V2201 Series Windows Software User's Manual

Edition 1.1, December 2015

www.moxa.com/product

V2201 Series Windows Software User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Moxa Americas
Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa China (Shanghai office)
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Europe
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa Asia-Pacific
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Moxa India
Tel: +91-80-4172-9088
Fax: +91-80-4132-1045

Table of Contents

1

Introduction

Thank you for purchasing a Moxa V2201 panel computer running the Windows 7 Embedded operating system. The Windows 7 Embedded OS provides a simple and familiar development environment for a variety of industrial applications.

Software Components

The following software components of the Windows Embedded Standard 7 OS come pre-installed on the V2201 computer.

Windows Embedded Standard 7

Core OS:

- 64-bit supported
- Remote Client
- Remote Procedure Call

Applications and Services Development:

- Remote Desktop Protocol 7.1
- COM OLE Application Support
- COM+ Application Support
- MSMQ

Internet Services:

- Internet Explorer 8
- IIS 7.0

File Systems and Data Storage:

- Windows Data Access Components
- Windows Backup and Restore

Diagnostics:

- Common Diagnostic Tools
- Problem Reports and Solutions

Fonts: Western, Middle Eastern, South East Asian, and South Asian Fonts

Graphics and Multimedia:

- MPEG Layer-3 Audio Codecs (MP3)
- MPEG4 Decoders
- DirectX and Windows Device Experience

Management:

- Group Policy Management
- Windows Management Instrument (WMI)
- Windows Update

Networking:

- Extensible Authentication Protocol (EAP)
- Internet Authentication Service
- Telnet Server
- Bluetooth
- Domain Services
- Network Access Protection
- Network and Sharing Center
- Quality of Service
- Remote Access Service (RAS)
- Telephony API Client
- Windows Firewall
- Wireless Networking

Security:

- Credential Roaming Service
- Credentials and Certificate Management
- Windows Authorization Manager (AZMAN)
- Windows Security Center
- Active Directory Rights Management
- Security Base
- Encrypted File System (EFS)

Embedded Features:

- Enhanced Write Filter (EWF)
- File-Based Write Filter (FBWF)
- Registry Filter
- WSDAPI for .NET

Embedded Self-Health Diagnostic Software: Moxa Proactive Monitoring & Moxa Smart Recovery

2

System Initialization

In this chapter, we describe how to initialize the system settings on the V2201 embedded computer when booting up for the first time.

The following topics are covered in this chapter:

- **Overview**
- **Initializing User Settings**

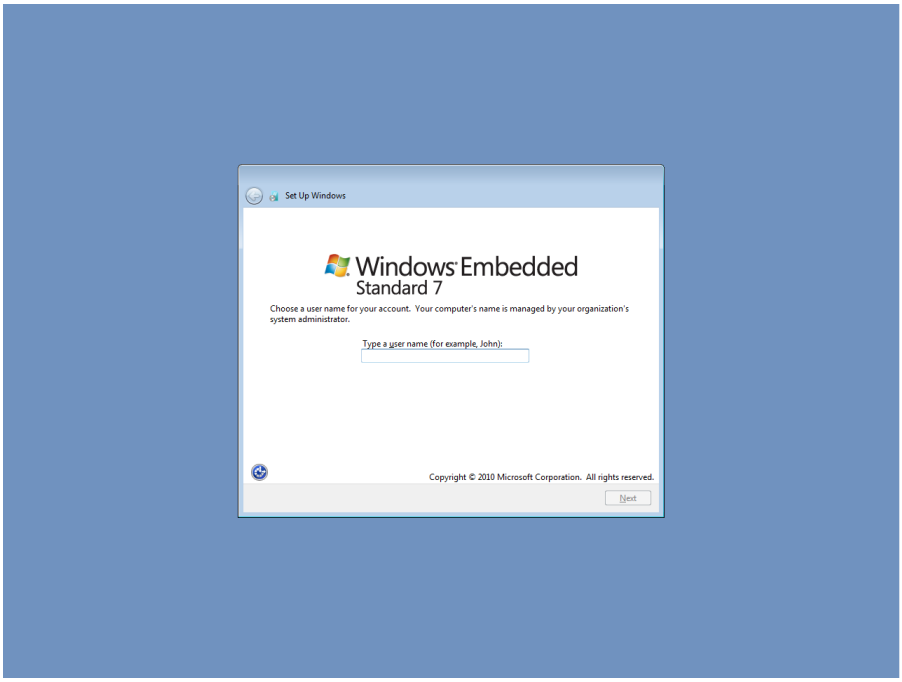
Overview

Similar to using a laptop computer for the first time, you need to specify a user name and create a user account to start using the V2201 embedded computer. Follow the procedure described in the next section.

NOTE If you perform a system recovery on the V2201 embedded computer, the system automatically resets to the factory defaults. You must initialize the user settings again.

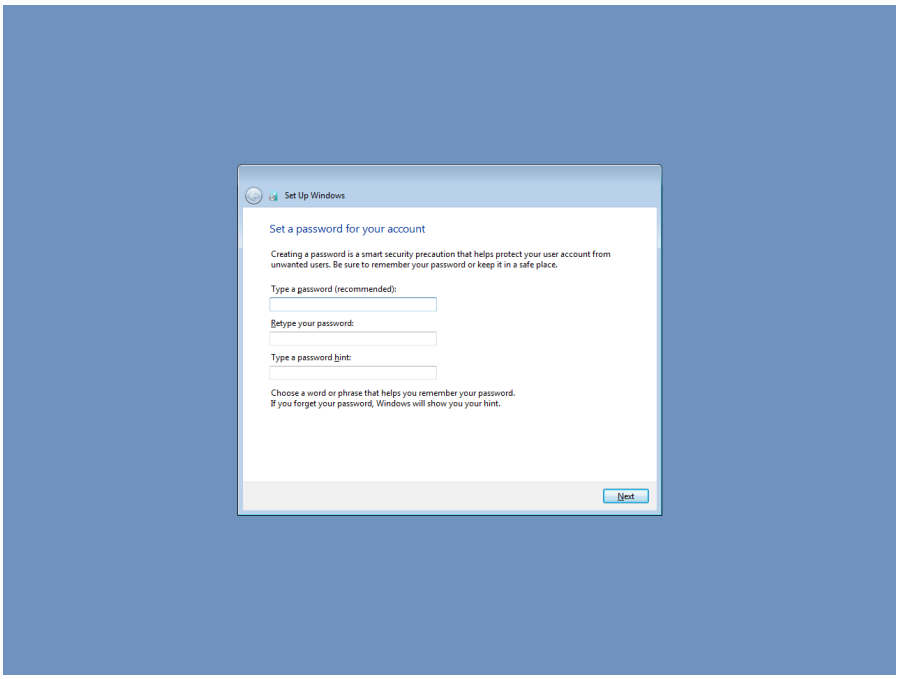
Initializing User Settings

1. When you turn on the embedded computer for the first time, enter a user name for the computer.

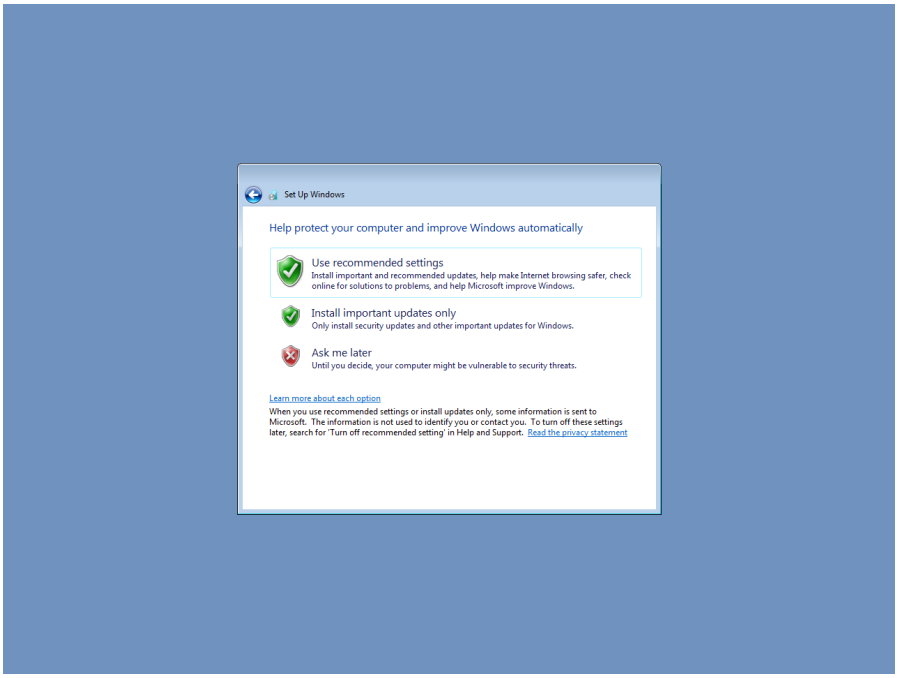


2. Type a password and retype the password to confirm.

   You may also type a password hint that you can refer to if you forget your password. If you do not want to set a password, leave all three fields blank. Click **Next** to continue.

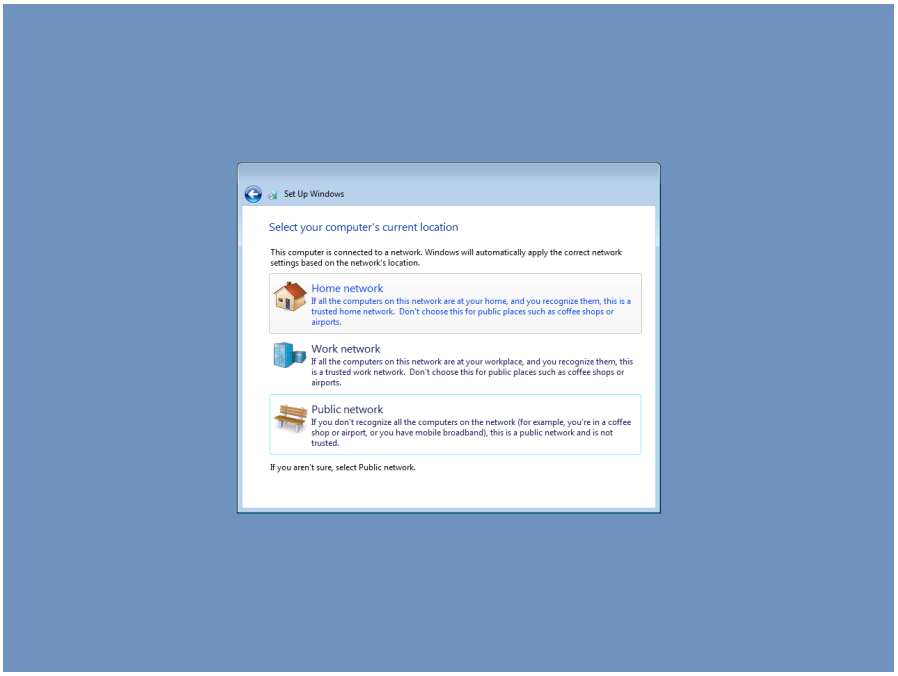


3. Select a Windows update option.



4. Select the computer's current location, and review the time and date settings.

   Windows automatically applies the appropriate network settings based on the type of network you select.



5. When the Windows desktop screen appears, you can start using your V2201 embedded computer.

3

Configuring the Serial Interface

This chapter describes how to configure the serial interface on the V2201 embedded computer.

The following topics are covered in this chapter:

- **Overview**
- **Configuring the Serial Interface Mode**

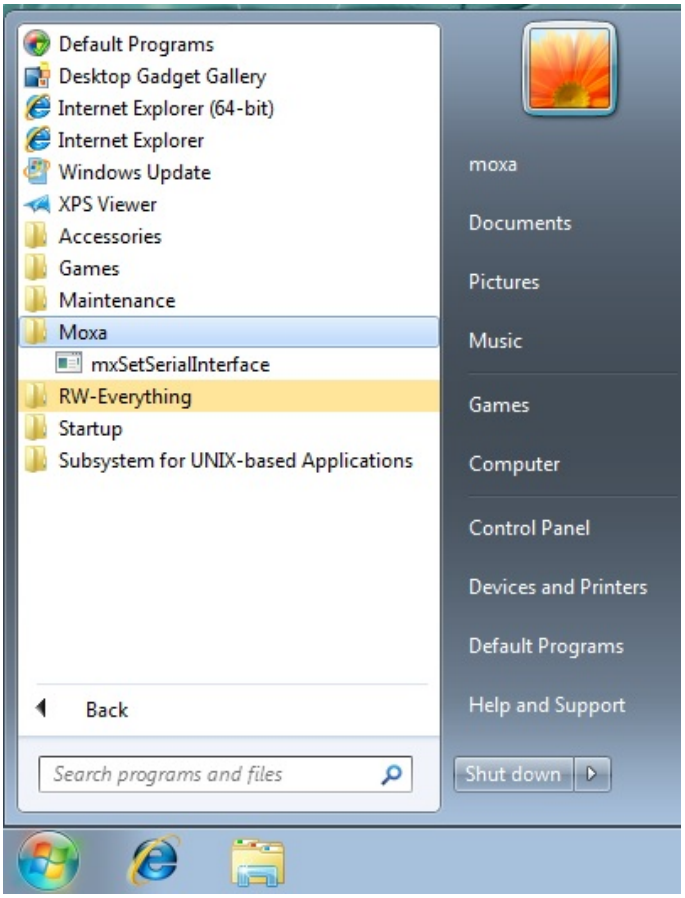
Overview

The V2201 supports the following serial modes: **RS-232, RS-485-2-wire** and **RS-422/485-4-wire**. These modes can be configured on COM1 and COM2.

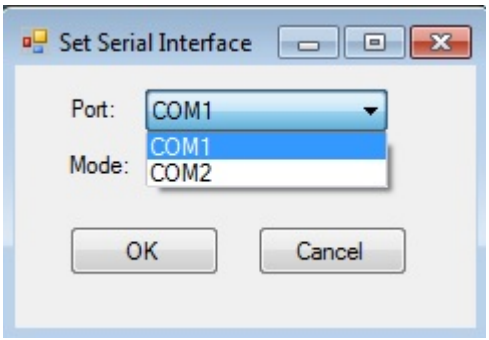
Configuring the Serial Interface Mode

Complete the following steps to configure the serial interface mode:

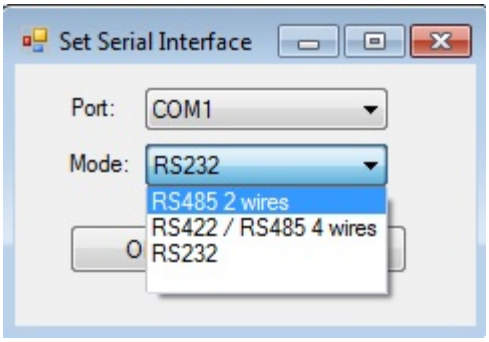
1. From the Start menu, Click **All Programs → Moxa → mxSetSerialInterface**.



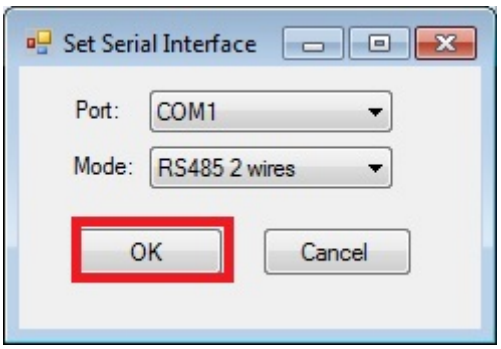
2. Select the port you would like to configure from the **Port** drop-down box



3. Select the serial interface mode for the port from the **Mode** drop-down box



4. Click **OK**.



4

Enabling Embedded Filters

In this chapter, we describe how to enable the V2201's embedded filters.

The following topics are covered in this chapter:

- **Enhanced Write Filter**
  - Overview
  - Enabling Enhanced Write Filter
  - Committing Data and/or Disabling EWF
- **File-Based Write Filter**
  - Configuring File-Based Write Filter
  - Excluding Files from FBWF Protection
  - Managing Temporary Files Cached in the Overlay

Enhanced Write Filter

Overview

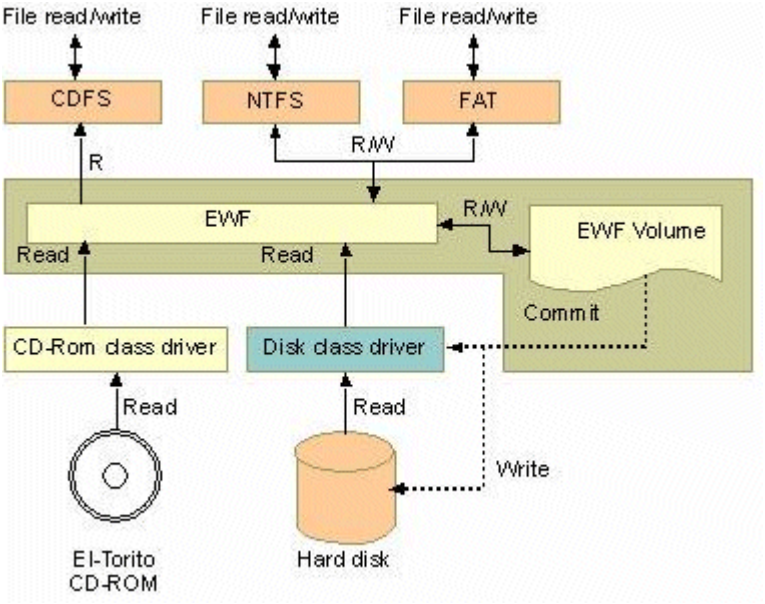
Enhanced Write Filter (EWF) enables you to protect a volume from unauthorized writes by making the main operating system (OS) drive a write-protected volume, effectively making the system a read-only system for most users. This provides much stronger protection against malicious computer attacks (such as trojans, worms, and viruses).

Enhanced Write Filter (EWF) allows Windows 7 users to protect data on their storage drive from permanent changes of any sort, at the lowest level of hardware protection available: the bit level. **EWF** allows the OS to boot from the hard disk, but protects the system by creating a virtual file system called an **overlay**. All writes to an EWF-protected volume (the **hard disk** in the following figure) are only recorded on this virtual overlay (the **EWF Volume** in the following figure), which is stored independently in random access memory (RAM).

Because EWF does not write data directly to the hard disk but instead only records system writes to this virtual RAM overlay, any data that is "written" during system operation will disappear upon the next re-boot. This approach allows the system to operate as if it is writeable when in reality all OS and user-space file systems are stored in a permanent, read-only state.

If required, data written to the overlay can be committed to the protected volume, but this requires additional setup and permissions that can only be granted by the administrator.

The following figure shows an overview of the EWF structure.



For more detailed information about EWF configuration and usage, refer to the following resources:

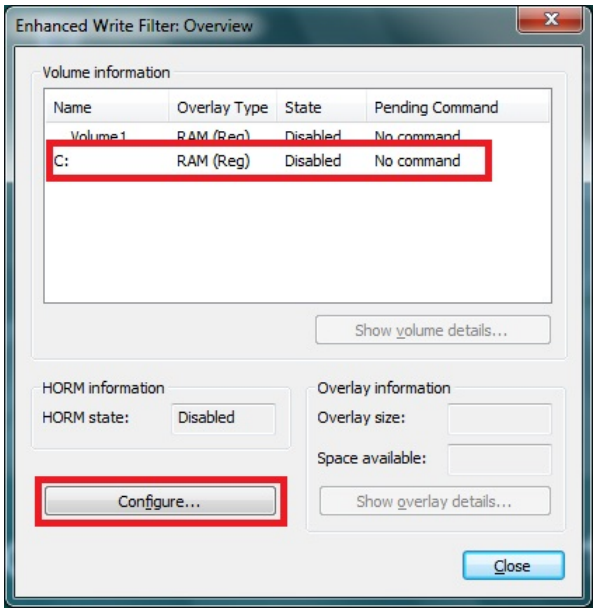
- Visit Microsoft's EWF Volume Configuration help pages.
- See Microsoft's EWF overview on the official Microsoft EWF help pages.
- See Microsoft's detailed description of EWF modes on the EWF help pages.
- See Microsoft's detailed description of the EWF API.
- For EWF commands, refer to the MSDN web site: http://msdn.microsoft.com/en-us/library/ms940853%28v=winembedded.5%29.aspx

Enabling Enhanced Write Filter

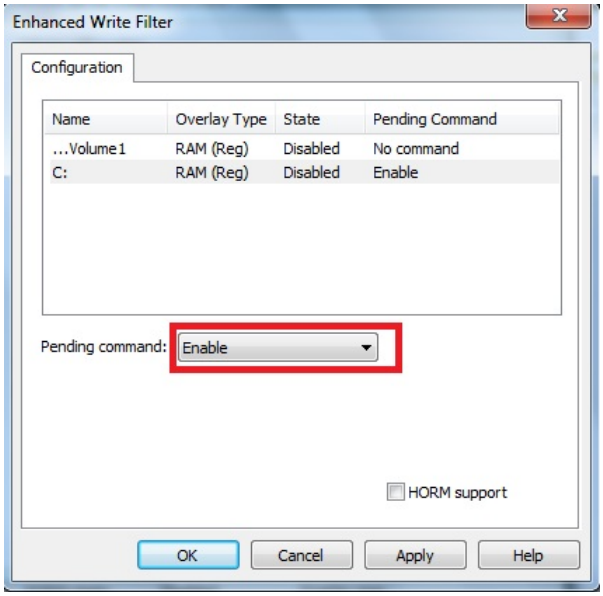
Follow these steps to enable Enhanced Write Filter:

1. To open EWF, double-click the padlock icon in the system tray.
   You may need to show hidden icons in the system tray.

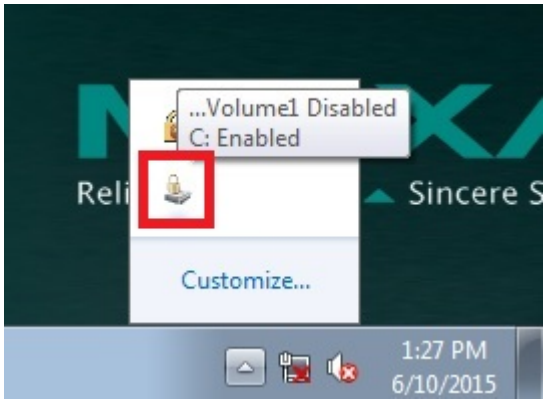
2. In the **Volume Information** area, select the partition you want to enable write-protection on and click **Configure...**.



3. The Configuration dialog box appears. Select **Enable** from the **Pending command** drop-down list and click **OK**.



4. Reboot the system.
5. Log into the system and verify that the padlock icon in the system tray indicates that the drive volume is locked with EWF.

