Differences between SSL/TLS vs STARTTLS

Ioanna Anifanti - 2022-11-09 - Email Clients

The terms SSL, TLS, and STARTTLS are often confused with one another. In this article we will look at the differences between them in order to clarify these concepts.

SSL/TLS

Secure Socket Layer (SSL) and Transport Layer Security (TLS) are both powerful encryption protocols that provide security for communication on a network. Network means for example, when a client connects to a server.

These protocols are used in our daily lives in many applications such as our web browsing, email service, file transfer, instant messaging, teleconferencing, VoIP, etc. TLS is the continuation of the SSL protocol.

The SSL and TLS version numbers from the oldest to the newest are: SSL v2, SSL v3, TLS v1.0, TLS v1.1, TLS v1.2, TLS v1.3.

The versions now supported by our infrastructure are TLS v1.2 & v1.3. The other versions have been removed due to known vulnerabilities.

Check which version of TLS is compatible with the software platform or operating system you are using.

STARTTLS

STARTTLS differs from SSL and TLS as it is not a communication protocol. It is a command protocol used to inform the email server that the email client wants to upgrade the connection from an insecure to a secure one by using an SSL or a TLS protocol.

More specifically, in the past, before the encrypted communication method using secure ports was established (e.g. 587, 465, 995, 993), many insecure connections between a

client and a server were performed by using default ports (such as 25, 143 & 110). This puts data and important information at risk of being intercepted. STARTTLS came to help reduce this risk by converting the unsecured connection to a secure one by using either an SSL or a TLS.

In other words, STARTTLS uses ports 25, 143 & 110 but in an encrypted way. That's how it works: during the first communication the connection is made without encryption. Then, the client sending the email will ask the server if it supports an encrypted method. Whether the server supports an encrypted method, then an encrypted communication will be set between them. If the server does not support an encrypted method, then the connection will not be upgraded and will return to the original insecure communication (something that is not recommended for security and privacy reasons). We suggest that this first communication should be always secured because sensitive information (such as username & password) shared should not be intercepted.

Here is an example. During SMTP communication, if the communication takes place on port 587, the connection is secure which is ideal. If the connection is made on port 25 then it will be insecure. However, by using STARTTLS sent commands will upgrade it to a secure connection.