Future-Proofing Compliance: Upgrading to FIPS 140-3 in Splunk Enterprise Security 10

PLA1507

.conf25
splunk>

Forward-looking statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk> .conf25

Future-Proofing Compliance: Upgrading to FIPS 140-3 in Splunk Enterprise Security 10

Nabeel
Samad

Sr Principal Engineer | Splunk

.conf25
splunk>

Table of Contents

1. What Is FIPS 140-3 and Why It Matters

   Understand the standard and its relevance to your compliance and security needs.

2. What's Changing in Splunk 10

   Key updates affecting forwarders, TLS, and cryptography modules.

3. How These Changes Impact You?

4. How to Prepare?

   Recommendations for planning, testing, and rolling out compliant deployments.

5. Resources and Support

   Where to find documentation, tooling, and help.

6. Q&A / Wrap-Up

NIST FIPS 140-2

NIST FIPS 140-3

What is FIPS?

- **FIPS (Federal Information Processing Standards)** are a set of publicly announced standards developed by the **National Institute of Standards and Technology (NIST)** for use in computer systems by **non-military US government agencies and their contractors**.
- **FIPS compliance helps organizations in regulated industries adhere to federal security standards** and enhances data security, leading to increased customer trust.
- Some of the technical implications include:
  - **Limiting crypto algorithms** the product may use to an approved sub-set.
    - For example, FIPS 140-3 list of approved algorithms.
  - Requiring procedures in place to **guarantee the validity** of the installed FIPS module.
  - **Limiting connections** which are not FIPS-compliant.

Overview

What is the feature?

- Splunk 10 will provide an upgrade path from FIPS 140-2 to FIPS 140-3.
- Splunk 10 supports dual FIPS modules (140-2 & 140-3).
- Splunk 10 is the bridge: upgrade to 10.0 140-2 now, flip to 10.0 140-3 later.

Why did Splunk develop it?

- NIST will deprecate FIPS 140-2 in September 2026. Upgrading to FIPS 140-3 ensures that Splunk platform deployments continue to meet federal security standards.

Affected Customers

- All customers who use the Splunk platform in FIPS compliant environments.

How can users access the feature?

- By configuring Splunk to be in FIPS mode and using an OS with FIPS enabled.

Splunk FIPS Versions

NIST FIPS 140-2

NIST FIPS 140-3

Splunk 9.4: FIPS 140-2

Certificate: 4990

- Compiled into OpenSSL v 1.0.2 binaries.
- Splunk 9.4 does not support FIPS 140-3.
- Due to being based off of OpenSSL v 1.0.2, this version is **not compatible with Splunk 10.0 FIPS 140-3**.
- **Cert Sunset Date**: March 8, 2026

Splunk 10.0: FIPS 140-2

Certificate: 5044

All FIPS 140-2 certificates are placed on the Historical List by NIST on Sept 22, 2026.

- Provided by OpenSSL version 3.0.9 as separate fips.[so,dll] shared object file.
- **Currently the default version that will be used if SPLUNK_FIPS_VERSION is not set.**
- **Cert Sunset Date**: Sept 21, 2026

Splunk 10.0 FIPS 140-3

Certificate: 4781

(Branded by CryptoComply (Safelogic) – A Splunk branded certificate is in progress)

- Provided by Safelogic as separate fips.[so,dll] shared object file.
- Selectable by setting SPLUNK_FIPS_VERSION=140-3 in splunk-launch.conf setting
- Will become the **new default when NIST deprecates 140-2**.
- List of deprecated and new algorithms in 140-3
- **Cert Sunset Date**: Aug 26, 2026*

Key Dates

Splunk 10 and FIPS Compliance Timeline

Splunk 10

Splunk Enterprise 10.0 GA:
July 30, 2025

Splunk Cloud Platform 10.0 GA:
July 30, 2025

FIPS 140-2

must be upgraded to Splunk 10 to maintain FIPS 140-2

(9.4 140-2 cert sunsets)

March 8, 2026

FIPS 140-3

must be upgraded to Splunk 10 and update their FIPS configuration to 140-3

(all 140-2 certs become historical)

