Server Authentication

Lumeta comes with a self-signed certificate that allows Secure Sockets Layer (SSL) for the web GUI out of the box. Best practice is to request and install a certificate from a trusted Certificate Authority (CA) that verifies the authenticity of the Lumeta system and avoids users from receiving warning messages like the one below:

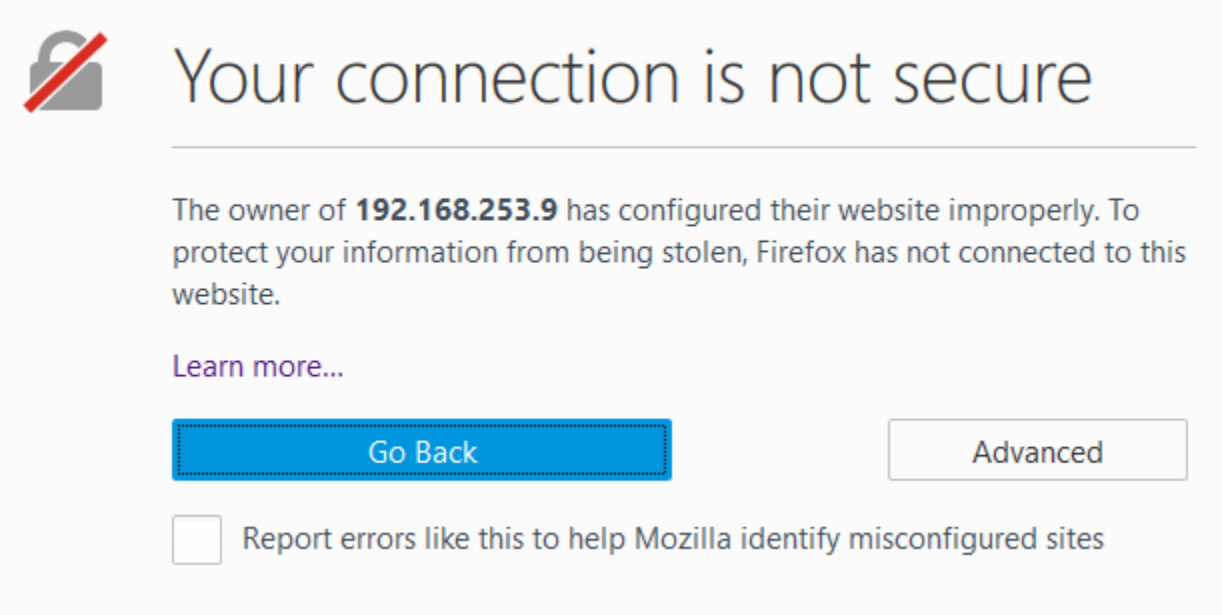

Figure 1: Warning when using untrusted Cert

It is recommended to enable Server Authentication for PKI User Authentication to be successful. Due to lock down restrictions, PKI User Authentication may not work without Server Authentication properly configured first.

A. Before you Begin

1. Verify tools putty, winscp, puttygen or similar are installed on your PC
2. Certificate Authority Public Chain has been installed.
    a. Discuss with your Network Admin how to access your company's CA public chain certificate and how it is recommended to install the chain.
3. Optional: Install the end CA Public certificate
    a. Your Network Admin may also supply the end CA certificate. This is the final CA of the chain. It can also be installed using the company recommended procedures.
4. Example how to Install the CA public certificate via your browser.
    a. On IE Navigate to Internet Options Content Certificates.
    b. Navigate to Trusted Root CA and select import to open the import tool and install the certificate.

