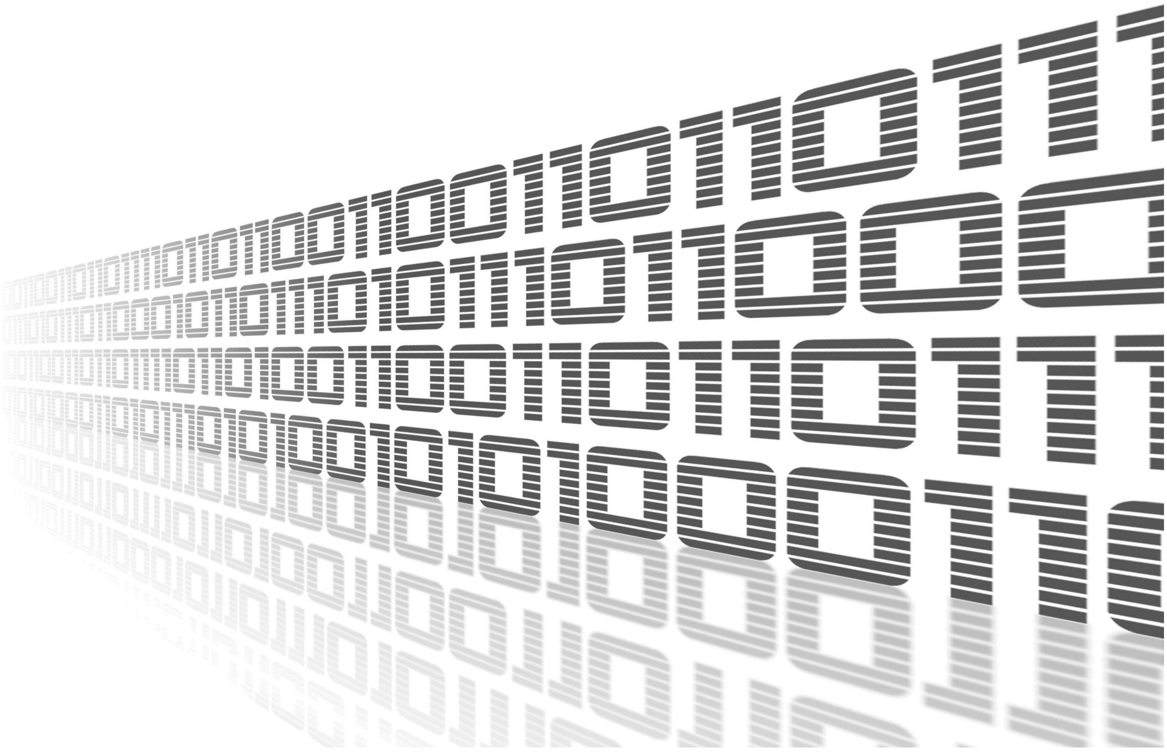
RouterApp

User Module

SCEP Client

APPLICATION NOTE



ADVANTECH

www.lucom.de

14-04-21

Used symbols

⚠ *Danger* – Information regarding user safety or potential damage to the router.

❗ *Attention* – Problems that may arise in specific situations.

ℹ *Information or notice* – Useful tips or information of special interest.

✎ *Example* – Example of function, command or script.

CE

TÜVRheinland® COTI ISO 9001

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Document No. APP-0062-EN, revised on February 17, 2021. Released in the Czech Republic.

Contents

List of Tables

1. Basic information

User module *SCEP Client* is not contained in the standard router firmware. Uploading of any user module is described in the Configuration manual (see [1]).

The user module is v2 and v3 router platforms compatible.

1.1 What is SCEP?

SCEP (Cisco System's Simple Certificate Enrollment Protocol) is a PKI communication protocol which leverages existing technology by using PKCS#7 and PKCS#10. SCEP is the evolution of the enrollment protocol developed by Verisign, Inc. for Cisco Systems, Inc. It now enjoys wide support in both client and CA implementations.

The goal of SCEP is to support the secure issuance of certificates to network devices in a scalable manner, using existing technology whenever possible. The protocol supports the following operations:

- CA and RA public key distribution
- Certificate enrollment
- Certificate and CRL query

Certificate and CRL access can be achieved by using the LDAP protocol, or by using the query messages defined in SCEP.

