# HOW TO.

## AXIS Device Manager

## IEEE 802.1X Certificate management

September 4, 2018
Rev. 1.1

# Introduction

IEEE 802.1X is an IEEE Standard for port-based Network Access Control. It provides an authentication mechanism to devices wishing to attach to a LAN.

IEEE 802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. In our case, the supplicant is an Axis network device that wishes to attach to the LAN. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

This guide explains how to manage IEEE 802.1X EAP-TLS certificates from AXIS Device Manager.

AXIS Device Manager can help the user to either import or generate, and then distribute client certificates and authentication certificates on the Axis network devices as well as enabling IEEE 802.1X EAP-TLS.

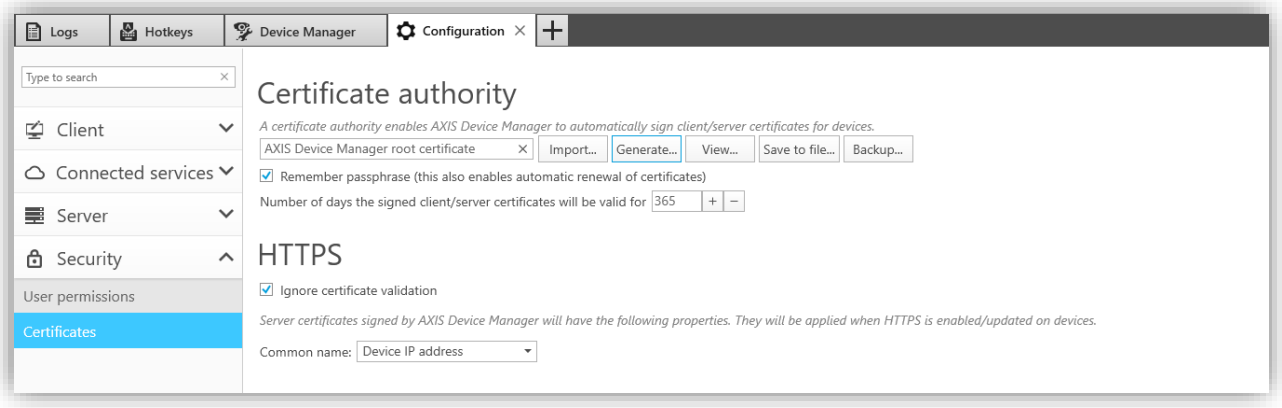
This configuration has been tested with AXIS Device Manager version 5.03 and devices with firmware 6.50.2.1 and 7.30.1.

**Requirements:** To use IEEE 802.1X certificates, devices require firmware 5.50, or 1.25 for Access control and Audio products.

**Important: 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.**

## Step 1 Choose Certificate Authority

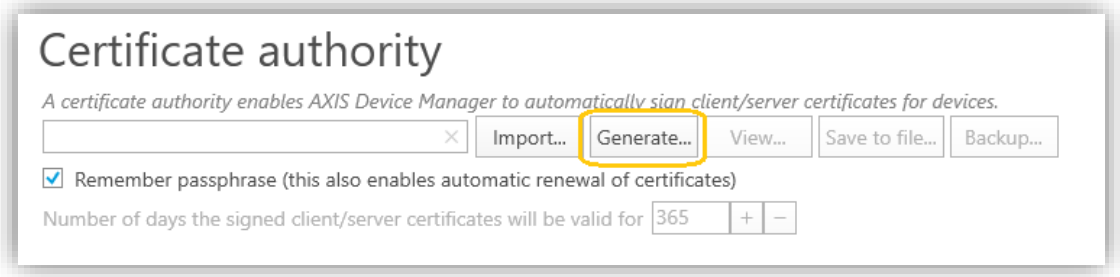
In the AXIS Device Manager **Configuration** tab, go to Security > Certificates.




### 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 client 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 client certificates), click Generate… and enter a Passphrase.
For increased security, it is recommended not to select "Remember passphrase".

