SPYRUS®

Secure Portable Workplace and Portable Workplace

A hardware encrypted, bootable USB 3.0 Windows® 8 and Windows® 10 environment for fast, secure access on the go.

Secure Portable Workplace from SPYRUS is a Microsoft-certified Windows To Go drive that securely boots your custom Windows 8 environment. Not a slow virtual machine, Secure Portable Workplace boots a native Windows 8.0/8.1 operating system using your computer hardware and the drive's ultra-fast SSD memory, and it never accesses or alters your computer's hard drive.

Run applications locally and access the Internet, your corporate network, and virtualized applications. When you're done, remove the device and leave no footprint behind.

Give your employees access to your corporate applications and data while mitigating hacking and data leakage. Add Secure Portable Workplace to your Windows domain and use Microsoft SCCM and AD group policy for centralized management. Even better, use SPYRUS Enterprise Management System (SEMS) for remote device management, including temporarily disabling the drive or permanently erasing all keys and data.

Unencrypted Portable Workplace is also available.

Features

- Optional Read Only mode erases all changes to the OS, applications, and data files when the drive shuts down to ensure an uncorrupted images every time the drive boots.
- Drives can be provisioned with a Data Vault read/write partition for saving user files even when Read Only mode is enabled. Separate data storage ensures the security of files on the main drive.
- Configure BitLocker encryption for an additional layer of SPYRUS "Defense-in-Depth" security on the main drive, Data Vault, or both.
- Secure pre-boot authentication validates the integrity of the Secure Portable Workplace and the operating system using on-board hardware security at boot time. If tampered with, it will not boot.
- Provision drives with your customized Windows image.

Designed For Security

- Microsoft Office—Install and run productivity software locally.
- Citrix, VPN, and more—Secure Portable Workplace is perfect for giving workers access to Citrix servers, virtualized applications, remote desktops, virtual private networks, and more.
- Office 365—Access your Office 365 work space from almost any PC, without fear of malware capturing your password or copying your files.
- Helps mitigate Insider and External Attacks—SEMS can be used for remote device management including freezing or disabling the device, or zeroizing the keys to effectively erase the operating system, applications, and data.

Additional Information

- Security designed, engineered, and manufactured in USA.
- Hardware-based full disk encryption (FDE) prevents data leakage.
- Dedicated cryptographic engines for fast response.
- Military strength cryptography inside FIPS 140-2 Level 3 compliant security boundary.
- Advanced hardware security includes XTS-AES 256, ECDH, ECDSA P-384, and SHA-384, which make up the US National Security Agency's Suite B cryptography. ¬
- Malware protection and sophisticated self-destruct mechanisms.
- No footprint left on host PC—as if you were never there. SPYRUS Enterprise Management System (SEMS) and remote kill stops unauthorized and rogue employee access.
- 32 GB, 64 GB, 128 GB, 256 GB, 512 GB capacities.
- Host machine must be certified for use with either Windows 7 or Windows 8. ¬ Minimum 2 GB RAM; performance improves with additional RAM.
- Minimum 2 GB RAM; performance improves with additional RAM.

SPYRUS®

Technical Specifications

Capacities & Dimensions (LxWxH)

32 GB, 64 GB, 128 GB, 256 GB
86.1 mm x 24.2 mm x 10.8 mm (+/- 0.20)

512 GB capacities
101.6 mm x 24.2 mm x 10.8 mm (+/- 0.20)

Performance (based on 512 GB drive)

USB 3.0 Super Speed; USB 2.0 Compatible

Please note Random Read and Random Write Performance is the most important metrix for bootable live drives.

Sequential Read: up to 249 MB/sec

Sequential Write: up to 238 MB/sec

Reliability

Data Retention: 10 years

Other Certifications

Microsoft Windows To Go

FIPS 140-2 Algorithm Certificates

FIPS 140-2 Level 3

Electrical

Operating Voltage Vcc = 3.3 to 5 VDC

Power Consumption 275mA @ 3.3 VDC

Other

Humidity 90%, noncondensing

Physical Device Integrity:

At SPYRUS, we understand that people rely on their WTG device for mission critical functions. In essence, it is their computer SSD drive. So unlike a traditional USB that is used less regularly and is much easier to replace, we realized early-on in our customer deployments that the device must withstand punishment from a physical design perspective. To that end we designed our Windows To Go devices meet the highest physical standards in design and component materials. The combination of stringent environmental testing and additional testing for magnetic fields, X-Ray and long term immersion demonstrate the usability of this high security configuration of the SPYRUS WTG devices in the challenging healthcare environments as well.

Microsoft Partner
Gold OEM Hardware
Silver Independent Software Vendor (ISV)

Environmental

Operating Temperature (MIL-STD-202, METH 503) 0ºC - 70ºC

Non-Operating Temperature Cycling (MIL-STD-810, METH 503) -40ºC - 85ºC

High Temperature Storage (MIL-STD-810, METH 501) 85ºC; 96 hours

EMI (FCC/CE) FCC Part 15, Class B/EN55022 - EN55024/etc

ESD (EN61000-4-2) Enclosure Discharge - Contact & Air

Dust Test (IEC 60529, IP6) As per defined

Waterproof Test (IEC 60529, IPX7) As per defined

Operating Shock, MIL-STD 883J, Method 2002.5, Cond. B, 1500g, 0.5ms, 1/2 sine wave

High Temperature Storage/Data Retention, MIL-STD-810, METH 501, 100ºC; 96 hours

Waterproof test, MIL-STD-810, METH 512.6,1 meter depth, 30 minutes

Hardware Security & Cryptographic Standards

SPYRUS Algoritm Agility includes Suite B (a set of cryptographic algorithms used for cryptographic modernization) and RSA based cryptography.

XTS - AES 256 Full Disk Encryption^

AES 128, 196, and 256 ECB, CBC, CTR, and Key Wrap Modes^

SP800 - 90 DRBG (Hash DRBG)

Elliptic Curve Cryptography (P-256, P-384, P-521)

ECDSA Digital Signature Algorithm

CVL (ECC CDH) [ECDH per SP 800-56A]

Concantenation KDF (SP800-56A)

RSA 1024 and 2048 Signature Algorithm (Note RSA 1024 has been depricated by NIST.)

RSA 1024 and 2048 Key Exchange (Note RSA 1024 has been depricated by NIST.)

PBKDF - 2 (per PKCS#5 version 2)^

DES, two-& three-key triple DES with ECB, CBC Mode (Note DES has been deprecated by NIST.)

SHA-1 and SHA-224/256/384/512 hash algorithms with HMAC Support

Support for the cryptography can vary depending on version.

^ Not available on WorkSafe

FIPS 140-2 Level 3 opaque epoxy filled housing can be modified by special order.

Corporate Headquarters
1860 Hartog Drive
San Jose, CA 95131-2203
+1 (408) 392-9131 phone
+1 (408) 392-0319 fax
info@SPYRUS.com

East Coast Office
+1 (732) 329-6006 phone
+1 (732) 832-0123 fax

UK Office
+44 (0) 113 8800494

Australia Office
Level 7, 333 Adelaide Street
Brisbane QLD 4000, Australia
+61 7 3220-1133 phone
+61 7 3220-2233 fax
www.spyrus.com.au

Document number 400-451001-04