SPYRUS®

WorkSafe Pro™

Encrypted USB 3.0 Windows To Go Drive

with Embedded Rosetta® Smart Card

Getting Started Guide

SUITE B ON BOARD®

Document No: 513-451002-09

Patents

This product is protected under one or more of the U.S. patents found at the following address: www.spyrus.com/company/patent-markings.html

Trademarks

SPYRUS, the SPYRUS logos, SPYCOS, ROSETTA, SPEX/, LYNKS, Security in a Box, Security to the Edge, Multisession, Cryptocalculator, Toughboot, DeviceSSL, TLS Platinum, TLS Gold, NcryptNshare, Secure Pocket Drive, Suite B On Board, Rosetta MicroSDHC, TrustedFlash, PocketVault, RES Pro, RESDisk, RES4Office, Secure Pocket Drive, Secure Portable Workplace, Secured by SPYRUS, Worksafe, Worksafe Pro, LINUX2Go, WTGXtreme, and SPYRUS Enterprise Management System (SEMS) are either registered trademarks or trademarks of SPYRUS in the United States and/or other countries.

SPYRUS Product Design Information License Agreement

PLEASE READ THIS! This is a legal agreement between SPYRUS Solutions, Inc. ("SPYRUS") and the recipient of this document, whether an individual or an entity ("You"). BY ACCESSING, USING OR PROVIDING FEEDBACK ON THE ATTACHED DOCUMENT ("this document"), YOU AGREE TO BE BOUND BY THESE TERMS.

1. **This document is SPYRUS confidential information under Your most recent Non-Disclosure Agreement with SPYRUS.** However, Your only rights to use this document are as described in Paragraph 2, below.

2. You may review the material in this document only (a) to provide feedback to SPYRUS; or (b) as a reference to assist You in planning and designing Your product, service or technology ("Your Product") to interface with a SPYRUS product, technology or service ("SPYRUS Product") as **described** in this document. All other rights are retained by SPYRUS; You have no other rights to use the intellectual property in this document. You may not (i) duplicate any part of this document, (ii) remove this Agreement or any notices from this document, or (iii) give any part of this document or assign or otherwise provide Your rights under this Agreement, to anyone else.

3. You have no obligation to give SPYRUS any suggestions, comments or other feedback. If You do give SPYRUS feedback on any version of this specification, You agree that:

   A. SPYRUS may freely use, disclose, reproduce, license or otherwise distribute, and exploit Your feedback in its products, services, technologies, specifications and other documentation ("SPYRUS Offerings"), without any intellectual property restrictions, payments or other obligations;

   B. You also grant SPYRUS' customers and other third parties, without charge, any patent or other rights necessary to use, and to enable their products, services or technologies to interface with, Your feedback that has been incorporated into any SPYRUS Product; and

   C. You will not give SPYRUS any feedback (i) which You have reason to believe is subject to any patent, copyright or other intellectual property claim or right of any third party; or (ii) which is subject to license terms that seek to require any SPYRUS Offering incorporating or derived from such feedback, or any SPYRUS intellectual property, to be licensed or otherwise shared with any third party.

4. This document contains preliminary information that may change prior to release of any associated SPYRUS Product, and is provided entirely "AS IS." To the extent permitted by law, SPYRUS MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND SHALL HAVE NO LIABILITY TO YOU FOR ANY DAMAGES, IN CONNECTION WITH THIS DOCUMENT OR ANY INTELLECTUAL PROPERTY IN IT.

5. If You are acquired, or if more than a 20% of Your ownership changes, this Agreement automatically terminates and You must destroy this document.

6. This Agreement is governed by the laws of the State of California. Any dispute involving it must be brought in the federal or state courts located in Santa Clara County, California, and You waive any defenses allowing the dispute to be litigated elsewhere. If there is litigation, the losing party must pay the other party's reasonable attorneys' fees, costs and other expenses. If any part of this Agreement is unenforceable, it will be considered modified to the extent necessary to make it enforceable, and the remainder shall remain in effect. This Agreement is the entire agreement between You and SPYRUS concerning this document; it may be changed only by a written document signed by both You and SPYRUS.

Table of Contents

Introduction

The WorkSafe Pro Windows To Go drive from SPYRUS is a tamper-proof, hardware-encrypted USB 3.0 drive that can boot your Windows 8.1 image on most PCs certified for Windows 7 or Windows 8, and on many Macintosh computers (see the section "Tips for Booting from a USB Drive" in this guide for more information). The SPYRUS Toughboot™ loader unlocks the WorkSafe Pro drive and allows it to boot Windows 8.1. After you boot the WorkSafe Pro drive, you use it like any Windows 8.1 computer.

Some WorkSafe Pro drives are configured with the Read Only option. When Read Only mode is enabled, any files that are added to or changed on the main drive while the WorkSafe Pro drive is booted are deleted (added files) or restored to the original state (changed files) the next time the drive is booted.

Your WorkSafe Pro drive may be configured with one or two Data Vault read/write partitions for storing data files. Data Vault partitions have read/write capability even when Read Only mode is enabled, so you can store changed or added files in the Data Vault without losing them. You can also access Data Vault on an unbooted WorkSafe Pro drive as an external USB storage drive.

The WorkSafe Pro and the optional Data Vaults can both be configured with BitLocker for an extra layer of encryption. You can use the same BitLocker password for both the main drive and the Data Vaults, or you can assign different BitLocker passwords for each. You can also configure BitLocker encryption for one or both Data Vaults only, or for the main drive only.

Organizations that use the SPYRUS Enterprise Management System (SEMS™) to manage USB devices can configure WorkSafe Pro drives for SEMS management. Use the procedure in the section "First-Time Boot to Register with SEMS" in this guide for information on registering a WorkSafe Pro drive with SEMS.

WorkSafe Pro drives also include smart card support on its FIPS 140-2 Level 3 validated EAL 5+ Rosetta crypto hardware. The embedded Rosetta Smart Card can be used with your digital certificates whether or not the WorkSafe Pro is booted.

Smart card interface is handled by the SPYRUS Rosetta Minidriver version 6, which is downloaded and updated automatically through Microsoft Update when you connect the WorkSafe Pro drive to a computer with access to the Internet. The SPYRUS Rosetta Minidriver supports both RSA and ECC PKI for most functions, and RSA only for smart card logon.

The SPYRUS Rosetta Minidriver Tools (Admin Tool and Token Utility) may be included on the WorkSafe Pro drive to manage the Rosetta Smart Card and your digital certificates. See the section "Using the Rosetta Smart Card" in this guide for more information.

Host System Requirements

Windows computers:

- PC certified for Windows 7 or higher
- USB 2.0 or USB 3.0 port or a powered USB hub connected to the computer
- Firmware (UEFI or BIOS) that supports booting from a USB port
- (SEMS only) Host computer for first boot must be a Windows computer connected to a network with access to the SEMS server.

See the section "Tips for Booting from a USB Drive" in this guide for requirements and more information on booting from other host systems and devices and changing settings to always boot from a USB drive.

Important: If the host computer has BitLocker enabled, suspend BitLocker before changing the BIOS/UEFI settings to always boot from a USB drive. Resume BitLocker only after changing the BIOS/UEFI settings. If BitLocker is not suspended first, the next time the computer is started it will boot into Recovery mode.

Using the WorkSafe Pro

You can boot Windows 8.1 from the WorkSafe Pro drive on nearly any PC certified for Windows 7 or higher and on many Apple Macintosh computers running OS X 10.6 or higher.

When the WorkSafe Pro drive is booted, you can access your digital certificates on the embedded Rosetta Smart Card just as you would from any connected smart card. You can also use an unbooted WorkSafe Pro drive as a USB smart card reader to access your certificates on the Rosetta Smart Card. See the section "Using the Rosetta Smart Card" in this guide for information on using and managing the embedded Rosetta Smart Card.

If your WorkSafe Pro drive is configured for use with the SPYRUS Enterprise Management System (SEMS™), use the procedure in the section "First-Time Boot to Register with SEMS" the first time you boot your drive. After registering with SEMS, use the procedure in the section "Boot WorkSafe Pro" to boot the drive.

If your WorkSafe Pro drive is *not* configured for SEMS, always use the procedure in the section "Boot WorkSafe Pro" to boot the drive, including the first time.

This section of the *WorkSafe Pro Getting Started Guide* explains the following procedures:

- (SEMS Only) First-Time Boot to Register with SEMS
- Boot WorkSafe Pro
- Shut Down WorkSafe Pro
- Access the Data Vault Partitions
- Enable or Disable Read Only Mode
- (SEMS Only) Enable a Disabled WorkSafe Pro
- (SEMS Only) Recover Forgotten WorkSafe Pro Boot Password

(SEMS Only) First-Time Boot to Register with SEMS

WorkSafe Pro drives configured for SEMS have the SEMS client software preinstalled. The first time you boot a SEMS-configured WorkSafe Pro drive, boot it on a Windows computer that is connected to a network with access to the SEMS server to allow the drive to register with SEMS. After your WorkSafe Pro is registered with SEMS, always use the procedure in the section "Boot WorkSafe Pro" in this guide to boot the WorkSafe Pro drive.

SPYRUS recommends that you configure the host computer to always boot from a USB drive when one is present. For more information about booting from a USB drive on various computers and operating systems, see the section "Tips for Booting from a USB Drive" in this guide.

When you receive your newly provisioned WorkSafe Pro drive, ask about the following information:

- What Windows logon account and password is configured for your use?
- What is the WorkSafe Pro boot password for the Toughboot loader?

Note: During SEMS registration you will be prompted to change the boot password.

- If the drive is configured with the Read Only option, is Read Only mode enabled?
- If BitLocker is enabled on the main drive, what is the BitLocker password?
- Is the SEMS for WTG Enable utility stored in the *Utils* folder of the WorkSafe Pro drive?

To boot a WorkSafe Pro configured for SEMS the very first time, do the following:

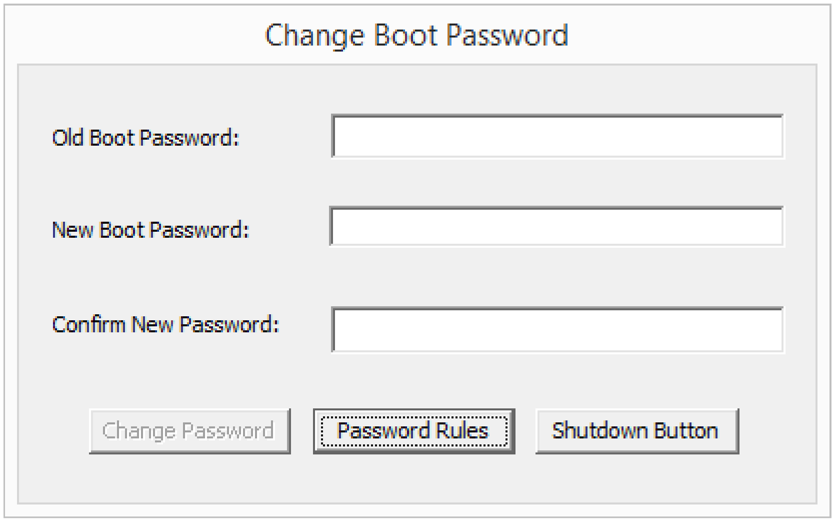
1. Ensure that the host computer meets the requirements outlined for Windows computers in the section "Host System Requirements" in this guide and is connected to a network with access to the SEMS server.
2. Shut down the host computer.
3. Insert the WorkSafe Pro drive into a USB port connected to the host computer.
4. Power-on the computer. If the computer is not configured to automatically boot from a USB drive, follow the procedure to manually boot the computer from a USB drive.

   Note: See the section "Tips for Booting from a USB Drive" in this guide for more information.
5. When prompted, enter the WorkSafe Pro boot password, and then press **Enter**.
6. If prompted for a BitLocker password, enter the BitLocker password for the main drive, and then click **Unlock**.
7. If the drive goes through an automatic Out of Box Experience (OOBE) procedure, wait for this to finish and follow any onscreen instructions. If the WorkSafe Pro drive automatically restarts and your computer is NOT configured to automatically boot from a USB drive, follow the procedure to manually boot the computer from a USB drive as soon as the computer restarts, and then continue.

