bsi.

...making excellence a habit.™

Microsoft Surface Tablet

Security configuration and auditing guide

Contents

Document control information

Document reference	Property
Title	Microsoft surface security configuration and auditing guide
Author	Daniel Compton
Version	1.0
Date	25/04/2016

The following document covers security options and audit techniques that can be used for assessing the configuration of a Microsoft Surface Tablet device.

All recommendations should be carried out on test devices before being applied to production devices.

Physical security

UEFI settings

What is UEFI?

The UEFI (Unified Extensible Firmware Interface) is very much like the traditional BIOS (Basic Input Output System) used for early personal computers. These control basic settings for the system such as hard disk settings, peripheral port settings, boot order of devices and power on passwords. The Microsoft Surface tablet range uses UEFI to control boot options and peripheral settings similar to what you would expect on a standard PC.

The UEFI settings and options varies depending on the Surface model, the newer pro models allow more control of the tablet settings.

Why are these settings important?

As will be shown within this paper, if these settings are insecurely configured it can result in the tablet device becoming compromised, potentially bypassing the Windows password completely.

UEFI Setup

There are two different methods to enter the UEFI firmware on the Surface tablets, either by using a button sequence at power on or by instructing Windows to enter UEFI on restart.

Button sequence method:

Step 1: Shut down the Surface tablet.

Step 2: Press and hold the volume-up button on your Surface and at the same time, press and release the power button.

Step 3: When you see the Surface logo, release the volume-up button.

The UEFI menu will be displayed within a few seconds.

Note: The power and volume locations vary between Surface tablet models. The above is a Surface Pro 3.

Software method

Step 1: Select Start, Settings

Step 2: Select Update and Security

Step 3: Select Recovery

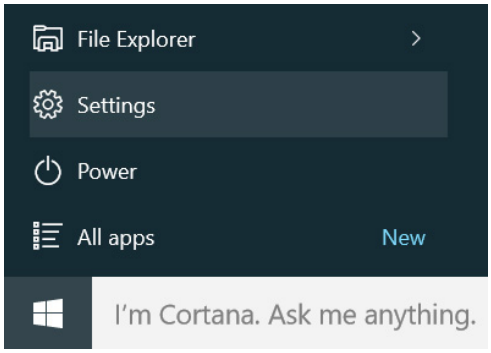
Step 4: Under the Advanced Start-up heading, select Restart now

