SPYRUS®

WorkSafe™ and WorkSafe Pro™

For Windows To Go 8.1 and Windows 10

WorkSafe & WorkSafe Pro

WorkSafe live drives from SPYRUS add new Windows 8.1 and Windows 10 support for USB CCID on FIPS 140-2 Level 3 validated EAL 5+ Rosetta® crypto hardware to the long list of features already available in our Secure Portable Workplace™ and Portable Workplace™ Windows To Go drives. Both WorkSafe (BitLocker enrypted) and WorkSafe Pro (hardware encrypted) live drives include an embedded FIPS 140-2 Level 3 PKI readerless smart card that authenticates user credentials. Enterprise users can enjoy the mobility of a pocket-sized, Microsoft-certified Windows To Go drive with authenticated access to all their enterprise network resources. Enterprise IT can rest assured that remote access to valuable resources is by authentic users running the corporate Windows image—even when booted from untrusted computers.

WorkSafe Pro provides military-grade XTS-AES 256 hardware encryption over the entire drive, providing the ultimate protection of the operating system, applications, and data storage. Both WorkSafe and WorkSafe Pro drives can utilize BitLocker software encryption.

The WorkSafe family of solid state drives delivers ultra-fast SSD performance with always-on data protection.

Bootable Live Drives Enable Mobile Work

WorkSafe transforms personal computers, including Macs supporting booting Windows, into compliant enterprise Windows computers—with or without connectivity. These devices have no impact on the host computer and leave no footprint behind.

Improves Endpoint Security

Take control of BYOD and remote computers. Unpatched, uncontrolled BYOD equipment creates a clear danger when permitted access to enterprise networks. WorkSafe live drives improve endpoint security by transforming BYOD and home computers into trustworthy network access points.

FIPS 140-2 Level 3 Embedded Tamper-Proof Smart Card for Multifactor Authentication

WorkSafe and WorkSafe Pro are Microsoft-certified drives that deliver the rich identity and authentication capability of an embedded Rosetta readerless smart card—nothing extra to carry or to lose.

USB CCID support means that WorkSafe includes built-in smart card capability that secures all keys in tamper-proof hardware. When WorkSafe is booted, your digital ID is automatically available for PKI digital certificate functions such as encrypted email, multifactor authentication, smart card logon, BitLocker To Go, and VPN access.

When not booted, WorkSafe serves as a readerless USB 3.0 smart card that enables you to use your digital certificates with any compatible computer.

WorkSafe supports PKCS #11 and CAPI/CNG crypto standards. The SPYRUS Minidriver Token Utility is included with WorkSafe for managing the smart card, certificates, and passwords.

Enables Seamless, Secure Remote Access

Remote or traveling workers see no difference in network experience between on-premises access or when using smart card authenticated VPNs from remote locations. With Microsoft DirectAccess VPN, users automatically connect and access the corporate network with the capability to store the keys and smartcard certificates on the embedded smart card controller.

Provides Layered Encryption

Always-on, tamper-proof hardware encryption in WorkSafe Pro prevents data at rest from being accessed, deleted, or modified. WorkSafe Pro encryption keys are never stored in flash memory. Optional BitLocker software encryption provides a second layer of security, and the BitLocker keys are stored in the hardware-encrypted compartment, inaccessible to hackers.

SPYRUS®

Hardware-Encrypted WorkSafe Pro Protects Windows 8.1 Integrity Even from Hostile PCs

WorkSafe Pro defends the integrity of the operating environment even when booted on compromised systems. Numerous health checks validate the integrity and detect tampering of the SPYRUS Toughboot™ loader, the hardware, and firmware prior to booting the OS.

The SPYRUS Toughboot loader is signed by Microsoft and meets all Secure Boot criteria. Secure Boot is a UEFI specification that checks for an approved digital signature in all drivers or OS loaders to prevent malware infections during the boot sequence.

