Upload of HTTPS certificates

Summary

Purpose

The HTTPS certificate allows secure access to the UWP 4.0 Web App using:
https://<UWP_IP_address>
Uploading a valid HTTPS certificate:

- Enables encrypted communication (TLS)
- Prevents browser security warnings caused by default certificates
- Increases cybersecurity compliance

UWP 4.0 does not generate HTTPS certificates internally.
The certificate and private key must be generated externally and then uploaded.

Certificate types: Self-signed vs CA-issued

For HTTPS secure access, two options are available:

- Self-signed certificate: a self-signed certificate is generated and signed locally.
- CA-issued certificate: a CA-issued certificate is signed by a trusted Certification Authority

Self-signed certificate

- Generated and signed locally
- Not automatically trusted by browsers
- Suitable for standalone or isolated systems

Use when:

- The device operates in a local network
- No corporate IT security policy applies

CA-issued certificate

- Signed by a trusted Certification Authority
- Automatically trusted (if CA is trusted)
- Managed within a corporate PKI

Use when:

- The device is integrated into a corporate network
- Remote access or internet exposure is involved
- Company IT policies require trusted certificates

IMPORTANT:
The certificate type must be aligned with the customer's IT security architecture and internal cybersecurity policies.

Certificate requirements

The following files are required:

File	Description	Format
Server certificate	Public certificate used by UWP	.crt or .pem (PEM format)
Private key	Private key associated with the certificate	.key (PEM format)

Generate a self-signed HTTPS certificate

This procedure is recommended for local installations without a corporate Certification Authority.

Prerequisites

- OpenSSL installed on PC
- Administrator rights

Step 1 – Generate private key

openssl genrsa -out uwp_https.key 2048

This command generates:

uwp_https.key

Step 2 – Generate self-signed certificate

openssl req -new -x509 -key uwp_https.key -out uwp_https.crt -days 3650 -sha256

When prompted, set:

- Common Name (CN) = UWP IP address or DNS hostname
  Example:
  - 192.168.1.50
  - uwp.local

Other fields may be left blank if not required.
The command generates:

uwp_https.crt

Generated files

You must now have:

- *uwp_https.key*
- *uwp_https.crt*

These two files are required for upload.

Upload procedure

1. Access the UWP Web App
2. Open the **Main menu**
3. Select **System settings**
4. Open the **Maintenance tab**
5. Select **Upload https certificates**
6. Upload:
    - HTTPS certificate (.crt / .pem)
    - Private key (.key)
7. Save configuration
8. Reboot the system if required

After reboot, access the device using:

https://<UWP_IP>

Verification

After upload:

1. Open browser
2. Enter:

https://<UWP_IP>

3. Check certificate details in browser security panel

Verify:

- Certificate Common Name matches IP or hostname
- Certificate validity date is correct
- Certificate is not expired

Note:
If the certificate is self-signed, the browser may still show a warning until the certificate is manually trusted on the client PC.