to it as "AXIS OS web version A (Classic)".

AXIS OS web version A (Classic)

The first version of AXIS OS web version A (Classic) was introduced in AXIS OS 4.0, but is now only supported in LTS 2016 (6.50). With the introduction of AXIS OS 7.10, this version was no longer the default interface, but it was still available via the URL *http://camera-ip/index.shtml* up until AXIS OS 9.20, after which it was completely removed.

Web interface



Web interface

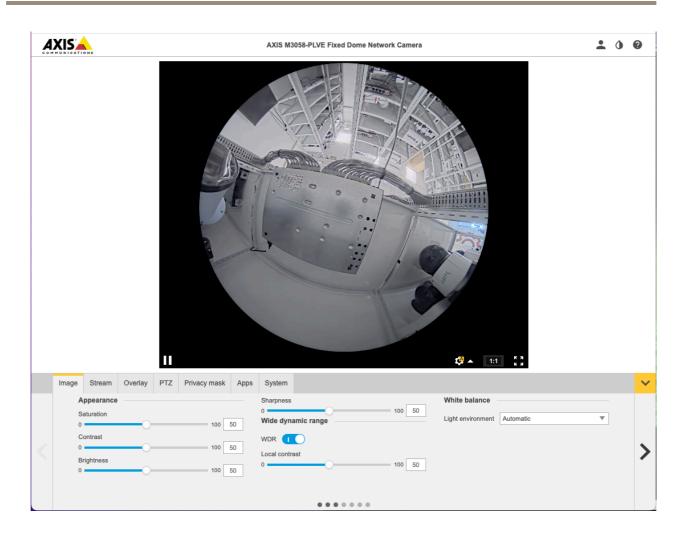
	IS P1353 Network Camera Live View Setup Help
• Basic Setup	Video Stream Settings
- Video & Audio	Image Audio H.264 MJPEG
Video Stream	Image Appearance
Stream Profiles	Resolution: 800x600 (4:3) V pixels
ONVIF Media Profiles	Compression: 30 [0100]
Camera Settings Overlay Image	Mirror image
Privacy Mask	Rotate image: 0 V degrees
Focus	Video Stream
Audio Settings	Maximum frame rate:
Audio Clips	Unlimited
Live View Config	Limited to [130] fps per viewer
	Overlay Settings
Detectors	Include overlay image at the coordinates: X [0] [0] Y [0] [0]
Applications	Include date Include time
Events	Include text:
Events	Text overlay size: medium
Recordings	Text color: White V Text background color: black V
	Place text/date/time at top 🗸 of image
Languages	
System Options	
About	Preview
	View image stream while configuring. Video format: MJPEG Open Save Reset

While AXIS OS web version A (Classic) lasted for 13 years, the rest of the world wide web moved on. In 2017, it was finally time to introduce AXIS OS web version B.

AXIS OS web version B

AXIS OS web version B had a more modern look than the previous version, and also supported a much wider range of browsers (including native support for H.264 streaming). Here, focus was on the video stream, and a key feature was the possibility to actually see the video while fine tuning image settings.

Web interface



This interface was officially introduced with Axis OS 7.10, but a preview version could be seen already in AXIS OS 6.50 via the URL *http://camera-ip/index.html.* LTS 2018 (8.40) and LTS 2020 (9.80) both use this interface. Note that it is only intended to be used with video products.

Axis product portfolio has been growing over time and now includes many more product types than just video products. Since AXIS OS web version B only supported video products, it soon became important to create a user interface that would work for all types of products. So, in 2020, AXIS OS web version C was introduced.

AXIS OS web version C

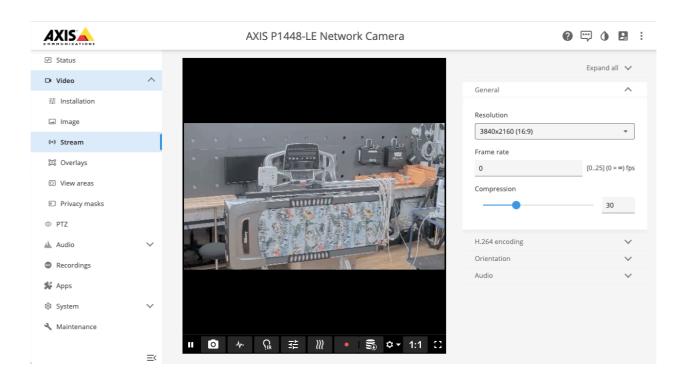
AXIS S3008 Recorder was the first product to officially get AXIS OS web version C, which was introduced with AXIS OS 10.0.0.

Web interface

	AXIS S3008 Recorder 🛛 😨 🛈			
🖂 Status				
Recordings	Onboard storage			
😫 Apps	🔀 Hard drive 1 (3.4 TB)			
🕸 System 🔨				
Date and time	Free: 100% Status: Mounted			
Network	File system: ext4 Encrypted: No Temperature: 45 °C (113 °F)			
Power over Ethernet	Overall health test: Passed			
Security	Write protect 🕥 🛈			
💄 Users				
👼 Storage	Tools			
ê Logs	Check Repair			
SSH server	O Format O Encrypt			
A Maintenance	O Decrypt O Change pass	sword		
•	Use tool			

Most video products had to wait some time before officially getting AXIS OS web version C, but it could be reached through *http://camera-ip/preview/index.html* already in 10.0 on a selected number of products (ARTPEC-7).

Web interface



API

API

VAPIX

VAPIX[®] Network Video API is a set of Application Programming Interfaces (API) for configuration and management of Axis network video products. For more information, visit the VAPIX Library.

You can use tools like Postman or cURL to interact with the VAPIX API. cURL offers a command-line alternative for sending API requests and retrieving data, while Postman provides a user-friendly interface for sending HTTP requests and viewing responses, making it ideal for testing and exploring the VAPIX API. Both tools enable you to experiment with API calls, troubleshoot issues, and develop custom integrations.

For examples on how to use cURL, see the VAPIX Library. To learn more about VAPIX and Postman, click here.

New APIs for configuring AXIS OS devices

AXIS has released new APIs for AXIS OS configuration. These APIs were introduced in AXIS OS 11.11, and more device configuration APIs will be added on an ongoing basis. See AXIS OS demonstration video *here*.

Available APIs can be seen on the device itself by typing: http://IP-adress/config/discover

API

```
Pretty-print 🗌
```

```
"apis": {
          "best-snapshot": {
                 "v1": {
    "doc": "/config/discover/apis/best-snapshot/v1/doc.md",
    "doc_html": "/config/web-ui/cu-doc.html?md-doc-loc=/config/discover/apis/best-snapshot/v1/doc.md",
    "doc_html": "/config/web-ui/cu-doc.html?md-doc-loc=/config/web-ui/cu-doc.md",
    "doc_html": "/config/web-ui/cu-doc.html?md-doc-loc=/config/web-ui/cu-doc.md",
    "doc_html": "/config/web-ui/cu-doc.html?md-doc-loc=/config/web-ui/cu-doc.md",
    "doc_html": "/config/web-ui/cu-doc.md",
    "doc_html": "/config/web-ui/cu-doc.md",
    "doc_html": "/config/web-ui/cu-doc.md",
    "doc_html": "/config/web-ui/cu-doc.md",
    "doc_html": "/config/web-ui/cu-doc.md",
    "doc_html": "/config/web-ui/cu-doc.md",
    "doc_html": "/config/web-ui/cu-doc_html": "/config/web-ui/cu-doc_html",
    "doc_html": "/config/web-ui/cu-doc_html": "/config/web-ui/cu-doc_html";
    "doc_html": "/config/web-ui/cu-doc_html;
    "doc_html": "/config/web-ui/cu-doc_html;
    "doc_html;
    "do
                            "model": "/config/discover/apis/best-snapshot/v1/model.json",
                           "rest_api": "/config/rest/best-snapshot/v1beta",
                          "rest_openapi": "/config/discover/apis/best-snapshot/v1/openapi.json",
"rest_ui": "/config/web-ui/swagger-ui/?url=/config/discover/apis/best-snapshot/v1/openapi.json",
                           "state": "beta",
                             "version": "1.0.0-beta.1"
                 }
      },
"cert": {
.". {
                  ert : {
"v1": {
"doc": "/config/discover/apis/cert/v1/doc.md",
"doc_html": "/config/web-ui/cu-doc.html?md-doc-loc=/config/discover/apis/cert/v1/doc.md",
                         "model": "/config/discover/apis/cert/v1/model.json",
"rest_api": "/config/discover/apis/cert/v1/openapi.json",
                          "rest_ui": "/config/web-ui/swagger-ui/?url=/config/discover/apis/cert/v1/openapi.json",
"state": "beta",
                            "version": "1.0.0-beta.1"
                 }
       },
"firewall": {
                 "vall : {
    "vall : {
        "vd:": {
            "doc": "/config/discover/apis/firewall/v1/doc.md",
            "doc": "/config/web-ui/cu-doc.html?md-doc-loc=/config/discover/apis/firewall/v1/doc.md",
            "doc_html": "/config/web-ui/cu-doc.html?md-doc-loc=/config/web-ui/cu-doc.md",
            "doc_html": "/config/web-ui/cu-doc.html?md-doc-loc=/config/web-ui/cu-doc.md",
            "doc_html": "/config/web-ui/cu-doc.html?md-doc-loc=/config/web-ui/cu-doc.md",
            "doc_html": "/config/web-ui/cu-doc.html?md-doc-loc=/config/web-ui/cu-doc.md",
            "doc_html": "/config/web-ui/cu-doc.html?md-doc-loc=/config/web-ui/cu-doc.md",
            "doc_html": "/config/web-ui/cu-doc.html?md-doc-loc=/config/web-ui/cu-doc.md",
            "doc_html": "/config/web-ui/cu-doc.html",
            "doc_html": "/config/web-ui/cu-doc.html",
            "doc_html": "/config/web-ui/cu-doc.html",
            "doc_html": "/config/web-ui/cu-doc_html",
            "doc_html",
            "doc_html": "/config/web-ui/cu-doc_html",
            "doc_html",
            "doc_htm
                           "model": "/config/discover/apis/firewall/v1/model.json",
                          "rest_api": "/config/rest/firewall/v1alpha",
"rest_api": "/config/discover/apis/firewall/v1/openapi.json",
"rest_ui": "/config/web-ui/swagger-ui/?url=/config/discover/apis/firewall/v1/openapi.json",
                          "rest_ui": "/con
"state": "alpha"
                             "version": "1.0.0-alpha.2"
                 }
      },
"log": {
                   v1": {

"doc": "/config/discover/apis/log/v1/doc.md",
                            "doc_html": "/config/web-ui/cu-doc.html?md-doc-loc=/config/discover/apis/log/v1/doc.md",
                             "model": "/config/discover/apis/log/v1/model.json",
```

The API documentation in the VAPIX library will be delayed, but it can be found on the device itself. To see API documentation on the device write: http://IP-adress /config/web-ui/cu-doc.html?md-doc-loc=/config/discover/apis/best-snapshot/v1/doc.md

Best Snapshot Configuration (Version 1.0.0-beta.1)

Overview

- Short Description: Configuration API for Best Snapshot feature
- ID: best-snapshot
- Version: 1.0.0-beta.1
- State: Beta

WARNING: This API is in **BETA** stage. The API is provided for testing purposes and is subject to backward-incompatible changes, including modifications to functionality, behavior, and availability. Please don't use in production environment.

Structure

Objects

best-snapshot.v1 (Entity)

- ▼ Details
 - Description: Configuration root object
 - Notification: false | Depresated: false

Now you get the responses from the device:

It is also possible to test the APIs through the Swagger GUI. To do this, go to the Swagger URL for the selected API, e.g. /config/web-ui/swagger-ui/?url=/config/discover/apis/best-snapshot/v1/openapi.json

API

	/config/discover	apis/best-snapshot/v1/openapi.json	Explore
/config/discover/api	napshot (1.0.0-beta.1) (0AS3) Subest-snapshot/Viopenapi json If for Best Snapshot feature		
Servers /config/rest	×		
best-sna	pshot.v1beta		^
GET /	best-snapshot/v1beta		^
Use this oper	ation to get the value of 'best-snapshot.v1'		
Parameters			Try it out
Name	Description		
traceparent string (header)	This options sets the traceparent used for the	acing request	
(neuver)	information		
Responses			
Code	Description		Links

Click on $\ensuremath{\text{Try}}$ it out button and fill in the values. Then click on the $\ensuremath{\text{Execute}}$ button.

Now you get the responses from the device:

Responses	
Curl	
-H 'acce -H 'Cont -d '{ "data": "enabl	177.25.155.86/config/rest/best-snapshot/vlbeta?strict+true' \ pri application/json' \ ent-Type: application/json' \
Request URI	
http://17	2.25.155.86/config/rest/best-snapshot/vlbeta?strict=true
Server respo	nse
Code	Details
200	Response body
	{ "status": "success" } Download
	Response headers
	connection: Keep-Alive

Now you can copy the code and place it to your application.

Storage & recording

Storage & recording

Edge storage support

SD card support

The following are supported filesystems and encryptions for SD cards.

- Supported filesystems: ext4 (recommended), vFAT
- Supported filesystem size:
 - Up to 2 TB for devices with SDXC slot support and AXIS OS 5.60 and higher
 - Up to 64 GB for devices with SDXC slot support and AXIS OS prior to 5.60
- Supported speed classes: class 10 or higher
- Supported encryptions:
 - AES-CBC 128-bit for all devices with AXIS OS 5.80.1 and higher
 - AES-CBC 256-bit for all devices with AXIS OS 8.40.1 and higher
 - AES-XTS-Plain64 (AES-XTS-512 256-bit) for newer devices with AXIS OS 8.30.1

Network share support

The following are supported storage network protocols and authentication modes for external storage media.

- Supported protocols:
 - CIFS/SMB 1.0 + NTLM authentication mode for devices with AXIS OS 5.90 and lower
 - CIFS/SMB 1.0, 2.0, 2.1, 3.0 and 3.02 + NTLM authentication mode for devices with AXIS OS 6.10 and higher
 - CIFS/SMB 3.1.1 + NTLM authentication mode with AXIS OS 10.12 or higher and Linux Kernel 4.17 or higher.
- Supported filesystem size: 8 ZB with AXIS OS 5.70 and higher, and 2 TB with AXIS OS 5.65 and lower

Basics

Video retention

AXIS OS 6.40 and higher

There are two types of disk clean-up operations for deleting old recordings; one is user-controllable, and one is performed automatically by the Axis device.

The first operation removes recordings older than a certain time in days. This can be configured by the user in the storage configuration in the web interface. For instance, when the user selects one week (i.e. 7 days), the clean-up operation will remove all recordings older than 7 days. It's important to note that this operation runs once per hour (i.e. every 60 minutes).

Storage & recording

Stora	ge
Netv	vork storage
	Server (100.0 GB) Host: 172.25.200.51 Share: network_share Free: 98.9 GB Status: Okay Write-protect
	7 days Tools Erase all X
	Safely remove the storage

AXIS P3248-LVE Network Camera

The second operation is an automatic clean-up that is always enabled and cannot be disabled by the user. This operation runs every second and checks that the network share or SD card has enough space for recording. The clean-up level is defined as an amount of free space. For locally attached storage, like SD cards, the clean-up level is defined as 5% of the total size of the SD card *unless* those 5% are less than 750 MB. When that is the case, 750 MB will be the clean-up level. For network shares, the clean-up level is fixed when max 750 MB remains. So for a 64 GB SD card, the clean-up level is 3.2 GB, while for an 8 TB NAS the clean-up level is 750 MB.

If there is less free space on the disk than what's defined in the clean-up level, the automatic clean-up operation will detect this and remove the oldest recordings (actually blocks) based on the needed space. Note that at least 1 GB will be removed in order to bring the free space size above the clean-up level. For instance, if the free space is 50 MB below the clean-up level, the operation will remove at least 1 GB, thus making 950 MB free above clean-up level.

If the disk is full, i.e. if the clean-up operation was not successful in removing the data on time, another level of 75 MB free space is defined. This is called the full level. If the full level is reached, the disk is declared full and the recordings should stop. At the same time, the clean-up operation continues until the free space is above the clean-up level. Once there is space above the clean-up level, recording will start again.

AXIS OS 5.50 - AXIS 6.30

In addition to the configuration that can be performed in AXIS OS 5.40 and lower, the clean-up of old recordings will start when there is less than 750 MB of storage space available. This is an additional algorithm that has been implemented to prevent exceeding the network share or SD card storage space.

AXIS OS 5.40 and lower

In AXIS OS 5.40 and lower, there are two user-controlled clean-up parameters that defines when the Axis device should be performing a clean-up of the storage. The first parameter is used to configure number of days until recordings should be overwritten, and the second parameter is a clean-up policy in percentage. Old recordings are deleted if either one or both of the conditions in these parameters are met.

It's recommended to set the clean-up policy to **80** for AXIS OS 5.20 and **90** for AXIS OS 5.40. As an example, a clean-up value of 90 corresponds to 72% usable storage, and the Axis device would then have 72 GB writable recording space when connected to a 100 GB network share. The clean-up level can be configured from **Plain Config > Storage**.

Storage & recording

Storage v	Select gr	roup
Storage		
Mount dir:	/var/spoo	ol/storage
Storage S0:		
Auto repair:	~	
Cleanup level:	90	[099]
Cleanup max age:	7	[07000]
Cleanup policy active:	FIFO V	
Device node:	/dev/mm	cblk0p1
Disk ID:	SD_DISK	
Extra mount options:		
File system:	vfat 👻	
Friendly name:		
Locked:		
Mount on boot:	Z	
Required file system:	none 🗸	
Storage S1:	-	
Auto repair:		10,001
Cleanup level:	90	[099]
Cleanup max age:	7	[07000]
Cleanup policy active:	FIFO V	
Device node:	NetworkS	
Disk ID:	NetworkS	ihare
Extra mount options:		
File system:	CIFS v	
Friendly name:		
Locked:		
Mount on boot:		
Required file system:	none 🗸	
Save page changes: Sa	Rese	et

Recording file split duration

For performance reasons and optimal read/write cycles to the edge storage medium, video is recorded in chunks of five minutes. This is defined in DefaultSplitDuration = "300", where "300" refers to 300 seconds, which in turn corresponds to five minutes. Note that it's not recommended to change the value since this could affect the memory buffers. It could also affect performance since a split duration that is too short could cause a high amount of files. If the value is changed, make sure it's tested accordingly. In AXIS Companion, it's possible to download a part of the video merged into one file in *asf* format, which is the recommended way to solve this issue. From AXIS OS 5.60 and onwards, the video export feature has been improved so that it's possible to export a recording.

ONVIF and VAPIX recordings

ONVIF and VAPIX recordings are completely separated. For example, recordings that are created via VAPIX through the web interface or VAPIX API are not visible or usable for ONVIF clients. In return, ONVIF recordings are not visible or usable for the user and are not showing in the recording section of the web interface. ONVIF clients have to create recordings through the ONVIF API separately to make use of recordings.

Metadata events

It's possible to listen to storage-related metadata events via the RTSP stream. Essentially there are two events available, both indicating a storage connection failure either for an SD card or a network share. These two events are called:

- Device/HardwareFailure/StorageFailure
- Storage/Disruption

Storage & recording

If for example the network share is disconnected due to the NAS no longer being available in the network, both events would be active.

Edge storage folder structure

When performing an edge recording on an Axis device, the below folder structure is being used*. This folder structure can not be modified.

Example recording path: *\axis-ACCC8E9C6BE7\20211214\11\20211214_110037_AAF2_ACCC8E9C6BE7\20211214_1	Example recording path	*\axis-ACCC8E9C6BE7\20211214\	11 \ 20211214 110037 AAF2 A	ACCC8E9C6BE7 \ 20211214 11
--	------------------------	-------------------------------	------------------------------------	-----------------------------------

Network share	SD card	Example	Format	Contains
V		axis-ACCC8E9C6BE7	axis-ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ	The Axis device serial number
\checkmark	V	20211214	YYYYMMDD	Date**
\checkmark	\checkmark	11	НН	Hours**
\checkmark	✓	20211214_110037_AA- F2_ACCC8E9C6BE7	YYYYMMDD_HH- MMSS_XXXX_ZZZZZZ- ZZZZZZ	Date and time**, a random identifier, the Axis device serial number
\checkmark	\checkmark	20211214_11	YYYYMMDD_HH	Date and hours**

* The "Send video" and "Send images" event options may use a different folder structure based on the configured recipient.

** The date and time reference is in the Axis device's local time and refers to the date and time when the recording was created.

Password encrypted export of edge recordings

From AXIS OS 10.10, Axis devices support password encrypted export of edge recordings (SD card, network share). This means it is possible to export a recording that is password encrypted, adding the possibility to securely share sensitive video data without the need to manually encrypting exported recordings.

Storage & recording

Recordings	1		-	. •	Recordings	1		3	F •
Mar 21 1 Completed (1 :20:01 AM - H.264)	11:20:10 AM	1		Mar 21 1 Completed	1:20:01 AM - (H.264)	11:20:10 AM	1	~
View Area 1 10 seconds	Network sto	rage		<u> </u>	View Area 1 10 seconds	Network sto	orage		
Recording ID:	220321_112	001_3969_AC	CC8ED9	C85F	Recording ID:	220321_112 <	001_3969_AC	CC8ED9	C85F
Disk ID:	NetworkSha	re			Disk ID:	NetworkSha	ire		
Event:	continuous	100			Event:	continuous			
Type:	Continuous				Type:	Continuous			
Status:	Completed				Status:	Completed			
Source:	View Area 1				Source:	View Area 1			
Video encoding:	H.264				Video encoding:	H.264	0		
Video type:	video/x-h26	4			Video type:	video/x-h26	4		
Frame rate (FPS):	30				Frame rate (FPS):	30			
Resolution (pixels): Audio:	No				Resolution (pixels): Audio:	No			
Set export range					Set export range				
From					From				
2022-03-21		11:20:01	AM	Ψ	2022-03-21		11:20:01	AM	•
То					То				
2022-03-21		11:20:10	AM	*	2022-03-21		11 <mark>:20:10</mark>	AM	*
Filename					Filename				
20220321_11200	1_3969_ACC	C8ED9C85F							
Encrypt					Encrypt				
Estimated file size: .	397.00 kB				Password				
Î			Ехро	rt	•••••				0
					Repeat password				
					•••••				0
					Estimated file size:	397.00 kB			
					Î			Ехро	-

Password encrypted recordings

• Supported file format: *.zip

Storage & recording

- Supported password length: maximum 128 bytes (128 characters). In the legacy web interface the maximum is 64 characters.
- Supported encryption: AES-256. Note that some operating systems do not have native support for this encryption. In those cases open-source tools such as 7-zip can be used to open password encrypted recordings.

Export file name

The file name of regular recording exports may contain sensitive information such as the date and time or the camera name. When doing a password encrypted export of a recording, leave the file name field empty and the file name of both the downloaded *.zip file and content names will get anonymized.

Example of a regular recording export	20220321_112001_3969_ACCC8ED9C85F.zip
Example of a password encrypted export	FBHY6A.zip

SD card

Disabling the SD card

The SD card and its slot can be disabled completely. This is done from **Plain Config > Storage > Storage.SO.Disabled**. When the SD card slot is disabled, the Axis device will not recognize any SD card inserted.

Mount dir		
S0		
Auto repair		
Cleanup level		
90	[099]	
Cleanup max a		
7	[07000]	
Cleanup policy	active	
FIFO		Ψ.
Device node		
/dev/mmcbl	k0p1	
Disk ID		

SD card health monitoring

From AXIS OS 6.20, Axis devices support health statistics for AXIS Surveillance Cards. This means it's possible to get an estimated wear out level for the SD card being used, which can help determine when to replace it.

Storage & recording

Note

Only available for AXIS Surveillance Cards, not for similar cards from the same manufacturer.

Onboard storage Format new cards to ext4
SD card (59.4 GB) Free: 100% Status: Okay File system: vfat Encrypted: No Wear: 2% Write-protect
Keep recordings up to
7 days 🔻
Tools
Format (erase all) 🔻 🔧
Trigger when wear reaches 90 [0200] % Safely remove the storage

From AXIS OS 10.3, it's possible to create an event based on the wear level of the SD card so that you can get notifications when a certain wear level is reached. More information is available in this video:



Decrypting Axis SD cards

We will now take a look at how an encrypted SD card operated in an Axis device can be decrypted or re-used again.

Note

The original passphrase (password) that was used to encrypt the SD card must be known in order to proceed with any of the guidelines below.

Storage & recording

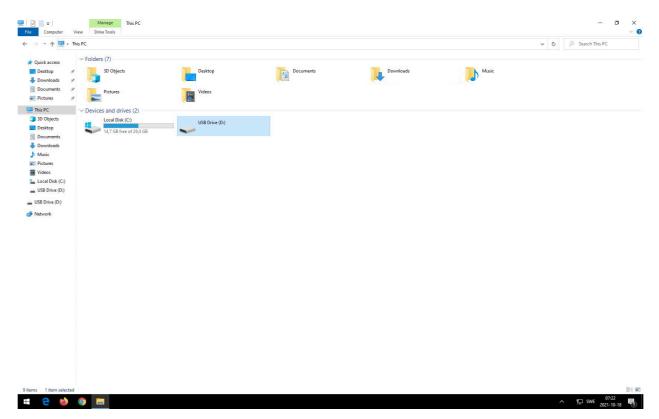
Axis device

An SD card that was encrypted and previously used in an Axis device can be inserted and used in another Axis device again. This could e.g. happen when an Axis device gets replaced during an RMA process.

Windows

To decrypt an SD card on a Windows computer, an open-source disk encryption tool like LibreCrypt can be used.

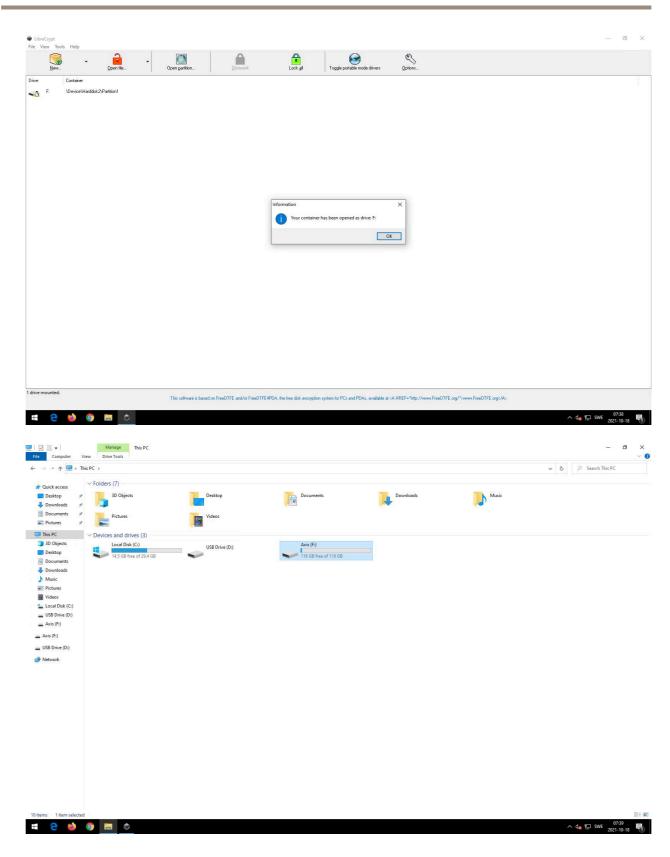
If the SD card is formatted to VFAT, follow the screenshot guide below. If EXT4 is used, you need to install a third-party driver like Ext2Fsd first in order for the Windows computer to recognize the filesystem on the card.



