Dell Edge Gateway 3200

Software User's Guide

Regulatory Model: EGW-3200
Regulatory Type: EGW-3200-NA
July 2024
Rev. A03

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Introduction

The Dell Edge Gateway 3200 supports Windows 10 IoT Enterprise 2019 and Ubuntu 20.04 LTS. The setup procedures for each of these operating systems are detailed in the following chapters.

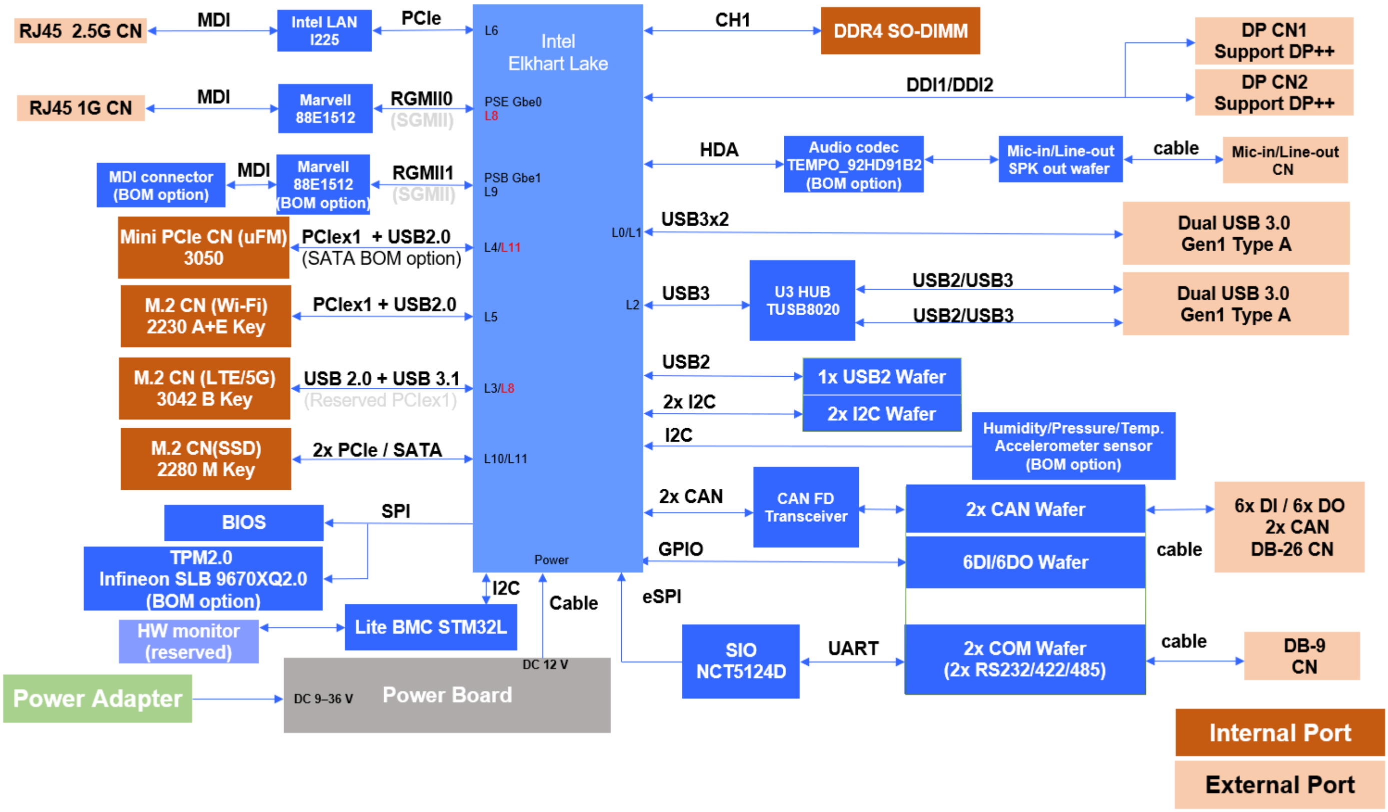


Figure 1. System block diagram

The following table defines the acronyms and abbreviations used throughout this document.

Table 1. Acronyms and abbreviations

Acronym or abbreviation	Definition
API	Application Programming Interfaces
BIOS	Basic Input Output System
CPU	Central Processing Unit
DI	Digital Input
DO	Digital Output
GPIO	General Purpose Input Output
HWMon	Hardware Monitor
I2C	Inter Integrated Circuit
LAN	Local Area Network
LTSC	Long Term Servicing Channel

Table 1. Acronyms and abbreviations (continued)

Acronym or abbreviation	Definition
PCI	Peripheral Component Interconnect
USB	Universal Serial Bus
UWF	Unified Write Filter
WDT	WatchDog Timer

2

Setting Up the Windows 10 Operating System

This chapter serves as a guide to install and use the Windows 10 IoT Enterprise 2019 operating system on the EGW-3200 hardware.

For more information on the Windows 10 operating system, see Microsoft Support.

ⓘ **NOTE:** For proper Windows boot up, please ensure the BIOS version used is 0.14.10 or above.

Topics:

Boot up and log in

Steps

1. Connect a keyboard, mouse, and monitor to the EGW-3200.
2. Power on the system. The system boots to the Windows 10 IoT Enterprise LTSC 2019 operating system.
3. Select your regional settings and keyboard layout. If needed, select the second keyboard layout. Otherwise, skip this step.
4. Connect to an available wireless or wired network. After the internet connection is established, the Windows license key is activated.
5. Read and Agree to the **End User License Agreement**.
6. Create a user account with a password.
7. After login, the system will reboot once for the settings to take effect.

Factory reset

About this task

Users can perform a factory reset of the Windows 10 IoT Enterprise 2019 LTSC on the EGW-3200 using the recovery operating system image on the boot partition. This resets the run-time image back to the standard Windows system, which does not contain any ODM-installed drivers. Users can download the necessary drivers from the Dell Technologies Support Site.

Steps

1. Connect a keyboard, mouse, and monitor to the system.
2. Power on the Edge Gateway and boot to the operating system's desktop.
3. Click the **Start** icon, hold the **Shift** key and click **Restart**.
4. Select **Troubleshoot** > **Reset this PC**.
5. Select **Reset this PC** > **Remove everything**.
6. Select **Fully clean the drive** > **Reset**.

System restore and backup recovery

Create a recovery drive

About this task

To recover from a major issue such as hardware failure, a recovery drive is needed to reinstall Windows 10. This section explains how to create a USB recovery drive. Personal files and any applications that did not come with the system will not be backed up.

Use a minimum of 4 GB USB storage and all data in the USB storage will be deleted. Perform the following steps to create a USB-based recovery drive.

Steps

1. In the search box next to the **Start** button, search for **Create a recovery drive** and then select it. You might be asked to enter an admin password or confirm your selection.
2. When the tool opens, make sure **Back up system files to the recovery drive** is selected and then select **Next**.
3. Connect a USB drive to your PC, select it, and then select **Next**.
4. Select **Create**. Many files need to be copied to the recovery drive, so this might take a while. After successfully creating the recovery drive, click **Finish**.

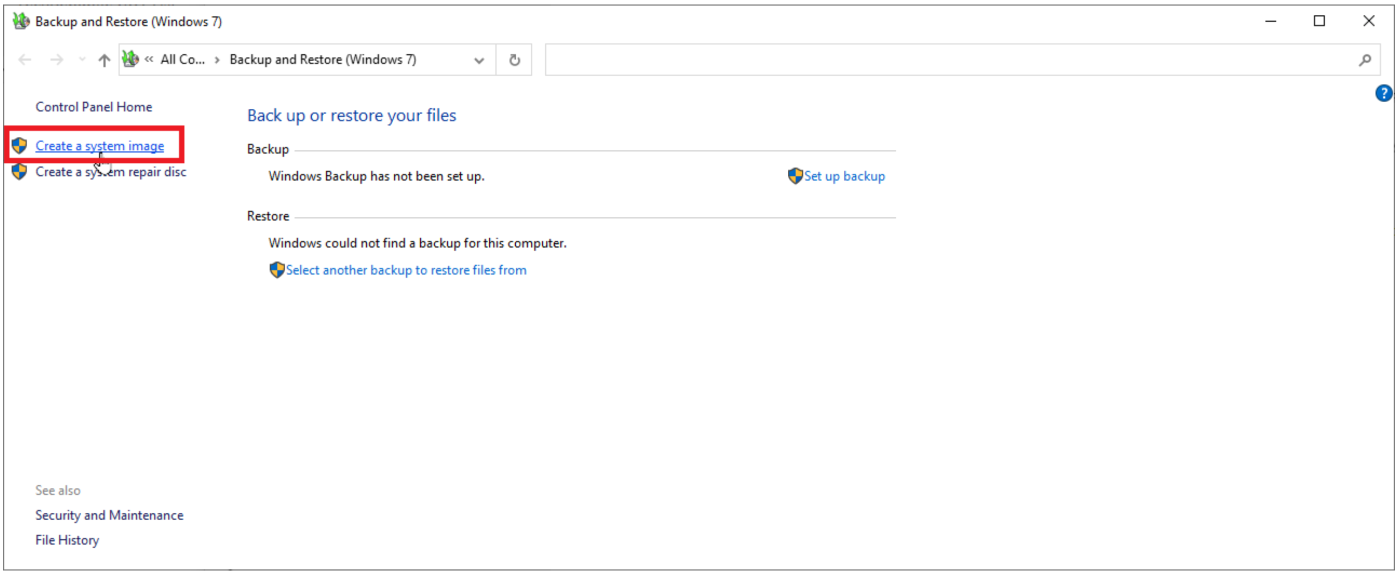
Create a system image

About this task

After successfully logging into Windows 10, the user can create a system image which can be used to restore the system in case of a Windows OS crash or hard disk failure.

Steps

1. Select **Control Panel** and Navigate to **Control Panel\System and Security\Backup and Restore (Windows 7)**.
2. In the **Backup and Restore (Windows 7)** window, click **Create a system image** in the upper-left corner.



Backup and Restore (Windows 7)

« All Co... › Backup and Restore (Windows 7)

Control Panel Home

Create a system image

Create a system repair disc

Back up or restore your files

Backup

Windows Backup has not been set up.

Set up backup

Restore

Windows could not find a backup for this computer.

Select another backup to restore files from

See also

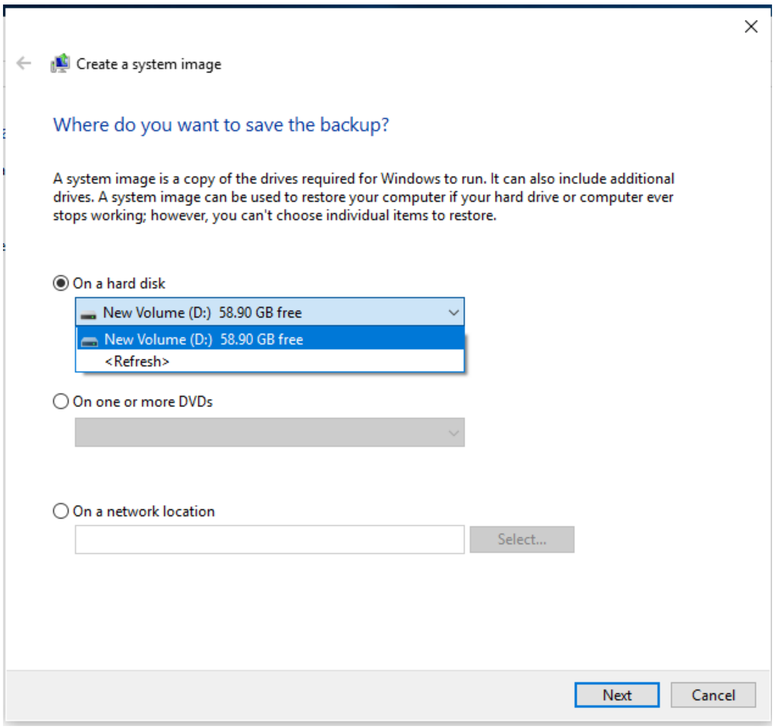
Security and Maintenance

File History

Figure 2. Create a system image

3. Windows looks for a backup destination on a hard drive, DVD, or network location. Choose an appropriate destination. Click **Next**.

   NOTE: In the following screenshot, a second SSD storage is used to create the backup.



Create a system image

Where do you want to save the backup?

A system image is a copy of the drives required for Windows to run. It can also include additional drives. A system image can be used to restore your computer if your hard drive or computer ever stops working; however, you can't choose individual items to restore.

● On a hard disk

New Volume (D:) 58.90 GB free

New Volume (D:) 58.90 GB free

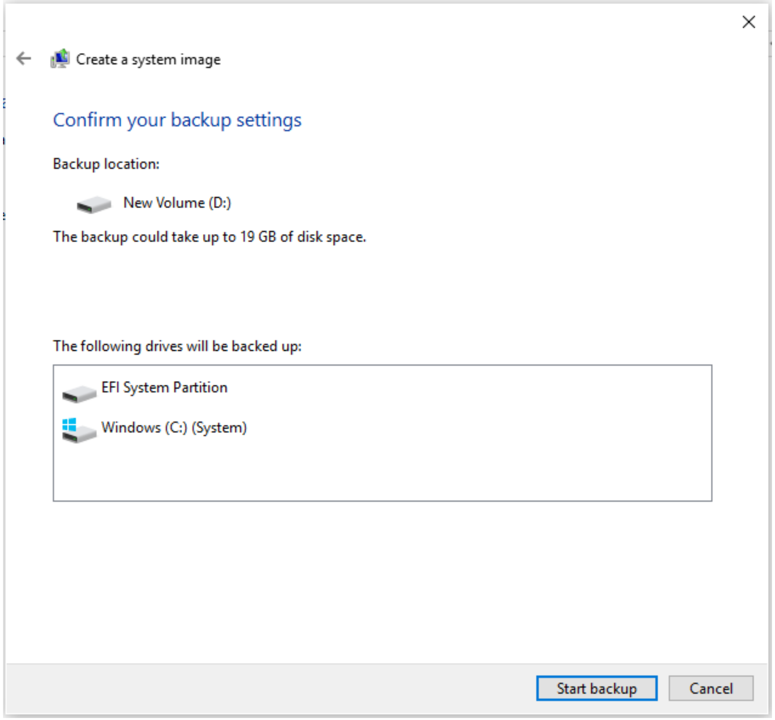
<Refresh>

○ On one or more DVDs

○ On a network location

Figure 3. Backup destination

4. Confirm which areas or partitions of your hard drive will be included in the image file, then click the **Start Backup** button.



Create a system image

Confirm your backup settings

Backup location:

New Volume (D:)

The backup could take up to 19 GB of disk space.

The following drives will be backed up:

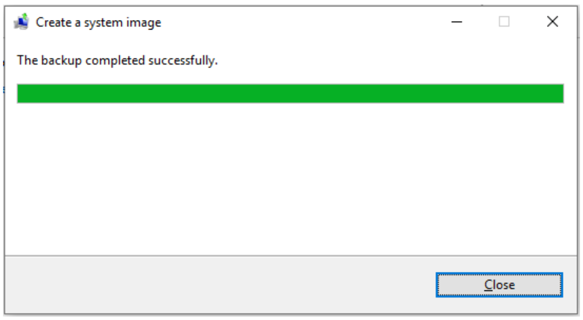
EFI System Partition

Windows (C:) (System)

Figure 4. Confirm backup

Results

Windows creates the system image file.



Create a system image

The backup completed successfully.

Figure 5. Backup completed successfully

Recover from system image

Steps

1. Connect the USB storage device that was created in Create a recovery drive.
2. Connect the hard drive or SSD that was used in Create a system image.
3. After power on, keep pressing **Delete** and go to the BIOS settings.
4. From **Save and Exit**, in **Boot Override**, select the USB storage device and press **Enter**.
5. At the **Choose your Keyboard layout** page, select the appropriate keyboard layout.
6. In the **Choose an option** window, go to **Troubleshoot** > **Advanced Options** > **System Image Recovery**. Follow the prompts in Windows to restore the system image file.

Results

Once the process is complete, the system restarts and boots into the updated system image.

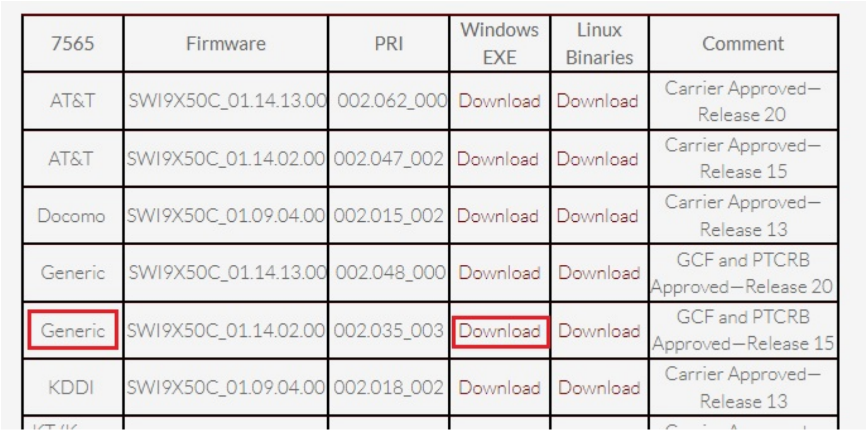
Security Baseline settings

The security settings in the image for the EGW-3200 default to those in the standard Windows 10 IoT Enterprise release. However, it is recommended to install Microsoft-provided security policies on top of this to enhance the security features in the device. Microsoft provides a set of policies called the Security Baseline with each Windows 10 release. Installing this Security Baseline is a good way to quickly enable recommended security settings on IoT devices. The Security Baseline is delivered as part of the Microsoft Security Compliance Toolkit. Detailed installation and customization instructions are available in the toolkit package.

4G module firmware update procedure

Steps

1. Download the firmware update tool (.exe) from the EM75xx Approved FW Packages page of the SEMTECH/Sierra Wireless website.



7565	Firmware	PRI	Windows EXE	Linux Binaries	Comment
AT&T	SWI9X50C_01.14.13.00	002.062_000	Download	Download	Carrier Approved–Release 20
AT&T	SWI9X50C_01.14.02.00	002.047_002	Download	Download	Carrier Approved–Release 15
Docomo	SWI9X50C_01.09.04.00	002.015_002	Download	Download	Carrier Approved–Release 13
Generic	SWI9X50C_01.14.13.00	002.048_000	Download	Download	GCF and PTCRB Approved–Release 20
Generic	SWI9X50C_01.14.02.00	002.035_003	Download	Download	GCF and PTCRB Approved–Release 15
KDDI	SWI9X50C_01.09.04.00	002.018_002	Download	Download	Carrier Approved–Release 13

Figure 6. 4G firmware update tool

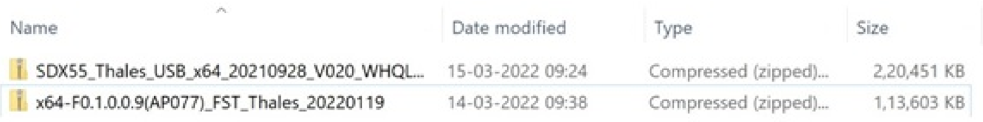
2. Right-click the .exe file and run as administrator. The firmware update runs automatically.

5G module firmware update procedure

Download Firmware Selector Tool and driver

Steps

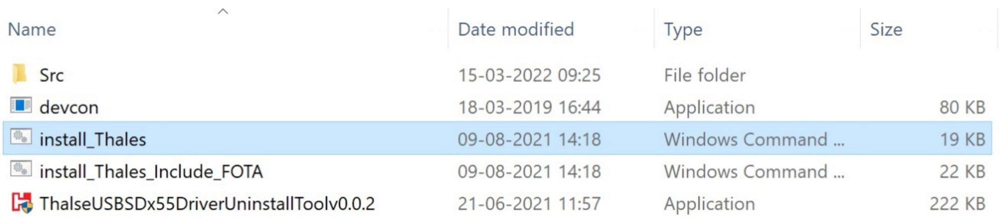
1. Download the Firmware Selector Tool from the EGW-3200 page of the Dell Technologies Support Site.
2. Unzip the files and open the unzipped folder.



Name	Date modified	Type	Size
SDX55_Thales_USB_x64_20210928_V020_WHQL...	15-03-2022 09:24	Compressed (zipped)...	2,20,451 KB
x64-F0.1.0.0.9(AP077)_FST_Thales_20220119	14-03-2022 09:38	Compressed (zipped)...	1,13,603 KB

Figure 7. Firmware tool and driver file

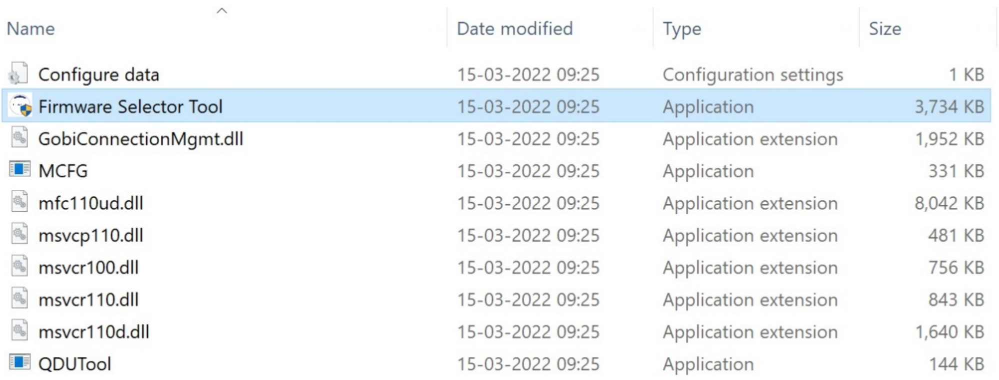
3. Save the driver to the following folder: **\F0.1.0.0.9_AP077\SDX55_Thales_USB_x64_20220208_V023_WHQL_INF_Injection\**.



Name	Date modified	Type	Size
Src	15-03-2022 09:25	File folder	
devcon	18-03-2019 16:44	Application	80 KB
install_Thales	09-08-2021 14:18	Windows Command ...	19 KB
install_Thales_Include_FOTA	09-08-2021 14:18	Windows Command ...	22 KB
ThalseUSBSDx55DriverUninstallToolv0.0.2	21-06-2021 11:57	Application	222 KB

Figure 8. 5G firmware driver

4. Save the **Firmware Selector Tool** to the following folder: **\F0.1.0.0.9_AP077 \x64-F0.1.0.0.9 (AP077)_FST_Thales_20220119\Utilities\x86-Firmware Selector Tool (V2.0.3.3)_Thales**.



Name	Date modified	Type	Size
Configure data	15-03-2022 09:25	Configuration settings	1 KB
Firmware Selector Tool	15-03-2022 09:25	Application	3,734 KB
GobiConnectionMgmt.dll	15-03-2022 09:25	Application extension	1,952 KB
MCFG	15-03-2022 09:25	Application	331 KB
mfc110ud.dll	15-03-2022 09:25	Application extension	8,042 KB
msvcp110.dll	15-03-2022 09:25	Application extension	481 KB
msvcr100.dll	15-03-2022 09:25	Application extension	756 KB
msvcr110.dll	15-03-2022 09:25	Application extension	843 KB
msvcr110d.dll	15-03-2022 09:25	Application extension	1,640 KB
QDUTool	15-03-2022 09:25	Application	144 KB

Figure 9. Firmware Selector Tool

Remove old and install new drivers

About this task

MV31-W modules require a WIN10 driver. However, this driver must be installed after removing old USB drivers that were automatically installed by WIN10 PC.

Steps

1. Before connecting the MV31-W module, open the **Device Manager**, click **View**, and select **Show hidden devices**.

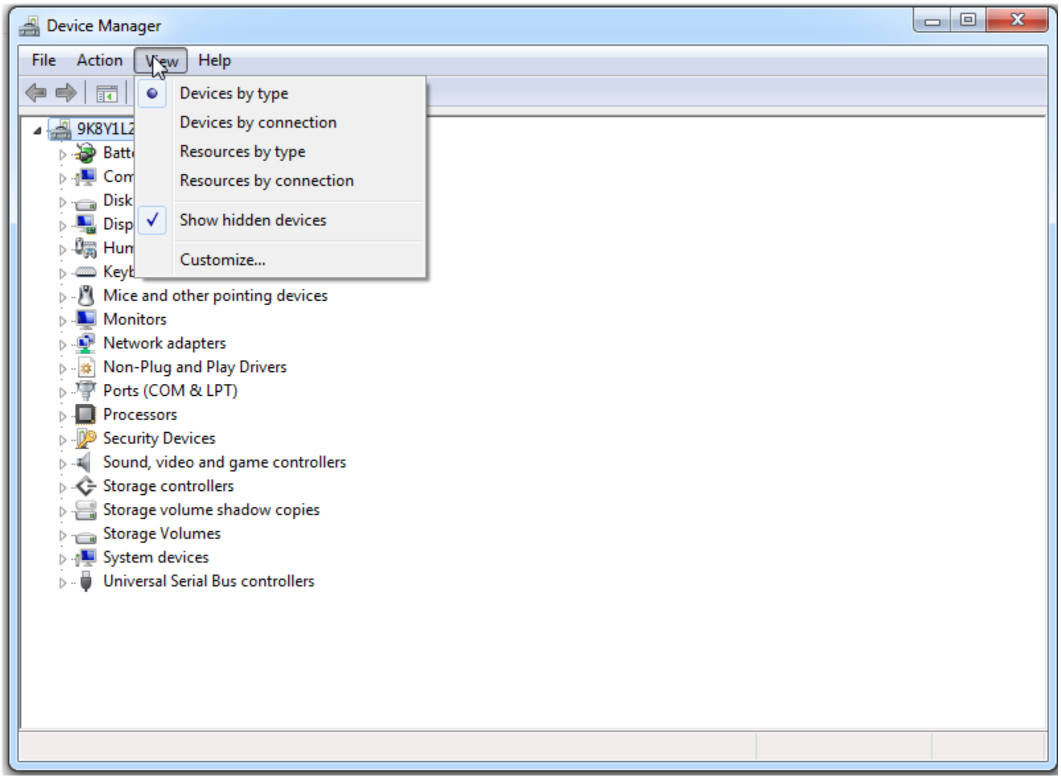
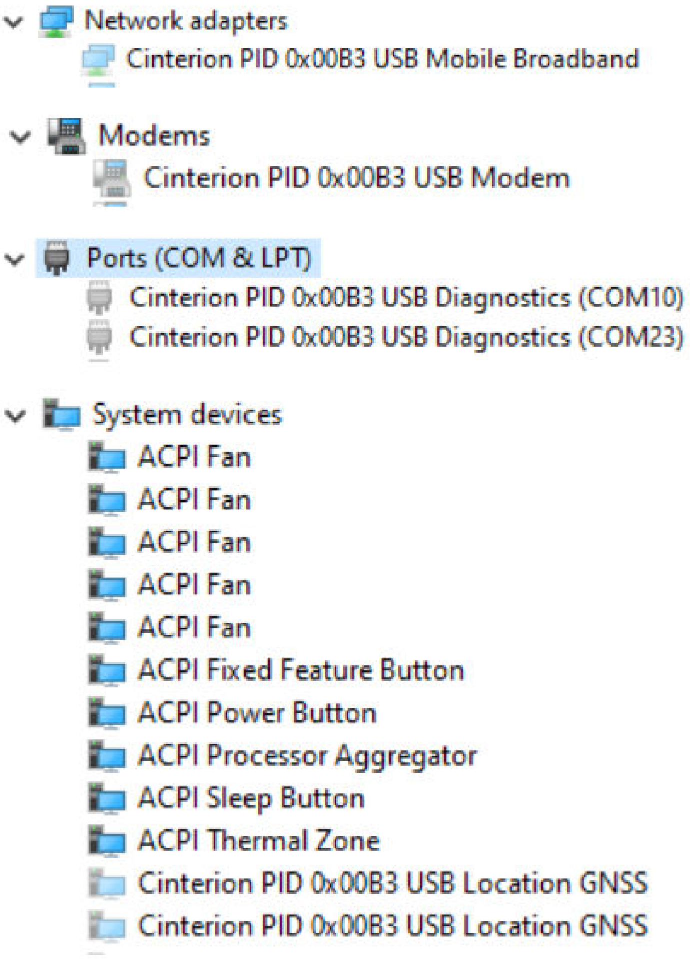


Figure 10. Show hidden devices

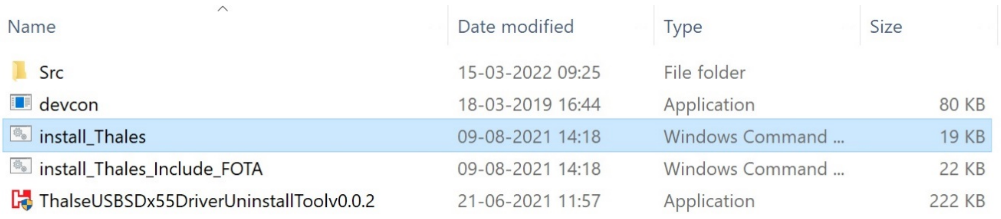
2. Remove (Uninstall) all devices that start with: **Cinterion PID 0x00B3**.



- Network adapters
  - Cinterion PID 0x00B3 USB Mobile Broadband
- Modems
  - Cinterion PID 0x00B3 USB Modem
- Ports (COM & LPT)
  - Cinterion PID 0x00B3 USB Diagnostics (COM10)
  - Cinterion PID 0x00B3 USB Diagnostics (COM23)
- System devices
  - ACPI Fan
  - ACPI Fan
  - ACPI Fan
  - ACPI Fan
  - ACPI Fan
  - ACPI Fixed Feature Button
  - ACPI Power Button
  - ACPI Processor Aggregator
  - ACPI Sleep Button
  - ACPI Thermal Zone
  - Cinterion PID 0x00B3 USB Location GNSS
  - Cinterion PID 0x00B3 USB Location GNSS

Figure 11. Uninstall Cinterion devices

3. Open the driver package folder (SDX55_Thales_USB_x64_*20220208_V023*_WHQL_INF_Injection) and run **install_Thales.cmd** as administrator.



Name	Date modified	Type	Size
Src	15-03-2022 09:25	File folder	
devcon	18-03-2019 16:44	Application	80 KB
install_Thales	09-08-2021 14:18	Windows Command ...	19 KB
install_Thales_Include_FOTA	09-08-2021 14:18	Windows Command ...	22 KB
ThalseUSBSDx55DriverUninstallToolv0.0.2	21-06-2021 11:57	Application	222 KB

Figure 12. Run driver command

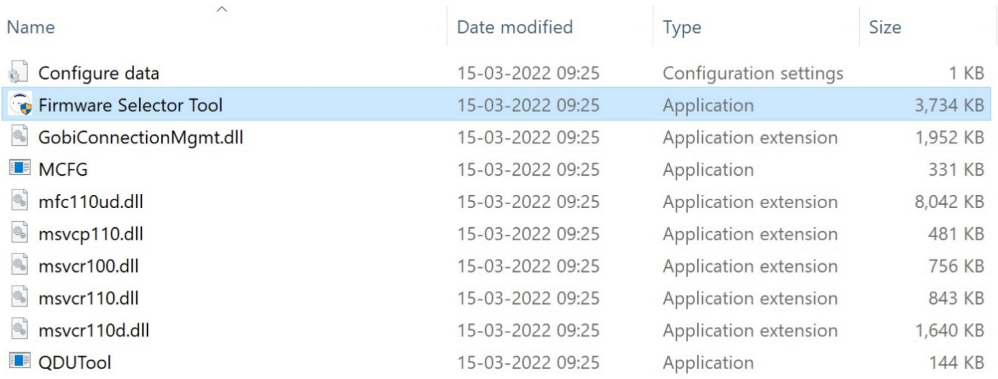
Update 5G firmware in Windows

About this task

After all the required drivers have been updated, use the **Firmware Selector Tool** provided by Thales DIS AIS to update the firmware.

Steps

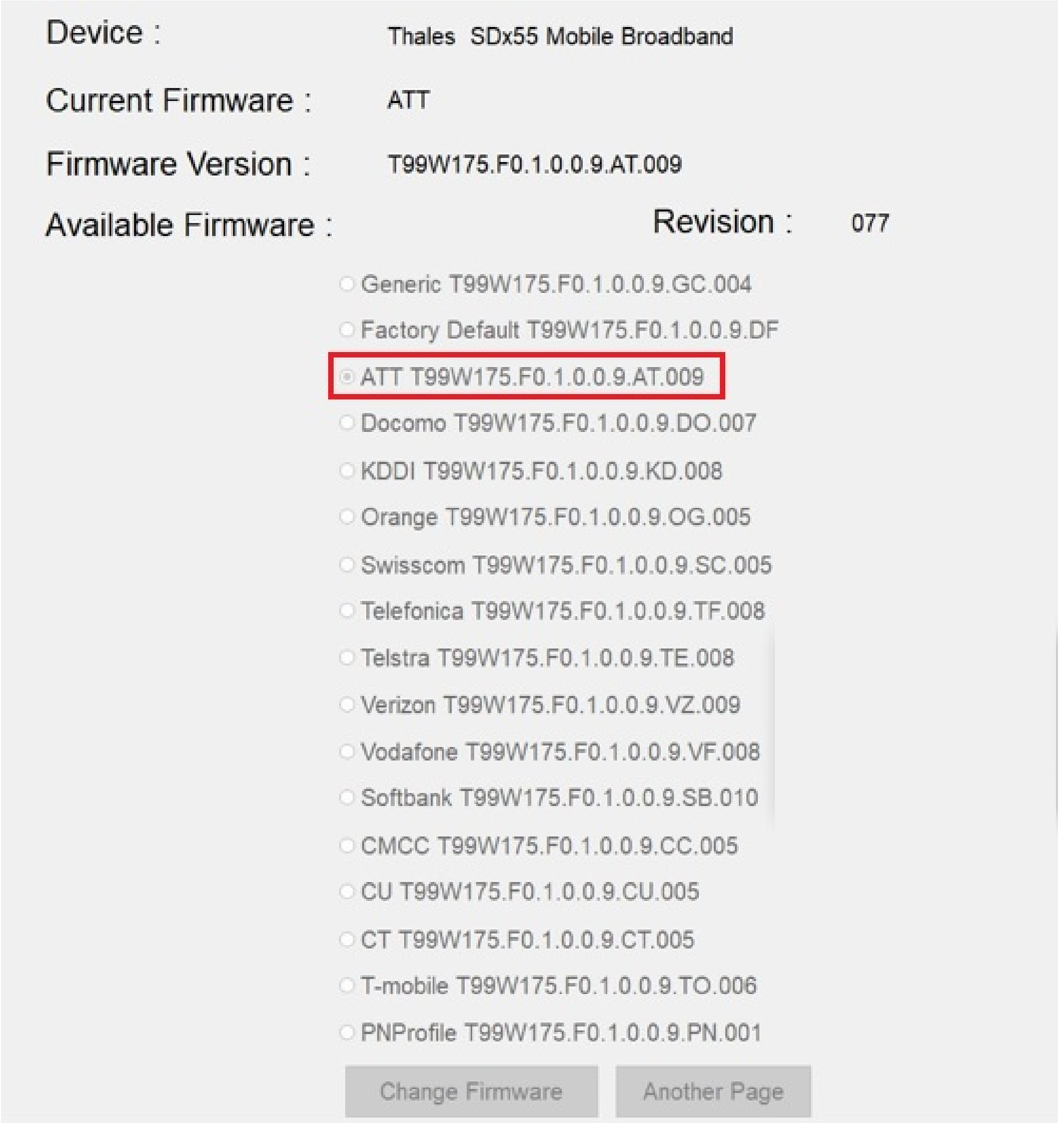
1. Go to **Utilities** > **Firmware**, and select the **Firmware Selector Tool**.



Name	Date modified	Type	Size
Configure data	15-03-2022 09:25	Configuration settings	1 KB
Firmware Selector Tool	15-03-2022 09:25	Application	3,734 KB
GobiConnectionMgmt.dll	15-03-2022 09:25	Application extension	1,952 KB
MCFG	15-03-2022 09:25	Application	331 KB
mfc110ud.dll	15-03-2022 09:25	Application extension	8,042 KB
msvcp110.dll	15-03-2022 09:25	Application extension	481 KB
msvcr100.dll	15-03-2022 09:25	Application extension	756 KB
msvcr110.dll	15-03-2022 09:25	Application extension	843 KB
msvcr110d.dll	15-03-2022 09:25	Application extension	1,640 KB
QDUTool	15-03-2022 09:25	Application	144 KB

Figure 13. Firmware Selector Tool

2. The tool will automatically select the ATT T99W175 firmware version to update.



Device : Thales SDx55 Mobile Broadband

Current Firmware : ATT

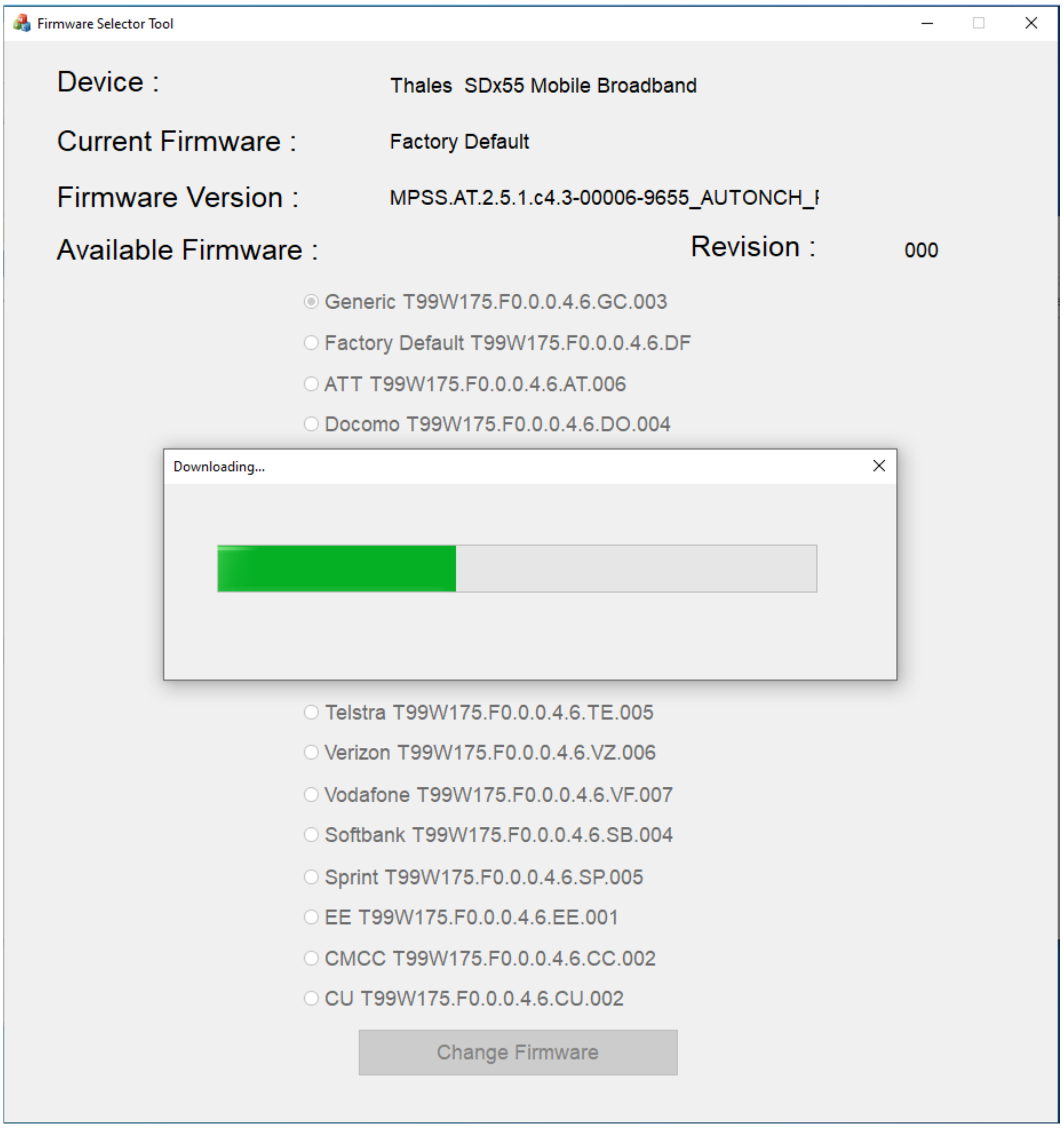
Firmware Version : T99W175.F0.1.0.0.9.AT.009

Available Firmware : Revision : 077

○ Generic T99W175.F0.1.0.0.9.GC.004
○ Factory Default T99W175.F0.1.0.0.9.DF
● ATT T99W175.F0.1.0.0.9.AT.009
○ Docomo T99W175.F0.1.0.0.9.DO.007
○ KDDI T99W175.F0.1.0.0.9.KD.008
○ Orange T99W175.F0.1.0.0.9.OG.005
○ Swisscom T99W175.F0.1.0.0.9.SC.005
○ Telefonica T99W175.F0.1.0.0.9.TF.008
○ Telstra T99W175.F0.1.0.0.9.TE.008
○ Verizon T99W175.F0.1.0.0.9.VZ.009
○ Vodafone T99W175.F0.1.0.0.9.VF.008
○ Softbank T99W175.F0.1.0.0.9.SB.010
○ CMCC T99W175.F0.1.0.0.9.CC.005
○ CU T99W175.F0.1.0.0.9.CU.005
○ CT T99W175.F0.1.0.0.9.CT.005
○ T-mobile T99W175.F0.1.0.0.9.TO.006
○ PNProfile T99W175.F0.1.0.0.9.PN.001

Figure 14. Firmware to update

3. Wait for the firmware download to finish.



Device : Thales SDx55 Mobile Broadband

Current Firmware : Factory Default

Firmware Version : MPSS.AT.2.5.1.c4.3-00006-9655_AUTONCH_I

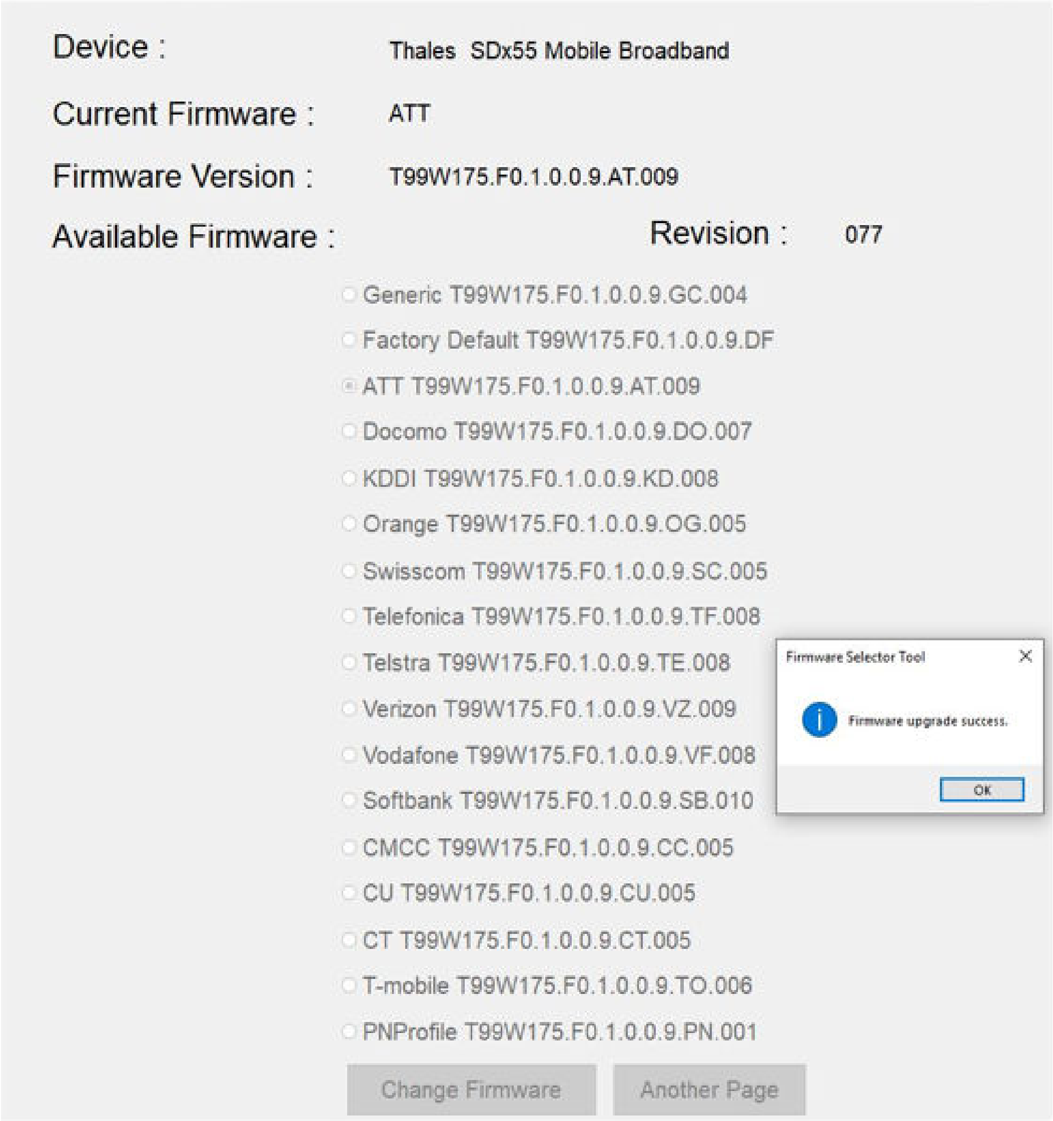
Available Firmware :

Revision : 000

● Generic T99W175.F0.0.0.4.6.GC.003
○ Factory Default T99W175.F0.0.0.4.6.DF
○ ATT T99W175.F0.0.0.4.6.AT.006
○ Docomo T99W175.F0.0.0.4.6.DO.004
○ Telstra T99W175.F0.0.0.4.6.TE.005
○ Verizon T99W175.F0.0.0.4.6.VZ.006
○ Vodafone T99W175.F0.0.0.4.6.VF.007
○ Softbank T99W175.F0.0.0.4.6.SB.004
○ Sprint T99W175.F0.0.0.4.6.SP.005
○ EE T99W175.F0.0.0.4.6.EE.001
○ CMCC T99W175.F0.0.0.4.6.CC.002
○ CU T99W175.F0.0.0.4.6.CU.002

Figure 15. Firmware download status bar

4. Once complete, the **Firmware upgrade success** message will appear. Click **OK**.



Device : Thales SDx55 Mobile Broadband

Current Firmware : ATT

Firmware Version : T99W175.F0.1.0.0.9.AT.009

Available Firmware : Revision : 077

- ○ Generic T99W175.F0.1.0.0.9.GC.004
- ○ Factory Default T99W175.F0.1.0.0.9.DF
- ● ATT T99W175.F0.1.0.0.9.AT.009
- ○ Docomo T99W175.F0.1.0.0.9.DO.007
- ○ KDDI T99W175.F0.1.0.0.9.KD.008
- ○ Orange T99W175.F0.1.0.0.9.OG.005
- ○ Swisscom T99W175.F0.1.0.0.9.SC.005
- ○ Telefonica T99W175.F0.1.0.0.9.TF.008
- ○ Telstra T99W175.F0.1.0.0.9.TE.008
- ○ Verizon T99W175.F0.1.0.0.9.VZ.009
- ○ Vodafone T99W175.F0.1.0.0.9.VF.008
- ○ Softbank T99W175.F0.1.0.0.9.SB.010
- ○ CMCC T99W175.F0.1.0.0.9.CC.005
- ○ CU T99W175.F0.1.0.0.9.CU.005
- ○ CT T99W175.F0.1.0.0.9.CT.005
- ○ T-mobile T99W175.F0.1.0.0.9.TO.006
- ○ PNProfile T99W175.F0.1.0.0.9.PN.001

Firmware Selector Tool

Firmware upgrade success.

Figure 16. Firmware upgrade success

Disabling bands in Windows after firmware update or SIM card change

Disabling bands is required if operating the device within the United States, as well as in other locations. The FCC sets limitations to radiated transmit power (EIRP) that are band-specific. Due to the 4G or 5G module installed, and the antennas provided by Dell Technologies, certain bands must be disabled. As such, additional commands must be sent to the module, under certain conditions outlined below, to meet FCC requirements.

Disabling bands is required:

- After the firmware in the module (4G or 5G) is updated
- After a SIM card change to a different telecom carrier

The following instructions provide information on how to correctly disable bands for the 4G or 5G module used in the EGW-3200.

Disable bands on 4G device in Windows

About this task

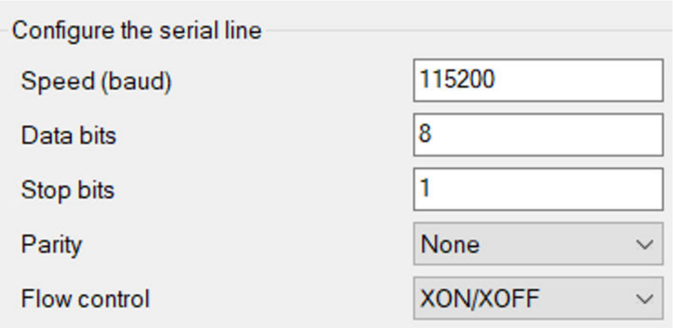
Disabling of these bands is required to meet FCC EIRP or other requirements.

Perform the following steps to disable the bands 42 and 48 on the 4G module.

