Ubuntu Core 16 OS
User Manual

Version 1.8

Dell IoT OS/Software

Revisions

Rev	Author	Description	Date
1.5	Crag Wang	Initial Release for UC16	03/23/2017
1.6	Crag Wang	Update for Caracalla	03/27/2017
1.7	Crag Wang	Fixed typo (PM)	03/30/2017
1.8	Crag Wang	Update Capsule update, Ignition pin, etc..	04/30/2017

TABLE OF CONTENTS

1. Overview

Ubuntu Core 16 is one of the Linux OS distribution that entirely new mechanism for managing the system and its apps. More generic details and references to the Ubuntu Snappy OS are available at the URL below.

http://www.ubuntu.com/cloud/snappy

Snap is a universal Linux package works on any distribution or device. Snaps are faster to install, easier to create, safer to run, and they update automatically and transitionally so your app is always fresh and never broken.

https://snapcraft.io/

1.1 Languages

- English only

1.2 Operating System

This manual applies to listed Operating Systems:

- Ubuntu Core 16

2. Out of Box Experience (OOBE)

2.1 Pre-requirements

Connect all necessary devices and power supply.

Edge Gateway 3003: Video output (DP) is supported, direct access to the gateway device.

Edge Gateway 3000/3001/3002: Without video output, logon via LAN1 (dhcp-client) or LAN 2(static IP assigned).

2.2 First boot (Direct)

Supported platforms: Edge Gateway 3003

Power on the device, system will setup the operating system automatically and go through multiple reboots to apply all the configurations. The process of transitioning system to READY FOR USE basically takes 1 minute.

The default username and password for Ubuntu Core 16 is “admin”.

The default computer name is pre-configured as <service tag>.

```
Ubuntu Core 16 on 127.0.0.1 (tty1)

localhost login: admin
Password:
```

Note: The username and password are both lowercase

2.3 Logon system (Under DHCP enabled network): LAN1/Ethernet Port1

Supported platforms: Edge Gateway 3000/3001/3002/3003

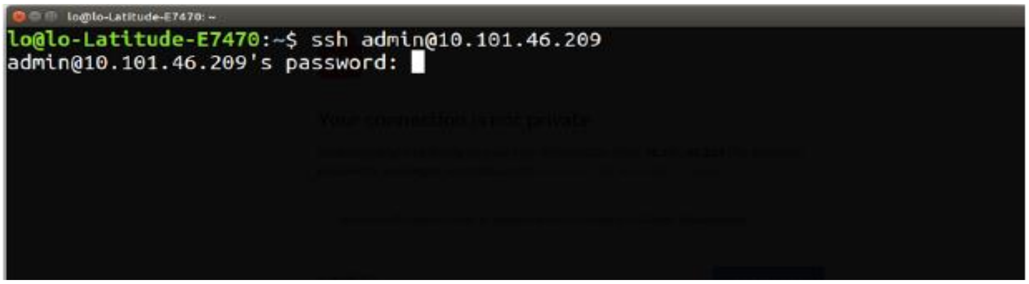
SSH service is default enabled in Ubuntu OS. User can logon system remotely with default credential.

1) Plug Ethernet cable to LAN1, the other end connect to a DHCP service enabled network environment.
2) In DHCP server, lookup the IP address associated to gateway system’s MAC address.

   Note: HW MAC address will be printed as a label on the box.
3) Use terminal or any other tool with ssh-client supported to setup ssh session.
4) In Linux, simply type following command and press Enter:

   ```
   ssh admin@10.101.46.209
   ```

   Note: The IP address above just an example. User should look up dhcp-lease-list to find out real IP by given MAC on the box.



```
lo@lo-Latitude-E7470:~$ ssh admin@10.101.46.209
admin@10.101.46.209's password: 
```

2.4 Logon system (static IPv4): LAN2/Ethernet Port2

Supported platforms: Edge Gateway 3002/3003

Gateway device is configured out of the factory with a static IP address. User can login to the system using the provided IP address. User does not need search for the device IP address from DHCP server lease list.

1) LAN #2 is set to a static IPv4 address by design:
   IP address: 192.168.2.1
   Subnet mask: 255.255.255.0
   DHCP server: N/A
2) Configure your host system (PC/Laptop) with a static IPv4 address under the same subnet, for instance set the IPv4 address to 192.168.2.X (192.168.2.2 ~ 192.168.2.254).

   Note: Do not set the IPv4 address to the same address as Edge Gateway LAN2 pre-configured.
3) Set the Subnet mask to 255.255.255.0
4) Directly connect the PC/Laptop to the Gateway device LAN2.

3. Ubuntu Core OS

3.1 Using snap in Core OS

If you are running Ubuntu 16.04 LTS or later, you can already use snaps from the command line. Otherwise do not despair, we have instructions for multiple distros.

1) To list all snaps installed on your machine:
```
$ sudo snap list
```
2) To find a snap in the store:
```
$ sudo snap find <text to search>
```
3) To install a snap:
```
$ sudo snap install <snap name>
```
4) To update a snap:
```
$ sudo snap refresh <snap name>
```
5) To revert a snap to the previously installed version:
```
$ sudo snap revert <snap name>
```
6) To remove the snap:
```
$ sudo snap remove <snap name>
```

3.2 UEFI BIOS Firmware Update in Ubuntu Core OS

This fwupgmgr tool/commands are used to update UEFI BIOS firmware on the system. The UEFI BIOS for this platform will be released through online Linux Vendor File System based methods.

Capsule update will be recommended to be default enabled, running in the background to get system firmware up to date.

