SSL Random File Requirements on UNIX Systems

If you will be using SSL on UNIX platforms, a random file is required. This file contains entropy data that is used for generating random numbers by the SSL symmetric key allocation routines. System random files can usually be found as **.rnd* files in the */dev/random* or */dev/urandom* directories. If these devices are not available on your system, contact your system administrator for assistance with installing them; some systems may require a patch.

In lieu of setting up a system random file, you can use a personal random file. For instructions on setting up a personal random file, refer to your system administrator.

Random files are identified to the system in one of the following ways:

- The $RANDFILE environment variable can be set to the location of the random file.
- A random file (**.rnd*) can be stored in the current directory.
- A random file (**.rnd*) can be stored in the $HOME directory.
- The RANDOM_FILE URL parameter can be used to specify the location of the random file.

Note:
Windows platforms have their own automated methods of establishing the random file; consequently the manual identification or setup of a random file is not necessary in Windows.