SIEMENS

FAQ • 10/2014

How to manage the X.509 Certificates in RUGGEDCOM WIN BS and CPEs Software Version 4.3

RUGGEDCOM WIN

http://support.automation.siemens.com/WW/view/en/103158899

This entry is from the Siemens Industry Online Support. The general terms of use (http://www.siemens.com/terms_of_use) apply.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com.

Table of Contents

1 Introduction

1.1 About This Document

This document provides a procedure for generating the X.509 certificates and loading them on RUGGEDCOM WIN CPE, Aptilo AAA server and Cisco ACS.

1.2 Related Documents

Table 1-1

Doc Name	Version	Notes
RUGGEDCOM_WIN_X509_Certificate_SW_V4-2	V1.0	For Software Version 4.2

2 Certificate generation

X.509 certificates generation has to be done on Linux host or Cygwin running on Windows. All the certificates are in X.509v3 format.

The procedure consists of 2 parts:

1. Modifying the relevant “cnf” files depending on the certificate type and the desired properties. There are two directories:
    a. Main directory. This is where the client certificate is generated. The “client.cnf” file and its matching Makefile and “run.sh“ script are located there.
    b. Main/CA directory. This is where the CA and server certificates are generated. The “server.cnf” file and “cacert.cnf” file and their matching Makefile and “run.sh“ script are located there.

The client and Server and CA certificates are separated, because the CA and server certificate files are only generated once, while client certificates that are signed by the CA are generated multiple times. Thus, there is no need (and it’s even harmful) to generate all of them every time the tool is running (as was with the original tool)

2. Running the “run.sh“ scripts from the folders where the “cnf” files are located. Running “run.sh“ from the Main/CA directory will create the CA and Server certificates. Running “run.sh“ from the Main directory will create the Client certificate and key signed by the CA certificate. Thus it is important first to generate the CA certificate.

The following files are relevant to the certificate generation procedure:

1. ca.cnf
2. server.cnf
3. client.cnf

2.1 CA certificate

The “ca.cnf” file contains all the needed parameters for customer CA certificate generation. CA certificate is needed in order to sign the server and client certificates.

The following subset of parameters is presented with their default values and can be modified in order to reflect customer’s specifics for the certificate. Also, an explanation of parameter meaning is provided.

Table 2-1: CA certificate properties

Parameter	Explanation
default_days = 10000	Certificate validity period.

[req]
input_password = password
output_password = password
	Both input and output fields have to have the same CA private key password. The significance of the password is local and it is only used during the actual server certificate signing procedure.

[certificate_authority]
countryName = CA
stateOrProvinceName = N/A
localityName = N/A
organizationName = N/A
emailAddress = N/A
commonName = "Certificate Authority"
	Country name must be 2 letters.

Parameter	Explanation
	This name will be shown in the “Issued to” and “Issued by” fields (when the certificate is presented in “.der” format)

2.2 Server certificate

The “server.cnf” file contains all the needed parameters for customer server certificate generation. As a part of the server certificate generation, a server private key is created as well. Server certificate file also includes the server private key (in the same file) and it is put on the AAA server.

When working with ACS, please make sure that an OpenSSL version 0.9.8 (or earlier) is used on the Linux PC (or Cygwin) that the tool is run on. Any later versions such as 1.0.0, 1.0.1 will result in having client private key in incompatible format for our CPE and the AAA as well.

Here are the sample differences between the keys:

Openssl 0.9.8 private key (the good format)

Figure 2-1

```
BEGIN RSA PRIVATE KEY
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,327E4B06D51C7728
grestO9v2wfiqFwBy8bBbpNjMWpFrrc/9y8q68n6c48enCFyDsdVlyqToOQ+Razt
d98I+rkTow33X83e9+Zt8rGlKJlPXn3zHTKbjNhfc7j6kk+ssWJft5OAvu5NShMx
FOATl4pW97qCf1x4pFwQGm8/8MhCqOpqv2cLfjz2T4Egu1qP2sHZ35QU/gHBLHYh
```

Openssl 1.0.0 private key (the bad format)

Figure 2-2

```
BEGIN ENCRYPTED PRIVATE KEY
MIIJnzBJBgkqhkiG9w0BBQ0wPDAbBgkqhkiG9w0BBQwwDgQI0Z45oYYRJ1cCAggA
MB0GCWCGSAFlAwQBAgQQF4QLI0IILDItqQFXHJeAxgSCCVBAo1Ed9BHwyhHeBzx2
rQELkAghar26CFsP7qvMwZ+vnATbArA2MvFWJWy0l2pl7/Rn7RcoztbSzg82c8IG
```

The following subset of parameters is presented with their default values and can be modified in order to reflect customer’s specifics for the certificate. Also, an explanation of parameter meaning is provided.

