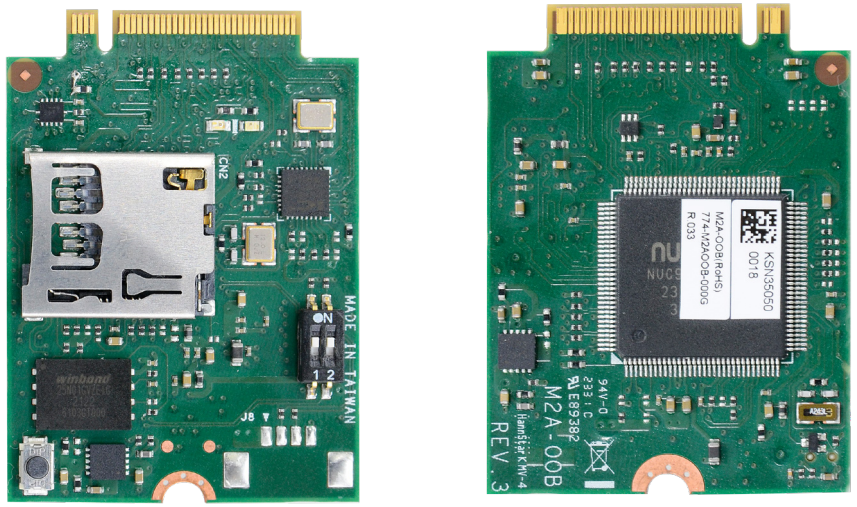
DFI



M2A-OOB

M.2 Out Of Band Module Compact BMC (cBMC)
User's Manual

Copyright

This publication contains information that is protected by copyright. No part of it may be reproduced in any form or by any means or used to make any transformation/adaptation without the prior written permission from the copyright holders.

This publication is provided for informational purposes only. The manufacturer makes no representations or warranties with respect to the contents or use of this manual and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The user will assume the entire risk of the use or the results of the use of this document. Further, the manufacturer reserves the right to revise this publication and make changes to its contents at any time, without obligation to notify any person or entity of such revisions or changes.

Changes after the publication's first release will be based on the product's revision. The website will always provide the most updated information.

© 2024. All Rights Reserved.

Trademarks

Product names or trademarks appearing in this manual are for identification purpose only and are the properties of the respective owners.

FCC and DOC Statement on Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio TV technician for help.

Notice:

1. The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
2. Shielded interface cables must be used in order to comply with the emission limits.

Table of Contents

About this Manual

This manual can be downloaded from the website.

The manual is subject to change and update without notice, and may be based on editions that do not resemble your actual products. Please visit our website or contact our sales representatives for the latest editions.

Warranty

1. Warranty does not cover damages or failures that occur from misuse of the product, inability to use the product, unauthorized replacement or alteration of components and product specifications.

2. The warranty is void if the product has been subjected to physical abuse, improper installation, modification, accidents or unauthorized repair of the product.

3. Unless otherwise instructed in this user's manual, the user may not, under any circumstances, attempt to perform service, adjustments or repairs on the product, whether in or out of warranty. It must be returned to the purchase point, factory or authorized service agency for all such work.

4. We will not be liable for any indirect, special, incidental or consequential damages to the product that has been modified or altered.

Static Electricity Precautions

It is quite easy to inadvertently damage your PC, system board, components or devices even before installing them in your system unit. Static electrical discharge can damage computer components without causing any signs of physical damage. You must take extra care in handling them to ensure against electrostatic build-up.

1. To prevent electrostatic build-up, leave the system board in its anti-static bag until you are ready to install it.

2. Wear an antistatic wrist strap.

3. Do all preparation work on a static-free surface.

4. Hold the device only by its edges. Be careful not to touch any of the components, contacts or connections.

5. Avoid touching the pins or contacts on all modules and connectors. Hold modules or connectors by their ends.

Important:
Electrostatic discharge (ESD) can damage your processor, disk drive and other components. Perform the upgrade instruction procedures described at an ESD workstation only. If such a station is not available, you can provide some ESD protection by wearing an antistatic wrist strap and attaching it to a metal part of the system chassis. If a wrist strap is unavailable, establish and maintain contact with the system chassis throughout any procedures requiring ESD protection.

Safety Measures

- To avoid damage to the system, use the correct AC input voltage range.

- To reduce the risk of electric shock, unplug the power cord before removing the system chassis cover for installation or servicing. After installation or servicing, cover the system chassis before plugging the power cord.

Chapter 1 - Introduction

▶ What's OOB (Out-Of-Band) Management

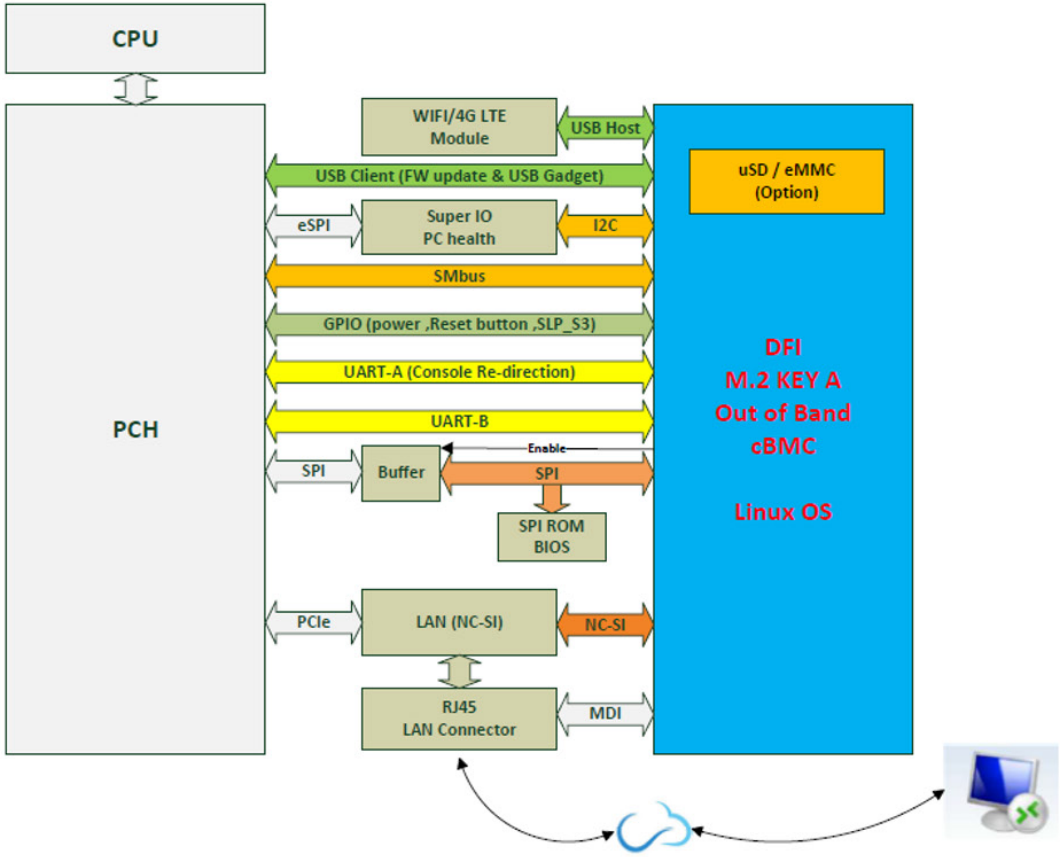
As Industrial IoT demands rise in recent decades, the number of connected IoT devices drastically grow. However, the personnel responsible for equipment maintenance cannot meet the growing numbers of IoT devices; additionally, unexpected factors occur, e.g. the global pandemic. It seems like it is harder to maintain and repair the equipment in a timely manner.

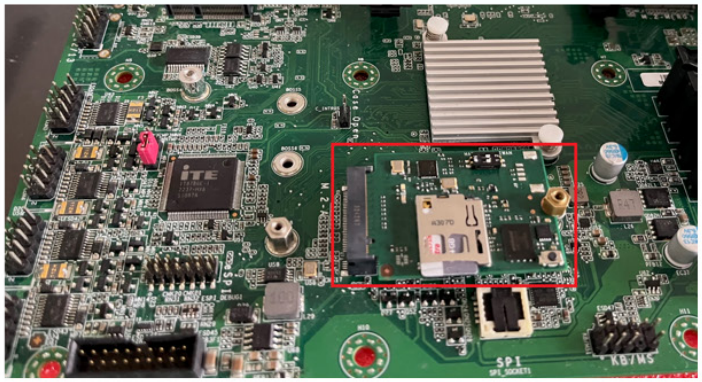
Remote management without running OS. Out-of-band (OOB) technology can timely predict equipment status before the shutdown and efficiently activate OS auto-backup and recovery despite host crashes. Furthermore, the data of device health status are collected automatically to the cloud, and users can easily monitor all connected devices through a customizable UX dashboard.