- ➢ Update BIOS firmware locally: (offline)

1) Get firmware.cab from BIOS-XXXXXX.zip
2) Check details of current firmware:
```
$ sudo uefi-fw-tools.fwupdmgr get-devices
```
3) Copy the firmware.cab file to /root/snap/uefi-fw-tools/common/f
```
$ sudo cp firmware.cab /root/snap/uefi-fw-tools/common/
```
4) Check details of the firmware from zip file:
```
$ sudo uefi-fw-tools.fwupdmgr get-details [Full path of firmware.cab]
```
5) Apply the update
```
$ sudo uefi-fw-tools.fwupdmgr install [Full path of firmware.cab] -v
```

6) Reboot the system

```
$ sudo reboot
```

➢ Update BIOS firmware from LVFS server: (online)

1) Connect to embargoed channel if necessary:

```
$ snap set uefi-fw-tools conf.downloaduri=https://secure-lvfs.rhcloud.com/downloads/firmware-
c1255377a9c3465f605183b8b648e57a5202a890.xml.gz
```

2) Check details of current firmware:

```
sudo uefi-fw-tools.fwupdmgr get-devices
```

3) Check if update available from LVFS service

```
sudo uefi-fw-tools.fwupdmgr refresh
```

4) Download the fimware

```
sudo uefi-fw-tools.fwupdmgr get-updates
```

5) Run following command to apply the update

```
sudo uefi-fw-tools.fwupdmgr update -v
```

6) Reboot the system

```
$ sudo reboot
```

Reference: http://www.fwupd.org/users

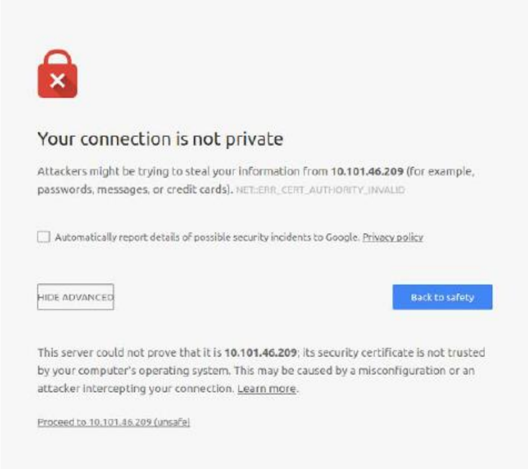
3.3 Snappy Auto update

Snappy Autoupdate is a feature running in the background that will guarantee your software always up to date. It's recommended to be enabled by default, the settings can be adjusted in the Ubuntu core.

Reference: https://developer.ubuntu.com/en/snappy/guides/autoupdate/

3.4 Access Snappy Store/Snapweb

1) Insert "ip_address:4200" in browser. It will redirect to the following page. Select "Advanced" then select "proceed to the ip_address(unsafe)".



Your connection is not private

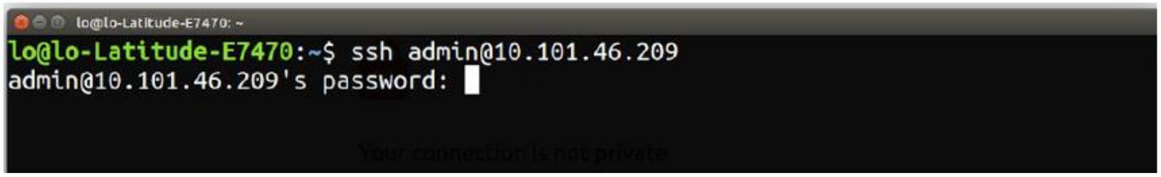
Attackers might be trying to steal your information from **10.101.46.209** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically report details of possible security incidents to Google. Privacy policy

This server could not prove that it is **10.101.46.209**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

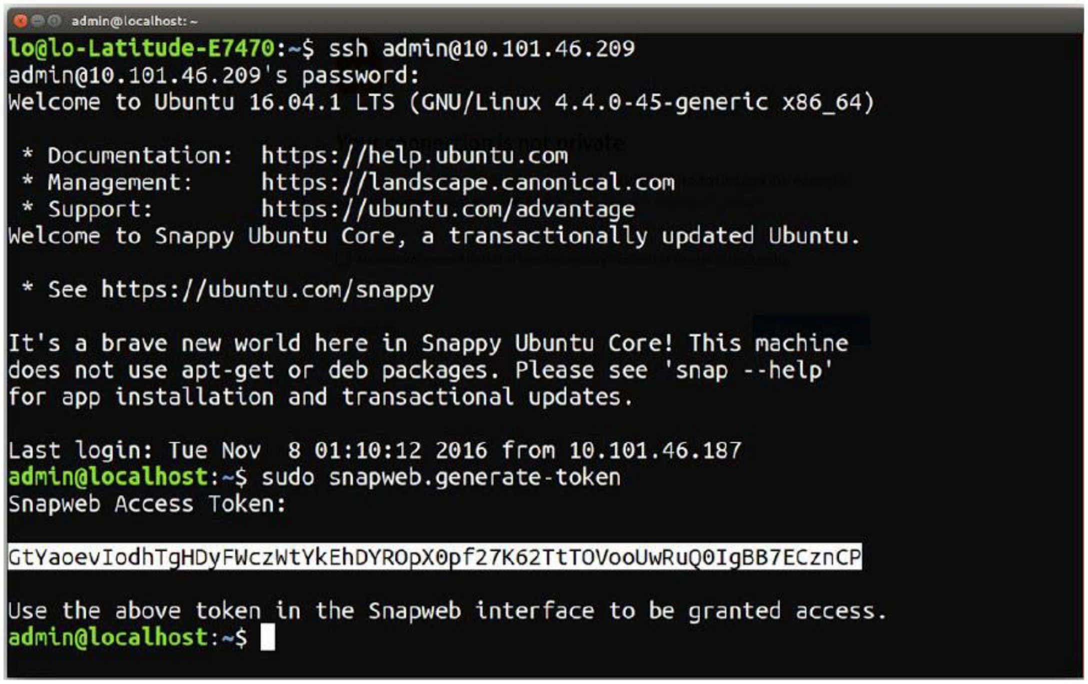
Proceed to 10.101.46.209 (unsafe)

2) Open Terminal and ssh remote login using default admin/admin.



