Com'X 210/510 Security Certificate Installation Guide

Schneider Electric

Introduction

For security purposes it is recommended to procure and install your own Public/Private SSL Certificate to harden your Com'X device. This guide details a multi-step process. The first part of the process involves creating a Com'X compliant certificate file from your SSL certificate & private key. The second part of the process instructs on how to install the certificate on a Com'X.

NOTE: This guide is applicable for Com'X firmware version 6.5 and above.

Additional resources

Document	References
Com'X 200/Com'X 210/Com'X 510 Instruction Sheet	5406AD002 5406AD005 5406AD006 5406AD007
Com'X 510 User Manual	DOCA0098EN DOCA0098FR DOCA0098ES DOCA0098DE DOCA0098PT DOCA0098IT DOCA0098ZH DOCA0098RU
Com'X 210 User Manual	DOCA0036EN DOCA0036FR DOCA0036ES DOCA0036DE DOCA0036PT DOCA0036IT DOCA0036ZH DOCA0036RU
Com'X 210/510 Hardening Guide	7EN12-0328

Safety Precautions

Installation, wiring, testing and service must be performed in accordance with all local and national electrical codes.

⚠**WARNING**
POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY   • Change default passwords to help prevent unauthorized access to device settings and information.   • Disable unused ports/services and default accounts, where possible, to minimize pathways for malicious attacks.   • Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).   • Use cybersecurity best practices (for example: least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, interruption of services, or unintended operation.   **Failure to follow these instructions can result in death, serious injury, or equipment damage.**

| *NOTICE* |
|---|
| **UNAUTHORIZED DATA ACCESS**

 • Immediately change the default password to a new, secure password.
 • Do not distribute the password to unauthorized or otherwise unqualified personnel.

 Failure to follow these instructions can result in equipment damage. |

Creating a Com'X complaint certificate

Validate the private key file

Prerequisite: Obtain an SSL Certificate from a trusted certificate authority. Save the Com'X certificate file (xxxxxxx.cert) and private key file (xxxxxxx.key) in a separate folder. This process requires the use of OpenSSL. Download and install OpenSSL by following the instructions provided on this website: https://tecadmin.net/install-openssl-on-windows/.

1. Open Command window as administrator:

2. Click ![Windows] button and type cmd.

3. Right click **Command Prompt** and select **Run as administrator**.
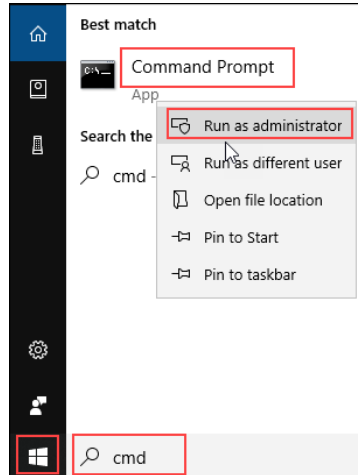
4. Enter openssl version in the command prompt and press Enter.

NOTE: This step ensures correct installation of OpenSSL.

5. Open the private key file using Windows Notepad or other text editor. The private key file typically ends with '.key' extension. The following steps assume the name of the key file is xxxxxxx.key as an example.

6. Close the private key file if the text begins with "-----BEGIN PRIVATE KEY-----".

7. Proceed to generate Diffie-Hellman parameters file.

Convert private key file

If the private key file content begins with "-----BEGIN RSA PRIVATE KEY-----", a conversion is required. Follow steps to convert an RSA private key to a private key.

1. Enter following command and press Enter.

```
openssl pkcs8 -topk8 -inform PEM -outform PEM -in
xxxxxxx.key -out new_xxxxxxx.key -nocrypt
```

2. Open the new private key file (`new_xxxxxxx.key`) in a text editor and verify the content begins with "-----BEGIN PRIVATE KEY-----".

3. If the text does not begin with "-----BEGIN PRIVATE KEY-----", go back to the step 1, and try again.

4. Close the new private key file.

   NOTE: Check if an output file (new_xxxxxxx.key) is created from the above command. If it is, warnings from OpenSSL command can be ignored.