File View Tools Help Rew Dimension Dimension Dimension Dimension			×
0 drive mounted. This software is based on FreeOTFE and/or FreeOTFE 4PDA, the free disk encryption system for PCs and PDAs, available at CA HREF="http://www.FreeOTFE.org/">http://www.FreeDTFE.org/">http://www.FreeDTFE.org/ <td></td> <td></td> <td></td>			
📲 🤮 🍏 🍘 🔚 🗢	07:37 2021-10	⊢18	5
Tie View Tools Help	- 6	a	×
New. Open gation Open gation Open gation Open gation Open gation			
Drive Container			
Odrive mounted. Odrive mounted. This software is based on FreeOTFE and/or FreeOTFE4PDA, the line dak enception system for PCs and PDAs, evaluable of CA HREF4"http://www.FreeOTFE.org/*/www.FreeOTFE.org/*/			

LibreCrypt le View Tools Help				
New Qpen file	Open gatition	Lock al Toggle portable mode drivers	Qptions	
ive Container				
	Select Partition		- u x	
	Please select from the fo Disk #0 Disk #1 D			
	119,06 GB	JISK #2		
	HPFS/MTFS			
		DK Cancel	Entire disk	
	L	UK Cancei		
frive mounted.				
4 😋 🄞 🦁 📷 🗢	I his sortware is based on FreeUTFE and/or FreeUTFE4PDA	A, the free disk encryption system for PCs and PDAs, available at <a< td=""><td>HHLH-"http://www.hned.IFE.arg/つwww.hned.IFE.arg/A></td><td></td></a<>	HHLH-"http://www.hned.IFE.arg/つwww.hned.IFE.arg/A>	

 LibreCrypt File View Tools Help 				- a ×
New Qpen file	Open gathion		Qptions	
Ditre Container	Key Phrase For LUKS Container Encyption Sev @ Use entered @ Read Itom keyfler @ Base IV opties on hach for Mount options Drive: Use default Mount and @ Mount for all	Keyle colana ASII pasword Inter PE FR options Seen: 0 Seen: 0 CV" indicates no sized OK Cancel		
ii 🦻 🏟 🎯 🖬 💠	This software is based on FreeOTFE and/or FreeOTFE4PDA, the free dail	er en suggenen agereen ver i Gestaffig FDHS, affallaufe al. OF	in all - inger men now in 2019. Awww.Fleeu incluiger	~ 4 ₈₆



Storage & recording

Linux

In Linux operating systems, the SD card can be decrypted directly using the command line and the following commands:

sudo cryptsetup open /dev/sdf1 qqq Enter passphrase for /dev/sdf1: mkdir /tmp/qq ~
sudo mount /dev/mapper/qqq /tmp/qq sudo su cd /tmp/qq root@mycomputer:/tmp/qq# ls
20160929 index.db lost+found root@mycomputer:/tmp/qq# exit sudo umount /tmp/qq sudo
cryptsetup close qqq

Formatting Axis SD cards

Formatting the SD card will only rewrite the parts of the SD card necessary to create the filesystem. This could be a couple of hundred MBs on a 64 GB SD card. Any of the old data, such as older recordings, will not be accessible via the new filesystem. However, a major part of the SD card data will be unmodified after formatting and may thus be accessible on a low level (i.e., it may be possible to extract the data if the card is inserted in a computer).

There are various methods to erase sensitive data on SD cards and they usually require writing the entire card with different patterns multiple times. Axis products do not have support for erasing data in such a way.

Network share

SMB/CIFS handshake

Here we'll take a closer look at the differences and negotiations in the SMB/CIFS protocol. The network traces in the table illustrate the process of negotiating a specific SMB version between an Axis device and a NAS and the corresponding session setup in order to mount a network share successfully. After the negotiating process is completed, we can observe some regular SMB protocol communication about listing, deleting and writing files to the network share.

Example network trace	SMB version	SMB dialect	NAS IP address	Axis device IP address
Axis_SMB_Handshake_S	MB <u>0</u> 1.0.pcapng	NT LM 0.12	172.25.200.50	172.25.201.100
Axis_SMB_Handshake_S	М <u>В.0</u> 2.0.pcapng	SMB 2.02 (0x0202)	172.25.200.50	172.25.201.100
Axis_SMB_Handshake_S	M B_1 2.1.pcapng	SMB 2.1 (0x0210)	172.25.200.50	172.25.201.100
Axis_SMB_Handshake_S	М <u>В.0</u> 3.0.pcapng	SMB 3.0 (0x0300)	172.25.200.50	172.25.201.100
Axis_SMB_Handshake_S	V1 <u>80</u> 2.02.pcapng	SMB 3.0.2 (0x0302)	172.25.200.50	172.25.201.100
Axis_SMB_Handshake_S	MB <u>u</u> tau+taegotijantgd	N/A	172.25.200.50	172.25.201.100

About CIFS/SMB support

SMB support in Axis devices

AXIS OS version	12.00 and higher	8.30 - 11.90	6.10 - 8.20	5.90 and lower
Enabled	SMB 2.1, 3.0, 3.02, 3.1.1	SMB 2.1, 3.0, 3.02, 3.1.1	SMB 1.0	SMB 1.0
Supported	SMB 2.1, 3.0, 3.02, 3.1.1	SMB 1.0, 2.0 2.1, 3.0, 3.02, 3.1.1	SMB 1.0, 2.0 2.1, 3.0, 3.02, 3.1.1	SMB 1.0
Auto-negotiation	Yes	Yes	N/A	N/A

AXIS OS 8.30 and higher

In Axis devices with AXIS OS 8.30 to 11.9, the insecure versions SMB 1.0 and SMB 2.0 are disabled per default in order to increase the overall minimum cybersecurity level of the device. Devices with AXIS OS 12 and higher only support secure versions of the SMB protocol.

Storage & recording

It's possible for the device to auto-negotiate its SMB version with the NAS or edge storage device starting with SMB 2.1, or with higher SMB versions such as SMB 3.0, SMB 3.02 and SMB 3.1.1.

AXIS OS 8.20 and lower

In Axis devices with AXIS OS 8.20.1 and lower, SMB 1.0 is enabled per default while all other supported SMB versions (SMB 2.0, 2.1, 3.0, 3.02) need to be set in **Plain config** as described below.

Setting SMB version in Plain config

If SMB 1.0 or SMB 2.0 is required due to compatibility issues, we recommend setting the extra mount options parameter in Settings > System > Plain config > Storage to a specific version, e.g. *vers=1.0* or *vers=2.0* for a network share. Note that there are two storage groups per mounted network share (normally Storage S1 and Storage S2), and both need to have the correct version set in extra mount options. If the setup also includes a network share recipient, then this recipient would be included in the S3 or S4 storage group and would also need modification. See the following example of how the configuration should look like when the NAS storage only supports SMB 1.0:

http://ip-address/axis-cgi/admin/param.cgi?action=update&troot.Storage.S1.ExtraMountOptions=vers=1.0

http://ip-address/axis-cgi/admin/param.cgi?action=update&troot.Storage.S2.ExtraMountOptions=vers=1.0

Extra mount options

Below you will find three configuration examples describing how the device is handling the extra mount options parameter. As you can see, the device will only consider the latter of the two SMB versions entered. Preferably only a single SMB version should be entered.

- vers=1.0: device tries to connect via SMB 1.0
- vers=1.0,vers=2.0: device tries to connect via SMB 2.0
- vers=1.0,vers=2.0,sec=ntlm: device tries to connect via 2.0 SMB with NTLM only

Automatic reconnection

In case the NAS is disconnected from the network, the Axis device will try to automatically remount a network share. A prerequisite for trying to remount a network share is that the NAS is online/available on the network, e.g. via PING. The first attempt to remount the network share will be executed after 2 seconds, and every failed attempt will double the time between new intervals:

- First try: executed after 2 seconds
- Second try: executed after 4 seconds
- Third try: executed after 8 seconds

This will continue until the last try, which will be executed after 600 seconds (10 minutes).

Network share in Plain Config

In the storage section in Plain Config, the complete storage configuration can be obtained from an Axis device. The storage section is splitted into S0-S2 storage groups, where S0 corresponds to the SD card configuration, and S1 and S2 are the network share configuration equivalents.

When mounting a network share on the Axis device, two storage groups – S1 and S2 – are created. S1 is the physical network share and its disk, while S2 is the network share recipient that e.g. could be used in the event system of the Axis device.

Cloud storage

Here's how to set up recording to cloud platforms like AWS S3 and Azure Blob Storage:

Note

Available in AXIS OS 11.11 and later.

Storage & recording

- 1. Set up your S3 or Azure server and create a bucket for the recordings. Then, create a destination on your device by providing the required parameters:
 - id (the ID of the destination, which isn't part of the S3 or Azure parameters)
 - accessKeyld
 - bucket
 - secretAccessKey
 - sessionToken (optional)
 - url (the URL to the S3 or Azure server)

Here's an example of what the data might look like:

```
{"id": "my_s3_dest", "s3": {"accessKeyId": "minioadmin", "bucket": "test-bucket",
"secretAccessKey": "minioadmin", "sessionToken": "session_token", "url":
"http://172.27.140.1:9000"}}
```

- 2. Create a recording group using the new recording group API. You'll need to provide the destination ID as a required parameter. You can do this by sending a request to: http://<target_ip>/config/rest/recording-group/v2/recordingGroups
- 3. Start a recording using the same group.

If you need help finding the APIs, you can use the discover feature: http://<camera IP>/config/discover.

You can also use the Swagger UI pages for the APIs to set up your destination and group quickly. You can find these at http://<camera_IP>/config/web-ui/swagger-ui/?url=/config/discover/apis/remote-object-storage/v1/openapi.json and http://<camera_IP>/config/web-ui/swagger-ui/?url=/config/discover/apis/recording-group/v2/openapi.json.

Best practices

Below you'll find some guidelines for setting up edge recording on your Axis device.

- Use H.264 to reduce bandwidth and avoid MJPEG streams.
- Use only one recording at a time when recording to an SD card to avoid shortening the SD card's lifespan and minimizing its wear level.
- When configuring your recordings, add at least 30 seconds of post-buffer recording to each event triggered recording in order to avoid many small recording segments
- Configure the Axis device properly with the correct date & time prior to starting a recording. Date & time can either be configured manually or automatically via the NTP server.
- Check with the NAS-vendor if the amount of (video) data can be processed by the NAS in order to avoid performance issues.
- Keep the bitrate of the video stream below 10 Mbit/s when recording to the SD card in order to avoid missing frames/recordings.
- On Axis devices with a legacy version, set the clean-up level (i.e. the limit when older recordings are erased) to max 80% on AXIS OS 5.20 and 90% on AXIS OS 5.40.

Timelapse recordings

There are several ways to configure timelapse recordings in Axis products. Below you will find more information and examples of different configuration setups.

Storage & recording

Note

A workaround previously described as saving images to the SD card using FTP and the IP address of the device itself is not supported by Axis. The configuration in question has been made unavailable in later AXIS OS versions. It's recommended to use one of the following alternatives instead.

Recording to SD card using third-party ACAP solutions

Axis recommends third-party solutions such as **Timelapse Server** and **Timelapse video** developed by Pandos Development (*https://pandosme.github.io/*). Some of the features these solutions offer include:

- Timelapse recordings to SD card or network share
- Ability to download the AVI-video directly from the ACAP with user-selectable frame rate and playback rate
- Several different timelapse recordings supported simultaneously
- Alert notification in case a timelapse recording has issues

Note

Depending on your Axis device and architecture, the Timelapse Me ACAP comes in three different application filetypes (mips, armv7hf or aarch64). Use the following VAPIX request http://ip-address/axis-cgi/param.cgi?action=list&tgroup=Properties.System.Architecture to find out which architecture is supported by your Axis device, and select the correct application filetype and upload it to your Axis device.

Recording to remote host using FTP server

Use FTP properly as it is a standard network protocol to transfer files from one host to another over the internet. Upload to a remote host, e.g., another computer or server on the network with a static path.

Example configuration in web interface in AXIS OS 6.53 and lower

Recipient S	Getup	0	Recurrence			Action Rul	e Setup		0
Name:	FTP Server		Recurrences List	Recurrence patte	rn A	Enable rule	Timelapse		
Type:	FTP		Every 10 Minutes	Every 10 minutes	S	Condition			
Network address:	192.168.1.150					Trigger:	Time Recurrence	×	Start condition only
Upload path:	timelapse						Every 10 Minutes	~	
Port number:	21		🛑 ڬ Events/Recu	rrence Setup 🗕		Schedule:	Always (No Schedule)	×	New Schedule
Login Credential	 5					Additional condition	ins		^
User name:	MyUser		🛛 🛛 🖉 🎽 lfp-fä	34-1.labnet.rnd. axis . •••	# ≡				4
Password:	•••••					Add	Modify Remove		
Advanced Settin	15		Recurrer	ice Setup	0	Wait at least 00:	00:00 before re-running the	rule (max 23:59:5	(9)
Use passive me	de		Name:	Every 10 Minutes		Actions Type:	Send Images	~	
Use temporary	mode				~	Stream profile:	JPEG		ew Stream Profile
Test			Recurrence pat			Image frequency:	1 frame(s) per second	d(s) 🗸	
	to the specified FTP server Test		Repeate	every 10 minutes(s)	×	Duration:	Pre-trigger time 1 se While the rule is active Post-trigger time 5 se		
				OK Cancel		Limit:	Send only the first 1	images	
	OK Cancel					Recipient:	FTP Server		New Recipient
						*Create folder:			
						*8ase file name:	Add date/time suffix Add sequence number suff Add sequence number suff		alue) and then start over
							Overwrite/Use own file form		
						*See help for mor		Cancel	

Example configuration in web interface in AXIS OS 9.30 and higher

Storage & recording

	After Hours Schedule Daily	 Timelapse Pulse Send images through FTP
lame		
FTP Server	Office Hours Schedule Daily	V Use this rule
ype		Name
FTP	Weekdays	✓ Timelapse
lost	Schedule Weekly	Wait between actions (max 23:59:59)
192.168.1.150		▼ 00:00:00
Port	Weekends Schedule Weekly	*
21		Condition
older	Even 40 Minutes	
timelapse	Every 10 Minutes Pulse Every 10 minutes	Pulse
Jsername	Name	Use this condition as a trigger
MyUser	Every 10 Minutes	Pulse
Password	Repeat every	Every 10 minutes
	10 Minutes V	+
Cancel Save		Recipient FTP Server There's no stream profile for images. To send images or easter an MUPEG profile Custom image frequency 1 frames per Second Prebuffer (seconds) 01 Postbuffer (mm:ss) 00:00 Maximum images (0 = ∞) 1 Create folder

Recording to remote host using network share

Example configuration in web interface in AXIS OS 6.53 and lower

Recipient Setup	Recurrences Action Rule Setup General General	• Ø
Name: Network Share Type: Network share Type: Network share Ig2.168.1.150 Share: Upload path: Ugload path: Uger name: MyUger Password: Test Test the connection to the specified network share OK Cancel	Test Recurrence Setup Name: Recurrence Setup Name: Repeat every 10 Minutes OK Cancel Mathematical Sector Se	

Example configuration in web interface in AXIS OS 9.30 and higher

Storage & recording

New recipient	After Hours Schedule Daily	~	 Timelapse Pulse Send images through FTP
lame	Office Hours	~	Fuise Send mages through FTF
Network Share	Schedule Daily	·	Use this rule
ype			Name
Network storage 🛛 🔻	Weekdays Schedule Weekly	~	Timelapse
ost			Wait between actions (max 23:59:59)
92.168.1.150	Weekends	~	00:00:00
hare	Schedule Weekly		
imelapse			Condition
older	Every 10 Minutes Pulse Every 10 minutes	^	Pulse
	Name		✓ Use this condition as a trigger
sername	Every 10 Minutes		Pulse
lyUser			Every 10 minutes
assword	Repeat every 10 Minutes		s
	10 Minutes +		+
			There's no stream profile for images. To send image create an MJPEG profile Custom image frequency Image frequency 1 frames per Second ▼ Prebuffer (seconds) 01 Postbuffer (mm:ss) 00:00 Maximum images (0 = ∞) 1 Create folder
			Maximum sequence number (0 = ∞)

Recording to remote host using mail

Example configuration in web interface in AXIS OS 6.53 and lower

Storage & recording

Recipient Setup	Recurrences	Action Rule Setup	0
Name: Mail Server Type: Email To: receiver@example.com Email Server Settings Provider: User defined \/ User authentication	Recurrence pattern Name Recurrence pattern Every 10 Minutes Every 10 minutes Image: Every 10 minutes Image: Every 10 minutes Image: Every 10 Minutes Image: Every 10 Minutes Recurrence pattern: Image: Every 10 Minutes Recurrence pattern: Image: Every 10 Minutes Recurrence pattern: Image: Every 10 Minutes Image: Every 10 Minutes Image: Every 10 Minut	Recurrance Every 10 Minutes Skheduler Additional conditions Additional conditions Additional conditions Material Material </th <th>m Profile</th>	m Profile

Example configuration in web interface in AXIS OS 9.30 and higher

lew recipient	After Hours Schedule Daily	 Timelapse Pulse Send images through FTP
lame	Office Hours	✓ Use this rule
Mail Server	Schedule Daily	
ype		Name
Email	Weekdays Schedule Weekly	✓ Timelapse
end email to	Concession (records)	Wait between actions (max 23:59:59)
receiver@example.com	Weekends	✓ 00:00:00
end email from	Schedule Weekly	
sender@example.com		Condition
Isername	Every 10 Minutes	Pulse
sender@example.com	Pulse Every 10 minutes	
	Name	Use this condition as a trigger
assword	Every 10 Minutes	Pulse Every 10 minutes
	Repeat every	Every to minutes
mail server (SMTP)	10 Minutes 🔻	
smtp.example.com		+
lort	1	Save
587		Action
incryption		Send images to email
TLS V		Recipient
Validate server certificate		Mail Server
OP authentication		There's no stream profile for images. To send image create an MJPEG profile
		Custom image frequency (1
Test		Image frequency
		1 frames per Second V
Cancel Save		Prebuffer (seconds)
		01
		Postbuffer (mm:ss)
		00:00
		Maximum images (0 = ∞)
		1
		Subject
		Message
		Send up to this many images per email
		1
		Filename
		image%y-%m-%d_%H-%M-%S-%f_#s.jpg
		Maximum sequence number (0 = ∞)
		0

Troubleshooting & maintenance

Troubleshooting & maintenance

How to upgrade

Axis offers product AXIS OS management according to the active track or the long-term support (LTS) tracks. Regardless of the track chosen, it's recommended to upgrade regularly in order to get the latest security updates. Upgraded can be done by using AXIS Device Manager, AXIS Camera Station, AXIS Companion or HTTP.

Note

- AXIS A1001 in cluster mode: If using AXIS A1001 in cluster mode, make sure to upgrade all controllers. Either all at a time using AXIS Device Manager or straight after each other using the web interface or FTP. The entire cluster should always be on the same version.
- Mandatory upgrade path (10.9): The following Axis devices require an upgrade via the latest available LTS 2018 (8.40) prior to upgrading to AXIS OS 10.9 or later: AXIS D2050-VE, AXIS FA54, AXIS M3057-PLVE, AXIS M3058-PLVE, AXIS P1367/-E, AXIS P1368-E, AXIS P1445-LE, AXIS P1445-LE-3, AXIS P1447-LE, AXIS P1448-LE, AXIS P3227-LV/-LVE, AXIS P3228-LV/-LVE, AXIS P3807-PVE, AXIS 01645/-LE, AXIS 01647/-LE, AXIS 01659, AXIS 03515-LV/-LVE, AXIS 03517-LV/-LVE/-SLVE, D101-A XF P3807, ExCam XF P1367, ExCam XF 01645 and F101-A XF P1367.
- Axis Edge Vault (10.11): From AXIS OS 10.11 and onwards, Axis Edge Vault will be upgraded automatically during an upgrade of the Axis device. The upgrade functionality introduces a non-backward compatible change to the behavior of Axis Edge Vault. The upgrade process is not reversible: once Axis Edge Vault has been upgraded, it cannot be downgraded. Installing an older release of AXIS OS on a device where Axis Edge Vault has been upgraded is highly discouraged. Core functionality such as HTTPS, 802.1x, and applications that are configured through the certificate management system will not work correctly. It is recommended to first upgrade through AXIS OS 10.10 and then to newer AXIS OS versions. This way, if the upgrade process fails or a rollback is triggered, the device will still be left with an AXIS OS system that is compatible with an upgraded Axis Edge Vault.

AXIS Device Manager or AXIS Camera Station

- 1. Go to the **Device Manager Tab** in Axis Device Manager or **Configuration Tab** > **Devices Management** in AXIS Camera Station.
- 2. Select all devices that should be upgraded.
- 3. Right click and select **Upgrade Firmware**, which will open a dialog with a list of device models and the current firmware version installed in each device.
- 4. In the Upgrade Firmware dialog there are two options:
 - Check for Updates which requires internet access.
 - Browse to locate the file e.g. on hard drive or memory stick.
- 5. Check for updates:
 - Select Check for Updates to download a list of all versions available for all device models.
- 6. Browse:
 - Select browse to locate the files and import them. It is possible to select and import several files at the same time.
- 7. Each device model will show a dropdown containing all available versions for a model, sorted by "Long Term Support" (LTS) and "Active" software tracks.
- 8. Select the version to install for each device model.
- 9. Click **OK** to start upgrading the devices.

Troubleshooting & maintenance

Note

By default, upgrade is done for all the selected devices at the same time. The upgrade order can be changed in **Configuration** > **Connected services** > **Firmware upgrade settings**. Once an update has been started, the devices will be unavailable until the installation and restart of the devices has completed successfully.

For more information, see the help in AXIS Device Manager/AXIS Camera Station.

HTTP

Upgrade instructions when using the old web interface

- 1. Download the upgrade file to a directory that is accessible from your local computer.
- 2. Open the product's start page (e.g. http://192.168.0.90) in a web browser.
- 3. Click the Setup link and log in as "root" (or any other user with administrator privileges). You must be logged in as an administrator to upgrade the unit.
- 4. Click System Options in the menu to the left.
- 5. Click Maintenance.
- 6. Click the Browse button in the Upgrade Server section.
- 7. Select the upgrade file you downloaded (and maybe decompressed) from our site. This file is typically named after the product and AXIS OS version.
- 8. Click the Open button.
- 9. Click the Upgrade button in the Upgrade Server section.
- 10. Wait for the flash load to complete, which may take 1-10 minutes. The upgrade procedure occurs in four steps:
 - Step 1: Shut down. Running applications are shut down and active connections are terminated.
 - Step 2: Uploading. The old version will be erased and the new will be saved. During this step, the power LED will blink green/amber. After a while the progress of the upgrade will be displayed in the web browser.
 - Step 3: Reboot. The system restarts automatically.
 - Step 4: Reconfiguration. The new versions settings are configured to match the previous settings. The color of the status LED will be amber during this step.
- 11. After the upgrade has completed, the unit will automatically initiate the system, during which the status LED blinks amber. When initiation is complete and the system is ready for use, the status LED will be green.

Upgrade instructions when using the new web interface

- 1. Download the upgrade file to a directory that is accessible from your local computer.
- 2. Open the product's start page (e.g. http://192.168.0.90) in a web browser.
- 3. Log in as "root" (or any other user with administrator privileges).
- 4. Click Settings to the right.
- 5. Click System-tab.
- 6. Click Maintenance.
- 7. Select the upgrade file you downloaded (and maybe decompressed) from our site. This file is typically named after the product and AXIS OS version.

Troubleshooting & maintenance

- 8. Click the Open button.
- 9. Click the Upgrade button in the Upgrade Server section.

10. Wait for the flash load to complete, which may take 1-10 minutes. The upgrade procedure occurs in four steps:

- Step 1: Shut down. Running applications are shut down and active connections are terminated.
- Step 2: Uploading. The old version will be erased and the new will be saved. During this step, the power LED will blink green/amber. After a while the progress of the upgrade will be displayed in the web browser.
- Step 3: Reboot. The system restarts automatically.
- Step 4: Reconfiguration. The new versions settings are configured to match the previous settings. The color of the status LED will be amber during this step.
- 11. After the upgrade has completed, the unit will automatically initiate the system, during which the status LED blinks amber. When initiation is complete and the system is ready for use, the status LED will be green.

FTP

Note

- Only applicable for AXIS OS versions 11.0 and below. With AXIS OS 11.1 and later, the FTP options has been removed to increase overall minimum cybersecurity level. For more information, visit SSH access on page 327.
- With AXIS OS 7.30.1 11.0, the FTP server is disabled by default. In order to use the instructions below it first needs to be enabled via the web interface: Settings > System > Plain config > Network > NetworkFTP
- This section is not applicable for AXIS Companion Line cameras.
- 1. You must be at the command prompt and in the directory that contains the upgrade file.

Example: C:\Axis\Product\Firmware

- From the command prompt, open an FTP connection to the unit you wish to upgrade. (Do not use a Windows based FTP program to do this, use command line FTP programs only.)
- 3. Log in as "root". You must be logged in as the root user to upgrade the unit.
- 4. Change to binary transfer mode by typing "bin" and press enter.
- 5. Type "hash" and press enter. This will allow you to see how the upgrade progresses.
- 6. Type the command "put XXX.bin flash" where XXX.bin is the name of the upgrade file you downloaded (and maybe decompressed) from our site. This file is typically named after the product and AXIS OS version.
- 7. Wait for the flash load to complete, which may take 1-10 minutes. The upgrade procedure occurs in four steps:
 - Step 1: Shut down. Running applications are shut down and active connections are terminated.
 - Step 2: Uploading. The old version will be erased and the new will be saved. During this step, the power LED will blink green/amber. After a while, the progress of the upgrade will be displayed in the command prompt.
 - Step 3: Reboot. The FTP session terminates and the system starts automatically.
 - Step 4: Reconfiguration. The new versions settings are configured to match the previous settings. The color of the status LED will be amber during this step.
- 8. After the upgrade has completed, the unit will automatically initiate the system, during which the status LED blinks amber. When initiation is complete and the system is ready for use, the color of the status LED will be green.

Troubleshooting & maintenance

How to downgrade

Downgrading an Axis product might be necessary in order to establish compatibility with the third party systems which do not support higher AXIS OS versions. The downgrade is performed in the same way as an upgrade. Instructions are available in *How to upgrade on page 322*.

If you have a device that has received a new hardware id (HWID), check the *Hardware changes on page 357* section to see the minimum compatible AXIS OS active and LTS versions for the product.

Note

Downgrading to a lower version could cause implications on a system's health and stability. It is only recommended to downgrade an Axis product using the standard upgrade process if performed in combination with a factory default of the product. The factory default can be performed simultaneously during the downgrade, or manually by the user afterwards. As of AXIS OS version 10.1, a factory default is mandatory when downgrading.

How to rollback

When upgrading an Axis product, a restore point of the previous state of the product and its entire configuration is made before the upgrade. This restore point is available to go back to after the upgrade has been performed in case of an unexpected issue. This feature is called **Rollback**.

