HOW TO

AXIS Device Manager

AXIS Device Manager
IEEE 802.1X Certificate distribution

Created: December 01, 2017
Last updated: December 01, 2017
Rev: 1.0

1 Please note that AXIS does not take any responsibility for how this configuration may affect your system. If the modification fails or if you get other unexpected results, you may have to restore the factory default settings as described in the User's manual.

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.

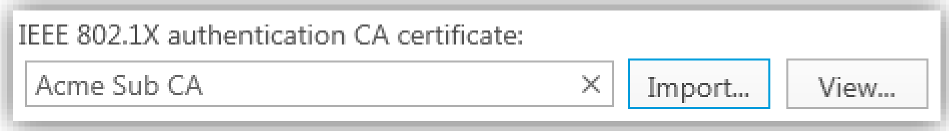
This guide explains how to distribute IEEE 802.1X certificates from AXIS Device Manager.
AXIS Device Manager can help the user to upload the CA and client certificates on the Axis network devices and enabled IEEE 802.1X.

This configuration has been tested with AXIS Device Manager version 5.00 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 Import CA certificate

In the AXIS Device Manager **Configuration** tab, go to *Security* > *Certificates*.
Choose your **EAPOL version** and **EAP identity**. Both parameters are defined by your Radius server.
The **IEEE 802.1X authentication CA certificate** must be an external CA certificate, generated by your root CA or another intermediate CA.



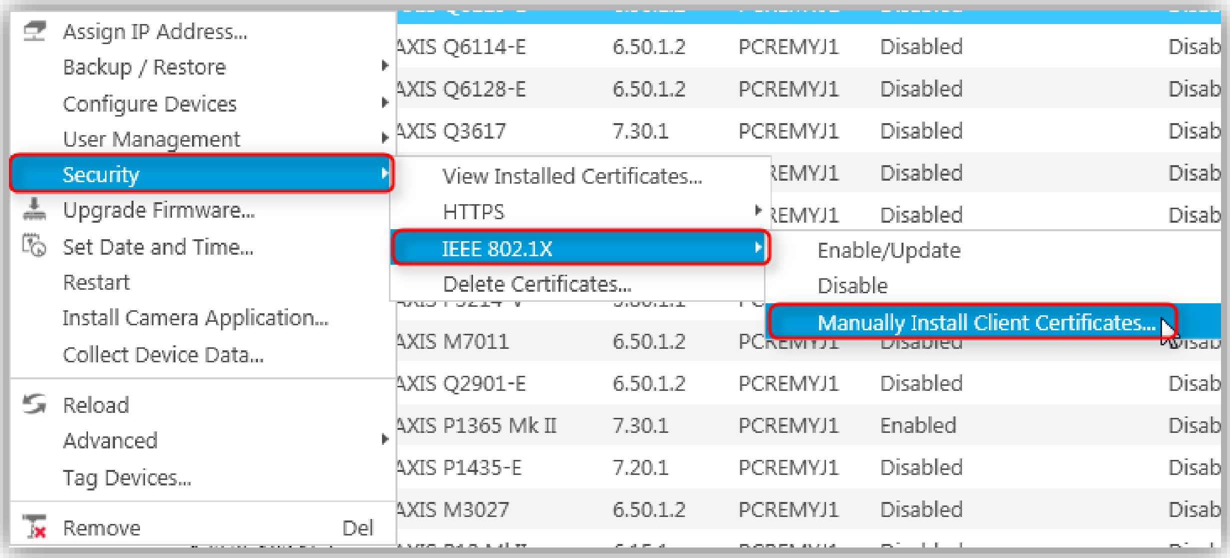
IEEE 802.1X authentication CA certificate:

Acme Sub CA

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.

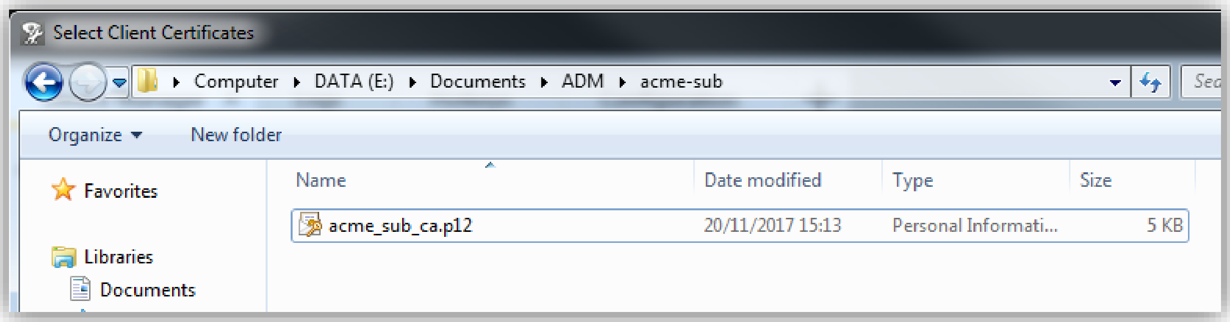
Step 2 manually install Client Certificates