Step 5: Select Troubleshoot

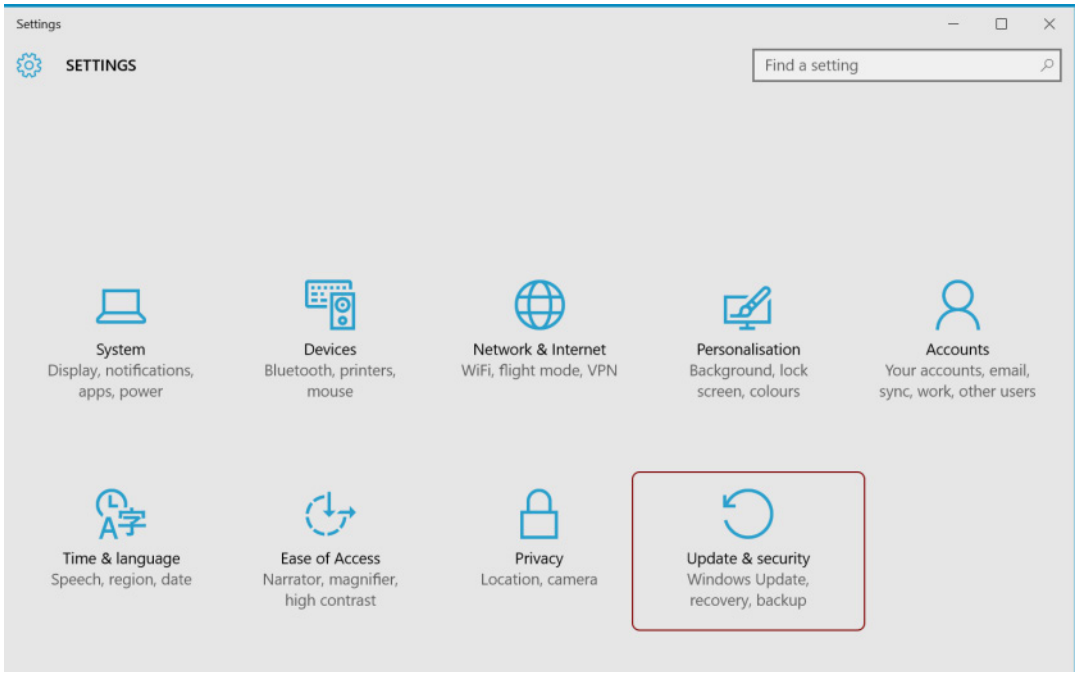
Step 6: Select Advanced options

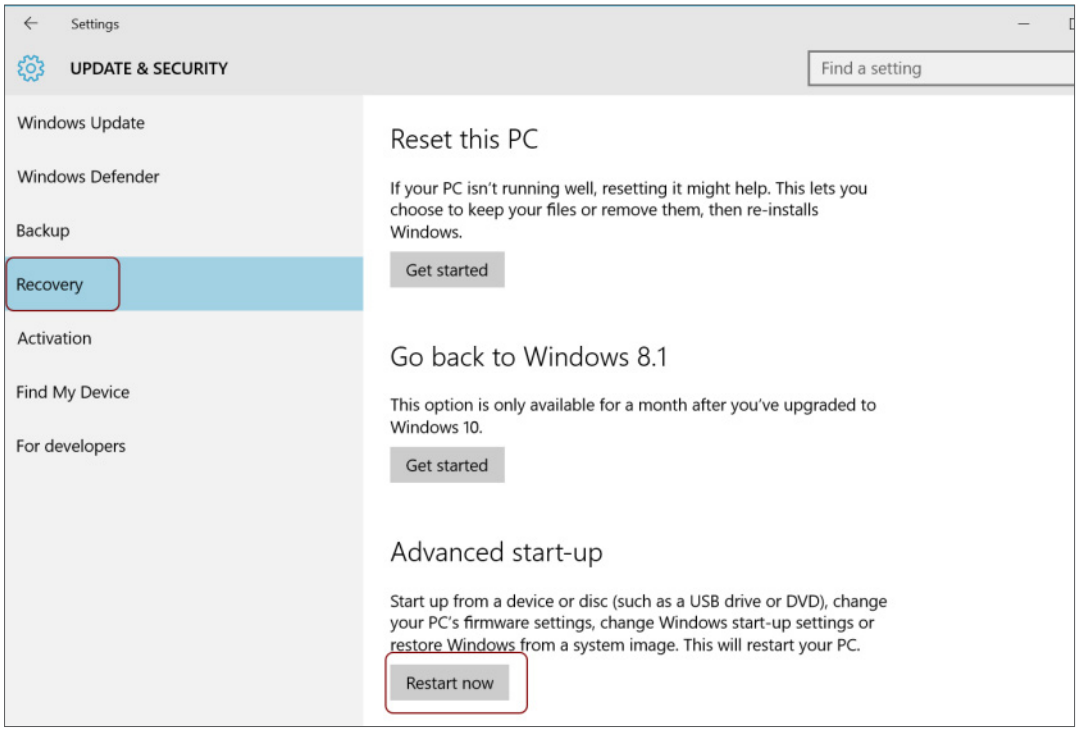
Step 7: Select UEFI Firmware Settings

Step 8: Select Restart

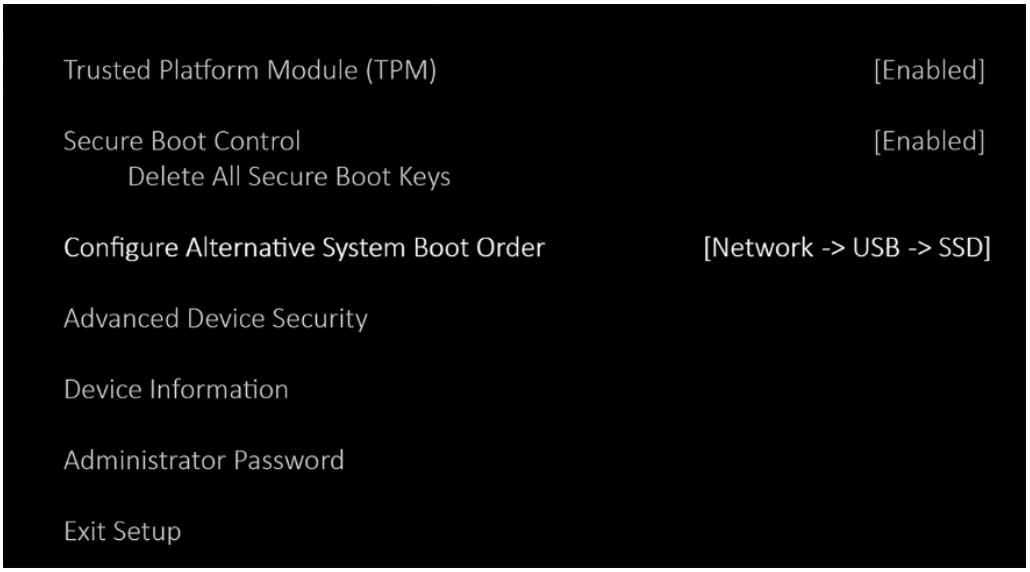


Note: The UEFI options vary between models. The below is using a Surface Pro 3.





The UEFI setup will then be shown.



Note: The UEFI options vary between models. The above is using a Surface Pro 3.

UEFI Options

The configuration options allowed within the UEFI varies between the different Surface tablet models. Some models such as the Pro 3 allow very granular options to be set, such as the disabling of USB booting, or UEFI password protection. Earlier models do not all have this option, therefore these cannot be secured to the same level.

The following table lists the UEFI security options of interest on various models of the Surface:

Feature	Surface Pro	Surface Pro 2	Surface 3	Surface Pro 3
Trusted Platform Module (TPM)	✔	✔	✔	
Secure Boot Control	✔	✔	✔	✔
Delete All Secure Boot keys	✔	✔	✔	✔
Install Default Secure Boot Keys	✔	✔	✔	✔
Configure Alternate System Boot Order	✖	✖	✔	✔
Advanced Device Security	✖	✖	✔	✔
Administrator Password	✖	✖	✔	✔

Note: The new Surface Pro 4 and Surface Book use a new Surface UEFI version that does include security options, however these are in a different format to the above but should allow similar controls for boot order and passwords.

Below is a summary of each UEFI option and the potential risks from a security aspect.

Trusted Platform Module (TPM)

The TPM is a hardware based cryptography chip used to work with disk encryption products to protect the keys and provide integrity to the hard disk boot image. The TPM encrypts, stores and decrypts the disk encryption keys.

Secure boot control

Secure Boot Control ensures that the device is booted using only software that is trusted by the device or manufacturer. Signatures are checked by the UEFI and if the signatures matched and are trusted, the UEFI then instructs the operating system to boot. For signatures that do not match when Secure Boot Control is enabled this could result in the operating system not booting.

To use an alternative operating system on the Surface tablets other than Microsoft products, the Secure Boot Control needs to be disabled. For instance if you wanted to install or boot from a Linux distribution, with Secure Boot Enabled it would prevent this working.

Example

The example right shows the Surface tablet with the secure boot option disabled. The Surface display icon screen will show red at power on to indicate that secure boot is disabled or the secure boot keys have been altered or deleted.

Delete all secure boot keys

This option deletes all installed Secure Boot keys including those originally installed with Windows.

Install default secure boot keys

This option reinstalled all of the Secure Boot keys that were originally installed with Windows only.

Configure alternate system boot order

This allows the order of devices to be checked for bootable media at power on. The following boot order options exist:

p p a = l å ä ó =
k É í ï ç ê â = J [= r p _ = J [= p p a = r p _ = J [=
k É í ï ç ê â = J [= p p a = k É í ï ç ê â = J [= p p a

Risk

Booting USB media before the SSD drive allows an alternative operating system to be used, which could allow the device to be used in a non-intended manner. If the device is not encrypted it would allow access to any locally stored data, password hashes and allow the local Windows password to be bypassed. If a UEFI bootable USB device is connected at power on, the USB device will be read automatically before the SSD where Windows is installed.

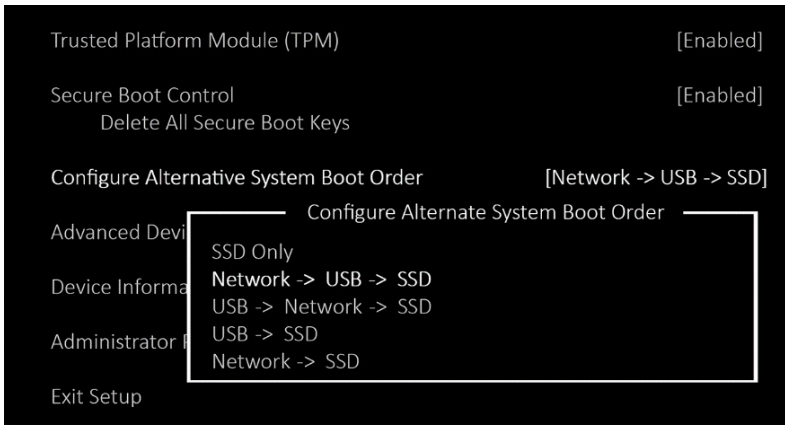
Recommendation

Configure to boot from "SSD Only". This does not 100% prevent USB from being bootable, see Advanced Device Security USB options.

Example

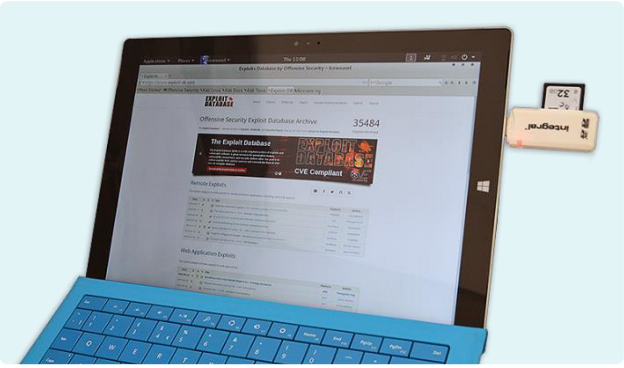
The following examples show the UEFI boot order options and associated risks.

This means at power on the device will check the network, then any USB media before attempting to boot from the SSD drive.



The example right shows a Surface Pro 3 booted from Kali2 Linux security testing distribution from the USB port. This could be used to launch an attack on the associated network, read data from the local hard disk (if not encrypted) or potentially bypass Internet browsing restrictions.

The above is browsing an exploit website that is typically blocked by corporate proxy server filter lists.



For information on how to make the Kali2 bootable for UEFI refer to Appendix A. Some tools exists that already come with UEFI bootable support.

The Enterprise version of PC Unlocker, automatically supports UEFI boot. This program easily allows you to boot a Surface tablet. Providing the Surface tablet does not have full disk encryption enabled, it will automatically obtain the Windows SAM file that contains the local user accounts and passwords.

It will also allow any password to be reset or bypassed, allowing the Windows operating system to be unlocked.

A Windows command prompt can be also launched and if not disk encryption is in use, it will allow access to the file system.

Advanced device security

This allows peripheral ports or features to be enabled or disabled. The following options exist.

k É í ï ç ê â = _ ç ç í =
p á Ç É = r p _ =
c ê ç å í = ` ~ ã É ê ~ =
o É ~ ê = ` ~ ã É ê ~ =
l å = ç ~ ê Ç ≙ ì Ç á ç ã á Å ê ç p a =
t á Ñ á = =
_ ä ì É í ç ç í Ü =
l å = p Å ê É É å = h É ó Ä ç ~ ê Ç

Risk

k É í ï ç ê â = Ä ç ç í W Could allow a network boot from an external PXE server.

p á Ç É = r p _ W Controls if the USB device is bootable. Even if the boot order prevents USB being read as above, USB devices can still be booted (as seen in the below example).

