

HOW TO.

AXIS Device Manager HTTPS certificate management

Introduction

HTTPS consists of communication over HTTP within a connection encrypted by Transport Layer Security (TLS).

Network encryption protects the communication between the client, VMS, and the network device. It prevents information being extracted by network traffic sniffing, and it prevents data being altered during transfer.

This guide explains how to configure and enable HTTPS communication on Axis devices from AXIS Device Manager.

This configuration has been tested with AXIS Device Manager version 5.03 and devices with firmware 6.50.1.3 and 7.30.1.

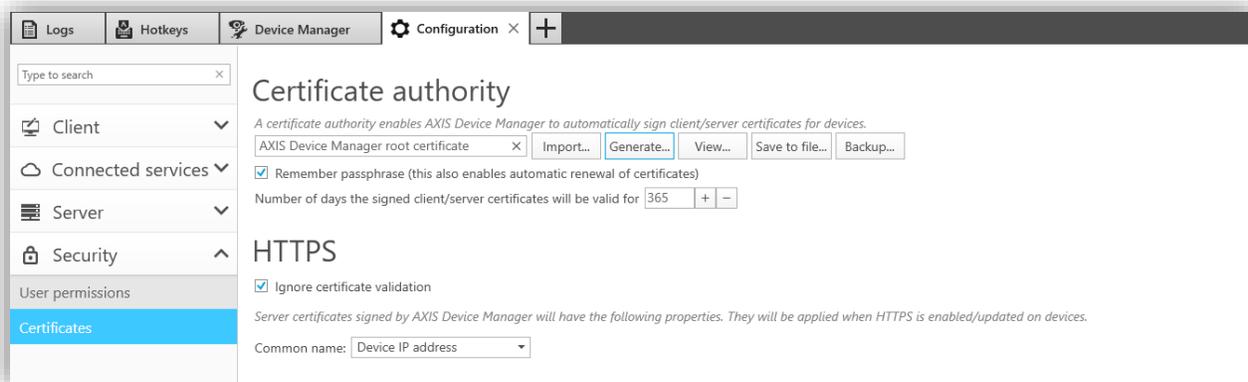
Requirements: To use HTTPS, devices require firmware 5.70, or 1.25 for Access control and Audio products.

Important notes:

- *Devices with firmware 7.20 and above are pre-configured with a self-signed certificate and require a special handling, described at the end of this document.*
- *Make sure your Video Management System supports HTTPS communication before enabling HTTPS. If your Video Management Software doesn't support HTTPS, it won't be able to communicate with the cameras and no Live View or Recording will be possible.*

Step 1 Choose Certificate Authority

In the AXIS Device Manager **Configuration** tab, go to Security > Certificates.



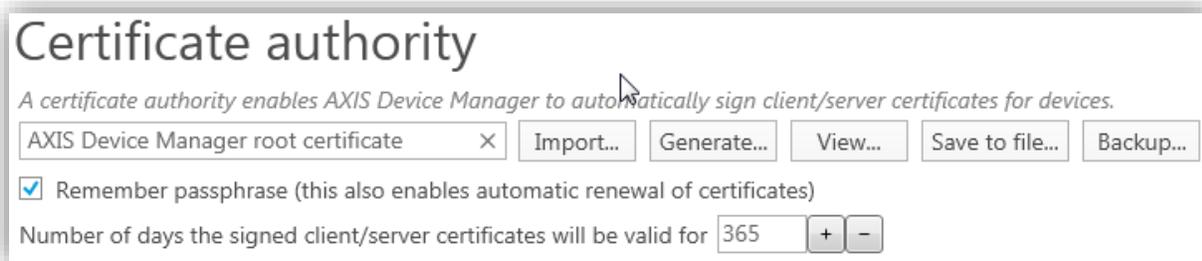
AXIS Device Manager as Certificate Authority (CA)

Using AXIS Device Manager as CA simplifies the whole process of deploying and renewing certificates for the administrator. It means AXIS Device Manager will use its own root certificate to issue server certificates and there is no other root CA involved in the process.

