congatec Application Note

Affected Products	All products featuring UEFI
Subject	How to create a bootable USB stick with a UEFI shell.
Confidential/Public	Public
Author	CJR

Revision History

Revision	Date (yyyy-mm-dd)	Author	Changes
1.0	2014-06-13	CJR	Initial release
1.1	2016-09-21	HHA	Format update, add new figures
1.2	2016-11-09	GMA	Updated section 2
1.3	2019-05-24	BEU	Updated links to binary files and updated template

Preface

This application note describes how to create a bootable UEFI shell USB stick. Most recent congatec products featuring UEFI firmware can boot such a stick.

Disclaimer

The information contained within this Application Note, including but not limited to any product specification, is subject to change without notice.

congatec AG provides no warranty with regard to this Application Note or any other information contained herein and hereby expressly disclaims any implied warranties of merchantability or fitness for any particular purpose with regard to any of the foregoing. congatec AG assumes no liability for any damages incurred directly or indirectly from any technical or typographical errors or omissions contained herein or for discrepancies between the product and the Application Note. In no event shall congatec AG be liable for any incidental, consequential, special, or exemplary damages, whether based on tort, contract or otherwise, arising out of or in connection with this Application Note or any other information contained herein or the use thereof.

Intended Audience

This Application Note is intended for technically qualified personnel. It is not intended for general audiences.

Electrostatic Sensitive Device

All congatec AG products are electrostatic sensitive devices and are packaged accordingly. Do not open or handle a congatec AG product except at an electrostatic-free workstation. Additionally, do not ship or store congatec AG products near strong electrostatic, electromagnetic, magnetic, or radioactive fields unless the device is contained within its original manufacturer's packaging. Be aware that failure to comply with these guidelines will void the congatec AG Limited Warranty.

Technical Support

congatec AG technicians and engineers are committed to providing the best possible technical support for our customers so that our products can be easily used and implemented. We request that you first visit our website at www.congatec.com for the latest documentation, utilities and drivers, which have been made available to assist you. If you still require assistance after visiting our website then contact our technical support department by email at support@congatec.com

Symbols

The following are symbols used in this application note.

Note

Notes call attention to important information that should be observed.

Caution

Cautions warn the user about how to prevent damage to hardware or loss of data.

Warning

Warnings indicate that personal injury can occur if the information is not observed.

Copyright Notice

Trademarks

Product names, logos, brands, and other trademarks featured or referred to within this user’s guide or the congatec website, are the property of their respective trademark holders. These trademark holders are not affiliated with congatec AG, our products, or our website.

1 UEFI Shell Introduction

UEFI provides a shell environment, which can be used to execute other UEFI applications including UEFI boot loaders. Apart from that, commands available in the UEFI shell can be used for obtaining various other information about the system or the firmware, including getting the memory map (memmap), modifying boot manager variables (bcfg), running partitioning programs (diskpart), loading UEFI drivers, and editing text files (edit).

There are two methods used for launching UEFI shell. UEFI firmware implementations may offer a built-in shell. This shell can be directly booted by assigning it as 'First boot priority' or selecting the Built-in shell as the boot device in the first boot menu.

congatec embedded BIOSes do not offer Built-in shell for security reasons. Built-in shell may allow users the possibility to bypass security mechanisms that are contained within the BIOS.

Given that, another solution must be used and this involves creating an appropriate USB flash drive with the compiled version of the shell on it. The procedure how to create such a bootable USB flash drive is explained in this document.

Note

On some congatec products one must set the 'Boot Priority Selection' setup node to 'Device Based' to enable the ability to assign the built-in UEFI shell a fixed boot priority. 'Type Based' boot priority selection only supports legacy boot options.

In addition to that, the 'Boot Option Filter' setup node must not be set to 'Legacy Only' for UEFI compatible boot devices.

Making a UEFI boot USB stick the first boot device is always possible with the aid of the First Boot Menu which can be launched by pressing F11 at the end of POST.

2 Procedure to Create the UEFI Shell Stick

2.1 Prepare the USB stick

There are no special requirements for the USB MSD device used. Simply create a FAT32 partition on the storage device.