ã á Å ê ç p a W Could allow media to be copied to and from the device. The microSD cannot be used as a boot device.

_ ä ì É í ç ç í Ü W Could be used to copy media to and from the device. Likely it may need to be an accepted risk as may be needed for phone headsets or external keyboard devices.

Recommendation

k É í ï ç ê â = Ä ç ç í W set to Disable

p á Ç É = r p _ W **set to** k ç å J _ ç ç í ~ Ä ä É K This does not disable the USB port, it only prevents it being bootable, and therefore it will still operate within Windows as normal. Apply further software restrictions as required.

ã á Å ê ç p a W = **set to** a á ë ~ Ä ä É or control via Software restrictions in Windows.

_ ä ì É í ç ç í Ü K **Set to** a á ë ~ Ä ä É if no Bluetooth is required.

Example

There are two different methods to boot from USB media on the Surface tablets, either by using a button sequence at power on or by instructing Windows to boot from USB on restart.

Button sequence method:

Step 1: Shut down the Surface tablet.

Step 2: Press and hold the volume-down button on your Surface and at the same time, press and release the power button

Step 3: When you see the Surface logo, release the volume-down button.

The USB media will then be read. Providing the USB media contains UEFI compatible boot files the media will boot.

Note: If the USB drive has been set to non-bootable within the UEFI settings, this option will not work until it has been made bootable again within the UEFI

Software method

Step 1: Select Start, Settings

Step 2: Select Update and Security

Step 3: Select Recovery

Step 4: Under the Advanced Start-up heading, select Restart now

Step 5: Select Use a device

Step 6: Select USB Drive

Note: If the USB drive has been set to Non-Bootable within the UEFI settings, this option will not work until it has been made bootable again within the UEFI.

Note: The power and volume locations vary between Surface tablet models. The above is a Surface Pro 3.

Administrator password

Allows a password to be configured to protect entry into the UEFI settings. This is not a power on password and is purely used if the user attempts to enter the UEFI to alter settings

Risk

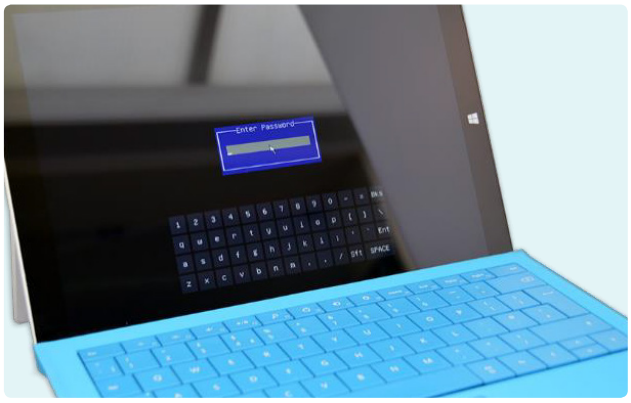
This is a very important setting, as if the UEFI is not protected end users could alter settings relating to the boot order or USB ports and use the device in a non-intended way eg boot an alternative operating system.

Recommendation

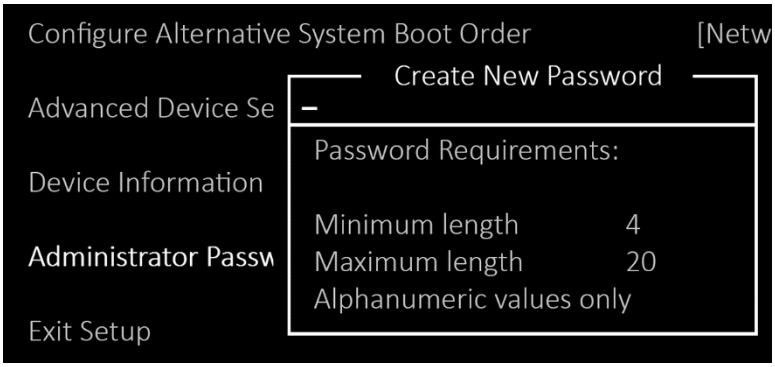
Configure the Administrator password in line with your security policy e.g. 9-12 characters, with mixture of uppercase, lower case, numbers, special symbols etc. This should be used by I.T support and not supplied to end users.

Example

The example right shows a Surface Pro 3 tablet entering the UEFI setup which has had an Administrator password enabled. This will prevent anyone accessing or changing settings without knowing the password.



The example right shows a UEFI password being set:



Automating UEFI changes

Windows Powershell

Summary

The UEFI firmware settings can be read and set using Windows PowerShell. This can be useful if you are deploying a large number of Surface Tablets within your organization and allows automation of control or auditing. The alternative way is to manually configure each device, which can be time consuming and any further changes would require the device to be manually reconfigured again.

For the Surface Tablet Pro 3 Microsoft have released a set of firmware tools which need to be installed onto each device in Windows. This then installs the required modules for PowerShell to access the UEFI firmware.

The software installer can be automatically rolled out within the organization as part of your software deployment, this is outside the scope of this document.

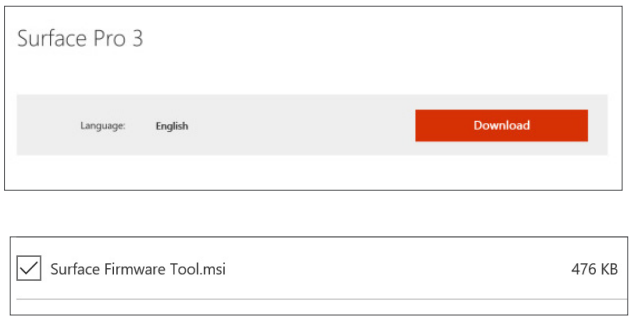
Requirements

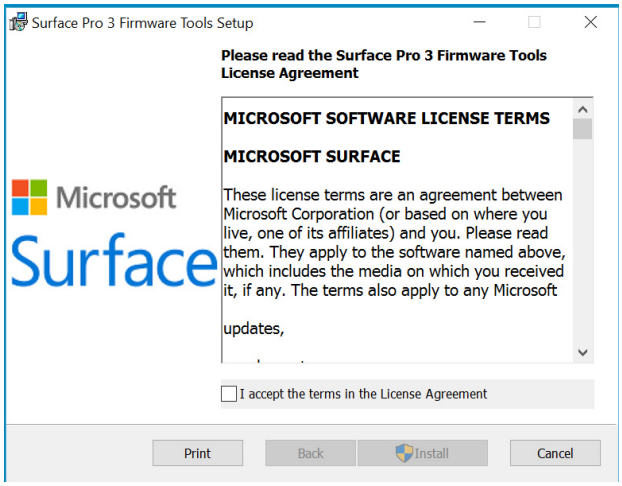
In order to access the UEFI settings the following requirements must be met.