   Note: If your WorkSafe Pro drive has already been configured for SEMS management, it might not go through the OOBE procedure.
8. When Windows 8.1 starts, log on to your Windows account.
9. In the Start menu, select the **Desktop**.
10. When the Change Boot Password dialog box appears, for Old Boot Password, type the current WorkSafe Pro boot password. For New Boot Password and Confirm New Password, type a new WorkSafe Pro boot password that complies with the password requirements, and then click **Change Password**.

    You can also click **Password Rules** to see the requirements for WorkSafe Pro boot passwords or click **Exit** to close the dialog box.

    Note: You must change the WorkSafe Pro boot password within three minutes to avoid cancelling the process. A notice appears when two minutes remain, and again when one minute remains.



11. Wait until you see the “Device Registered in SEMS” message, and then click **OK**.
12. In the Password Successfully Changed dialog box, click **OK**.

    Note: If you do not click OK, the notice disappears automatically after a few moments.

Boot WorkSafe Pro

SPYRUS recommends that you configure the host computer to always boot from a USB drive when one is present. For more information about booting from a USB drive on various computers and operating systems, see the section "Tips for Booting from a USB Drive" in this guide.

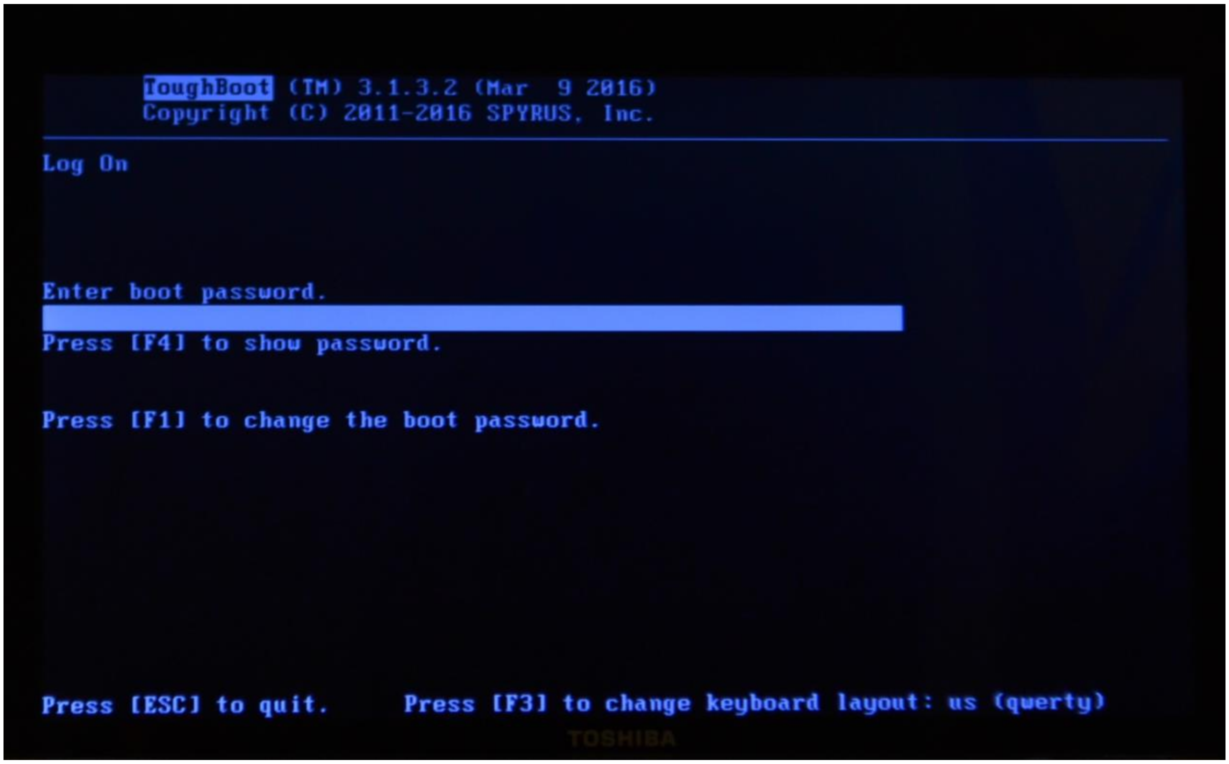
When you receive your newly provisioned WorkSafe Pro drive, ask about the following:

- What Windows logon account and password is configured for your use?
- If the drive is configured with the Read Only option, is Read Only mode enabled?
- If BitLocker is enabled on the main drive, what is the BitLocker password?
- If any Data Vaults are configured, is BitLocker enabled? If yes, you need the BitLocker password(s).
- If you will boot the WorkSafe Pro on a Macintosh computer, has the drive been set up to do this?

To boot WorkSafe Pro, do the following:

1. Ensure that the host computer meets the requirements outlined in the section "Host System Requirements" in this guide.
2. Shut down the host computer.
3. Insert the WorkSafe Pro drive into a USB port connected to the host computer.
4. Power-on the computer. If the computer is not configured to automatically boot from a USB drive, follow the procedure to manually boot the computer from a USB drive.

   Note: See the section "Tips for Booting from a USB Drive" in this guide for more information.
5. The ToughBoot logon screen should appear as shown below.

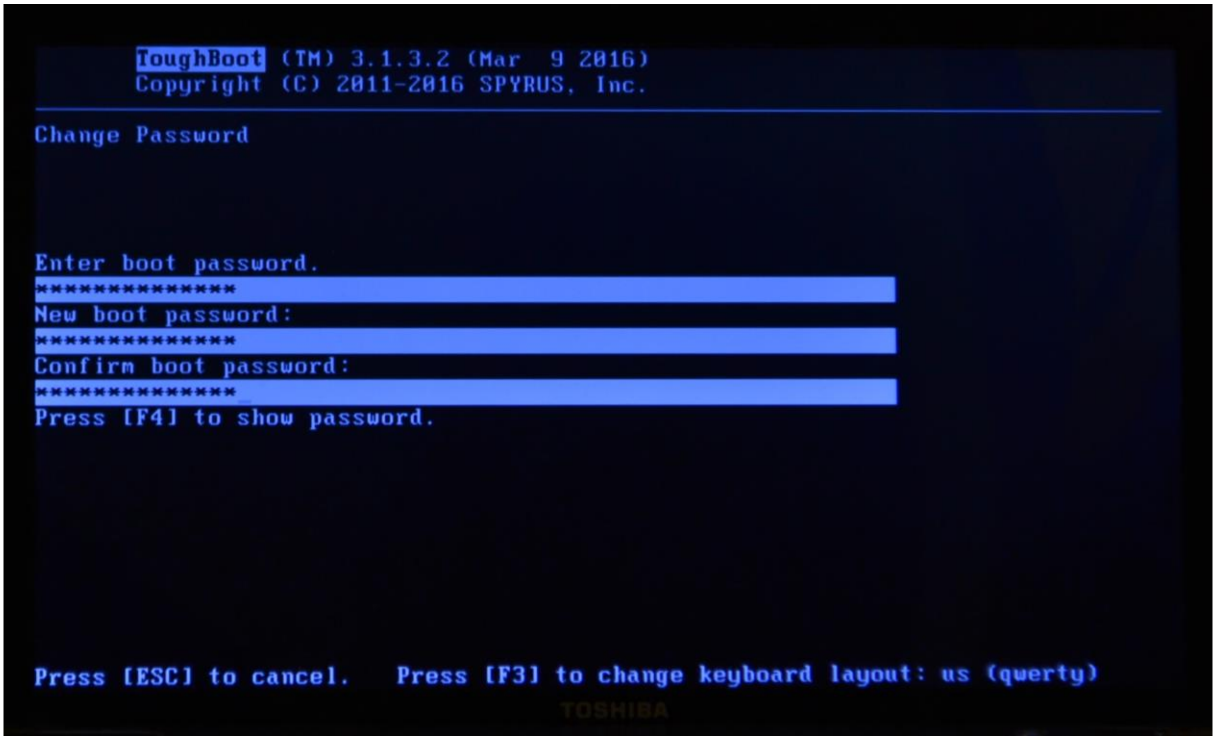


```
      ToughBoot (TM) 3.1.3.2 (Mar  9 2016)
      Copyright (C) 2011-2016 SPYRUS, Inc.

Log On


Enter boot password.

Press [F4] to show password.


Press [F1] to change the boot password.





Press [ESC] to quit.    Press [F3] to change keyboard layout: us (querty)
```

6. By default, ToughBoot starts up assuming it is connected to a "US English keyboard." If you have a different language keyboard, you can press the F3 function key and cycle through the available options. The last selected option will be remembered by ToughBoot for future booting of the drive. [Note: With this release the available options are: US English, French, and German.]

7. By default, Toughboot will hide the actual password characters as they are typed in. If you want to see what you have entered (which may be helpful when using a foreign language keyboard), you can press the F4 function key. This will toggle between showing and hiding the password characters.

8. If the selected profile has been configured to allow the user to change their password during the boot process, you can press the F1 function key initiate this process. This will bring up the Change Password screen as shown below.



```
       ToughBoot (TM) 3.1.3.2 (Mar  9 2016)
       Copyright (C) 2011-2016 SPYRUS, Inc.

Change Password



Enter boot password.
**************
New boot password:
**************
Confirm boot password:
**************
Press [F4] to show password.







Press [ESC] to cancel.   Press [F3] to change keyboard layout: us (qwerty)
```

After changing your password, you will be returned to the Log On screen.

9. When prompted, enter the WorkSafe Pro boot password and press **Enter**.

10. If prompted for a BitLocker password, enter the BitLocker password for the main drive, and then click **Unlock**.

11. (First-time boot only) If the drive goes through an automatic OOBE procedure, wait for this to finish and follow any onscreen instructions. If the WorkSafe Pro drive automatically restarts and your computer is NOT configured to automatically boot from a USB drive, follow the procedure to manually boot the computer from a USB drive as soon as the computer restarts, and then continue.

12. When Windows starts, log on to your Windows account.

Shut Down WorkSafe Pro

To shut down a booted WorkSafe Pro drive, do the following:

Note: It is always wise to save all open files and close all open applications prior to shutting down any operational Windows system.

1. In Windows on the booted WorkSafe Pro drive, press **Ctrl+Alt+Del** to show the power on/off button.
2. Click the **power on/off button** to shut down the host computer.
3. Safely remove the WorkSafe Pro drive from the computer.

Access Data Vault Partitions

The WorkSafe Pro drive can be configured with one or two Data Vault read/write partitions, which appear as lettered drives when your WorkSafe Pro drive is booted. You can save and store changed or new files to Data Vault read/write partitions, even if Read Only mode is enabled on your WorkSafe Pro.

You can also access Data Vault partitions when the WorkSafe Pro is not booted but is inserted into an already booted Windows 7 (or later) system. To do this you must enter the boot password through a special utility to unlock the encrypted drive. If a Data Vault has BitLocker encryption enabled, you must also provide the BitLocker password to access the Data Vault volume once the encrypted drive is unlocked.

Access Data Vault on a Booted WorkSafe Pro

To access a Data Vault on a booted WorkSafe Pro drive, do the following:

1. In Windows Explorer, on the booted WorkSafe Pro drive, select the lettered Data Vault drive.

   Note: If a Data Vault drive does not appear in Windows Explorer, an administrator may need to assign a drive letter manually.

2. If prompted for a BitLocker password, enter the Data Vault BitLocker password, and then click **Unlock**.
3. If the Data Vault is BitLocker protected and you are not prompted for the BitLocker password, right click on the lettered Data Vault drive and select the "Unlock Drive…" option to get prompted appropriately. As an alternative, you can use the *BitLocker Drive Encryption* utility in the Control Panel to log on to the BitLocker protected Data Vault volume.

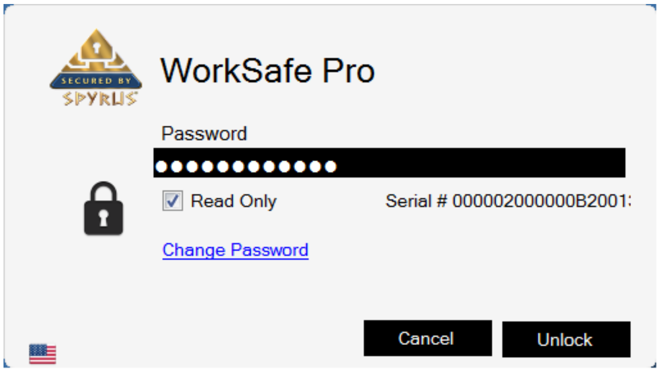
Access Data Vault on an Unbooted WorkSafe Pro

To access a Data Vault on an unbooted WorkSafe Pro drive, do the following:

1. Insert the WorkSafe Pro drive into a USB port connected to a computer certified to use and is running Windows 7 or Windows 8.
2. In Windows Explorer, select the lettered WorkSafe Pro drive (it is labeled *WSPBOOT* by default).

