Choosing your Ciphers Suites to enhance security

Overview

TLS/SSL, the security behind HTTPS, can use several different algorithms to secure, encrypt and authenticate a connection.

The choice of the algorithm to use is decided by an agreement between the server and the client, depending on which algorithms are available on each side.

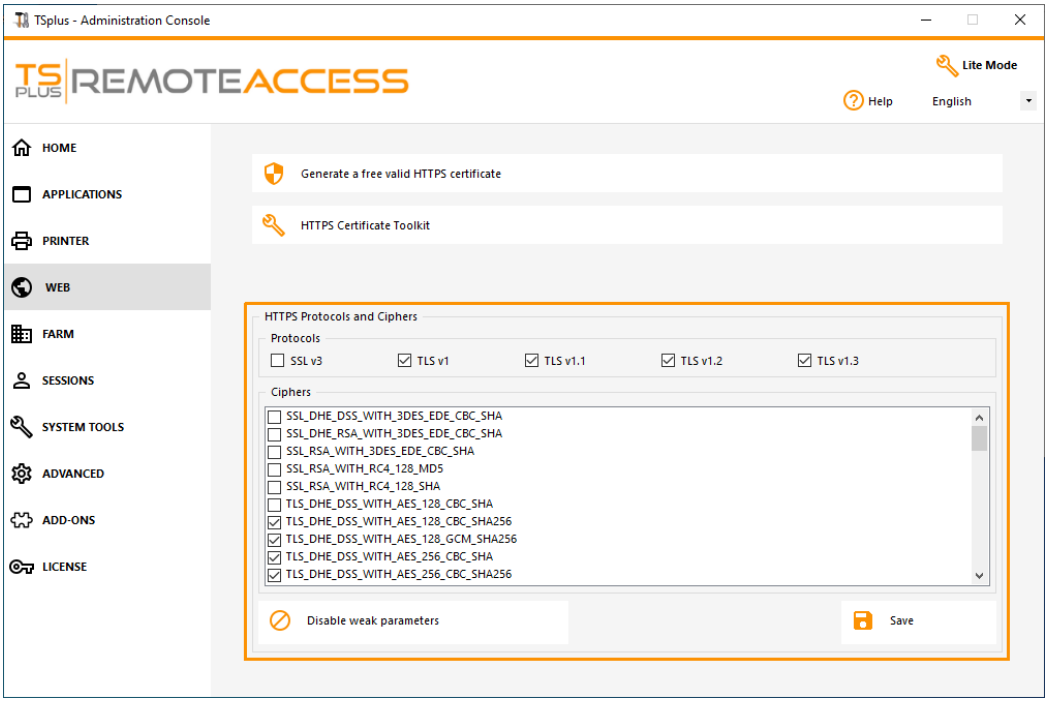
A cipher suite is a named combination of authentication, encryption, message authentication and key exchange algorithms.

Terminal Service Plus server can handle a lot of different ciphers suites. Some of them are more secure than others, but some old/legacy browsers might require relatively weak algorithms to connect.

This is the reason why Terminal Service Plus let you choose the ciphers suites you want to enable. Of course, Terminal Service Plus also has an easy setting to disable the weakest algorithms, thus enhancing your connections security.

HTTPS Protocols and Ciphers Selection

To see Terminal Service Plus Ciphers Selection, open Terminal Service Plus AdminTool, click on the "Web - HTTPS" tab, where you will see HTTPS Protocols and Ciphers:



Enabling/Disabling a Cipher Suite

You can easily enable a cipher suite by checking its checkbox and disable a cipher suite by unchecking it.

When your selection is done, click on "Save".

This will save your selection and reload the new configuration in Terminal Service Plus built-in web server. Your new ciphers suites selection is instantly applied for every new connection to your server.

Recommended Ciphers Suites Selection

We recommend to most administrators to use our recommended ciphers suites selection, by simply clicking on the "Disable weak parameters" button and then on the "Save" button.

This action will disable all ciphers suites which are currently known to be weak.

You can check with SSL Labs Online Testing Tool: without those weak ciphers suites you should get the maximum grade: A!