HOW TO.

Configure AXIS cameras via AXIS Device Manager to support IEEE 802.1X authentication with FreeRADIUS

December 27, 2019
Rev. 1.3

Introduction

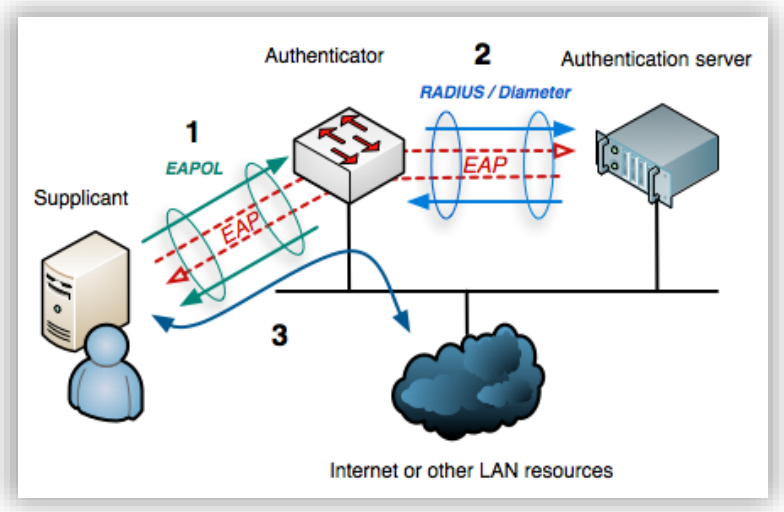
This document provides basic instructions as to how to use AXIS Device Manager to configure AXIS cameras to support IEEE 802.1X authentication.

Utilizing IEEE 802.1X authentication between the cameras and the switch benefits the system in that it provides additional security, particularly for those ethernet points which may terminate outside of the physical boundaries of the premises and are thus more vulnerable to physical tampering.

Also, even if an enterprise already utilizes Active Directory for its employee users, the enterprise may not want to integrate the camera network into that authentication solution.

By running a FreeRADIUS server, the investment costs and the effort to implement an isolated authentication solution are kept low while still providing substantial security to the camera network without the need for an existing Active Directory setup. Also the camera system can be kept not only logically separate, but physically separate from other IT infrastructure.

A standard IEEE 802.1X setup: Supplicant, Authenticator and Authentication Server:



In this guide the Authentication server is a Raspberry Pi running Raspbian Stretch (but could be many of the available Linux distributions running on dedicated hardware or as a virtual machine) and an instance of the 'FreeRADIUS' IEEE 802.1X authentication server made available by NetworkRadius.

The Authenticator is the managed switch: an AXIS T85 series switch.

The supplicant is of course the AXIS camera(s).

Prerequisites

A familiarity with Linux, IEEE 802.1X and AXIS devices is assumed.

Needed:

- One or more AXIS device/camera *[supplicant(s)]*

- A managed network switch that has support for IEEE 802.1X EAP-TLS
  Here an AXIS T8516 switch is utilized *[authenticator]*

NOTE: if you are not using an AXIS switch, please be sure to check that it supports EAP-TLS specifically as part of its IEEE802.1X support.

- FreeRADIUS server *[authentication server]*

- AXIS Device Manager (ADM) *[manages authentication and supplicant certificates]*

Important! *1. The FreeRADIUS server, cameras, switch and ADM instance should ideally all synchronize date and time with the an NTP server with correct time zone and daylight savings settings in order to avoid authentication issues.*

Important! *2. The certificates used in these instructions are for demonstration only and should be replaced by appropriate operational certificates once the initial system set up is completed.*

Overview

1. Setup a FreeRADIUS server.

Administrator access to a FreeRADIUS server is needed. See: https://freeradius.org/

Determine or set the IP address of the server as this information will be needed later:

```
>ip a
```

will display the current IP assigned.

Or to set the IP to a static IP address, edit the **/etc/dhcpcd.conf** file to contain the following entry:

```
interface eth0
static ip_address = <IPaddr>
```

Where **<IPaddr>** is the IP of the Authentication Server.

If installing a new instance, the following commands should help (make sure the server has access to the internet):

```
>sudo apt-get update
```

```
>sudo apt-get install freeradius
```

See also: http://deployingradius.com

Don't start the server just yet! But note the following:

Useful commands

Start server: `>sudo freeradius` or `>sudo freeradius -XXX` to display debug info

Restart server as deamon: `>sudo service freerad restart`

Stop server as deamon: `>sudo service freerad stop`

2. Certificates.

The FreeRADIUS server needs a server certificate. This needs to be signed by a Trusted CA (such as Symantec or LetsEncrypt), a private CA or a self-signed certificate. For testing purposes, FreeRADIUS includes a script that uses OpenSSL to generate a private CA certificate, a signed server certificate and a signed client certificate. We will use the CA and server certificate.