- Install firmware tools for Surface Pro 3 from the following URL: https://www.microsoft.com/en-gb/download/details.aspx?id=38826
- Run PowerShell/Script within Administrator rights “run as Administrator”

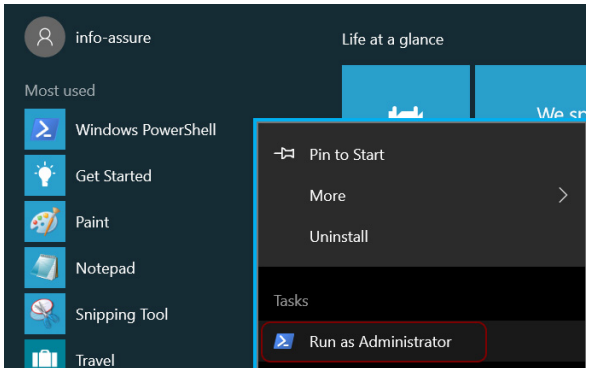
Example

Install the firmware tools from the above URL





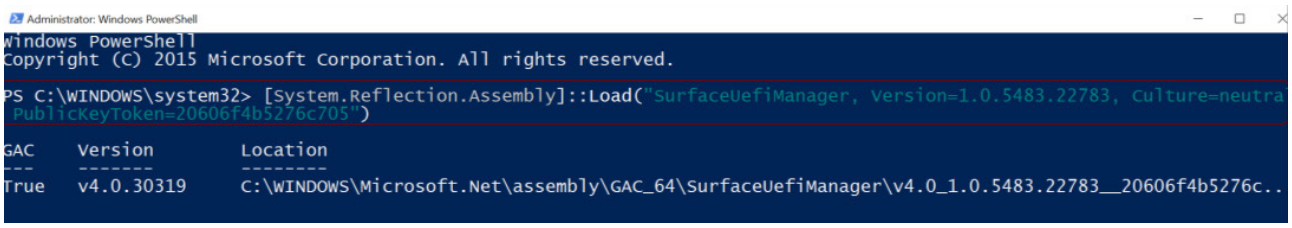
Once installed, open a PowerShell prompt as the Administrator (“run as Administrator”)



Copy and paste the below code into the PowerShell console and run. This loads the UEFI firmware module required.

```
xpóëíÉãKoÉÑäÉÅíáçåK
^ëëÉãÄäózWWçç~ÇE±pìêÑ~ÅÉrÉÑájç~å~ÖÉêI=
sÉêëáçåZNKMKRQUPKOOTUPI=
`ìäíìêÉZåÉìíêç~äI=
mìÄáÅhÉóqçâÉåZOMSMSÑQÄROTSÅTMR≤F=
```

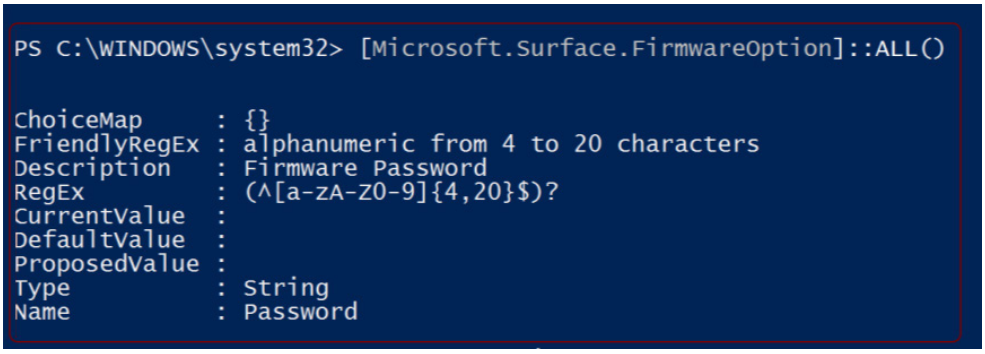
The below version information should be shown, indicating it was successfully loaded.



The UEFI firmware can then be queried retrieving all settings and options by pasting the following code into the PowerShell console.

```
xjáÅêçëçÑíKpìêÑ~ÅÉKcáêãï~êÉléíáçåzWW^iiEF
```

A complete list of all values and options are listed for the UEFI. The below example shows that there currently is not UEFI password set as the `ìêêÉåísäÉ is empty.



Values can also be set from the PowerShell console, this could be used to automate a configuration change across multiple devices using login scripts of deployment software.

For instance if you wanted to alter the boot order to only allow the SSD drive to be checked at boot time, the following command could be used.

To view the current value and options you would enter the following command into PowerShell:

```
xjáÅêçëçÑíKpìêÑ~ÅÉKcáêãï~êÉléíáçåzWWcáåÇE±^äí_ççílêÇÉê≤F
```

This displays all the values and options for the boot order.

```
PS C:\WINDOWS\system32> [Microsoft.Surface.FirmwareOption]::Find("AltBootOrder")


ChoiceMap     : {[4, SSD Only], [0, Network -> USB -> SSD], [1, USB -> Network -> SSD], [2, USB -> SSD]...}
FriendlyRegEx : 4 (SSD Only), 0 (Network -> USB -> SSD), 1 (USB -> Network -> SSD), 2 (USB -> SSD), or 3 (Network ->
                SSD)
Description   : Alternate Boot Order
RegEx         : 4|0|1|2|3
CurrentValue  : 0
DefaultValue  : 4
ProposedValue :
Type          : ChooseOne
Name          : AltBootOrder
```

Note: If you currently have a UEFI password configured you will need to enter the password to unlock access to alter settings using the following command. In this example the UEFI password is "1234" (not recommended).

```
xj áÅêçëçÑí Kpì êÑ~ÅÉKcáêãï ~êÉl éí áçåz WWr åäç ÅâE±NOPQ≤F
```

From the options displayed it shows the current boot order value is 0, which is shown in the ChoiceMap as "Network -> USB -> SSD ". To set the value to "SSD Only", this is option 4.

The following command will configure the UEFI boot order to be "SSD Only"

```
xj áÅêçëçÑí Kpì êÑ~ÅÉKcáêãï ~êÉl éí áçåz WWcáåÇE±^äí _ççí l êÇÉê≤FKmêçéçëÉÇs ~äì É=
Z≤Q≤
```

To confirm the change has been accepted, view the options again using the following command:

```
xj áÅêçëçÑí Kpì êÑ~ÅÉKcáêãï ~êÉl éí áçåz WWcáåÇE±^äí _ççí l êÇÉê≤F
```

```
PS C:\WINDOWS\system32> [Microsoft.Surface.FirmwareOption]::Unlock("1234")
PS C:\WINDOWS\system32> [Microsoft.Surface.FirmwareOption]::Find("AltBootOrder").ProposedValue = "4"
PS C:\WINDOWS\system32> [Microsoft.Surface.FirmwareOption]::Find("AltBootOrder")


ChoiceMap     : {[4, SSD Only], [0, Network -> USB -> SSD], [1, USB -> Network -> SSD], [2, USB -> SSD]...}
FriendlyRegEx : 4 (SSD Only), 0 (Network -> USB -> SSD), 1 (USB -> Network -> SSD), 2 (USB -> SSD), or 3 (Network ->
                SSD)
Description   : Alternate Boot Order
RegEx         : 4|0|1|2|3
CurrentValue  : 0
DefaultValue  : 4
ProposedValue : 4
Type          : ChooseOne
Name          : AltBootOrder
```

This shows that the proposed change of 4 has been entered. The Surface tablet must be rebooted for the change to take effect.

This demonstrates how it is possible to automate these changes if dealing with a large number of Surface tablets that require security hardening.

Please refer to the following Microsoft article for more information:
https://blogs.technet.microsoft.com/askpfeplat/2015/04/19/how-to-manage-surface-pro-3-uefi-through-powershell/

Surface auditor script

Summary

To assist with the auditing of Surface tablet security settings, Info-Assure have created a PowerShell script that will audit the system. This will check all security related values, display the current value and give it a pass or fail grade. It will also recommend the values that should be set. This script does not change any settings, it purely allows the end user or a security professional to use the script for ease. It could also be used as part of login scripts or deployed to audit a large range of tablets and piped into a text file.

Requirements

The script will only run on a Surface Pro 3, it is possible it may work on other models but this has not been tested. This is due to the firmware versions on older Surface tablets not supporting the firmware tools or options.

- Install firmware tools for Surface Pro 3 from the following URL: https://www.microsoft.com/en-gb/download/details.aspx?id=38826
- Set PowerShell restriction to Bypass or Unrestricted to enable scripts within the system
- Run PowerShell/Script within Administrator rights “Run as Administrator”
- Surface Pro 3 end device

Example

PowerShell by default will run in restricted mode, this means it will block any scripts that are attempted to be run. Commands that are entered manually into the console are not blocked, only automated scripts.

