

Safe Access is compliant with FIPS 140-2 standards for cryptographic modules as described in this technical note.

## Safe Access and external communications

Safe Access communications that reach outside of the Safe Access server use OpenSSL encryption ciphers and are limited to the following:

- Application Programming Interface (API)
- Test Updates
- Product Updates
- User Interface (UI)
- Agent Communications
- Remote Administration (via SSH)

For details on the encryption methods used for the above communications, see the table below, *OpenSSL Encryptions used in Safe Access*.

## OpenSSL meets FIPS regulations

OpenSSL, an open-source security toolkit has received approval from the Cryptographic Module Validation Program (CMVP) verifying that OpenSSL (<http://www.openssl.org/>) meets the Federal Information Processing Standard (FIPS) 140-2 regulations. For more information, visit the following link:

<http://trends.newsforge.com/trends/06/01/23/0429219.shtml?tid=136&tid=138>

## FIPS Validation list

Once the approval documentation is complete, OpenSSL will be listed on the following Validated Cryptographic Module page, with links to their Security Policy and Validation Certificate:

<http://csrc.nist.gov/cryptval/140-1/1401val.htm>

## FIPS PUB 140-2

FIPS PUB 140-2 defines the security requirements necessary for protecting sensitive (but not classified) information. This document can be found at the following location:

<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

## FIPS PUB 140-2 Annex A

The approved security functions are described in Annex A: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules. This document can be found at the following location:

<http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf>

Table 1. Encryptions used in Safe Access

Safe Access Communications	Encryption Cipher	Annex A Reference	Hashing Algorithm	Annex A Reference
Application Programming Interface (API)	AES Symmetric Key <sup>1</sup>	Page 1	SHA-1	Page 2
Test Updates	AES Symmetric Key <sup>1</sup>	Page 1	SHA-1	Page 2
Product Updates	AES Symmetric Key <sup>1</sup>	Page 1	SHA-1	Page 2
User Interface	RSA Asymmetric Key <sup>1</sup>	Page 1	SHA-1	Page 2
Agent Communications	AES Symmetric Key <sup>1</sup>	Page 1	SHA-1	Page 2
Remote Administration (SSH)	AES128-BC <sup>2</sup>			
1 – OpenSSL		2 – OpenSSH (OpenSSH uses OpenSSL)		