Steps

1. Open the Putty application.

   Putty is used to send AT commands to the module within the Windows operating system.
2. Set the COM port to match that of the module in **Windows Device Manager**.
3. Under **Line discipline options**, set both **Local echo:** and **Local line editing:** radio buttons to the **Force on** setting.
4. In the **Configure the serial line** window, set the following serial interface parameters for communication with the module:
   - Speed (buad): 115200
   - Data bits: 8
   - Stop bis: 1
   - Parity: None
   - Flow control: XON/XOFF

   Configure the serial line

   Speed (baud): 115200

   Data bits: 8

   Stop bits: 1

   Parity: None

   Flow control: XON/XOFF

   Figure 17. Configure the serial line

5. Open the COM port defined previously using Putty.
6. Run the following command:

   ```
   at!entercnd="A710"
   ```

   This command is required before any other commands can be sent.
7. To set a profile called 0A that can be called upon with the band mask settings, run the following command:

   ```
   at!band=0A,"Disable LTE B42,B48",100600000EC00000,00002500BA0E19DF,0000000000000002
   ```

8. To set the profile to 0A, as defined in the previous step, run the following command:

   ```
   at!band=0A
   ```

9. To confirm that band settings are set to 0A and not some other setting, run the following command:

   ```
   at!band?
   ```

10. To reset the device for new band settings to take effect, run the following command:

    ```
    at!reset
    ```

    Reset takes a few minutes, then the device is available again.

    NOTE: Close the Putty terminal immediately after sending this command.

Disable bands on 5G device in Windows

About this task

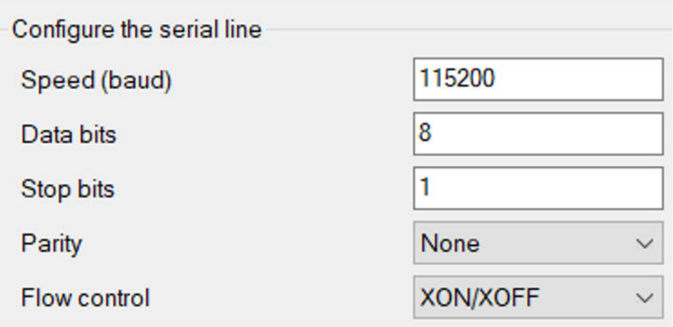
Disabling of these bands is required to meet FCC EIRP or other requirements.

Perform the following steps to disable the bands 30, 42, and 48 on the 5G module.

Steps

1. Open the Putty application.

   Putty is used to send AT commands to the module within the Windows operating system.
2. Set the COM port to match that of the module in **Windows Device Manager**.
3. Under **Line discipline options**, set both **Local echo:** and **Local line editing:** radio buttons to the **Force on** setting.
4. In the **Configure the serial line** window, set the following serial interface parameters for communication with the module:
   - Speed (buad): 115200
   - Data bits: 8
   - Stop bis: 1
   - Parity: None
   - Flow control: XON/XOFF

   Configure the serial line

Speed (baud)	115200
Data bits	8
Stop bits	1
Parity	None
Flow control	XON/XOFF

   Figure 18. Configure the serial line

5. Open the COM port defined previously using Putty.
6. To recover existing default band settings from the module, run the following command:

   ```
   at^slband
   ```

7. To disable bands 30, 42, and 48, run the following command:

   ```
   at^slband=LTE,1,30,42,48
   ```

   This requires a module reset to take effect.
8. To display band settings to confirm that bands 30, 42, and 48 are disabled, run the following command:

   ```
   at^slband?
   ```

9. To reset the device for new band settings to take effect, run the following command:

   ```
   at+reset
   ```

   Reset takes a few minutes, then the device is available again.

   NOTE: Close the Putty terminal immediately after sending this command.

Windows 10 IoT Enterprise LTSC basic functions

The EGW-3200 provides various interfaces. The following sections provide further details on these interfaces.

UART controller

For setting the port type of serial ports 1 and 2, change the BIOS settings as detailed in the following table.

Table 2. UART controller settings

S. No	Port type	Connector	Device node	BIOS setting configuration
1	RS232/422/485	DB9	COM1	**Advanced** > **Onboard Devices Configuration** > **COM1 Control**, select **RS232/422/485**
2	RS232/422/485	DB9	COM2	**Advanced** > **Onboard Devices Configuration** > **COM2 Control**, select **RS232/422/485**

TPM support

Windows 10 IoT Enterprise LTSC 2019 supports TPM 2.0. For more information on TPM resources, see the Trusted Platform Module Technology Overview from Microsoft.

RHProxy driver - I2C and GPIO

The RHProxy driver enables user mode access to I2C and GPIO (GPIO from the Intel chipset). For details about Windows RHProxy, refer to Enable user mode access to GPIO, I2C, and SPI. The BIOS of the EGW-3200 is already updated with the necessary changes for enabling RHProxy for the I2C and GPIO pins.

The following table shows the I2C and GPIO-friendly names and pin mappings.

Table 3. I2C and GPIO names and pin mappings

S No.	Peripheral detail	Hardware signal name	Name/Number to use with RHProxy	Comments
1	GPIO Pin 0	DO2	0	GPIO number to use for RHProxy: 0
2	GPIO Pin 1	DO3	1	-
3	GPIO Pin 2	DO1	2	-
4	GPIO Pin 3	DO0	3	-
5	GPIO Pin 4	I2C1_GPIO	4	I2C1 (CN13) interrupt pin
6	GPIO Pin 5	I2C0_GPIO	5	I2C0 (CN13) interrupt pin
7	GPIO Pin 6	User LED 1	6	-
8	GPIO Pin 7	User LED 2	7	-
9	GPIO Pin 8	User LED 3	8	-
10	GPIO Pin 9	DI0	9	-
11	GPIO Pin 10	DI1	10	-
12	GPIO Pin 11	DI2	11	-
13	GPIO Pin 12	DI3	12	-
14	GPIO Pin 13	DI4	13	-

Table 3. I2C and GPIO names and pin mappings (continued)

S No.	Peripheral detail	Hardware signal name	Name/Number to use with RHProxy	Comments
15	GPIO Pin 14	DI5	14	-
16	GPIO Pin 15	DO4	15	-
17	GPIO Pin 16	DO5	16	-

System shutdown and restart

Steps

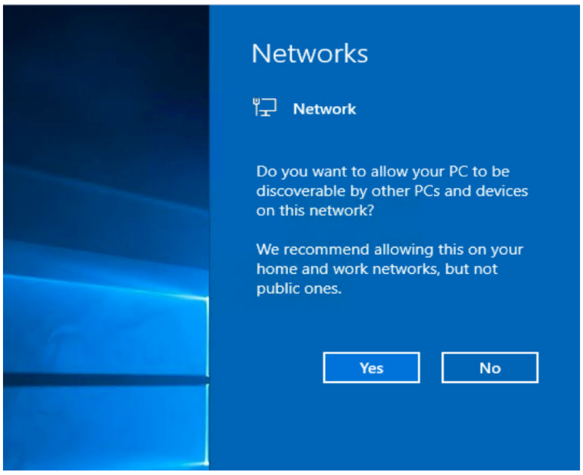
1. Click the **Start** icon.
2. Click **Power**, then select **Restart** or **Shut down**.

Configure LAN network

Steps

1. Connect an Ethernet cable to the Ethernet port.

   The following prompt is displayed:



Networks

Do you want to allow your PC to be discoverable by other PCs and devices on this network?

We recommend allowing this on your home and work networks, but not public ones.

Figure 19. Prompt for discoverable in network

2. Select **Yes**.

Optional expansion modules

The EGW-3200 supports several expansion modules, in mini PCI express (mPCIe), M.2, and I2C formats. The required Windows software package is already installed in the Windows image for the following modules. Refer to the website of the manufacturer for more details.

Table 4. Optional expansion modules

S No.	Format	Interface details	Reference link to manufacturer product page
1	mPCIe	EMUC-B202 Isolated Canbus	EMUC-B202 Product Page
2	mPCIe	EMPL-G2P1 GbE with PoE out	EMPL-G2P1 Product Page
3	mPCIe	EMP2-X4S2 Isolated RS-422 and RS-485	EMP2-X4S2 Product Page

Table 4. Optional expansion modules (continued)

S No.	Format	Interface details	Reference link to manufacturer product page
4	mPCIe	EMP2-X2S1 Isolated RS-232	EMP2-X2S1 Product Page
5	mPCIe	EMPL-G201 Isolated GbE LAN	EMPL-G201 Product Page
6	M.2 2230	WiFi AX210	Intel Wi-Fi 6E AX210 Product Page
7	M.2 3042	EM7565 4G LTE-Advanced Pro Module	EM7565 Product Page
8	M.2 3042	MV31-W 5G Ultra High Speed IoT Modem Card	MV31 Product Page
9	Internal I2C wafer	ADLINK 55-49071 Isolated DI/O	N/A

Configure WWAN network

Prerequisites

Follow the procedures in the service manual to install and configure the WWAN module and the corresponding carrier USIM card for the system.

About this task

After the WWAN module and the SIM cards are installed, perform the following steps.

Steps

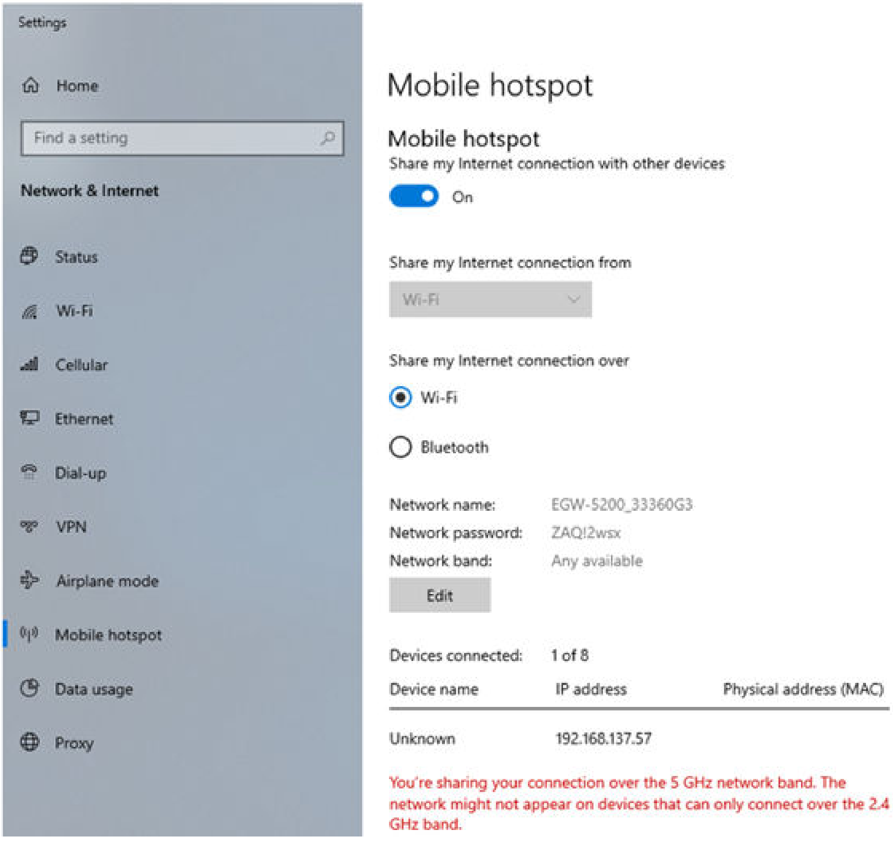
1. Click the **Start** icon.
2. Type Settings and click the **Settings** app.
3. Select **Network & Internet**.
4. Locate the WWAN connection in the **WiFi** section and select the entry to connect and disconnect from the WWAN adapter.

Enable Mobile hotspot

About this task

Steps

1. Go to the Mobile hotspot settings in **Settings** > **Network & Internet** > **Mobile hotspot**.
2. Change the **Share my Internet connection with other devices** setting to **On**.



Mobile hotspot

Mobile hotspot

Share my Internet connection with other devices

On

Share my Internet connection from

Wi-Fi

Share my Internet connection over

● Wi-Fi

○ Bluetooth

Network name: EGW-5200_33360G3

Network password: ZAQ!2wsx

Network band: Any available

Devices connected: 1 of 8

Device name	IP address	Physical address (MAC)
Unknown	192.168.137.57	

You're sharing your connection over the 5 GHz network band. The network might not appear on devices that can only connect over the 2.4 GHz band.

Figure 20. Mobile hotspot settings

3. Confirm that the **Network name** can be found from end devices, and connect it to ensure that the network function is working properly.

Configure Bluetooth

Steps

1. Click the **Start** icon.
2. Type Settings and click **Settings**.
3. Select **Devices** from the **Settings** menu, then select **Bluetooth** from the menu on the left panel.

Cellular network configuration

If the optional cellular network (4G or 5G) is used, see the Cellular settings in Windows page from Microsoft for information about configuration and usage.

DSSA

Dual SIM Single Active (DSSA) is the only form of multi-SIM operation that is fully supported in Windows 10. DSSA allows for two SIM cards to be used with the modem, with the restriction that only one SIM can be active at any given time.

For more information, go to the Dual SIM Single Active page from Microsoft.

Accessing GPS

Go to the Windows location service and privacy page from Microsoft for information about accessing the GPS and for various Windows settings.

Use the Unified Write Filter

Prerequisites

UWF is installed.

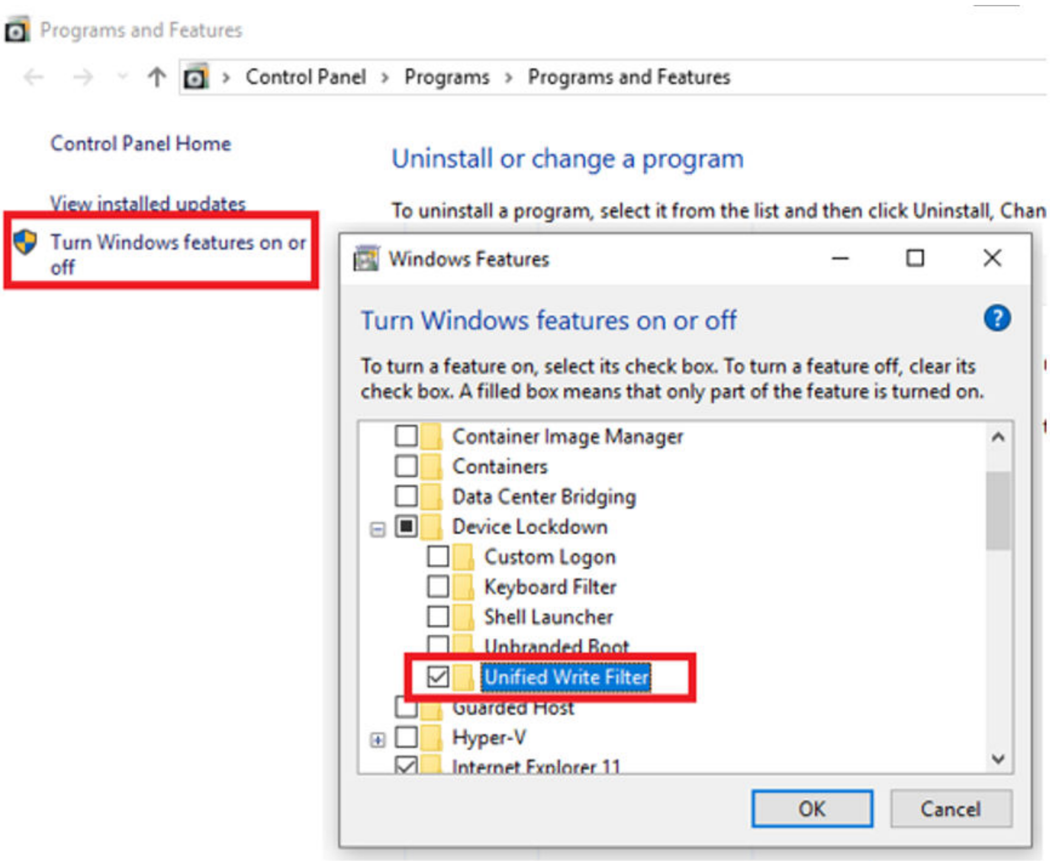
About this task

The Unified Write Filter (UWF) is an optional Windows 10 feature.

For detailed information, see Use the Unified Write Filter (UWF) feature from Microsoft.

Steps

1. Configure UWF. The first time you enable UWF on your device, UWF makes the following changes to your system to improve the performance of UWF:
   - Paging files are disabled.
   - System restore is disabled.
   - SuperFetch (also known as SysMain service) is disabled.
   - File indexing service is turned off.
   - Fast boot is disabled.
   - Defragmentation service (also known as Optimize drives service) is turned off.
   - BCD setting **bootstatuspolicy** is set to **ignoreallfailures**.
2. To enable UWF on a running device, perform the following steps:
   a. Click **Start**, then type **Turn Windows features on or off**.
   b. In the **Windows Features** window, expand the **Device Lockdown** node, and check **Unified Write Filter** > **OK**. There will be a notification for necessary restart.


Programs and Features
Control Panel › Programs › Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Uninstall or change a program
To uninstall a program, select it from the list and then click Uninstall, Chan
Windows Features
OK
Cancel

Turn Windows features on or off

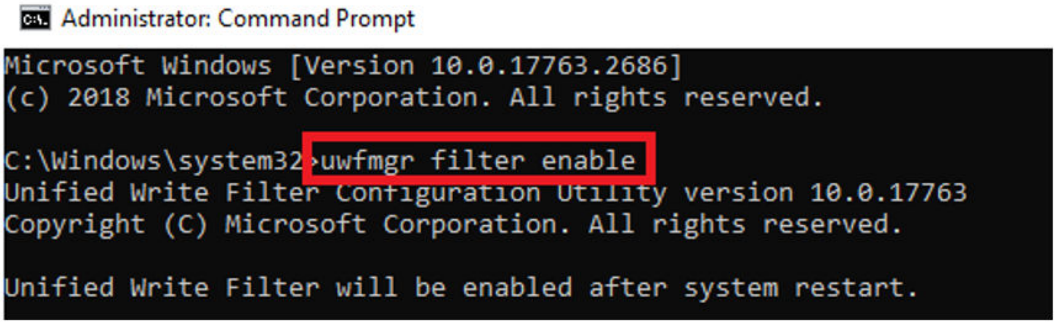
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- □ Container Image Manager
- □ Containers
- □ Data Center Bridging
- ■ Device Lockdown
  - □ Custom Logon
  - □ Keyboard Filter
  - □ Shell Launcher
  - □ Unbranded Boot
  - ☑ Unified Write Filter
- □ Guarded Host
- □ Hyper-V
- ☑ Internet Explorer 11

Figure 21. UWF in Windows Features

c. There will be a notification for reboot, click **Restart Now**.

3. To enable the filter, use the Windows Command Prompt: `uwfmgr filter enable`

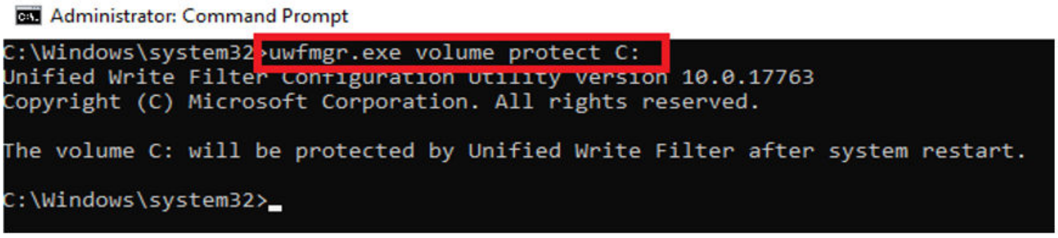


Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.2686]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>uwfmgr filter enable
Unified Write Filter Configuration Utility version 10.0.17763
Copyright (C) Microsoft Corporation. All rights reserved.

Unified Write Filter will be enabled after system restart.
```

Figure 22. UWF enable

4. To enable write protection for a drive, use the Windows Command Prompt: `uwfmgr.exe volume protect C:`

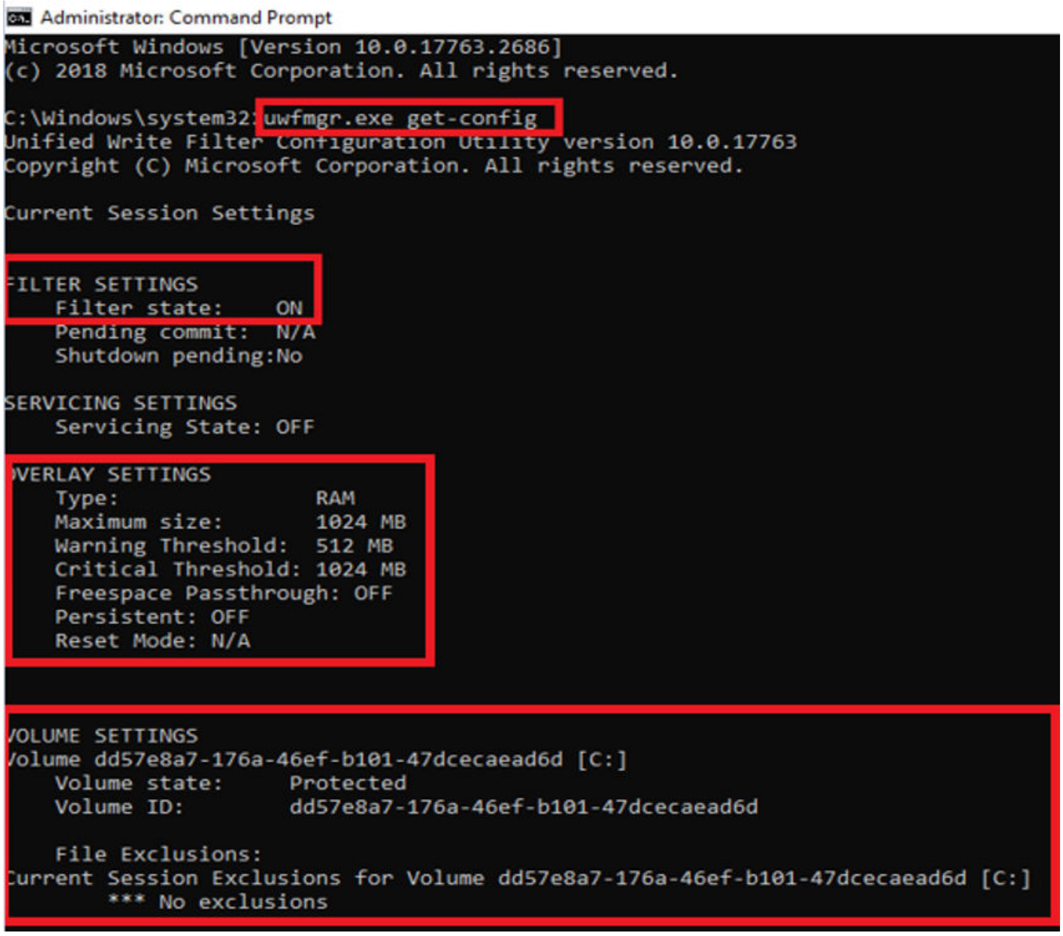


Administrator: Command Prompt

```
C:\Windows\system32>uwfmgr.exe volume protect C:
Unified Write Filter Configuration Utility version 10.0.17763
Copyright (C) Microsoft Corporation. All rights reserved.

The volume C: will be protected by Unified Write Filter after system restart.

C:\Windows\system32>_
```

Figure 23. UWF volume protect

5. Restart the computer.
6. To confirm that UWF is running, use the Windows Command Prompt: `uwfmgr.exe get-config`



```
Microsoft Windows [Version 10.0.17763.2686]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>uwfmgr.exe get-config
Unified Write Filter Configuration Utility version 10.0.17763
Copyright (C) Microsoft Corporation. All rights reserved.

Current Session Settings


FILTER SETTINGS
    Filter state:     ON
    Pending commit:   N/A
    Shutdown pending:No

SERVICING SETTINGS
    Servicing State: OFF

OVERLAY SETTINGS
    Type:                RAM
    Maximum size:        1024 MB
    Warning Threshold:   512 MB
    Critical Threshold: 1024 MB
    Freespace Passthrough: OFF
    Persistent: OFF
    Reset Mode: N/A


VOLUME SETTINGS
Volume dd57e8a7-176a-46ef-b101-47dcecaead6d [C:]
    Volume state:      Protected
    Volume ID:         dd57e8a7-176a-46ef-b101-47dcecaead6d

    File Exclusions:
Current Session Exclusions for Volume dd57e8a7-176a-46ef-b101-47dcecaead6d [C:]
        *** No exclusions
```

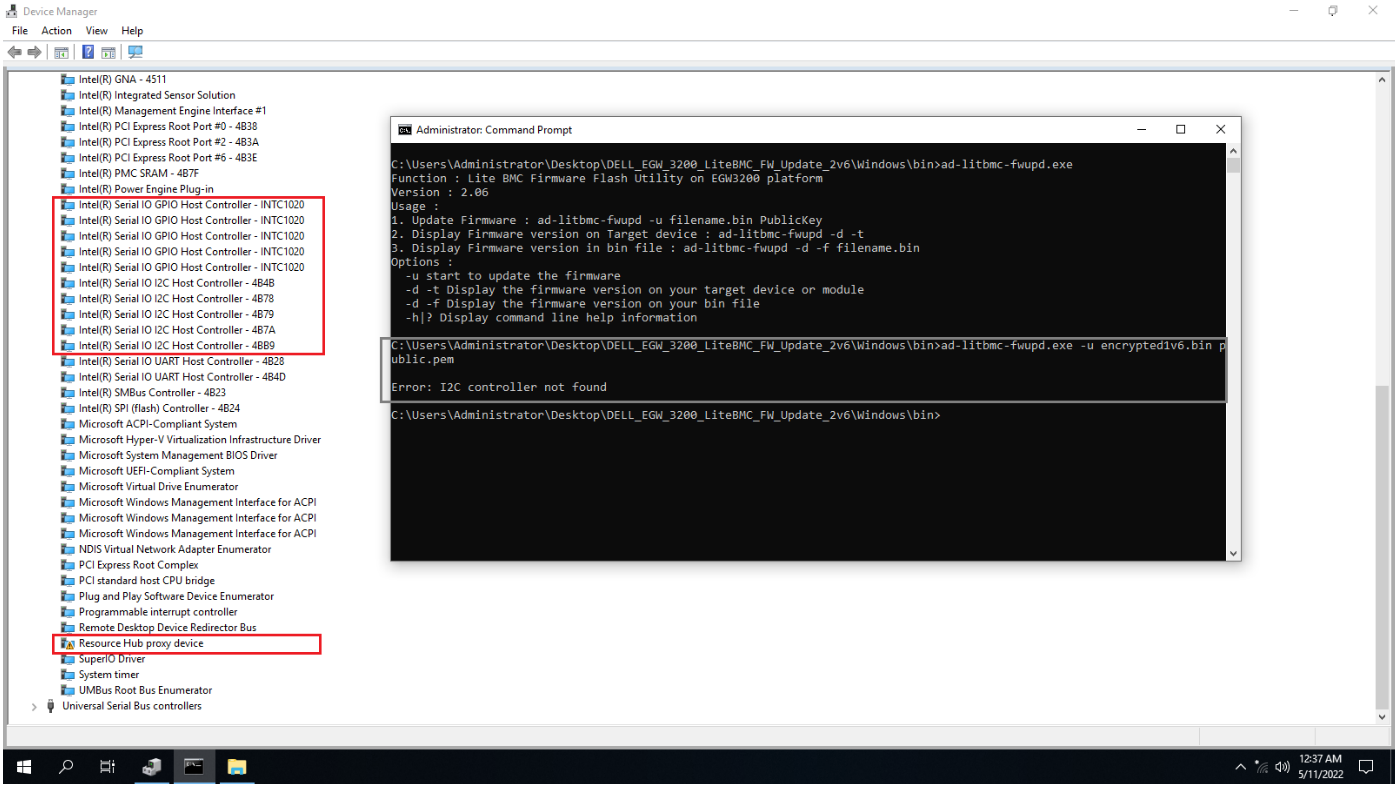
Figure 24. UWF get config

BMC firmware update procedure

Steps

1. Confirm that the Intel Serial IO - I2C and GPIO drivers are installed.

   If the I2C driver is not installed, there will be a yellow triangle with an exclamation point over the menu icon in **System devices > Resource Hub proxy device** in the **Device Manager**.



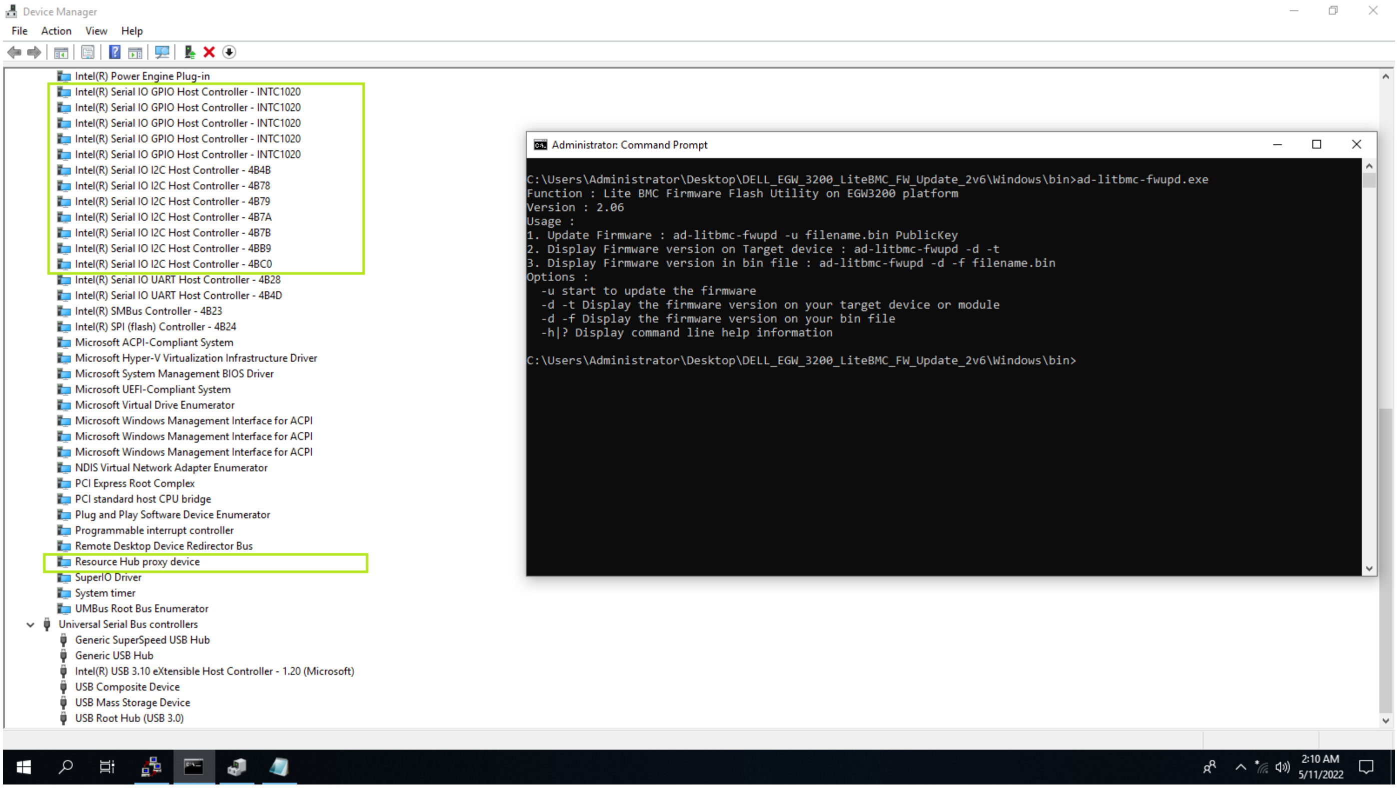
Intel(R) GNA - 4511
Intel(R) Integrated Sensor Solution
Intel(R) Management Engine Interface #1
Intel(R) PCI Express Root Port #0 - 4B38
Intel(R) PCI Express Root Port #2 - 4B3A
Intel(R) PCI Express Root Port #6 - 4B3E
Intel(R) PMC SRAM - 4B7F
Intel(R) Power Engine Plug-in
Intel(R) Serial IO GPIO Host Controller - INTC1020
Intel(R) Serial IO GPIO Host Controller - INTC1020
Intel(R) Serial IO GPIO Host Controller - INTC1020
Intel(R) Serial IO GPIO Host Controller - INTC1020
Intel(R) Serial IO GPIO Host Controller - INTC1020
Intel(R) Serial IO I2C Host Controller - 4B4B
Intel(R) Serial IO I2C Host Controller - 4B78
Intel(R) Serial IO I2C Host Controller - 4B79
Intel(R) Serial IO I2C Host Controller - 4B7A
Intel(R) Serial IO I2C Host Controller - 4BB9
Intel(R) Serial IO UART Host Controller - 4B28
Intel(R) Serial IO UART Host Controller - 4B4D
Intel(R) SMBus Controller - 4B23
Intel(R) SPI (flash) Controller - 4B24
Microsoft ACPI-Compliant System
Microsoft Hyper-V Virtualization Infrastructure Driver
Microsoft System Management BIOS Driver
Microsoft UEFI-Compliant System
Microsoft Virtual Drive Enumerator
Microsoft Windows Management Interface for ACPI
Microsoft Windows Management Interface for ACPI
Microsoft Windows Management Interface for ACPI
NDIS Virtual Network Adapter Enumerator
PCI Express Root Complex
PCI standard host CPU bridge
Plug and Play Software Device Enumerator
Programmable interrupt controller
Remote Desktop Device Redirector Bus
Resource Hub proxy device
SuperIO Driver
System timer
UMBus Root Bus Enumerator
Universal Serial Bus controllers

```
C:\Users\Administrator\Desktop\DELL_EGW_3200_LiteBMC_FW_Update_2v6\Windows\bin>ad-litbmc-fwupd.exe
Function : Lite BMC Firmware Flash Utility on EGW3200 platform
Version : 2.06
Usage :
1. Update Firmware : ad-litbmc-fwupd -u filename.bin PublicKey
2. Display Firmware version on Target device : ad-litbmc-fwupd -d -t
3. Display Firmware version in bin file : ad-litbmc-fwupd -d -f filename.bin
Options :
  -u start to update the firmware
  -d -t Display the firmware version on your target device or module
  -d -f Display the firmware version on your bin file
  -h|? Display command line help information

C:\Users\Administrator\Desktop\DELL_EGW_3200_LiteBMC_FW_Update_2v6\Windows\bin>ad-litbmc-fwupd.exe -u encrypted1v6.bin p
ublic.pem

Error: I2C controller not found

C:\Users\Administrator\Desktop\DELL_EGW_3200_LiteBMC_FW_Update_2v6\Windows\bin>
```

Figure 25. I2C controller not found

If this is the case, perform the following steps:

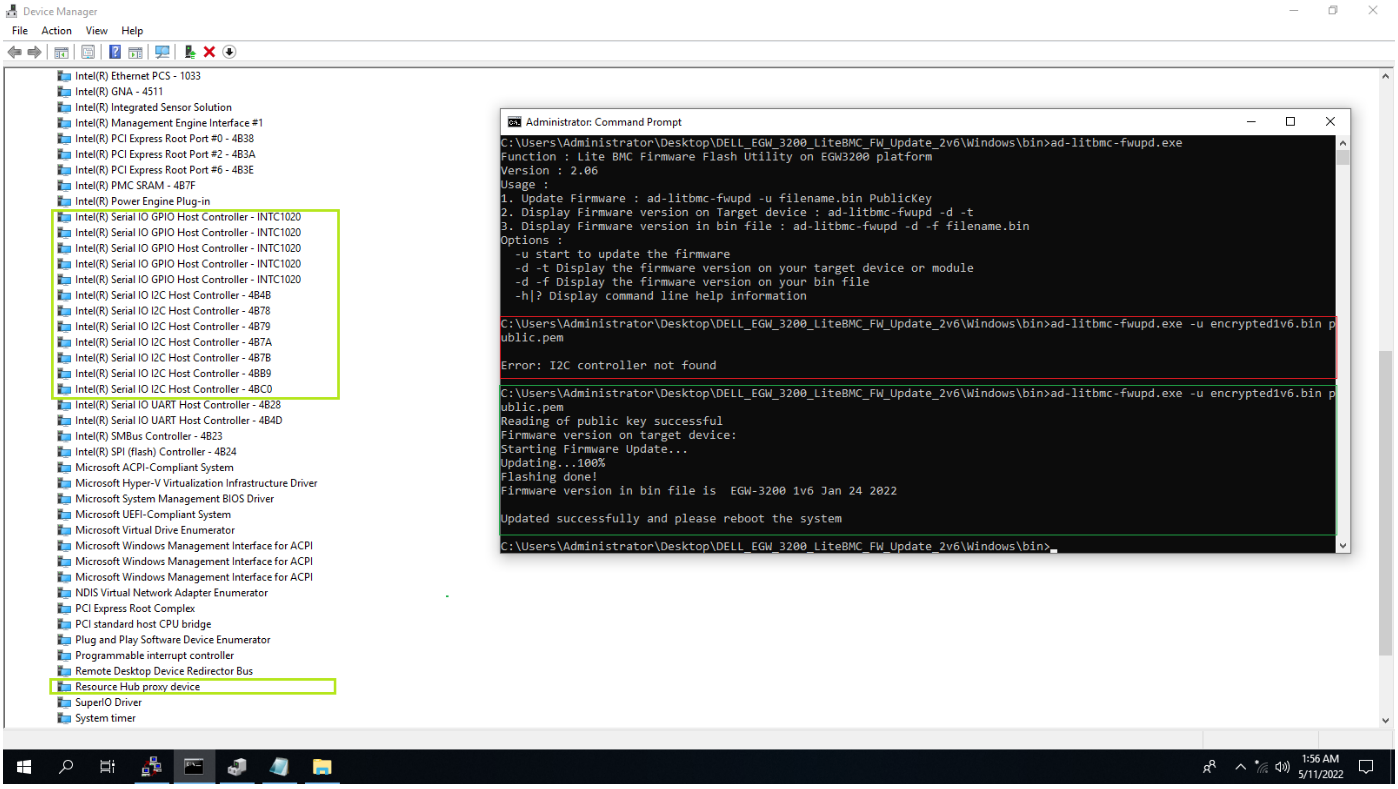
a. Download both drivers from the EGW-3200 page of the Dell Technologies Support Site.
b. Install the drivers. When all the required drivers are installed, there is no yellow triangle with an exclamation point over the icon in the device manager.


Device Manager
File Action View Help
Intel(R) Power Engine Plug-in
Intel(R) Serial IO GPIO Host Controller - INTC1020
Intel(R) Serial IO GPIO Host Controller - INTC1020
Intel(R) Serial IO GPIO Host Controller - INTC1020
Intel(R) Serial IO GPIO Host Controller - INTC1020
Intel(R) Serial IO GPIO Host Controller - INTC1020
Intel(R) Serial IO I2C Host Controller - 4B4B
Intel(R) Serial IO I2C Host Controller - 4B78
Intel(R) Serial IO I2C Host Controller - 4B79
Intel(R) Serial IO I2C Host Controller - 4B7A
Intel(R) Serial IO I2C Host Controller - 4B7B
Intel(R) Serial IO I2C Host Controller - 4BB9
Intel(R) Serial IO I2C Host Controller - 4BC0
Intel(R) Serial IO UART Host Controller - 4B28
Intel(R) Serial IO UART Host Controller - 4B4D
Intel(R) SMBus Controller - 4B23
Intel(R) SPI (flash) Controller - 4B24
Microsoft ACPI-Compliant System
Microsoft Hyper-V Virtualization Infrastructure Driver
Microsoft System Management BIOS Driver
Microsoft UEFI-Compliant System
Microsoft Virtual Drive Enumerator
Microsoft Windows Management Interface for ACPI
Microsoft Windows Management Interface for ACPI
Microsoft Windows Management Interface for ACPI
NDIS Virtual Network Adapter Enumerator
PCI Express Root Complex
PCI standard host CPU bridge
Plug and Play Software Device Enumerator
Programmable interrupt controller
Remote Desktop Device Redirector Bus
Resource Hub proxy device
SuperIO Driver
System timer
UMBus Root Bus Enumerator
Universal Serial Bus controllers
Generic SuperSpeed USB Hub
Generic USB Hub
Intel(R) USB 3.10 eXtensible Host Controller - 1.20 (Microsoft)
USB Composite Device
USB Mass Storage Device
USB Root Hub (USB 3.0)
Administrator: Command Prompt
2:10 AM
5/11/2022

```
C:\Users\Administrator\Desktop\DELL_EGW_3200_LiteBMC_FW_Update_2v6\Windows\bin>ad-litbmc-fwupd.exe
Function : Lite BMC Firmware Flash Utility on EGW3200 platform
Version : 2.06
Usage :
1. Update Firmware : ad-litbmc-fwupd -u filename.bin PublicKey
2. Display Firmware version on Target device : ad-litbmc-fwupd -d -t
3. Display Firmware version in bin file : ad-litbmc-fwupd -d -f filename.bin
Options :
  -u start to update the firmware
  -d -t Display the firmware version on your target device or module
  -d -f Display the firmware version on your bin file
  -h|? Display command line help information

C:\Users\Administrator\Desktop\DELL_EGW_3200_LiteBMC_FW_Update_2v6\Windows\bin>
```

Figure 26. Drivers installed

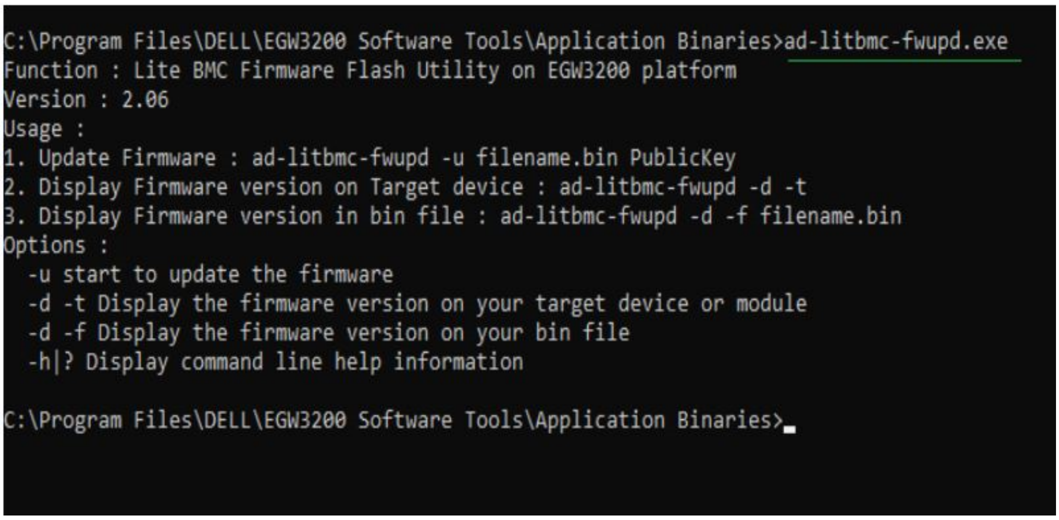
c. When prompted, reboot the system.


Device Manager
File Action View Help
Intel(R) Ethernet PCS - 1033
Intel(R) GNA - 4511
Intel(R) Integrated Sensor Solution
Intel(R) Management Engine Interface #1
Intel(R) PCI Express Root Port #0 - 4B38
Intel(R) PCI Express Root Port #2 - 4B3A
Intel(R) PCI Express Root Port #6 - 4B3E
Intel(R) PMC SRAM - 4B7F
Intel(R) Power Engine Plug-in
Intel(R) Serial IO GPIO Host Controller - INTC1020
Intel(R) Serial IO GPIO Host Controller - INTC1020
Intel(R) Serial IO GPIO Host Controller - INTC1020
Intel(R) Serial IO GPIO Host Controller - INTC1020
Intel(R) Serial IO GPIO Host Controller - INTC1020
Intel(R) Serial IO I2C Host Controller - 4B4B
Intel(R) Serial IO I2C Host Controller - 4B78
Intel(R) Serial IO I2C Host Controller - 4B79
Intel(R) Serial IO I2C Host Controller - 4B7A
Intel(R) Serial IO I2C Host Controller - 4B7B
Intel(R) Serial IO I2C Host Controller - 4BB9
Intel(R) Serial IO I2C Host Controller - 4BC0
Intel(R) Serial IO UART Host Controller - 4B28
Intel(R) Serial IO UART Host Controller - 4B4D
Intel(R) SMBus Controller - 4B23
Intel(R) SPI (flash) Controller - 4B24
Microsoft ACPI-Compliant System
Microsoft Hyper-V Virtualization Infrastructure Driver
Microsoft System Management BIOS Driver
Microsoft UEFI-Compliant System
Microsoft Virtual Drive Enumerator
Microsoft Windows Management Interface for ACPI
Microsoft Windows Management Interface for ACPI
Microsoft Windows Management Interface for ACPI
NDIS Virtual Network Adapter Enumerator
PCI Express Root Complex
PCI standard host CPU bridge
Plug and Play Software Device Enumerator
Programmable interrupt controller
Remote Desktop Device Redirector Bus
Resource Hub proxy device
SuperIO Driver
System timer
Administrator: Command Prompt
1:56 AM
5/11/2022

```
C:\Users\Administrator\Desktop\DELL_EGW_3200_LiteBMC_FW_Update_2v6\Windows\bin>ad-litbmc-fwupd.exe
Function : Lite BMC Firmware Flash Utility on EGW3200 platform
Version : 2.06
Usage :
1. Update Firmware : ad-litbmc-fwupd -u filename.bin PublicKey
2. Display Firmware version on Target device : ad-litbmc-fwupd -d -t
3. Display Firmware version in bin file : ad-litbmc-fwupd -d -f filename.bin
Options :
  -u start to update the firmware
  -d -t Display the firmware version on your target device or module
  -d -f Display the firmware version on your bin file
  -h|? Display command line help information

C:\Users\Administrator\Desktop\DELL_EGW_3200_LiteBMC_FW_Update_2v6\Windows\bin>ad-litbmc-fwupd.exe -u encryptedlv6.bin p
ublic.pem

Error: I2C controller not found

C:\Users\Administrator\Desktop\DELL_EGW_3200_LiteBMC_FW_Update_2v6\Windows\bin>ad-litbmc-fwupd.exe -u encryptedlv6.bin p
ublic.pem
Reading of public key successful
Firmware version on target device:
Starting Firmware Update...
Updating...100%
Flashing done!
Firmware version in bin file is  EGW-3200 1v6 Jan 24 2022

Updated successfully and please reboot the system

C:\Users\Administrator\Desktop\DELL_EGW_3200_LiteBMC_FW_Update_2v6\Windows\bin>_
```

Figure 27. Reboot system

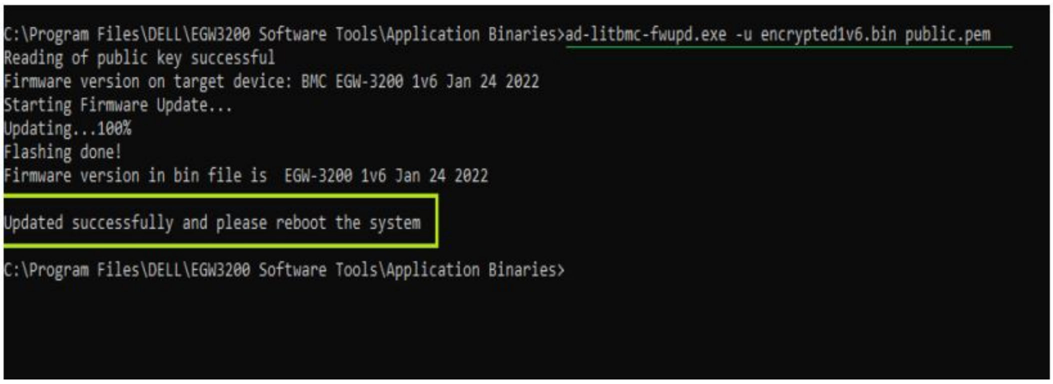
2. Execute **ad-litbmc-fwupd.exe** in command prompt to show usage of the tool.



```
C:\Program Files\DELL\EGW3200 Software Tools\Application Binaries>ad-litbmc-fwupd.exe
Function : Lite BMC Firmware Flash Utility on EGW3200 platform
Version : 2.06
Usage :
1. Update Firmware : ad-litbmc-fwupd -u filename.bin PublicKey
2. Display Firmware version on Target device : ad-litbmc-fwupd -d -t
3. Display Firmware version in bin file : ad-litbmc-fwupd -d -f filename.bin
Options :
  -u start to update the firmware
  -d -t Display the firmware version on your target device or module
  -d -f Display the firmware version on your bin file
  -h|? Display command line help information

C:\Program Files\DELL\EGW3200 Software Tools\Application Binaries>_
```

Figure 28. Show usage

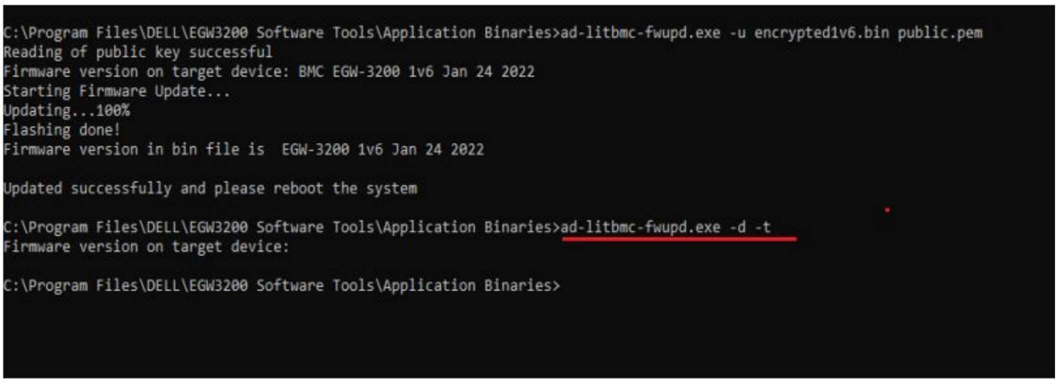
3. Update the firmware version by using the **ad-litbmc-fwupd.exe -u <firmware> <public key>** command. After the update, a message shows that it is mandatory to reboot the system for changes to take affect. The tool also prints this message.