Table 2-2: Server certificate properties

Parameter	Explanation
default_days = 10000	Certificate validity period
[req] input_password = password output_password = password	Both input and output fields have to have the same server private key password. The significance of the password is local and it doesn’t have to be equal to the CA private key password. This password has to be entered in the AAA, so it would be able to decrypt the key when needed.

Parameter	Explanation
[server] countryName =CA	Country name must be 2 letters.

stateOrProvinceName = N/A
localityName = N/A
organizationName = N/A
emailAddress = N/A
commonName = "Server Certificate
	This name will be shown in the “Issued to” field (when the certificate is presented in “.der” format). If the certificate is signed correctly, the “Issued by” field will be the commonName of the CA certificate from above.

2.3 Client certificate

The “client.cnf” file contains all the needed parameters for customer server certificate generation. As a part of the client certificate generation, a client private key is created as well.

Make sure that OpenSSL version 0.9.8e-fips-rhel5 (01 Jul 2008) is used on the Linux PC (or Cygwin) that the tool is run on. **It’s also important NOT to use any OpenSSL version between September 2006 and May 2008, as there was some bug that produced weak keys**.

Any later versions such as 1.0.0, 1.0.1 will result in having client private key in incompatible format for our CPE and the AAA as well.

Here are the sample differences between the keys:

Openssl 0.9.8 private key (the good format)

Figure 2-3

```
BEGIN RSA PRIVATE KEY
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,327E4B06D51C7728
grestO9v2wfiqFwBy8bBbpNjMWpFrrc/9y8q68n6c48enCFyDsdVlyqToOQ+Razt
d98I+rkTow33X83e9+Zt8rGlKJlPXn3zHTKbjNhfc7j6kk+ssWJft5OAvu5NShMx
FOATl4pW97qCf1x4pFwQGm8/8MhCqOpqv2cLfjz2T4Egu1qP2sHZ35QU/gHBLHYh
```

Openssl 1.0.0 private key (the bad format)

Figure 2-4

```
BEGIN ENCRYPTED PRIVATE KEY
MIIJnzBJBgkqhkiG9w0BBQ0wPDAbBgkqhkiG9w0BBQwwDgQI0Z45oYYRJ1cCAggA
MB0GCWCGSAFlAwQBAgQQF4QLI0IILDItqQFXHJeAxgSCCVBAo1Ed9BHwyhHeBzx2
rQELkAghar26CFsP7qvMwZ+vnATbArA2MvFWJWy0l2pl7/Rn7RcoztbSzg82c8IG
```

Client certificate and client key are needed only if EAP-TLS authentication method is used. If EAP-TTLS is used, only CA certificate (and the “random” seed file) is enough on the CPE side.

The following subset of parameters is presented with their default values and can be modified in order to reflect customer’s specifics for the certificate. Also, an explanation of parameter meaning is provided.

Table 2-3: Client certificate properties

Parameter	Explanation
default_days = 10000	Certificate validity period

[req]
input_password = **Cisco**
output_password = **Cisco**
	Both input and output fields have to have the same client private key password. The significance of the password is local and it doesn’t have to be equal to the server or CA private key password. This password has to be entered in the CPE GUI, **but currently in 4.21 version this is NOT supported and the password shall remain Cisco. In 4.4 it will be possible to change this password via GUI.**

[client]
countryName = CA
stateOrProvinceName = Ontario
localityName = Concord
organizationName = Siemens
organizationalUnitName = N/A
commonName = "Client Certificate"
	Country name must be 2 letters.
	This name will be shown in the “Issued to” and “Issued by” fields (when the certificate is presented in “.der” format). If the certificate is signed correctly, the “Issued by” field will be the “commonName” of the CA certificate from above. For EAP-TLS usage, this filed would generally be some unique identifier for the CPE, such as its MAC address.

2.4 Certificate generation script

Once all the above-mentioned certificate properties are modified and all the relevant “cnf” files are saved, the “run.sh” scripts have to be executed from the relevant directories.