If you have an existing root CA, you shouldn't use this method but use AXIS Device Manager as Intermediate CA instead (section below).

If you want AXIS Device Manager to act as your CA (i.e. automatically issuing your server certificates), click **Generate...** and enter a Passphrase.

For increased security, it is recommended not to select "Remember passphrase".



Certificate authority

A certificate authority enables AXIS Device Manager to automatically sign client/server certificates for devices.

AXIS Device Manager root certificate × Import... Generate... View... Save to file... Backup...

Remember passphrase (this also enables automatic renewal of certificates)

Number of days the signed client/server certificates will be valid for 365 + -

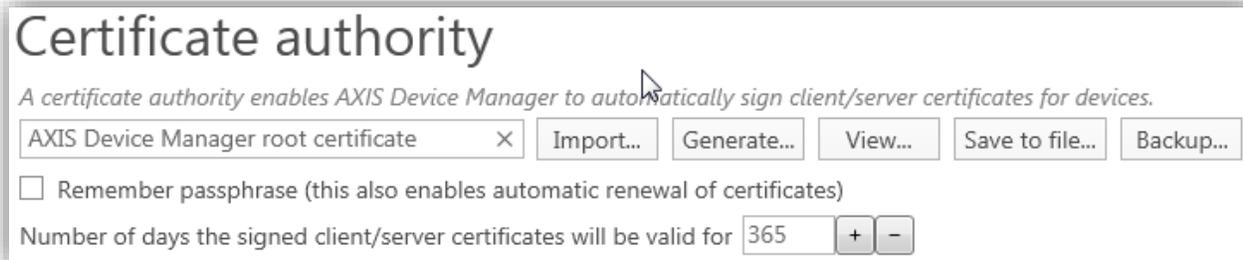
Once generated, click **Save to file...** and save **ADM_root_certificate.crt** on your computer. This certificate can be provided to any third-party application in order to trust the camera certificate.

AXIS Device Manager as Intermediate Certificate Authority (CA)

Using AXIS Device Manager as Intermediate CA implies that you have an existing CA (root or intermediate CA) which can issue CA certificates to other intermediate CAs (e.g. AXIS Device Manager). In this scenario you need to import a CA certificate in AXIS Device Manager in order to sign and issue server certificates for the Axis devices. This CA certificate may be a root certificate or a subordinate CA certificate (intermediate certificate).

To set AXIS Device Manager as intermediate Certificate Authority, click **Import...** and select your existing CA certificate.

For increased security, it is recommended not to select "Remember passphrase".



Certificate authority

A certificate authority enables AXIS Device Manager to automatically sign client/server certificates for devices.

AXIS Device Manager root certificate × Import... Generate... View... Save to file... Backup...

Remember passphrase (this also enables automatic renewal of certificates)

Number of days the signed client/server certificates will be valid for 365 + -

Step 2 Choose Common name for server certificate

Select the **Common name** from **Device IP address** or **Device host name (FQDN)**.

This setting specifies what device specific property will be written as the common name in the individual certificates that are created for each device when AXIS Device Manager acts as a Certificate Authority.

HTTPS

Ignore certificate validation

Server certificates signed by AXIS Device Manager will have the following properties. They will be applied when HTTPS is enabled/updated on devices.