▶ Key Features

- ▶ Open SSH login
- ▶ Remote power on/off & reset control
- ▶ Remote hardware monitor log
- ▶ Recovery (Factory Mode)
- ▶ Remote BIOS setup & uefi shell (serial over lan)
- ▶ Remote BIOS update SPI-NAND
- ▶ Remote BIOS update SOL & DFI USB-Storage
- ▶ Change OOB IP address

▶ M.2 KEY A cBMC


CPU
PCH
WIFI/4G LTE Module
USB Host
USB Client (FW update & USB Gadget)
eSPI
Super IO PC health
I2C
SMbus
GPIO (power ,Reset button ,SLP_S3)
UART-A (Console Re-direction)
UART-B
SPI
Buffer
Enable
SPI
SPI ROM BIOS
PCIe
LAN (NC-SI)
NC-SI
RJ45 LAN Connector
MDI
uSD / eMMC (Option)
DFI
M.2 KEY A
Out of Band
cBMC
Linux OS



Chapter 2 - Getting Started

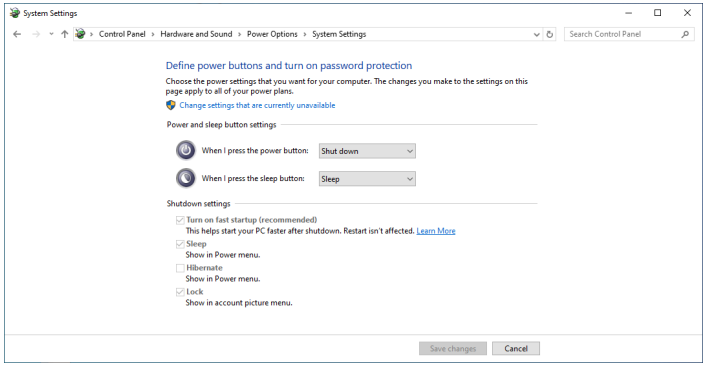
Please follow the steps to configure M2A-OOB.

▶ Hardware Requirements

1. x86 PC Including OOB x1
2. LAN Cable x1
3. x86 PC x1
4. OOB x1

▶ System Requirements

- The remote PC can remotely control the DFI system which installed OOB feature. Remote PC and DFI system shall be in the same network domain
- To avoid setting OOB's power_button.sh as a power on/off function, please make sure to choose '**shut down**' from '**When I press the power button:**' on System Settings.

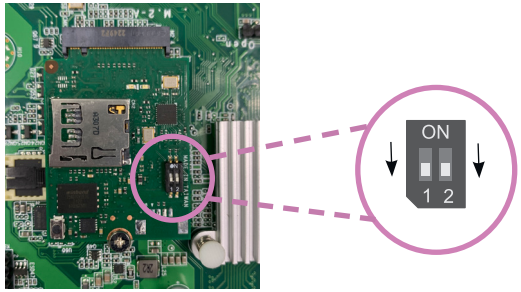


- TeraTerm is already included in the DFI system.

▶ OOB Normal Boot

Step 1:

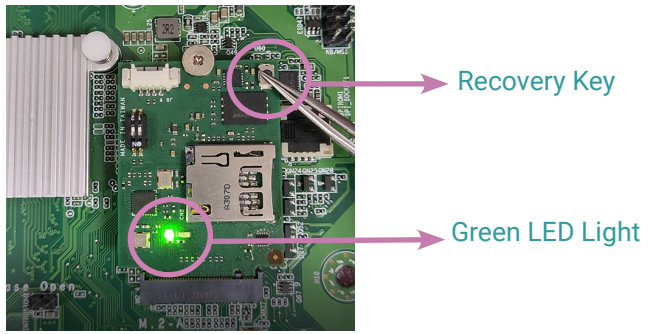
Make sure the switch 1 & 2 change to off.



Step 2:

Start up the main board.

It takes about 2 minutes to wait for the green LED lights up. OOB has been started successfully.



Note:

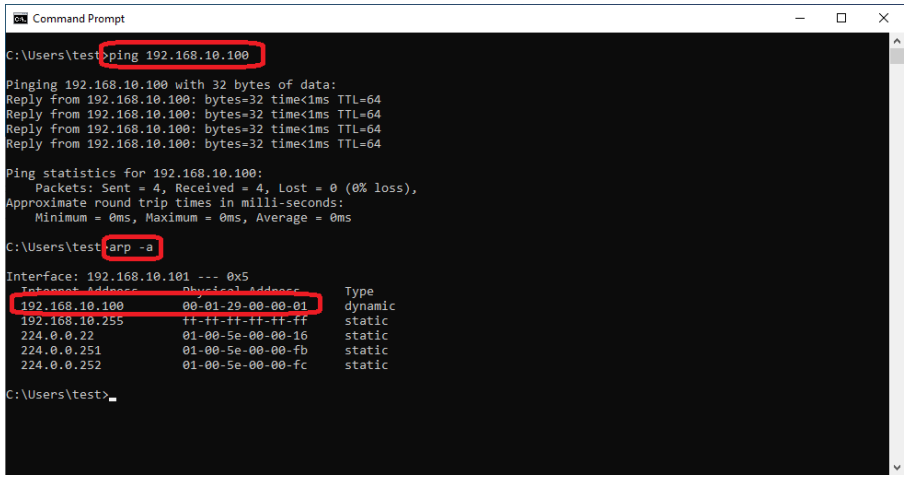
For every system recovery of M2A-OOB, please follow the instruction below.

Once the green LED is on, press and hold the recovery key within 15 seconds.
The green LED light starts blinking for a few seconds until the light stays back on.
The recovery action is completed.

▶ Default Password Setting

Step 1:

The default password can be obtained through the "ping" and "arp -a" commands.



After entering **ping OOB IP address** and execute **"arp -a"** commands, the screen will show OOB MAC address.

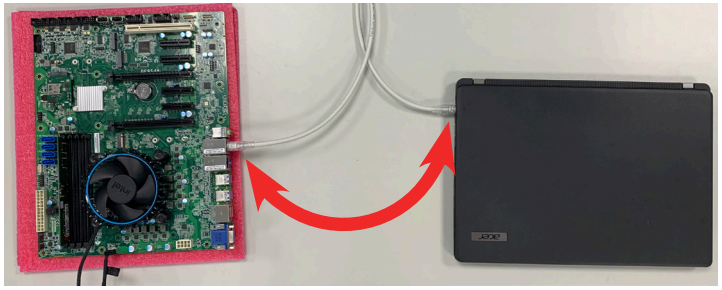
The default password is **OOB MAC address -1**. If there are letters from A to F, make sure they are all uppercase letters.

For example 1: 000129000001-1 --> 000129000000

For example 2: 000129110000-1 --> 00012910FFFF

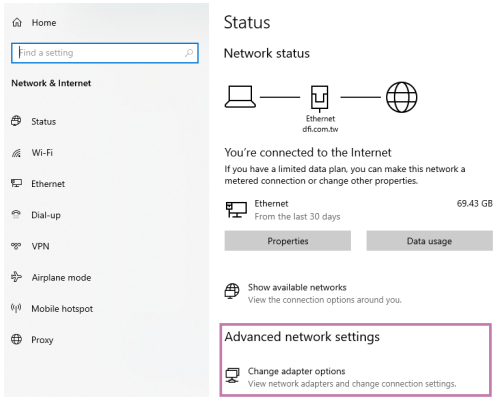
Step 2:

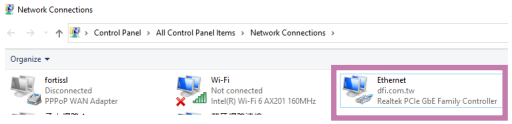
Use a LAN cable to connect a LAN port on PC and a LAN port (i210) on the board.



Step 3: ***(Please note that this setup is only required for the first time use.)***

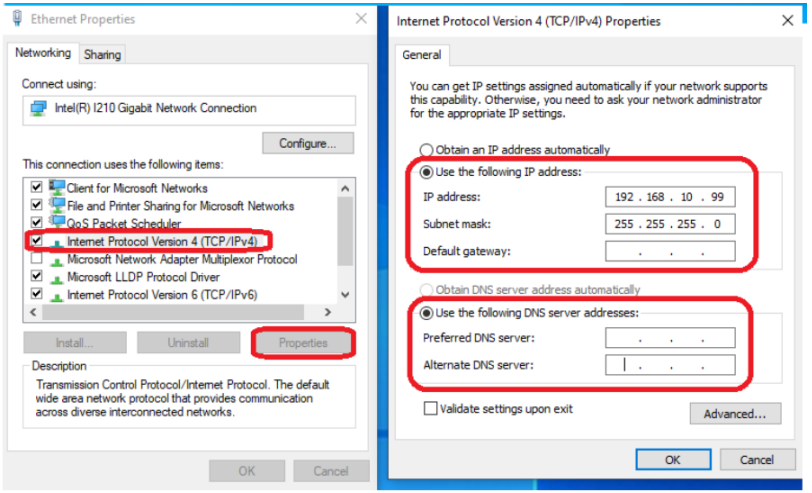
Setup Lan IP Address - Open **Network Status** go to **Advanced network settings** and click **Change adapter options,** double click **Ethernet.**





Click **Priorities** - Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Priorities.**
Type in the following information, then press **OK**.

IP address: 192.168.10.99
Subnet mask: 255.255.255.0



Note:

Remote PC and DFI system shall be in the same network domain.

Step 4:

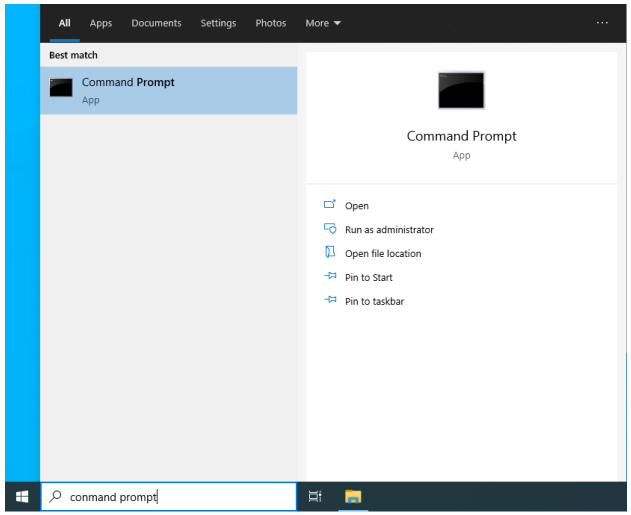
Execute windows Command Prompt.