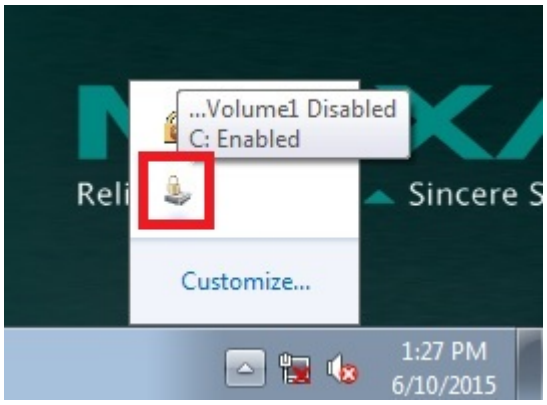


Committing Data and/or Disabling EWF

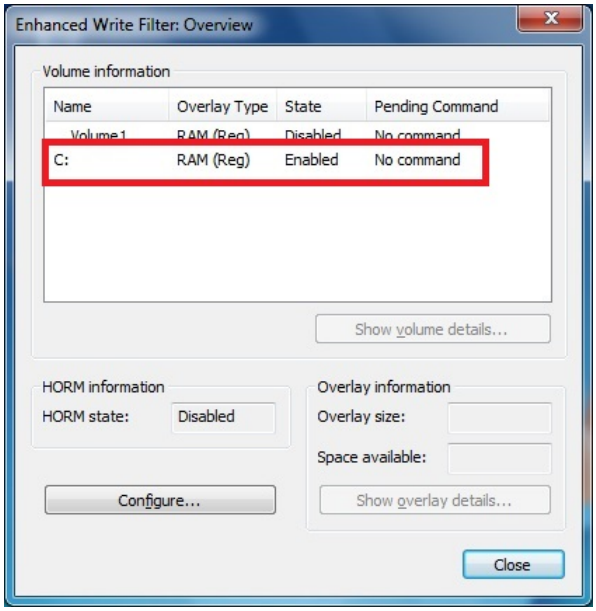
Perform the following steps to write (or commit) data to an EWF-enabled drive.

NOTE You must have administrator privileges to commit data to the drive.

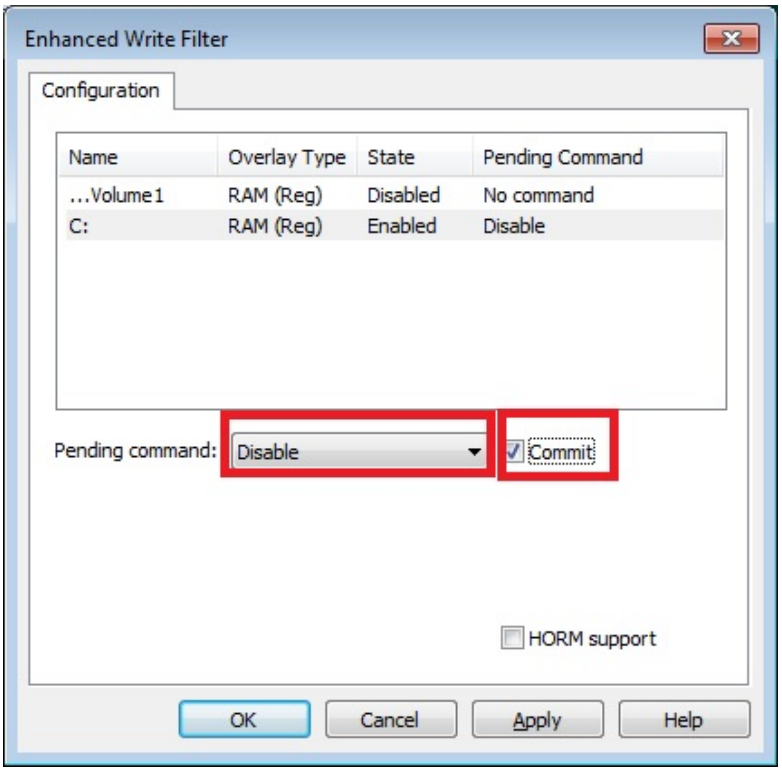
1. Double-click the padlocked drive in the system tray.
   You may need to show hidden icons in the system tray.



2. In the **Enhanced Write Filter: Overview** dialog box, select the drive you want to configure and click **Configure**.



3. In the Enhanced Write Filter Configuration screen, select a drive volume; then, select an option from the **Pending Command** drop-down list:
   - **No Command**
   - **Disable:** Disables EWF on the selected drive. You will need to select the "commit" checkbox and reboot the system for changes to take effect.
   - **Commit:** Writes all current system changes to the hard drive.
   - **Commit and Disable Live:** Writes all current data and changes to the system, and also turns off EWF on the selected drive (so that all future data and system changes will also be committed to the drive). The system does not automatically reboot if you select this option.



NOTE For detailed information, go to the Microsoft website at http://msdn.microsoft.com/en-us/library/ff794092(v=winembedded.60).aspx.

File-Based Write Filter

This section describes how to use the File-Based Writer Filter (FBWF). Note that when Enhanced Writer Filter is enabled, the File-Based Writer Filter function will not work.

According to Microsoft:

"File-Based Write Filter (FBWF) allows the Windows Embedded platform to maintain the appearance of read and write access on write-sensitive or read-only storage. FBWF makes read and write access transparent to applications.

Writing to storage media may be undesirable or impossible in embedded devices. FBWF redirects all writes targeted for protected volumes to a RAM cache called an overlay. Used in this context, an overlay is similar to a transparency overlay on an overhead projector. Any change made to the overlay affects the picture as seen in the aggregate, but if the overlay is removed, the underlying picture remains unchanged."

FBWF supports an advanced ESF feature, which allows users to specify which directory to write data to. The default directory is c:\temp. The advanced feature allows you can read/write data to disk without committing an action.

Configuring File-Based Write Filter

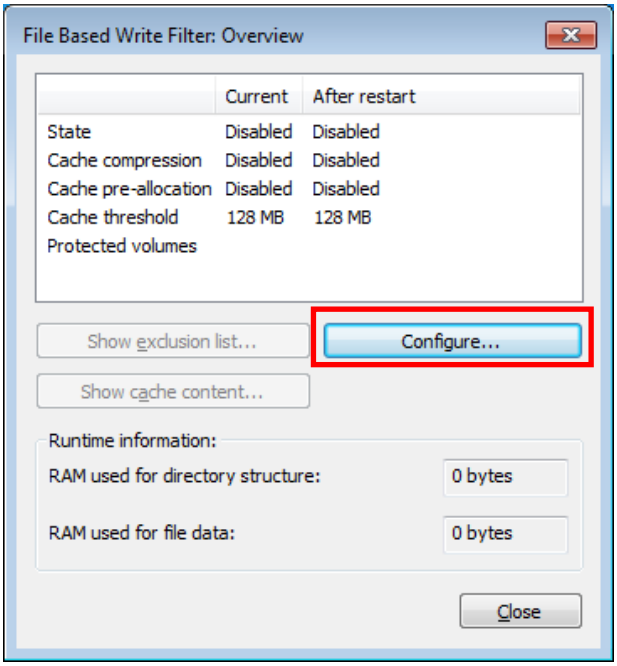
Complete the following steps to enable the File-Based Write Filter (FBWF) feature. Although you can enable FBWF and EWF on the same computer, FBWF does not protect a volume that is already protected by EWF. Similarly, EWF does not protect a volume that is already protected by FBWF.

NOTE Before using FBWF, make sure that you disable EWF.

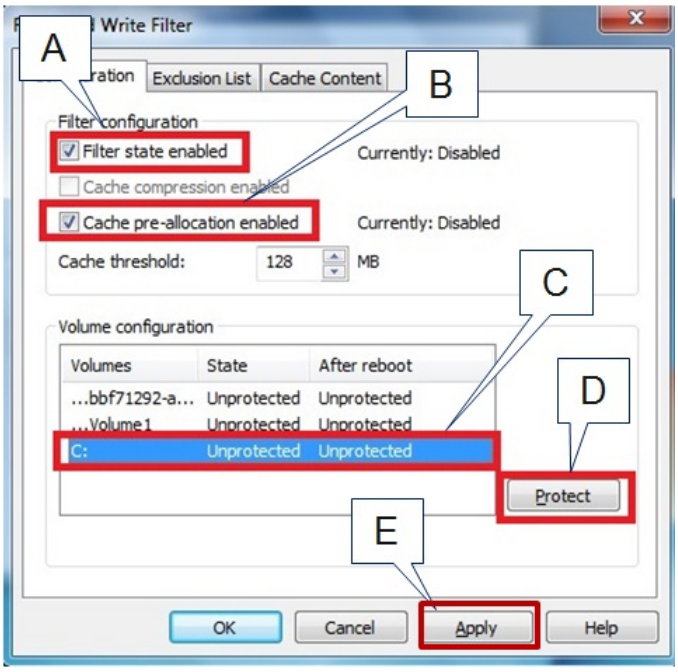
1. Double-click the padlock icon in the system tray.
   You may need to show hidden icons in the system tray.

NOTE When disabled, the EWF and FBWF icons in the system tray look the same. To verify that you have opened the correct writer filter program, check the screen title.

2. In the **File Based Writer Filter: Overview** screen, click **Configure**.

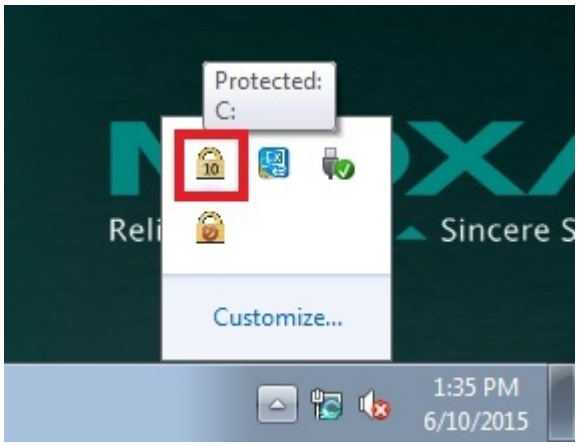


3. To enable FBWF protection on a storage drive, perform the following actions:
   a. Select **Filter state enabled** and **Cache pre-allocation enabled**.
   b. In the **Volume Configuration** area, select the storage drive you want to protect and click **Protect**.
   c. Click **Apply** or **OK**.



NOTE To minimize memory usage on the overlay cache, select **Cache compression enabled**. However, cache compression decreases performance when accessing protected volumes.
Select **Cache pre-allocation enable** to set the memory space available for the overlay cache when the system starts up, instead of adjusting it as needed.
You cannot enable cache pre-allocation and cache compression at the same time.
The **cache threshold** field sets the amount of memory that can be used by the write filter for the overlay cache. The default value and size limits for the overlay cache vary depending on the operating system.

4. Reboot the system.
5. Log into the system and verify that the padlock icon in the system tray displays a number and indicates that FBWF is enabled on a drive. The following figure shows an example.

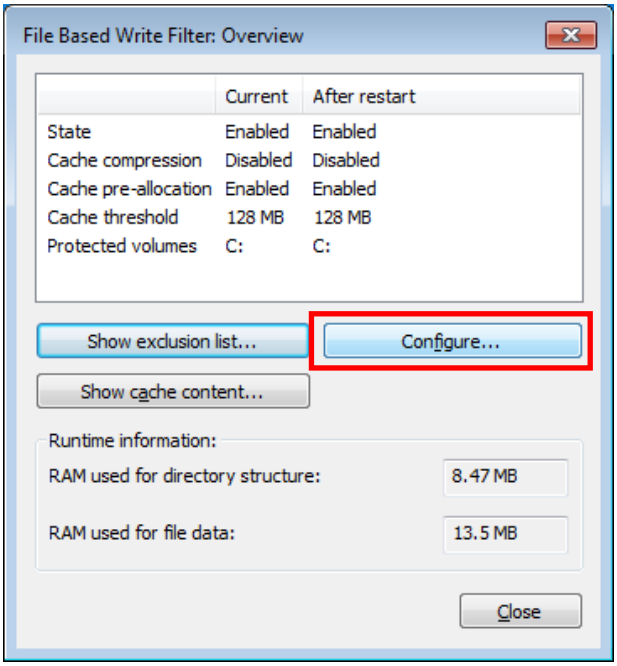


Excluding Files from FBWF Protection

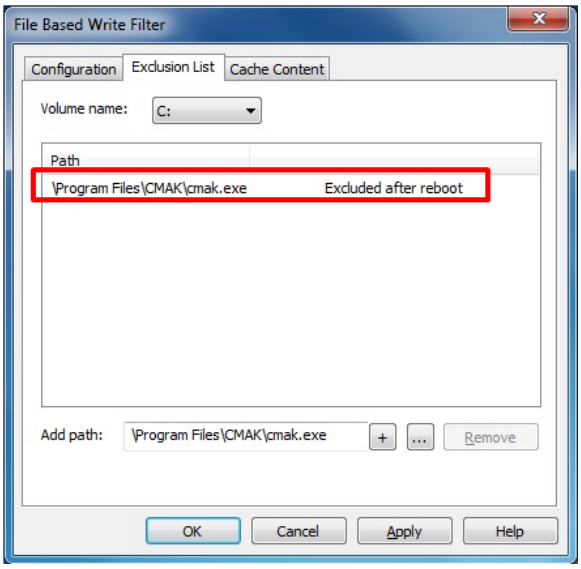
1. Double-click the FBWF icon in the system tray.

   You may need to show hidden icons in the system tray.

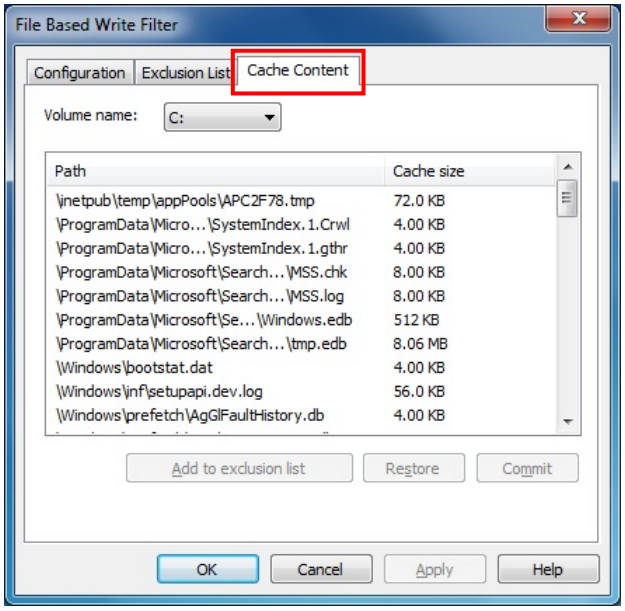
2. In the **File Based Write Filter:** Overview window, click **Configure**.



3. Click the **Exclusion List** tab and configure the following fields:
   - **Volume name** – Select a drive volume from the drop-down list.
   - **Add path** – click the ellipsis (**...**) button to select a directory or file you want to exclude from FBWF protection; then click the **+** button. The system displays the selected directory or file in the **Path** table.



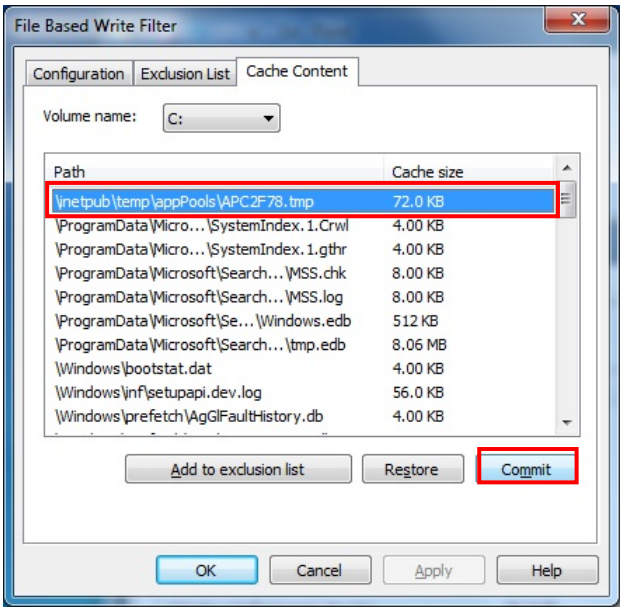
4. Click the **Cache Content** tab and click **Apply** and **OK**



5. Reboot the system to make the changes take effect.

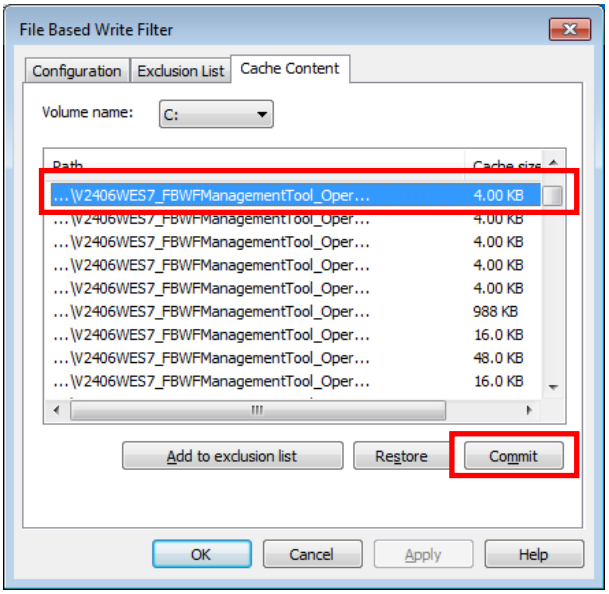
Managing Temporary Files Cached in the Overlay

1. On the **Cached Content** tab, you will see all the files currently cached in the RAM overlay. Three commands are available:
   - **Commit**: Save a file from the cache to permanent storage, delete the file from the overlay, and overwrite the original file.
   - **Restore**: Return the file to its original state, remove the file from the overlay cache and discard the changes that added the file to the cache.
   - **Add to exclusion list**: Adds the file to the exclusion list after the next restart. This will delete the file from the cached overlay and replace the current file in permanent storage with the modified cache file.



2. The most common usage of the Cache Content filter will likely be to permanently write content to the hard drive. To do this, select the file you wish to write to permanent memory and click on the **commit** button. This will delete the file from the cached overlay and replace the current file in permanent storage with the modified cache file.

   Keep in mind that committing a configuration or application file will permanently alter the setup and/or performance of the application or system.



For more details about FBWF configuration and usage, refer to the Microsoft help file that came with your computer, or go to the following websites:

- Microsoft's FBWF Installation and Configuration help pages.
- Microsoft's FBWF overview on the official Microsoft FBWF help pages.
- Microsoft's detailed description of FBWF features on the FBWF help pages.
- Microsoft's detailed description of the FBWF API.

5

Examples

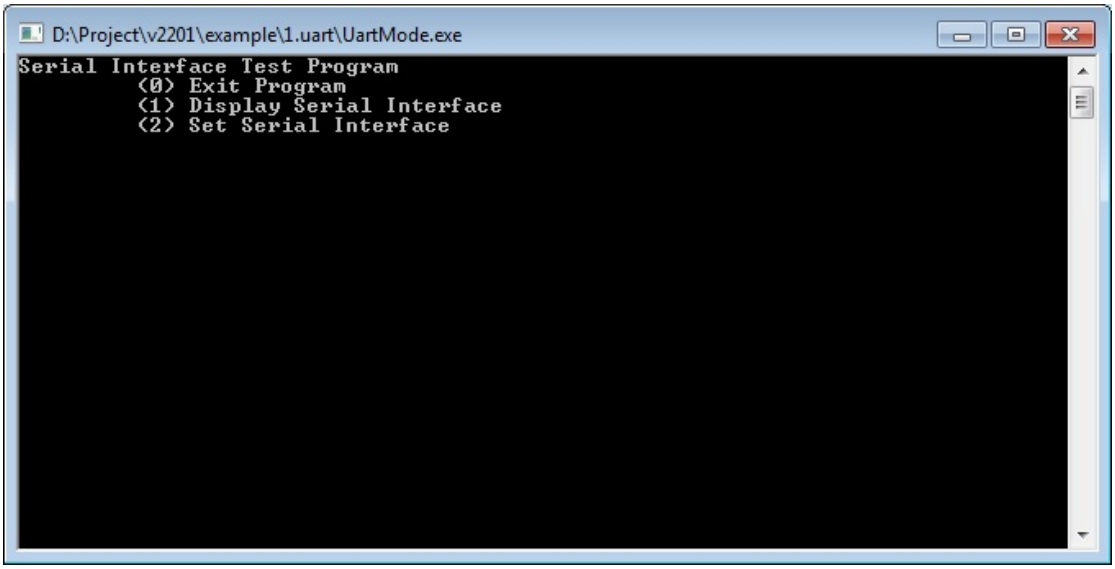
This chapter provides examples to illustrate how to use the V2201 computer for a variety of applications.

