

Synopsys CVD License Verification Checklist

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:

- **Overview of Synopsys Secure Server Technology**
- **Verifying the Keys Obtained from Synopsys**
- **Verifying that SCL is Serving Licenses**
- **Managing Temporary Keys**
- **Troubleshooting SSS / sssverify problems**

Overview of Synopsys Secure Server Technology

Synopsys Secure Server, or SSS, is a security technology that is incorporated into SCL binaries that requires a valid license file security feature name (SSS or SSST) in every Synopsys license file using the standard combined vendor daemon (cvd) format. This technology is designed to ensure that customers use only the most recent licenses received from Synopsys, without any additions or subtractions.

All regular (release) keys must have a valid SSS key. Temporary keys require an SSST feature.

A license file should never contain more than one SSS feature, but may have more than one SSST feature if multiple temporary licenses have been issued. A missing or invalid SSS (or SSST) key makes the license file invalid and will result in license checkout denials. To avoid possible license denials by the SCL license server, the following instructions must be followed:

- Use the complete license file as received from Synopsys or as retrieved from the SmartKeys system. DO NOT add, remove or modify any INCREMENT lines within the license file.

Exception: If you receive temporary keys from Synopsys, you can append them to the existing revenue license file. However, it is recommended that you maintain a separate server for temporary keys. See the “Managing Temporary Keys” section of this document for details.

- Verify the Synopsys licenses using the procedure below. (Every time a license file is changed in any way, follow these procedures again.)

Verifying the Keys Obtained from Synopsys

Before using any new keyfile received from Synopsys, run the SCL “`sssverify`” utility to identify any errors before starting the server. For example:

```
% scl_root/linux/bin> sssverify -v

Synopsys Corporate Licensing (SCL) Release: version
SCL_11.1, Build 1; Label: SCL_11.1; Built on Sep 22 2009
at 23:41:36
```

Synopsys supports SCL versions 10.9.3 or later; ignore the Build number. Also, SCL 11.1 or later is required to support Synplicity licenses in the SCL / `snpslmd` combined vendor daemon format.

Note:

If you have Synplicity features in the license file, you must use only the 32-bit binary (“`sparcOS5`”). for the Solaris platform. Also, if you have a dongle on a Linux platform, you must use only 32-bit binaries (“`linux`” or “`suse32`”). See the SCL 11.1 Release Notes for details.

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

The “`sssverify`” utility verifies the integrity 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:

```
% sssverify synopsys.lic

Integrity check report for license file "synopsys.lic".
Report generated on 07-Dec-2009
-----
Checking the integrity of the license file..
Valid SSS feature found.
License file integrity check PASSED
-----
You may now use this license file to start the license server.
```

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:**

```
Checking the integrity of the license file...
No SSS or SSST features were found in the license file.
All revenue keys ("SN=RK:..." on feature line) have been excluded.
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.
```

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

```
Checking the integrity of the license file...
Valid SSS feature found. Invalid license file fingerprint.
2 features are missing from this file.
[Or, "You have added 2 new features to this file," followed by a list
of features.]
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.)

Error 1: Warning

```
-----
(snpslmd) WARNING: SSS errors.
(snpslmd) Use the sssverify utility to check the integrity of your license file.
(snpslmd) The license file should be used exactly as received from Synopsys, Inc.
-----
```

Error 2: Fingerprint error

```
-----
(snpslmd) Valid SSS feature found. INVALID license file fingerprint.
(snpslmd) This feature is required to enable other keys in your license file.
(snpslmd) 91 features are missing from this file.
(snpslmd) All revenue keys ("SN=RK:..." on feature line) have been excluded.
-----
```

IMPORTANT:

If the license server log file has either of the above error message, users will experience license denials. To resolve this, see the “Troubleshooting SSS / sssverify Problems” section, below.

2. Verify that a License Can Be Checked Out

If the debug logfile does not show any checkouts (“OUT”) or denials (“DENIED”), you can use the sclsh utility included with SCL to verify that a license can be checked out. For example,

```
% setenv SNPSLMD_LICENSE_FILE 27000@my_server
% /synopsys/scl/linux/bin/sclsh
(sclsh) co hspice
No job handle for snpslmd, init being done for you
chain: 1-th handle[0] lc_init(snpslmd) = 0
lc_checkout(*1,hspice,1.0,1,LM_CO_NOWAIT,&code,4000)=0
hspice: checked out
```

After a successful checkout, there will be a corresponding, time-stamped message in the debug logfile:

