Splunk Enterprise 9.0.4

Supplemental Administrative Guidance for Common Criteria

Version 1.0
March 15, 2023

Splunk
270 Brannan Street
San Francisco, CA 94107

Prepared By:

Booz | Allen | Hamilton
delivering results that endure

Cyber Assurance Testing Laboratory
1100 West Street
Laurel, MD 20707

Contents

Table of Tables

1 Introduction

The Splunk Enterprise 9.0.4 (TOE) is an application software product that is installed on a Linux operating system (OS). The Protection Profile for Application Software Version 1.4 (APP_PP) defines an application as "software that runs on a platform and performs tasks on behalf of the user or owner of the platform, as well as its supporting documentation."

As a Common Criteria evaluated product, this guidance serves to define the 'evaluated configuration' in which the evaluation was performed and to summarize how to perform the security functions that were tested as part of the evaluation.

2 Intended Audience

This document is intended for administrators responsible for installing, configuring, and/or operating Splunk Enterprise 9.0.4. Guidance provided in this document allows the reader to deploy the product in an environment that is consistent with the configuration that was evaluated as part of the product's Common Criteria (CC) testing process. It also provides the reader with instructions on how to exercise the security functions that were claimed as part of the CC evaluation. The reader is also expected to be familiar with the Splunk Enterprise 9.0.4 Security Target and the general CC terminology that is referenced in it. This document references the Security Functional Requirements (SFRs) that are defined in the Security Target document and provides instructions for how to perform the security functions that are defined by these SFRs. The Splunk product, as a whole, provides a great deal of security functionality but only those functions that were in the scope of the claimed PP are discussed here. Any functionality that is not described here or in the Splunk Enterprise 9.0.4 Security Target was not evaluated and should be exercised at the user's risk. For a full set of vendor documentation visit: https://docs.splunk.com/Documentation/Splunk/9.0.4. The Security Administrator is encouraged to reference these documents in full in order to have in-depth awareness of the security functionality of Splunk, including functions that may be beyond the scope of this evaluation.

3 Terminology

In reviewing this document, the reader should be aware of the terms listed below. These terms are also described in the Splunk Enterprise 9.0.4 Security Target.

CC: stands for Common Criteria. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

SFR: stands for Security Functional Requirement. An SFR is a security capability that was tested as part of the CC process.

TOE: stands for Target of Evaluation. This refers to the aspects of the Splunk product that contain the security functions that were tested as part of the CC evaluation process. TOE indexer refers to a configuration item or procedure that only applies to the Splunk application being configured as an indexer. TOE forwarder refers to a configuration item or procedure that only applies to the Splunk application being configures as a forwarder. The generic use of TOE means that it applies to both indexer and forwarder.

Security Administrator: A security administrator is an individual who has permissions to modify the behavior of the TOE. This includes the individual that installs it on the underlying platform but can also include other individuals if administrator access is granted to them on Splunk Web or Splunk CLI.

User: An individual who has access to the TOE but is not able to manage its behavior.

4 References

The following documents were created and evaluated as part of the Splunk Enterprise CC evaluation:

[1] Splunk Enterprise 9.0.4 Security Target – (ST)

[2] Splunk Enterprise 9.0.4 Supplemental Administrative Guidance for Common Criteria (AGD – this document)

5 Evaluated Configuration of the TOE

This Section lists the components that have been included in the TOE's evaluated configuration, whether they are part of the TOE itself, environmental components that support the security behavior of the TOE, or non-interfering environmental components that were present during testing but are not associated with any security claims.

5.1 TOE Components

The TOE is the Splunk Enterprise 9.0.4 ("Splunk") application executing on a Linux OS. In the evaluated configuration, Splunk Enterprise 9.0.4 is installed on top of the RHEL OS and configured with either the indexer (TOE indexer) or forwarder (TOE forwarder) functionality enabled. The administrative interfaces include a local CLI and a web UI for remote access.

