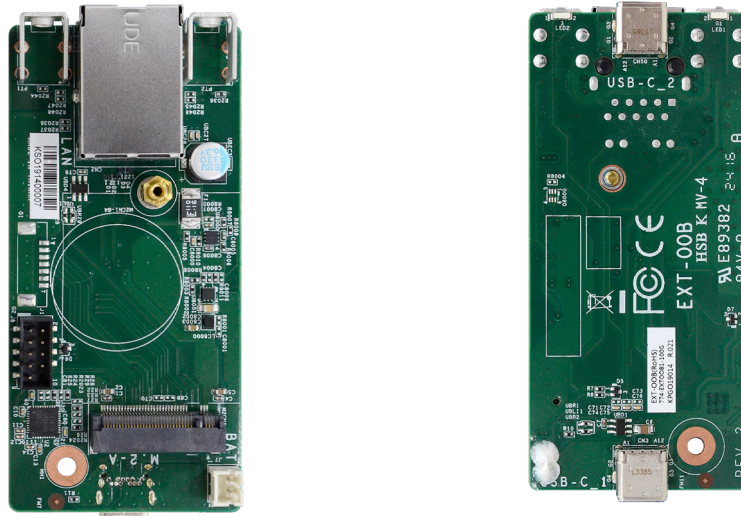




EXT-OOB

EXT 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

Chapter 1 - Introduction.....	5
What's OOB (Out-Of-Band) Management	5
Key Features	5
EXT cBMC	5
Chapter 2 - Getting Started	6
Hardware Requirements	6
System Requirements	6
How To Connect EXT OOB To A Carrier Board.....	9
Pin Assignment	10
SPI Cable (J1).....	10
USB Cable (CN3)	10
Front Panel, COM, I2C (J8)	10
OOB SPI Header	11
OOB I2C Header	11
USB Port.....	11
Front Panel.....	11
COM Port	11
OOB Normal Boot	12
Default Password Setting	12
Remote Control PC Power On/Off	19
PC Power On/Off Status Check	20
Turn On/Off PC Remotely	20
Perform a Timed Force Shutdown.....	21
PC Rebooting	21
Remote Hardware Monitor Log (Super I/O).....	22
Super I/O Log	22
How to Export Super I/O Logs From OOB.....	23
Using USB Storage / MicroSD Card to run actions	24
The shell scripts for USB storage	24
The shell scripts for MicroSD card.....	24
Formatting a microSD Card under OOB.....	24
Chapter 3 - BIOS	25
Remote BIOS Update	25
Remote BIOS Update (Via Teraterm).....	27
Check BIOS Set Up from USB Storage	28
Chapter 4 - OOB IP Address Change.....	31
SSH.....	31
Console Redirection	32

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

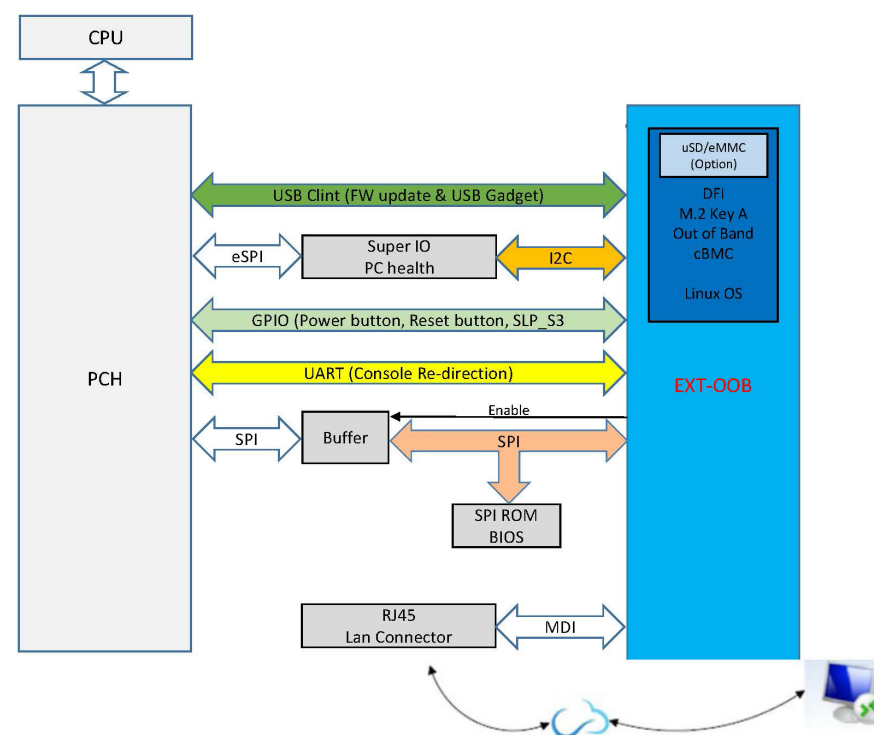
As Industrial IoT demands rise in recent decades, the number of connected IoT devices drastically grow. However, the personnel responsible for equipment maintenance cannot meet the growing numbers of IoT devices; additionally, unexpected factors occur, e.g. the global pandemic. It seems like it is harder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

► EXT cBMC



Chapter 2 - Getting Started

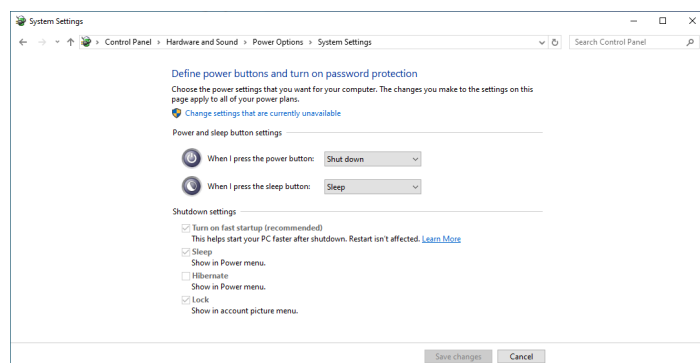
Please follow the steps to configure EXT-OOB.

► 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.



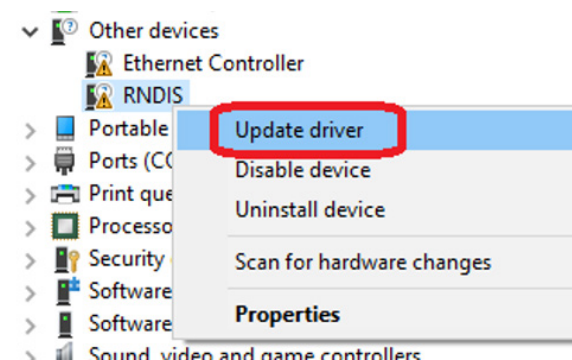
- TeraTerm is already included in the DFI system.

■ Update Driver

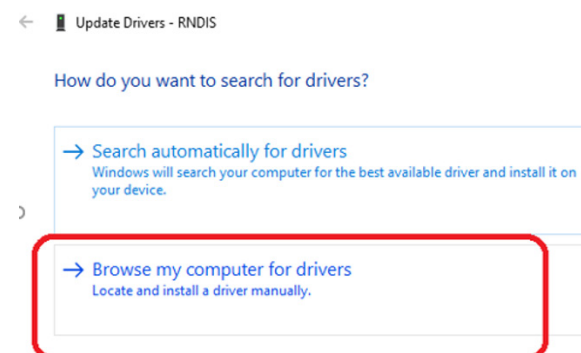
To fix a yellow exclamation mark of an RNDIS USB-enabled device icon on windows device manager, please update RNDIS driver.

The instructions to update driver are as follows:

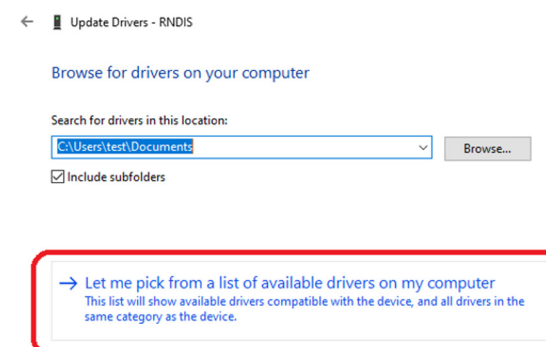
Step 1:



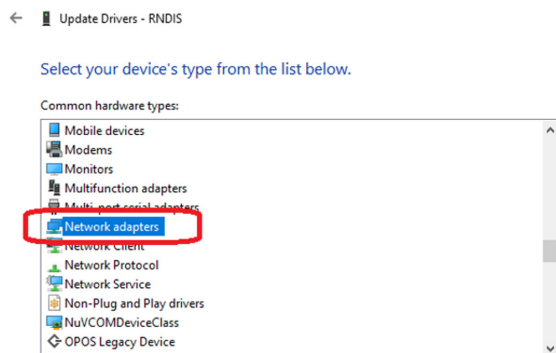
Step 2:



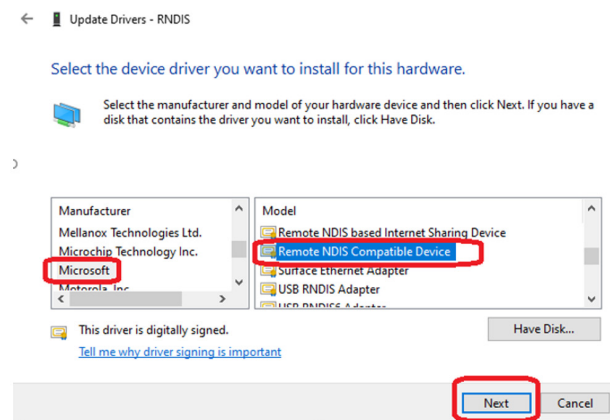
Step 3:



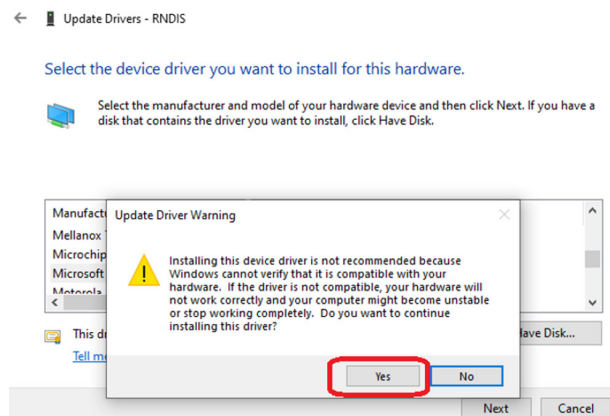
Step 4:



