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.

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

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:
**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.

**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.

**Client 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 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).
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

- AXIS Device Manager cannot generate or sign client or CA certificates. It 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).