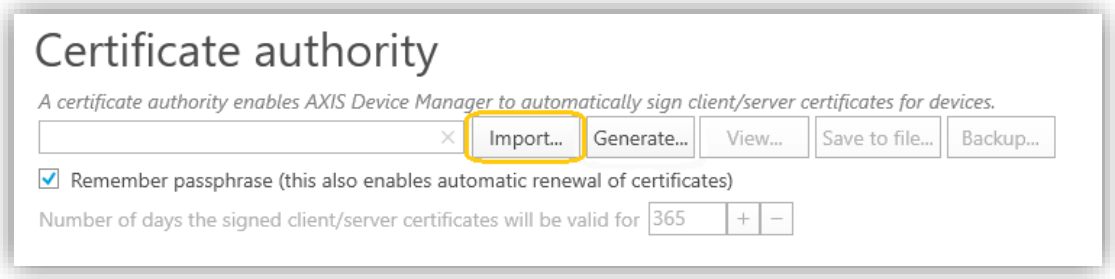



Once generated, click **Save to file**… and save **ADM_root_certificate.crt**. This certificate can be provided to any third-party application in order to trust the client/server certificate.

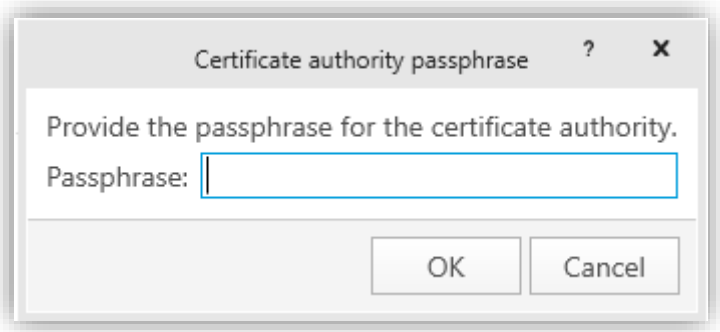
### AXIS Device Manager as Intermediate Certificate Authority (CA)

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 client 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”. You will be asked to enter the passphrase for this certificate:



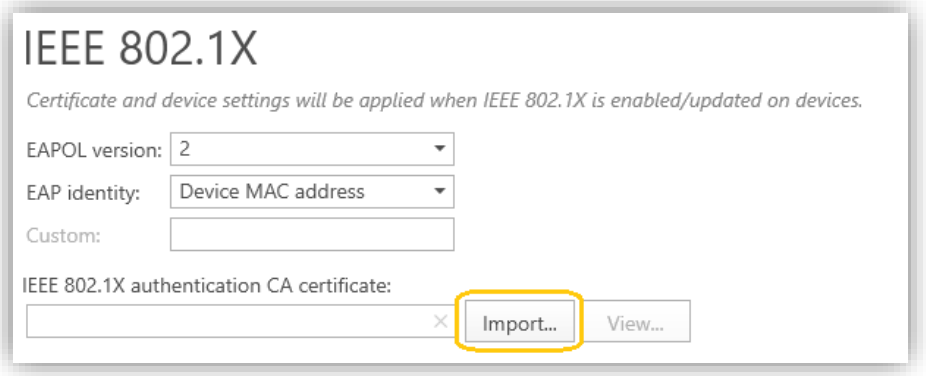

## Step 2 Select the Authentication CA certificate

A certificate for the authentication can either be sourced externally e.g. from the IEEE 802.1X **authentication server,** or directly from **AXIS Device Manager**.

In the case where the authentication CA certificate is from AXIS Device Manager, use the ‘save to file…’ option of the Certificate Authority to save a local copy of the certificate and its public key.

Using the locally saved copy of the CA certificate as the authentication certificate, or the authentication certificate obtained from the authentication server.