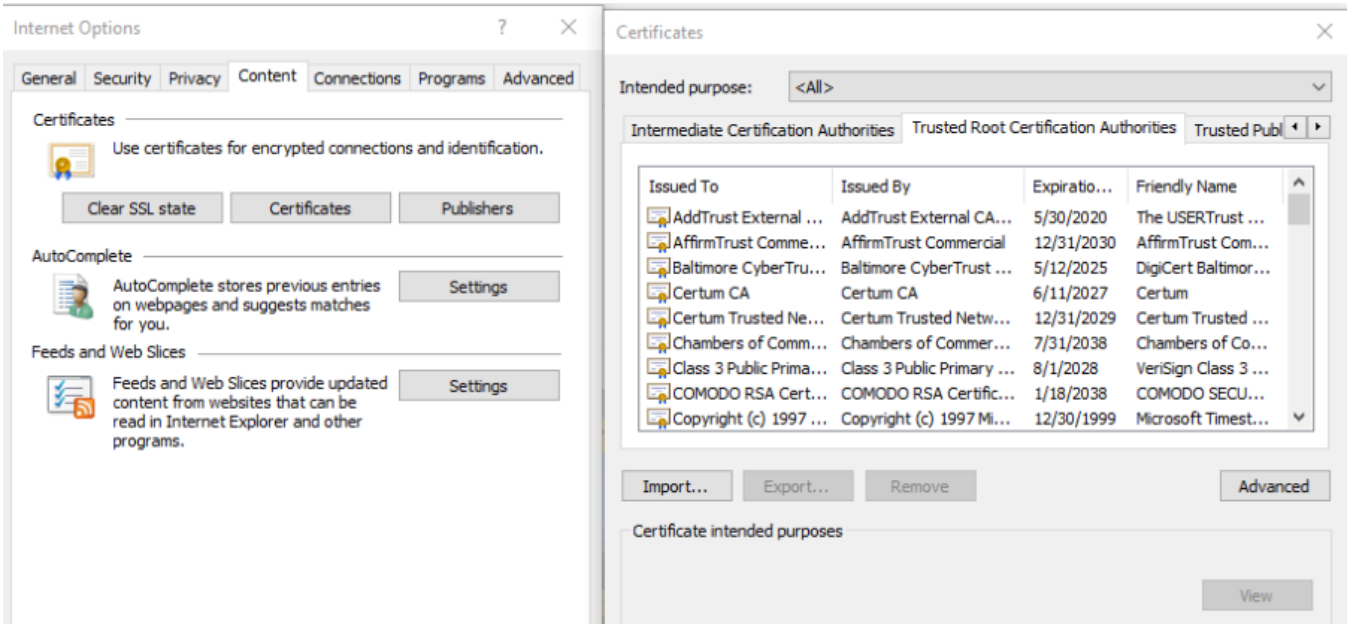

Figure 2: Import CA Certs to PC

B: Server Authentication

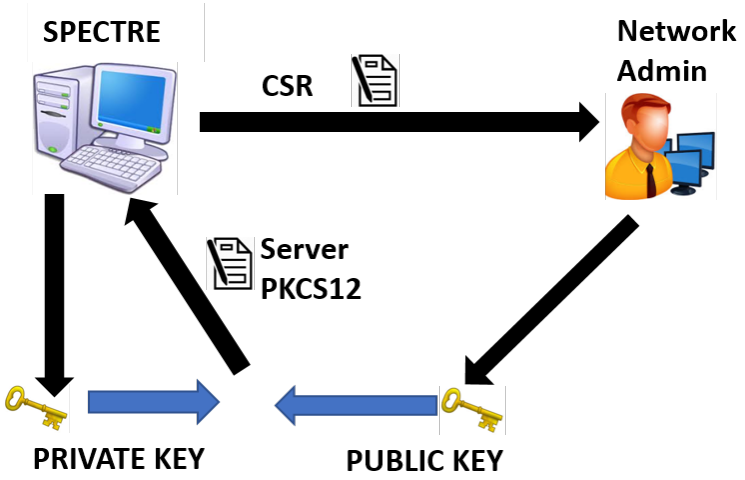

Figure 2: Sever Authorization

1. Certificate files you will need for Server Authorization

Below are the files you will need to obtain to configure server authorization. In parenthesis is the common format these files are in, however your Administrator may distribute the files in a different format.

1. Private Key of the Command Center (.key)
2. Certificate Signing Request for the Command Center (.csr)
3. Certificate Authority Public Certificate for Command Center (.cer)

2. Obtaining Server certificate files

Listed are openssl commands you can use to obtain the Command Center private key, the Certificate request, and the Command Center CA public key. These are only suggestions; please talk with your Network Admin if your company has specific ways to generate these files.