For example:

1. Perform “cd /home/user” and then “./run.sh” for generating client certificates.
   The generated client certificates in “`.pem`” and in “`.der`” formats will be stored in the “Main/output” directory.
2. Perform “cd /home/user/ca” and then “./run.sh” for generating CA and server certificates.
   The generated CA and server certificates in “.pem” and in “.der” formats will be stored in the “Main/ca/output” directory.

NOTE

Important!

As a part of the script, for Linux machines there is command that shifts the date on the generation machine to year 2008. After the generation is over, the date is set back to the current date. The reason for shifting the date back is due to CPE internal clock that is set to this date (there is no GPS in the CPE) and the certificate validity start time has to match it in order to work properly. In 4.3 there will be no need for this time shift, as NTP protocol will be supported. Also, if Cygwin is used, the date on the Windows PC has to be set manually.

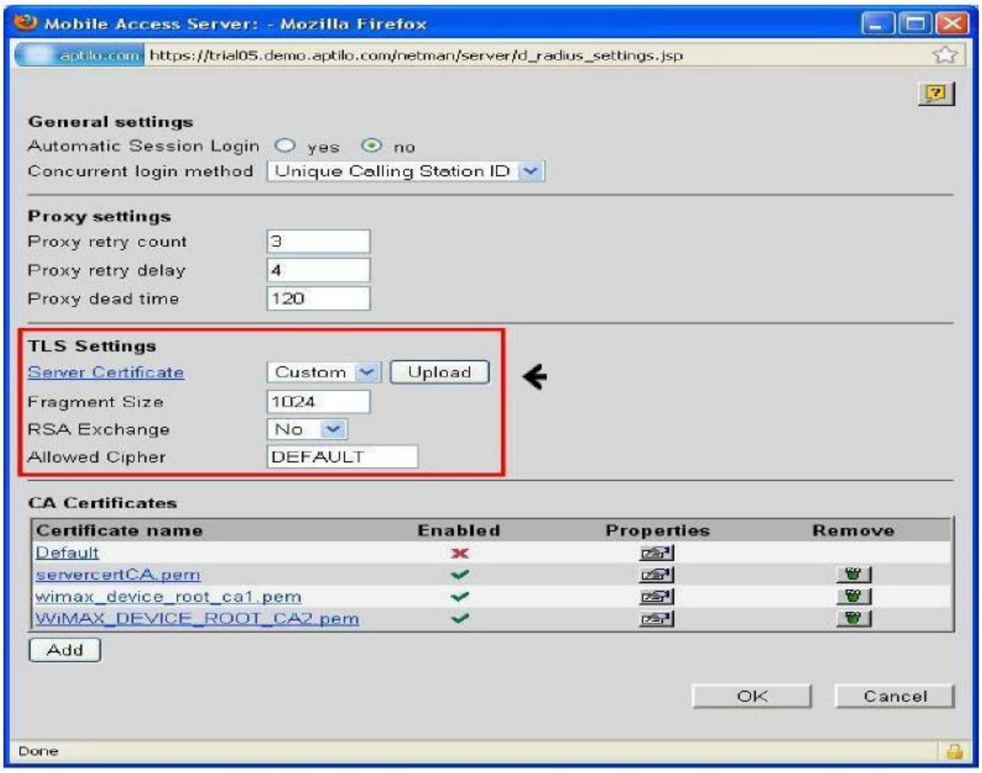
3 Certificate loading

3.1 Aptilo AAA

The following certificates shall be uploaded to Aptilo: cacert.pem and servercert.pem (the private key is in the same file).

In order to upload the servercert.pem, access the TLS settings under RADIUS settings choose Custom in the drop-down menu and press the Upload button:

Figure 3-1: Server certificate loading



Mobile Access Server: - Mozilla Firefox
aptilo.com
https://trial05.demo.aptilo.com/netman/server/d_radius_settings.jsp
?