The following topics are covered in this chapter:

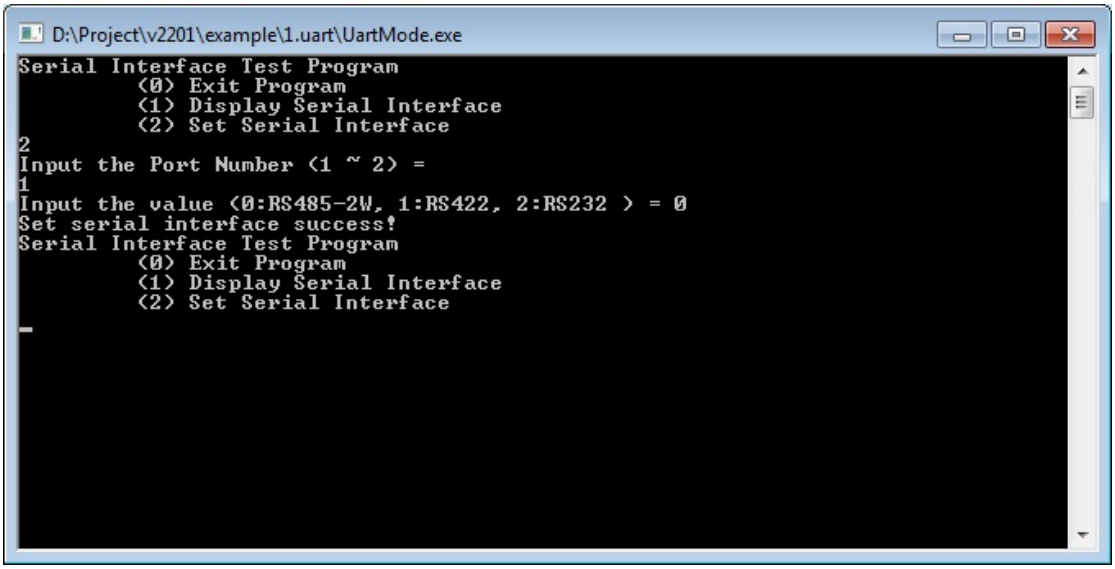
- **Serial Interface**
- **Digital Input/Output**
- **Watchdog**
- **LED**
- **Power Control**
- **Power Reset**

Serial Interface

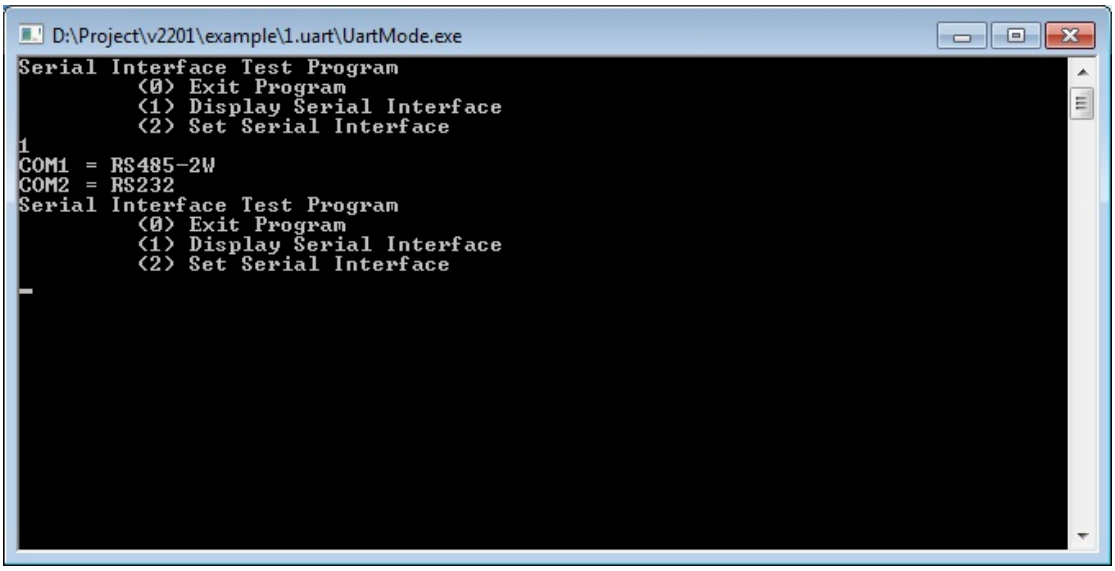
1. Copy the following files from the software CD/DVD to a folder on the V2201.
   - **mxsp.dll:** \examples\V2201-W7E-example\3.lib\mxsp\x64\
   - **sysinfo.dll:** \examples\V2201-W7E-example\3.lib\mxsp\x64\
   - **sysinfo.sys:** \examples\V2201-W7E-example\3.lib\mxsp\x64\
   - **sysinfoX64.sys:** \examples\V2201-W7E-example\3.lib\mxsp\x64\
   - **mxGeneralIo.dll:** \examples\V2201-W7E-example\3.lib\MxGeneralIo\x64\
   - **UartMode.exe:** \examples\V2201-W7E-example\Release\x64\
2. Execute **UartMode.exe**.



3. Type **2** to set the serial interface, and then follow the on-screen instructions.

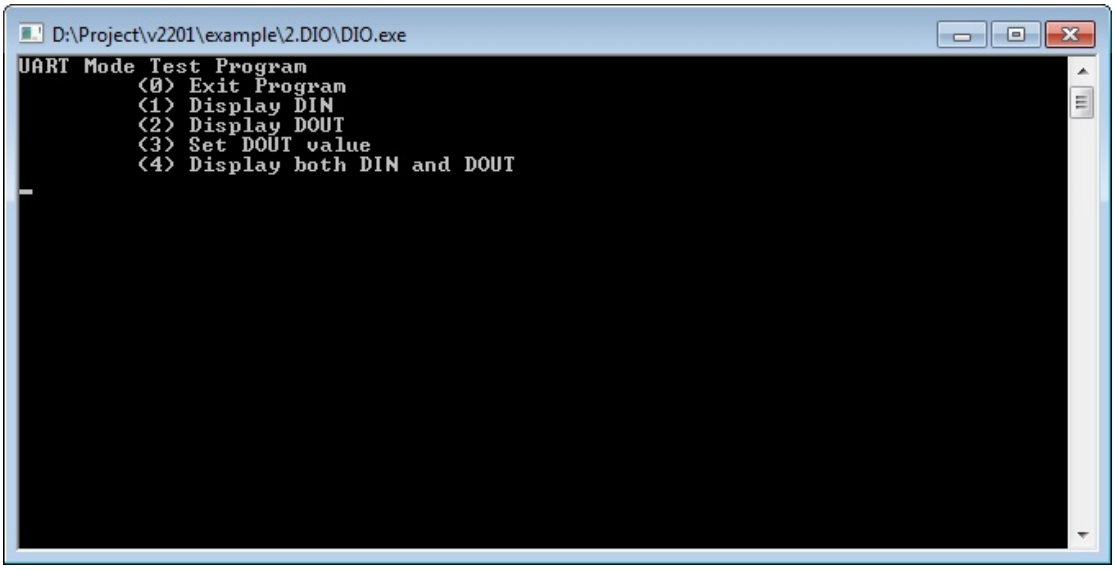


4. Type **1** to display the current serial interface settings.

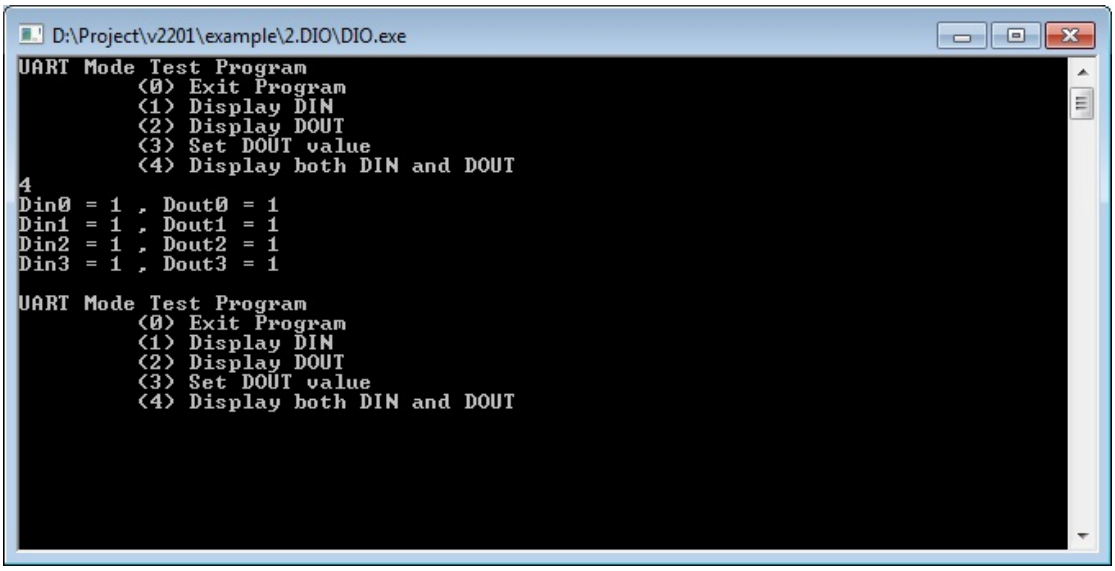


Digital Input/Output

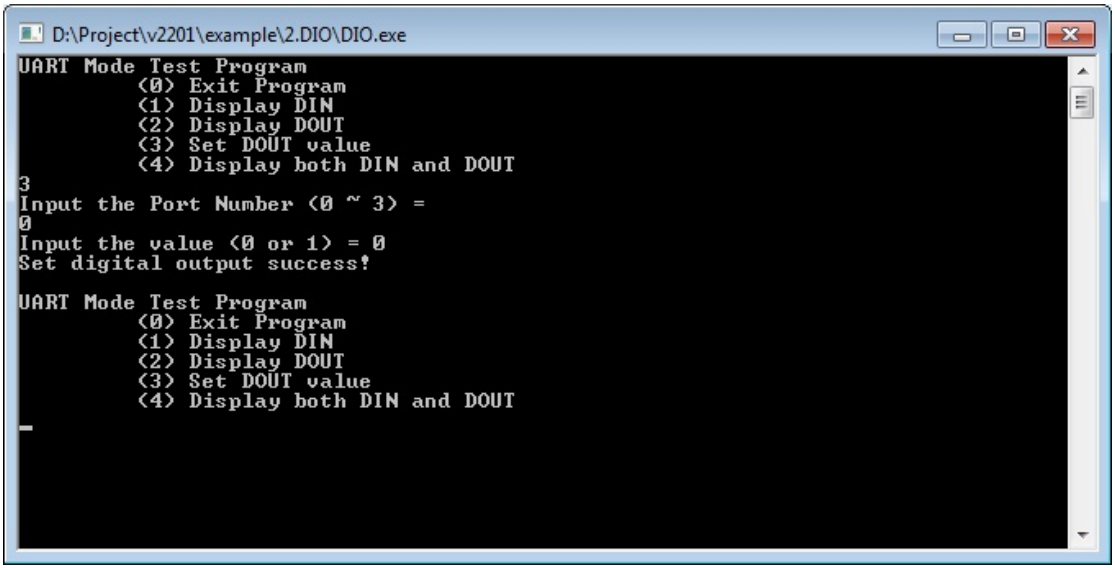
1. Copy the following files from the software CD/DVD to a folder on the V2201.
   - **mxdgio.dll:** \examples\V2201-W7E-example\3.lib\mxdgio\x64\
   - **mxGeneralIo.dll:** \examples\V2201-W7E-example\3.lib\MxGeneralIo\x64\
   - **DIO.exe:** \examples\V2201-W7E-example\Release\x64\
2. Execute **DIO.exe.**



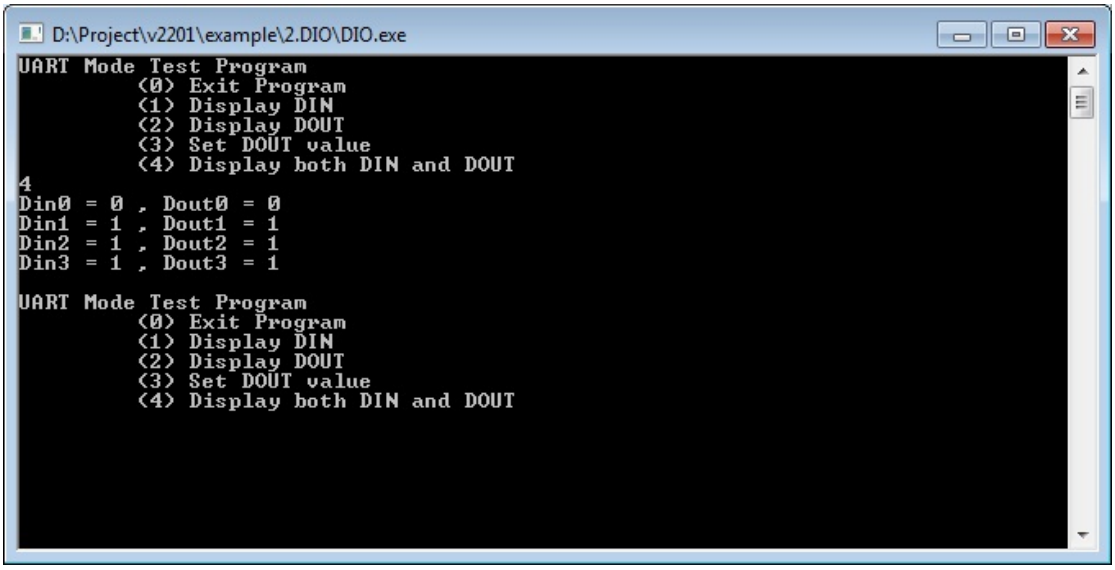
3. Type **4** to display the current DI and DO values.



4. Type **3** to set the DOUT port number, and then follow the on-screen instructions.

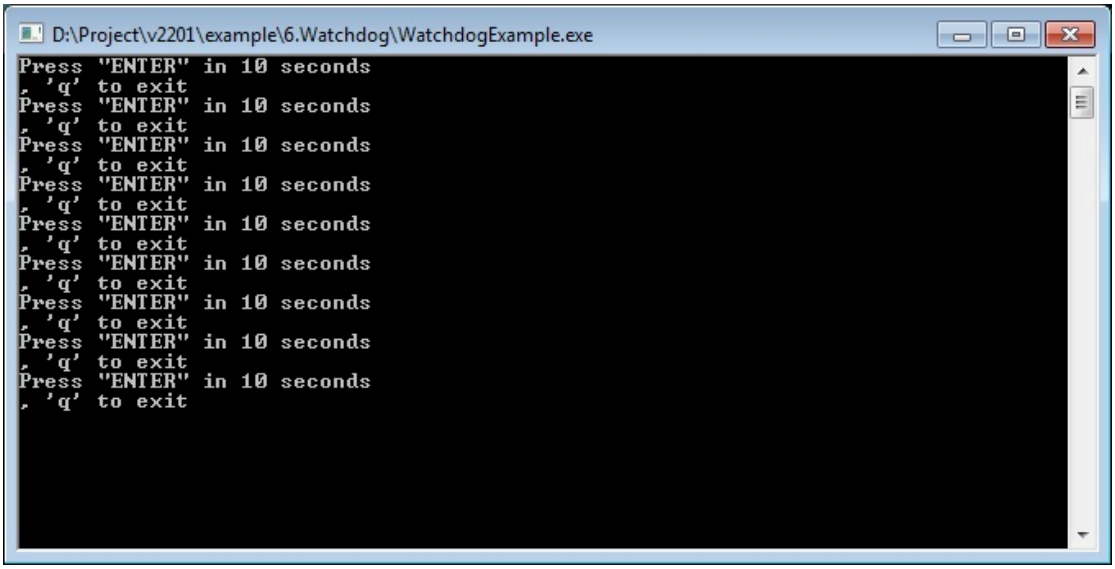


5. Type **4** to check if the port value was set correctly.



Watchdog

1. Copy the following files from the software CD/DVD to a folder on the V2201.
   - **mxdwg.dll:** \examples\V2201-W7E-example\3.lib\mxdwg\x64\
   - **mxGeneralIo.dll:** \examples\V2201-W7E-example\3.lib\MxGeneralIo\x64\
   - **Watchdog.exe:** \examples\V2201-W7E-example\Release\x64\
2. To prevent the system from rebooting, press [Enter] at least once every 10 seconds; otherwise, the system will reboot automatically.

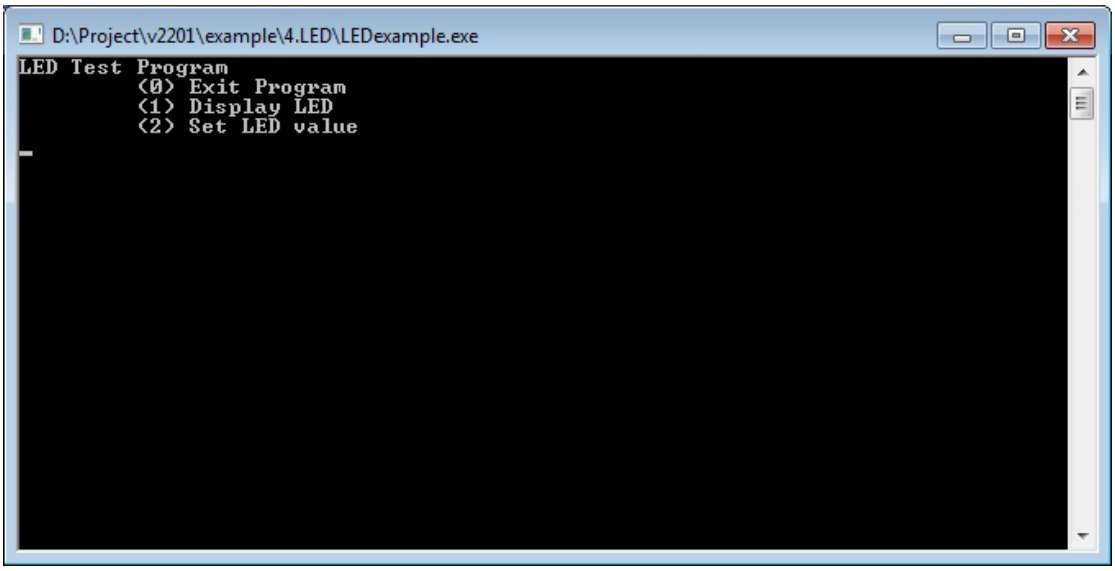


3. To stop the watchdog, press **q** to exit the program

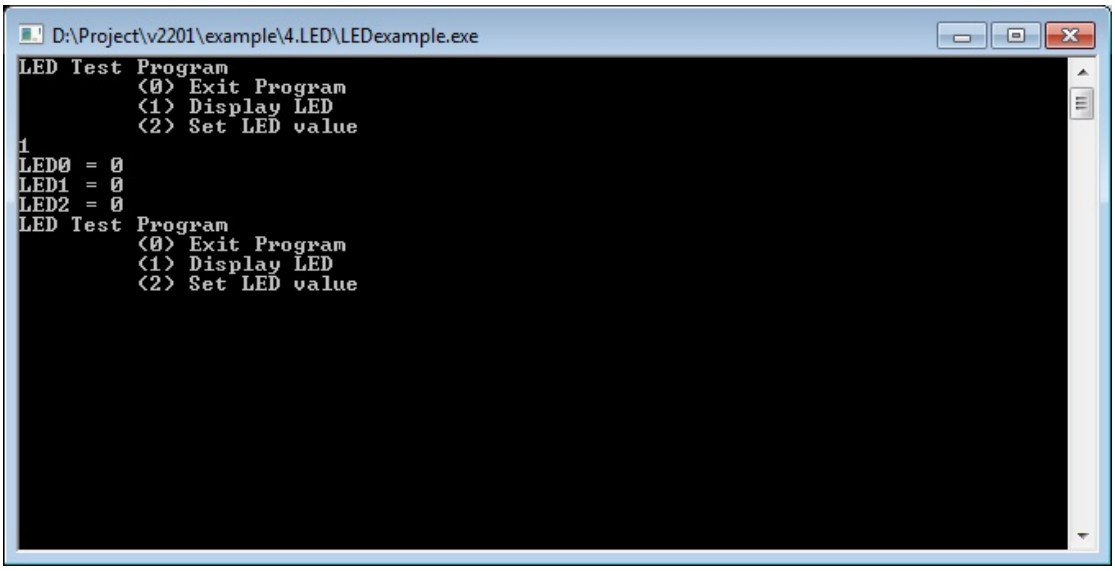
LED

In this section we illustrate how to use the test utility to display and set LED values.

1. Copy the following files from the product software DVD.
   - **mxgpio.dll:** \examples\V2201-W7E-example\3.lib\mxgpio\x64\
   - **mxGeneralIo.dll:** \examples\V2201-W7E-example\3.lib\MxGeneralIo\x64\
   - **LED.exe:** \examples\V2201-W7E-example\Release\x64\
2. Execute **LED.exe**.



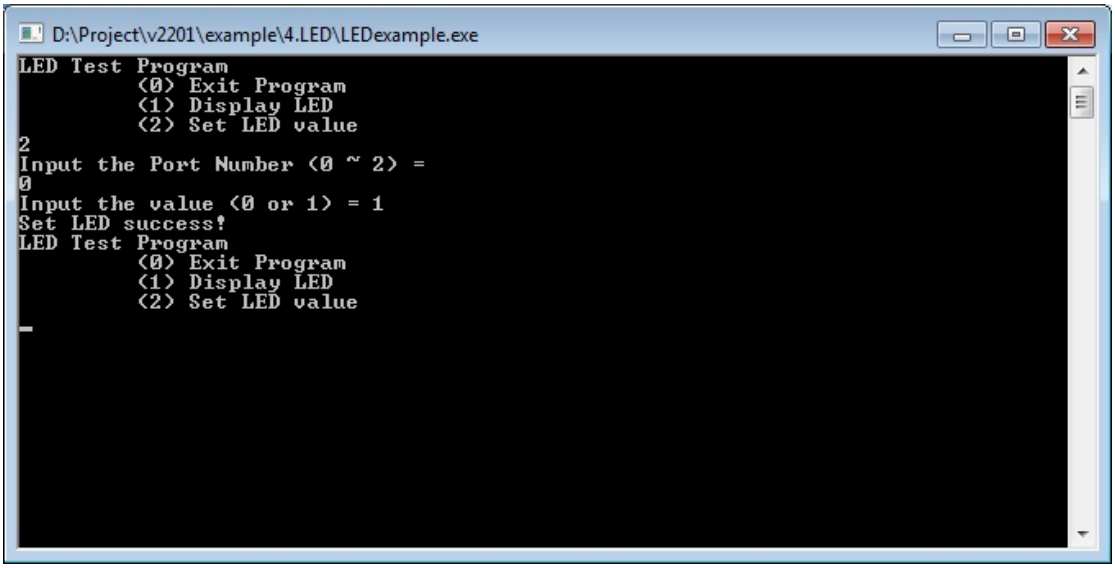
3. Type **1** to display the current LED value.



4. Type **2** and follow the on-screen instruction to set the LED value.

   When you set the LED value to 0, the LEDs turn off.

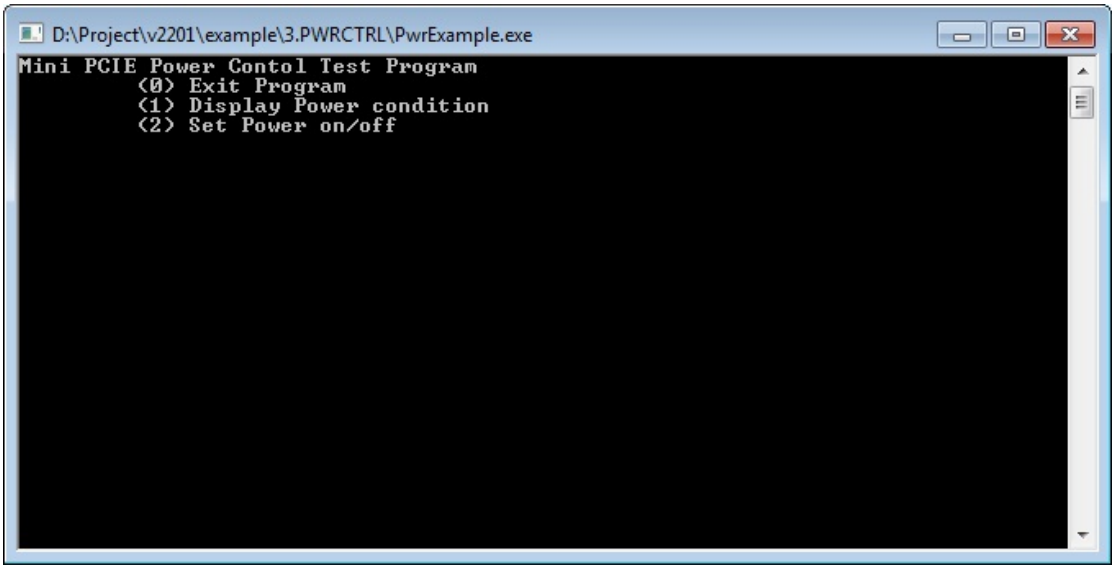
   When you set the LED value to 1, the LEDs turn on.



