

[Products](#) > [Software](#) > [Host Transaction Processing](#) > [TPF](#) > [Tools](#) >

## Installing the Secure Apache 1.3 HTTPS Server on TPF

This document outlines the steps needed to install Apache with security enabled onto a TPF system. Note that there are differences between this procedure and the non-secure Apache 1.3 procedure.

You should first read [readme\\_https.htm](#) for basic information on the port of Apache to TPF including required maintenance levels.

### Download

Releases of the Apache server are compressed into a "tarball" file that must be downloaded to your PC. Additionally the source code from the tarball will need to be copied onto an OS/390 UNIX System Services machine (later referred to simply as "OS/390 UNIX") for compiling. Here are all the details on how to get Apache and how to get it where it needs to be:

1.Download the compressed Apache files (the "tarball") to your PC. The file name on the web site will be something like `https_1.3.xx.tar.Z`. TIP: Be sure to keep the `.tar.Z` extension when choosing the name of the PC file.

2.Decompress the tarball on your PC using WinZip or some other PC decompression tool. TIP: If you are using WinZip verify that the "TAR File Smart CR/LF Conversion" option (under Options, Configuration) is NOT checked. This is what you can expect if you use WinZip:

open the tarball with WinZip (this can usually be done simply by double-clicking on the downloaded tarball)

you will be told that the archive contains one file (such as `https_1.3.xx.tar`) - allow WinZip to decompress it to a temporary folder

extract the archived files onto your PC - you'll be using files from the `conf`, `htdocs`, and

`icons` directories later in the install phase

3.FTP the tarball to your OS/390 UNIX machine using binary mode:

activate FTP in an MSDOS window: `ftp your.os390.unix.machine.com`

sign in

set mode to binary: `binary`

send the file to OS/390 UNIX:

send `c:\downloaded_filename.tar.Z os390_unix_filename.tar.Z`

exit FTP: `bye`

TIP: UNIX file names are case sensitive. If you use an NFS client to transfer files from your PC to OS/390 UNIX (instead of using FTP as described above) verify that the NFS drive will transfer the file names with upper/lower case preserved.

4.Decompress and extract the archived files necessary for compiling Apache:

```
pax -rvz kf os390_unix_filename.tar.Z -o from=ISO8859-1,to=IBM-1047
```

5. From the location where you just ran pax, change the directory to the source tree:

```
cd apache_1.3.23/src
```

## Compilation

NOTE: Apache in `https_1.3.xx.tar.Z` is already configured for `mod_ssl` and a standard set of modules. Normally, you shouldn't need to run `configure`. If you do, always call `configure` as follows:

```
export SSL_BASE=/your_ssl_location/openssl-0.9.6
```

```
configure --enable-module=ssl ...remaining options as specified in install_ap.htm...
```

1. Indicate if you would like to use the TCP/IP network services database. (This only applies if you are using TCP/IP native stack.)

If you are on a PUT16 or higher system, or have PJ28195 installed, you can use the TCP/IP network services database. To do so, you must do one of the following:

```
add "#define TPF_HAVE_NSD" to os/tpf/os.h or
```

```
add "-DTPF_HAVE_NSD" to the _C89_OPTIONS export in os/tpf/TPFExport
```

See TPF Transmission Control Protocol/Internet Protocol for more information about the TCP/IP network services database: <http://www.ibm.com/tpf/pubs/tpfpubs.htm>.

2. Indicate location of include directories

In the file `os/tpf/TPFExport`, update the variable `_C89_INCDIRS` to point to the directories of your SSL includes, `mod_ssl` includes and TPF includes.

3. Set the TPF environment variables: `. os/tpf/TPFExport`

TIP: The initial period and blank on the command are required to ensure the environment variables exist beyond the scope of the shell script.

This script will set the environment variables required to compile the programs for TPF. Verify that the export variables are valid for your installation, in particular, the system include file directories. The system include files must reside on your OS/390 UNIX system in the appropriate file structure similar to `/usr/include` and `/usr/include/sys`. DO NOT modify the `TPF=YES` export variable if you plan to run the "Configure" script.

4. Now compile the programs: `gnumake`

Besides compiling, `make` also runs `main/gen_test_char.c` and `main/gen_uri_delims.c` in order to create `main/test_char.h` and `main/uri_delims.h` respectively.

