September 10, 2021

To Whom It May Concern

A conformance review of Cisco Intersight, version 1.0 ("the Product") deployed in the following:

1. Intersight Connected Virtual Appliance
2. Intersight Private Virtual Appliance
3. Intersight Assist

was completed and found that the Product incorporates the following two FIPS 140-2 validated cryptographic modules:

1. Cisco FIPS Object Module version 6.2 (FIPS 140-2 Cert #2984) used for SSH service
2. Cisco FIPS Object Module version 7.2 (FIPS 140-2 Cert #3790) used for TLS services

Cisco confirms that the following features leverage the embedded cryptographic modules listed above and they provide all the cryptographic services for the TLS and SSH protocols in Intersight:

1. Session establishment supporting each service,
2. All underlying cryptographic algorithms supporting each services' key derivation functions,
3. Hashing for each service,
4. Symmetric encryption for each service.

Cisco Intersight enters FIPS mode at build time requiring no additional commands.

Details of Cisco's review, which consisted of build process, source code review and operational testing, can be provided upon request. The intention of this letter is to provide an assessment and assurance that the Product correctly integrates and uses the validated cryptographic modules listed above within the scope of the claims indicated above. The Cryptographic Module Validation Program (CMVP) has not independently reviewed this analysis, testing or the results.

Any questions regarding these statements may be directed to the Cisco Global Certification Team (certteam@cisco.com).

Thank you,

Edward D Paradise

Ed Paradise
VP Engineering
Cisco S&TO