```
C:\Program Files\DELL\EGW3200 Software Tools\Application Binaries>ad-litbmc-fwupd.exe -u encrypted1v6.bin public.pem
Reading of public key successful
Firmware version on target device: BMC EGW-3200 1v6 Jan 24 2022
Starting Firmware Update...
Updating...100%
Flashing done!
Firmware version in bin file is  EGW-3200 1v6 Jan 24 2022

Updated successfully and please reboot the system

C:\Program Files\DELL\EGW3200 Software Tools\Application Binaries>
```

Figure 29. Reboot message

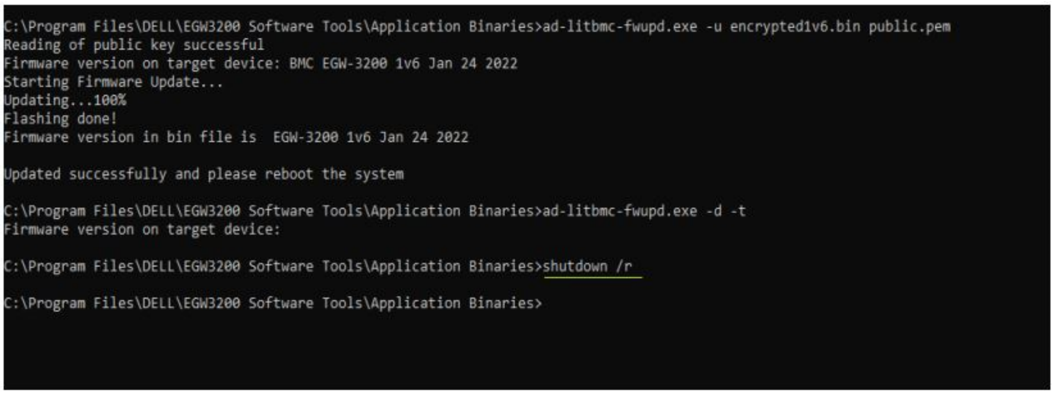
Reading the firmware version without rebooting will not show the updated version.



```
C:\Program Files\DELL\EGW3200 Software Tools\Application Binaries>ad-litbmc-fwupd.exe -u encrypted1v6.bin public.pem
Reading of public key successful
Firmware version on target device: BMC EGW-3200 1v6 Jan 24 2022
Starting Firmware Update...
Updating...100%
Flashing done!
Firmware version in bin file is  EGW-3200 1v6 Jan 24 2022

Updated successfully and please reboot the system

C:\Program Files\DELL\EGW3200 Software Tools\Application Binaries>ad-litbmc-fwupd.exe -d -t
Firmware version on target device:

C:\Program Files\DELL\EGW3200 Software Tools\Application Binaries>
```

Figure 30. Updated version not shown

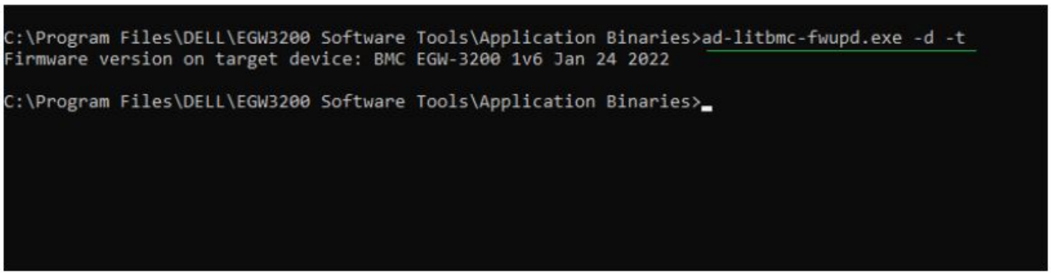
4. Reboot the device.



```
C:\Program Files\DELL\EGW3200 Software Tools\Application Binaries>ad-litbmc-fwupd.exe -u encrypted1v6.bin public.pem
Reading of public key successful
Firmware version on target device: BMC EGW-3200 1v6 Jan 24 2022
Starting Firmware Update...
Updating...100%
Flashing done!
Firmware version in bin file is  EGW-3200 1v6 Jan 24 2022

Updated successfully and please reboot the system

C:\Program Files\DELL\EGW3200 Software Tools\Application Binaries>ad-litbmc-fwupd.exe -d -t
Firmware version on target device:

C:\Program Files\DELL\EGW3200 Software Tools\Application Binaries>shutdown /r

C:\Program Files\DELL\EGW3200 Software Tools\Application Binaries>
```

Figure 31. Reboot device

5. After the reboot is complete, read the firmware version to confirm that it shows in the output.



```
C:\Program Files\DELL\EGW3200 Software Tools\Application Binaries>ad-litbmc-fwupd.exe -d -t
Firmware version on target device: BMC EGW-3200 1v6 Jan 24 2022

C:\Program Files\DELL\EGW3200 Software Tools\Application Binaries>_
```

Figure 32. Update successful

Accessing and updating the BIOS

Basic Input/Output System (BIOS) is a program that provides a basic level of communication between the processor and peripherals. In addition, the BIOS also contains codes for various advanced features applied to the EGW-3200. The BIOS setup program includes menus for configuring settings and enabling features of the EGW-3200. Most users do not need to use the BIOS setup program, as the EGW-3200 ships with default settings that work well for most configurations.

Access the BIOS settings

Steps

1. Enter the BIOS setup by pressing the **Delete** key on the keyboard when the system is powered on. The **POST** (Power On Self Test) message is displayed.

   NOTE: The EGW-3200 controller supports a one-time boot menu allowing the selection of the boot device.

2. Enter the Boot Menu by selecting **F7** at POST.

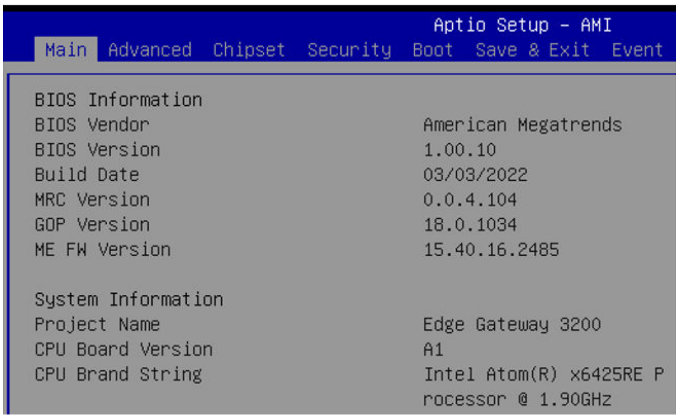
Update the BIOS using UEFI capsule update from Windows

About this task

The EGW-3200 supports UEFI capsule updates and can be updated natively within the Windows OS.

NOTE: Windows allows updating of the BIOS only if it is a newer version of the BIOS than what is already on the system.

The BIOS version number is available from the BIOS **Main** tab.

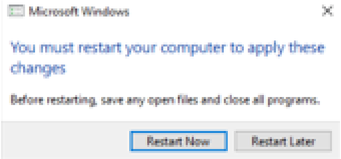


```
                                     Aptio Setup - AMI
 Main  Advanced  Chipset  Security  Boot  Save & Exit  Event

 BIOS Information
 BIOS Vendor                          American Megatrends
 BIOS Version                         1.00.10
 Build Date                           03/03/2022
 MRC Version                          0.0.4.104
 GOP Version                          18.0.1034
 ME FW Version                        15.40.16.2485

 System Information
 Project Name                         Edge Gateway 3200
 CPU Board Version                    A1
 CPU Brand String                     Intel Atom(R) x6425RE P
                                      rocessor @ 1.90GHz
```

Figure 33. BIOS version number under Main tab

Steps

1. Download the newer version of the BIOS in .msi format from the Dell Technologies Support Site and run the executable from an elevated command prompt with administrator privileges.
   Windows prompts to restart the system for a firmware change.

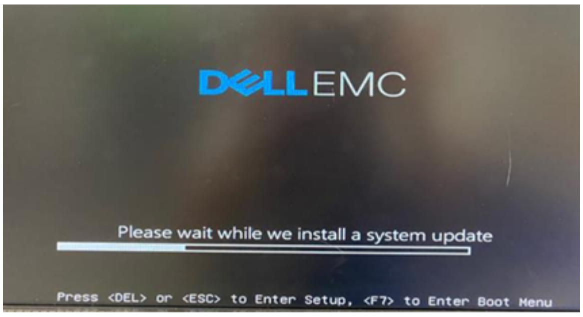
   Microsoft Windows

   You must restart your computer to apply these changes

   Before restarting, save any open files and close all programs.

   Figure 34. Restart computer

2. Click **Restart Now** to restart the system.
   The system will start the BIOS firmware update process.

   Please wait while we install a system update

   Press <DEL> or <ESC> to Enter Setup, <F7> to Enter Boot Menu

   Figure 35. System update progress bar

Results

After the update is complete, the BIOS screen will show the newer version details.

SuperIO Function Library

This section describes use of the SuperIO (SIO) function library for the EGW-3200. The SIO function library includes the watchdog timer function and the hardware monitor function. The watchdog timer is a hardware mechanism provided to reset the system if the operating system or an application stalls. After starting, the watchdog timer in the application must be periodically reset before the timer expires. Once the watchdog timer expires, a hardware-generated signal is sent to reset the system. The hardware monitor is a mechanism provided to collect the wide range of information related to hardware health, including CPU temperature, board temperature, and various voltage values.

Windows SIO API

The SIO API library files and a demo program (including source code) are part of the board support package for the EGW-3200 (BSP/Sample_App_Source/SuperIO) and can be downloaded from the Dell Technologies Support Site.

SIO_WDT_Set

Sets the timeout value of the watchdog timer. SIO_WDT_Stop should be called before the expiration of watchdog timer, or the system will reset.

I32 SIO_WDT_Set (unsigned char val, int mode)

Parameters	**val**—Specifies the value for the watchdog timer. A valid value is 1 - 255.
	mode—Specifies the mode of the timeout value. The valid mode of the timeout value is seconds (0) or minutes (1).
Return codes	0 if timeout value of watchdog timer is successfully set.
	Negative error if timeout value of watchdog timer is failed to set.

SIO_WDT_GetCurrentTime

Gets the current timeout value of the watchdog timer, gives remaining watchdog timer timeout value and mode.

I32 SIO_WDT_GetCurrentTime (unsigned char* pTime, int* mode)

Parameters	**pTIme**—Pointer variable to return the remaining watchdog time for expiry.
	Mode—Pointer variable to return the current watchdog mode.
Return codes	0 if timeout value of watchdog timer is available.
	Negative error if failed to get the current timeout value and mode of the watchdog timer.

SIO_WDT_Stop

Stops the watchdog timer.

I32 SIO_WDT_Stop ()

Parameters	None
Return codes	0 if watchdog timer is successfully stopped.
	Negative error if watchdog timer fails to stop.

GetCurrentCPUTemp

Gets the hardware monitor values.

I32 GetCurrentCPUTemp (int *temp)

Parameters	**temp**—Integer pointer for getting the CPU temperature.
Return codes	0 if temperature is read successfully. Negative error if failed to get the data from hardware monitor.

Error codes

For the various functions previously listed, the following is the error values in case of failure.

```
enum SIO_ERRORS_LIST{
        ERROR_SIO_INVALID_DEVICE_HANDLE = -100,
        ERROR_SIO_IOCTL,
        ERROR_SIO_INVALID_RW_SEL,
        ERROR_SIO_INVALID_MODE_SEL,
        ERROR_SIO_WDT_NOT_ENABLED
};
```

Build the SIO sample application

Prerequisites

Visual Studio 2019 is required for this task. To download and install, perform the following steps:

1. Select **Workloads**.
2. Open **Visual Studio Installer** and click **Modify** to customize your installation.
3. Select **Desktop development with C++** workload.
4. Select **UWP**.
5. Select **Individual components**, and under **Complier, build tools, and runtimes**, make sure that the following boxes are checked:
   a. MSVC v142 -VS 2019 C++ x64/x86 buildtools (latest) is checked.
   b. MSVC v142 -VS 2019 C++ x64/x86 Spectre-mitigated libs (latest) is checked.
6. Make sure the SDK is installed. Download and install the corresponding WDK version.
7. Install the latest supported English (en-us) Microsoft Visual C++ redistributable packages for Visual Studio 2015, 2017, 2019, and 2022 from the following link: VC_redist.x64.exe.

About this task

NOTE: The sample executable binaries are built with SDK-10.0.19041.685 and WDK-10.0.19041.685 versions. The procedure may vary slightly if using other versions.

To build the sample application, perform the following steps.

Steps

1. Open Sample_App_Source/SuperIO/superior_nct.sln in Visual Studio.
2. Change **Solution configuration** to **Release** and **Solution platform** to **x64**.
3. Under the **Build** menu, select **Build Solution**.

Execute the SIO sample application

About this task

The EGW-3200 Windows image includes pre-installed sample application binaries.

Steps

1. Open the command prompt in administrator mode.

2. Change to the following directory: `C:\Program Files\Dell\EGW3200 Software tools\Application Binaries`
3. Use the following commands to execute the SIO sample application:
   a. To set the watchdog timer:

      ```
      > superiotest wdtset <time> <mode>
      ```

      Where time is between 1 to 255, and mode is seconds or minutes.

   b. To stop the watchdog timer:

      ```
      > superiotest wdtstop
      ```

   c. To get the remaining watchdog time and mode:

      ```
      > superiotest wdtgettime
      ```

   d. To get CPU temperature:

      ```
      > superiotest getcputemp
      ```

Digital Input/Output Function of the Intel PCH Controller

The EGW-3200 uses Microsoft's RHProxy interface for accessing the GPIO pins from PCH chipset. All the necessary changes are done in the BIOS. For a sample program, the GpioTestTool source code from the Microsoft GitHub can be used.

The EGW-3200 has six DI pins, six DO pins, and three user LEDs. For the pin details and pin numbers to be used for the sample application, refer the table in RHProxy driver - I2C and GPIO.

Build the GPIO sample application

Prerequisites

Visual Studio 2019 is required for this task. Do download and install, perform the following steps:

1. Select **Workloads**.
2. Open **Visual Studio Installer** and click **Modify** to customize your installation.
3. Select **Desktop development with C++** workload.
4. Select **UWP**.
5. Select **Individual components**, and under **Complier, build tools, and runtimes**, make sure that the following boxes are checked:
   a. MSVC v142 -VS 2019 C++ x64/x86 buildtools (latest) is checked.
   b. MSVC v142 -VS 2019 C++ x64/x86 Spectre-mitigated libs (latest) is checked.
6. Make sure the SDK is installed. Download and install the corresponding WDK version.
7. Install the latest supported English (en-us) Microsoft Visual C++ redistributable packages for Visual Studio 2015, 2017, 2019, and 2022 from the following link: VC_redist.x64.exe.

About this task

> **NOTE:** The sample executable binaries are built with SDK-10.0.19041.685 and WDK-10.0.19041.685 versions. The procedure may vary slightly if using other versions.

To build the sample application, perform the following steps.

Steps

1. Open Sample_App_Source/GPIOTestTool/windows-iot-bus-tools.sln in Visual Studio.

2. Change **Solution configuration** to **Release** and **Solution platform** to **x64**.
3. Under the **Build** menu, select **Build Solution**.

Execute the GPIO sample application

About this task

The EGW-3200 Windows image includes pre-installed sample application binaries.

Steps

1. Open the command prompt in administrator mode.
2. Change to the following directory: `C:\Program Files\Dell\EGW3200 Software tools\Application Binaries`
3. Use the following commands to execute the GPIO sample application:
   a. To open the pin connection:

   ```
   > GpioTestTool.exe <pin>
   ```

   b. To set the drive mode to output:

   ```
   > setdrivemode output
   ```

   c. To set the DO0 pin to low:

   ```
   > write 0
   ```

   d. To set the DO0 pin to high:

   ```
   > write 1
   ```

   Similarly, the pin can be opened and set to drive mode input and the current value can be read using a `read` command. Use the `help` command for detailed usage.

Digital Input/Output Function from PCA9535 GPIO

Users can opt to connect a PCA9535 GPIO expander module to one of the I2C buses of the EGW-3200.

PCA9535 GPIO Expander API

The PCA9535 GPIO module’s API library files and a demo program (including source code) are included in the board support package for the EGW-3200.

PCA9535Init

This function is used to initialize the directions of the GPIO pins. Also, it opens the handle to the I2C bus and it is necessary to call this function before executing any of the other APIs.

int PCA9535Init (unsigned int i2cnumber)

Parameters	**i2cnumber**—The I2C bus number to which the PCA9535 board is connected. Can be 0 or 1.
Return codes	0 if the initialization is successful. Negative error if failed.

DioSetLevel

Sets the GPIO level for output pins.

int DioSetLevel (unsigned char data, unsigned char mask)

Parameters

data—The new GPIO level to be set for the output pins.

mask—GPIO output pins are changed only for those corresponding to the bits that are set to 1 in the mask. Other pin values remain unchanged.

Return codes

0 if the initialization is successful.

Negative error if failed.

DioGetLevel

Gets the current GPIO level for both input and output pins.

int DioGetLevel (unsigned int mask, unsigned int* GetPinLevel)

Parameters

mask—The GPIO input pins are updated in the GetPinLevel only for the bits which are set to 1 in the mask.

GetPinLevel—Pointer to store the read value. The first eight bits (Bit 0 to 7) contain the GPIO input pin's voltage level. The second eight bits (Bit 8 to 15) contain the GPIO output pin's voltage level.

Return codes

0 if the initialization is successful.

Negative error if failed.

Error codes

For the various functions previously listed, the following is the error values in case of failure.

```
enum errorcodes {
    Error_Pointer_Invalid = -100,
    Error_I2C_controller_NotFound,
    Error_I2C_Open_Failed,
    Error_I2C_Bus_Invalid,
    Error_Mutex_Failed,
    Error_I2CTransfer_Partial,
    Error_I2CTransfer_SlaveAddressNotAcknowledged,
    Error_I2CTransfer_ClockStretchTimeout,
    Error_I2CTransfer_UnknownError
};
```

Build the PCA9535 sample application

Prerequisites

Visual Studio 2019 is required for this task. Do download and install, perform the following steps:

1. Select **Workloads**.
2. Open **Visual Studio Installer** and click **Modify** to customize your installation.
3. Select **Desktop development with C++** workload.
4. Select **UWP**.

5. Select **Individual components**, and under **Complier, build tools, and runtimes**, make sure that the following boxes are checked:
    a. MSVC v142 -VS 2019 C++ x64/x86 buildtools (latest) is checked.
    b. MSVC v142 -VS 2019 C++ x64/x86 Spectre-mitigated libs (latest) is checked.
6. Make sure the SDK is installed. Download and install the corresponding WDK version.
7. Install the latest supported English (en-us) Microsoft Visual C++ redistributable packages for Visual Studio 2015, 2017, 2019, and 2022 from the following link: VC_redist.x64.exe.

About this task

ⓘ **NOTE:** The sample executable binaries are built with SDK-10.0.19041.685 and WDK-10.0.19041.685 versions. The procedure may vary slightly if using other versions.

To build the sample application, perform the following steps.

Steps

1. Open Sample_App_Source/PCA9535/PCA9535_I2C.sln in Visual Studio.
2. Change **Solution configuration** to **Release** and **Solution platform** to **x64**.
3. Under the **Build** menu, select **Build Solution**.

Execute the PCA9535 sample application

About this task

The EGW-3200 Windows image includes pre-installed sample application binaries.

Steps

1. Open the command prompt in administrator mode.
2. Change to the following directory: `C:\Program Files\Dell\EGW3200 Software tools\Application Binaries`
3. Use the following commands to execute the PCA9535 sample application:
    a. Use the following command to execute the pca9535_interrupt.exe with two arguments (<I2c Number> and <GPIO Number>):

    ```
    > pca9535_interrupt.exe 0 8
    ```

    b. Execute the pca9535App.exe for write functionality:

    Pca9535App.exe i2c <i2cnumber> write <write value in hex> <mask value in hex>

    ```
    > pca9535App.exe i2c 0 write 0xff 0xff
    ```

    <writes all output pins to high>

    c. Execute the pca9535App.exe for read functionality:

    pca9535App.exe i2c <i2cnumber> read <mask value in hex>

    ```
    > Pca9535App.exe i2c 0 read 0xff
    ```

    <reads all pins>

Hardware monitor API

The EGW-3200 has various hardware monitor features which can be retrieved by using the following function parameters.

EApiLibInitialize

Initialize function. Call this function before accessing any of the API.

int EApiLibInitialize ()

Parameters	None
Return codes	0 if the initialization is a success. Negative error if failed.

EApiBoardGetValue

Gets the hardware monitor (current/voltage/temperature) values.

int EApiBoardGetValue (int parameter)

Parameters	The parameters could be one of the following, and the macro is self-explanatory. ● EAPI_ID_HWMON_SYSTEM_TEMP ● EAPI_ID_HWMON_VOLTAGE_VBAT ● EAPI_ID_HWMON_VOLTAGE_5VSB ● EAPI_SEMA_ID_BOARD_MAIN_CURRENT ● EAPI_SEMA_ID_HWMON_VOLTAGE_VIN
Return codes	0 if the initialization is a success. Negative error if failed.

EApiUnInitialize

Un-initialize function. Call this function before exiting the application.

Humidity and temperature sensor setup

Prerequisites

Windows standard APIs: FromIdAsync(String), GetCurrentReading(), and GetDeviceSelector(Guid interfaceId) are used for accessing the sensor. For details, go to the Windows.Devices.Sensors.Custom Namespace Microsoft page.

About this task

The HDC1010 humidity and temperature sensor is connected to I2C bus 2 of the EGW-3200. This sensor is detected as a custom sensor and follows Windows sensor framework.

Build the sample application

Prerequisites

Visual Studio 2019 is required for this task. To download and install, perform the following steps:

1. Select **Workloads**.
2. Open **Visual Studio Installer** and click **Modify** to customize your installation.
3. Select **Desktop development with C++** workload.
4. Select **UWP**.
5. Select **Individual components**, and under **Complier, build tools, and runtimes**, make sure that the following boxes are checked:
    a. MSVC v142 -VS 2019 C++ x64/x86 buildtools (latest) is checked.
    b. MSVC v142 -VS 2019 C++ x64/x86 Spectre-mitigated libs (latest) is checked.

6. Make sure the SDK is installed. Download and install the corresponding WDK version.
7. Install the latest supported English (en-us) Microsoft Visual C++ redistributable packages for Visual Studio 2015, 2017, 2019, and 2022 from the following link: VC_redist.x64.exe.

About this task

To build the sample application, perform the following steps.

Steps

1. Open the solution file of the source code in Visual Studio.
2. Change **Solution configuration** to **Release** and **Solution platform** to **x64**.
3. In the **Solution Explorer** pane, right-click on the project and select **Properties**.

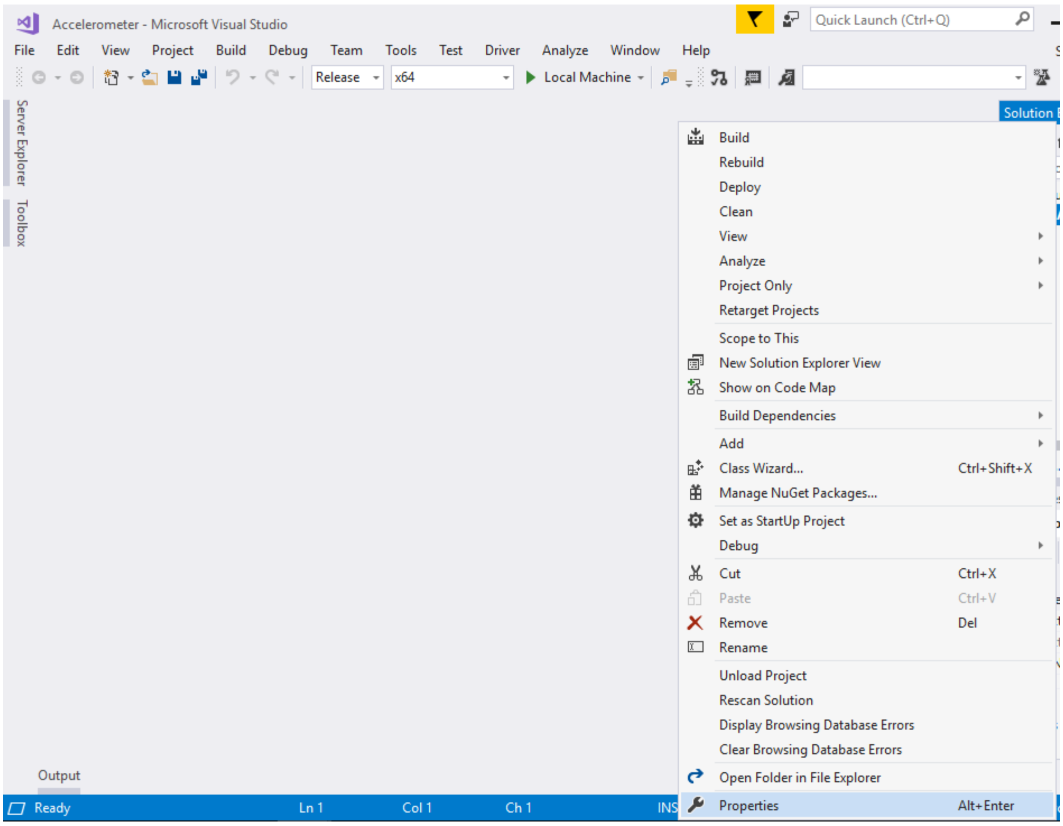
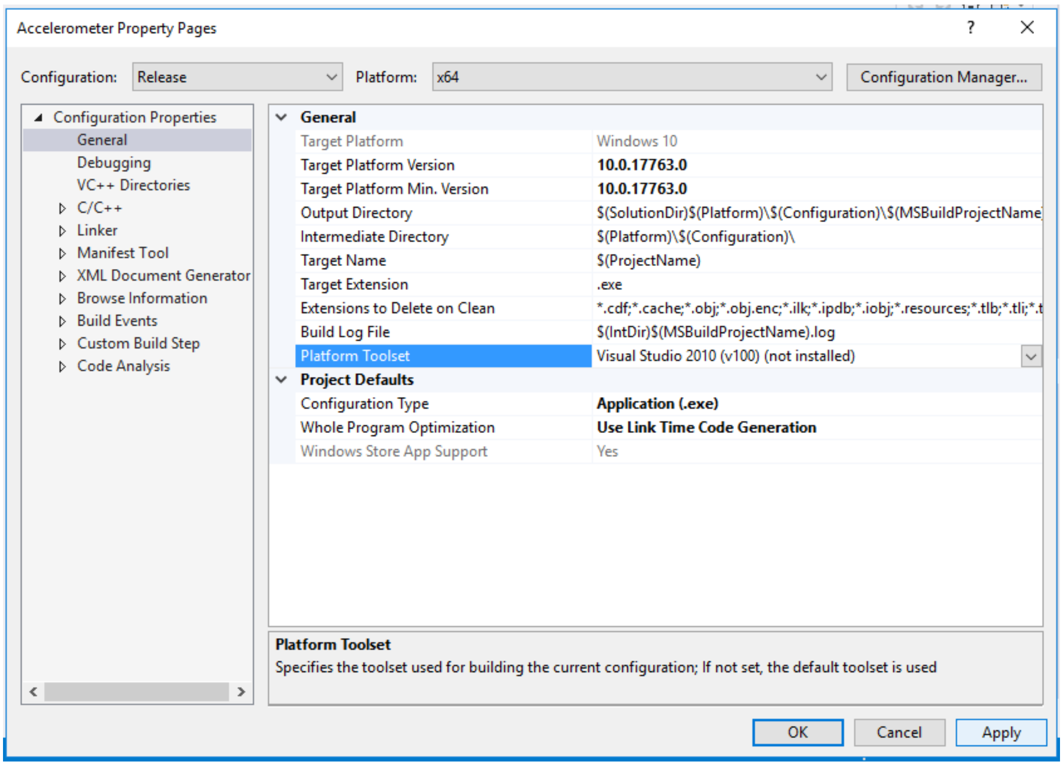


Figure 36. Solution Explorer - Properties

4. Change the **Target Platform Version** and **Target Platform Min. Version** to **10.0.17763.0** and **Platform Toolset** to the Visual Studio version used. Set the **Configuration** to **Release** and **Platform** to **x64**. Click **Apply** and **OK**.



Configuration: Release   Platform: x64   Configuration Manager...

General	
Target Platform	Windows 10
Target Platform Version	10.0.17763.0
Target Platform Min. Version	10.0.17763.0
Output Directory	$(SolutionDir)$(Platform)\$(Configuration)\$(MSBuildProjectName)
Intermediate Directory	$(Platform)\$(Configuration)\
Target Name	$(ProjectName)
Target Extension	.exe
Extensions to Delete on Clean	*.cdf;*.cache;*.obj;*.obj.enc;*.ilk;*.ipdb;*.iobj;*.resources;*.tlb;*.tli;*.t
Build Log File	$(IntDir)$(MSBuildProjectName).log
Platform Toolset	Visual Studio 2010 (v100) (not installed)
Project Defaults	
Configuration Type	Application (.exe)
Whole Program Optimization	Use Link Time Code Generation
Windows Store App Support	Yes

Platform Toolset

Specifies the toolset used for building the current configuration; If not set, the default toolset is used

Figure 37. Properties - Platform Toolset

5. Select **Build** > **Build Solution** to build the project.

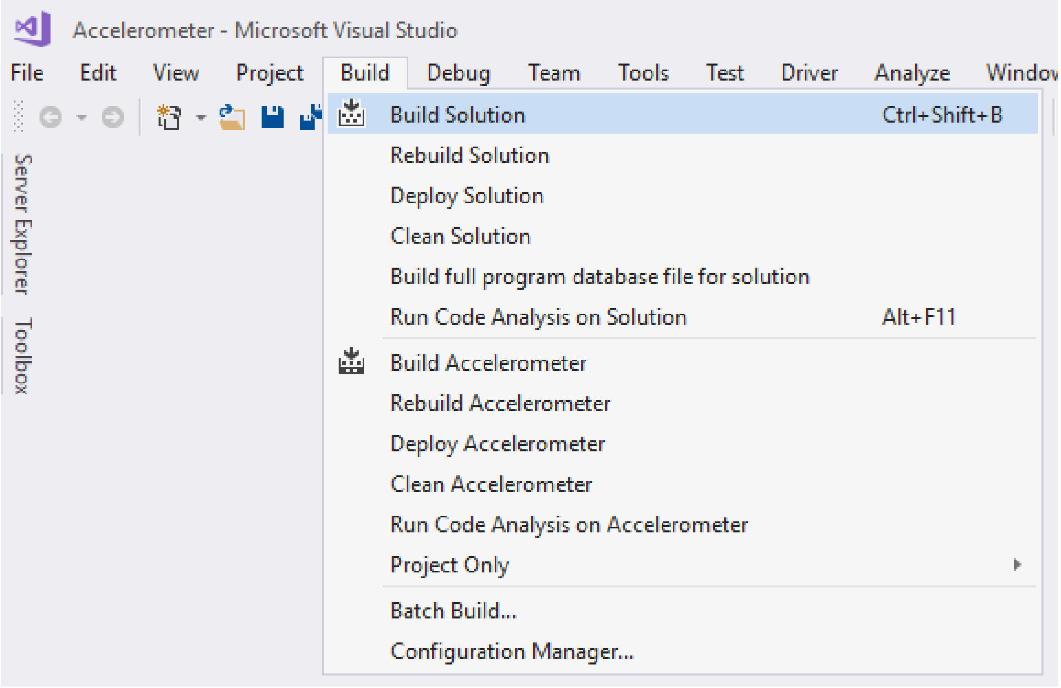
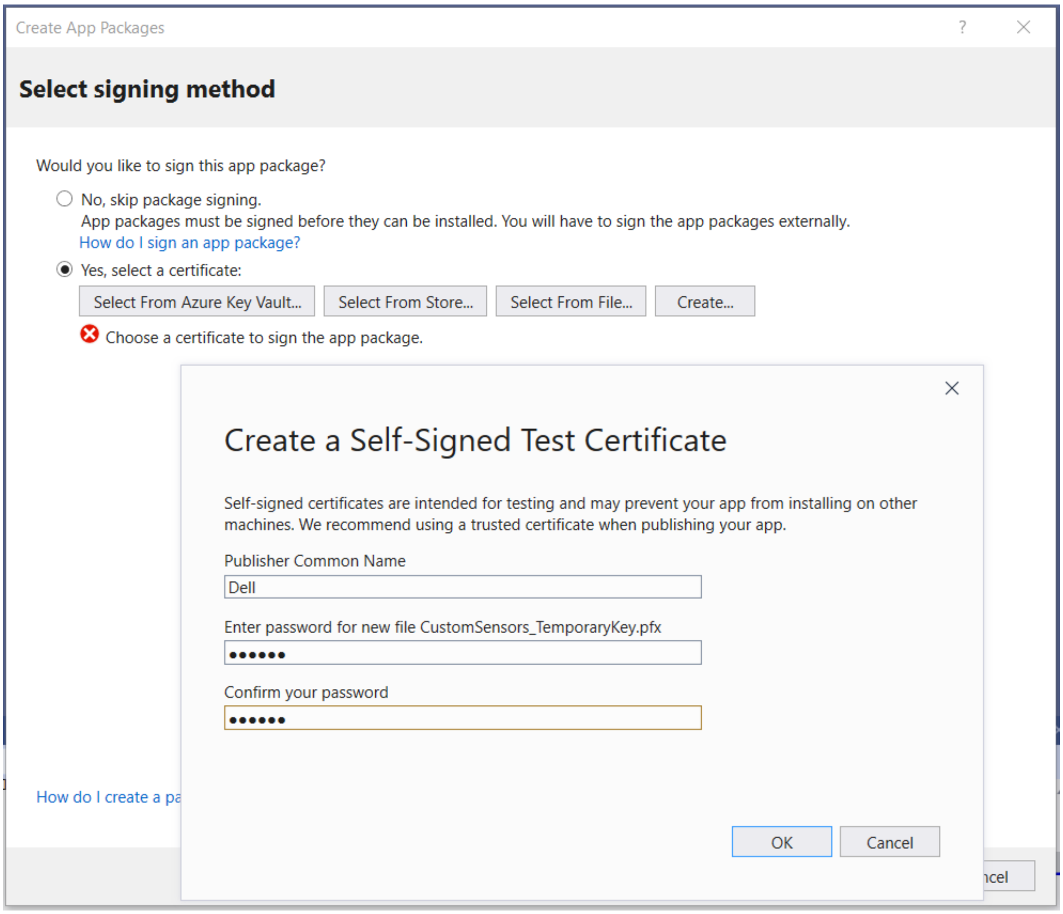


Figure 38. Build Solution

Create the MSIX package

Steps

1. Place the **Assets** folder in the current directory (Path: x64/Release/ilc/in).
2. Right-click on the project and Select **Publish** > **Create App Packages**.
3. Enable Side-loading in the first page of the wizard and then click **Next**.
4. On the **Select signing method** page, select whether to skip packaging signing or select a certificate for signing. For an MSIX package to be installed, it must be signed with a certificate that is trusted on the machine. The certificate is password-protected. It is imported to the certificate store for package signing.



Would you like to sign this app package?

○ No, skip package signing.
App packages must be signed before they can be installed. You will have to sign the app packages externally.

● Yes, select a certificate:

Choose a certificate to sign the app package.

Create a Self-Signed Test Certificate

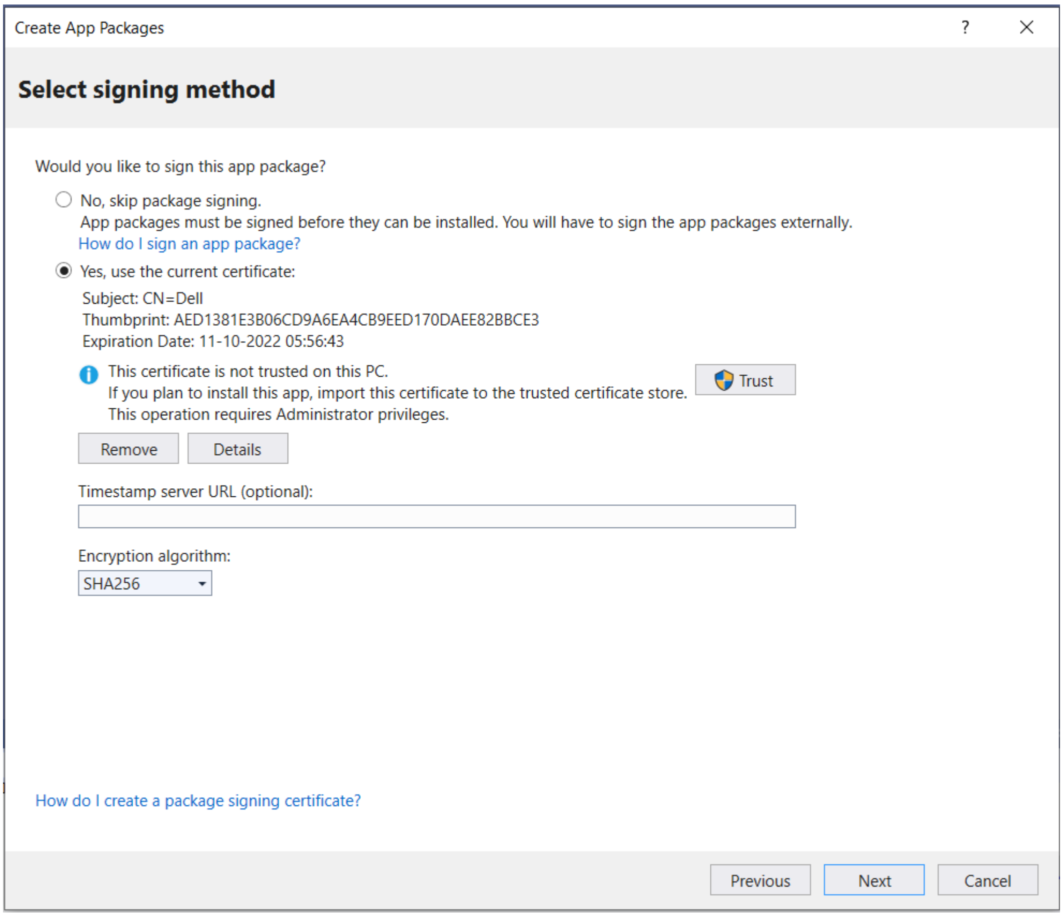
Self-signed certificates are intended for testing and may prevent your app from installing on other machines. We recommend using a trusted certificate when publishing your app.

Publisher Common Name: Dell

Enter password for new file CustomSensors_TemporaryKey.pfx: ••••••

Confirm your password: ••••••

Figure 39. Create Certificate



Create App Packages

Select signing method

Would you like to sign this app package?

○ No, skip package signing.
App packages must be signed before they can be installed. You will have to sign the app packages externally.
How do I sign an app package?

● Yes, use the current certificate:

Subject: CN=Dell
Thumbprint: AED1381E3B06CD9A6EA4CB9EED170DAEE82BBCE3
Expiration Date: 11-10-2022 05:56:43

This certificate is not trusted on this PC.
If you plan to install this app, import this certificate to the trusted certificate store.
This operation requires Administrator privileges.

Timestamp server URL (optional):

Encryption algorithm: SHA256

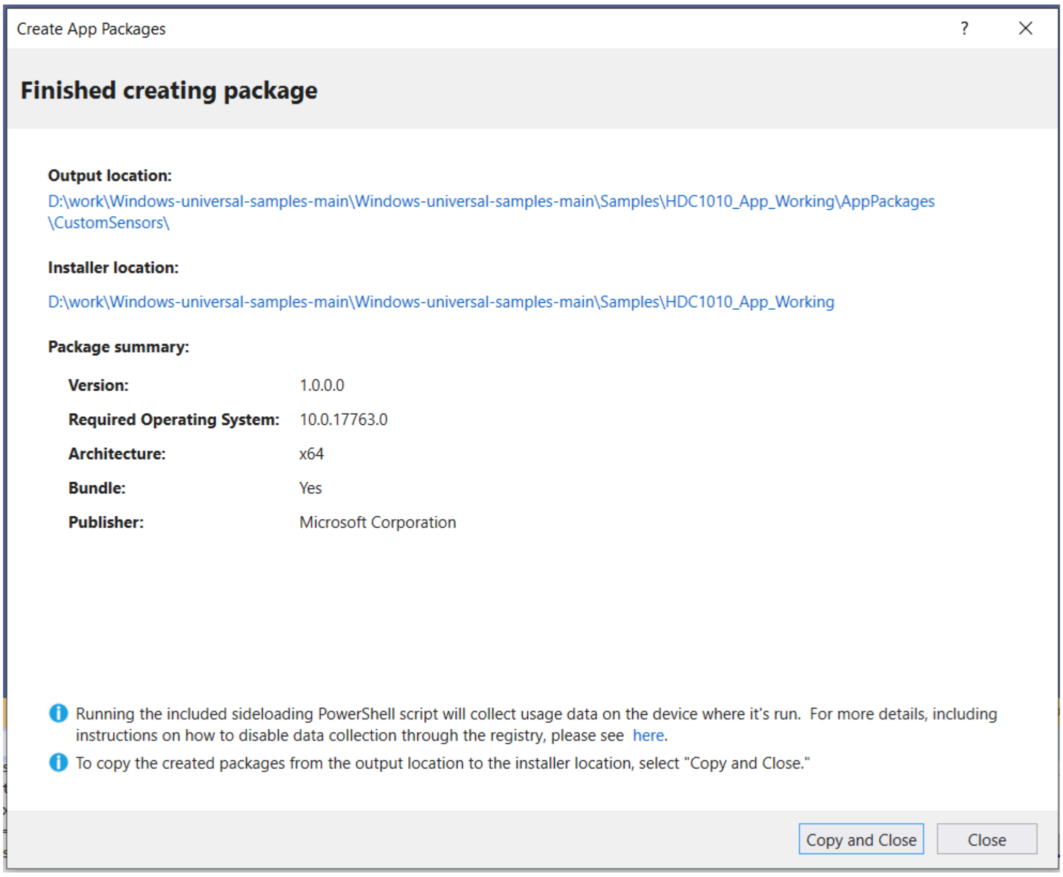
How do I create a package signing certificate?

Figure 40. Certificate Trust

5. In **Select and configure packages** wizard, select the **Architecture** as **x64** and **Solution Configuration** as **Release (x64)** and click **Next**.
6. Provide the path for the **Installer location** (where the app is published) and select **Create**.

Results

The project builds and App bundle is created. The package summary appears.



Create App Packages

Finished creating package

Output location:

D:\work\Windows-universal-samples-main\Windows-universal-samples-main\Samples\HDC1010_App_Working\AppPackages\CustomSensors\

Installer location:

D:\work\Windows-universal-samples-main\Windows-universal-samples-main\Samples\HDC1010_App_Working

Package summary:

Version:	1.0.0.0
Required Operating System:	10.0.17763.0
Architecture:	x64
Bundle:	Yes
Publisher:	Microsoft Corporation

Running the included sideloading PowerShell script will collect usage data on the device where it's run. For more details, including instructions on how to disable data collection through the registry, please see here.

To copy the created packages from the output location to the installer location, select "Copy and Close."

Figure 41. Finished creating package

Import the certificate

Steps

1. Unzip the folder **Sensor Applications.7z** containing the MSIX bundle.
2. Locate the certificate files for this application in folder **HDC1010**.
3. Go to **Start** > **Manage computer certificates**. On the left pane of the certlm wizard, select **Trusted People**.
4. Select **Action** > **All Tasks** > **Import**. The **Certificate Import Wizard** appears. Click **Next**.

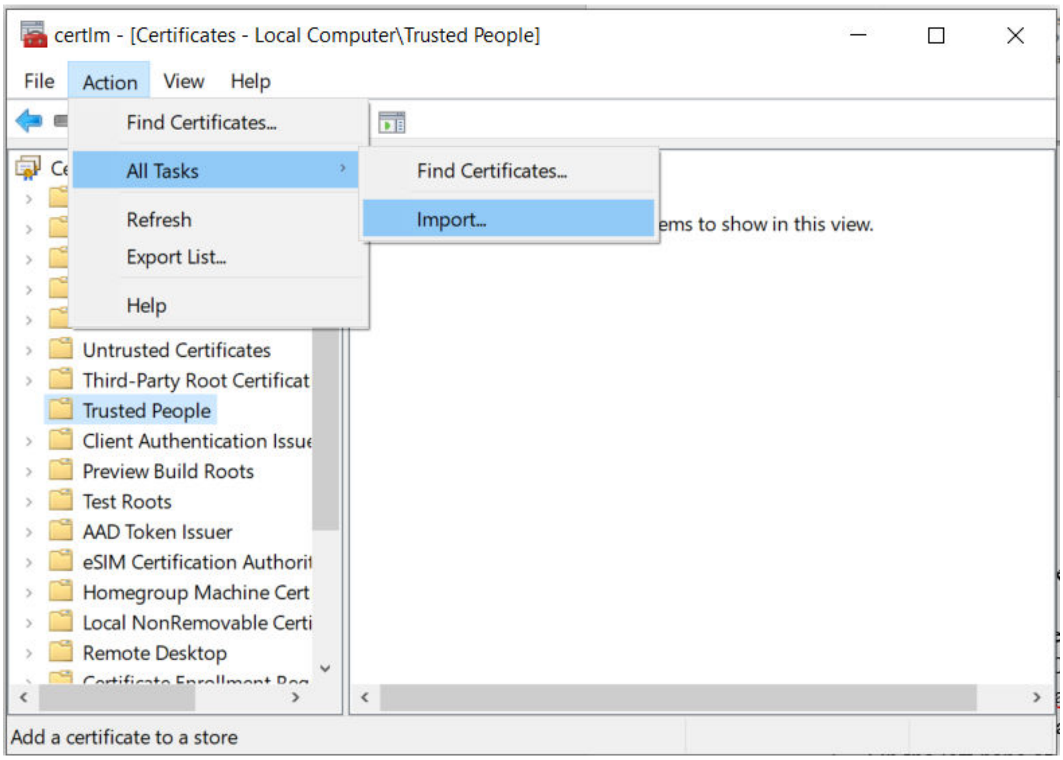
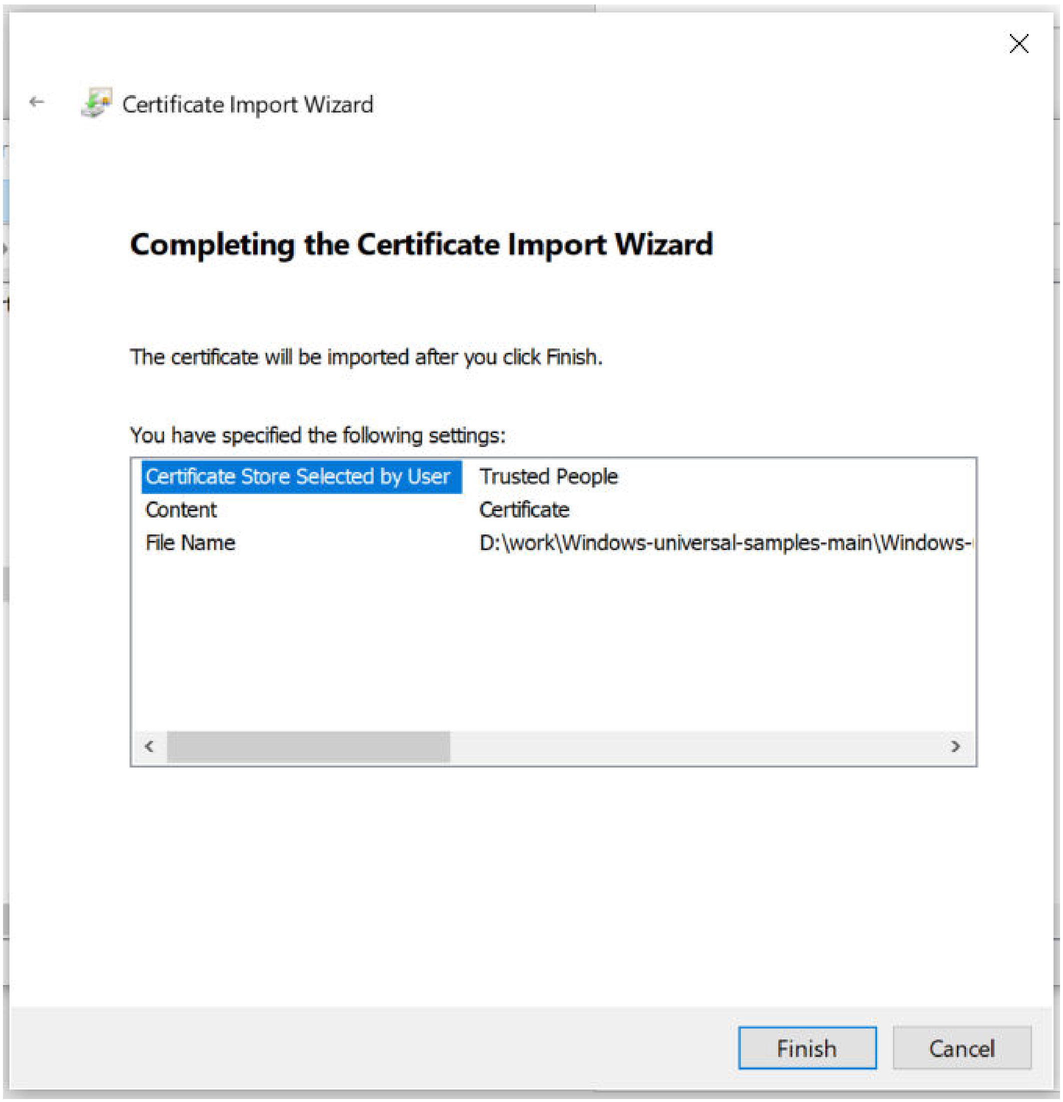


Figure 42. Import Certificate

5. Include the path where the certificate is located. Click **Next**.
6. The certificate is imported. Click **Finish**.



Completing the Certificate Import Wizard

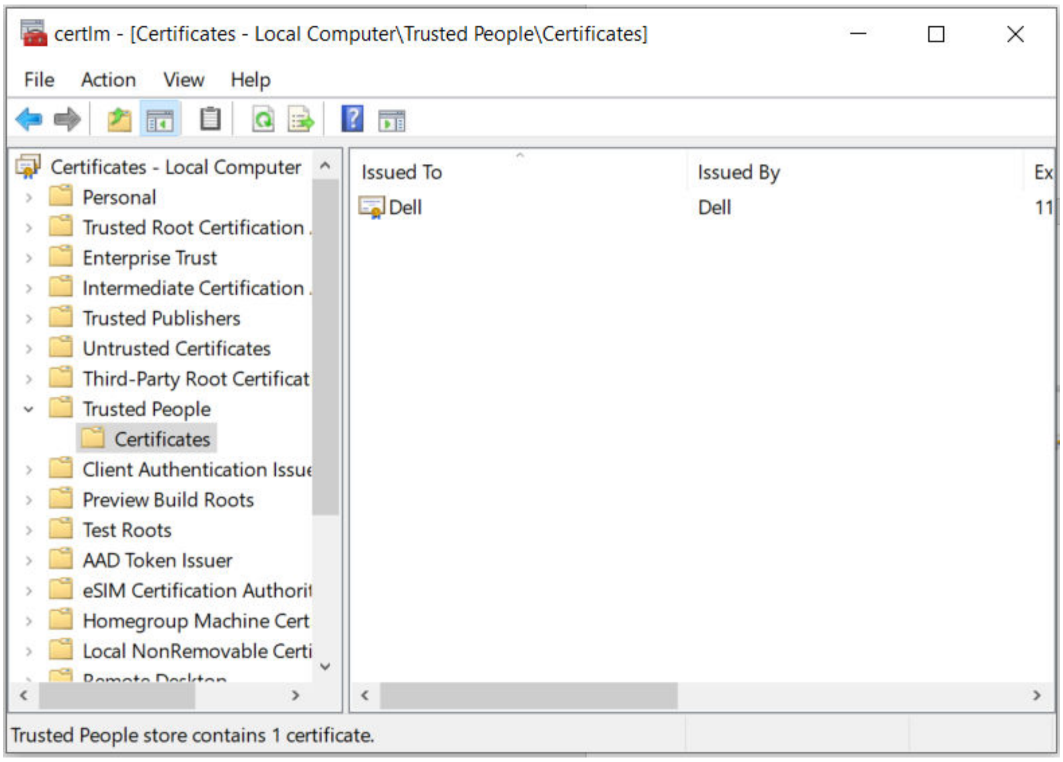
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted People
Content	Certificate
File Name	D:\work\Windows-universal-samples-main\Windows-

Figure 43. Completing the Certificate Import Wizard

7. The imported certificate is added in the **Certificates** directory under **Trusted People**. If not, select **Action** > **Refresh**, and the certificate is added.


certlm - [Certificates - Local Computer\Trusted People\Certificates]
File
Action
View
Help
Certificates - Local Computer
Personal
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Certificates
Client Authentication Issue
Preview Build Roots
Test Roots
AAD Token Issuer
eSIM Certification Authorit
Homegroup Machine Cert
Local NonRemovable Certi
Remote Desktop

Issued To	Issued By	Ex
Dell	Dell	11

Trusted People store contains 1 certificate.

Figure 44. Certificates

Install the application

About this task

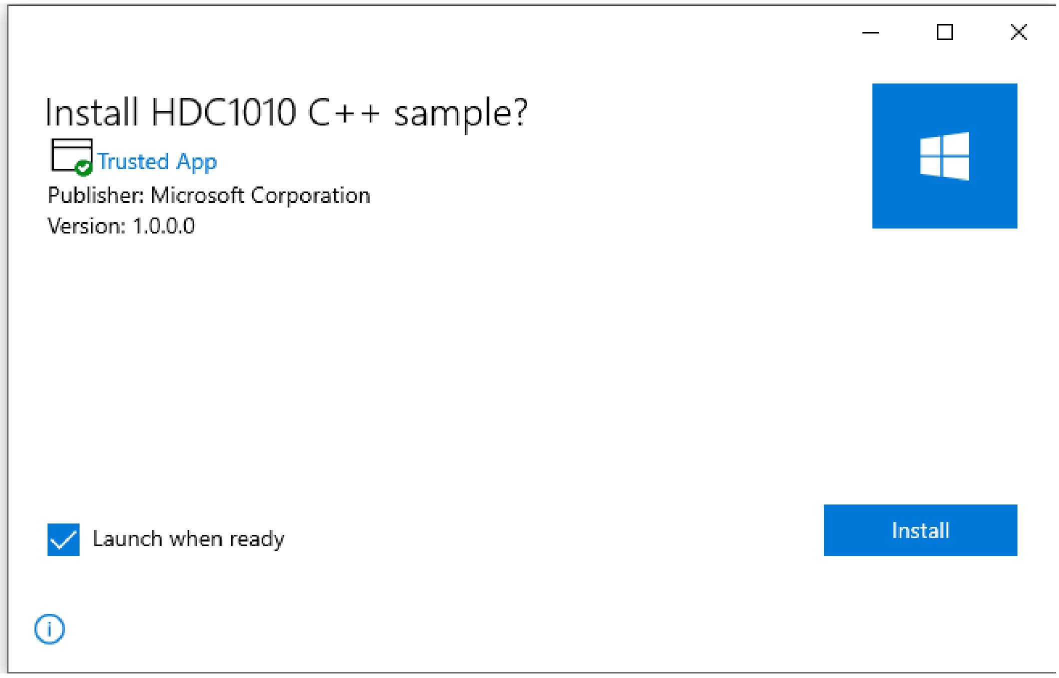
The example referred to in the following steps is for the HDC1010 humidity sensor application. The same steps are applicable for other two sensors.

Steps

1. Install the App Installer from the Microsoft store. To do this, open the POWERSHELL in ADMINISTRATOR Mode and execute the following command:

```
Get-AppXPackage*WindowsStore* -AllUsers| Foreach
{Add-AppxPackage-DisableDevelopmentMode-Register
"$($_.InstallLocation)\AppXManifest.xml"}
```

2. Run the **.msixbundle** file. A window appears prompting to install the application. Click **Install**.



Install HDC1010 C++ sample?

Trusted App

Publisher: Microsoft Corporation

Version: 1.0.0.0

Figure 45. Install prompt

The application is installed and the UWP application appears.

3. Click **Start**.
   The application name appears.

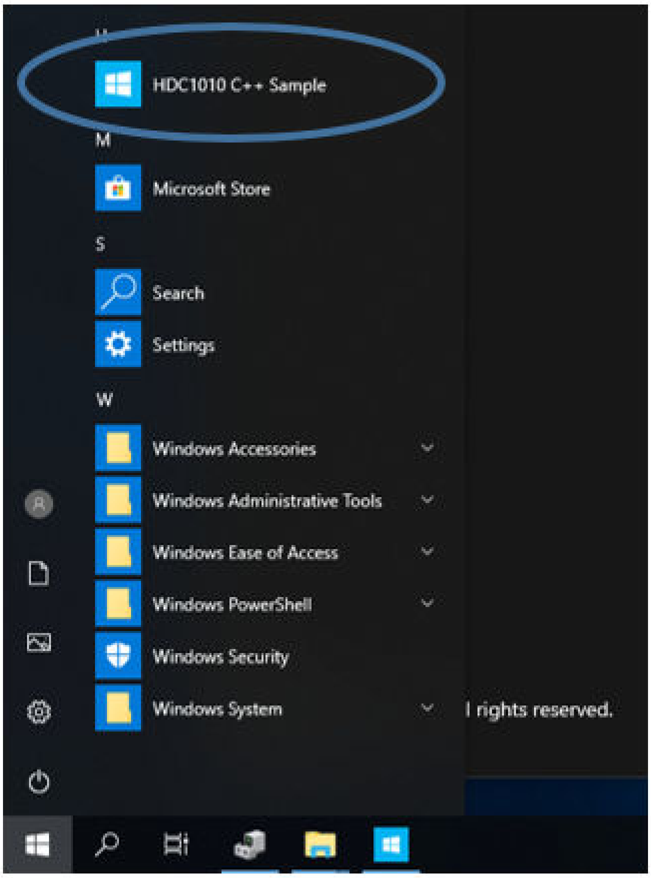


Figure 46. Application name in Start Menu

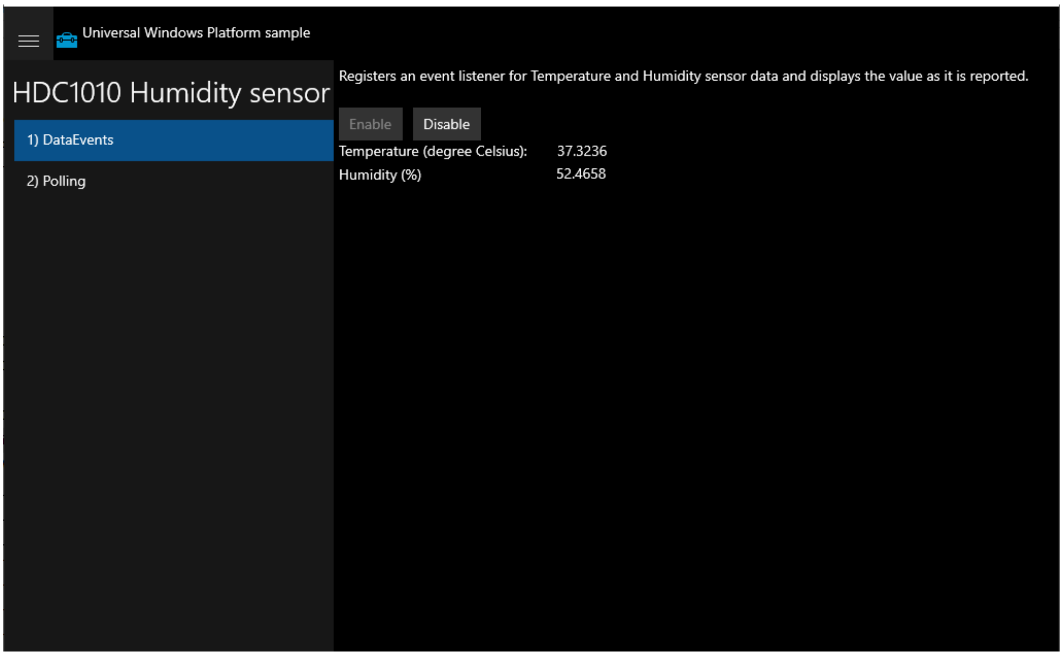
Run the temperature sensor application

About this task

Two events are registered for the application: DataEvents and Polling.

Steps

1. Select **DataEvents** > **Enable**. **Temperature** and **Relative Humidity** values are displayed.
2. Select **DataEvents** > **Disable** and follow Step 1 to obtain the next set of readings.

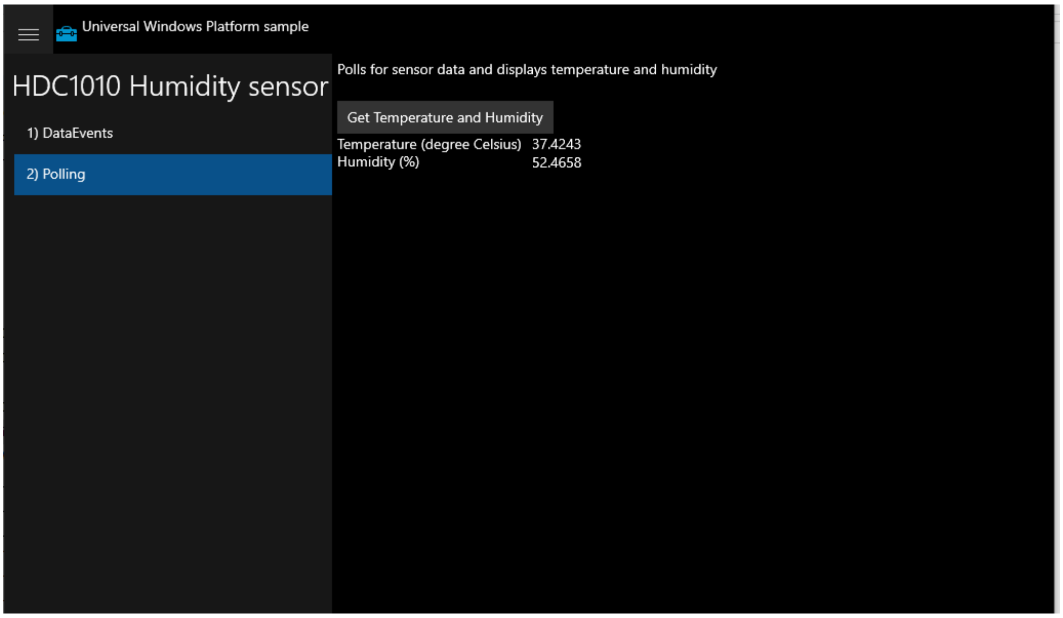


Registers an event listener for Temperature and Humidity sensor data and displays the value as it is reported.

Temperature (degree Celsius): 37.3236
Humidity (%) 52.4658

Figure 47. DataEvents

3. Select **Polling** and repeat Steps 1 and 2.


Universal Windows Platform sample
HDC1010 Humidity sensor
1) DataEvents
2) Polling
Get Temperature and Humidity

Polls for sensor data and displays temperature and humidity

Temperature (degree Celsius) 37.4243
Humidity (%) 52.4658

Figure 48. Polling

Pressure sensor setup

Prerequisites

Windows standard APIs: FromIdAsync(String), GetCurrentReading(), GetDefault(), and GetDeviceSelector(Guid interfaceId) are used for accessing the sensor. For details, go to the Windows.Devices.Sensors.Custom Namespace Microsoft page.

About this task

The DPS310 pressure sensor is connected to I2C bus 2 of the EGW-3200. This sensor is detected as a barometer sensor and follows Windows sensor framework.

See the Humidity and temperature sensor setup section for the following tasks:

- Build the sample application
- Create the MSIX package
- Import the certificate
- Install the application

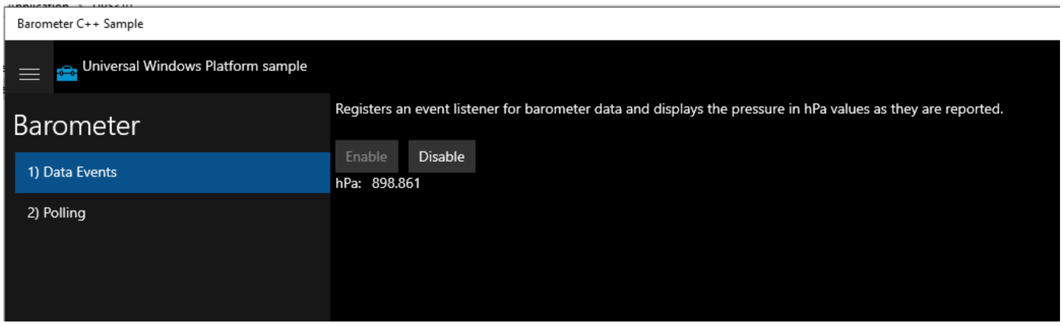
Run the pressure sensor application

About this task

Two events are registered for the application: DataEvents and Polling.

Steps

1. Select **DataEvents** > **Enable**. The **Pressure** value is displayed in hectopascals.
2. Select **DataEvents** > **Disable** and follow Step 1 to obtain the next set of readings.

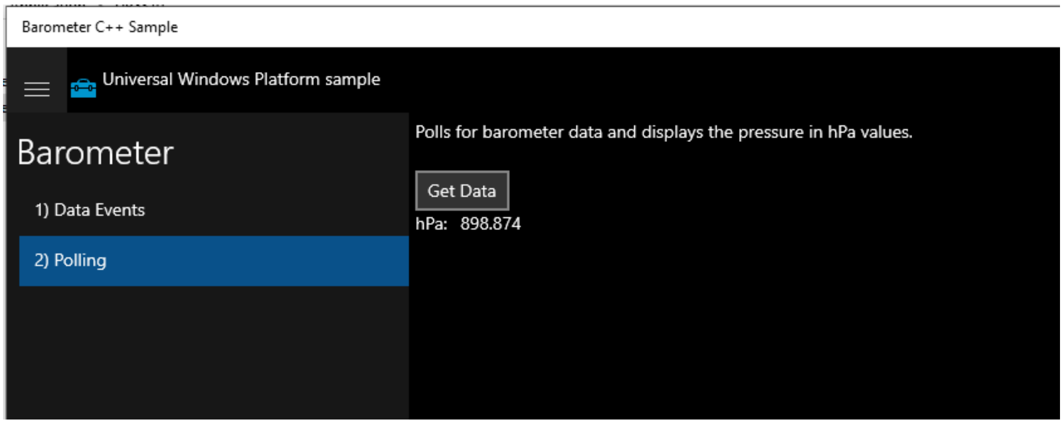


Registers an event listener for barometer data and displays the pressure in hPa values as they are reported.

hPa: 898.861

Figure 49. DataEvents

3. Select **Polling** > **Get Data** and repeat Steps 1 and 2.



Polls for barometer data and displays the pressure in hPa values.

hPa: 898.874

Figure 50. Polling

Accelerometer sensor setup

Prerequisites

Windows standard APIs: FromIdAsync(String), GetCurrentReading(), GetDefault(), and GetDeviceSelector(Guid interfaceId) are used for accessing the sensor. For details, go to the Windows.Devices.Sensors.Custom Namespace Microsoft page.

About this task

The ADXL345 accelerometer sensor is connected to I2C bus 2 of the EGW-3200. This sensor is detected as a accelerometer sensor and follows Windows sensor framework.

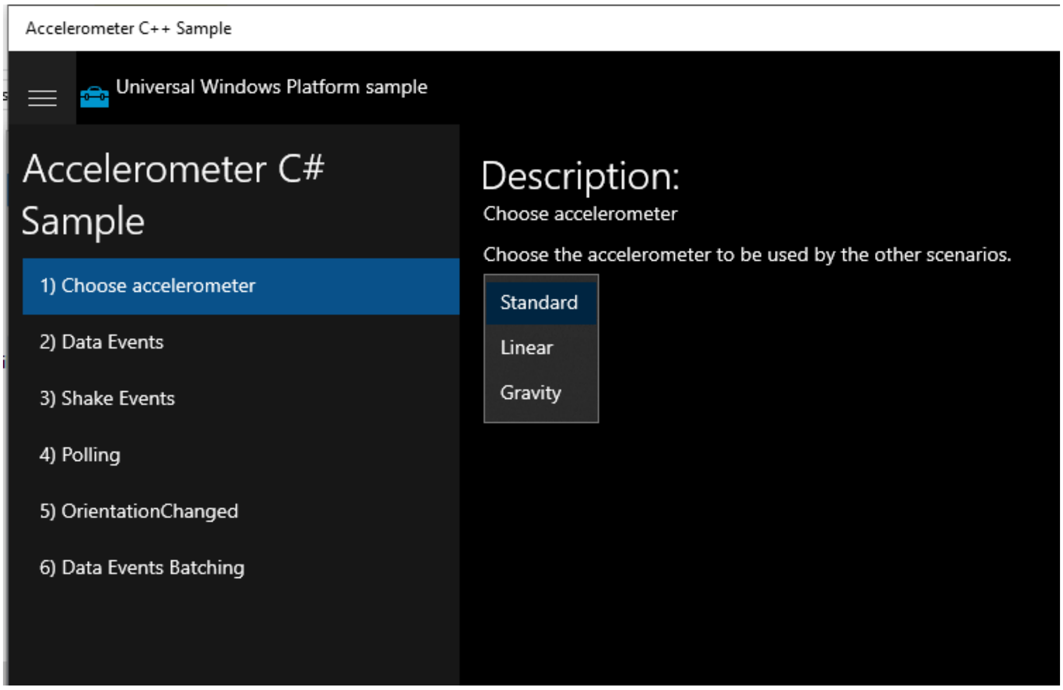
See the Humidity and temperature sensor setup section for the following tasks:

- Build the sample application
- Create the MSIX package
- Import the certificate
- Install the application

Run the accelerometer sensor application

Steps

1. **Choose accelerometer**: Click the **Standard** type of accelerometer.



Accelerometer C++ Sample

Universal Windows Platform sample

Accelerometer C# Sample

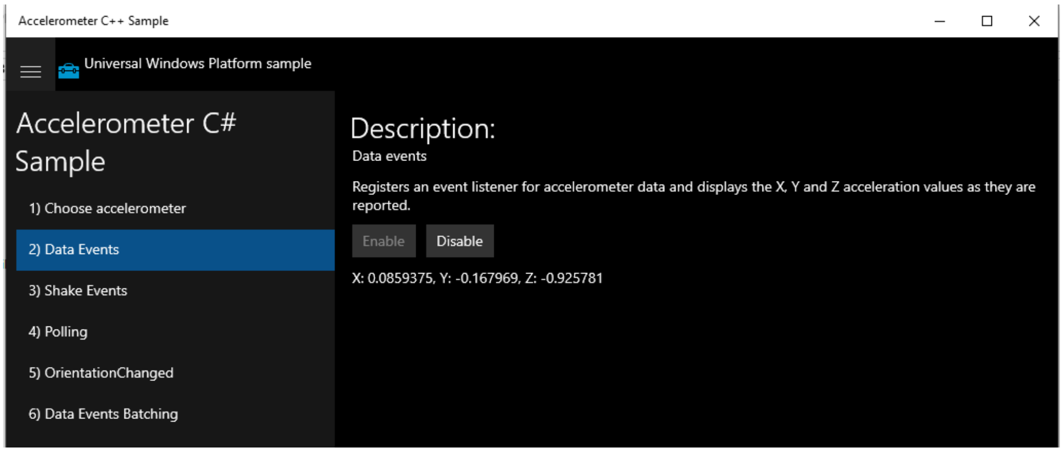
Description:

Choose accelerometer

Choose the accelerometer to be used by the other scenarios.

Figure 51. Choose accelerometer

2. **Data Events**: Click **Enable**. The corresponding x, y, and z values are displayed as you change the position of the sensor.



Description:

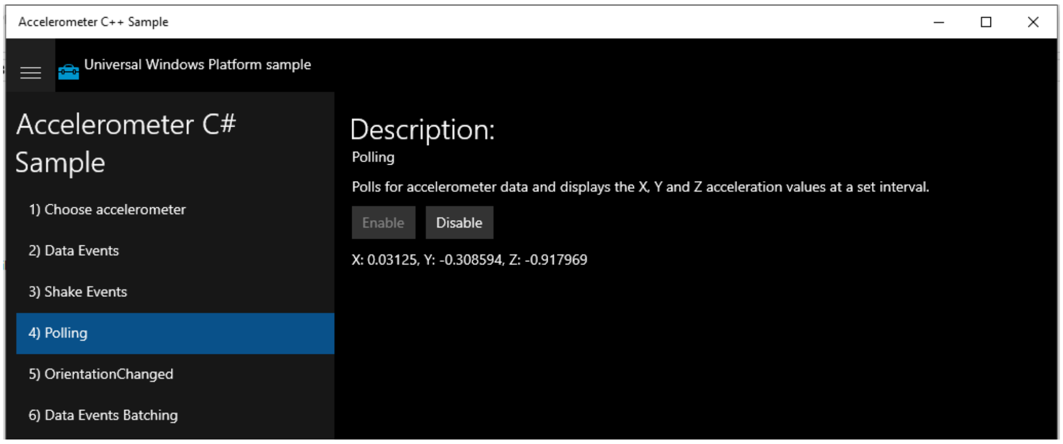
Data events

Registers an event listener for accelerometer data and displays the X, Y and Z acceleration values as they are reported.

X: 0.0859375, Y: -0.167969, Z: -0.925781

Figure 52. Data Events

3. **Polling**: Click **Enable**. Acceleration values at a particular time interval are displayed.



Description:

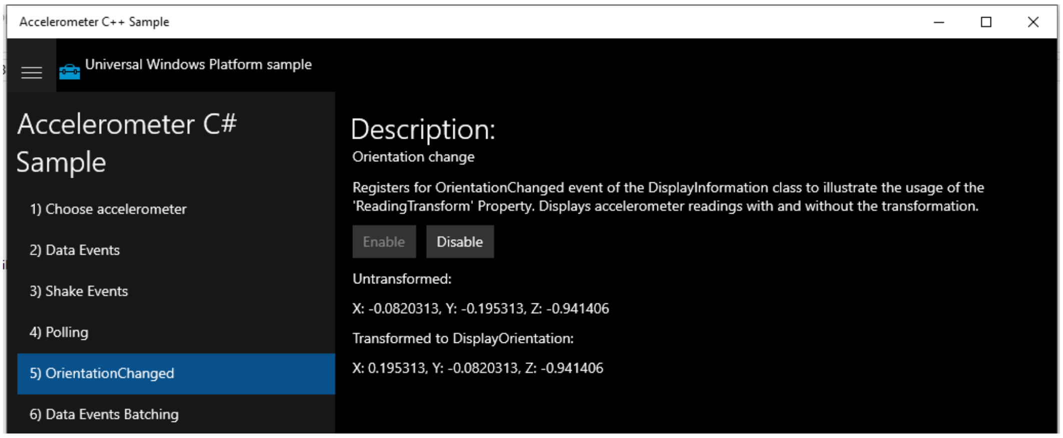
Polling

Polls for accelerometer data and displays the X, Y and Z acceleration values at a set interval.

X: 0.03125, Y: -0.308594, Z: -0.917969

Figure 53. Polling

4. **OrientationChanged**: Click **Enable** to display the accelerometer readings with and without the transformation.



Description:

Orientation change

Registers for OrientationChanged event of the DisplayInformation class to illustrate the usage of the 'ReadingTransform' Property. Displays accelerometer readings with and without the transformation.

Untransformed:

X: -0.0820313, Y: -0.195313, Z: -0.941406

Transformed to DisplayOrientation:

X: 0.195313, Y: -0.0820313, Z: -0.941406

Figure 54. OrientationChanged

Intel OOB

Out-of-Band (OOB) is the service that is performed if the processor platform runs on the ARM Cortex-M7 processor that is independent of the system's main CPU complex and host OS. The OOB service is enabled through PSE and allows users to execute cloud-initiated commands such as reboot, shutdown, and powerup, and to decommission device operations using the scalable device management clouds as the Azure IOT central cloud.

Table 5. Hardware requirements

Device	Specification
Linux OS (development machine)	Ubuntu OS version 18.04 LTS installed with display monitor, keyboard, and mouse
Edge Gateway 3200 (target board)	Windows 10 OS installed with display monitor, keyboard, and mouse
Other hardware	A router with ethernet LAN cable (wired)

Host and target setup

Host setup

The development machine (host) should have the Linux Ubuntu OS (version 18.04 LTS and above) installed.

NOTE: We have used Ubuntu version 20.04 LTS.

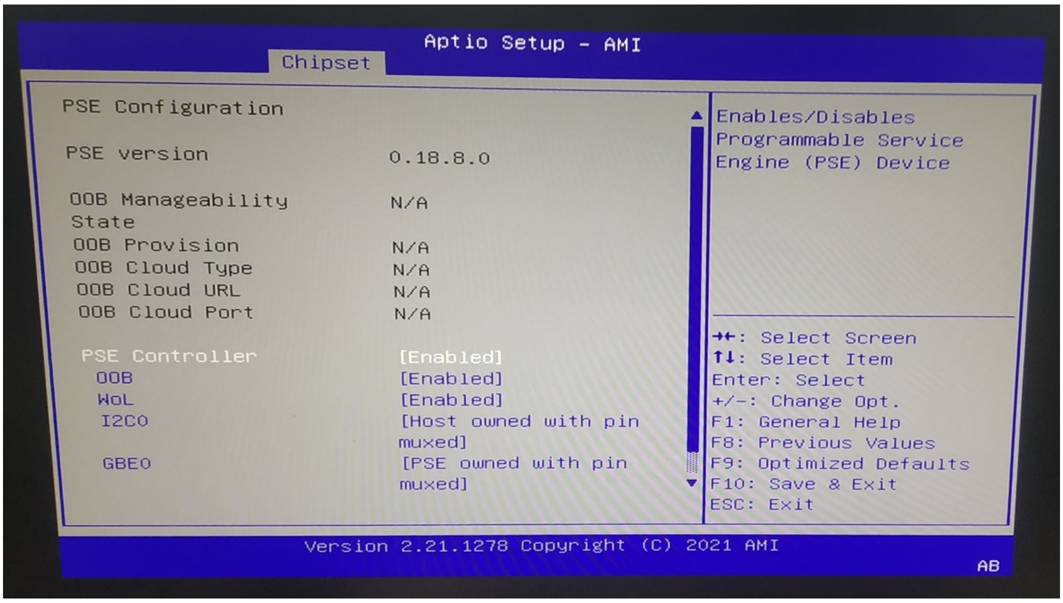
Target setup

The Dell Edge Gateway 3200 with the Elkhart Lake Platform and with Windows 10 Enterprise LTSC 2019 installed.

Perform changes in the BIOS

Steps

1. At the BIOS menu, select **Chipset** > **PCH-IO Configuration** > **PSE Configuration** > **OOB [Enabled**].
2. Set this OOB to be **Enabled**. OOB provisioning will fail in OOB service provisioning if this is not set to **Enabled**.
3. At the BIOS menu, select **Chipset** > **PCH-IO Configuration** > **PSE Configuration** > **GBE0 [PSE owned with pin muxed]**.



```
                    Aptio Setup - AMI
              Chipset
  PSE Configuration                                 Enables/Disables
                                                    Programmable Service
  PSE version                  0.18.8.0             Engine (PSE) Device

  OOB Manageability            N/A
  State
  OOB Provision                N/A
  OOB Cloud Type               N/A
  OOB Cloud URL                N/A
  OOB Cloud Port               N/A
                                                    →←: Select Screen
  PSE Controller               [Enabled]            ↑↓: Select Item
    OOB                        [Enabled]            Enter: Select
    WoL                        [Enabled]            +/-: Change Opt.
    I2C0                       [Host owned with pin F1: General Help
                               muxed]               F8: Previous Values
    GBE0                       [PSE owned with pin  F9: Optimized Defaults
                               muxed]               F10: Save & Exit
                                                    ESC: Exit
          Version 2.21.1278 Copyright (C) 2021 AMI
                                                            AB
```

Figure 55. Configure OOB enabled

4. Press the **Esc** button to return to the main menu. When prompted with **Save Changes and exit?**, press **Y** to save the settings.
5. Perform a hard reset by turning the power off and on again. This is necessary when changing a PSE-related setting.
6. Connect an Ethernet cable to PSE GbE0.

Results

You have now set up hardware network connectivity on the target board, which is now ready to connect with the Cloud Service Provider (CSP), as detailed in the following sections.

Cloud setup and configuration

About this task

The cloud adapter module maps specific cloud functions based on the cloud service provider and implements specific cloud customizations such as Message Queuing Telemetry Transport (MQTT) topics and message formats.

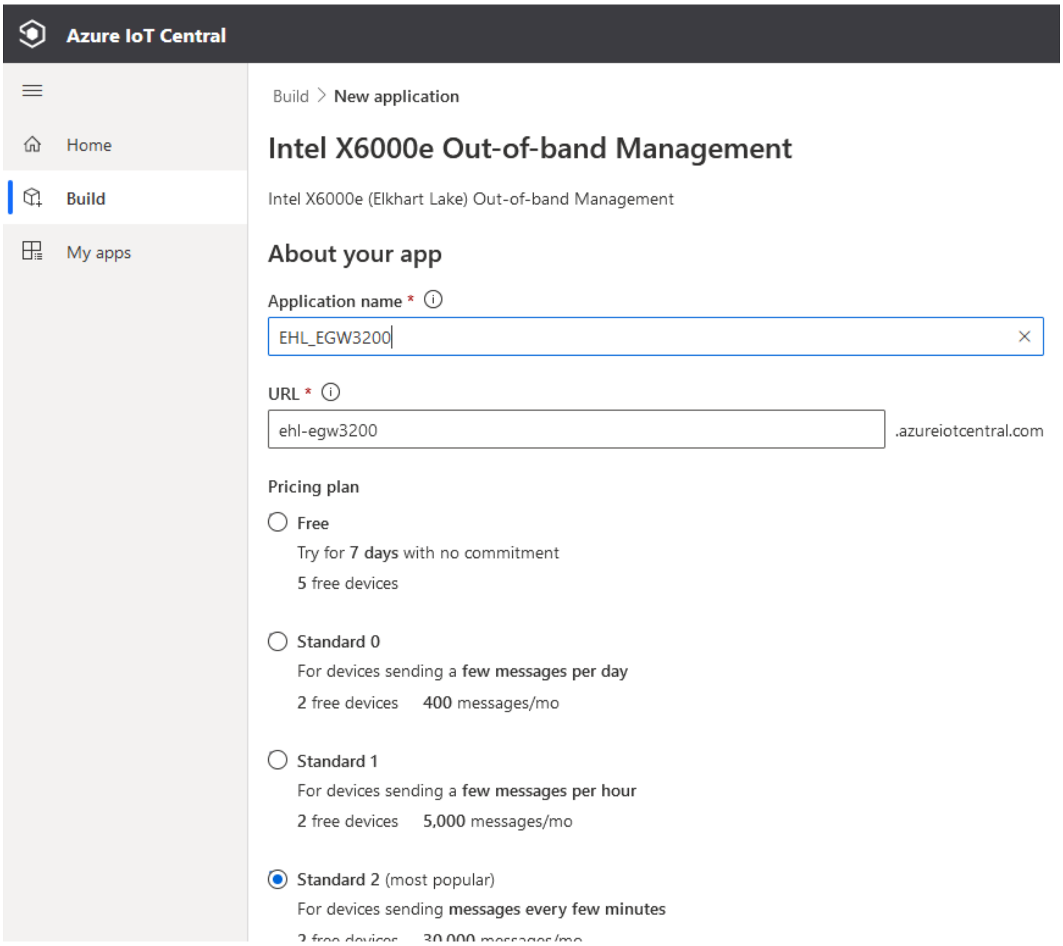
Set up Azure IoT Central for device management

About this task

Intel provides the connectivity reference implementation for the Microsoft Azure device management solution.

Steps

1. Create an Azure account and an Azure IoT Central application for the device to connect to its intended portal customers. Refer to the instructions on the Azure website to create an Azure account.
2. Create an IoT Central application by importing the reference template from the Azure IoT Central site.
3. Create a template application name and URL, then click **Create** to create an IoT central application template.



Build > New application

Intel X6000e Out-of-band Management

Intel X6000e (Elkhart Lake) Out-of-band Management

About your app

Application name * ⓘ

EHL_EGW3200

URL * ⓘ

ehl-egw3200 .azureiotcentral.com

Pricing plan

○ Free
Try for **7 days** with no commitment
5 free devices

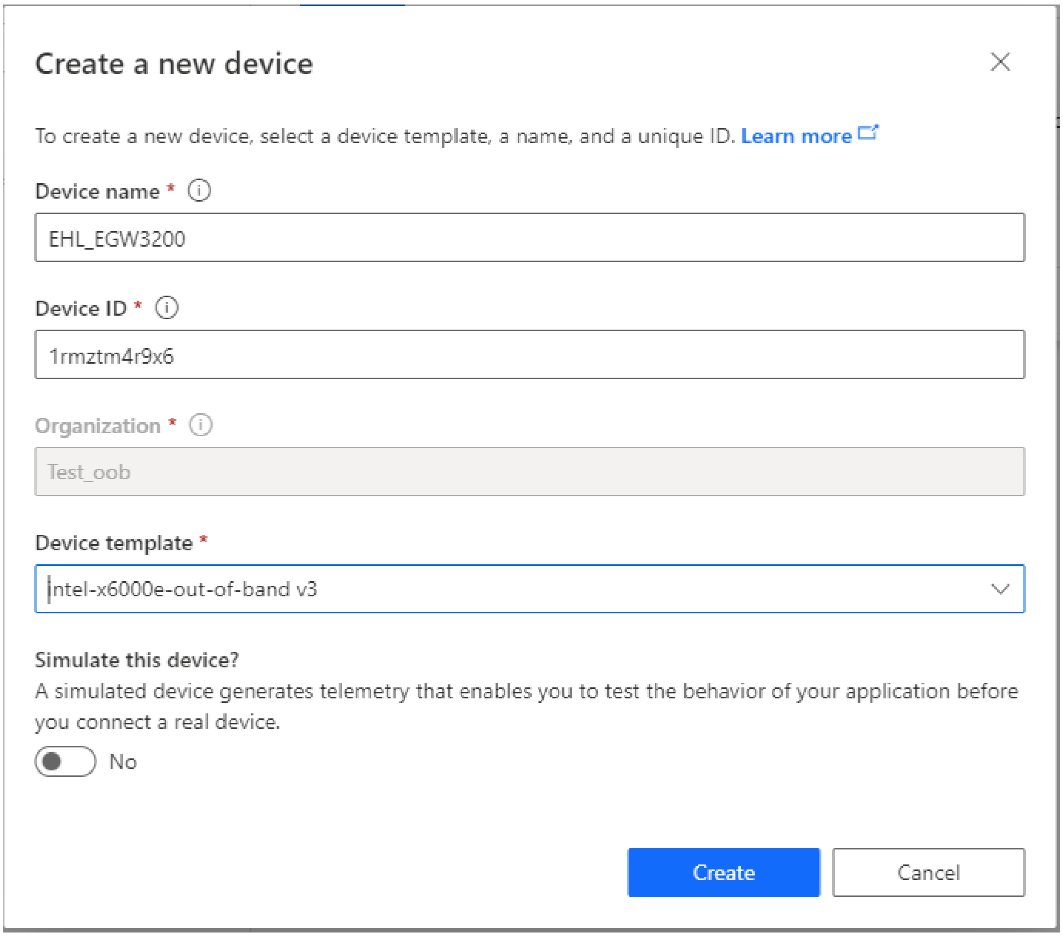
○ Standard 0
For devices sending a **few messages per day**
2 free devices 400 messages/mo

○ Standard 1
For devices sending a **few messages per hour**
2 free devices 5,000 messages/mo

● Standard 2 (most popular)
For devices sending **messages every few minutes**
2 free devices 30,000 messages/mo

Figure 56. Azure IoT central application template

4. After creating the Azure portal and template, add a new device. Click the **Devices** tab, select the Intel template, and then click the **+** symbol to create a real device.



Create a new device

To create a new device, select a device template, a name, and a unique ID. Learn more

Device name * ⓘ

EHL_EGW3200

Device ID * ⓘ

1rmztm4r9x6

Organization * ⓘ

Test_oob

Device template *

intel-x6000e-out-of-band v3

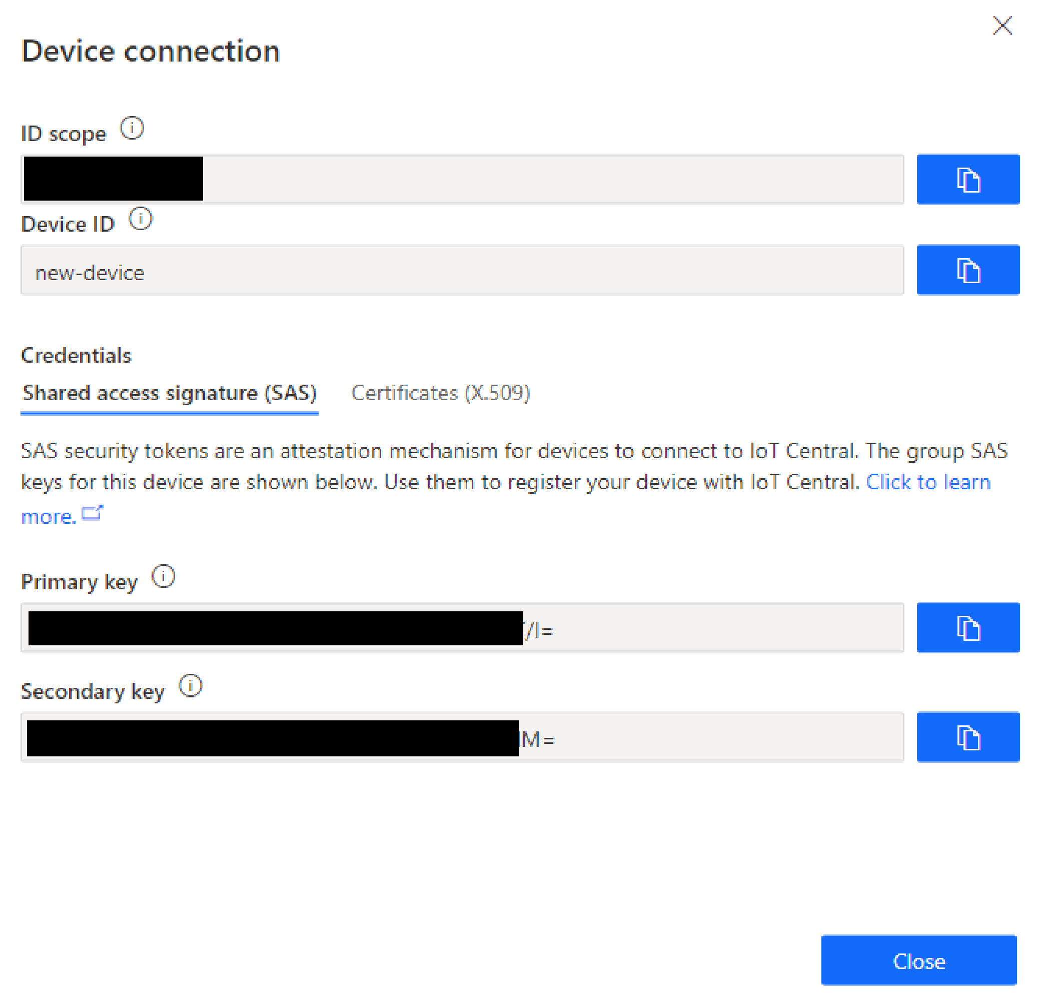
Simulate this device?

A simulated device generates telemetry that enables you to test the behavior of your application before you connect a real device.

○ No

Figure 57. Create a new device

5. Copy the connectivity credentials for the device to connect back to the portal. Copy the connection credentials by clicking the **Connect** button. The following screen appears.



Device connection

ID scope

[redacted]

Device ID

new-device

Credentials

SAS security tokens are an attestation mechanism for devices to connect to IoT Central. The group SAS keys for this device are shown below. Use them to register your device with IoT Central. Click to learn more.

Primary key

[redacted]/I=

Secondary key

[redacted]M=

Figure 58. Device connection

6. Keep a copy of the following data. Use these data to create credentials for the target device to connect to the portal over the MQTT protocol. Intel provides a sample script that gives the credentials by invoking the Azure IoT Hub Device Provisioning Service (DPS).
   - ID scope
   - Device ID
   - Primary key

Create an OOB capsule binary

About this task

In this task, the user generates the OOB credentials capsule binary in the host machine.

Steps

1. Prepare the OOB credentials capsule from the host machine.
2. Get the Intel Programmable Service Engine SDK source code.
3. Download the Firmware and BIOS Utilities (FBU), which is the configuration tool for provisioning data into BIOS subregions. The latest open-source FBU release package can be downloaded from the iotg-fbu page at the GitHub software development platform.

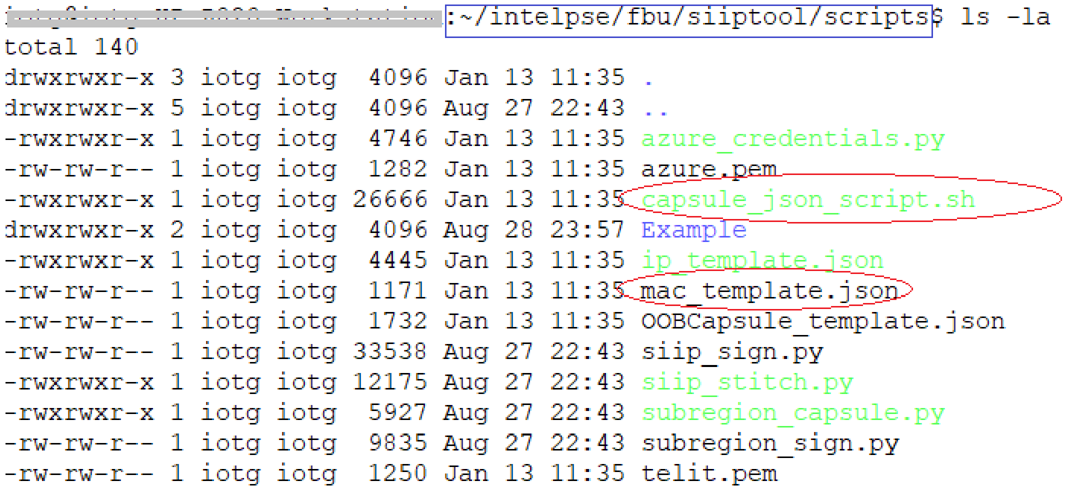
4. Copy all files from the pse-dev-code-base/tools/capsule_script folder to the scripts folder of the FBU tool. This ensures that you have all of the files needed to generate the MAC and OOB credentials capsules in the correct location:

```
cp ~/intelpse/pse_sdk/code/pse-dev-code-base/tools/capsule_scripts/* ~/intelpse/fbu/
siiptool/scripts/
```

5. Go to the scripts folder of the FBU tool:

```
cd ~/intelpse/fbu/siiptool/scripts
```

6. Confirm that the files were added to the scripts folder, as shown in the following figure.



```
[redacted]:~/intelpse/fbu/siiptool/scripts$ ls -la
total 140
drwxrwxr-x 3 iotg iotg  4096 Jan 13 11:35 .
drwxrwxr-x 5 iotg iotg  4096 Aug 27 22:43 ..
-rwxrwxr-x 1 iotg iotg  4746 Jan 13 11:35 azure_credentials.py
-rw-rw-r-- 1 iotg iotg  1282 Jan 13 11:35 azure.pem
-rwxrwxr-x 1 iotg iotg 26666 Jan 13 11:35 capsule_json_script.sh
drwxrwxr-x 2 iotg iotg  4096 Aug 28 23:57 Example
-rwxrwxr-x 1 iotg iotg  4445 Jan 13 11:35 ip_template.json
-rw-rw-r-- 1 iotg iotg  1171 Jan 13 11:35 mac_template.json
-rw-rw-r-- 1 iotg iotg  1732 Jan 13 11:35 OOBCapsule_template.json
-rw-rw-r-- 1 iotg iotg 33538 Aug 27 22:43 siip_sign.py
-rwxrwxr-x 1 iotg iotg 12175 Aug 27 22:43 siip_stitch.py
-rwxrwxr-x 1 iotg iotg  5927 Aug 27 22:43 subregion_capsule.py
-rw-rw-r-- 1 iotg iotg  9835 Aug 27 22:43 subregion_sign.py
-rw-rw-r-- 1 iotg iotg  1250 Jan 13 11:35 telit.pem
```

Figure 59. Capsule script file

7. Run the user script using the following commands:

```
chmod +x capsule_json_script.sh
```

8. Launch the script according to your cloud certificate:

```
./capsule_json_script.sh azure.pem
```

NOTE: `azure.pem` is the cloud certificate.

9. The script will prompt for the following user inputs:
    a. **Select Capsule Type**: Type **`1`** for OOB.
    b. **Enter Capsule file name**: Type a **`filename`** for the capsule binary, for example "OobCapsule".
    c. **Select Cloud Provider**: Type **`2`** for Azure.
    d. **Enter Scope ID**: Provide the scope ID copied in the previous task, Set up Azure IoT Central for device management.
    e. **Enter Device ID**: Provide the device ID copied in the previous task, Set up Azure IoT Central for device management.
    f. **Enter Primary Key**: Provide the primary key copied in the previous task, Set up Azure IoT Central for device management.
    g. **Enter Proxy (SOCKS5) IP**: Enter the proxy address of your organization. Press **Enter** for a blank field entry if there is no proxy address.
10. At completion, a JSON file (.json) and its capsule binary file (.bin) are created.
11. Copy the .bin file to the USB flash drive.

Results

The flash drive now includes the MAC capsule (Phy.zip) and OOB credentials capsule files.

OOB service provisioning

About this task

In this task, the user connects the USB flash drive with the capsule files from the host machine, inserts the flash drive to a USB port on the EGW-3200 target board, and updates the MAC capsule and OOB capsule binary files.

Update the MAC capsule

Steps

1. To update the MAC capsule, use the tool (**Phy.zip**) and update the MAC address under UEFI Shell.
2. Use **CapsuleApp.efi** to update the MAC capsule under UEFI Shell directly.

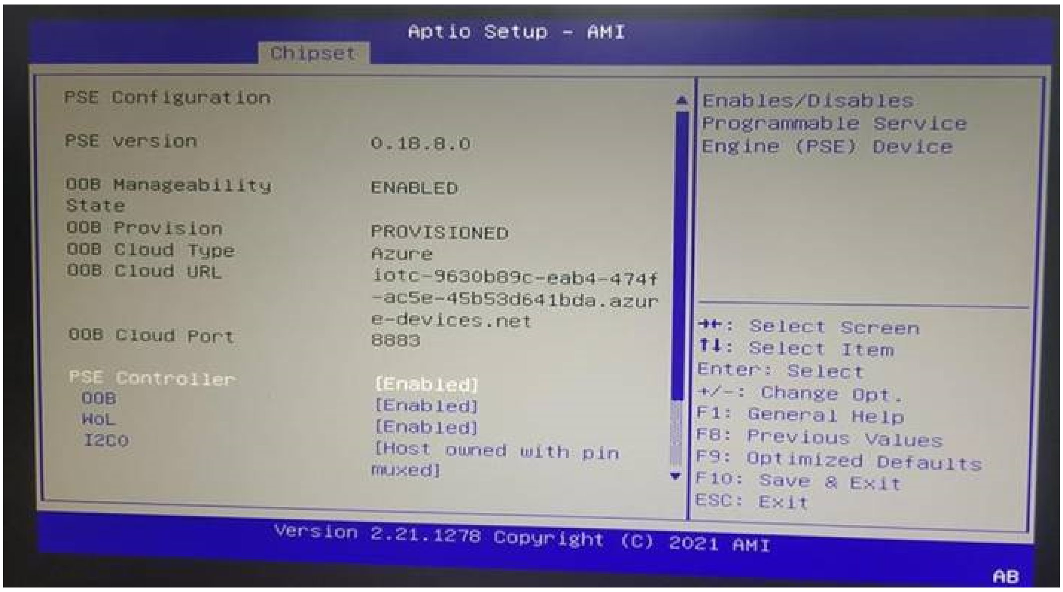
   Usage: **CapsuleApp.efi capsule.out.bin**
3. Perform a hard reset by turning the power off and on after updating the MAC address.

Update the OOB credentials capsule

Steps

1. To update the OOB capsule, use **CapsuleApp.efi** with capsule binary under UEFI Shell directly.

   Usage: **CapsuleApp.efi OobCapsule.bin**
2. Perform a hard reset by turning the power off and on after updating the OOB capsule.
3. At the BIOS menu, select **Chipset**, as shown in the following figure.
4. Find the **OOB Cloud Type**, **OOB Cloud URL**, and **OOB Cloud Port** information. The OOB feature state and provisioning state should be **Enabled**, as shown in the following figure.



