Certificates for EzUGCC Web Server and/or FTP server

This information applies to both the TLS support within the monitor's integrated FTP server, as well as EzUGCC's integrated webserver. Therefore, the same certificate can be used for both. Be sure to read through the entire guide.

Certificate type

An x509 certificate is expected. These may be also called PFX or PKCS #12 files. They typically have a file extension of .pfx or .p12. It may be binary (DER) or Base64 encoded.

We'll use openSSL to generate our private key, CSR, and finally the X509 certificate. For simplicity we'll use openSSL to accomplish this.

OpenSSL is typically included in most Linux distributions. Windows users can download a copy from: https://wiki.openssl.org/index.php/Binaries.

If you are using Windows, and have a Linux system available, you can still generate a cert for use with EzUGCC/Monitor on the Linux box and copy the resulting pfx/p12 file to the windows box.

Generate your certificate

1. Generate CSR, this step is OS Dependent
    a. Linux
        i. First, create your private key:
            1. openssl genrsa -out server.key 2048
        ii. Next create a certificate signing request (CSR):
            1. openssl req -new -key server.key -out server.csr
        iii. Answer the questions. When you get to the Common Name field, be sure to enter the fully qualified domain name (FQDN) of the server this certificate will be used with (i.e. www.brainless.us).
    b. Windows
        i. I used the Firedaemon build to generate this documentation (https://kb.firedaemon.com/support/solutions/articles/4000121705)
        ii. First, create your private key:
            1. openssl genrsa -out server.key 2048
        iii. Next create a certificate signing request (CSR):
            1. openssl req -new -key server.key -out server.csr -config ..\..\ssl\openssl.cnf
        iv. Answer the questions. When you get to the Common Name field, be sure to enter the fully qualified domain name (FQDN) of the server this certificate will be used with (i.e. www.brainless.us).
2. Purchase a certificate. I've had good experiences with ssls.com and they are very affordable. Steps 2-4 will vary depending on what type of certificate you purchase and whom you purchase from.
3. Once purchased, provide your CSR generated in step 1. (server.csr)

4. The certificate vendor will have to verify you own the domain, business, etc. (these steps are determined by the type of certificate you order)
5. Once verification is complete, a certificate is provided to you. We'll now need to create an X509 certificate using this certificate and the private key we generated earlier.
    a. The below command will create a pfx certificate without a password. You can skip the -certfile option if no bundle was provided.
        i. openssl pkcs12 -export -nodes -out server.pfx -inkey server.key -in file_from_ssl_vendor.crt -certfile optional_bundle_file -passout pass:

Config files to update and where to place certificate files

NOTE: You should give your resulting pfx/p12 file a unique name (don't use ftp.pfx or cert.p12) as they may be overwritten when performing updates!

- Monitor Integrated FTP Server
    - ugccmon.cfg
        - Windows: c:\windows\system32\ugccmon.cfg
        - Linux: same folder as where the ugccmonsvc.exe is located (?/ugcc/mon)
        - Set the [FtpSSLCert] config line to server.pfx (or whatever name you choose)
            - If you don't have a [FtpSSLCert] line, simply add it. i.e.:
                - [FtpSSLCert]
                - server.pfx
        - Place the server.pfx file in the directory of your [LogConfig] setting
        - Restart the monitor server
            - Windows: net stop ugccmon and then net start ugccmon
            - Linux: systemctl stop ugccmon and then systemctl start ugccmon
        - Review the ugccmon.log log, the monitor will only complain if it can't find the file
- EzUGCC Webserver (for Windows only)
    - EzUGCC-WWW.exe.config
        - Located in C:\Program Files\EzUGCC (unless you specified a different path when installing)
        - Find the line
            - `<setting name="Certificate" serializeAs="String">`
        - Find the value line directly below and update the filename to server.pfx (or whichever name you choose)
            - If the line is missing, add it (i.e.)
                - `<setting name="Certificate" serializeAs="String">`
                - `<value>server.pfx</value>`
                - `</setting>`
        - Place your server.pfx certificate in the same folder as the config file and EzUGCC-WWW.exe executable
        - Restart the ezugcc-www service

        - net stop ugcc-www
        - net start ugcc-www
- Review the EzUGCC.log. The EzUGCC server will complain if it's unable to find the certificate.