Secure Remote Access FIPS 140-2 Compliance Statement

Summary

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) run the FIPS 140 program. The NVLAP accredits independent testing labs to perform FIPS 140 testing; the CMVP validates modules meeting FIPS 140 validation. *Validated* is the term given to a module that is documented and tested against the FIPS 140 criteria.

This document details the FIPS 140-2 approved third-party cryptographic modules are the only modules used in BeyondTrust Appliance B Series. The compliance of Secure Remote Access (both Remote Support and Privileged Remote Access) with FIPS 140-2 is ensured by the use of exclusively FIPS 140-2 compliant, third-party cryptographic algorithms, and using the algorithms as the only providers of cryptographic services as applicable for product operation.

> ***Note:*** *FIPS Mode enforces that no changes can be made to the cryptographic algorithms for FIPS Certified Deployments.*

Third-Party Cryptographic Modules

Product Area	Encryption	Library	Manufacturer, Version
All data encryption and network communications	AES-256 AES-128 SHA-256 SHA-384	FIPS compliant OpenSSL	OpenSSL, 1.0.2