Technical paper

AXIS Camera Station Pro Certificate Infrastructure

May 11, 2026
Rev. 1.0

Table of contents

Introduction

There are several different times that certificates are used within Axis Camera Station for securing communications between the Axis Camera Station Server, Axis Camera Station Client, Devices, and Components. This document explains the relevant details for the different use cases for certificates within Axis Camera Station. This document is based on AXIS Camera Station version 6.16. If you are on an older version, some features may function differently.

1 Certificate Authority

Certificate name
CA certificate
Alternative names
AXIS Camera Station root certificate
Subject alternative names (SAN)
None
Location/s

- In main database (KEY_VALUE table)
- Windows certificate store (Local computer - Trusted Root Certification Authorities)
- Windows certificate store (Local computer – Intermediate Certification Authorities)
- Disk (ProgramData\Axis Communications\AXIS Camera Station Server\certs\ca.cert.pem)

Private key location/s

- In main database (KEY_VALUE table)

Chain
Self-signed
Validity period
10 years
Replaceable/Renewal
Replaceable and renewable from client UI (Configuration/Security/Certificates - Certificate Authority)
Key algorithm
RSA (4096 bits) **Feature documentation:**

With a certificate authority, the AXIS Camera Station server can automatically create, sign, and install client/server certificates on devices as needed when enabling HTTPS and IEEE 802.1X. This negates the requirement to manually install certificates on devices before enabling HTTPS and IEEE 802.1X.

1. The subject common name (CN) of the certificate authority (CA) certificate that is currently installed on the AXIS Camera Station server (along with its private key). This certificate can be used to authenticate the signature of all client/server certificates that are signed (using the private key) by the AXIS Camera Station server. The Axis Camera Station server will install CA certificate on all devices as well if it is missing upon enabling HTTPS on the cameras, as well as during the nightly refresh.
2. Imports an existing CA certificate and its private key, and stores its passphrase so that Axis Camera Station can use the CA without prompting the user. Must be a PKCS#12 file, the certificate must have a *basic constraint (2.5.29.19)*[1] indicating that it's a CA certificate, and the current time must be within the certificate's validity period. This also must be RSA 4096. Importing a new certificate authority, will replace all component certificates and restart all the components. Any devices that were setup with HTTPS will be automatically updated. An

intermediate certificate authority can be imported only if its full certificate chain, including the root CA, is already trusted and available in the Windows Certificate Store. The whole chain cannot be imported at once, only the intermediate CA should be imported.

3. Generate a new key pair with a 4096 bit key length and self-signed CA certificate that is valid for 10 years. The certificate will have a *basic constraint (2.5.29.19)* [1] indicating that it's a CA certificate, and a *key usage (2.5.29.15)* [1] indicating that it may be used for certificate signing. Generating a new certificate authority will replace all component certificates and restart all the components. CA certificate will be updated on all devices. Any devices that were setup with HTTPS need to be updated.
4. Display details about the currently installed CA certificate.
5. Exports the currently installed CA certificate to file, with or without the private key. The public key is needed to verify the certificates that were self-signed by the private key of this CA root. Without the private key, this CA root can then be installed in the *Trusted Root Certification Authorities certificate store* so that other applications (i.e web-browsers) can verify the CA signed certificates without getting a warning. When exported with the private key, this can be imported into another Axis Camera Station Server or Axis Device Manager Server to be used for signing other device certificates with the same CA.
6. Client/server certificates which are automatically created and signed by the certificate authority when enabling/updating HTTPS and/or IEEE 802.1X will be valid for this long. Note that the certificate authority will not sign certificates that are valid beyond its own expiration date.

1: These are key extensions. See the glossary for more details.

When the server starts and no Certificate Authority is configured, one will automatically be generated as if the user pressed the "Generate" button, but with a random password. Axis Camera Station will also make sure that the Certificate Authority that is stored in the database is also installed on the server machine's *Trusted Root Certification Authorities'* and on the file system in an admin accessible folder *(C:\ProgramData\Axis Communications\AXIS Camera Station Server\certs).* When Axis Camera Station is uninstalled, it will remove from the store any certificates that it installed before as long as they are certificates that Axis Camera Station created (i.e. automatically or via the *Generate* button). Third party certificates that were imported in Axis Camera Station and installed in the trust store, will not be removed upon uninstallation. The certificate authority stored on the file system will always be removed at uninstallation even if it is a third-party certificate authority.