The TOE indexer was configured to securely communicate with the following external IT entities: SMTP server (TOE acts as client only), an external trusted data feed (TOE acts as server), and a management workstation (TOE acts as server). The external trusted data feed was an instantiation of Splunk software configured as a forwarder and is considered part of the operational environment for the TOE indexer.

The TOE forwarder was configured to securely communicate with the following external IT entities: an external trusted data receiver (TOE acts as client). The external trusted data feed receiver was an instantiation of Splunk software configured as an indexer and is considered part of the operating environment for the TOE forwarder.

5.2 Supporting Environmental Components

The following table lists components and applications in the environment that the TOE relies upon in order to function properly:

Table 1: Components of the Operational Environment

Component	Definition
External Trusted Data Feed	External data source for transmitting non-TSF related data to the TOE indexer for populating Splunk's datastore (indexes). The external data source must use HTTPS/TLS to communicate with the TOE.
External Trusted Data Feed Receiver	External data source for receiving non-TSF related data from the TOE forwarder. The external data source must use HTTPS/TLS to communicate with the TOE.
Host Platform	A general-purpose computer on which the Linux operating system and the TOE is installed. The TOE requires network resources from the host platform. Note that the host platform can also be used to administer the TOE locally.
Management Workstation	Any general-purpose computer that is used by a security administrator to manage the TOE remotely via a web browser.
SMTP Server	An email server that can receive alerts from the TOE and deliver them to users in the Operational Environment via email.
CRL Distribution Point	A server that provides updated revocation lists for the TOE's certificate validation functionality.

5.3 Assumptions

In order to ensure the product is capable of meeting its security requirements when deployed in its evaluated configuration, the following conditions must be satisfied by the organization, as defined in the claimed Protection Profile:

- **Platform:** The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
- **Proper administrator:** The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.
- **Proper user:** The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.

6 Secure Installation and Configuration

Documentation for how to order and acquire the TOE is described under the pricing link on the Splunk website: www.splunk.com. Section 5.1 of this document lists the components that are associated with the TOE. When downloading the TOE, this documentation should be checked as part of the acceptance procedures so that the correctness of the software application can be verified.

Physical installation and first-time setup of the TOE can be accomplished by following the steps outlined in Section 6. Once the TOE is installed, it is recommended that an administrator perform all steps in Section 7, and perform a secure update as discussed in Section 7.12.

6.1 Prerequisites

To ensure Splunk works as expected and the configuration is Common Criteria compliant, do not start Splunk until all steps have been performed as described in this Section. Skipping any steps can lead to a non-Common Criteria complaint installation, even if the steps are performed later.

1. Red Hat Subscription Manager should be enabled and properly configured. Packages can be installed by running:

   ```
   yum install <package>
   ```

   Point to repository locations (internal/external) as needed.

2. SELinux should be in "Enforcing" mode, running targeted policy, and policy version 31. Check the current status and configuration of SELinux. The system needs to be configured to boot with SELinux in `Enforcing` mode. To do this either:
   - Open the file `/etc/selinux/config` and make sure `SELINUX=` is set to `SELINUX=enforcing`.
   - Run `getenforce` and look for the result `enforcing.` If SELinux is not in Enforcing mode, run the command `setenforce 1`.
   - Open the grub configuration file `/boot/grub2/grub.cfg`. Ensure there is no mention of selinux in this file. Some individuals will disable SELinux by adding the line `selinux=disbled` to the kernel arguments, this should never be present.

3. Splunk leverages Python provided by RHEL (/usr/bin/python) for the GNOME keyring. Ensure the Python version matches with the following version.

   ```
   $ / usr/bin/python3 --version
   Python 3.6.8
   ```

4. Make sure GNOME keyring and Python system dependencies are installed:
   - yum install libsecret

5. Two additional LUKS encrypted partitions should be available (for $SPLUNK_HOME and $SPLUNK_ETC). For instructions on setting up LUKS encryption, see:
   - https://gitlab.com/cryptsetup/cryptsetup
   - https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-Encryption.html

6. Create a "splunk" user:

   ```
   useradd splunk
   ```

   If a "splunk" user already exists, make sure its home directory points to `/home/splunk` by checking /etc/passwd file. If not, modify the user to change its home directory.