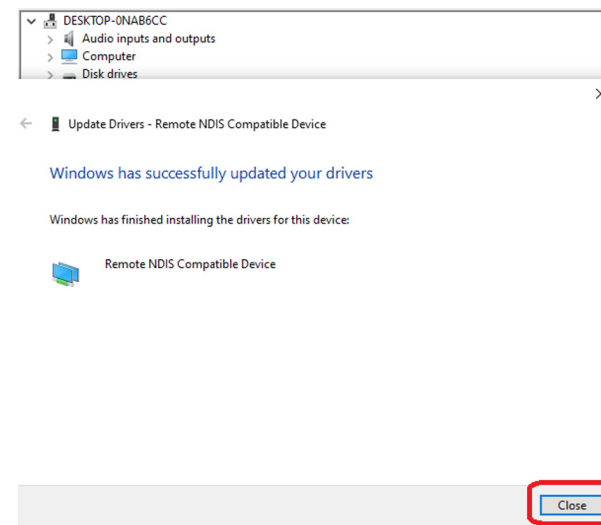
Step 5:



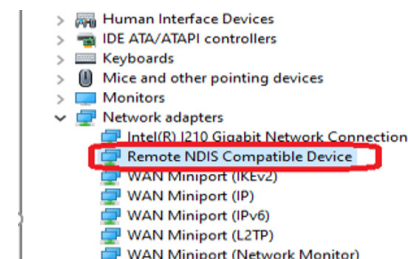
Step 6:



Step 7:



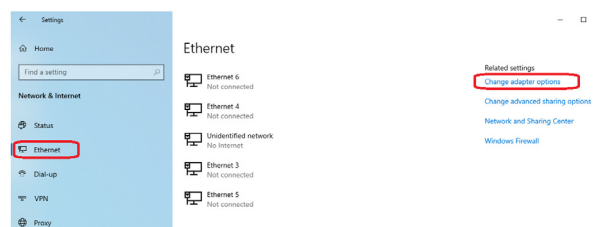
Step 8:



Step 9:

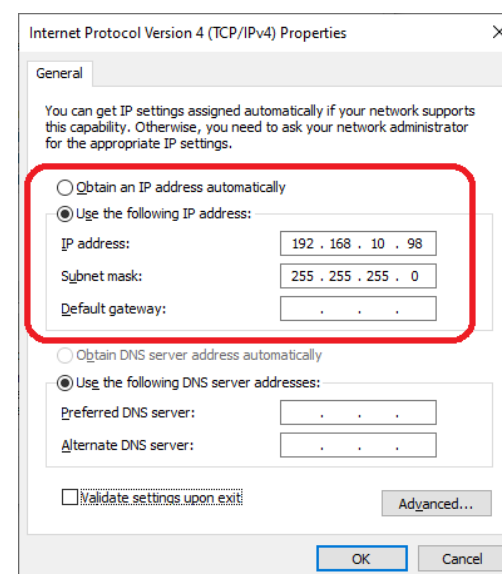
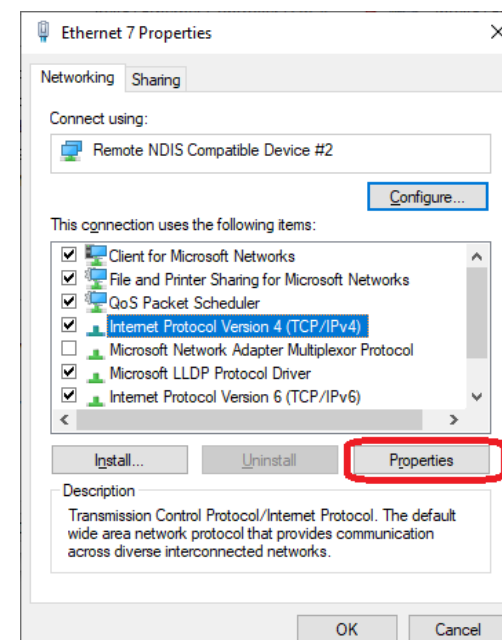
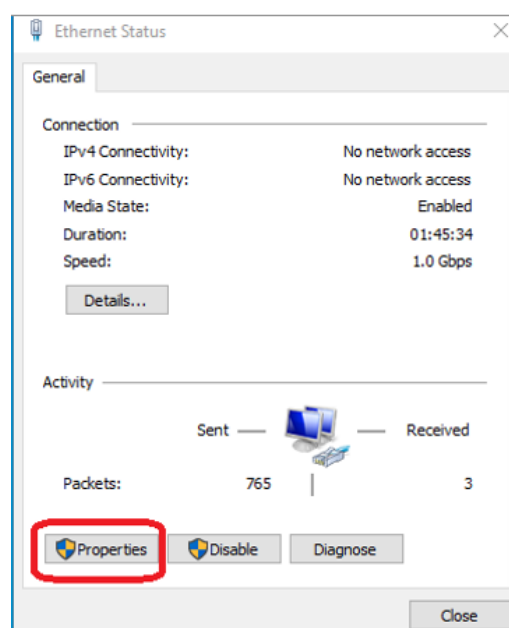
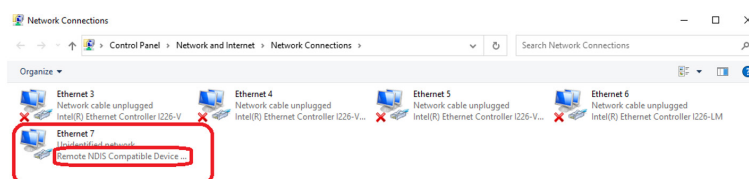
Setup "RNDIS" IP address for windows remote desktop connection

Open Windows Settings → Network & Internet → Ethernet → Change adapter options



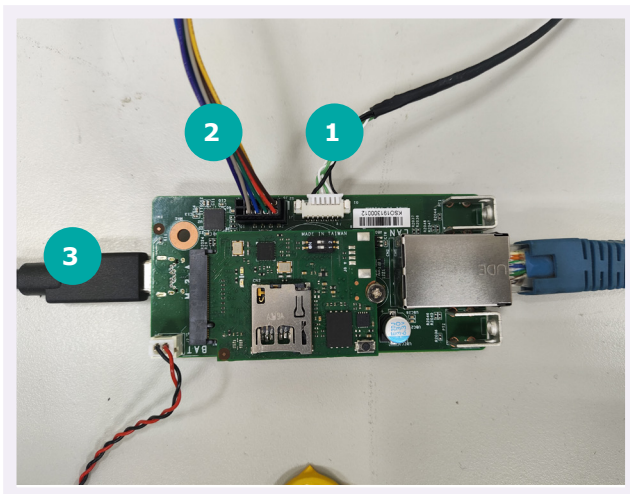
Step 10:

Select "RNDIS" device and change IP



► How To Connect EXT OOB To A Carrier Board

Please follow the corresponding numeral to connect each cable between EXT OOB and a carrier board as pictures shown below.

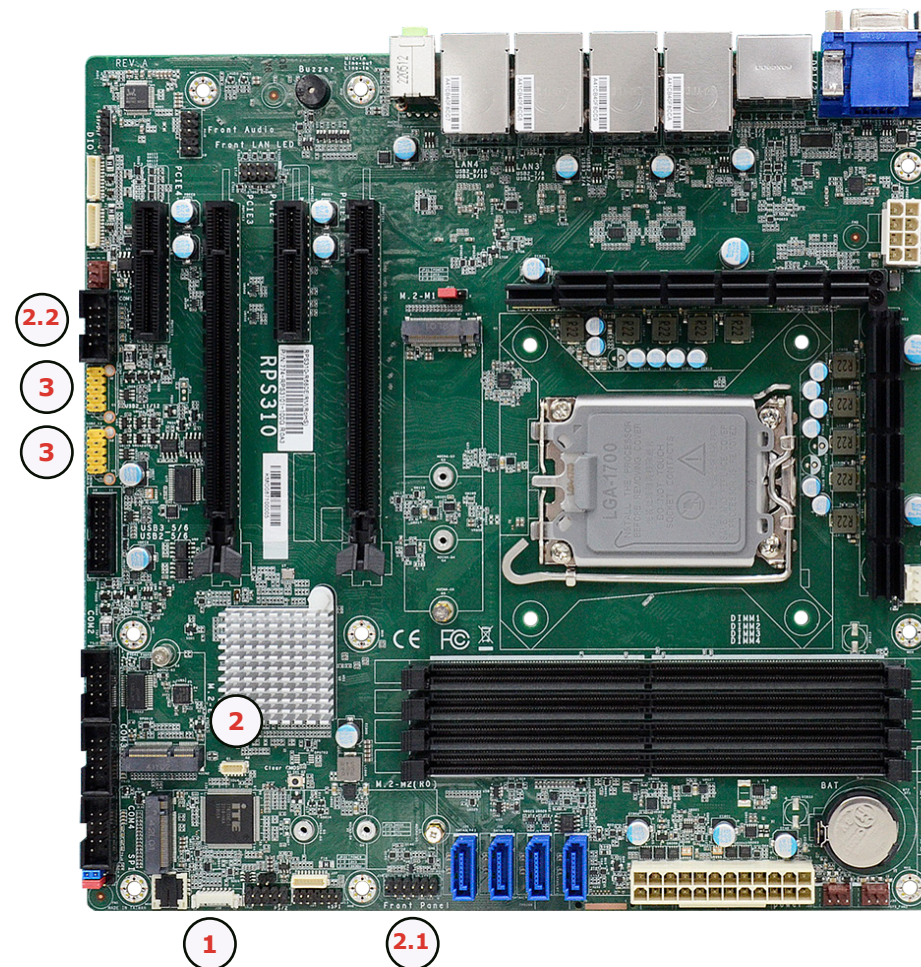


• EXT-OOB

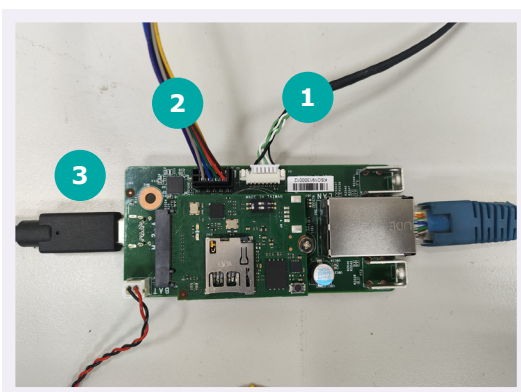
- 1 SPI Cable
- 2 J8 Cable (Front Panel, COM, I2C)
- 3 USB Cable