To run the command prompt:

■ Pressing Windows key + R key to open "Run" box. Type "cmd" and then click "OK".

Or

■ Using the search bar in the Windows 10, type “cmd” into the search bar and press enter.



Open SSH login

Please obtain a default password before logging in, and type in the information as follows:

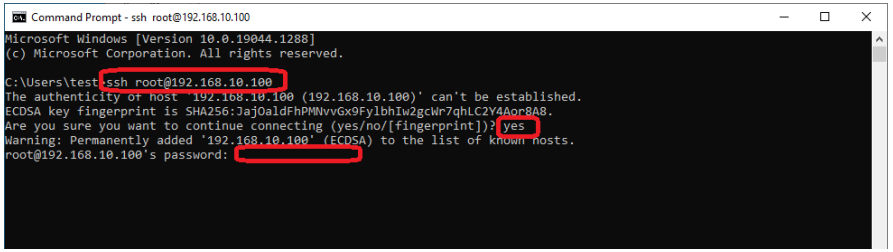
C:\users\user name> : ssh root@192.168.10.100

Are you sure you want to continue connecting : yes
(This question only appears for the first time login.)

Please go to the next page for how to use SSH key pair to log in without entering a password.

Note:

For creating a default password, please refer to Default Password Setting - Step 1.



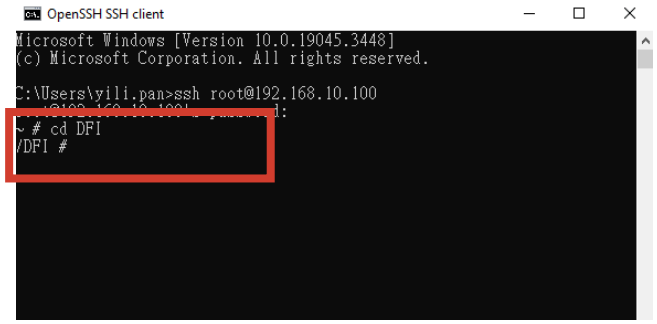
Note:

When you enter a default password in Command Prompt, it doesn't appear or show up on the screen.

After entering the password, you will see **~#**

Then type in **cd DFI**.

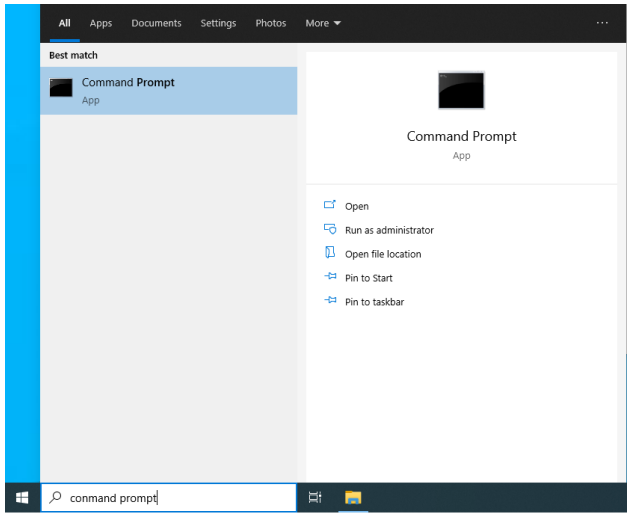
When it displays **/DFI #**, you may now start typing in commands for each function.



Change Password

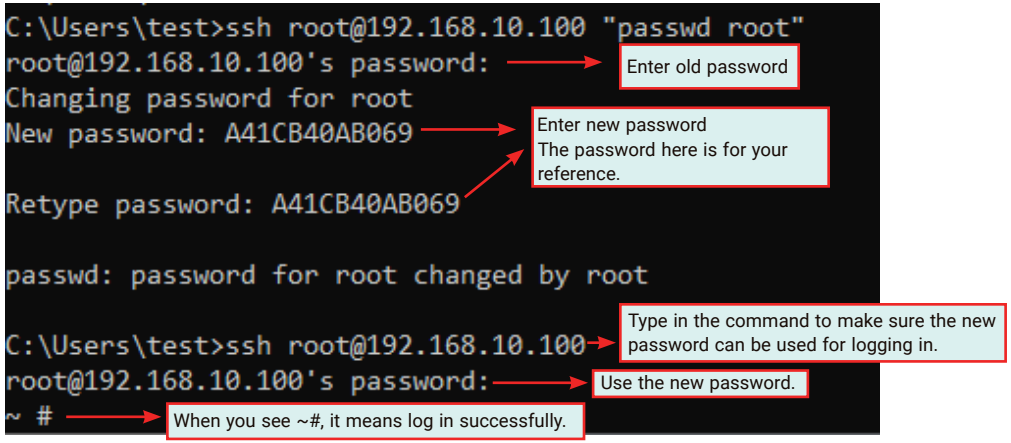
To change the default password, please follow the instructions below.
Please make sure to log out OOB before changing the password.

Step 1:
Execute windows Command Prompt.
To run the command prompt:
■ Pressing Windows key + R key to open "Run" box. Type "cmd" and then click "OK".
Or
■ Using the search bar in the Windows 10, type “cmd” into the search bar and press enter.



Step 2:
Enter the command below.

Shell Script : **ssh root@192.168.10.100 "passwd root"**



Use SSH key Pair Login

Step 1:

Execute windows Command Prompt.

To run the command prompt:

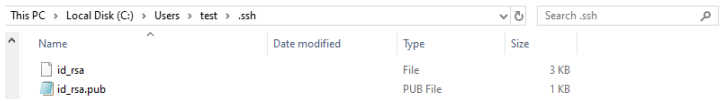
■ Pressing Windows key + R key to open "Run" box. Type "cmd" and then click "OK".

Or

■ Using the search bar in the Windows 10, type “cmd” into the search bar and press enter.

Please enter the command as follows: **C:\users\user name> : ssh-keygen**

The file will be saved in **C:\users\user name\.ssh** folder.



Step 2:

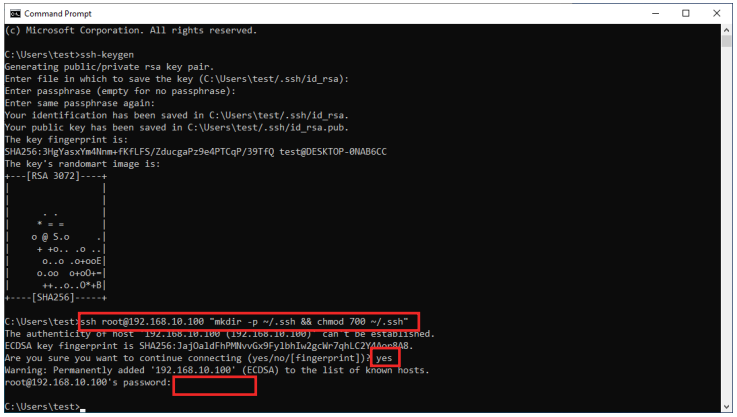
Please obtain a default password before logging in, and type in the information as follows:

C:\users\user name> : ssh root@192.168.10.100 "mkdir -p ~/.ssh && chmod 700 ~/.ssh"

Are you sure you want to continue connecting : yes
(This question only appears for the first time log in)

Note:

- For creating a default password, please refer to Default Password Setting - Step 1.
- When you enter a default password in Command Prompt, it doesn't appear or show up on the screen.



Step 3:

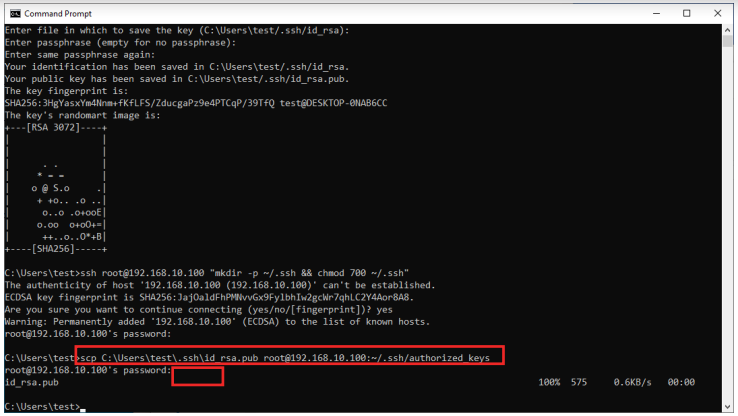
Please enter the command as follows:

scp C:\Users\test\.ssh\id_rsa.pub root@192.168.10.100:~/.ssh/authorized_keys

And then enter the password.

Note:

- For creating a default password, please refer to Default Password Setting - Step 1.
- When you enter a default password in Command Prompt, it doesn't appear or show up on the screen.

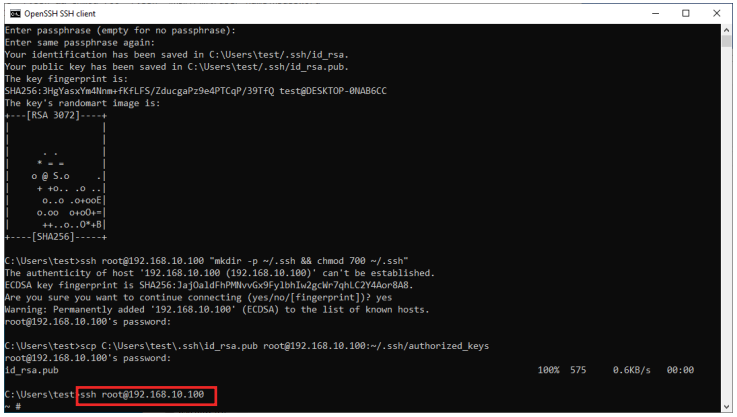


Step 4:

Please enter the command as follows: **ssh root@192.168.10.100**

It will log in automatically, no need to enter any password.