```
                          Aptio Setup - AMI
              Chipset
 PSE Configuration                                   ▲ Enables/Disables
                                                       Programmable Service
 PSE version              0.18.8.0                     Engine (PSE) Device

 OOB Manageability        ENABLED
 State
 OOB Provision            PROVISIONED
 OOB Cloud Type           Azure
 OOB Cloud URL            iotc-9630b89c-eab4-474f
                          -ac5e-45b53d641bda.azur
                          e-devices.net
 OOB Cloud Port           8883                         →←: Select Screen
                                                       ↑↓: Select Item
 PSE Controller           [Enabled]                    Enter: Select
  OOB                     [Enabled]                    +/-: Change Opt.
  WoL                     [Enabled]                    F1: General Help
  I2C0                    [Host owned with pin         F8: Previous Values
                          muxed]                       F9: Optimized Defaults
                                                     ▼ F10: Save & Exit
                                                       ESC: Exit
              Version 2.21.1278 Copyright (C) 2021 AMI
                                                                   AB
```

Figure 60. BIOS menu

Activate OOB commands using Azure

Prerequisites

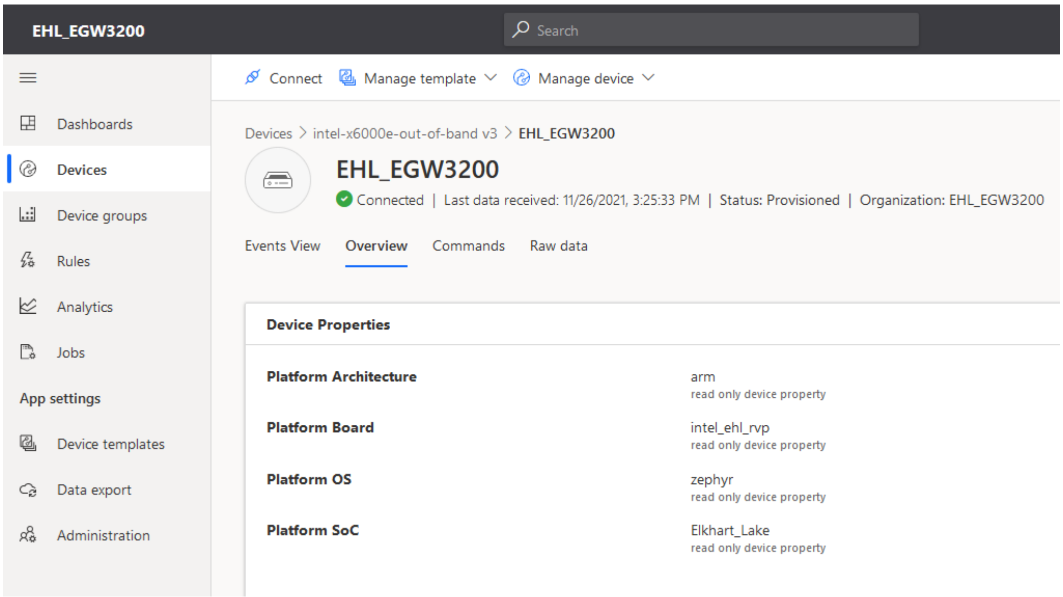
A device management cloud account is created and the EGW-3200 is successfully provisioned with the OOB credentials to connect to the cloud.

About this task

In this task, the user sends an OOB command from the Azure IoT Central portal.

Steps

1. After provisioning and connecting the device to the Azure IoT Central portal, the device status changes to **provisioned**.
2. Click on the device and then navigate to the following for more information:
   a. **Overview**: To view the **Device Properties**.



Devices > intel-x6000e-out-of-band v3 > EHL_EGW3200

EHL_EGW3200

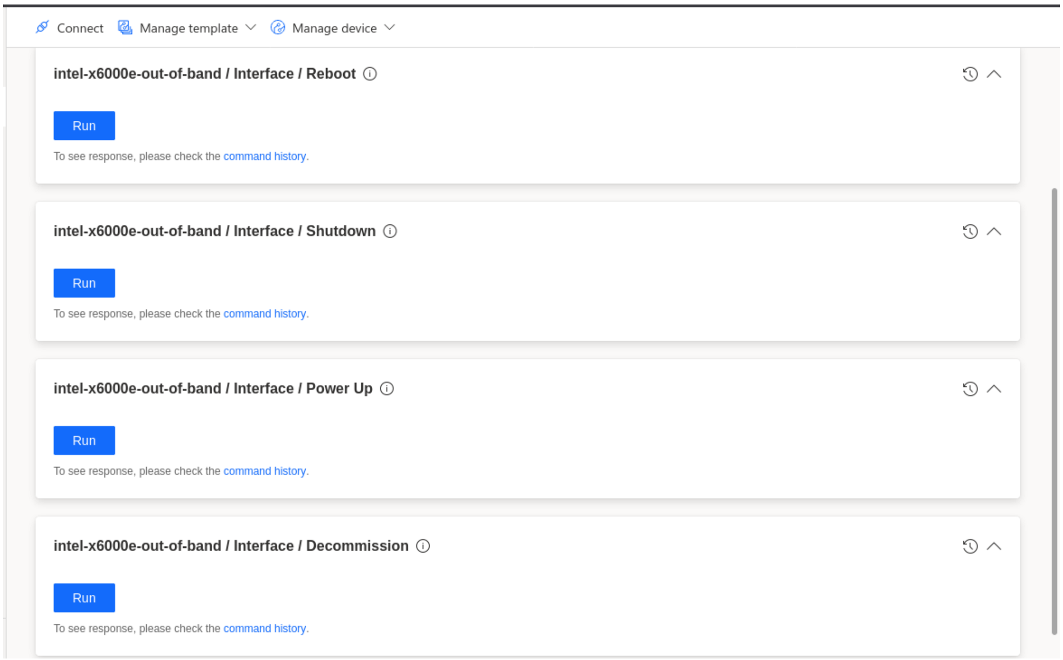
Connected | Last data received: 11/26/2021, 3:25:33 PM | Status: Provisioned | Organization: EHL_EGW3200

Device Properties

Platform Architecture	arm read only device property
Platform Board	intel_ehl_rvp read only device property
Platform OS	zephyr read only device property
Platform SoC	Elkhart_Lake read only device property

Figure 61. Overview

   b. **Commands**: to send OOB power control commands to the device.
3. The OOB service, enabled through the PSE, allows the user to execute the following commands:
   - **Reboot**: Reboots platform.
   - **Shutdown**: Puts the platform in a low power state.
   - **Power Up**: Brings the platform out of low power state.
   - **Decommission**: Un-registers the platform, withdrawing the device from remote management using the cloud.



intel-x6000e-out-of-band / Interface / Reboot

Run

To see response, please check the command history.

intel-x6000e-out-of-band / Interface / Shutdown

Run

To see response, please check the command history.

intel-x6000e-out-of-band / Interface / Power Up

Run

To see response, please check the command history.

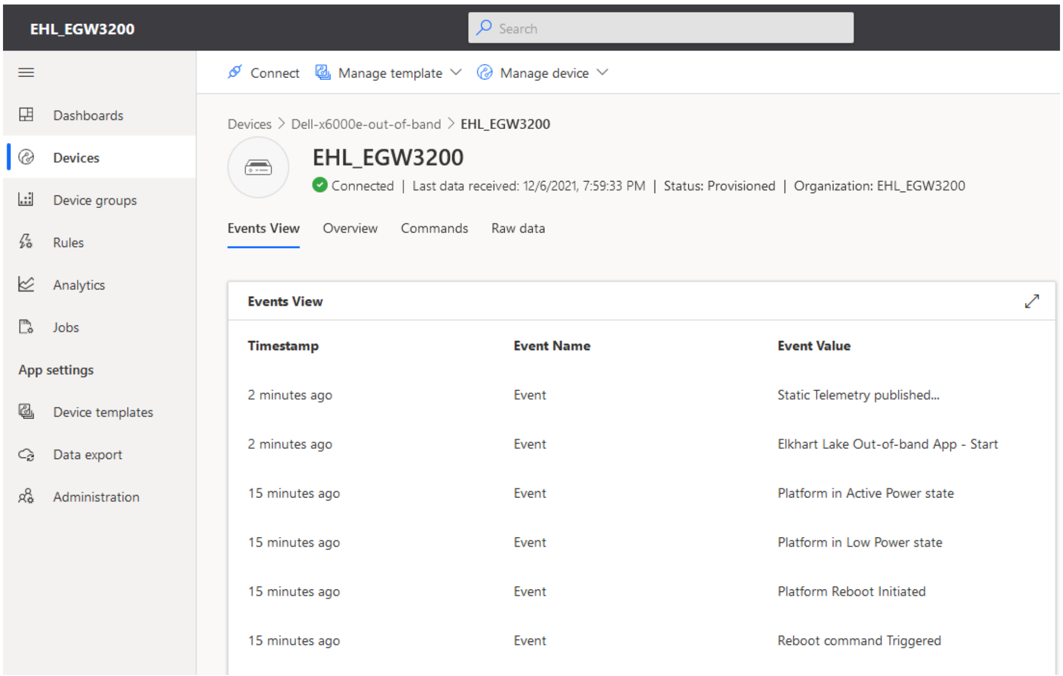
intel-x6000e-out-of-band / Interface / Decommission

Run

To see response, please check the command history.

Figure 62. Commands

4. The user can view the device events and responses under the **Events View** or **Raw data** tabs.



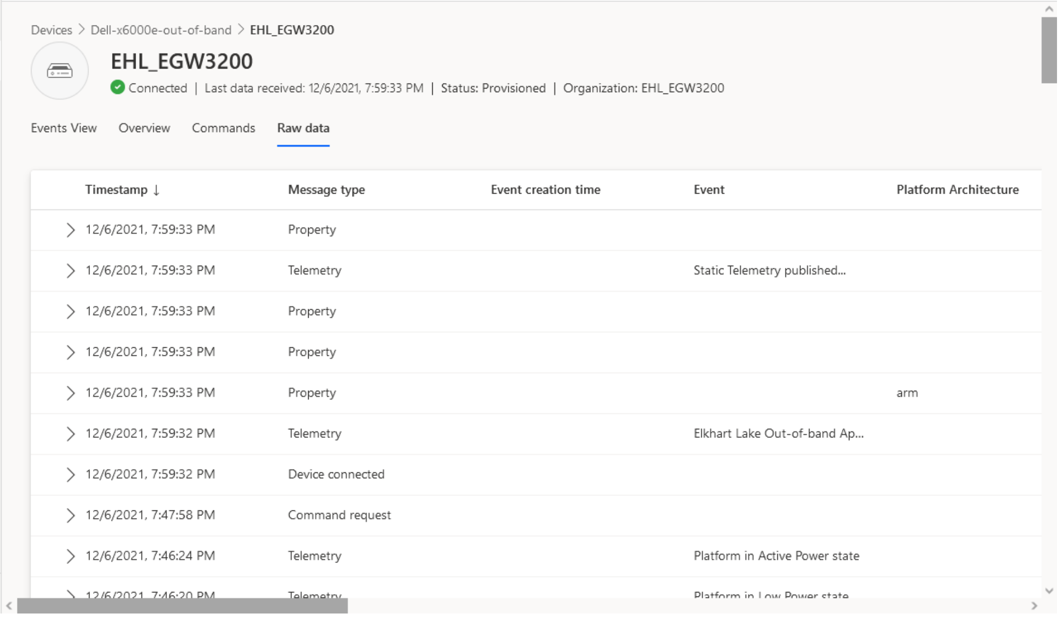
EHL_EGW3200

Connected | Last data received: 12/6/2021, 7:59:33 PM | Status: Provisioned | Organization: EHL_EGW3200

Events View

Timestamp	Event Name	Event Value
2 minutes ago	Event	Static Telemetry published...
2 minutes ago	Event	Elkhart Lake Out-of-band App - Start
15 minutes ago	Event	Platform in Active Power state
15 minutes ago	Event	Platform in Low Power state
15 minutes ago	Event	Platform Reboot Initiated
15 minutes ago	Event	Reboot command Triggered

Figure 63. Events View



Devices > Dell-x6000e-out-of-band > EHL_EGW3200

EHL_EGW3200

Connected | Last data received: 12/6/2021, 7:59:33 PM | Status: Provisioned | Organization: EHL_EGW3200

Timestamp ↓	Message type	Event creation time	Event	Platform Architecture
12/6/2021, 7:59:33 PM	Property			
12/6/2021, 7:59:33 PM	Telemetry		Static Telemetry published...	
12/6/2021, 7:59:33 PM	Property			
12/6/2021, 7:59:33 PM	Property			
12/6/2021, 7:59:33 PM	Property			arm
12/6/2021, 7:59:32 PM	Telemetry		Elkhart Lake Out-of-band Ap...	
12/6/2021, 7:59:32 PM	Device connected			
12/6/2021, 7:47:58 PM	Command request			
12/6/2021, 7:46:24 PM	Telemetry		Platform in Active Power state	
12/6/2021, 7:46:20 PM	Telemetry		Platform in Low Power state	

Figure 64. Raw data

COM Port and Ethernet Names for Mini PCIe Cards

Table 6. Mini PCIe card details

S.No	mPCie module	Isolated COM A (port type)	Isolated COM B (port type)	Remarks
1	EMP2-X4S2	RS422/RS485	RS422/RS485	Total of four COM ports are detected in the Device Manager. However, only two COM ports can be accessed. Assume that the first COM port of EMP2-X4S2 is COM X, as seen in the device manager, then, based on the cable tag: RS-422 A - COM X RS-422 B - COM X+1 RS-485 A - COM X+2 RS-485 B - COM X+3
2	EMP2-X2S1	RS232	RS232	Total of two COM ports are detected in the Device Manager. Assume that the first COM port of EMP2-X2S1 is COM X, then, based on the cable tag: Isolated COM A - COM X Isolated COM B - COM X+1

For EMP2-X2S1:

Both EMP2-X2S1 and EMP2-X4S2 use the same VID and DID. By default, the EMP2-X2S1 module uses the driver files of the EMP2-X4S2 module, and so the device manager shows four COM ports. To overcome this issue, manually install the EMP2-X2S1 Windows 10 64-bit driver package.

For EMPL-G2P1 and EMPL-G201:

Get the Ethernet name from **Control Panel** > **Network and Internet** > **Network Connections**, based on the MAC address of the Ethernet ports.

Sensor APIs

The sensors of the EGW-3200 use Microsoft default sensor APIs. This section serves as a programming reference of the Win32 API. For more details, see the sensorsapi.h header Microsoft page.

Table 7. Console application APIs for ADXL345/HDC1010/DPS310

S.No	Console application APIs	Description	Supported/not supported
1.	GetSensorsByType	Retrieves a collection containing all sensors associated with the specified type.	Supported
2.	GetData	Retrieves the most recent sensor data report.	Supported
3.	GetAt	Retrieves the sensor at the specified index in the collection.	Supported
4.	GetCategory	Retrieves the identifier of the sensor category.	Supported
5.	GetSensorValue	Retrieves a single data field value from the data report.	Supported
6.	GetSensorValues	Retrieves a collection of data field values.	Supported
7.	GetCount	Retrieves the count of sensors in the collection.	Supported
8.	GetFriendlyName	Retrieves the sensor name that is intended to be seen by the user.	Supported
9.	GetState	Retrieves the current operational state of the sensor.	Supported
10.	SetEventSink	Specifies the interface through which to receive sensor event notifications.	Supported
11.	GetSensorByID	Retrieves a pointer to the specified sensor.	Supported
12.	GetProperties	Retrieves multiple sensor properties.	Supported
13.	GetProperty	Retrieves a property value.	Supported
14.	GetSupportedDataFields	Retrieves a set of PROPERTYKEYs that represent the data fields the sensor can provide.	Supported
15.	SetProperties	Specifies sensor properties.	Supported
16.	Add	Adds a sensor to the collection.	Supported
17.	GetTimestamp	Retrieves the time at which the data report was created.	Supported
18.	OnDataUpdated	Provides sensor event data.	Supported
19.	OnEvent	Provides custom event notifications.	Supported
20.	OnLeave	Provides notification that a sensor device is no longer connected.	Supported
21.	OnStateChanged	Provides a notification that a sensor state has changed.	Supported
22.	GetEventInterest	Retrieves the current event interest settings.	Supported
23.	SetEventInterest	Specifies the list of sensor events to receive.	Supported
24.	SupportsEvent	Indicates whether the sensor supports the specified event.	Supported

Table 8. UWP application APIs for ADXL345/HDC1010/DPS310

S.No	UWP application APIs	Description	Supported/not supported
1.	FromIdAsync	Asynchronously obtains the sensor from its identifier.	Supported
2.	GetCurrentReading	Gets the current sensor reading.	
3.	GetDefault	Returns the default sensor type.	
4.	GetDeviceSelector(Guid interfaceId)	Gets the device selector.	

Table 9. UWP application sensor events for ADXL345

S.No	Event name	Supported/not supported
1.	Choose accelerometer	Supported
2.	Data Events	
3.	Polling	
4.	OrientationChanged	
5.	Shake Events	Not supported[a, b]
6.	Data Events Batching	

[a] The interrupts which can be enabled from the driver side are Single tap, Double tap, Activity, Inactivity, and Free fall (in INT_ENABLE register). The detection of Shake events is not supported.

[b] Data Events Batching is not supported due to the fact that the driver does not implement it.

Table 10. UWP application sensor events for DPS310

S.No	Event name	Supported/not supported
1.	Data Events	Supported
2.	Polling	

Table 11. UWP application sensor events for HDC1010

S.No	Event name	Supported/not supported
1.	Data Events	Supported
2.	Polling	

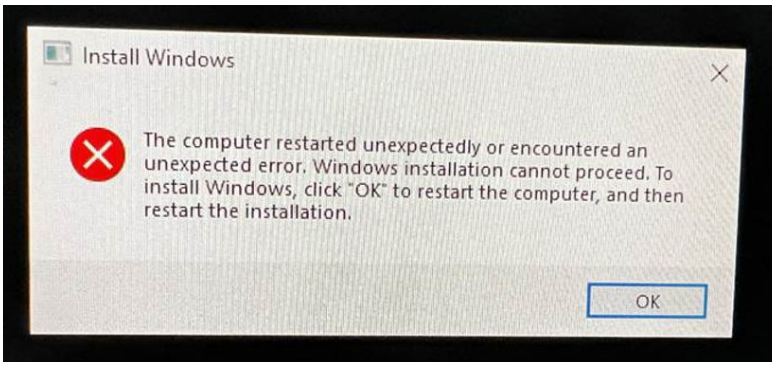
Windows troubleshooting

The following tasks describe how to recover from errors when using Windows.

Recover from Install Windows error

About this task

The **Install Windows** error in the following figure may appear while the system is loading Windows. This is caused by an unexpected restart or error during the system boot up.



Install Windows

The computer restarted unexpectedly or encountered an unexpected error. Windows installation cannot proceed. To install Windows, click "OK" to restart the computer, and then restart the installation.

Figure 65. Install Windows error message

To recover from this error, perform the following steps.

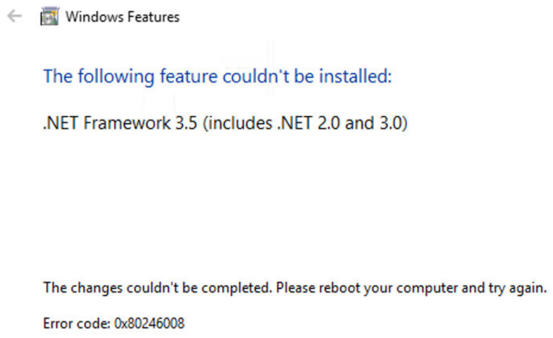
Steps

1. Navigate to the Command Prompt, or use the Shift + F10 keyboard shortcut.
2. Type the command: `regedit.`, then press **Enter** on your keyboard to start the **Registry Editor**.
3. If prompted by the **User Account Control**, click **Yes**.
4. In this new window, navigate to the following path:
   `HKEY_LOCAL_MACHINE\SYSTEM\Setup\Status\Child\Completion`
5. In the right pane, click `setup.exe` twice.
6. Change the `Value  Data` from 1 to 3, then click **OK** to save the change.
7. Close this window and reboot the system.

Recover from .NET Framework installation error

About this task

The **.NET Framework** error in the following figure may appear while the system boots.



Windows Features

The following feature couldn't be installed:

.NET Framework 3.5 (includes .NET 2.0 and 3.0)

The changes couldn't be completed. Please reboot your computer and try again.

Error code: 0x80246008

Figure 66. .NET Framework installation error

To recover from this error, perform the following steps.

Steps

1. Confirm that the system has a network connection.
2. Download the .NET Framework 3.5 SP1 Web Installer from the Microsoft website.
3. Open the installer and wait for the installation to complete.

3

Setting Up the Ubuntu Operating System

This chapter serves as a guide to install and use the Ubuntu 20.04 LTS operating system on the EGW-3200 hardware.

For more information on this operating system, see the Ubuntu 20.04 LTS Home Page.

Topics:

Boot up and log in

Steps

1. Connect a keyboard, mouse, and monitor to the EGW-3200.
2. Power on the system. The system boots to the Ubuntu 20.04 LTS operating system.
3. Log in to the sysem. At initial login, the user must change the password of the default account.

   ⓘ **NOTE:** The default username/password is ubuntu/ubuntu.

Create bootable USB stick for restore

About this task

Perform this task for restoration of the system.

Steps

1. Install the image. Download the Ubuntu Desktop image 21.10 or a newer version from the Canonical website.
2. To create a bootable USB stick, perform the steps in the Create a bootable USB stick on Ubuntu tutorial.

   To create a bootable USB stick with Rufus on Windows, perform the steps in the Create a bootable USB stick with Rufus on Windows tutorial.

Back up and restore Ubuntu 20.04 LTS

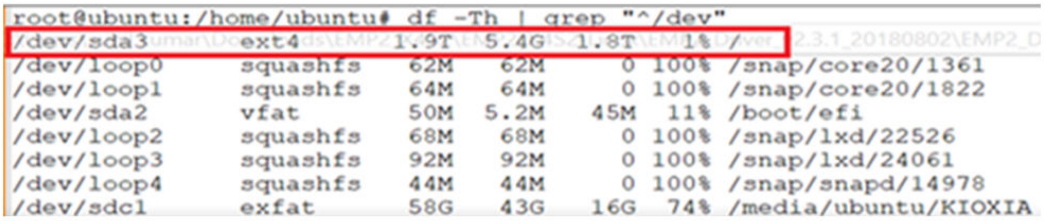
Prerequisites

Before performing the following recovery process, it is recommended to clear the target SSD. For a secure-erase supported SSD, see SSD security-erase, or use the basic clear command:

```
$ sudo dd if=/dev/zero of=/dev/sdx bs=<block size> count=<block number> status=progress
```

Steps

1. For the backup process, perform the following steps to prepare two USB sticks:
   a. One USB stick is used to store the target Ubuntu image, and it should have sufficient space to store the backup data. The space required for the backup is based on the used space on the disk. For example, on a 2 TB disk, if the used space is 5.4 GB, then the space required on the USB stick should be around 5 GB, as the backup process compresses the image. For example, a 5.4 GB image is compressed to 1.9 GB, as shown in the following figure.



```
root@ubuntu:/home/ubuntu# df -Th | grep "^/dev"
/dev/sda3      ext4       1.9T  5.4G  1.8T   1% /
/dev/loop0     squashfs    62M   62M     0 100% /snap/core20/1361
/dev/loop1     squashfs    64M   64M     0 100% /snap/core20/1822
/dev/sda2      vfat        50M  5.2M   45M  11% /boot/efi
/dev/loop2     squashfs    68M   68M     0 100% /snap/lxd/22526
/dev/loop3     squashfs    92M   92M     0 100% /snap/lxd/24061
/dev/loop4     squashfs    44M   44M     0 100% /snap/snapd/14978
/dev/sdc1      exfat       58G   43G   16G  74% /media/ubuntu/KIOXIA
```

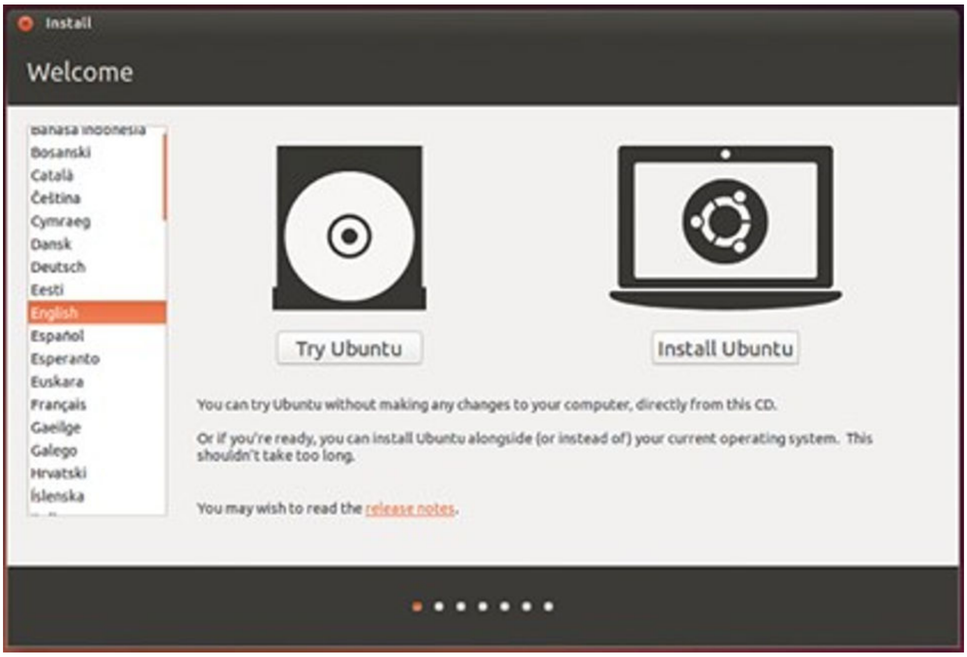
   Figure 67. Image compression

   b. Use the following command to back up your SSD data as an image on the USB stick. Depending on the size of the SSD, this process may take a while. For example, 2 TB takes around three hours to back up.

```
$ sudo fstrim / | sudo dd if=/dev/sdx status=progress | gzip -c > /media/ubuntu/
<USB stick name>/<image file name>
  $ xz -9v /media/ubuntu/<USB stick name>/<image file name>
```

   c. The other USB stick is made as Ubuntu Desktop live USB with version 21.10 or newer, as detailed in Create bootable USB stick for restore.

2. For the restore process, perform the following steps:
   a. Use Ubuntu Desktop live USB to boot up the device by BIOS, and then select **Try Ubuntu**:



You can try Ubuntu without making any changes to your computer, directly from this CD.

Or if you're ready, you can install Ubuntu alongside (or instead of) your current operating system. This shouldn't take too long.

You may wish to read the release notes.

Figure 68. Try Ubuntu

b. Plug in the USB stick that stores the backup image file, then open the Ubuntu terminal to enter the following command to flash the backup image into the target SSD:

```
$ xz -dv /media/ubuntu/<USB stick name>/<image file name>.xz
$ gzip -dc  /media/ubuntu/<USB stick name>/<image file name> | sudo dd of=/dev/sdx
status=progress;sync;
```

Typically, the image USB stick is mounted under /media/ubuntu/*<USB stick name>*, and the target SSD is mounted as /dev/sdx.

This image restore is a slow process. For example, a 2 TB SSD can take up to seven hours.

c. When the SSD restore is finished, reboot the platform and boot up with the target SSD.

Results

You can now return to your backup environment.

Update BIOS capsule

Prerequisites

Use the following command to ensure that the fwupd and libjcat1 versions are compatible:

```
$ apt list --installed | grep -e fwupd -e libjcat1
```

The fwupd should be v1.7.5 or later, and the libjcat1 should be v0.1.4. If either installed version is lower, use the following command for an Ubuntu OTA update:

```
$ sudo apt update; sudo apt upgrade
```

Steps

1. Download the BIOS capsule file from the Dell Technologies Support Site and save it to the USB disk.
2. Boot to Ubuntu and open the terminal. Enter the following command and press **y** to restart the system after update.

To update with the same version:

```
$ fwupdmgr install <BIOS capsule cab file> --allow-reinstall
```

To update to a newer version:

```
$ fwupdmgr install <BIOS capsule cab file>
```

3. After system restart, provide *<password>* to enter the BIOS setup page.

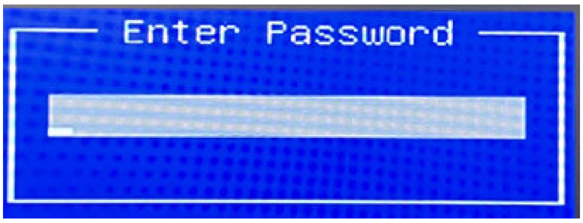
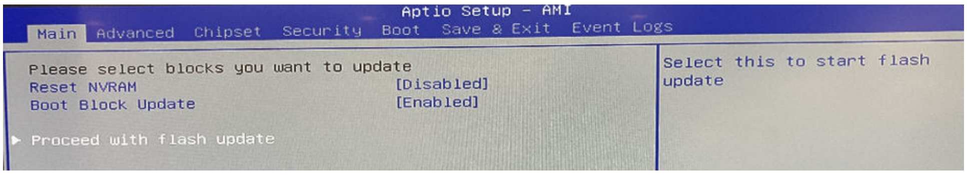


Figure 69. BIOS password prompt

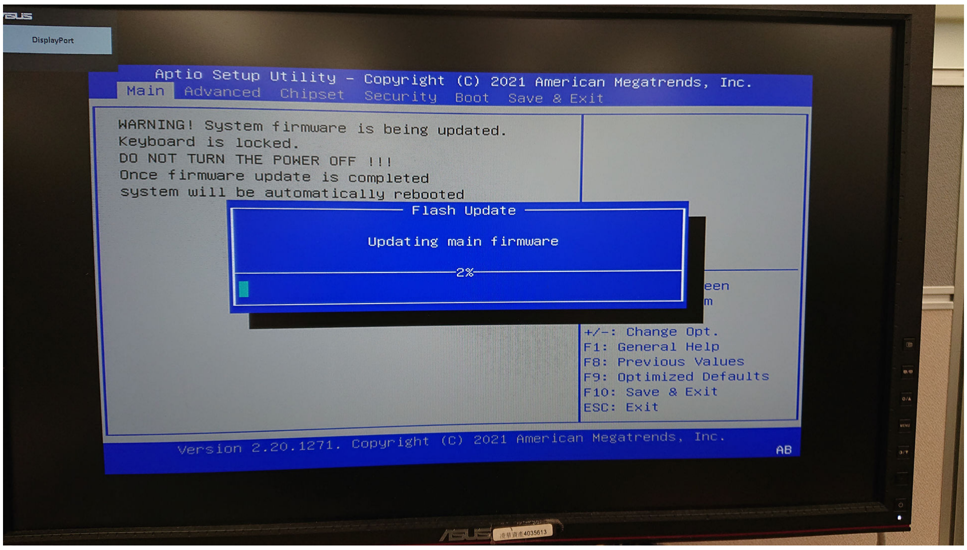
4. Select **Proceed with flash update** item in BIOS **Main** page.



```
Please select blocks you want to update                Select this to start flash
Reset NVRAM                      [Disabled]            update
Boot Block Update                [Enabled]

▸ Proceed with flash update
```

Figure 70. Proceed with flash update

The system starts to install the firmware update, as shown in the following figure:



```
WARNING! System firmware is being updated.
Keyboard is locked.
DO NOT TURN THE POWER OFF !!!
Once firmware update is completed
system will be automatically rebooted

Updating main firmware
2%

+/-: Change Opt.
F1: General Help
F8: Previous Values
F9: Optimized Defaults
F10: Save & Exit
ESC: Exit

Version 2.20.1271. Copyright (C) 2021 American Megatrends, Inc.
```

Figure 71. Firmware update

5. Wait for the update to finish, and then the system BIOS is updated to the version specified.

Update 4G module firmware

Prerequisites

- Update the kernel to 5.15 for driver compatibility.
- Download the driver and tool from the Dell Technologies Support Site.
- Download the firmware from the EM75xx Approved FW Packages site.

About this task

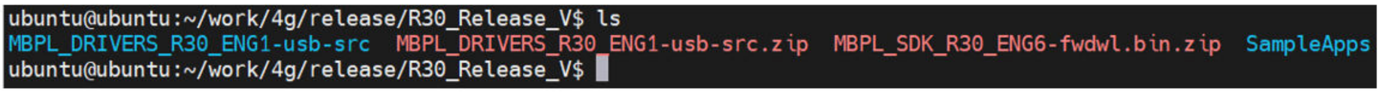
For 4G LTE Sierra Wireless EM7565, hardware version 1.0, the certified version for each carrier is:

- SWI9X50C_01.14.20.00 for AT&T
- SWI9X50C_01.14.07.00 for Verizon

Steps

1. Unzip and copy the package on your platform with the Ubuntu environment:

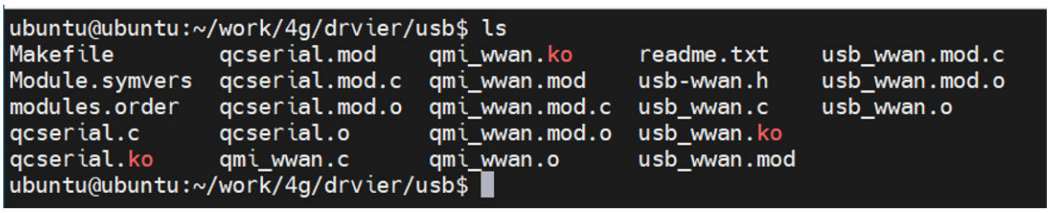
```
$ sudo apt install unzip
$ unzip <firmware>.zip -d <firmware directory>
$ unzip MBPL_DRIVERS_R30_ENG1-usb-src.zip
$ unzip MBPL_SDK_R30_ENG6-fwdwl.bin.zip
```



```
ubuntu@ubuntu:~/work/4g/release/R30_Release_V$ ls
MBPL_DRIVERS_R30_ENG1-usb-src  MBPL_DRIVERS_R30_ENG1-usb-src.zip  MBPL_SDK_R30_ENG6-fwdwl.bin.zip  SampleApps
ubuntu@ubuntu:~/work/4g/release/R30_Release_V$
```

2. Build the driver and install it:

```
$ cd MBPL_DRIVERS_R30_ENG1-usb-src
$ sudo apt install make gcc
$ make clean
$ make
$ openssl req -new -x509 -newkey rsa:2048 -nodes -days 36500 -outform DER -keyout
"MOK.priv" -out "MOK.der" -subj "/CN=$(hostname) module signing key/"
$ kmodsign sha512 MOK.priv MOK.der qcserial.ko
$ kmodsign sha512 MOK.priv MOK.der qmi_wwan.ko
$ kmodsign sha512 MOK.priv MOK.der usb_wwan.ko
```



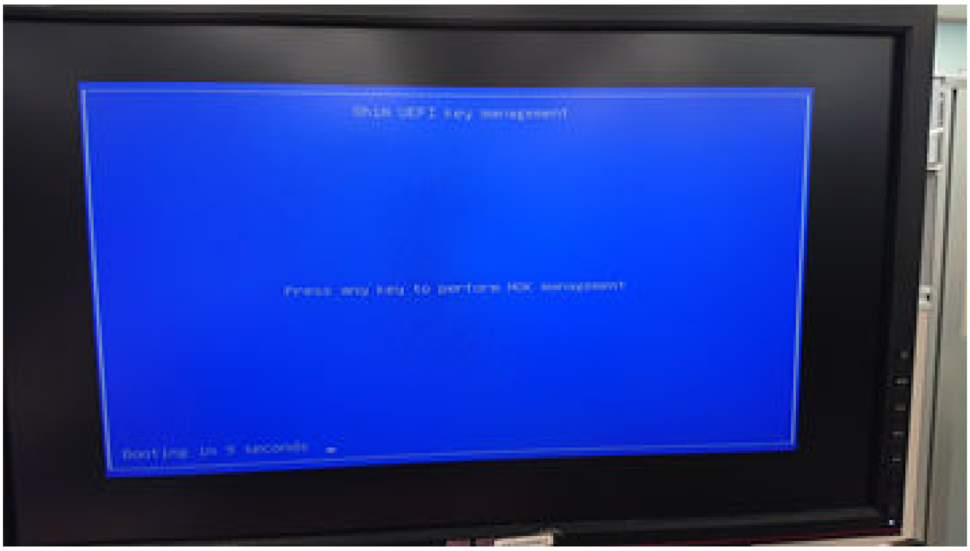
```
ubuntu@ubuntu:~/work/4g/drvier/usb$ ls
Makefile        qcserial.mod    qmi_wwan.ko     readme.txt    usb_wwan.mod.c
Module.symvers  qcserial.mod.c  qmi_wwan.mod    usb-wwan.h    usb_wwan.mod.o
modules.order   qcserial.mod.o  qmi_wwan.mod.c  usb_wwan.c    usb_wwan.o
qcserial.c      qcserial.o      qmi_wwan.mod.o  usb_wwan.ko
qcserial.ko     qmi_wwan.c      qmi_wwan.o      usb_wwan.mod
ubuntu@ubuntu:~/work/4g/drvier/usb$
```

```
$ sudo make install
$ sudo mokutil --import MOK.der
```

Enter a password twice. Make a note of this password, as it will be used during bootup.

```
$ sudo reboot
```

3. Before the BIOS loads GRUB, the device shows a blue screen called **MOK management**. Press any key to continue.



Shim UEFI key management

Press any key to perform MOK management

Booting in 5 seconds

Figure 72. MOK management

4. Select **Enroll MOK** and follow the menus to finish the enrolling process.

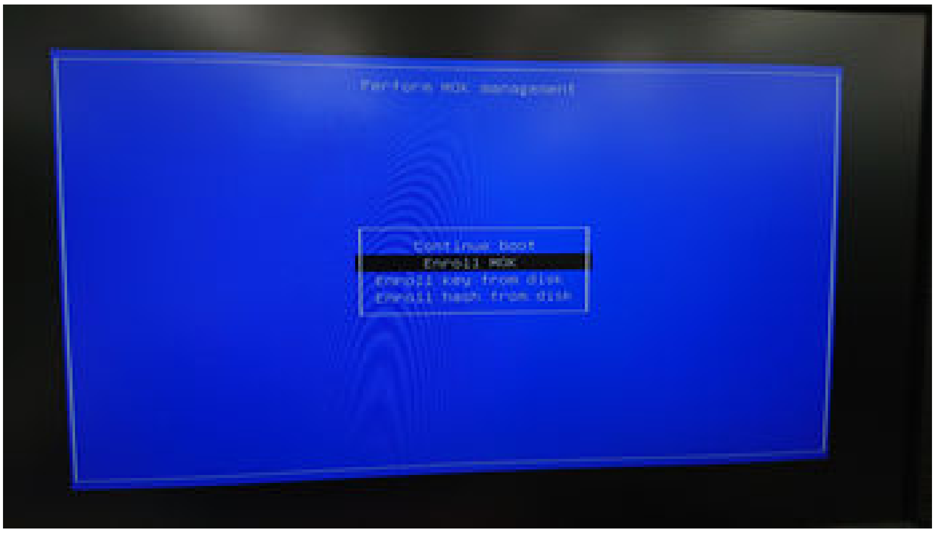


Figure 73. Enroll MOK

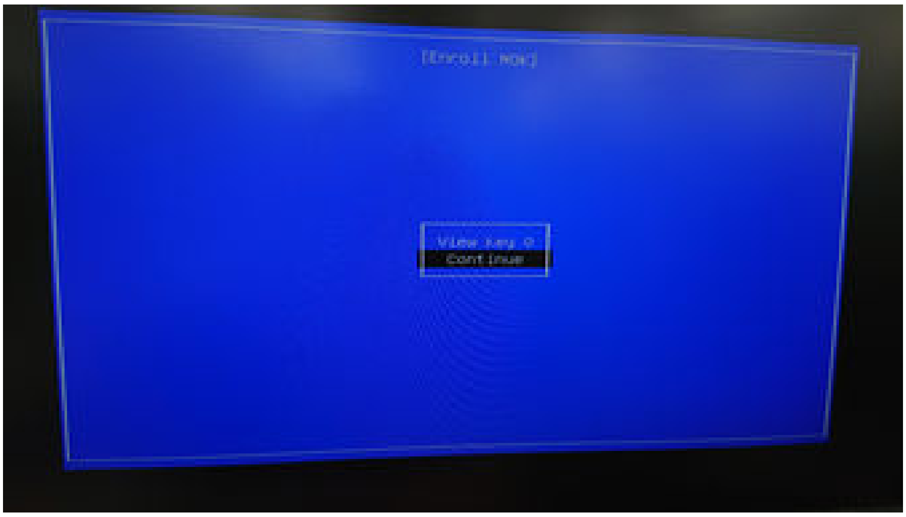


Figure 74. Enroll MOK Continue

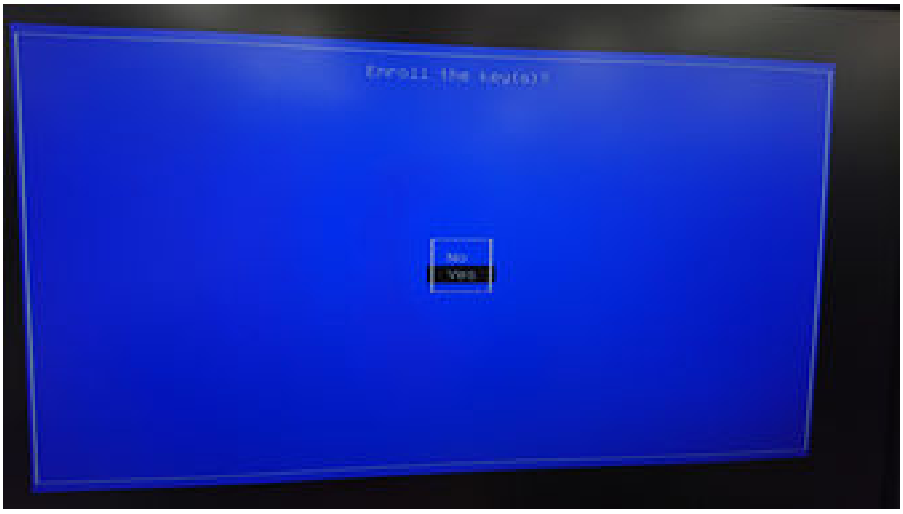


Figure 75. Enroll the keys

5. The MOK Management screen prompts for the password that was provided when running mokutil, and then saves the key. Once complete, reboot again.

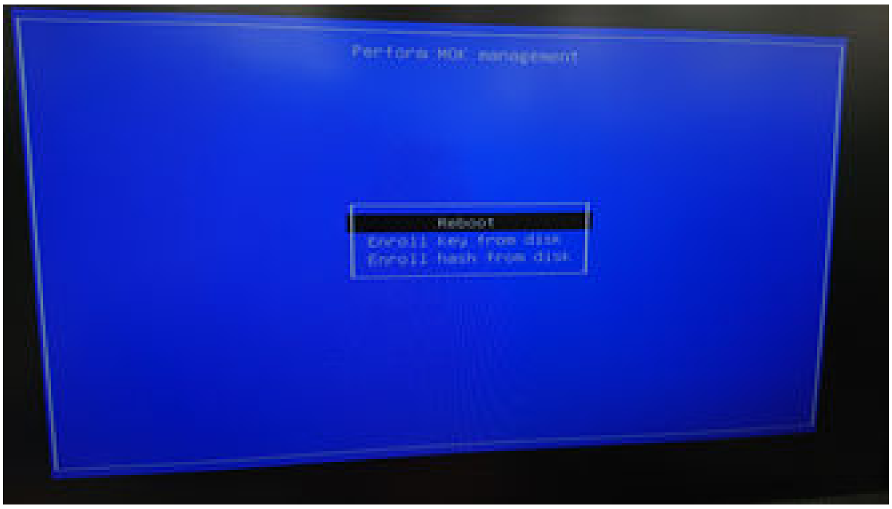
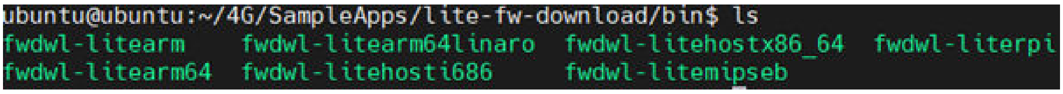


Figure 76. MOK management Reboot

6. Upgrade the firmware:

```
$ sudo systemctl stop ModemManager
$ cd SampleApps/lite-fw-download/bin
```



```
ubuntu@ubuntu:~/4G/SampleApps/lite-fw-download/bin$ ls
fwdwl-litearm    fwdwl-litearm64linaro  fwdwl-litehostx86_64  fwdwl-literpi
fwdwl-litearm64  fwdwl-litehosti686     fwdwl-litemipseb
```

```
# (For Linux kernel 5.13 version, Using R24 driver and R26 tool)
$ sudo ./fwdwl-litehostx86_64 -d /dev/ttyUSB0 -p /dev/cdc-wdm0 -f <firmware
directory> -t 1 -w <firmware>.cwe -n <firmware>.nvu
# (For Linux kernel 5.15 version, Using R30 driver and tool)
$ sudo ./fwdwl-litehostx86_64 -f <firmware directory> -t 1 -w <firmware>.cwe -n
<firmware>.nvu
$ sudo reboot
```

Use `$ sudo mmcli -m <modem number>` to confirm the firmware revision.

Results

A firmware update enables all the bands. For more information, see Disabling bands in Ubuntu after firmware update or SIM card change.

Update 5G module firmware

About this task

For the Telit Centerion (formerly Thales) MV31-W 5G module, hardware version V065, the certified version for each carrier is shown below. Only version 1.0.0.9 has been certified, and cannot be upgraded beyond 1.0.0.9.

- T99W175.F0.1.0.0.9.AT.009 for AT&T
- T99W175.F0.1.0.0.9.VZ.009 for Verizon

Steps

1. Firmware update:
   a. Download the 5G firmware update tool (mbimcli) and firmware (for example, x64-F0.1.0.0.9(AP077).zip) from the Dell Technologies Support Site:

      ⓘ **NOTE:** The firmware is updated on the Dell Technologies Support Site when a new version is available.

   b. Stop the modem manager and untar the mbimcli tool:

      ```
      $ sudo systemctl stop ModemManager
      $ sudo apt-get install unzip
      $ sudo unzip mbimcli.tar.zip
      $ tar Jxvf mbimcli.tar.xz
      ```

   c. Unzip the 5G firmware to your destination path:

      ```
      $ sudo apt-get install unzip
      $ sudo unzip x64-F0.1.0.0.9\(AP077\).zip
      $ sudo cp x64-F0.1.0.0.9\(AP077\)/T99W175.F0.1.0.0.9/ota.bin ./mbimcli/
      ```

   d. Update the 5G firmware:

      ```
      $ cd mbimcli
      $ sudo ./mbimcli -d /dev/cdc-wdm0 --qdu-ota-update=ota.bin
      $ reboot
      ```

2. Install minicom, if not already installed:

   ```
   sudo apt install minicom
   ```

3. Stop the Modem Manager:

   ```
   sudo systemctl stop ModemManager.service
   ```

4. Query the SIM-based firmware switching status with minicom using `at^sbfs?` The following setting determines if the firmware switches automatically based on the network carrier SIM card inserted, or if the user desires to set the network carrier explicitly (for example, AT&T or Verizon).

   SIM based FW switching:

   ```
   at^sbfs=<state>
   ```

   where state=0 (disabled) or 1(enabled).

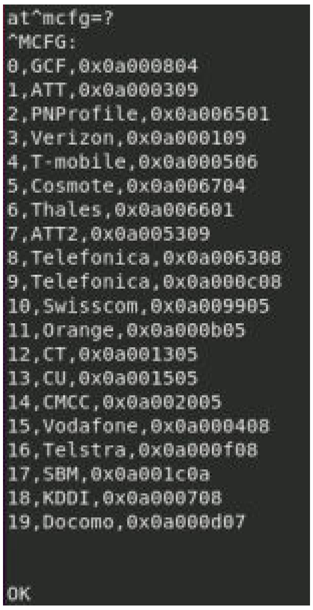
   For example, to enable SIM-based firmware switching:

   `at^sbfs=1` (enable)

`at^sbfs=0` (disable)

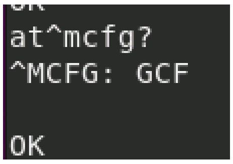
> **NOTE:** Any change to the setting for sbfs state results in an automatic reset of the module. A reset causes the modem to be unresponsive for about 60 seconds.

5. The sbfs setting determines the next steps:
   a. If desired sbfs=1, then skip to Step 9.
   b. If desired sbfs=0, then additional steps are needed to configure the carrier profile in the modem to match that of the SIM card.
6. Query the carrier profiles available in modem using `at^mcfg=?`. Index 0 is the current active profile.