Limitations:

1. Using a custom Certificate Authority with the private key in CNG format is not supported.
2. No support for revoking specific compromised certificates. If a certificate which is signed by the Axis Camera Station CA is compromised, the CA needs to be replaced and a new set of certificates need to be distributed to all devices.
3. Imported root certificates without protected private keys are not fully supported. Axis Camera Station will ask for a password every time Https/IEEE is enabled or a new device is added to the system.
4. An intermediate certificate authority can be imported only if its full certificate chain, including the root CA, is already trusted and available in the Windows Certificate Store.
5. Imported third party certificates will not be removed from the windows store when Axis Camera Station is uninstalled.
6. If a user has changed permissions on folders or files under %programdata%\Microsoft\Crypto , certificates might not work as expected. A symptom of this could be: CryptographicException with the message ‘Access is denied’ or ‘Keyset as registered is invalid’.
7. When using the Axis Camera Station CA certificate as the IEEE 802.1X CA certificate (by exporting it and then selecting it for IEEE 802.1X under Configuration - Security - Certificates), the CA certificate will not be automatically updated on devices that have IEEE 802.1X enabled.
8. Devices on AXIS OS versions lower than 6.10 only support TLS 1.1, which AXIS Camera Station Pro does not support. TLS 1.2 or TLS 1.3 are required, therefore these older versions cannot utilize HTTPS to communicate with the server.

2 Client → Server communication, Axis Camera Station API, Web client (on-prem) → Server communication (Reverse proxy)

Certificate name
Server Certificate
Alternative names
- <Computer name>.axis.remoting
- Remoting certificate
- External API certificate

Subject alternative names (SAN)
Public IP addresses and DNS Names for all network interfaces
Location/s
- Windows certificate store (Local computer - Personal)
- Disk, only end-entity certificate (ProgramData\Axis Communications\AXIS Camera Station Server\Components\Axis Camera Stationpublic.pem)
- Disk, with chain inlcuding intermediate CAs (ProgramData\Axis Communications\AXIS Camera Station Server\certs\server.crt)

Private key location/s
- Windows certificate store (Local computer - Personal)
- Disk (ProgramData\Axis Communications\AXIS Camera Station Server\certs\server.key.pem)

Chain
Self-signed
Validity period
10 years
Replaceable/Renewal
Replaceable and renewable from the Certificate tab in the service control
Key algorithm
RSA (2048 bits)
Feature documentation

Description
The certificate enables secure communication between the AXIS Camera Station server and remote clients like the windows client, components, the web client, or other 3rd party applications which call the Axis Camera Station API.

Certificate creation in Axis Camera Station
The certificate is created automatically with the format *<current machine name>.axis.remoting* and is referred to as "*default Axis.Remoting certificate*" in the following sections.
It is stored in the computer certificate store under: Certificates - Local Computer / Personal / Certificates. Within Windows, use *Manage computer certificates* to see the store.

When Axis Camera Station starts up, the following happens with regards to the AXIS Camera Station server API certificate:
1. If no certificate exists in ***Local Machine*** certificate store location with the format *<current machine name>.axis.remoting*, a new certificate will be created.
2. If no certificate is registered on the port, the default Axis.Remoting certificate will be registered to the AXIS Camera Station server HTTPS port.
3. The certificate *registered on the port* is exported to disk for components to use during SSL handshake.
4. AXIS Camera Station server API is set up and published.

Certificate properties

The certificate contains a Subject Alternate Name (SAN) containing all the server's IP addresses and DNS Names which are needed to accept the certificate from a browser without warning. There is also a check when connecting via the Desktop client that this certificate is valid and trusted. This is also important for Axis Camera Station Components as these sometimes require access to the API gateway.

Certificate renewal or import:
In Axis Camera Station version 6.8 or older: Configuration → Security → Certificates, there is the possibility to renew default Axis.Remoting certificate. In Axis Camera Station Version 6.9 or newer, this has been moved to the AXIS Camera Station Service control. In order to manage this certificate, the Service Control must be run as an Administrator. One can generate the certificate or can import their own certificate. The certificate only requires a *key usage (2.5.29.15)* indicating that it may be used for TLS Web Server Authentication. If importing your own certificate, be mindful to include all relevant SAN which are intended to be used to connect to the server via the desktop client, mobile app, or web client.

This will remove the old default certificate, create a new one and replace current registration with this new certificate on the API port.

Note
The new certificate will not be used for Client / Mobile App and Server communication until after the server is restarted.

The old certificate will not be removed from the windows certificate store if it was previously imported instead of being generated by AXIS Camera Station.

3 Server → Device communication

Certificate name
Device Certificate
Alternative names
- e.g. [GS]_D0CD1_device-example-Q6078-E
- Device server certificate

Subject alternative names (SAN)
IP address or DNS name
Location/s
- On the device
- In main database (CERTIFICATE table)

Private key location/s
- On the device

Chain
CA certificate → Device certificate
Validity period
1 year, configurable from client UI (Configuration/Security/Certificates - Certificate authority)
Replaceable/Renewal
Renewable from client UI (Devices/Management - Manage devices)
Key algorithm
RSA (2048 bits)
Feature documentation

Use cases:

- **I have an existing company root CA and want to allow AXIS Camera Station to act as an intermediate CA**
  If one is using an existing CA, having AXIS Camera Station as root is not an option. If they are willing to allow AXIS Camera Station to act as an intermediate CA they can still use the

automatic certificate signing by creating an intermediate CA externally and importing it into AXIS Camera Station.