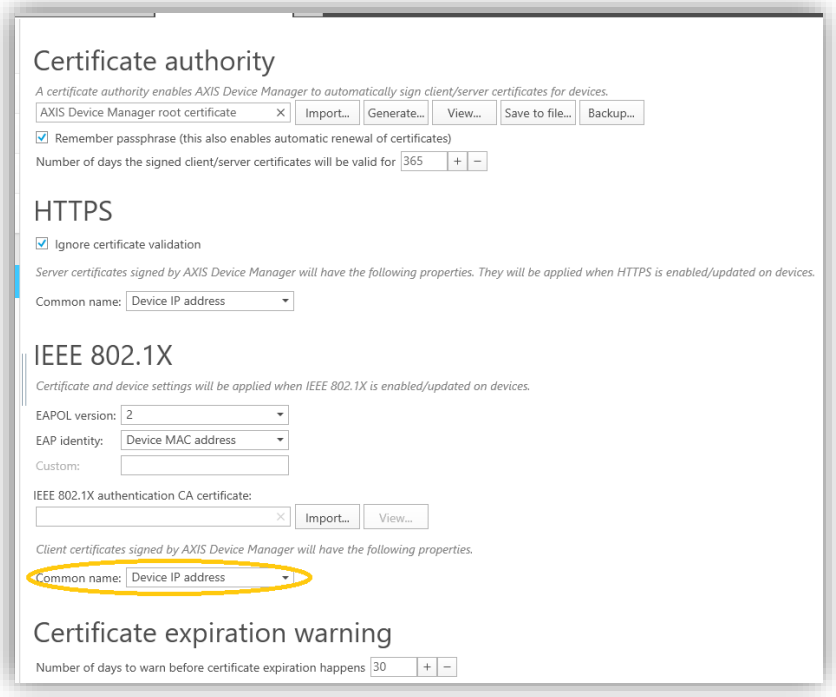
The certificate should be (re)imported in AXIS Device Manager in the IEEE 802.1X section, and the EAPOL version and EAP identity specified according to the system:




Supported format for the **IEEE 802.1X authentication CA certificate** are *.cer* and *.crt*. This certificate will be installed on each Axis device and used to verify the authentication server.

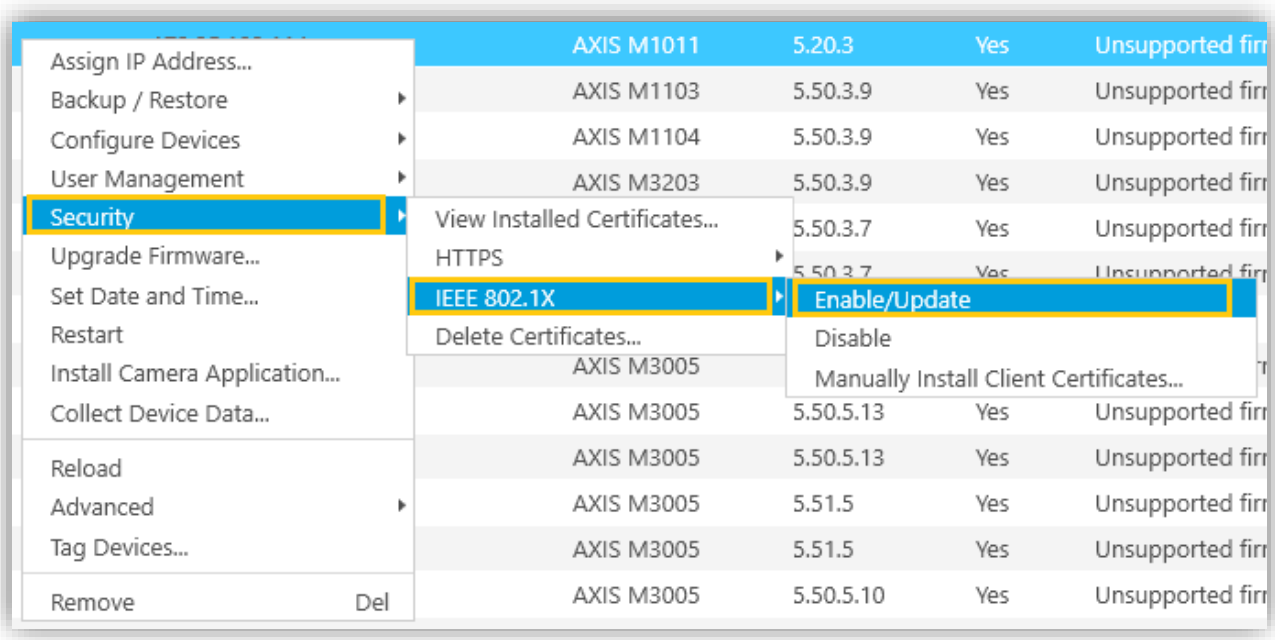
## Step 3 Select client certificate common name

Client certificates common name should be selected before enabling IEEE 802.1X on the devices.