• microATX Industrial Motherboard : RPS310

- 1 OOB SPI Header
- 2 OOB I2C Header
- 2.1 Front Panel
- 2.2 COM Port
- 3 USB Ports



► Pin Assignment



- 1 SPI cable
- 2 J8 cable (Front Panel, COM. I2C)
- 3 USB Cable

1 ► SPI Cable (J1)

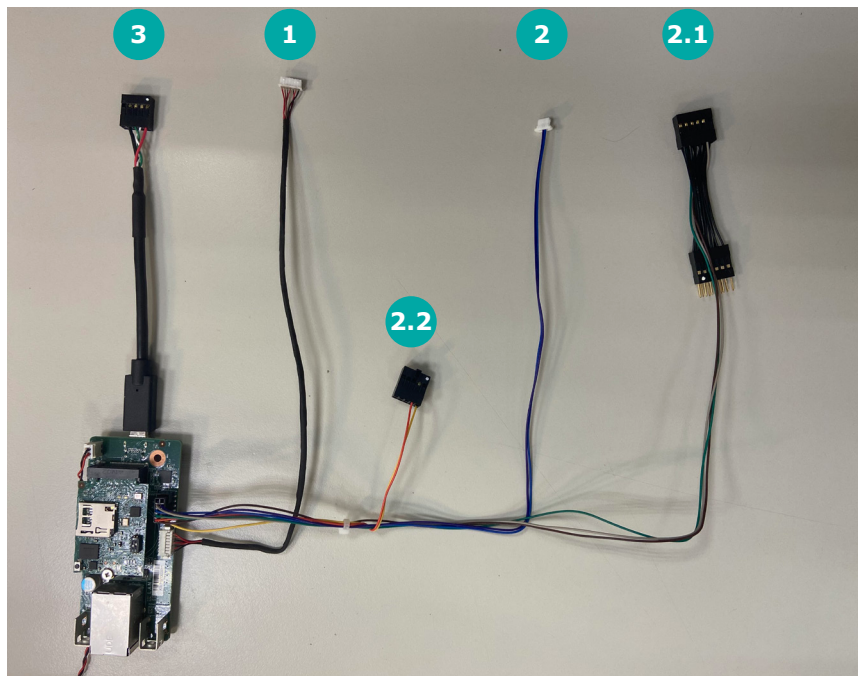
Pin	Assignment
1	GPO_SPI_SW
2	SPI_DO
3	SPI_DI
4	SPI_CLK
5	SPI_SS0
6	GND (Power)
7	SPI_PWR (Power)

2 ► Front Panel, COM. I2C (J8)

Pin	Assignment	Pin	Assignment
1	SYS_RSYS_N	2	UART_RX
3	UART_TX	4	SLP_S3_N
5	GND (Power)	6	I2C0_SDA
7	I2C0_SCL	8	PWR_BTN_N
9	5VSB (Power)	10	----

3 ► USB Cable (CN3)

Pin	Assignment	Pin	Assignment
A1	GND (Power)	B1	GND (Power)
A2	NC	B2	NC
A3	NC	B3	NC
A4	5VSB (Power)	B4	5VSB (Power)
A5	CC1	B5	CC2
A6	USB_DP	B6	USB_DP
A7	USB_DN	B7	USB_DN
A8	NC	B8	NC
A9	5VSB (Power)	B9	5VSB (Power)
A10	NC	B10	NC
A11	NC	B11	NC
A12	GND (Power)	B12	GND (Power)



1 ► OOB SPI Header

Pin	Assignment
1	GPO_SPI_SW
2	SPI_DO
3	SPI_DI
4	SPI_CLK
5	SPI_SS0
6	GND (Power)
7	SPI_PWR (Power)

2 ► OOB I2C Header

Pin	Assignment
1	NC
2	NC
3	I2C_SCL
4	I2C_SDA
5	NC

3 ► USB Port

Pin	Assignment	Pin	Assignment
1	5VSB (Power)	2	NC
3	USB_DN	4	NC
5	USB_DP	6	NC
7	GND (Power)	8	NC
9	----	10	NC

2.1 ► Front Panel

Pin	Assignment	Pin	Assignment
1	NC	2	NC
3	SLP_S3_N	4	NC
5	NC	6	NC
7	NC	8	NC
9	SYS_RST_N	10	PWR_BTN_N
11	NC	12	---

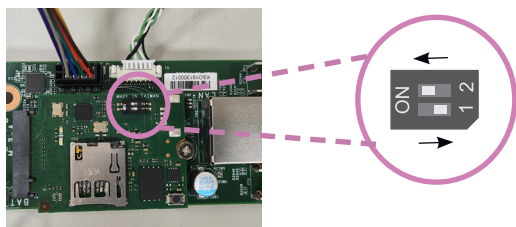
2.2 ► COM Port

Pin	Assignment	Pin	Assignment
1	NC	2	UART_TX
3	UART_RX	4	NC
5	NC	6	NC
7	NC	8	NC
9	NC	10	----

► OOB Normal Boot

Step 1:

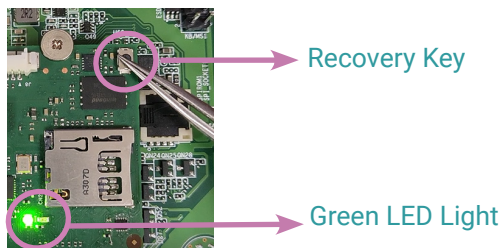
Make sure the switch change to switch 1 (off) & switch 2 (on).



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 EXT-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.

```

C:\Users\test>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:
Reply from 192.168.10.100: bytes=32 time<1ms TTL=64
Reply from 192.168.10.100: bytes=32 time<1ms TTL=64
Reply from 192.168.10.100: bytes=32 time<1ms TTL=64
Reply from 192.168.10.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\test>arp -a

Interface: 192.168.10.101 --- 0x5
    Internet Address      Physical Address        Type
192.168.10.100          00-01-29-00-00-01      dynamic
192.168.10.255          ff-ff-ff-ff-ff-ff      static
224.0.0.22              01-00-5e-00-00-16      static
224.0.0.251             01-00-5e-00-00-fb      static
224.0.0.252             01-00-5e-00-00-fc      static
  
```

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

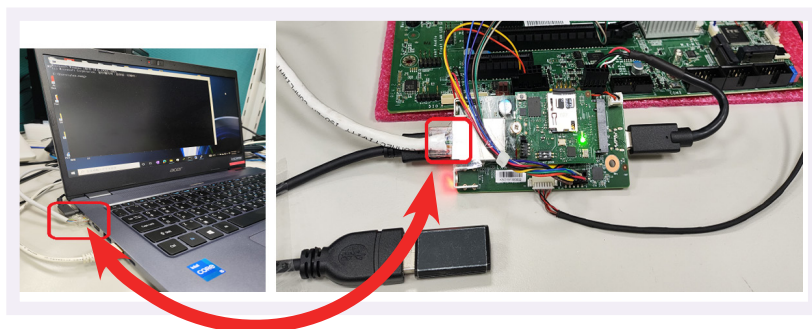
The default password is **OOB MAC address -1**. If there are letters from A to F, make sure they are all uppercase letters.

For example 1: 000129000001-1 --> 000129000000

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

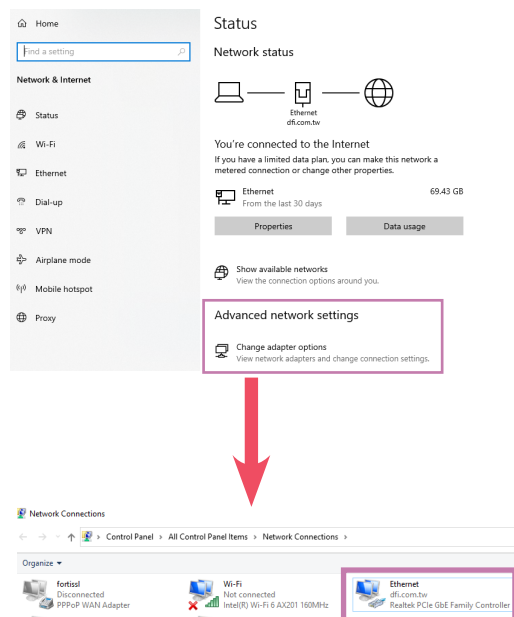
Step 2:

Use a LAN cable to connect a LAN port on PC and a LAN port 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**.



Note:

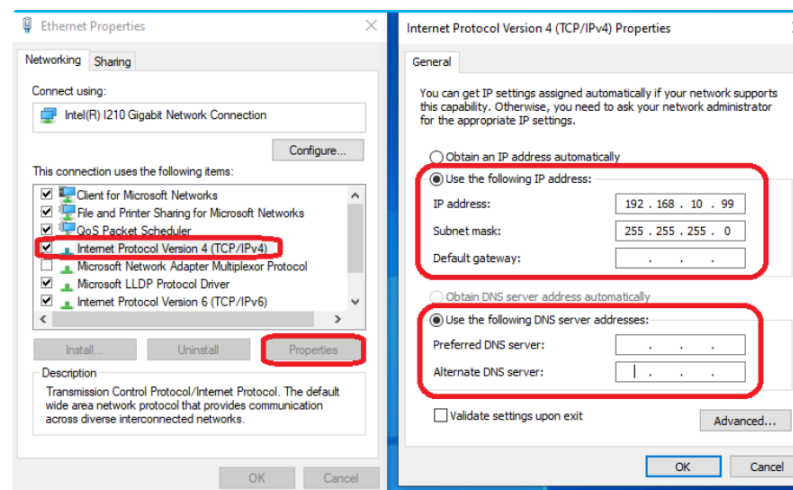
Remote PC and DFI system shall be in the same network domain.