The rollback feature can be found in the Axis product's web interface under **Settings > System > Maintenance**. A video clip with instructions can also be found in *Configuration tips on page 287*. The feature was introduced in AXIS OS version 7.40, which means that the Axis product must have been upgraded to 7.40 or later in order to be able to perform a rollback.

It is recommended to use the rollback function to re-establish system functionality and to contact Axis Technical Support for further instructions and troubleshooting techniques. No restore point is available when the product is in a factory defaulted state.

Factory default and restore

When troubleshooting or preparing your device for redeployment, you may need to reset it to a previous state. Axis devices offer two options: Factory default and Restore. While both options reset the device, they differ in the extent of the reset and the settings that are preserved.

Factory default resets the device to its original state, removing all custom configurations, including network settings and user accounts. The device will return to its out-of-the-box condition. You can perform a factory default from the Maintenance page in the web interface or by using the hardware button on the device. For instructions on using the hardware button, see the user manual for your specific product.

Restore is similar to factory default, but keeps some network settings intact. You can perform a restore from the **Maintenance** page in the web interface. The settings kept after a restore varies slightly between products, but typically the device will retain the following settings:

- Boot protocol (DHCP or static)
- Static IP address
- Default router
- Subnet mask
- Broadcast IP address
- IEEE 802.1X settings
- 03C settings
- DNS server IP address
- System time

Troubleshooting & maintenance

Important

After performing a factory default or restore, you won't be able to roll back to previous settings. Additionally, all installed ACAP applications and certificates not originally included with the device will be deleted.

Basic troubleshooting

AXIS OS supports a variety of troubleshooting tools and commands that can be used to identify, analyze and solve issues experienced by a user. The list below contains some tools and methods. Support and instructions can also be provided by *Axis Technical Services*.

Purpose / Action	HTTP(S) URL command	Additional information
Download server report	https://172.25.201.191/axis-cgi/serverre- port.cgi?mode=zip_with_image	Downloads a server report from the Axis device.
Download crash report	https://172.25.201.191/axis- cgi/debug/debug.tgz	Downloads a crash report from the Axis device. This may take several minutes to complete.
Download network trace	https://172.25.201.191/axis-cgi/de- bug/debug.tgz?cmd=pcapdumpEtdura- tion=30Etinterface=eth0	 Downloads a network trace from the Axis device. This can also be done via the web interface in newer AXIS OS versions in Settings > System > Maintenance. When the direct URL is used; a custom time in seconds can be specified in the duration= parameter. the interface that should be captured can be specified in the interface parameter. Without the interface parameter, all interfaces are included. When specifying multiple interfaces, use the follwing format: "Einterface=eth0,eth1.1,eth1.2". The interface parameter is available from AXIS OS 10.10 and onwards.
Ping test IP address	https://172.25.201.191/axis- cgi/pingtest.cgi?ip=172.25.201.10	The ping test is always issued from a source device, in this case the Axis device at 172.25.201.191 followed by the parameter that determines the target IP address or hostname.
Ping test hostname	https://172.25.201.191/axis- cgi/pingtest.cgi?ip=computer.lab.net	The ping test is always issued from a source device, in this case the Axis device at 172.25.201.191 followed by the parameter that determines the target IP address or hostname.
Port open test	https://172.25.201.191/axis- cgi/tcptest.cgi?ad- dress=172.25.201.102&tport=80	The port test is always issued from a source device, in this case the Axis device at 172.25.201.191 followed by the parameter that determines the target IP address and port that should be checked for availability.

Troubleshooting & maintenance

Collect core dump	http://172.25.201.191/axis- cgi/debug/debug.tgz?listen	Starts listening to available core dumps on the Axis device. It's recommended to use Google Chrome or Mozilla Firefox. Note that the web browser might time out, in this case the command has to be sent again.
Collect core dump wget –TO –O core	"http://root:mypass- word@172.25.201.191/axis-cgi/de- bug/debug.tgz?listen"	Starts listening to available core dumps on the Axis device from the <i>WGET console</i> that is installed as an application on a computer in the same network. Open the Windows command prompt in administrator mode and change the directory with the cd command to where wget is installed, e.g. C:\Program Files (x86)\GnuWin32\bin. To go to this file location you would type e.g. "cd C:\Program Files (x86)\GnuWin32\bin" and then execute the HTTP(S) URL command as seen, for instance wget -TO -0 core "http://root:mypass- word@172.25.201.191/axis-cgi/de- bug/debug.tgz?listen"

Telnet access

Note

The below documentation should only be used according to the instructions given by Axis Technical Services in maintenance and troubleshooting situations.

Telnet is supported by Axis devices with version 5.50 and lower. Follow the instructions below in order to use Telnet on the device:

- 1. Access http://ip-address/admin-bin/editcgi.cgi?file=/etc/inittab
- 2. Remove the hash from the below line in the configuration file: #tnet:35:once:/usr/sbin/telnetd
- 3. After removing the hash, the line should look like this: tnet:35:once:/usr/sbin/telnetd
- 4. Save the file and restart the Axis device

SSH access

Note

The below documentation should only be used according to the instructions given by Axis Technical Services in maintenance and troubleshooting situations.

Accessing the Axis device using SSH for maintenance purposes only is recommended due to the connection being encrypted and sensitive information being transferred securely. SSH access can be achieved using the plain Linux command console or Microsoft Windows power shell. Note that administrator privileges may be required for this and/or firewall and security settings of the computer need to be adjusted in order to allow SSH connections.

SSH in AXIS OS 5.50 - 5.55

Follow the instructions below in order to use SSH on devices with AXIS OS 5.51 and lower:

- 1. Access the SSH file by using this link: http://ip-address/admin-bin/editcgi.cgi?file=/etc/conf.d/ssh
- 2. Enable SSH by setting SSHD_ENABLED="yes"

Troubleshooting & maintenance

- 3. Save the SSH file.
- 4. Restart the Axis device.

SSH in AXIS OS 5.60 - 11.4

Follow the instructions below in order to use SSH on devices with AXIS OS 5.60 and AXIS OS 11.4:

- 1. Enable SSH from Plain Config > Network > SSH.
- 2. Save the settings. The Axis device is now reachable via SSH, no restart is needed.

Alternatively SSH can be enabled/disabled using the direct VAPIX API calls:

- https://ip-address/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=Yes
- https://ip-address/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=No

SSH in AXIS OS 11.5 and higher

To increase the overall system security of AXIS OS, the system-wide root privileges are changed to prevent information leakage and compromised integrity. With AXIS OS 11.5, VAPIX users and SSH users are handled separately. Please see additional information about these change *here*.

For clarification:

- "VAPIX user" is the user used to for example log into the web interface of the Axis device.
- "SSH user" is the user used to log into the Axis device through SSH.

AXIS OS	Additional information
Factory defaulted AXIS OS 11.4 or earlier	The initial password set during first boot for the root user is valid for bot
Upgrading from AXIS 11.4. or earlier to AXIS OS 11.5.	Upgrading to AXIS OS 11.5 will migrate all existing users to become VAPI password is changed, a separate SSH user password change is required to
Factory defaulted AXIS OS 11.5.	The initial password set during first boot for the root user is valid for bot separate SSH user password change is required to change the SSH user

Above changes do not change the (default) state of the SSH service. The SSH service is still disabled by default and is separated from SSH user creation. It is possible to enable SSH without creating SSH users and vice versa.

It is possible to create/use the same username for VAPIX users and SSH users. User created SSH users do not have root privileges. Existing SSH users (AXIS OS 11.5 or higher) on the Axis device, can be found in the web-interface using Settings > System > Users > SSH users.

Troubleshooting & maintenance

Users	
+ Add user	
Role	Username
Administrator	root
Anonymous users	
Allow anonymous viewing	Allow anonymous PTZ operating
SSH users	
+ Add SSH user	
Username	Comment
andre	
peter	

Command overview

The following main commands are available and supported when logged in via SSH to the Axis device. Make sure you are using the commands according to the instructions given by Axis Technical Services.

Action / Purpose	Windows OS command line	Linux OS command line
Connect & login	ssh root@192.168.0.90	ssh root@192.168.0.90
Disconnect & logout	exit	exit
Restart	reboot	reboot
Download crash report	ssh root@192.168.0.90 /usr/sbin/dbox debugar.cgi -d > debug.tgz	ssh root@192.168.0.90 /usr/sbin/dbox debugar.cgi -d > debug.tgz
Upload AXIS OS*	scp C:\Users\psadmin\Down- loads\P1375_9_80_2_4.bin root@172.25.201.191:/var/tmp	
Update AXIS OS	upgrade -f/var/tmp/P1375_9_80_2_4.bin	cat P1375_9_80_2_4.bin ssh root@172.25.201.191 upgrade
Update AXIS OS & perform a factory default	upgrade -d -f /var/tmp/P1375_9_80_2_4.bin	cat P1375_9_80_2_4.bin ssh root@172.25.201.191 upgrade -d
Perform a factory restore and keep IP settings	fwmgr factorydefault soft	fwmgr factorydefault soft
Perform a factory default	fwmgr factorydefault hard	fwmgr factorydefault hard

Troubleshooting & maintenance

*Uploading AXIS OS to the Axis device is only needed when the user is trying to update the device using the Windows OS command line. This step is not needed when using the Linux OS command line.

The commands below are illustrated using the Windows OS command lines from the table.

Connect & login

OpenSSH SSH client

C:\WINDOWS\system32>ssh root@172.25.201.191 root@172.25.201.191's password: root@axis-accc8ed910b9:~# _

Disconnect & logout

Administrator: Command Prompt

```
C:\WINDOWS\system32>ssh root@172.25.201.191
root@172.25.201.191's password:
root@axis-accc8ed910b9:~# exit
Connection to 172.25.201.191 closed.
```

C:\WINDOWS\system32>

Download Crash Report

Administrator: Command Prompt

```
C:\WINDOWS\system32>ssh root@172.25.201.191 /usr/sbin/dbox debugar.cgi -d > debug.tgz
root@172.25.201.191's password:
/proc/sys/net/ipv4/route/flush: Bad file descriptor
/proc/sys/net/ipv6/route/flush: Bad file descriptor
/proc/sys/vm/compact_memory: Bad file descriptor
/proc/sysrq-trigger: Input/output error
/proc/sysrq-trigger: Input/output error
/proc/sys/net/ipv4/route/flush: Bad file descriptor
/proc/sys/net/ipv6/route/flush: Bad file descriptor
/proc/sys/net/ipv6/route/flush: Bad file descriptor
/proc/sys/net/ipv6/route/flush: Bad file descriptor
/proc/sys/net/ipv6/route/flush: Bad file descriptor
/proc/sys/vm/compact_memory: Bad file descriptor
```

Restart

Troubleshooting & maintenance

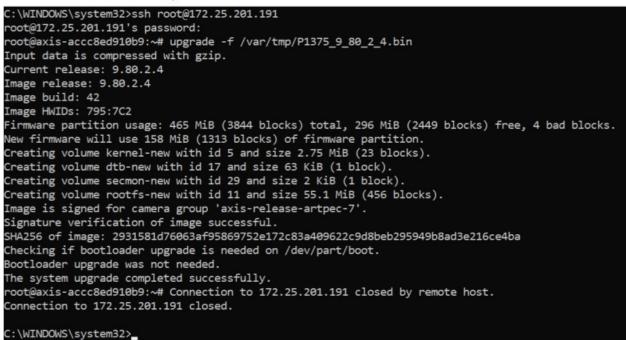
OpenSSH SSH client

```
C:\WINDOWS\system32>ssh root@172.25.201.191
root@172.25.201.191's password:
root@axis-accc8ed910b9:~# reboot
root@axis-accc8ed910b9:~#
```

AXIS OS update

as Administrator: Command Prompt			_		\times
C:\WINDOWS\system32>scp C:\Users\psadmin\Downloads\P1375_9_80 root@172.25.201.191's password:	_2_4.bin ssh r	oot@17	2.25.201.19	91:/var/t	mp
P1375_9_80_2_4.bin ssh: No such file or directory	100%	58MB	19.2MB/s	00:03	
C:\WINDOWS\system32>_					

Administrator: Command Prompt

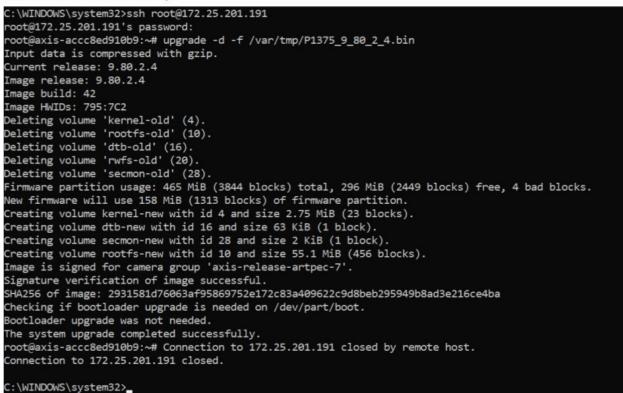


AXIS OS update & factory default

Troubleshooting & maintenance

Administrator: Command Prompt			_		\times
C:\WINDOWS\system32>scp C:\Users\psadmin\Downloads\P137 root@172.25.201.191's password:	5_9_80_2_4.bin ssh	root@17	2.25.201.19	91:/var/	tmp
P1375_9_80_2_4.bin	100%	58MB	19.2MB/s	00:03	
ssh: No such file or directory					

Administrator: Command Prompt



FTP access

Note

- Only applicable for AXIS OS versions 11.0 and below. With AXIS OS 11.1 and later, the FTP options has been removed to increase overall minimum cybersecurity level. For more information, visit SSH access on page 327
- The below documentation should only be used according to the instructions given by Axis Technical Services in maintenance and troubleshooting situations.

Accessing the Axis device using FTP for maintenance purposes only is not recommended due to the connection being unencrypted and sensitive information being transferred in plain text readable. Therefore, SSH access is recommended. FTP access can be achieved using the plain Linux command console or Microsoft Windows power shell. Note that administrator privileges may be required for this and/or firewall and security settings of the computer need to be adjusted in order to allow FTP connections. FTP can be enabled in the Axis device via **Plain config > Network > FTP**. Alternatively FTP can be enabled/disabled using the direct VAPIX API calls:

• https://ip-address/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=Yes

Troubleshooting & maintenance

• https://ip-address/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=No

Command overview

The following main commands are available and supported when logged in via FTP to the Axis device. Make sure you are using the commands according to the instructions given by Axis Technical Services.

Action / Purpose	Windows OS command line
Connect & login	ftp 192.168.0.90
Disconnect & logout	bye
Restart	quote site reboot
Download crash report*	get debug.tgz
Update AXIS OS*	put P1375_9_80_2_4.bin flash
Update AXIS OS & factory default*	put P1375_9_80_2_4.bin flash_all

*The hash command followed by the bin command can be used to enable verbose logging prior to executing the selected commands.

Connect & login

Administrator: Command Prompt - ftp 172.25.201.191

```
Microsoft Windows [Version 10.0.17763.1697]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>ftp 172.25.201.191
Connected to 172.25.201.191.
220 AXIS P1375 Network Camera 9.80.2.4 (2020) ready.
503 Bad sequence of commands.
User (172.25.201.191:(none)): root
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp> _
```

Disconnect & logout

Troubleshooting & maintenance

Administrator: Command Prompt

Download Crash Report

Administrator: Command Prompt - ftp 172.25.201.191

```
Microsoft Windows [Version 10.0.17763.1697]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>ftp 172.25.201.19
^C
C:\WINDOWS\system32>ftp 172.25.201.191
Connected to 172.25.201.191.
220 AXIS P1375 Network Camera 9.80.2.4 (2020) ready.
503 Bad sequence of commands.
User (172.25.201.191:(none)): root
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp> get debug.tgz
200 Command okay.
150 Opening data connection.
226 Transfer complete.
ftp: 25459061 bytes received in 68.37Seconds 372.37Kbytes/sec.
ftp>
```

Restart

Troubleshooting & maintenance

Administrator: Command Prompt - ftp 172.25.201.191

Microsoft Windows [Version 10.0.17763.1697] (c) 2018 Microsoft Corporation. All rights reserved. C:\WINDOWS\system32>ftp 172.25.201.191 Connected to 172.25.201.191. 220 AXIS P1375 Network Camera 9.80.2.4 (2020) ready. 503 Bad sequence of commands. User (172.25.201.191:(none)): root 331 User name okay, need password. Password: 230 User logged in, proceed. ftp> quote site reboot 200 Command okay. ftp>

AXIS OS update

Troubleshooting & maintenance

Command Prompt - ftp 172.25.201.191

```
C:\WINDOWS\system32>ftp 172.25.201.191
Connected to 172.25.201.191.
220 AXIS P1375 Network Camera 9.80.2.4 (2020) ready.
503 Bad sequence of commands.
User (172.25.201.191:(none)): root
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp> put C:\Users\psadmin\Downloads\P1375_9_80_2_4.bin flash
200 Command okay.
150-Shutting down processes.
150 Opening data connection.
214-Virtual target execution.
Input data is compressed with gzip.
Current release: 9.80.2.4
Image release: 9.80.2.4
Image build: 42
Image HWIDs: 795:7C2
Firmware partition usage: 465 MiB (3844 blocks) total, 296 MiB (2449 blocks) free, 4 bad blocks.
New firmware will use 158 MiB (1313 blocks) of firmware partition.
Creating volume kernel-new with id 5 and size 2.75 MiB (23 blocks).
Creating volume dtb-new with id 17 and size 63 KiB (1 block).
Creating volume secmon-new with id 29 and size 2 KiB (1 block).
Creating volume rootfs-new with id 11 and size 55.1 MiB (456 blocks).
Image is signed for camera group 'axis-release-artpec-7'.
Signature verification of image successful.
SHA256 of image: 2931581d76063af95869752e172c83a409622c9d8beb295949b8ad3e216ce4ba
Checking if bootloader upgrade is needed on /dev/part/boot.
Bootloader upgrade was not needed.
The system upgrade completed successfully.
214 Virtual target exit.
221 Goodbye.
Connection closed by remote host.
ftp>
```

AXIS OS update & factory default

Troubleshooting & maintenance

Command Prompt - ftp 172.25.201.191

```
C:\WINDOWS\system32>ftp 172.25.201.191
Connected to 172.25.201.191.
220 AXIS P1375 Network Camera 9.80.2.4 (2020) ready.
503 Bad sequence of commands.
User (172.25.201.191:(none)): root
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp> put C:\Users\psadmin\Downloads\P1375_9_80_2_4.bin flash_all
200 Command okay.
150-Shutting down processes.
150 Opening data connection.
214-Virtual target execution.
Input data is compressed with gzip.
Current release: 9.80.2.4
Image release: 9.80.2.4
Image build: 42
Image HWIDs: 795:7C2
Deleting volume 'kernel-old' (4).
Deleting volume 'rootfs-old' (10).
Deleting volume 'dtb-old' (16).
Deleting volume 'rwfs-old' (20).
Deleting volume 'secmon-old' (28).
Firmware partition usage: 465 MiB (3844 blocks) total, 296 MiB (2449 blocks) free, 4 bad blocks.
New firmware will use 158 MiB (1313 blocks) of firmware partition.
Creating volume kernel-new with id 4 and size 2.75 MiB (23 blocks).
Creating volume dtb-new with id 16 and size 63 KiB (1 block).
Creating volume secmon-new with id 28 and size 2 KiB (1 block).
Creating volume rootfs-new with id 10 and size 55.1 MiB (456 blocks).
Image is signed for camera group 'axis-release-artpec-7'.
Signature verification of image successful.
SHA256 of image: 2931581d76063af95869752e172c83a409622c9d8beb295949b8ad3e216ce4ba
Checking if bootloader upgrade is needed on /dev/part/boot.
Bootloader upgrade was not needed.
The system upgrade completed successfully.
214 Virtual target exit.
221 Goodbye.
Connection closed by remote host.
ftp>
```

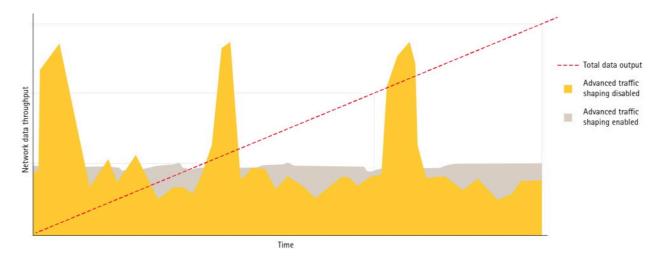
Network traffic shaping

Axis devices can transmit video using the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP). TCP has a control mechanism, so in the event a packet is being lost or corrupt, it will be resent. The UDP protocol doesn't have a mechanism to ensure that all transmitted packets have been received. So, if a packet is discarded or corrupt, its retransmission is not requested. UDP is commonly used in multicast networks. The discarded packets associated with a video stream will result in unsatisfactory video performance as the associated pixels will not be displayed within the end users' video. Packet drops are caused by different things, e.g. the incorrect specification of the network infrastructure, a network that had alterations over time (more traffic added), or a network that becomes congested at peak times. Network switches with insufficient processing power and memory capabilities will cause packet drops when faced with unexpected or inconsistent peaks of incoming data.

Axis devices will by default transmit their data as fast as possible and due to the nature of H.264 video, we encounter peaks or bursts of network traffic that is sent out by the Axis device into the network. The bursts or peaks of data are associated with the I-frames contained within the video stream, where the whole video frame is updated. In between the I-frames are the P-frames,

Troubleshooting & maintenance

which are much smaller in data size. This can cause issues when there is insufficient capacity on the network hardware and when using the UDP method of transmission.



Network bottlenecks and throughput

Even though the network infrastructure through its switches and routers gets increased capabilities and become more powerful in dealing with network spikes and bursts, and even though it's trying to overcome the temporal bottleneck by buffering the incoming data, this might eventually still fail depending on the setup.

Below are a couple of possible scenarios where traffic shaping is a recommended technique for avoiding network related issues. The use cases illustrate how to plan and manage network related traffic by understanding possible bottleneck positions within the network. This is done by simply computing the uplink speed of the network infrastructure and potential incoming data from e.g. Axis devices or other network equipment that coexists and contributes to data traffic in the network.



But it's not only the uplink speed that is important. In some use cases the network equipment is simply not performant enough to cope with the amount of network traffic or spikes that might be generated. It's also possible that the accumulative number of devices connected to the same network switch eventually will overwhelm it and cause it to drop network packets. Proactive planning of the expected network traffic and use case is key in avoiding potential issues.

Troubleshooting & maintenance



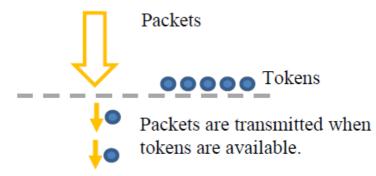
Basic traffic shaping

There are several techniques for controlling the data output from an Axis device. The first step is to always use a suitable compression level to optimize the device's output. H.264 compression is the industry standard method of compression due to its efficiency, but a suitable compression level must still be applied (this reduces the amount of data whilst maintaining picture quality). Axis Zipstream is an even more efficient compression algorithm, which increases the compression further whilst still maintaining picture quality when compared to H.264. H.264 and Zipstream algorithms are based on the movement or non-movement within a scene, and as such it's quite difficult to predict the actual output of the camera. Maximum bitrate (MBR), variable bitrate (VBR) as well as average bitrate (ABR) are techniques to limit the output of a camera, and can be used to contain the transmitted data within a certain average perimeter. However this doesn't restrict the actual peaks or bursts. Learn more about the different bit rate controls in the white paper *Bitrate control for IP video*.

A completely different example of applying basic traffic shaping is the simple decision between having two video streams per Axis device, one each for live view and recording versus using the same streaming and network parameters for reusing a single video stream for both live view and recording. Using only one video stream instead of two is reducing the amount of network throughput generated by the Axis device by 50%. This may even be enough to avoid network-related bottlenecks in an aggregated scenario of, let's say, having many Axis devices being connected to a fully utilized 48-port network PoE switch.

Advanced traffic shaping

In case basic traffic shaping mechanics are not suitable, more advanced techniques can be applied on the network layer of the Axis device. To control peaks or bursts of data being transmitted from an Axis device, the **bandwidth limit** parameter in **Plain Config > Bandwidth** can be used. The bandwidth parameter was introduced in AXIS OS 6.20 and makes use of the hierarchical token bucket (HTB) and token bucket filter (TBF). TBF controls the transmitted output by controlling the data by the use of a token. When a token is available – data can be sent. The bandwidth limit is not the capped data rate but what HTB/TBF uses to organize the data output in a controlled manner.



TBF is a queuing method that acts as a timing mechanism which effectively spreads peaks of data over a longer period. More information about HTB and TBF can be found via the following links:

- http://luxik.cdi.cz/~devik/qos/htb/manual/userg.htm
- http://www.lartc.org/howto/lartc.qdisc.classless.html#AEN690

Troubleshooting & maintenance

Configuration in AXIS OS

The bandwidth parameter can be found in Plain Config > Bandwidth. When limiting the traffic you need to set a bandwidth limit value that matches your total bandwidth needs from your Axis device. It's recommended to gather statistics from the network switch that the Axis device is connected to in order to learn the usual bandwidth usage. As an example, an Axis device under operation is a multisensor device with four image sensors and a combined quad view that sends out two streams each per channel for recording and live view. These 10 parallel video streams generate an average network bandwidth consumption of 70-80 Mbit/s. To include some margin, the bandwidth parameter should be configured to 100mbit or 125mbit.

Important

The Axis device will drop packets if the bandwidth parameter is configured unreasonably, i.e. lower or very close to the actual network bandwidth consumption. Applying good margin above the actual network bandwidth consumption is always recommended. The bandwidth limit is not the capped data rate but what HTB/TBF uses to organize the data output in a controlled manner.

Example 1: Default configuration, 0 means no traffic shaping is applied.

Plain config	
To see the effect of your changes, you might have to refresh the webpage or restart the camera.	Bandwidth
API	0
Audio	Cancel Save
AudioSource	
Bandwidth >	

Example 2: Traffic shaping is enabled, and the maximum output is capped at 100 mbit/s.

Troubleshooting & maintenance

Plain config

To see the effect of your changes, you might have to refresh the webpage or restart the camera.	Bandwidth
API	100mbit
Audio	Cancel Save
AudioSource	
Bandwidth >	

Example 3: Traffic shaping is enabled, and the maximum output is capped at 10000 kbit/s (=10 mbit/s).

Plain config

To see the effect of your changes, you might have to refresh the webpage or restart the camera.	Bandwidth
API	10000kbit
Audio	Cancel Save
AudioSource	
Bandwidth >	

Wireshark network analysis

Filters and macros

This is a list of common basic operators as well as network and video streaming related filters that are useful when troubleshooting network traffic between an Axis device, the network infrastructure and third party video management systems and other applications.