The client certificate has to be created outside AXIS Device Manager (by another CA) and then installed on the device(s) from AXIS Device Manager:
In the **Device Manager** tab, right-click on the device(s) and go to *Security* > *IEEE 802.1X* > *Manually Install Client Certificates…*



AXIS Q6114-E	6.50.1.2	PCREMYJ1	Disabled	Disab
AXIS Q6128-E	6.50.1.2	PCREMYJ1	Disabled	Disab
AXIS Q3617	7.30.1	PCREMYJ1	Disabled	Disab
		REMYJ1	Disabled	Disab
		REMYJ1	Disabled	Disab
AXIS M7011	6.50.1.2	PCREMYJ1	Disabled	Disab
AXIS Q2901-E	6.50.1.2	PCREMYJ1	Disabled	Disab
AXIS P1365 Mk II	7.30.1	PCREMYJ1	Enabled	Disab
AXIS P1435-E	7.20.1	PCREMYJ1	Disabled	Disab
AXIS M3027	6.50.1.2	PCREMYJ1	Disabled	Disab

Select your client certificate(s) created by your CA:

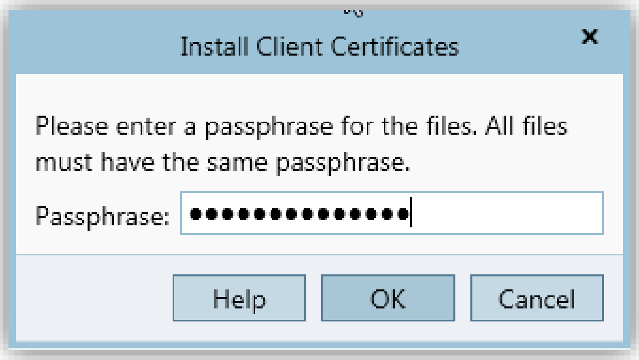

Select Client Certificates
Computer ▸ DATA (E:) ▸ Documents ▸ ADM ▸ acme-sub
Sea
Organize ▾
New folder
Favorites
Libraries
Documents

Name	Date modified	Type	Size
acme_sub_ca.p12	20/11/2017 15:13	Personal Informati...	5 KB

Remarks:

- Supported formats for Clients Certificates are *.pfx* and *.p12*
- There can only be a single client certificate on each device. If several client certificates are uploaded to a device, enabling IEEE 802.1X will fail. This limitation exists so it is always clear which certificate is used when enabling IEEE 802.1X.
- 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.

Enter the passphrase of the client certificate:



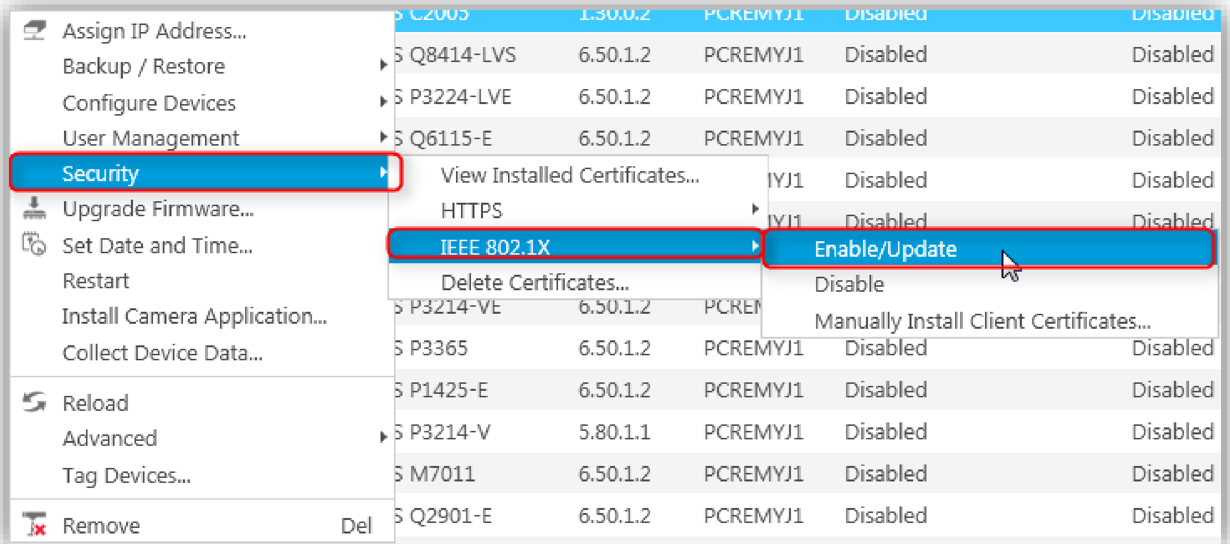
Please enter a passphrase for the files. All files must have the same passphrase.