Common name: Device IP address

Device IP address

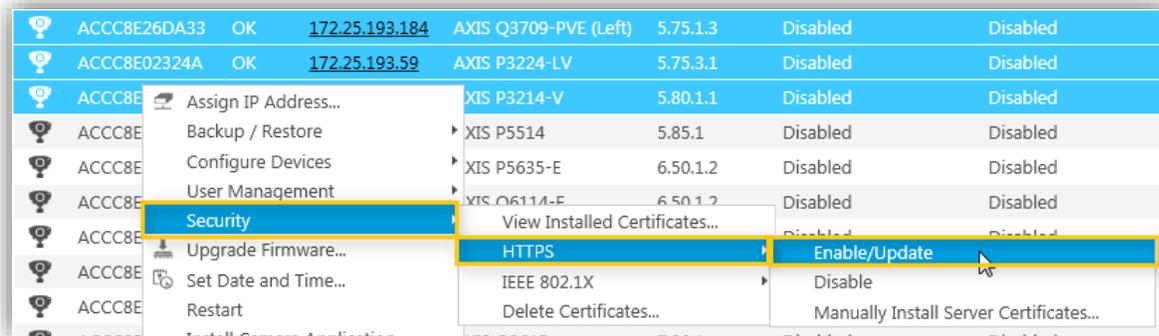
Device host name (FQDN)

In the **Device Manager** tab, the HTTPS column should change from **Disabled (Missing server certificate)** to **Disabled** for supported devices.

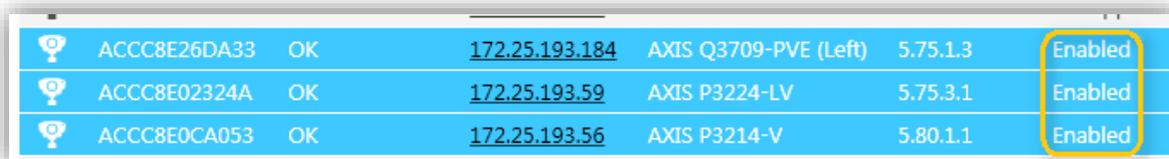
	MAC address	Status	Address	Model	Firmware ^	HTTPS
	ACCC8E2CDAE9	OK	172.25.193.126	AXIS P8221	5.10.3	Unsupported firmware
	ACCC8E0C0B69	OK	172.25.193.155	AXIS P1224-E	5.50.9.2	Unsupported firmware
	ACCC8E26DA33	OK	172.25.193.184	AXIS Q3709-PVE (Left)	5.75.1.3	Disabled
	ACCC8E022A4D	OK	172.25.193.181	AXIS Q6114-E	6.50.1.2	Disabled
	ACCC8E68D4D2	OK	172.25.193.119	AXIS P1367	7.15.1.1	Disabled

Step 3 Enable HTTPS on the device(s)

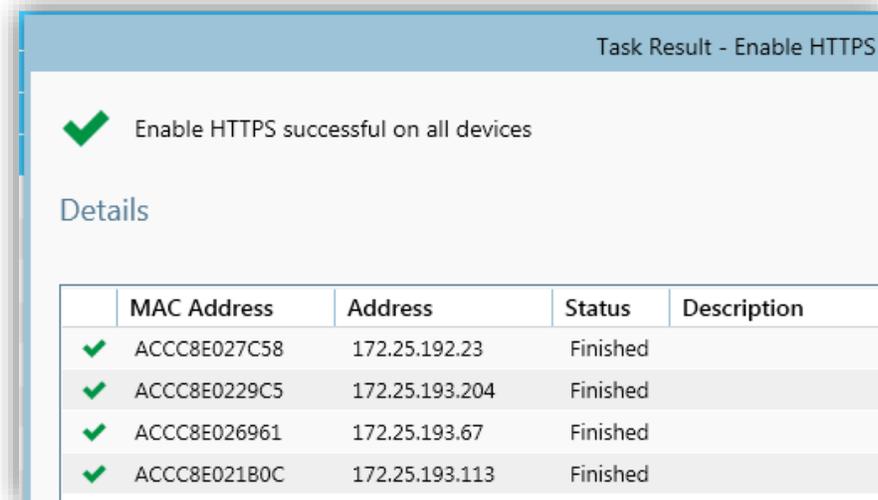
To enable HTTPS on the device(s), right-click on the selected device(s) and go to *Security > HTTPS > Enable/Update*.



The HTTPS column should change to **Enabled** for the selected device(s). You are done!



