SPYRUS®

Linux2Go™ Drives

Full Linux operating environment on a USB 3.0 SSD drive

Linux2Go

SPYRUS Linux2Go drives bring a new dimension to the world of secure mobility operations allowing secure Linux operating system on a USB 3.0 SSD drive. The drives are built on the features of the award winning Microsoft certified 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.

Secure Portable Workplace & WorkSafe Pro for Linux environments

Two models of SPYRUS Linux2Go drives are available: the Secure Portable Workplace (SPW) and the WorkSafe Pro (WSP). Both models combine Secured by SPYRUS™ encryption and security technologies with a USB 3.0 drive. The WSP 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 PKCS#11 software.

Same high assurance security profile available on all SPYRUS Secure Linux2Go Live Drives

SPYRUS WTG drives provide the same robust set of security features available on all of the SPYRUS Secure Windows To Go live drives.

Linux2Go Drive Level Security Features

Secure Boot – The Linux2Go 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 Linux2Go 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, none of the encrypted memory on the drive can be accessed. This way, when the drive is "At Rest" only the read only boot compartment is exposed to possible cyber-attack.

Hardware Read-Only on Encrypted Profiles – All Linux2Go drives can be configured so that the hardware encrypted operational compartments can be additionally 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 or encrypted profiles. In addition, until successful user authentication, none of the encrypted memory on the drive can be accessed.

This way, when the drive is "At Rest" both the read only boot compartment and the encrypted operating compartment are safeguarded from possible cyberattack. A read only mode device is ideal for organizations who only want to the user to access corporate networks from a trusted "thin client" and not allowing saving the data locally to the device.

Built-in PKI Smart Card – On the WSPversion of the Linux2Go drives the embedded SPYRUS Rosetta smart card, along with the SPYRUS PKCS#11 driver, allows enterprises to perform standard smart card security functions such as multi-factor authentication and VPN access, using strong PKI credentials from a FIPS 140-2 Level 3 certified hardware security module.

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 metric 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 Linux2Go 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 Linux2Go 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 Linux2Go devices in the challenging healthcare environments as well.

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 Algorithm 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]

Concatenation KDF (SP800-56A)

RSA 1024 and 2048 Signature Algorithm (Note RSA 1024 has been deprecated by NIST.) RSA 1024 and 2048 Key Exchange (Note RSA 1024 has been deprecated 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.

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

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 400-540001-01