## Step 4 Enable/Update IEEE 802.1X - Upload certificates

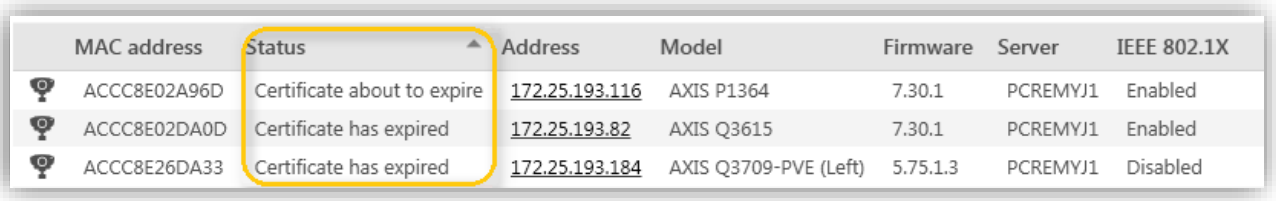
In the Device Manager tab, right-click on the device(s) and go to Security > IEEE 802.1X > Enable/Update.



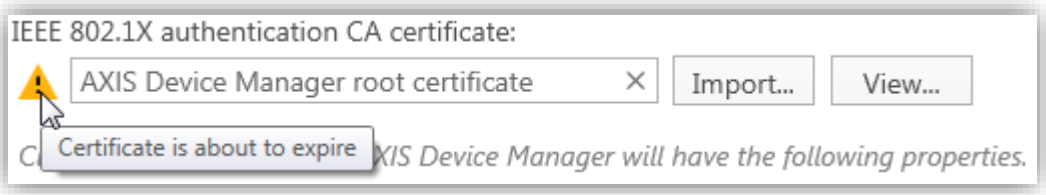

All the selected devices should now be configured to support communication on the IEEE 802.1X network.

## Step 5 Update/renew IEEE 802.1X certificates

If a client certificate expired or is about to expire this will be shown in the **status** column or in the **Configuration** tab under **Security** for IEEE 802.1X authentication CA certificates.