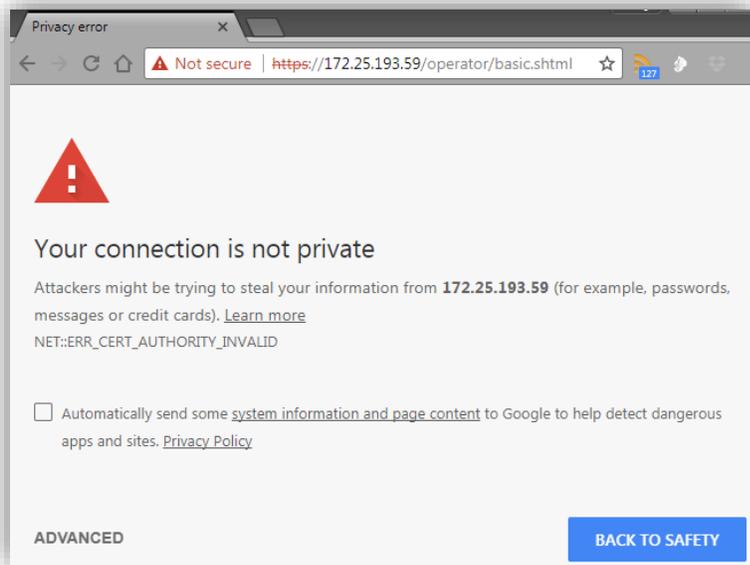
Double-click on the task to check the result for each device.



Note: Since AXIS Device Manager is set to “Ignore certificate validation” by default, it is necessary to disable this option after HTTPS has been enabled in order to get an exclusive HTTPS connection to the device from the software. This can be done from the **Configuration** tab under **Security**.

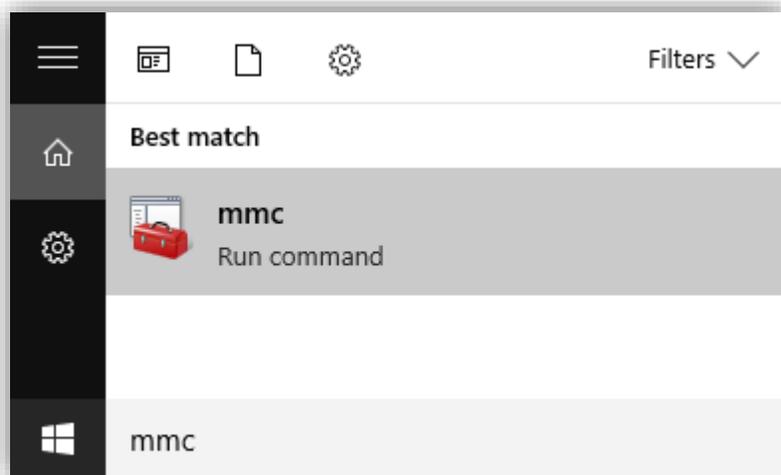
Step 4 Add the CA certificate to certificate store (Optional)

It is recommended to add the CA certificate to your Windows certificate store so your web browser won't pop-up a security warning regarding invalid security certificate and won't block the connection to the device. This will ensure a secure HTTPS connection to your devices.

