SPYRUS®

Windows To Go Xtreme Drives

For multiple Windows To Go operating environments on a single drive

Windows To Go Xtreme (WTGXtreme™)

SPYRUS WTGXtreme drives bring a new dimension to the world of Windows To Go operations. The drives are built on the features of the award winning SPYRUS Windows To Go family, incorporating the most advanced encryption and security technologies with the greatest versatility in size and performance features in the industry. WTGXtreme takes an evolutionary leap forward by allowing multiple processing environments with their own independent operational profile on the same drive. Strong cryptographic separation ensures a high assurance environment for each profile.

Secure Portable Workplace Xtreme & WorkSafe Pro Xtreme

Two models of SPYRUS WTGXtreme drives are available: the Secure Portable Workplace Xtreme (SPWXtreme™) and the WorkSafe Pro Xtreme (WSPXtreme™). Both models combine Secured by SPYRUS™ encryption and security technologies with a USB 3.0 drive certified for Windows To Go (WTG). The WSPXtreme drive also provides fully integrated PKI smart card support from the embedded Rosetta® Micro FIPS 140-2 Level 3 certified EAL5+ security controller when used with the SPYRUS Mini-Driver or PKCS#11 software. All WTGXtreme drives can be provisioned with multiple independent profiles, each with its own Windows 8, 8.1, or 10 operating system and independently encrypted with its own unique set of media encryption keys. This provides the organization with options of different processing environments, or profiles, for up to four independent users, administrators, or applications while maintaining a strong cryptographic separation between each environment.

Same high assurance security profile available on all SPYRUS Secure Windows To Go Drives

SPYRUS WTGXtreme drives provide the same robust set of security features available on all of the SPYRUS Secure Windows To Go drives. Some of these features apply to the drive as a whole but many can be uniquely configured for each profile that is provisioned on any particular drive.

WTGXtreme Drive Level Security Features

Secure Boot – The WTGXtreme drives defend the integrity of the operating environment throughout the boot process of each profile, even when the drive is booted on compromised systems. Numerous health checks validate the integrity and detect tampering of the hardware and firmware of the drive, as well as the SPYRUS ToughBoot™ loader and the Windows bootloader, prior to booting the OS. The SPYRUS ToughBoot loader is signed by Microsoft and meets all UEFI Secure Boot criteria allowing an additional integrity check during the boot process. This is done to prevent malware infections from corrupting the boot sequence.

Hardware Read-Only on Boot Compartment – To add additional protection to the boot environment of the WTGXtreme drives, the entire Boot Compartment can be protected by placing it in a hardware enforced read only mode. This will block changes that are attempted to be made on the boot component of the drive. In addition, until successful user authentication into one of the configured profiles, none of the encrypted memory on the drive can be accessed via the USB interface. This way, when the drive is "At Rest" only the read only boot compartment is exposed to possible cyber-attack.

Access Privilege Control – All WTGXtreme drives can be configured with a policy that controls the conditions under which the encrypted memory on the drive can be accessed. These include:

- Boot Only – The drive memory can only be accessed from the successfully authenticated and booted drive.
- Limited Access – The drive can be logged on and accessed from a different machine but read only access is enforced.
- Full Access – Full read-write access will be allowed from a different machine once the drive is logged on.

Built-in PKI Smart Card – On the WSPXtreme version of the WTGXtreme drives the embedded SPYRUS Rosetta smart card, along with the Microsoft certified Minidriver, allows enterprises to perform standard smart card security functions such as Office file encryption and signing, signed and encrypted e-mail, multi-factor authentication, smart card logon, and VPN access, using strong PKI credentials from a FIPS 140-2 Level 3 certified EAL5+ hardware security module. In addition, a PKCS#11 library is available to support applications that utilize this interface standard.

SPYRUS®

Profile Unique Security Features

Hardware Full Disk Encryption – Always-on, tamper-proof hardware full disk encryption within all WTGXtreme drives provides the ultimate protection of the operating system, applications, and data storage, preventing data at rest from being accessed, deleted, or modified. This is implemented in a way that allows all of the memory configured for each profile on a WTGXtreme drive to be encrypted using its own unique full-entropy encryption keys. These keys are never stored in flash memory and are only made available after successful authentication into a specified profile. This provides for strong cryptographic separation between profiles, thereby enabling independent and isolated operation of the operating environment in each profile, and preventing data leakage between profiles.

Optional Read Only Protection for Operating System Volume Read Only mode assures the use of an uncorrupted operating system image every time a particular profile on the WTGXtreme drive boots. Each WTGXtreme profile may be configured with the SPYRUS "Read Only" option. When Read Only mode is enabled, all changes to the Windows partition of that profile are reset when the user shuts down the drive; returning it to its original known media state. Since it prevents unauthorized persistent data storage, Read Only mode is ideal for enforcing users to only work on the network, through VDI or in the cloud, and to further prevent storing data locally; helping to prevent data leakage of important or critical enterprise information.