Note that by default these certificates will have a 2-month expiration time. For production systems it is recommended to replace these certificates with appropriate production certificates. Navigate to the directory containing the script:

```
>cd /etc/freeradius/3.0/certs
```

The script can either be run manually using the command below, or it will be automatically executed the first time the FreeRADIUS server is started in debug mode (if no other certificates are present in that directory):

```
>sudo make
```

There should now be a number of files ending with pem, key, csr in the /certs directory. Those of interest are:

```
/etc/freeradius/3.0/certs/ca.pem
/etc/freeradius/3.0/certs/server.crt
/etc/freeradius/3.0/certs/server.key
```

In order to keep track of certificates it is a good idea to have descriptive names. Make a copy of **ca.pem** with different name.

```
>sudo cp ca.pem RADIUS_CA.crt
```

This file needs to be copied to the Windows PC that hosts AXIS Device Manager.
We will also create a file the holds the trusted CA certificate that signs the client certificates. In our case this will be the AXIS Device Manager root certificate. We create this file as a placeholder for the certificate that ADM creates to be stored in and referred to by the RADIUS config file:

```
>sudo touch trusted_CA.pem
```

In order for the RADIUS server to be able to read the certificate files, the user rights for user freerad need to be applied to the server and CA files as follows:

```
chown freerad /etc/freeradius/3.0/certs/trusted_CA.pem
chown freerad /etc/freeradius/3.0/certs/server.crt
chown freerad /etc/freeradius/3.0/certs/server.key
```

We will later copy the ADM root certificate to **trusted_CA.pem** after we configured AXIS Device Manager.

3. EAP-TLS configuration for RADIUS.

We need to configure FreeRADIUS to enable TLS and identify which certificates to use:

```
>sudo nano /etc/freeradius/3.0/mods-available/eap
```

Under section **eap** set

```
default_eap_type = tls
```

Under section **tls-config tls-common** set

```
private_key_password = whatever (as specified in the server.cnf file)
private_key_file = /etc/freeradius/3.0/certs/server.key
certificate_file = /etc/freeradius/3.0/certs/server.crt
ca_file = /etc/freeradius/3.0/certs/trusted_CA.pem
```

Note: *in this example the server key is encrypted using the password as defined in the config file, however if your own key file is not encrypted, comment out the 'private_key_password' line above.*

4. Add authenticator (client).

The RADIUS server, needs to know all the trusted 'clients' (Where 'clients' are the managed switch(es) in this case). In `directory` **/etc/freeradius/3.0/** `rename` the existing **client.conf** and save for future reference:

```
>sudo mv clients.conf clients_original.conf
```

Then create a new **clients.conf**:

```
>sudo touch clients.conf
```

Copy, the text below into that new **client.conf** file, then edit the bold items, and then save it:

```
client localhost {
      ipaddr      = 127.0.0.1
      proto       = *
      secret      = testing123
      nas_type    = other     # localhost isn't usually a NAS...
}

client axis_switch {
      ipaddr      = <IPaddr>
      secret      = password
}
```

Where **<IPaddr>** should be the IP of the switch such as: 10.11.12.13/24
And the **password** is as specified in the Switch setup in step **8.c**.

5. Import CA Certificates to ADM.

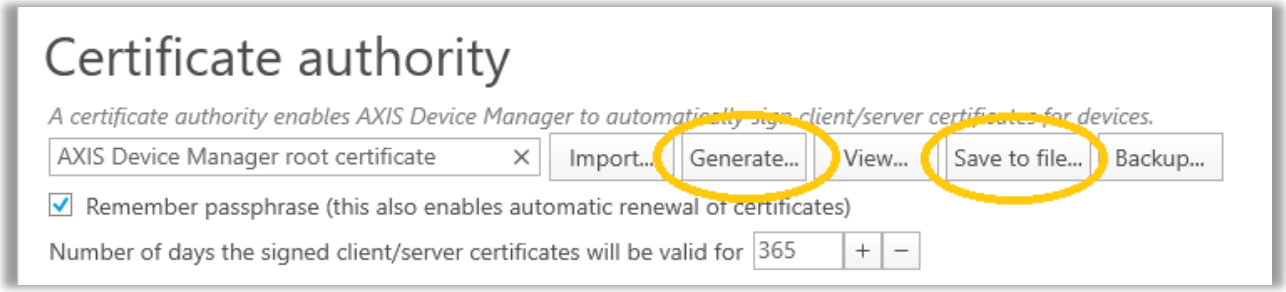
In our example we use two different CA (it is also possible to use the same CA for both purposes):

- One that signs the RADIUS server. This was generated by the script included in the **/certs** directory and copied to **RADIUS_CA.crt**.