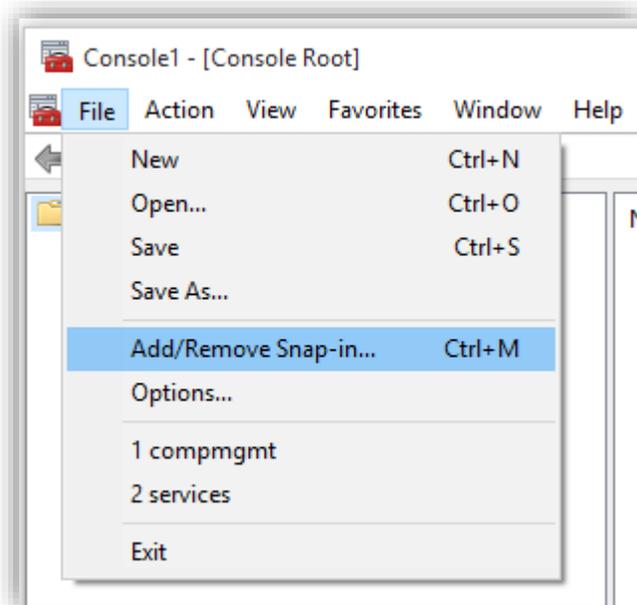


Instructions for Windows 10

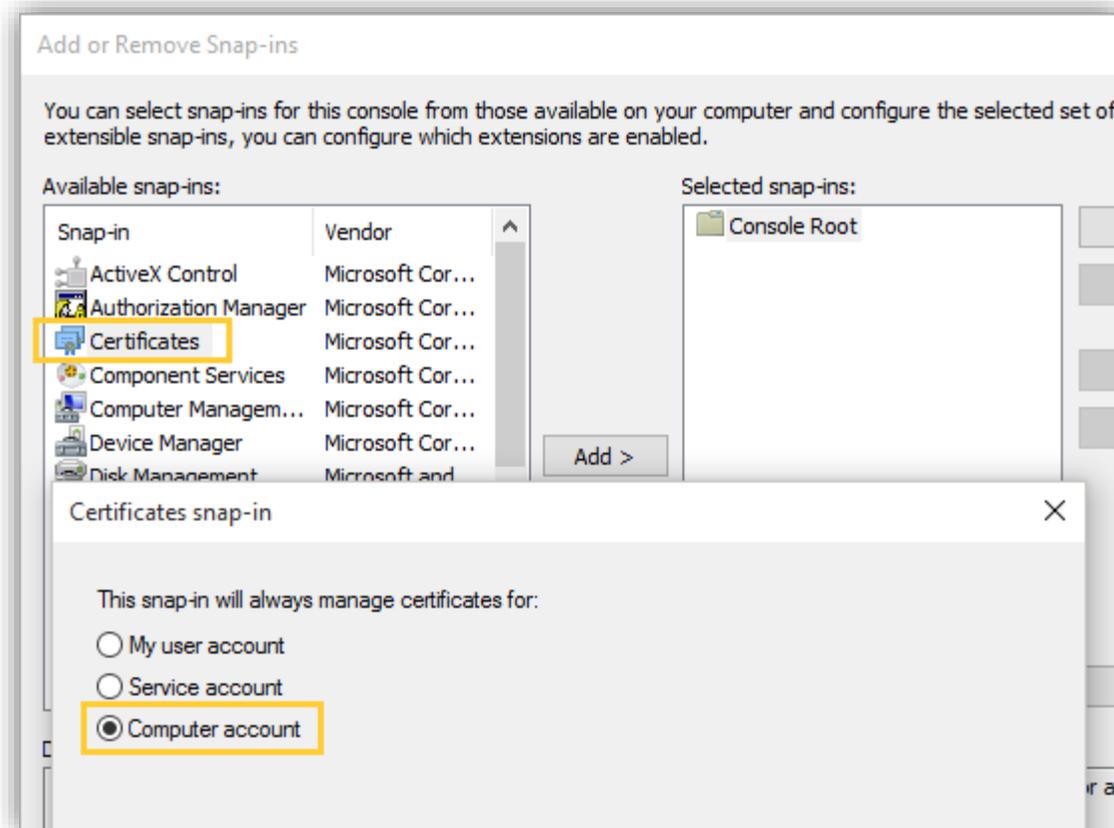
Open the Windows **Start** menu and enter **mmc** to open the **Console Root**.