   ```
   usermod -m -d /home/splunk splunk
   ```

6.2 Initial Installation

6.2.1 Install Splunk Enterprise

1. Download Splunk at https://www.splunk.com/en_us/download/splunk-enterprise.html

2. Install Splunk 9.0.4 as 'root' user.

   ```
   rpm -i splunk-9.0.4-<xxxxxxxxxxxx>-linux-2.6-x86_64.rpm
   ```

3. Move Splunk's configuration files from their default location to `/etc/opt/splunk`:

   ```
   mv / opt/splunk/etc/* /etc/opt/splunk

   rmdir /opt/splunk/etc

   export SPLUNK_ETC=/etc/opt/splunk
   ```

4. Common Criteria installation requires that the user to provide all needed cryptographic keys and certificates. At first-run, the specific key-pairs described here must be present. Splunk does not generate these keys. A FIPS-compliant version of OpenSSL can be used or any other FIPS-compliant tool to generate the keys. The cryptographic module used must be FIPS-compliant and the module properly configured to ensure that its algorithms are properly implemented, and the key-pairs produced are acceptable for use. If using OpenSSL, the following procedures must be performed:

   ```
   export OPENSSL_FIPS=1

   export LD_LIBRARY_PATH=/opt/splunk/lib
   ```

   Use the `which` command to verify OpenSSL and then confirm FIPS status using the `openssl version` command.

   For example, for the `audit.conf` public and private key pair:

   ```
   openssl ecparam -name prime256v1 -genkey -out
   $SPLUNK_ETC/auth/audit/private.pem -noout

   openssl ec -aes256 -in $SPLUNK_ETC/auth/audit/private.pem -
   out $SPLUNK_ETC/auth/audit/private.encrypted.pem

   openssl ec -in $SPLUNK_ETC/auth/audit/private.pem -out
   $SPLUNK_ETC/auth/audit/public.pem -outform PEM -pubout
   ```

   For the `distServerKeys.conf` public and private key pair:

   ```
   openssl ecparam -name prime256v1 -genkey -out
   $SPLUNK_ETC/auth/distServerKeys/private.pem -noout

   openssl ec -aes256 -in
   $SPLUNK_ETC/auth/distServerKeys/private.pem -out
   $SPLUNK_ETC/auth/distServerKeys/private.encrypted.pem
   ```

```
openssl ec -in $SPLUNK_ETC/auth/distServerKeys/private.pem
-out $SPLUNK_ETC/auth/distServerKeys/trusted.pem -outform
PEM -pubout
```

6.2.2 Install the Splunk SELinux .rpm file

1. Download `splunk-selinux-<version>.rpm`, from the Splunk customer portal, for Common Criteria. This `.rpm` file contains SELinux policies that can be configured and the ability to run Splunk Enterprise in Common Criteria mode.
2. Install the file:

```
yum install splunk-selinux-<version>.rpm
```

7 Secure Management of the TOE

The following Sections provide information on managing TOE functionality that is relevant to the claimed Protection Profile. This information is summarized here to discuss only actions that are required as part of the 'evaluated configuration'; any cryptographic engines outside of those provided by the TOE in its evaluated configuration were not evaluated or tested.

7.1 Authenticating to the TOE

Users must authenticate to the TOE in order to perform any management functions. As part of the initial startup process, Splunk provides a prompt to create credentials for the administrator user. In order to minimize the risk of account compromise, it is recommended to use a password that includes a mixture of uppercase, lowercase, numeric, and special characters and is not a common word or phrase but is not so complex that it must be written down in order to be remembered. Both a username and password must be used for Splunk to start and operate normally.

