SIEMENS

FAQ • 10/2014

How to manage the X.509 Certificates in RUGGEDCOM WIN BS and CPEs Software Version 4.2

RUGGEDCOM WIN

http://support.automation.siemens.com/WW/view/en/103158417

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 and Aptilo AAA server.

1.2 Related Documents

Table 1-1

Doc Name	Version	Notes
[1] IEEE 802.16e	D8	
RUGGEDCOM_WIN_X509_Certificate_SW_V4-3	V2.1	For Software Version 4.3

2 Certificate generation

X.509 certificates generation has to be done on Linux host. The procedure consists of 2 parts:

1. Modifying the relevant “cnf” files depending on the certificate type and the desired properties.
2. Running the “run.sh“ script from the folder where the “cnf” files are located. This script will create all the needed certificates for both server and client (CPE) sides and sign them with the CA certificate.

The following files are relevant to the certificate generation procedure:

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

NOTE For all the certificates generation the key size has to remain 1024 bits and hash algorithm shall remain MD5 at this stage.

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 (as per RUGGEDCOM specifics) 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 = 3650	Certificate validity period
[req]	
input_password = Cisco output_password = Cisco	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 = Ontario localityName = Concord organizationName = Siemens. emailAddress = info@Siemens.com commonName = "Siemens Certificate Authority"	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)

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.

The following subset of parameters is presented with their default values (as per RUGGEDCOM specifics) 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 = 3650	Certificate validity period
[req] input_password = Cisco output_password = Cisco	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.
[server] countryName = CA stateOrProvinceName = Ontario localityName = Concord organizationName = Siemens emailAddress = info@ruggedcom.com commonName = "Siemens Server 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.

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. Client certificate file also includes the client private key (in the same file) and it is put on the CPE. This is 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 (as per RuggedCom specifics) 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 = 3650	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, **in 4.1version this is NOT supported and the password shall remain Cisco. Moreover, EAP-TLS is not supported in 4.1.**
[client] countryName = CA stateOrProvinceName = Ontario localityName = Concord organizationName = Siemens. emailAddress = info@ruggedcom.com commonName = "Siemens 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.

2.4 Certificate generation script

Once all the above-mentioned certificates are modified and all the relevant “cnf” files are saved, the “run.sh“ script has to be executed from the directory where all the files are located in the following way: “./run.sh”

The result certificates will be stored in the “output” directory.

2.5 Format conversion

Sometimes, it’s useful to be able to see the exact values in the certificate in an understandable way. For this sake, the certificate has to be converted to “.der” format. In order to convert from “.pem” to “.der” format the following command has to be issued in openssl:

```
openssl x509 -in servercert.pem -out servercert.der -outform DER
```