September 21, 2026

Upgrade Process

Compatibility Matrix

Universal Forwarder to Splunk		Universal Forwarder		
		Splunk UF 9.x FIPS 140-2	Splunk UF 10 FIPS 140-2	Splunk UF 10 FIPS 140-3
Splunk Enterprise / Cloud	Splunk 9.x FIPS 140-2	✅	✅	❌
	Splunk 10 FIPS 140-2	✅	✅	✅
	Splunk 10 FIPS 140-3	❌	✅	✅

Splunk to Splunk		Splunk Enterprise / Cloud		
		Splunk 9.x FIPS 140-2	Splunk 10 FIPS 140-2	Splunk 10 FIPS 140-3
Splunk Enterprise / Cloud	Splunk 9.x FIPS 140-2	✅	✅	❌
	Splunk 10 FIPS 140-2	✅	✅	✅
	Splunk 10 FIPS 140-3	❌	✅	✅

Migration From <= 9.4 140-2 To 10.0 140-3

- The upgrade to Splunk 10 and FIPS 140-3 happens in **two phases**:
  - **Phase 1: Upgrade to Splunk 10**
    - Completing this phase upgrades your deployment to Splunk 10 and gives access to, but does not turn on, the FIPS 140-3 module
  - **Phase 2: Migrate from FIPS 140-2 to FIPS 140-3**
    - Completing this phase turns on the FIPS 140-3 module and gives your Splunk 10 deployment full compliance with FIPS beyond September 2026

- Customers must complete **Phase 1** of the upgrade **by March 8, 2026** to remain compliant with FIPS at version FIPS 140-2
- Customers must complete **both phases** of the upgrade **by September 21, 2026** to remain FIPS compliant beyond then
- **Splunk Cloud Platform FedRAMP** customers should **contact Splunk Support to coordinate both phases** of the upgrade

Procedure for Upgrading Splunk Enterprise to Version 10

1. **Please reference the PDF on Splunk Docs for a diagram & links to the documentation for a high-level overview.**
    a. Planning & Preparation
    b. Environment Health Checks
    c. Address Compatibility Issues
    d. Component Upgrade Sequence
    e. Validation

    https://docs.splunk.com/images/d/d3/Splunk_upgrade_order_of_ops.pdf

2. **Carefully review all the Splunk 10 information in the full upgrade guide, release notes, and FIPS 140-3 documentation, paying special attention to:**

    a. Premium apps capability
    b. Hardware / OS requirements
    c. Python 3.9 / OpenSSL3 / node.js 20.18 / Mongo 7.0.18 (for FIPS 140-3 compliance)
    d. TLS 1.2

Procedure for Upgrading Splunk Enterprise to Version 10

3. **Upgrade Splunk to 10.0 (Default FIPS 140-2 Mode):**
    a. Perform a standard Splunk Enterprise upgrade on your indexers, cluster manager, search heads, and other server-tier components to version 10.0.
        i. Refer to the upgrade section in the General process to upgrade Splunk Enterprise
        ii. **Caution:** Ensure you have a migration plan in place for Forwarders before proceeding.
        iii. **Note: Do not turn on FIPS 140-3 mode yet**. Keep the system running with the existing FIPS 140-2 module during and after the upgrade. Splunk 10 will continue to use the 140-2 crypto module by default, so the upgrade should be transparent to your users and apps.
    b. Validate that after the upgrade, core services are running and search, indexing, and KV Store (if applicable) are functioning as you expect in FIPS 140-2 mode.
        i. **Note:** In an indexer cluster, all indexers should ideally be on the same major and minor version to ensure compatibility.

Procedure for Upgrading Splunk Enterprise to Version 10

4. Upgrade Universal Forwarders to 10.0 (Default FIPS 140-2 Mode):

Upgrade your universal forwarders to version 10.0. You can do this manually or by using Deployment Server or another deployment tool to push the new forwarder package. During this phase, all forwarders remain in the default FIPS 140-2 mode. Forwarders in Splunk 10 will log their FIPS mode on startup. For example, in splunkd.log you might see an INFO-level message indicating FIPS-140-2 mode enabled. Indexers will log the forwarders' FIPS versions as forwarders connect. This lets you verify that upgraded forwarders are connecting successfully.