   Note: If the WorkSafe Pro drive does not appear in Windows Explorer, an administrator may need to assign a drive letter manually.

3. Open the *Utils* folder on the WorkSafe Pro drive.
4. In the *Utils* folder, run the *xLauncher.exe* application.
5. In the SPYRUS WorkSafe Pro dialog box, type the WorkSafe Pro boot password, and then click **Unlock**.



WorkSafe Pro

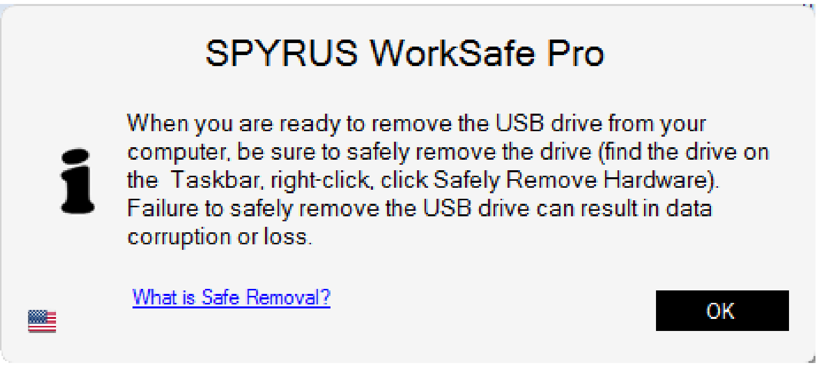
Password

●●●●●●●●●●●●

☑ Read Only Serial # 000002000000B2001:

Note: By default, the xLauncher will unlock the drive with hardware read-only protection turned on to prevent unintentional changes to the contents of the drive. If you want to make changes, such as storing additional files to a Data Vault, you will need to uncheck the **Read Only** option before you click **Unlock**.

6. Read the message reminding you to safely remove the WorkSafe Pro from the host computer, and then click **OK**.



SPYRUS WorkSafe Pro

When you are ready to remove the USB drive from your computer, be sure to safely remove the drive (find the drive on the Taskbar, right-click, click Safely Remove Hardware). Failure to safely remove the USB drive can result in data corruption or loss.

You can now see accessible Data Vault partitions as lettered drives in Windows Explorer.

Set Up Read Only

To complete the set up for SPYRUS WTG drives with the Read Only option, you must perform additional steps after provisioning.

Important: If the drives you provision include both SEMS support and Read Only, set the drives up for SEMS *first*, and *then* set up Read Only.

Read Only setup requires you to boot the SPYRUS WTG drive.

- To boot from a SPYRUS WTG drive on a Windows 8, 8.1, or 10.0 certified computer, press **Windows logo key + W**, search Settings for **Windows to Go startup options**, and then press **ENTER**. Select **Yes**, and then click **Save Changes**.
- To boot on a Windows 7 certified computer, you must either configure the BIOS in the host computer to always boot from a USB drive when connected or follow a procedure at startup (usually pressing a function key) to configure the one-time boot device order. See your setup computer's user documentation for this information.

For more information on booting SPYRUS WTG Drives, see the *Getting Started Guide* (available as PDF files in the *Documents* folder in the setup package) for the specific drive.

SPYRUS Windows To Go drives go through a sealing and setup process (Out of Box Experience, or OOBE) the first time they are booted after provisioning. For information on setting up a newly provisioned drive, consult the resources in the section “Microsoft Windows To Go Resources” in this guide.

Read Only setup requires the following:

- A Windows logon account with Administrator permissions on the provisioning computer.
- A removable drive, such as a USB flash drive or other external drive, containing a copy of the *ReadOnlyInstall* folder (found inside the *SPYRUS_WTGSetup* folder) from the setup package.

  Note: Copy the *ReadOnlyInstall* folder to the removable drive but leave the original *ReadOnlyInstall* folder on the provisioning computer as a backup.

- A SPYRUS WTG drive provisioned with the Read Only option.
- (Encrypted drives only) The boot password.
- BitLocker password(s), if BitLocker is enabled on the main drive and/or the Data Vault.

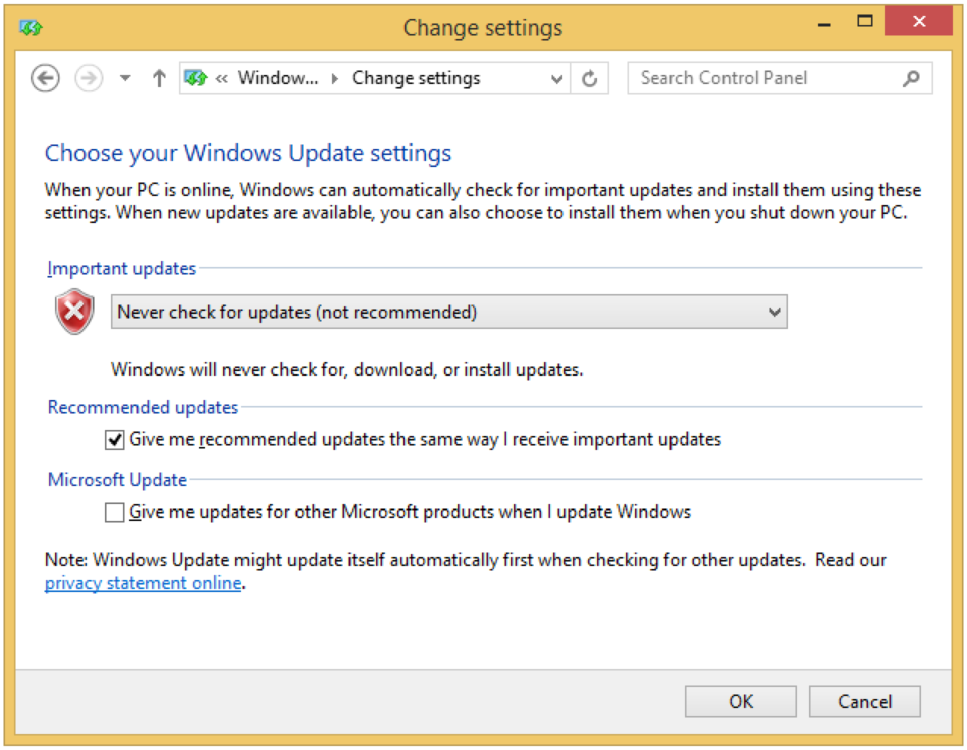
To set up a Read Only drive, do the following:

1. Shut down the provisioning computer.
2. Insert *one* provisioned SPYRUS WTG drive into a USB port or USB hub connected to the provisioning computer.
3. Boot the SPYRUS WTG drive.
4. (First boot only) Allow the drive to complete the Out of Box Experience (OOBE) process. When the OOBE process completes, reboot the SPYRUS WTG drive.
5. Log on to the drive as a Windows user with Administrator permissions.
6. Ensure that all drivers are installed, including Rosetta Minidriver drivers, and all automatic software updates that you want included are complete.

   Note: You will disable Windows Update in this procedure.

7. In the Control Panel under Windows Update, select Change Settings, then click **Never check for updates,** and then *clear* the check box for **Give me recommended updates the same way I receive important updates**. Click **OK.**

   Important: This step is optional but highly recommended. Updates will not persist if downloaded and installed while Read Only mode is enabled on the drive.



Choose your Windows Update settings

When your PC is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also choose to install them when you shut down your PC.

Important updates

Never check for updates (not recommended)

Windows will never check for, download, or install updates.

Recommended updates

☑ Give me recommended updates the same way I receive important updates

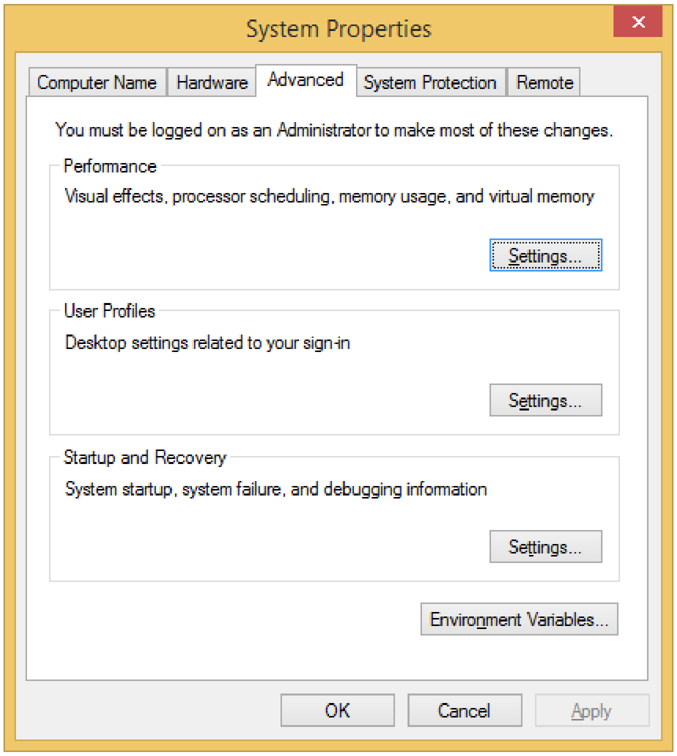
Microsoft Update

□ Give me updates for other Microsoft products when I update Windows

Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.

8. In Control Panel, select System, and then click **Advanced system settings**.

9. In System Properties on the Advanced tab, in the Performance area click **Settings**.



You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

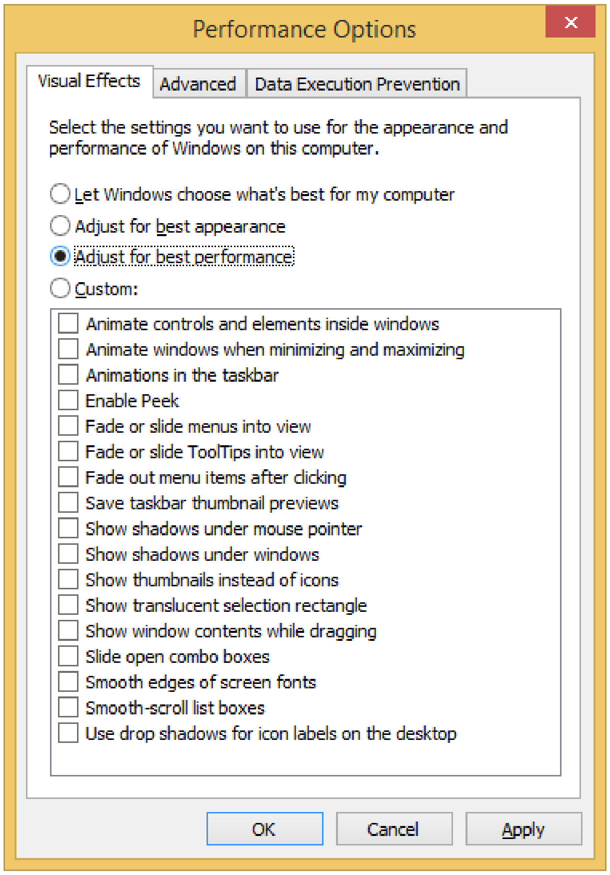
User Profiles

Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

10. In Performance Options on the Visual Effects tab, select **Adjust for best performance**, and then click **OK**.



Select the settings you want to use for the appearance and performance of Windows on this computer.