- The other CA is AXIS Device Manager root certificate that issues client certificates for cameras.

Launch **Axis Device Manager client** and select:

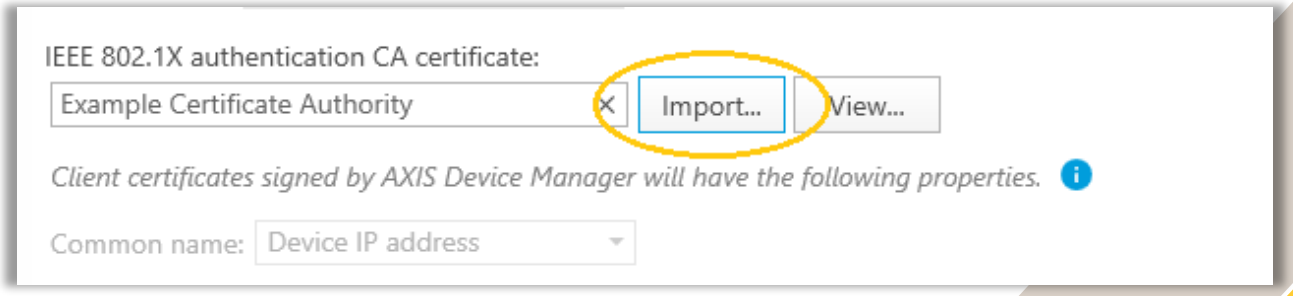
Configuration tab > **Security** > **Certificates** > "**Certificate Authority**" > "**Generate…**" …and add a memorable passphrase for the certificate. Then… "**Save to file**…" and save it as **ADM_root_certificate.crt**



Now copy the content of **ADM_root_certificate.crt** to the empty **/etc/freeradius/3.0/certs/trusted_CA.pem** we created earlier.

Note that **trusted_CA.pem** can have a list of multiple CA certificates that are trusted to issue client certificates, however, it is not recommended add public CA certificates to the list because external parties could potentially get that CA to issue client certificates for your system.

In Axis Device Manager
Configuration > **Security** > **Certificates** > **IEEE 802.1X auth. CA certificate** > **"Import…**".
Locate the file **RADIUS_CA.crt** that we previously copied from the RADIUS server and import it.



6. Starting the RADIUS sever.

Now we can start the RADIUS server

```
>sudo freeradius -X
```

When it has successfully initialized, the following output should be seen:

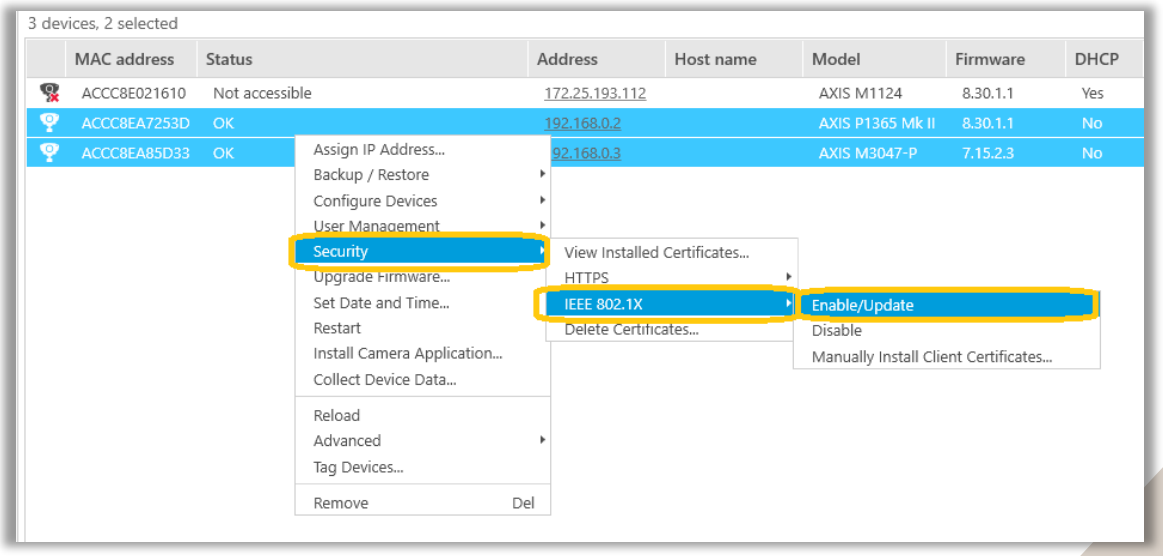
```
Tue Sep 25 17:13:45 2018 : Debug: Listening on auth address * port 1812 bound to server default
Tue Sep 25 17:13:45 2018 : Debug: Listening on acct address * port 1813 bound to server default
Tue Sep 25 17:13:45 2018 : Debug: Listening on auth address :: port 1812 bound to server default
Tue Sep 25 17:13:45 2018 : Debug: Listening on acct address :: port 1813 bound to server default
Tue Sep 25 17:13:45 2018 : Debug: Listening on auth address 127.0.0.1 port 18120 bound to server inner-tunnel
Tue Sep 25 17:13:45 2018 : Debug: Opened new proxy socket 'proxy address * port 33221'
Tue Sep 25 17:13:45 2018 : Debug: Listening on proxy address * port 33221
Tue Sep 25 17:13:45 2018 : Debug: Opened new proxy socket 'proxy address :: port 54203'
Tue Sep 25 17:13:45 2018 : Debug: Listening on proxy address :: port 54203
Tue Sep 25 17:13:45 2018 : Info: Ready to process requests
```

*See appendix for instructions describing how to set FreeRADIUS as an autostart deamon at server boot up.

7. Enabling the cameras.

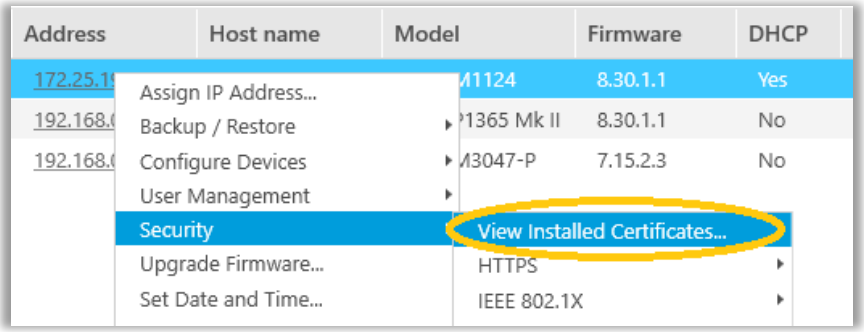
In AXIS Device Manager, moving to the **Device Management** tab, select the cameras that should have IEEE 802.1X enabled. Right click on the selection and choose:

Security > **IEEE 802.1X** > **Enable/Update**

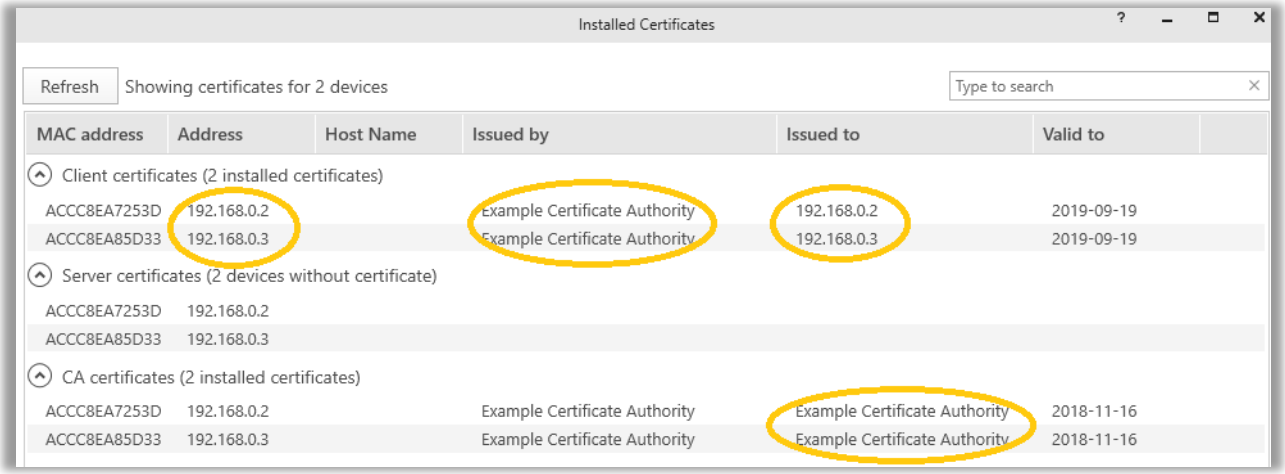


Verify the certificates (optional)