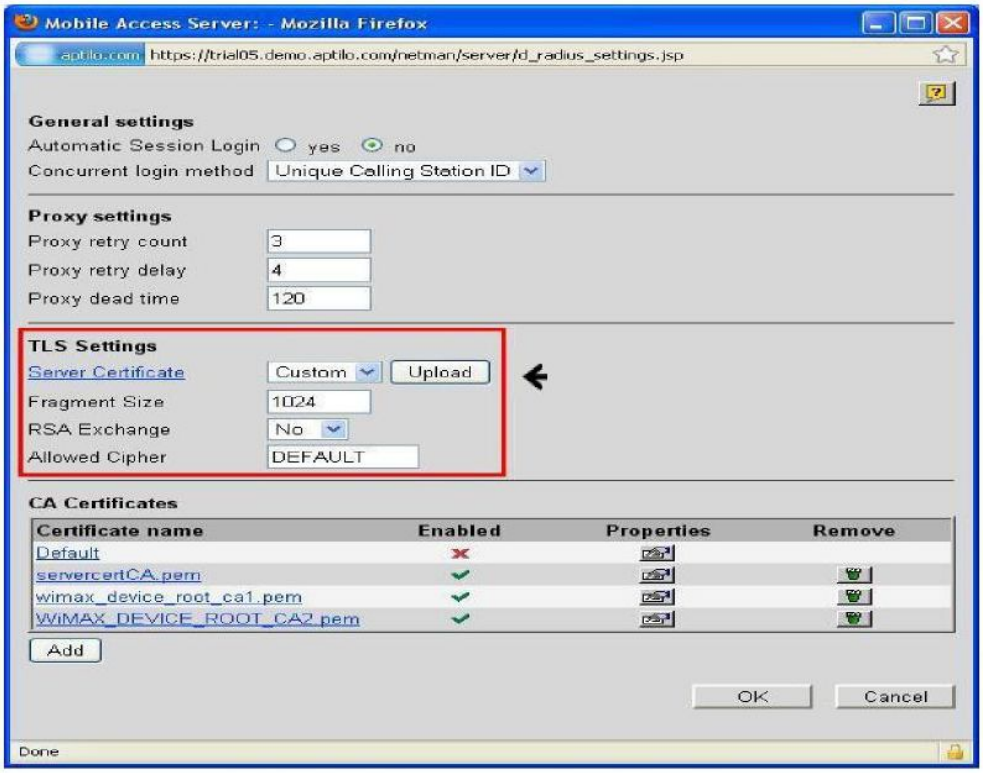
3 Certificate loading

3.1 Aptilo AAA side

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



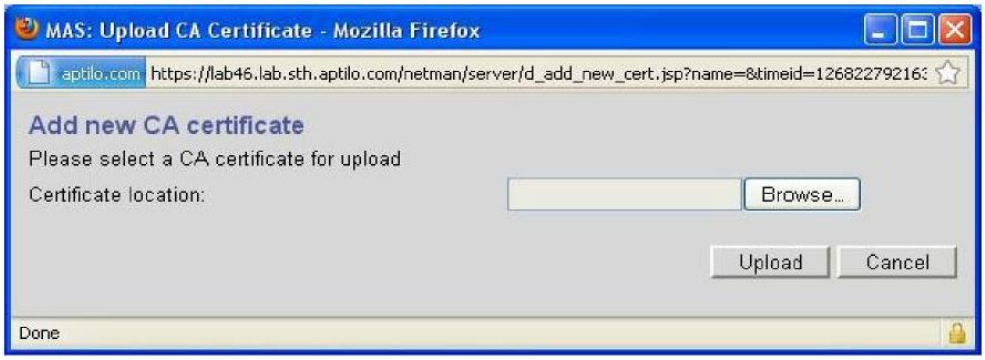
Pressing the “Upload” button opens the following screen.

Figure 3-2: Adding server certificate

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.

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



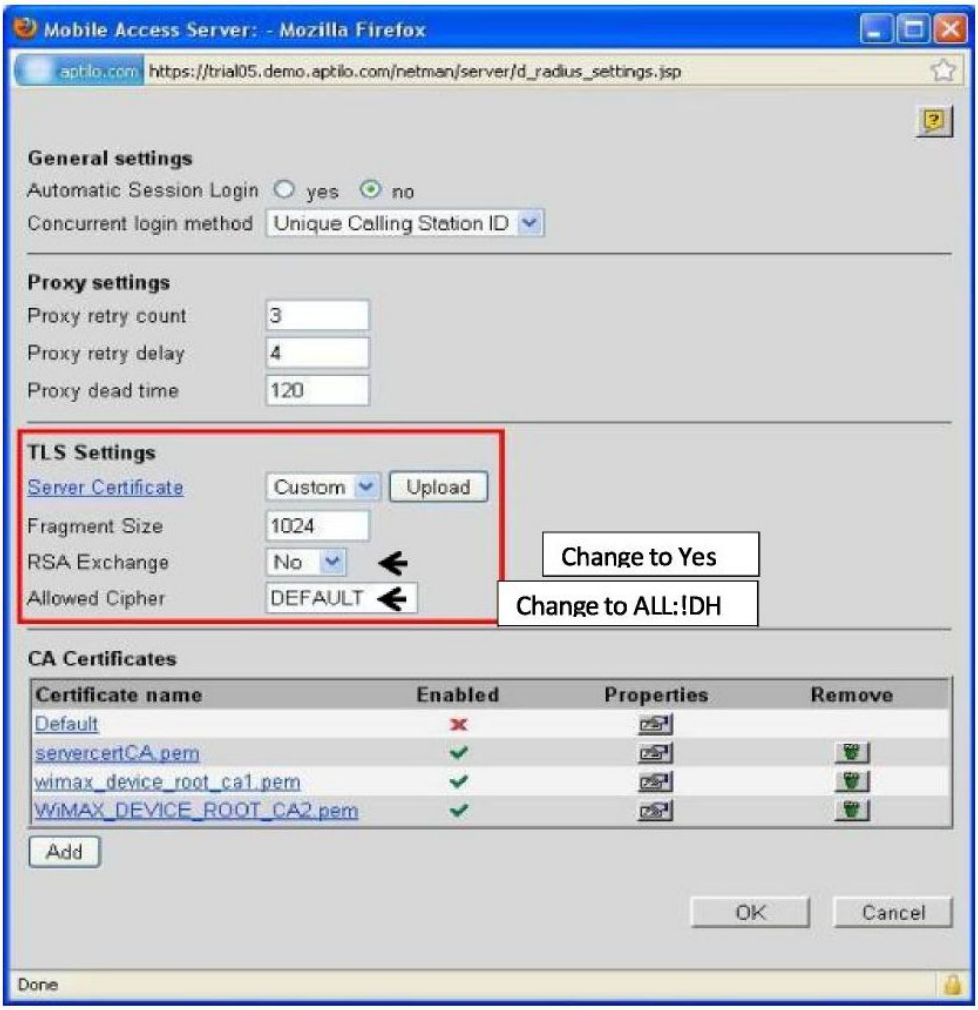
Use the “Browse” button and upload the CA certificate to “Certificate Location”.

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:

1. RSA key exchange from “No” to “Yes”.
2. Allowed ciphers from “DEFAULT” to “ALL:!DH”.
3. Restart Aptilo service. No need to reboot the server.

Here is the Aptilo GUI snapshot:

Figure 3-4: Aptilo cipher suite support



3.2 CPE side

1. The certificate upload to the CPE shall be performed from the CLI.
2. Telnet 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.