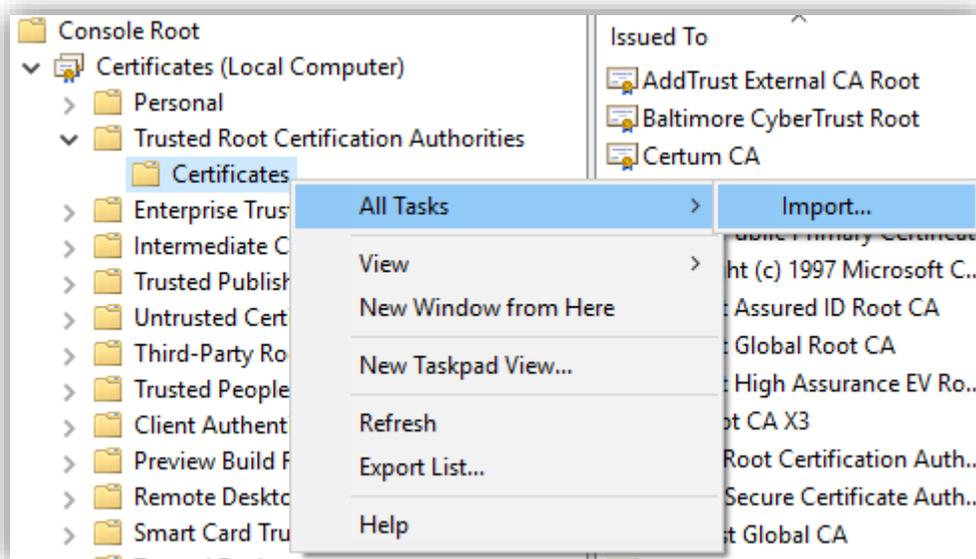
In the console, go to *File > Add/Remove Snap in...*



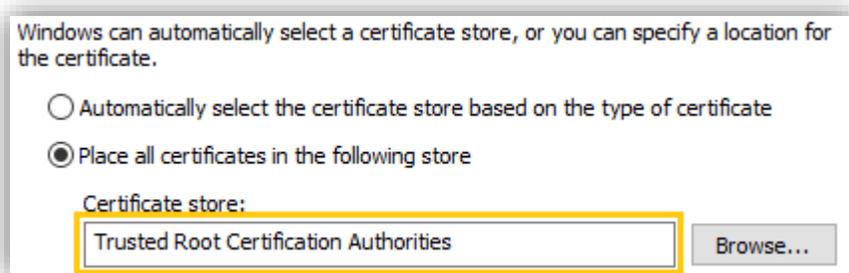
In the list on the left side, select **Certificates** and choose to manage the certificates for the **Computer account**. Click OK.



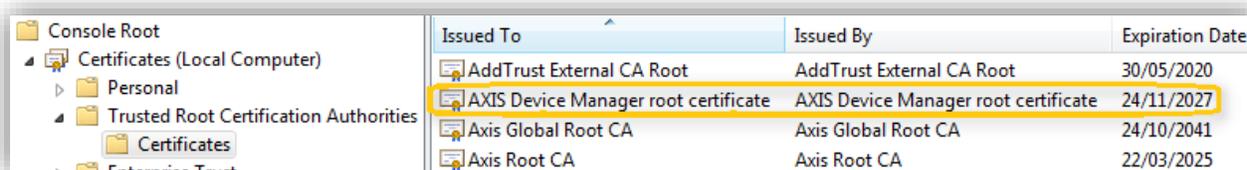
Navigate to *Certificates – Local computer > Trusted Root Certification Authorities* and right-click on **Certificates**. Choose *All Tasks > Import...*



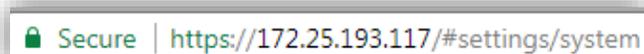
Select the **ADM_root_certificate.crt** saved on your computer or your own CA certificate and place it in the **Trusted Root Certification Authorities** store.



