Synopsys License Verification

This document summarizes the license file verification methodology for Synopsys licenses in the combined vendor daemon (cvd) format used by Synopsys Common Licensing.

This document contains these sections:

require an SSST feature. To avoid startup errors and possible license denials by the SCL license server, the following instructions must be followed:

Modify only the SERVER and VENDOR lines of the license file. The SERVER line must be modified to contain the correct server hostname, and the VENDOR line must be modified to contain the full path to the snpslmd daemon. The hostid (usually the 12-character

```
% scl_root/linux/bin> sssverify /path/to/synopsys.lic
```

tegrity of the license file and detects any formatting errors in the file. If there are no errors in the license file, you will see a message like the one below:

As indicated in this message, it is safe to use the license file if there are no SSS errors.

If the license file is corrupt, you will receive one of the following errors:

If the SSS (or SSST) key is missing or corrupt, you will receive this message:

If you have removed any features from the license file, you will see a message like this:

```
                    Invalid license file fingerprint.

License file integrity check FAILED!
-----------------------------------------------------------
This is an invalid license file. You should not use this license file.
Please use the license file as received from Synopsys, Inc.
```

As indicated in the above error messages, if the integrity check fails, the license file should NOT be used to start the license server.

Verifying that SCL is Serving Licenses

1. Check the Debug Logfile for Start-Up errors

Search the SCL server debug logfile and make sure that lmgrd and snpslmd have started properly. Also, search for SSS and make sure there are no errors. Below are two possible error messages that might be present in the debug logfile. (This step needs to be performed only after verifying the license file with sssverify, and starting the license server.)

(2) An SSS (security) denial error:

The first denial message is a normal message indicating that all the available licenses have been checked out by other users or jobs. However, the second denial error ( ) is a serious error that means the SCL version needs to be upgraded, or the license file is corrupted. Troubleshooting SSS / sssverify Problems section, below.

Managing Temporary Keys

All temporary keys (except for non-cvd-format temporary keys issued for a legacy daemon) require an SSST feature. (A license file should never contain more than one SSS feature but may contain more than one SSST feature if multiple temporary license

In this example, the INCREMENT lines are temporary keys (SN=TK) that contain the same transaction ID (593733). Thus, these keys must be added to or removed from the license file only as a block.

Troubleshooting SSS / sssverify Problems