General settings

Automatic Session Login ○ yes ● no

Concurrent login method: Unique Calling Station ID

Proxy settings

Proxy retry count: 3

Proxy retry delay: 4

Proxy dead time: 120

TLS Settings

Server Certificate: Custom [Upload]

Fragment Size: 1024

RSA Exchange: No

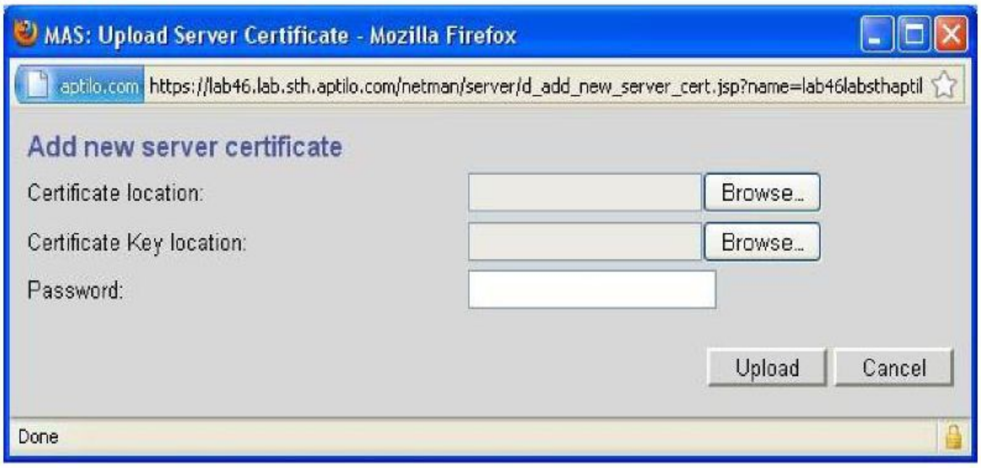
Allowed Cipher: DEFAULT

CA Certificates

Certificate name	Enabled	Properties	Remove
Default	✗	✎	
servercertCA.pem	✓	✎	🗑
wimax_device_root_ca1.pem	✓	✎	🗑
WiMAX_DEVICE_ROOT_CA2.pem	✓	✎	🗑

Pressing the “Upload” button opens the following screen:

Figure 3-2: Adding server certificate



MAS: Upload Server Certificate - Mozilla Firefox

aptilo.com https://lab46.lab.sth.aptilo.com/netman/server/d_add_new_server_cert.jsp?name=lab46labsthaptil

Add new server certificate

Certificate location:

Certificate Key location:

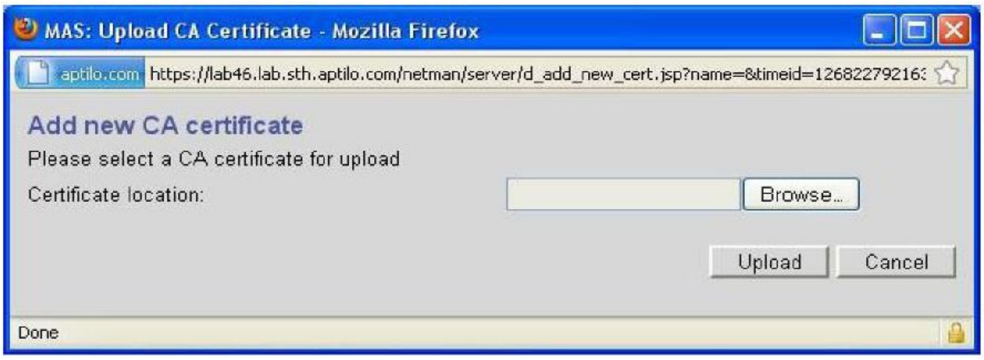
Password:

Done

Use the “Browse” button and upload the server certificate in “Certificate Location” and in the “Certificate Key Location” (again, this is due to the server certificate and key being in the same file). Also enter the private key password as configured in the “server.cnf”.

1. In order to upload the CA certificate, refer to Figure 3-1 and press the “Add button” in the bottom of the page. The following screen will open:

Figure 3-3: Adding CA certificate



MAS: Upload CA Certificate - Mozilla Firefox

aptilo.com https://lab46.lab.sth.aptilo.com/netman/server/d_add_new_cert.jsp?name=&timeid=12682279216:

Add new CA certificate

Please select a CA certificate for upload

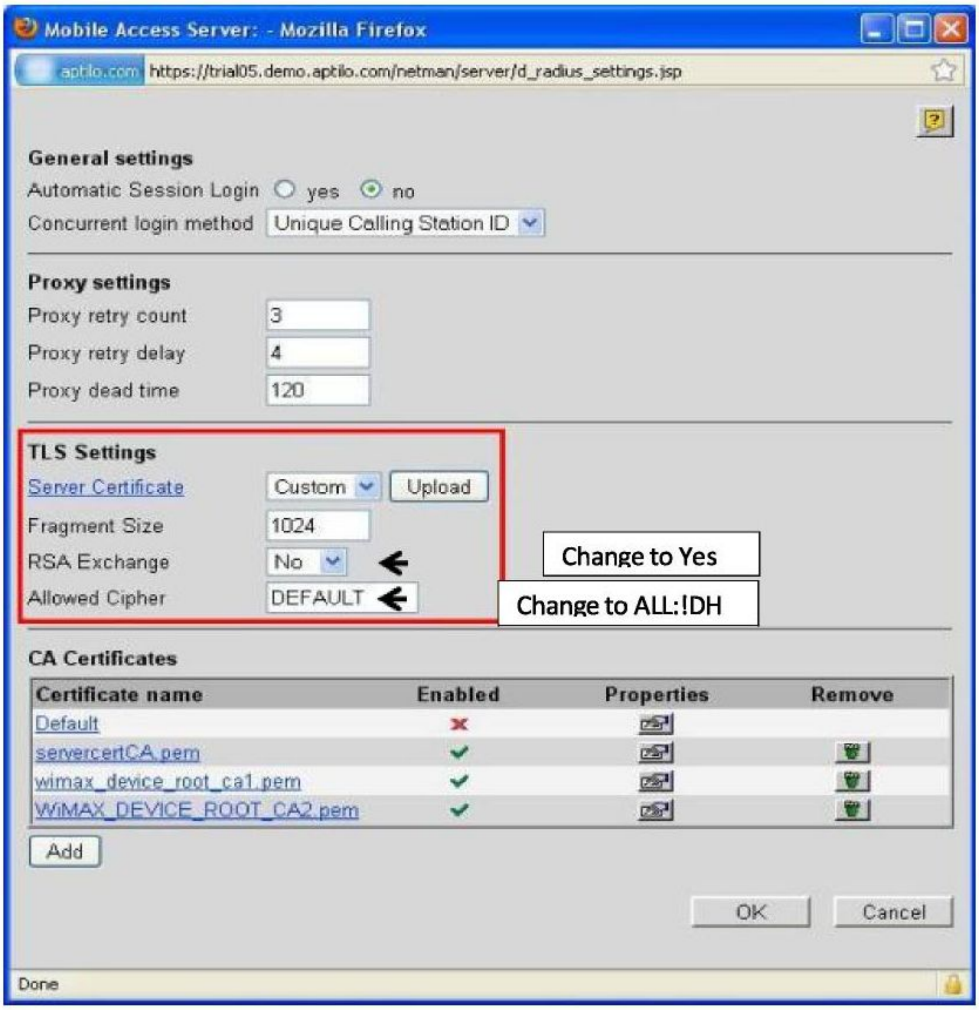
Certificate location:

Done

Use the “Browse” button and upload the CA certificate to “Certificate Location”.

2. RUGGEDCOM WIN CPE doesn’t support Diffie-Hellman crypto suites, thus there is a need to disable them in Aptilo and enable RSA key exchange functionality. This is done by changing the TLS settings under RADIUS settings, as per the following guidance:
   a. RSA key exchange from “No” to “Yes”.
   b. Allowed ciphers from “DEFAULT” to “ALL:!DH”.
   c. Restart Aptilo service. No need to reboot the server. Here is the Aptilo GUI snapshot:

Figure 3-4: Aptilo cipher suite support



Mobile Access Server: - Mozilla Firefox

aptilo.com https://trial05.demo.aptilo.com/netman/server/d_radius_settings.jsp

General settings

Automatic Session Login ○ yes ● no

Concurrent login method: Unique Calling Station ID

Proxy settings

Proxy retry count: 3

Proxy retry delay: 4

Proxy dead time: 120

TLS Settings

Server Certificate: Custom

Fragment Size: 1024

RSA Exchange: No

Allowed Cipher: DEFAULT

Change to Yes

Change to ALL:!DH

CA Certificates

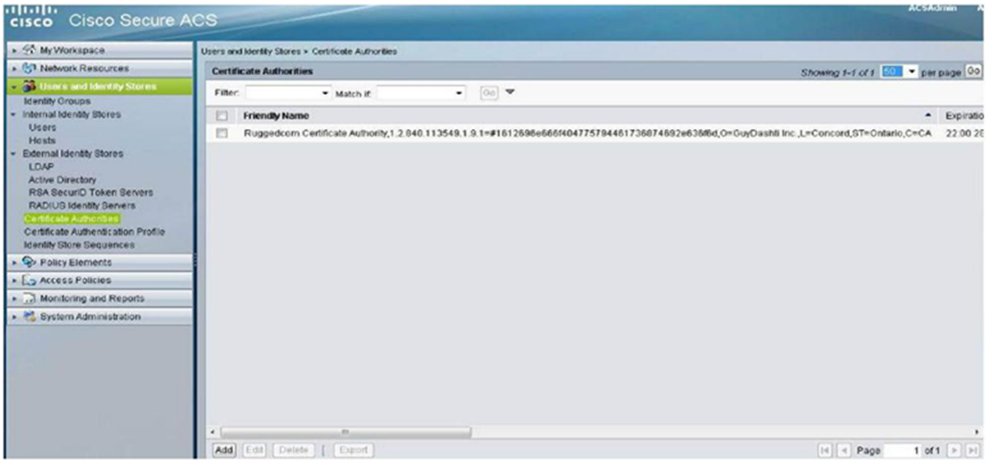
Certificate name	Enabled	Properties	Remove
Default	✗	✎	
servercertCA.pem	✓	✎	🗑
wimax_device_root_ca1.pem	✓	✎	🗑
WiMAX_DEVICE_ROOT_CA2.pem	✓	✎	🗑

3.2 Cisco ACS

Load the CA certificate

In order to load the CA certificate, go to the “Users and Identity Stores” screen and press “Certificate Authorities”. Below is the screenshot of the relevant screen:

Figure 3-5



Users and Identity Stores > Certificate Authorities

Certificate Authorities

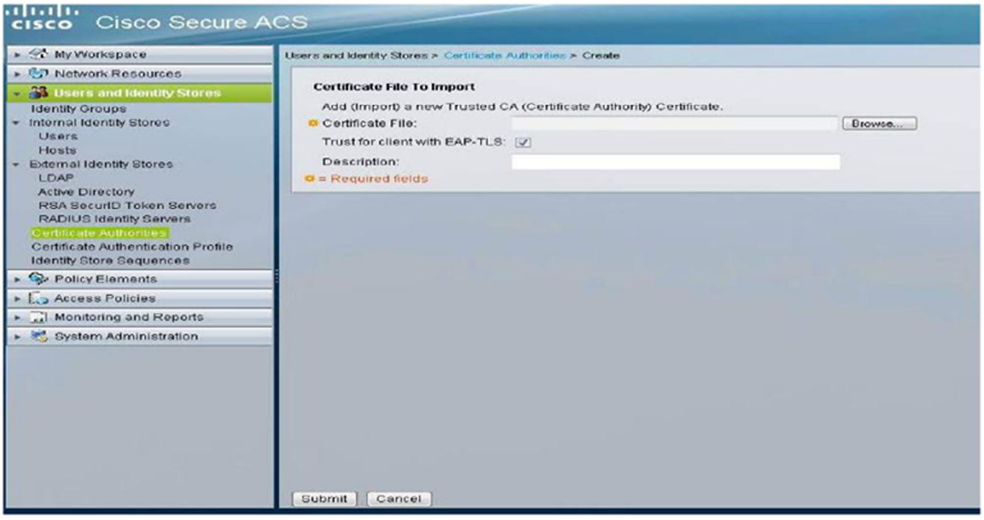
Showing 1-1 of 1 50 per page Go

Filter: Match if: Go

□	Friendly Name	Expiratio
□	Ruggedcom Certificate Authority,1.2.840.113549.1.9.1=#1612696e666f404775794461736874692e636f6d,O=GuyDashti Inc.,L=Concord,ST=Ontario,C=CA	22:00:2

Press the “Add” button. This will lead to the following screen.

Figure 3-6



Users and Identity Stores > Certificate Authorities > Create

Certificate File To Import

Add (Import) a new Trusted CA (Certificate Authority) Certificate.

Certificate File:

Trust for client with EAP-TLS: ☑

Description:

= Required fields

Use the “Browse” button to point to the correct file on your local PC. Then press “Submit”.