Continuing from Section 6.2.2, a prompt for a username, password, and password confirmation will be displayed (password will be hidden):

```
Please enter an administrator username: admin

Please enter a new password: ********

Please enter a new password: ********
```

7.2 Creating Scripts to Start and Stop Splunk

To start and stop Splunk, create the following scripts in `/home/splunk`:

run_splunk.sh

```
#!/bin/bash

export SPLUNK_ETC=/etc/opt/splunk

export PATH=/usr/bin:$PATH

export OPENSSL_FIPS=1
```

```
. /opt/splunk/bin/setSplunkEnv

runcon -u system_u -t splunk_t -r system_r
/opt/splunk/bin/splunk start
```

stop_splunk.sh

```
export SPLUNK_ETC=/etc/opt/splunk

export PATH=/usr/bin:$PATH

export OPENSSL_FIPS=1

. /opt/splunk/bin/setSplunkEnv

runcon -u system_u -t splunk_t -r system_r
/opt/splunk/bin/splunk stop
```

Run the following commands as root to ensure that the scripts have the correct SELinux file contexts:

```
chown -R splunk:splunk /home/splunk/*

chcon -u system_u -r object_r -t initrc_exec_t
/home/splunk/run_*

chcon -u system_u -r object_r -t initrc_exec_t
/home/splunk/stop_*

chmod 755 /home/splunk/run_* /home/splunk/stop_*

chcon -u system_u -r object_r -t splunk_usr_t /home/splunk
```

7.3 Splunk User Account Environment Setup

To set the Splunk user environment, the steps below must be performed as the "splunk" user. This is the userid under which the Splunk application runs. If any files are created/modified as the admin or any other user, the splunk user will be unable to access Splunk, causing unexpected behavior.

```
su - splunk

export SPLUNK_HOME=/opt/splunk

export SPLUNK_ETC=/etc/opt/splunk
```

7.4 Cryptographic Configuration Notice

The administrator installing the TOE is expected to perform all of the operations in Sections 7.5 and 7.6 of this document. This will result in the TOE's cryptographic operations being limited to the claims made within the Common Criteria evaluation. There is no further configuration required on the TOE's cryptographic engine as the TOE already comes pre-configured to meet many of the Common Criteria requirements. Section 7.6 automates many of the remaining configurations through the Common Criteria Mode, and the remaining configurations are handled in Section 7.5 which has the administrator manually configuring the remaining items (i.e. ciphersuites, algorithms).

NOTE: The use of other cryptographic engines and cryptographic settings were not evaluated nor tested during the Common Criteria evaluation of the TOE.

7.5 Securing Splunk Communications

NOTE: If Splunk-generated default certificates are used, Splunk will not have network communication. The CLI, as well as Splunk Web, will be non-functional. Any errors will be logged in `splunkd.log`.

An administrator must use a FIPS-compliant version of OpenSSL or any other FIPS-compliant tool to generate certificates. These certificates must be FIPS-compliant. Certificates issued by CAs such as Verisign/GlobalSign can also be used. The certificates must be in PEM format. Encryption and/or authentication can be applied using certificates for:

- Communications between the browser and Splunk Web (HTTPS/TLS server)
- Communications between TOE indexer (HTTPS/TLS server) and an external data feed (such as a Splunk forwarder).
- Communications between TOE forwarder (HTTPS/TLS client) and an external data feed receiver (such as a Splunk indexer)
- Communication between TOE indexer (TLS client) and SMTP server

7.5.1 List of certificates/keys

Provide certificates/keys for Splunk to work in Common Criteria mode. Some of these certificates (for example, inputs.conf) are optional, depending on whether the functionality is required. The details of these attributes can be found in `/etc/opt/splunk/system/README/*.conf.spec`.

```
<conf-file>, <stanza-name>, <attribute-name>
server.conf, [sslConfig], serverCert
server.conf, [sslConfig], sslRootCAPath
server.conf, [kvstore], serverCert
web.conf, [settings], serverCert
#these should have been provided in the install step before installing splunk-selinux.rpm
audit, [auditTrail], privateKey
audit, [auditTrail], publicKey
distsearch, [tokenExchKeys], publicKey
distsearch, [tokenExchKeys], privateKey
#needed for indexer configuration uses splunktcp-ssl for getting input from forwarders
inputs, [SSL], serverCert
#needed for forwarder configuration
outputs, [tcpout], clientCert
```

```
#CRLs: must store CRL files under /etc/opt/splunk/auth/crl directory. Look at README in that directory.
```