2. Web Interface

Once the installation of the module is complete, the module's GUI can be invoked by clicking the module name on the User modules page of router's web interface.

Left part of this GUI contains menu with Configuration menu section and Information menu section. Customization menu section contains only the Return item, which switches back from the module's web page to the router's web configuration pages. The main menu of module's GUI is shown on Figure 2.

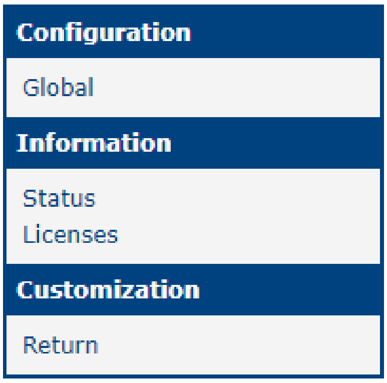
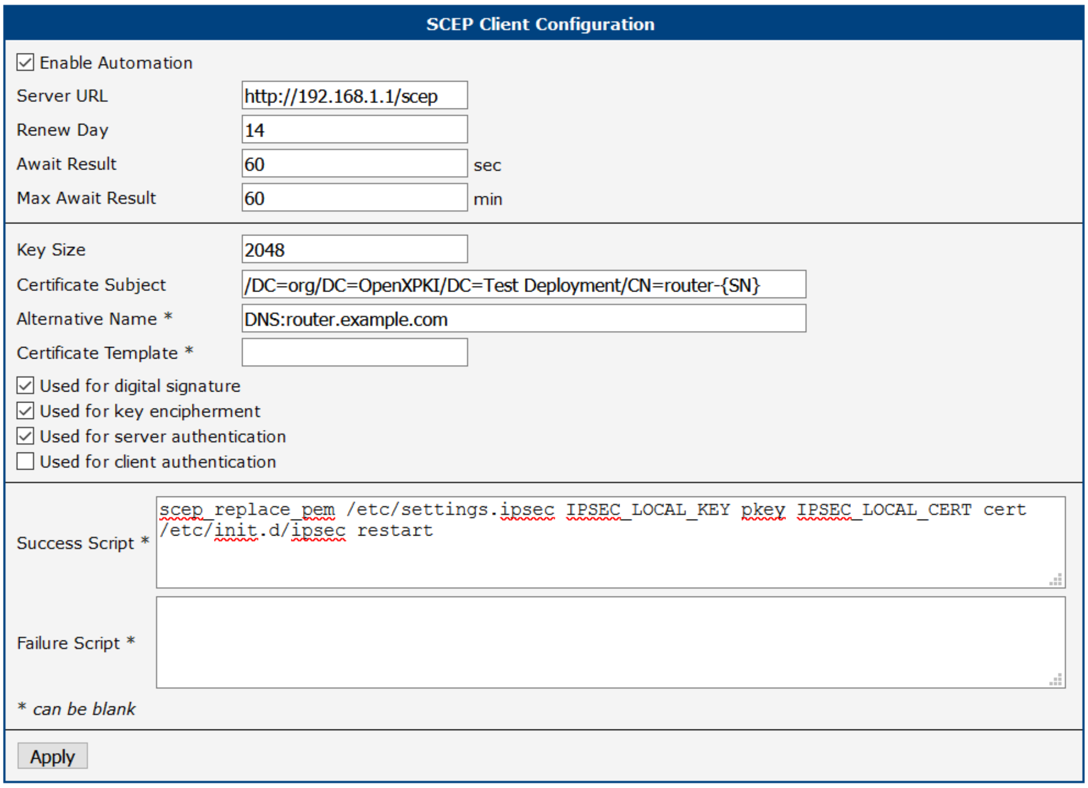


Figure 1: Menu

3. Configuration

3.1 Global

All SCEP user module settings can be configured by clicking on the *Global* item in the main menu of module web interface. An overview of configurable items is given below.