Basic operators	Description
==	Equal

Troubleshooting & maintenance

	Not equal
>	Greater than
<	Less than
2	Greater than or equal to
<u>≤</u>	Less than or equal to
8t8t	And
!	Not
	Or
Network display filter	Description
ip.addr ≥ 224.0.0.0	Filter for network traffic with IP-Multicast addresses
ip.addr == 172.25.201.0/24	Filter for network traffic with IP-address sub net
ip.addr == 10.0.0.1	Filter for network traffic with IP-address 10.0.0.1
ip.addr == 10.0.0.1 &t&t ip.addr == 10.0.0.2	Filter for network traffic with IP-address 10.0.0.1 and 10.0.0.2
ipv6.addr == 2019:db8:abcd:a:3cf5:6c7e:f780:1085	Filter for network traffic with IPv6 address 2019:db8:abcd:a:3cf5:6c7e:f780:1085
! (ip.addr == 172.25.154.7)	Filter for network traffic excluding this specific IP-address
ip.dst == 10.0.0.1	Filter for network traffic with a specific IP-address 10.0.0.1 as destination
ip.src == 10.0.0.1	Filter for network traffic with a specific IP-address as source
eth.dst == 00:00:cd:37:00:c0	Filter for network traffic with a specific destination MAC address
eth.src == ac:cc:8e:c2:22:7b	Filter for network traffic with a specific source MAC address
icmp	Filter for ICMP traffic (ping)
! icmp.resp_in and icmp.type==8	Filter for ICMP traffic (ping) that did not respond/failed
dns	Filter for DNS traffic
ntp	Filter for NTP traffic
igmp	Filter for IGMP traffic
eap eapol	Filter for 802.1x traffic
snmp	Filter for SNMP traffic
http	Filter for HTTP traffic
http.request	Filter for HTTP GET requests
http.request.full_uri contains "onvif"	Filter for HTTP Get Requests containing ONVIF related information
http.request.full_uri contains "action=update"	Filter for HTTP Get Requests where a VAPIX param.cgi parameter is changed
http.time > 2	Filter for HTTP responses that were sent longer than 2 seconds after the request.
!(arp or icmp or dns)	Exclude network traffic related to ARP, ICMP and DNS protocol
udp contains 33:27:58	Sets a filter for the HEX values of 0x33 0x27 0x58 at any offset

Troubleshooting & maintenance

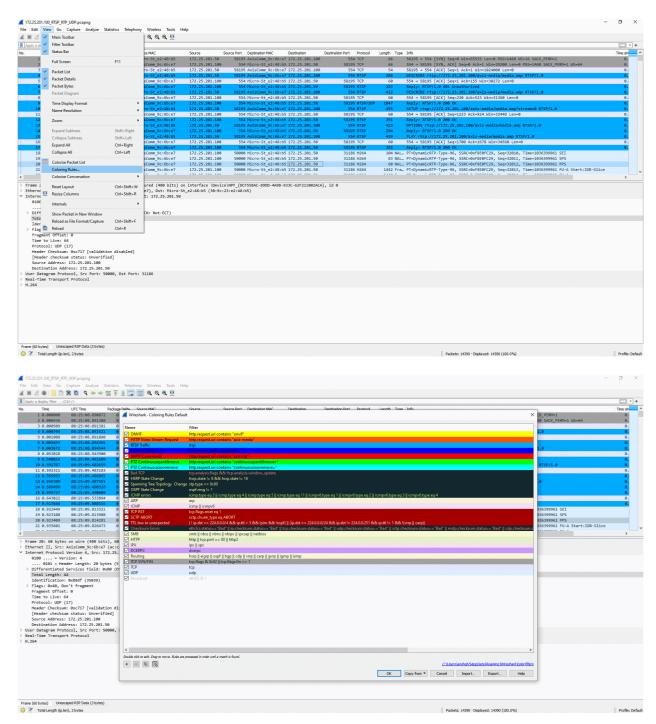
tcp contains traffic	Filter for TCP packets that contain the word 'traffic' in their payload					
tcp.flags.reset == 1	Filter for TCP resets					
tcp.analysis.retransmission	Filter for TCP retransmissions					
tcp.analysis.out_of_order	Filter for multiple paths between source and destination					
tcp.analysis.window_full	Filter for TCP Window Buffer Full Condition					
tcp.analysis.zero_window	Filter for TCP Window Buffer Full Condition					
frame.time_delta > 0.04	Filter for network traffic that are send with 40ms or more latency compared to the previous packet					
tcp.port == 80	Filter for network traffic with TCP port 80					
udp.port == 64000	Filter for network traffic with UDP port 64000					
udp.srcport==50000	Filter for network traffic with UDP source port 50000					
udp.dstport==50001	Filter for network traffic with UDP destination port 50001					
smb2 smb	Filter for SMB network protocol traffic					
p.dsfield.dscp == 0x0b	Filter for Quality of Service DSCP values, a Hex converter is needed to convert the 0x00 values					
macc.opcode == pause	Filter for Ethernet Pause-Frames					
Video streaming display filter	Description					
rtsp.request	Filter for RTSP requests such as Options, Get Parameter, Play, Setup etc					
rtsp contains "backchannel"	Filter for RTSP streams using ONVIF backchannel					
rtsp contains "onvif"	Filter for RTSP streams using the onvif protocol					
rtsp h264	Filter for RTSP and H.264 decoded RTP streams					
rtp.ssrc == 0x76747D52	Filter for RTP streams with specific source ID					
rtp contains "VirtualInput"	Filter for RTP streams containing specific keywords to identify metadata such as the Virtual Input					
(ip.src==10.25.195.92 && udp.srcport==50000 && ip.dst==10.25.185.75 && udp.dstport==31018 && rtp.ssrc==0x9c37fd6)	Filter for RTP stream with a number of specific details					
h264.nal_unit_type == 1	Filter for P-Frames only					
h264.nal_unit_type == 5	Filter for I-Frames only					
h264.start.bit == 1 & the h264.slice_type == 2	Filter for I-Frame start packages only					
h264.start.bit == 1 & t the h264.slice_type == 0	Filter for P-Frame start packages only					
h264.nal_unit_hdr == 6	Filter for SEI Frames (UserData needs to be enabled in the Axis device)					
h264.nal_unit_hdr == 7	Filter for SPS Frames					
h264.nal_unit_hdr == 8	Filter for PPS Frames					
rtp.ext eq 1	Filter for SRTP (RTSPS) streams					

Troubleshooting & maintenance

Coloring and column preferences

In Wireshark, you can set coloring rules and select and organize columns to get a better overview of the network traffic. In the following screenshots you will see how this can be configured.

With coloring rules it's possible to highlight certain types of network traffic – e.g. RTSP/RTP – in a certain color, which makes it easier to identify for the user. Configuring coloring rules works in the same way as setting display filters in Wireshark, and you can actually use the same filters.



Troubleshooting & maintenance

			i F 🛓 📜 🔍 Q Q 💷							
	y a display filter <c< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></c<>									
6	Time	UTC Time P	Package Delta Source MAC	Source	Source Port Destination MAC	Destination	Destination Port Protocol	Length Ty	pe Info	Time sin
	1 0.000000	08:25:08.890872	0.000000 Micro-St_e2:48:b5	172.25.201.50	58195 AxisComm_9c:6b:	e7 172.25.201.100	554 TCP	66	58195 -> 554 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 SACK_PERM=1	0.
	2 0.000436	08:25:08.891308	0.000436 AxisComm_9c:6b:e7	172.25.201.100	554 Micro-St_e2:48:	b5 172.25.201.50	58195 TCP	66	554 → 58195 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERN=1 WS=64	0.
	3 0.000509	08:25:08.891381	0.000073 Micro-St e2:48:b5	172.25.201.50	58195 AxisComm 9c:6b:	e7 172.25.201.100	554 TCP	54	58195 → 554 [ACK] Seg=1 Ack=1 Win=1024000 Len=0	0.
	4 0.000749	08:25:08.891621	0.000240 Micro-St e2:48:b5	172.25.201.50	58195 AxisComm 9c:6b:	e7 172.25.201.100	554 RTSP	208	DESCRIBE rtsp://172.25.201.100/axis-media/media.amp RTSP/1.0	θ.
	5 0.001008	08:25:08.891880	0.000259 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St e2:48:	b5 172.25.201.50	58195 TCP	60	554 → 58195 [ACK] Seq=1 Ack=155 Win=30272 Len=0	0.
	6 0.003493	08:25:08.894365	0.002485 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St e2:48:	b5 172.25.201.50	58195 RTSP	283	Reply: RTSP/1.0 401 Unauthorized	θ.
	7 0.003672	08:25:08.894544	0.000179 Micro-St e2:48:b5	172.25.201.50	58195 AxisComm 9c:6b:	e7 172.25.201.100	554 RTSP	422	DESCRIBE rtsp://172.25.201.100/axis-media/media.amp_RTSP/1.0	θ.
	8 0.053028	08:25:08.943900	0.049356 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St e2:48:	b5 172.25.201.50	58195 TCP	60	554 → 58195 [ACK] Seq=230 Ack=523 Win=31360 Len=0	θ.
	9 0.590816	08:25:09.481688	0.537788 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St e2:48:	b5 172.25.201.50	58195 RTSP/SDP	1847	Reply: RTSP/1.0 200 OK	θ.
	10 0.591787	08:25:09.482659	0.000971 Micro-St e2:48:b5	172.25.201.50	58195 AxisComm_9c:6b:	e7 172.25.201.100	554 RTSP	455	SETUP rtsp://172.25.201.100/axis-media/media.amp/stream=0 RTSP/1.0	θ.
	11 0.592311	08:25:09.483183	0.000524 AxisComm_9c:6b:e7	172.25.201.100			58195 TCP	60	554 → 58195 [ACK] Seq=1223 Ack=924 Win=32448 Len=0	0.
	12 0.595993	08:25:09.486865	0.003682 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St e2:48:	65 172.25.201.50	58195 RTSP	291	Reply: RTSP/1.0 200 OK	0.
	13 0,596709	08:25:09.487581	0.000716 Micro-St e2:48:55	172.25.201.50	58195 AxisComm 9c:6b:	e7 172.25.201.100	554 RTSP	423	OPTIONS rtsp://172.25.201.100/axis-media/media.amp_RTSP/1.0	0.
	14 0.599456	08:25:09.490328	0.002747 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St e2:48:	b5 172.25.201.50	58195 RTSP	294	Reply: RTSP/1.0 200 OK	θ.
	15 0.599737	08:25:09.490609	0.000281 Micro-St e2:48:b5	172.25.201.50	58195 AxisComm 9c:6b:	e7 172.25.201.100	554 RTSP	439	PLAY rtsp://172.25.201.100/axis-media/media.amp RTSP/1.0	θ.
	16 0.643022	08:25:09.533894	0.043285 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St e2:48:	b5 172.25.201.50	58195 TCP	60	554 → 58195 [ACK] Seq=1700 Ack=1678 Win=34560 Len=0	θ.
	17 0,917644	08:25:09.808516	0.274622 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St e2:48:		58195 RTSP	302	Reply: RTSP/1.0 200 OK	θ.
	18 0.922449	08:25:09.813321	0.004805 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:		31186 H264		L_ PT=DynamicRTP-Type-96, SSRC=0xF8E0FC29, Seq=32010, Time=1036399961 SEI	
	19 0.923108	08:25:09.813980	0.000659 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:		31186 H264		L PT=DynamicRTP-Type-96, SSRC=0xF8E0FC29, Seq=32011, Time=1036399961 SPS	
	20 0.923409	08:25:09.814281	0.000301 AxisComm 9c:6b:e7	172.25.201.100	50000 Micro-St e2:48:		31186 H264		L_ PT=DynamicRTP-Type-96, SSRC=0xF8E0FC29, Seg=32012, Time=1036399961 PPS	

Columns can be selected and organized to make the network traffic analysis more logical and the information more easily accessible, e.g. when following traffic from two network devices in the network.

Find Packet Find Next	Ctrl+F							C
FIND NEXT	Ctrl+N							
Find Previous		elta Source MAC			estination Port Protocol	Length Typ		Time
Find Previous	Ctrl+B	00000 Micro-St_e2:48:b5 00436 AxisComm 9c:6b:e7	172.25.201.50	58195 AxisComm_9c:6b:e7 172.25.201.100 554 Micro-St e2:48:b5 172.25.201.50	554 TCP 58195 TCP	66 66	58195 → 554 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 SACK_PERN=1 554 → 58195 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK PERN=1 WS=64	
Mark/Unmark Packet	Ctrl+M	0073 Micro-St_e2:48:b5	172.25.201.100	58195 AxisComm_9c:6b:e7 172.25.201.100	554 TCP	54	554 + 56195 [51N, ALK] SEQ=0 ACK=1 WIN=20200 Len=0 HSS=1400 SALK_PENN=1 WS=04 58195 → 554 [ACK] Seq=1 Ack=1 WIN=1024000 Len=0	
Mark All Displayed	Ctrl+Shift+M	0240 Micro-St_e2:48:b5	172.25.201.50	58195 AxisCom_9c:6b:e7 172.25.201.100	554 RTSP	208	DESCRIBE rtsp://172.25.201.100/axis-media/media.amp RTSP/1.0	
Unmark All Displayed	Ctrl+Alt+M	0259 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St_e2:48:b5 172.25.201.50	58195 TCP	60	554 → 58195 [ACK] Seg=1 Ack=155 Win=30272 Len=0	
		2485 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St e2:48:b5 172.25.201.50	58195 RTSP	283	Reply: RTSP/1.0 401 Unauthorized	
Next Mark	Ctrl+Shift+N	0179 Micro-St_e2:48:b5	172.25.201.50	58195 AxisComm_9c:6b:e7 172.25.201.100	554 RTSP	422	DESCRIBE rtsp://172.25.201.100/axis-media/media.amp RTSP/1.0	
Previous Mark	Ctrl+Shift+B	9356 AxisComm_9c:6b:e7	172.25.201.100	554 Micro-St_e2:48:b5 172.25.201.50	58195 TCP	60	554 → 58195 [ACK] Seq=230 Ack=523 Win=31360 Len=0	
Ignore/Unignore Packet	Ctrl+D	7788 AxisComm_9c:6b:e7	172.25.201.100	554 Micro-St_e2:48:b5 172.25.201.50	58195 RTSP/SDP		Reply: RTSP/1.0 200 OK	
		0971 Micro-St_e2:48:b5	172.25.201.50	58195 AxisComm_9c:6b:e7 172.25.201.100	554 RTSP	455	SETUP rtsp://172.25.201.100/axis-media/media.amp/stream=0 RTSP/1.0	
Ignore All Displayed	Ctrl+Shift+D	0524 AxisComm_9c:6b:e7	172.25.201.100	554 Micro-St_e2:48:b5 172.25.201.50	58195 TCP 58195 RTSP	60 291	554 → 58195 [ACK] Seq=1223 Ack=924 Win=32448 Len=0	
Unignore All Displayed	Ctrl+Alt+D	3682 AxisComm_9c:6b:e7 0716 Micro-St e2:48:b5	172.25.201.100	554 Micro-St_e2:48:b5 172.25.201.50 58195 AxisComm 9c:6b:e7 172.25.201.100	58195 KTSP 554 RTSP	423	Reply: RTSP/1.0 200 OK OPTIONS rtsp://172.25.201.100/axis-media/media.amp RTSP/1.0	
5.00	Ctrl+T	2747 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St e2:48:b5 172.25.201.50	58195 RTSP	294	Reply: RTSP/1.0 200 OK	
Set/Unset Time Reference		0281 Micro-St e2:48:b5	172.25.201.50	58195 AxisComm 9c:6b:e7 172.25.201.100	554 RTSP	439	PLAY rtsp://172.25.201.100/axis-media/media.amp RTSP/1.0	
Unset All Time References	Ctrl+Alt+T	3285 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St e2:48:b5 172.25.201.50	58195 TCP	60	554 → 58195 [ACK] Seg=1700 Ack=1678 Win=34560 Len=0	
Next Time Reference	Ctrl+Alt+N	4622 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St e2:48:b5 172.25.201.50	58195 RTSP	302	Reply: RTSP/1.0 200 OK	
Previous Time Reference	Ctrl+Alt+B	4805 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.201.50	31186 H264	104 NA	L_ PT=DynamicRTP-Type-96, SSRC=0xF8E0FC29, Seq=32010, Time=1036399961 SEI	
		10659 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.201.50	31186 H264		L_ PT=DynamicRTP-Type-96, SSRC=0xF8E0FC29, Seq=32011, Time=1036399961 SPS	
Time Shift	Ctrl+Shift+T	0301 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.201.50	31186 H264		L. PT=DynamicRTP-Type-96, SSRC=0xF8E0FC29, Seq=32012, Time=1036399961 PPS	
Packet Comment	Ctrl+Alt+C	2192 AxisComm_9c:6b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.201.50	31186 H264	1442 Fr	a. PT=DynamicRTP-Type-96, SSRC=0xF8E0FC29, Seq=32013, Time=1036399961 FU-A Start:IDR-Slice	
Delete All Packet Comments					54467 USC4			
. 0101 = Header Length:	- 00 huter (E)	-						
	4-14- 0-00 (00							
Ifferentiated Services Fi	ield: 0x00 (DS	CP: CS0, ECN: Not-ECT)						
ifferentiated Services Fi otal Length: 44		CP: CS0, ECN: Not-ECT)						
lfferentiated Services Fi stal Length: 44 dentification: 0x88df (35	5039)	CP: CS0, ECN: Not-ECT)						
ifferentiated Services Fi stal Length: 44 lentification: 0x88df (35 lags: 0x40, Don't fragmer agment Offset: 0	5039)	CP: CS0, ECN: Not-ECT)						
ifferentiated Services Fi stal Length: 44 lentification: 0x88df (35 lags: 0x40, Don't fragmer agment Offset: 0 ime to Live: 64	5039)	CP: CS0, ECN: Not-ECT)						
ifferentiated Services Fi ital Length: 44 lentification: 0x88df (35 lags: 0x40, Don't fragmer agment Offset: 0 me to Live: 64 rotocol: UDP (17)	5039) nt							
ifferentiated Services Fi tal Length: 44 lentification: 0x88df (35 ags: 0x40, Don't fragmer agment Offset: 0 ime to Live: 64 rotocol: UDP (17) ader Checksum: 0xc717 [v	5039) nt validation dis							
<pre>ifferentiated Services Fi tal Length: 44 lentification: 0x88df (35 ags: 0x40, Don't fragmer agment Offset: 0 me to Live: 64 rotocol: UDP (17) cader Checksum: 0xc717 [v leader Checksum status: L</pre>	5039) nt validation dis Unverified]							
Ifferentlated Services Fi tal Length: 44 dentification: 00x8df (3) lags: 0x40, Don't fragmer agment Offset: 0 ime to Live: 64 otocol: UDP (17) eader Checksum: 0x7217 [v teader checksum: status: L surce Address: 172.25.203	5039) nt validation dis Unverified] 1.100							
fferentiated Services Fi rtal Length: 44 lentification: 0x88df (35 ags: 0x40, Don't fragmer agment Offset: 0 me to Live: 64 votocol: UDP (17) adder Checksum: 0x7217 [teader checksum: 0x7217 [teader checksum: 0x727 [tea	validation dis Unverified] 1.100 25.201.50	ebled]						
fferentiated Service F; tal Length: 44 Mentification: 0x88df (3 ages: 0x40, Don't fragmer agment Offset: 0 me to Live: 64 otocol: UDP (17) ader Checksum: 0xc717 [teader Checksum status: L urce Address: 172.25.20 stimation Address: 172.15 Datagram Protocol, Src i Time Transport Protocol	validation dis Unverified] 1.100 25.201.50 Port: 50000, D	ebled]						
fferentiated Service F; tal Length: 44 Mentification: 0x88df (3 ages: 0x40, Don't fragmer agment Offset: 0 me to Live: 64 otocol: UDP (17) ader Checksum: 0xc717 [teader Checksum status: L urce Address: 172.25.20 stimation Address: 172.15 Datagram Protocol, Src i Time Transport Protocol	validation dis Unverified] 1.100 25.201.50 Port: 50000, D	ebled]						
Ifferentiated Service F: tal Length: 44 Aentification: 0x88df (3 Lags: 0x40, Don't fragmer agment Offset: 0 Lime to Live: 64 orbocol: UDP (17) aader Checksum: 8xc717 [teader Checksum: status: L surce Address: 172.25.20 Setimation Address: 172.25.25 Setimation Address: 172.25	validation dis Unverified] 1.100 25.201.50 Port: 50000, D	ebled]						
Ifferentiated Service F: tal Length: 44 Aentification: 0x88df (3 Lags: 0x40, Don't fragmer agment Offset: 0 Lime to Live: 64 orbocol: UDP (17) aader Checksum: 8xc717 [teader Checksum: status: L surce Address: 172.25.20 Setimation Address: 172.25.25 Setimation Address: 172.25	validation dis Unverified] 1.100 25.201.50 Port: 50000, D	ebled]						
033 - Mediare Lengin: Hiferentitad Services F1 Henrification: 0x886f (3 Lags: 0x40, Don't fragmen agenet Offset: 0 Henrice Context: 0 Henrice Charles (1) adder Checksum: 80c727 [V Hendress: 172.3, Soft Surce Address: 172.3, Soft Datagram Protocol, Src I Henrice Transport Protocol 4	validation dis Unverified] 1.100 25.201.50 Port: 50000, D	ebled]						
fferentiated Service F; tal Length: 44 Mentification: 0x88df (3 ages: 0x40, Don't fragmer agment Offset: 0 me to Live: 64 otocol: UDP (17) ader Checksum: 0xc717 [teader Checksum status: L urce Address: 172.25.20 stimation Address: 172.15 Datagram Protocol, Src i Time Transport Protocol	validation dis Unverified] 1.100 25.201.50 Port: 50000, D	ebled]						
Ifferentiated Service F: tal Length: 44 Aentification: 0x88df (3 Lags: 0x40, Don't fragmer agment Offset: 0 Lime to Live: 64 orbocol: UDP (17) aader Checksum: 8xc717 [teader Checksum: status: L surce Address: 172.25.20 Setimation Address: 172.25.25 Setimation Address: 172.25	validation dis Unverified] 1.100 25.201.50 Port: 50000, D	ebled]						
Ifferentiated Service F: tal Length: 44 Aentification: 0x88df (3 Lags: 0x40, Don't fragmer agment Offset: 0 Lime to Live: 64 orbocol: UDP (17) aader Checksum: 8xc717 [teader Checksum: status: L surce Address: 172.25.20 Setimation Address: 172.25.25 Setimation Address: 172.25	validation dis Unverified] 1.100 25.201.50 Port: 50000, D	ebled]						
fferentiated Service F; tal Length: 44 Mentification: 0x88df (3 agent Offset: 0 me to Live: 64 otocal: UDP (17) ader Checksum: 0xc717 [keder Checksum statust L urce Address: 172.25.20 stimation Address: 172.15 Datagram Protocol, Src i Time Transport Protocol	validation dis Unverified] 1.100 25.201.50 Port: 50000, D	ebled]						
fferentiated Service F; tal Length: 44 Mentification: 0x88df (3 agent Offset: 0 me to Live: 64 otocal: UDP (17) ader Checksum: 0xc717 [keder Checksum statust L urce Address: 172.25.20 stimation Address: 172.15 Datagram Protocol, Src i Time Transport Protocol	validation dis Unverified] 1.100 25.201.50 Port: 50000, D	ebled]						