Once the task is successfully completed, the certificates uploaded to the selected cameras can be viewed as follows:



Each camera should now contain a copy of the CA (root) certificate (bottom section) as well as a device specific client certificate (top section) generated using the CA certificate imported into AXIS Device Manager in section 4.1:



8. Configuring the switch.

Login to the management console of the Axis T8516 network switch. For other managed switches you will need to adapt these instructions by referring to the relevant User Manual.

8a. Basic Config.

First set the time & date to sync via NTP and make sure the switch's IP address matches that entered in step 4 for the client config:

Basic > **Basic settings** > **TCP/IP**

Confirm the IPv4 Address is the same as entered in step 4: **clients.conf**

Then using the **Advanced** setting tab on the left-hand column of the user interface for the rest of section 8:

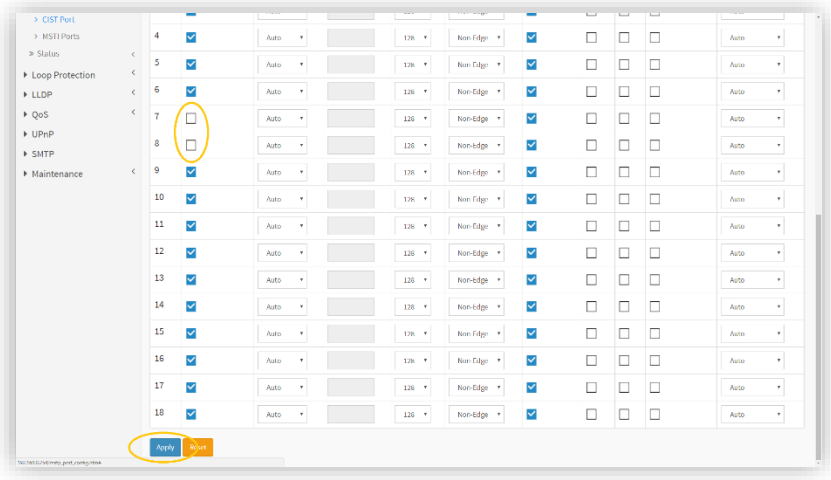
.

8b. Spanning Tree settings.

Disable the spanning tree for the ports on the Switch that will support IEEE 802.1X authentication as follows:

Spanning tree > **Configuration** > **CIST**

and then uncheck **STP Enabled** for the relevant ports (ports 7 & 8 in this example):

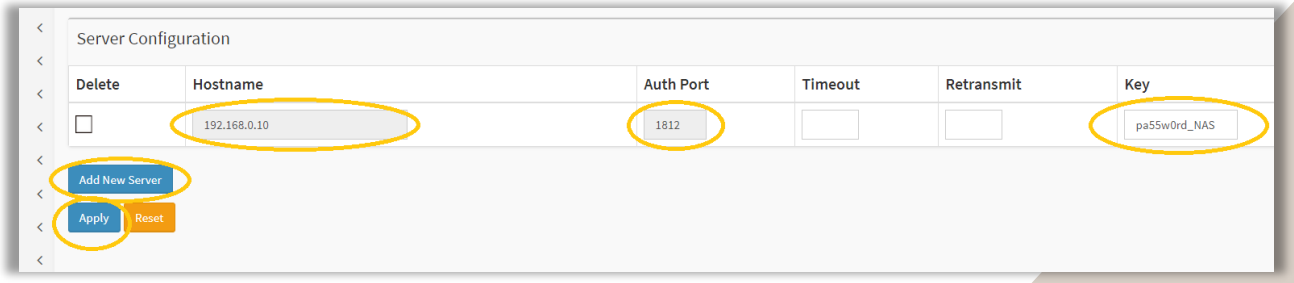


Don't forget to **Apply** the settings at the bottom of the page.

8c. Set the FreeRADIUS server details.