And then you will see **~#**



- **Use SSH key Pair Login - Change A Path and Create A Filename**

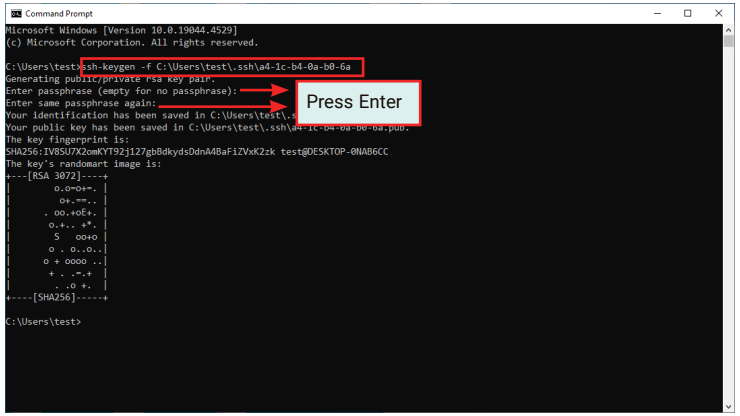
You can also type in a path location where you want to save the file and create a file name.

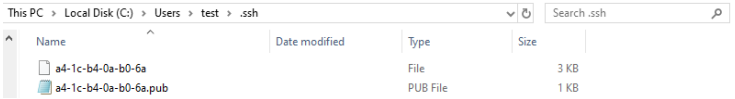
For example :

Please enter the command as follows: **ssh-keygen -f C:\Users\test\.ssh\a4-1c-b4-0a-b0-6a**

The file will be located in **C:\users\test folder**.

The file name is **a4-1c-b4-0a-b0-6a**.





Step 1:

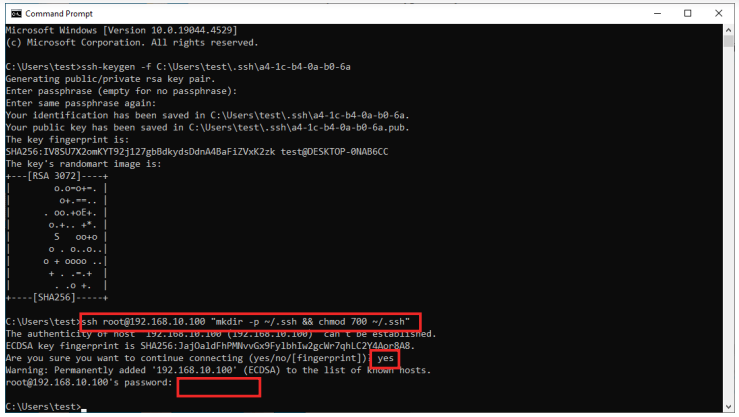
Please obtain a default password before logging in, and type in the information as follows:

C:\users\user name> : ssh root@192.168.10.100 "mkdir -p ~/.ssh && chmod 700 ~/.ssh"

Are you sure you want to continue connecting : yes
(This question only appears for the first time log in)

Note:

- For creating a default password, please refer to Default Password Setting - Step 1.
- When you enter a default password in Command Prompt, it doesn't appear or show up on the screen.



Step 2:

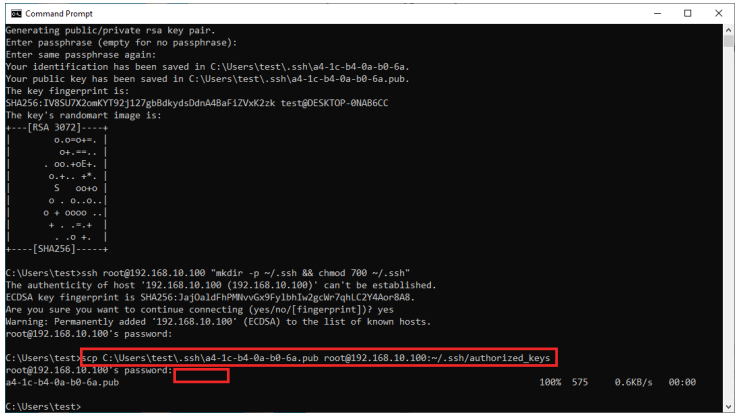
Please enter the command as follows:

scp C:\Users\test\.ssh\a4-1c-b4-0a-b0-6a. pub root@192.168.10.100:~/.ssh/authorized_keys

And then enter the password.

Note:

- For creating a default password, please refer to Default Password Setting - Step 1.
- When you enter a default password in Command Prompt, it doesn't appear or show up on the screen.

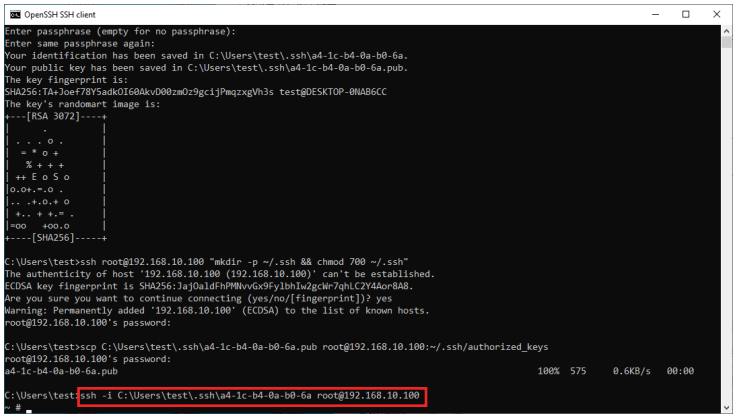


Step 3:

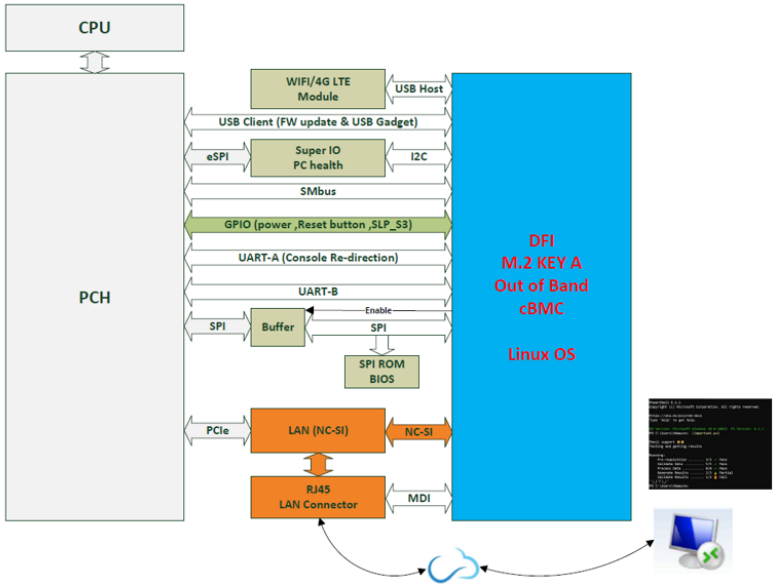
Please enter the command as follows:
ssh -i C:\Users\test\.ssh\a4-1c-b4-0a-b0-6a root@192.168.10.100

It will log in automatically, no need to enter any password.

And then you will see **~#**



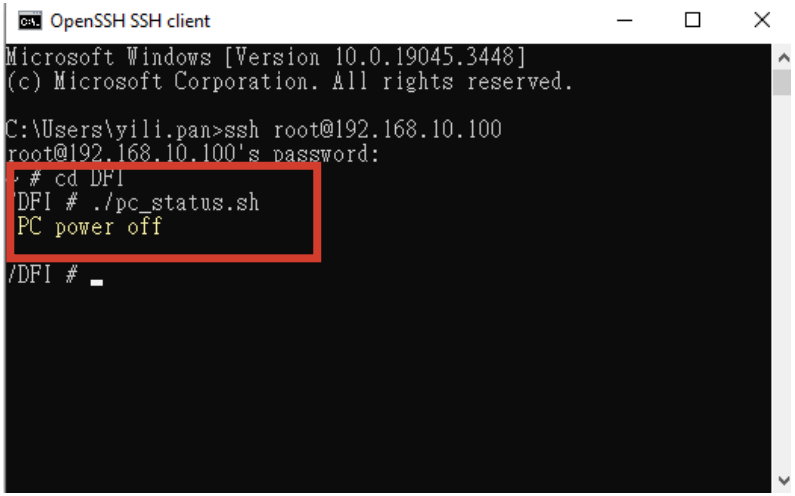
▶ Remote Control PC Power On/Off



PC Power On/Off Status Check

Please complete Default Password Setting - Step 4 before entering the following command.
Check the current power On/Off status remotely by typing in following command.

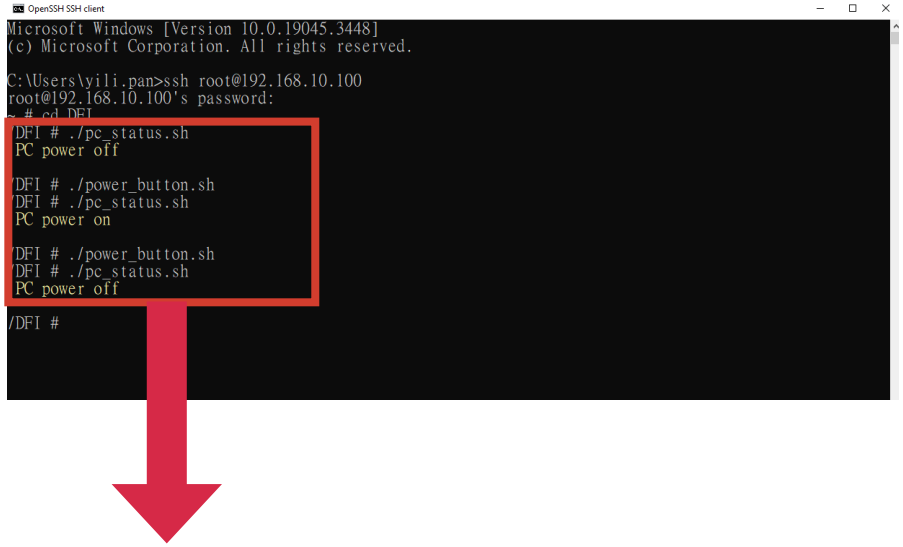
Shell Script : **./pc_status.sh**



Turn On/Off PC Remotely

After the status check, you can control PC power on/off remotely.
Please complete Default Password Setting - Step 4 before entering the following command.
To toggle power on or power off, just type in the same command again.