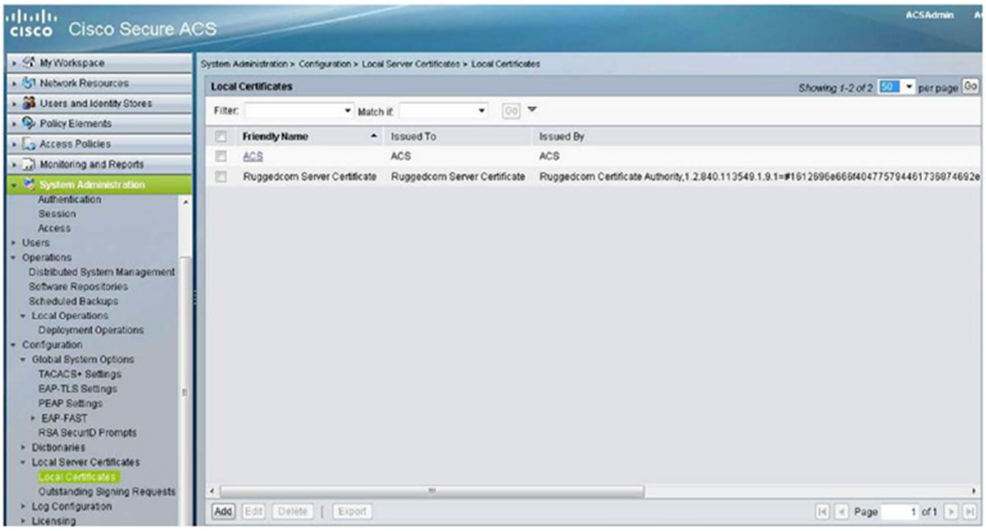
Make sure that the CA certificate is in the “.pem” format.

Make sure that you check the “Trust for client with EAP-TLS” checkbox.

Load server certificate

In order to load the server certificate, go to the “System Administration” screen and press “Local Certificates”. Below is the screenshot of the relevant screen.

Figure 3-7



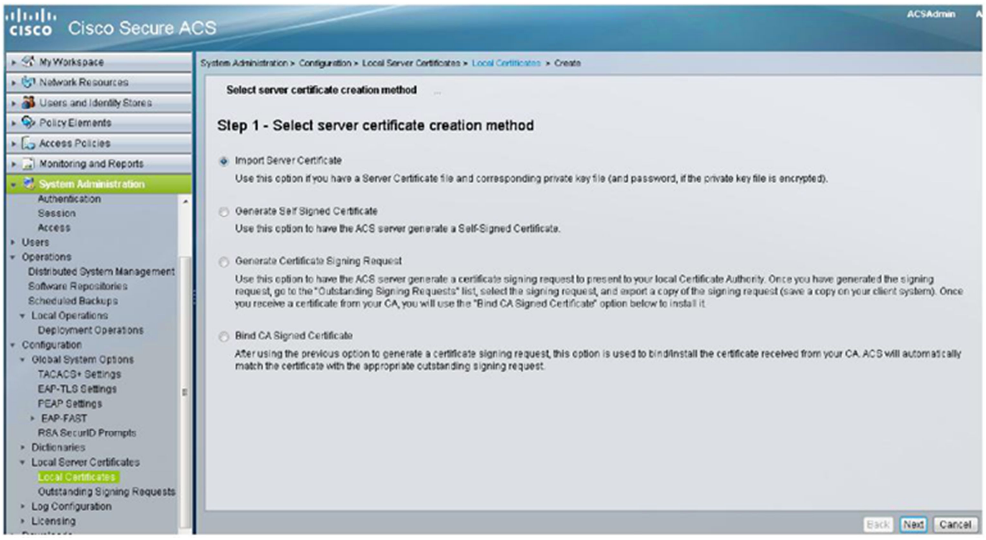
System Administration > Configuration > Local Server Certificates > Local Certificates

Local Certificates — Showing 1-2 of 2 | 50 per page

	Friendly Name	Issued To	Issued By
□	ACS	ACS	ACS
□	Ruggedcom Server Certificate	Ruggedcom Server Certificate	Ruggedcom Certificate Authority,1.2.840.113549.1.9.1=#1612696e666f404775794461736874692e

Press the “Add” button. This will lead to the following screen.

Figure 3-8



System Administration > Configuration > Local Server Certificates > Local Certificates > Create

Select server certificate creation method

Step 1 - Select server certificate creation method

● Import Server Certificate
Use this option if you have a Server Certificate file and corresponding private key file (and password, if the private key file is encrypted).

