September 26, 2025

To Whom It May Concern

A compliance review of the Cisco Meraki MS platform with software version 18 ("the Product") was completed and found that the Product incorporates the following FIPS 140-3 compliant cryptographic module:

- Cisco FIPS Object Module version 7.3a (Certificate #4747)

Cisco confirms that the cryptographic module listed above provides cryptographic services for the following:

- TLS v1.2 (Meraki Cloud, Nextunnel, cURL)

The review/testing confirmed that:

1. The cryptographic module (mentioned above) does initialize in a manner that is compliant with its Security Policy.
2. All cryptographic algorithms used for session establishment are handled within the cryptographic module.
3. All underlying cryptographic algorithms support each service's key derivation function.

This letter has been generated, with caveats, in accordance with guidance provided by the Cryptographic Module Validation Program (CMVP). The CMVP has not independently reviewed this analysis, testing, or the results.

Any questions regarding these statements may be directed via e-mail to the Cisco Global Certification Team (GCT) at certteam@cisco.com.

Sincerely,

Ed Paradise
Cisco Senior Vice President
Foundational & Government Security