○ Let Windows choose what's best for my computer

○ Adjust for best appearance

● Adjust for best performance

○ Custom:

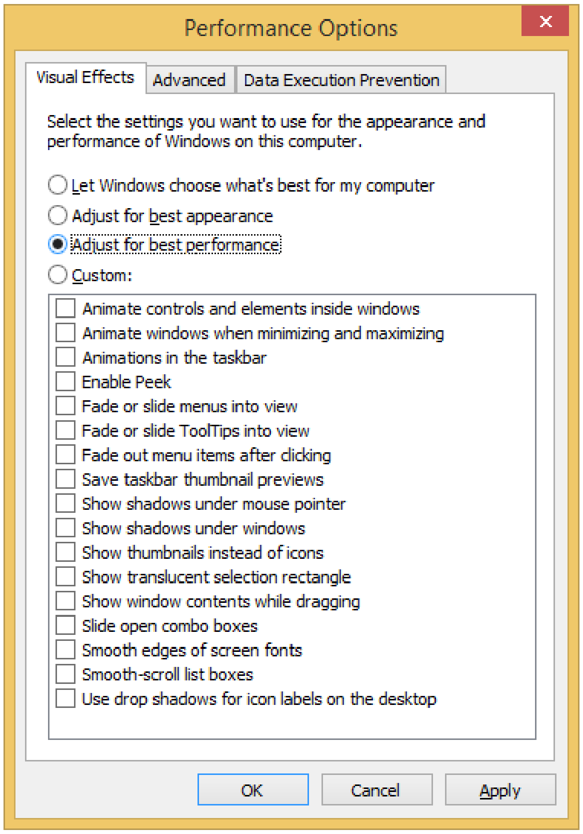
- □ Animate controls and elements inside windows
- □ Animate windows when minimizing and maximizing
- □ Animations in the taskbar
- □ Enable Peek
- □ Fade or slide menus into view
- □ Fade or slide ToolTips into view
- □ Fade out menu items after clicking
- □ Save taskbar thumbnail previews
- □ Show shadows under mouse pointer
- □ Show shadows under windows
- □ Show thumbnails instead of icons
- □ Show translucent selection rectangle
- □ Show window contents while dragging
- □ Slide open combo boxes
- □ Smooth edges of screen fonts
- □ Smooth-scroll list boxes
- □ Use drop shadows for icon labels on the desktop

11. Close Control Panel.
12. Connect the removable drive containing the *ReadOnlyInstall* folder to the computer where you booted the SPYRUS WTG drive.
13. Copy the *ReadOnlyInstall* folder from the removable drive to the Desktop on the provisioned SPYRUS WTG drive.
14. Run Command Prompt as an Administrator. In the Command Prompt window, use the **cd** command to navigate to the *ReadOnlyInstall* folder on the SPYRUS WTG drive.
15. In Command Prompt, at the prompt, type

    ConfigureSvcAndPageFile.cmd

    and then press **Enter**. Press any key when prompted (twice).

    When the script completes, the computer will immediately reboot.
16. Log on to the SPYRUS WTG drive using the same Windows Administrator logon account and verify that the Control Panel setting for Performance Options on the Visual Effects tab is still **Adjust for best Performance** (see steps 7 and 8).
17. On the Advanced tab, verify that the Total paging file size for all drives in the Virtual Memory area is at least **256 MB**.



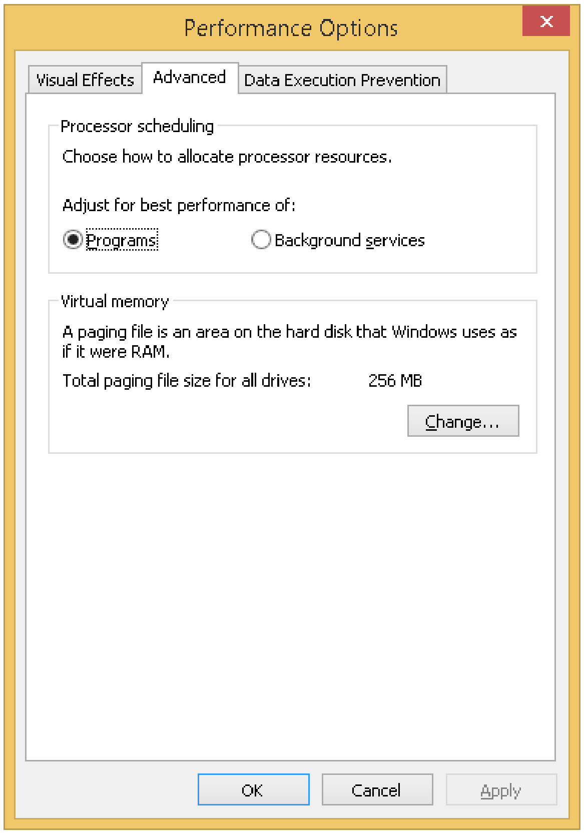
Performance Options

Visual Effects | Advanced | Data Execution Prevention

Select the settings you want to use for the appearance and performance of Windows on this computer.

○ Let Windows choose what's best for my computer
○ Adjust for best appearance
● Adjust for best performance
○ Custom:

□ Animate controls and elements inside windows
□ Animate windows when minimizing and maximizing
□ Animations in the taskbar
□ Enable Peek
□ Fade or slide menus into view
□ Fade or slide ToolTips into view
□ Fade out menu items after clicking
□ Save taskbar thumbnail previews
□ Show shadows under mouse pointer
□ Show shadows under windows
□ Show thumbnails instead of icons
□ Show translucent selection rectangle
□ Show window contents while dragging
□ Slide open combo boxes
□ Smooth edges of screen fonts
□ Smooth-scroll list boxes
□ Use drop shadows for icon labels on the desktop



Performance Options

Visual Effects | Advanced | Data Execution Prevention

Processor scheduling

Choose how to allocate processor resources.

Adjust for best performance of:

● Programs ○ Background services

Virtual memory

A paging file is an area on the hard disk that Windows uses as if it were RAM.

Total paging file size for all drives: 256 MB

18. Close Control Panel.
19. Run Command Prompt as an Administrator. In the Command Prompt window, use the **cd** command to navigate to the *Install* subfolder in the *ReadOnlyInstall* folder.
20. In Command Prompt, at the prompt, type

    InstallSpwDFlt.cmd

    and then press **Enter**.

    When the script completes, your computer will shut down automatically after 60 seconds. The next time you boot the SPYRUS WTG drive, Read Only mode is enabled.
21. (SEMS) If you were directed to this Read Only setup procedure from a SEMS setup procedure, return to the SEMS setup procedure now and continue from the step where you were directed to the Read Only setup procedure.
22. Include the following information with each drive when it is issued to a user:

    - The Windows account name and password to use with the drive.
    - The appropriate Getting Started Guide (available as PDF files in the *Documents* folder in the setup package).

        - *SPWGettingStartedGuide.pdf* (for encrypted Secure Portable Workplace™)
        - *WorkSafeProGettingStartedGuide.pdf* (for encrypted WorkSafe Pro)
        - *PWGettingStartedGuide.pdf* (for unencrypted Portable Workplace™)
        - *WorkSafeGettingStartedGuide.pdf* (for unencrypted WorkSafe™)

- Any applicable BitLocker passwords.
- (Secure Portable Workplace and WorkSafe Pro only) The boot password.
- (WorkSafe and WorkSafe Pro only) If the user needs to manage certificates or change the PIN on the Rosetta Smart Card, make the *RosettaMinidriverV6* folder (in the setup package) available. Provide the User PIN and Admin key if required.

Enable or Disable Read Only Mode

Some WorkSafe Pro drives are configured with the Read Only option. After the post-provisioning set up is complete, when Read Only mode is enabled, any files that are added to or changed on the main drive while the WorkSafe Pro drive is booted are deleted (added files) or restored to the original state (changed files) the next time the drive is booted. Any changes you make or files that you add are lost when you reboot the WorkSafe Pro drive.

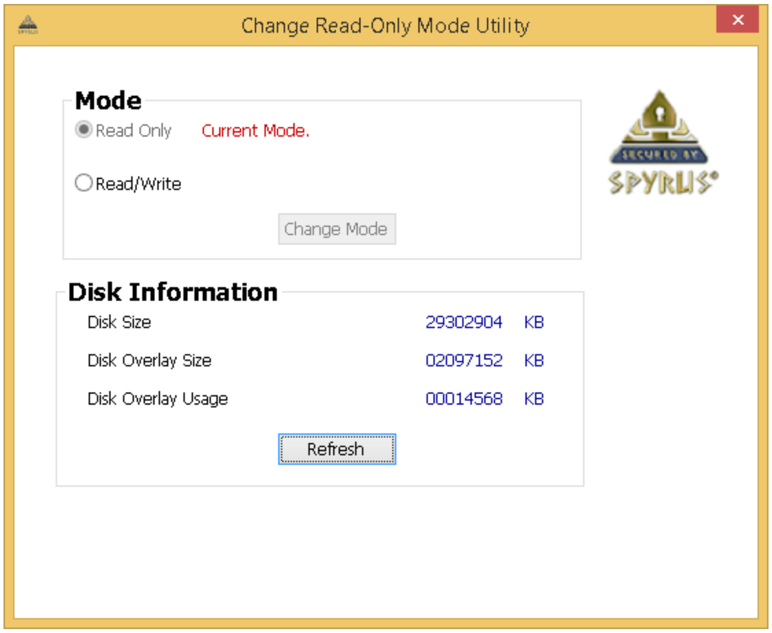
To save changes on the WorkSafe Pro drive, copy changed or added files to a Data Vault if available, or to an external storage drive before you shut down or reboot the WorkSafe Pro drive.

Note: Windows Update is disabled during setup on drives with the Read Only option. If you disable Read Only mode and want to receive automatic updates, enable Windows Update in the Control Panel.

To enable or disable Read Only mode, do the following:

1. On the booted WorkSafe Pro drive, log on as a Windows user with Administrator permissions.
2. Locate the file *SPWCpl.exe* on the drive. It is placed on the Desktop of the Windows administrator who set up the Read Only option on the WorkSafe Pro drive during provisioning.

   Note: The *SPWCpl.exe* application is installed only on the Desktop of the Windows user that set up the Read Only option on the drive. If you log on as a different Windows user, the *SPWCpl.exe* application will not appear on your Desktop but may be accessible on the set-up user's Desktop, depending on the permissions of your Windows user account.
3. Right-click *SPWCpl.exe*, and then click **Run as Administrator**.


Change Read-Only Mode Utility

Mode

● Read Only Current Mode.

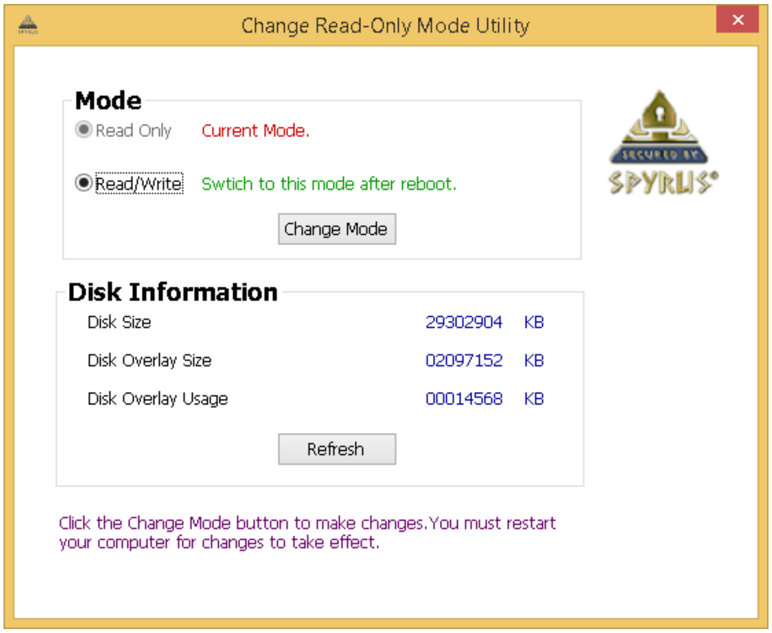
○ Read/Write

Disk Information

Disk Size	29302904	KB
Disk Overlay Size	02097152	KB
Disk Overlay Usage	00014568	KB

4. In the Change Read Only Mode Utility, select the new mode, and then click **Change Mode**. In the dialog box, click **Yes** to restart the SPYRUS WTG drive in the new mode.

   Note: You must select a new mode before the Change Mode button becomes available.


Change Read-Only Mode Utility

Mode

○ Read Only Current Mode.

● Read/Write Swtich to this mode after reboot.

Disk Information

Disk Size	29302904	KB
Disk Overlay Size	02097152	KB
Disk Overlay Usage	00014568	KB

Click the Change Mode button to make changes.You must restart your computer for changes to take effect.