NOTE: Node/leaf certificates should be in PEM format, and include their corresponding private key immediately after the public certificate portion. For example:

```
-----BEGIN CERTIFICATE-----
<node-certificate-data>
-----END CERTIFICATE-----
-----BEGIN ENCRYPTED PRIVATE KEY-----
<node-certificate-privatekey-data>
-----END ENCRYPTED PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<intermediate-CA-issuer-certificate-data>
-----END CERTIFICATE-----
```

7.5.2 Cipher Suites and TLS Encryption

Update or create the `/etc/opt/splunk/system/local` conf files with these settings. The paths shown in these samples are for illustration and can be different if desired.

For full copy-paste examples, go to Section 7.13 below.

server.conf

```
#Contains a variety of settings for configuring the overall state of a Splunk Enterprise instance.
[general]
requireBootPassphrase = true
allowRemoteLogin = never
[sslConfig]
cipherSuite = ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384
allowSslRenegotiation = false
# Note: ECDHE-ECDSA-AES256-SHA384 equates to TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in the Security Target.
ecdhCurves = prime256v1,secp384r1,secp521r1
sendStrictTransportSecurityHeader = true
serverCert = <absolute_path_to_server_certificate>
```

```
sslAltNameToCheck = <comma_separated_list_of_SANs>
sslCommonNameList = <comma_separated_list_of_CNs>
# This will be typically '/etc/pki/tls/certs/ca-bundle.crt'.
# For any additional CAs that need to be trusted, append them to this file.
sslRootCAPath = <path_to_OS_root_cert_store>
sslVerifyServerCert = true
sslVersions = tls1.2
sslVersionsForClient = tls1.2
[kvstore]
serverCert = <absolute_path_to_kvstore_certificate>
[applicationsManagement]
allowInternetAccess = false
```

web.conf

```
#Used when configuring Remote administration Web UI
[settings]
cipherSuite= ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384
ecdhCurves = prime256v1,secp384r1,secp521r1
enableSplunkWebSSL = 1
privKeyPath = <absolute_path_to_encrypted_private_key>
serverCert = <absolute_path_to_public_certificate>
sslVersions = tls1.2
requireClientCert = false
```

authentication.conf

```
#When Splunk is configured for common criteria mode, disabled must equal false
[secrets]
disabled = false
[secrets]
filename = secret_tool_keyring.py
python.version = python3
namespace = splunk
```

alert_actions.conf

#Used when configuring Splunk as an indexer for evaluated configuration

[email]

```
cipherSuite = ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384

ecdhCurves = prime256v1,secp384r1,secp521r1

pdf.html_image_rendering = false

sslAltNameToCheck = <comma_separated_list_of_SANs>

sslCommonNameToCheck = <comma_separated_list_of_CNs>

sslVerifyServerCert = true

sslVersions = tls1.2

use_tls = 1
```

inputs.conf

#Use only if configuring Splunk as an indexer, which can receive data from the forwarders.

[SSL]

```
cipherSuite = ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384

ecdhCurves = prime256v1,secp384r1,secp521r1

requireClientCert = true

allowSslRenegotiation = false

serverCert = <absolute_path_to_server_cert>

sslAltNameToCheck = <comma_separated_list_of_SANs>

sslCommonNameToCheck = <comma_separated_list_of_CNs>

sslVersions = tls1.2
```

Note: To configure the TOE into mutual authentication the `requireClientCert` must be set to true. If missing or false the TOE is not using mutual authentication.

outputs.conf

#Use only if configuring Splunk as a forwarder, which can send data to indexers.