- **I have an existing root CA, and I am unwilling to let AXIS Camera Station act as an intermediate CA**
  If one has an existing CA but is unwilling to allow AXIS Camera Station to sign certificates on its behalf, certificates will have to be created externally and manually installed on devices using the Security context menu in Device Management.
- **I got certificates from a third party CA**
  Certificates will have to be created externally and manually installed on devices using the Security context menu in Device Management.
- **I don’t have an existing CA, but I want to have HTTPS with minimal effort**
  For one who wants HTTPS communication, but doesn't have nor want to deal with a CA (e.g. mandatory HTTPS regulations), can use AXIS Camera Station as a root CA by generating a new key pair and insert the created certificate into parts of the system that access the devices. This is the default behavior if certificates are left untouched by the system administrator.

Note:
All certificates which are imported to devices and are generated from Axis Camera Station or Axis Device Manager will have a header between brackets within the certificate name, for example: [GS] Generated Server, [CA] Certificate Authority, [T] Temporary (for the purposes of signing), Etc.

5 Component → Component communication (mTLS)

Certificate name:
Component Server certificate
Alternative names

- <Component id>

Subject alternative names (SAN)

- Computer name
- localhost
- Public IP addresses for all network interfaces
- 127.0.0.1 (IPv4 localhost loopback)
- ::1 (IPv6 localhost loopback)

Location/s

- Disk (ProgramData\Axis Communications\AXIS Camera Station Server\Components\Certificates\<component id>.server.cert.pem)

Private key location/s

- Disk (ProgramData\Axis Communications\AXIS Camera Station Server\Components\Certificates\<component id>.server.key.pem)

Chain
CA certificate → Component Server certificate
Validity period
10 years

Replaceable/Renewal
Automatic renewal during startup of Axis Camera Station Server
Automatic replacement after Certificate Authority is generated

Key algorithm
RSA (2048 bits)

Certificate name:
Component Server certificate
Alternative names
- <Component id>

Subject alternative names (SAN)
- <component id>.component@natsbroker.localhost

Location/s
- Disk (ProgramData\Axis Communications\AXIS Camera Station Server\Components\Certificates\<component id>.client.cert.pem)

Private key location/s
- Disk (ProgramData\Axis Communications\AXIS Camera Station Server\Components\Certificates\<component id>.client.key.pem)

Chain
CA certificate → Component Client certificate
Validity period
10 years

Replaceable/Renewal
Automatic renewal during startup of Axis Camera Station Server
Automatic replacement after Certificate Authority is generated
Key algorithm
RSA (2048 bits)
Feature documentation
Axis Camera Station creates and signs (using the Certificate Authority certificate) a set of certificates stored as pem files. The components can use these certificates to authenticate as Client or Server when communicating with another component or NATS via mTLS via the NATS Broker / NATS Administrator components. Both NATS components must be running in order for other components to function.

6 Axis Camera Station → My Systems (part of Axis Connected services)

Certificate name
Axis Cloud Client certificate
Alternative names
- Cloud Certificate

Subject alternative names (SAN)
- N/A

Location/s
- Disk (See path in registry key *Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Axis Communications\AXIS Camera Station Cloud Service)* ○ *E.g. C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Camera Station Cloud Service\CloudConnectClientCerts\cert.crt*

Private key location/s
- Disk (See path in registry key *Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Axis Communications\AXIS Camera Station Cloud Service)* ○ *E.g. C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Camera Station Cloud Service\CloudConnectClientCerts\key.pem* **Chain**

Service Platform CA Stage G2 → Cloud Certificate
Validity period
1 year
Replaceable/Renewal
Auto renew
Key algorithm
RSA (2048 bits)

Feature documentation
This certificate is automatically generated when onboarding a system to My Systems and cannot be modified by a user.

Glossary

Self-signed:
A self-signed certificate is a certificate that is signed by the same entity whose identity it certifies.
https://en.wikipedia.org/wiki/Self-signed_certificate **mTLS**:
Mutual TLS, or mTLS for short, is a method for mutual authentication where both the client and server are authenticated.
https://www.cloudflare.com/learning/access-management/what-is-mutual-tls/ **Key extensions:**
Key extensions describe the functionality related to key usage, certificate policies and constraints, and more.
https://learn.microsoft.com/en-us/windows/win32/seccertenroll/about-version-3-extensions