Windows 8.1
Windows 10

Mobile Device, Identity, and Desktop Management

WorkSafe drives can be managed at multiple levels with the Microsoft Ecosystem and SPYRUS Solutions:

- Certificate services from Microsoft or others allow an organization to manage the issuing, renewal and revocation of certificates.
- Microsoft Certificate Services supports Active Directory. The enterprise CA publishes user certificates and certificate revocation lists (CRL) to the Active Directory.
- Microsoft Forefront Identity Manager enables administrators to reset, restore, revoke, and manage user certificates on the embedded smart card.
- Microsoft Direct Access for remote access allows connecting seamlessly and more securely to the corporate network without the need for a VPN. You can store the Direct Access keys and certs on the embedded smart card chip
- With the optional BitLocker software encryption, enterprises can add a second layer of encryption to the hardware encrypted SPYRUS WorkSafe Pro, providing defense-in-depth security. BitLocker can also be used to encrypt data on WorkSafe live drives.
- Microsoft System Center allows administrators to update and patch the OS and applications when WorkSafe devices are joined to the domain and also provision devices in the field remotely..
- The embedded SPYRUS Rosetta smart card, along with the SPYRUS Minidriver, allows enterprises to perform standard smart card security functions such as encrypted email, multi-factor authentication, smart card logon, and VPN access.

Read Only Protection

The optional Read Only mode assures an uncorrupted corporate image every time the drive boots. All changes to the OS, applications, or data files are erased when the drive shuts down. Enterprises can ensure that users work ONLY on the corporate network and do not store data locally on the drive.

Data Vault Read/Write Partition

WorkSafe drives can be provisioned with a Data Vault read/write partition where modified user files can be stored even when Read-Only mode is enabled. Data Vault can also be accessed on an unbooted WorkSafe drive as an external USB storage device.

Data Vault can be protected using Rosetta smart card security and/or BitLocker To Go.

Central Enterprise Device Management

The SPYRUS Enterprise Management System (SEMS™) for device management includes features to remotely disable and destroy devices, remotely reset passwords, enforce policy, audit transactions, and more.

SPYRUS®

Enterprise Users Insist on Mobility

WorkSafe and WorkSafe Pro drives provide continuity and security for mobile workers:

- Temporary or contract workers
- BYOD computers at the office
- Telework from home computer
- Road Warrior traveling light
- Continuity of Operations for disaster recovery

Access legacy Windows XP and Windows 7 computers with dual booting from hard disk or WorkSafe drive.

SPYRUS WorkSafe drives make an ideal configuration for remote access/VDI/Cloud, and Office 365, providing a true secure trusted endpoint. Your enterprise can enforce access to only your network and prevent local access or data storage.

As a cost-effective teleworker solution, use SPYRUS 32 GB Windows To Go drives with the Read Only option to boot SPYRUS drives securely from untrusted home computers. Your organization can enforce work and data saving to the enterprise network, or if required, modified files can be saved on a Data Vault read/write partition.

	XTS-AES 256 Hardware Encryption	Layered Data Security	Built in PKI Smart Card	Data Vault Read/Write	Read Only Configuration	SEMS Device Management Option	Bit Locker full disk and/or Data Vault
WorkSafe Pro	✓	✓	✓	✓	✓	✓	✓
WorkSafe			✓	✓	Upgrade	✓	✓
Secure Portable Workplace	✓	✓		✓	✓	✓	✓
Portable Workplace				✓	Upgrade	✓	✓

Features of SPYRUS WorkSafe and SPYRUS Portable Workplace Windows To Go Drives

About SPYRUS

SPYRUS delivers innovative encryption solutions that offer the strongest protection for data in motion, data at rest and data at work. For over 20 years, SPYRUS has delivered leading hardware-based encryption, authentication, and digital content security products to government, financial, and health care enterprises. To prevent the insertion of untrusted components, patented Secured by SPYRUS™ security technology is proudly designed, engineered, and manufactured in the USA to meet FIPS 140-2 Level 3 standards. SPYRUS has collaborated closely with Microsoft to deliver certified portable platforms for Windows 7, Windows 8, Window 8.1. and Windows 10. SPYRUS is headquartered in San Jose, California.

See *www.spyrus.com* for more information.

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 (1 TB coming soon)
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) 0°C - 70°C

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

High Temperature Storage (MIL-STD-810, METH 501) 85°C; 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, 100°C; 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 400-451001-05