5. Verify Forwarder Connections:

Use the MC or CMC to confirm that all forwarders appear as you expect. In Splunk 10, the monitoring dashboards include FIPS version telemetry. For example, you might see a new column or indicator for each forwarder showing "FIPS 140-2" (or "FIPS 140-3" after you turn it on). In CMC, a Forwarder Compliance view will highlight any forwarders that are not on the expected FIPS version. At this stage, all forwarders and indexers should report **FIPS 140-2**. This verification step is important to catch any stragglers or compatibility issues before changing crypto modules.

Procedure for Upgrading Splunk Enterprise to Version 10

6. **Enable FIPS 140-3 Mode (Planned Switch):**
    a. After all Splunk components are on version 10.0 and stable in FIPS 140-2 mode, you can schedule a controlled switch to FIPS 140-3. Splunk 10 uses an environment variable to select the FIPS module: set SPLUNK_FIPS_VERSION=140-3 to load the new FIPS 140-3 certified crypto module at startup (the default is 140-2 if you do not set the variable).
    b. To minimize downtime, plan to do this in a maintenance window. **On all Splunk platform instances (indexers, CMs, search heads, heavy forwarders, and UFs)**, update the Splunk launch configuration to include SPLUNK_FIPS_VERSION=140-3. For example, in the $SPLUNK_HOME/etc/splunk-launch.conf file, add or edit the line:

Rollback Plan

Rollback Scenario: If after switching to FIPS 140-3 you experience systemic problems (e.g. forwarders cannot communicate, apps malfunctioning due to crypto issues, etc.), you should do the following:

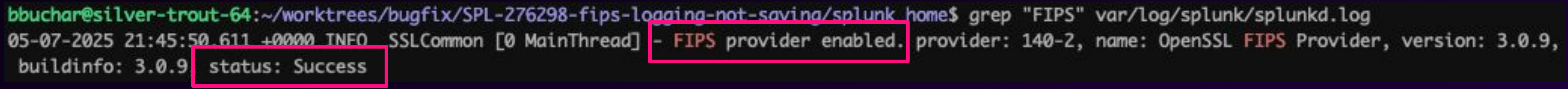
1. **Revert the FIPS Version Variable:** On all Splunk platform instances, change SPLUNK_FIPS_VERSION back to 140-2 (or remove the variable, since 140-2 is the default).
2. **Restart Splunk Enterprise services:** Bring the indexers, search heads, and forwarders back up. They will now load the FIPS 140-2 module again. Confirm through reading logs that the old module is back in use.
3. **Validate Functionality:** Check whether or not the issues are resolved by using FIPS 140-2. In most cases, any issues introduced by the new crypto will disappear once the environment is back in FIPS 140-2 mode. Your data flows and search functions should return to the pre-upgrade state.

Troubleshooting

Logging: splunkd.log

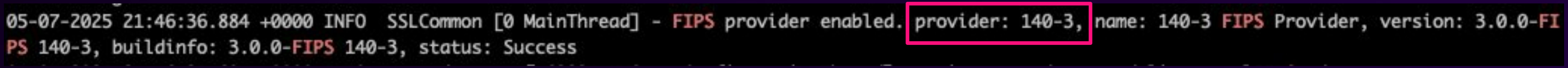
Search for “**FIPS**” in `$SPLUNK_HOME/var/log/splunk/splunkd.log` to learn about a Splunk instance’s FIPS status:

- Provider is **enabled**:



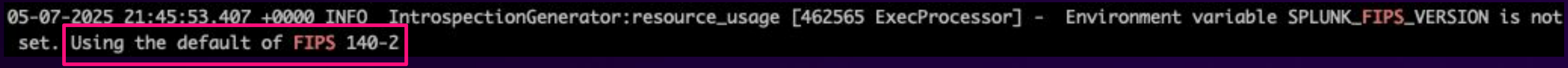
```
bbuchar@silver-trout-64:~/worktrees/bugfix/SPL-276298-fips-logging-not-saving/splunk_home$ grep "FIPS" var/log/splunk/splunkd.log
05-07-2025 21:45:50.611 +0000 INFO  SSLCommon [0 MainThread] - FIPS provider enabled. provider: 140-2, name: OpenSSL FIPS Provider, version: 3.0.9,
 buildinfo: 3.0.9, status: Success
```

