Remote Access and SSL

If you want to use pimatic over the internet you should always use a SSL-Connection (https) for security reasons. You can configure pimatic to run just the http- or https-Server or both. By default only the (insecure) http server is enabled.

Preparation

To connect to your Raspberry Pi from the internet , you need first to set up two things:

1. A Dynamic DNS for your home internet ip. So it can be accessed independent of the assigned IP-Address from you internet service provider. Most routers have an option for this, so check the user manual of your router.
2. Configure your router to forward the port of the https-server (default 443) to the local IP-Address of your Raspberry Pi. Check again the user manual of your router.

Creating a SSL-Certificate

To use the https-Server properly you need to create a self-signed certificate. This involves creating a certificate authority (CA) to sign it. Luckily we have written a script to simplify this:

```
sudo apt-get install wget
cd pimatic-app
wget https://raw.githubusercontent.com/pimatic/pimatic/master/install/ssl-s
etup
chmod +x ./ssl-setup
./ssl-setup
```

You have to give some information including your dynamic DNS address. At the end it creates 3 files:

- The public certificate `ca/pimatic-ssl/public/cert.pem`, that will be used for the SSL-Connection
- A private key `ca/pimatic-ssl/private/privkey.pem`, that should be kept secret and is used for the SSL-Connection
- A authority certificate `ca/certs/cacert.crt`, that should be imported to all your devices (smartphone, desktop, ...).

Configuration

Edit or add the `https`-Configuration options in the `settings`-Section of your `config.json`. It should look like this:

```
"httpsServer": {
  "enabled": true,
  "port": 443,
  "hostname": "",
  "keyFile": "ca/pimatic-ssl/private/privkey.pem",
  "certFile": "ca/pimatic-ssl/public/cert.pem",
  "rootCertFile": "ca/certs/cacert.crt"
},
```

The last step is to import the authority certificate to all your devices by going to: `http://your-ddns/root-ca-cert.crt` on each device and accepting the import. If you don't do this, you will get SSL-warnings when accessing pimatic and experience issues with caching (see: #282).