```
at^mcfg=?
^MCFG:
0,GCF,0x0a000804
1,ATT,0x0a000309
2,PNProfile,0x0a006501
3,Verizon,0x0a000109
4,T-mobile,0x0a000506
5,Cosmote,0x0a006704
6,Thales,0x0a006601
7,ATT2,0x0a005309
8,Telefonica,0x0a006308
9,Telefonica,0x0a000c08
10,Swisscom,0x0a009905
11,Orange,0x0a000b05
12,CT,0x0a001305
13,CU,0x0a001505
14,CMCC,0x0a002005
15,Vodafone,0x0a000408
16,Telstra,0x0a000f08
17,SBM,0x0a001c0a
18,KDDI,0x0a000708
19,Docomo,0x0a000d07


OK
```

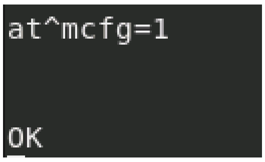
7. Query the current profile with `at^mcfg?`



```
at^mcfg?
^MCFG: GCF

OK
```

8. Set desired profile using `at^mcfg=<Index#>` as shown on the device.

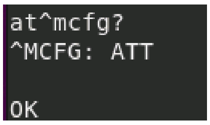
   See the example below to set AT&T profile based on the `at^mcfg=?` from the previous step.



```
at^mcfg=1


OK
```

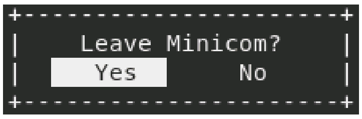
> **NOTE:** Any change to the setting for mcfg profile results in an automatic reset of the module. A reset causes the modem to be unresponsive for about 60 seconds.

9. When the modem returns from reset, query the current profile with `at^mcfg?` to verify the desired setting. If not, verify the sbfs setting again.



```
at^mcfg?
^MCFG: ATT

OK
```

10. Exit minicom using the following key strokes: **`<CTRL-A>`**, **`x`**, **`<ENTER>`**.



```
+----------------------+
|    Leave Minicom?    |
|     Yes       No     |
+----------------------+
```

11. Restart the modem manager:

```
sudo systemctl start ModemManager.service
```

Disabling bands in Ubuntu after firmware update or SIM card change

Disabling bands is required if operating the device within the United States, as well as in other locations. The FCC sets limitations to radiated transmit power (EIRP) that are band-specific. Due to the 4G or 5G module installed, and the antennas provided by Dell Technologies, certain bands must be disabled. As such, additional commands must be sent to the module, under certain conditions outlined below, to meet FCC requirements.

Disabling bands is required:

- After the firmware in the module (4G or 5G) is updated
- After a SIM card change to a different telecom carrier

The following instructions provide information on how to correctly disable bands for the 4G or 5G module used in the EGW-3200.

Disable bands on 4G device in Ubuntu

About this task

Disabling of these bands is required to meet FCC EIRP or other requirements.

Perform the following steps to disable LTE bands b42 and b48 on the 4G module.

Steps

1. Install minicom, if not already installed:

```
sudo apt install minicom
```

2. Stop the modem manager:

```
sudo systemctl stop ModemManager.service
```

3. Open minicom on the com port of the modem:

```
minicom -D /dev/ttyUSB0
```

4. Ensure that the modem is responding to commands. Type **`at`** or **`ati`** to get a response.
5. Enter the following command to change settings on the 4G Sierra modem:

```
at!entercnd="A710"
```

6. Disable LTE bands 42 and 48, as per FCC requirements, by entering the following two commands:

```
at!band=0A,"Disable b42 b48",100600000EC00000,00002500BA0E19DF,0000000000000002
```

```
at!band=0A
```

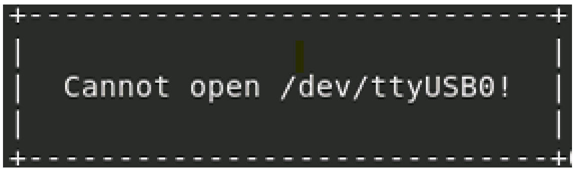
7. Confirm that the bands are disabled:

```
at!band?
```

8. Reset the modem:

```
at!reset
```

NOTE: The modem disappears from minicom for about 60 seconds. Then it reappears and can be communicated with again.

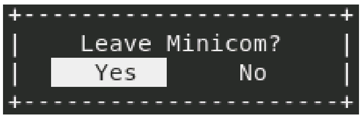


```
+-----------------------------+
|                             |
|   Cannot open /dev/ttyUSB0! |
|                             |
+-----------------------------+
```

9. When the modem returns from reset, confirm that the bands are disabled:

```
at!band?
```

10. Exit minicom using the following key strokes: **<CTRL-A>**, **x**, **<ENTER>**.



```
+----------------------+
|     Leave Minicom?   |
|     Yes        No    |
+----------------------+
```

11. Restart the modem manager:

```
sudo systemctl start ModemManager.service
```

Disable bands on 5G device in Ubuntu

About this task

Disabling of these bands is required to meet FCC EIRP or other requirements.

Perform the following steps to disable LTE bands b30, b42, and b48 on the 5G module.

Steps

1. Install minicom, if not already installed:

```
sudo apt install minicom
```

2. Stop the modem manager:

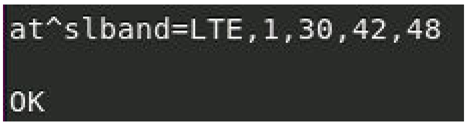
```
sudo systemctl stop ModemManager.service
```

3. Open minicom on the com port of the modem:

```
minicom -D /dev/ttyUSB0
```

4. Ensure that the modem is responding to commands. Type **at** or **ati** to get a response.
5. Disable LTE bands 30, 42, and 48, as per FCC requirements, by entering the following command:

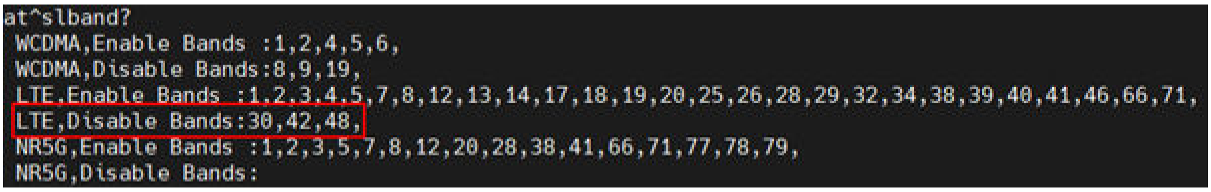
```
at^slband=LTE,1,30,42,48
```



```
at^slband=LTE,1,30,42,48

OK
```

6. Confirm that the bands are disabled:

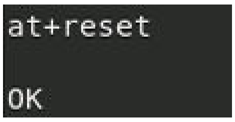
```
at^slband?
```



```
at^slband?
 WCDMA,Enable Bands :1,2,4,5,6,
 WCDMA,Disable Bands:8,9,19,
 LTE,Enable Bands :1,2,3,4,5,7,8,12,13,14,17,18,19,20,25,26,28,29,32,34,38,39,40,41,46,66,71,
 LTE,Disable Bands:30,42,48,
 NR5G,Enable Bands :1,2,3,5,7,8,12,20,28,38,41,66,71,77,78,79,
 NR5G,Disable Bands:
```

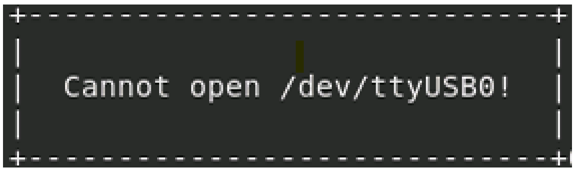
7. To reset the device for new band settings to take effect, run the following command:

```
at+reset
```



```
at+reset

OK
```

NOTE: The modem disappears from minicom for about 60 seconds. Then it reappears and can be communicated with again.

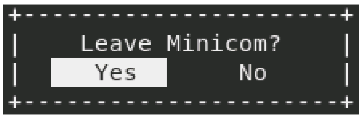


```
+----------------------------+
|                            |
|   Cannot open /dev/ttyUSB0!|
|                            |
+----------------------------+
```

8. Confirm that the bands are disabled:

```
at^slband?
```

9. Exit minicom using the following key strokes: **<CTRL-A>**, **x**, **<ENTER>**.



```
+----------------------+
|    Leave Minicom?    |
|   Yes        No      |
+----------------------+
```

10. Restart the modem manager:

```
sudo systemctl start ModemManager.service
```

Ubuntu 20.04 LTS basic functions

System shutdown and restart

Steps

1. Shutdown command:

```
$ sudo shutdown -h now
```

2. Reboot command:

```
$ sudo shutdown -r now
```

Ubuntu OTA update

About this task

> **NOTE:** Dell Technologies recommends the following OTA update to upgrade to the latest version of the Linux Kernel and drivers for bug fixes and security issues.

OTA update command:

```
$ sudo apt update
$ sudo apt upgrade
```

List installed packages

About this task

List installed packages command:

```
$ apt list --installed
```

Update the system name

About this task

Update system name command:

```
$ sudo nmcli general hostname <NAME>
```

Change the time zone

About this task

Reference the time and date help information with the following command:

```
$ sudo timedatectl --help
```

Root user credential

About this task

Root user credential command:

```
$ sudo su -
```

Create new user

About this task

Add user command:

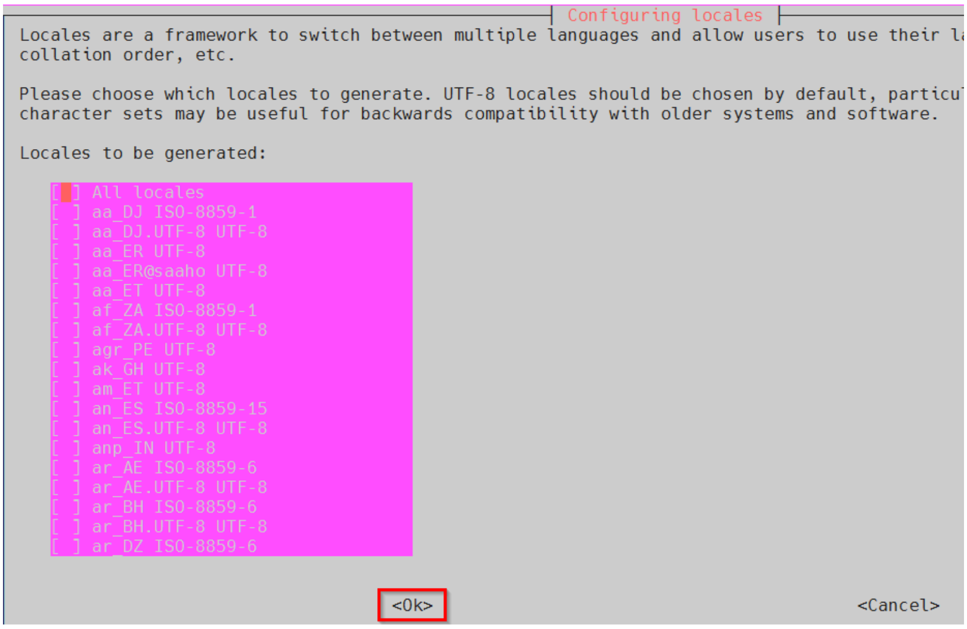
```
$ sudo adduser <USER NAME>
```

Select language

Steps

1. Use the following command to select your preferred language, then select **<Ok>**.

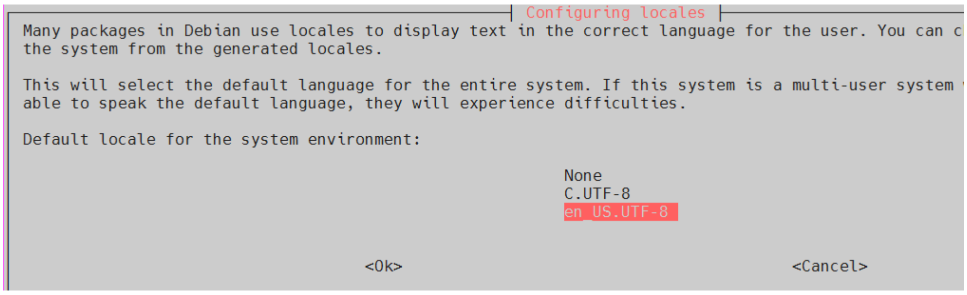
```
$ sudo dpkg-reconfigure locales
```



```
Configuring locales
Locales are a framework to switch between multiple languages and allow users to use their la
collation order, etc.

Please choose which locales to generate. UTF-8 locales should be chosen by default, particu
character sets may be useful for backwards compatibility with older systems and software.

Locales to be generated:

    [ ] All locales
    [ ] aa_DJ ISO-8859-1
    [ ] aa_DJ.UTF-8 UTF-8
    [ ] aa_ER UTF-8
    [ ] aa_ER@saaho UTF-8
    [ ] aa_ET UTF-8
    [ ] af_ZA ISO-8859-1
    [ ] af_ZA.UTF-8 UTF-8
    [ ] agr_PE UTF-8
    [ ] ak_GH UTF-8
    [ ] am_ET UTF-8
    [ ] an_ES ISO-8859-15
    [ ] an_ES.UTF-8 UTF-8
    [ ] anp_IN UTF-8
    [ ] ar_AE ISO-8859-6
    [ ] ar_AE.UTF-8 UTF-8
    [ ] ar_BH ISO-8859-6
    [ ] ar_BH.UTF-8 UTF-8
    [ ] ar_DZ ISO-8859-6

                              <Ok>                                        <Cancel>
```

Figure 77. Configuring locales

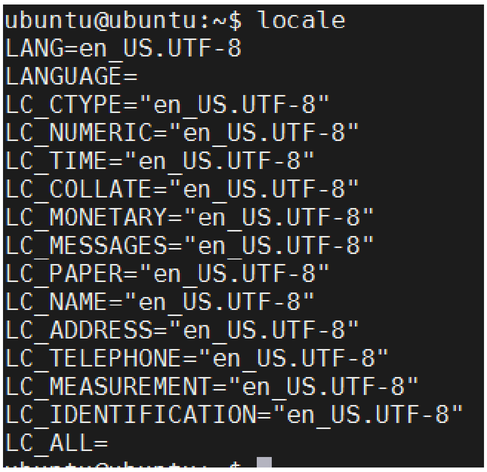
2. Select your target language and select **<Ok>** again.



```
Configuring locales
Many packages in Debian use locales to display text in the correct language for the user. You can c
the system from the generated locales.

This will select the default language for the entire system. If this system is a multi-user system
able to speak the default language, they will experience difficulties.

Default locale for the system environment:

                                             None
                                             C.UTF-8
                                             en_US.UTF-8

                              <Ok>                                    <Cancel>
```

Figure 78. Default locale for system environment

3. Log out and log in, then use the `$ locale` command to confirm your language settings.



```
ubuntu@ubuntu:~$ locale
LANG=en_US.UTF-8
LANGUAGE=
LC_CTYPE="en_US.UTF-8"
LC_NUMERIC="en_US.UTF-8"
LC_TIME="en_US.UTF-8"
LC_COLLATE="en_US.UTF-8"
LC_MONETARY="en_US.UTF-8"
LC_MESSAGES="en_US.UTF-8"
LC_PAPER="en_US.UTF-8"
LC_NAME="en_US.UTF-8"
LC_ADDRESS="en_US.UTF-8"
LC_TELEPHONE="en_US.UTF-8"
LC_MEASUREMENT="en_US.UTF-8"
LC_IDENTIFICATION="en_US.UTF-8"
LC_ALL=
ubuntu@ubuntu:~$
```

Figure 79. Confirm locale

Display

About this task

Acquire screen output from the D-SUB/DVI/DP ports.

USB

About this task

The Ubuntu OS detects USB devices from the six USB ports on the front I/O panel.

Use the `$ dmesg | grep usb` command to check USB devices status.

Configure humidity, pressure, and accelerometer sensors

About this task

Three sensors are ready under the Linux iio interface with specific Linux kernel versions.

The following table is a sample list of seven SKUs with their sensor suite status.

Table 12. SKUs and sensor suite status

ID	Sensor suite	Part number	Humidity/temperature Sensor HDC1010YPAT	Accelerometer Sensor ADXL345BCCZ	Pressure Sensor DPS310
1A	No	XH0YG	No	No	No
2A	Yes	KR44F	Yes	Yes	Yes
3A	Yes	2054J	Yes	Yes	Yes
4A	No	2M7NN	No	No	No
5A	Yes	VT5G6	Yes	Yes	Yes
6A	No	R12R5	No	No	No
7A	Yes	DX1TJ	Yes	Yes	Yes

NOTE: The humidity and pressure sensors require a kernel version 5.13.0-1011-intel or later.

NOTE: The accelerometer sensor requires a kernel version 5.13.0-1014-intel or later.

Steps

1. To upgrade the kernel, use the following command:

```
$ sudo apt update
$ sudo apt upgrade
$ reboot
```

2. After rebooting, use the following command to confirm the kernel version:

```
$ uname -r
```

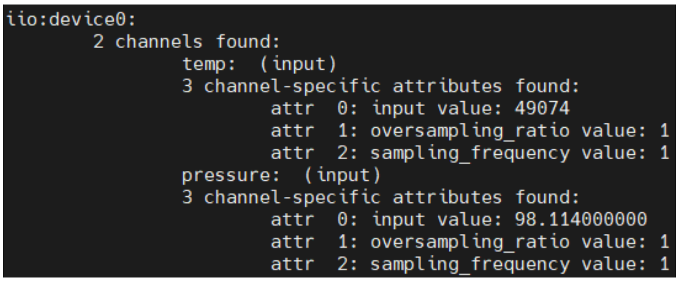
3. Use libiio-utils to fetch sensor data:

```
$ sudo apt install libiio-utils
```

4. Use iio utility commands to fetch sensor data. For example, use the following command:

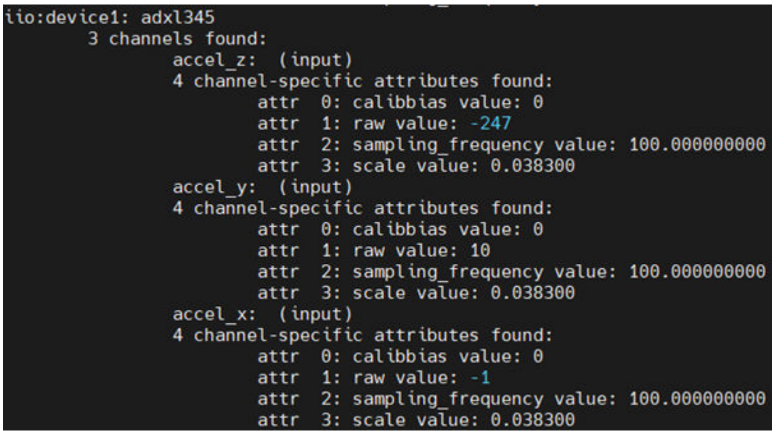
```
$ iio_info
```

Example



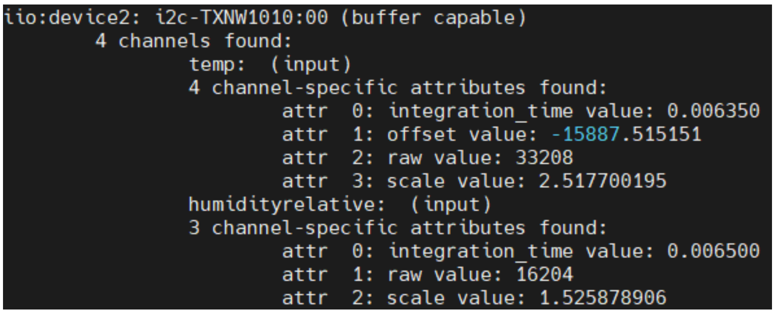
```
iio:device0:
        2 channels found:
                temp:  (input)
                3 channel-specific attributes found:
                        attr  0: input value: 49074
                        attr  1: oversampling_ratio value: 1
                        attr  2: sampling_frequency value: 1
                pressure:  (input)
                3 channel-specific attributes found:
                        attr  0: input value: 98.114000000
                        attr  1: oversampling_ratio value: 1
                        attr  2: sampling_frequency value: 1
```

Figure 80. Pressure sensor example



```
iio:device1: adxl345
        3 channels found:
                accel_z:  (input)
                4 channel-specific attributes found:
                        attr  0: calibbias value: 0
                        attr  1: raw value: -247
                        attr  2: sampling_frequency value: 100.000000000
                        attr  3: scale value: 0.038300
                accel_y:  (input)
                4 channel-specific attributes found:
                        attr  0: calibbias value: 0
                        attr  1: raw value: 10
                        attr  2: sampling_frequency value: 100.000000000
                        attr  3: scale value: 0.038300
                accel_x:  (input)
                4 channel-specific attributes found:
                        attr  0: calibbias value: 0
                        attr  1: raw value: -1
                        attr  2: sampling_frequency value: 100.000000000
                        attr  3: scale value: 0.038300
```

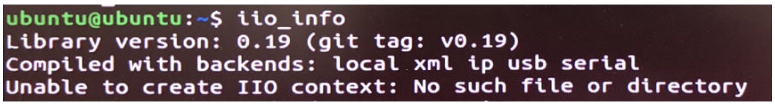
Figure 81. Accelerometer sensor example



```
iio:device2: i2c-TXNW1010:00 (buffer capable)
        4 channels found:
                temp:  (input)
                4 channel-specific attributes found:
                        attr  0: integration_time value: 0.006350
                        attr  1: offset value: -15887.515151
                        attr  2: raw value: 33208
                        attr  3: scale value: 2.517700195
                humidityrelative:  (input)
                3 channel-specific attributes found:
                        attr  0: integration_time value: 0.006500
                        attr  1: raw value: 16204
                        attr  2: scale value: 1.525878906
```

Figure 82. Humidity sensor example

NOTE: In the case of a non-sensor SKU, the iio_info utility output is as shown in the following figure:



```
ubuntu@ubuntu:~$ iio_info
Library version: 0.19 (git tag: v0.19)
Compiled with backends: local xml ip usb serial
Unable to create IIO context: No such file or directory
```

Figure 83. iio_info utility example

Configure Ethernet

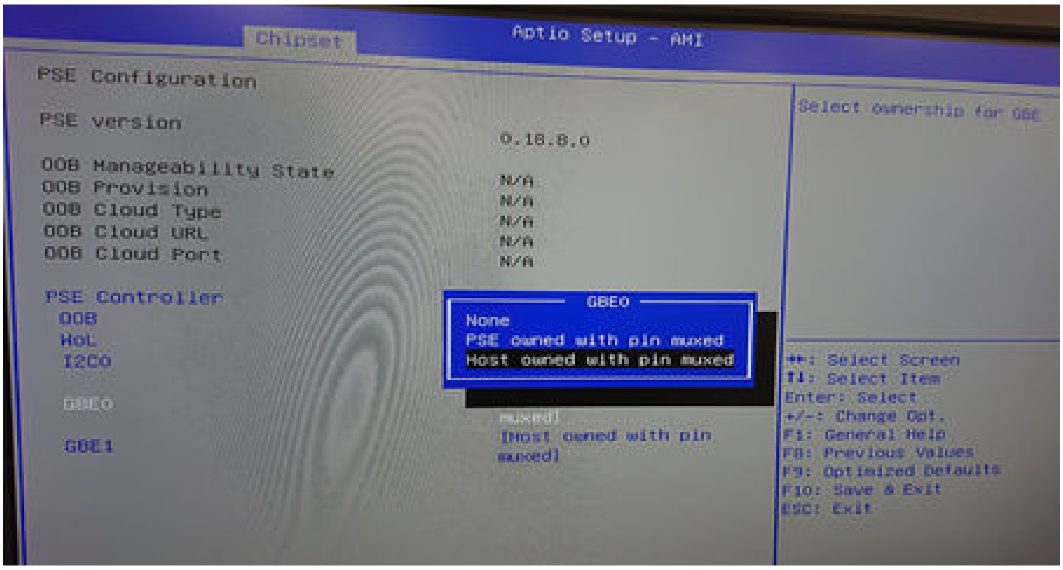
Steps

1. The Ethernet cards function in DHCP client mode by default. Use the `$ip addr` command to confirm.

   NOTE: The Ethernet card names for port1, port2, and port3 are **enp3s0**, **enp0s29f1**, and **enp0s29f2**, respectively.

2. To set up a static IP address, use the following commands:
   a. `nmcli con down <connection name >`
   b. `nmcli con mod <connection name> ipv4.addresses <xx.xx.xx.xx>/24`
   c. `nmcli con mod <connection name> ipv4.gateway <xx.xx.xx.xx>`
   d. `nmcli con mod <connection name> ipv4.dns <xx.xx.xx.xx>`
   e. `nmcli con mod <connection name> ipv4.method manual`
   f. `nmcli con up <connection name>`
3. To roll back to dynamic IP by DHCP, use the following commands:
   a. `nmcli con down <connection name>`
   b. `nmcli con mod <connection name> ipv4.method auto`
   c. `nmcli con up <connection name>`

   NOTE: port2 and port3 ETH PHY LED have different definitions when the ports are assigned to Ubuntu than when they are assigned to Intel PSE. Make this selection under the BIOS menu by clicking **Chipset** > **PSE Configuration** > **GBE0** or **GBE1**. GBE0 is port2 and the GBE1 is port3. When **Host owned with pin muxed** is selected, the port is assigned to Ubuntu.



```
Aptio Setup - AMI
Chipset

PSE Configuration

PSE version                         0.18.8.0

OOB Manageability State             N/A
OOB Provision                       N/A
OOB Cloud Type                      N/A
OOB Cloud URL                       N/A
OOB Cloud Port                      N/A

PSE Controller
 OOB
 HoL
 I2C0

 GBE0                               muxed]

 GBE1                               [Host owned with pin
                                    muxed]

GBE0
None
PSE owned with pin muxed
Host owned with pin muxed
```

Select ownership for GBE

Figure 84. BIOS setting

Table 13. LAN LED behavior for both LAN ports

OS	LAN controller	1 G/100 MbE	1 G/100 MbE	10 MbE	10 MbE
		LED[1]	LED[0]	LED[1]	LED[0]
Ubuntu Linux LED[1]: 0110 LED[0]: 0001	enp0s29f1 and enp0s29f2	Link: solid green No-Link: off	No traffic: solid yellow Traffic: blink yellow	Off	No traffic: solid yellow Traffic: blink yellow
Intel PSE LED[1]: 0011 LED[0]: 0000		Traffic: blink green No traffic: off	No traffic: solid yellow Traffic: blink yellow	Traffic: blink green No traffic: off	Link: solid yellow

NOTE: The Ubuntu Linux LED behavior requires a kernel version 5.13.0-1014-intel or later.

Configure WiFi network

About this task

Use the following commands to connect an AP using a WiFi interface (wlp6s0).

Steps

1. Scan APs:

```
$ nmcli dev wifi list
```

2. Create a connection to the target SSID. If the AP requires a password, add a password parameter:

```
$ sudo nmcli dev wifi connect <SSID>
$ sudo nmcli dev wifi connect <SSID> password "<PASSWORD>"
```

3. To disconnect from the target SSID:

```
$ sudo nmcli con down <SSID>
```

Next steps

Optionally, users can create and delete a WiFi hotspot using the WiFi interface (wlp6s0) by performing the following steps:

1. To create a hotspot connection, use the following nmcli command:

```
$ sudo nmcli dev wifi hotspot ifname <IF NAME> con-name <CONNECTION NAME> ssid <SSID>
password "<PASSWORD>"
```

- IF NAME: wlp6s0 on EGW-3200
- CONNECTION NAME: user-assigned
- SSID: user-assigned name for WiFi client device connection

Then use a WiFi client device to connect SSID with PASSWORD.

2. To delete the hotspot connection, use the following nmcli command:

```
sudo nmcli c delete <CONNECTION NAME>
```

Configure Bluetooth

About this task

Use the following commands to power on Bluetooth and scan target devices.

Steps

1. Enter bluetoothctl mode:

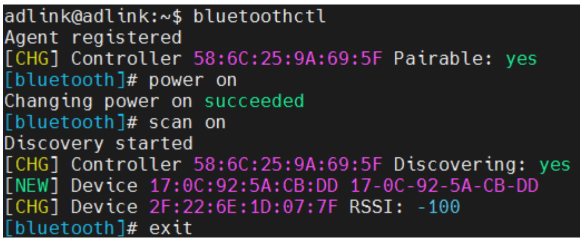
```
$ bluetoothctl
```

2. Power on Bluetooth:

```
$ power on
```

3. Scan Bluetooth devices:

```
$ scan on
```



```
adlink@adlink:~$ bluetoothctl
Agent registered
[CHG] Controller 58:6C:25:9A:69:5F Pairable: yes
[bluetooth]# power on
Changing power on succeeded
[bluetooth]# scan on
Discovery started
[CHG] Controller 58:6C:25:9A:69:5F Discovering: yes
[NEW] Device 17:0C:92:5A:CB:DD 17-0C-92-5A-CB-DD
[CHG] Device 2F:22:6E:1D:07:7F RSSI: -100
[bluetooth]# exit
```

Figure 85. Scan Bluetooth devices

4. Trust target device by MAC address:

```
$ trust <MAC>
```

5. Pair with target device by MAC address:

```
$ pair <MAC>
```

6. Connect target device by MAC address:

```
$ connect <MAC>
```

7. Disconnect target device by MAC address:

```
$ disconnect <MAC>
```

8. Unpair with target device by MAC address:

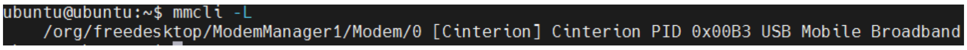
```
$ remove <MAC>
```

Connect 4G or 5G WWAN

Steps

1. Insert your USIM card into the SIM 2 slot. Use the following commands to check the modem status:

```
$ mmcli -L
```

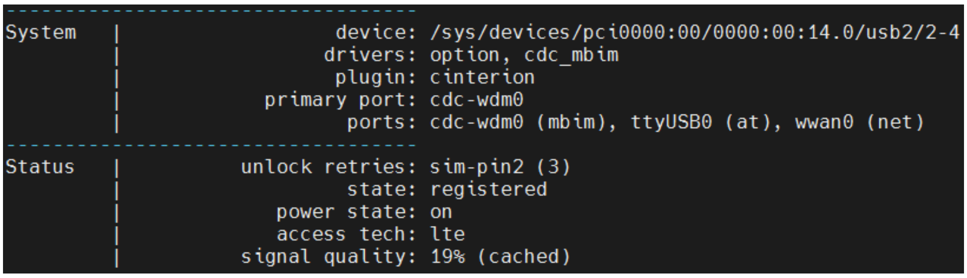


```
ubuntu@ubuntu:~$ mmcli -L
    /org/freedesktop/ModemManager1/Modem/0 [Cinterion] Cinterion PID 0x00B3 USB Mobile Broadband
```

Figure 86. Check modem status

In this example, the modem number is 0.

```
$ mmcli -m 0
```



```
  ----------------------------------
  System    |                 device: /sys/devices/pci0000:00/0000:00:14.0/usb2/2-4
            |                drivers: option, cdc_mbim
            |                 plugin: cinterion
            |           primary port: cdc-wdm0
            |                  ports: cdc-wdm0 (mbim), ttyUSB0 (at), wwan0 (net)
  ----------------------------------
  Status    |         unlock retries: sim-pin2 (3)
            |                  state: registered
            |            power state: on
            |            access tech: lte
            |         signal quality: 19% (cached)
```

Figure 87. Modem 0 status

2. If your USIM card requires a PIN code, the Status is locked. Use the following command to enter your PIN code, change the state to registered, and allow the USIM card to access a cell site.

```
$ sudo mmcli -i <SIM NUMBER> --pin=<PIN CODE>
```

3. Use the following nmcli command to register an auto connection for the target modem and the USIM card:

```
$ sudo nmcli c add type gsm ifname <IF NAME> con-name <CONNECTION NAME> apn <APN NAME>
```

Use the following settings:

- IF NAME: the primary port of the mmcli modem log
- CONNECTION NAME: user-assigned
- APN NAME: must be provided by your USIM card ISP owner

If the Telecom provider is emome:

```
$ sudo nmcli c add type gsm ifname cdc-wdm0 con-name cdc-wdm0 apn emome
```

4. Use the following command to remove auto connection by CONNECTION NAME:

```
$ sudo nmcli c delete <CONNECTION NAME>
```

5. Use the following commands to enable and disable the WWAN service of nmcli:

   Enable:

```
$ nmcli r wwan0 on
```

   Disable:

```
$ nmcli r wwan0 off
```

6. If your USIM card is not detected by the 5G modem module, it may be misaligned with the eSIM slot. Perform the following steps to switch to the physical slot (SIM 2):

   a. Use the following commands:

```
$ sudo apt install minicom
$ sudo systemctl stop ModemManager.service # stop Modem Manager service.
$ sudo minicom -D /dev/ttyUSB0
```

   b. Use the following AT command to switch the SIM slot:

```
AT^SWITCH_SLOT=0
```

   ⓘ **NOTE:** Value 0: physical USIM slot (SIM1); Value 1: physical USIM slot (SIM2).

Identify 4G or 5G module

About this task

There are two ways to identify a 4G or 5G module. Users can either use Minicom, a text-based modem control and terminal emulator program for Unix-like operating systems; or they can use the modem manager command line interface (mmcli). Both are detailed in the following sections.

Use Minicom

About this task

For more information about Minicom, visit the Official Website.

Steps

1. Use the following AT commands with the minicom serial tool:

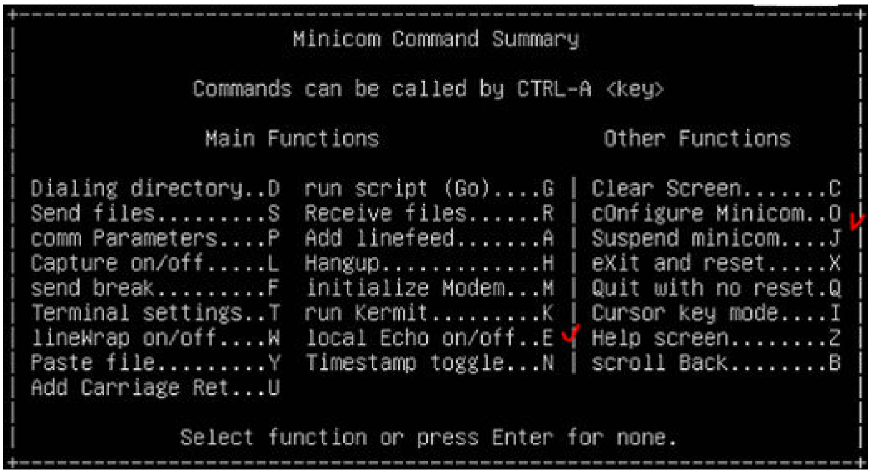
```
$ sudo apt install minicom
$ sudo systemctl stop ModemManager.service # stop Modem Manager service.
$ sudo minicom -D /dev/ttyUSB2
```

   ⓘ **NOTE:** To enable user local echo on minicom, use the following command:

```
$ sudo minicom -D /dev/ttyx      # ttyx is serial device, such as ttyUSB0.
```

   Use one of the following methods:

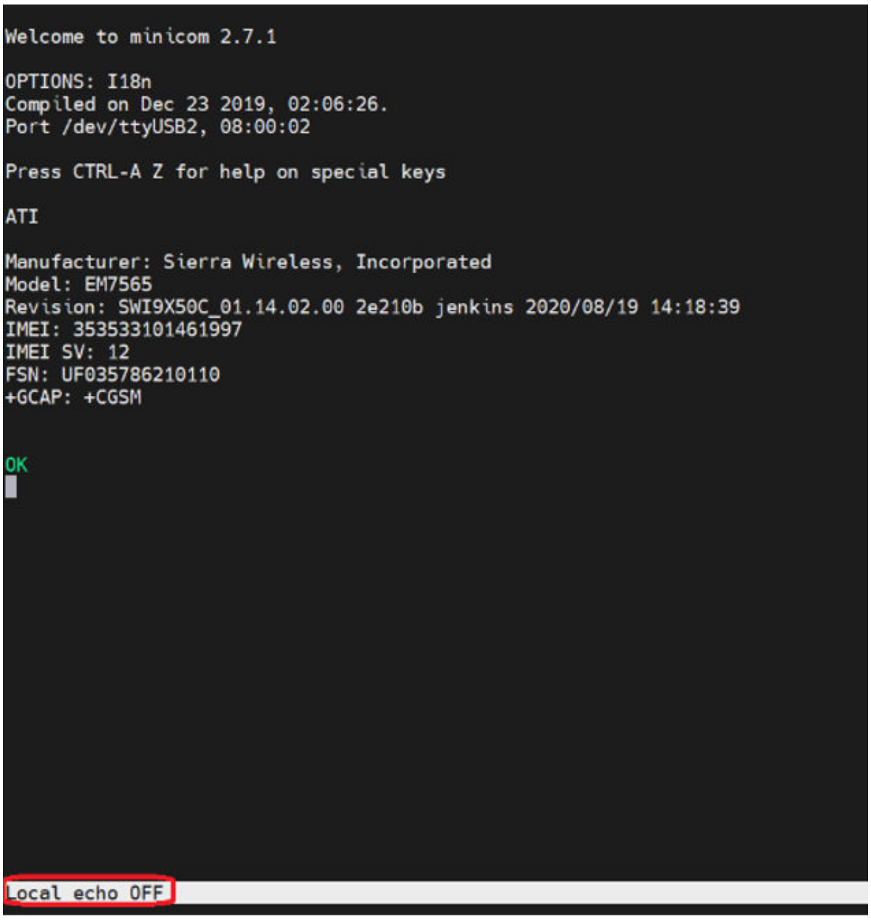
   a. CTRL+A, Z, E //local echo On/Off



```
+-----------------------------------------------------------------------+
|                        Minicom Command Summary                        |
|                                                                       |
|                 Commands can be called by CTRL-A <key>                |
|                                                                       |
|                Main Functions                    Other Functions      |
|                                                                       |
| Dialing directory..D  run script (Go)....G | Clear Screen.......C |
| Send files.........S  Receive files......R | cOnfigure Minicom..O | ✓
| comm Parameters....P  Add linefeed.......A | Suspend minicom....J |
| Capture on/off.....L  Hangup.............H | eXit and reset.....X |
| send break.........F  initialize Modem...M | Quit with no reset.Q |
| Terminal settings..T  run Kermit.........K | Cursor key mode....I |
| lineWrap on/off....W  local Echo on/off..E ✓ Help screen........Z |
| Paste file.........Y  Timestamp toggle...N | scroll Back........B |
| Add Carriage Ret...U                                                  |
|                                                                       |
|              Select function or press Enter for none.                 |
+-----------------------------------------------------------------------+
```

Figure 88. Minicom Command Summary

b. CTRL+A, E // local echo On/Off, directly.



```
Welcome to minicom 2.7.1

OPTIONS: I18n
Compiled on Dec 23 2019, 02:06:26.
Port /dev/ttyUSB2, 08:00:02

Press CTRL-A Z for help on special keys

ATI

Manufacturer: Sierra Wireless, Incorporated
Model: EM7565
Revision: SWI9X50C_01.14.02.00 2e210b jenkins 2020/08/19 14:18:39
IMEI: 353533101461997
IMEI SV: 12
FSN: UF035786210110
+GCAP: +CGSM


OK

Local echo OFF
```

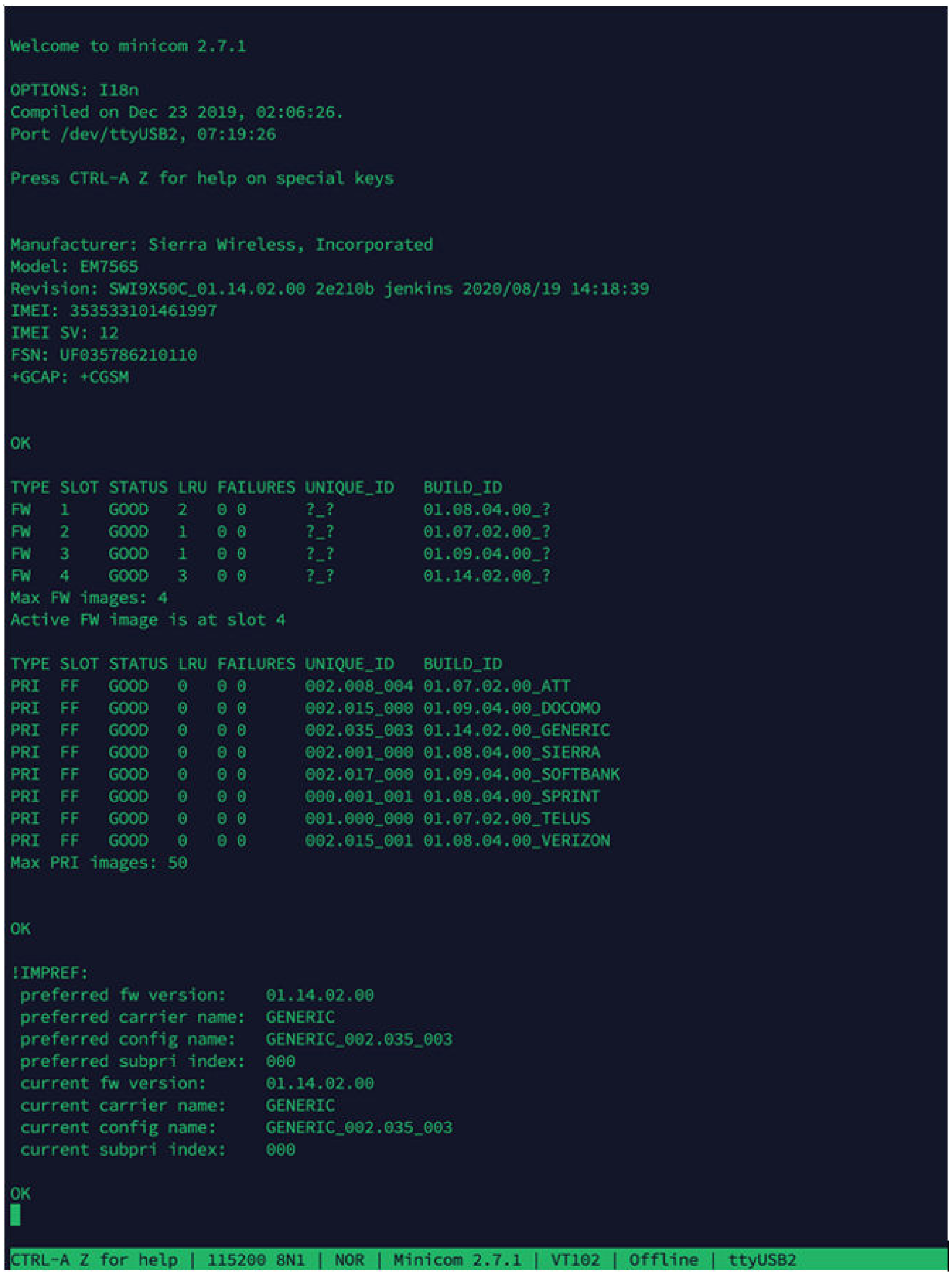
Figure 89. Minicom direct

2. Enter the following AT commands to get module information:
   a. ATI
   b. AT!IMAGE?

      NOTE: This applies to 4G module only.

   c. AT!IMPREF?

      NOTE: This applies to 4G module only.



```
Welcome to minicom 2.7.1

OPTIONS: I18n
Compiled on Dec 23 2019, 02:06:26.
Port /dev/ttyUSB2, 07:19:26

Press CTRL-A Z for help on special keys


Manufacturer: Sierra Wireless, Incorporated
Model: EM7565
Revision: SWI9X50C_01.14.02.00 2e210b jenkins 2020/08/19 14:18:39
IMEI: 353533101461997
IMEI SV: 12
FSN: UF035786210110
+GCAP: +CGSM


OK

TYPE SLOT STATUS LRU FAILURES UNIQUE_ID   BUILD_ID
FW   1    GOOD   2   0 0      ?_?         01.08.04.00_?
FW   2    GOOD   1   0 0      ?_?         01.07.02.00_?
FW   3    GOOD   1   0 0      ?_?         01.09.04.00_?
FW   4    GOOD   3   0 0      ?_?         01.14.02.00_?
Max FW images: 4
Active FW image is at slot 4

TYPE SLOT STATUS LRU FAILURES UNIQUE_ID   BUILD_ID
PRI  FF   GOOD   0   0 0      002.008_004 01.07.02.00_ATT
PRI  FF   GOOD   0   0 0      002.015_000 01.09.04.00_DOCOMO
PRI  FF   GOOD   0   0 0      002.035_003 01.14.02.00_GENERIC
PRI  FF   GOOD   0   0 0      002.001_000 01.08.04.00_SIERRA
PRI  FF   GOOD   0   0 0      002.017_000 01.09.04.00_SOFTBANK
PRI  FF   GOOD   0   0 0      000.001_001 01.08.04.00_SPRINT
PRI  FF   GOOD   0   0 0      001.000_000 01.07.02.00_TELUS
PRI  FF   GOOD   0   0 0      002.015_001 01.08.04.00_VERIZON
Max PRI images: 50


OK

!IMPREF:
 preferred fw version:    01.14.02.00
 preferred carrier name:  GENERIC
 preferred config name:   GENERIC_002.035_003
 preferred subpri index:  000
 current fw version:      01.14.02.00
 current carrier name:    GENERIC
 current config name:     GENERIC_002.035_003
 current subpri index:    000

OK

CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.7.1 | VT102 | Offline | ttyUSB2
```

Figure 90. Module information

3. Exit minicom:

   CTRL+A, X

   ```
   $ sudo systemctl start ModemManager.service # restart Modem Manager service.
   ```

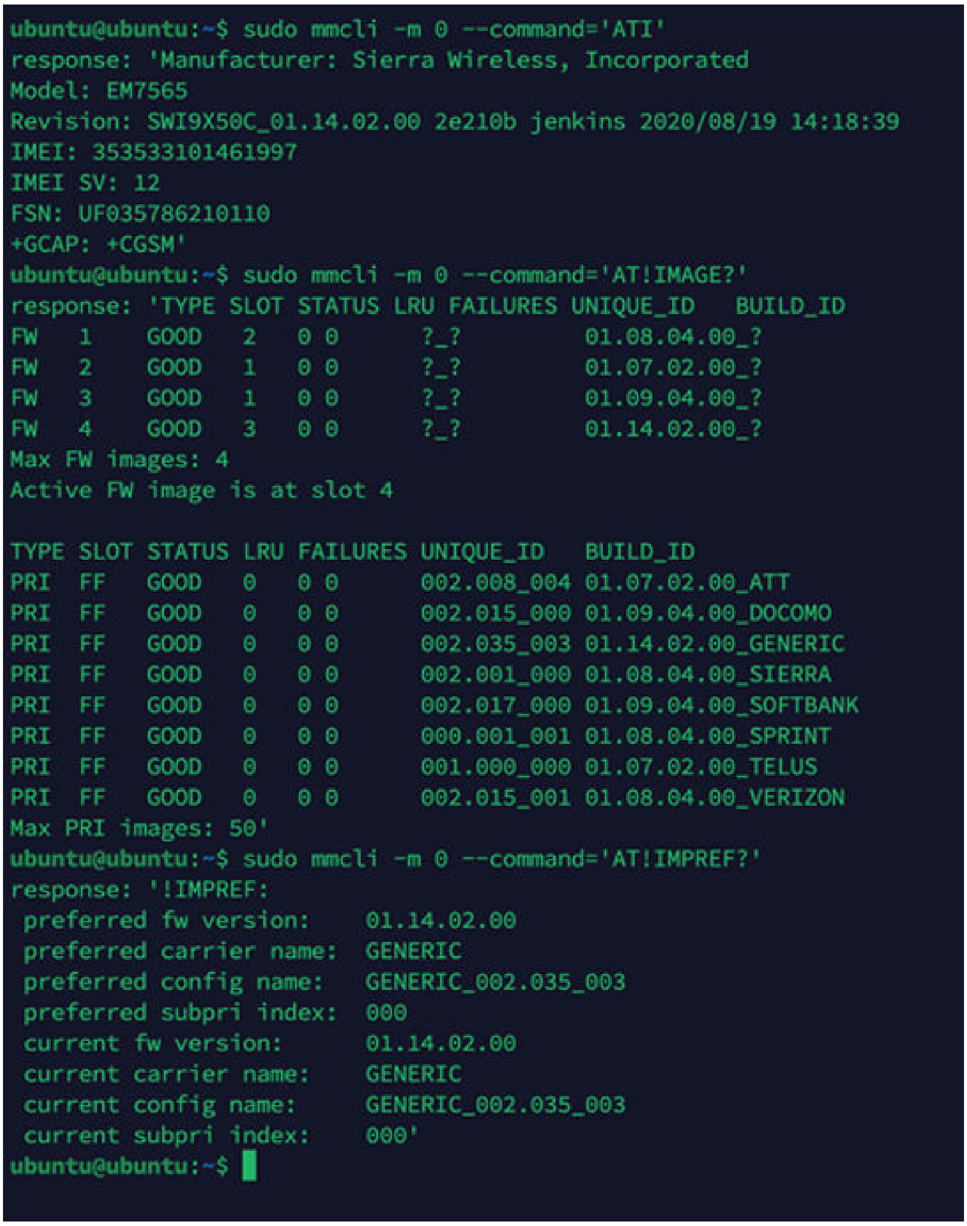
Use mmcli

Steps

Use the following AT commands in the modem manager command line interface (mmcli):

```
$ sudo systemctl stop ModemManager.service # stop Modem Manager service.
$ sudo /usr/sbin/ModemManager - debug  # start Modem manager with debug mode.
#
```

```
# Modem manager is a foreground process now.
# Open another terminal to send AT command to 4G/5G module
#
$ sudo mmcli -m 0 --command='ATI'
$ sudo mmcli -m 0 --command='AT!IMAGE?'  # This is 4G module only.
$ sudo mmcli -m 0 --command='AT!IMPREF?'  # This is 4G module only.
#
# Stop debug mode Modem Manager and restart normal one in service mode.
#
$ sudo killall ModemManager
$ sudo systemctl start ModemManager.service  # restart Modem Manager service.
```



```
ubuntu@ubuntu:~$ sudo mmcli -m 0 --command='ATI'
response: 'Manufacturer: Sierra Wireless, Incorporated
Model: EM7565
Revision: SWI9X50C_01.14.02.00 2e210b jenkins 2020/08/19 14:18:39
IMEI: 353533101461997
IMEI SV: 12
FSN: UF035786210110
+GCAP: +CGSM'
ubuntu@ubuntu:~$ sudo mmcli -m 0 --command='AT!IMAGE?'
response: 'TYPE SLOT STATUS LRU FAILURES UNIQUE_ID   BUILD_ID
FW   1    GOOD   2   0 0      ?_?         01.08.04.00_?
FW   2    GOOD   1   0 0      ?_?         01.07.02.00_?
FW   3    GOOD   1   0 0      ?_?         01.09.04.00_?
FW   4    GOOD   3   0 0      ?_?         01.14.02.00_?
Max FW images: 4
Active FW image is at slot 4

TYPE SLOT STATUS LRU FAILURES UNIQUE_ID   BUILD_ID
PRI  FF   GOOD   0   0 0      002.008_004 01.07.02.00_ATT
PRI  FF   GOOD   0   0 0      002.015_000 01.09.04.00_DOCOMO
PRI  FF   GOOD   0   0 0      002.035_003 01.14.02.00_GENERIC
PRI  FF   GOOD   0   0 0      002.001_000 01.08.04.00_SIERRA
PRI  FF   GOOD   0   0 0      002.017_000 01.09.04.00_SOFTBANK
PRI  FF   GOOD   0   0 0      000.001_001 01.08.04.00_SPRINT
PRI  FF   GOOD   0   0 0      001.000_000 01.07.02.00_TELUS
PRI  FF   GOOD   0   0 0      002.015_001 01.08.04.00_VERIZON
Max PRI images: 50'
ubuntu@ubuntu:~$ sudo mmcli -m 0 --command='AT!IMPREF?'
response: '!IMPREF:
 preferred fw version:    01.14.02.00
 preferred carrier name:  GENERIC
 preferred config name:   GENERIC_002.035_003
 preferred subpri index:  000
 current fw version:      01.14.02.00
 current carrier name:    GENERIC
 current config name:     GENERIC_002.035_003
 current subpri index:    000'
ubuntu@ubuntu:~$
```

Figure 91. Modem manager command line interface

Change 5G SIM slot and connect to the Internet

Prerequisites

This task requires the following utilities:

- Minicom (AT command)

- mmcli (Modem Manager CLI)
- nmcli (Network Manager CLI)

About this task

This example uses the following settings and parameters:

- The SIM slot change is from Slot 1 to Slot 2.
- The 5G module path index is 0 from mmcli -L command.
- The 5G module port names are cdc-wdm0 (mbim), ttyUSB0 (at), and wwan0 (net) from mmcli -m 0 command.
- The connection name is "Far EasTone / KGT Default".
- The APN name is "internet".

Steps

1. Create a connection name if one does not exist in the system:

```
$ sudo nmcli c add type gsm ifname cdc-wdm0 con-name "Far EasTone / KGT Default" apn
internet
```

2. Disconnect the connection:

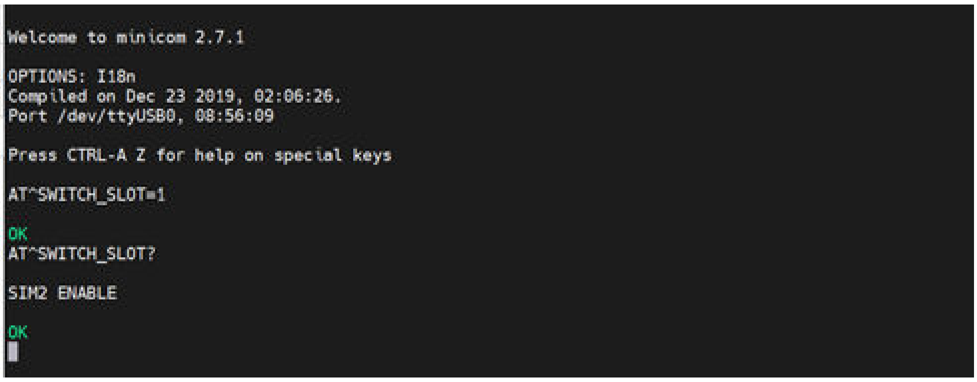
```
$ sudo nmcli radio wwan off
$ sudo mmcli -m 0 --simple-disconnect
```

3. Stop Modem Manager before manual AT command operation:

```
$ sudo systemctl stop ModemManager.service
```

4. Change and confirm the active SIM slot:

```
$ sudo minicom -D /dev/ttyUSB0
AT^SWITCH_SLOT=1    # Switch active sim slot to SIM2
AT^SWITCH_SLOT?     # Get current active SIM slot
```



```
Welcome to minicom 2.7.1

OPTIONS: I18n
Compiled on Dec 23 2019, 02:06:26.
Port /dev/ttyUSB0, 08:56:09

Press CTRL-A Z for help on special keys

AT^SWITCH_SLOT=1

OK
AT^SWITCH_SLOT?