Troubleshooting & maintenance

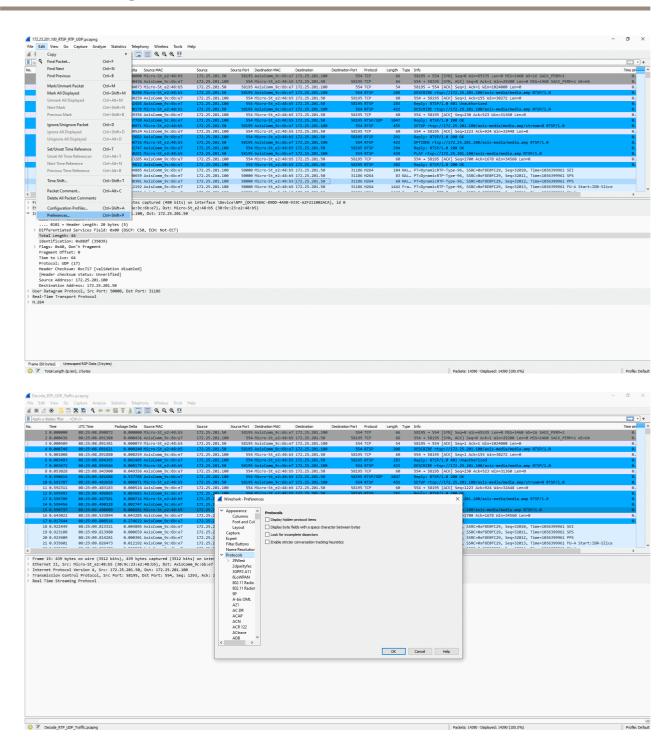
		I T 1 其 📃 Q Q Q 🖽							
oly a display filter <									
Time 1 0.000000		Package Delta Source MAC 0.0000000 Micro-St e2:48:b5	Source S 172.25.201.50	S8195 AxisComm 9c:6b:e7	Destination Destination Port	Protocol Length Typ TCP 66		eq=0 Win=65535 Len=0 MSS=1460 WS=16 SACK_PERM=1	Time
2 0.000436	08:25:08.890872 08:25:08.891308	0.0000436 AxisComm_9c:6b:e7	172.25.201.100	58195 AxisComm_90:60:e7 554 Micro-St_e2:48:b5				29=0 Win=65535 Len=0 MSS=1460 WS=16 SALK_PERM=1 [K] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=64	
3 0.000509	08:25:08.891381	0.000073 Micro-St_e2:48:b5	172.25.201.50	58195 AxisComm_9c:6b:e7	172.25.201.100 554	TCP 54	58195 → 554 [ACK] S	eq=1 Ack=1 Win=1024000 Len=0	
4 0.000749 5 0.001008	08:25:08.891621 08:25:08.891880	0.000240 Micro-St_e2:48:b5 0.000259 AxisComm_9c:6b:e7	172.25.201.50 172.25.201.100	58195 AxisComm_9c:6b:e7 554 Micro-St_e2:48:b5		RTSP 208 TCP 60		.25.201.100/axis-media/media.amp RTSP/1.0 eq=1 Ack=155 Win=30272 Len=0	
6 0.003493	08:25:08.894365	0.002485 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St_e2:48:b5	172.25.201.50 58195		Reply: RTSP/1.0 401		
7 0.003672	08:25:08.894544	0.000179 Micro-St_e2:48:b5	172.25.201.50	58195 AxisComm 9c:6b:e7	172.25.201.100 554	RTSP 422	DESCRIBE rtsp://172	.25.201.100/axis-media/media.amp RTSP/1.0	
8 0.053028	08:25:08.943900	0.049356 AxisComm_9c:6b:e7 0.537788 AxisComm 9c:6b:e7	172.25.201.100	554 Micro-St_e2:48:b5 554 Micro-St_e2:48:b5	172.25.201.50 58195 172.25.201.50 58195		554 → 58195 [ACK] St Reply: RTSP/1.0 200	eq=230 Ack=523 Win=31360 Len=0	
10 0.591787	08:25:09.482659	0.000971 Micro-St_e2:48:b5	172.25.201.50	58195 AxisComm 9c:6b:e7	172.25.201.100 554	RTSP 455	SETUP rtsp://172.25	.201.100/axis-media/media.amp/stream=0 RTSP/1.0	
11 0.592311 12 0.595993	08:25:09.483183	0.000524 AxisComm_9c:6b:e7	172.25.2 Wires	hark - Preferences			×	=1223 Ack=924 Win=32448 Len=0	
13 0.596709	08:25:09.487581	0.000716 Micro-St e2:48:55	172.25.2 × App					.201.100/axis-media/media.amp_RTSP/1.0	
14 0.599456	08:25:09.490328	0.002747 AxisComm_9c:6b:e7	1/2.25.2	Columns Displayed little		Туре	Fields Field C	c	
15 0.599737 16 0.643022	08:25:09.490609 08:25:09.533894	0.000281 Micro-St_e2:48:b5 0.043285 AxisComm_9c:6b:e7		ont and Colors No.		Number		1.100/axis-media/media.amp RTSP/1.0 =1700 Ack=1678 Win=34560 Len=0	
17 0.917644	08:25:09.808516	0.274622 AxisComm 9c:6b:e7	172.25.2 Can	ayout 🗠		Time (format as specified UTC time)	1/06 MCK-10/6 W1H-54506 CEN-6	
18 0.922449	08:25:09.813321	0.004805 AxisComm_9c:6b:e7	172.25.2 Expe	rt 🗹 Pack	age Delta	Delta time displayed		, SSRC=0xF8E0FC29, Seq=32010, Time=1036399961 SEI	
19 0.923108 20 0.923409	08:25:09.813980 08:25:09.814281	0.000659 AxisComm_9c:6b:e7 0.000301 AxisComm 9c:6b:e7		Buttons Sour	ce MAC	Hardware src addr Source address		, SSRC=0xF8E0FC29, Seq=32011, Time=1036399961 SPS , SSRC=0xF8E0FC29, Seq=32012, Time=1036399961 PPS	
21 0.935601	08:25:09.826473	0.012192 AxisComm_9c:6b:e7	172.25.2 > Prot	e Resolution Sour	ce ce Port	Source address Source port		<pre>SSRC=0xF8E0FC29, Seq=32013, Time=1036399961 FU-A Start:IDR-Slice</pre>	
			RSA	Keys 🗹 Desti	ination MAC	Hardware dest addr			
e 20: 60 byte:	on wire (480 bits)	, 60 bytes captured (480 bits)	> Stati	tics 🗹 Desti	ination ination Port	Destination address			
		ac:cc:8e:9c:6b:e7), Dst: Micro-	St_e2:48:b5	inced Desti		Destination port Protocol			
rnet Protocol 100 = Ver		2.25.201.100, Dst: 172.25.201.50		✓ Leng		Packet length (bytes)			
	der Length: 20 byte	s (5)		☑ Type ☑ Info		Custom	h264.nal_unit_hdr 0		
fferentiated	Services Field: 0x0	0 (DSCP: CS0, ECN: Not-ECT)		⊠ info ⊡ Time	since previous frame in this TCP stream		tcp.time_delta 0		
otal Length: 4	4 0x88df (35039)			Time TCP V	Window Size	Custom	tcp.window_size 0		
lags: 0x40, Do									
ragment Offset	:: 0								
ime to Live: 6									
rotocol: UDP (17) 1: 0xc717 [validatio	n disabled]		<			>		
[Header checksu	m status: Unverifie	d]	<	> + - Sho	ow displayed columns only				
	172.25.201.100 iress: 172.25.201.50					OK	Cancel Help		
		900, Dst Port: 31186	NAMES PARTY OF THE SECOND			UN	Calicei Hep		
1-Time Transpor	rt Protocol								
	aped RSP Data (3 bytes)								
							Pac	Setti: 14090 - Displayed: 14090 (100.0%)	Pro
							Pa	Sect: 14396 - Decklyed: 14390 (100.0%)	Pri
Total Length (p. le	c.pcapng						Pa	šets: 14090 - Displayes: 14000 (100.0%)	
Total Length (p.le le_RTP_UDP_Traffi it View Go	n), 2 bytes c.pcapng Capture Analyze Sta	tástica Telegobory Wireless Tools I	Help				Par	Sets: 14399 - Digdayed: 14590 (100.0%) —	
Total Length (p.le de_RTP_UDP_Traffi dit View Go	n), 2 bytes c.pcapng Capture Analyze Sta X 2 4 + + + + + + + + + + + + + + + + + +	tistics Telephony Wireless Tools ■ 🐨 差 👮 🚍 🚍 🗣 🔍 🤻 🕂	itelp				Pa	Sets: (4390 - Daplayed: 14390 (100.0%) —	Pro
Total Length (p.le de_RTP_UDP_Traffi dit View Go d @	n), 2 bytes c.pcapng Capture Analyze Sta X III (: Ŧ ± <mark>.</mark>			Declarity Declarity	Rebrief Tech		Sets: 14390 - Disolayes: 14390 (130.0%) ————————————————————————————————————	0
Total Length (p.le de_RTP_UDP_Traffi dit View Go	n), 2 bytes c.pcapng Capture Analyze Sta X III (e T 🛓 🚍 🔍 🔍 🔍 🛄	Source S		Destivation Destination Port	TCP 66	e Info		σ
Total Length (p.le de_RTP_UDP_Traffi it View Go @	n), 2 bytes cpcapng Capture Analyze Ste Capture	Image Delta Source MAC 0.000000 Micro-St_e2:48:b5 0.000045 AxisComm_9c:6b:e7	Source S 172.25.201.50 172.25.201.100	58195 AxisComm_9c:6b:e7 554 Micro-St_e2:48:b5	172.25.201.100 554 172.25.201.50 58195	TCP 66 TCP 66	e Info 58195 + 554 [SYN] S 554 + 58195 [SYN, A	- RegP Win-65535 Lemit RSS-1468 US-10 SACC (2001-1 CC) Seq10 Acket Min-20200 Lemit RSS-1468 SACC (2001-1 US-64	٥
Total Length (p.le de_RTP_UDP_Traffi it View Go @ @	n), 2 bytes Capture Analyze Sta	Image Deta Source MAC 0.0000000 Micro-St_e2:48:55 0.0000036 Micro-St_e2:48:55 0.000037 Micro-St_e2:48:55	Source S 172.25.201.50 172.25.201.100 172.25.201.50	58195 AxisComm_9c:6b:e7 554 Micro-St_e2:48:b5 58195 AxisComm_9c:6b:e7	172.25.201.100 554 172.25.201.50 58195 172.25.201.100 554	TCP 66 TCP 66 TCP 54	e Info 58195 → 554 [SWN] S 554 → 58195 [SWN, S 58195 → 554 [ACK] S 58195 → 554 [ACK] S	- Rep# Mine5535 Lene# MS5=1468 MS=16 S4CK_PE8H=1 CK] Sece# Ackst Mine2280 Lene# MS5=1468 S4CK_PE8H=1 MS=64 April Ackst Mine2480 Lene#	٥
Total Length (p.le de_RTP_UDP_Traffi it View Go @	n), 2 bytes cpcapng Capture Analyze Ste Capture	Image Delta Source MAC 0.0000000 Nicro-St_e2:48:55 0.0000073 Nicro-St_e2:48:155 0.0000073 Nicro-St_e2:448:155	Source S 172.25.201.50 172.25.201.100 172.25.201.50 172.25.201.50	58195 AxisComm_9c:6b:e7 554 Micro-St_e2:48:b5 58195 AxisComm_9c:6b:e7 58195 AxisComm_9c:6b:e7	172.25.201.100 554 172.25.201.50 58195 172.25.201.100 554 172.25.201.100 554	TCP 66 TCP 66 TCP 54 RTSP 208	e Info 58195 + 554 [SYN] S 554 + 58195 [SYN, A 58195 + 554 [ACK] S DESCREE ertspt//122	- Pepel Mines5535 Law-P RSS-1468 US-16 SECK (POIN-1 CC) Seque Acket Mines25200 Law-P RSS-1640 SECK (POIN-1 Security Content of the Security Secu	C) Time
Total Length (p.le le_RTP_UDP_Traffit it View Go © © © © © © display filter <1 Time 1 6,060000 2 6,060569 4 0.060549 5 0.061085 6 0.063493	n), 2 bytes Capture Analyze Sta Capture Analyze Sta Capture Analyze Sta Capture Analyze Sta Capture Analyze Sta Capture P 08:25:06.091308 08:25:06.091308 08:25:06.091308 08:25:06.091308 08:25:06.091308	************************************	Source S 172.25.201.50 172.25.201.100 172.25.201.50 172.25.201.50 172.25.201.100 172.25.201.100	58195 AxisComm_9c:6b:e7 554 Micro-St_e2:48:b5 58195 AxisComm_9c:6b:e7 58195 AxisComm_9c:6b:e7 554 Micro-St_e2:48:b5 554 Micro-St_e2:48:b5	172.25.201.100 554 172.25.201.50 58195 172.25.201.100 554 172.25.201.100 554 172.25.201.50 58195 172.25.201.50 58195 172.25.201.50 58195	TCP 66 TCP 66 TCP 54 RTSP 208 TCP 60 RTSP 283	e Info 58185 → 554 [SWN] 5 554 + 58195 [SYN, A 58195 → 554 [ACK] 5 DESCRIEC #Exp://322 554 + 58195 [ACK] 5 Reply: RTSP1,0 481	- eq=0 k1m65535 Lem0 PISS-1460 kS-16 SACC PE0H-1 CC] Secto Actor 1 k1m52200 Lem0 PISS-1460 SACC PE0H-1 kS-64 eq=1 Actor 1 k1m52200 Lem0 PISS/140 Pisstber 1220 Pissber 1220 Lem0	5
Total Length (p.le le, RTP_UDP_Traffi it View Go control (Control (Contr	n), 2 bytes Capture Analyze Sta S S S S S S S S S S S S S S S S S S S	************************************	Source S 172.25.201.50 172.25.201.50 172.25.201.50 172.25.201.50 172.25.201.100 172.25.201.100 172.25.201.100 172.25.201.50	58195 AxisCom_9c:6b:e7 554 Micro-St_e2:48:b5 58195 AxisCom_9c:6b:e7 58195 AxisCom_9c:6b:e7 554 Micro-St_e2:48:b5 554 Micro-St_e2:48:b5 58195 AxisCom_9c:6b:e7	172.25.201.100 554 172.25.201.50 5510 172.25.201.100 554 172.25.201.100 554 172.25.201.100 554 172.25.201.50 5510 172.25.201.50 5510	TCP 66 TCP 66 TCP 54 RTSP 208 TCP 60 RTSP 283 RTSP 422	e Info 55195 + 554 [5VN] S 554 + 58195 [5VN, A 55195 + 554 [SVN, A 55195 + 55195 [ACK] S 554 + 58195 [ACK] S 754 + 58195 [ACK] S 754 + 58195 [ACK] S	- Rept Min-65535 Lamer RSS-1468 US-16 SACC (2689-1 CC) Seqte Ackst Min-32280 Leme RSS-1468 SACC (2689-1 US-64 egal Ackst Min-32480 Leme Sci 2524, 109 Acid Sci 2689-1 US-64 egal Ackst Min-3227 Leme 2524, 109 Acid Sci 2689-1 US-64 Example Acid Min-3289 Leme 2524, 109 Acid Sci 2689, 2014 2524, 109 Acid Sci 268, 2014 2524, 2014 Acid	5
Total Length (p.le le, RTP_UDP_Traffi it View Go control (Control (Contr	n), 2 bytes Capture Analyze Sta Capture Analyze Sta Capture Analyze Sta Capture Analyze Sta Capture Analyze Sta Capture P 08:25:06.091308 08:25:06.091308 08:25:06.091308 08:25:06.091308 08:25:06.091308	************************************	Source S 172, 25, 201, 50 172, 25, 201, 100 172, 25, 201, 50 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100	58195 AxisCom_9c:6b:e7 554 Micro-5t_e2:48:b5 58195 AxisCom_9c:6b:e7 58195 AxisCom_9c:6b:e7 554 Micro-5t_e2:48:b5 58195 AxisCom_9c:6b:e7 58195 AxisCom_9c:6b:e7 58195 AxisCom_9c:6b:e7	172.25.201.100 554 172.25.201.50 5519 172.25.201.100 554 172.25.201.100 554 172.25.201.50 5519 172.25.201.50 5619 172.25.201.50 5619 172.25.201.50 5619 172.25.201.50 5619 172.25.201.50 5619 172.25.201.50 5619	TCP 66 TCP 66 TCP 54 RTSP 288 TCP 60 RTSP 283 RTSP 283 TCP 60 COMPARISON 60	e Info 58105 + 554 [SVN] S 554 + 58105 [SVN, A 58105 + 554 [ACK] S DESCREE resp.//J22 554 + 58105 [ACK] S 554 + 58105 [ACK] S 554 + 58105 [ACK] S	eq=0 klim65535 Lem0 765-1460 k5-16 SACC PE0H-1 CCJ Sector Ack-1 klim25280 Lem0 7655-160 SACC PE0H-1 k5-64 eq=0 Ack-1 klim25280 Lem0 25-261 Ack-1 klim25280 Lem0 25-261 Ack-1 klim2522 Lem0 25-261 Ack-125 Allocation State 25-261 Allocation State 25-	5
Total Length (p.le RTP_UDP_Traffit it View Go © © © © © © © Time 1 6.000000 2 6.000436 3 0.000549 5 0.000549 5 0.0003493 7 0.0003672 8 0.053028 9 0.550816	n), 2 bytes Cectopro Capture Analyze Sta X Q Q Q Q Q Q UTC Tme P 00:225:06.090730 00:225:06.09130 00:225:00.09130 00:25:0000 00:25:000 0	************************************	Source S 172.25.201.50 172.25.201.50 172.25.201.50 172.25.201.50 172.25.201.100 172.25.201.100 172.25.201.100 172.25.201.50	58195 AxisCom_9c:6b:e7 554 Micro-St_e2:48:b5 58195 AxisCom_9c:6b:e7 58195 AxisCom_9c:6b:e7 554 Micro-St_e2:48:b5 554 Micro-St_e2:48:b5 58195 AxisCom_9c:6b:e7	172,25,201,100 554 172,25,201,50 561 172,25,201,100 554 172,25,201,100 554 172,25,201,100 554 172,25,201,50 56195 172,25,201,50 56195 172,25,201,50 56195	TCP 66 TCP 66 TCP 54 RTSP 288 TCP 60 RTSP 283 RTSP 283 TCP 60 COMPARISON 60	e Info 56105 + 554 [57N] 5 554 + 58105 [57N], A 554 + 58105 [57N], A 554 + 58105 [57N], A 554 + 58105 [67C] 5 Reply: RTSP1, B 750 [570] 7 860]); RTSP1, B 750 [5710] 7 870 [5700] 7 870 [57		0
Total Length (p.)e	n), 2 bytes Ceptang Cepture Andyze Sta Station Control (Control (Contro)	E T A T B C	Source S 172, 25, 201, 50 172, 25, 201, 50 172, 25, 201, 50 172, 25, 201, 50 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100	58195 AxisCom 9c:6b:e7 554 Hicro-5t, e2:48:05 58195 AxisCom 9c:6b:e7 58195 AxisCom 9c:6b:e7 554 Hicro-5t, e2:48:05 554 Hicro-5t, e2:48:05 555 Hicro-5t, e2:48:05 554 Hicro-5t, e2:48:05 554 Hicro-5t, e2:48:05 55195 AxisCom 9c:6b:e7 554 Hicro-5t, e2:48:05	172.25.201.100 555 172.25.201.100 551 172.25.201.100 554 172.25.201.100 554 172.25.201.50 5615 172.25.201.50 5615 172.25.201.50 5615 172.25.201.50 5615 172.25.201.50 5615 172.25.201.50 5615	TCP 66 TCP 66 TCP 54 RTSP 283 RTSP 283 RTSP 422 TCP 60 RTSP 422 TCP 60 RTSP 422 TCP 60 RTSP 1847 RTSP 455 TCP 60	e bró 81355 + 554 (511) 5 5419 + 555 (511) 5 5419 + 555 (511) 5 5419 + 510 5 545 + 5119 5 (521) 5 545 + 5119 5 (521) 5 554 + 5105 (521) 5 554 + 5105 (521) 5 554 + 5105 (521) 5		0
Total Length (p. le RE, PL, UDP, Tradific t: View Go Goody filter <1 Time 10,000000 20,000000 40,0000749 50,000000 40,0000749 50,000000 60,0001493 70,000072 50,000000 60,0001493 70,000072 50,000000 10,00000 10,000000 10,00000 10,00000 10,00000 10,000000 10	n), 2 bytes Capture Analyze Sta Sta Capture	************************************	Source S 172, 25, 281, 59 172, 25, 201, 59 172, 25, 201, 59 172, 25, 201, 59 172, 25, 201, 109 172, 25, 201, 109 172, 25, 201, 59 172, 25, 201, 59 172, 25, 201, 59 172, 25, 201, 59 172, 25, 201, 59 172, 25, 201, 59 172, 25, 201, 59 172, 25, 201, 59 172, 25, 201, 59 172, 25, 201, 59	58155 Avia Com 9: ecibire7 554 Micro-St, e2:48:65 58155 Avia Com 9: ecibire7 584 Micro-St, e2:48:65 584 Micro-St, e2:48:65 585 Micro-St, e2:48:65	172.25.201.100 555 172.25.201.100 555 172.25.201.100 555 172.25.201.100 555 172.25.201.100 555 172.25.201.50 5519 172.25.201.50 5519 172.50 5519 172.50 5519 172.50 5519 172.50 5519 172.50 5519 1	TCP 66 TCP 66 TCP 54 RTSP 288 TCP 60 RTSP 283 RTSP 283 RTSP 422 TCP 60 RTSP 422 RTSP 455 TCP 60 RTSP/S2F 1047 RTSP 455 TCP 60 RTSP 291	e 1x60 50.055 + 554 [570] 5 554 + 50.055 [570], 5 50155 + 5540 [570], 5 504 + 36.05 [570], 5 504 + 36.05 [670] 5 564 + 36.05 [670] 5 564 + 36.05 [670] 5 564 + 50.05 [670] 5 574 + 50.05 [770] 5 574 + 50.05 [770	- Require Mannessiss Learning MSS-1464 MS-16 SACC, PEBH-1 CCJ Sequire Ackes Mannessiss Learning MSS-1464 SACC, PEBH-1 MS-64 eq-1 Acket Mannessiss and REMOVED as MISP/1.4 Social Saction Removed Saction Removed Action Mannessis and REMOVED as MISP/1.4 Mannessiss and REMOVED as MISP/1.4 Mannessiss and REMOVED as MISP/1.4 Mannessiss and REMOVED as MISP/1.4 MISP/REMOVED as MISP/1.4 MISP/REMOVED as MISP/REMOVED as MISP/1.4 MISP/REMOVED as MISP/REMOVED as MISP/1.4 MISP/REMOVED as	5
Total Length (p. k Me, RTP, UDP, Traffic Wiew Go Image: Comparison of the state of	n), 2 bytes Capture Analyze State Capture Analyze State Capture Analyze State Capture Capture Analyze State Capture Capture Analyze State S	T I	Source S 172, 25, 201, 50 172, 25, 201, 50 172, 25, 201, 50 172, 25, 201, 50 172, 25, 201, 50 172, 25, 201, 100 172, 25, 201, 50 172, 25, 201, 50 172, 25, 201, 50 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 100 172, 25, 201, 50 172, 25, 201, 50	5105 Aviscom 9:erőber 554 Nicros 9:erőber 554 Nicros 9:erőber 554 Nicros 9:erőber 554 Nicros 5, erőkös 515 Aviscom 9:erőber 515 Aviscom 9:erőber 554 Nicros 5, erőkös 555 Aviscom 9:erőber 555 Nicros 5, erőkös 555 Nicros 5, erőkös 555 Nicros 5, erőkös 555 Nicros 5, erőkös 555 Nicros 5, erőkös	122, 25, 201, 160 555 122, 25, 201, 160 559 122, 25, 201, 160 559 122, 25, 201, 160 559 122, 25, 201, 160 559 122, 25, 201, 160 561 122, 25, 201, 160 561 122, 25, 201, 160 551 122, 25, 201, 160 551 122, 25, 201, 50 5510 122, 25, 201, 50 5510 122, 25, 201, 50 5510 122, 25, 201, 50 5510 122, 25, 201, 50 5510 122, 25, 201, 50 5510 122, 25, 201, 50 5510 122, 25, 201, 50 5510 122, 25, 201, 50 5510 122, 25, 201, 50 5510 122, 25, 201, 50 5510 122, 25, 201, 50 5510 122, 25, 201, 50 5510 122, 25, 201, 50 5510 122, 25, 201, 50 5510 122, 25, 201, 50 5510 122, 25, 201, 50 5510 124, 25, 201, 50 5510 <t< td=""><td>TCP 66 TCP 66 TCP 54 RTSP 283 RTSP 283 RTSP 422 RTSP 425 TCP 60 RTSP 455 TCP 60 RTSP 455 TCP 60 RTSP 291 RTSP 291 RTSP 423</td><td>e 1x60 50.055 + 554 [570] 5 554 + 50.055 [570], 5 50155 + 5540 [570], 5 504 + 36.05 [570], 5 504 + 36.05 [670] 5 564 + 36.05 [670] 5 564 + 36.05 [670] 5 564 + 50.05 [670] 5 574 + 50.05 [770] 5 574 + 50.05 [770</td><td>- sq=0 kine65535 Lem0 /RSS-1460 kS-16 SACC /PEBH-1 C2 [Sector Action & MSS-1460 BS-16 SACC /PEBH-1 SS-64 SS-160 SACC /PEBH-1 KS-64 SS-283 Lem0 /PSS-100 SACC /PEBH-1 KS-64 SS-283 Lem0 /PSS-284 Lem0 /PSS-100 SACC /PEBH-1 /PSC-100 SACC /PEBH-1 /</td><td>5</td></t<>	TCP 66 TCP 66 TCP 54 RTSP 283 RTSP 283 RTSP 422 RTSP 425 TCP 60 RTSP 455 TCP 60 RTSP 455 TCP 60 RTSP 291 RTSP 291 RTSP 423	e 1x60 50.055 + 554 [570] 5 554 + 50.055 [570], 5 50155 + 5540 [570], 5 504 + 36.05 [570], 5 504 + 36.05 [670] 5 564 + 36.05 [670] 5 564 + 36.05 [670] 5 564 + 50.05 [670] 5 574 + 50.05 [770] 5 574 + 50.05 [770	- sq=0 kine65535 Lem0 /RSS-1460 kS-16 SACC /PEBH-1 C2 [Sector Action & MSS-1460 BS-16 SACC /PEBH-1 SS-64 SS-160 SACC /PEBH-1 KS-64 SS-283 Lem0 /PSS-100 SACC /PEBH-1 KS-64 SS-283 Lem0 /PSS-284 Lem0 /PSS-100 SACC /PEBH-1 /PSC-100 SACC /PEBH-1 /	5
Total Length (p. le le, RTP_LUPP_Traffic t View Go Ime Ime 1 0.000000 Image: Image Strategy Image Strategy 2 0.000000 3 0.000000 4 0.000000 5 0.000000 6 0.000000 9 0.500010 10 0.500010 10 0.500010 10 0.500010 10 0.500010 10 0.500010 10 0.500010 10 0.500010 10 0.500010 10 0.500010 10 0.500010 10 0.500010 10 0.500010 10 0.500010 10 0.500010 10 0.500010 10 0.500010 10 0.500010	n), 2 bytes Coptons Copture Analyze Sta Statistics Copture Analyze Statistics Copture Analyze Statistics Copture Analyze Statistics Copture Company Copture Company Cop	T 2	Source 5 172, 25, 201, 50 172, 25, 201, 100 172, 25, 201, 100	50155 AvisCom 9:er6bre7 554 Nicro-51; er248/55 50155 AvisCom 9:er6bre7 50155 AvisCom 9:er6bre7 504 Nicro-51; er248/55 504 Nicro-51; er248/55	$\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	TCP 66 TCP 66 TCP 54 RTSP 288 RTSP 283 RTSP 422 TCP 60 RTSP 422 RTSP 1047 RTSP 455 TCP 60 RTSP 291 RTSP 423 RTSP 294 RTSP 294 RTSP 294 RTSP 294 RTSP 243	 bio 5519 - 554 [SW] 5 554 - 5305 [SW], 5 5554 - 5305 [SW], 6 5554 - 5410 - 420 5554 - 5410 - 5410 5554 - 5410 - 5410 554 - 5510 - 5420 555 - 5510 - 5510 555 - 5510 - 5510 555 - 5510 - 5510 556 - 5510 - 5510	- Repeb Min-055335 Leme9 HS5-1460 NS-12 SACC PEBH-1 CC] Sequed Ack-1 Min-32240 Leme9 HS5-1460 SACC PEBH-1 NS-64 eq:1 Ack-1 Min-322400 Leme9 eq:1 Ack-1 Min-322400 Leme9 eq:2 Ack-13 Min-32400 Leme9 Min-3440 Ack-13 Min-3140 Leme9 Min-3440 Ack-13 Min-3140 Leme9 Min-3440 Ack-13 Min-3440 Leme9 Min-3440	0
Total Length (p. le E.T.P. UDP. Traffic View Go October Time 1 0.000407	n), 2 bytes Cpcapeng Captore Analyze State Captore Capt	Image: The second sec	Source S 172: 25: 261: 50 107 172: 25: 201: 198 172: 25: 201: 198 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36	5015 Ailcom Becker 554 Nicro-54 2248405 8519 Ailcom Becker 5519 Ailcom Becker 5519 Ailcom Becker 554 Nicro-54 2244405 554 Nicro-54 224405 554 Nicro-54 224405	172:25:201:160 554 172:25:	TCP 66 TCP 66 TCP 54 RTSP 208 RTSP 208 RTSP 283 RTSP 283 RTSP 283 RTSP 422 TCP 60 RTSP 455 RTSP 455 RTSP 291 RTSP 294 RTSP 294 RTSP 439 RTSP 60	 b6 5355 + 554 [571] 5 554 + 5515 [571, 3 554 + 5515 [571, 3 554 + 5515 [571] 5 	-	0
Total length (p.le ■ RTP_UDP_Traffic t View Go 2 ● Traffic 1 0.000001 2 ● Golden 2 0.000010 3 0.000010 4 0.000010 5 0.001000 6 0.000100 7 0.000100 9 0.500100 0 0.500100 0 0.500100 0 0.500100 0 0.500010 0 0.500010 0 0.500010 0 0.500010 0 0.500010 0 0.500010 0 0.500010 0 0.500010 0 0.500010 0 0.500010 0 0.500010 0 0.500010 0 0.500010 0 0.500010 0 0.500010 0 0.500010	n), 2 bytes Copcaping Capture Analyze Sta Standing Capture Analyze Sta Capture Analyze Sta Capture Canady Standing Capture Capture Canady Standing Capture Capture Canady Standing Capture Capture Capture Capture Capture Capture Capture Capture Capture Capture Capture	T 1 1 1 1 1 Hold State Source MAC 0	Source 5 172, 25, 261, 36 172, 25, 261, 36	58195 Acistom g.ccbirt 2 554 Nicro-52 c2448105 2010 Acistom Scröber 2 519 Nicro-52 c2448105 2010 Acistom Scröber 2 544 Nicro-52 c2448105 554 Nicro-52 c2448105 554 Nicro-52 c2448105 554 Nicro-52 c2448105 519 Acistom Scröber 2 519 Acistom Scröber 2 510 Acistom Scröb	$\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	TCP 66 TCP 66 TCP 54 RTSP 288 RTSP 283 RTSP 283 RTSP 283 RTSP 422 TCP 60 RTSP 455 RTSP 291 RTSP 293 RTSP 294 RTSP 293 RTSP 294 RTSP 294 RTSP 294 RTSP 294 RTSP 294 RTSP 294 RTSP 392	e 1/5 53139 + 554 [511] 554 + 53139 [554] 554 + 53139 [554] 554 + 53139 [554] 554 + 53139 [554] 554 + 53159 [557] 554 +		5
Total Length (p. k de, RTP_UDP_Traffi ist View Go deptoy filter de mene 0 .0000435 3 0.000549 2 0.000549 3 0.0	n), 2 bytes Cpcapeng Captore Analyze State Composition	Image: The second sec	Source S 172: 25: 261: 50 107 172: 25: 201: 198 172: 25: 201: 198 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36 172: 25: 201: 36	5015 Ailcom Becker 554 Nicro-54 2248405 8519 Ailcom Becker 5519 Ailcom Becker 5519 Ailcom Becker 554 Nicro-54 2244405 554 Nicro-54 224405 554 Nicro-54 224405	$\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	TCP 66 TCP 66 TCP 54 RTSP 288 TCP 60 RTSP 223 RTSP 422 RTSP 422 RTSP 425 TCP 60 RTSP 425 RTSP 291 RTSP 423 RTSP 424 RTSP 429 RTSP 439 TCP 60 RTSP 439 TCP 60 RTSP 392 H224 104	 job S1055 = 555 (2017) S1055 = 55155 (2017) S1055 = 55155 (2017) S1055 = 5515 (2017) S1055 = 55105 (2017) S1055 = 55105	-	0

Decode RTP/UDP traffic

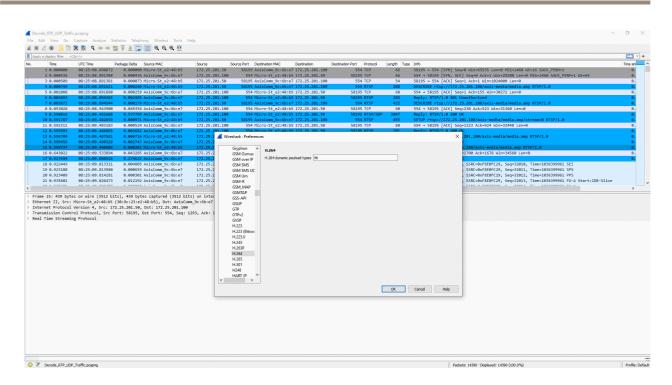
In order to analyze H.264 network related traffic successfully, it's essential that you configure Wireshark to decode video streaming related traffic. With this in place, more useful display filters can be used too. The following screenshots illustrate the correct configuration (i.e. **H.264 dynamic payload types** set to "96") to decode RTP network traffic transported via UDP since H.264 needs to be in place for that.