Configure the switch with the FreeRADIUS Server details:

Security > **Configuration** > **AAA** > **RADIUS** > **Add new server**



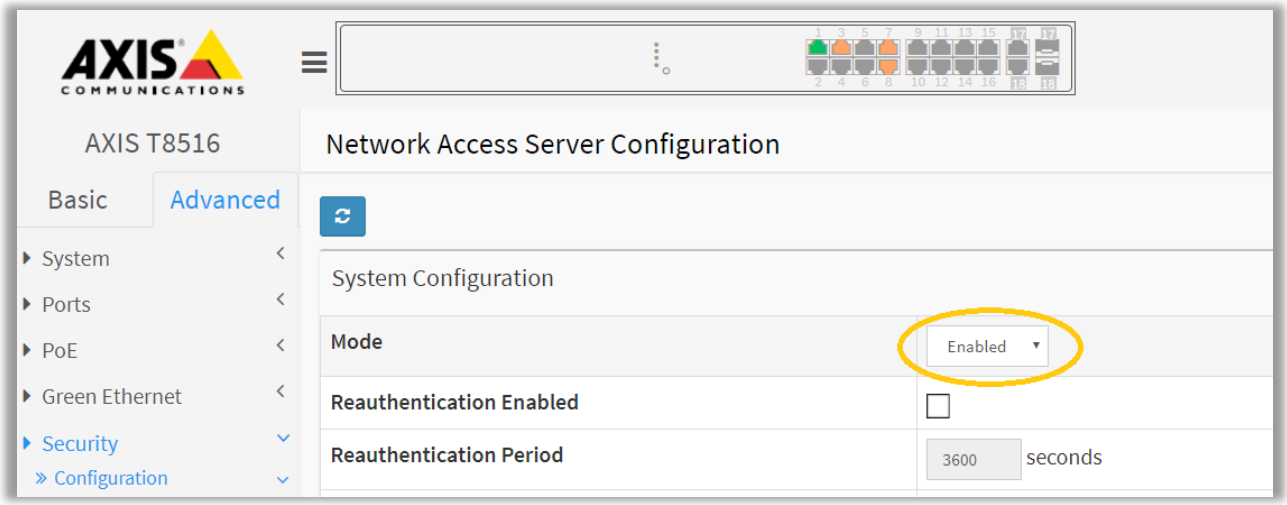
Hostname: Server IP address (as set/determined in step 1)
Auth port: 1812
Key: same **password** as entered in the **clients.conf** file in step 4

Select **Apply** to save the settings changes.

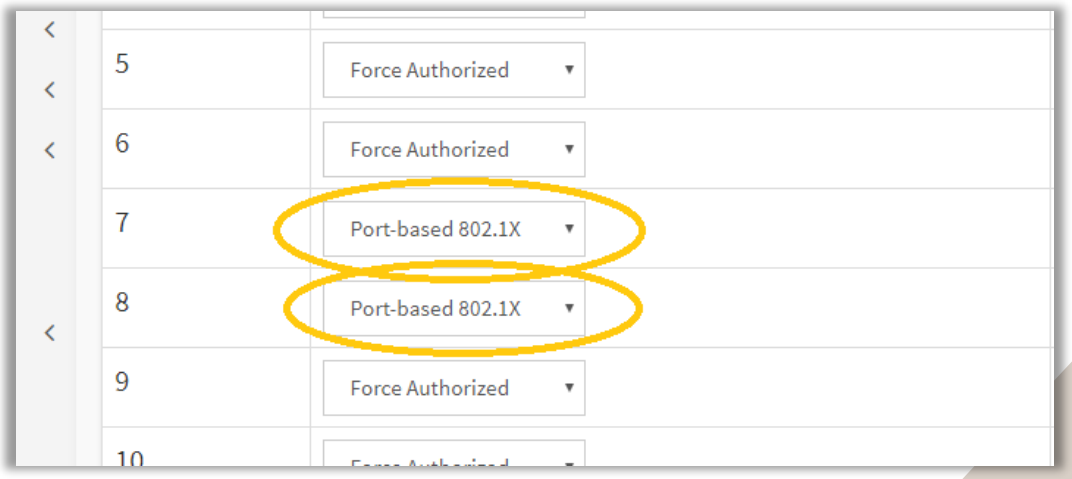
8d. Enable the IEEE 802.1X ports.

Security > **Configuration** > **Network** > **NAS**

At the top of the page set the **Mode** to **Enabled.**



Then set the **Admin State** of the ports that will use the IEEE 802.1X authentication to "**Port based 802.1X**":



Select **Apply** at the bottom of the page to save the settings.