SIM2 ENABLE

OK
```

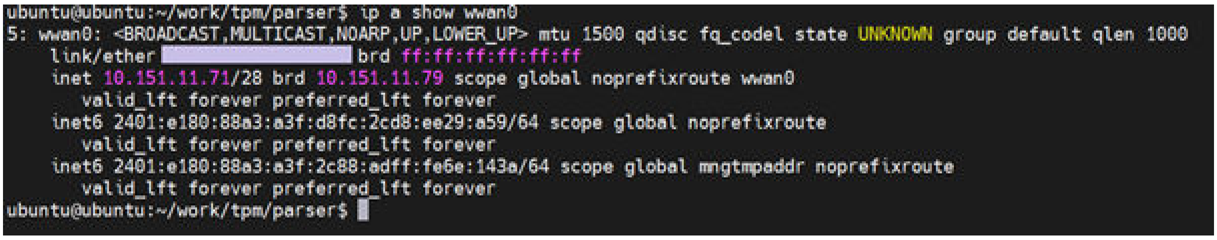
Figure 92. Switch or get SIM slot

5. Exit the Minicom application and restart Modem Manager:

```
$ sudo systemctl start ModemManager.service
$ sudo mmcli -m 0 --simple-connect="apn=internet"
$ sudo nmcli radio wwan on
$ sudo nmcli connection up id "Far EasTone / KGT Default"
```

6. Check the wwan0 status:

```
$ ip a show wwan0
```



```
ubuntu@ubuntu:~/work/tpm/parser$ ip a show wwan0
5: wwan0: <BROADCAST,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
    inet 10.151.11.71/28 brd 10.151.11.79 scope global noprefixroute wwan0
       valid_lft forever preferred_lft forever
    inet6 2401:e180:88a3:a3f:d8fc:2cd8:ee29:a59/64 scope global noprefixroute
       valid_lft forever preferred_lft forever
    inet6 2401:e180:88a3:a3f:2c88:adff:fe6e:143a/64 scope global mngtmpaddr noprefixroute
       valid_lft forever preferred_lft forever
ubuntu@ubuntu:~/work/tpm/parser$ 
```

Figure 93. Show WWAN0

Set up 5G Stand-Alone mode for private networking

Prerequisites

The following instructions require the use of a program to communicate serially over USB with the 5G MV31 module that is installed in the gateway to send AT commands. Linux has a tool called Minicom that provides this functionality. To install Minicom within Ubuntu, use the following command:

```
$ sudo apt -y install minicom
```

About this task

The following information is to assist in setting up the 5G modem (Telit Centerion, formerly Thales MV31-W) installed in the gateway for 5G Stand-Alone (SA) Private Networking operation running Ubuntu OS. 5G Standalone operation means that the modem connects to a 5G Core network.

In order for the modem to connect to a 5G core network, AT commands must be sent to the device to configure it for this operation, as the default settings for the modem are set for NSA (Non Standalone) operation, which is the typical configuration with the public MNOs (Mobile Network Operators). 5G NSA means that the device utilizes a 4G Core network to establish the initial connection for 5G operations.

NOTE: 5G Stand-Alone (SA) mode is not supported for mobile network operators (MNOs) with the MV31-W. It is only supported in private networking usage with the PNProfile. As such, 5G SA cannot be used with carrier networks. In addition, the MV31-W does not support C-band n77 or n48 band in the United States.

Once Minicom is installed, perform the following steps to set up the device in the 5G SA mode of operation for private networking.

Steps

1. Stop the Modem Manager service from the Ubuntu command line, if it is running. This frees up the port for communication with Minicom.

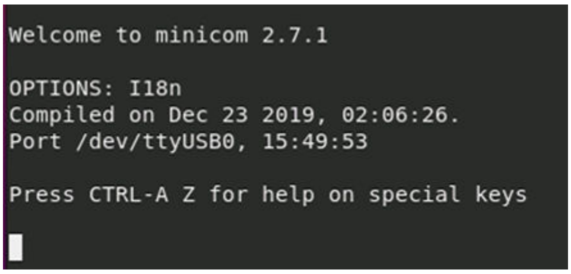
   ```
   $ sudo systemctl stop ModemManager.service
   ```

   NOTE: The device is assumed to be on USB0, but could potentially use a different ttyUSB port.

2. Open the Minicom terminal to communicate with the modem.

   ```
    $ sudo Minicom -D /dev/ttyUSB0
   ```

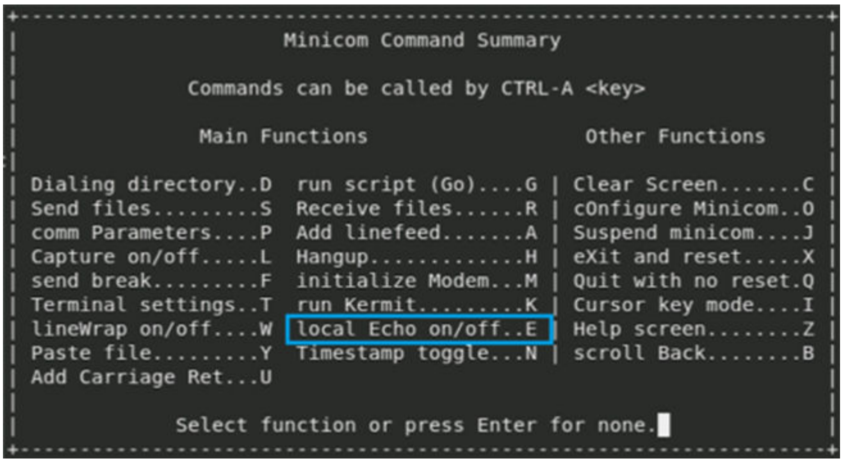
3. Once Minicom loads, the following screen or similar appears.



```
Welcome to minicom 2.7.1

OPTIONS: I18n
Compiled on Dec 23 2019, 02:06:26.
Port /dev/ttyUSB0, 15:49:53

Press CTRL-A Z for help on special keys

█
```

Figure 94. Minicom Welcome screen

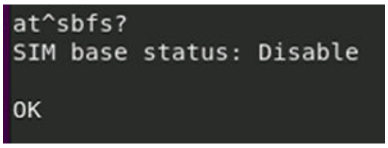
Press **CTRL-A** followed by **z** for options. Common options are to turn on local echo e to see typed commands or to configure serial port o.



```
+-------------------------------------------------------------------+
|                      Minicom Command Summary                      |
|                                                                   |
|              Commands can be called by CTRL-A <key>               |
|                                                                   |
|               Main Functions                  Other Functions    |
|                                                                   |
| Dialing directory..D  run script (Go)....G | Clear Screen.......C |
| Send files.........S  Receive files......R | cOnfigure Minicom..O |
| comm Parameters....P  Add linefeed.......A | Suspend minicom....J |
| Capture on/off.....L  Hangup.............H | eXit and reset.....X |
| send break.........F  initialize Modem...M | Quit with no reset.Q |
| Terminal settings..T  run Kermit.........K | Cursor key mode....I |
| lineWrap on/off....W  local Echo on/off..E | Help screen........Z |
| Paste file.........Y  Timestamp toggle...N | scroll Back........B |
| Add Carriage Ret...U                                              |
|                                                                   |
|             Select function or press Enter for none.█             |
+-------------------------------------------------------------------+
```

Figure 95. Minicom Command Summary

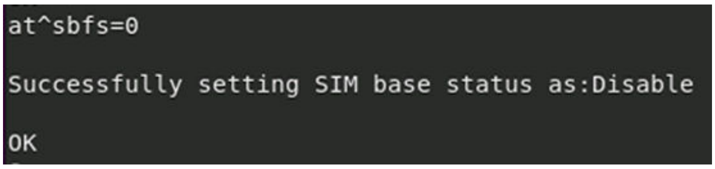
4. Query the sbfs state of the modem by running the `at^sbfs?` command.



```
at^sbfs?
SIM base status: Disable

OK
```

Figure 96. Query sbfs

5. If the modem already has sbfs set to 0 (disabled), go to the next step, otherwise run the `at^sbfs=0` command.



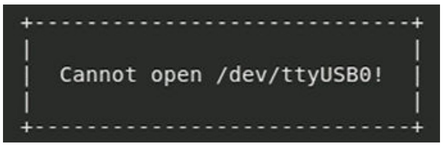
```
at^sbfs=0

Successfully setting SIM base status as:Disable

OK
```

Figure 97. Set SIM base status

NOTE: Changing sbfs causes the device to automatically reset shortly after the **OK** response appears. Module reset may take up to 90 seconds to complete.

This setting disables sbfs. This prevents the firmware from switching automatically based on what SIM card is inserted when using a private networking profile.

The device port disappears for about one minute as the device automatically resets. The Minicom terminal temporarily displays the following message:

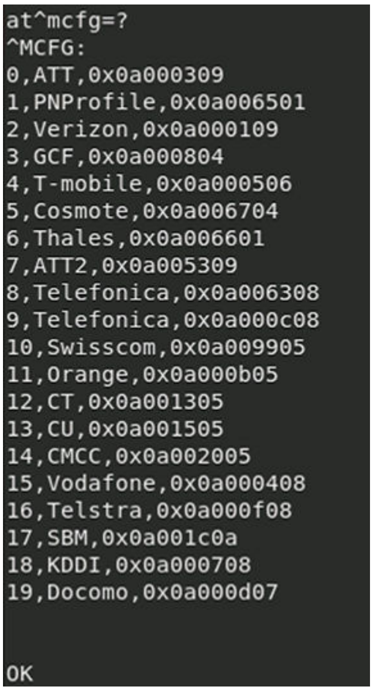


```
+-----------------------------+
|                             |
|  Cannot open /dev/ttyUSB0!  |
|                             |
+-----------------------------+
```

Figure 98. Temporary message

When the modem returns from reset, the message disappears and it is possible to send commands to the modem again.

6. Once sbfs has been disabled and the modem returns from reset, run the `at^mcfg=?` query. This lists all of the carrier profiles available on the modem. The active profile is shown in index 0.



```
at^mcfg=?
^MCFG:
0,ATT,0x0a000309
1,PNProfile,0x0a006501
2,Verizon,0x0a000109
3,GCF,0x0a000804
4,T-mobile,0x0a000506
5,Cosmote,0x0a006704
6,Thales,0x0a006601
7,ATT2,0x0a005309
8,Telefonica,0x0a006308
9,Telefonica,0x0a000c08
10,Swisscom,0x0a009905
11,Orange,0x0a000b05
12,CT,0x0a001305
13,CU,0x0a001505
14,CMCC,0x0a002005
15,Vodafone,0x0a000408
16,Telstra,0x0a000f08
17,SBM,0x0a001c0a
18,KDDI,0x0a000708
19,Docomo,0x0a000d07


OK
```

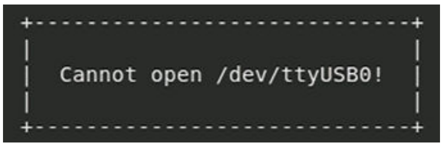
Figure 99. Carrier profiles

ⓘ **NOTE:** It is also possible to run `at^mcfg?` to query the current active profile that is in use.

7. Choose an option: `at^mcfg=`*`<index # for PNProfile>`*. Choose the Private Networking Profile.

   ⓘ **NOTE:** Changing mcfg causes the device to automatically reset shortly after the **OK** response appears. Module reset may take up to 90 seconds to complete.

   The PNProfile is selected (index 1), and after five seconds, the modem responds with **OK**.
   The device port disappears for about one minute as the device automatically resets. The Minicom terminal temporarily displays the following message:

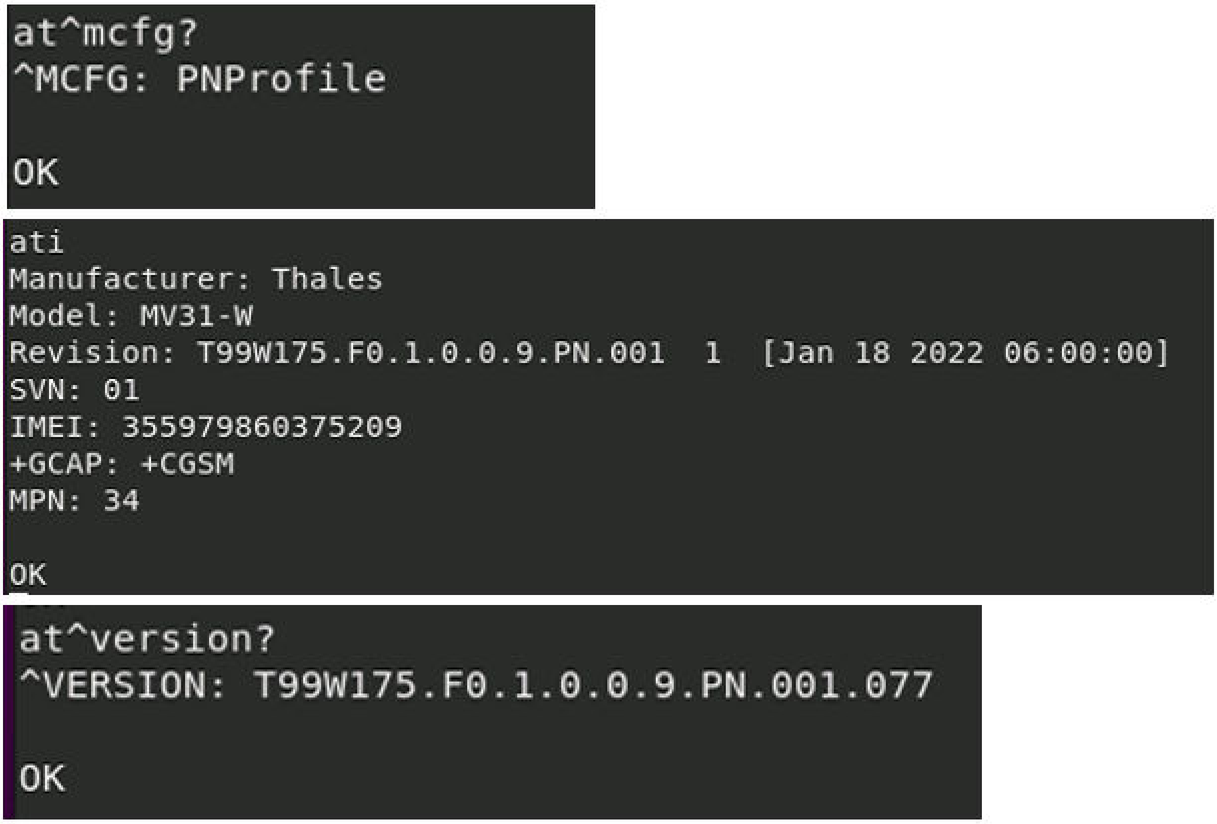


```
+-----------------------------+
|                             |
|  Cannot open /dev/ttyUSB0!  |
|                             |
+-----------------------------+
```

Figure 100. Temporary message

When the modem returns from reset, the message disappears, and it is possible to send commands to the modem again.

8. After the modem returns from reset, run the `at^mcfg?` or `at^version?` command to ensure that the PN profile has been selected. If PN is shown in response for firmware version, then the Private Networking Profile has been selected. The PN profile is the only setting that allows a 5G SA Private Network connection.



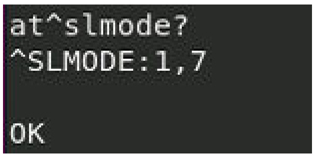
```
at^mcfg?
^MCFG: PNProfile

OK
```

```
ati
Manufacturer: Thales
Model: MV31-W
Revision: T99W175.F0.1.0.0.9.PN.001  1  [Jan 18 2022 06:00:00]
SVN: 01
IMEI: 355979860375209
+GCAP: +CGSM
MPN: 34

OK
```

```
at^version?
^VERSION: T99W175.F0.1.0.0.9.PN.001.077

OK
```

Figure 101. PNProfile, Manufacturer, and Version

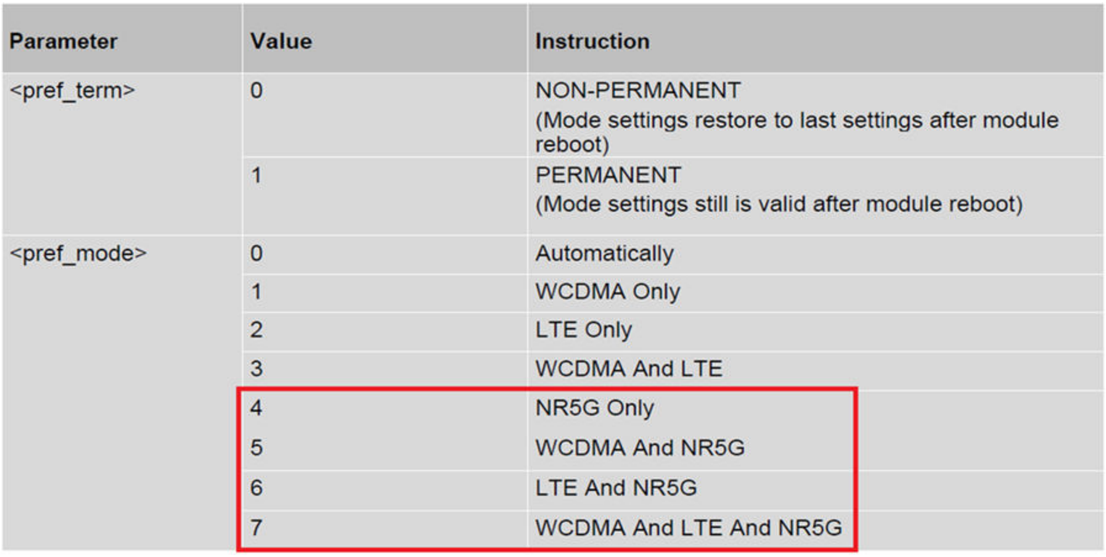
9. Query `at^slmode?`. This ensures the proper mode for 5G operation.



```
at^slmode?
^SLMODE:1,7

OK
```

Figure 102. Query slmode

The default is 1, 7; however, values of 4, 5, or 6 can be used, as long as the value selected for `<pref_mode>` includes NR5G. The `at^slmode?` query returns two values: `<pref_term>` and `<pref_mode>`.

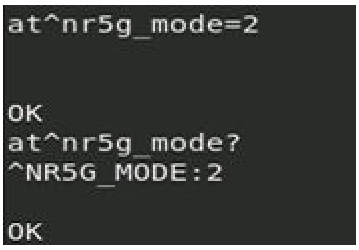


Parameter	Value	Instruction
<pref_term>	0	NON-PERMANENT (Mode settings restore to last settings after module reboot)
	1	PERMANENT (Mode settings still is valid after module reboot)
<pref_mode>	0	Automatically
	1	WCDMA Only
	2	LTE Only
	3	WCDMA And LTE
	4	NR5G Only
	5	WCDMA And NR5G
	6	LTE And NR5G
	7	WCDMA And LTE And NR5G

Figure 103. <pref_mode> values

To set the SLMODE, use `at^slmode=<pref_term >,<pref_mode>`.

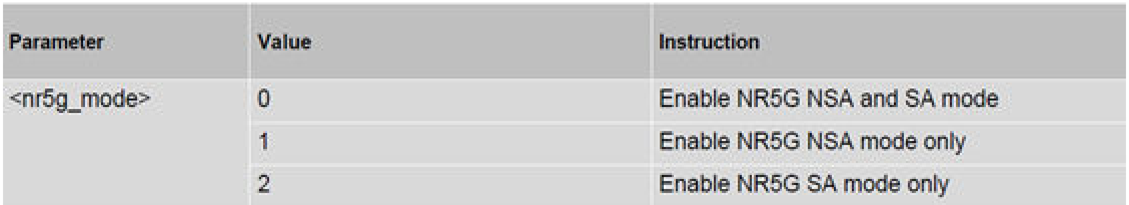
10. Check and/or set the `at^nr5g_mode?`. For private networking, SA only, set `at^nr5g_mode=2`.



```
at^nr5g_mode=2

OK
at^nr5g_mode?
^NR5G_MODE:2

OK
```

Figure 104. Set Private Networking mode

See the following for 5G mode settings.

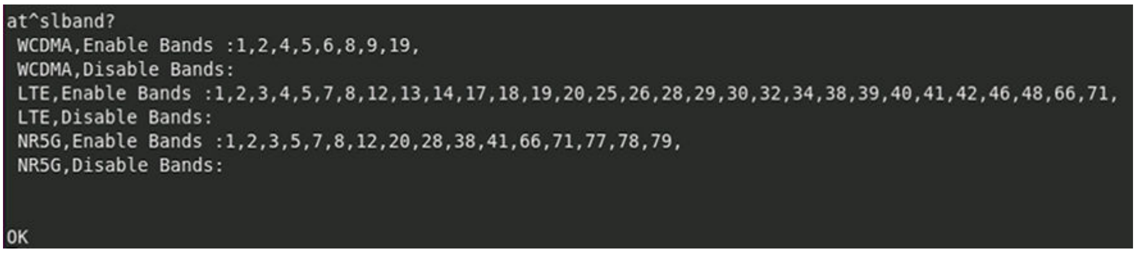


Parameter	Value	Instruction
<nr5g_mode>	0	Enable NR5G NSA and SA mode
	1	Enable NR5G NSA mode only
	2	Enable NR5G SA mode only

Figure 105. 5G mode settings

11. Configure the bands.

Changing to the PNProfile enables all the bands in the hardware. This may not be desirable, as additional bands are not required in the private networking use case and may slow the network search time for attaching the device. After changing to the PNprofile, disable any unnecessary bands for the private networking application. The following figure shows the bands available with `at^slband?` after setting the PNprofile (all bands enabled).



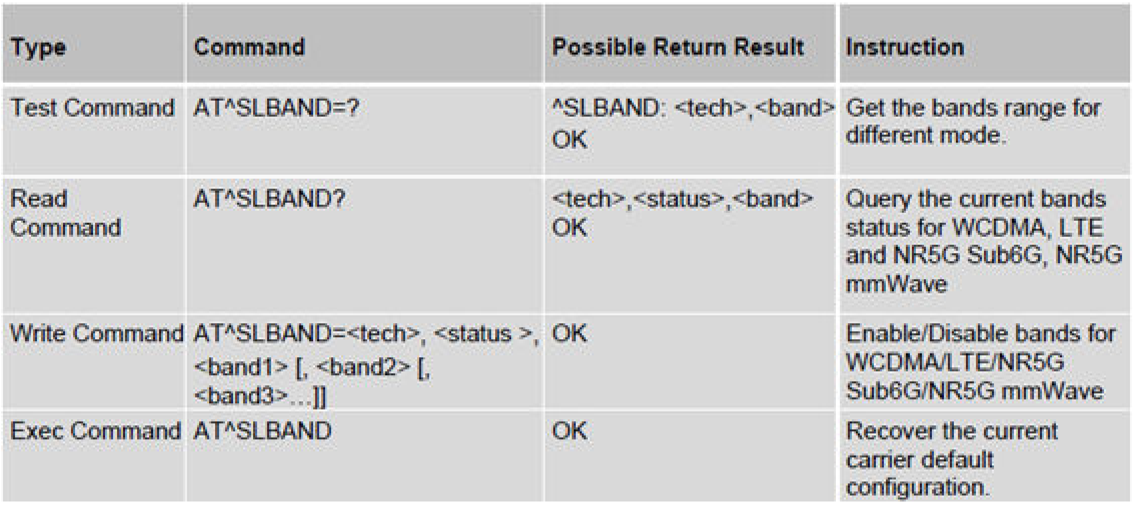
```
at^slband?
 WCDMA,Enable Bands :1,2,4,5,6,8,9,19,
 WCDMA,Disable Bands:
 LTE,Enable Bands :1,2,3,4,5,7,8,12,13,14,17,18,19,20,25,26,28,29,30,32,34,38,39,40,41,42,46,48,66,71,
 LTE,Disable Bands:
 NR5G,Enable Bands :1,2,3,5,7,8,12,20,28,38,41,66,71,77,78,79,
 NR5G,Disable Bands:


OK
```

Figure 106. Available bands

Use the following command to disable any 5G band which is enabled after setting the PNprofile. A value of 1 is used to disable, and 2 for enabling.

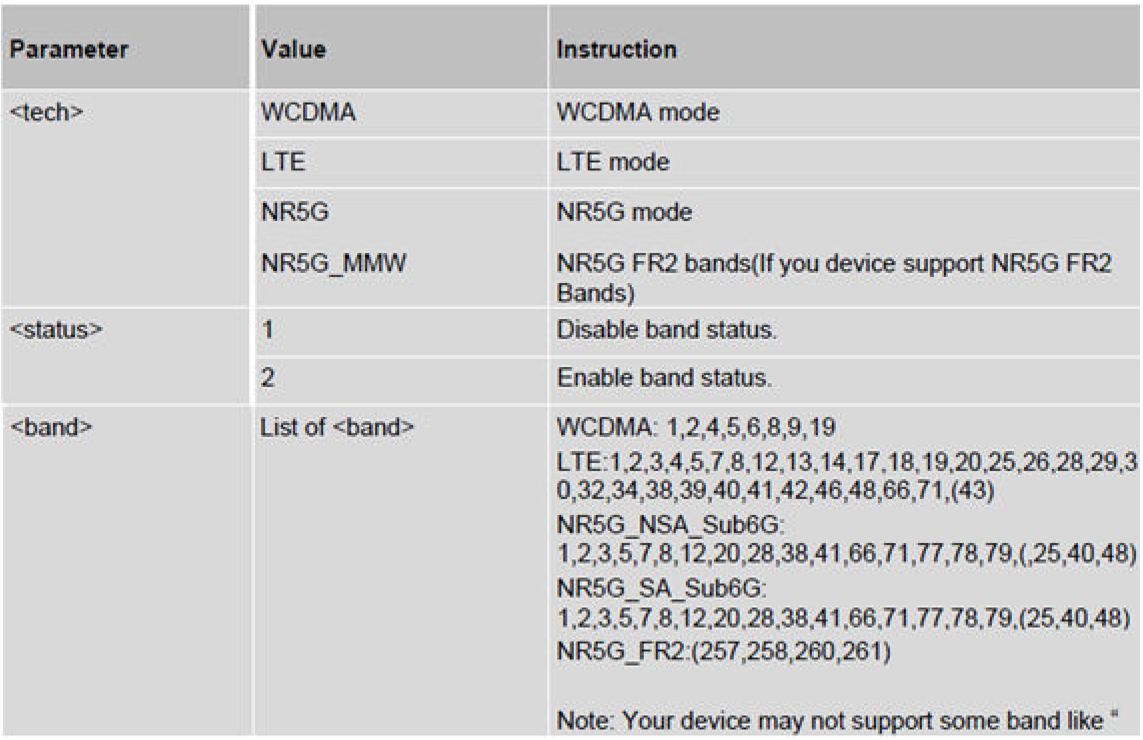
```
at^slband= NR5G, 1,<band1> [, <band2> [,<band3>…]]
```

NOTE: For any new band restrictions to work, the card must be reset by running the `at+reset` command after making changes to the slband settings.



Type	Command	Possible Return Result	Instruction
Test Command	AT^SLBAND=?	^SLBAND: <tech>,<band> OK	Get the bands range for different mode.
Read Command	AT^SLBAND?	<tech>,<status>,<band> OK	Query the current bands status for WCDMA, LTE and NR5G Sub6G, NR5G mmWave
Write Command	AT^SLBAND=<tech>, <status >, <band1> [, <band2> [, <band3>…]]	OK	Enable/Disable bands for WCDMA/LTE/NR5G Sub6G/NR5G mmWave
Exec Command	AT^SLBAND	OK	Recover the current carrier default configuration.

Figure 107. Command syntax

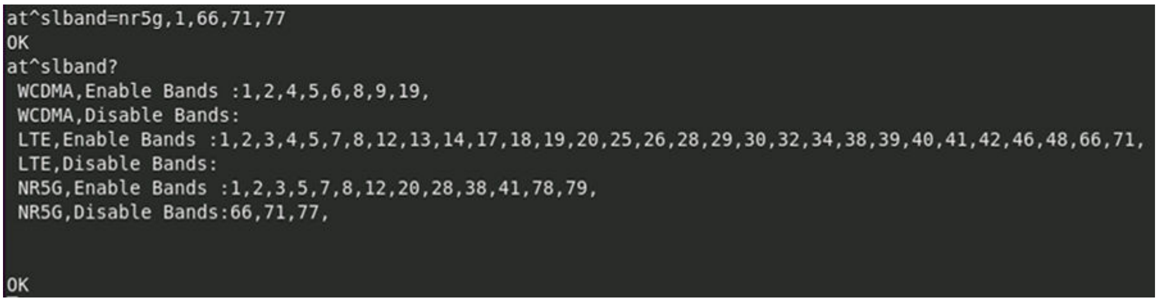


Parameter	Value	Instruction
<tech>	WCDMA	WCDMA mode
	LTE	LTE mode
	NR5G NR5G_MMW	NR5G mode NR5G FR2 bands(If you device support NR5G FR2 Bands)
<status>	1	Disable band status.
	2	Enable band status.
<band>	List of <band>	WCDMA: 1,2,4,5,6,8,9,19 LTE:1,2,3,4,5,7,8,12,13,14,17,18,19,20,25,26,28,29,30,32,34,38,39,40,41,42,46,48,66,71,(43) NR5G_NSA_Sub6G: 1,2,3,5,7,8,12,20,28,38,41,66,71,77,78,79,(,25,40,48) NR5G_SA_Sub6G: 1,2,3,5,7,8,12,20,28,38,41,66,71,77,78,79,(25,40,48) NR5G_FR2:(257,258,260,261) Note: Your device may not support some band like "

Figure 108. Parameters

Example: Disable 5G bands 66, 71, and 77:

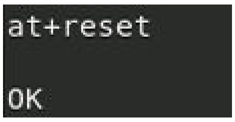
```
at^slband=nr5g,1,66,71,77
```



```
at^slband=nr5g,1,66,71,77
OK
at^slband?
 WCDMA,Enable Bands :1,2,4,5,6,8,9,19,
 WCDMA,Disable Bands:
 LTE,Enable Bands :1,2,3,4,5,7,8,12,13,14,17,18,19,20,25,26,28,29,30,32,34,38,39,40,41,42,46,48,66,71,
 LTE,Disable Bands:
 NR5G,Enable Bands :1,2,3,5,7,8,12,20,28,38,41,78,79,
 NR5G,Disable Bands:66,71,77,


OK
```

Figure 109. Disable bands

Followed by `at+reset` to take effect.

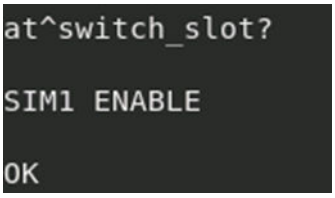


```
at+reset

OK
```

Figure 110. Reset

NOTE: To remove any bands what were disabled and revert any changes to slband, run the `at^slband` command with no arguments and reset the device again.

12. Query the active SIM slot using `at^switch_slot?` and adjust if necessary. The default SIM for the gateway is SIM slot 1, but this can be changed if slot 2 is preferred.



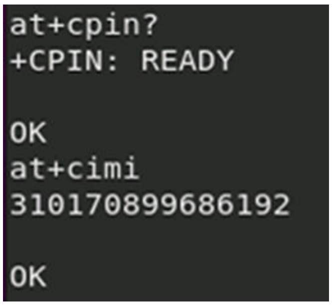
```
at^switch_slot?

SIM1 ENABLE

OK
```

Figure 111. SIM slot selection

The gateway SIM slots are mapped as follows:

- Enable SIM slot 1 = `at^switch_slot=0`
- Enable SIM slot 2 = `at^switch_slot=1`

13. Insert a SIM card in the desired slot (matching that of the previous step) to ensure that the SIM card can be read. Read the SIM using `at+cpin?` or `at+cimi`. The response from the modem should be similar to the following figure, otherwise an error is returned.



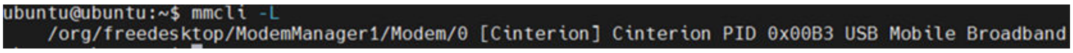
```
at+cpin?
+CPIN: READY

OK
at+cimi
310170899686192

OK
```

Figure 112. Example response from SIM card

14. Once complete with all AT commands, exit Minicom using the following keystrokes in succession: **CTRL-A**, **z**, **x**, **<Enter>**.
15. Restart the Modem Manager service in Ubuntu by running the following command. Modem Manager must be restarted for the device to connect to any network.

```
$ sudo systemctl start ModemManager.service
```

16. Ensure that the SIM card is inserted into the active SIM card slot of the gateway.
17. Ensure that the four WWAN antennas are attached to the appropriate WWAN RF ports of the EGW-3200 (ANT3, ANT4, ANT5, ANT6).
18. Verify connection of the Modem Manager to query the device by running the `mmcli -L` command.

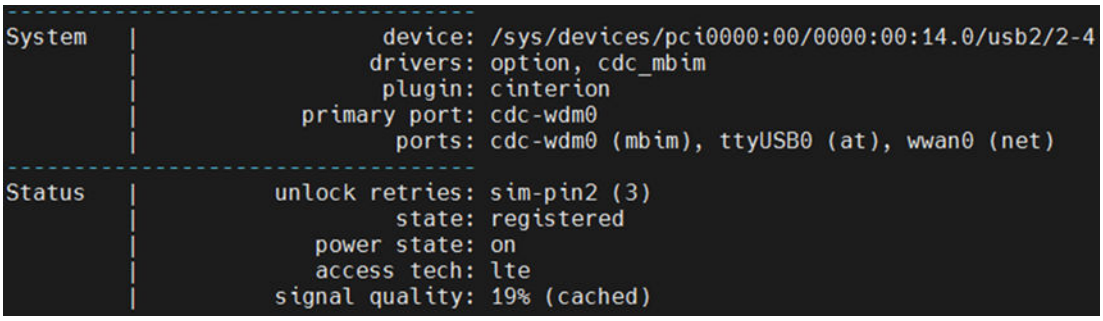


```
ubuntu@ubuntu:~$ mmcli -L
    /org/freedesktop/ModemManager1/Modem/0 [Cinterion] Cinterion PID 0x00B3 USB Mobile Broadband
```

Figure 113. Verify modem connection

NOTE: It may take up to one minute for the modem to appear after issuing this command. Keep reissuing the command until the modem is available.

19. Run the `mmcli -m 0` command to view the details for the Modem Manager service. This example shows the modem on Modem/0.



```
  --------------------------------
  System    |                  device: /sys/devices/pci0000:00/0000:00:14.0/usb2/2-4
            |                 drivers: option, cdc_mbim
            |                  plugin: cinterion
            |            primary port: cdc-wdm0
            |                   ports: cdc-wdm0 (mbim), ttyUSB0 (at), wwan0 (net)
  --------------------------------
  Status    |          unlock retries: sim-pin2 (3)
            |                   state: registered
            |             power state: on
            |             access tech: lte
            |          signal quality: 19% (cached)
```

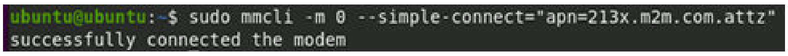
Figure 114. Modem Manager details

NOTE: The status of the modem from `mmcli -L` provides information about the SIM, state of the modem on the network (registered, connected, and so on), as well as the technology and signal quality seen by the device through the WWAN antennas.

20. There are two ways to connect the modem to the network with known APN. Choose one of the following methods:

    a. Use Modem Manager (mmcli) using **Simple Connect** for the APN setting. The APN NAME must be provided in the following format:

    ```
    sudo mmcli -m 0 --simple-connect="apn=<APN NAME>"
    ```

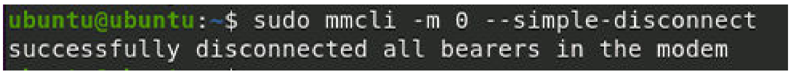
    

    ```
    ubuntu@ubuntu:~$ sudo mmcli -m 0 --simple-connect="apn=213x.m2m.com.attz"
    successfully connected the modem
    ```

    Figure 115. Modem Manager Simple Connect

    To disconnect from the network:

    ```
    sudo mmcli -m 0 --simple-disconnect
    ```

    ```
    ubuntu@ubuntu:~$ sudo mmcli -m 0 --simple-disconnect
    successfully disconnected all bearers in the modem
    ```

    Figure 116. Modem Manager simple disconnect

    b. Use Network Manager (nmcli) commands to register an APN. This only needs to be done once for any given IF NAME, as results are stored in Network Manager.

    ```
    $ sudo nmcli c add type gsm ifname <IF NAME> con-name <CONNECTION NAME> apn <APN
    NAME>
    ```

    - *<IF NAME>* should be the primary port of mmcli modem log (for example, cdc-wdm0). This is shown when the `mmcli -L` command is used, under **System**. See the previous figure.
    - *<CONNECTION NAME>* is a reference to the connection name in Network Manager. This is user-defined and can be any name to identify this network connection.
    - *<APN NAME>* depends on the SIM card that is installed for the private network. Consult your Private Network for the proper APN details.

    Examples:

    Connection Name = myPrivate Network

    APN name = m2m.data.com

    ```
    sudo nmcli c add type gsm ifname cdc-wdm0 con-name myPrivateNetwork apn
    m2m.data.com
    ```

    Once the network connection has been created, the modem can be connected or disconnected from the network using the following two commands in Network Manager:

    - Disconnect from network: `sudo nmcli c down <CONNECTION NAME>`
    - Reconnect to network: `sudo nmcli c up <CONNECTION NAME>`

NOTE: Use this command to remove any network connection: `$ sudo nmcli c delete <CONNECTION NAME>`

21. Confirm connection to the network again using one of the following commands:
    - `mmcli -m 0`
    - Monitor in the terminal window in real time using `mmcli -m 0 -w`.

Access GPS

About this task

There are two ways to access GPS. Users can either use Minicom, a text-based modem control and terminal emulator program for Unix-like operating systems; or they can use the modem manager command line interface (mmcli). Both are detailed in the following sections.

Use Minicom

About this task

For more information about Minicom, visit the Official Website.

Steps

1. Access the modem console (ttyUSB0) using Minicom:

```
$ sudo apt install minicom
$ sudo systemctl stop ModemManager.service # stop Modem Manager service.
$ sudo minicom -D /dev/ttyUSB0
```

2. Enter the following AT commands to enable the GPS function:

```
AT+GPS?
```

Return result of 1 indicates that the modem module supports the GPS function.