- Provider **version**:



```
05-07-2025 21:46:36.884 +0000 INFO  SSLCommon [0 MainThread] - FIPS provider enabled. provider: 140-3, name: 140-3 FIPS Provider, version: 3.0.0-FI
PS 140-3, buildinfo: 3.0.0-FIPS 140-3, status: Success
```

- Splunk **defaulting** to **default version**:

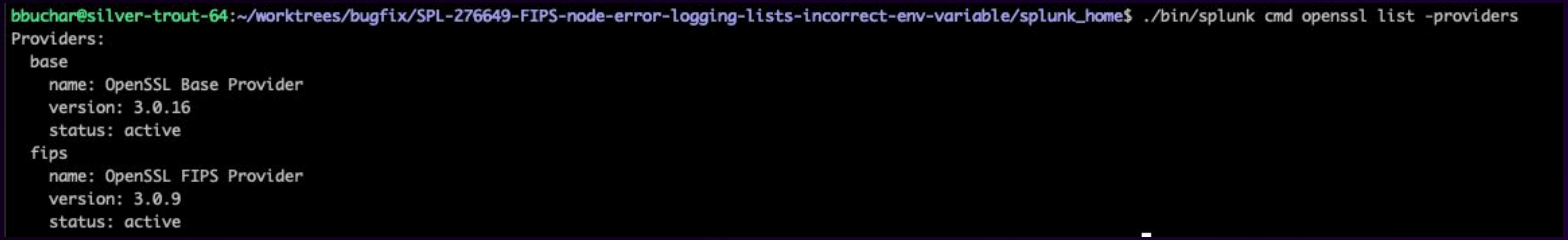


```
05-07-2025 21:45:53.407 +0000 INFO  IntrospectionGenerator:resource_usage [462565 ExecProcessor] -  Environment variable SPLUNK_FIPS_VERSION is not
 set. Using the default of FIPS 140-2
```

OpenSSL
List Providers

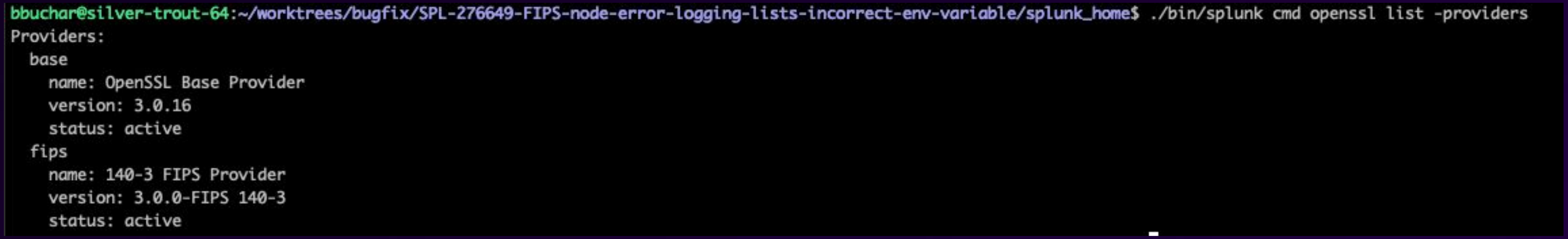
Another way to verify the providers active on a splunk installation is to use `bin/splunk cmd openssl list -providers`:

- OpenSSL FIPS Provider (140-2)



```
bbuchar@silver-trout-64:~/worktrees/bugfix/SPL-276649-FIPS-node-error-logging-lists-incorrect-env-variable/splunk_home$ ./bin/splunk cmd openssl list -providers
Providers:
  base
    name: OpenSSL Base Provider
    version: 3.0.16
    status: active
  fips
    name: OpenSSL FIPS Provider
    version: 3.0.9
    status: active
```