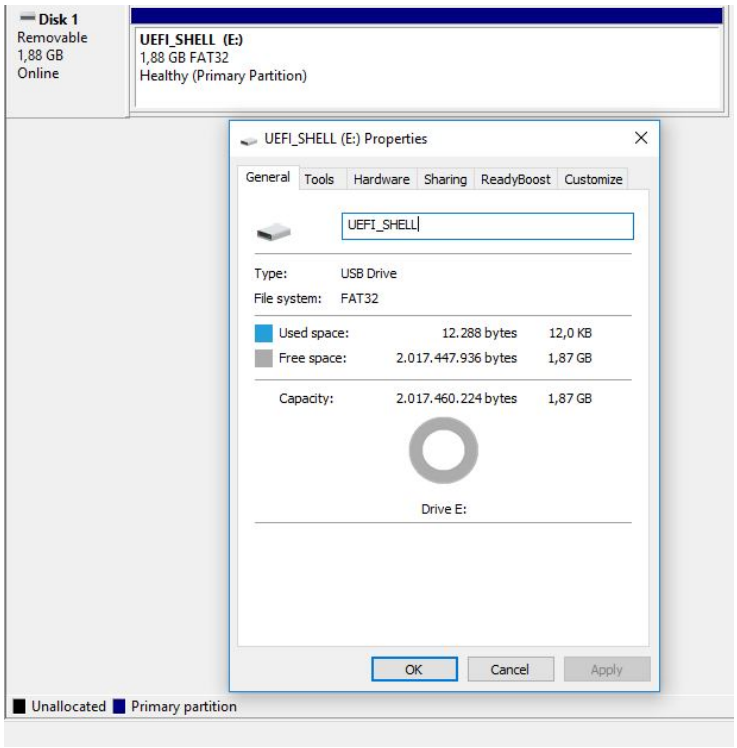

Figure 1: Properties of the USB MSD device used

2.2 Download the UEFI Shell Binary Files

The EDK2 UEFI shell binaries can be downloaded from the links below. There are two separate UEFI Shell binaries for 32bit and 64bit x86 PC architecture. Most modern PCs are running in 64bit mode but in order to create a universal UEFI Shell stick it is recommended to support both architectures.
For 32bit (Ia32):
https://github.com/tianocore/edk2/blob/UDK2018/ShellBinPkg/UefiShell/Ia32/Shell.efi

For 64bit (X64):
https://github.com/tianocore/edk2/blob/UDK2018/ShellBinPkg/UefiShell/X64/Shell.efi

Download and save the UEFI shell binaries for the 32 bit (Ia32) and the 64 bit (X64) architecture in a directory of your choice. In this example UefiShell\X64 directory for 64 bit PC architecture and UefiShell\Ia32 directory for 32 bit PC architecture.