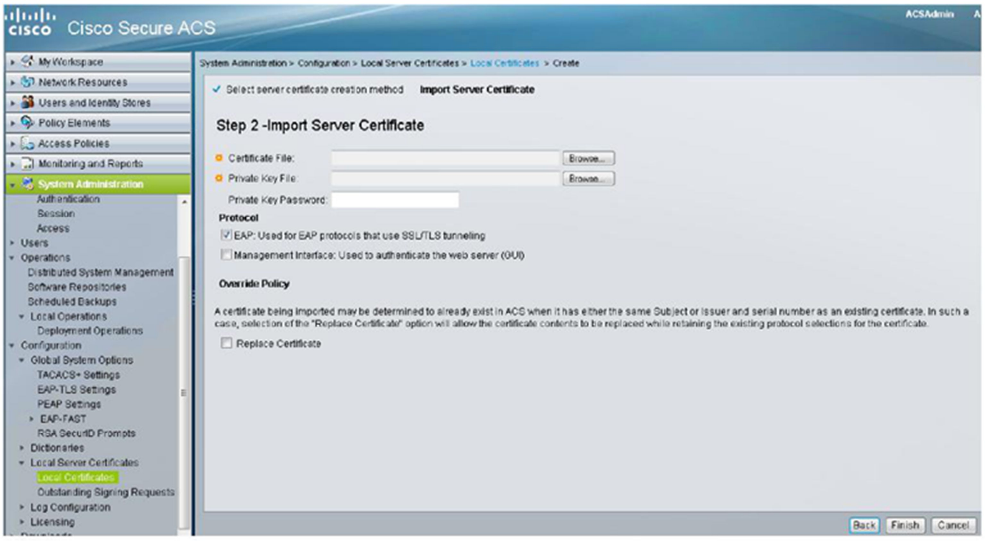
○ Generate Self Signed Certificate
Use this option to have the ACS server generate a Self-Signed Certificate.

○ Generate Certificate Signing Request
Use this option to have the ACS server generate a certificate signing request to present to your local Certificate Authority. Once you have generated the signing request, go to the "Outstanding Signing Requests" list, select the signing request, and export a copy of the signing request (save a copy on your client system). Once you receive a certificate from your CA, you will use the "Bind CA Signed Certificate" option below to install it.

○ Bind CA Signed Certificate
After using the previous option to generate a certificate signing request, this option is used to bind/install the certificate received from your CA. ACS will automatically match the certificate with the appropriate outstanding signing request.

Choose the preferable option. Basically we use the “Import” option as we load external certificates. Press “Next”.

Figure 3-9



System Administration > Configuration > Local Server Certificates > Local Certificates > Create

✓ Select server certificate creation method **Import Server Certificate**

Step 2 -Import Server Certificate

Certificate File:

Private Key File:

Private Key Password:

Protocol

☑ EAP: Used for EAP protocols that use SSL/TLS tunneling

□ Management Interface: Used to authenticate the web server (GUI)

Override Policy

A certificate being imported may be determined to already exist in ACS when it has either the same Subject or Issuer and serial number as an existing certificate. In such a case, selection of the "Replace Certificate" option will allow the certificate contents to be replaced while retaining the existing protocol selections for the certificate.

□ Replace Certificate

Use the “Browse” button to point to the correct Certificate and Private key files on your local PC.

Make sure that the Server certificate is in the “.der” format and the private key is in the “.pem” format and that OpenSSL 0.9.8 version and lower was used for their generation.

Enter the private key password that was used to generate the server private key.

Make sure that you check the “EAP: Used for EAP protocols that use SSL/TLS tunneling” checkbox.

Make sure the “Management interface” checkbox is unchecked (this is the default configuration).

Then press “Submit”.

3.3 CPE side

1. The certificate upload to the CPE shall be performed from the CLI. **In 4.3 version it will be possible via intuitive GUI screen.**
2. SSH the CPE and enter the shell.
3. Perform “ls” command and make sure there is ftp connectivity to the folder in which the certificates reside. “ls” will present you the remote (ftp) directory. Make sure that you copied there all the relevant certificates: cacert.pem, clientcert.pem (TLS only), clientkey.pem (TLS only) and random.
4. If it’s a brand new CPE, perform the following command to create the directories:
   mkdir “/tffs/certs/”
   mkdir “/tffs/certs/random”
5. Issue the following commands in the CPE shell to copy the files to flash:
   cp “random”,”/tffs/certs/random/random”
   cp “cacert.pem”,”/tffs/certs/cacert.pem”
   cp “clientcert.pem”,”/tffs/certs/clientcert.pem” (for TLS only)
   cp “clientkey.pem”, “/tffs/certs/clientkey.pem” (for TLS only)
6. Reboot the CPE.