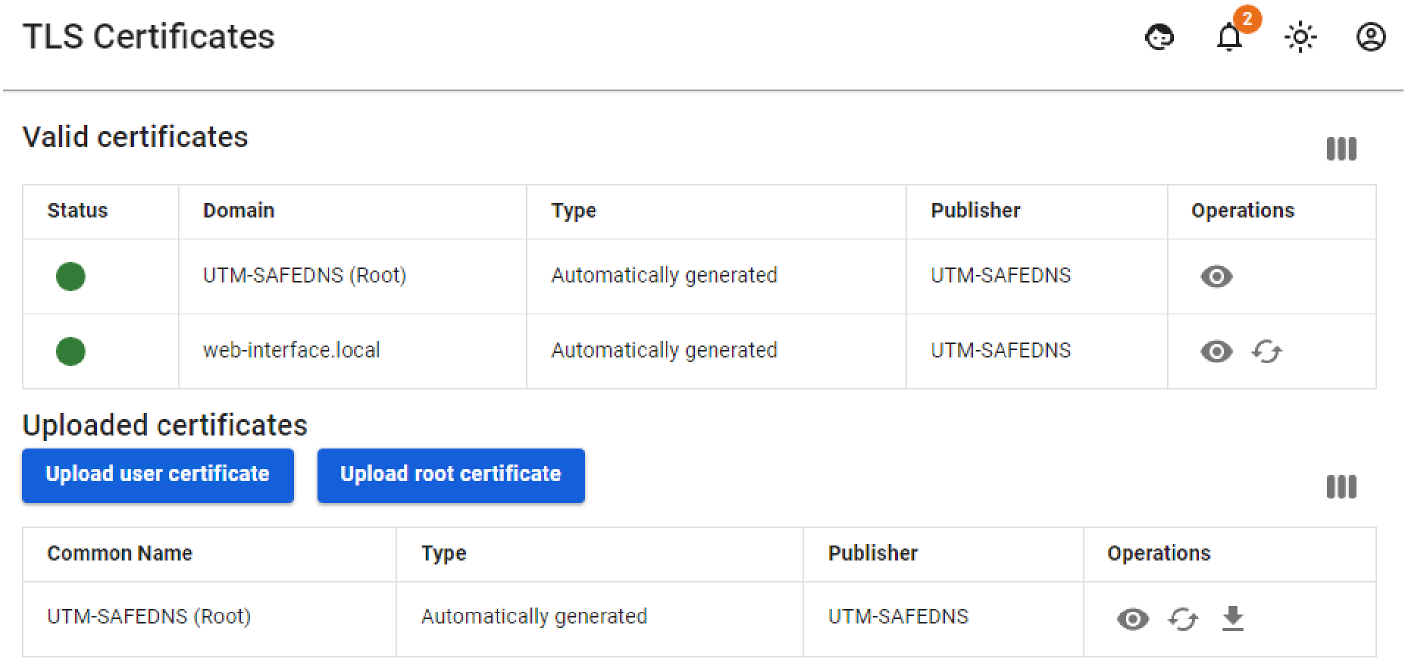
TLS Certificates

Section with information about SSL certificates.

This section displays SSL certificates/certificate chains, the list of which is formed by the following modules: reverse proxying module, IKEv2, SSTP VPN servers, web interface, web authorization, mail, etc.



Status	Domain	Type	Publisher	Operations
●	UTM-SAFEDNS (Root)	Automatically generated	UTM-SAFEDNS	👁
●	web-interface.local	Automatically generated	UTM-SAFEDNS	👁 ⟳

Common Name	Type	Publisher	Operations
UTM-SAFEDNS (Root)	Automatically generated	UTM-SAFEDNS	👁 ⟳ ⤓

Valid certificates

The table *Valid Certificates* shows the ones generated automatically, as well as the downloaded certificate chains used by SafeUTM.

> If the same certificate chain is listed in several rows of the *Valid Certificates* table, then this chain is used by several modules.

Downloaded certificates

The *Downloaded Certificates* table shows all downloaded certificate chains, as well as the SafeUTM root certificate. For more information, see **Uploading your SSL certificate to server**.

> To view basic information about the certificate (serial number, expiration date, etc.), click the eye icon.

How is the certificate issued?

1. A local certificate chain is created, and signed by a root (self-signed) certificate.
2. Simultaneously with the creation of a local certificate chain, a request is sent to issue the chain to Let's Encrypt.
3. If the Let's Encrypt certificate chain is successfully issued, it will replace the local chain.
4. If the Let's Encrypt certificate chain issue fails, then the local certificate chain will be used.

How is the certificate reissued?

When reissuing a non-root certificate chain, UTM will try to update the chain as follows:

- It checks the downloaded certificates. If the certificate is found, it will replace the previous chain with the found downloaded one.
- If there are no downloaded certificates, then SafeUTM will turn to Let's Encrypt to issue a new certificate chain.
- If the chain from Let's Encrypt is received, it will be displayed in the table.
- If it was not possible to get a chain of certificates from Let's Encrypt, then a local chain of certificates is created and signed by the root certificate.

When the root certificate is reissued, UTM will replace the previous certificate with an automatically generated root certificate.

Features

If you want to try again to get a Let's Encrypt certificate instead of a self-signed one, you need to click **Reissue** in column **Management**.

When replacing/reissuing the root certificate chain, **IPsec connections** **Head office <-> Branch** will stop working and they will need to be recreated.
If you want to replace an automatically issued certificate chain with your own, then when uploading your own certificate chain, the **CN (Common name)** of the last certificate in the chain must match the domain for which the certificate is being uploaded.
Let's Encrypt certificate is **issued for 3 months** and will be **automatically reissued** upon expiration.
From this section, you can download the root (self-signed) certificate by clicking on the corresponding link.

To upload an SSL certificate to the server, see the article **Uploading your SSL certificate to server**.

Revision #5
Created 27 August 2022 17:10:29 by Val Redman
Updated 13 October 2022 15:40:25 by Val Redman