BeyondInsight, Password Safe, and U-Series Appliance 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 Standard (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 (EMI) / electromagnetic compatibility (EMC); self-tests; design assurance; and mitigation of other attacks.

This document details the FIPS 140-2 approved third-party cryptographic modules used in BeyondTrust BeyondInsight, Password Safe, and U-Series Appliance. It also provides information on enabling FIPS mode in the U-Series Appliance, which ensures that only approved algorithms are used for product operation.

> ***Note:** FIPS mode is not supported in BeyondInsight and Password Safe Cloud deployments.*

Third-Party Cryptographic Modules Used in BeyondInsight, Password Safe, and U-Series Appliance

Product Area	Encryption	Library	Manufacturer, Version
Web Services	TLS 1.2	.NET System.DLL	Microsoft, v4.0.0.0
Password passing	RSA	RSACryptoServiceProvider	Microsoft, v4.0.0.0
Credential storage	AES	AesCryptoServiceProvider	Microsoft, v4.0.0.0
Database connection string	DPAPI	Crypto API32	Microsoft, v6.3.9600
Password storage	AES	AesCryptoServiceProvider	Microsoft, v4.0.0.0
RCS key export	AES	AesCryptoServiceProvider	Microsoft, v4.0.0.0
Create RDP 2-factor codes	SHA1	SHA1CryptoServiceProvider	Microsoft, v2.0.0.0
High availability credentials storage	AES	AesCryptoServiceProvider	Microsoft, v4.0.0.0
Zip Library	AES	AesCryptoServiceProvider	Microsoft, v4.0.0.0
	SHA256	HMAC-SHA256	Microsoft, v4.0.0.0
Auto-Logon / Session Proxy Only			

Product Area	Encryption	Library	Manufacturer, Version
Session Manager (SSH)	AES 3DES DH SHA RSA DSA	OpenSSL crypto library	OpenSSL, v3.0.8
Session Manager (RDP)	During the RDP connection process, the TLS cipher suite will be negotiated with FIPS valid cipher suites defined in OpenSSL.	OpenSSL crypto library	OpenSSL, v3.0.8
Session Manager (IoLog)	AES	OpenSSL crypto library	OpenSSL, v3.0.8
Session manager (secure token)	SHA512	SHA512Managed	Microsoft, v4.0.0.0

Use BeyondInsight, Password Safe, and U-Series Appliance in FIPS Mode

On-premises installations of BeyondInsight and Password Safe can be configured to run in a FIPS 140-2 approved mode of operation, commonly referred to as *FIPS mode*, by setting the **FIPS State** to **Yes** in the U-Series Appliance **Security Settings**, under **FIPS Compliance Checking**.

***Note:** This is a Windows feature supported in Windows Server. When FIPS mode is enabled, the Cryptographic Primitives Library (**bcryptprimitives.dll**) and Kernel Mode Cryptographic Primitives Library (**CNG.sys**) modules run self-tests before Windows runs cryptographic operations. These self-tests are run according to FIPS 140-2 Section 4.9 and ensure that the modules are functioning properly.*

- *For more information on FIPS 140-2 Validation in Windows, please see FIPS 140-2 Validation at https://learn.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation.*
- *For more information on U-Series Appliance Security Settings, please see Manage U-Series Appliance Security Settings.*