(SEMS Only) Enable a Disabled WorkSafe Pro

A SEMS-managed WorkSafe Pro drive is disabled when:

- A SEMS administrator issues a DISABLE command to the WorkSafe Pro drive from the SEMS console.
- The WorkSafe Pro drive exceeds the allowed number of incorrect logon attempts allowed by policy.
- The WorkSafe Pro drive exceeds the number of offline logons allowed by SEMS policy.

A disabled WorkSafe Pro drive cannot be booted on a computer.

If the SEMS policy for the drive requires the boot password to be stored, when next you boot the drive after it is re-enabled, on a computer connected to a network with access to the SEMS server, SEMS will require a boot password change.

The enable process involves an exchange of information between the WorkSafe Pro user and the SEMS administrator to authenticate the user and the drive for security reasons. The steps in this section describe the user procedure.

> **Important:** Enable codes are valid only *within the same hour on the clock during which they are generated* at the SEMS console. For example, an enable code generated at 3:04 PM must be entered into the SEMS WTG Enable utility within 56 minutes before it expires at 4:00 PM, but an enable code generated at 3:52 PM expires in 8 minutes at 4:00 PM.

To ensure that the task is completed within the time limit, ensure that both the SEMS administrator and the WorkSafe Pro user are ready and in communication.

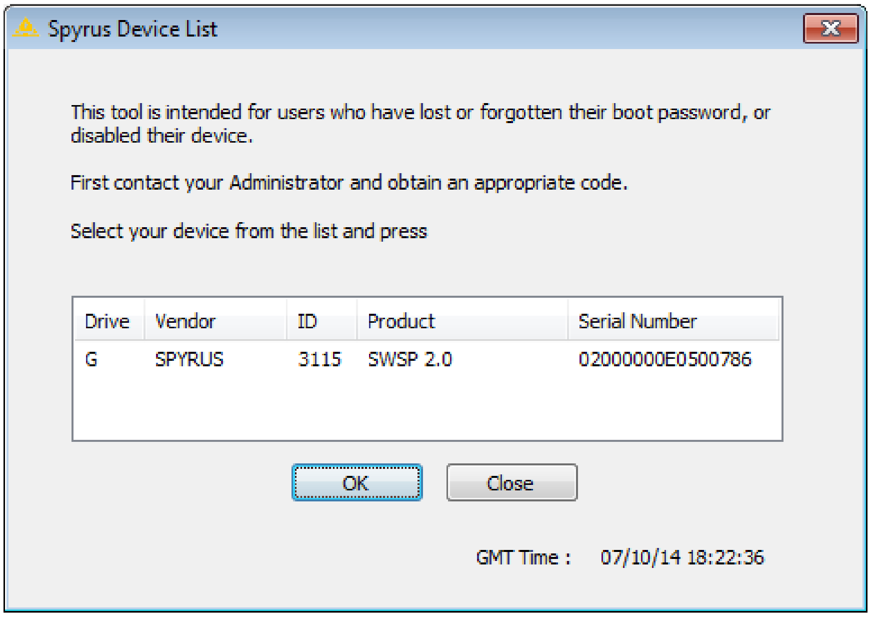
You need your WorkSafe Pro and a computer running Windows 7 or Windows 8 to enable the drive. The computer does *not* need to be connected to a network with access to the SEMS server, and your Windows account does *not* need Administrator permissions.

To enable a disabled SEMS-managed WorkSafe Pro drive, do the following:

1. Using the method preferred by your organization, contact the SEMS administrator to request an Enable Authorization Code. If the SEMS administrator asks, provide the serial number of the WorkSafe Pro drive (see step 7 of this procedure for the serial number if it is not on a label on the drive). If you do not know how to contact the SEMS administrator, click the Code button in step 7 of this procedure.
2. Insert the WorkSafe Pro drive into a USB port connected to a computer certified for use and running Windows 7 or Windows 8.
3. In Windows Explorer, select the lettered WorkSafe Pro drive (it is labeled *WSPBOOT* by default).

   Note: If the WorkSafe Pro drive does not appear in Windows Explorer, an administrator may need to assign a drive letter manually.
4. Open the *Utils* folder on the WorkSafe Pro drive.
5. From the *Utils* folder, copy the SEMSforWTG Enable folder to the hard drive of the computer.
6. Double-click the file ***SEMSforWTGEnable.exe*** to start the SEMS WTG Enable utility.
7. In the SEMS WTG Enable utility, on the SPYRUS Device List page, select your WorkSafe Pro from the list, and then click **OK**.

   If you need the serial number of the drive, look in the Serial Number column on this page.



This tool is intended for users who have lost or forgotten their boot password, or disabled their device.

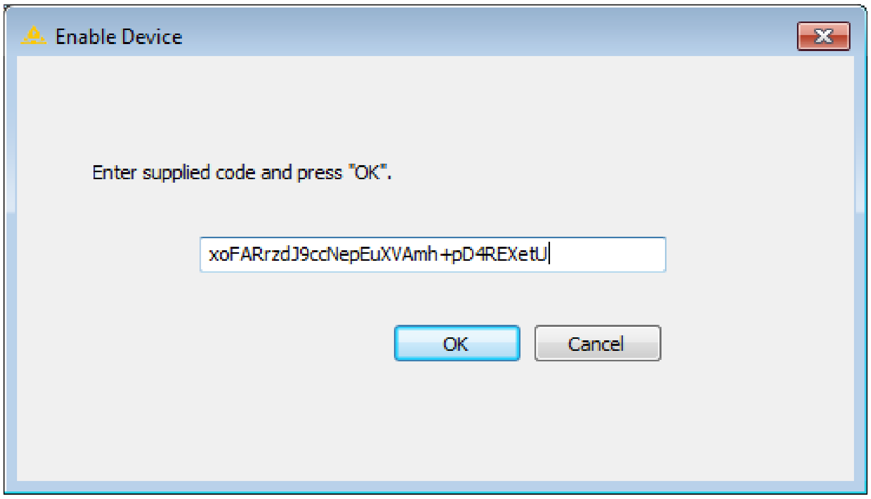
First contact your Administrator and obtain an appropriate code.

Select your device from the list and press

Drive	Vendor	ID	Product	Serial Number
G	SPYRUS	3115	SWSP 2.0	02000000E0500786

GMT Time : 07/10/14 18:22:36

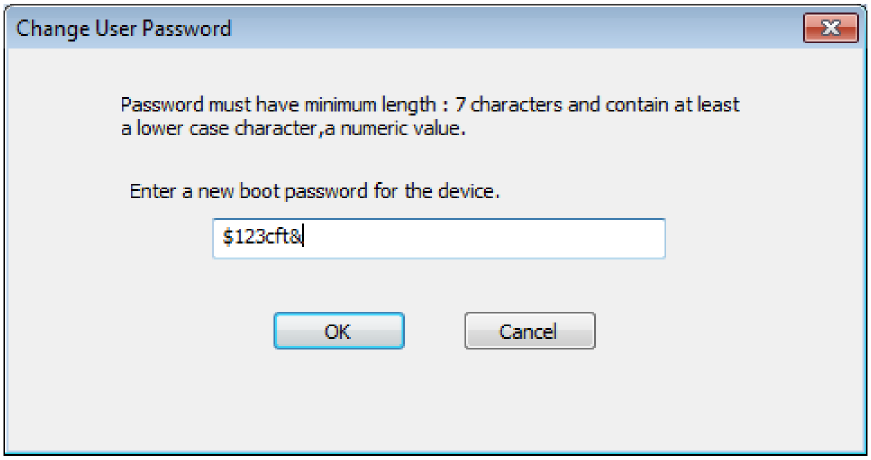
8. In the SEMS WTG Enable utility, on the Enable Device page, enter the enable code, and then click **OK**.



Enter supplied code and press "OK".

xoFARrzdJ9ccNepEuXVAmh+pD4RExetU

9. In the SEMS WTG Enable utility, on the Change User Password page, enter a new WorkSafe Pro boot password, and then click **OK**.



Password must have minimum length : 7 characters and contain at least a lower case character,a numeric value.

Enter a new boot password for the device.

$123cft&

10. When you see the SEMSforWTGEnable dialog box, click **OK**.

(SEMS Only) Recover Forgotten Boot Password

If the boot password for a WorkSafe Pro drive is lost or forgotten, and the drive is registered with SEMS, the boot password can be recovered from the SEMS database by using the SEMS WTG Enable utility.

> **Important:** The drive must have a SEMS policy that stores the boot password. If the policy does not store the boot password (default policy does NOT store the boot password), recovery is not possible.
>
> **Note:** When next you boot the WorkSafe Pro drive with the recovered boot password, on a computer connected to a network with access to the SEMS server, SEMS will require a boot password change.

The recovery process involves an exchange of information between the WorkSafe Pro user and the SEMS administrator to authenticate the user and the drive for security reasons. The steps in this section describe the user procedure.

> **Important:** Password recovery codes are valid only *within the same hour on the clock during which they are generated* at the SEMS console. For example, a recovery code generated at 3:04 PM must be entered into the Display Recovered Password Tool within 56 minutes before it expires at 4:00 PM, but a recovery code generated at 3:52 PM expires in 8 minutes at 4:00 PM.

To ensure that the task is completed within the time limit, ensure that both the SEMS administrator and the WorkSafe Pro user are ready and in communication.

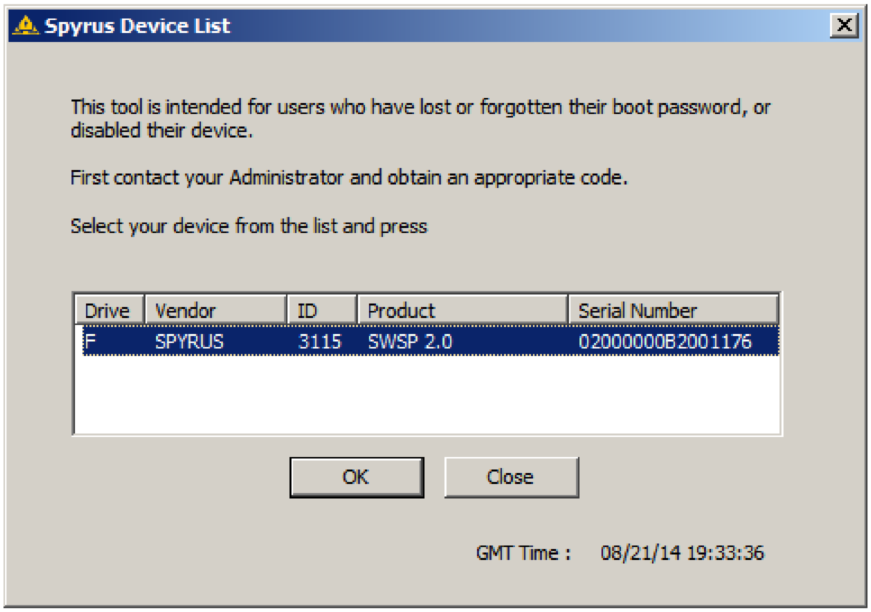
You need your WorkSafe Pro and a computer running Windows 7 or Windows 8 to recover the boot password. The computer does *not* need to be connected to a network with access to the SEMS server, and your Windows account does *not* need Administrator permissions.

To recover a SEMS-registered WorkSafe Pro boot password, do the following:

1. Insert the WorkSafe Pro drive into a USB port connected to a computer certified for use and running Windows 7 or Windows 8.
2. In Windows Explorer, select the lettered WorkSafe Pro drive (it is labeled *WSPBOOT* by default).

   Note: If the WorkSafe Pro drive does not appear in Windows Explorer, an administrator may need to assign a drive letter manually.
3. Open the *Utils* folder on the WorkSafe Pro drive.
4. From the *Utils* folder, copy the SEMSforWTG Enable folder to the hard drive of the computer.
5. Double-click the file ***SEMSforWTGEnable.exe*** to start the SEMS WTG Enable utility.
6. In the SEMS WTG Enable utility, on the SPYRUS Device List page, select your WorkSafe Pro from the list, and then click **OK**.

   Note: If the serial number is not available from the label on the WorkSafe Pro, it is displayed in the SEMS WTG Enable utility.



This tool is intended for users who have lost or forgotten their boot password, or disabled their device.

First contact your Administrator and obtain an appropriate code.

