HTTPS & SSL Certificates Tutorial

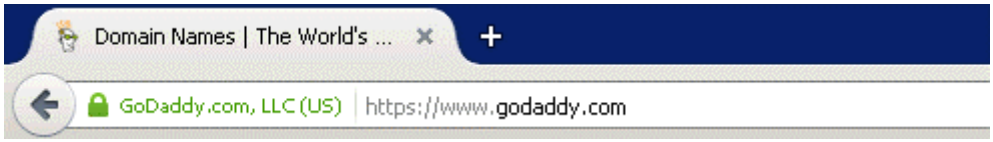
Terminal Service Plus HTTPS & SSL Features

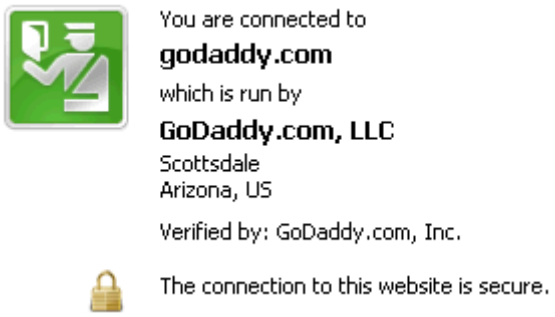
The Web Server included with Terminal Service Plus can manage HTTPS protocol, SSL encryption with either self-signed certificate or CA certificate delivered by a Certificate Authority (CA).

The HTTPS protocol encrypts the communication between the client and the server.

The unique certificate, generated from a 2048 Bits RSA key, includes the encryption key and the certification of the Server or the Domain Name on which the user is connected.

The user is informed that the communication is encrypted and the Server or Domain name is certified by a Certification Authority.
This information appears in the address bar of the navigator, as a green padlock.





In this tutorial, we will learn how to install a certificate in the Terminal Service Plus Web Server, providing users the security of HTTPS, 2048 SSL encryption and Domain name certification.

In order to receive an SSL Certificate we recommend you purchase it from a trusted vendor as GoDaddy or DigiCert .

Please follow this procedure to order and install your SSL on the TSplus Gateway / Server.

Tutorial Content

4. Important notice about the Key Pair (Private Key)

2. How to do a CA Request and Get a Certificate

    1. Reminder - Certification process
    2. How to generate a CSR (Certificate Signing Request)
    3. How to get a SSL Cert
    4. How do I generate what I need for TSplus?

3. Trouble shooting

    1. I received only one file (.crt or cer) which contains MydomainName.com Certificate
    2. My private key is .pem. I cannot import my private key in Portecle
    3. HTTPS errors
    4. Notice concerning Terminal Service Plus and Microsoft IIS web server

Note: You can use this SSL Server Test tool in order to validate the good quality of a web portal in HTTPS.