Enable configuration for system ready iot

This section tells you how to enable the following configuration options required for SystemReady IR - IoT certification requirements:

UEFI support with U-Boot

* Device Firmware Update to enable UpdateCapsule support
* UEFI support with U-Boot

### Enable UEFI support with U-Boot

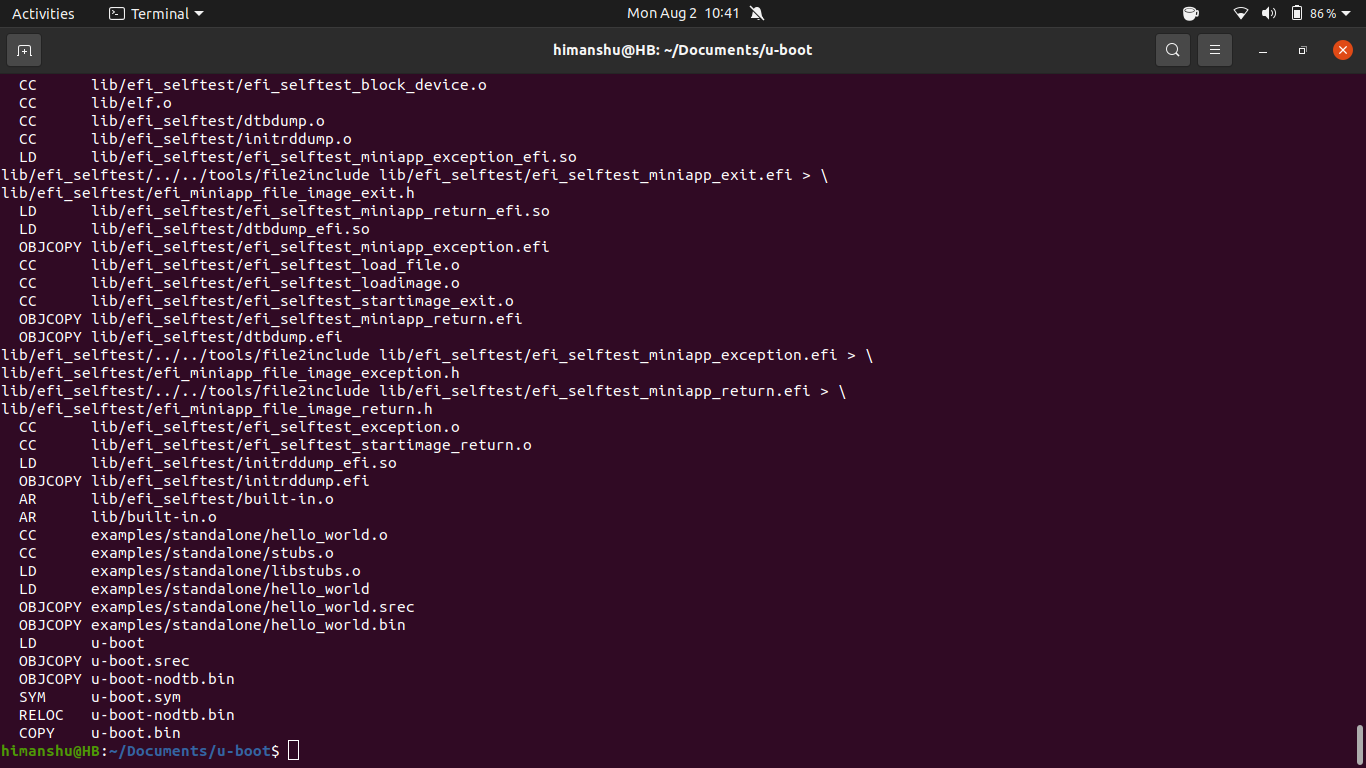
Enable the configuration options in root\_workspace/u-boot/configs/platform\_name\_defconfig as shown in the following code:

CONFIG\_BOOTM\_EFI=y CONFIG\_CMD\_BOOTEFI=y CONFIG\_CMD\_NVEDIT\_EFI=y CONFIG\_CMD\_EFIDEBUG=y CONFIG\_CMD\_GPT=y CONFIG\_EFI\_PARTITION=y CONFIG\_EFI\_LOADER=y CONFIG\_EFI\_DEVICE\_PATH\_TO\_TEXT=y CONFIG\_EFI\_UNICODE\_COLLATION\_PROTOCOL2=y CONFIG\_EFI\_UNICODE\_CAPITALIZATION=y CONFIG\_EFI\_HAVE\_RUNTIME\_RESET=y CONFIG\_CMD\_EFI\_VARIABLE\_FILE\_STORE=y

Add the configuration options to enable the UEFI UpdateCapsule() interface to update firmware as follows:

CONFIG\_CMD\_DFU=y CONFIG\_FLASH\_CFI\_MTD=y CONFIG\_EFI\_CAPSULE\_FIRMWARE\_MANAGEMENT=y CONFIG\_EFI\_CAPSULE\_FIRMWARE=y CONFIG\_EFI\_CAPSULE\_FIRMWARE\_RAW=y CONFIG\_EFI\_CAPSULE\_FMP\_HEADER=y

So we did the changes accordingly in the u-boot config



also you can save that config using the commands

**make savedefconfig**

**cp defconfig arch/arm/configs/my\_cool\_defconfig**

**CONFIG\_BOOTM\_EFI=y** # enable bootm command to launch FIT image with UEFI binary

**CONFIG\_CMD\_BOOTEFI=y** # command bootefi to lauch UEFI binaries

**CONFIG\_CMD\_NVEDIT\_EFI=y** # commands to display and edit UEFI variables

**CONFIG\_HEXDUMP=y** # required for display of UEFI variable content; CONFIG\_SPL\_HEXDUMP is not needed

**CONFIG\_CMD\_EFIDEBUG=y** # command to edit boot options

**CONFIG\_CMD\_GPT=y**  # command to display and alter GUID partition table

**CONFIG\_EFI\_PARTITION=y** # partition table support

**CONFIG\_EFI\_LOADER=y** # enable UEFI sub-system

**CONFIG\_EFI\_DEVICE\_PATH\_TO\_TEXT=y** # provide EFI\_DEVICE\_PATH\_TO\_TEXT\_PROTOCOL

**CONFIG\_EFI\_UNICODE\_COLLATION\_PROTOCOL2=y** # provide FI\_UNICODE\_COLLATION\_PROTOCOL2

**CONFIG\_EFI\_UNICODE\_CAPITALIZATION=y** # support lower/upper conversion for non-ANSI characters

**CONFIG\_EFI\_HAVE\_RUNTIME\_RESET=y** # enable reset runtime service at runtime

**CONFIG\_CMD\_EFI\_VARIABLE\_FILE\_STORE=Y** # store UEFI variables in file, if OP-TEE StandAloneMM is available choose EFI\_MM\_COMM\_TEE instead

**CONFIG\_EFI\_SECURE\_BOOT=y** # enable secure boot