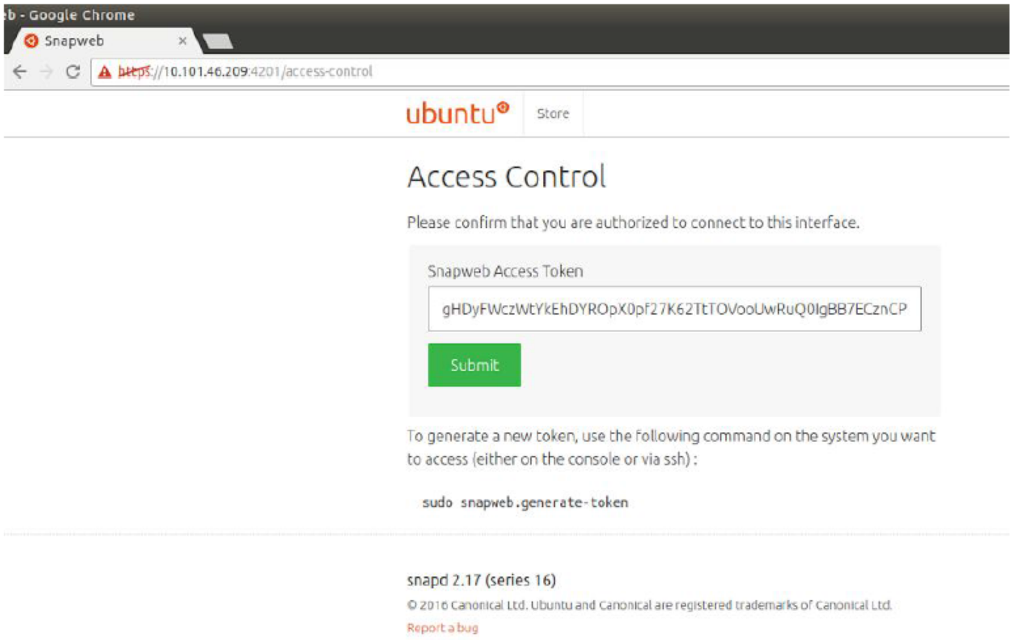
```
lo@lo-Latitude-E7470:~$ ssh admin@10.101.46.209
admin@10.101.46.209's password:
```

3) Running "sudo snapweb.generate-token", and copy the token.



```
lo@lo-Latitude-E7470:~$ ssh admin@10.101.46.209
admin@10.101.46.209's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Welcome to Snappy Ubuntu Core, a transactionally updated Ubuntu.

 * See https://ubuntu.com/snappy

It's a brave new world here in Snappy Ubuntu Core! This machine
does not use apt-get or deb packages. Please see 'snap --help'
for app installation and transactional updates.

Last login: Tue Nov  8 01:10:12 2016 from 10.101.46.187
admin@localhost:~$ sudo snapweb.generate-token
Snapweb Access Token:

GtYaoevIodhTgHDyFWczWtYkEhDYROpX0pf27K62TtTOVooUwRuQ0IgBB7ECznCP

Use the above token in the Snapweb interface to be granted access.
admin@localhost:~$
```

4) Paste the token back to the web page, and press "Submit".



Access Control

Please confirm that you are authorized to connect to this interface.

Snapweb Access Token: gHDyFWczWtYkEhDYROpX0pf27K62TtTOVooUwRuQ0IgBB7ECznCP

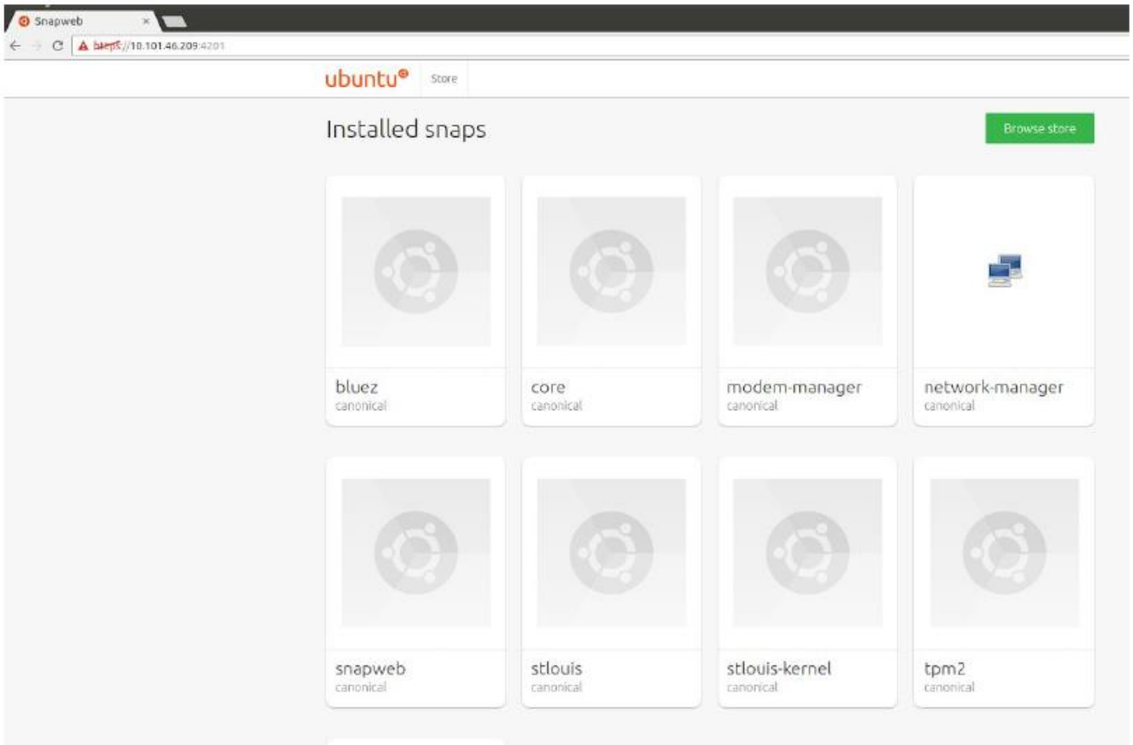
To generate a new token, use the following command on the system you want to access (either on the console or via ssh) :

```
sudo snapweb.generate-token
```

snapd 2.17 (series 16)

© 2016 Canonical Ltd. Ubuntu and Canonical are registered trademarks of Canonical Ltd.