Select your device from the list and press

Drive	Vendor	ID	Product	Serial Number
F	SPYRUS	3115	SWSP 2.0	02000000B2001176

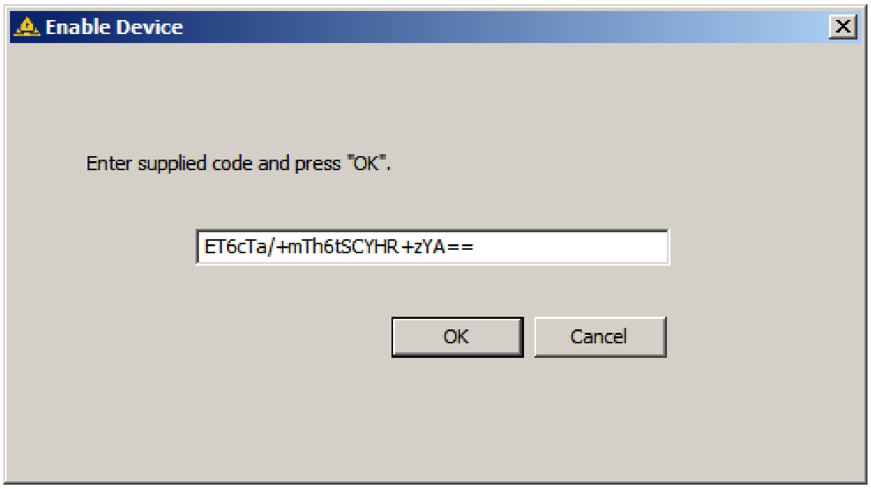
GMT Time : 08/21/14 19:33:36

7. Use the method of transmission approved by your organization to transmit the WorkSafe Pro serial number to the SEMS administrator. The SEMS administrator uses the serial number to generate a Password Recovery Code Value that you will use to recover the boot password in the following step.

8. Obtain the Password Recovery Code Value and the expiration time from the SEMS administrator.

   Important: You must enter the Password Recovery Code Value into the Display Recovered Password Tool and retrieve the password before the Password Recovery Code Value expires. If the Password Recovery Code Value expires, the SEMS administrator must generate a new Password Recovery Code Value.

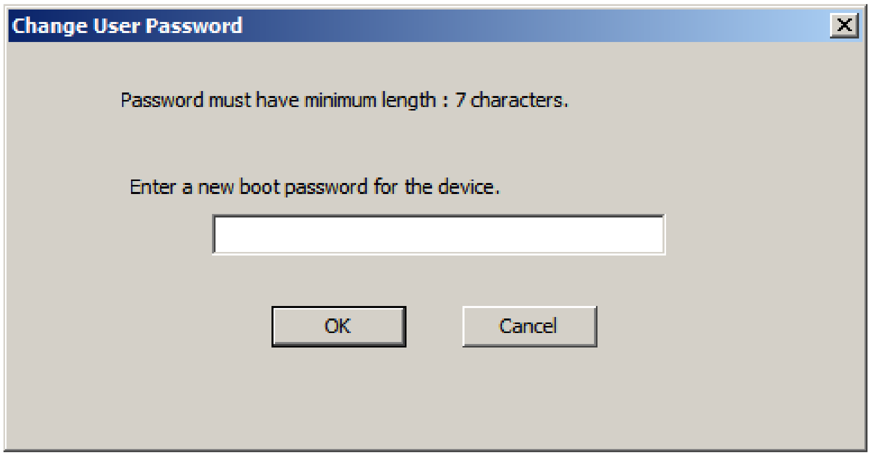
9. In the SEMS WTG Enable utility, on the Enable Device page, enter the Password Recovery Code Value, and then click **OK**.



Enter supplied code and press "OK".

ET6cTa/+mTh6tSCYHR+zYA==

10. In the SEMS WTG Enable utility, on the Change User Password page, enter a new WorkSafe Pro boot password, and then click **OK**.



Change User Password

Password must have minimum length : 7 characters.

Enter a new boot password for the device.

11. When you see the SEMSforWTGEnable dialog box, click **OK**.

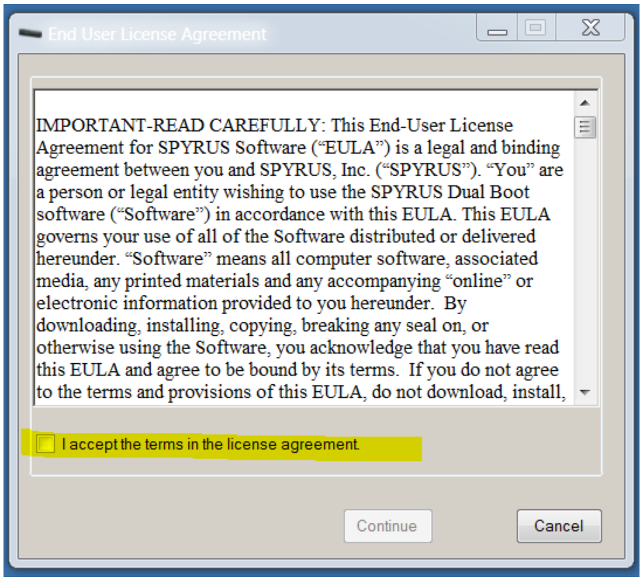
Using the Dual Boot Application

The SPYRUS Dual boot application lets users set up an additional boot menu entry on their Windows host systems to allow easy USB boot from a SPYRUS Windows To Go drive. When the dual boot application is installed onto your host machine hard drive's Windows operating system, an additional Windows System startup option named "Boot Windows To-Go" is created. Once installed, every time the host machine boots up one can choose to boot either from the host hard drive operating systems or the Windows To Go drive. This application is intended to facilitate USB boot on older BIOS based host machines without requiring the user to change BIOS settings. It is NOT supported on the newer UEFI firmware-based host computers. Use the table below as a quick reference to determine dual boot support for your host OS and hardware combination.

	Encrypted WTG drives	Non-Encrypting WTG drives	Notes
UEFI host PC firmware	Not supported. You will need to change the host firmware settings to enable WTG boot.	Dual boot is not supported. Instead use native Windows To Go startup options in Windows8/8.1 host operating systems to set up WTG boot. All others will require host firmware settings to be modified to enable WTG boot.	
BIOS PC firmware	Dual boot supported	Dual boot supported	The BIOS firmware must have USB disk support.

To install the Dual boot application on your host machine's Windows operating system, do the following:

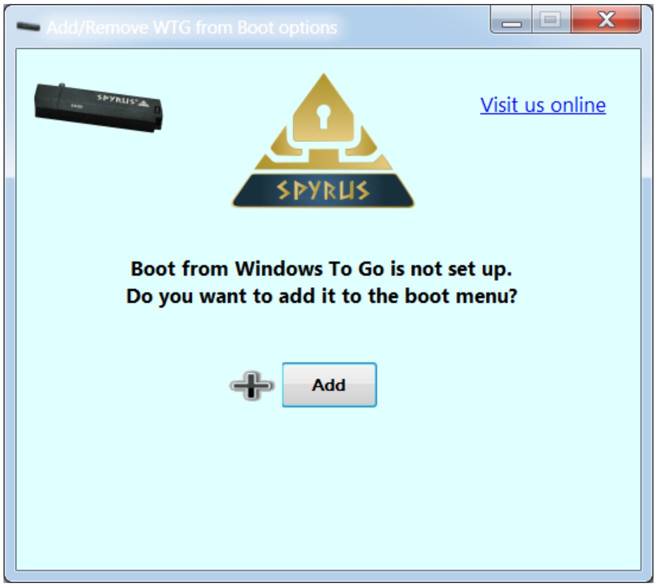
1. Boot into your host machine's Windows operating system.
2. If you are on a Windows 8 or newer host operating system double click on the **ManageWTGBootOptions.exe**. On Windows 7 and older operating systems click on the **ManageWTGBootOptions_XP_Win7.exe**. You must be logged into an account with Administrator privileges to install the dual boot application.
3. Click on the **check box** to accept the End User license agreement then click **Continue**.



IMPORTANT-READ CAREFULLY: This End-User License Agreement for SPYRUS Software ("EULA") is a legal and binding agreement between you and SPYRUS, Inc. ("SPYRUS"). "You" are a person or legal entity wishing to use the SPYRUS Dual Boot software ("Software") in accordance with this EULA. This EULA governs your use of all of the Software distributed or delivered hereunder. "Software" means all computer software, associated media, any printed materials and any accompanying "online" or electronic information provided to you hereunder. By downloading, installing, copying, breaking any seal on, or otherwise using the Software, you acknowledge that you have read this EULA and agree to be bound by its terms. If you do not agree to the terms and provisions of this EULA, do not download, install,

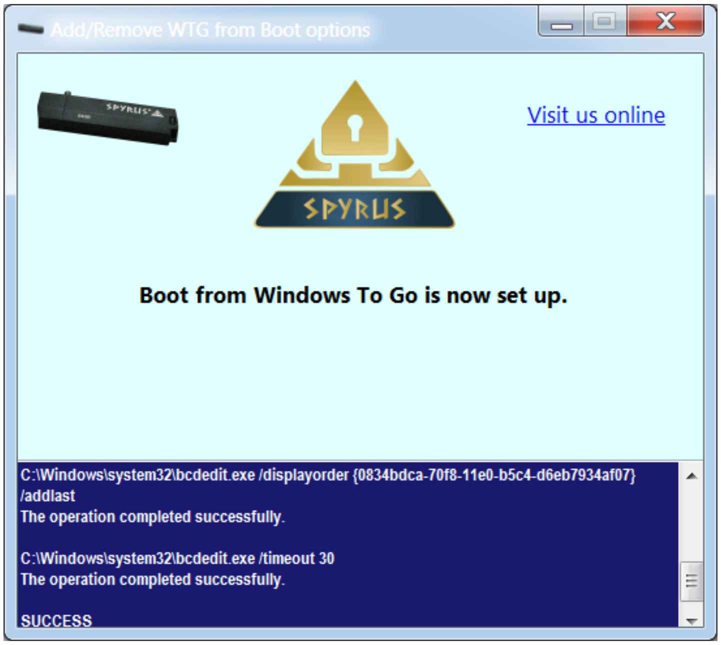
□ I accept the terms in the license agreement

4. Click **Add** to insert the Windows To Go boot menu option.



Boot from Windows To Go is not set up.
Do you want to add it to the boot menu?

Wait until the files are finished copying.

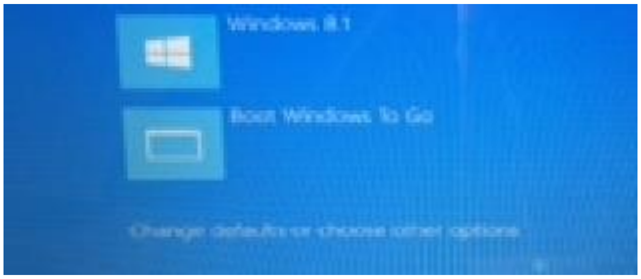


Boot from Windows To Go is now set up.

```
C:\Windows\system32\bcdedit.exe /displayorder {0834bdca-70f8-11e0-b5c4-d6eb7934af07}
/addlast
The operation completed successfully.

C:\Windows\system32\bcdedit.exe /timeout 30
The operation completed successfully.

SUCCESS
```

Close the Window. The Windows To Go boot option is now set up.

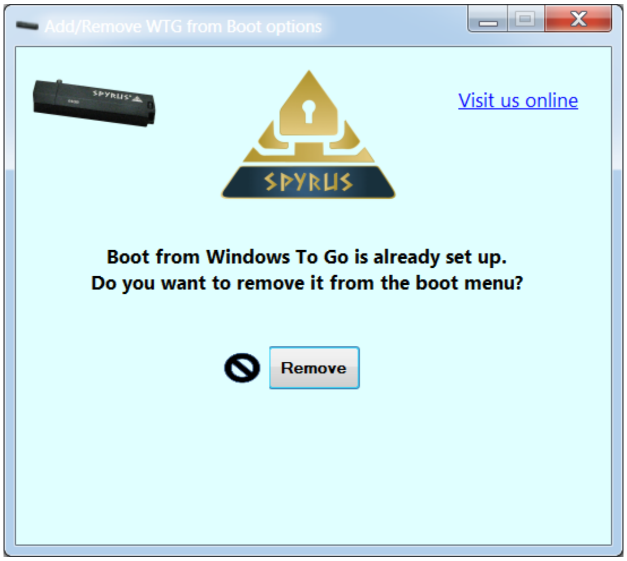
The next time you reboot your machine, you will see an additional boot option like the following:



To boot the Windows To Go drive, insert the SPYRUS Windows To Go drive, the select the Boot Windows To Go option. The system will quickly restart and scan inserted SPYRUS drives. It will search for Encrypted drives first followed by a search for non-encrypting drives. If one is found boot up will continue and boot the inserted drive.