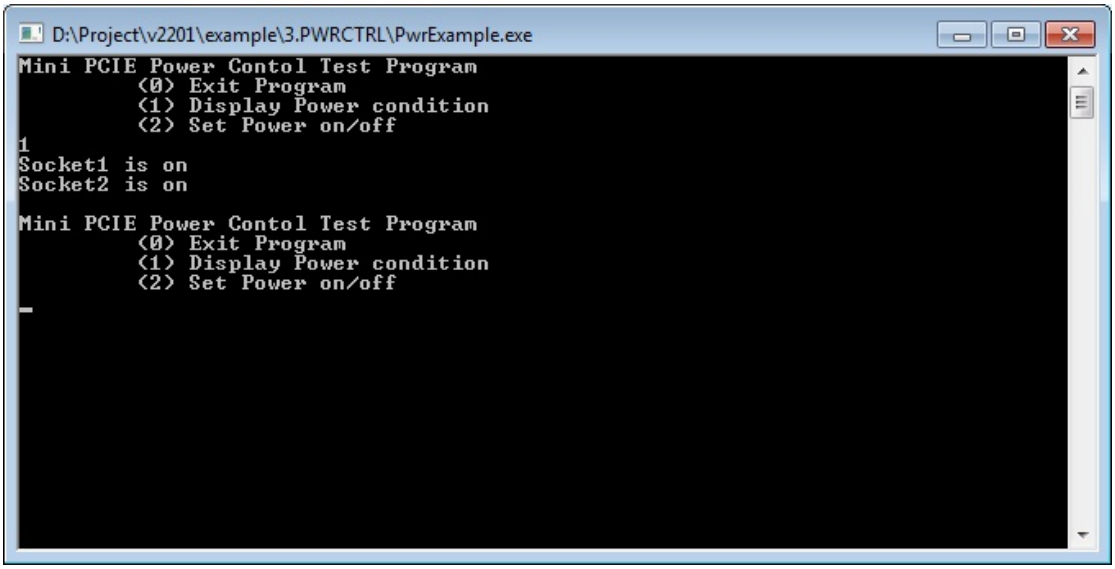
Power Control

In this section, we illustrate how to use the test utility to control power through the mini-PCIE interface.

1. Copy the following files from the product software DVD.
   - **mxgpio.dll:** \examples\V2201-W7E-example\3.lib\mxgpio\x64\
   - **mxGeneralIo.dll:** \examples\V2201-W7E-example\3.lib\MxGeneralIo\x64\
   - **PwrExample.exe:** \examples\V2201-W7E-example\Release\x64\
2. Execute **PwrExample.exe**.

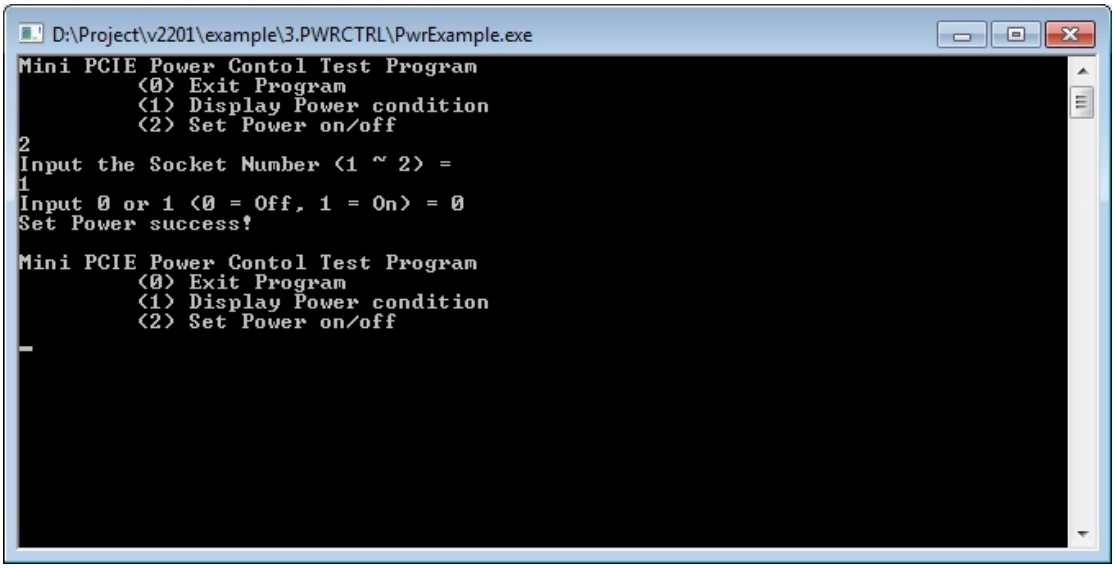


3. Type **1** to display the current power status.



4. Type **2** and follow the on-screen instructions to set the power value.

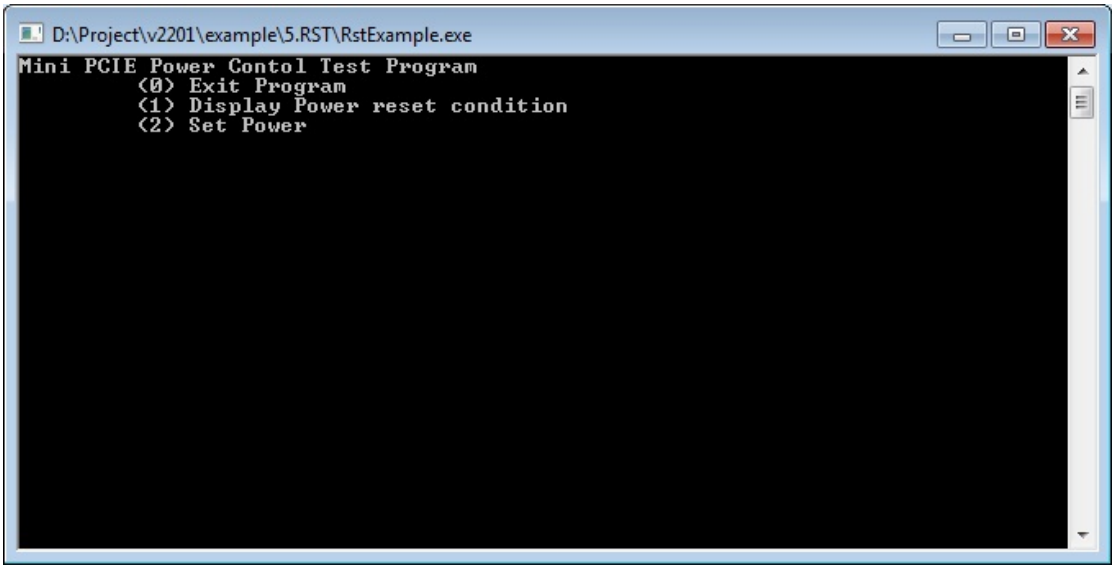
   When you set the power value to 0, the power turns off.
   When you set the power value to 1, the power turns on.



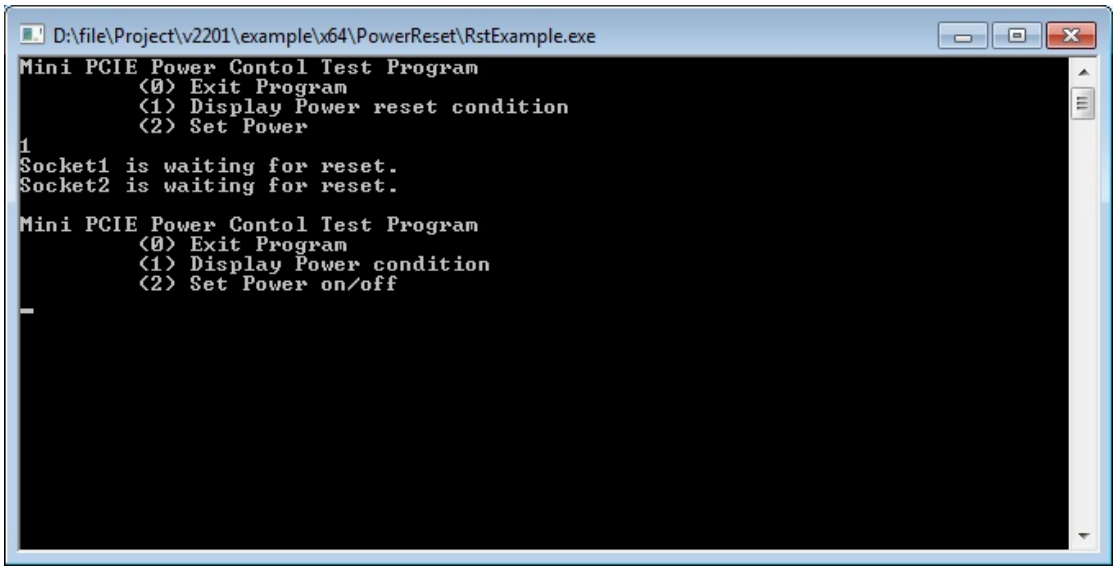
Power Reset

In this section, we illustrate how to use the test utility to reset the power through the mini-PCIE interface.

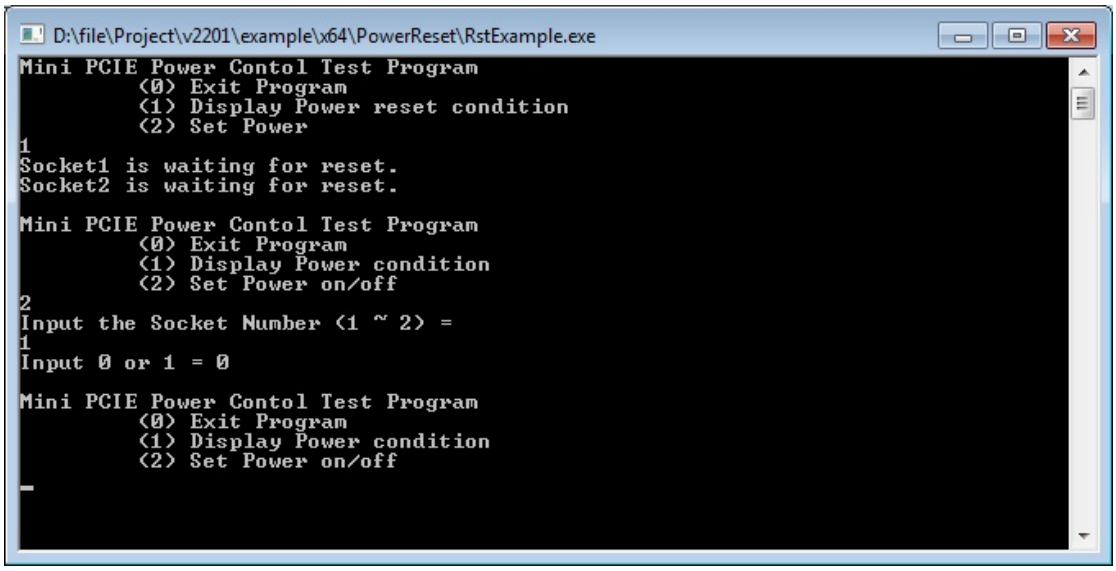
1. Copy the following files from the product software DVD.
   - **mxgpio.dll:** \examples\V2201-W7E-example\3.lib\mxgpio\x64\
   - **mxGeneralIo.dll:** \examples\V2201-W7E-example\3.lib\MxGeneralIo\x64\
   - **RstExample.exe:** \examples\V2201-W7E-example\Release\x64\
2. Execute **RstExample.exe**.



3. Type **1** to display the current power reset status



4. Type **2** and follow the on-screen instructions to set the reset pin.



6

Module Card

In this chapter we discuss installation and usage of the software utility.

The following topics are covered in this chapter:

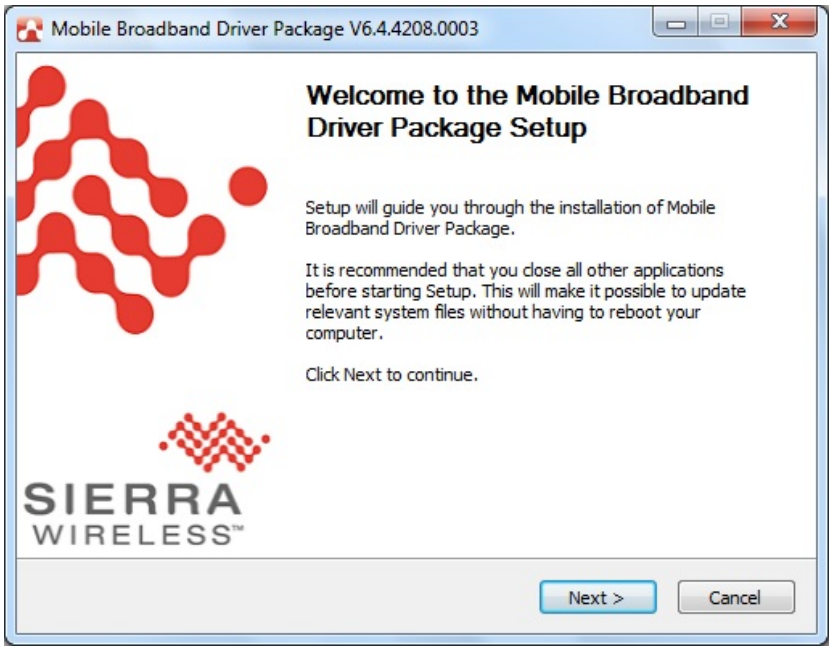
- **Overview**
- **Installing the Cellular Module Driver for the MC-9090, MC-7304, and MC-7354**
- **Installing the Cellular Module Dial Utility**
- **Cellular Module Configuration**
- **Installing the WiFi Module Driver for the WPEA-252NI**
- **WiFi Module Configuration**
- **Choosing the Gateway when WiFi and Cellular are Connected at the Same Time**

Overview

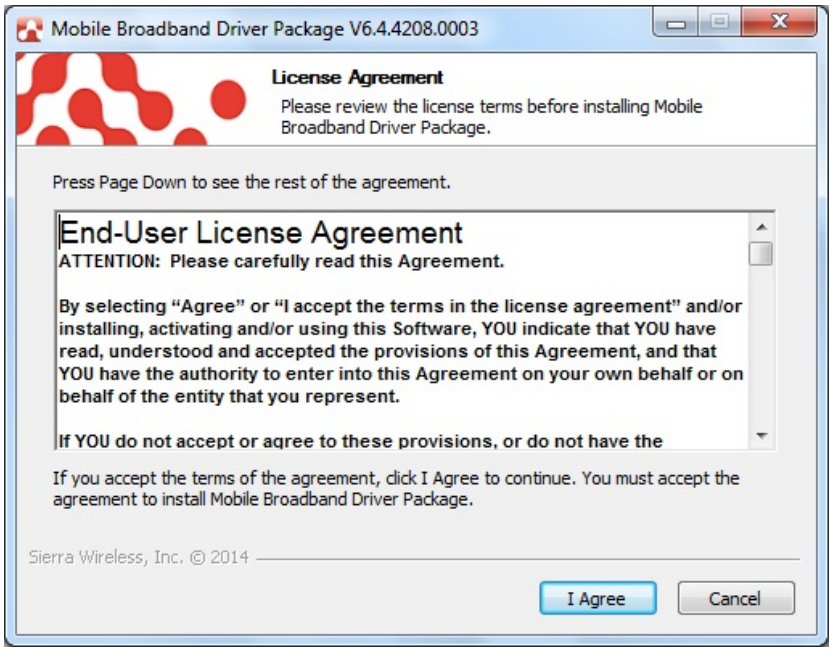
Moxa provides drivers and utilities for the MC-9090, MC-7304, and MC-7354 cellular modules, and WPEA-252NI Wi-Fi modules. All of the drivers and utilities are pre-tested with the V2201. The relevant files are located in \driver\V2201-W7E_V1.0_Expansion_Module.

Installing the Cellular Module Driver for the MC-9090, MC-7304, and MC-7354

1. Run **driver\V2201-W7E_V1.0_Expansion_Module\x64\Modules\MC-9090\Build4208.exe** to begin installation and then click **Next**.

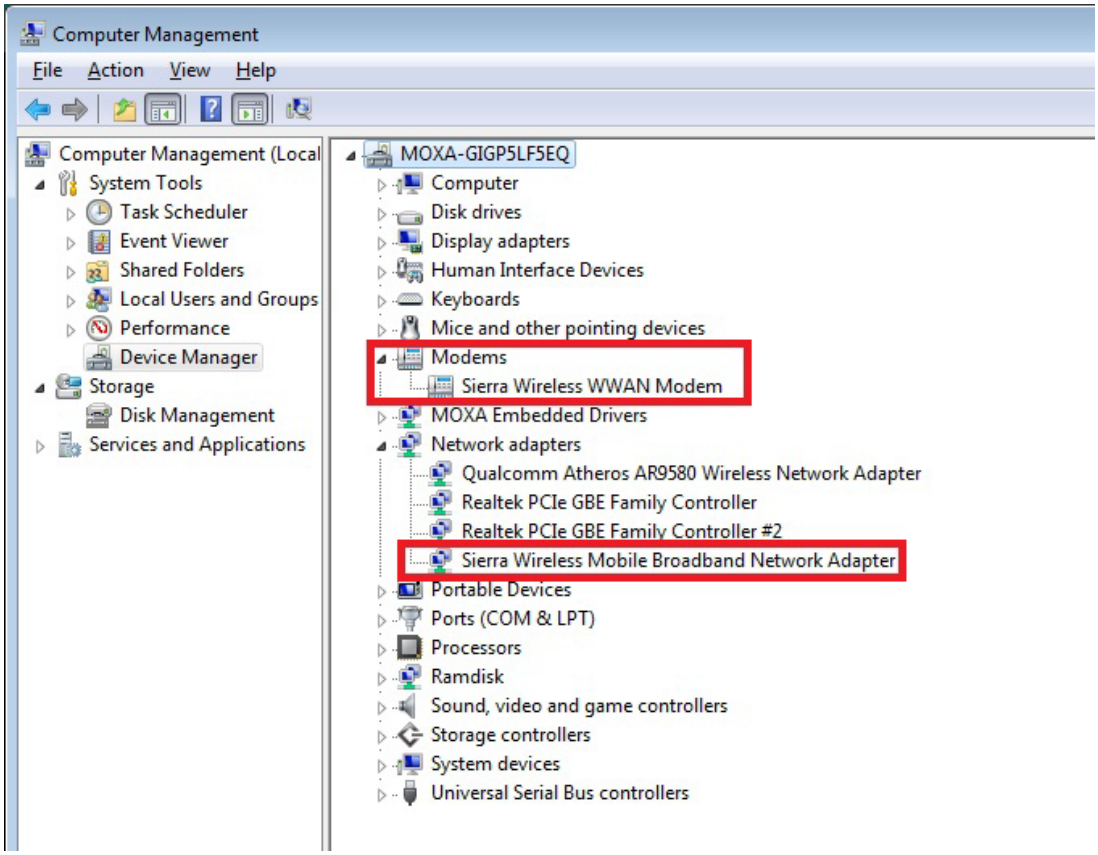


2. Click **I Agree** to accept the license.



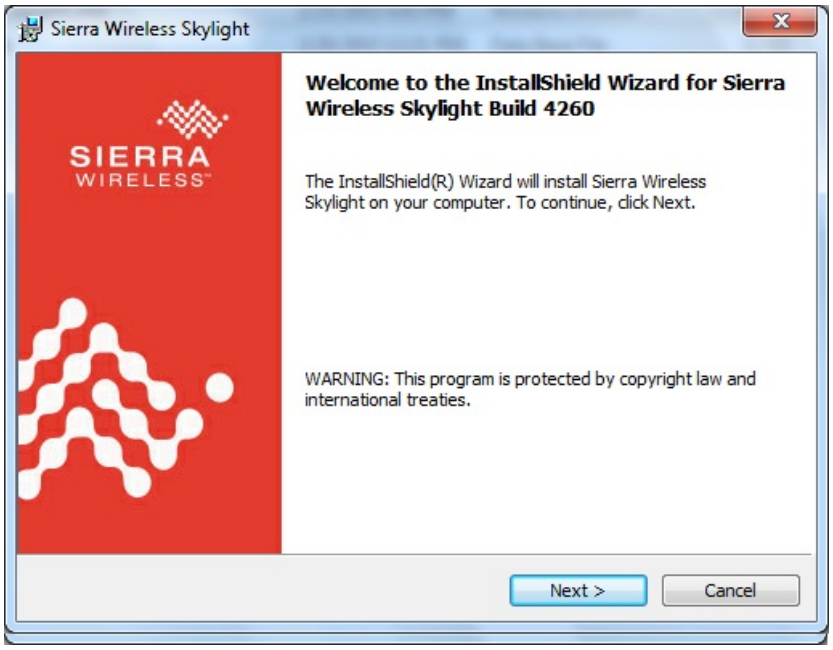
3. Click **Finish** to complete installation.

4. The system should locate the new hardware and install the driver automatically. Check **Windows Device Manager** to verify.