9. Verify functionality.

To verify the authorization is functioning correctly, the easiest option is to use the switch interface, go to:

Security > **Configuration** > **Network** > **NAS**

and verify that the ports set to port authentication are now shown to be verified as shown below:

Done!

10. Other useful information.

Software/firmware versions used in the preparation of this document:

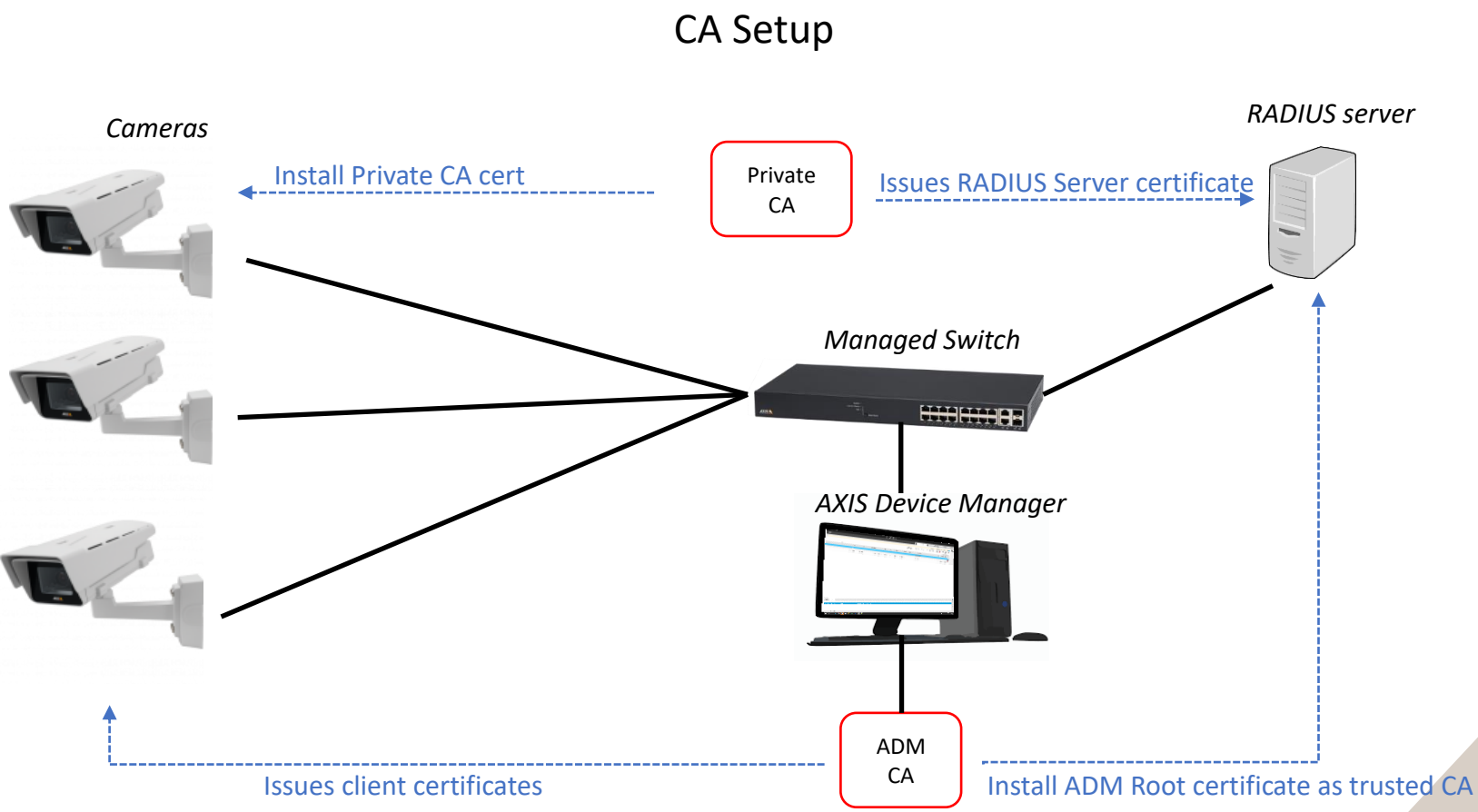
FreeRADIUS	3.0.12
AXIS Device Manager	5.03.002
T8516 firmware version	6.54.2168

FreeRADIUS troubleshooting - http://deployingradius.com/

further notes on the EAP configuration:
https://networkradius.com/doc/3.0.10/raddb/tls/tls-config_tls-common.html

How to set FreeRADIUS as an autostart deamon on the server:
https://raspberrypi.stackexchange.com/questions/8734/execute-script-on-start-up

Appendix A – Schematic Overiew.