To check the current restriction mode and to alter it temporarily follow these steps:

- Open PowerShell with “Run As Administrator” – See above section
- Enter the following command into the PowerShell Console:

```
dÉí J b ñ É Åì í á ç å m ç ä á Åó
```

This will likely display “Restricted”, unless this has already been altered.

```
PS C:\WINDOWS\system32> Get-ExecutionPolicy
Restricted
PS C:\WINDOWS\system32>
```

- To temporarily allow the script to run enter the following command. Note: you can set everything globally to be Unrestricted but this is not recommended for security reasons. Unfortunately this cannot be a part of the script so must be run before the script is launched. If the script restriction is not set the following error will be displayed.

```
PS C:\users\info-assure\Documents> .\surface_auditor.ps1
.\surface_auditor.ps1 : File C:\users\info-assure\Documents\surface_auditor.ps1 cannot be loaded because running
scripts is disabled on this system. For more information, see about_Execution_Policies at
http://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\surface_auditor.ps1
+ ~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
```

The following command will allow a temporary bypass for the current PowerShell console only. This only alters the current window, all new PowerShell consoles will still be restricted.

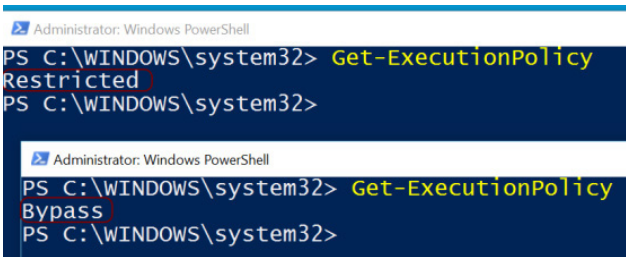
```
p É í J b ñ É Åì í á ç å m ç ä á Åó = ó é ~ ë ë ¥ p Åç é É ╤ ê ç ÅÉ ë ë
```

Select “Y” to allow.

- To check the policy run the following command again:

```
dÉí J bñÉÅì í á ç å mç ä á Åó
```

The policy should now show “Bypass” as per the above foreground image. The background image shows another PowerShell console being launched that has retained its “Restricted” policy which is recommended.



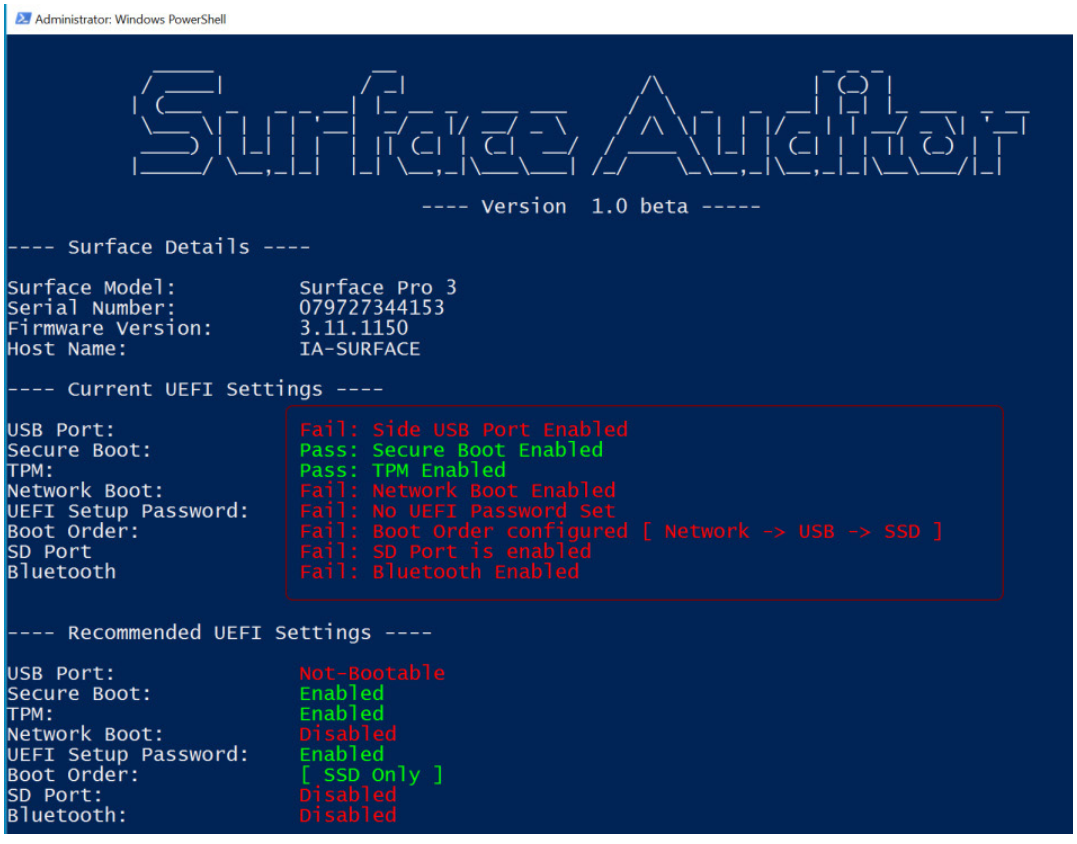
Download the Surface Auditor script from the BSI GitHub repository below:

https://github.com/bsi-group/surfaceauditor

Run the script within the same PowerShell console that the restriction policy was configured above.

```
KLëì êÑ~ÅÉ| ~ì Çáí ç ê Ké ë N
```

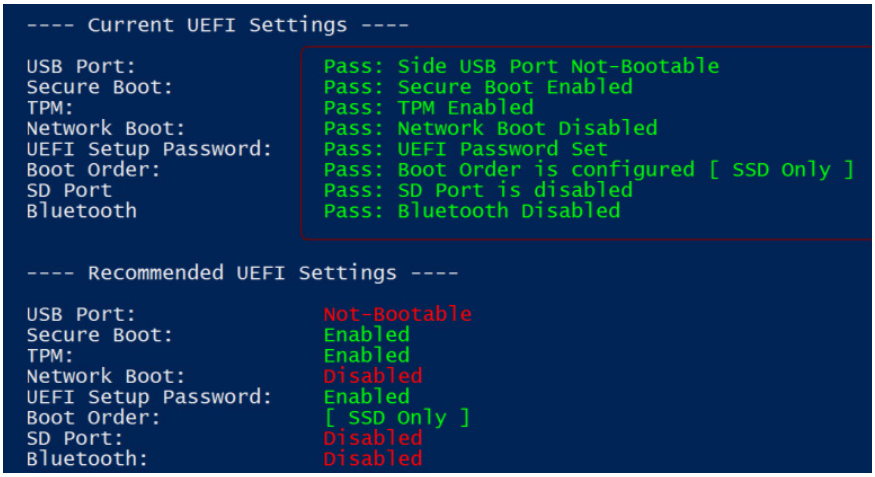
Depending on the current configuration of the UEFI settings, the auditor will display the following:



Any detected issues will be reported, along with the best practice recommendations.

Once the recommended settings have been changed, either manually in the UEFI or via PowerShell commands, re-run the auditor script again.

As can be seen right, all settings are now correctly configured.



Full disk encryption

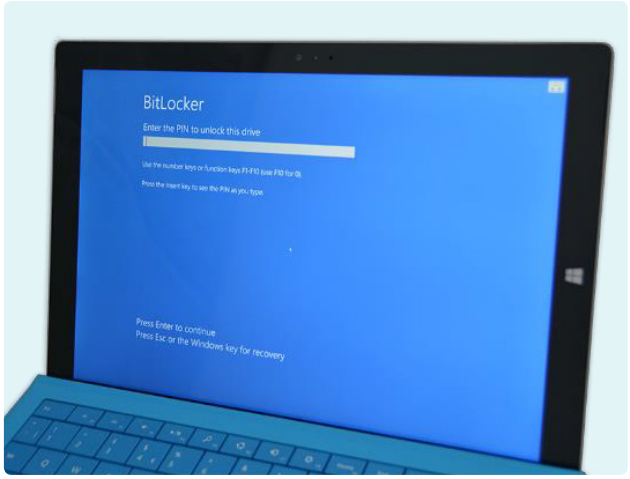
Surface Pro encryption options

Summary

As the Surface tablet device is portable it is highly recommend that the device is configured with full disk encryption. If the device is lost or stolen and the hard disk is not encrypted, any data, password hashes could be extracted from the device.