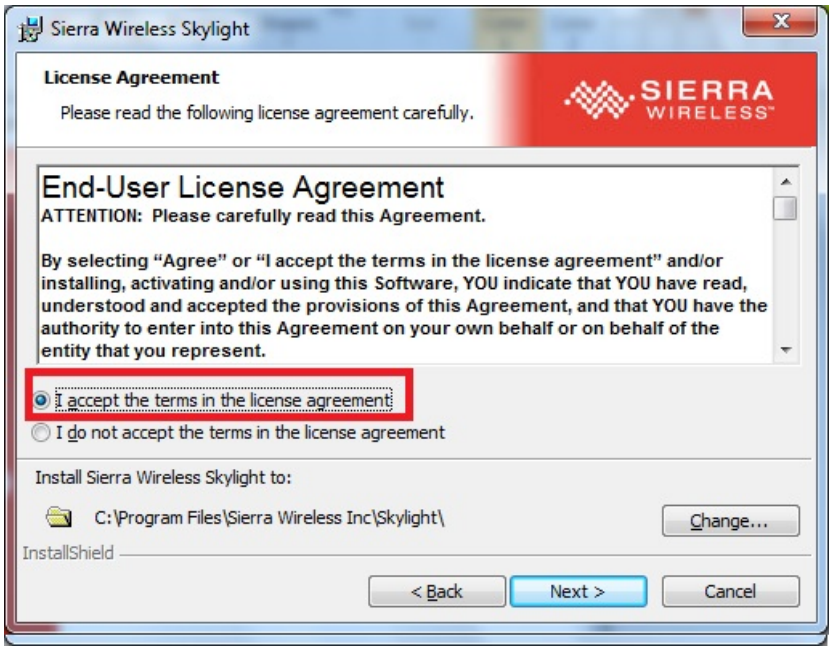


Installing the Cellular Module Dial Utility

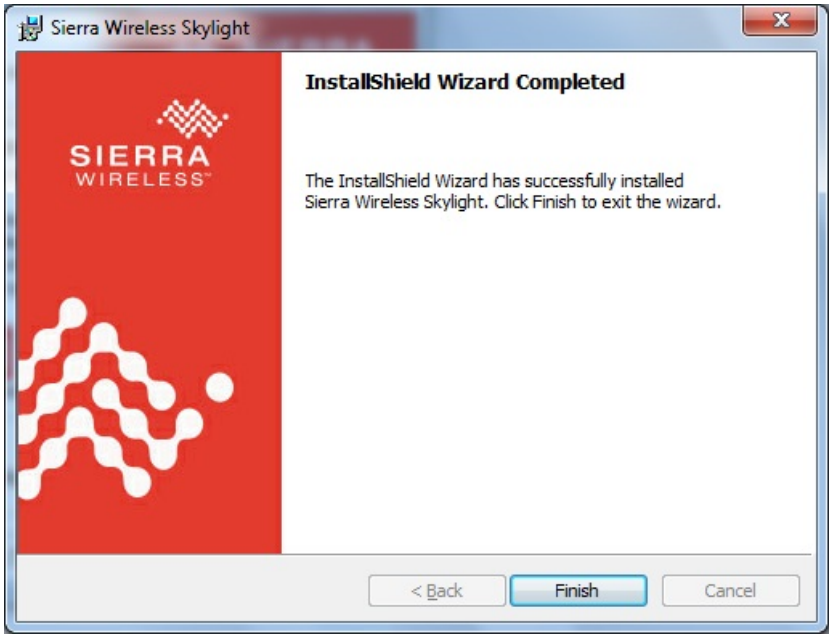
1. Run **\driver\V2201-W7E_V1.0_Expansion_Module\x64\Modules\MC-9090\Build4260\Skylight64_Generic.msi** to begin installation and then click **Next**.



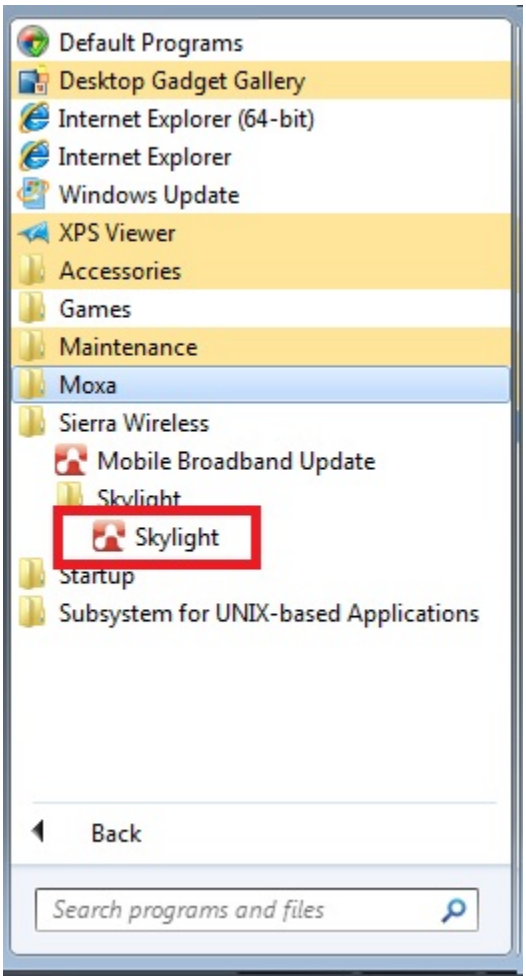
2. Check **I accept the terms in the license agreement** and then click **Next**.



3. Click **Finish** to complete the installation.



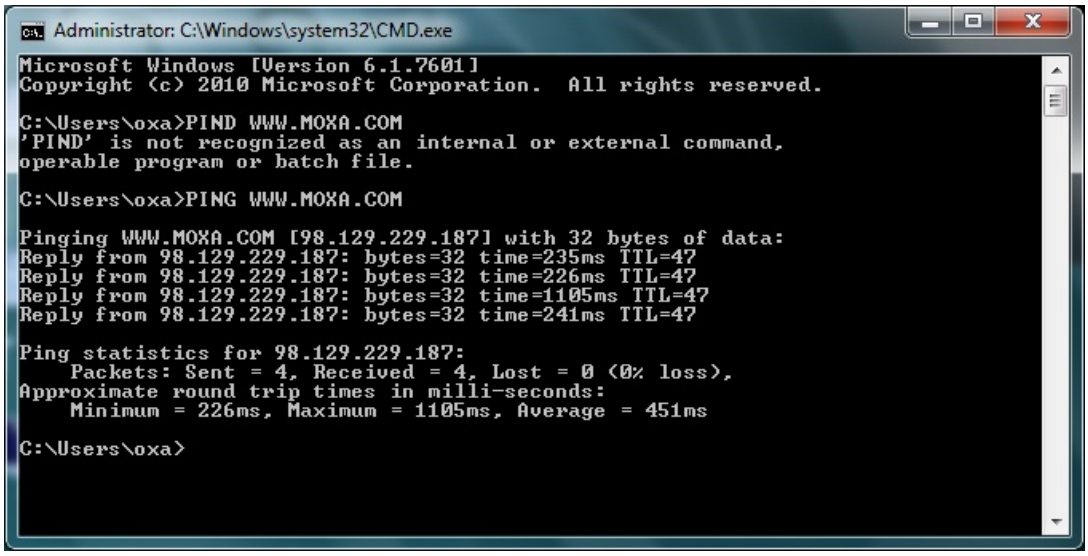
4. The system should locate the new hardware and install the driver automatically. Check **Skylight** under **Sierra Wireless** to double check.



Cellular Module Configuration

1. After installing the cellular module driver and utility, if you want to establish a cellular connection, start **Skylight** and click **Connect**.

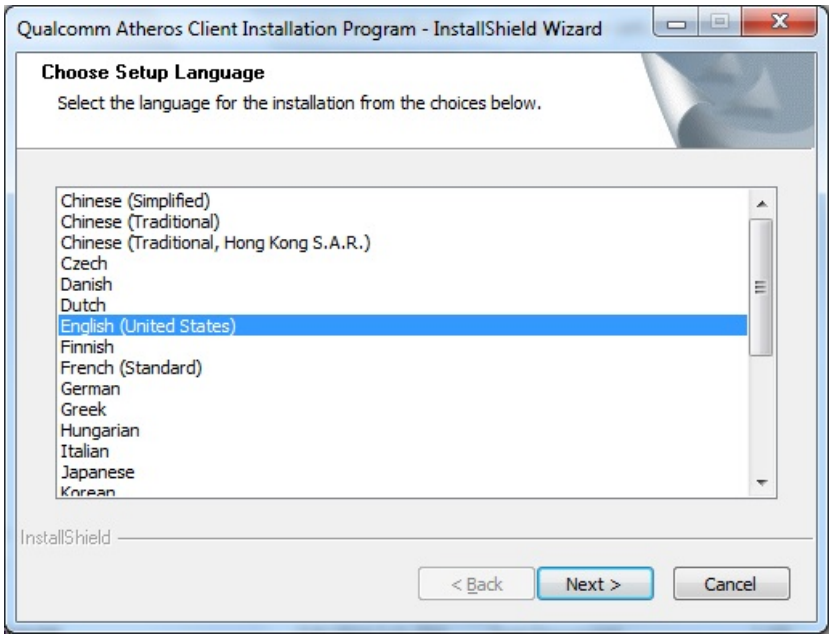
2. You can verify the cellular connection by pinging the interface once the connection is established.



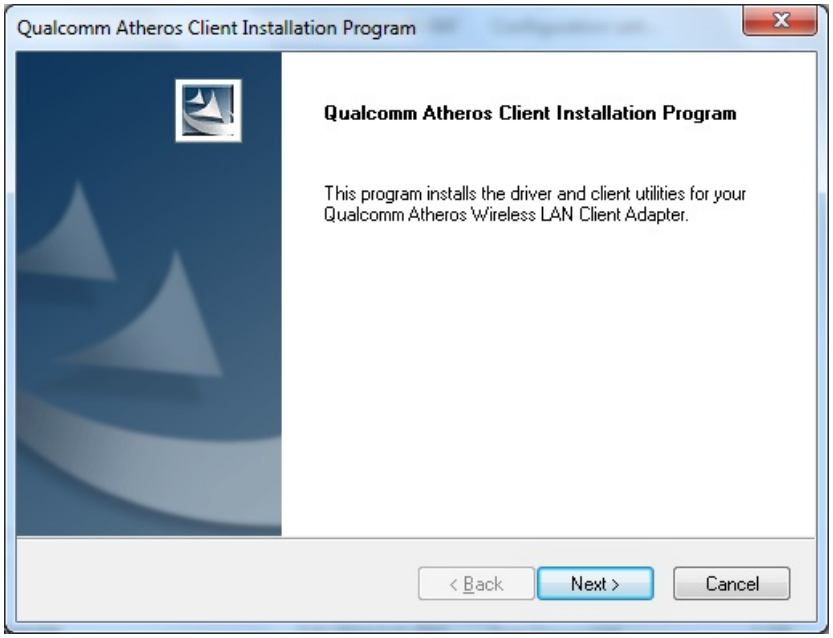
3. If you want to interrupt the cellular connection, click **Disconnect**.

Installing the WiFi Module Driver for the WPEA-252NI

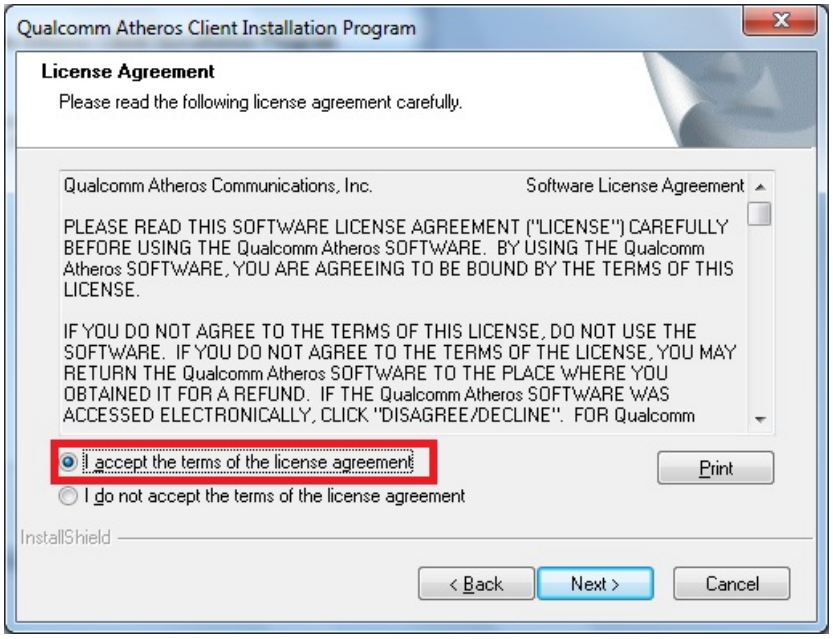
1. Run **driver\V2201-W7E_V1.0_Expansion_Module\x64\Modules\WPEA-252NI\Install_CD\setup.exe** to begin the installation.
2. Select which language you would like to use and then click **Next**.



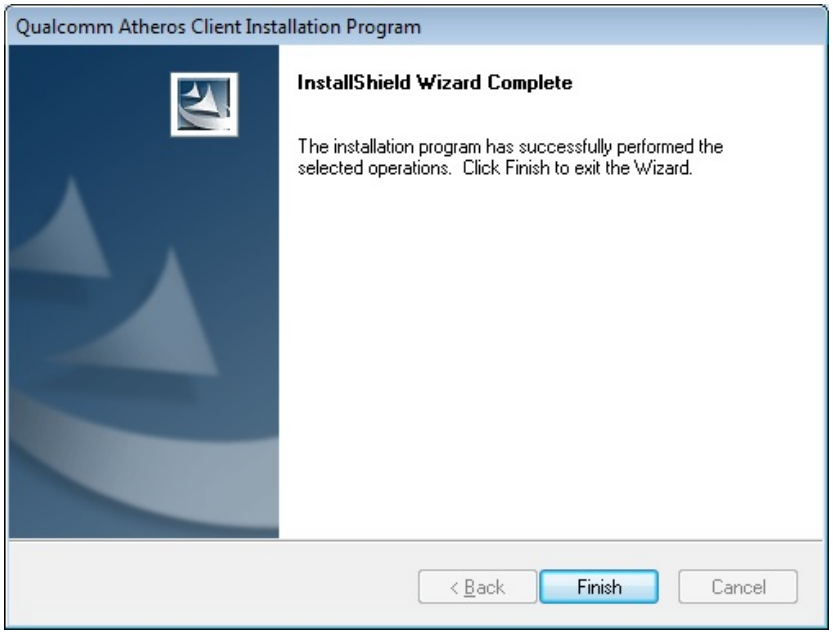
3. Click **Next**.



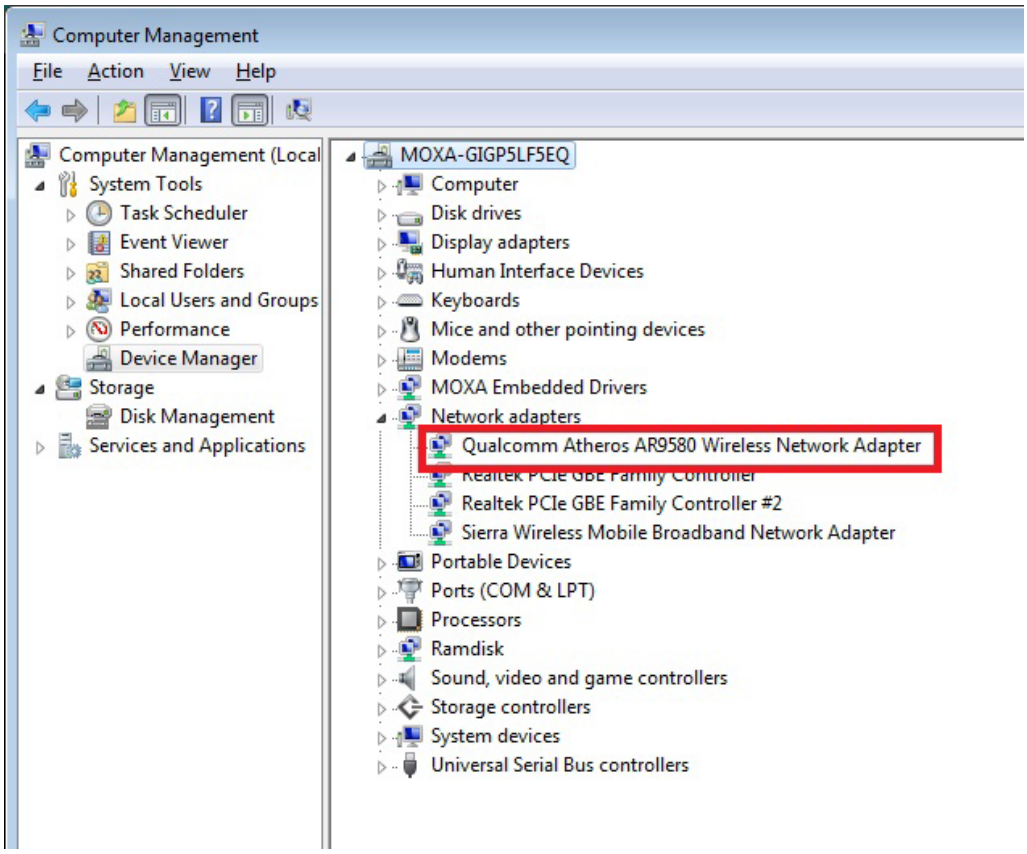
4. Check **I accept the terms of the license agreement** and click **Next**.



5. Click **Finish** to complete the installation.

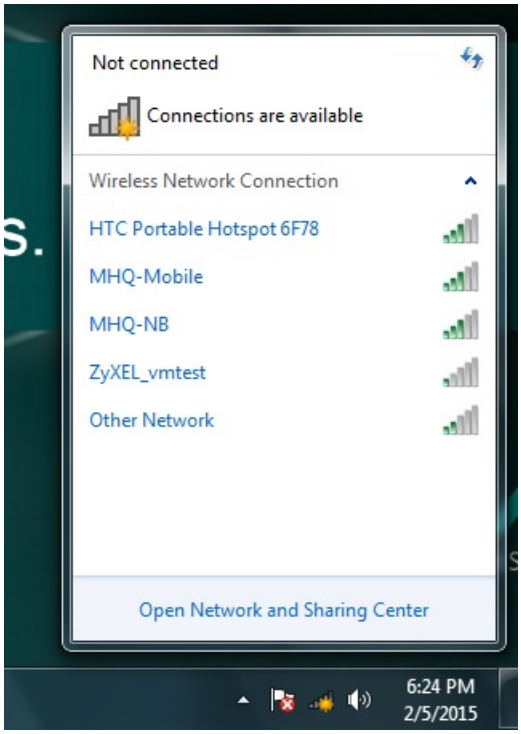


6. The system should locate the new hardware and install the driver automatically. Check **Windows Device Manager** to verify.



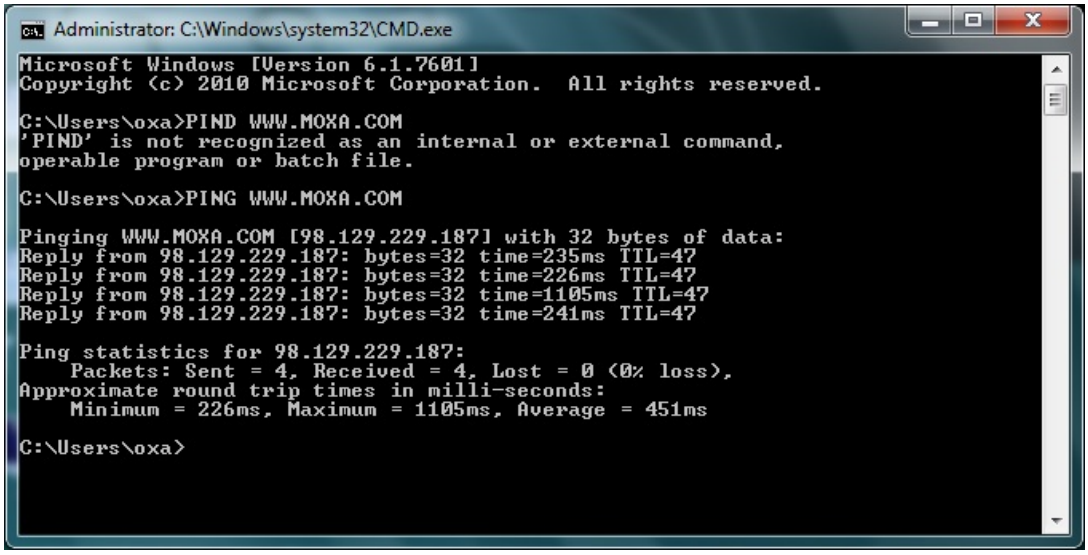
WiFi Module Configuration

1. After installing the WiFi module driver, select wireless network connection from the taskbar.



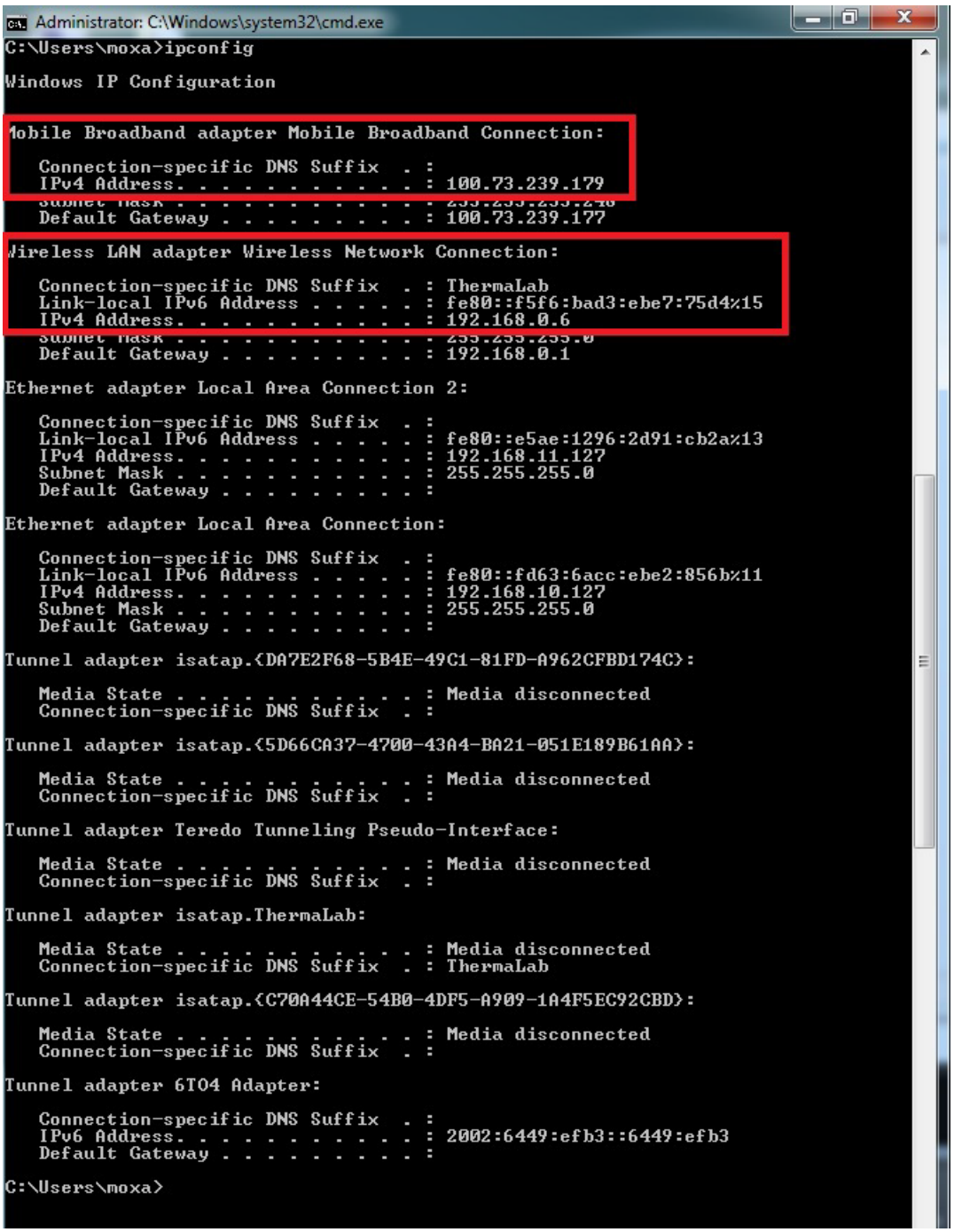
2. Enter the password to connect to the network.