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

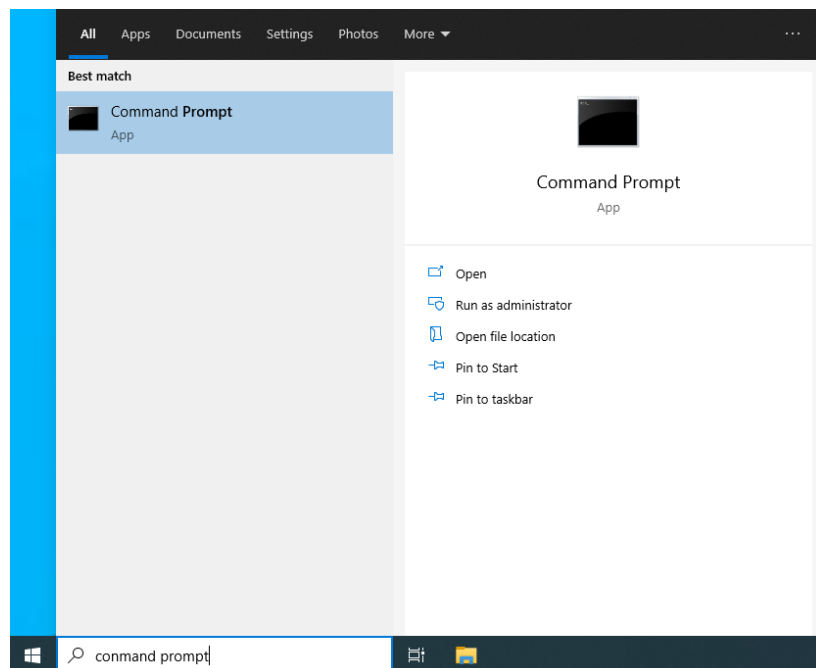


Step 4:

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**

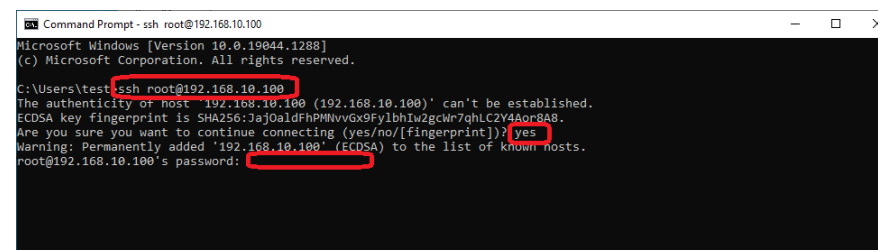
Please obtain a default password before logging in, and type in the information as follows:

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 log in)

**Note:**

For creating a default password, please refer to [Default Password Setting - Step 1](#).

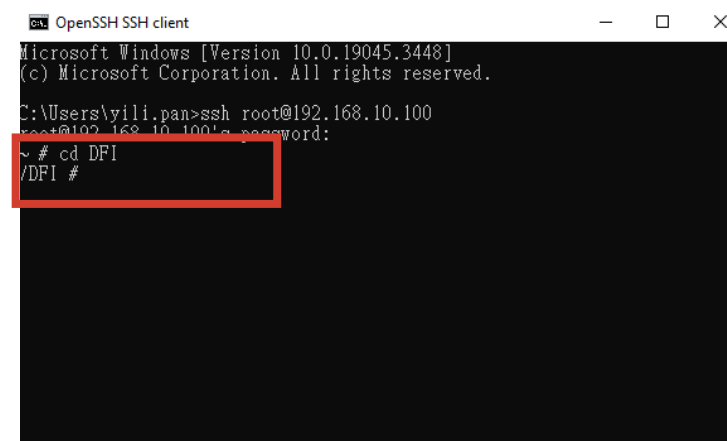
**Note:**

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.

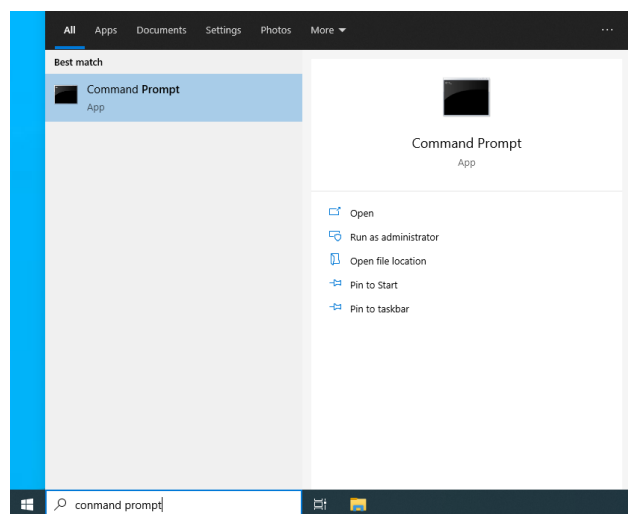
Please make sure to log out OOB before changing the password.

Step 1:

Execute windows Command Prompt.

To run the command prompt:

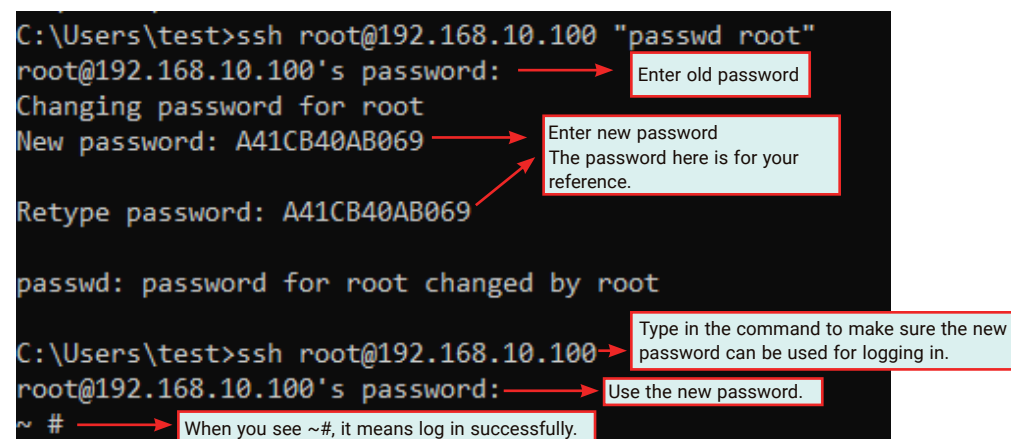
- Pressing Windows key + R key to open "Run" box. Type "cmd" and then click "OK".
- Or
- Using the search bar in the Windows 10, type "cmd" into the search bar and press enter.



Step 2:

Enter the command below.

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



Use SSH key Pair Login

Step 1:

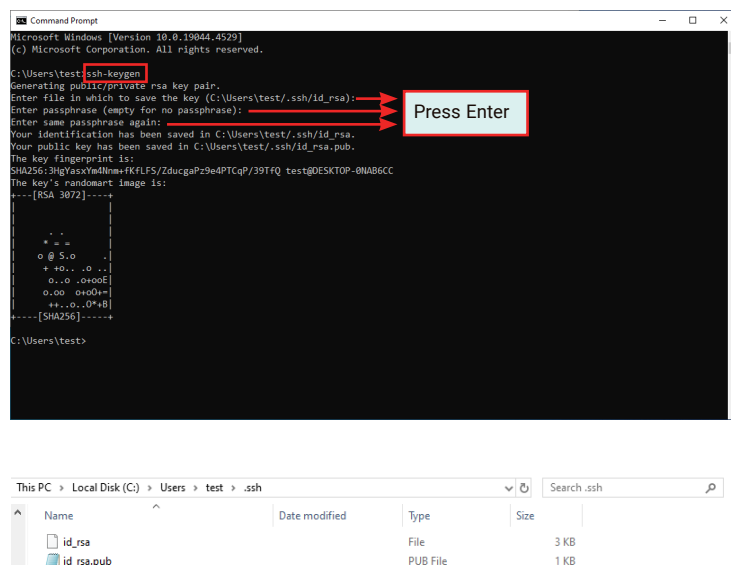
Execute windows Command Prompt.

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.



```
Microsoft Windows [Version 10.0.19044.4529]
(c) Microsoft Corporation. All rights reserved.

C:\Users\test>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\test\.ssh\id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\test\.ssh\id_rsa.
Your public key has been saved in C:\Users\test\.ssh\id_rsa.pub.
The key fingerprint is:
SHA256:3HgYasxYmDnm+FKFLFS/ZducgaPz9e4PTCqP/39TFQ test@DESKTOP-0NA86CC
The key's randomart image is:
+-----[RSA 3072]-----+
|
|..
|+..
|o @ S.o .
|+ +o.. .o ..
|o..o .o+oOE
|o..oo o+oD+
|++..o..O*+B
+-----[SHA256]-----+
C:\Users\test>
```

Name	Date modified	Type	Size
id_rsa		File	3 KB
id_rsa.pub		PUB File	1 KB

Step 2:

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

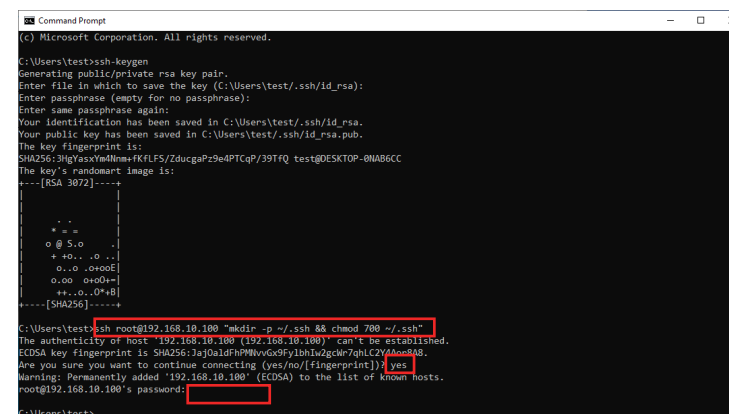
C:\users\user name> : ssh root@192.168.10.100 "mkdir -p ~/.ssh && chmod 700 ~/.ssh"