Passphrase: ••••••••••••••

Step 3 Enable/Update IEEE 802.1X - Upload CA certificate

Prior to enabling IEEE 802.1X, a device needs to have a **client certificate** already uploaded (from step 2) and an **IEEE 802.1X authentication CA certificate** needs to be imported into AXIS Device Manager (step 1).

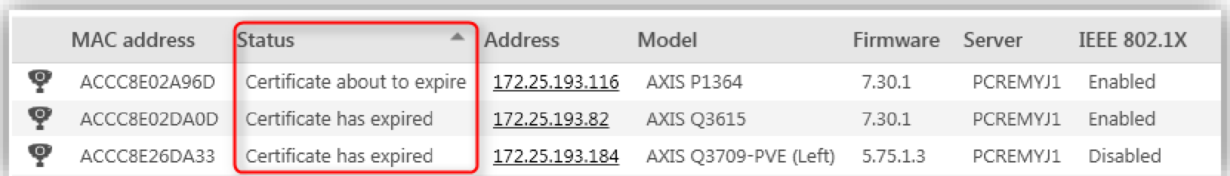
In the **Device Manager** tab, right-click on the device(s) and go to *Security > IEEE 802.1X > Enable/Update.*



S C2005	1.30.0.2	PCREMYJ1	Disabled	Disabled
S Q8414-LVS	6.50.1.2	PCREMYJ1	Disabled	Disabled
S P3224-LVE	6.50.1.2	PCREMYJ1	Disabled	Disabled
S Q6115-E	6.50.1.2	PCREMYJ1	Disabled	Disabled
		YJ1	Disabled	Disabled
		YJ1	Disabled	Disabled
S P3214-VE	6.50.1.2	PCREM		
S P3365	6.50.1.2	PCREMYJ1	Disabled	Disabled
S P1425-E	6.50.1.2	PCREMYJ1	Disabled	Disabled
S P3214-V	5.80.1.1	PCREMYJ1	Disabled	Disabled
S M7011	6.50.1.2	PCREMYJ1	Disabled	Disabled
S Q2901-E	6.50.1.2	PCREMYJ1	Disabled	Disabled

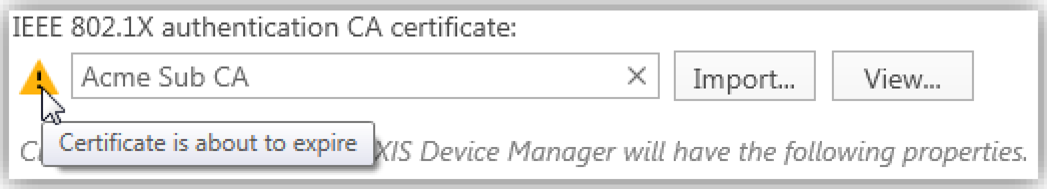
Step 4 Update/renew IEEE 802.1X certificates

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.