The following compilation warnings may occur and can be ignored:

util\_uri.c: Function argument assignment between types "unsigned

char\*" and "const unsigned char\*" is not allowed.

ssl\_engine\_io.c Function argument assignment between types "struct iovec\*\*

and "const struct iovec\*\*" is not allowed.

If you get a 'Duplicate type specifier "long" ignored' error, add

"-W 0,langlvl(extended)" to the \_C89\_OPTIONS export in os/tpf/TPFExport and

start back at the export step

## Installation

1.Link the compiled object files into a DLM. Sample link JCL has been included as os/tpf/samples/linkhttps.jcl. You will need to modify this JCL:

Change the IDs, data set names, and libraries for your particular site.

Beware using a global change to the paths of the object names that will shift the continuation character from column 72. The JCL continuation must always be in column 72.

TIP: Do NOT include gen\_test\_char.o or gen\_uri\_delims.o in the link JCL since these files are only used during the make step.

If you have "ld" installed, you may use the sample makefile.chta instead. Edit the dataset names and the chta suffix in makefile.chta as necessary and invoke it as follows:

```
make -f makefile.chta
```

2.Create a loadset. Sample loadset JCL has been included as os/tpf/samples/loadset.jcl. You will need to modify this JCL for your particular site.

A JCL condition code of 4 is expected since the C load module will contain no link map data.

You can may use make instead of JCL if you have "tpfldr" installed. Edit the tpfldr statement in makefile.chta accordingly. Also edit the file chta.older as appropriate and then run it as follows:

```
make -f makefile.chta load
```

3.Load (ZOLDR LOAD) and activate (ZOLDR ACT) the loadset on your test system.

4.Ensure that the program name you are using for Apache has RESTRICT and KEY0 authorization.

zdpac chta (c-c) will display allocation information. You can use zapac chta restrict key0 (c-c) to alter the authorization. Note that if the program name is unallocated, you must have the loadset for it activated or you will receive INVALID PROGRAM NAME from the zdpac/zapac entries.

5. Create the Apache run-time configuration file. The server requires a configuration file to initialize itself during activation. (Previously three configuration files were used.) Move to the conf directory with the command `cd ../conf`, then copy the distribution version `httpd.conf-tpfssl` to `httpd.conf`, `cp httpd.conf-tpfssl httpd.conf`. Edit `httpd.conf` with your site specific information.

The minimum changes to `httpd.conf` are as follows:

every occurrence of "`@ @ServerRoot@ @`" to your document server root (for example `"/usr/local/apache"`)

Following the `<VirtualHost _default_:443>` statement, edit the following:

`ServerName xx.xx.xx.xx`

`SSLCertificateFile /path-to-your-certificate`

`SSLCertificateKeyFile /path-to-your-key`

You may also need to edit `SSLCertificateChainFile`, `SSLCACertificatePath`, and `SSLCARevocationPath` if your site uses these features (refer to [www.modssl.org](http://www.modssl.org) for more information).

6. On TPF activate a TCP/IP interface with ZCLAW, ZTTCP or ZOSAE as appropriate.

Refer to the TPF TCP/IP publication for more information:

<http://www.ibm.com/tpf/pubs/tpfpubs.htm>.

7. Using either TFTP or FTP, transfer the configuration file, icons, and web pages to your TPF system. A typical directory structure for Apache is as follows:

`/usr/local/apache/conf`

`/usr/local/apache/logs`

`/usr/local/apache/icons`

`/usr/local/apache/htdocs`

All gif, jpg, and zip files should be transferred as binary; the configuration file and html pages should be transferred as text.

Make sure Apache can write into the logs subdirectory by doing a `zfile chmod` on it with the appropriate permission settings.

Refer to the TFTP and FTP sections of the TPF TCP/IP publication for more information:

<http://www.ibm.com/software/http/tpf/pubs/tpfpubs.htm>

8. On TPF add Apache to the Internet Daemon's tables using ZINET entries, the common case:

Refer to the Internet Daemon section of the TPF TCP/IP publication for more information:

<http://www.ibm.com/software/http/tpf/pubs/tpfpubs.htm>.

9.Start the server using the ZINET START S-APACHE command.

10.Request a non-secure page from your browser: <http://xx.xx.xx.xx> (where xx.xx.xx.xx is your IP address) and a secure page with <https://xx.xx.xx.xx>