[tcpout]

```
defaultGroup = group1

cipherSuite = ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384

ecdhCurves = prime256v1,secp384r1,secp521r1
```

```
clientCert = <absolute_path_to_client_certificate>
sslAltNameToCheck = <comma_separated_list_of_SANs>
sslCommonNameToCheck = <comma_separated_list_of_CNs>
sslVerifyServerCert = true
sslVersions = tls1.2
useClientSSLCompression = true
```

7.6 Enabling Common Criteria Mode

Additional security settings will need to be configured to meet the requirements of the Common Criteria certification.

Modify the `/etc/opt/splunk/splunk-launch.conf`

```
PYTHONHTTPSVERIFY=1
SPLUNK_COMMON_CRITERIA=1
SPLUNK_FIPS=1
# Do not generate python byte code
PYTHONDONTWRITEBYTECODE=1
```

7.7 Environment Setup

Include the lines below in the `/home/splunk/.bashrc` so that environment is setup properly when using the Splunk CLI.

```
export SPLUNK_ETC=/etc/opt/splunk
export OPENSSL_FIPS=1
. /opt/splunk/bin/setSplunkEnv
```

7.8 Initializing Secret Storage

Splunk relies on operating environment to provide data-at-rest encryption. In addition to securely storing credential data in the GNOME keyring, the private keys and filesystem objects that comprise Splunk must be stored on a drive partition that is secured using Linux Unified Key Setup (LUKS) encryption.

Before starting Splunk, as root, switch to the splunk user context and initialize `dbus-run-session`:

```
sudo -Hu splunk runcon -u system_u -t splunk_t -r system_r
dbus-run-session -- bash
```

Check that the dbus process is running with the splunk_dbusd_t SELinux context

```
ps auxZ | grep dbus
```

Initialize the GNOME keyring daemon with the “--unlock” option, specify a password (e.g., password123!) at the input, then using the keyboard, press [ENTER] followed by [CTRL] + [D]:

```
gnome-keyring-daemon --unlock
```

`password123!`[ENTER]

[CTRL] + [D]

To see list of keys available for secret storage:

```
runcon -u system_u -t splunk_t -r system_r
/opt/splunk/bin/splunk secret-storage
```

7.8.1 List of Secrets

```
<conf-file>, <stanza-name>, <attribute-name>

alert_actions, [email], auth_password

audit, [auditTrail], privatekeyPassphrase

distsearch, [tokenExchKeys], privateKeyPassphrase

inputs, [SSL], sslPassword

outputs, [tcpout], sslPassword

server, [sslConfig], sslPassword

server, [kvstore], sslPassword

web, [settings], sslPassword
```

NOTE: For the evaluated configuration:

- The outputs.conf file is only needed when configuring Splunk as a forwarder.
- The inputs.conf and alert_actions.conf files are only needed when configuring Splunk as an indexer.

7.8.2 Adding Secrets to Secret Storage

The command to add secrets to the GNOME keyring is:

```
runcon -u system_u -t splunk_t -r system_r
/opt/splunk/bin/splunk secret-storage --write --no-prompt
<conf-file> <stanza-name> <attribute-name> <passphrase>
```

The portions of the above command have the following meaning: `conf-file`: configuration file (e.g. server.conf) `stanza-name`: name of stanza (e.g. sslConfig) `attribute-name`: name of attribute (e.g. sslPassword) `passphrase`: passphrase to be used

7.9 Starting Splunk and Configuration Validation

Start Splunk:

```
/home/splunk/run_splunk.sh
```

Check that the Splunk is running with the splunk_t SELinux context:

```
            ps auxZ | grep splunk
```

To verify that Splunk is in Common Criteria mode, check the `/opt/splunk/var/log/splunk/splunkd.log`. Look for the following message or something similar to indicate that Splunk is running in Common Criteria Mode:

```
            ServerConfig - Splunk is starting in Common Criteria Mode.
```

Both splunkd and splunkweb should work normally in the Common Criteria mode.

NOTE: Ensure there is a valid Splunk Enterprise license installed.