	MAC address	Status	Address	Model	Firmware	Server	IEEE 802.1X
	ACCC8E02A96D	Certificate about to expire	172.25.193.116	AXIS P1364	7.30.1	PCREMYJ1	Enabled
	ACCC8E02DA0D	Certificate has expired	172.25.193.82	AXIS Q3615	7.30.1	PCREMYJ1	Enabled
	ACCC8E26DA33	Certificate has expired	172.25.193.184	AXIS Q3709-PVE (Left)	5.75.1.3	PCREMYJ1	Disabled

Client Certificate about to expire or expired in status column



IEEE 802.1X authentication CA certificate: Acme Sub CA

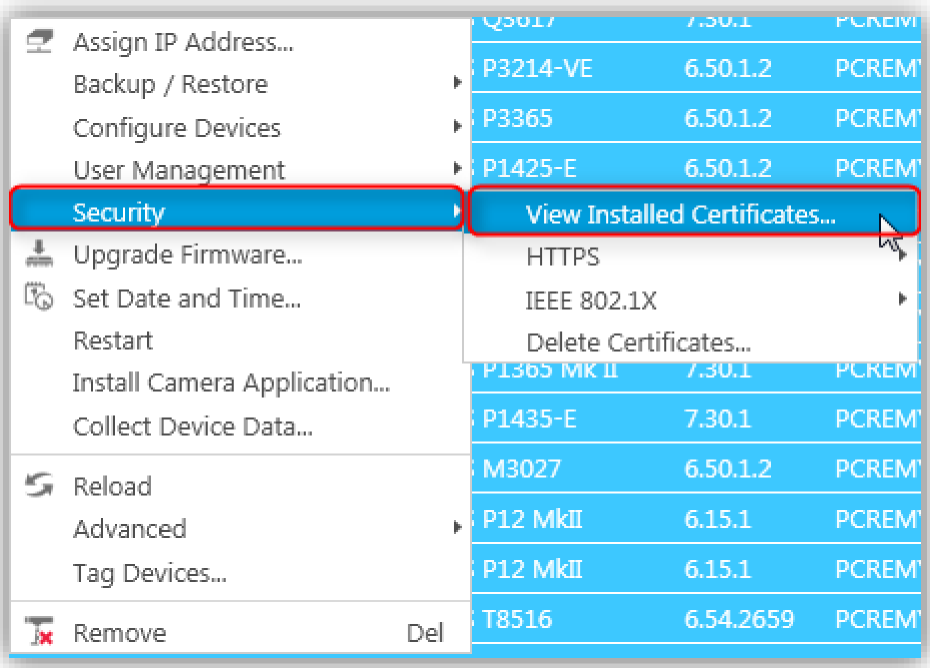
Import...
View...
Certificate is about to expire
C
XIS Device Manager will have the following properties.

IEEE 802.1X authentication CA certificate about to expire

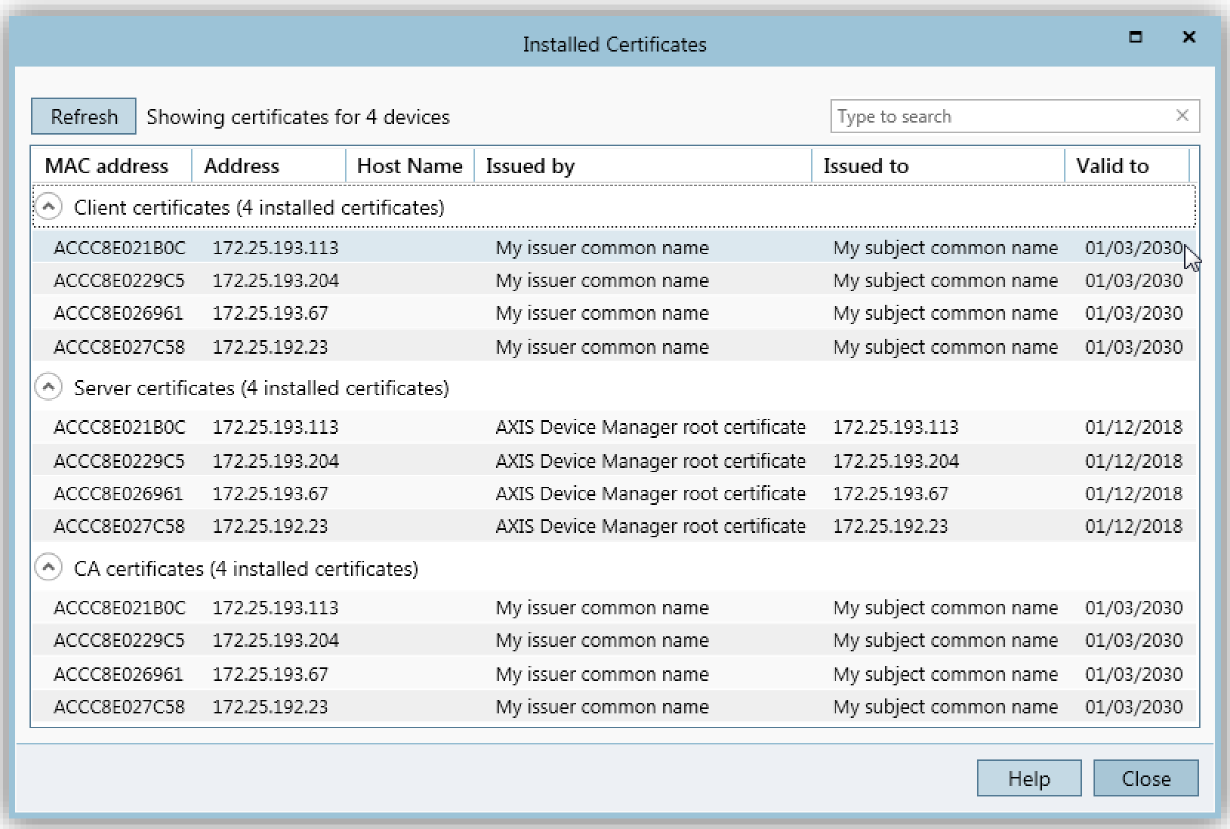
How long time before expiration the warning should come is configurable in **Configuration** tab under **Security**. A system alarm will be triggered if a certificate is or will be expired. A certificate needs to be renewed manually by the user. This can be done by following the same steps as enabling IEEE 802.1X (steps 1-2-3).