Shell Script : **./power_button.sh**

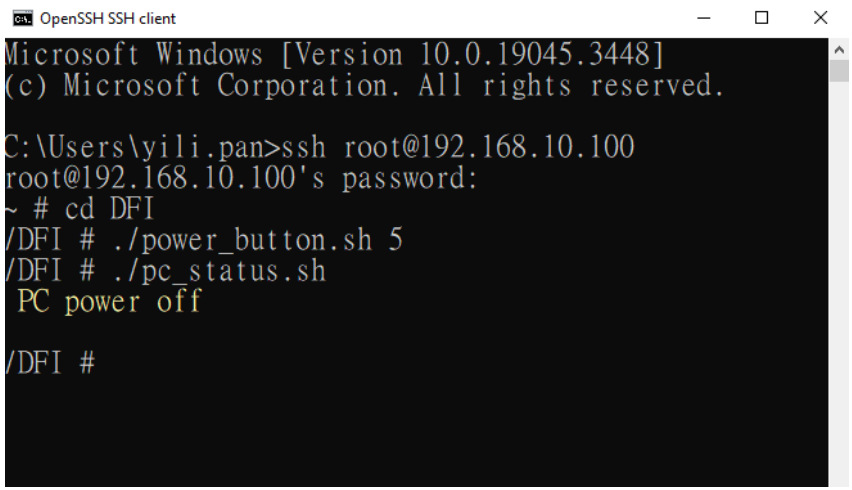


1. Check the PC power on/off status to make sure the current power status.
2. Type in shell script: **./power_button.sh** to power on or power off the PC.
3. Then check the staus again.

Perform a Timed Force Shutdown

To forcibly shut down the PC, please type in the following command.
Please complete Default Password Setting - Step 4 before entering the following command.
Numbers means this will force shutdown your PC in xx seconds (waiting time).
Setting it to 5 will shutdown your PC after 5 seconds.

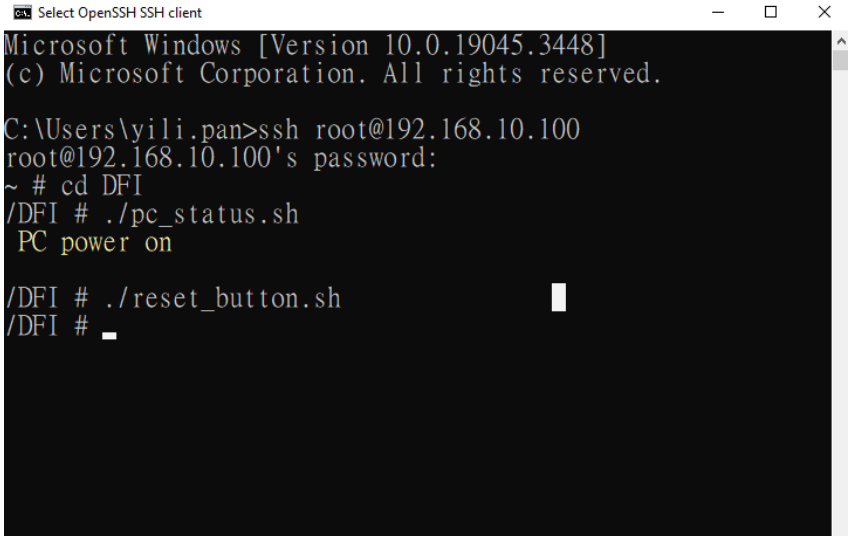
Shell Script : **./power_button.sh 5**



PC Rebooting

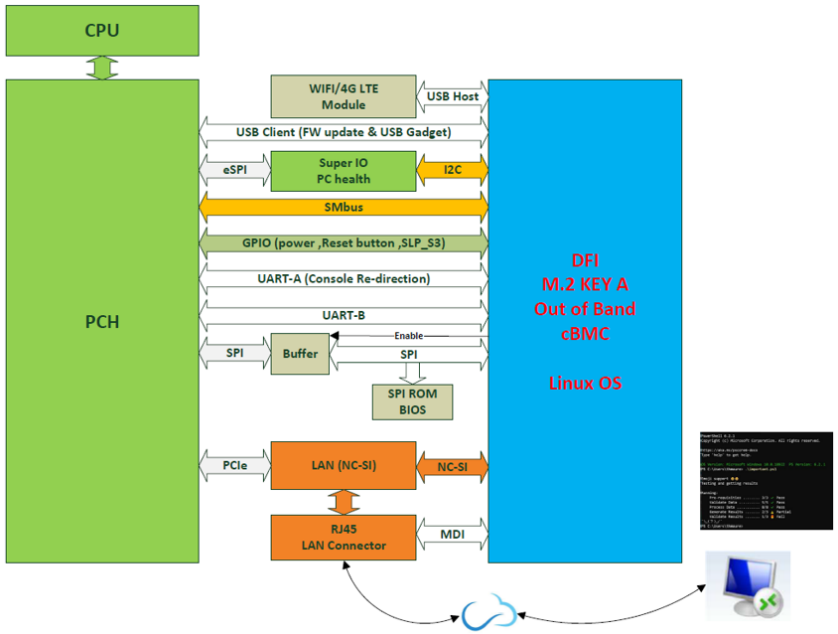
To reboot the PC, please type in the following command.
You will hear a single beep, it means PC rebooted successfully.
Please complete Default Password Setting - Step 4 before entering the following command.

Shell Script : **./reset_button.sh**



▶ Remote Hardware Monitor Log (Super I/O)

I2C bus:
Super I/O: Voltage, Temperature, Fan Speed
PCH: CPU Temperature



Super I/O Log

To start/stop super I/O log, please type in the following commands.
Please complete Default Password Setting - Step 4 before entering the following command.

To start super I/O log:
Shell Script : **./sio_start_log.sh YYYY-MM-DD hh:mm:ss hours /DFI/sio_log &**
For example: ./sio_start_log.sh 2024-05-24 09:00:00:00 24 /DFI/sio_log &
Make sure to add the ampersand "&" at the end to run in the background.

```
/DFI # ./sio_start_log.sh 2024-05-24 09:00:00 24 /DFI/sio_log &
/DFI # Fri May 24 09:00:00 UTC 2024
Save Path=/DFI/sio_log
Start log ......


/DFI #
```

To stop super I/O log:
Shell Script : **./sio_stop_log.sh**

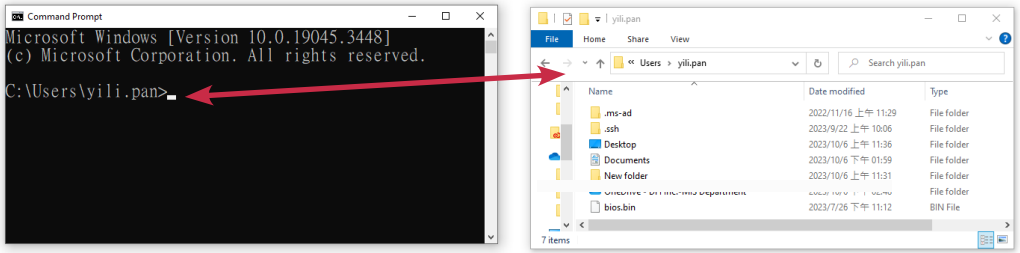
```
/DFI # ./sio_stop_log.sh

=== DFI OOB ===
1]+  Terminated              ./sio_start_log.sh 2024-05-24 09:00:00 24 /DFI/sio_log
/DFI #
```

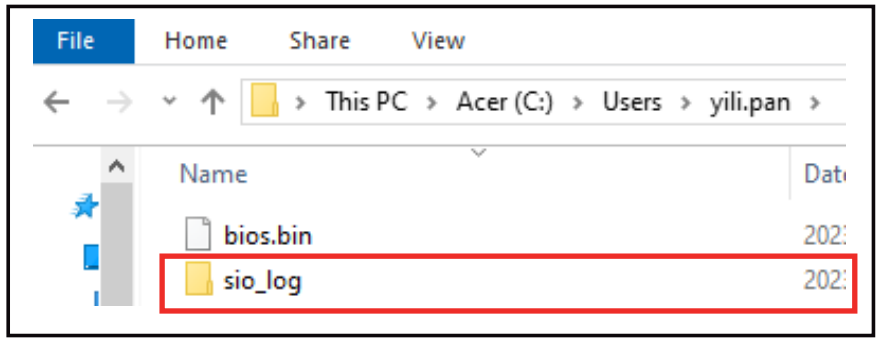
How to Export Super I/O Logs From OOB

To export super I/O log, please type in the following command.
Please complete Default Password Setting - Step 4 before entering the following command.

Shell Script : **scp -r root@192.168.10.100:/DFI/sio_log C:\Users\username\.ssh**
For example: scp -r root@192.168.10.100:/DFI/sio_log C:\Users\yili.pan\.ssh



The log file is saved in C drive.



▶ Using USB Storage / MicroSD Card to run actions

The shell scripts for USB storage

Please execute the following commands to switch between the USB flash drive and the microSD card for the device operations.