SCEP Client Configuration

☑ Enable Automation

Server URL	http://192.168.1.1/scep	
Renew Day	14	
Await Result	60	sec
Max Await Result	60	min
Key Size	2048	
Certificate Subject	/DC=org/DC=OpenXPKI/DC=Test Deployment/CN=router-{SN}	
Alternative Name *	DNS:router.example.com	
Certificate Template *		

☑ Used for digital signature
☑ Used for key encipherment
☑ Used for server authentication
☐ Used for client authentication

Success Script *

```
scep_replace_pem /etc/settings.ipsec IPSEC_LOCAL_KEY pkey IPSEC_LOCAL_CERT cert
/etc/init.d/ipsec restart
```

Failure Script *

** can be blank*

Figure 1: Configuration

Item	Description
Enable Automation	Enable for automatic certificate enrollment.
Server URL	Address of a SCEP server.
Renew day	Start automatic renewal when the certificate lifetime is less than the given amount of days.

Continued on the next page

Continued from previous page

Item	Description
Await Result [sec]	How long shall the client wait before asking for issued certificate. This is useful when issuing a certificate requires a manual approval.
Max Await Result [min]	When the certificate is not ready yet, the client will wait and ask again and again until this limit is reached.
Key Size	Length of the RSA key [bits].
Certificate Subject	Requested subject of the certificate. The string may include the following wildcards: SN = Serial Number of the router For example: /DC=org/DC=OpenXPKI/DC=Test Deployment/CN=router-SN
Alternative Name	Requested subject alternative name. Comma separated list of email:, URI:, DNS:, RID:, IP:, dirName: and otherName: prefixed items, for example: DNS:one.domain.com,DNS:other.domain.org email:my@other.address,RID:1.2.3.4
Certificate Template	Microsoft proprietary “1.3.6.1.4.1.311.20.2“ extension. Your CA (e.g. OpenXPKI) may use this value to choose the type of certificate to issue. Other CA may not support this extension.
Used for digital signature	Requests the “digitalSignature” usage. Please note that depending on its configuration your CA may ignore this value for security reasons. For example, OpenPKI by default ignores all usage requests; the templates (see above) need to be used when clients may choose the intended usage.
Used for key encipherment	Requests the “keyEncipherment” usage.
Used for server authentication	Requests the “serverAuth” extended usage.
Used for client authentication	Requests the “clientAuth” extended usage.
Success Script	Shell commands to execute upon successful deployment (see also the section on Certificate Distribution).
Failure Script	Shell commands to execute upon deployment failure.

Table 1: Configuration items description

The enrolled certificates are stored in /var/data/scepClient. Each private key (.key) and corresponding certificate (.crt) are stored under its serial number. The directory also contains the CA certificate chain ca.crt-0, ca.crt.1, . . . Each certificate in the chain is stored in a separate file.

The symbolic links latest.key and latest.crt point to the most recent (active) certificate.

Upon router (re)start, or when the “Apply” button is clicked, the latest.crt is checked. If the certificate does not exist, or if it will expire in less than “Renew Days”, the enrollment is started.

3.2 Certificate Distribution

The generated key/certificate needs to be explicitly distributed to router services using a *Success Script* and scep_replace_pem commands. The command takes the following parameters:

- Full path to the configuration file to be modified, e.g. etc/settings.ipsec
- A list of values to be modified as pairs of two:
  - Name of the configuration parameter to be changed, e.g. IPSEC_LOCAL_KEY
  - Information type to be replaced, which can be one of the following values:
    - “pkey” to use the private key from the latest.key file;
    - “cert” to use the certificate from the latest.crt file

For example, to use the enrolled information as the *Local Private Key* and the *Local Certificate* of a 1st IPsec Tunnel do:

```
scep_replace_pem /etc/settings.ipsec \
IPSEC_LOCAL_KEY pkey IPSEC_LOCAL_CERT cert
```

After changing a service configuration you need to restart the service or just reload its configuration. For example, restart the IPsec with

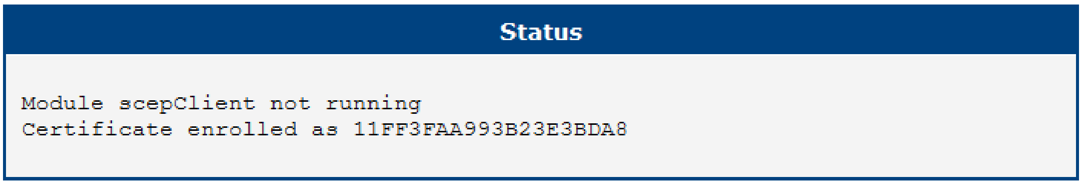
```
/etc/init.d/ipsec restart
```

3.3 Status

The enrollment may require manual approval on the server side. Hence, the enrollment process may take several minutes. This does not block the router (re)start though. To check status of certificate enrollment, click Information – Status. This will print two lines.