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.



```
Microsoft Windows [Version 10.0.19044.4529]
(c) Microsoft Corporation. All rights reserved.

C:\Users\test>ssh root@192.168.10.100 "mkdir -p ~/.ssh && chmod 700 ~/.ssh"
The authenticity of host '192.168.10.100 (192.168.10.100)' can't be established.
ECDSA key fingerprint is SHA256:3HgYasxYmDnm+FKFLFS/ZducgaPz9e4PTCqP/39TFQ test@DESKTOP-0NA86CC.
Are you sure you want to continue connecting (yes/no/fingerprint)? yes
Warning: Permanently added '192.168.10.100' (ECDSA) to the list of known hosts.
root@192.168.10.100's password:
```

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.

```

Command Prompt
Enter file in which to save the key (C:\Users\test\.ssh\id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\test\.ssh\id_rsa.
Your public key has been saved in C:\Users\test\.ssh\id_rsa.pub.
The key fingerprint is:
SHA256:3hgYasxYmDnm+FKFLFS/ZducgaPz9edPTCqP/39TFQ test@DESKTOP-0NAB6CC
The key's randomart image is:
+--[RSA 3072]-----
  o @ S.o .
+ + + + +
o . o . o o o E
o . o . o o o =
++ . o . o + B
+----[SHA256]-----

C:\Users\test>ssh root@192.168.10.100 "mkdir -p ~/ssh && chmod 700 ~/ssh"
The authenticity of host '192.168.10.100 (192.168.10.100)' can't be established.
ECDSA key fingerprint is SHA256:JaJ0aldFhPWvGx9Fylbhlw2gcW7qhlCZY4Aor8A8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.100' (ECDSA) to the list of known hosts.
root@192.168.10.100's password:
C:\Users\test>scp C:\Users\test\.ssh\id_rsa.pub root@192.168.10.100:~/ssh/authorized_keys
root@192.168.10.100's password:
id_rsa.pub 100% 575 0.6KB/s 00:00
C:\Users\test>

```

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 **~#**

```

OpenSSH SSH client
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\test\.ssh\id_rsa.
Your public key has been saved in C:\Users\test\.ssh\id_rsa.pub.
The key fingerprint is:
SHA256:3hgYasxYmDnm+FKFLFS/ZducgaPz9edPTCqP/39TFQ test@DESKTOP-0NAB6CC
The key's randomart image is:
+--[RSA 3072]-----
  o @ S.o .
+ + + + +
o . o . o o o E
o . o . o o o =
++ . o . o + B
+----[SHA256]-----

C:\Users\test>ssh root@192.168.10.100 "mkdir -p ~/ssh && chmod 700 ~/ssh"
The authenticity of host '192.168.10.100 (192.168.10.100)' can't be established.
ECDSA key fingerprint is SHA256:JaJ0aldFhPWvGx9Fylbhlw2gcW7qhlCZY4Aor8A8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.100' (ECDSA) to the list of known hosts.
root@192.168.10.100's password:
C:\Users\test>scp C:\Users\test\.ssh\id_rsa.pub root@192.168.10.100:~/ssh/authorized_keys
root@192.168.10.100's password:
id_rsa.pub 100% 575 0.6KB/s 00:00
C:\Users\test>ssh root@192.168.10.100
~#

```

- 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\4-1c-b4-0a-b0-6a**

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

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

```

Command Prompt
Microsoft Windows [Version 10.0.19044.4529]
(c) Microsoft Corporation. All rights reserved.

C:\Users\test>ssh-keygen -f C:\Users\test\.ssh\4-1c-b4-0a-b0-6a
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\test\.ssh\4-1c-b4-0a-b0-6a.pub.
Your public key has been saved in C:\Users\test\.ssh\4-1c-b4-0a-b0-6a.pub.
The key fingerprint is:
SHA256:1V8SU7XZmKvT92j127qb8dkysDdnA8afIZVxk2zk test@DESKTOP-0NAB6CC
The key's randomart image is:
+--[RSA 3072]-----
  o o o o o .
  o o o o o .
  o o o o o .
  o o o o o .
  o o o o o .
  o o o o o .
  o o o o o .
  o o o o o .
  o o o o o .
  o o o o o .
+----[SHA256]-----

C:\Users\test>

```

This PC > Local Disk (C:) > Users > test > .ssh

Name	Date modified	Type	Size
a4-1c-b4-0a-b0-6a		File	3 KB
a4-1c-b4-0a-b0-6a.pub		PUB File	1 KB

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.

```

Microsoft Windows [Version 10.0.19044.4529]
(c) Microsoft Corporation. All rights reserved.

C:\Users\test>ssh-keygen -f C:\Users\test\.ssh\4-1c-b4-0a-b0-6a
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\test\.ssh\4-1c-b4-0a-b0-6a.
Your public key has been saved in C:\Users\test\.ssh\4-1c-b4-0a-b0-6a.pub.
The key fingerprint is:
SHA256:1V8SU7Z2omVT9z127gb8dKyd5DdnA4Baf1Zvk2zk test@DESKTOP-0NA86CC
The key's randomart image is:
+--[RSA 3072]-----
  o.o+o+..+
  o+..+..+
  .oo..+E+
  o..+..+*
  S .oo+
  o .o.o..
  o + oooo ..
  + .-+
  ..o+
+-----[SHA256]-----

C:\Users\test>ssh root@192.168.10.100 "mkdir -p ~/.ssh && chmod 700 ~/.ssh"
The authenticity of host '192.168.10.100 (192.168.10.100)' can't be established.
ECDSA key fingerprint is SHA256:1aj0aidfhPMvvgG9fy1bhw2gcw7qhlC2Y6Aor8AB.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.100' (ECDSA) to the list of known hosts.
root@192.168.10.100's password:
C:\Users\test>

```

Step 2:

Please enter the command as follows:

scp C:\Users\test\.ssh\4-1c-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.

```

Command Prompt

Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\test\.ssh\4-1c-b4-0a-b0-6a.
Your public key has been saved in C:\Users\test\.ssh\4-1c-b4-0a-b0-6a.pub.
The key fingerprint is:
SHA256:1V8SU7Z2omVT9z127gb8dKyd5DdnA4Baf1Zvk2zk test@DESKTOP-0NA86CC
The key's randomart image is:
+--[RSA 3072]-----
  o.o+o+..+
  o+..+..+
  .oo..+E+
  o..+..+*
  S .oo+
  o .o.o..
  o + oooo ..
  + .-+
  ..o+
+-----[SHA256]-----

C:\Users\test>ssh root@192.168.10.100 "mkdir -p ~/.ssh && chmod 700 ~/.ssh"
The authenticity of host '192.168.10.100 (192.168.10.100)' can't be established.
ECDSA key fingerprint is SHA256:1aj0aidfhPMvvgG9fy1bhw2gcw7qhlC2Y6Aor8AB.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.100' (ECDSA) to the list of known hosts.
root@192.168.10.100's password:
C:\Users\test>scp C:\Users\test\.ssh\4-1c-b4-0a-b0-6a.pub root@192.168.10.100:~/.ssh/authorized_keys
root@192.168.10.100's password:
4-1c-b4-0a-b0-6a.pub 100% 575 0.6KB/s 00:00
C:\Users\test>

```

Step 3:

Please enter the command as follows:

ssh -i C:\Users\test\.ssh\4-1c-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 ~#

```

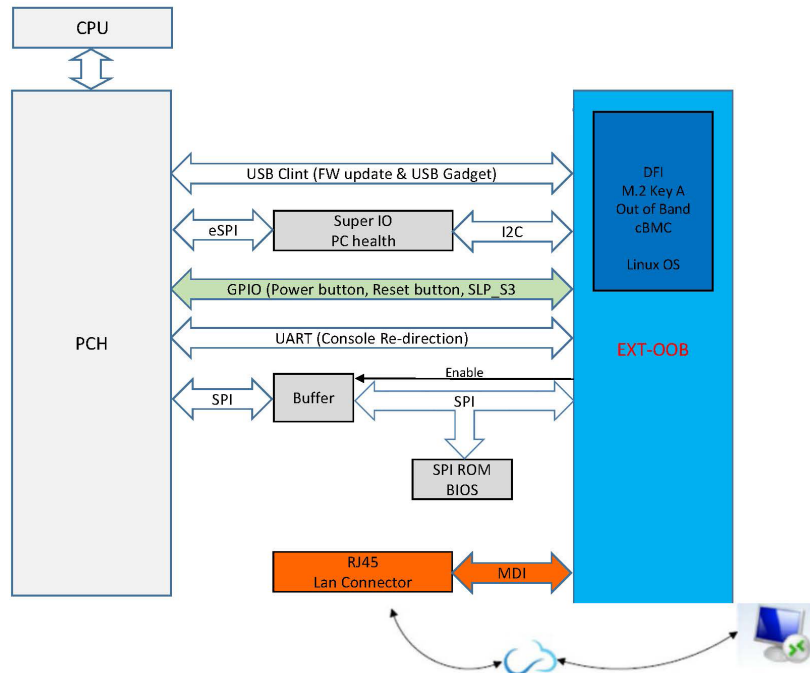
OpenSSH SSH client

Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\test\.ssh\4-1c-b4-0a-b0-6a.
Your public key has been saved in C:\Users\test\.ssh\4-1c-b4-0a-b0-6a.pub.
The key fingerprint is:
SHA256:1aJ0aidfhPMvvgG9fy1bhw2gcw7qhlC2Y6Aor8AB
The key's randomart image is:
+--[RSA 3072]-----
  . . .
  +*o+
  %++
  ++EoS
  o.o+..o
  ..+..+..o
  +..+..+
  +..+..+
  +..+..+
  +..+..+
+-----[SHA256]-----

C:\Users\test>ssh root@192.168.10.100 "mkdir -p ~/.ssh && chmod 700 ~/.ssh"
The authenticity of host '192.168.10.100 (192.168.10.100)' can't be established.
ECDSA key fingerprint is SHA256:1aJ0aidfhPMvvgG9fy1bhw2gcw7qhlC2Y6Aor8AB.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.100' (ECDSA) to the list of known hosts.
root@192.168.10.100's password:
C:\Users\test>scp C:\Users\test\.ssh\4-1c-b4-0a-b0-6a.pub root@192.168.10.100:~/.ssh/authorized_keys
root@192.168.10.100's password:
4-1c-b4-0a-b0-6a.pub 100% 575 0.6KB/s 00:00
C:\Users\test>ssh -i C:\Users\test\.ssh\4-1c-b4-0a-b0-6a root@192.168.10.100
~#