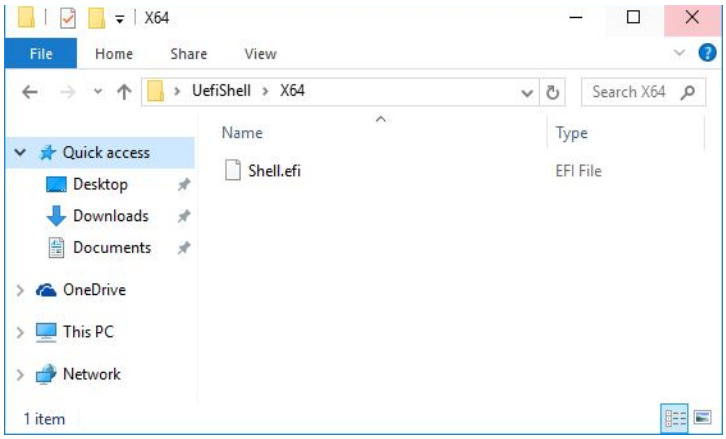

Figure 3: Files in UefiShell\x64

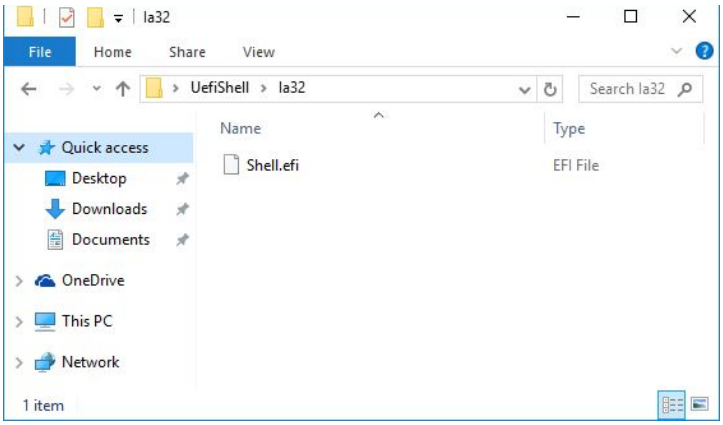

Figure 4: Files in UefiShell\Ia32

Rename the Shell.efi file in \x64 to BOOTX64.efi.

Rename the Shell.efi file in \ia32 to bootia32.efi.

2.3 Copy the UEFI Shell Binaries to the Stick

Create the following directory structure on the USB stick: efi\boot\

Copy the BOOTX64.efi and the bootia32.efi files into this directory.

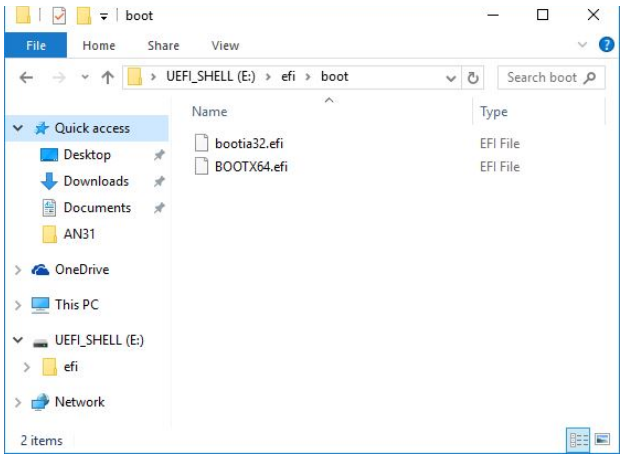

Figure 4: Files on the USB stick in the sub directory \efi\boot

2.4 Boot to the UEFI Shell

Attach the USB stick to the system running a UEFI enabled congatec BIOS firmware.

Either press F11 to open the BBS Boot Menu and select the UEFI USB stick.

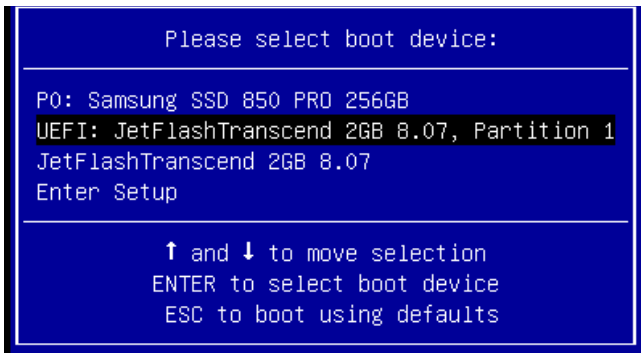

Figure 5: BBS Boot Popup Menu

Or select the USB stick as first boot device in the Device Based Boot Priority list in BIOS setup.

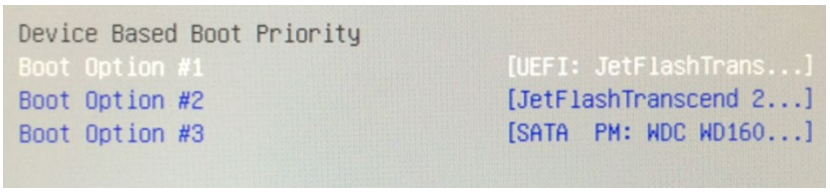

Figure 6: Device based Boot Priority list in the congatec BIOS setup

Note

The UEFI shell cannot be selected in the Type Based (default) Boot Priority list because only legacy boot devices are supported by the Type Based list.

The 'Boot Option Filter' setup node in the CSM sub menu must not be set to 'Legacy Only' for UEFI compatible boot devices.

Conclusion

If all the above steps are followed correctly, the USB stick you created provides you with the ability to utilize the UEFI shell within your system.