7.10 Using Splunk in Common Criteria Mode

Splunk CLI commands should be run as the “splunk user” and prefixed with the SELinux 'runcon' to set proper SELinux context:

```
            runcon -u system_u -t splunk_t -r system_r
            /opt/splunk/bin/splunk <cli_cmd>
```

To stop Splunk, use the provided stop_splunk.sh script:

```
            /home/splunk/stop_splunk.sh
```

As the “splunk” user:

```
            ps -aux | grep gnome-keyring

            pkill gnome-keyring
```

As the “root” user, remove the gnome-keyring storage files:

```
            rm -rf /home/splunk/.local/share/keyrings/*
```

7.11 Updating CRL Information

Splunk expects to find the CRLs for revocation checking under `$SPLUNK_ETC/auth/crl` directory in PEM format.

7.12 Secure Updates

The TOE provides the ability for security administrators to determine its currently installed version by using the Help→About in the web UI or through the underlying platform’s package manager. The CLI command `splunk version` can also be used to query the current version of the TOE.

To maintain security throughout the lifecycle of the Splunk product, Splunk provides a mechanism to apply updates. Splunk automatically checks to see if an update is available when a user is authenticated to the web UI. Splunk will notify the authenticated user with a message displayed on the post-authentication page, underneath the “Messages” menu if there is an update available. There is no update message presented to the authenticated user if there is no update available. Splunk does not download updates automatically.

If the login screen presents a message complete the following:

1. Click the Update URL in Splunk Web. The site is redirected to the authorized Splunk customer portal site.
2. Authenticate to the portal, then manually download the .rpm package to the underlying platform.
3. As root administrator, run the "`rpm -K <filename.rpm>`" command to verify the update against the installed Splunk public key prior to installation. Splunk provides a public key within the RPM and is installed during the initial installation.
4. Determine the currently installed version by querying the latest version: `splunk version`.
5. Manually install the package as root using the platform's .rpm application.
6. Verify update was success by querying the latest version and ensure it was updated: `splunk version`.

NOTE: To ensure that the product is up to date, the user should periodically compare the current version to the latest version listed on the Splunk customer portal site.

7.12.1 Uninstalling Splunk

Stop Splunk by using this script: `/home/splunk/stop_splunk.sh`, then run the following commands as root:

```
yum remove splunk-selinux

cp -R /etc/opt/splunk/ /opt/splunk/etc

rm -rf /etc/opt/splunk/*

yum remove splunk

rm -rf /opt/splunk
```

List and terminate the "gnome-keyring-daemon --unlock" process(es) (as the splunk user):

```
ps -aux | grep gnome-keyring

pkill gnome-keyring
```

Remove the gnome-keyring storage files (as the root user):

```
rm -rf /home/splunk/.local/share/keyrings/*
```

7.13 Basic Setup using Sample Self-Signed ECDSA Certificates

Extract `<splunk-ecdsa-certs.zip>` to `/etc/opt/splunk/auth` and append `root-ca.crt` to `/etc/pki/tls/certs/ca-bundle.crt`.

Passphrase is `password`.

server.conf

```
[general]

requireBootPassphrase = true

allowRemoteLogin = never

[sslConfig]
```

```
cipherSuite = ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384
ecdhCurves = prime256v1,secp384r1,secp521r1
sendStrictTransportSecurityHeader = true
serverCert = /etc/opt/splunk/auth/splunk-cc.pem
sslAltNameToCheck = splunk-cc
sslCommonNameList = splunk-cc
sslRootCAPath = /etc/pki/tls/certs/ca-bundle.crt
sslVerifyServerCert = true
sslVersions = tls1.2
sslVersionsForClient = tls1.2
[kvstore]
serverCert = /etc/opt/splunk/auth/splunk-cc.pem
[applicationsManagement]
allowInternetAccess = false
```