```

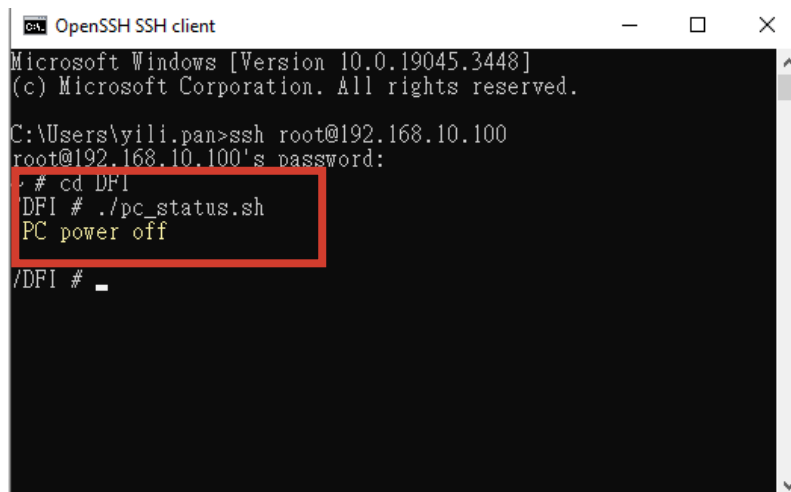
► Remote Control PC Power On/Off



PC Power On/Off Status Check

Please complete [Default Password Setting - Step4](#) before entering the following command.
Check the current power On/Off status remotely by typing in following command.

Shell Script : `./pc_status.sh`



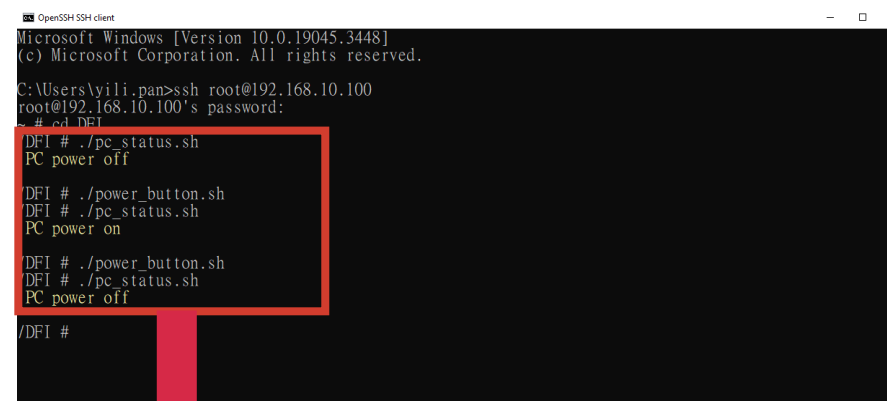
```
ca. OpenSSH SSH client
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Users\yili.pan>ssh root@192.168.10.100
root@192.168.10.100's password:
# cd DFI
DFI # ./pc_status.sh
PC power off
/DFI #
```

Turn On/Off PC Remotely

After the status check, you can control PC power on/off remotely.
Please complete [Default Password Setting - Step4](#) before entering the following command.
To toggle power on or power off, just type in the same command again.

Shell Script : `./power_button.sh`



```
ca. OpenSSH SSH client
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Users\yili.pan>ssh root@192.168.10.100
root@192.168.10.100's password:
# cd DFI
DFI # ./pc_status.sh
PC power off

DFI # ./power_button.sh
DFI # ./pc_status.sh
PC power on

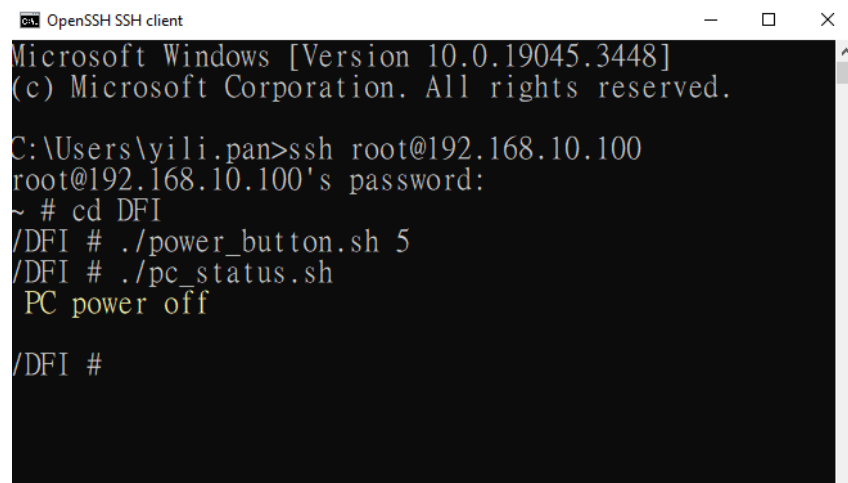
DFI # ./power_button.sh
DFI # ./pc_status.sh
PC power off
/DFI #
```

- 
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 status again.

Perform a Timed Force Shutdown

To forcibly shut down the PC, please type in the following command.
Please complete [Default Password Setting - Step4](#) 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**



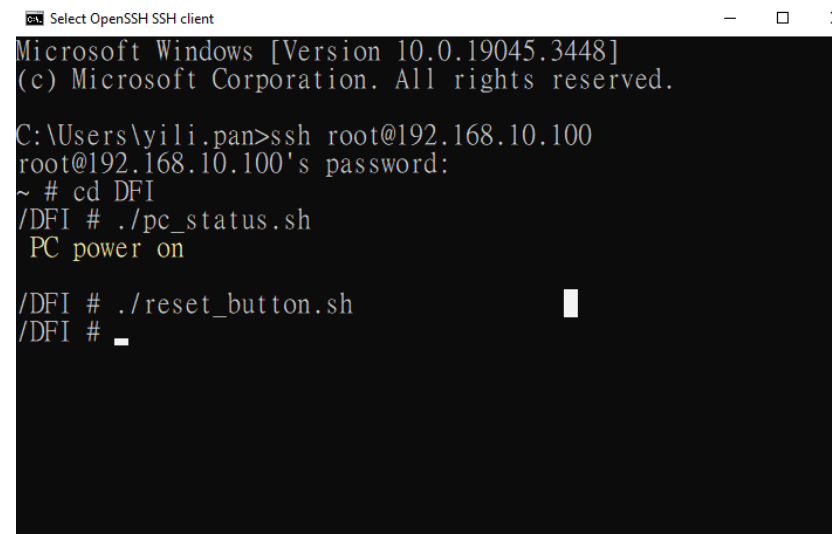
```
OpenSSH SSH client
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Users\yili.pan>ssh root@192.168.10.100
root@192.168.10.100's password:
~ # cd DFI
/DFI # ./power_button.sh 5
/DFI # ./pc_status.sh
PC power off
/DFI #
```

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**



```
Select OpenSSH SSH client
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Users\yili.pan>ssh root@192.168.10.100
root@192.168.10.100's password:
~ # cd DFI
/DFI # ./pc_status.sh
PC power on

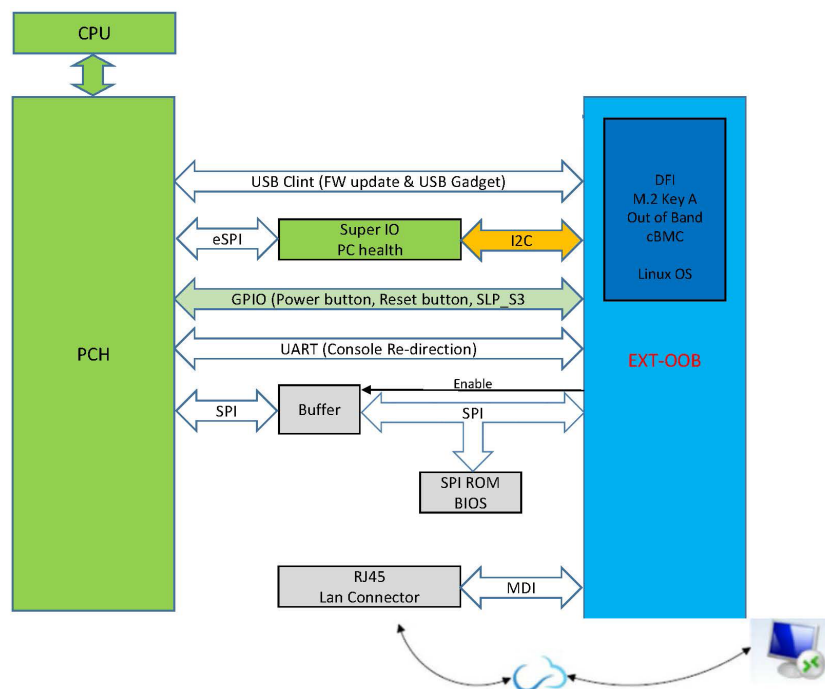
/DFI # ./reset_button.sh
/DFI #
```

