

Statement of FIPS 140-2 Compliance

This statement is in accordance with the NIST guideline¹: *"When selecting a module from a vendor, verify that the product or application that is being offered is either a validated cryptographic module itself (e.g. VPN, SmartCard, etc) or the product or application uses an embedded validated cryptographic module (toolkit, etc). Ask the vendor to supply a signed letter stating their application, product or module is a validated module or incorporates a validated module, the module provides all the cryptographic services in the solution, and reference the modules validation certificate number from this listing."*

FIPS Validation certificate #1012 issued by NIST on 08/22/2008, to Microsoft for Windows Server 2003 Enhanced Cryptographic Provider (RSAENH), when operated in FIPS mode, states *"Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate."*

EventTracker v8.1 is a software program designed to operate on Microsoft Windows and uses the "Microsoft Enhanced Cryptographic Provider (RSAENH)" (CAPI) with FIPS compliant cryptographic algorithms, Triple-DES (FIPS 46-3) and SHA1 (FIPS 180-3) to perform encryption and compute SHA-1 checksums. This CAPI is available on all Windows platforms including (but not limited to) Server 2003, 2008, 2008 R2, 2012, Windows 10, Windows 8/8.1, Windows 7, Vista and XP. When installed on a Windows platform, EventTracker v8.1 incorporates the validated version of the CAPI as identified herein; its usage is in accordance with the guidelines described in the reference².

EventTracker v8.1 provides configurable options for encryption of communications between its Windows Agent and the Manager Console components and between the Collection Point and Collection Master components, using this validated CAPI. EventTracker v8.1 EventVault component computes SHA1 checksums on archived event log data; these computations also use the validated CAPI.

Accordingly, EventTracker v8.1 is compliant with requirements of FIPS 140-2 as described herein.

A N Ananth
President

March 2, 2016

¹ <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2010.htm>

² <http://technet.microsoft.com/en-us/library/cc750357.aspx>