3. You may verify the cellular connection by pinging the interface once the connection is established.

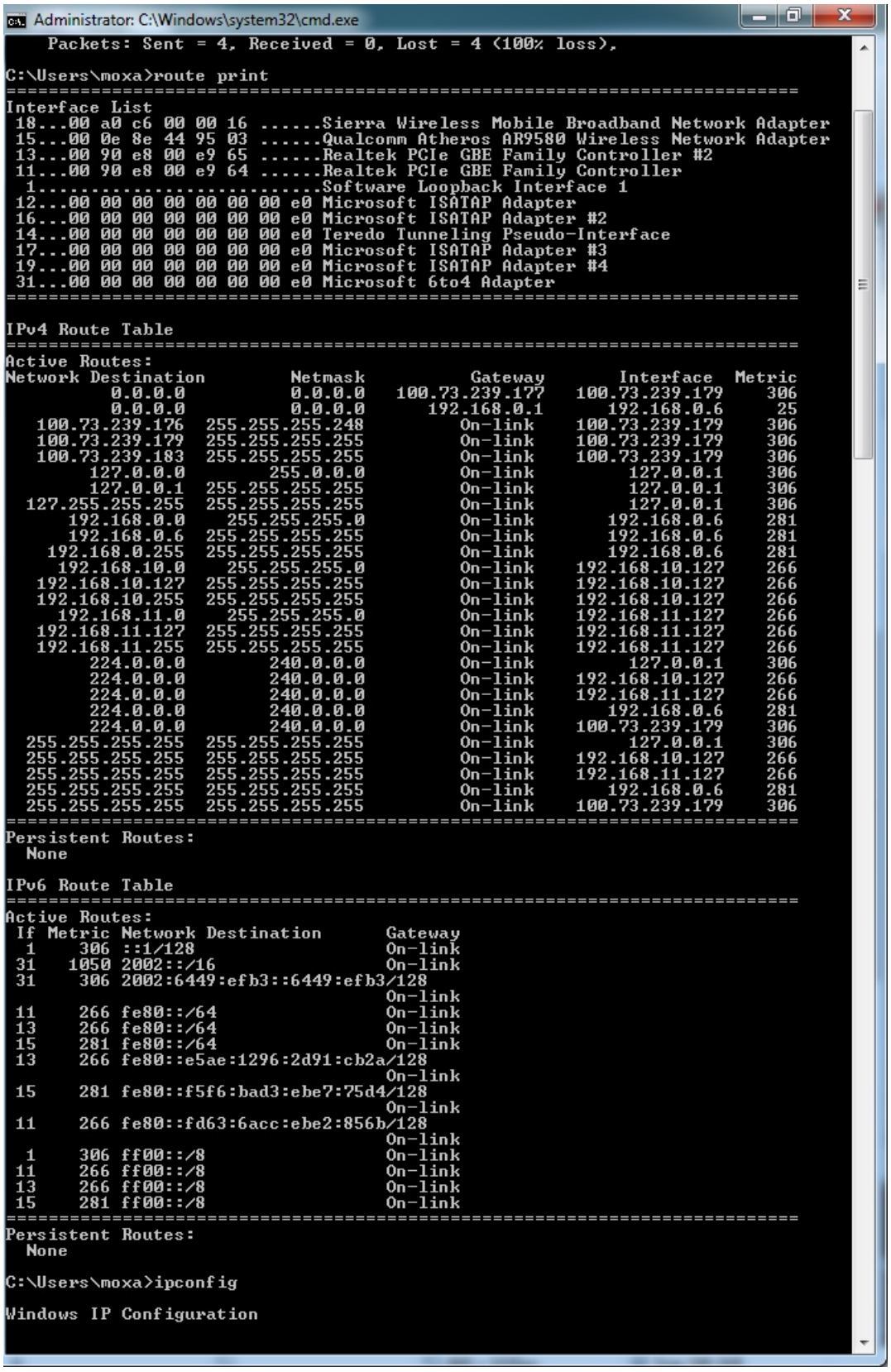


Choosing the Gateway when WiFi and Cellular are Connected at the Same Time

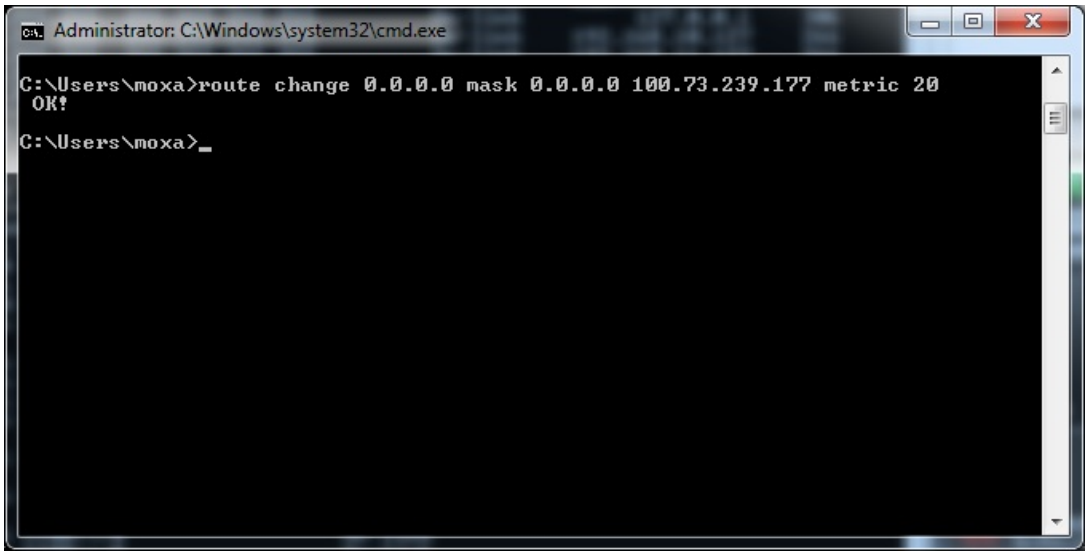
1. Open the **Start Menu** and type **cmd** in the Start Menu search box.
2. Click cmd from the search results, which should appear directly under Programs.
3. When the Command Prompt window opens, type **ipconfig** in the command prompt window to display the IP addresses of the WiFi connection and cellular connection. In the example shown below, the IP address of the WiFi connection is **192.168.0.6**, and the IP address of the cellular connection is **100.73.239.179**.



4. Windows 7 will choose the lowest Metric value for the connection interface if there are several routes with the same network destination and netmask. In this case, the WiFi interface is the connection interface.



5. If you want to change to using cellular as the connection interface, just reduce the Metric value of the cellular interface so that the value is less than the WiFi's Metric value.



7

System Recovery

This chapter describes the system recovery process that you can perform if the system is not functioning properly.

The following topics are covered in this chapter:

- **Overview**
- **Setting Up the Recovery Environment**
- **Setting Up a Factory Default Recovery Image**
  - Step 1: Prepare the USB drive
  - Step 2: Setting the BIOS to Boot via USB
  - Step 3: How to Perform a System Recovery
  - Step 4: Reset the BIOS to its Original State
- **Creating a Custom System Image**

Overview

This section describes how to prepare your computer for recovery in the event the system becomes unstable. You can perform a system recovery using one of the following system images:

- A clean factory default image.
- A user-generated image created from a fully configured, fully set up system.

Before you perform a system recovery, set up the system environment.

Setting Up the Recovery Environment

To set up the recovery environment on a V2201 computer, prepare a USB drive that has at least 4 GB of memory and a copy of the recovery suite.

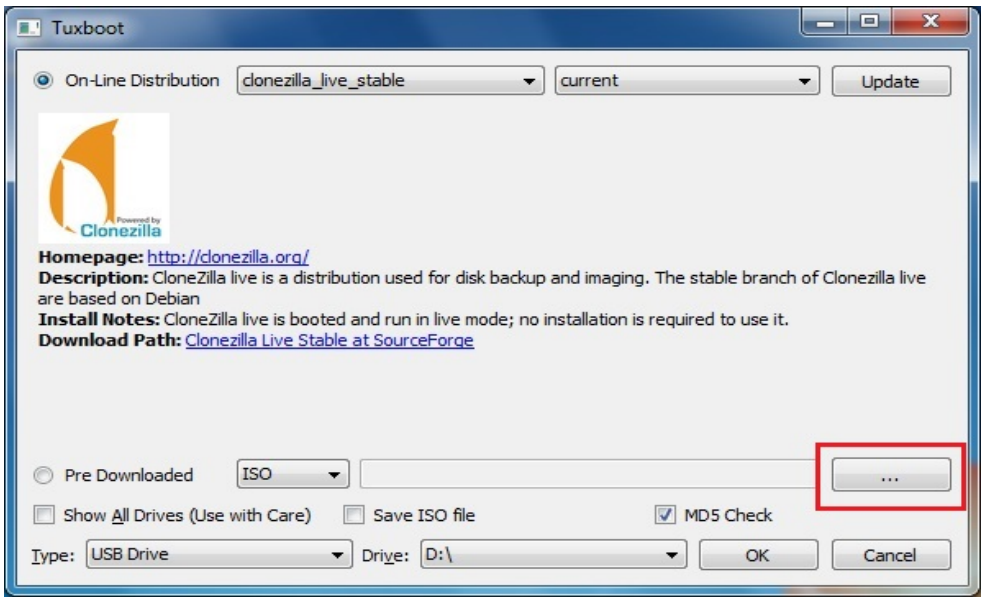
The following lists the major steps in the recovery procedure:

1. Copy the recovery programs and system image file on to the USB drive. Set up the drive as a live-drive system with an ISO image of the boot environment.
2. Reboot the system and configure the BIOS to boot the recovery system from the USB port.
3. An image of the current software system will be created on the USB drive. The recovery environment will use this image when restoring the system.
4. Reboot the system again and the BIOS will return to its original state.

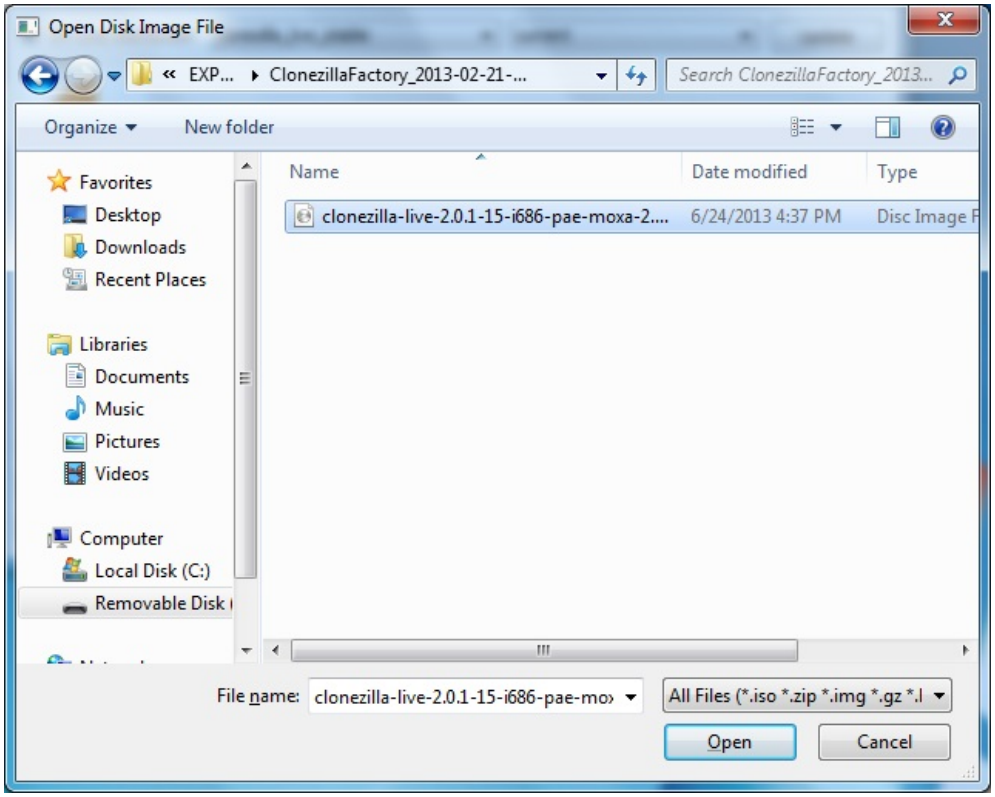
Recovery Procedure

Step 1: Prepare your USB drive

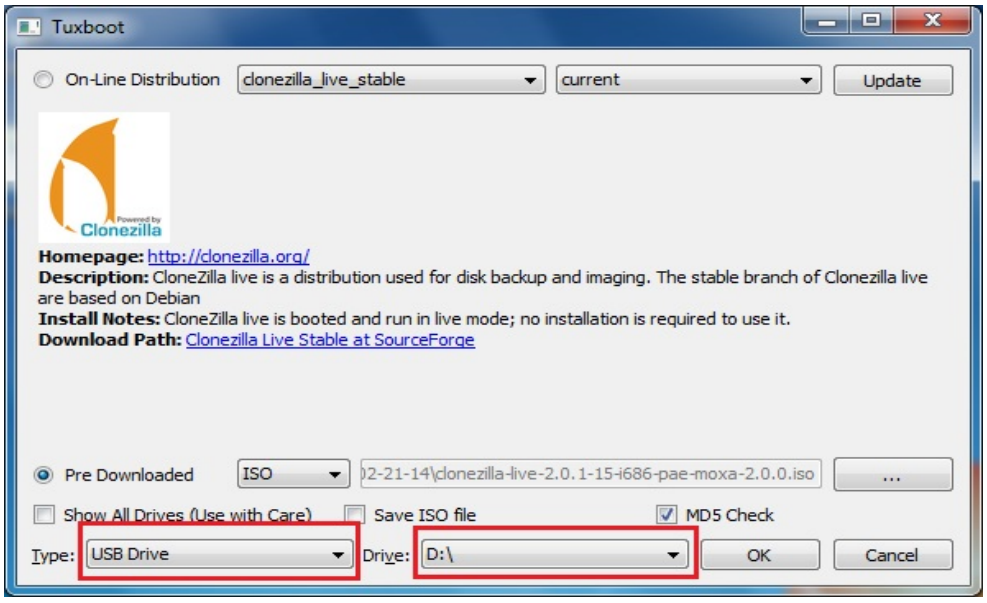
1. Execute **tuxboot-windows-23.exe** from the **Recovery** folder on the Software CD, select **Pre Download**, and then click "**...**"



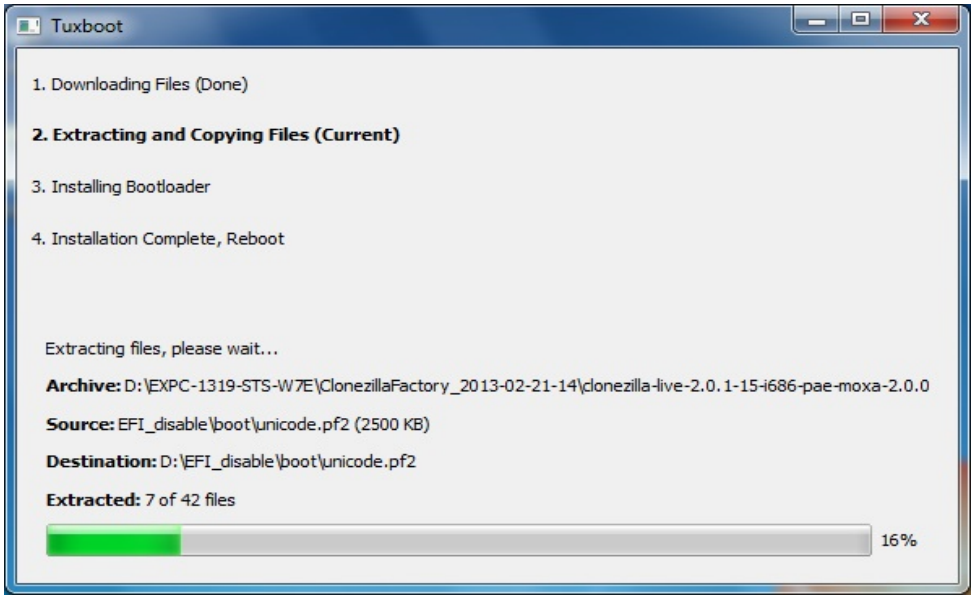
2. Select the ISO file in the directory **<Software DVD> \Recovery**



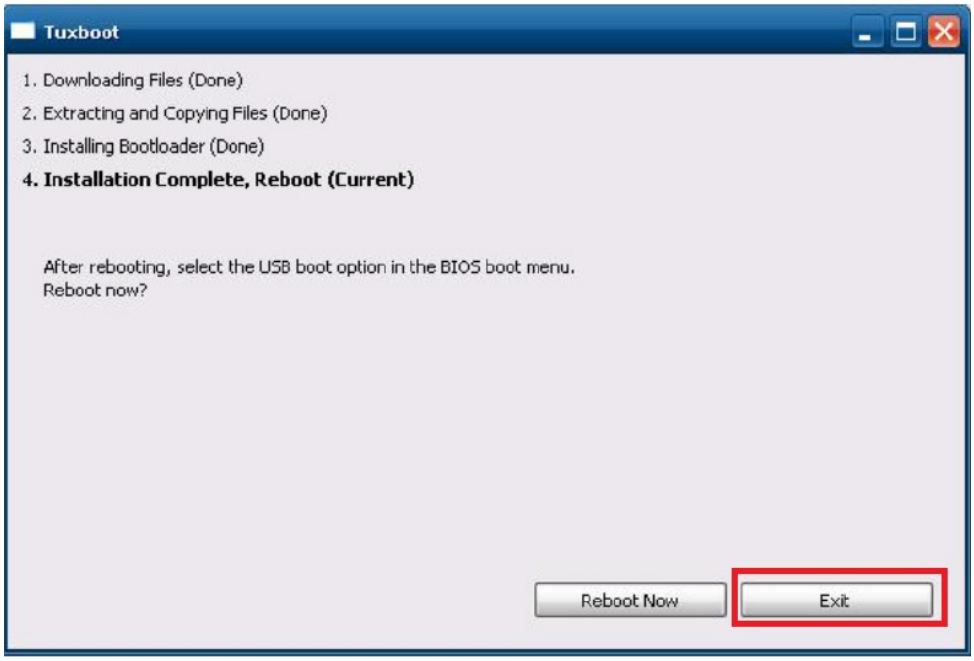
3. Select **USB Drive** type, select a **Drive**, and then click **OK** to continue.



4. The boot files will be copied to your USB drive.



5. When finished, click **Exit** to stop the program.



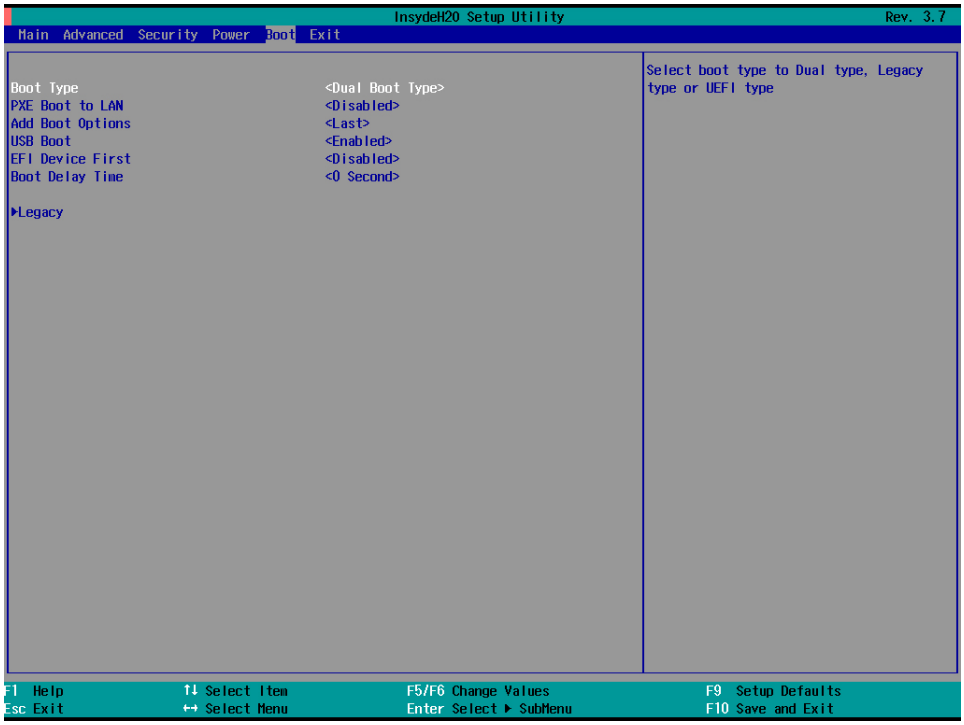
6. Manually copy the **os_image** directory from the <Software DVD> \Recovery\V2201-LX_V1.0_FW\FWR_V2400A-LX_V1.0_Build_15102815 on the Software DVD to **\home\partimag** on the USB drive.