```
AT+GPS=1
```

If modem feedback is "GPS is enabled, module reboot", reboot device one and use the `$ sudo minicom -D /dev/ttyUSB0` command a second time.

3. To access TTFF and CN GPS data, use the following AT commands:

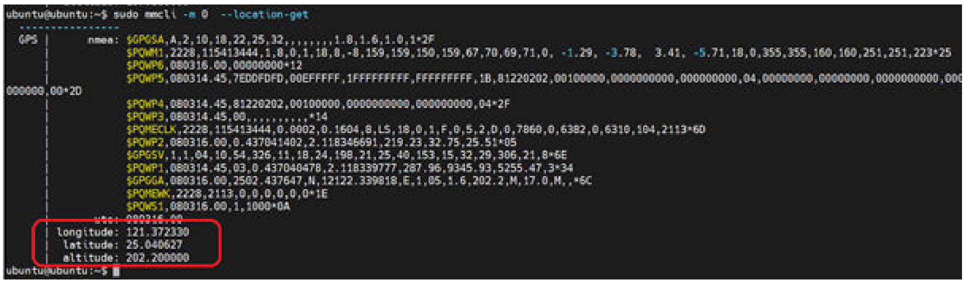
```
AT^GPS_START=0
AT+GPS_INFO
$ sudo systemctl start ModemManager.service # restart Modem Manager service.
```

Use mmcli

Steps

To get GPS location fixing using mmcli, use the following commands:

```
sudo mmcli -m 0 \
              --location-enable-gps-raw \
              --location-enable-gps-nmea
mmcli -m 0 --location-status
$ sudo mmcli -m 0 --location-get
```



```
ubuntu@ubuntu:~$ sudo mmcli -m 0  --location-get
  -----------------
  GPS |       nmea: $GPGSA,A,2,10,18,22,25,32,,,,,,,,1.8,1.6,1.0,1*2F
      |             $PQWM1,2228,115413444,1,8,0,1,18,8,-8,159,159,150,159,67,70,69,71,0, -1.29, -3.78,  3.41, -5.71,18,0,355,355,160,160,251,251,223*25
      |             $PQWP6,080316.00,00000000*12
      |             $PQWP5,080314.45,7EDDFDFD,00EFFFFF,1FFFFFFFFF,FFFFFFFFF,1B,81220202,00100000,0000000000,000000000,04,00000000,00000000,0000000000,000
000000,00*2D
      |             $PQWP4,080314.45,81220202,00100000,0000000000,000000000,04*2F
      |             $PQWP3,080314.45,00,,,,,,,,,,,*14
      |             $PQMECLK,2228,115413444,0.0002,0.1604,8,LS,18,0,1,F,0,5,2,D,0,7860,0,6382,0,6310,104,2113*6D
      |             $PQWP2,080316.00,0.437041402,2.118346691,219.23,32.75,25.51*05
      |             $GPGSV,1,1,04,10,54,326,11,18,24,198,21,25,40,153,15,32,29,306,21,8*6E
      |             $PQWP1,080314.45,03,0.437040478,2.118339777,287.96,9345.93,5255.47,3*34
      |             $GPGGA,080316.00,2502.437647,N,12122.339818,E,1,05,1.6,202.2,M,17.0,M,,*6C
      |             $PQMEWK,2228,2113,0,0,0,0,0,0,0*1E
      |             $PQWS1,080316.00,1,1000*0A
      |        utc: 080316.00
      |  longitude: 121.372330
      |   latitude: 25.040627
      |   altitude: 202.200000
ubuntu@ubuntu:~$ 
```

Figure 117. GPS location fixing

Remote login

About this task

The SSH server runs by default on port 22. Use your PC/NB to open a SSH connection (using terminal tools such as PuTTY or MobaXterm) to the EGW-3200. The PC/NB and EGW-3200 share a network connection under a local network.

Set up audio and microphone

Steps

1. Install ALSA utilities:

   ```
   $ sudo apt install alsa-utils
   ```

2. Adjust audio and microphone volume by alsamixer:

   ```
   $ alsamixer
   ```

3. Prepare an audio .wav file and connect to the speaker on the device:

   ```
   $ aplay xxx.wav
   ```

4. Connect to the microphone on the device and start to record audio after entering the following command. Use **ctrl + c** to stop the recording.

   ```
   $ arecord xxx.wav
   ```

5. To replay the .wav file recording:

   ```
   $ aplay xxx.wav
   ```

SSD security-erase

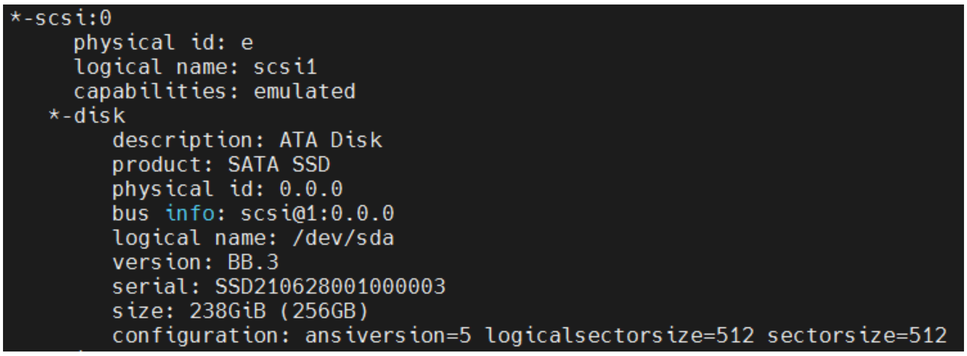
About this task

⚠ CAUTION: **Performing this task will permanently swipe the disk content.**

Steps

1. Check out your target disk to be mounted as /dev/sdx:

   ```
   $ sudo lshw
   ```

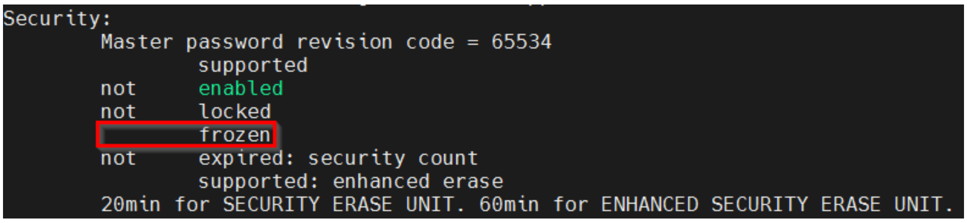


```
*-scsi:0
     physical id: e
     logical name: scsi1
     capabilities: emulated
   *-disk
        description: ATA Disk
        product: SATA SSD
        physical id: 0.0.0
        bus info: scsi@1:0.0.0
        logical name: /dev/sda
        version: BB.3
        serial: SSD210628001000003
        size: 238GiB (256GB)
        configuration: ansiversion=5 logicalsectorsize=512 sectorsize=512
```

Figure 118. $ sudo lshw

2. Confirm that the target disk is not frozen. To check:

```
$ sudo hdparm -I /dev/sdx
```



```
Security:
        Master password revision code = 65534
                supported
        not     enabled
        not     locked
                frozen
        not     expired: security count
                supported: enhanced erase
        20min for SECURITY ERASE UNIT. 60min for ENHANCED SECURITY ERASE UNIT.
```

Figure 119. Example: target disk is frozen

If the target disk is frozen,

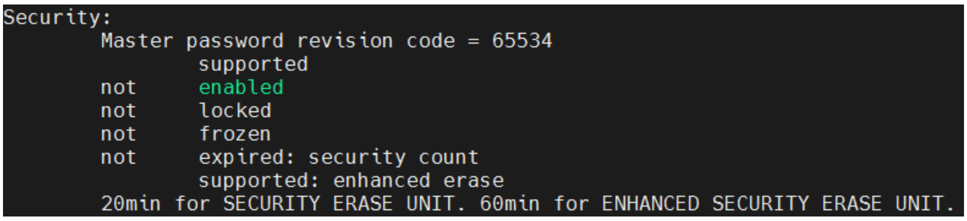
a. Use the following commands to enter the system into standby mode:

```
$ sudo su -
$ echo -n mem > /sys/power/state
```

The power button LED blinks when the system is in standby mode.

b. Press the power button once to wake up the system.

c. Use the `hdparm` command a second time, and status is now “not frozen”, as shown in the following figure:

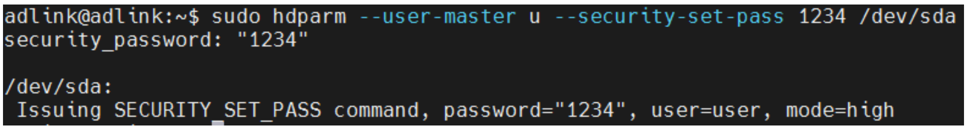


```
Security:
        Master password revision code = 65534
                supported
        not     enabled
        not     locked
        not     frozen
        not     expired: security count
                supported: enhanced erase
        20min for SECURITY ERASE UNIT. 60min for ENHANCED SECURITY ERASE UNIT.
```

Figure 120. Disk not frozen

3. Set up a security password before executing the security-erase:

```
$ sudo hdparm --user-master u --security-set-pass <password> /dev/sdx
```

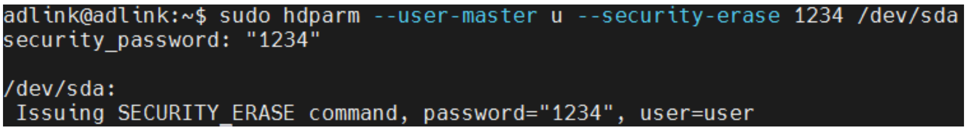


```
adlink@adlink:~$ sudo hdparm --user-master u --security-set-pass 1234 /dev/sda
security_password: "1234"

/dev/sda:
 Issuing SECURITY_SET_PASS command, password="1234", user=user, mode=high
```

Figure 121. Set security password

4. Run the security-erase command with the password:

```
$ sudo hdparm --user-master u --security-erase <password> /dev/sdx
```



```
adlink@adlink:~$ sudo hdparm --user-master u --security-erase 1234 /dev/sda
security_password: "1234"

/dev/sda:
 Issuing SECURITY_ERASE command, password="1234", user=user
```

Figure 122. Security erase

Results

When the security-erase is finished, all data on the /dev/sdx disk is swiped (0x00).

Get system current and voltage

Steps

1. Download the **Read_Voltage_and_Current.zip** file from the Dell Technologies Support Site and unzip it to a local folder location.
2. Run the following commands:

```
chmod a+x [current_voltage_script]
sudo ./[current_voltage_script]     # get current and voltage with root privileges.
```

Connect to the serial port

Steps

1. Connect suitable DB9 cables to the device COM ports.
   - Map COM1 port to /dev/ttyS0.
   - Map COM2 port to /dev/ttyS1.
2. Set the control mode as RS232/RS422/RS485 from the BIOS menu. Map the pins according to the following table:

Table 14. DB9 connector pin definitions

Pin	Signal name		
	RS-232	**RS-422**	**RS-485**
1	DCD	TXD422–	485DATA–
2	RXD	TXD422+	485DATA+
3	TXD	RXD422+	N/S
4	DTR	RXD422-	N/S
5	GND	N/S	N/S
6	DSR	N/S	N/S
7	RTS	N/S	N/S
8	CTS	N/S	N/S
9	RI	N/S	N/S

3. Execute the following command on two systems, where # is the port number corresponding to the port being used:

```
$ sudo chmod 777 /dev/ttyS#
```

4. To test COM port loopback, use the following commands.
   a. Data receive command:

   ```
   $ cat < /dev/ttyS#
   ```

   b. Data transmit command:

   ```
   $ echo "test" > /dev/ttyS#
   ```

NOTE: The port number (`#`) must be different between data receive and data transmit.

Connect to the Canbus

Steps

1. Install the tool:

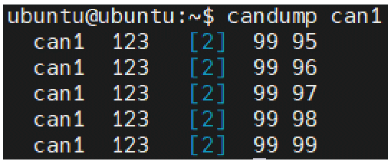
```
$ sudo apt install can-utils
```

2. Enable the Canbus interfaces:

```
$ sudo ip link set can0 type can bitrate 500000
$ sudo ip link set up can0
$ sudo ip link set can1 type can bitrate 500000
```

3. Receive can frame from a terminal:

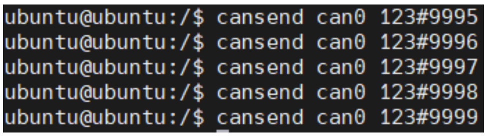
```
$ candump can1
```



```
ubuntu@ubuntu:~$ candump can1
  can1  123   [2]  99 95
  can1  123   [2]  99 96
  can1  123   [2]  99 97
  can1  123   [2]  99 98
  can1  123   [2]  99 99
```

4. Send can frame from another terminal:

```
$ cansend can0 123#9995
$ cansend can0 123#9996
$ cansend can0 123#9997
$ cansend can0 123#9998
$ cansend can0 123#9999
```



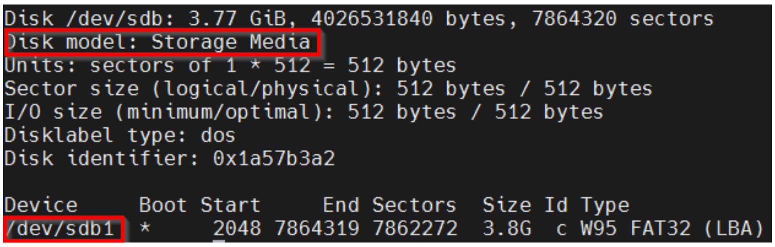
```
ubuntu@ubuntu:/$ cansend can0 123#9995
ubuntu@ubuntu:/$ cansend can0 123#9996
ubuntu@ubuntu:/$ cansend can0 123#9997
ubuntu@ubuntu:/$ cansend can0 123#9998
ubuntu@ubuntu:/$ cansend can0 123#9999
```

Mount USB storage

Steps

1. Plug your USB storage into the device and use the following command to identify the disk as /dev/sdxx:

   ```
   $ sudo fdisk -l
   ```

   ```
   Disk /dev/sdb: 3.77 GiB, 4026531840 bytes, 7864320 sectors
   Disk model: Storage Media
   Units: sectors of 1 * 512 = 512 bytes
   Sector size (logical/physical): 512 bytes / 512 bytes
   I/O size (minimum/optimal): 512 bytes / 512 bytes
   Disklabel type: dos
   Disk identifier: 0x1a57b3a2

   Device     Boot Start     End Sectors  Size Id Type
   /dev/sdb1  *     2048 7864319 7862272  3.8G  c W95 FAT32 (LBA)
   ```

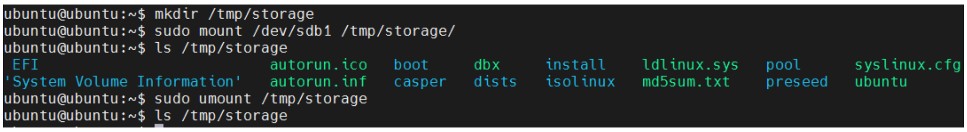
   Figure 123. Identify USB storage

2. Create a directory to be the mount point:

   ```
   $ mkdir /tmp/storage
   ```

3. Mount storage on /tmp/storage:

   ```
   $ sudo mount /dev/sdb1 /tmp/storage
   $ sudo umount /tmp/storage
   ```

   ```
   ubuntu@ubuntu:~$ mkdir /tmp/storage
   ubuntu@ubuntu:~$ sudo mount /dev/sdb1 /tmp/storage/
   ubuntu@ubuntu:~$ ls /tmp/storage
    EFI                           autorun.ico   boot     dbx     install    ldlinux.sys   pool      syslinux.cfg
   'System Volume Information'    autorun.inf   casper   dists   isolinux   md5sum.txt    preseed   ubuntu
   ubuntu@ubuntu:~$ sudo umount /tmp/storage
   ubuntu@ubuntu:~$ ls /tmp/storage
   ```

   Figure 124. Mount USB storage

Configure watchdog

Steps

1. Install watchdog service:

   ```
   $ sudo apt update
   $ sudo apt install watchdog
   ```

2. Edit /etc/default/watchdog:

   ```
   $ sudo vim /etc/default/watchdog
   ```

   Edit watchdog_module parameter as below:

   ```
   #load module before starting watchdog
   watchdog_module="w83627hf_wdt"
   ```

3. Edit /etc/watchdog.conf:

   ```
   $ sudo vim /etc/watchdog.conf
   ```

Ensure that the following parameters exist in the configuration and are not disabled as comment code.

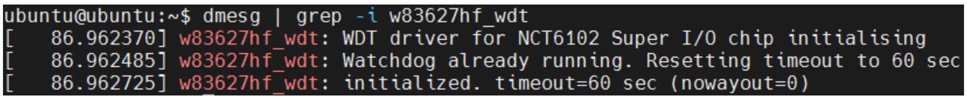
```
retry-timeout = 60
repair-maximum = 1
watchdog-device = /dev/watchdog
interval = 1
logtick = 1
log-dir = /var/log/watchdog
realtime = yes
priority = 1
```

Add a new parameter:

```
# To set the watchdog device timeout, default is 60 seconds
watchdog-timeout = 20
```

4. Reboot the device once, then use the following commands to confirm that the driver and service are working:

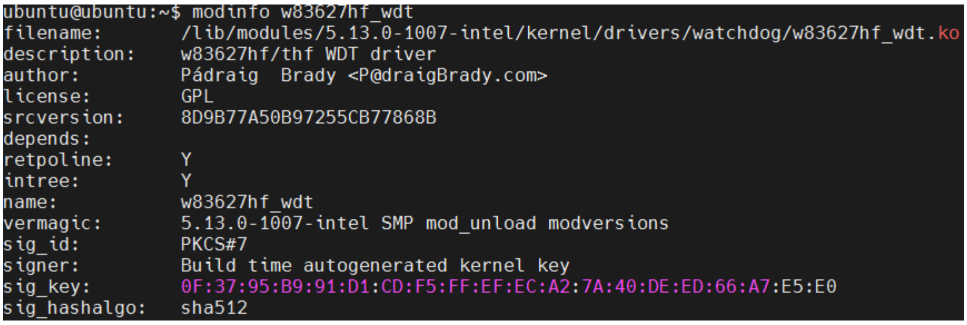
```
$ dmesg | grep -i w83627hf_wdt
```



```
ubuntu@ubuntu:~$ dmesg | grep -i w83627hf_wdt
[   86.962370] w83627hf_wdt: WDT driver for NCT6102 Super I/O chip initialising
[   86.962485] w83627hf_wdt: Watchdog already running. Resetting timeout to 60 sec
[   86.962725] w83627hf_wdt: initialized. timeout=60 sec (nowayout=0)
```

Figure 125. View watchdog

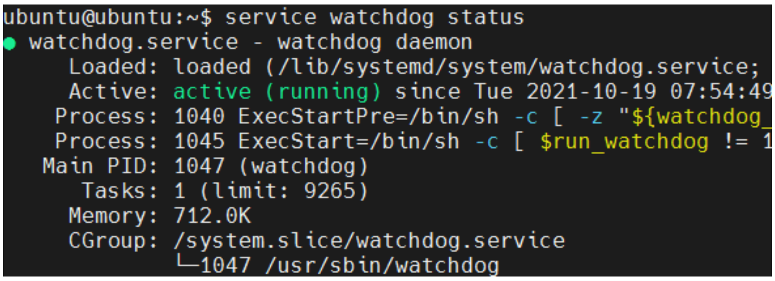
```
$ modinfo w83627hf_wdt
```



```
ubuntu@ubuntu:~$ modinfo w83627hf_wdt
filename:       /lib/modules/5.13.0-1007-intel/kernel/drivers/watchdog/w83627hf_wdt.ko
description:    w83627hf/thf WDT driver
author:         Pádraig  Brady <P@draigBrady.com>
license:        GPL
srcversion:     8D9B77A50B97255CB77868B
depends:
retpoline:      Y
intree:         Y
name:           w83627hf_wdt
vermagic:       5.13.0-1007-intel SMP mod_unload modversions
sig_id:         PKCS#7
signer:         Build time autogenerated kernel key
sig_key:        0F:37:95:B9:91:D1:CD:F5:FF:EF:EC:A2:7A:40:DE:ED:66:A7:E5:E0
sig_hashalgo:   sha512
```

Figure 126. Watchdog info

```
$ service watchdog status
```



```
ubuntu@ubuntu:~$ service watchdog status
● watchdog.service - watchdog daemon
     Loaded: loaded (/lib/systemd/system/watchdog.service;
     Active: active (running) since Tue 2021-10-19 07:54:49
    Process: 1040 ExecStartPre=/bin/sh -c [ -z "${watchdog_
    Process: 1045 ExecStart=/bin/sh -c [ $run_watchdog != 1
   Main PID: 1047 (watchdog)
      Tasks: 1 (limit: 9265)
     Memory: 712.0K
     CGroup: /system.slice/watchdog.service
             └─1047 /usr/sbin/watchdog
```

Figure 127. Watchdog status

5. To test the watchdog device, force the Linux kernel to crash:

```
$ sudo sysctl -w kernel.sysrq=1
$ sudo su -
$ echo c > /proc/sysrq-trigger
```

The system hangs and watchdog reboots the system after 20 seconds (if `watchdog-timeout = 20`).

Configure GPIO

About this task

The EGW-3200 is equipped with six Digital in and six Digital out. To access the registers to read and write to them, perform the following steps.

Steps

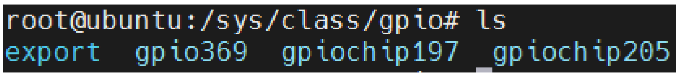
1. Run the following command:

```
$ sudo su -
```

2. Export GPIO:

```
$ echo 369 > /sys/class/gpio/export
```

369 GPIO is USER_LED_1, 370 GPIO is USER_LED_2, and 371 GPIO is USER_LED_3.



```
root@ubuntu:/sys/class/gpio# ls
export  gpio369  gpiochip197  gpiochip205
```

Figure 128. Export GPIO

NOTE: 369 is for kernel v5.13 only.

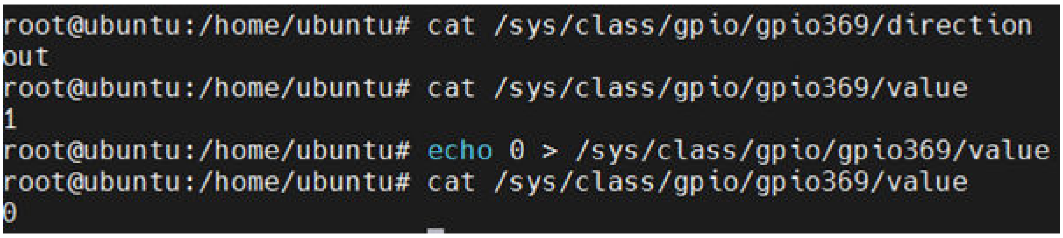
3. Check the GPIO direction and value using the following commands:

```
$ cat /sys/class/gpio/gpio369/direction
$ cat /sys/class/gpio/gpio369/value
```

NOTE: 369 is for kernel v5.13 only.

4. Set the GPIO value using the following command:

```
$ echo {0 or 1} > /sys/class/gpio/gpio369/value
```



```
root@ubuntu:/home/ubuntu# cat /sys/class/gpio/gpio369/direction
out
root@ubuntu:/home/ubuntu# cat /sys/class/gpio/gpio369/value
1
root@ubuntu:/home/ubuntu# echo 0 > /sys/class/gpio/gpio369/value
root@ubuntu:/home/ubuntu# cat /sys/class/gpio/gpio369/value
0
```

Figure 129. Set GPIO value

NOTE: 369 is for kernel v5.13 only.

Results

The low level triggers the USER_LEDs. When the value is 0, the USER_LED is illuminated, as shown in the following figure.

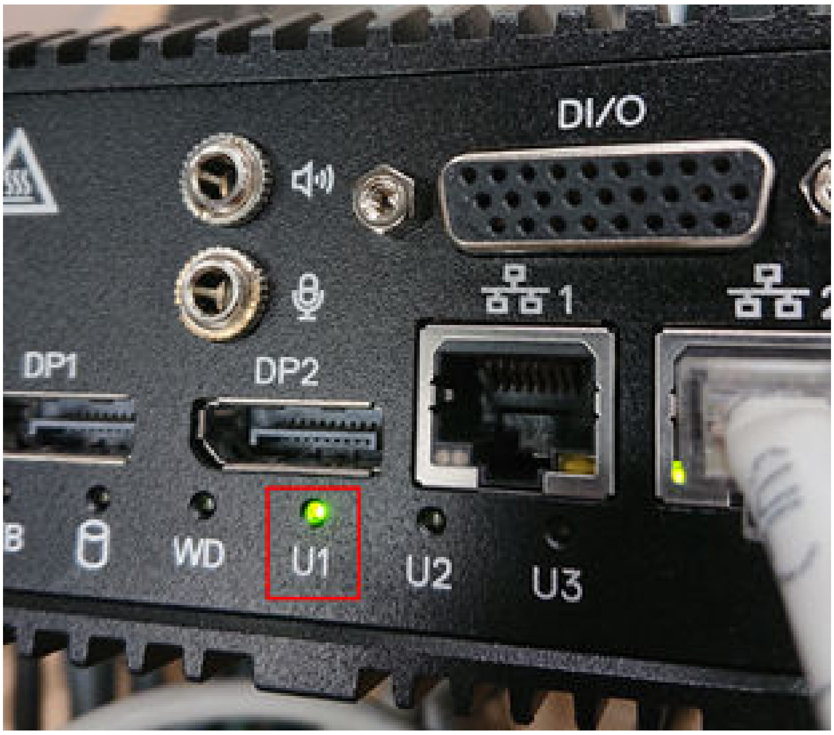


Figure 130. GPIO USER_LED illuminated

The following tables show the GPIO export values.

Table 15. GPIO export values for kernel 5.13.0-xxx-intel

LED	Export value	Digital output	Export value	Digital input	Export value
U1	369	DO0	474	DI0	372
U2	370	DO1	473	DI1	373
U3	371	DO2	471	DI2	374
—		DO3	472	DI3	375
—		DO4	400	DI4	385
—		DO5	404	DI5	386

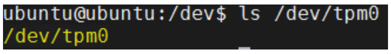
Table 16. GPIO export values for kernel 5.15.0-xxx-intel

LED	Export value	Digital output	Export value	Digital input	Export value
U1	881	DO0	986	DI0	884
U2	882	DO1	985	DI1	885
U3	883	DO2	983	DI2	886
—		DO3	984	DI3	887
—		DO4	912	DI4	897
—		DO5	916	DI5	898

TPM tasks

About this task

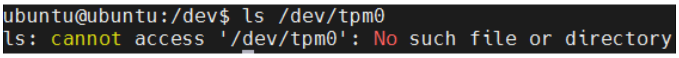
If TPM is turned on, the device node (/dev/tpm0) exists.



```
ubuntu@ubuntu:/dev$ ls /dev/tpm0
/dev/tpm0
```

Figure 131. TPM on

If TPM is turned off, the device node (/dev/tpm0) does not exist.



```
ubuntu@ubuntu:/dev$ ls /dev/tpm0
ls: cannot access '/dev/tpm0': No such file or directory
```

Figure 132. TPM off

TPM can be enabled/disabled from the BIOS **Advanced** menu > **TPM 2.0 Configuration** > **Security Device Support**.

List PCR values

About this task

Use the following command:

```
$ sudo tpm2_pcrread
```

Results

The tpm2_pcrlist is renamed to tpm2_pcrread.

Get random data by TPM

About this task

Use the following command:

```
$ sudo tpm2_getrandom -o <output file> <number of random bytes>
```

For example:

```
$ sudo tpm2_getrandom -o random.out 20
```

Get hash by TPM

About this task

Use the following command:

```
sudo tpm2_hash -g <algorithm> -o <output data> <input data>
```

For example:

```
$ echo "Dell" > message
$ sudo tpm2_hash -g sha1 -o hash.bin message
```

Wake events

Trigger Ubuntu OS to enter S3 status

Steps

1. Use the following command:

   ```
   $ sudo su
   ```

2. Use the following command:

   ```
   $ echo mem > /sys/power/state
   ```

3. Use a USB keyboard to enter any key to wake up the Ubuntu OS.

   > **NOTE:** Use a physical keyboafd to wake up the system. If the keyboard is on a remote SSH session, the box does not wake up.

Use RTC as wake event

Steps

1. Use the following command:

   ```
   $ sudo rtcwake -u -s <second> -m <mode>
   ```

2. The *<mode>* can use the **mem** parameter to enter S3, and the **off** parameter can enter S5.

Wake-on-LAN

Steps

1. Make Ubuntu OS of target device enter S3 or S5.
2. Using another Ubuntu OS device that is working under the same local network, use the following commands:

   ```
   $ sudo apt install wakeonlan
   $ wakeonlan <target device NIC MAC>
   ```

   For example:

   ```
   $ wakeonlan 00:30:64:3a:ad:80
   ```

Results

The target device is waked up as a result of the WoL function.

Wake-on-WLAN

Prerequisites

If the device is not already connected to a WiFi network, see Configure WiFi network to connect.

Steps

1. Use the following command to check the AX210 WiFi card WoWLAN status:

```
$ iw phy0 wowlan show
```

2. If WoWLAN is disabled, use the following command to enable it:

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

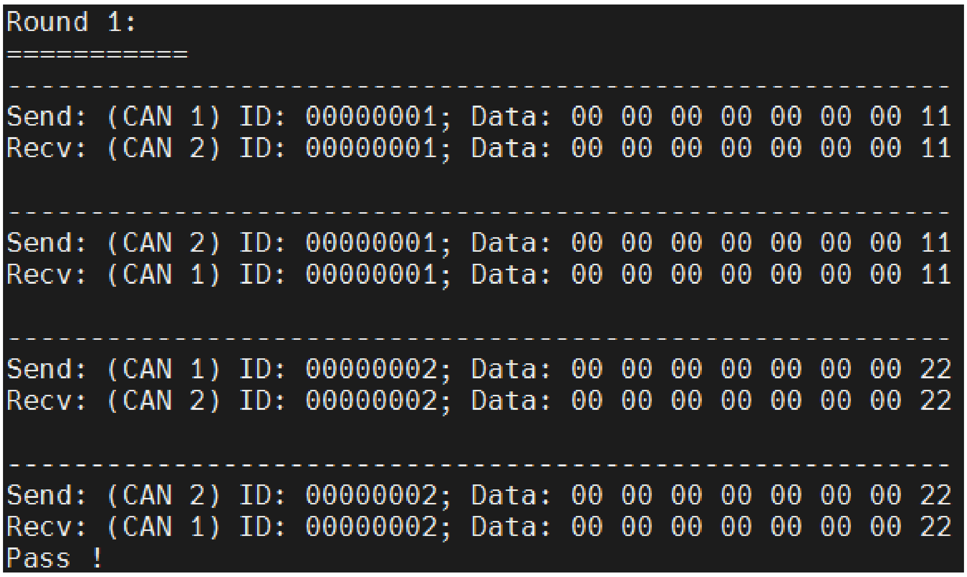
3. Use the `ifconfig` command to make sure your WiFi card (wlp6s0) is connected on a SSID to get an IP address. Record the IP and WiFi MAC address.
4. Use another WiFi client device that is connected to the same SSID and trigger WoL magic packet to wake up the target device.
   For example, use an Android smart phone to install the WoL tool (available on the Wake On LAN page of the Google Play site), then enter the IP and MAC address of the WiFi card of the target device. Trigger the WoL magic packet using the tool to wake up the target device.

Isolated Canbus uFM expansion module

Steps

1. Download the utility tool (EMUC-B202.zip) from the Innodisk official website: EMUC-B202 Driver
2. Unzip the file and copy the driver package onto your platform with the Ubuntu environment.
3. Unzip Linux/EMUC-B202_API_Linux_<DATE>.zip, using the following commands:

```
$ cd EMUC-B202-W1_CAN_API_V2.3.7_Linux/Loopback_EMUC2
$ sudo chmod +x emuc_64
$ sudo ./emuc_64
```



```
Round 1:
===========
---------------------------------------------------------
Send: (CAN 1) ID: 00000001; Data: 00 00 00 00 00 00 00 11
Recv: (CAN 2) ID: 00000001; Data: 00 00 00 00 00 00 00 11

---------------------------------------------------------
Send: (CAN 2) ID: 00000001; Data: 00 00 00 00 00 00 00 11
Recv: (CAN 1) ID: 00000001; Data: 00 00 00 00 00 00 00 11

---------------------------------------------------------
Send: (CAN 1) ID: 00000002; Data: 00 00 00 00 00 00 00 22
Recv: (CAN 2) ID: 00000002; Data: 00 00 00 00 00 00 00 22

---------------------------------------------------------
Send: (CAN 2) ID: 00000002; Data: 00 00 00 00 00 00 00 22
Recv: (CAN 1) ID: 00000002; Data: 00 00 00 00 00 00 00 22
Pass !
```

Figure 133. EMUC-B202 API

4. Edit the **setup.ini** file for different test cases, as detailed in the following table.

Table 17. Setup.ini settings

Parameter	Settings
COM Port	0 = auto scan (Windows), –1 = auto scan (Linux)
Baud rate	4 = 100K, 5 = 125K, 6 = 250K, 7 = 500K, 8 = 800K, 9 = 1M

Table 17. Setup.ini settings (continued)

Parameter	Settings
Interval	1, 2, ..., 1000 [ms], sending interval between each frame
Test time	0 = once, 1, 2, ..., 60 [min], length of test time
Test file	Pattern.txt file includes ID and data used for sending test frames.
Log file	Log.txt is used for saving the test result.

5. Before starting the test, prepare a special port cable that can jump each pin. Connect cable-A and cable-B as below:

   Cable-A-pin2 and cable-B-pin2 are connected using a cable.

   Cable-A-pin7 and cable-B-pin7 are connected using a cable.

EMP2-X2S1 card with isolated RS-232 uFM expansion module

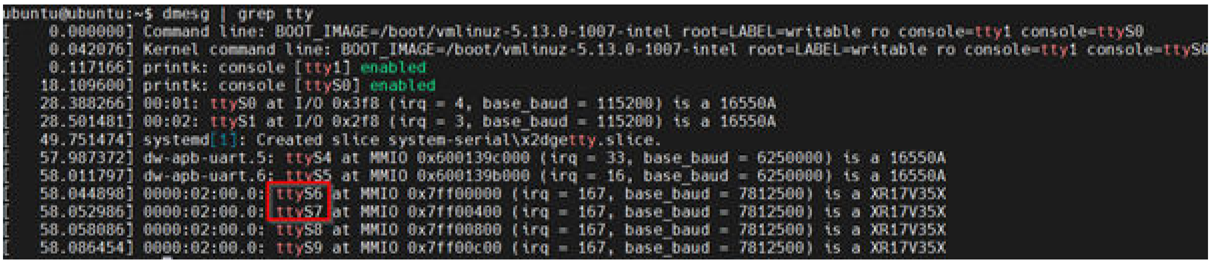
About this task

Map the pins according to the following table.

Table 18. RS-232 pin assignment

Signal	Pin
CD	1
RXD	2
TXD	3
DTR	4
GND	5
DSR	6
RTS	7
CTS	8
RI	9

The EMP2-X2S1 uFM card supports two RS-232 ports, however there are four ports from the OS, as shown in the red box in the following figure:



```
ubuntu@ubuntu:~$ dmesg | grep tty
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.13.0-1007-intel root=LABEL=writable ro console=tty1 console=ttyS0
[    0.042076] Kernel command line: BOOT_IMAGE=/boot/vmlinuz-5.13.0-1007-intel root=LABEL=writable ro console=tty1 console=ttyS0
[    0.117166] printk: console [tty1] enabled
[   18.109600] printk: console [ttyS0] enabled
[   28.388266] 00:01: ttyS0 at I/O 0x3f8 (irq = 4, base_baud = 115200) is a 16550A
[   28.501481] 00:02: ttyS1 at I/O 0x2f8 (irq = 3, base_baud = 115200) is a 16550A
[   49.751474] systemd[1]: Created slice system-serial\x2dgetty.slice.
[   57.987372] dw-apb-uart.5: ttyS4 at MMIO 0x600139c000 (irq = 33, base_baud = 6250000) is a 16550A
[   58.011797] dw-apb-uart.6: ttyS5 at MMIO 0x600139b000 (irq = 16, base_baud = 6250000) is a 16550A
[   58.044898] 0000:02:00.0: ttyS6 at MMIO 0x7ff00000 (irq = 167, base_baud = 7812500) is a XR17V35X
[   58.052986] 0000:02:00.0: ttyS7 at MMIO 0x7ff00400 (irq = 167, base_baud = 7812500) is a XR17V35X
[   58.058086] 0000:02:00.0: ttyS8 at MMIO 0x7ff00800 (irq = 167, base_baud = 7812500) is a XR17V35X
[   58.086454] 0000:02:00.0: ttyS9 at MMIO 0x7ff00c00 (irq = 167, base_baud = 7812500) is a XR17V35X
```

Figure 134. RS-232 ports

Use the first two ports, ttyS6 and ttyS7, as shown in the red square in the previous figure, for the RS-232 port function. The test method references the "serial port" section.

EMP2-X4S2 card with isolated RS-422/485 uFM expansion module

About this task

Map the pins according to the following table.

Table 19. RS-422/485 pin assignment

RS-422 full duplex	Pin	RS-485 half duplex
-	1	-
TX+	2	D+
RX+	3	-
-	4	-
GND	5	GND
-	6	-
RX–	7	-
TX–	8	D–
-	9	-

Steps

1. Download the latest driver (EMP2-X4S2_Linux_driver_<DATE>.zip) from the Dell Technologies Support Site. Unzip the file and copy the driver package on your platform with the Ubuntu environment.
2. Use the following cd commands in the driver directory.

```
$ sudo apt install make gcc
$ sudo make clean
$ sudo make
$ openssl req -new -x509 -newkey rsa:2048 -nodes -days 36500 -outform DER -keyout
"MOK.priv" -out "MOK.der" -subj "/CN=$(hostname) module signing key/"
$ kmodsign sha512 MOK.priv MOK.der xr17v35x.ko
$ sudo make install
$ sudo vim /etc/modules-load.d/modules.conf
```

3. Add **xr17v35x** into the file to make Ubuntu auto load this driver during boot up.

```
$ sudo vim /etc/modules-load.d/modules.conf
```

4. Add **blacklist 8250_exar** into the file to make the standard serial port driver not conflict with xr17v35x.

```
$ sudo vim /etc/modprobe.d/blacklist.conf
```

> **NOTE:** This step is to roll back the modifications of modules.conf/blacklist.conf by the EMP2-X2S1 driver if you previously used the EMP2-X2S1 card.
>
> ```
> $ sudo mokutil --import MOK.der
> ```
>
> Enter your password twice.
>
> ```
> $ sudo reboot
> ```
>
> While the BIOS loads GRUB, the device displays a blue screen for **MokManager**. On this screen, perform the following steps:
>
> a. Select **Enroll MOK**.

b. Use the menus to finish the enrolling process.
c. Use the same password used when running mokutil.
d. Save the key.
e. Reboot again.

5. For RS-422, use RS-422 cables with the EMP2-X4S2 card.

   For the RS-422 port-to-port test, connect the RS-422-A and RS-422-B as detailed in the following:

   - RS-422-A-pin2 and RS-422-B-pin3 are connected with a cable.
   - RS-422-A-pin3 and RS-422-B-pin2 are connected with a cable.
   - RS-422-A-pin7 and RS-422-B-pin8 are connected with a cable.
   - RS-422-A-pin8 and RS-422-B-pin7 are connected with a cable.

6. After the RS-422 hardware is prepared, open two terminal windows.

   For the first terminal window:

   ```
   $ sudo minicom -D /dev/ttyXR0
   ```

   For the second terminal window:

   ```
   $ sudo minicom -D /dev/ttyXR1
   ```

   Type some words in the first terminal to confirm that you can see the words displayed in the second terminal.

7. For RS-485, use RS-485 cables with the EMP2-X4S2 card.

   For the RS-485 port-to-port test, connect the RS-485-A and RS-485-B as detailed in the following:

   - RS-485-A-pin2 and RS-485-B-pin2 are connected with a cable.
   - RS-485-A-pin8 and RS-485-B-pin8 are connected with a cable.

8. After the RS-485 hardware is prepared, open two terminal windows.

   For the first terminal window:

   ```
   $ sudo minicom -D /dev/ttyXR2
   ```

   For the second terminal window:

   ```
   $ sudo minicom -D /dev/ttyXR3
   ```

   Type some words in the first terminal to confirm that you can see the words displayed in the second terminal.

Connect a PCA9535 GPIO expander board

About this task

A PCA9535 GPIO expander board and connector are shown in the following figure.

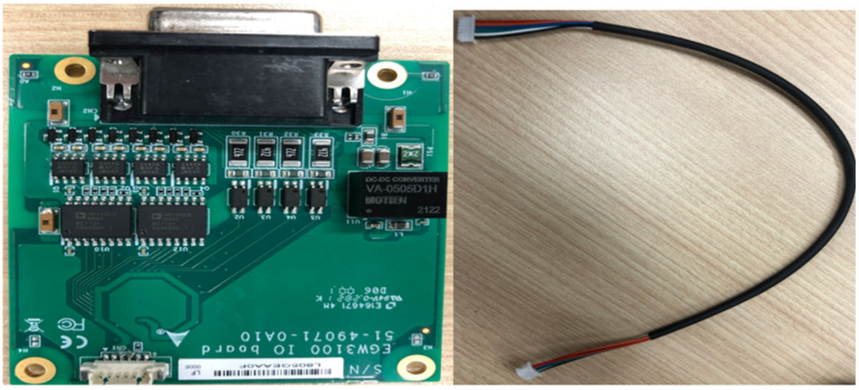


Figure 135. PCA9535 GPIO expander board and connector

The PCA9535 7-bit device address is 0x20.

CN13 is the connector for the PCA9535 expander. CN13 is connected to I2C bus #3, as shown in the following figure.

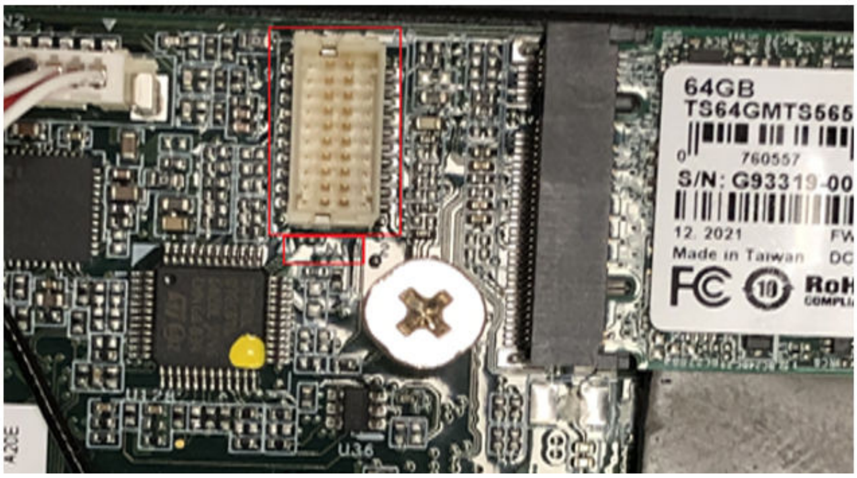


Figure 136. Board connection for the PCA9535 GPIO expander

Steps

1. Connect the expander board according to the previous figures, then reboot the system.
2. Install the i2c-tools using the following command:

```
$sudo apt update
$sudo apt -y install i2c-tools
```

3. The probe function of the i2c-dev driver does not necessarily map to a fixed bus number, so the mapping system node is not always the same after a system reboot. To resolve this, perform the following sub-steps:
   a. Scan and list the I2C bus controllers, and see that there are seven i2c buses, as shown in the following example:

```
$ sudo i2cdetect -l | grep -i Synopsys
i2c-3   i2c            Synopsys DesignWare I2C adapter         I2C adapter
i2c-1   i2c            Synopsys DesignWare I2C adapter         I2C adapter
i2c-6   i2c            Synopsys DesignWare I2C adapter         I2C adapter
i2c-4   i2c            Synopsys DesignWare I2C adapter         I2C adapter
i2c-0   i2c            Synopsys DesignWare I2C adapter         I2C adapter
i2c-7   i2c            Synopsys DesignWare I2C adapter         I2C adapter
i2c-5   i2c            Synopsys DesignWare I2C adapter         I2C adapter
```

   The PCA9535 is on one of these *${busnum}* nodes.

   b. Perform the following command to check all I2C nodes until the register 0x02 of device address 0x20 (PCA9535) has a standard output 0xff, which means that a PCA9535 has been found on *${busnum}*.

```
$ sudo i2cget -y ${busnum} 0x20 0x02 2>/dev/null
```

   For example:

```
$ sudo i2cget -y 3 0x20 0x02 2>/dev/null
0xff
$ sudo i2cget -y 1 0x20 0x02 2>/dev/null
$ sudo i2cget -y 6 0x20 0x02 2>/dev/null
$ sudo i2cget -y 4 0x20 0x02 2>/dev/null
$ sudo i2cget -y 0 0x20 0x02 2>/dev/null
$ sudo i2cget -y 7 0x20 0x02 2>/dev/null
$ sudo i2cget -y 5 0x20 0x02 2>/dev/null
```

4. Confirm that the PCA9536 GPIO expander board driver PCA953x is loaded using the following command:

```
$ lsmod | grep pca
gpio_pca953x          28672  16
```

If the gpio_pca953x module is not found, load the module using the following command:

```
$ sudo modprobe gpio-pca953x
```

Confirm that the module is loaded using the following command:

```
$ sudo dmesg | grep pca953x
[   75.638778] pca953x 3-0020: supply vcc not found, using dummy regulator
[   75.638862] pca953x 3-0020: using no AI
```

5. Initialize the PCA9535 GPIO expander board using the following command:

```
$ echo pca9535 $busaddr | sudo tee /sys/bus/i2c/devices/i2c-${busnum}/new_device
```

   For example: `$ echo pca9535 0x20 | sudo tee /sys/bus/i2c/devices/i2c-3/new_device`

6. To verify that the device is active and working, use the following command:

```
$ sudo i2cdetect -y -r ${busnum}
```

   For example:

```
$ sudo i2cdetect -y -r 3
     0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00:          -- -- -- -- -- -- -- -- -- -- -- -- --
10: -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
20: UU -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
30: -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
40: -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
50: -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
60: -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
70: -- -- -- -- -- -- -- --
```

7. Depending on the kernel version, test the GPIO port by performing the steps in one of the following:
   a. To test the GPIO port on kernel version 5.13, use the following command:

```
$ sudo su
$ echo 181 > /sys/class/gpio/export
$ echo 182 > /sys/class/gpio/export
$ echo 183 > /sys/class/gpio/export
$ echo 184 > /sys/class/gpio/export
$ echo 185 > /sys/class/gpio/export
$ echo 186 > /sys/class/gpio/export
$ echo 187 > /sys/class/gpio/export
$ echo 188 > /sys/class/gpio/export
$ echo 189 > /sys/class/gpio/export
$ echo 190 > /sys/class/gpio/export
$ echo 191 > /sys/class/gpio/export
$ echo 192 > /sys/class/gpio/export
$ echo 193 > /sys/class/gpio/export
$ echo 194 > /sys/class/gpio/export
$ echo 195 > /sys/class/gpio/export
$ echo 196 > /sys/class/gpio/export

$ echo out > /sys/class/gpio/gpio181/direction
$ echo out > /sys/class/gpio/gpio182/direction
$ echo out > /sys/class/gpio/gpio183/direction
$ echo out > /sys/class/gpio/gpio184/direction
$ echo out > /sys/class/gpio/gpio185/direction
$ echo out > /sys/class/gpio/gpio186/direction
$ echo out > /sys/class/gpio/gpio187/direction
$ echo out > /sys/class/gpio/gpio188/direction

$ echo in > /sys/class/gpio/gpio189/direction
$ echo in > /sys/class/gpio/gpio190/direction
$ echo in > /sys/class/gpio/gpio191/direction
$ echo in > /sys/class/gpio/gpio192/direction
$ echo in > /sys/class/gpio/gpio193/direction
$ echo in > /sys/class/gpio/gpio194/direction
$ echo in > /sys/class/gpio/gpio195/direction
$ echo in > /sys/class/gpio/gpio196/direction
```

Write 0 or 1 on the OUT port and read the IN port using the external loop back board, as shown in the following figure:

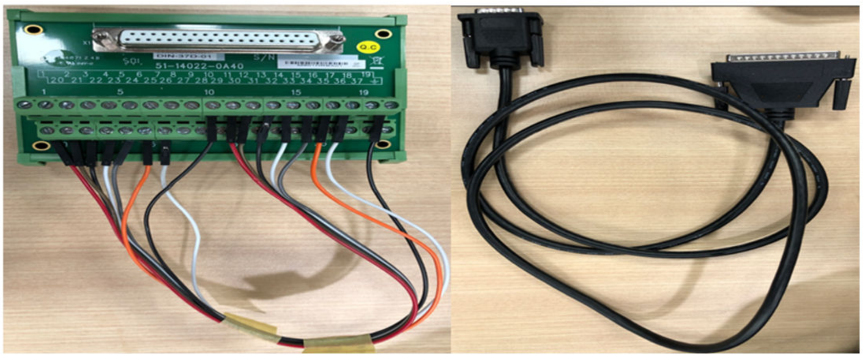


Figure 137. External loop back board and connector

```
$ echo 0 > /sys/class/gpio/gpio181/value
$ cat /sys/class/gpio/gpio189/value
0
$ echo 1 > /sys/class/gpio/gpio182/value
$ cat /sys/class/gpio/gpio190/value
1
$ echo 0 > /sys/class/gpio/gpio183/value
$ cat /sys/class/gpio/gpio191/value
0
$ echo 1 > /sys/class/gpio/gpio184/value
$ cat /sys/class/gpio/gpio192/value
1
$ echo 0 > /sys/class/gpio/gpio185/value
$ cat /sys/class/gpio/gpio193/value
0
$ echo 1 > /sys/class/gpio/gpio186/value
$ cat /sys/class/gpio/gpio194/value
1
$ echo 0 > /sys/class/gpio/gpio187/value
$ cat /sys/class/gpio/gpio195/value
0
$ echo 1 > /sys/class/gpio/gpio188/value
$ cat /sys/class/gpio/gpio196/value
1
$ echo 1 > /sys/class/gpio/gpio181/value
$ cat /sys/class/gpio/gpio189/value
1
$ echo 0 > /sys/class/gpio/gpio182/value
$ cat /sys/class/gpio/gpio190/value
0
$ echo 1 > /sys/class/gpio/gpio183/value
$ cat /sys/class/gpio/gpio191/value
1
$ echo 0 > /sys/class/gpio/gpio184/value
$ cat /sys/class/gpio/gpio192/value
0
$ echo 1 > /sys/class/gpio/gpio185/value
$ cat /sys/class/gpio/gpio193/value
1
$ echo 0 > /sys/class/gpio/gpio186/value
$ cat /sys/class/gpio/gpio194/value
0
$ echo 1 > /sys/class/gpio/gpio187/value
$ cat /sys/class/gpio/gpio195/value
1
$ echo 0 > /sys/class/gpio/gpio188/value
$ cat /sys/class/gpio/gpio196/value
0
```

b. To test the GPIO port on kernel version 5.15, use the following command:

```
$ sudo su
$ echo 693 > /sys/class/gpio/export
$ echo 694 > /sys/class/gpio/export
$ echo 695 > /sys/class/gpio/export
$ echo 696 > /sys/class/gpio/export
$ echo 697 > /sys/class/gpio/export
$ echo 698 > /sys/class/gpio/export
$ echo 699 > /sys/class/gpio/export
$ echo 700 > /sys/class/gpio/export
$ echo 701 > /sys/class/gpio/export
$ echo 702 > /sys/class/gpio/export
$ echo 703 > /sys/class/gpio/export
$ echo 704 > /sys/class/gpio/export
$ echo 705 > /sys/class/gpio/export
$ echo 706 > /sys/class/gpio/export
$ echo 707 > /sys/class/gpio/export
$ echo 708 > /sys/class/gpio/export

$ echo out > /sys/class/gpio/gpio693/direction
$ echo out > /sys/class/gpio/gpio694/direction
$ echo out > /sys/class/gpio/gpio695/direction
$ echo out > /sys/class/gpio/gpio696/direction
$ echo out > /sys/class/gpio/gpio697/direction
$ echo out > /sys/class/gpio/gpio698/direction
$ echo out > /sys/class/gpio/gpio699/direction
$ echo out > /sys/class/gpio/gpio700/direction

$ echo in > /sys/class/gpio/gpio701/direction
$ echo in > /sys/class/gpio/gpio702/direction
$ echo in > /sys/class/gpio/gpio703/direction
$ echo in > /sys/class/gpio/gpio704/direction
$ echo in > /sys/class/gpio/gpio705/direction
$ echo in > /sys/class/gpio/gpio706/direction
$ echo in > /sys/class/gpio/gpio707/direction
$ echo in > /sys/class/gpio/gpio708/direction
```

Write 0 or 1 on the OUT port and read the IN port using the external loop back board, as shown in the previous figure.

```
$ echo 0 > /sys/class/gpio/gpio693/value
$ cat /sys/class/gpio/gpio701/value
0
$ echo 1 > /sys/class/gpio/gpio694/value
$ cat /sys/class/gpio/gpio702/value
1
$ echo 0 > /sys/class/gpio/gpio695/value
$ cat /sys/class/gpio/gpio703/value
0
$ echo 1 > /sys/class/gpio/gpio696/value
$ cat /sys/class/gpio/gpio704/value
1
$ echo 0 > /sys/class/gpio/gpio697/value
$ cat /sys/class/gpio/gpio705/value
0
$ echo 1 > /sys/class/gpio/gpio698/value
$ cat /sys/class/gpio/gpio706/value
1
$ echo 0 > /sys/class/gpio/gpio699/value
$ cat /sys/class/gpio/gpio707/value
0
$ echo 1 > /sys/class/gpio/gpio700/value
$ cat /sys/class/gpio/gpio708/value
1
$ echo 1 > /sys/class/gpio/gpio693/value
$ cat /sys/class/gpio/gpio701/value
1
$ echo 0 > /sys/class/gpio/gpio694/value
$ cat /sys/class/gpio/gpio702/value
0
$ echo 1 > /sys/class/gpio/gpio695/value
$ cat /sys/class/gpio/gpio703/value
```

```
1
$ echo 0 > /sys/class/gpio/gpio696/value
$ cat /sys/class/gpio/gpio704/value
0
$ echo 1 > /sys/class/gpio/gpio697/value
$ cat /sys/class/gpio/gpio705/value
1
$ echo 0 > /sys/class/gpio/gpio698/value
$ cat /sys/class/gpio/gpio706/value
0
$ echo 1 > /sys/class/gpio/gpio699/value
$ cat /sys/class/gpio/gpio707/value
1
$ echo 0 > /sys/class/gpio/gpio700/value
$ cat /sys/class/gpio/gpio708/value
0
```

Ubuntu troubleshooting

The following tasks describe how to recover from errors when using Ubuntu.

Recover from cloud-init process failure

About this task

During boot up, one of the following failure symptoms may occur:

- Ethernet ports do not work. This is due to the improper power-up and a failed cloud-init process.
- The system does not require an Ubuntu password change on first boot up. This occurs when the user logs in to the system before the cloud-init process has finished.

To recover from these failure scenarios, perform the following steps to retrigger the cloud-init (init-local) process.

Steps

1. Run the following commands to clear the cloud-init log and clean the cloud-init process:

   ```
   $ sudo rm -rf /var/lib/cloud/instances
   $ sudo cloud-init clean
   $ sudo rm /var/log/cloud-init*.log
   $ sudo poweroff
   ```

2. Reboot the system to start a new init-local process.