Generate Diffie-Hellman parameters file

1. Enter the following command and press Enter.

   ```
   openssl dhparam -out dhparams.pem 4096
   ```


   The dhparams.pem file will be generated after several minutes (up to 15 minutes or longer).

Generate Com'X compliant certificate file

1. Create a new text file named [filename of your choice]. pem.

2. Copy and paste content from the new private key file (new_xxxxxxx.key). Text in this file begins with "-----BEGIN PRIVATE KEY-----".

3. Copy and paste content from SSL certificate file (xxxxxxx.cert). Text in this file begins with "-----BEGIN CERTIFICATE-----".

4. Copy and paste content from Diffie-Hellman parameters file (dhparams.pem). Text in this file begins with "-----BEGIN DH PARAMETERS -----".

   NOTE: Content to the .pem file must be pasted in the order shown below.

5. Save the new compliant certificate file with a .pem extension.

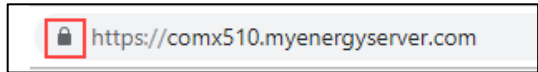# Installing Security Certificate

Install certificate file to Com'X

1. Open Com'X HMI and login as administrator.

2. Navigate to **Settings** > **Security** > **Certificates**.

3. Click Install a new certificate field and browse to select the compliant certificate (.pem) file.
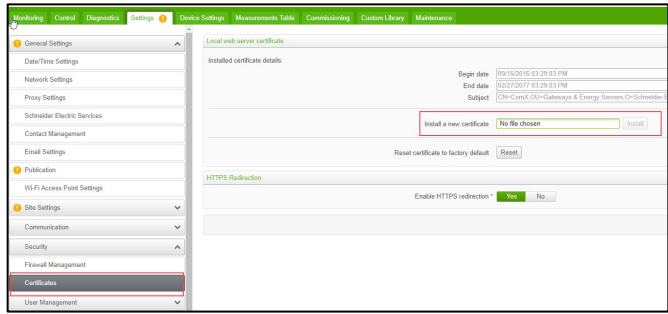
4. Click **Install**.

   The lock icon next to the Com'X URL in browser indicates successful installation.

5. Refresh page if the HMI is greyed out and displays "Application unreachable" after installing the new certificate.
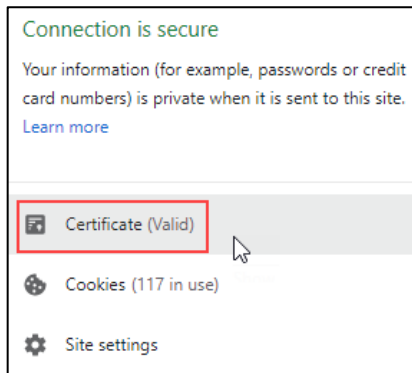
Check expiration date of SSL certificate file

The Com'X SSL certificate file (comx.cert) must be valid when using it to create a new Com'X compliant certificate file.
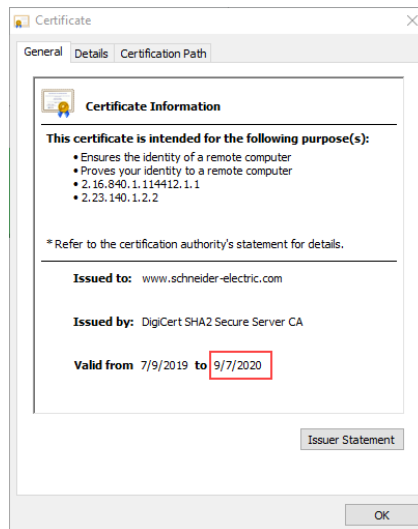
1. Click the lock icon next to the URL in a browser.

2. Click **Certificate** to view details.

3. Expiration date can be noted from the **Valid from – to** field.

The certificate must be renewed before the expiration date. Once you receive the renewed certificate, repeat process outlined in this document to create and install a new Com'X compliant certificate.