This network trace can be used for testing the steps below.

Troubleshooting & maintenance



Troubleshooting & maintenance



Decode RTP/TCP traffic

In order to analyze H.264 network related traffic successfully, it's essential that you configure Wireshark to decode video streaming related traffic. With this in place, more useful display filters can be used too. The following screenshots illustrate the correct configuration (RTP over RTSP encapsulated) to decode RT(S)P network traffic transported via TCP since H.264 needs to be in place for that.

This network trace can be used for testing the steps below.

a display filter <c< th=""><th></th><th>Display Filters</th><th></th><th>N.</th><th></th><th></th><th></th><th></th><th></th><th></th></c<>		Display Filters		N.						
	HL/S	Display Filter Macros		-						E
Time	UTC Te	Display Filter Expression	n		Source S	ource Port Destination MAC Destination	Destination Port Protocol	Length Type	Tala	Time
1 0.000000	08:25			:b5	172.25.201.50	58195 AxisComn 9c:6b:e7 172.25.201.100	554 TCP	66	58195 → 554 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 SACK PERM=1	Ime
2 0.000436	08:25	Apply as Column	Ctrl+Shift+I	:e7	172.25.201.100	554 Micro-St_e2:48:b5 172.25.201.50	58195 TCP	66	554 → 58195 [SYN, ACK] Seq-0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=64	
3 0.000509	08:25	Apply as Filter	•	:b5	172.25.201.50	58195 AxisComm 9c:6b:e7 172.25.201.100	554 TCP	54	58195 -> 554 [ACK] Seg=1 Ack=1 Win=1024000 Len=0	
4 0.000749	08:25	Prepare as Filter	•	: b5	172.25.201.50	58195 AxisComm 9c:6b:e7 172.25.201.100	554 RTSP	208	DESCRIBE rtsp://172.25.201.100/axis-media/media.amp RTSP/1.0	
5 0.001008	08:25	Conversation Filter		:e7	172.25.201.100	554 Micro-St_e2:48:b5 172.25.201.50	58195 TCP	60	554 → 58195 [ACK] Seq=1 Ack=155 Win=30272 Len=0	
6 0.003493	08:25	conversation rater		:e7	172.25.201.100	554 Micro-St_e2:48:b5 172.25.201.50	58195 RTSP	283	Reply: RTSP/1.0 401 Unauthorized	
7 0.003672	08:25	Enabled Protocols	Ctrl+Shift+E	: b5	172.25.201.50	58195 AxisComm_9c:6b:e7 172.25.201.100	554 RTSP	422	DESCRIBE rtsp://172.25.201.100/axis-media/media.amp RTSP/1.0	
8 0.053028	08:25	Decode As	Ctrl+Shift+U	:e7	172.25.201.100	554 Micro-St_e2:48:b5 172.25.201.50	58195 TCP	60	554 → 58195 [ACK] Seq=230 Ack=523 Win=31360 Len=0	
9 0.590816 10 0.591787	08:25	Reload Lua Plugins	Ctrl+Shift+L	:e7	172.25.201.100 172.25.201.50	554 Micro-St_e2:48:b5 172.25.201.50	58195 RTSP/SDP	1047	Reply: RTSP/1.0 200 OK	
10 0.591787	08:25 08:25	iteloba caa riagina	curr shiner c	:05 :e7	172.25.201.50	58195 AxisComm_9c:6b:e7 172.25.201.100 554 Micro-St e2:48:b5 172.25.201.50	554 RTSP 58195 TCP	455 60	SETUP rtsp://172.25.201.100/axis-media/media.amp/stream=0 RTSP/1.0 554 → 58195 [ACK] Seq=1223 Ack=924 Win=32448 Len=0	
L1 0.592311 L2 0.595993	08:25	SCTP	•	.e/	172.25.201.100	554 Micro-St_e2:48:05 172.25.201.50 554 Micro-St_e2:48:05 172.25.201.50	58195 TCP 58195 RTSP	291	SS4 → S8195 [ACK] SEq=1223 ACK=924 MIN=32448 Len=0 Reply: RTSP/1.0 200 OK	
13 0.596709	08:25	Follow	,	eb5	172.25.201.100	58195 AxisComm 9c:6b:e7 172.25.201.100	554 RTSP	423	OPTIONS rtsp://172.25.201.100/axis-media/media.amp RTSP/1.0	
14 0.599456	08:25			107	172.25.201.100	554 Micro-St e2:48:b5 172.25.201.50	58195 RTSP	294	Reply: RTSP/1.0 200 OK	
5 0.599737	08:25	Show Packet Bytes	Ctrl+Shift+O	eb5	172.25.201.50	58195 AxisComm 9c:6b:e7 172.25.201.100	554 RTSP	439	PLAY rtsp://172.25.201.100/axis-media/media.amp RTSP/1.0	
6 0.643022	08:25	Expert Information		:e7	172.25.201.100	554 Micro-St e2:48:b5 172.25.201.50	58195 TCP	60	554 → 58195 [ACK] Seg=1700 Ack=1678 Win=34560 Len=0	
7 0.917644	08:25:0		AXISCOM 9C:0	0:e7	172.25.201.100	554 Micro-St_e2:48:b5 172.25.201.50	58195 RTSP	302	Reply: RTSP/1.0 200 OK	
8 0.922449			AxisComm 9c:6	b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.201.50	31186 H264		. PT=DynamicRTP-Type-96, SSRC=0xF8E0FC29, Seq=32010, Time=1036399961 SEI	
9 0.923108			AxisComm_9c:6		172.25.201.100	50000 Micro-St_e2:48:b5 172.25.201.50	31186 H264		. PT=DynamicRTP-Type-96, SSRC=0xF8E0FC29, Seq=32011, Time=1036399961 SPS	
0 0.923409	08:25:0	9.814281 0.000301	AxisComm_9c:6	b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.201.50	31186 H264	60 NAL	. PT=DynamicRTP-Type-96, SSRC=0xF8E0FC29, Seq=32012, Time=1036399961 PPS	
1 0.935601	08:25:0	9.826473 0.012192	AxisComm 9c:6	b:e7	172.25.201.100	50000 Micro-St_e2:48:b5 172.25.201.50	31186 H264	1442 Fra.	. PT=DynamicRTP-Type-96, SSRC=0xF8E0FC29, Seq=32013, Time=1036399961 FU-A Start:IDR-Slice	
15: 439 byte net II, Src: net Protocol mission Contr	Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8		WZACA}, id 0			
e 15: 439 byte rnet II, Src: rnet Protocol smission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	WZACA}, id 0			
rnet II, Src: rnet Protocol	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	WZACA}, id 0			
e 15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	WZACA}, id 0			
e 15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	12ACA}, id 0			
: 15: 439 byte met II, Src: met Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	22ACA}, id 0			
15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	22ACA}, id 0			
15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	22ACA}, id 0			
15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	22CA}, id 0			
15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	ZACA}, id e			
15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	224CA}, id 0			
15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	224CA}, id e			
15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	ZZACA}, id e			
15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	22ACA), id e			
15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	22ACA), id e			
15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	22ACA}, id 0			
15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	22ACA}, id e			
: 15: 439 byte met II, Src: met Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	224CA), 14 0			
: 15: 439 byte met II, Src: met Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	226A), 14 0			
15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	226A), id 0			
15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	226A), 14 0			
15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	226A); id 0			
15: 439 byte net II, Src: net Protocol mission Contr	s on wire Micro-St_e Version 4, ol Protoco	(3512 bits), 439 byt e2:48:b5 (30:9c:23:e2 , Src: 172.25.201.50, ol, Src Port: 58195,	2:48:b5), Dst: Dst: 172.25.2	AxisCon 01.100	m_9c:6b:e7 (ac:cc:8	3e:9c:6b:e7)	226A), 14 0			

Troubleshooting & maintenance

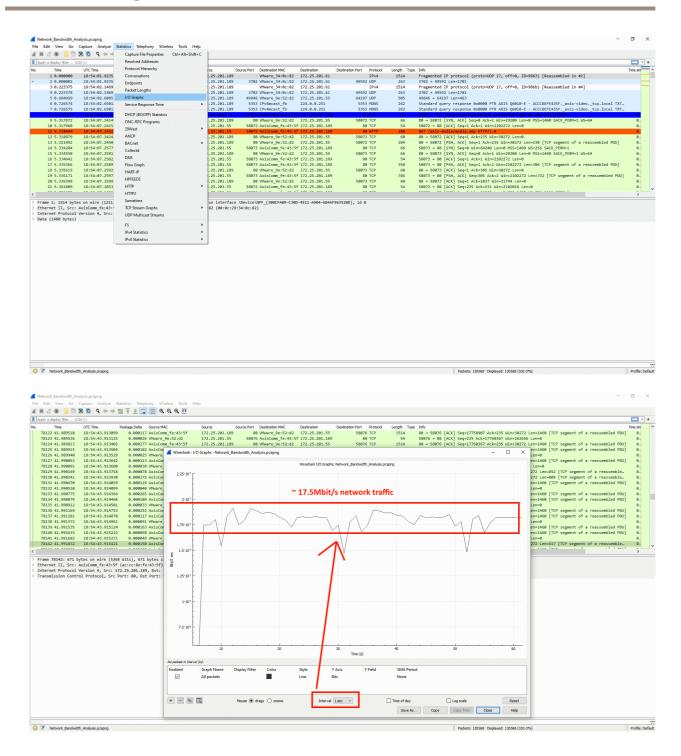
	Ctrl-/>	ackage Delta Source MAC	Source Sour	ce Port Destination MAC Destination Des	tination Port Protocol	Length Type	1.1.				Time
Time 1 0.000000	08:25:08.890872	0.000000 Micro-St e2:48:		58195 AxisComm 9c:6b:e7 172.25.201.100	554 TCP	66		54 [SYN] Seg=0 Win=	65535 Le	1-0 MSS=1460 WS=16 SACK PERM=1	line
2 0.000436	08:25:08.891308	0.000436 AxisComm_9c:6b:	27 172.25.201.100	554 Micro-St_e2:48:b5 172.25.201.50	58195 TCP	66	554 → 581	.95 [SYN, ACK] Seq=0	Ack=1 W	in=29200 Len=0 MSS=1460 SACK_PERM=1 WS=64	
3 0.000509	08:25:08.891381	0.000073 Micro-St_e2:48:		58195 AxisComm_9c:6b:e7 172.25.201.100	554 TCP	54		54 [ACK] Seq=1 Ack=			
4 0.000749 5 0.001008	08:25:08.891621 08:25:08.891880	0.000240 Nicro-St_e2:48:1 0.000259 AxisComm 9c:6b;		58195 AxisComm_9c:6b:e7 172.25.201.100	554 RTSP	208		rtsp://1/2.25.201.1		nedia/media.amp RTSP/1.0	
6 0.003493	08:25:08.894365	0.002485 AxisComm 9c:6b:	Wireshark - Enabled Protocols						×		
7 0.003672	08:25:08.894544	0.000179 Micro-St_e2:48:								edia/media.amp RTSP/1.0	
8 0.053028	08:25:08.943900	0.049356 AxisComm_9c:6b:	Search:			Every	where	v in any protocol	~	-31360 Len=0	
9 0.590816 0 0.591787	08:25:09.481688 08:25:09.482659	0.537788 AxisComm_9c:6b: 0.000971 Micro-St e2:48:	Protocol	Description					^	a/media.amp/stream=0 RTSP/1.0	
1 0.592311	08:25:09.483183	0.000524 AxisComm 9c:6b:	RTAC Serial	RTAC Serial						h=32448 Len=0	
2 0.595993	08:25:09.486865	0.003682 AxisComm 9c:6b:	RTCDC	WebRTC Datachannel Protocol							
3 0.596709	08:25:09.487581	0.000716 Micro-St_e2:48:	RTcfg	RTcfg						dia/media.amp RTSP/1.0	
4 0.599456	08:25:09.490328	0.002747 AxisComm_9c:6b:	RTCMEM	ITS message - RTCMEM							
5 0.599737 5 0.643022	08:25:09.490609 08:25:09.533894	0.000281 Nicro-St_e2:48: 0.043285 AxisComm 9c:6b:	V RTCP	Real-time Transport Control Protocol RTCP over TURN						/media.amp RTSP/1.0 in=34560 Len=0	
7 0.917644	08:25:09.808516	0.274622 AxisCom 9c:6b:	rtcp_udp	RTCP over UDP						LH=34360 Len=0	
8 0.922449	08:25:09.813321	0.004805 AxisComm 9c:6b:	V RTITCP	RTI TCP Transport Protocol						9, Seq=32010, Time=1036399961 SEI	
9 0.923108	08:25:09.813980	0.000659 AxisComm_9c:6b:	rtitcp	RTI TCP Layer						9, Seq=32011, Time=1036399961 SPS	
0.923409	08:25:09.814281	0.000301 AxisComm_9c:6b:	RTLS	Real Time Location System						9, Seq=32012, Time=1036399961 PPS	
1 0.935601	08:25:09.826473	0.012192 AxisComm_9c:6b:	RTmac RTMP	Real-Time Media Access Control Routing Table Maintenance Protocol						9, Seq=32013, Time=1036399961 FU-A Start:IDR-Slid	e
				Real Time Messaging Protocol							
15: 439 byte	es on wire (3512 bits	s), 439 bytes captured (35	rtmpt_tcp	RTMPT over TCP							
		30:9c:23:e2:48:b5), Dst: A	rtnetlink	Linux rtnetlink (route netlink) protocol							
		.25.201.50, Dst: 172.25.20 rt: 58195, Dst Port: 554, 1	✓ RTP Ttp_classicstun	Real-Time Transport Protocol RTP over CLASSICSTUN							
Time Streamin		C. 30133, DSC POLC. 334, .	rtp_rtsp	RTP over RTSP							
			rtp_stun	RTP over TURN							
			rtp_udp	RTP over UDP					100		
			RTP compression (RFC25)								
			RTP Event RTP-ED137	RFC 2833 RTP Event							
			RIP-ED137	Real-Time Transport Protocol ED137 Extension: RFC 4695/6295 RTP-MIDI							
			RIPproxy	Sippy RTPproxy Protocol							
			✓ ✓ RTPS	Real-Time Publish-Subscribe Wire Protocol					~		
			Diabling a protocol prevents higher layer	protocols from being displayed							
			Enable All Disable All	Invert							
							OK	Cancel	Help		

Network bandwidth anlysis

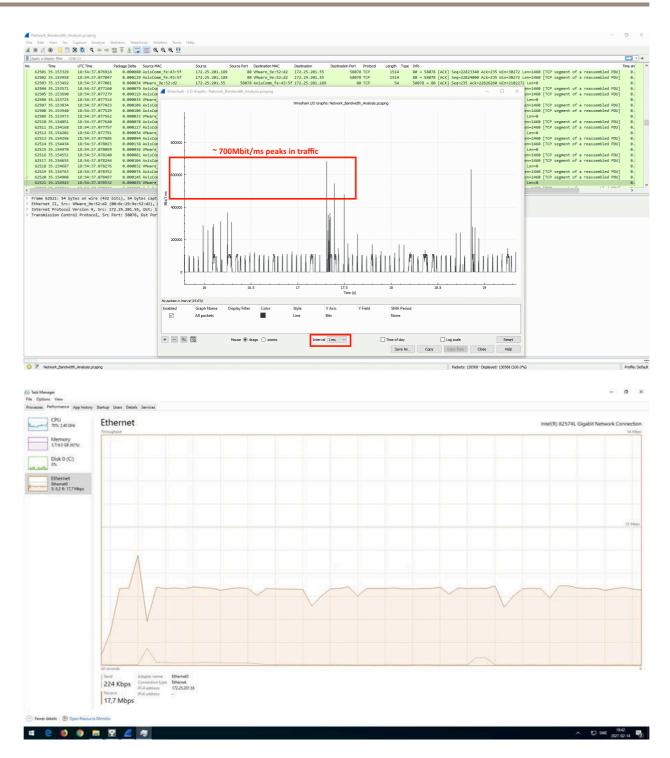
Analyzing the amount of network bandwidth between network devices can be used to identify network bottlenecks and overuse of the existing network infrastructure. Another aspect of this analysis is to identify network peaks (i.e. moments where exceptionally large amounts of network traffic is sent), which is a common behavior due to the low-size P-Frames and larger I-Frames in H.264 video streaming.

The following screenshots illustrate how to identify the amount of network traffic sent from one network device to another. This information can then be cross-referenced against other measuring tools, such as Windows Task Manager.

Troubleshooting & maintenance



Troubleshooting & maintenance



Useful information can also be found in the capture statistics of the network trace file.