- Safelogic / CryptoComply FIPS Provider (140-3)



```
bbuchar@silver-trout-64:~/worktrees/bugfix/SPL-276649-FIPS-node-error-logging-lists-incorrect-env-variable/splunk_home$ ./bin/splunk cmd openssl list -providers
Providers:
  base
    name: OpenSSL Base Provider
    version: 3.0.16
    status: active
  fips
    name: 140-3 FIPS Provider
    version: 3.0.0-FIPS 140-3
    status: active
```

Configuration Errors

The `fipsmodule.cnf` files are now included in customer diag:

```
openssl3/
├── fips140-2/
│   └── fipsmodule.cnf
└── fips140-3/
    └── fipsmodule.cnf
```

The fipsmodule.cnf file includes a checksum for the FIPS module. **If the FIPS module failed to load**, the `fipsmodule.cnf` may have a mismatched `module-mac` value. Validate the fipsmodule.cnf files using the `fipsinstall` command:

```
$ $SPLUNK_HOME/bin/splunk cmd openssl fipsinstall -module $SPLUNK_HOME/lib/ossl-modules/fips140-x/fips.so -in
absolute/path/to/customer's/fipsmodule.cnf  -provider_name fips -verify
```

You can also manually run `fipsinstall` on the release version's FIPS binaries `($SPLUNK_HOME/lib/ossl-modules/fips140-x/fips.[so,dll])` and compare the resulting `fipsmodule.cnf` files with the ones in the customer's diag:

```
$ $SPLUNK_HOME/bin/splunk cmd openssl fipsinstall -module $SPLUNK_HOME/lib/ossl-modules/fips140-x/fips.so -out ./fipsmodule.cnf
-provider_name fips
```

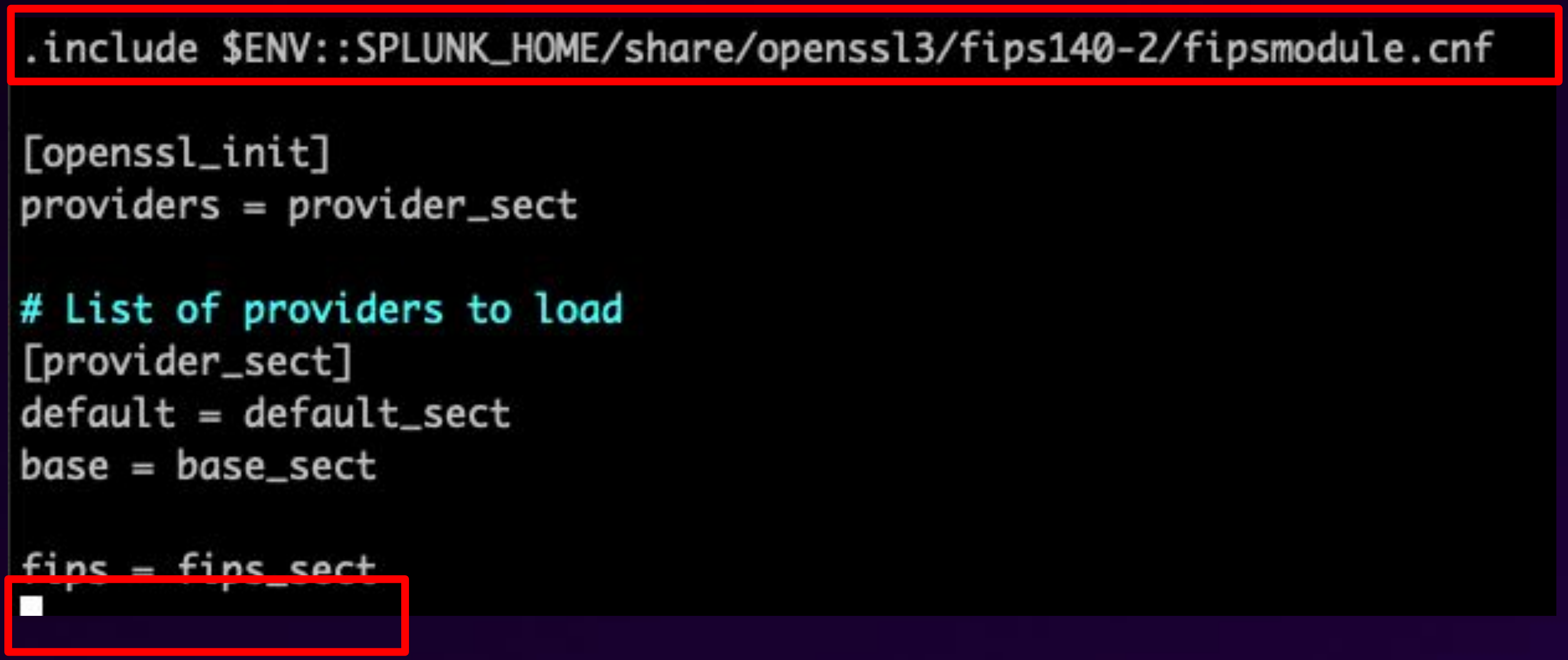
Configuration Errors cont.