Several encryption options exist, however not all Encryption products will support the UEFI firmware in use on the Surface tablets.

The free and most likely option that would be used is Microsoft BitLocker which comes included with the operating system. By default configuring BitLocker on the Surface tablets will not allow any form of two-factor authentication, therefore any lost or stolen devices will boot straight to the Windows login screen when powered on. The hard disk data is encrypted, but if the Windows password can be brute forced or guessed, then the data will be unlocked and readable.



The recommended configuration would to be use a power on Pin Code with BitLocker. This is presented at power on and the system will not boot into Windows until the valid pin code is entered.

The image right shows the Surface Pro at power on with the BitLocker pin code set.

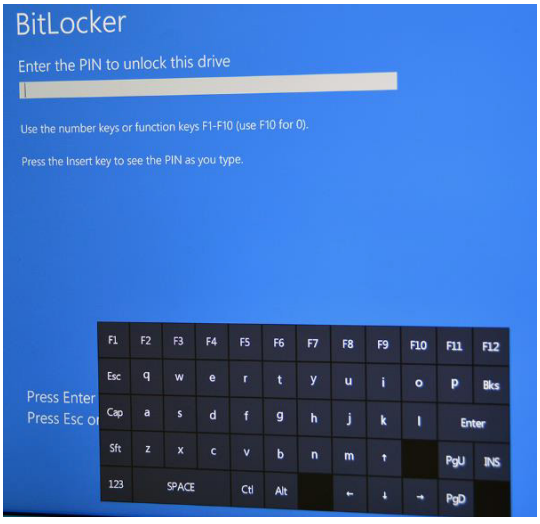
Configuring BitLocker pin code

In order to use the pin code option with BitLocker you need to ensure the device supports a virtual keyboard at power on.

If the device does not support this, a physical keyboard would have to be plugged into the device at power on, otherwise it would not be possible to enter the code and boot the device.

Models before the Surface 3 do not support the virtual keyboard option, therefore it would require a keyboard to be connected at boot.

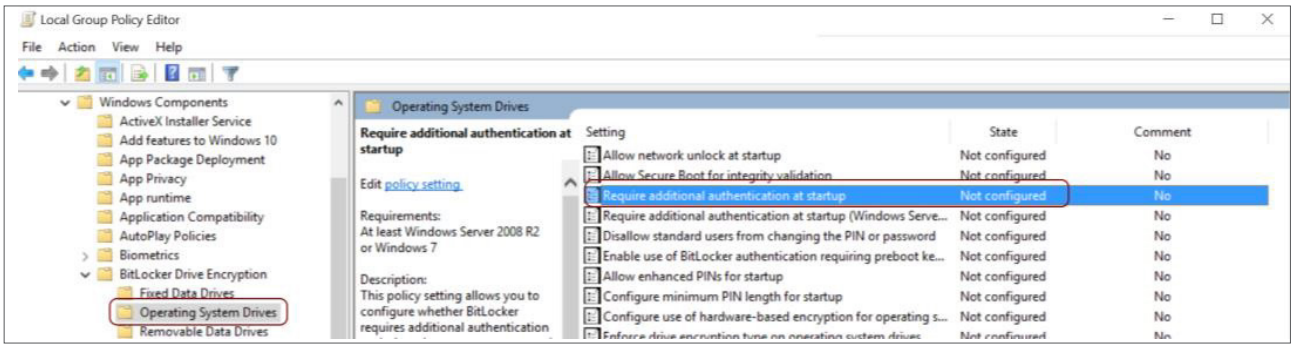
The right image shows the virtual keyboard at power on for BitLocker on Microsoft Surface Pro 3 tablet.



In order to configure the pin code for BitLocker, manual changes must be set within the Group Policy to force a pin code to be used.

This can be configured within Group Policy at the following location:

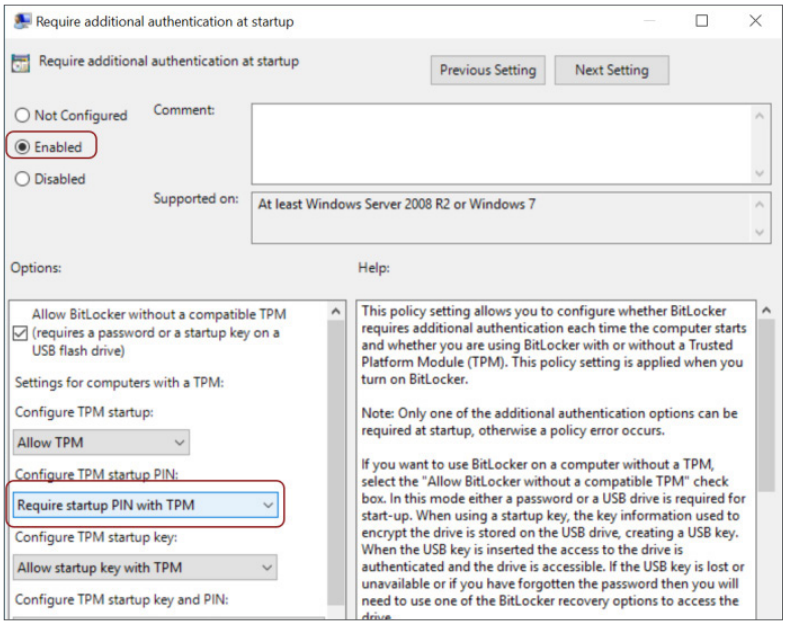
` ç ã é ì í Éê ≐ ç å Ñá Öì ê ~ í á ç å ╡ ≕ ç ä á ÅÉë ╡ ≙ Çã á å á ë í ê ~ í á î É ╕ Éã é ä ~ í Éë ╡ ╪ á å Çç ï ë = ` ç ã é ç å Éå í ë ╡ = á í i ç Åâ Éê ¤ ê á î É ╊ å Âê ó é í á ç å ╡ ╪ é Éê ~ í á å Ö ╼ ó ë í Éã ¤ ê á î Éë ╡ = o Éè ì á ê É = ~ ÇÇá í á ç å ~ ä = ~ ì í ÜÉå í á Å ~ í á ç å = ~ í = ë í ~ ê í ì é

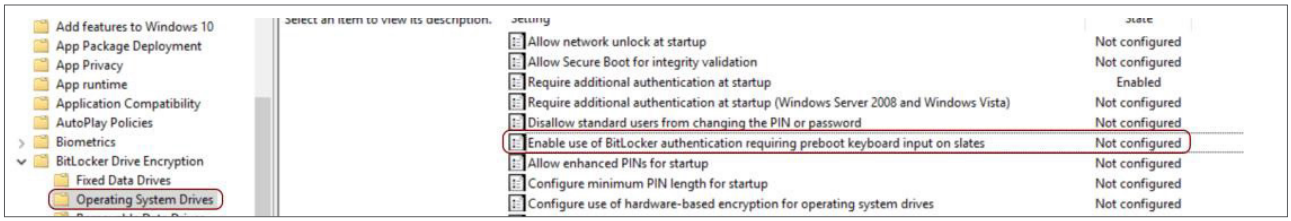


This should then be set to= b å ~ Ää ÉÇ and o Éè ì á ê É = ë í ~ ê í ì é = mf k = ï á í Ü = q mj

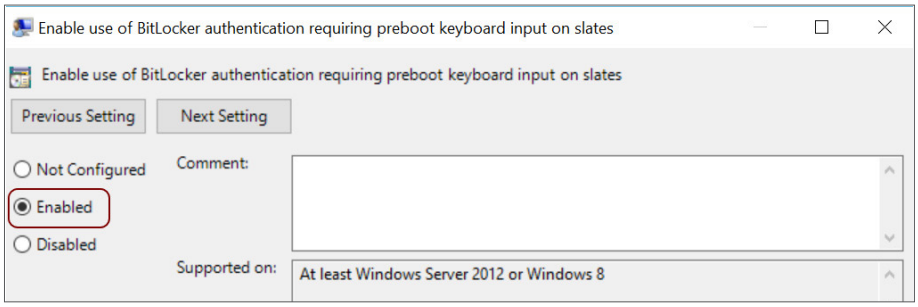
Additionally the following needs to be set to allow the keyboard to be used at startup for BitLocker.