Troubleshooting & maintenance

2. CTC Ime al: 541-73, CPC 49 al: 541-74, CP	Reoked Addresses Protocol Hierarchy Conversions Endpoints Packet Lengths UO Graphs Service Response Time DHCF (BOOTD) Statistics OHC-ROC Program 20West AACP BACAR BACAR Collected DHS Rew Graph HAUTI-D HerFEDDS HAUTI-D HerFEDDS HITTP Sametime UTD Stream Graphs UDP Multicas Streams F5 IP-4 Statistics	.25.201.189 B0 When .25.201.55 58076 Ad:15 .25.201.55 58076 Ad:15 .25.201.105 58076 Ad:16 .25.201.105 58076 Ad:16 .25.201.105 58077 Ad:16 .25.201.105 80 When .25.201.105 80 Wh	stant MAC Destination Destination reg_eff:221 27,25,201,25 5 reg_eff:221 27,25,201,25 5 5 Game_ff:e315 17,25,201,201,25 5 5 5 Game_ff:e315 17,25,201,201,201 5 5 5 5 Game_ff:e315 17,25,201,201,201 5	when Port Protect Length T S0073 TCP 1554 S0073 TCP 15154 S0073 TCP 15154 S0073 TCP 15154 S0073 TCP 15154 S0073 TCP 15154 S0077 TCP 15154 S00777 TCP 15154 S00777 TCP 15154 S00777 TCP	B0 − 58077 [AC] 5qc=228.240 Ack-235 M B0 − 58077 [AC] 5qc=228.240 Ack-235 M 50778 − 80 [AC] 5qc=228.240 Ack-235 M B0 − 58077 [AC] 5qc=225 Ack-225500 M B0 − 58077 [AC] 5qc=225 Ack-225500 M B0 − 58077 [AC] 5qc=225 Ack-235500 Ack-235 M B0 − 58077 [AC] 5qc=255 Ack-23570 Ack-235 M B0 − 58077 [AC] 5qc=255 Ack-23570 Ack-235 M B0 − 58077 [AC] 5qc=255 Ack-24570 M B0 − 5807 [AC] 5qc=255 Ack-2570 M B0 − 5807 [AC] 5qc	LinsW222 LensAd0 [TCP segment of a reassembled missW21 LensAd0 [TCP segment of a reassembled missW21 LensAd0 [TCP segment of a reassembled missW22 LensAd0 [TCP seg	PDU] 6 PD
8:54:27,0708 8:54:27,0778 8:54:27,0778 8:54:27,0778 8:54:27,0778 8:54:27,0773 8:54:27,0773 8:54:27,0773 8:54:27,0773 8:54:27,0778 8:54:27,0778 8:54:27,0778 8:54:27,0788 8:552,0788 8:552,0788 8:552,0788 8:552,0788 8:552,0788	Endpoints Packel Lengths Hockel Lengths Service Response Time DUCP (BOOTD) Statistics ONC-NPC Poogram Service Service Collectd Collectd Collectd Collectd PMS BACcent Response HOTS Hock Time HOTS HOTS HOTS Packet Collectd Collect	125:201.189 B0 When -25:201.390 B0 When -25:201.390 B0 When -25:201.391 B0 When -25:201.395 B0 When -25:201.495 B0 When -25:201.495 B0 When	$\label{eq:response} \begin{split} respective (respective) (respecti$	50073 TCP 1514 80 TCP 54 80 TCP 54 50073 TCP 1514 50073 TCP 1514 50073 TCP 1514 50073 TCP 1514 50073 TCP 1514 80 TCP 54 80 TCP 54 80 TCP 54 50073 TCP 1514 50073 TCP 1514 5	B0 = 58077 [AC] Seq=228.2340 Ack-235 B0 = 58077 [AC] Seq=228.240 Ack-235.45 S071 = 16 [AC] Seq=228.240 Ack-235.45 S071 = 16 [AC] Seq=227.45 Ack-2325.45 S071 = 16 [AC] Seq=227.85 Ack-2325.45 S071 = 80 [AC] Seq=227.85 Ack-2325.46 S071 = 80 [AC] Seq=227.85 Ack-2325.46 S071 = 80 [AC] Seq=227.85 Ack-233.940 S071 = 80 [AC] Seq=227.85 Ack-233.940 S073 = 80 [AC] Seq=227.85 Ack-233.940 S074 = 80 [AC] Seq=227.81 Ack-235.940 S073 = 80 [AC] Seq=227.84 Ack-235.940 S074 = 80	Inin98222 Lem-1460 [TCP segment of a reassembled Inin98222 Lem-1460 [TCP segment of a reassembled Inin98272 Lem-1460 [TCP segment of a reassembled Inin9827 Lem-1460 [TCP segment of a reassembled	PDU] 6 PD
8:54:27,0778 8:54:27,0771 8:54:27,0771 8:54:27,0773 8:54:27,0773 8:54:27,0773 8:54:27,0775 8:54:27,0775 8:54:27,0778 8:54:27,0778 8:54:27,0778 8:54:27,0788 8:54:27,0788 8:54:27,0788 8:54:27,0788 8:54:27,0788 8:54:27,0788 8:54:27,0788 8:54:27,0788 8:54:27,0788 8:54:27,0788 8:54:27,0788 8:54:27,0784 8:	Packet Langths UO Graphs Service Response Time DHCP (BODTP) Statistics ONCK-RPC Programs 29West ANCP ANCP Collected DNS Revo fragh Collected DNS Revo fragh HUTP HEFELDS HUTP Collected DNS TOP Stream Graphs UDP Multicast Streams FS PM-Statistics	-25-201.55 59076 A.13 -25-201.35 98076 A.13 -25-201.35 98 00 Wen -25-201.35 98 00 Wen -25-201.35 98 00 Wen -25-201.35 98 00 Wen -25-201.35 98076 A.13 -25-201.35 98076 A.13 -25-201.55 98076 A.13 -25	$\begin{split} & Com_{m}(+3) \le 17.2, 3.2, 3.21, 109 \\ & cm_{m}(+3) \le 17.2, 3.2, 3.2, 3.2, 3.2, 3.2, 3.2, 3.2, 3$	00 TCP 54 50078 TCP 1514 60 TCP 54 50078 TCP 1514	5077 = 00 [LCC] 5eep25 Ack-2232240 M 80 = 5407 [LCC] 5eep2220273 Ack-233 M 80 = 5407 [LCC] 5eep220273 Ack-233 M 80 = 5407 [LCC] 5eep220273 Ack-233 M 80 = 5407 [LCC] 5eep230240 Ack-233 M 80 = 5407 [LCC] 5eep230240 Ack-233 M 80 = 5407 [LCC] 5eep23040 Ack-233 M 80 = 5407 [LCC] 5eep230400 Ack-233 M	inimized 22 Lem-06 inimized 22 Lem-06 inimized Lem-160 [TCP segment of a reassembled inimized Lem-160 [TCP segment of a rea	PDU] 0
8:54:37, 0772 8:54:37, 0773 8:54:37, 0773 8:54:37, 0773 8:54:37, 0775 8:54:37, 0775 8:54:37, 0775 8:54:37, 0776 8:54:37, 0776 8:54:37, 0778 8:54:37, 0780 8:54:37, 0780 8:54:37, 0782 8:54:37, 0782 8:54:37, 0783 8:54:37, 0783 8:54:37, 0783 8:54:37, 0783 8:54:37, 0784 8:54:37, 0784 8:54:3	UO Grapha Service Response Time DHCP (80070) Statistics ONC-RPC Polyarem Service Service Calledd ANCP Hew Graph HAUT-IP Hew Graph HAUT-IP HEFEDS HITTP Sametime TCP Stream Graphs UDP Multicas Streams FS PM-Statistics	.25,201.189 B0 When .25,201.55 \$9878 Acti .25,201.55 \$9878 Acti .25,201.189 B0 When .25,201.189 B0 When .25,201.189 B0 When .25,201.189 B0 When .25,201.189 B0 When .25,201.189 B0 When .25,201.189 B0 When .25,201.55 \$9878 Acti .25,201.189 B0 When .25,201.55 \$9878 Acti .25,201.55 \$9878	$\label{eq:response} \begin{split} r_e & e_{12} (22, 23, 24, 213, 25, 20, 21, 36) \\ r_e & e_{12} (23, 24) & (27, 25, 20, 21, 16) \\ r_e & e_{12} (23, 24) & (27, 25, 20, 21, 53) \\ r_e & e_{12} (23, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 23, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 22, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 22, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 22, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 22, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 22, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 22, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 22, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 22, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 22, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 22, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 22, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 22, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 22, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 22, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 22, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 53) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 54) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 54) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 54) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 54) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 54) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 54) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 54) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 54) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 54) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 54) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 54) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 54) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 54) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 54) \\ r_e & (25, 24, 24) & (27, 25, 20, 21, 54) \\ r_e & (25, 24) & (27, 25, 20$	50073 TCP 1514 4 50073	80 - 58077 [AC] 5ee-2287729 Ack-235 58078 - 80 (AC] 5ee-228.7c8 Ack-235 10 80 - 58078 [AC] 5ee-228.7c8 Ack-235 10 80 - 58078 [AC] 5ee-228.7c8 Ack-235 10 500 - 807 [AC] 5ee-228.7c8 Ack-235 10 500 - 807 [AC] 5ee-238.7c8 Ack-235 10 50078 - 80 [AC] 5ee-238.7c8 Ack-235 10 80 - 58078 [AC] 5ee-238.7c8 Ack-235 10	Linol0222 Lenv1400 [TCP segment of a reassembled Linol0222 Lenv1400 [TCP segment of a reassembled Linol022 Linol1400 [TCP segment of a reassembled Linol022 Linol1400 [TCP segment of a reassembled Linol022 Linol140 [TCP	PDU] (PDU] (
8:54:37,0774 8:54:37,0775 8:54:37,0775 8:54:37,0775 8:54:37,0776 8:54:37,0776 8:54:37,0776 8:54:37,0778 8:54:37,0788 8:54:37,0788 8:54:37,0782 8:54:37,0783 8:54:37,0783 8:54:37,0784 8:55:2142 8:55	DHCP (BOOTP) Statistics ONC-RPC Programs 29West ANCP Calledd ANCP Flow Graph HAIT-IP HEFEDS HITTP Sametime TTP2 Sametime TTP2 Sametime TTP2 Sametime TTP2 Sametime HTTP PH-Statistics		$\label{eq:response} \begin{split} re_{re}^{-} er(s) 21, 23, 24, 23, 24, 23, 55, 24, 24, 25, 25, 24, 24, 25, 25, 24, 24, 25, 24, 24, 25, 24, 24, 24, 24, 24, 24, 24, 24, 24, 24$	500781707 1514 152 801707 54 801707 54 500781707 1514 500781707 1514 500781707 1514 801707 54 801707 54 80070 75 4 80070 75 4 80070 75 4 80070 75 4 80070 75 4 80070 75 1514 80070 7514 80070 7515 80070 7515 80	B0 − 58077 [AC] 5qc=22873B Ack-235 B0 − 58077 [AC] 5qc=228840 Ack-235 58071 − 80 [AC] 5qc=238 Ack-2383 Jb 58071 − 80 [AC] 5qc=238 Ack-2383 Jb 58071 − 80 [AC] 5qc=238 Ack-2353 Jb 58071 − 80 [AC] 5qc=238 Ack-2353 Jb 80 − 58077 [AC] 5qc=238 Ack-2353 Jb 80 − 58078 [AC] 5qc=238 Ack-235 Jb 80 − 58078 [A	in-98272 Len-3460 [TP segment of a reassembled in-28272 Len-3460 [TP segment of a reassembled in-28272 Len-3460 [TP segment of a reassembled in-28272 Len-3460 [TP segment of a reassembled in-28222 Len-3460 [TP segment of a reassembled	PDU] 6 PDU] 6
18:54:37,0775 8:54:37,0776 8:54:37,0777 8:54:37,0777 8:54:37,0778 8:54:37,0778 8:54:37,0788 8:54:37,0788 8:54:37,0782 8:54:37,0782 8:54:37,0784 8:55:42,0784 8	ONC-BPC Programs 28Vect ANCP BAChet Collected DNS Flow Graph HAITT-P HAITT-P HAITT-P HAITT-P HTTP Collected USP Multicas Streams 55 PA-Statistics	.2.2.01.189 B0 When .2.3.201.29 B0 When .2.3.201.59 B0 When .2.3.201.55 S0 When .2.3.201.55 S0 When .2.3.201.55 S0 When .2.3.201.55 <td< td=""><td>$\label{eq:response} \begin{split} re_e ers (21.2, 23$</td><td>S8075 TCP 1514 80 TCP 544 S8075 TCP 1514 S8075 TCP 544 S8075 TCP 544 S8075 TCP 1514 S8075 TCP 544 S8075 TCP 544 S8075 TCP 1514 S8075 TCP 544</td><td>BB = 5807T [AC] 5qc=228364b Ack-235 b 5807T = 10 (AC] 5qc=25 Ack-232310 b BB = 5807T [AC] 5qc=25 Ack-232310 b Ack-350 b 5807T = 10 (AC] 5qc=228310 Ack-235 b 5807T = 10 (AC] 5qc=228340 Ack-235 b BB = 5807T [AC] 5qc=228460 Ack-235 b BB = 5807T [AC] 5qc=228460 Ack-235 b BB = 5807T [AC] 5qc=228460 Ack-235 b BB = 5807T [AC] 5qc=2248460 Ack-235 b BB = 5807T [AC] 5qc=248460 Ack-235</td><td>Lin-NB272 Lem-M400 [TCP segment of a reassembled Lin-NB272 Lem-M400 [TCP segment of a reassembled</td><td>PDU] 6 PDU] 6</td></td<>	$\label{eq:response} \begin{split} re_e ers (21.2, 23$	S8075 TCP 1514 80 TCP 544 S8075 TCP 1514 S8075 TCP 544 S8075 TCP 544 S8075 TCP 1514 S8075 TCP 544 S8075 TCP 544 S8075 TCP 1514 S8075 TCP 544	BB = 5807T [AC] 5qc=228364b Ack-235 b 5807T = 10 (AC] 5qc=25 Ack-232310 b BB = 5807T [AC] 5qc=25 Ack-232310 b Ack-350 b 5807T = 10 (AC] 5qc=228310 Ack-235 b 5807T = 10 (AC] 5qc=228340 Ack-235 b BB = 5807T [AC] 5qc=228460 Ack-235 b BB = 5807T [AC] 5qc=228460 Ack-235 b BB = 5807T [AC] 5qc=228460 Ack-235 b BB = 5807T [AC] 5qc=2248460 Ack-235 b BB = 5807T [AC] 5qc=248460 Ack-235	Lin-NB272 Lem-M400 [TCP segment of a reassembled Lin-NB272 Lem-M400 [TCP segment of a reassembled	PDU] 6 PDU] 6
18:54:37,0776 18:54:37,0777 18:54:37,0777 18:54:37,0778 18:54:37,0780 18:54:37,0780 18:54:37,0780 18:54:37,0782 18:54:37,0782 18:54:37,0782 18:54:37,0783 18:54:37,0783 18:54:37,0785 - on wire (43: are-ge:52:1d2 - soin 4,5rc;	29Wet ANCP ANCP Collected DNS Rev Graph HATT-P HATTEP HATTEP HATTEP USP Multicast Streams F5 PA-Statistics	. 25.201.189 08 0 Mea. . 25.201.189 08 0 Mea. . 25.201.55 59078 A131 . 25.201.55 59078 A131 . 25.201.59 08 0 Mea. . 25.201.39 08 0 Mea. . 25.201.39 08 0 Mea. . 25.201.189 08 0 Mea. . 25.201.185 88078 A131 . 25.201.55 58078 A131 . 25.201	$\label{eq:response} \begin{split} & re_{re}^{2}(e_{1}^{2}2,z_{2}^{2},z_{2}^{2}1,z_{2}^{2},z_{2}^{2}1,z_{2}^{2},z_{2}^{2}1,z_{2}^{2},z_{2}^{2}1,z_{2}^{2},z_{2}^{2}1,z_{2}^{2},z_{2}^{2}1,z$	S8075 TCP 1514 S8075 TCP 1514 807 TCP 1514 S8075 TCP 1514 8076 TCP 1514 8077 TCP 1514 8077 TCP 1514 8077 TCP 1514 8070 TCP 1514 8070 TCP 1514 8070 TCP 1514 8070 TCP 1514 5070 TCP 1514	B0 - 58077 [AC] 5q-22832100 Ack-235 10 B0 - 58077 [AC] 5q-2283250 Ack-235 10 50778 - 80 [AC] 5q-2283500 Ack-235 10 80 - 58078 [AC] 5q-2235400 Ack-235 10 80 - 58078 [AC] 5q-2254000 Ack-235 10 80 - 58078 [AC] 5q-2245400 Ack-235 10 80 - 58078 [AC] 5q-2246400 Ack-235 10 80 - 58078 [AC] 5q-246400 Ack-235 10 80 - 58078 [AC] 5q-24	Idi-B022 Len-140 [TC regent of a reaseable din-B022 Len-040 [TC segment of a reaseable din-B022 Len-0400 [TC segment of a reaseable din-B022 Len-0400 [TC segment of a reaseable din-B022 Len-0400 [TC segment of a reaseable din-B022] Len-0400 [TC segment of a reaseable]	PDU] PDU] PDU] PDU] PDU] PDU]
8:54:37.0777 8:54:37.0780 8:54:37.0780 8:54:37.0780 8:54:37.0781 8:54:37.0782 8:54:37.0782 8:54:37.0782 8:54:37.0784 8:54:37.0784 8:54:37.0784 9:54:37.0784 9:54:37.0785 9:54:37.0785 9:54:37.0785 9:54:37.0785 9:54:37.0785 9:54:37.0785 9:54:37.0785 9:54:37.0785 9:54:37.0785 9:54:37.0785 9:54:37.0785 9:54:37.0785 9:54:37.0785 9:54:37.0785 9:54:37.0785 9:54:37.0785 9:55:	AACC Collected Collected DNS Few Graph NAUTEP HEFEDS HITTP Sametime TCP Stram Graphs UDP Multices Streams 55 PK-Statistics	-25.201.55 59078 Ad31 -25.201.50 80 When -25.201.80 80 When -25.201.80 80 When -25.201.80 80 When -25.201.80 80 When -25.201.80 80 When -25.201.85 59078 Ad31 -25.201.85 59078 Ad31 -25.201.85 59078 Ad31 -25.201.55 59078 A	Comm [fc:43:5f 172.25.201.189 rc=9e552:d2 172.25.201.55 rc=9e552:d2 172.25.201.55 rc=9e552:d2 172.25.201.55 rc=9e552:d2 172.25.201.55 rc=9e552:d2 172.25.201.189 rc=9e552:d2 172.25.201.189 rc=9e552:d2 172.25.201.185 rc=9e552:d2 172.25.201.55 rc=9e552:d2 172.25.201.55	80 TCP 54 58075 TCP 1514 80 TCP 1514 80 TCP 54 58075 TCP 1514 80 TCP 54 58075 TCP 1514 80 TCP 54 58075 TCP 1514 58075 TCP 1514 58075 TCP 54 58075 TCP 54	50070 + 00 (ACL) 5emp-235 Ack+22835020 M 80 + 55077 (ACL) 5emp-2355020 Ack+235 M 80 + 55077 (ACL) 5emp-235502 Ack+235 M 80 + 55077 (ACL) 5emp-2357460 Ack+235 M 80 + 55077 (ACL) 5emp-23640560 Ack+235 M	III-22022 Len-0 III-22022 Len-0460 [TCP segment of a reassembled III-30222 Len-0460 [TCP segment of a reassembled III-302022 Len-0460 [TCP segment of a reassembled III-302022 Len-0460 [TCP segment of a reassembled IIII-302022 Len-0460 [TCP segment of a reassembled	PDU] PDU] PDU] PDU] PDU] PDU]
18:54:37.0780 18:54:37.0780 18:54:37.0781 18:54:37.0782 18:54:37.0782 18:54:37.0783 18:54:37.0784 18:54:37.0785 19:55:37.0785 19:55:	Cellectd DNS Flow Graph HART-P HHTDD HHTDD VETT2 Sametime UDP Multicas Streams FS PM-Statistics	. 25:201.189 80 What .52:201.289 80 What .52:201.55 80 80 What .52:201.25 80 80 What .5	re_9ei52:d2 172.25.201.55 com_fei45:f2 172.25.201.55 com_fei45:f2 172.25.201.55 com_fei45:f5 172.25.201.189 re_9ei52:d2 172.25.201.55 com_fei43:f5 172.25.201.55 com_fei43:f5 172.25.201.55 com_fei43:f5 172.25.201.189	58078 TCP 1514 80 TCP 54 58078 TCP 1514 58078 TCP 1514 80 TCP 554 58078 TCP 1514 58078 TCP 1514 58078 TCP 1514 80 TCP 554	80 + 58078 [ACC] Seq=22835628 ACx=25 M 80 + 58078 [ACK] Seq=22836480 ACx=25 M 80 + 58078 [ACK] Seq=225 ACx=225 M 80 + 58078 [ACK] Seq=225 ACx=22537940 ACx=25 M 80 + 58078 [ACK] Seq=22839400 ACx=25 M 80 + 58078 [ACK] Seq=2284940 ACx=25 M 80 + 58078 [ACK] Seq=22840660 ACx=25 M 80 + 58078 [ACK] Seq=22840660 ACx=25 M	Hin-3022 Len-1460 [TC segment of a reassembled in-210222 Len-466 [TC segment of a reassembled in-2102222 Len-46 ini-3022 Len-1466 [TC segment of a reassembled ini-3022 Len-1466 [TC segment of a reassembled ini-30222 Len-466 [TC segment of a reassembled ini-30222 Len-466 [TC segment of a reassembled	PDU] PDU] PDU] PDU] PDU]
<pre>18:54:37.0780 18:54:37.0781 18:54:37.0782 18:54:37.0782 18:54:37.0783 18:54:37.0784 18:54:37.0784 18:54:37.0785 10:0:0:0:0:0:0 10:0:0:0 10:0:0:0 10:0:0:0 10:0:0:0 10:0:0:0 10:0:0:0 10:0:0:0 10:</pre>	DNS Flow Graph Hart-IP HAFEEDS HTTP HTTP CS Secare Graphs UDP Multiciae Streams FS PM-Statistics	-25.201.55 50078 A131 -25.201.309 00 VMem -25.201.109 00 VMem -25.201.109 00 VMem -25.201.59 50078 A131 -25.201.109 00 VMem -25.201.59 50078 A231 -25.201.55 50078 A231 -25.201.	Comm. fe:43:57 172.25.201.189 re_9e:52:02 172.25.201.55 re_9e:52:02 172.25.201.55 Comm_fe:43:57 172.25.201.55 Comm_fe:43:57 172.25.201.55 re_9e:52:02 172.25.201.55 Comm_fe:43:55 172.25.201.189	80 TCP 54 58078 TCP 1514 58078 TCP 1514 80 TCP 54 58078 TCP 1514 58078 TCP 1514 800 TCP 54	56078 - 80 [ACK] 5cq-235 Ack=22837940 80 + 58078 [ACK] 5cq-22837940 Ack=235 W 80 + 58078 [ACK] 5cq-22839400 Ack=235 W 56078 - 80 [ACK] 5cq-2283400 Ack=2240860 80 + 58078 [ACK] 5cq-22840860 Ack=235 W 80 + 58078 [ACK] 5cq-22840860 Ack=235 W	<pre>lin=210227 Len=0 in=3027 Len=1460 [TCP segment of a reassembled in=3027 Len=1460 [TCP segment of a reassembled in=2102272 Len=0 in=3027 Len=1460 [TCP segment of a reassembled in=3027 Len=1460 [TCP segment of a reassembled</pre>	PDU] PDU] PDU] PDU]
18:54:37.0782 18:54:37.0782 18:54:37.0783 18:54:37.0784 18:54:37.0785 19:55:37.0785 19:52:42 19:52:	Flow Graph HatT=P HPEEDS HTTP TTP2 Sametime TCP Stream Graphs UDP Multicas Streams FS FS PM-Statitics	-25.201.189 08 UMen -25.201.189 08 UMen -25.201.55 98078 Acid -25.201.55 98078 Acid -25.201.189 08 UMen -25.201.189 08 UMen -25.201.55 58078 Acid -25.201.55 58078 Acid -25.201.	re_9e:52:d2 172.25.201.55 re_9e:52:d2 172.25.201.55 Comm_fe:43:5f 172.25.201.189 re_9e:52:d2 172.25.201.189 re_9e:52:d2 172.25.201.55 form_fe:43:5f 172.25.201.58	58078 TCP 1514 80 TCP 54 58078 TCP 1514 58078 TCP 1514 80 TCP 54	80 + 58078 [ACK] Seq=22839400 Ack=235 W 58078 + 80 [ACK] Seq=225 Ack=22840860 80 + 58078 [ACK] Seq=22840860 Ack=235 W 80 + 58078 [ACK] Seq=22842320 Ack=235 W	<pre>lin=30272 Len=1460 [TCP segment of a reassembled lin=2102272 Len=0 lin=30272 Len=1460 [TCP segment of a reassembled lin=30272 Len=1460 [TCP segment of a reassembled</pre>	PDU] PDU] PDU]
8:54:37.0782 8:54:37.0783 8:54:37.0784 8:54:37.0785 0 on wire (43: ware_9e:52:d2 sion 4, Src:	HART-P HIPEEDS HTTP HTTP2 Sametime TCP Stream Graphs UDP Multisast Streams F5 F5 F94 Statistics	.25.201.55 S0978 Acti .25.201.189 80 VHwa .25.201.189 80 VHwa .25.201.55 S0978 Acti nterface \Device\VPP_{300C} Sf (acics#rfer43:5f) : 22843780, Len: 0	Com_fe:43:5f 172.25.201.189 re_de:52:d2 172.25.201.55 re_de:52:d2 172.25.201.55 Com_fe:43:5f 172.25.201.189	80 TCP 54 58078 TCP 1514 58078 TCP 1514 80 TCP 54 58078 TCP 54	58078 → 80 [ACK] Seq=235 Ack=22840860 W 80 → 58078 [ACK] Seq=22840860 Ack=235 W 80 → 58078 [ACK] Seq=22842320 Ack=235 W	Min=2102272 Len=0 Min=30272 Len=1460 [TCP segment of a reassembled Min=30272 Len=1460 [TCP segment of a reassembled	PDU] PDU]
8:54:37.0784 8:54:37.0785 0 on wire (43: mare_9e:52:d2 rsion 4, Src:	HTTP HTTP2 Sametime TCP Stream Graphs UDP Multicast Streams F5 IPv4 Statistics	.25.201.189 80 VMwa .25.201.55 50078 Avis nterface \Device\UPF_(300Cf 5f (ac:cc:8e:fe:43:5f) : 22843780, Len: 0	re_9e:52:d2 172.25.201.55 Comm_fe:43:5f 172.25.201.189	58078 TCP 1514 80 TCP 54	80 + 58078 [ACK] Seq=22842320 Ack=235 W	in=30272 Len=1460 [TCP segment of a reassembled	PDU] PDU]
on wire (43: mare_9e:52:d2	HTTP2 Sametime TCP Stream Graphs UDP Multicast Streams F5 IPv4 Statistics	<pre>.25.201.55 58078 Axis(nterface \Device\WPF_{300CF}) 5f (ac:cc:8e:fe:43:5f) :: 22843780, Len: 0 ;</pre>	Comm_fe:43:5f 172.25.201.189		5077 - 80 [ACL] 544-235 ACK-2384778 W	219-219272 Len-0	
are_9e:52:d2 sion 4, Src:	Sametime TCP Stream Graphs UDP Multicast Streams F5 IPv4 Statistics	<pre>> 5f (ac:cc:8e:fe:43:5f) :: 22843780, Len: 0</pre>	7409-C30D-4511-A904-684AF9635208).	id 0			
are_9e:52:d2 sion 4, Src:	UDP Multicast Streams FS IPv4 Statistics	<pre>> 5f (ac:cc:8e:fe:43:5f) :: 22843780, Len: 0</pre>	N9 (30 - 11 - 1994 - 04N 303200)	10 6			
	F5 IPv4 Statistics	*					
	IPv4 Statistics						
		,					
	IPPO Statistics						
nalysis.pcapng					Packets: 130568 · Displayed: 13	30568 (100.0%)	Pr
8:54:37.076918 8:54:37.077047 8:54:37.077081 8:54:37.077160 8:54:37.077279 8:54:37.077314	0.000080 Ax1sComm_fe:43:5f 0.000129 Ax1sComm_fe:43:5f 0.00034 Whene Ge:52:d2 Wireshark - Capture File Properties - Netw Details	122, 25, 201, 189 80 Whee 122, 25, 201, 189 80 Whee 122, 25, 201, 55 58078. Act ist work_Bandwidth Analysis.pcapng C: Users Under D: Downloads Wetwork _5 1996 b-x080cs8fs.ddfb.ceffb0.ceffb0.cf	re, 9e:52:42 172.25.201.55 come: fe:43:5f 172.25.201.15 come: fe:43:5f 172.25.201.189 andwidth_Anelysis.pcapng en:31:40=4545/60/20128285ad beb/700	800767070200 88574 500731702 1514 20071702 1514 2007029 54	80 → 58078 [ACK] Seq=22823340 Ack=235 W 80 → 58078 [ACK] Seq=22824800 Ack=235 W	Un-19222 Len-1460 [TO segment of a reassembled in-19222 Len-1460 [TO segment of a reassembled model (TO segment of a reassembled) not provide the sequence of a reassembled in-100 [TO segment of a reassembled] in-200 [TO segment of a reassembled] in-200 [TO segment of a reassembled] id-200 [TO segment of a reassembled]	PDU] PDU] PDU] PDU] PDU] PDU] PDU] PDU]
8:54:37,078059 8:54:37,078149 8:54:37,078244 8:54:37,078244 8:54:37,078252 8:54:37,078352 8:54:37,078352 8:54:37,078352 9:54:37,078457 8:55:37,078457 8:55:3	Time Time model: lang model: tappent: Capture Androne: Mardinare: Statistics Deres PF # 552500 Statistics Statistics Statistics Statistics	2021-02-14 99-54-01 2021-02-14 99-58-07 00-01-09 Intel(R) Yacol(R) (CPU E9-45 @ 2.4-00-4c 46-84 Windows ID, kuld 18/83 Dumpcag (Windows ID, kuld 18/83) Dumpca	756965a) Caphare filter host 172.25,201.189	Link hans Ethernet	Eadert size limi 65530 bytes Morked	1460 [TO segment of a reasonabled n=0 1460 [TO segment of a reasonabled 1460 [TO segment of a reasonabled n=0 n=0 n=0 n=0 n=0 n=0 n=0 n=0 n=0 n=0	PDU] PDU]
8:54:37.078059 8:54:37.078240 8:54:37.078244 8:54:37.078246 8:54:37.078252 8:54:37.078552 8:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078555 9:55:37.0785555 9:55:37.07855555 9:55:37.0785555555555555555555555	Lat poket: Essect: Capture Andrare: Ci: Ci: Andrakes DeviceWer (20007409-200-9511- A09-6409/951200) Statistice Maaureman	2021-02-14 19:55:07 00:01:05 Intel(R) Xeon(R) CPU E5645 (b 2.40GHz 64-bit Windows Jo, build 18763 Dumpcop (Winstherh) 2.6.5 (v2.6.5-0-g1	F766965a)	Ethernet	Eadot size limit 65330 bytes Marked —	1460 [TCP segment of a reassembled n=0 1460 [TCP segment of a reassembled	PDU] PDU]
8:54:37.078059 8:54:37.078240 8:54:37.078244 8:54:37.078246 8:54:37.078252 8:54:37.078552 8:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078555 9:55:37.0785555 9:55:37.07855555 9:55:37.0785555555555555555555555	Lat podet: Bisnoch: Capture Hardnare: OS: Agoleston: Taterface Dencepter Dencepter Dencepter Statistics Statistics Batastics Management Pacate	2012-02-14 (19:58:07 00:11:09 10:10:09 10:00(10) Norv(0) (21) E54:5 (0:2.63:0 6-64) Windows (0: 0, build 1353) Dumps (0) Windows (0: 0, build 1353) Dumps (0) Windows (0: 0, build 1353) Dumps (0: 0	756965a) Gastare_Bite: hest 172.25.201.189 100568 (1 65.793 (1 9194	Ethernet	65333 bytes <u>Marked</u> 	1460 [TCP segment of a reassembled n=0 1460 [TCP segment of a reassembled	PDU] PDU]
8:54:37.078059 8:54:37.078240 8:54:37.078244 8:54:37.078246 8:54:37.078252 8:54:37.078552 8:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078555 9:55:37.0785555 9:55:37.07855555 9:55:37.0785555555555555555555555	Lat podet: Based: Capture Nerdane: 05: 06: Apolextor: Deres VP Sectors: Deres VP Sectors: Sectors: Sectors: Sectors: Pades Pades	2012-02-14-05-507 00010-05 Intel(N) Xeon(N) CPU ESI45 @ 2.400Hz 6445 Windows 10, bald 1353 Damparay (Windows 10, bald 1353 Damparay (Windows 10, bald 1353 Damparay (Windows 10, bald 1353 Damparay (Windows 10, bald 1353 0, 0.0%) Catchard 1054 1055 1054 1054 1054 1054 1054 1055	766965a) Cacture Effect Instel 172.25.201.189 Disclared 130568 (1 65.793 1984,5 0 1994,5 1994,5 1	Ethernet	65535 bytes Marked	1460 [TCP segment of a reassembled n=0 1460 [TCP segment of a reassembled	PDU] PDU]
8:54:37.078059 8:54:37.078240 8:54:37.078244 8:54:37.078246 8:54:37.078252 8:54:37.078552 8:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:54:37.078532 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078545 9:55:37.078555 9:55:37.0785555 9:55:37.07855555 9:55:37.0785555555555555555555555	Lat podet: Based: Based: Verdame: 05: Ascharter: 06: 06: 06: 06: 06: 06: 06: 06: 06: 06	2012-07-14 95:5:07 0010-05 Intel(R) Yaco(R) (CPL ES45 @ 2.4:03+6 4-841 Windows ID, kuld 1353 Dumpces (Windows ID, kuld 135	766965a) Gashar: filter hott 172: 25: 2011 189 Usslaved 130568 (1 130568 (1 130568 (1 130568 (1) 13056 (1) 13056 (1) 13056 (1) 13056 (1)	Ethernet	65333 bytes <u>Marked</u> 	1460 [TCP segment of a reassembled n=0 1460 [TCP segment of a reassembled	PDU] PDU]
8:54:37,078059 8:54:37,078140 8:54:37,078244 8:54:37,078246 8:54:37,078276 8:54:37,078276 8:54:37,078532 8:54:37,078532 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:55:37,078544 9:55:37,0785455555555555555555555555555555555555	Last podet: Bispoci: Capture Verdaner: OS: Adoktor: Derece Verdaner: Derece Verdaner: Statisfica: Derece Verdaner: Statisfica: Maaceman Pasch: Maaceman Pasch: Average podet site, 8 Average boltes, 8	2012-02-14-05-507 00010-05 Intel(N) Xeon(N) CPU ESI45 @ 2.400Hz 6445 Windows 10, bald 1353 Damparay (Windows 10, bald 1353 Damparay (Windows 10, bald 1353 Damparay (Windows 10, bald 1353 Damparay (Windows 10, bald 1353 0, 0.0%) Catchard 1054 1055 1054 1054 1054 1054 1054 1055	766965a) Cacture Effect Instel 172.25.201.189 Disclared 130568 (1 65.793 1984,5 0 1994,5 1994,5 1	Ethernet	65333 bytes <u>Marked</u> 	1460 [TCP segment of a reassembled n=0 1460 [TCP segment of a reassembled	PDU] PDU]
8:54:37,078059 8:54:37,078140 8:54:37,078244 8:54:37,078246 8:54:37,078276 8:54:37,078276 8:54:37,078532 8:54:37,078532 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:55:37,078544 9:55:37,0785455555555555555555555555555555555555	Lat podet: Bisnoci: Capture Verdaner: OS: Apolicitar: Distribution Dis	2012-02-14-05-507 00010-05 Intel(N) Xeon(N) CPU ESI45 @ 2.400Hz 6445 Windows 10, bald 1353 Damparay (Windows 10, bald 1353 Damparay (Windows 10, bald 1353 Damparay (Windows 10, bald 1353 Damparay (Windows 10, bald 1353 0, 0.0%) Catchard 1054 1055 1054 1054 1054 1054 1054 1055	766965a) Cacture Effect Instel 172.25.201.189 Disclared 130568 (1 65.793 1984,5 0 1994,5 1994,5 1	Ethernet	65333 bytes <u>Marked</u> 	1460 [TCP segment of a reassembled n=0 1460 [TCP segment of a reassembled	PDU] PDU]
8:54:37,078059 8:54:37,078140 8:54:37,078244 8:54:37,078246 8:54:37,078276 8:54:37,078276 8:54:37,078532 8:54:37,078532 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:55:37,078544 9:55:37,0785455555555555555555555555555555555555	Lat podet: Bisnoci: Capture Verdaner: OS: Apolicitar: Distribution Dis	2012-02-14-05-507 00010-05 Intel(N) Xeon(N) CPU ESI45 @ 2.400Hz 6445 Windows 10, bald 1353 Damparay (Windows 10, bald 1353 Damparay (Windows 10, bald 1353 Damparay (Windows 10, bald 1353 Damparay (Windows 10, bald 1353 0, 0.0%) Catchard 1054 1055 1054 1054 1054 1054 1054 1055	766965a) Cacture Effect Instel 172.25.201.189 Disclared 130568 (1 65.793 1984,5 0 1994,5 1994,5 1	Ethernet	65333 bytes <u>Marked</u> 	1460 [TCP segment of a reassembled n=0 1460 [TCP segment of a reassembled	PDU] PDU]
8:54:37,078059 8:54:37,078140 8:54:37,078244 8:54:37,078246 8:54:37,078276 8:54:37,078276 8:54:37,078532 8:54:37,078532 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:54:37,078542 9:55:37,078544 9:55:37,0785455555555555555555555555555555555555	Lat podet: Bisnoci: Capture Verdaner: OS: Apolicitar: Distribution Dis	2012-02-14-05-507 00010-05 Intel(N) Xeon(N) CPU ESI45 @ 2.400Hz 6445 Windows 10, bald 1353 Damparay (Windows 10, bald 1353 Damparay (Windows 10, bald 1353 Damparay (Windows 10, bald 1353 Damparay (Windows 10, bald 1353 0, 0.0%) Catchard 1054 1055 1054 1054 1054 1054 1054 1055	766965a) Cacture Effect Instel 172.25.201.189 Disclared 130568 (1 65.793 1984,5 0 1994,5 1994,5 1	Ethernet	65333 bytes <u>Marked</u> 	1440 [TC segment of a reasonabled magnetic processing of the second seco	PDU] PDU]
	C Tome P2 St4337, 077081 8:54:37, 077081 8:54:37, 077087 8:54:37, 077087 8:54:37, 077087 8:54:37, 077229 8:54:37, 077528 8:54:37, 077528 8:54:37, 077588	Apropagy Antinica Statistics Telephony Wireles Tools Hell Construction Antinica Statistics Telephony Wireles Tools Hell Construction Antinica Statistics Antinica Statis	Lpropring Statistics Tatephony Winders Tools Help Vmr Analys Statistics Tatephony Winders Tools Help Vmr Analys Statistics Tools Help Statistics Statistics Vmr Analys Statistics Tools Norme Mill Norme Vmr Analysis Statistics Tools Statistics Statistics </td <td>Component Despinory Windows Total Help Component Component</td> <td>Capceproj Statutors <</td> <td>Component Destination Destination</td> <td>Spectry Spectry <</td>	Component Despinory Windows Total Help Component	Capceproj Statutors <	Component Destination	Spectry <