► 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 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 ===
[]+ Terminated
DFI #
  
```

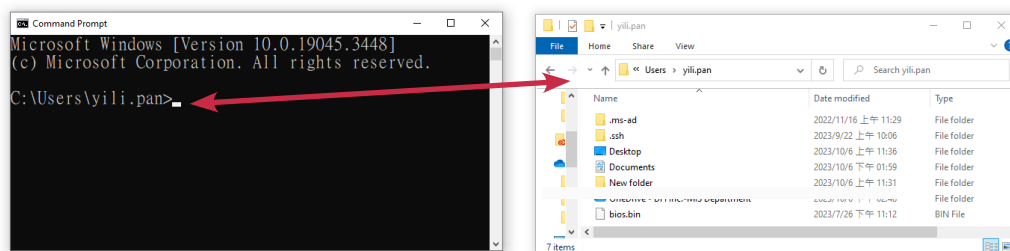
How to Export Super I/O Logs From OOB

To export super I/O log, please type in the following command.

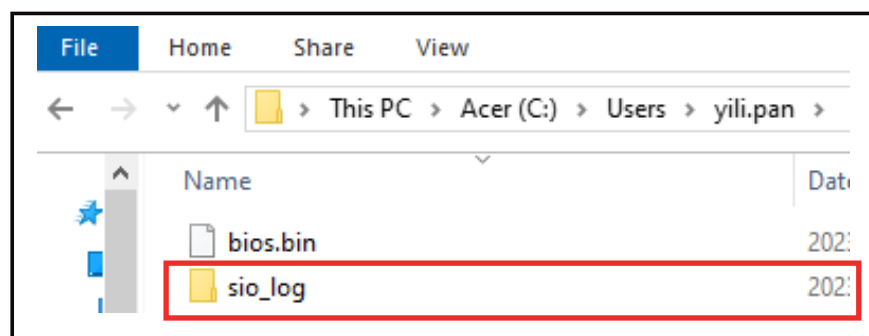
Please complete [Default Password Setting - Step 4](#) before entering the following command.

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 MicroSD card is not formatted as FAT32.

The instructions are as follows :

```

~ # fdisk /dev/mmcblk0

The number of cylinders for this disk is set to 480896.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
 1) software that runs at boot time (e.g., old versions of LILO)
 2) booting and partitioning software from other OSs
   (e.g., DOS fdisk, 2 fdisk)

Command (m for help): n
Partition type
  p   primary partition (1-4)
  e   extended

Partition number (1-4): 1
First sector (16-30777343, default 16):
Using default value 16
Last sector or +size{K,M,G,T} (16-30777343, default 30777343):
Using default value 3343

Command (m for help): w
partition table has been altered.
Calling ioctl() to re-read partition table
~ # mkdosfs /dev/mmcblk0p1
~ # reboot
  
```

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:

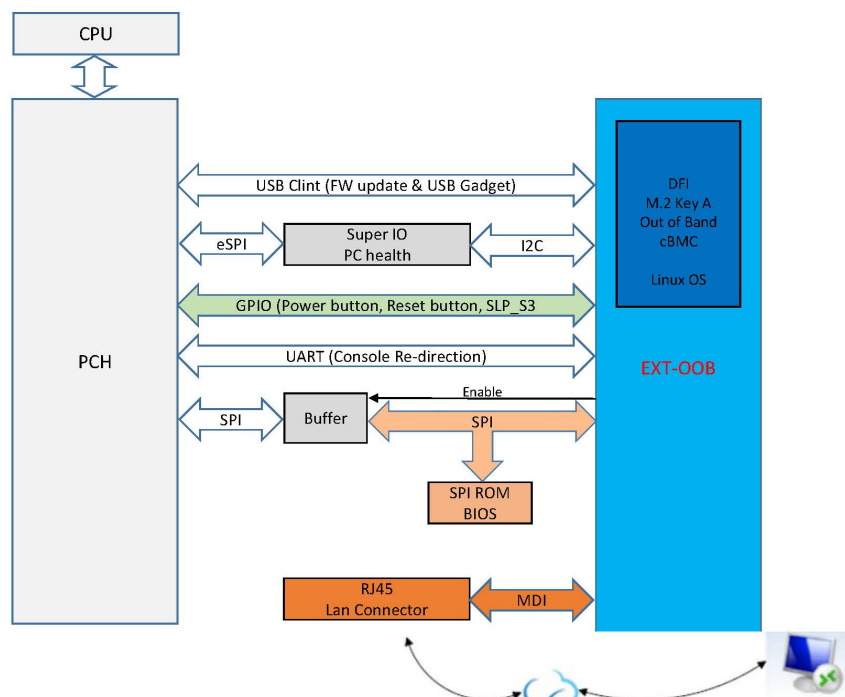
Shell Script : **./eject_uSD.sh**

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



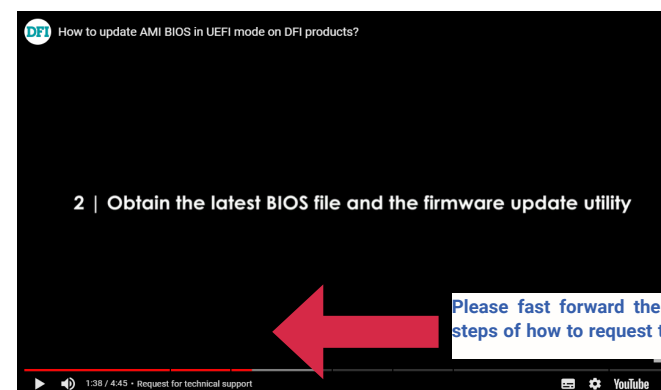
Step 1:

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.)

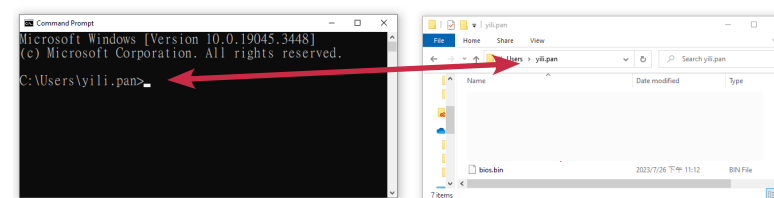
How to request to obtain the files and update BIOS, please watch the video below for more information:

<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

```
OpenSSH SSH client
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Users\yili.pan>ssh root@192.168.10.100
root@192.168.10.100's password:
~ # cd /DFI/bios/.
/DFI/bios # ./updatebios.sh B246.18A
Please shut down the PC, and execute again

/DFI/bios # cd ..
/DFI # ./power_button.sh
/DFI # cd bios/
/DFI/bios # ./updatebios.sh B246.18A

=== DFI OOB ===
Using clock_gettime for delay loops (clk_id: 1, resolution: 1ns).
The following protocols are supported: SPI.
Probing for Winbond W25Q256JV_Q, 32768 kB; compare id: id1 0xef, id2 0x4019
Found Winbond flash chip "W25Q256JV_Q" (32768 kB, SPI) on linux_spi.
Chip status register is 0x00.

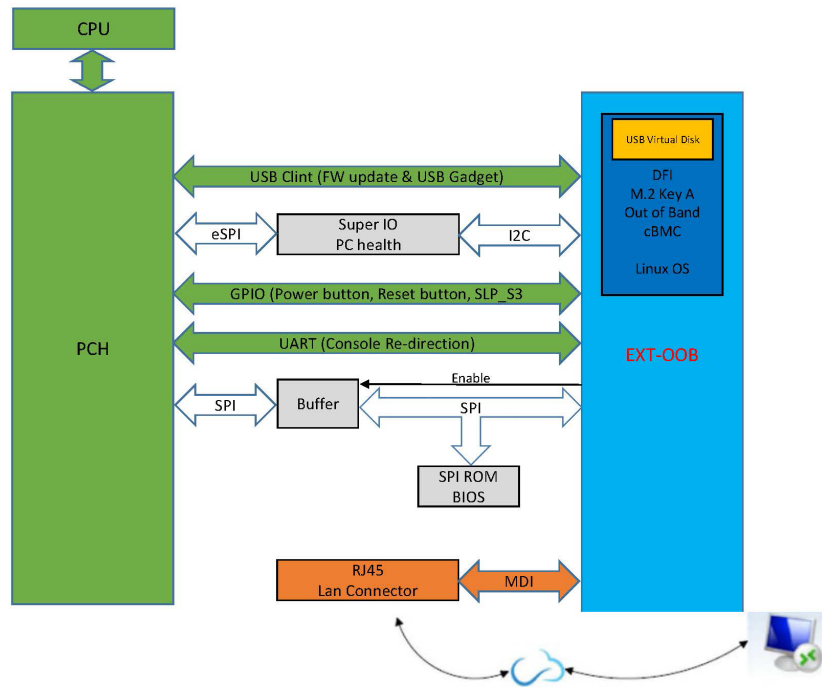
Please wait...

Reading old flash chip contents... Reading old flash chip contents... done.
Erasing and writing flash chip... ..
Verifying flash... VERIFIED.
BIOS update is finished

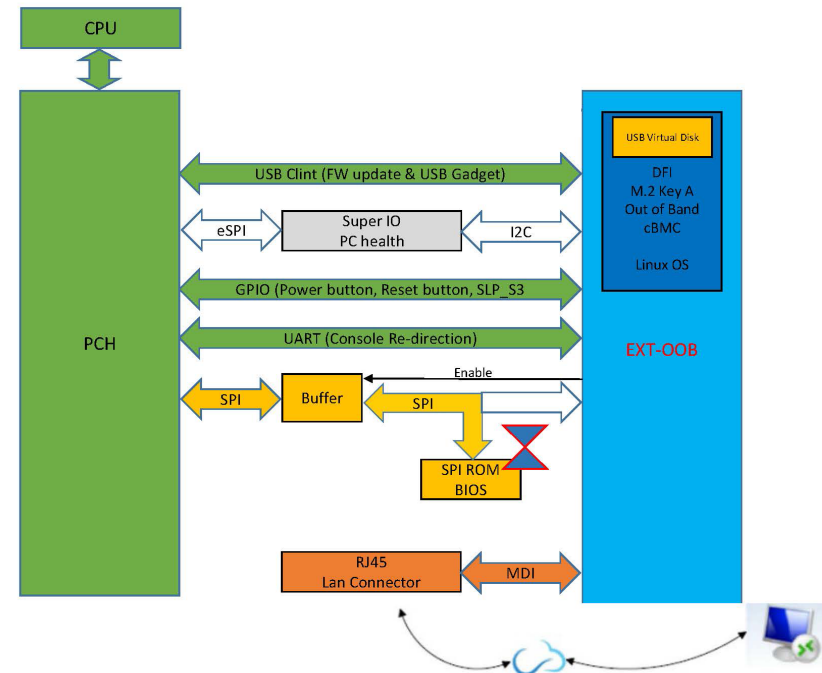
/DFI/bios # _
```

► 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**.