```
9:53:29 (snpslmd) OUT: "hspice" jflores@jove
```

If there is a checkout failure, this will also be entered into the debug logfile. For example,

```
-----
8:35:58 (snpslmd) ERROR: SSS feature is required!
8:35:58 (snpslmd) DENIED: hspice - excluded by SSS. Server is unstable.
-----
```

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 files have been merged.)

Maintain a separate server for temporary keys

By design, an on-support “revenue” key will void a temporary key with the same feature name and a prior issued date. If possible, keep your temporary keys and production keys separated, by hosting them on separate servers. This will ensure that the temporary keys are not voided by later production (revenue) keys.

Temporary keys must be added or removed as a block, not individually

Since temporary keys are issued in “blocks” of two or more, they may never be removed individually. Instead, they must be added or removed as blocks, where all the keys in the block contain the same transaction ID. For example, consider these keys:

```
INCREMENT SSST snpslmd 1.0 31-may-2010 1 0DB62FEB8D74757952F2 \
  VENDOR_STRING="a88b1 297ef b3e2c e314e 15518 a3784 a5314 e1551..." \
  NOTICE="Licensed to XYZ Corp. [DO NOT DELETE/MODIFY SSST...]" \
  SN=TK:0:0:593733 ISSUER="Synopsys Inc. [12/28/2009 21:09:09 1234]" \
  START=31-may-2009
INCREMENT PrimeTime snpslmd 2009.06 31-may-2010 1 ISSUED=31-may-2009 \
  ck=36 SN=TK:3222-0:229054:593733 START=31-may-2009 AUTH={ \
  snpslmd=( LK=6D48B13764E3B921D8D9) }
```

```
INCREMENT PrimeTime-SI snpslmd 2009.06 31-may-2009 1 \  
ISSUED=31-may-2009 ck=11 SN=TK:3222-0:229054:593733 \  
START=31-may-2009 AUTH={ snpslmd=( LK=6D7881C7D0A033B1E33E) }
```

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.

For more details on adding or removing temporary keys from a license file, see the SolvNet article on managing temporary keys at <https://solvnet.synopsys.com/retrieve/023020.html>

Troubleshooting SSS / sssverify Problems

sssverify fails

The following three steps resolve 99.5% of sssverify or other SSS security errors:

1. Download the latest license file from SmartKeys at <http://www.synopsys.com/keys>
2. Make sure the SCL version is 10.9.3 or later. (SCL 11.1 is required if your cvd-format license file contains Synplicity licenses.)

You can determine the snpslmd version by searching the debug logfile for “SCL.” If necessary, upgrade to the latest version of SCL.

3. Do not add or remove any keys to the license file. The only exception is for temporary keys, which may be added or removed as a block (that is, all the temporary keys issued at one time may be added, or they may all be removed). See the section titled “Managing Temporary Keys” for details.

Note:

If production keys have expired, do not remove them. Instead, obtain a new license file from SmartKeys.

Other things to look for:

- The license file must contain only one SERVER and VENDOR line. (If you have redundant licenses, there must be three SERVER lines.)
- There must be a USE_SERVER line following the VENDOR line. Remove any duplicate USE_SERVER lines that might be present in the file.
- Remove any keys for third-party daemons and licenses from the file.
- Make sure all comment lines start with # and do not wrap.
- Make sure all INCREMENT keywords are at the beginning of the line.
- An INCREMENT key may only wrap after a space and a continuation character (“\”).

sssverify passes, but the debug logfile has SSS or fingerprint errors

- Check the license server debug logfile to make sure that the SCL version is 10.9.3 or later. If necessary, upgrade to the latest version of SCL. SCL 11.1 is required if your cvd-format license file contains Synplicity licenses.
- Restart the license server

If you are not able to rectify the sssverify errors (or SSS error messages in debug logfile) then open a case with the Synopsys Support Center. You may open a case on the Web at <https://solvnet.synopsys.com/EnterACall>. (To route the call to the correct application engineer, choose “Keys” or “Synopsys Common Licensing” as the product.)

Alternately, you may call (800) 245-8005 or send e-mail to support_center@synopsys.com. If you are located outside North America, contact your local Synopsys Support Center.