5) Now you can access the snapweb.



Installed snaps

bluez
canonical

core
canonical

modem-manager
canonical

network-manager
canonical

snapweb
canonical

stlouis
canonical

stlouis-kernel
canonical

tpm2
canonical

Note: An initial connection to snapweb will display a page with a warning about the connection not being secure.

4. Detailed System Features

4.1 Watchdog Timer

WDT is recommended to be default enabled to active the fail-safe circuitry, Snappy is a Watchdog Timer compatible OS provides capability to detect and recover system from malfunctions, the design reacts by itself when system hangs unexpected crash.

1) Check the runtime daemon status

```
$ systemctl show | grep –i watchdog
```

Expected result:

```
RuntimeWatchdogUSec=1min
ShutdownWatchdogUSec=10min
```

2) Configure the timer

```
$ sudo vi /etc/systemd/system.conf.d/watchdog.conf
```

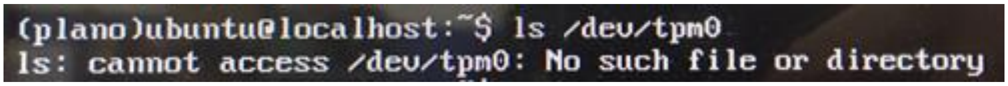
Reference: http://www.sat.dundee.ac.uk/~psc/watchdog/Linux-Watchdog.html

4.2 Trusted Platform Module

TPM is naturally supported only on devices that have TPM hardware presented, for those products Snappy offers enhanced security support natively. TPM on/off settings is configurable in the firmware and manageable in the OS.

1) IF TPM turn off: The device node (/dev/tpm0) should not exist

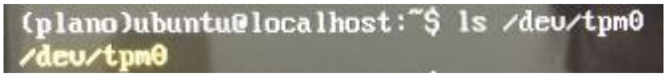
```
$ ls /dev/tpm0
```



```
(plano)ubuntu@localhost:~$ ls /dev/tpm0
ls: cannot access /dev/tpm0: No such file or directory
```

2) IF TPM turn on: The device node (/dev/tpm0) should exist.

```
$ ls /dev/tpm0
```



```
(plano)ubuntu@localhost:~$ ls /dev/tpm0
/dev/tpm0
```

Reference: https://developer.ubuntu.com/en/snappy/guides/security-whitepaper/

4.3 Cloud LED On/Off

This feature is only supported on hardware presented product.

Supported platforms:

1. Edge Gateway 5000/5100
2. Edge Gateway 3000/3001/3002/3003

Instructions:

1) Export Cloud LED PIN:

   ```
   #sudo su –

   #echo 346 > /sys/class/gpio/export

   #echo out > /sys/class/gpio/gpio346/direction
   ```

2) Turn on Cloud LED:

   ```
   #echo 1 > /sys/class/gpio/gpio346/value
   ```

3) Turn off Cloud LED:

   ```
   #echo 0 > /sys/class/gpio/gpio346/value
   ```

4.4 Audio

Supported platforms:

1. Edge Gateway 3003

Instructions:

1) MIC record

   ```
   $ sudo alsa-utils.arecord -D hw:baytrailcraudio -f cd -t wav /tmp/test.wav
   ```

2) Playback:

   ```
   $ sudo alsa-utils.play -D hw:baytrailcraudio -f cd -t wav /tmp/test.wav
   ```

4.5 GPS (location)

NMEA is supported, feature is only supported on hardware presented product. In the OS, locationd is a central hub for multiplexing access to positioning subsystems available via hard- and software. It provides a client API offering positioning capabilities to applications and other system components, abstracting away the details of individual positioning solutions.

Supported platforms:

1. Edge Gateway 3001/3002/3003

Instructions:

To retrieve NMEA streaming data:

- Device node for NMEA streaming: Edge Gateway 3001/3003

```
$ cat /dev/ttyS4
```

- Device node for NMEA streaming: Edge Gateway 3002

```
$ cat /dev/ttyS5
```

To access location service:

```
$ sudo locationd.monitor

Enabled position/heading/velocity updates...
Update(Position(lat: 26.9511 deg, lon: 155.087 deg, alt: n/a, hor.acc.: n/a, ver.acc.: n/a),
1489044234694526189)
Update(0.552 m s^-1, 1489044234695698701)
Update(Position(lat: 26.9477 deg, lon: 155.098 deg, alt: n/a, hor.acc.: n/a, ver.acc.: n/a),
1489044234718316599)
```

Reference: http://locationd.readthedocs.io/en/latest/intro.html

4.6 Serial Port

This feature is only supported on hardware presented product, sample instructions listed hereunder.

- RS232

1) Set to RS232 from BIOS, those command are under BIOS script.

```
#Platcfg64E.efi 0x046F:0x0001

#Platcfg64E.efi 0x0472:0x0001
```

Alternatively, use Dell application “Dell Command Configure” to switch BIOS configuration:

```
$ dcc.cctk -h --serial1

$ dcc.cctk --serial1

$ dcc.cctk --serial1=rs232
```

2) Set serial port mode

```
$ sudo stty -F /dev/ttyXRUSB0 ispeed 115200 ospeed 115200 -echo -onlcr -ixon -ixoff

$ sudo stty -F /dev/ttyXRUSB1 ispeed 115200 ospeed 115200 -echo -onlcr -ixon -ixoff
```

3) Transfer/Receive data between two ports (Wired RS232 between two serial ports on the device)
4) Transfer data:

```
$ sudo su

$ echo abcdefg > /dev/ttyXRUSB0

(Keep repeating this command to send data)
```