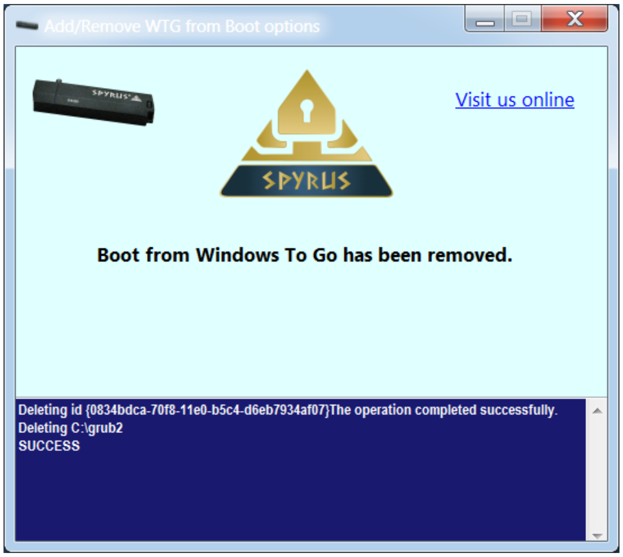
To remove the Dual boot application and the Boot Windows To Go option from your host machine's Windows operating system do the following:

1. Boot into your host machine's Windows operating system.
2. Double click on the **ManageWTGBootOptions.exe** that was copied to the Desktop during install. You can also launch this executable from the original package location.
3. Click **Remove**.



Boot from Windows To Go is already set up.
Do you want to remove it from the boot menu?

4. Wait until removal is complete.



Boot from Windows To Go has been removed.

```
Deleting id {0834bdca-70f8-11e0-b5c4-d6eb7934af07}The operation completed successfully.
Deleting C:\grub2
SUCCESS
```

Using the Rosetta Smart Card

The embedded Rosetta Smart Card on your WorkSafe Pro drive secures your digital certificates and works just like any smart card. Because the Rosetta Smart Card is embedded within the WorkSafe Pro drive, you do not need a separate reader. When the WorkSafe Pro drive is booted, you can access the Rosetta Smart Card just as you would any smart card connected to your computer.

You can also use the WorkSafe Pro drive as a readerless smart card when it is *not* booted by connecting it to a Windows computer where Smart Card Service is enabled.

Before using the Rosetta Smart Card, ensure that the following requirements are met:

- When accessing the smart card on a booted WorkSafe Pro, the Rosetta Minidriver must be installed on the WorkSafe Pro drive. (Read Only mode must be disabled, and automatic Windows Update must be enabled to install the Rosetta Minidriver.) This will be done automatically when the booted WorkSafe Pro has a connection to the internet.

- When used on an unbooted WorkSafe Pro as a smart card, Smart Card Service must be enabled (enabled by default in Windows 7 and Windows 8/8.1) on Windows computers where you use the Rosetta Smart Card. If you have disabled Smart Card Service, restart it before using the Rosetta Smart Card on the computer.

To access the Rosetta Smart Card when the WorkSafe Pro drive is *not* booted, do the following:

1. Insert the WorkSafe Pro drive into a USB port connected to a computer certified for use with Windows 7 or Windows 8.

2. The Rosetta Smart Card will be recognized by plug-N-play and will automatically come on line.

3. In Windows Explorer, select the lettered WorkSafe Pro drive (it is labeled *WSPBOOT* by default).

   Note: If the WorkSafe Pro drive does not appear in Windows Explorer, an administrator may need to assign a drive letter manually.

4. Open the *Utils/Minidriver_V6_SpyrusFRC_Utilities* folder on the WorkSafe Pro drive to access the Minidriver Admin Tool and Token Utility (if they have been made available).

If your organization policy permits you to manage the Rosetta Smart Card and your certificates on it, you will be provided with the Rosetta Minidriver Tools (the Rosetta Minidriver Admin Tool and the Rosetta Minidriver Token Utility) and user documentation for them.

Use the Rosetta Minidriver Admin Tool to:

- Verify that the Rosetta Minidriver is installed
- Initialize the Rosetta Smart Card
- Change the Admin Key (password required to reset blocked or forgotten User PIN)
- Reset blocked or forgotten Rosetta Smart Card User PIN

See the *Rosetta Minidriver Admin Tool User Guide* for more information.

Use the Rosetta Minidriver Token Utility to:

- View certificates on the Rosetta Smart Card
- Register certificates with the Microsoft certificate store

- Delete certificates from the Rosetta Smart Card
- Import certificates to the Rosetta Smart Card
- Change the Rosetta Smart Card User PIN
- Reset blocked or forgotten Rosetta Smart Card User PIN

See the *Rosetta Minidriver Token Utility User Guide* for more information.

Tips for Booting from a USB Drive

The procedure to boot a WorkSafe Pro drive can differ between operating systems and even between various devices running the same operating system. Although no single resource can cover every difference, this section explains the basic concepts and procedures for booting a WorkSafe Pro drive.

Boot WorkSafe Pro on Windows Computers

SPYRUS recommends that you configure the host computer to always boot from a USB drive when one is present.

Important: If the host computer has BitLocker enabled, suspend BitLocker before changing the BIOS/UEFI settings. Resume BitLocker only after changing the BIOS/UEFI settings. If BitLocker is not suspended first, the next time the computer is started it will boot into Recovery mode.

To configure a Windows 8 or 8.1 computer to always boot a WorkSafe Pro or other bootable USB drive when present, in Windows 8/8.1, press **Windows logo key + W**, search Settings for "Windows to Go startup options," and then press **Enter**. Select **Yes**, and then click **Save Changes**.

On a Windows 7 computer, see your computer documentation for the procedure to configure it to always boot from a USB drive if one is present (the procedure varies depending on the manufacturer).

Windows 7 or Windows 8/8.1 computers that are not configured to always boot from a USB drive can follow a procedure at startup to manually boot the computer from a USB drive. The most common procedure is to press a function key before the operating system begins loading, and then select **USB Device**. This procedure also varies depending on manufacturer, so consult your computer documentation.

Boot WorkSafe Pro on Macintosh Computers

WorkSafe Pro drives that have been set up with Boot Camp support can be booted on many Macintosh computers. See the Apple list (http://support.apple.com/kb/HT5628) of Macs that support booting on Windows 8 or 8.1.

Macs on the list must also be running OS X 10.6 or higher, have the latest Apple OS updates applied, and have a USB 2.0 or USB 3.0 port or a powered USB hub connected to the computer.

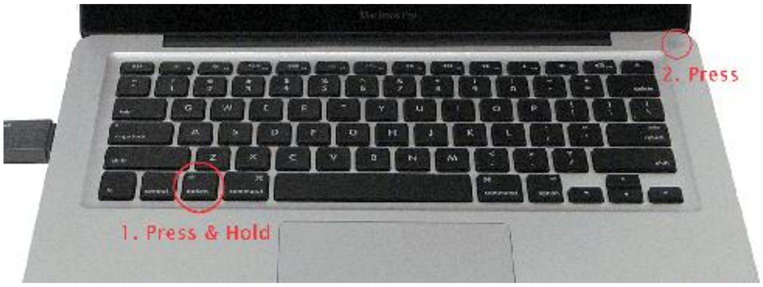
Apple Macintosh computers cannot be configured to always boot from a USB.

To boot a WorkSafe Pro drive on a Mac, do the following:

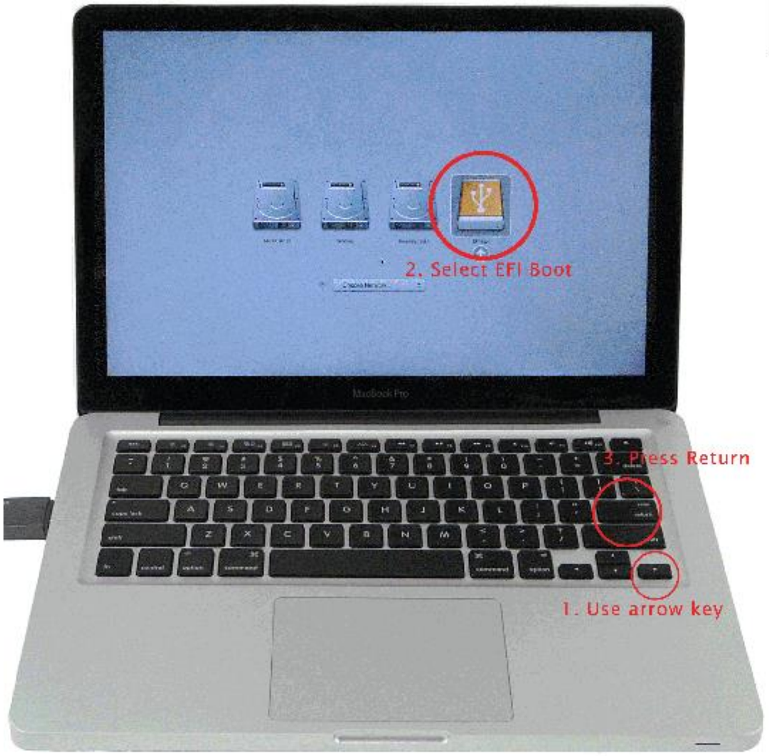
1. Hold down the **Option/Alt** key and then start the computer. Keep holding **Option/Alt** until the startup drive options appear.
2. Use the arrow keys to select the drive labeled **EFI** or **EFI Boot** from the startup drive options.
3. Press **Return**.
4. When the WorkSafe Pro drive boots, type the boot password, and then log on to Windows 8.1.

   Important: If you see an error message headed "Recovery" stating that your PC needs to be repaired, try the following procedure. Your Mac and WTG drive are unharmed; this error occurs in the presence of certain hardware, such as older MacBook Pro computers.
5. Insert the WorkSafe Pro drive into a USB port connected to your Mac.
6. Shut down the Mac if it is not already shut down.

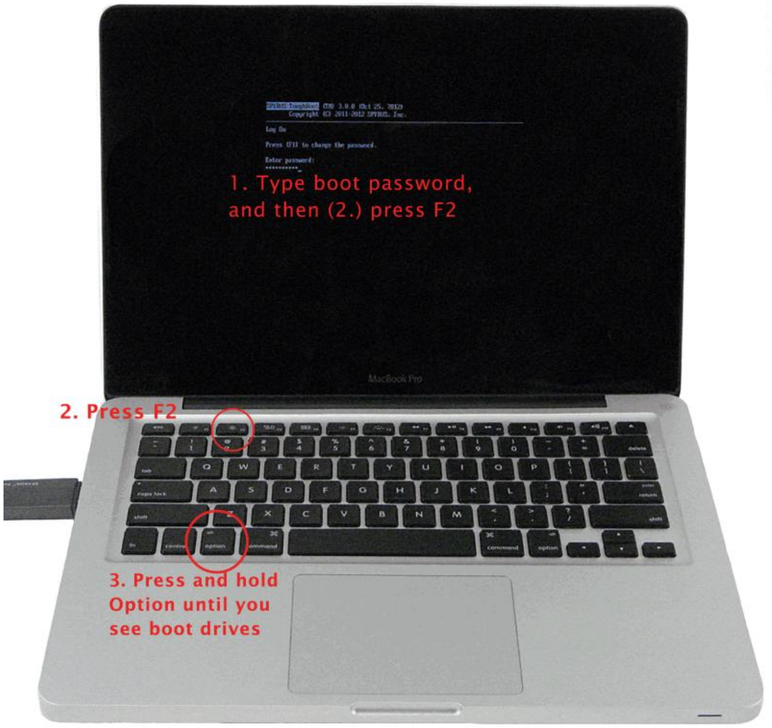
7. Hold down the **Option/Alt** key and then press the Power button to start the Mac. Keep holding **Option/Alt** until the startup drive options appear on the screen.