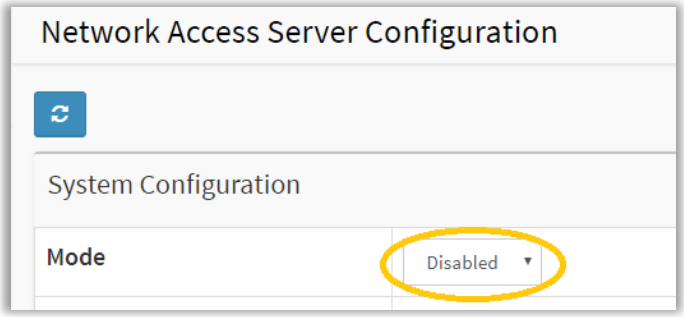
Appendix B - Certificate Revocation.

A simple way of decommissioning an existing certificate using AXIS Device Manager is as follows:

1. Disable IEEE 802.1X authentication

Log in to the Switch's management console, then select:

Advanced > **Security** > **Configuration** > **Network** > **NAS** and set **Mode** to **disabled:**

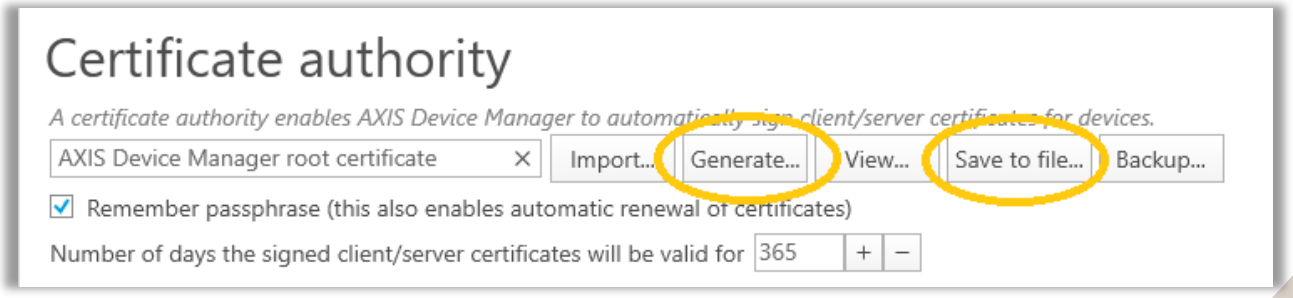


Don't forget to click **Apply** at the bottom of the page!

2. Generate a new Certificate Authority

In AXIS Device Manager, generate a new self-signed Certificate Authority:

Configuration tab > **Security** > **Certificates** > **Certificate Authority** > **"Generate…"**



Enter a memorable passphrase, and then "**Save to file**".

3. Copy the new CA to the RADIUS server

Using your favourite SHH client, replace the contents of the new certificate file just saved in ADM to the FreeRADIUS server and save the content in the **/etc/freeradius/3.0/certs/trusted_CA file**.

4. Provision cameras with new certificates

In AXIS Device Manager, using the **Device Manager** tab, select the cameras to be updated (all), then select:

Right click on the selection > **Security** > **IEEE 802.1X** > **Enable/Update**

Once that task completes in AXIS Device Manager, restart the FreeRADIUS sever:

Restart server as deamon: `>sudo service freerad restart`

OR

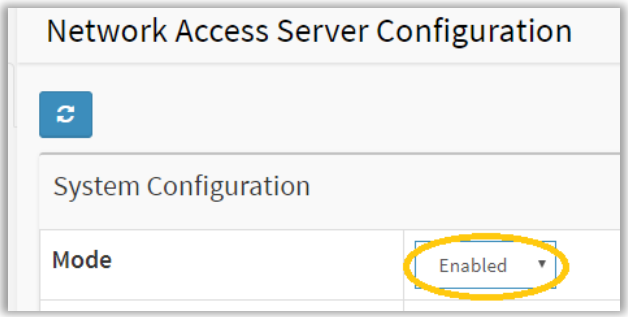
Restart server as application: `>Ctrl & C`

`>sudo freeradius -X`

5. Re-enable IEEE 802.1X authentication

Log in to the Switch's management console, then select:

Advanced > **Security** > **Configuration** > **Network** > **NAS** and set **Mode** to **enabled:**



Don't forget to click **Apply** at the bottom of the page!

Done!