The first line show status of the module process:

```
Module scepClient disabled
Module scepClient running
Module scepClient not running
```



Status

```
Module scepClient not running
Certificate enrolled as 11FF3FAA993B23E3BDA8
```

Figure 2: Status

The second line show status of the certificate enrollment:

```
Certificate not enrolled
Certificate enrollment
Certificate re-enrollment
Certificate enrolled xxxxxxxxxxxxxxxxxxxx
```

Where xxxxxxxxxxxxxxxxxxxx represents the serial number of the certificate.

3.4 Periodic Checks

To schedule own regular validity checks, create or modify /var/scripts/crontab to regularily invoke /opt/scepClient/bin/check-cert.sh (without arguments) and (re)start crond&

For example: to check certificates for renewal every day, 5 minutes after midnight, do:

```
5 0 * * *    root /opt/scepClient/bin/check-cert.sh
```

4. Command-Line Tool

The sscep client can also be used directly as a command-line tool.

Running the command *sscep* without any arguments should give you a list of arguments and command line options. For more informations about SCEP usage see documentation[1].

Usage: /opt/scepClient/bin/sscep **Operation** [**Options**]

Available **Operations** are:

Operation	Description
getca	Get CA/RA certificate(s)
enroll	Enroll certificate
getcert	Query certificate
getcrl	Query CRL
getcaps	Query SCEP capabilities

Table 2: Available Operations

General **Options**:

Option	Description
-u <url>	SCEP server URL
-p <host:port>	Use proxy server at host:port
-g <engine>	Use the given cryptographic engine
-f <file>	Use configuration file
-c <file>	CA certificate file or '-n' suffixed files (write if Operation is getca)
-E <name>	PKCS#7 encryption algorithm (des|3des|blowfish|aes[128]|aes192|aes256)
-S <name>	PKCS#7 signature algorithm (md5|sha1|sha224|sha256|sha384|sha512)
-v	Verbose output (for debugging the configuration)
-d	Debug output (more verbose, for debugging the implementation)

Table 3: General Options

[1] https://github.com/certnanny/sscep/blob/master/README.md

Options for **operation** *getca* are:

Option	Description
-i <string>	CA identifier string
-F <name>	Fingerprint algorithm (md5|sha1|sha224|sha256|sha384|sha512)

Table 4: Options for operation *getca*

Options for **operation** *enroll* are:

Option	Description
-k <file>	Private key file
-r <file>	Certificate request file
-K <file>	Signature private key file, use with -O
-O <file>	Signature certificate (used instead of self-signed)
-l <file>	Write enrolled certificate in file
-e <file>	Use different CA cert for encryption
-L <file>	Write selfsigned certificate in file
-t <secs>	Polling interval in seconds
-T <secs>	Max polling time in seconds
-n <count>	Max number of GetCertInitial requests
-R	Resume interrupted enrollment

Table 5: Options for operation *enroll*

Options for **operation** *getcert* are:

Option	Description
-k <file>	Signature private key file
-l <file>	Signature local certificate file
-s <number>	Certificate serial number (decimal)
-w <file>	Write certificate in file

Table 6: Options for operation *getcert*

Options for **operation** *getcrl* are:

Option	Description
-k <file>	Private key file
-l <file>	Local certificate file
-w <file>	Write CRL in file

Table 7: Options for operation *getcrl*

5. Related Documents

[1] Advantech Czech: **v2 Routers Configuration Manual** (MAN-0021-EN)
[2] Advantech Czech: **SmartFlex Configuration Manual** (MAN-0023-EN)
[3] Advantech Czech: **SmartMotion Configuration Manual** (MAN-0024-EN)
[4] Advantech Czech: **SmartStart Configuration Manual** (MAN-0022-EN)
[5] Advantech Czech: **ICR-3200 Configuration Manual** (MAN-0042-EN)

Product related documents can be obtained on *Engineering Portal* at www.ep.advantech-bb.cz address.