5) Receive data from another terminal by ssh from PC.

```
$ ssh admin@<IP addr of caracalla>

(passwd: admin)

$ sudo su

$ cat /dev/ttyXRUSB1

(Check the string be received correctly)
```

- RS422FD / RS485FD

1) Set to RS422/485 FD from BIOS, those command are under BIOS script.

```
#Platcfg64E.efi 0x0470:0x0003

#Platcfg64E.efi 0x0473:0x0003
```

Alternatively, use Dell application “Dell Command Configure” to switch BIOS configuration:

```
dcc.cctk -h --serial1

dcc.cctk --serial1
dcc.cctk --serial1=rs422
```

2) Set serial port mode

```
$ sudo stty -F /dev/ttyXRUSB0 ispeed 115200 ospeed 115200 -echo -onlcr -ixon -ixoff

$ sudo stty -F /dev/ttyXRUSB1 ispeed 115200 ospeed 115200 -echo -onlcr -ixon -ixoff
```

3) Transfer/Receive data between two ports (Wired RS422/485 FD between two serial ports on the device)
4) Transfer data:

```
$ sudo su

$ echo abcdefg > /dev/ttyXRUSB0

(Keep repeating this command to send data)
```

5) Receive data from another terminal by ssh from PC.

```
$ ssh admin@<IP addr of caracalla>

(passwd: admin)

$ sudo su

$ cat /dev/ttyXRUSB1

(Check the string be received correctly)
```

➢ RS485HD

1) Set to RS485 HD from BIOS, those command are under BIOS script.

```
Platcfg64E.efi 0x0471:0x0002

Platcfg64E.efi 0x0474:0x0002
```

Alternatively, use Dell application “Dell Command Configure” to switch BIOS configuration:

```
dcc.cctk -h --serial1

dcc.cctk --serial1

dcc.cctk --serial1=rs485
```

2) Set serial port mode

```
$ sudo stty -F /dev/ttyXRUSB0 ispeed 115200 ospeed 115200 -echo -onlcr -ixon -ixoff

$ sudo stty -F /dev/ttyXRUSB1 ispeed 115200 ospeed 115200 -echo -onlcr -ixon -ixoff
```

3) Transfer/Receive data between two ports (Wired RS485 HD between two serial ports on the device)
4) Transfer data:

```
$ sudo su

$ echo abcdefg > /dev/ttyXRUSB0

(Keep repeating this command to send data)
```

5) Receive data from another terminal by ssh from PC.

```
$ ssh admin@<IP addr of caracalla>

(passwd: admin)
```

```
$ sudo su
$ cat /dev/ttyXRUSB1
(Check the string be received correctly)
```

4.7 Setting of minicom

Hereunder describes how to setup a terminal emulation program minicom on the host machine to talk to debug serial port on Caracalla headless SKUs.

1) Install minicom:

   ```
   $ sudo snap install classic --devmode --beta
   $ sudo classic.create
   $ sudo classic
   $ (classic) sudo apt-get update
   $ (classic) sudo apt-get install minicom
   ```

2) Setting minicom:

   ```
   $ sudo minicom -s
   ```

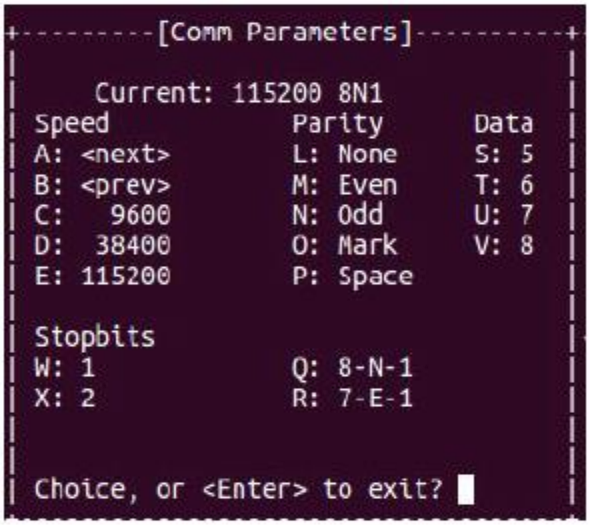
3) Choose ''Serial port setup'. Then, press A to edit the Serial Device to ttyUSB0 (it could be other number if there are more USB serial cable). Then, press Enter to exit:

   ```
   A - Serial Device : /dev/ttyUSB0
   ```

4) Press F, to disable Hardware Flow Control to 'No'
5) Press E, to edit Baud rate/Parity/Bits.

   ■ Press E, Q to configure as 115200 and 8-N-1

   ■ Press Enter to exit:

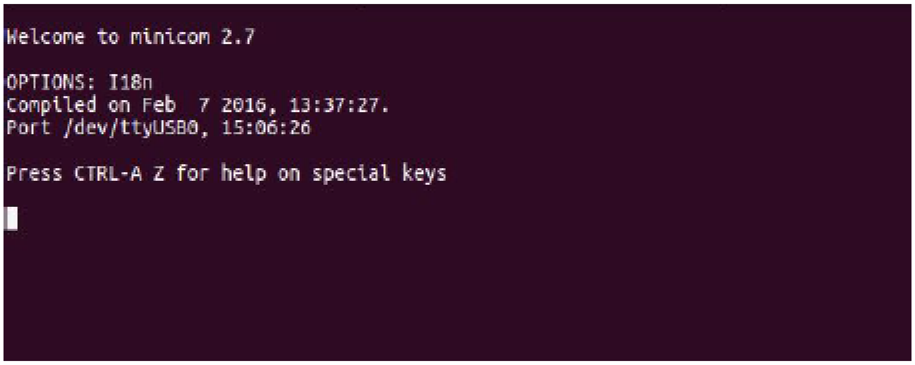


```
+---------[Comm Parameters]----------+
|                                     |
|     Current: 115200 8N1             |
| Speed             Parity     Data   |
| A: <next>         L: None    S: 5   |
| B: <prev>         M: Even    T: 6   |
| C:   9600         N: Odd     U: 7   |
| D:  38400         O: Mark    V: 8   |
| E: 115200         P: Space          |
|                                     |
| Stopbits                            |
| W: 1              Q: 8-N-1          |
| X: 2              R: 7-E-1          |
|                                     |
|                                     |
| Choice, or <Enter> to exit?         |
```

6) Press Enter to complete setting.
7) Choose "Save setup as dfl".
8) Choose "Exit from minicom".

