Free and Easy-to-install HTTPS Certificate

Overview

Starting with version 9.20, Terminal Service Plus provides an easy to use feature to generate of a free and valid HTTPS certificate.

In 3 mouse clicks you will get a secured valid certificate, renewed automatically, and configured automatically into Terminal Service Plus built-in web server.

This feature uses Let's Encrypt to provide a free and secure HTTPS certificate for your HTTPS connections.

Prerequisites

Please ensure that your Terminal Service Plus server meet these requirements before using the Free Certificate Manager:

- You must **use Terminal Service Plus built-in web server listening on port 80 for HTTP**. This is required by Let's Encrypt domain ownership validation process.

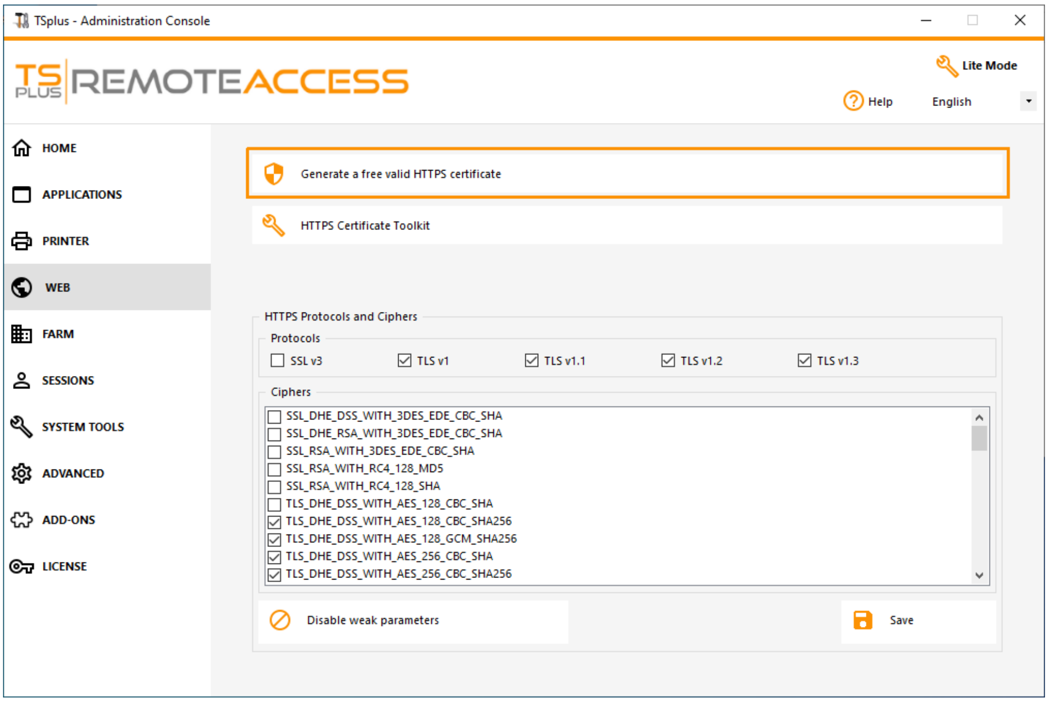
- Your **server's domain name must be accessible** from the public Internet. This is required as well to validate that you are the real owner of the domain.

- You must **run this program on the Gateway server or a Standalone server, not an Application server** (except if your Application Server is accessible from the public Internet and has a public domain name).

It is not possible to get a certificate for an IP address, be it public or private.
It is not possible to get a certificate for an internal domain name (i.e. a domain which only resolves inside your private network).

Free Certificate Manager GUI

To open Terminal Service Plus Free Certificate Manager GUI, open Terminal Service Plus AdminTool, click on the "Web - HTTPS" tab, then click on "Generate a free valid HTTPS certificate" as shown in the screenshot below:



HTTPS Protocols and Ciphers

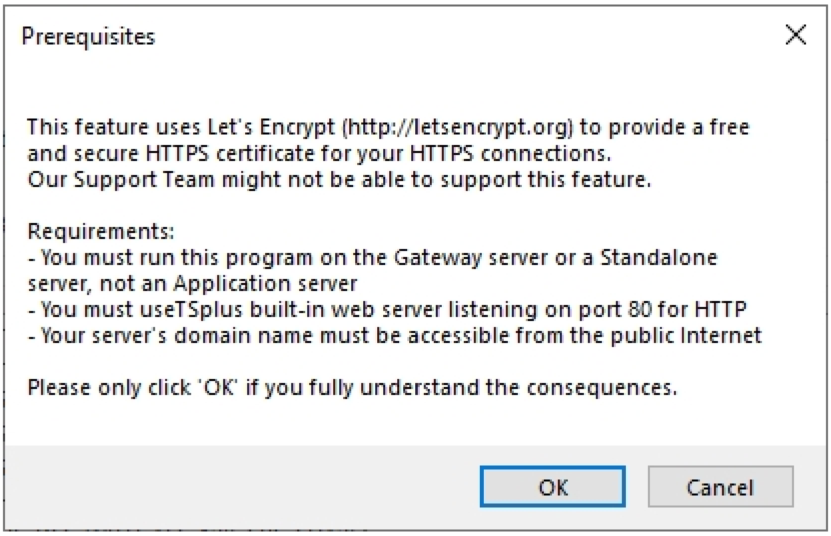
Protocols

☐ SSL v3 ☑ TLS v1 ☑ TLS v1.1 ☑ TLS v1.2 ☑ TLS v1.3

Ciphers

☐ SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
☐ SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
☐ SSL_RSA_WITH_3DES_EDE_CBC_SHA
☐ SSL_RSA_WITH_RC4_128_MD5
☐ SSL_RSA_WITH_RC4_128_SHA
☐ TLS_DHE_DSS_WITH_AES_128_CBC_SHA
☑ TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
☑ TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
☑ TLS_DHE_DSS_WITH_AES_256_CBC_SHA
☑ TLS_DHE_DSS_WITH_AES_256_CBC_SHA256

The Free Certificate Manager GUI will open and remind you about the prerequisites, as shown in the screenshot below:



This feature uses Let's Encrypt (http://letsencrypt.org) to provide a free and secure HTTPS certificate for your HTTPS connections.
Our Support Team might not be able to support this feature.

Requirements:
- You must run this program on the Gateway server or a Standalone server, not an Application server
- You must useTSplus built-in web server listening on port 80 for HTTP
- Your server's domain name must be accessible from the public Internet

Please only click 'OK' if you fully understand the consequences.

Please read carefully and check that your server meet all the requirements, then click on the "Ok" button.

Step 1: Enter your Email

This email will not be used to spam you. Actually it will not even be sent to TSplus or any third party, except the certificate issuer: Let's Encrypt.

They will only contact you if needed, according to their Terms Of Service.

Step 2: Enter the server's Domain Name

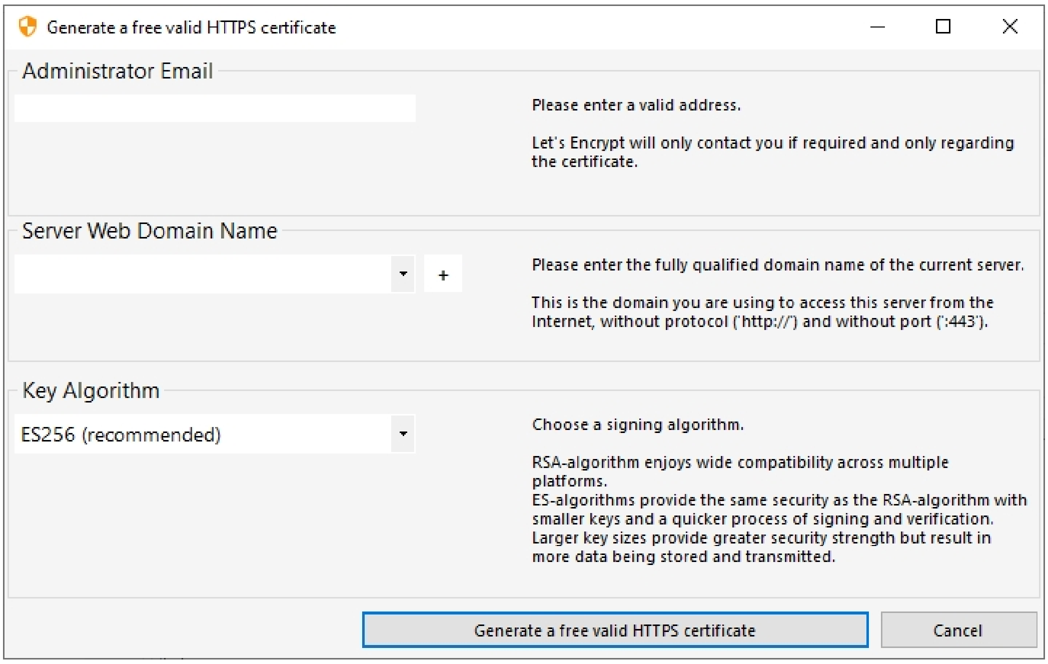
This is the public Internet accessible Domain Name, something like gateway.your-company.com. You can also add another domain name or a subdomain name after clicking on the "+" button.