Limit network captures

During troubleshooting it's sometimes required to take Wireshark captures over a longer period of time since it's uncertain when a problem appears. As this typically requires a lot of disk space, it's recommended to limit the Wireshark capture. This can be done by using the options below and *dumpcap*, which is part of Wireshark. The default installation path for dumpcap is: C:\Program Files\Wireshark\

Troubleshooting & maintenance

Command line option	Description
-D	Find interface number.
-i	The interface number the capture should be done on.
-q	Quiet mode, eliminates displaying packet count.
-b filesize:n	The file size to create in KB per capture file.
-b duration:n	The amount of time in seconds to run per capture file.
-b files:n	The maximum number of files to create. Once the maximum number of files have been saved, the oldest file is deleted and a new empty file is created in its place.
-f	The capture filter. For more information, see this page.
-w <path>.pcap</path>	The location to write the output files. The path specified must exist.

When using the "-b files:n" option the contents of the specified traces folder would contain files with a sequence number and timestamp as follows: *mytrace_00001_20220626164602.pcap...mytrace_00024_20220627154602.pcap*.

Variable	Description
mytrace	Name of the trace.
00001	File sequence number.
2022	Year.
0626	Month/day.
164202	Hour/min/sec in 24 h format. The time indicates when the file capture was "started".

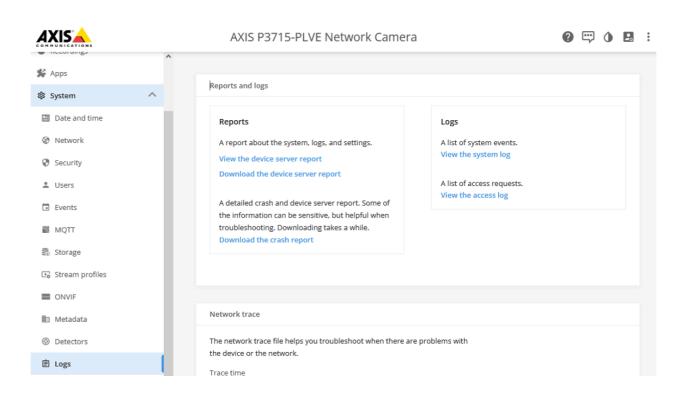
Example use cases:

Example	Output
dumpcap -i 3 -q -b duration:3600 -b files:10 -w c:\traces\mytrace.pcap	10 capture files x 1 hour long.
dumpcap -i 3 -q -b duration:3600 -b files:10 -f "host 192.168.0.90" -w c:\traces\mytrace.pcap	10 capture files x 1 hour long + a capture filter to only capture traffic for the IP "192.168.0.90".
dumpcap -i 3 -q -b filesize:200000 -b files:10 -w c:\traces\mytrace.pcap	10 capture files x 200 MB.

Server report

The server report includes actual, and to some extent historical, information about health-monitoring, general system and configuration information, as well as valuable log files. Information that will help Axis Technical Support to analyze your device. Always include a server report when contacting AXIS Support.

Troubleshooting & maintenance



The server report can be downloaded as a .zip file.

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

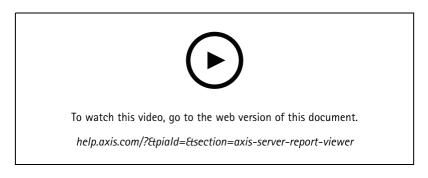
AXIS Server Report Viewer is a web based, graphical user interface that makes it possible to upload and visualize the data of the server report. The tool is developed by Axis and greatly enhances the speed and efficiency of analyzing the data in the server report.

You can access AXIS Server Report Viewer after logging in to www.axis.com with your MyAxis account.

Troubleshooting & maintenance

CISA Uplo	Dad report About SRV	Feedback						Logged in as	
	P3715-PLV 170003_B8A44F03F3B1.zi		work	. Came	era				
XIS P3715-PLVE,	Saturday Jul 23 16:59:58 2022	(UTC+02:00)		🛓 Download original	Dpen unformatted	Expand all sections	🖌 Collap	se all sections 🛧 🧿 R	ecent repo
Product Overview									
Product Status					Feature Status				
Product: AXIS P	3715-PLVE Network Camera			B8A44F03F3B1	Disabled # O3C		Disabled	Continuous Recording	
Firmware: 10.11.6	5 🖉				Disabled CSSH Server		Disabled	FTP Server	
Load: 0.42, 0	.52, 0.49 🕑				Enabled ATTPS (Diges	st) 😧	Enabled	IP Address Filter	
Memory: 360 ME	3 available / 492 MB total				Disabled ASNMP		Enabled		
					Disabled Audio		Enabled	 Zipstream (Low) 	
Firmware Status					Disabled Dynamic GOP		Disabled	 Dynamic FPS 	
Installed Firmware		10.11.65			Disabled 📌 User Data		Disabled	Always Multicast	
		None 🕜			Disabled		Disabled	A Bonjour	
Rollback Firmware					Disabled		Enabled	 Brute Force Delay Protection 	
	Statistics								
Rollback Firmware Product Lifetime Current Uptime:	Statistics 12 days 4 h 15 mins @	Boot-up counter:	36 🕜		Enabled Replay Attack	Protection			

Watch the introduction video to learn more about AXIS Server Report Viewer.



AXIS VAPIX[®] Test Tool

The purpose of this tool is to aid in the troubleshooting of the Axis VAPIX[®] library requests when used in conjunction with the device event system as described in the *Get started with rules for events* section of the Axis documentation.

You can download the tool here: AXIS VAPIX® Test Tool.

AXIS OS Know

Troubleshooting



Product specific information

Product specific information

Hardware changes

When Axis makes hardware changes, to an existing model, that is not backwards compatible, the device gets a new Hardware ID. This is necessary as new components may require changes in how AXIS OS interacts with the hardware. All Axis device models have a Hardware ID that is used to identify that specific hardware configuration. An older device of a certain model may have one Hardware ID while a newer device of the same model may have another, new Hardware ID. Axis strives to avoid changing Hardware IDs for existing models as far as possible. Historically Hardware ID changes has been rare, but in recent years, due to the global component shortage situation, parts of the Axis portfolio already on the market has gotten new Hardware ID's.

All AXIS OS versions have a reference to the hardware ID that it supports. When a device gets a new Hardware ID, it is released on the latest Active as well as the latest versions of the available LTS tracks for that model. This means that if you have a device of a certain model, and buy a newer one that has had a hardware ID change, it will not be possible to downgrade the new model to an older AXIS OS version that does not support the new hardware ID. The same device with the previous Hardware ID supports all AXIS OS versions released since that Hardware ID was introduced.

To be transparent with changes that has been made we are listing all the products that has been affected by hardware ID changes. In the table below you can find which version you at least must use to not have issues when downgrading.

As always we recommend to use the latest supported version on the track you are using to have the latest patches and security updates. Read more about the AXIS OS tracks in AXIS OS Portal and follow the updates in each track in AXIS OS Release Notes.

Note

The <u>minimum active</u> is not recommended if there is a higher version LTS available, since they no longer are supported and replaced by the newer LTS.

The minimum LTS 6.50 or 8.40 is not recommended if there is a higher version of LTS available as this is no longer maintained.

Product	Track	Version	Release date
AXIS A8105-E	LTS 2016	1.58.2.2	2017-04-21
AXIS A8207-VE Mk II	Active (legacy)	11.0.89	2022-09-21
Product	Track	Version	Release date
AXIS C1310-E	Active (legacy)	10.12.66.1	2022-07-08
	Active (legacy)	10.10.73.3	2022-05-25
Product	Track	Version	Release date
AXIS Companion 360	Active (legacy)	8.40.1	2018-09-19
	Active (legacy)	7.15.2.2	2017-10-30
AXIS Companion Cube L/LW	LTS 2020	9.80.1.2	2020-05-20
	LTS 2018	8.40.1	2018-09-19
	Active (legacy)	7.40.1	2017-11-30
AXIS Companion Dome V/WV	LTS 2020	9.80.1	2020-05-04
	LTS 2018	8.40.1	2018-09-19
	Active (legacy)	7.40.1	2017-11-30
AXIS Companion Recorder 8CH/	4 CHTS 2020	9.80.1	2020-05-04
	Active (legacy)	1.11.1.3	2017-11-10

Product specific information

Product	Track	Version	Release date
AXIS M1045-LW	LTS 2020	9.80.1	2020-05-04
	LTS 2018	8.40.1	2018-09-19
	Active (legacy)	7.40.1	2017-11-30
AXIS M1065-L/-LW	LTS 2020	9.80.1.2	2020-05-20
	LTS 2018	8.40.1	2018-09-19
	Active (legacy)	7.40.1	2017-11-30
AXIS M1124/-E AXIS M1125/-E	LTS 2020	9.80.1	2020-05-04
	LTS 2018	8.40.1	2018-09-19
	Active (legacy)	8.15.1	2018-03-18
	LTS 2016	6.50.1.2	2017-06-14
AXIS M1134 AXIS M1135/-E AXIS M1137/-E	LTS 2022	10.12.104	2022-09-05
	Active (legacy)	10.3.0.1	2021-01-11
	LTS 2020	9.80.3.1	2021-03-03
AXIS M2026-LE Mk II	LTS 2020	9.80.1	2020-05-04
	LTS 2018	8.40.1	2018-09-19
	Active (legacy)	7.30.1.1	2017-10-16
AXIS M3044-V/-WV AXIS M3045-V/-WV	LTS 2020	9.80.1	2020-05-04
	LTS 2018	8.40.1	2018-09-19
	Active (legacy)	7.40.1	2017-11-30
AXIS M3046-V	LTS 2020	9.80.1	2020-05-04
	LTS 2018	8.40.1	2018-09-19
	Active (legacy)	6.15.7.2	2017-10-18
AXIS M3047-P AXIS M3048-P	LTS 2018	8.40.1	2018-09-19
	Active (legacy)	7.15.2.2	2017-10-30
AXIS M3067-P AXIS M3068-P	LTS 2022	10.12.104	2022-09-05
	Active (legacy)	10.11.87	2022-06-16
	LTS 2020	9.80.3.13	2022-07-22
AXIS M3088-V	Active	12.1.60	2024-11-13
	LTS 2024	11.11.127	2024-12-06
AXIS M3106-L/-LVE Mk II	LTS 2020	9.80.1	2020-05-04
	LTS 2018	8.40.1	2018-09-19
	Active (legacy)	7.30.1.1	2017-10-20

Product specific information

AXIS M3115-LVE AXIS M3116-LVE	LTS 2022	10.12.104	2022-09-05
	Active (legacy)	10.11.85	2022-06-14
	LTS 2020	9.80.3.13	2022-07-22
AXIS M3128-LVE	Active	12.1.60	2024-11-13
	LTS 2024	11.11.128	2024-12-18
AXIS M4216-V/-LV	Active (legacy)	11.0.89	2022-09-21
	Active (legacy)	10.12.73	2022-07-13
AXIS M4218-V AXIS M4218-LV	Active	12.1.60	2024-11-13
	LTS 2024	11.11.127	2024-12-06
AXIS M5074 AXIS M5075/-G	Active (legacy)	11.0.89	2022-09-21
	Active (legacy)	10.12.91	2022-08-16
Product	Track	Version	Release date
AXIS P1375	Active (legacy)	11.0.89	2022-09-21
	Active (legacy)	10.12.65	2022-07-01
	LTS 2020	9.80.28	2023-04-21
AXIS P1375-E	Active (legacy)	11.2.53	2022-12-22
	LTS 2022	10.12.135	2022-12-09
AXIS P1377 ExCam XF P1377 F101-A XF P1377 AXIS P1378	Active (legacy)	11.0.89	2022-09-21
	Active (legacy)	10.12.65	2022-07-01
	LTS 2020	9.80.3.13	2022-07-22
AXIS P1377-LE AXIS P1378-LE	Active (legacy)	11.2.53	2022-12-22
	LTS 2022	10.12.135	2022-12-09
	LTS 2020	9.80.28	2023-04-21
AXIS P1385 AXIS P1385-BE AXIS P1385-E AXIS P1385-LE	LTS 2024	11.11.124	2024-11-25
AXIS P1447-LE AXIS P1448-LE	LTS 2022	10.12.104	2022-09-05
	Active (legacy)	10.3.0.1	2021-01-11
	LTS 2020	9.80.3.1	2021-03-03
AXIS P1455-LE	LTS 2022	10.12.104	2022-09-05
	Active (legacy)	10.8.3	2021-11-30

Product specific information

AXIS P1465-LE AXIS P1465-LE-3	Active	12.1.60	2024-11-13
	LTS 2024	11.11.124	2024-11-25
AXIS P3224-LV/-V Mk II AXIS P3225-LV/-LVE/-V/-VE Mk	LTS 2020	9.80.1	2020-05-04
	LTS 2018	8.40.1	2018-09-19
	Active (legacy)	7.40.1.1	2018-01-31
AXIS P3245/-LV/-LVE/-V/-VE	LTS 2022	10.12.104	2022-09-05
	Active (legacy)	10.11.85	2022-06-14
	LTS 2020	9.80.3.13	2022-07-22
AXIS P3245-LVE 22mm	LTS 2022	10.12.104	2022-09-05
	Active (legacy)	10.4.3	2021-03-10
AXIS P3247-LV/-LVE	LTS 2022	10.12.104	2022-09-06
	Active (legacy)	10.11.89	2022-06-20
	LTS 2020	9.80.3.13	2022-07-22
AXIS P3248-LV/-LVE	LTS 2022	10.12.104	2022-09-06
	Active (legacy)	10.11.89	2022-06-2
	LTS 2020	9.80.3.13	2022-07-22
AXIS P3267-LV/-LVE AXIS P3268-LV/-LVE	Active (legacy)	11.0.89	2022-09-21
	Active (legacy)	10.12.55	2022-06-16
AXIS P3727-PLE	LTS 2022	10.12.104	2022-09-05
	Active (legacy)	10.7.8	2021-10-29
AXIS P3738-PLE	Active	12.1.60	2024-11-13
AXIS P3925-LRE	Active (legacy)	11.0.89	2022-09-21
	LTS 2022	10.12.104	2022-09-05
	LTS 2020	9.80.3.14	2022-09-07
AXIS P3925-R	Active (legacy)	11.0.93	2022-09-30
	LTS 2022	10.12.104	2022-09-05
	LTS 2020	9.80.3.14	2022-09-07
AXIS P3935-LR	Active (legacy)	11.0.95	2022-10-04
	LTS 2022	10.12.104	2022-09-05
	LTS 2020	9.80.3.14	2022-09-07
AXIS P4708-PLVE	Active	12.1.60	2024-11-13
Product	Track	Version	Release date
AXIS Q1615/-LE Mk III	Active (legacy)	11.0.89	2022-09-21
	Active (legacy)	10.12.65	2022-07-01

Product specific information

AXIS Q1715	Active (legacy)	11.0.89	2022-09-21
	Active (legacy)	10.12.55	2022-06-16
AXIS Q1798-LE	Active (legacy)	11.0.89	2022-09-21
	Active (legacy)	10.12.65	2022-07-01
	LTS 2020	9.80.3.13	2022-07-22
AXIS Q1805-LE	Active	12.0.91	2024-09-30
	LTS 2024	11.11.124	2024-11-25
AXIS Q3538/-LVE/-SLVE	LTS 2022	10.12.104	2022-09-05
	Active (legacy)	10.9.6	2022-02-09
AXIS Q3819-PVE	LTS 2022	10.12.104	2022-09-05
	Active (legacy)	10.11.85	2022-06-14
AXIS Q6010-E	Active (legacy)	11.0.89	2022-09-21
	Active (legacy)	10.12.73	2022-07-13
	LTS 2020	9.80.10	2022-11-18
AXIS Q6074/-E AXIS Q6075/-E/-SE	LTS 2022	10.12.104	2022-09-05
	Active (legacy)	10.11.87	2022-06-16
	LTS 2020	9.80.3.13	2022-07-22
AXIS Q6100-E	Active (legacy)	11.0.89	2022-09-21
	Active (legacy)	10.12.73	2022-07-13
AXIS Q6215-LE	Active (legacy)	11.2.53	2022-12-22
	LTS 2022	10.12.130	2022-11-25
	LTS 2020	9.80.10	2022-11-18
AXIS Q6315-LE	LTS 2022	10.12.104	2022-09-05
	Active (legacy)	10.9.1	2022-12-22
AXIS Q9216-SLV	LTS 2022	10.12.104	2022-09-05
	Active (legacy)	10.11.55	2022-04-21
	LTS 2020	9.80.3.11	2022-05-06
Product	Track	Version	Release date
AXIS S3016	Active (legacy)	11.10.65	2024-03-11

Overlay image support

Overlay images are part of a device specific feature set since the images that can be used depend on the device's image sensor size, resolution and other parameters. In general, the following needs to be considered when uploading an overlay image to an Axis device:

- Supported files:
 - 24-bit BMP file support in AXIS OS 9.80 LTS and lower.
 - 24-bit BMP, jpeg, png & svg+xml file support from AXIS OS 10.7 and onwards*.

Product specific information

- The height and width of the overlay image cannot exceed the resolution of the Axis device. For example, if the resolution of the Axis device is set to 1280x720, the overlay image cannot be larger than that.
- Max 256 colors supported. It's recommended to use 250 colors to spare the remaining colors for transparency and configuration purposes.
- Depending on AXIS OS version, some Axis devices support a maximum number of pixels (width by height) that is capped either to 109920 (older versions) or 64000 pixels (newer versions). Width and height needs to be dividable by 32.
- The maximum resolution for the overlay image is 1920x1080 pixels for ARTPEC-based devices. For Ambarella-based devices, see the table below.

*Also supported by AXIS P1375/-E, AXIS P1377/-LE, AXIS P1378/-LE, AXIS P5654-E, AXIS P5655-E, AXIS M1134, AXIS M1135/-E, AXIS M1137/-E, AXIS M3064-V, AXIS M3065-V, AXIS M3066-V, AXIS M3115-LVE, AXIS P3245-V/-VE/-LV/-LVE, AXIS P3247-LV/-LVE, AXIS P3248-LV/-LVE, AXIS P3715-PLVE, AXIS P3717-PLE, AXIS P3719-PLE, AXIS P3925-R/-LRE, AXIS P3935-LR, AXIS Q6074/-E, AXIS Q6075/-E/-S/-SE and AXIS Q6078-E in AXIS O 9.80 LTS

Maximum resolution for overlay images					
System-on-chip	Max width (pixels)	Max height (pixels)	Max number of pixels		
Ambarella S2L	1920	1080	64000		
Ambarella S3L	1920	1080	64000		
Ambarella S5L	1920	1080	92160		
Ambarella S5	1920	1080	92160		
Ambarella CV25	1920	1080	138240		
Ambarella S6Lm	1504	1080	138240		

Image overlay transparency support			
BMP 8-bit + 24-bit	Yes, through assigning one color for the transparency. Other bit depths are not supported.		
JPEG	Not supported		
PNG	Native support*		
SVG+XML	Native support*		

* Support for transparency through the image format. This means you can import the image which already contains the transparent information.

Set image size in GIMP

The screenshot below illustrates how to set the correct image size of an image in GIMP.

Product specific information



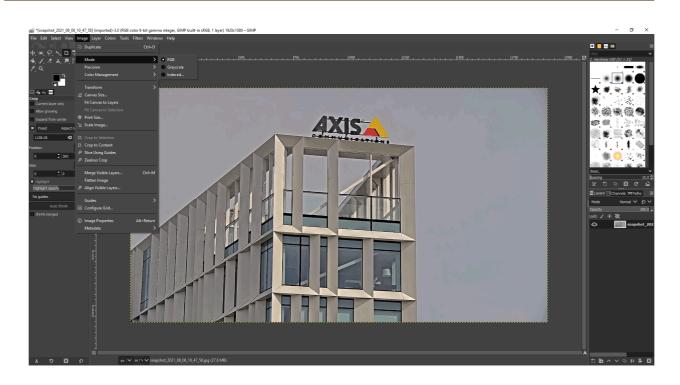
Set max colors in GIMP

The screenshots below illustrate how to set max color in an image using GIMP. Note that the amount of colors has to be set in Image > Mode > Indexed. When done, switch back to Image > Mode > RGB. Note: If transparency is to be used, make sure to use the pipette tool to check which color the transparent part has after max

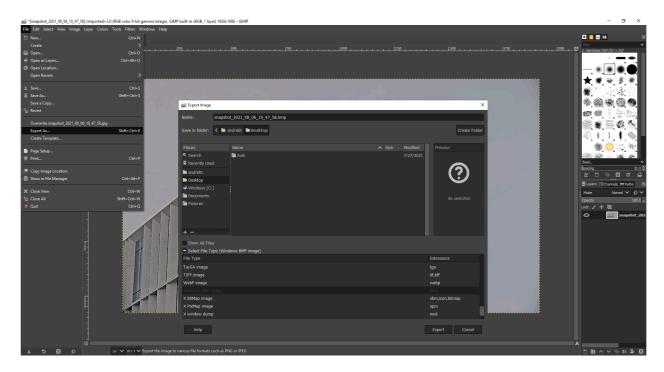
colors have been set.



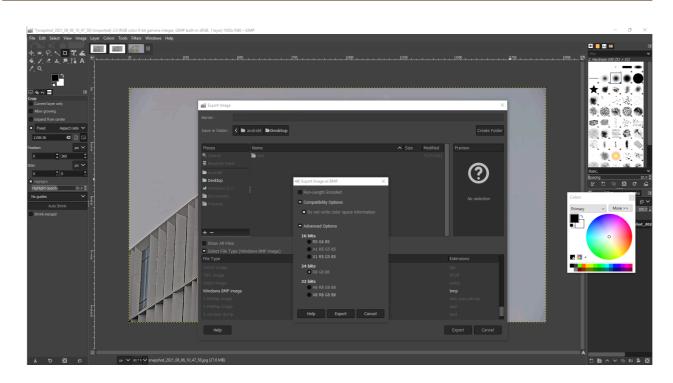
Product specific information



Export 24-bit bmp file in GIMP The screenshots below illustrate how to export an image as a 24-bit bitmap image.



Product specific information



Send mail

AXIS OS devices support sending mail to various mail services through the built-in event system. While you can customize the settings, some public mail server choices are pre-configured. When using public mail services such as Gmail, Yahoo etc. you are limited to the requirements of their services. From May 30, 2022, Google (and thus the Gmail mailing service) will *no longer support* the use of third-party apps or devices which ask you to sign in to your Google account using only your username and password. This means that AXIS OS devices will not be able to send mail using a Gmail address as sender without using *a Google App Password*. Using a Gmail address as a receiver will still work after this date without additional configuration. Further more, Microsoft will no longer support *Basic authentication* from Dec 30, 2022. This means Hotmail, Outlook etc will stop to work if using basic authentication. Microsoft don't have their own solution for this.

(C) 2022 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC and VAPIX are registered trademarks of Axis AB in various jurisdictions. All other trademarks are the property of their respective owners.

AXIS OS Knowledge base © Axis Communications AB, 2023 - 2024 Ver. M25.2 Date: November 2024 Part no.