

EasyCwmp[®] Command Line Reference

EasyCwmp is a GPLv2 open source implementation of the **TR-069 cwmp** standard.

EasyCwmp is developed by PIVA Software[®].

The aim of EasyCwmp is to be fully conform with the TR069 CWMP standard.

It has integrated file transfer support (HTTP, HTTPS, FTP), and provided SSL, IPv6 protocols.

Supports the following compliant standards:

- **TR-069:** CPE WAN Management Protocol v1.1
- **TR-098:** Internet Gateway Device version 1 (Data Model for TR-069)
- **TR-181:** Device version 2.
- **TR-104:** Provisioning Parameters for VoIP CPE version 2
- **TR-106:** Data Model Template for TR-069-Enabled Devices
- **TR-111:** Applying TR-069 to Remote Management of home networking devices

Checking Easycwmp settings by the UCI command line tool

Check UCI settings for the **easycwmp**:

```
#uci show easycwmp
```

Check the required **easycwmp** element:

```
#uci get element.argument
```

where *element* can be:

- [easycwmp.@local\[0\]](#) - local settings
- [easycwmp.@acs\[0\]](#) - ACS remote server settings
- [easycwmp.@device\[0\]](#) - device settings

where the *argument* is the property of settings (like *username*, *password*, *etc.*).

e.g. the server user account:

```
#uci get easycwmp.@acs[0].username
```

About the TR-069 certification

There is a stored, unique certification for allowing the TR-069 protocol based connection between your modem and a configurable TR-069 management server.

The certification is located on the modem by default, and can be used well. But if it is necessary you can change it – e.g. by safety reasons – you can be do it, as it is listed here below.

Creating a Certification file

The certification file (**.CERT**) contains two parts in sequence:

- a **standard X509 certification** in Secure Transport "PEM" format "P12" with extension **.CRT**
- a **private key** (with RSA or EC encryption depending on the server you are using), which must be created where X509 the certification was made (in PEM format). The file has **.KEY** extension

Important!

It is PROHIBITED to secure the private key (.KEY file) by any key or password!

The .CERT certification file can be generated by the following command by appending the private key after the X509 certification, like:

```
#cat easycwmp.crt easycwmp.key > easycwmp.cert
```

Applying the certification

The certification file (e.g. easycwmp.cert) must be placed (copied) on the modem in the following directory: **/etc/easycwmp/**

Then you should configure the easycwmp by UCI in CLI (command line interface), when connecting to the modem by SSH terminal application.

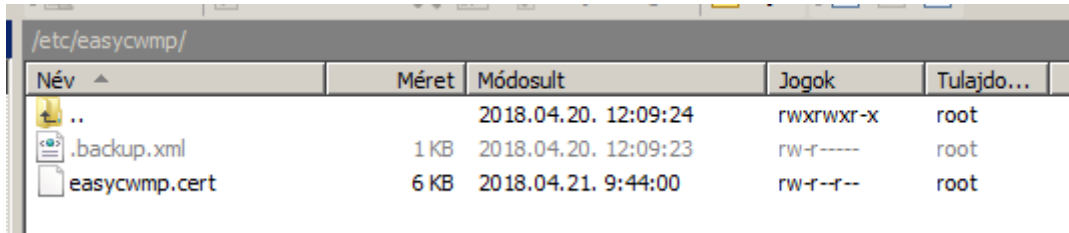
Set or configure the required **easycwmp** element:

```
#uci set element.part
```

Using as described above.

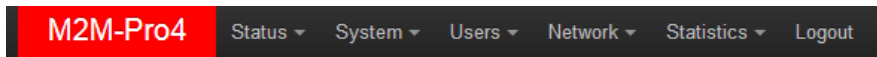
Configuring the SSL certification

First of all copy the .cert file to the **/etc/easycwmp/ directory** to the modem. You can use e.g. the **WinSCP** tool for that (**SCP** protocol, **port 22**, by defining an **account** and **password** for the connection).



Név	Méret	Módosult	Jogok	Tulajdo...
..		2018.04.20. 12:09:24	rw-rw-r-x	root
.backup.xml	1 KB	2018.04.20. 12:09:23	rw-r-----	root
easycwmp.cert	6 KB	2018.04.21. 9:44:00	rw-r--r--	root

You can use the OpenWrt LuCi web user interface, System / TR-069 item, by filling the **ACS URL** field (remote server URL) and the **Certificate** field (cert. file location on the local modem).



TR-069 Settings

ACS Login

ACS URL	<input type="text" value="http://192.168.1.110:8080/openacs"/>
Certificate	<input type="text" value="/etc/easycwmp/easycwmp.cert"/>

Or you can do it through the UCI CLI, like this:

To setup TR-069 certification file, use the following commands, setup the **url** (with the ACS server and http(s) URL, and **ssl_cert** (with path and filename of the certification file on the local modem) entries.

Then you have to commit the changes to apply.

```
#uci set easycwmp.@acs[0].url='192.168.1.110:8080/openacs/acs'  
  
#uci set easycwmp.@acs[0].ssl_cert='/etc/easycwmp/easycwmp.cert'  
  
#uci commit
```

Important!

For using the certification file, you have to copy to the path you were given.

Further help

Some hints for creating the .cert and .key files by the following scripts:

Creation by these commands:

```
#curl_easy_setopt(curl, CURLOPT_SSLCERT, config->acs->ssl_cert);  
  
#openssl x509 -in easycwmp.cert -text -noout
```