*Client Certificate about to expire or expired in status column*



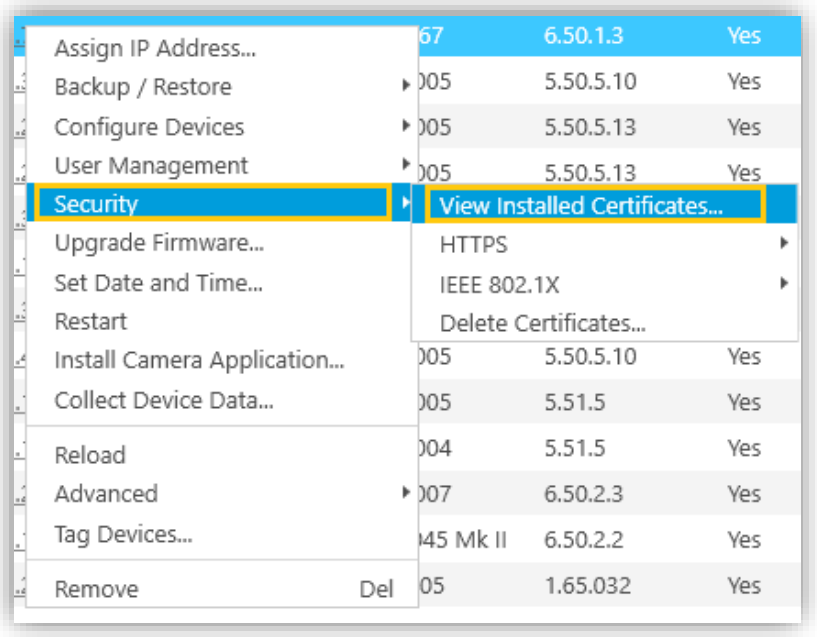

*IEEE 802.1X authentication CA certificate about to expire*

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

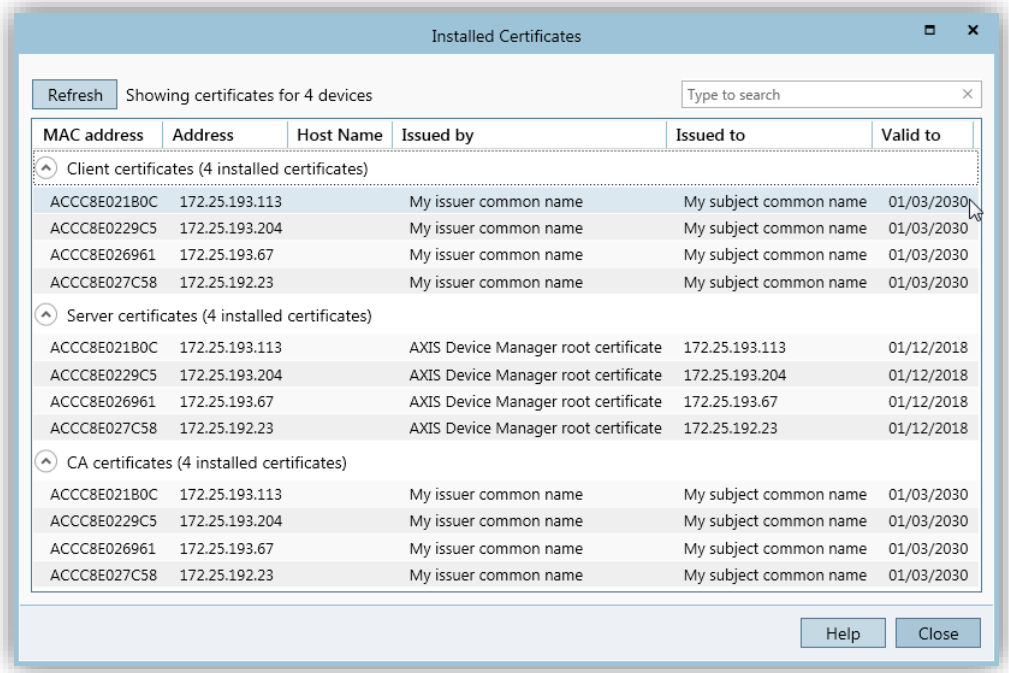
If you want to renew/update a certificate manually, follow the same steps as enabling IEEE 802.1X.

## List installed certificates on devices

To list all certificates installed on one or several devices, select the device(s), right-click and go to *Security* > *View Installed Certificates*.

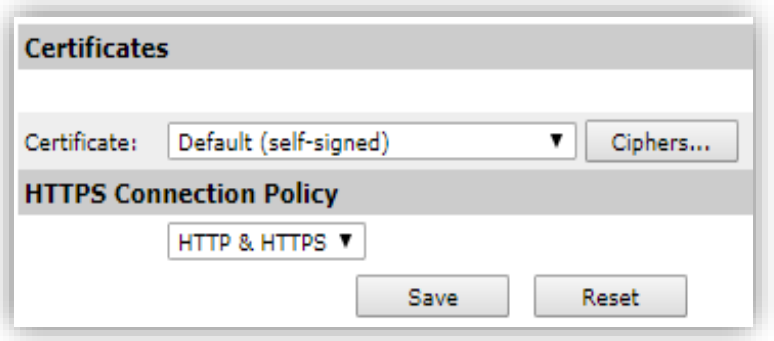



This will list all installed certificates on the devices (client/server and CA certificates).



## 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.

You also need to delete the self-signed certificate before manually uploading your own client certificate because AXIS Device Manager only allows one client certificate per device, and the default self-signed certificate qualifies as both, client and server certificate.

## Limitations

- All client certificates in a single install batch must have same passphrase.
- Supported formats for Clients Certificates are *.pfx* and *.p12*
- For devices with several network adapters (such as wireless cameras), IEEE 802.1X can only be enabled for the first adapter, typically the wired connection.
- Devices missing parameter "*Network.Interface.I0.dot1x.Enabled*" are not supported (e.g. AXIS P39 Series, T85 Series and T87 Video Decoder).
- 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.
- Make sure the time on the Axis Devices is synchronized with other devices on the network (Video Management Software, AXIS Device Manager, other servers).
- Note that If AXIS Device Manager is not configured with a Certificate Authority, the client certificates need to be manually uploaded to the devices.
    - When uploading multiple client certificates to several devices, if a device's entire FQDN, MAC address or IP address is found somewhere in the subject common name field of the certificate, it is considered a match for the device. A match must be unique.
    - There can only be a single client certificate on each device. If no unique match is found when uploading several client certificates, enabling IEEE 802.1X via AXIS Device Manager will fail. This limitation exists so it is always clear which certificate is used when enabling IEEE 802.1X.