1. Private Key of the Command Center
    a. Below is an example how to create your Command Center Private Key.
        i. On the Command Center as the admin user type:
        openssl genrsa -aes256 -out "CC-private-key".key 2048
        ii. You will be prompted to enter a pass phrase twice. Type 'pwd' to show the file path your private key now resides. You will need to be in this path for all future opensslcommands in this section.
2. Certificate Signing Request for the Command Center
    a. Using the Command center private key from step a you will need to create a Certificate Signing Request to send to your PKI group or Network Administrator. Here is an example command to create your Command Center Certificate Signing Request.
        i. On the Command Center as the admin user type:
        openssl req -new -key "CC-private-key".key -out "CC-signing-req".csr
        ii. You will be prompted for the private key passphrase. You will then need to enter information for the request; please discuss with your Admin how to complete this form.
3. Certificate Authority public key for Command Center
    a. Submit the "**CC-signing-req".csr** from step b to your PKI group or Network Administrator. They will supply you with the Command Center public key verified by your company's Certificate Authority; usually named "**Command-Center-IP".cer**. Please confirm with your admin the format of this file; Lumeta recommends the file be in pkcs7 format.

3. Convert Server Certificate Files into the Correct Format

Transfer the "Command-Center-IP".cer public key to the Command Center via winscp into the same directory as the private key. Lumeta requires the Server certificate file be in pkcs12 format and a bundle of the Server private key and public key. The below openssl commands assumes the Command Center public key "Command-Center-IP".cer is in pkcs7 format.

1. Convert Command Center Public Key from pkcs7 to. pem format.
    a. On the Command Center as Admin User:
    openssl pkcs7 -print_certs -in "Command-Center-IP".pk7 -out "CC-certificate-pem".pem
2. Bundle the Command Center Private Key and the newly formatted Command Center Public Key into a pkcs12 file.
    a. On the Command Center as Admin User:
    openssl pkcs12 -export -in " CC-certificate-pem".cer -inkey "CC-private-key".key -out "CC-IPaddress-pkcs12".p12 -name "friendly-name"
    b. Provide a friendly name, you will be prompted for this name when installing the certificate.
    c. User will be prompted to enter the pass phrase for the private.key. Also the user will need to provide twice the Export Password.
    d. Remember the file name "CC-ipaddress-pkcs12".p12 file you created. If needed type pwd to remind yourself of the path this file resides.

4. Installing the Server Certificate

1. Through CLI: On the Command Center CLI type the following command to install the certificate:
    certificate server install "pathto/file/filename" "friendly-name" "private.key password"
2. Through WEB UI:
    a. Copy the "CC-ipaddress-pkcs12".p12 off the Command Center to your directory.
    b. On the UI navigate to Lumeta Systems and Manage PKI.
    c. Select Server Certificate from the Certificate Type. Upload the Certificate and input the Friendly Name and Password.