Click **Next** and **Finish**. The certificate is now added to the store:



Restart your web browser, the connection is now secure:

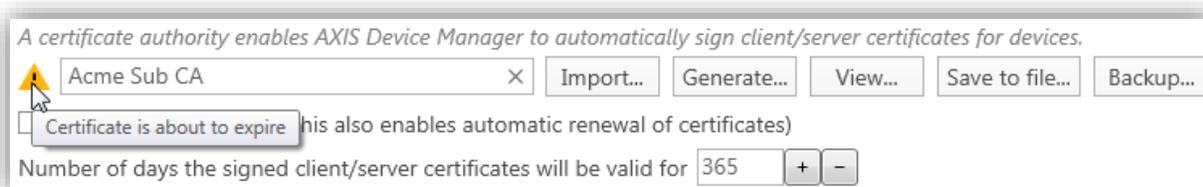


Step 5 Update/renew HTTPS certificates

If a server certificate expired or is about to expire this will be shown in the **status** column or in the **Configuration** tab under **Security** for CA certificates.

MAC address	Status	Address	Model	Firmware	Server	HTTPS
ACCC8E3BABC	Certificate about to expire	172.25.193.66	AXIS M3027	6.50.1.2	PCREMYJ1	Enabled
ACCC8E0C6636	Certificate has expired	172.25.193.69	AXIS P3365	6.50.1.2	PCREMYJ1	Enabled
ACCC8E68CFD4	Certificate about to expire	172.25.193.75	AXIS M3048-P	7.15.2.1	PCREMYJ1	Enabled

Server Certificate about to expire or expired in status column



How long time before expiration the warning should come is configurable in **Configuration** tab under **Security**. A system alarm will be triggered if a CA certificate is or will be expired. If AXIS Device Manager has been configured as a **Certificate Authority**, AXIS Device Manager generated server certificates will automatically be renewed seven days before the expiration warning is configured to appear. This task is done during the nightly jobs. If you want to renew/update a certificate manually, follow the same steps as enabling HTTPS.

Special handling of devices with firmware 7.20 and above

By default, Axis devices with firmware 7.20 (and above) allow **HTTP & HTTPS** connections and are pre-configured in production with a self-signed certificate.



Before adding such device to AXIS Device Manager, make sure “Ignore certificate validation” is selected (default state = selected) in the **Configuration** tab under **Security**. This is because AXIS Device Manager can contact the device with HTTPS but cannot verify the certificate and won’t be able to add it to the system.

If a Certificate Authority has not been configured in AXIS Device Manager (step 1 on this document), you cannot install your own server certificates manually without first removing the

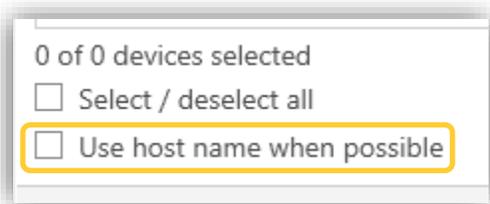
default certificate (since AXIS Device Manager only allows one server certificate per device, and the default certificate qualifies as both, client and server certificate).

If a Certificate Authority has been configured in AXIS Device Manager in step 1 (root CA or intermediate CA), it is not required to remove the self-signed certificate on the device because AXIS Device Manager will know the certificate which needs to be used is the one just generated.

By default, devices with 7.20 and above allow "HTTP & HTTPS", which means an exclusive HTTPS connection will be available after Enabling HTTPS in AXIS Device Manager.

Limitations

- Non-default ports (other than 443) are not supported.
- All certificates in an install batch must have same passphrase.
- If a device has HTTPS active and an already-uploaded certificate only containing the hostname (i.e. not an IP address), then:
 - Automatic discovery: It is possible to find and add the device as long as "use hostname when possible" is checked. If it is not checked, the device cannot be added.
 - IP range discovery: It is not possible to find or add the device, regardless of the "use hostname when possible" checkbox, since IP range discovery doesn't handle any hostname.
 - Add device from address: It is possible to add the devices as long as the hostname is entered in the Address field, not the IP.



Use hostname checkbox mentioned in previous section

- Certificate operations over unencrypted channels, i.e. "Basic" are not supported. Devices should be set to "Encrypted & unencrypted" or "Encrypted only" to allow "Digest" communication.
- HTTPS cannot be enabled on the AXIS T85 PoE+ Network switch series.