The `openssl.cnf` files are **not** included in customer diag due to the possibility of containing customer secrets. It should not be modified by the customer, and **should automatically be set up correctly for them.**

However, `openssl.cnf` configuration that can cause the FIPS module to fail to load are:

- The `.include` line does not point to a valid `fipsmodule.cnf` file. (This must be an **absolute path.**)
- The `[provider_sect]` does not define a `fips` value or defines it to an incorrect value. (The definition of `[fips_sect]` in the `fipsmodule.cnf` file.)

openssl.cnf



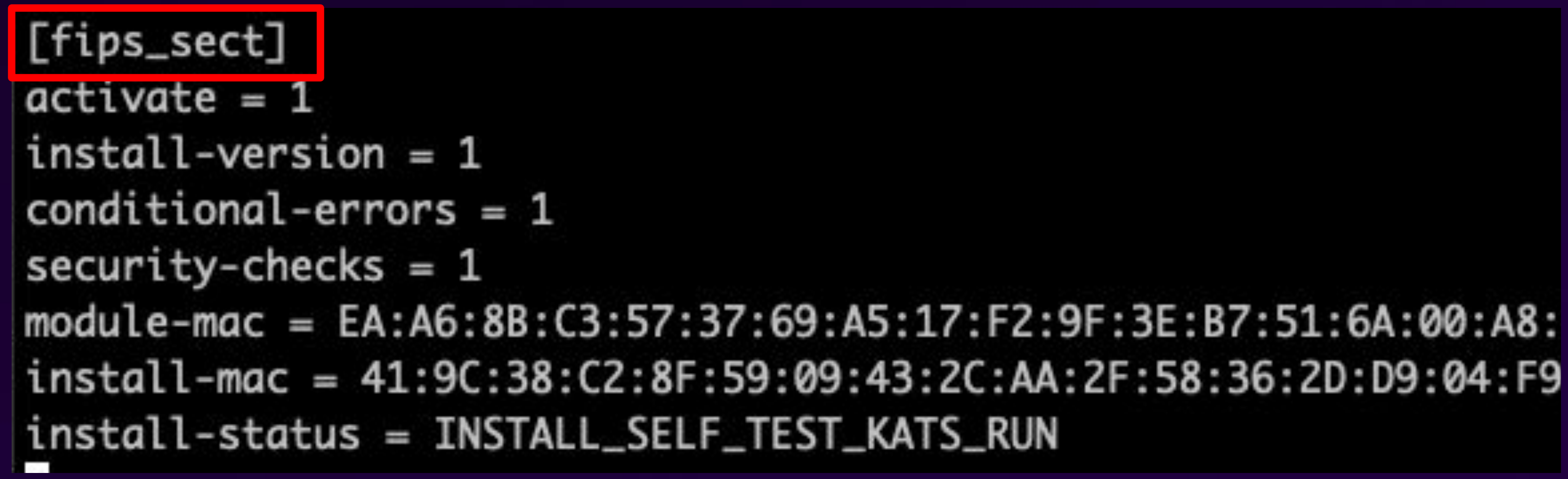
```
.include $ENV::SPLUNK_HOME/share/openssl3/fips140-2/fipsmodule.cnf

[openssl_init]
providers = provider_sect

# List of providers to load
[provider_sect]
default = default_sect
base = base_sect

fips = fips_sect
```