` ç ã é ì í Éê ≐ ç å Ñá Öì ê ~ í á ç å ╡ = mç ä á ÅÉë ╡ ≙ Çã á å á ë í ê ~ í á î É = q Éã é ä ~ í Éë = [ = t á å Çç ï ë = ` ç ã é ç å Éå í ë ╡ = á í i ç Åâ Éê = a ê á î É = b å Âê ó é í á ç å = [= l é Éê ~ í á å Ö = p ó ë í Éã = a ê á î Éë ╡ ╼ b å ~ Ää É ┤ ë É ╕ Ñ = _ á í ä ç Åâ Éê ═ ì í ÜÉå í á Å ~ í á ç å = ê Éè ì á ê á å Ö = é ê É Äç ç í = â Éó Äç ~ ê Ç = á å é ì í = ç å = ë ä ~ í Éë





Set to b å ~ Ää ÉÇ



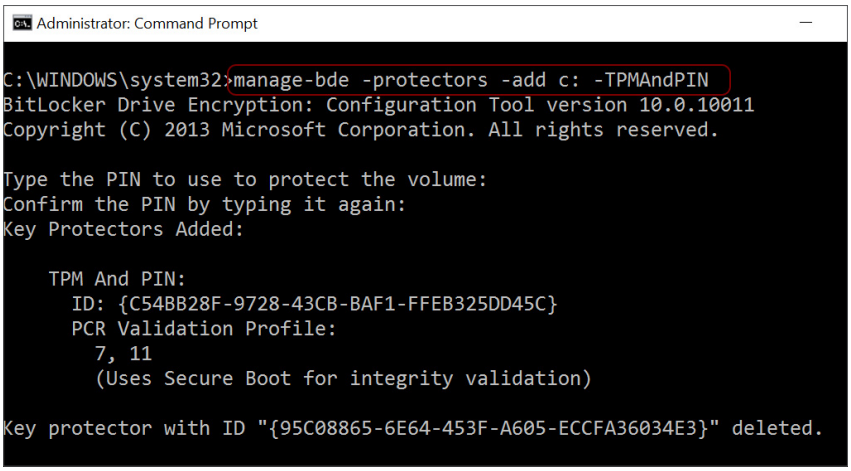
The final step is to configure the pin code for BitLocker to use at pre-boot.

The pin code can then be set using the following command from an administrative command prompt:

```
ã ~å ~ÖÉJ ÄÇÉ∓é ê ç í ÉÅí ç ê ë ∓ ~ÇÇ≠ÅW∓ q mj ^ å Çmf k
```

At next boot the BitLocker pin code will be requested.

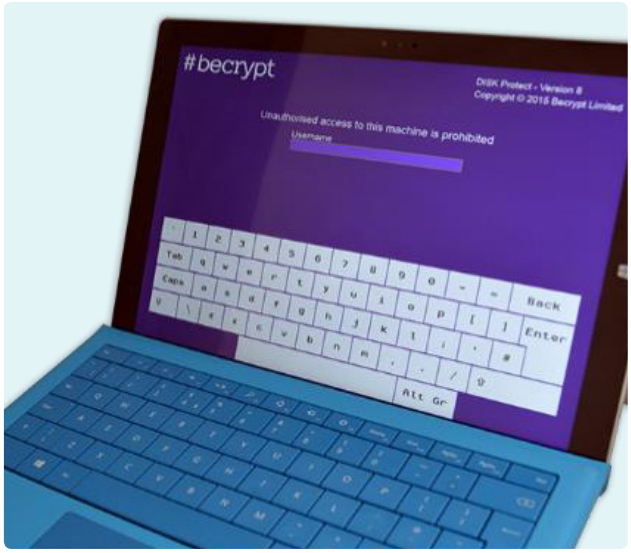
This options needs consideration as it could result in extra support calls for lost pin codes.



Other encryption products

Other commercial disk encryption products exist, however not all will work with the UEFI firmware in use.

Becrypt supports UEFI and has successfully been tested on the Surface Pro 3 as shown here.



Appendix A – Creating bootable UEFI media

Creating bootable USB media is not as straight forward for UEFI firmware devices. Typically on a PC using a BIOS you can just download a bootable ISO and burn it or use USB media creation tools and the system will boot from this.

For UEFI the majority of commonly used tools for security auditing will not boot out of the box on the Surface pro due to the UEFI firmware. So for security professionals, do not expect your Ophcrack or Linux live ISO you typically use on workstation reviews to just boot on a Surface Pro tablet.

The following guide is more suited to security professionals such as penetration testers. Creating a Kali2 UEFI USB stick that will work on the Surface tablet:

Image Name	Direct
Kali Linux 64 bit	ISO

Download the Kali2 ISO from the below URL: https://www.kali.org/downloads/

Several software tools exist that can be used to create USB bootable media:

Rufus: http://rufus.akeo.ie/

ISO2Disc: http://www.top-password.com/

In the below example the Rufus product will be used.

The following options should be set:

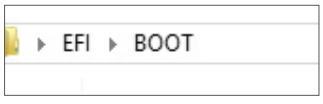
- MBR partition schedule for BIOS or UEFI-CSM
- FAT32 (Ensure your USB stick is 32GB or less)
- Point it to the Kali Linux ISO downloaded

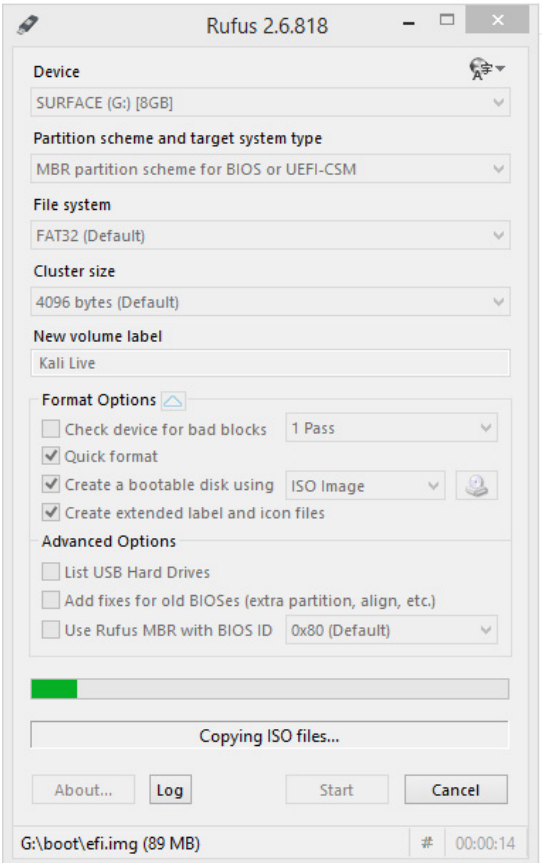
Then click Start

Further steps are required before the USB stick and distro will be fully UEFI bootable.

- Create a new directory in the root (/) of the newly created USB stick named b c f
- Create a subdirectory within b c f named _ l l q

You should have the following folder structure L b c f L _ l l q L =





You will need to download two extra EFI boot files. These can be taken from another Linux distribution such as Fedora or Scientific Linux.