To insert a USB flash drive, please execute a shell script as following:
Shell Script : **./insert_usb_storage.sh**

To remove a USB flash drive, please execute a shell script as following:
Shell Script : **./eject_usb_storage.sh**

To format a USB flash drive to factory settings, please execute a shell script as following:
Shell Script : **./format_usb_storage.sh**

If file operations are performed via a USB flash drive under OOB, need to refresh windows to update. To update a USB flash drive, please execute a shell script as following:
Shell Script : **./refresh_usb_storage.sh**

The shell scripts for MicroSD card

Please format your MicroSD card to FAT32 before executing any commands, and then insert it into the OOB MicroSD card slot.

There are two ways to format a MicroSD card :

1. You can format a microSD card using your Windows computer. Make sure that once you have formatted, your card will be formatted to FAT32 filesystem type.
2. You can format a micro SD card using commands.

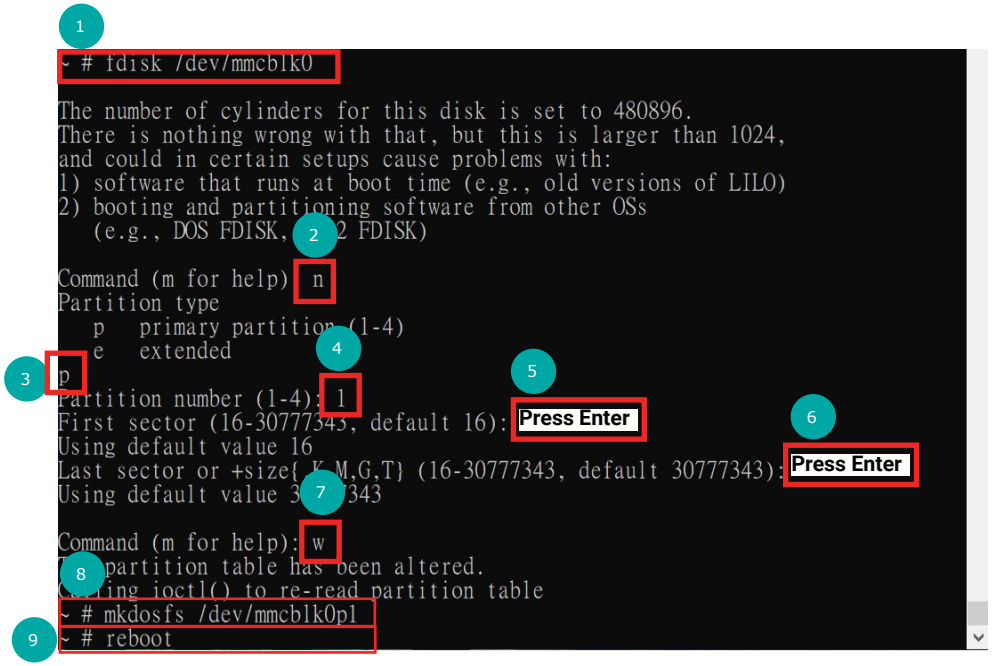
Formatting a microSD Card under OOB

Please format a MicroSD card before using it to log in OOB.

What are the situations do you need to format a MicroSD card :

- A brand new MicroSD card.
- Your MicorSD card is not formatted as FAT32.

The instructions are as follows :



1. Type in **fdisk /dev/mmcblk0**
2. Choose : **n** (a lowercase letter)
3. Choose : **p** (a lowercase letter)
4. Choose : **1**
5. Press enter
6. Press enter
7. Choose : **w** (a lowercase letter)
8. Type in **mkdosfs /dev/mmcblk0p1**
9. Type in **reboot**

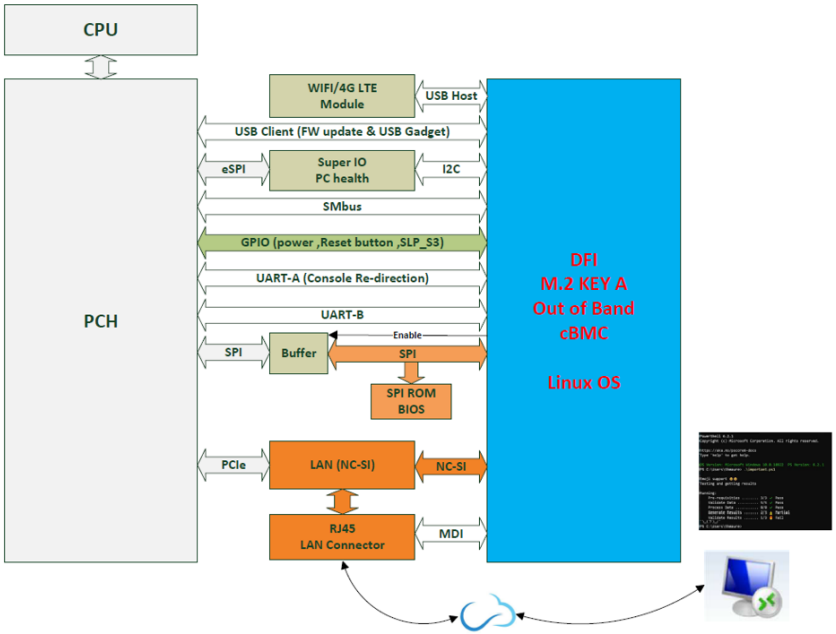
To insert a MicroSD card, please execute a shell script as following:
Shell Script : **./insert_uSD.sh /dev/mmcblk0p1**

To remove a MicroSD card, please execute a shell script as following:
Shell Script : **./eject_uSD.sh**

If file operations are performed via a MicroSD card under OOB, need to refresh windows to update. To update a USB flash drive, please execute a shell script as following:
Shell Script : **./refresh_uSD.sh /dev/mmcblk0p1**

Chapter 3 - BIOS

▶ Remote BIOS Update



Step 1:

Before starting the update, you will have to prepare **BIOS bin file**.

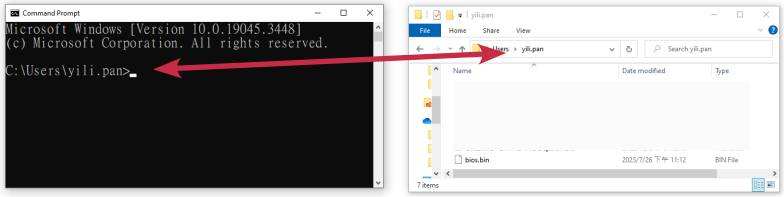
BIOS bin file *(Every BIOS file has a different file name to be used as a command, please enter the file name accordingly.)*

How to request to obtain the files and update BIOS, please watch the video below for more information:

https://www.dfi.com/tw/knowledge/video/5

Step 2:

Copy BIOS bin file to its corresponding users folder in C drive.



Step 3:

Open command prompt and type in the command below.

Every BIOS file has a different file name used as a command, please enter the file name accordingly.

Shell Script : **scp bios.bin file name root@192.168.10.100:~/DFI/bios/**

For example:

BIOS file name : B246.18A

Shell Script : scp B246.18A root@192.168.10.100:~/DFI/bios/

```
C:\Users\test>scp B246.18A root@192.168.10.100:~/DFI/bios/
```

Please enter a default password.

root@192.168.10.100's password:

Note:

For creating a default password, please refer to *Default Password Setting - Step 1*.

Refresh DFI USB storage to notify windows

Shell Script : **ssh root@192.168.10.100 ./DFI/refresh_usb_storage.sh**

```
C:\Users\test>ssh root@192.168.10.100 ./DFI/refresh_usb_storage.sh
root@192.168.10.100's password:

=== DFI OOB ===

C:\Users\test>
```

Step 4:

Run SSH command:

Please type in the information as follows:

C:\users\user name> : ssh root@192.168.10.100

Are you sure you want to continue connecting : yes
(This question only appears for the first time log in)

root@192.168.10.100's password:

For creating a default password, please refer to *Default Password Setting - Step 1*.

After entering the password, you will see **~#** Then type in **cd /DFI/bios/**

Step 5:

For the next step, you will have to shut down the PC if the power is still on.

To turn off the pc, enter **cd ..** to go back one level.

Type in **./power_button.sh** to execute shutdown.

Then type in **cd bios/**

and the final step, type in **/DFI/bios #./update_bios.sh BIOS bin file name** to begin the BIOS update.