- Start minicom as terminal program:

```
$ sudo minicom
```



```
Welcome to minicom 2.7

OPTIONS: I18n
Compiled on Feb  7 2016, 13:37:27.
Port /dev/ttyUSB0, 15:06:26

Press CTRL-A Z for help on special keys
```

- Exit minicom:

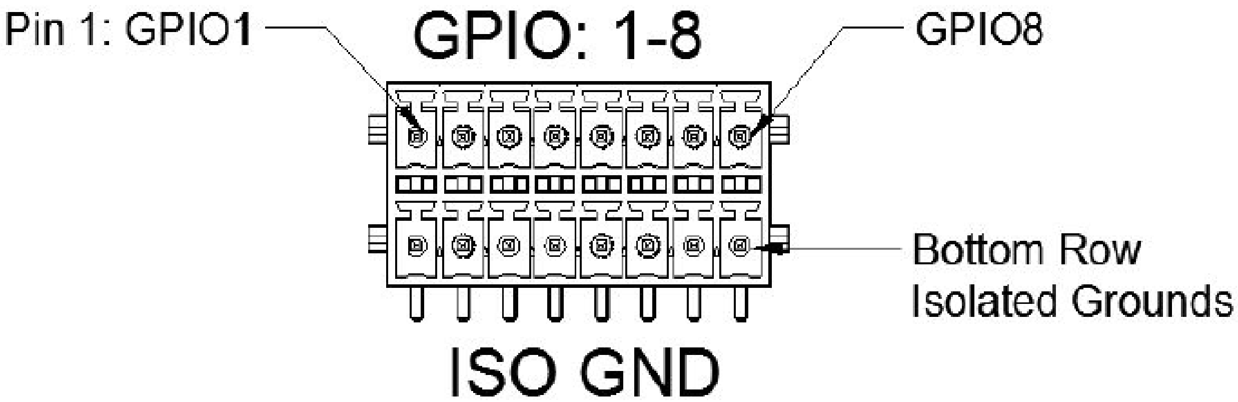
1) To exit Minicom when in terminal mode press 'Ctrl-A' to get a message bar at the bottom of the terminal window and then press 'X'.

4.8 GPIO

Support platform:

1) Edge Gateway 3001

GPIO controller AD5593R has 8 pins on the Gateway 3001 SKU. GPIO can be controlled by Linux standard GPIO interface in sysfs. The GPIOs number maps 330 to 337.



- Example 1 (as root):

1) Set GPIO 1 as output, value as 1

```
$ echo 330 > /sys/class/gpio/export

$ echo out > /sys/class/gpio/gpio330/direction

$ echo 1 > /sys/class/gpio/gpio330/value
```

- Example 2 (as root):

1) Set GPIO 8 as input, and read value

```
$ echo 337 > /sys/class/gpio/export

$ echo out > /sys/class/gpio/gpio337/direction

$ cat /sys/class/gpio/gpio337/value

0
```

- Example 3 (as root):

1) Connect GPIO 1 to 8
2) Read GPIO 8 pin value

```
$ cat /sys/class/gpio/gpio337/value

1
```

The detail of GPIO sysfs interface document:

https://www.kernel.org/doc/Documentation/gpio/sysfs.txt.

4.9 Zigbee (Hardware dependency)

This feature is only supported if hardware module presented, OS provides the capability of mutual communication between user space application and physical module. If there is a specific Zigbee programming requirement of user mode application, contact the hardware provider of that module for API documentation.

Supported platforms:

1) **Edge Gateway 3000/3001/3002/3003**
    - Qualified Zigbee module: Telegesis ETRX358USB
    - Qualified Zigbee module: Silicon Labs ETRX3587HR-D1

4.10 CAN/Controller Area Network

This feature is only supported if hardware module presented, OS provides the capability of mutual communication between user space application and physical module. If there is a specific CAN bus programming requirement of user mode application, contact the hardware provider of that module for API documentation.

Supported platforms:

1) **Edge Gateway 3002**
    - Qualified CAN module: Atmel ATSAME70N19A-CNT

CAN module is optional, find the device bus if HW presented:

```
for i in /dev/ttyACM*; do udevadm info $i | grep -q 03eb_2404_USB_CAN_FD && echo "path: /dev/$(basename $i)"; done
```

4.11 Sensors

Supported platforms:

1) **Edge Gateway 3001/3002/3003**

Sensor - Pressure	ST Micro LPS22HB
Sensor - Relative humidity and temperature	ST Micro HTS221
Sensor - 3-axis "femto" accelerometer	ST Micro LNG2DMTR

Industrial I/O Subsystem:

1) Query sensor devices

```
$ cat /sys/bus/iio/devices/iio:device*/name
```

   - hts221 <-- device0, Humidity and temp.
   - lng2dm_accel <-- device1, G-sensor
   - lps22hb <-- device2, Pressure

2) Humidity and temp.:

```
$ cat in_humidityrelative_offset

$ cat in_humidityrelative_raw

$ cat in_humidityrelative_scale

$ cat in_temp_offset

$ cat in_temp_raw

$ cat in_temp_scale
```

3) G-sensor:

```
$ cat in_accel_scale_available

$ cat in_accel_*_scale

$ cat in_accel_*_raw
```

4) Pressure:

```
$ cat in_pressure_raw

$ cat in_pressure_scale
```

4.12 Ignition pin

Supported platforms:

1) **Edge Gateway 3000/3001/3002/3003**

Ignition pin can be used to wake the system from S3, S4, and S5 power states. User will configure S3, S4, and S5 power states and graceful shutdown using OS power management system. The behavior can be configured in the OS.

