

[Products](#) > [Software](#) > [Transaction Systems](#) > [TPF](#) > [Tools](#) >

## Overview of Apache with SSL

A secure web server combines the features of the a web server (Apache) with secure sockets layer (SSL) or transport layer security (TLS). In order to do this, an interface module is needed between Apache and SSL. The module we have ported to TPF is called `mod_ssl`.

The protocol between the web browser or client and the web server is called hypertext transfer protocol (HTTP). When HTTP is combined with SSL, it is called hypertext transfer protocol with security (HTTPS). This is described in more detail in RFC 2818.

In a non-secure web server, the HTTP data moving between the web browser and web server flows 'in the clear'—anyone in the network can see it or even tamper with it and you won't be the wiser. In secure mode however, web data has all the benefits of SSL: data privacy (no one can see your data), data integrity (no one can tamper with your data) and authentication (you are talking to a server you trust and it hasn't been spoofed).

We distribute Apache 1.3.26 and `mod_ssl` 2.8.10 together already configured for TPF in a tarball. You must use the file supplied by TPF; the source at [www.apache.org](http://www.apache.org) and [www.modssl.org](http://www.modssl.org) does NOT have the TPF changes.

Apache and `mod_ssl` have the following TPF system requirements:

PUT15 APARs PJ27863 and PJ28118 (these implement OpenSSL 0.9.6)

PUT15 APAR PJ28021 (`tpf_select_bsd`)

PUT16 APAR PJ28369 (allows `mod_ssl` to link to OpenSSL 0.9.6)

In addition, you need to obtain a SSL digital certificate. It may be in the form of one file containing both a key and certificate, or separate key and certificate files. You must upload them to TPF and update your `httpd.conf` file accordingly (see [install\\_https.htm](#) for more information). Without a digital certificate, Apache can not run in secure mode.

## Current restrictions

`Mod_ssl` runs as a single process (a single long-running ECB). Do not remove the option `-DONEPROC` from the file `src/os/tpf/TPFExport`.

The Apache server is stopped with the command `ZINET STOP S-APACHE`. However in the single process mode supported by `mod_ssl`, the ECB will remain in the system following a stop until there is activity on the listener sockets, at which point the ECB exits since it then sees the pending stop.

The SSL key file must not be encrypted or password protected. We expect this is only a temporary restriction. We suggest that you set the ownership and permission bits as follows to minimize access to the SSL key:

```
zfile chmod 400 /path_to_your_key_file
```

```
zfile chown http:http /path_to_your_key_file
```

CGI scripts may fail in secure mode from Netscape browsers. If you get unexpected failures in secure CGI scripts, switch to a different browser.

Any restrictions listed in [readme\\_ap.htm](#) also apply.

To install the secure web server, follow the instructions in [install\\_https.htm](#) instead of [install\\_ap.htm](#).

## More information

TPF Systems Technical Newsletter articles:

["Serve Up a Nice Web Dish, but Keep It Covered Until It Gets to the Table"](#) 1Q2002

"Make Sure Your System Is Securely Fastened While Traffic Is Flowing". 3Q2001

RFC 2818

[www.modssl.org](http://www.modssl.org) (again, don't download code from this site for TPF, but it has a very good reference for the SSL specific tags in `httpd.conf`)