

Check SSL installation

Test SSL connectivity with `s_client` commands to check whether the certificate is valid, trusted, and complete. The OpenSSL toolkit helps to check the SSL certificate installation on a server both remotely and locally. In the command line, enter **`openssl s_client -connect <hostname>:<port>`**. This opens an SSL connection to the specified hostname and port and prints the SSL certificate.

Command Options	Description	Example
-connect	Tests connectivity to an HTTPS service.	<code>openssl s_client -connect <hostname>:<port></code>
-showcerts	Prints all certificates in the certificate chain presented by the SSL service. Useful when troubleshooting missing intermediate CA certificate issues.	<code>openssl s_client -connect <hostname>:<port> -showcerts</code>

Port using STARTTLS

In order to check STARTTLS ports, the following command should be run. Replace [port] with the port number and [protocol] with smtp, pop3 or imap value:

```
openssl s_client -connect example.com:[port] -servername example.com -starttls [protocol]
openssl s_client -connect 192.168.178.xx:25 -servername oscardegroot.nl -starttls smtp
openssl s_client -connect 192.168.178.xx:143 -servername oscardegroot.nl -starttls imap
```

Port not using STARTTLS

In order to check non-STARTTLS ports, use the following command:

```
openssl s_client -connect 192.168.178.xx:443 -servername www.oscardegroot.nl
openssl s_client -connect example.com:[port] -servername example.com
```

From:

<https://wiki.oscardegroot.nl/> - HomeWiki

Permanent link:

<https://wiki.oscardegroot.nl/doku.php?id=networking:ssl-installation>

Last update: **2024/08/14 16:45**