Data Vault Read/Write Volumes – Each WTGXtreme profile may be configured with one or two optional size settable Data Vault read/write volumes for storing data files. Data Vault volumes have read/write capability even when Read Only mode is enabled, so users can store data files in a Data Vault without losing them. Administrators can have the Windows OS and applications set to Read Only mode, which helps prevent transfer of malware to the enterprise networks, while maintaining the ability for users to store data on the device. These Data Vault volumes can be accessed, if the configured policy allows (see "Access Privilege Control" above), from an already booted Windows environment without directly booting from the drive. This allows a user to transfer files to and from their Data Vault volumes from another operational desktop environment.

Layered Data Security – Using the optional BitLocker software encryption from Microsoft, enterprises can add a second layer of encryption to the Windows volume or either Data Vault volume on any profile on the WTGXtreme drive. This allows additional defense in depth protection to be configured wherever it is needed. And wherever it is used, the BitLocker keys are stored within the hardware-encrypted compartment, making them inaccessible to hackers during Data-At-Rest.

Versatile Use Cases

By allowing multiple processing environments on the same drive, each with its own independent operational profile, the WTGXtreme drives bring the versatility and security of the SPYRUS WTG technology to an ever increasing number of use cases. A sampling of these use cases is described below.

Bring Your Own Device (BYOD)

If an enterprise employee is going to share the use of a computing device for both corporate and personal use (such as doing on-line banking over lunch), both parties are going to want to assure strong separation between their operating environments to ensure there is no compromise of sensitive data from either environment.

The SPYRUS WTGXtreme drives satisfy this requirement in a single convenient package. The independent authentication and drive encryption of each profile provides very strong firewalling between operating environments.

Protected Internet Access

Some organizations do not allow access to the Internet from organization owned computing platforms or organization specific operating system images which sometimes causes employee work inefficiencies. WTGXtreme solves this issue by having the capability to boot only into the locked down organization image or conversely when Internet is required, to boot into an alternative profile image that allows internet access when operating outside of the organization mandates.

SPYRUS®

Shared PC

Many organizations run 24x7 help desk support. The WTGXtreme with multiple profiles supported can allow up to four individuals to operate from the same device to provide the necessary four shift help desk support. Similarly, multiple healthcare professionals can be given access to a single device, for example, at a nurse's station or critical care computing resources in an emergency room.

Enterprise Migration

As enterprises transition from Windows 7 to Windows 8.1 and on to Windows 10, it is virtually impossible to make the roll-over to a new operating environment instantaneously. There will be legacy applications that are essential to enterprise operations which haven't yet been ported to the new operating system. Add to this the training time for employees to learn the new operating environment and most likely you are looking at an extended transition interval. To minimize inefficiencies and a general disruption of enterprise operations, it is helpful if employees can have access to both their current environment and the new environment they are expected to transition to.

The SPYRUS WTGXtreme drives are an ideal solution to ease this transition. With a WTGXtreme drive a user can boot into either environment, have full operational capability in each, and have access to either environment on their existing machine.

Domain Administration

Many system administrators manage multiple networks spanning different administrative domains. For additional secure access to each domain, administrators can use a different profile for managing each network. Additionally, by utilizing the read only mode on each or specific profiles, the transfer of malware across domains is dramatically minimized.

WTGXtreme drives are also ideal for implementing the Microsoft Privileged Access Workstation (PAW), which, for sensitive tasks, provides a dedicated operating system that is protected from Internet attacks and threat vectors. Separating these sensitive tasks and accounts from the administrator's daily use workstations and devices provides very strong protection against a wide variety of attacks and other system vulnerabilities.

Cross Domain Use

Many organizations segregate user access to different types of data based on that individual's need to see the type of data stored on the networks. Users could potentially use a specific profile for multi-domain type of access to different levels of data classification. By using the embedded smart card in the WSPXtreme, different certificates can be stored for the different profiles providing another layer of secure authentication to that specific information stored on the network.

Many government organizations restrict access to users based upon levels of data classification stored on the networks. For example, the United States has data classifications such as Sensitive But Unclassified (SBU), SECRET and TOP SECRET, with each requiring different user credentials. Using multiple profiles in the WTGXtreme, with different credentials stored in the respective profiles for domain access to the different levels of data classification, one device can be used to access multiple domains with strong cryptographic separation between profiles, providing a trusted cross domain platform.

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 capacity: 101.6 mm x 24.2 mm x 10.8 mm (+/- 0.20)
1 TB capacity: 104 mm x 24.2 mm x 12 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)

Configurability

SPYRUS WTG Xtreme drives can be provisioned with up to 4 independent, cryptographically isolated, Windows operating environments to support multi-user, cross-domain, enterprise migration, BYOD, and other operational scenarios. It is recommended each profile have a minimum 64 GB capacity.

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.

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 400-530001-02