Instruction:

```
$ snap set core system.power-key-action=reboot
```

Reference:

https://docs.ubuntu.com/core/en/reference/core-configuration

System.power-key-action

Available since: 2.23

Specify the action to take when the power button is pressed.

The configuration option accepts the following values:

- ignore: Do nothing.
- poweroff (default): Shut down the system.
- reboot: Reboot the system.
- halt: Halt the system.
- kexec: Directly boot a new kernel.
- suspend: Suspend the system.
- hibernate: Hibernate the system.
- hybrid-sleep: Suspend to both disk and RAM.
- lock: Screen-lock all running sessions.

5. System Power Management

5.1 Low Power State: S3/S4

- Sleep
  1) S3 is supported on Edge Gateway 3000/3001/3002/3003,

```
$ sudo systemctl suspend
```

- Hibernate
  1) S4 is supported on Edge Gateway 3000/3001/3002/3003.

```
$ sudo systemctl hibernate
```

5.2 Power Cycle

- System Reboot

```
$ sudo reboot
```

- System Power Off

```
$ sudo poweroff
```

5.3 System Wake Up

- System wake from LAN/WLAN (WLAN supported: S3/S4)
  1) Enable WoWLAN in BIOS
  2) Connect SUT to a wireless network

```
$ sudo network-manager.nmcli dev wifi connect $SSID password $PSK ifname wlan0
```

  3) Enable wowlan:

```
$ sudo iw phy0 wowlan enable magic-packet
```

  4) recheck its support status:

```
$ sudo iw phy phy0 wowlan show
```

  5) Make sure wlan0 is up and running with IP address
  6) Perform sleep

```
$ sudo systemctl sleep
```

  Or, perform hibernation

```
$ sudo systemctl hibernate
```

  7) Use another system to wake from wlan (Supported tools: wakeonlan, and etherwake)

```
$ sudo wakeonlan MAC
$ sudo etherwake MAC
```

6. Network Management

Network-Manager is a program selected to be native Snappy Connection Manger, the software handles multiple network devices, provides detection and configuration for system to automatically connect to network.
A command line utility *nmcli* is included with Network-Manager to support non-graphical user interface.

Reference: https://wiki.archlinux.org/index.php/NetworkManager

6.1 WWAN

1) Check if modem presents:

```
$ sudo modem-manager.mmcli –L
```

2) Check modem status by

```
$ sudo modem-manager.mmcli -m 0
```

3) Create profile

```
$ sudo network-manager.nmcli c add con-name test type gsm ifname ttyACM0 apn internet
```

4) Check wwan status by

```
$ network-manager.nmcli r wwan
```

5) Turn on wwan:

```
$ sudo network-manager.nmcli r wwan on
```

6) Find wwan0 in the interface list

```
$ ifconfig -a
```

7) Enable the connection profile:

```
$ sudo network-manager.nmcli c up test
```

8) Check Network Manager status

```
$ network-manager.nmcli d
```

9) Disable the connection profile:

```
$ sudo network-manager.nmcli c down test
```

10) Check Network Manager status

```
$ network-manager.nmcli d
```

6.2 WLAN

Operating mode value	WiFi station	softAP	BT/BLE modes supported	Clients supported by softAP
1	X		N/A	N/A
1		X	N/A	32
13	X		Dual (BT classic and BTLE)	N/A
14		X	Dual (BT classic and BTLE)	4
5	X		BT Classic	N/A
6		X	BT Classic	32

- Instructions to switch WLAN/BT modes:

1) Unload WLAN/BT driver

```
$ modprobe -r ven_rsi_sdio
```

2) Adjust the mode in /etc/modprobe.d/rs9113.conf
3) Reload the WLAN/BT driver

```
$ modprobe ven_rsi_sdio
```

4) Verify the operation mode

```
$ cat /sys/module/ven_rsi_sdio/parameters/dev_oper_mode
```

- Instructions to obtain WLAN connectivity:

1) Show network interfaces, which will list things like eth0, eth1, wlan0, mlan0, and etc...

```
$ network-manager.nmcli d
```

2) List wireless APs:

```
$ network-manager.nmcli d wifi
```

3) Wireless connection with nmcli: Run the following commands and replace $SSID, $PSK, and $WIFI_INTERFACE of your environment.

✓ *Connect:*

```
$ sudo network-manager.nmcli dev wifi connect $SSID password $PSK ifname $WIFI_INTERFACE
```

Or

```
$ sudo network-manager.nmcli dev wifi connect $SSID password $PSK
```

✓ *Disconnect:*

```
$ sudo network-manager.nmcli dev disconnect $WIFI_INTERFACE
```

6.3 SoftAP (Virtual wireless Access-Point)

This feature depends on Wi-Fi card and associated driver support to act as a wireless access point.

Instructions:

1) Check the status

```
$ wifi-ap.status
```

2) SoftAP is default disabled, following command to turn it on:

```
$ wifi-ap.config set disabled=false
```

This will mark the access point as being enabled.

3) If you want to secure the WiFi access point with WPA 2 personal you have to change two configuration items.

```
$ wifi-ap.config set wifi.security=wpa2 wifi.security-passphrase=Test1234
```

This enables WPA2 security with the passphrase set to Test1234.

