



April 14, 2020

To Whom It May Concern

A conformance review of Cisco Smart Software Manager On-Prem 8 (CSSM On-Prem) ("the Product") was completed and found that the Product integrates the following FIPS 140-2 approved cryptographic modules:

1. Cisco FIPS Object Module (FIPS 140-2 Cert. #3341)

Specifically, the review confirmed that:

1. The cryptographic module (mentioned above) is initialized in a manner that is compliant with its individual security policy.
2. All cryptographic algorithms used in SSH v2 and TLS for session establishment, are handled within the Cisco FIPS Object Module, FIPS 140-2 Cert. #3341
3. Bulk data encryption for the established SSH v2 and TLS secure connections use the Cisco FIPS Object Module with FIPS 140-2 Cert. #3341

Details of Cisco's review, which consisted of 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 module 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](mailto:certteam@cisco.com)).

Thank you,

A handwritten signature in black ink that reads "Edward D Paradise".

Ed Paradise  
VP Engineering  
Cisco S&TO