fipsmodule.cnf



```
[fips_sect]
activate = 1
install-version = 1
conditional-errors = 1
security-checks = 1
module-mac = EA:A6:8B:C3:57:37:69:A5:17:F2:9F:3E:B7:51:6A:00:A8:
install-mac = 41:9C:38:C2:8F:59:09:43:2C:AA:2F:58:36:2D:D9:04:F9
install-status = INSTALL_SELF_TEST_KATS_RUN
```

Connection Issues

Errors resulting from FIPS refusing connections with non-FIPS-compliant connection requests can occur. The Splunk 10 FIPS HEC/S2S w/LB FIPS Testing Document details HEC & S2S connection requests between LBs & UFs with some example logs on failure:

HEC:

curl: (35) error:1C8000E9:Provider routines::ems not enabled

- EMS refers to Extended Master Secret, a check which is required by FIPS 140-3. When attempting to connect with a 9.x FIPS 140-2 server, the request fails (as expected).

S2S:

```
06-05-2025 17:25:19.976 +0000 WARN  SSLCommon [8087 TcpOutEloop] - Received fatal SSL3 alert. ssl_state='SSLv3 read server session ticket
A', alert_description='internal error'.
06-05-2025 17:25:19.976 +0000 ERROR TcpOutputFd [8087 TcpOutEloop] - Connection to host=56.136.165.228:9997 failed
```

Resolution: If the customer is having issues connecting nodes together:

- Verify no Splunk <= 9.4 FIPS 140-2 nodes are attempting to connect with Splunk 10.0 FIPS 140-3 nodes.
  - Direct the customer to the upgrade guidance material to upgrade.
- Verify the node's host OS or cloud platform supports FIPS 140-3.
  - e.g. AWS Classic Load Balancers are not FIPS 140-3 compliant.

OS Compatibility

Node Type	FIPS 140-3	FIPS 140-2
• Search Heads • Indexers • Heavy Forwarders	• Windows Server 2022 x86 (64-bit) (Expected in future Windows release) • Windows Server 2025 x86 (64-bit) (Expected in future Windows release) • Ubuntu 22.04 x86 (64-bit) • Ubuntu 24.04 x86 (64-bit) • Red Hat Enterprise Linux 9 x86 (64-bit) • Amazon Linux 2023	• Windows Server 2019 x86 (64-bit) • Windows Server 2022 x86 (64-bit) • Windows Server 2025 x86 (64-bit) • Ubuntu 20.04 x86 (64-bit) • Ubuntu 22.04 x86 (64-bit) • Ubuntu 24.04 x86 (64-bit) • Red Hat Enterprise Linux 8 x86 (64-bit) • Red Hat Enterprise Linux 9 x86 (64-bit) • Amazon Linux 2023

OS Compatibility

Node Type	FIPS 140-3	FIPS 140-2
• Universal Forwarders	• Windows 11 x86 (64-bit) • Windows Server 2022 x86 (64-bit) • Windows Server 2025 x86 (64-bit) • Ubuntu 22.04 x86 (64-bit) • Ubuntu 24.04 x86 (64-bit) • Red Hat Enterprise Linux 9 x86 (64-bit) • Amazon Linux 2023	• Windows Server 2019 x86 (64-bit) • Windows Server 2022 x86 (64-bit) • Windows Server 2025 x86 (64-bit) • Ubuntu 20.04 x86 (64-bit) • Ubuntu 22.04 x86 (64-bit) • Ubuntu 24.04 x86 (64-bit) • Red Hat Enterprise Linux 8 x86 (64-bit) • Red Hat Enterprise Linux 9 x86 (64-bit) • Amazon Linux 2023

Q&A