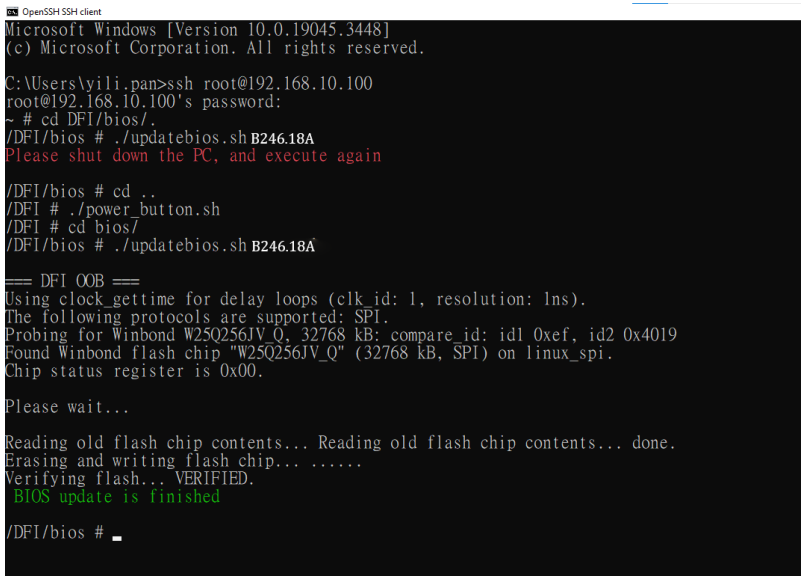
Enter the following command to start updating BIOS:

Shell Script : **./updatebios.sh bios bin file name**

For example:

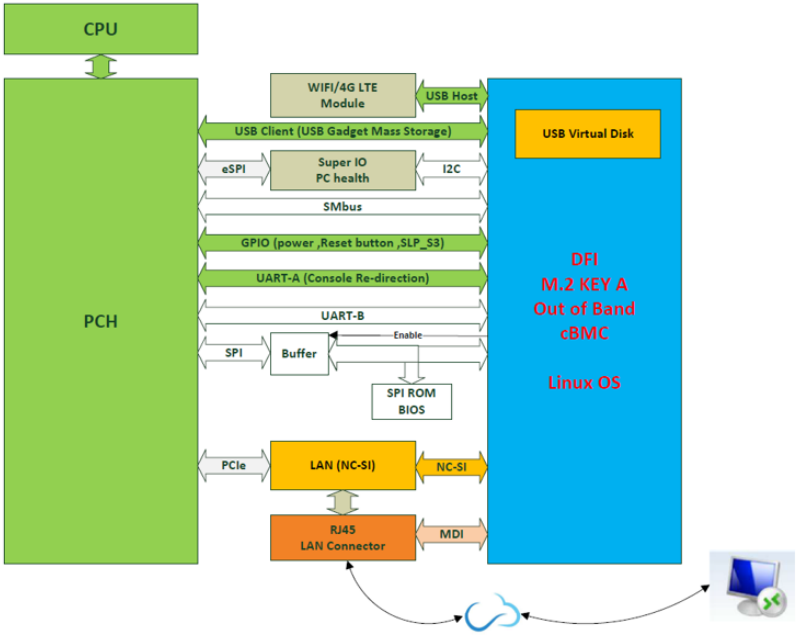
BIOS file name : B246.18A

Shell Script : ./updatebios.sh B246.18A

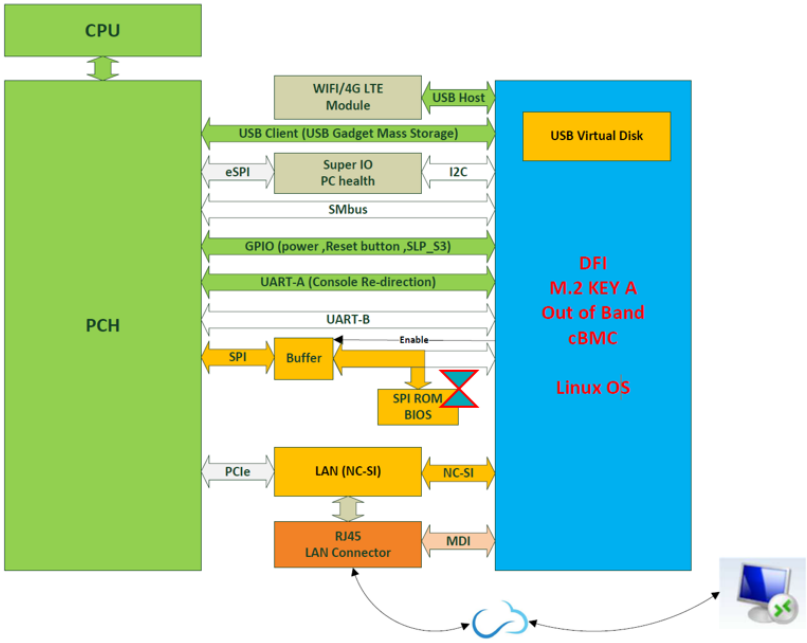


▶ Remote BIOS Update (Via Teraterm)

- **Remote BIOS Setup & UEFI shell (Serial Over Lan)**



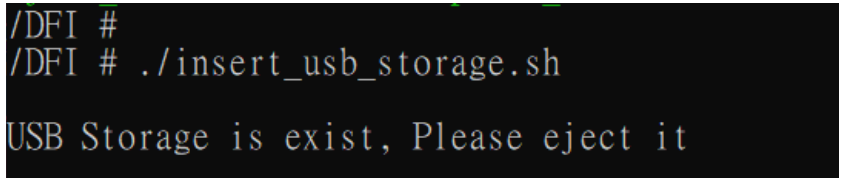
- **Remote BIOS Update (SOL & DFI USB-Storage)**



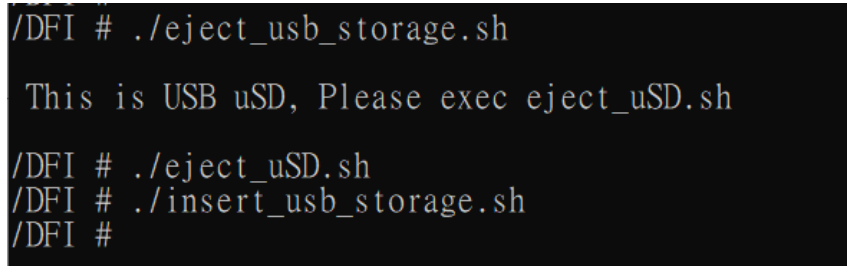
▶ Check BIOS Set Up from USB Storage

Before starting BIOS update, please make sure the BIOS set up is on USB storage.

To check BIOS set up, please execute a shell script as following:
Shell Script : **./insert_usb_storage.sh**
If BIOS set up is on USB storage, it shows **USB Storage is exist, Please eject it.**



If BIOS set up is on MircoSD, it shows **This is USB uSD, Please execute eject_uSD.sh.**
and execute **./eject_uSD.sh**
and then execute **./insert_usb_storage.sh**



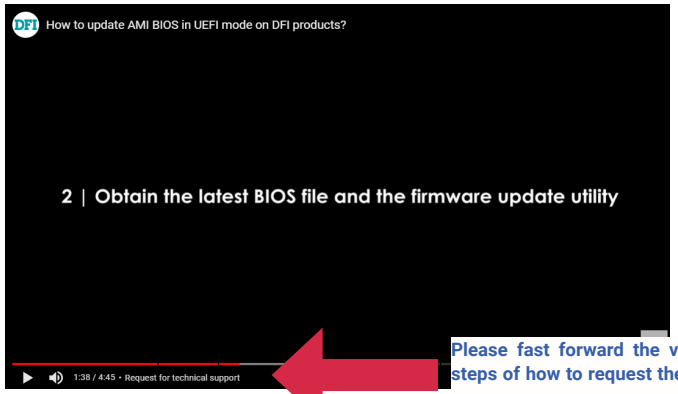
Step 1:

Before starting the update, you will have to prepare two files:

1. AfuEfiU64.efi

2. BIOS bin file

How to request to obtain the files and update BIOS, please watch the video below for more information:
https://www.dfi.com/tw/knowledge/video/5



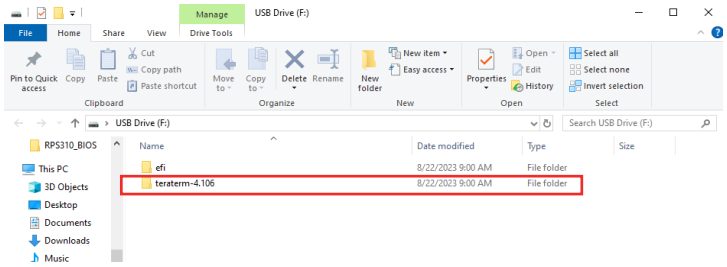
Please fast forward the video to 1:31 and follow the steps of how to request the BIOS files from DFI.

Step 2:

TeraTerm is already included in the DFI system.

After successfully booting to OOB, you will see a USB flash drive in the DFI system.

Please copy the teraterm folder from the USB flash drive to the computer where you want to operate the OOB.



Go to Teraterm folder and open **telnet.bat.**
Press "**ESC**" key ,when system power on.

Run SSH command:

Please type in the information as follows:

- Copy BIOS from local PC to remote OOB module

scp AfuEfiU64.efi root@192.168.10.100:~/DFI/USB/files
scp bios.bin file name root@192.168.10.100:~/DFI/USB/files

Shell Script : **scp bios.bin file name root@192.168.10.100:~/DFI/USB/files**

For example:
BIOS file name : B246.18A
Shell Script : scp B246.18A root@192.168.10.100:~/DFI/USB/files

Shell Script : **scp AfuEfiU64.efi root@192.168.10.100:~/DFI/USB/files**

```
C:\Users\test>scp B246.18A root@192.168.10.100:/DFI/USB/files
root@192.168.10.100's password:
B246.18A                                      100%   32MB 953.4KB/s   00:34

C:\Users\test>scp AfuEfiU64.efi root@192.168.10.100:/DFI/USB/files
root@192.168.10.100's password:
AfuEfiU64.efi                                 100%  606KB 554.6KB/s   00:01

C:\Users\test>
```

Refresh DFI USB storage to notify windows

```
C:\Users\test>ssh root@192.168.10.100 ./DFI/refresh_usb_storage.sh
root@192.168.10.100's password:

=== DFI OOB ===

C:\Users\test>
```

- How to Access BIOS Setup Menu When Power on

If the DFI system is power on which installed OOB, executing **power_button.sh** script to off/on the system. The script must be executed twice, first is for powering off the system, second is for powering on the system.

After the first execution, check if the system status is power off, then proceed with the second execution to be able to enter BIOS setup menu.

For the baud rate setting change, please input the shell script below to choose from 115200 or 921600. Make sure the baud rate setting from BIOS console redirection is matched.