web.conf

```
[settings]
cipherSuite= ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384
ecdhCurves = prime256v1,secp384r1,secp521r1
enableSplunkWebSSL = 1
privKeyPath = /etc/opt/splunk/auth/splunk-cc.encrypted.key
serverCert = /etc/opt/splunk/auth/splunk-cc.web.pem
sslVersions = tls1.2
requireClientCert = false
```

authentication.conf

```
[secrets]
disabled = false
[secrets]
filename = secret_tool_keyring.py
python.version = python3
namespace = splunk
```

alert_actions.conf #Used only for configuring Splunk as an indexer in evaluated configuration.

```
[email]
cipherSuite = ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384
ecdhCurves = prime256v1,secp384r1,secp521r1
pdf.html_image_rendering = false
sslAltNameToCheck = splunk-cc
sslCommonNameToCheck = splunk-cc
sslVerifyServerCert = true
sslVersions = tls1.2
use_tls = 1
```

inputs.conf #Used only for configuring Splunk as an indexer in evaluated configuration.

```
[SSL]
cipherSuite = ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384
ecdhCurves = prime256v1,secp384r1,secp521r1
requireClientCert = true
serverCert = /etc/opt/splunk/auth/splunk-cc.pem
sslAltNameToCheck = splunk-cc
sslCommonNameToCheck = splunk-cc
sslVersions = tls1.2
[splunktcp-ssl:9998]
```

outputs.conf #Used only for configuring Splunk as an forwarder in evaluated configuration.

```
[tcpout]
defaultGroup = group1
cipherSuite = ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384
ecdhCurves = prime256v1,secp384r1,secp521r1
clientCert = /etc/opt/splunk/auth/splunk-cc.pem
sslAltNameToCheck = splunk-cc
sslCommonNameToCheck = splunk-cc
sslVerifyServerCert = true
```

```
sslVersions = tls1.2

useClientSSLCompression = true
```

[tcpout:group1]

```
server = <indexer_host>:9998
```

Add passphrases to secret storage:

```
runcon -u system_u -t splunk_t -r system_r
/opt/splunk/bin/splunk secret-storage --write --no-prompt
server sslConfig sslPassword password

runcon -u system_u -t splunk_t -r system_r splunk secret-
storage --write --no-prompt server kvstore sslPassword
password

runcon -u system_u -t splunk_t -r system_r splunk secret-
storage --write --no-prompt web settings sslPassword
password

runcon -u system_u -t splunk_t -r system_r splunk secret-
storage --write --no-prompt audit auditTrail
privatekeyPassphrase password

runcon -u system_u -t splunk_t -r system_r splunk secret-
storage --write --no-prompt distsearch tokenExchKeys
privateKeyPassphrase password
```

Indexer passphrases:

```
runcon -u system_u -t splunk_t -r system_r splunk secret-
storage --write --no-prompt alert_actions email
auth_password <passphrase_for_your_mail_server>

runcon -u system_u -t splunk_t -r system_r splunk secret-
storage --write --no-prompt inputs SSL sslPassword password
```

Forwarder passphrases:

```
runcon -u system_u -t splunk_t -r system_r splunk secret-
storage --write --no-prompt outputs tcpout sslPassword
password
```

8 Operational Modes

When the TOE is first installed, it is considered to be in its normal operational mode. After initial installation, the TOE must still be placed into its evaluated configuration by performing the steps described in Sections 6 and 7 of this document. Once placed in its evaluated configuration, the TOE is considered to be running in Common Criteria mode and will perform the functions as described in [1].

There is no separate error mode or other degraded mode of operation. In the event that the application fails, the TOE will need to be restarted or re-installed. If the TOE has been corrupted or the application has failed such that restarting the app will not resolve the issue, an Administrator will need to contact Splunk support per the guidance in Section 9.

9 Additional Support

Splunk provides technical support for its products, if needed. Customers can register for a support account at https://www.splunk.com/page/sign_up?redirecturl=https://www.splunk.com/, Additionally, customers can open a ticket with Splunk support by calling +1 (855) 775-8657 (in the U.S. or Canada); see the Support link on their website for additional international phone numbers: https://www.splunk.com/.