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).

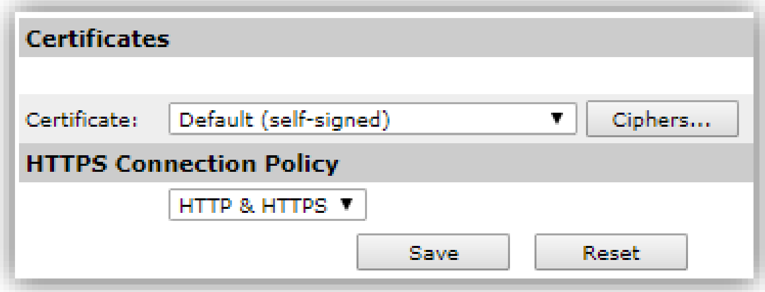


Showing certificates for 4 devices

MAC address	Address	Host Name	Issued by	Issued to	Valid to
Client certificates (4 installed certificates)					
ACCC8E021B0C	172.25.193.113		My issuer common name	My subject common name	01/03/2030
ACCC8E0229C5	172.25.193.204		My issuer common name	My subject common name	01/03/2030
ACCC8E026961	172.25.193.67		My issuer common name	My subject common name	01/03/2030
ACCC8E027C58	172.25.192.23		My issuer common name	My subject common name	01/03/2030
Server certificates (4 installed certificates)					
ACCC8E021B0C	172.25.193.113		AXIS Device Manager root certificate	172.25.193.113	01/12/2018
ACCC8E0229C5	172.25.193.204		AXIS Device Manager root certificate	172.25.193.204	01/12/2018
ACCC8E026961	172.25.193.67		AXIS Device Manager root certificate	172.25.193.67	01/12/2018
ACCC8E027C58	172.25.192.23		AXIS Device Manager root certificate	172.25.192.23	01/12/2018
CA certificates (4 installed certificates)					
ACCC8E021B0C	172.25.193.113		My issuer common name	My subject common name	01/03/2030
ACCC8E0229C5	172.25.193.204		My issuer common name	My subject common name	01/03/2030
ACCC8E026961	172.25.193.67		My issuer common name	My subject common name	01/03/2030
ACCC8E027C58	172.25.192.23		My issuer common name	My subject common name	01/03/2030

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.



Certificates

Certificate: Default (self-signed) ▼

HTTPS Connection Policy

HTTP & HTTPS ▼

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

- AXIS Device Manager cannot generate or sign client or CA certificates. Is can only distribute client certificates to one or several devices as well as CA certificates if they have been imported beforehand.
- All client certificates in a single install batch must have same passphrase.
- 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.
- Importing a Certificate Authority (under *Configuration tab* > *Security* > *Certificates*) will only change the HTTPS certificate management behaviour. It has no effect on the IEEE 802.1X certificate distribution function. For more information regarding HTTPS, refer to our *AXIS Device Manager HTTPS certificate management* guide available on axis.com
- Make sure the time on the Axis Devices is synchronized with other devices on the network (Video Management Software, AXIS Device Manager, other servers).