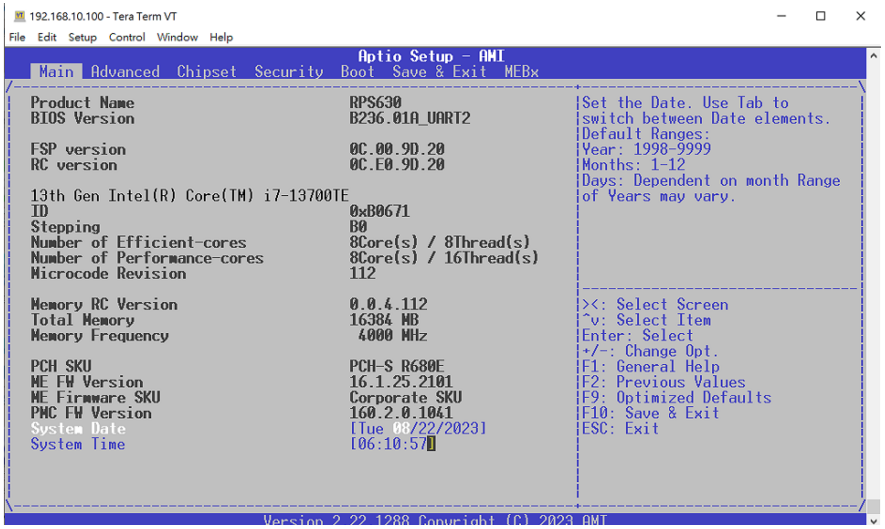
Shell Script : **./setbaudrate.sh**
For example:
baud rate : 921600
Shell Script : ./setbaudrate.sh 921600

```
~ #
~ # cd DFI/
/DFI # ./setbaudrate.sh 921600
/DFI #
```

Step 3:

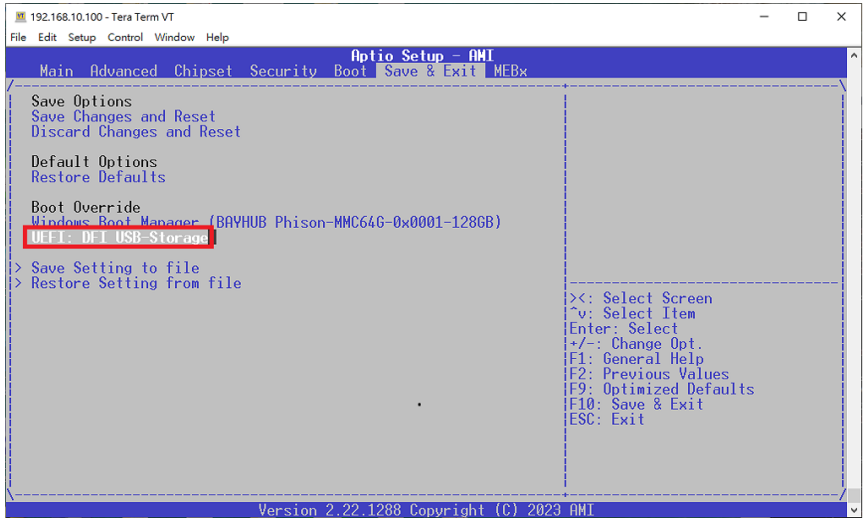
Access BIOS setup menu.

When system power is on, press "ESC" key in the teraterm window.



Boot from DFI USB-Storage device &Update BIOS in uefi mode.

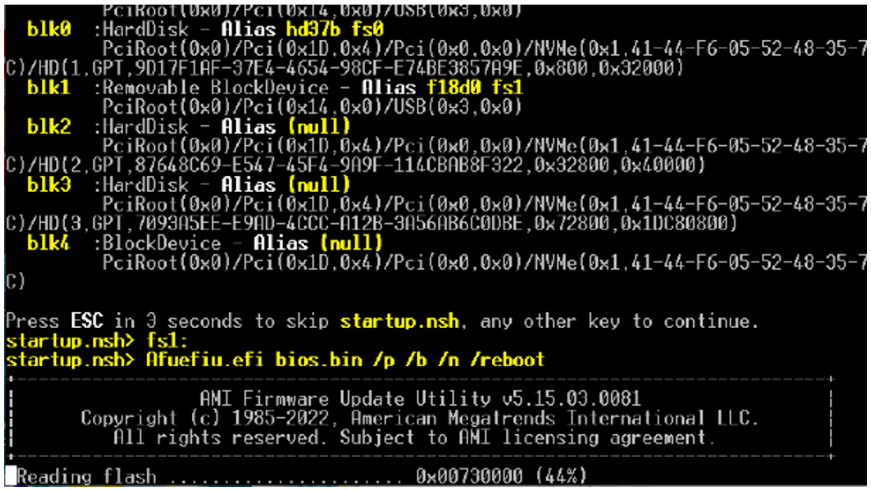
Use arrow key to select **Save & Exit ---> UEFI: DFI USB-Storage**



Step 4:

Please contact technical support or your sales representative for the files and specific instructions about how to update BIOS with the flash utility.

When there is no error message displayed, the BIOS update will be completed successfully.



Chapter 4 - OOB IP Address Change

▶ SSH

Step 1:
Execute windows Command Prompt.
To run the command prompt:
■ Pressing Windows key + R key to open "Run" box. Type "cmd" and then click "OK".
Or
■ Using the search bar in the Windows 10, type “cmd” into the search bar and press enter.

Typing in following command and you will see a message to ask for a new IP address.

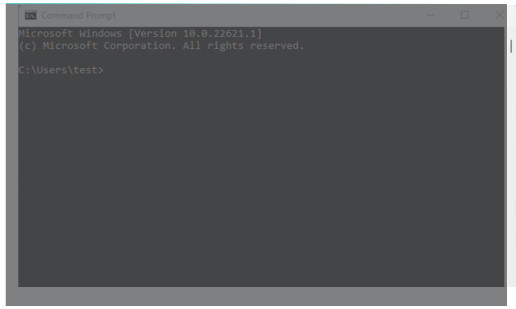
(For example: 192.168.10.88)

Shell Script : **ssh root@192.168.10.100 ./DFI/ipconfig.sh**

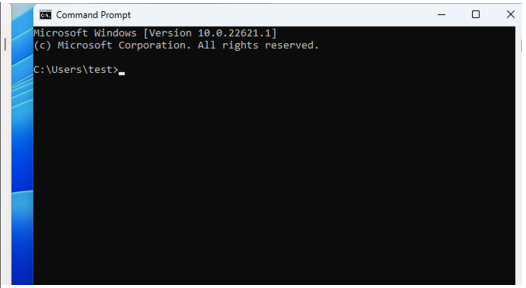
```
C:\Users\test>ssh root@192.168.10.100 ./DFI/ipconfig.sh
root@192.168.10.100's password:
 [1;33m Please input IP address  [0m

192.168.10.88
```

Press Enter and close the current window since it is frozen and unable to operate.
Please open a new window to login new IP address and run command prompts.
After the network changes, make sure it should be in the same network domain as OOB.



Close a frozen window →



Open a new window to run command prompts with new IP address.

Step 2:
In the new command prompts window, login to OOB with SSH
ssh root@(Input new IP address)

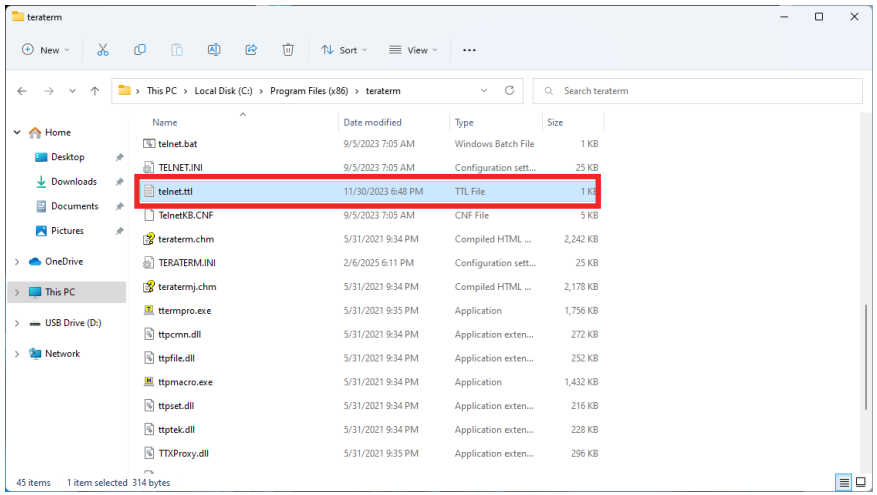
Shell Script : **ssh root@192.168.10.88**

```
C:\Users\test>ssh root@192.168.10.88
The authenticity of host '192.168.10.88 (192.168.10.88)' can't be established.
ECDSA key fingerprint is SHA256:JajOaldFhPMNvvGx9Fy1bhIw2gcWr7qhLC2Y4Aor8A8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.88' (ECDSA) to the list of known hosts.
root@192.168.10.88's password:
~ #
```

▶ Console Redirection

Step 1:

After the IP address changes, Console Redirection is unable to run commands.
To fix the problme, please navigate to **C:\Program Files (x86)\teraterm**
to look for a TTL file named '**telnet.ttl**.' This file needs to be modified.
After that, Console Redirection has been updated successfully.



The old IP address

```
show 0
connect '192.168.10.100:50005 /nossh /T=1'
:detpwd
loadkeymap 'TelnetKB.CNF'
wait "Enter Password"
testlink
if result=0 then
  mpause 200
  end
```

Change to the new IP address

```
show 0
connect '192.168.10.88:50005 /nossh /T=1'
:detpwd
loadkeymap 'TelnetKB.CNF'
wait "Enter Password"
testlink
if result=0 then
  mpause 200
  end
endif
loadkeymap 'KEYBOARD.CNF'
```