Step 2: Change the BIOS Settings

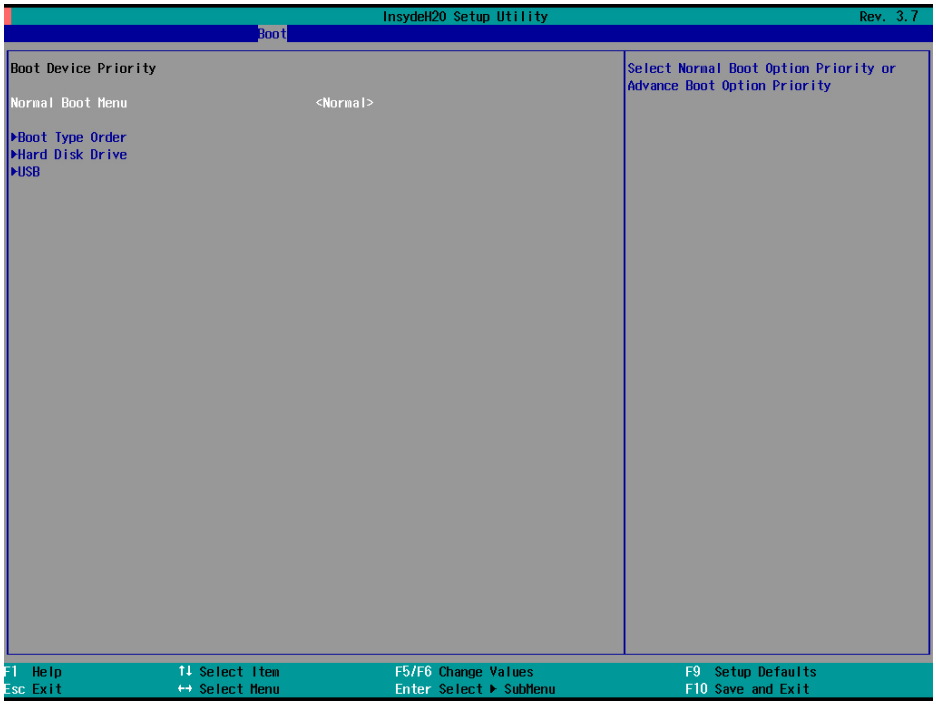
You will need to change the BIOS settings to boot from the USB disk.

1. Turn on the computer and press **F2.** Select **SCU** in the following screen.

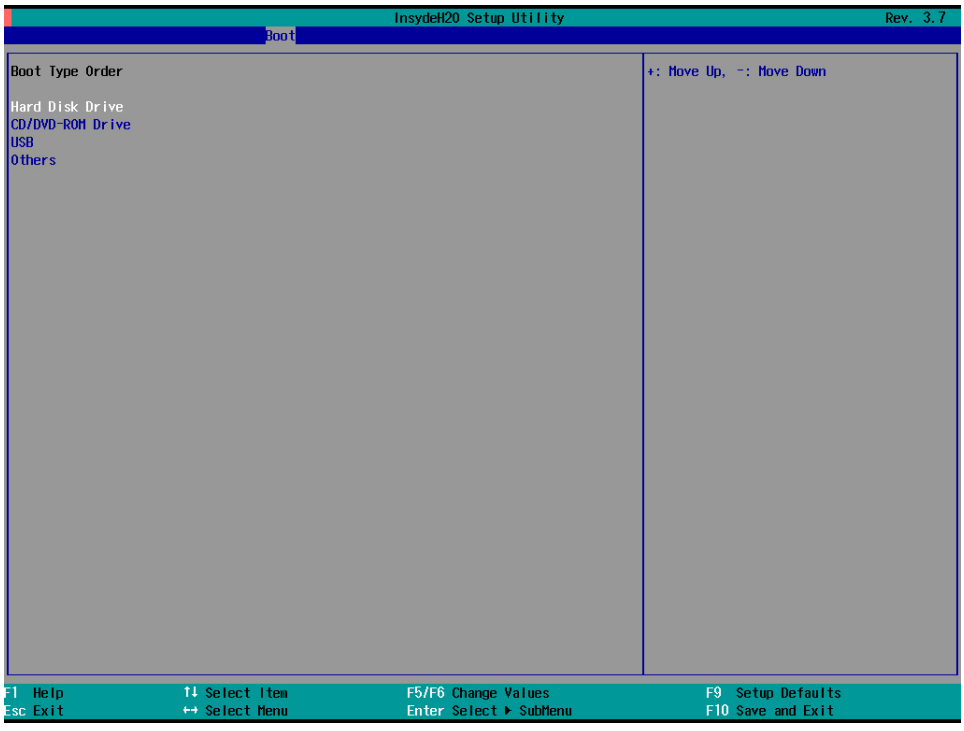
2. Select **Boot** and then select **Legacy**. Press **Enter** to continue.



3. Select **Boot Type Order**.



4. Select **USB disk** and then press "**+**" to move it to the first boot device position.
   Warning: An incorrect boot priority will lead to recovery failure.

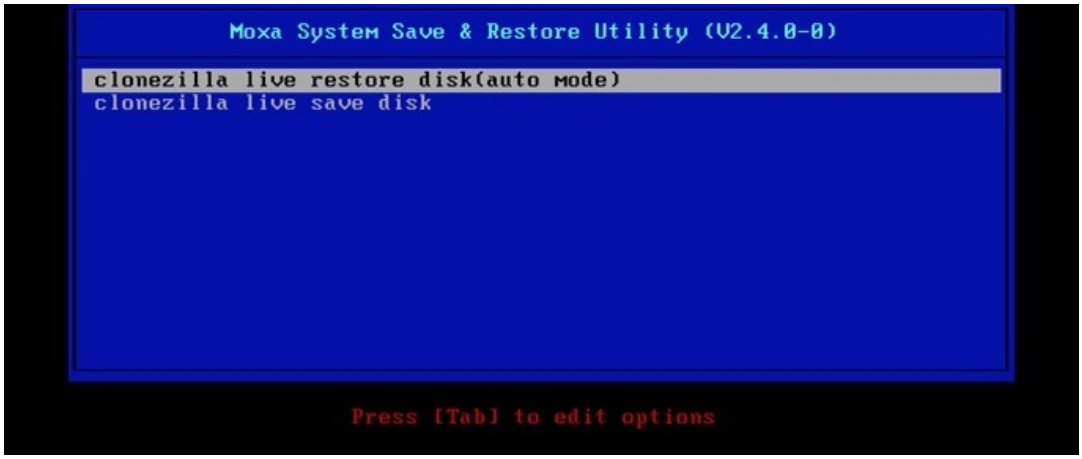


5. Press **F10** and then press **Enter** to save and exit the BIOS setup.

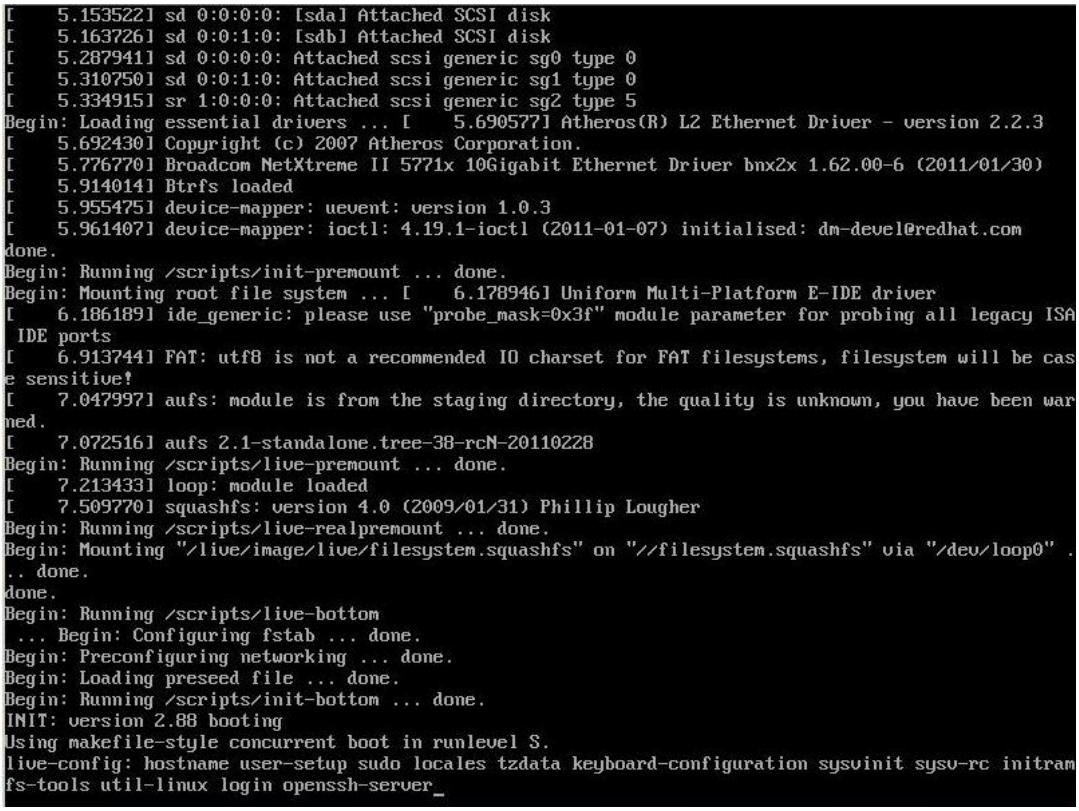
Step 3: Restore the system from the USB drive

Connect the USB disk to any of the V2201's USB ports and then reboot the computer. The system will boot from the USB disk and the Pre-installation Environment and the recovery utility will appear.

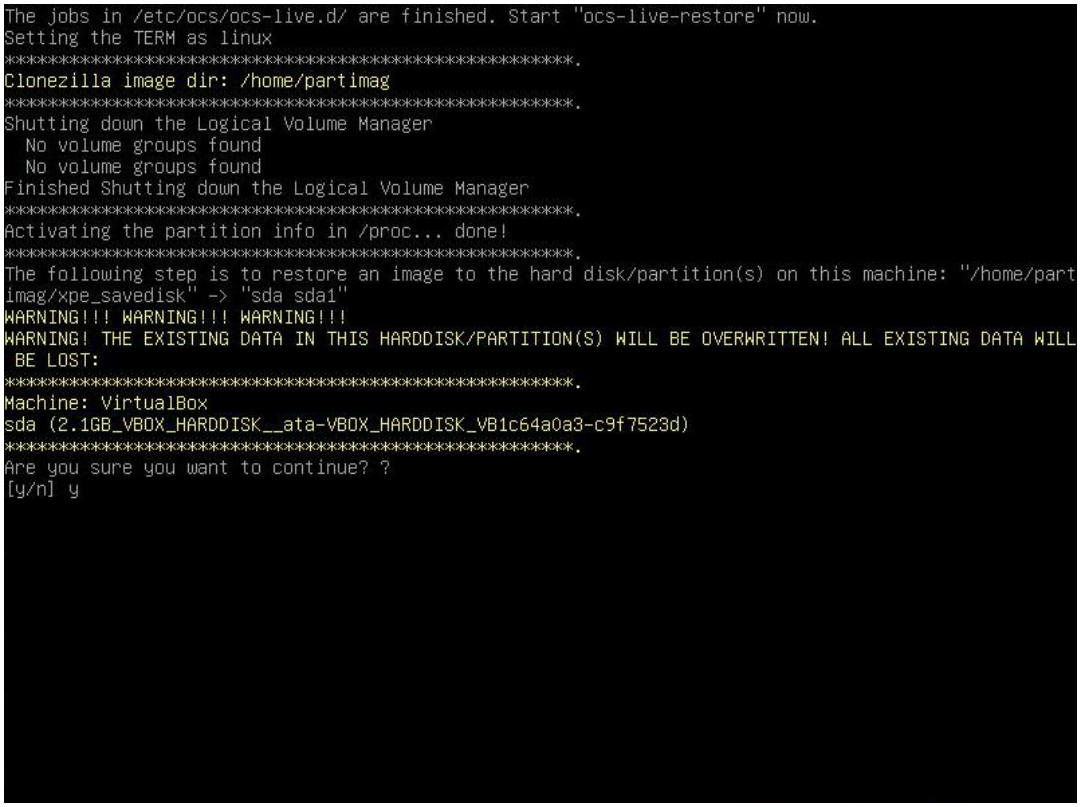
1. Select **clonezilla live restore disk(auto mode)** to complete the recovery task **if you want clonezilla to help you recover the MBR and expand the image automatically**.



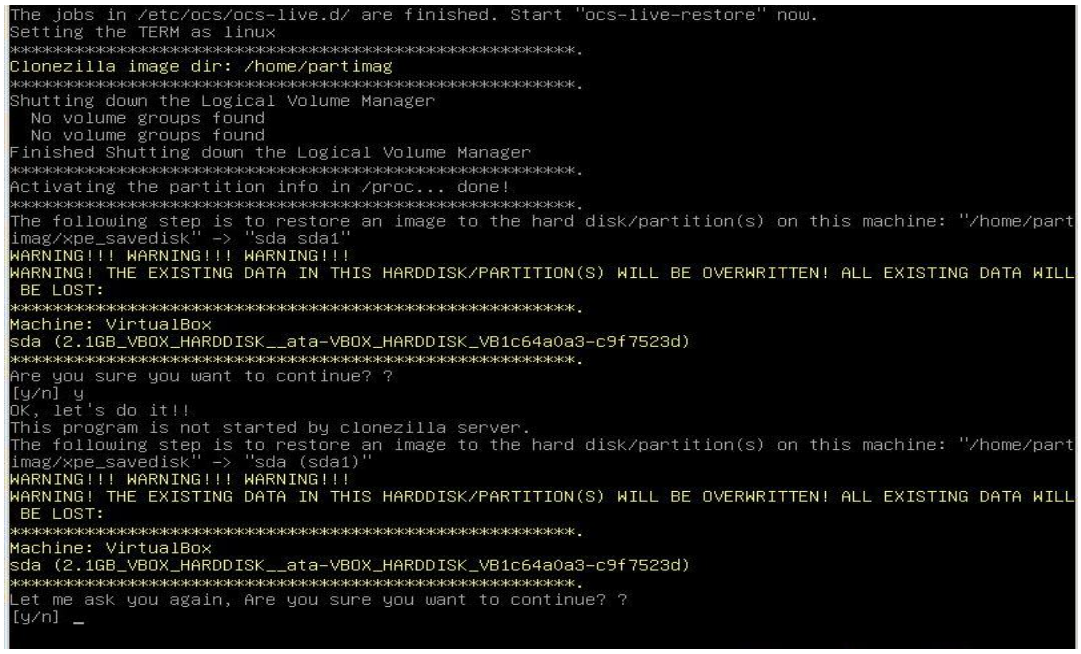
2. Wait for the USB drive boot process to finish.



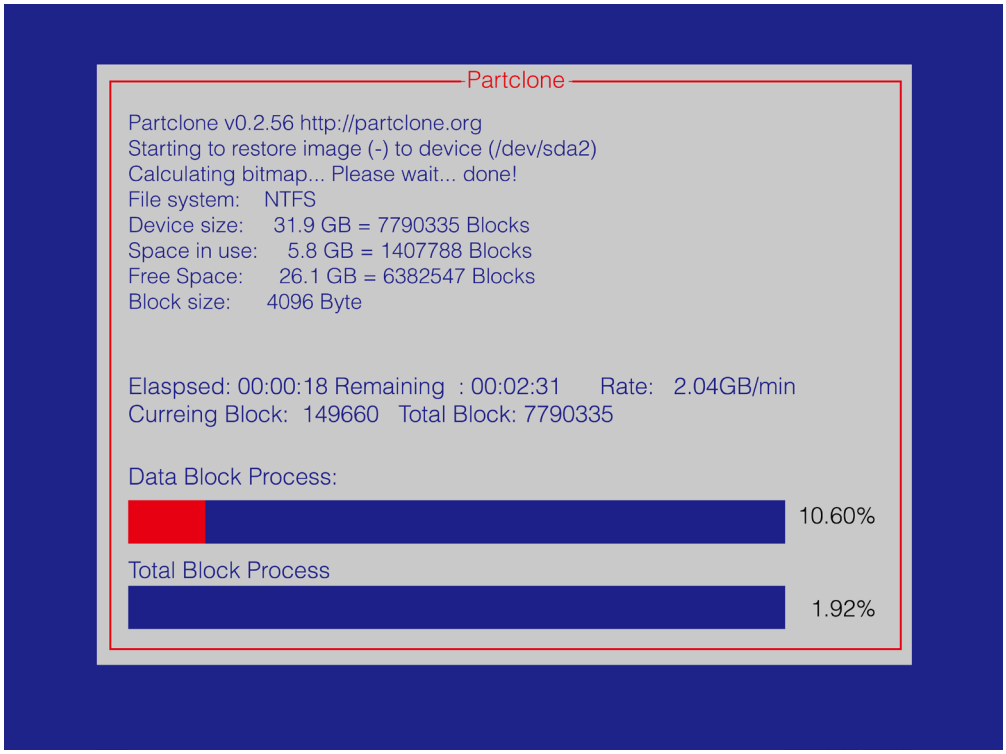
3. Enter **y** to continue the restore process.



4. Enter **y** to confirm again.

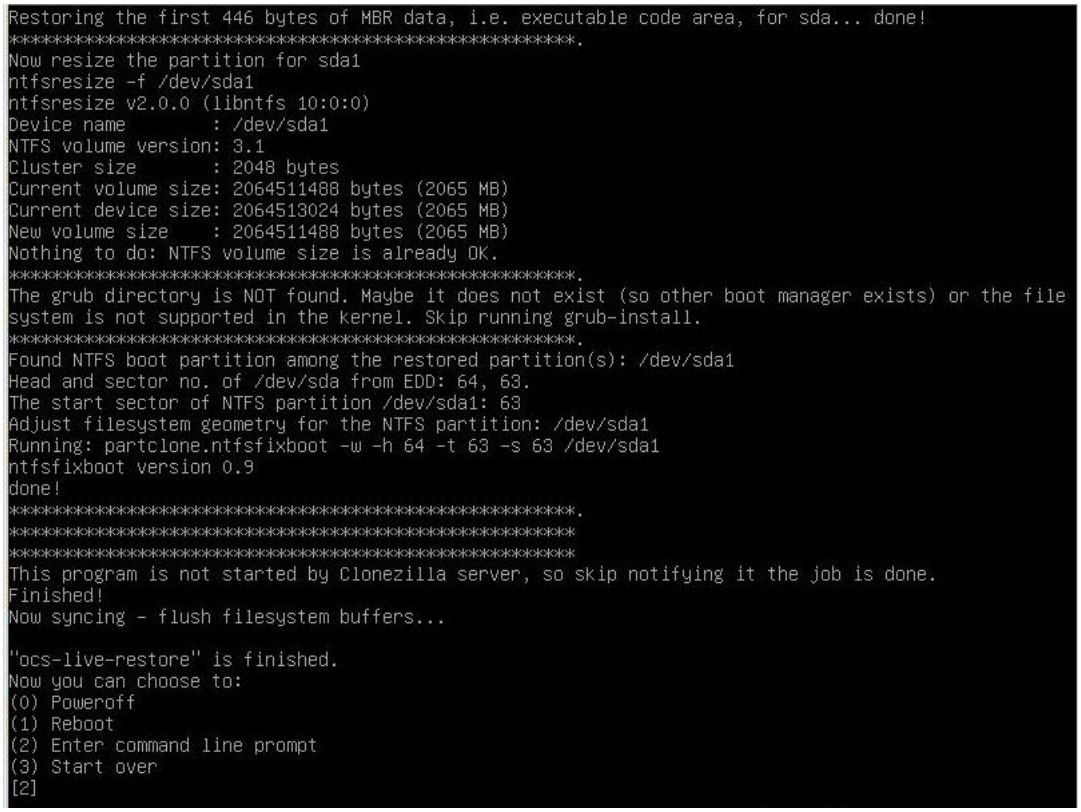


5. Wait for the process to finish.



NOTE You can press any key or use **CTRL+C** to cancel the recovery process and exit Clonezilla.

6. Select **(0) Power off** to power off the computer.

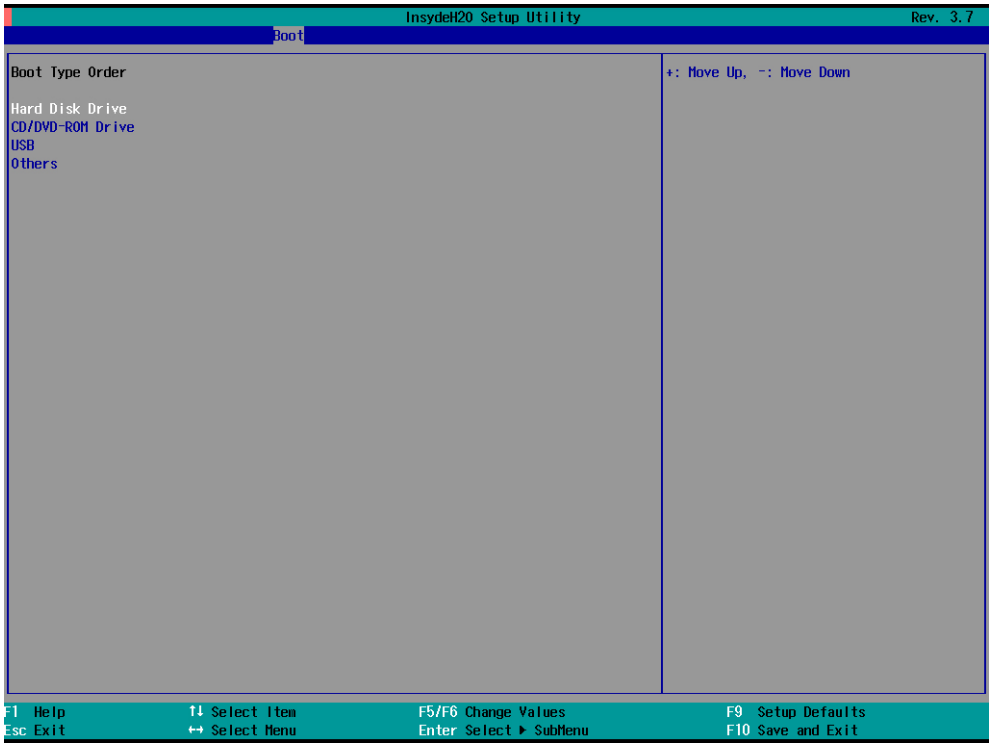


7. Remove the USB drive after the computer has been powered off.

Step 4: Change the BIOS Settings to Boot from the Original Disk

Now you will need to change the boot priority so that it can boot from the original disk. As the system reboots, press **F2** to enter the BIOS setup menu.

1. Select **Hard Disk Drive** and then press + to move to the first boot device position, and then press **Enter**. Make sure the hard disk has first boot priority.