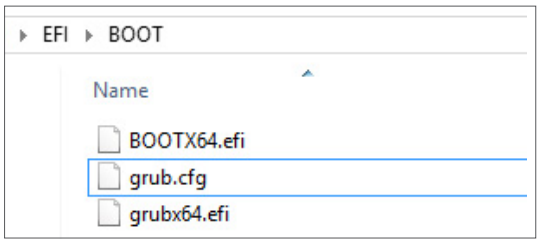
_ l l qu SQKÉÑá	http://ftp.scientificlinux.org/linux/fedora/releases/18/Fedora/x86_64/os/EFI/BOOT/BOOTX64.efi
Öê ì Äu SQKÉÑá	http://ftp.scientificlinux.org/linux/fedora/releases/18/Fedora/x86_64/os/EFI/BOOT/grubx64.efi

A Grub file will also be required. You can write your own, but for ease a very good one can be found at the following link, credit to the author for publishing this.
http://linuxhow2s.blogspot.co.uk/2013/06/install-force-kali-linux-on-efi-based.html

The below code can be pasted into a file name grub.cfg

```
@=` ç å Ñá Ö=Ñá ä É=Ñç ê=d o r _ O=J =q ÜÉ=d k r =d o ~ å Ç=r å á Ñá É Ç=_ ç ç í ä ç ~ ÇÉ ê =
@=L Äç ç í LÖê ì ÄL Öê ì ÄKÅÑÖ=
@=a b s f ` b=k ^ j b=` l k s b o p f l k p=
@=
@=i á å ì ñ=d ê ì Ä=
@=J J J J J J J J J J J J J J J J J J J J =
@=L ÇÉ î L ÑÇM=E ÑÇMF =
@=L ÇÉ î Lë Ç~ =E ÜÇMF =
@=L ÇÉ î Lë ÇÄO=E ÜÇNI OF =
@=L ÇÉ î Lë Ç~ P=E ÜÇMI P F=
@=
@=ê ç ç í Zr r f a ZÇÅMUÉRÄMJ ÉTMQJ QRTPJ ÄP ÑOJ ÅÑÉQNÄTPÉSOÄ=é Éê ë á ë í Éå í =
ë Éí =ã Éå ì | Åç ä ç ê | å ç ê ã ~ ä ZóÉä ä ç ï LÄä ì É=
ë Éí =ã Éå ì | Åç ä ç ê | Üá ÖÜä á ÖÜí ZÄä ì ÉLóÉä ä ç ï =
Ñì å Åí á ç å=ä ç ~ Ç| î á ÇÉ ç =ô=
á å ë ã ç Ç=ÉÑá | Öç é =
á å ë ã ç Ç=ÉÑá | ì Ö~ =
á å ë ã ç Ç=î á ÇÉ ç | Äç ÅÜë =
á å ë ã ç Ç=î á ÇÉ ç | Åá ê ê ì ë =
á å ë ã ç Ç=~ ä ä | î á ÇÉ ç =
õ=
ä ç ~ Ç| î á ÇÉ ç =
ë Éí =ÖÑñ é ~ ó ä ç ~ ÇZâ ÉÉé =
@=q á ã É ç ì í =Ñç ê=ã Éå ì =
ë Éí =í á ã É ç ì í ZR=
@=p Éí =ÇÉÑ~ ì ä í =Äç ç í =Éå í ê ó=~ ë=b å í ê ó=M=
ë Éí =ÇÉÑ~ ì ä í ZM=
ë Éí =Åç ä ç ê | å ç ê ã ~ ä ZóÉä ä ç ï LÄä ì É=
ã Éå ì Éå í ê ó=± h ~ ä á=J =_ ç ç í =k ç å=mÉ ê ë á ë í Éå í =j ç ÇÉ ≤=ô=
ë Éí =ê ç ç í ZEÜÇMI NF=
ä á å ì ñ ÉÑá Ł ä á î ÉLî ã ä á å ì ò Äç ç í Zä á î É ç Åç å Ñá ÖZë ì Çç ⊧ ë Éê å ~ ã ÉZê ç ç í Ü ç ë í å ~ ã ÉZâ ~ ä á =
á å á í ê ÇÉÑá=Lä á î ÉLá å á í ê ÇKá ã Ö=
õ=
ã Éå ì Éå í ê ó=± h ~ ä á=J =_ ç ç í =mÉ ê ë á ë í Éå í ≤=ô=
ë Éí =ê ç ç í ZEÜÇMI NF=
ä á å ì ñ ÉÑá Ł ä á î ÉLî ã ä á å ì ò Äç ç í Zä á î É ç Åç å Ñá ÖZë ì Çç ⊧ ë Éê å ~ ã ÉZê ç ç í Ü ç ë í å ~ ã ÉZâ ~ ä á =
é Éê ë á ë í Éå ÅÉ=
á å á í ê ÇÉÑá=Lä á î ÉLá å á í ê ÇKá ã Ö=
õ=
ã Éå ì Éå í ê ó=± h ~ ä á=c ~ á ä ë ~ ÑÉ ≤=ô=
ë Éí =ê ç ç í ZEÜÇMI NF=
ä á å ì ñ ÉÑá Ł ä á î ÉLî ã ä á å ì ò Äç ç í Zä á î É Åç å Ñá Ö ã Éã í Éë í å ç ~ é á Å å ç ~ é ã å ç Çã ~ å ç ã ÅÉ=
å ç ä ~ é á Å=å ç ã ç ÇÉë Éí =å ç ë ã é=å ç ë é ä ~ ë Ü=î Ö~ Zå ç ê ã ~ ä =
á å á í ê ÇÉÑá=Lä á î ÉLá å á í ê ÇKá ã Ö=
õ=
ã Éå ì Éå í ê ó=± h ~ ä á=c ç ê Éå ë á Åë =J =k ç =a ê á î É=ç ê=p ï ~ é=j ç ì å í ≤=ô=
ë Éí =ê ç ç í ZEÜÇMI NF=
ä á å ì ñ ÉÑá Ł ä á î ÉLî ã ä á å ì ò Äç ç í Zä á î É å ç Åç å Ñá ÖZë ì Çç ⊧ ë Éê å ~ ã ÉZê ç ç í Ü ç ë í å ~ ã ÉZâ ~ ä á =
å ç ë ï ~ é=å ç ~ ì í ç ã ç ì å í =
á å á í ê ÇÉÑá=Lä á î ÉLá å á í ê ÇKá ã Ö=
õ=
ã Éå ì Éå í ê ó=± h ~ ä á=d ê ~ é Üá Å~ ä=f å ë í ~ ä ä ≤=ô=
ë Éí =ê ç ç í ZEÜÇMI NF=
ä á å ì ñ ÉÑá =Lá å ë í ~ ä ä LÖí â Lî ã ä á å ì ò =î á ÇÉç Zî Éë ~ Wó ï ê ~ é I ã í ê ê =î Ö~ ZTUU=
á å á í ê ÇÉÑá=Lá å ë í ~ ä ä LÖí â Lá å á í ê ÇKÖò =
õ=
ã Éå ì Éå í ê ó=± h ~ ä á=q Éñ í =f å ë í ~ ä ä ≤=ô=
ë Éí =ê ç ç í ZEÜÇMI NF=
ä á å ì ñ ÉÑá=Lá å ë í ~ ä ä Lî ã ä á å ì ò=î á ÇÉç Zî Éë ~ Wó ï ê ~ é I ã í ê ê =î Ö~ ZTUU=
á å á í ê ÇÉÑá=Lá å ë í ~ ä ä Lá å á í ê ÇKÖò =
```

Save all three files into the Lbcf L_lll q directory on the USB stick.



When attempting to boot from the newly created USB stick, you must ensure that the Secure Boot Control is disabled within the BIOS and USB booting is allowed. With Secure Boot Enabled you will get an invalid signature error and it will not boot from the USB media.

Boot the Surface tablet with the USB stick inserted and it should boot straight into Kali2 Linux.

Cybersecurity and Information Resilience

BSI Cybersecurity and Information Resilience help you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that effect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:

Cybersecurity

Penetration testing, vulnerability management, incident response and cloud security services.

Security awareness

Phishing and user awareness training, SaaS solutions, social engineering and simulation testing

Data management and privacy

GDPR services, information lifecycle management and eDiscovery and forensics

Compliance and testing

PCI DSS services, cyber lab testing and product and software assessments (CC, CAS-T/CPA)

Our expertise is accredited by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

CYBER ESSENTIALS

CREST STAR

UKAS TESTING 8237

Find out more

Call UK: +44 345 222 1711
Call IE: +353 1 210 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com

bsi.