

Let's encrypt webitel

[Let's encrypt](#) — CA that started beta operation since December 3, 2015, provides free [X.509](#) cryptographic certificates for [TLS](#) encryption ([HTTPS](#)). The process of issuing certificates is fully automated. [Webitel 3.6.0](#), included in the base distribution.

Preparation



FQDN

The certificate is issued only for the real name, the server must be accessible via HTTP \ HTTPS ports from the Internet, as the certification authority checks the correctness of the name.

In the [env/environment](#) file, list the FQDN name for your Webitel server:

```
# Please, use the FQDN hostname for HTTPS site
export WEBITEL_HOST="my-server.webitel.com"
```

Restart the Webitel:

```
/opt/orchestration/bin/reboot.sh
```

Getting a certificate

Run the command:

```
/opt/orchestration/bin/bootstrap.sh letsencrypt
```

In the [env/environment](#) file, change to:

```
# WebSocket protocol: ws or wss (WebSocket with SSL)
export WEBITEL_WS="wss"
# WebSocket protocol: off or on (for HTTPS)
export WEBITEL_SSL="on"
# WebSocket protocol: http or https
export WEBITEL_PROTO="https"
# Webitel IP or hostname.
# Please, use the FQDN hostname for HTTPS site
export WEBITEL_HOST="my-server.webitel.com"
```

Restart the Webitel:

```
/opt/orchestration/bin/reboot.sh
```

Site signed by:

Auto-renewal certificates

Since the certificate is issued only for 3 months, we can automate the process of updating it, just copy the file:

```
sudo cp /opt/orchestration/etc/cron.d/letsencrypt /etc/cron.d/
```