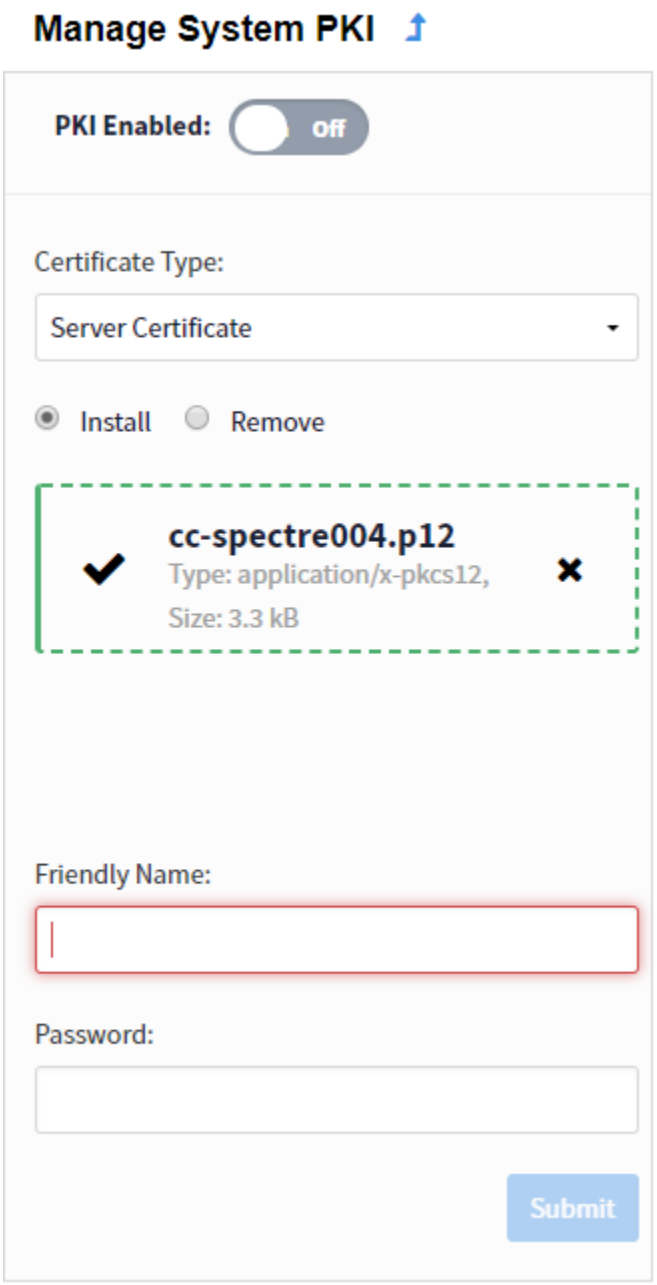

Figure 4: Install pkcs12 Server Certificate

APPENDIX A: Verifying Certificates

1. Verify the subject line of the CA-public.pem file matches the issuer line of the public-user.cer file using these openssl commands.
   openssl x509 -in public-user.cer -noout -subject -issuer
   openssl x509 -in CA-chain.pem -noout -subject -issuer
2. You can change the extension of the "public-user.cer" file to "public-user.txt" to view the certificate in notepad. Then this public-user certificate can be verified by comparing it to the "public-user".cer in the database by running this db command.
   select * from system.user_certificate;
3. The CA certificate can be verified in /etc/pki/lumeta folder. There will be a file 'httpd_ca.crt.' The timestamp should be updated to when the CA cert was uploaded. You can cat the file or run the below command to check the file:
   openssl x509 -in CA-chain.pem -noout -subject -issuer
4. View the issuers on the pkcs12 private/public bundle. Private Key Password needed.
   openssl pkcs12 -in hostname.site.ds.army.mil.pfx -nokeys | grep subject

5. Openssl command to check if certificate is in PEM format:
   openssl x509 -in cert.pem -text -noout
   a. If you get the following error it means that you are trying to view a non-PEM cert.
      unable to load certificate
      12626:error:0906D06C:PEM routines:PEM_read_bio:no start line:pem_lib.c:647:Expecting: TRUSTED CERTIFICATE

APPENDIX B: Common Errors

1. When Generating the pkcs 12 bundle for Server Authorization you may see this error:

   Please review the .key and .cer file for spaces or line returns. The CA .cer file is in the wrong format. Please confirm the .cer file is in PEM format
2. Passphrases with special characters:
   a. Special characters like exclamation points may cause problems since shell can misinterpret these characters. A workaround is to force input the passphrases into the openssl command. This will bypass the passphrase prompt.
      openssl pkcs12 -export -in CC-CA-public.cer -inkey*private.key -out cc-server.pfx * **-name CNAME -passin 'pass:exp@ss!!!word' -passout 'pass:exp@ss!!!word'**
3. Pkcs7 to PEM conversion fails with below error:

   This can occur if the file uses DER cipher. Please use the openssl command to perform the file conversion:
   openssl pkcs7 -in cert.p7b -inform DER -print_certs -out cert.pem

APPENDIX C: Log Debugging

1. In the CLI type the below commands to turn on proper log debugging to view Certificate info:
   log level set DEBUG API com.lumeta.api.impl.SessionServiceImpl
   log level set DEBUG API com.lumeta.api.dao.UserDaoImpl
2. View the Lumeta-webapp.out for "Looking for DN" and match the DN column with the database command select * from sytem.user_certificate.