As explained in the GUI, do not add a protocol prefix and/or a port suffix, just enter the clean domain name(s).

The certificate will be generated for this domain name, and it will only be valid on a web page hosted at this domain name. If your users connect to your Web Portal using https://server1.example.com:1234, then you must enter "server1.example.com".

Step 3: Choose a Key Algorithm

It will be used to create key pairs and perform digital signature operations.



Generate a free valid HTTPS certificate

Administrator Email

Please enter a valid address.

Let's Encrypt will only contact you if required and only regarding the certificate.

Server Web Domain Name

Please enter the fully qualified domain name of the current server.

This is the domain you are using to access this server from the Internet, without protocol ('http://') and without port (':443').

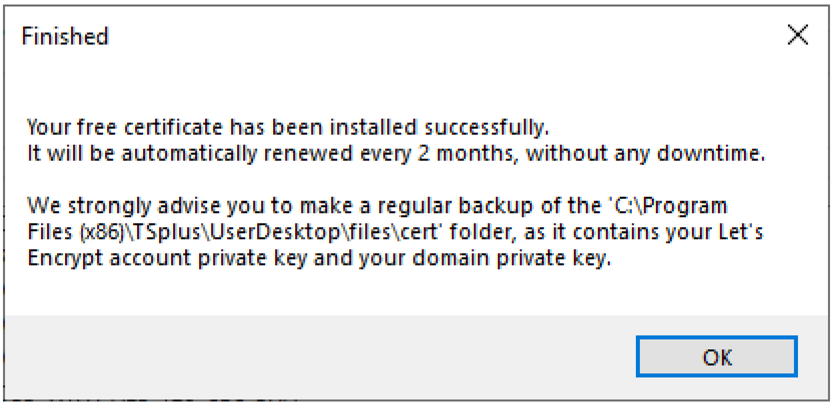
Key Algorithm

ES256 (recommended)

Choose a signing algorithm.

RSA-algorithm enjoys wide compatibility across multiple platforms.
ES-algorithms provide the same security as the RSA-algorithm with smaller keys and a quicker process of signing and verification.
Larger key sizes provide greater security strength but result in more data being stored and transmitted.

Enjoy your Certificate!



Finished

Your free certificate has been installed successfully.
It will be automatically renewed every 2 months, without any downtime.

We strongly advise you to make a regular backup of the 'C:\Program Files (x86)\TSplus\UserDesktop\files\cert' folder, as it contains your Let's Encrypt account private key and your domain private key.

Terminal Service Plus Free Certificate Manager will now use all the data to connect with Let's Encrypt, validate that you really own the domain name you typed, and get the matching valid certificate.

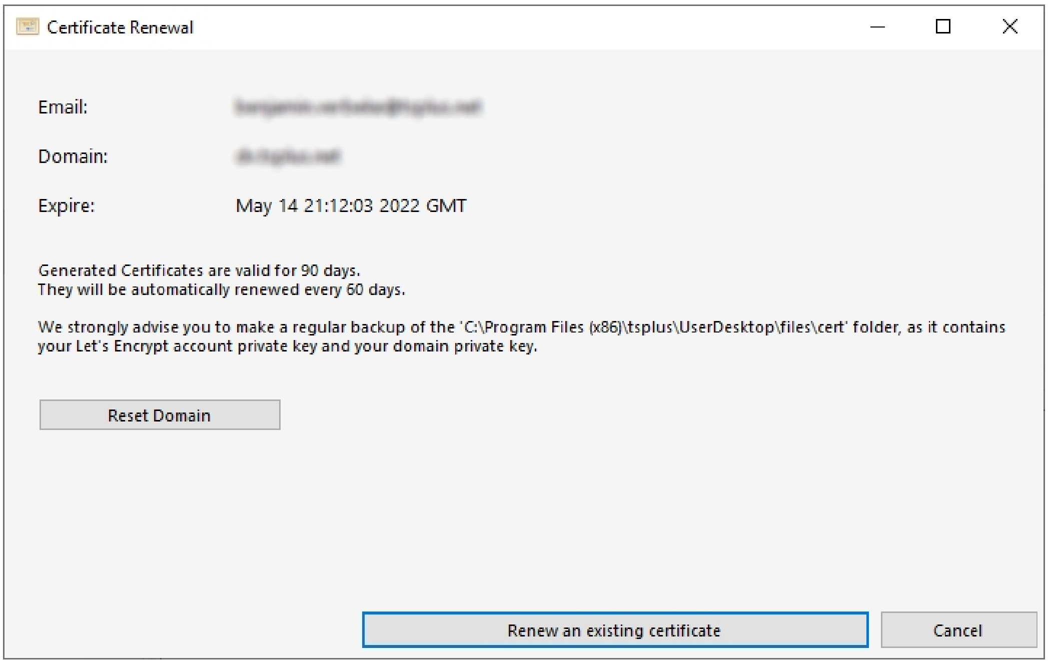
Once the program receives the certificate, it will automatically handle all the required file format conversions and softly reload Terminal Service Plus built-in web server in order to apply the new certificate to every new connection. The web server is **not** restarted and no connection is stopped.

