SolarWinds FIPS 140-2 Compliant Components Letter

Last Updated: November 6, 2020 Ed 29

SolarWinds provides this FIPS 140-2 Compliant Components Letter to help federal government customers understand which encryption algorithms are used in SolarWinds MSP products.

This document is based on instructions found in this NIST Cryptographic Module Validation program document and outlines that the following SolarWinds MSP products, when installed in FIPS mode, only run the cryptographic modules listed.

This document is updated periodically with the latest information so be sure to check for the latest version. For more information about this document, please contact productmanagers@solarwinds.com.

SolarWinds MSP Product Versions

This document covers the SolarWinds MSP product versions listed below. Service Releases generally contain bug fixes that do not impact FIPS compliance. Accordingly, all Service Releases (identified by an incrementing third set of digits) for listed versions are also certified.

Take Control (or Dameware® Remote Everywhere) uses FIPS (140-2)-compliant cryptographic library modules to help secure Windows® device to Windows device remote connections.

Product	Oldest Version	Oldest Supported FIPS Compliant Version	Latest Version
Take Control – All versions (Windows)	6.90.00	6.90.00	7.00.19

All versions of Take Control conform with AES256 cryptography.

SolarWinds FIPS 140-2 Compliant Components Letter

SolarWinds Products Crypto Module Use

The following cryptographic modules are run by the versions listed above.

Products	Cryptographic Module	Algorithm Implementation Certificate/Vendor Validation Certificate
Take Control	OpenSSL 1.0.1u, FIPS core 2.0.2 [1]	OpenSSL Software Foundation - #1747