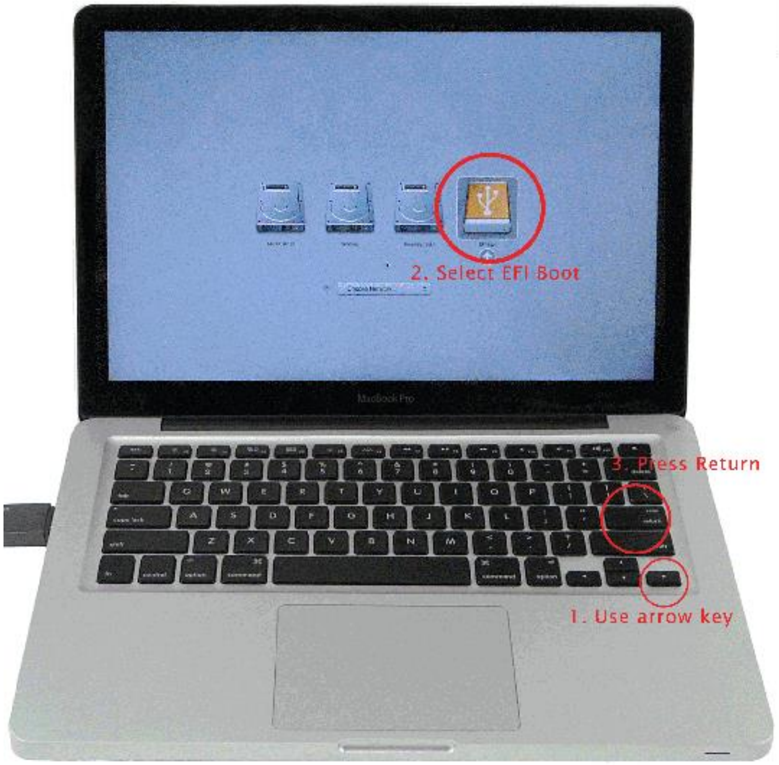
8. Use the arrow keys to select the drive labeled **EFI** or **EFI Boot**. Press **Return**.



9. When prompted by Toughboot boot loader, type the WorkSafe Pro boot password, press **F2**, and then *immediately* press and hold down the **Option/Alt** key. Keep holding **Option/Alt** until the startup drive options appear.



10. Use the arrow keys to select the drive labeled **EFI** or **EFI Boot**. Press **Return**



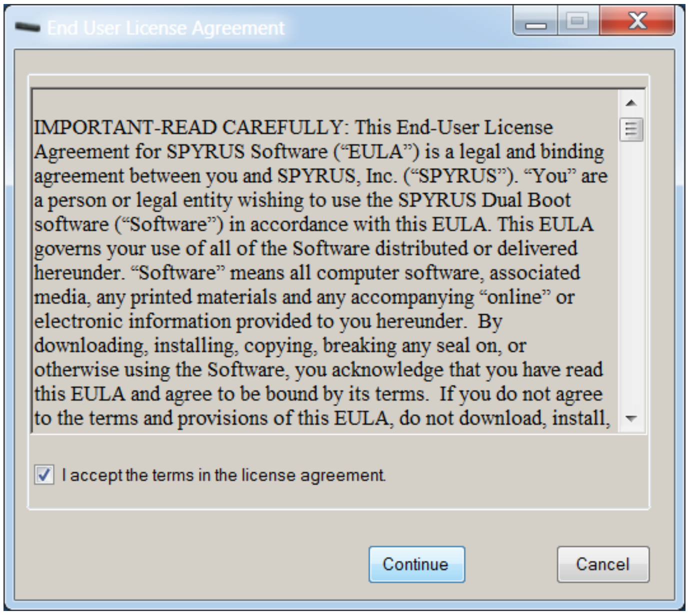
11. When Windows 8 starts, log on to your Windows account.

Adding WindowsToGo Boot Menu Option on an Already Booted Windows Host Computer

Note: This feature is not supported on all WTG drive types and host systems. See compatibility matrix at the end of this section.

To set up a WindowsToGo boot menu option on an already booted Windows host, do the following:

1. Login to a user account with Administrative privileges.
2. Locate the WTGDualBootInstall folder on the install media. (Install media might be in the Utils subfolder of a provisioned WSP/SPW drive or supplied as a standalone application install package)
3. Double click on the **ManageWTGBootOptions.exe** if you are on a Windows 8/8.1 or newer host operating system platform OR **ManageWTGBootOptions_XP_Win7.exe** for older operating systems.

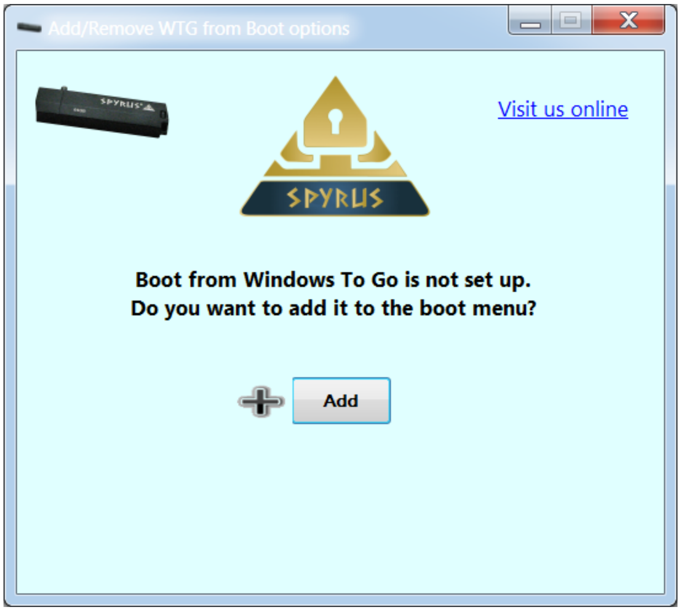


End User License Agreement

IMPORTANT-READ CAREFULLY: This End-User License Agreement for SPYRUS Software (“EULA”) is a legal and binding agreement between you and SPYRUS, Inc. (“SPYRUS”). “You” are a person or legal entity wishing to use the SPYRUS Dual Boot software (“Software”) in accordance with this EULA. This EULA governs your use of all of the Software distributed or delivered hereunder. “Software” means all computer software, associated media, any printed materials and any accompanying “online” or electronic information provided to you hereunder. By downloading, installing, copying, breaking any seal on, or otherwise using the Software, you acknowledge that you have read this EULA and agree to be bound by its terms. If you do not agree to the terms and provisions of this EULA, do not download, install,

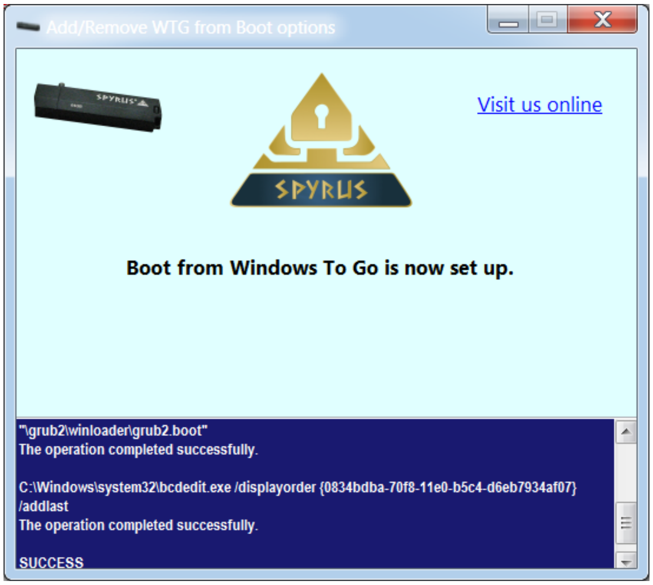
☑ I accept the terms in the license agreement

4. Read the license agreement, click on **I accept** and then click **Continue**. The next screen lets you add the new boot option.



Boot from Windows To Go is not set up.
Do you want to add it to the boot menu?

5. Click **Add**.



Boot from Windows To Go is now set up.

```
"\grub2\winloader\grub2.boot"
The operation completed successfully.

C:\Windows\system32\bcdedit.exe /displayorder {0834bdba-70f8-11e0-b5c4-d6eb7934af07}
/addlast
The operation completed successfully.

SUCCESS
```

6. When the install completes successfully, close the application window. You will now have a ManageWTGBootOptions executable on the user desktop.

The next time you reboot Windows, you will see an additional boot menu option named "Boot Windows To Go." If you select this option during the boot process, the computer will reboot and search for a SPYRUS WTG drive to boot. If one is found the computer will then boot from the WTG drive.

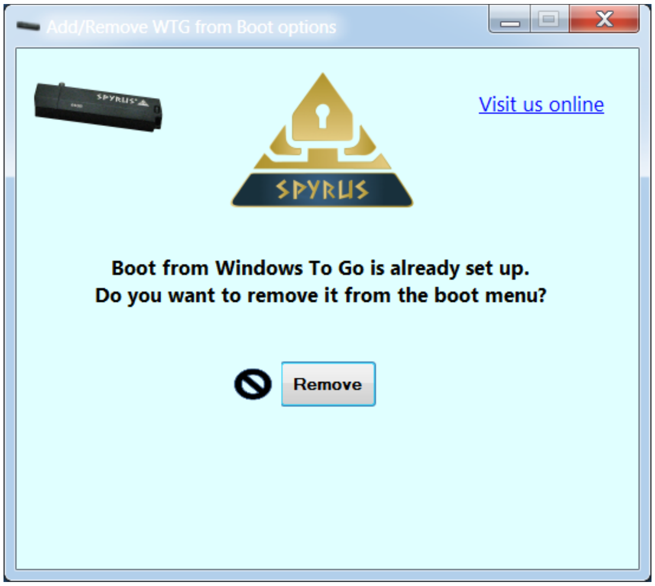
BOOT option setup Compatibility Matrix

SPYRUS WTG Drive	Host PC firmware type		
	EFI	BIOS	Comment
WorkSafe	✓	✓	
Portable Workplace	✓	✓	
WorkSafe Pro	✗	✓	*You need to change PC EFI firmware settings to boot from a WSP WTG drive.*
Secure Portable Workplace	✗	✓	*You need to change PC EFI firmware settings to boot from a SPW WTG drive.*

Removing WindowsToGo Boot Menu Option from a Booted Windows Host Computer

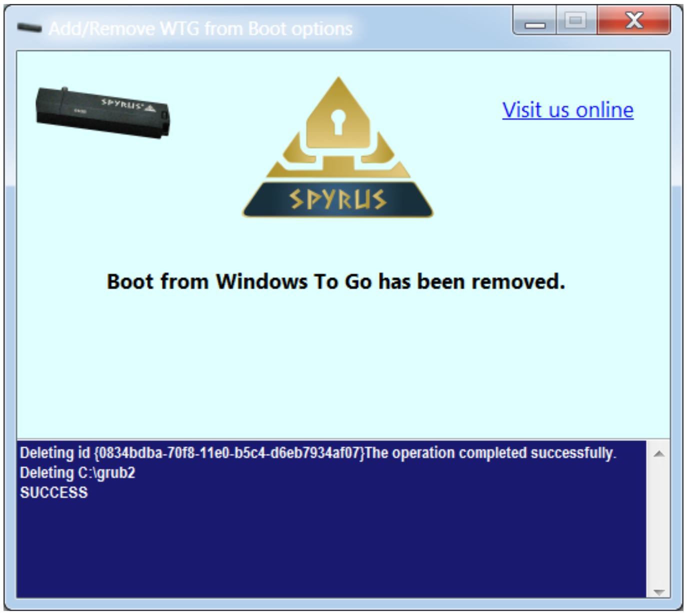
To remove a previously set up WindowsToGo boot menu option on an already booted Windows host, do the following:

1. Login to a user account with Administrative privileges.
2. Locate the ManageWTGBootOptions executable that was copied to the user desktop during installation.
3. Double click on the **ManageWTGBootOptions.exe** if you are on a Windows 8/8.1 or newer host operating system platform OR **ManageWTGBootOptions_XP_Win7.exe** for older operating systems.



Boot from Windows To Go is already set up.
Do you want to remove it from the boot menu?

4. Click **Remove**.



Boot from Windows To Go has been removed.

```
Deleting id {0834bdba-70f8-11e0-b5c4-d6eb7934af07}The operation completed successfully.
Deleting C:\grub2
SUCCESS
```

5. When removal is complete close the application window. You will no longer have a Boot From WindowsToGo boot menu option when you restart windows and the ManageWTGBootOptions executable will be deleted from the user desktop.