Note: remember to always quote or escape the value when it contains special characters or spaces, eg. 'My WiFi', 'Pa$$word' or "Alan's AP"

Reference: https://docs.ubuntu.com/core/en/stacks/network/wifi-ap/docs/index

6.4 Bluetooth

1. Bluetooth (example: BT Keyboard)

a) Run following command to start bluetoothctl console:

```
#bluez.bluetoothctl -a
```

****Following steps are run in bluetoothctl console****

b) Power on the device:

```
$power on
```

c) Register agent for keyboard:

```
$agent KeyboardOnly

$default-agent
```

d) Put controller in pairable mode:

```
$pairable on
```

e) Scan nearby bluetooth device:

```
$scan on
```

f) Stop Scanning after bluetooth keyboard is found:

```
$scan off
```

g) Pair bluetooth

```
$pair [MAC address of bluetooth keyboard]
```

h) Enter PIN Code on bluetooth keyboard if needed

i) Trust the bluetooth keyboard

```
$trust [MAC address of bluetooth keyboard]
```

j) Connect to bluetooth keyboard:

```
$connect [MAC address of bluetooth keyboard]
```

k) Quit bluetoothctl console

```
$quit
```

l) Use bluetooth keyboard to input

7. Ubuntu Core OS Recovery (Recovery Partition)

The following steps refer to different methods through which the Ubuntu Core Linux OS can be recovered to the factory image.

7.1 Recover from on-board storage (Recovery Partition)

Recovery Partition, is a native solution for users to recover their software back to factory state. Reset the system back to the factory image if you have any of the following situations:

- You are unable to start the operating system normally.
- The operating system is damaged.

➢ Instructions to trigger OS Recovery (In Boot Menu):

Supported platform: Edge gateway 3003

1) Connect a keyboard and monitor the system, follow steps below:
2) Power on the system
3) Press F12 when the Dell logo is displayed on the screen to enter the boot menu.
4) Select Factory Restore from the boot menu.
   Note: All data will lost.
5) Press “Y” when below message prompted up:
6) Factory Restore will delete all user data, are you sure? [Y/N]

➢ Instructions to trigger OS Recovery (During BIOS POST):

Supported platform: Edge gateway 3000, 3001, 3002, 3003

1) Connect keyboard
2) Power on the system
3) Press combination key < Ctrl+F > to trigger OS Recovery process.

➢ Instructions to trigger OS Recovery (In Core OS):

Supported platform: Edge gateway 3000, 3001, 3002, 3003

```
$ sudo efibootmgr -n $(efibootmgr | grep "factory_restore" | sed 's/Boot//g' | sed 's/[^0-9A-B]*//g') ; reboot
```

7.2 Visualized Cloud LED indication during recovery process:

Visualized LED indication to expose the progress of image recovery process, user can interact with headless devices to recover Ubuntu image in blind mode.

System state	LED Indication	
	Power LED	**Cloud LED**
Power on	**OFF > ON**	**OFF**
"Factory Restore" entered		
System is waiting for user's input # Timeout: 30s		**Blinking**
✓ User input [y/Y] [Enter] # Take ~60s or more to finish, then reboot		**ON**
✓ User input [n/others] [Enter] # Do nothing and reboot immediately	**ON > OFF**	

8. Ubuntu Core OS Recovery (Recovery USB)

On supported platforms, it's allowed to download factory image from dell.com .to restore system by external media kit. More details on creating a bootable key at the following URL.

Reference: https://www.dell.com/support/

8.1 Hardware and software requirements

1. USB 2.0 or USB 3.0 flash drive (8GB min).
2. A released Ubuntu Core image (*.img)

8.2 Instructions to Create Bootable USB (Using Windows)

Ubuntu Core Linux OS USB key can be created in Windows environment using Win32DiskImager software. This software is available at Sourceforge. Once the Win32DiskImager software is installed, download the OS image in compressed zip format. Unzip the downloaded image twice to get ".img" image file.

Note: All the contents in the USB key being used will be erased and OS image will be written on that USB key when you follow the steps below.

Instructions:

1. Insert the USB key in your Windows system where the Win32DiskImager tool is installed as well as where the OS image .img file is downloaded.
2. Launch Win32DiskImager tool.
3. The USB key that was inserted would show up in the Win32DiskImager tool under "Device" menu with a drive letter assigned, eg., it might show up a D: or E: etc.,
4. Using the folder button on the Win32DiskImager tool, browse and select the downloaded and un-compressed OS Image file, ie, the .img file.
5. Once the image is read by the tool, select "Write" button on the Win32DiskImager tool. This will write the whole image on to the USB disk

Once completed, exit from the Win32DiskImager tool and safely remove the USB key from the Windows system.

8.3 Instructions to Create Bootable USB (Using Ubuntu Desktop)

Instructions:

1. Insert USB flash drive into Ubuntu Workstation.
2. Extract Ubuntu Core image as *.img.xz file format
3. Start “Terminal” application. It can be found by typing “Terminal” in the Unity Dash.
4. Explicitly unmount the USB drive as it may be auto-mounted when inserted.
5. Type the following command and press Enter:

   ```
   sudo umount /dev/sdb1
   ```

   Note: The “sdb1” may need to be replaced with the actual name of the drive on the system.

6. Type the following command and press Enter:

   ```
   xzcat stlouis-a02-20161118-0.img.xz | sudo dd of=/dev/sdb bs=32M ; sync
   ```

   Note: The “stlouis-a02-20161118-0.img.xz” may needs to be replaced with the actual name of the image you have downloaded.

   Note: The “sdb” may need to be replaced with the actual name of the drive on the system.

   Warning: dd command will erase the content of the drive it writes to.

7. Unmount and remove USB flash drive.

8.4 Flash Ubuntu Image to machine By Recovery USB

Instructions:

1. Connect necessary devices, insert USB flash drive.
2. Power-up and boot-up the device from USB.

   Note: Power LED On.

3. The installation USB disk will flash Ubuntu Core installation image into storage automatically.

   Note: Cloud LED Blinking

4. After USB installation complete, it will shutdown the system.

   Note: Power LED Off.

5. Remove the USB disk.
6. Log file created at the USB thumb drive, Path:\installer_log\YYYYMMDDHHmmSS-ServiceTag.log

9. Q & A

1. **How to add a new user if libnss-extrausers is pre-installed?**

```
$sudo adduser --extrausers testuser
```

2. **How to change user's password?**

```
$sudo passwd <user-name>
```

3. **How to remount Snappy 16 root file system as read/write?**

   Snappy 16 rootfs is Read-Only.