```
/DFI #  
/DFI # ./insert_usb_storage.sh  
  
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`

```
/DFI # ./eject_usb_storage.sh  
  
This is USB uSD, Please exec eject_uSD.sh  
  
/DFI # ./eject_uSD.sh  
/DFI # ./insert_usb_storage.sh  
/DFI #
```

Step 1:

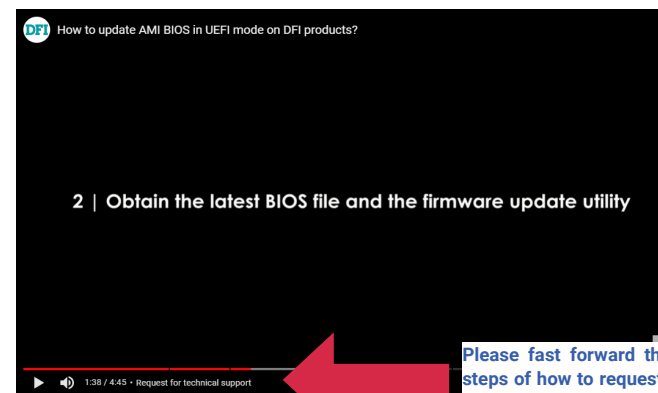
Before starting the update, you will have to prepare two files:

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>



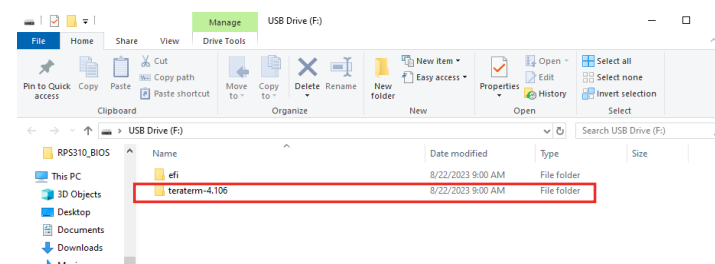
Please fast forward the video to 1:31 and follow the steps of how to request the BIOS files from DFI.

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

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>
```

- [How to Access BIOS Setup Menu When Power on](#)

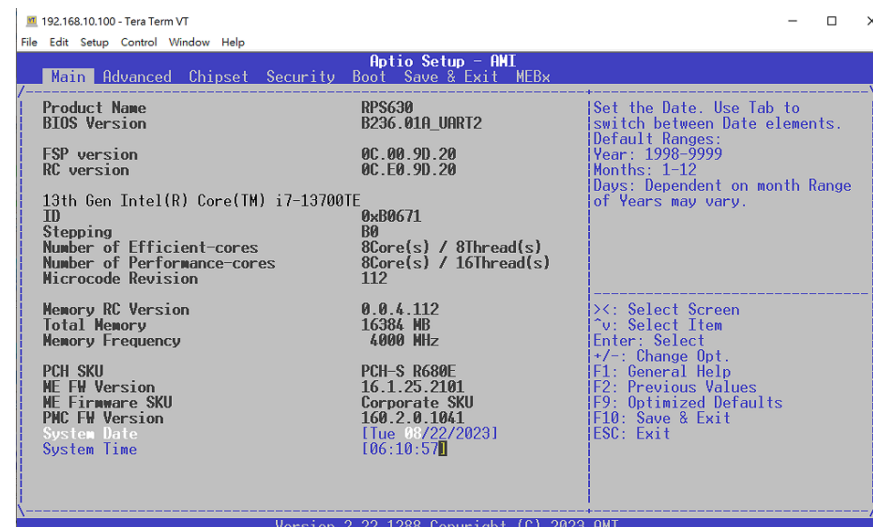
If the DFI system is power on which installed OOB, executing **power_button.sh** script to off/on the system. The script must be executed twice, first is for powering off the system, second is for powering on the system.

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.

Step 3:

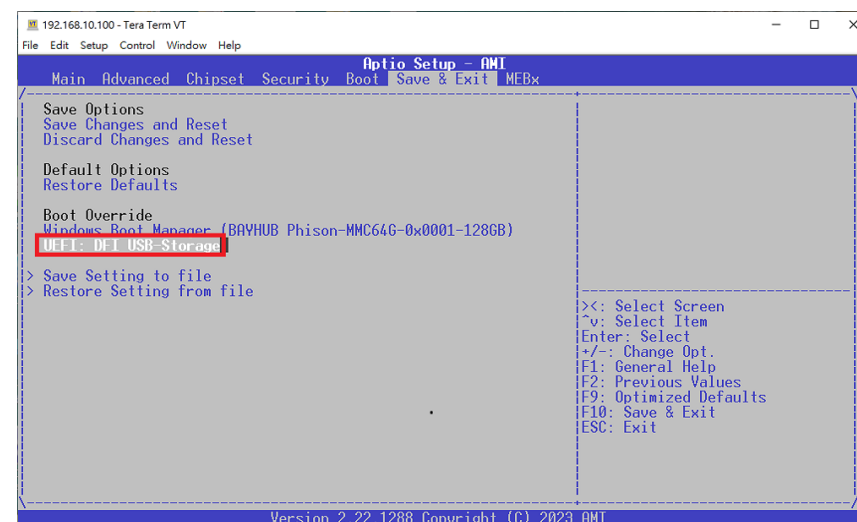
Access BIOS setup menu.

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.

```

PciRoot(0x0)/Pci(0x14,0x0)/USB(0x3,0x0)
blk0 :HardDisk - Alias hd37b fs0
PciRoot(0x0)/Pci(0x10,0x4)/Pci(0x0,0x0)/NVMe(0x1,41-44-F6-05-52-48-35-7
C)/HD(1,GPT,9D17F1AF-37E4-4654-98CF-E74BE3857A9E,0x800,0x32000)
blk1 :Removable BlockDevice - Alias f18d0 fs1
PciRoot(0x0)/Pci(0x14,0x0)/USB(0x3,0x0)
blk2 :HardDisk - Alias (null)
PciRoot(0x0)/Pci(0x10,0x4)/Pci(0x0,0x0)/NVMe(0x1,41-44-F6-05-52-48-35-7
C)/HD(2,GPT,87648C69-E547-45F4-9A9F-114CBAB8F322,0x32800,0x40000)
blk3 :HardDisk - Alias (null)
PciRoot(0x0)/Pci(0x10,0x4)/Pci(0x0,0x0)/NVMe(0x1,41-44-F6-05-52-48-35-7
C)/HD(3,GPT,7093A5EE-E900-4CCC-A12B-3A56AB6C0DBE,0x72800,0x1DC80800)
blk4 :BlockDevice - Alias (null)
PciRoot(0x0)/Pci(0x10,0x4)/Pci(0x0,0x0)/NVMe(0x1,41-44-F6-05-52-48-35-7
C)

Press ESC in 3 seconds to skip startup.nsh, any other key to continue.
startup.nsh> fs1:
startup.nsh> !fuefiu.efi bios.bin /p /b /n /reboot

+-----+
+      AMI Firmware Update Utility v5.15.00.0081      +
+ Copyright (c) 1985-2022, American Megatrends International LLC. +
+ All rights reserved. Subject to AMI licensing agreement.      +
+-----+
Reading flash ..... 0x00730000 (44%)

```

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.

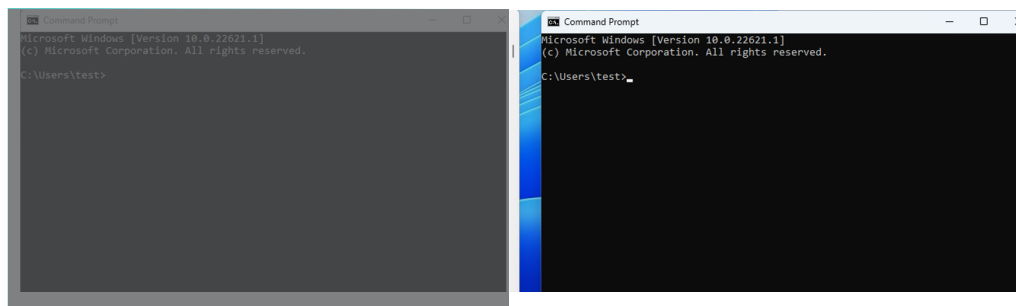
Typing in following command and you will see a message to ask for a new IP address.

(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**

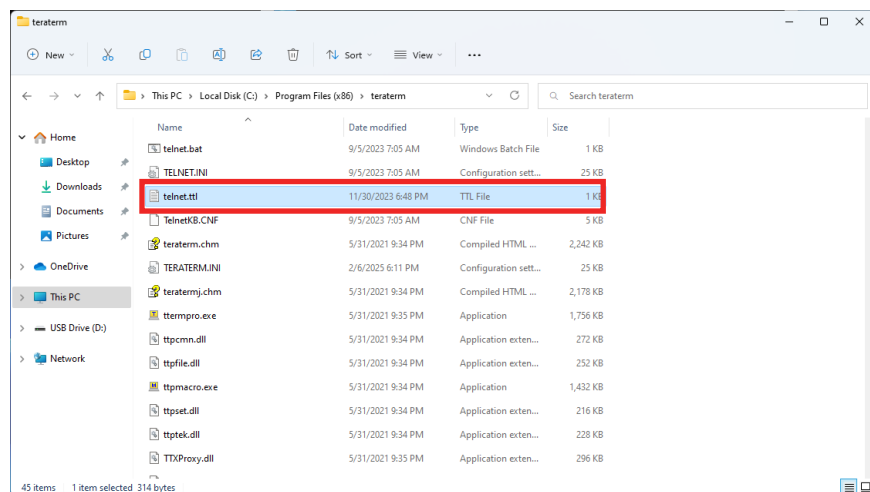
```
C:\Users\test>ssh root@192.168.10.88
The authenticity of host '192.168.10.88 (192.168.10.88)' can't be established.
ECDSA key fingerprint is SHA256:JajOaldFhPMNvvGx9FylbhIw2gcWr7qhLC2Y4Aor8A8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.88' (ECDSA) to the list of known hosts.
root@192.168.10.88's password:
~#
```

► Console Redirection

After the IP address changes, Console Redirection is unable to run commands.

To fix the problem, please navigate to Teraterm folder and 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'

```