Secure Remote Access FIPS 140-2 Compliance Statement

Summary

When you need to protect Sensitive but Unclassified data with cryptography, you want to use a cryptographic module that meets the federal government (US and Canada) security standard FIPS 140-2, so that you can trust that the module is *tested* and *validated* by independent authorities. Products validated as conforming to FIPS 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or protected information (Canada).

Definition

The **Federal Information Processing Standards Publication 140-2 or FIPS**, specifies the security requirements that will be satisfied by a cryptographic module, providing four increasing, qualitative levels intended to cover a wide range of potential applications and environments. The areas covered, related to the secure design and implementation of a cryptographic module, include specification; ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

This document details the FIPS 140-2 approved third-party cryptographic modules, which 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 3.0