Certificate Renewal

Let's Encrypt certificates are valid for 90 days.

Terminal Service Plus will automatically renew the certificate every 60 days for safety. A check is done at every reboot of the Windows server, and then every 24 hours.

You can manually renew your certificate by opening the Free Certificate Manager tool. It will display the domain name of the certificate and its expiration date, as shown in the screenshot below.



Certificate Renewal

Email: [redacted]

Domain: [redacted]

Expire: May 14 21:12:03 2022 GMT

Generated Certificates are valid for 90 days.
They will be automatically renewed every 60 days.

We strongly advise you to make a regular backup of the 'C:\Program Files (x86)\tsplus\UserDesktop\files\cert' folder, as it contains your Let's Encrypt account private key and your domain private key.

To manually renew your certificate, just click on the "Next" button.

The "Reset Domain" button on this window deletes the SSL certificate and reconfigure the Web Server to its original state before using the Certificate Manager.

Best Practices

If no error occurs, Terminal Service Plus will renew the certificate automatically every 60 days. We recommend that you **check every 60-70 days** that your certificate has been automatically renewed.

We also recommend that you **backup at least every month** the following folder and its sub-folders:

```
C:\Program Files (x86)\TSplus\UserDesktop\files\.lego
```

This is an internal folder, containing your Let's Encrypt account private key, as well as the key pair of your certificate.

Troubleshooting

In case of an error, please contact support and email them the following log file:

```
C:\Program Files (x86)\TSplus\UserDesktop\files\.lego\logs\cli.log
```

This log file (and maybe the other log files in the same folder) should help our support team to investigate and to better understand the issue.

If you want to restore a previously used certificate, go to the folder:

```
C:\Program Files (x86)\TSplus\Clients\webserver
```

It will contain every "cert.jks" files used. These are the "key store" files and we never delete them, we only rename them with the date and time of their disabling.

Error Codes

- Error 801: Free Certificate Manager was not able to register your Let's Encrypt account. Check your Internet connection. Check that your email is not already registered at Let's Encrypt. Try again with another email.

- Error 802 & Error 803: Free Certificate Manager could not retrieve Let's Encrypt Terms Of Service URL address. This is a non blocking error: you can still continue and accept Let's Encrypt Terms Of Service - be sure to read them from your browser first of course.

- Error 804: Free Certificate Manager was not able to validate your agreement to Let's Encrypt Terms Of Service with Let's Encrypt servers. Check you Internet connection. Try again.

- Error 805 & Error 806: Free Certificate Manager was not able to validate that you own the domain you entered during certificate creation (Error 805) or certificate renewal (Error 806). Check again all the prerequisites. Check your Internet connection. Check that your web server is listening on port 80. Check that you do not use a third-party web server such as IIS or Apache. Check that your domain name is accessible from the public Internet.

HTTPS Certificate Command Line

Preparing the Certificate Configuration File

Inside the “C:\Program Files (x86)\TSplus\UserDesktop\files\cert” folder, create a file named “FreeCertificateManager.ini” if it does not already exist. Make sure your text editor and/or Windows file explorer does not add an ending “.txt” extension.

Edit the file and write or update it so it has the following format, then save it:

```
[settings]

email = your.email@company.com

domain = your-server- domain-name.company.com
```

Creating the Certificate

As a server administrator, run the following command:

```
"C:\Program Files (x86)\TSplus\UserDesktop\files\cert\CertificateManager.exe" /create
```

In order for this command to be successful:

- The “FreeCertificateManager.ini” file must exist and use the expected format
- Your TSplus Remote Access server must be up and running
- Your TSplus Remote Access Web Portal must be available with protocol

HTTP on port 80 from the internet public network, as TSplus HTTPS certificate provider will use that to validate the server domain name

Renewing the Certificate

Once the certificate is configured and created, TSplus Remote Access will automatically renew it every two months to make sure it never expires.