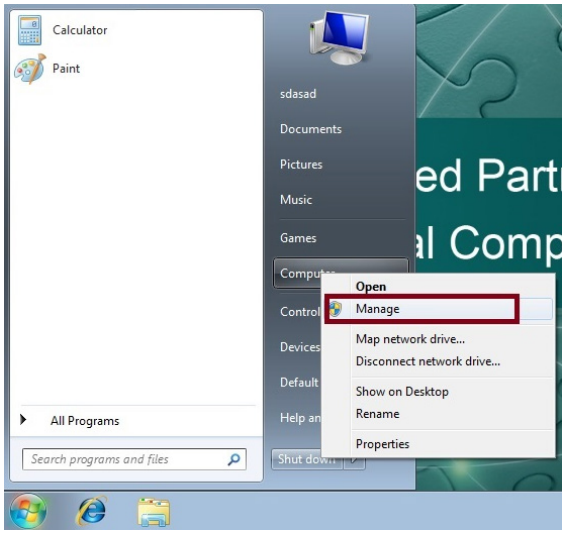
2. Press **F10** and then press **Enter** to save and exit BIOS settings.

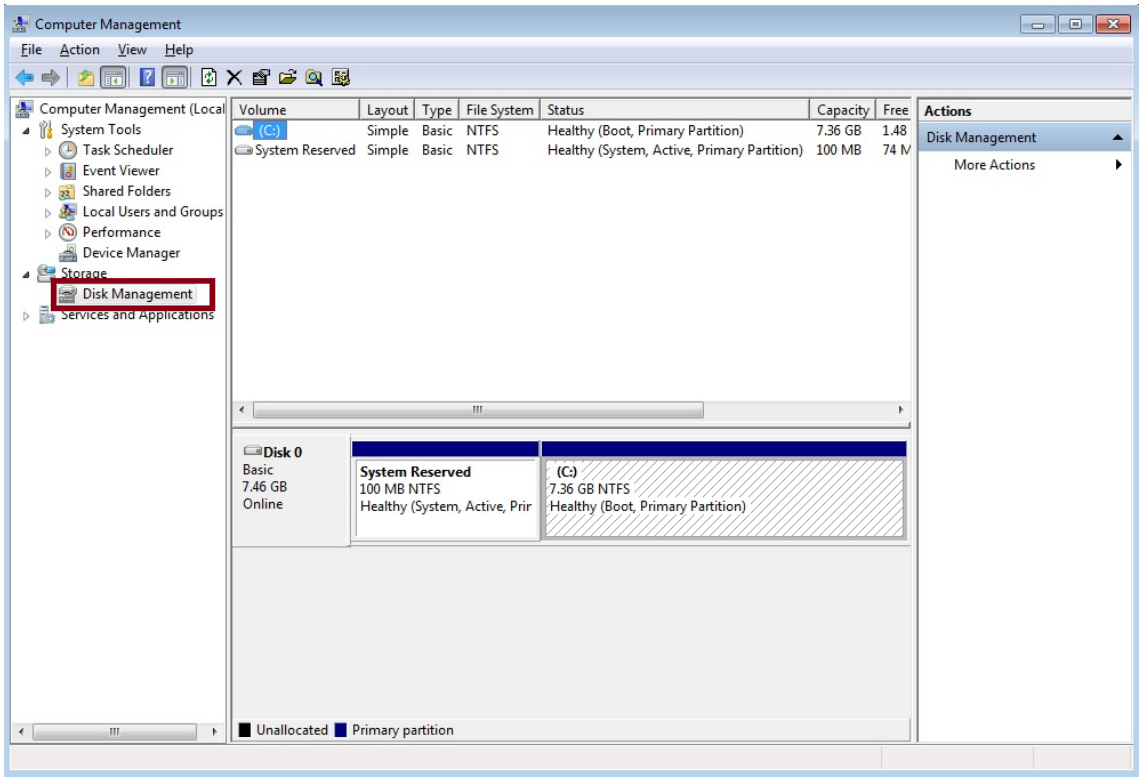
Saving the System to the USB Drive

You may also save the current system to the USB drive for system recovery in case the system crashes. Before saving the system to the USB drive, we suggest removing all files under **\home\partimag** on the USB drive. And please shrink the file system by default to ensure that the task will be saved successfully. Follow the steps below to shrink the file system.

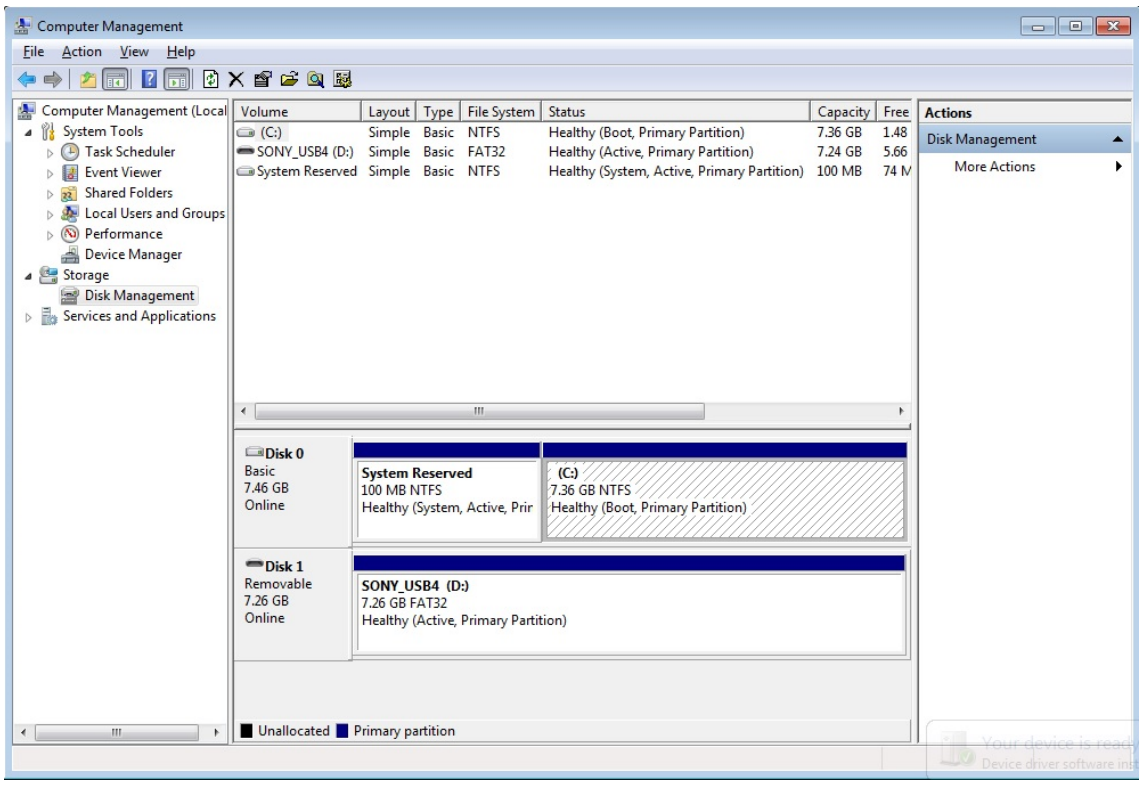
Shrink file system on Windows Embedded 7

1. Right click **Computer**, select **Manage** and open **Disk Manager** from left side bar.



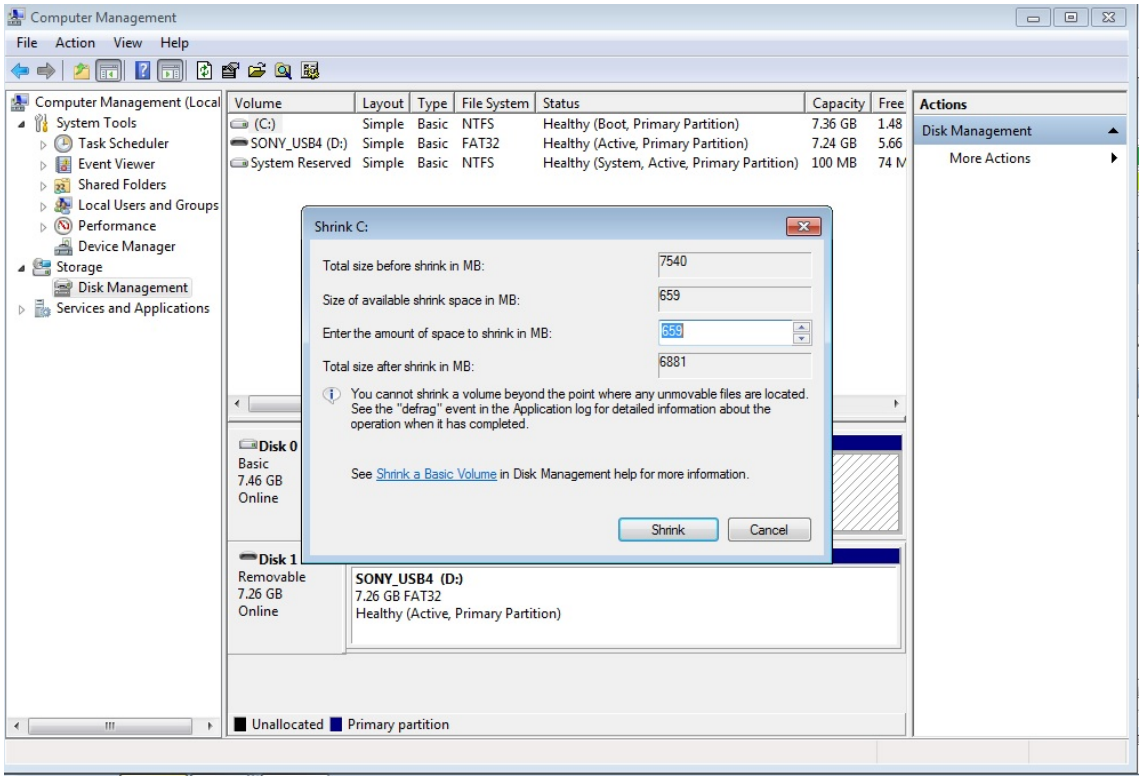


2. Insert the USB disk that you want to save the image to and it will be listed on the Disk Manager. The size of the file system is now equal to Disk 0 (sum of "**System Reserved**" and "**C:**").

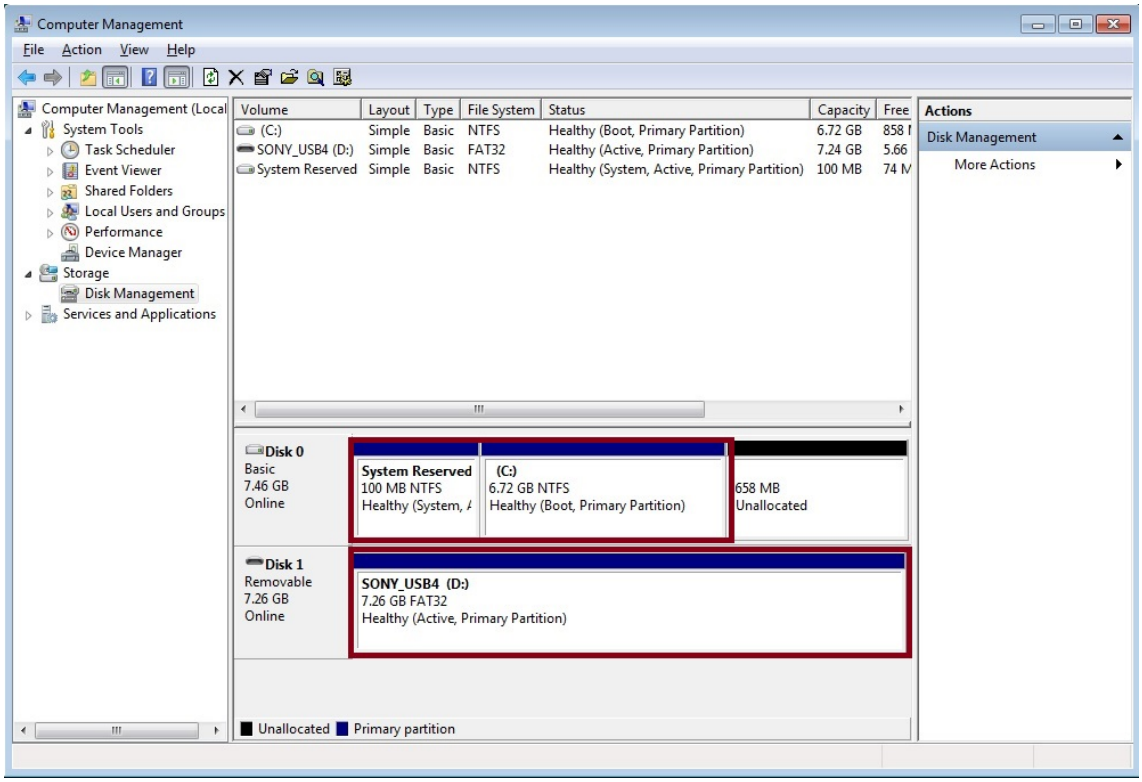


3. Right click disk **C:** and select **Shrink Volume.**

4. **Enter the amount of space to shrink in MB**. The **Total size after shrink in MB** must to be smaller than the size of USB disk. Then click **Shrink**.

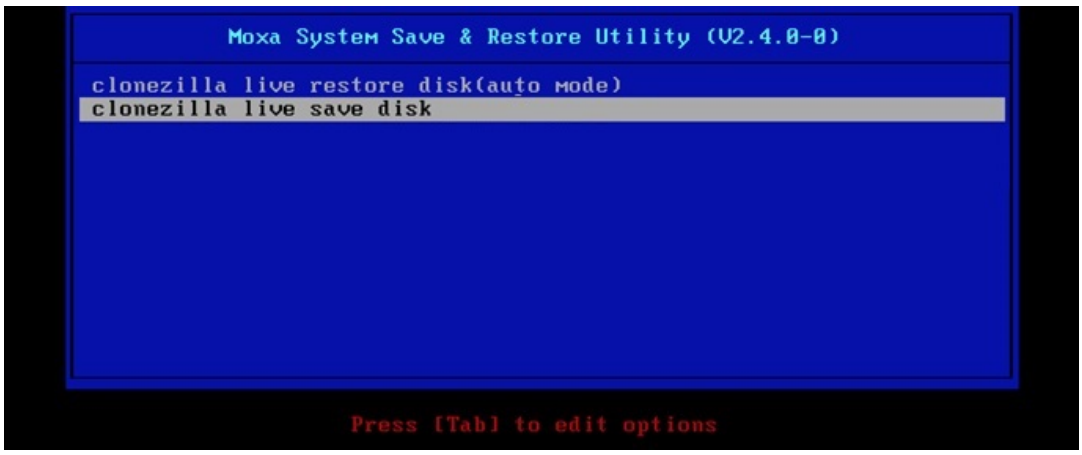


5. Make sure that the **Total size after shrink in MB** is smaller than the size of the USB disk.

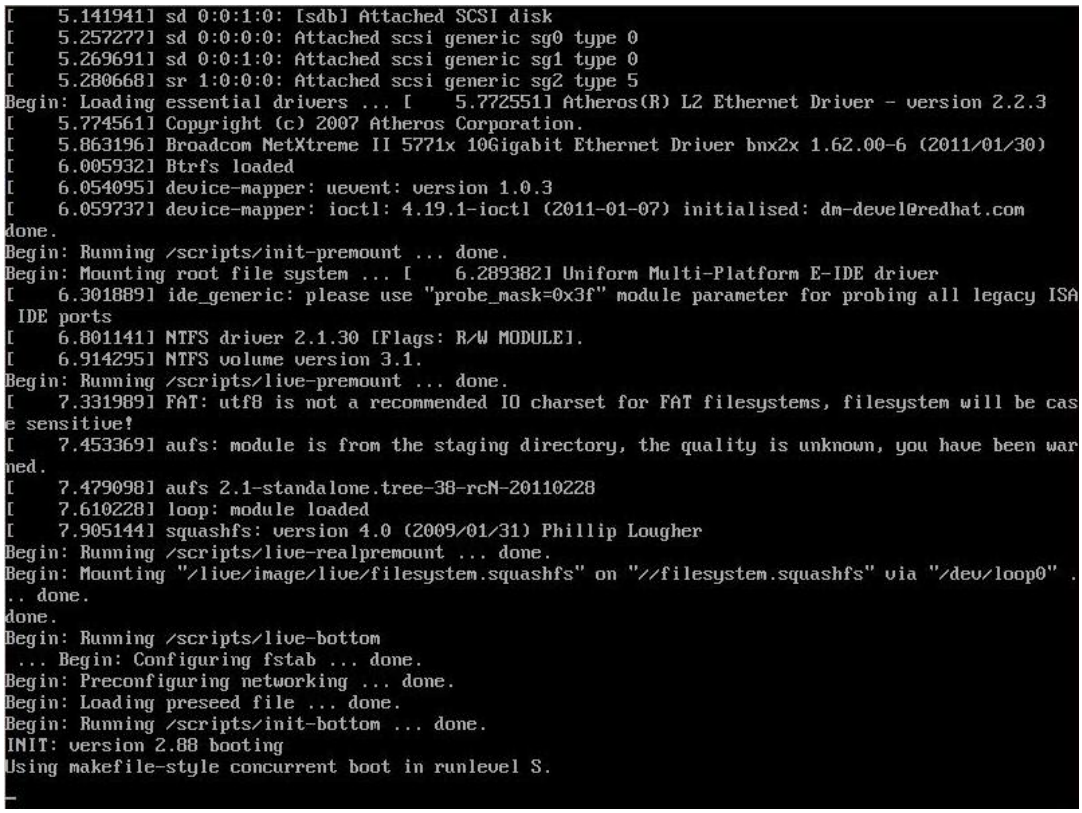


When the system has launched, change the BIOS settings to make the USB drive the first boot priority and then follow the steps below:

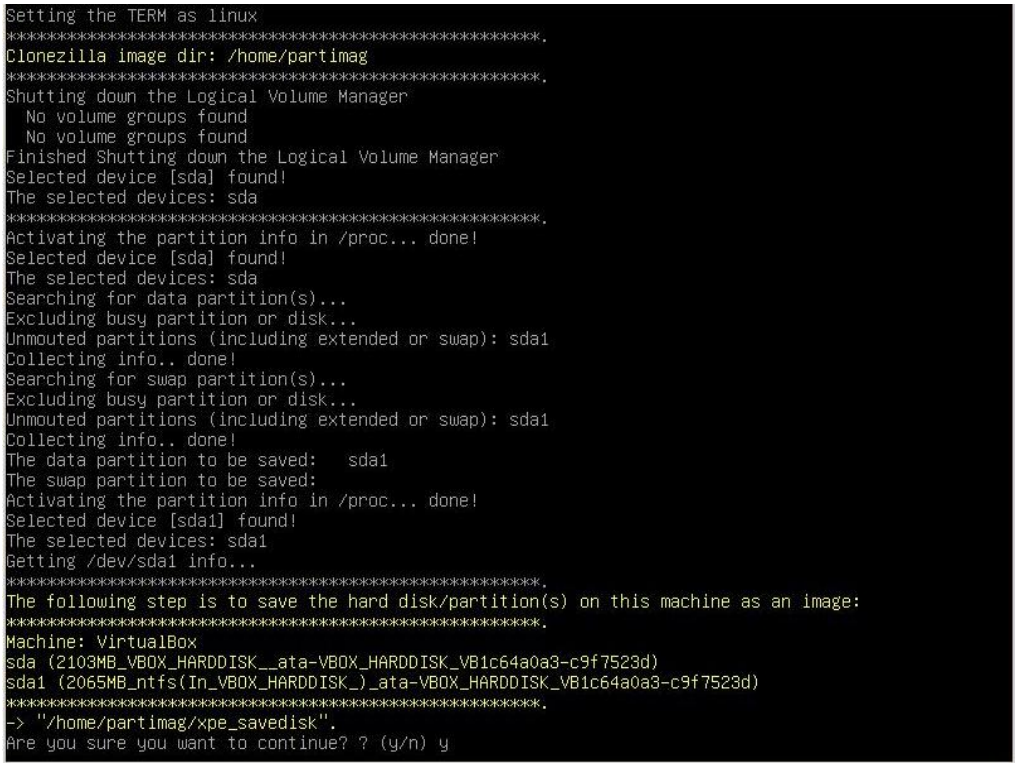
1. Select **clonezilla live save disk.** (If you want to configure more parameters, refer to next section: "Expert mode.")



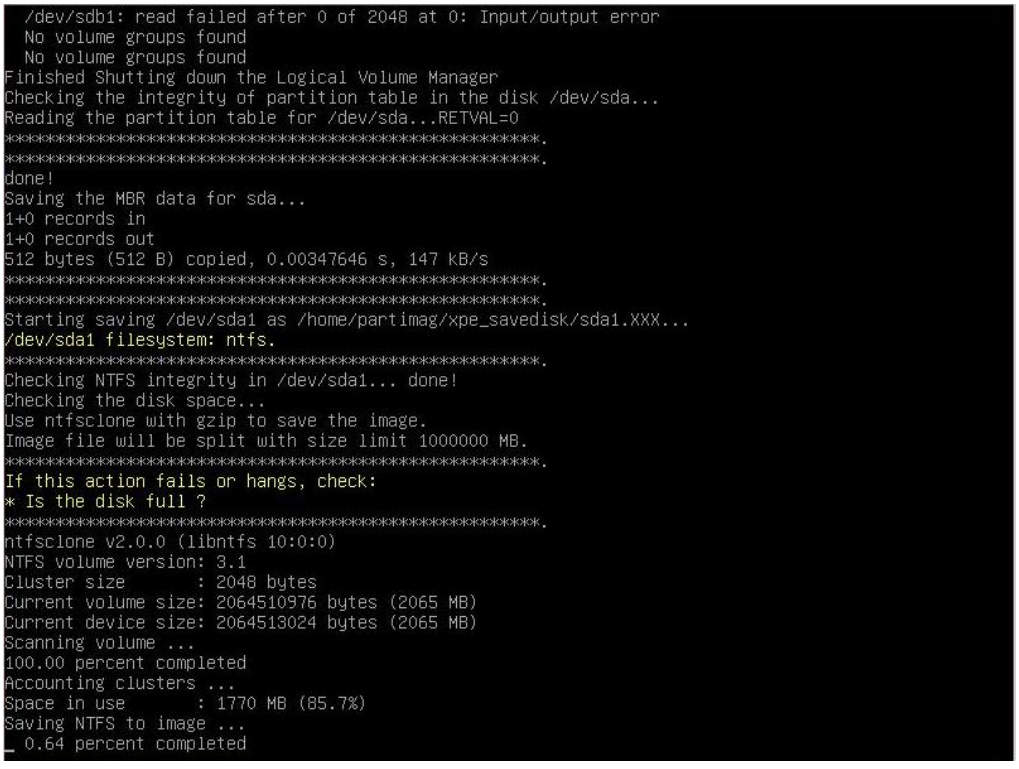
2. Wait for the USB drive boot process to finish.



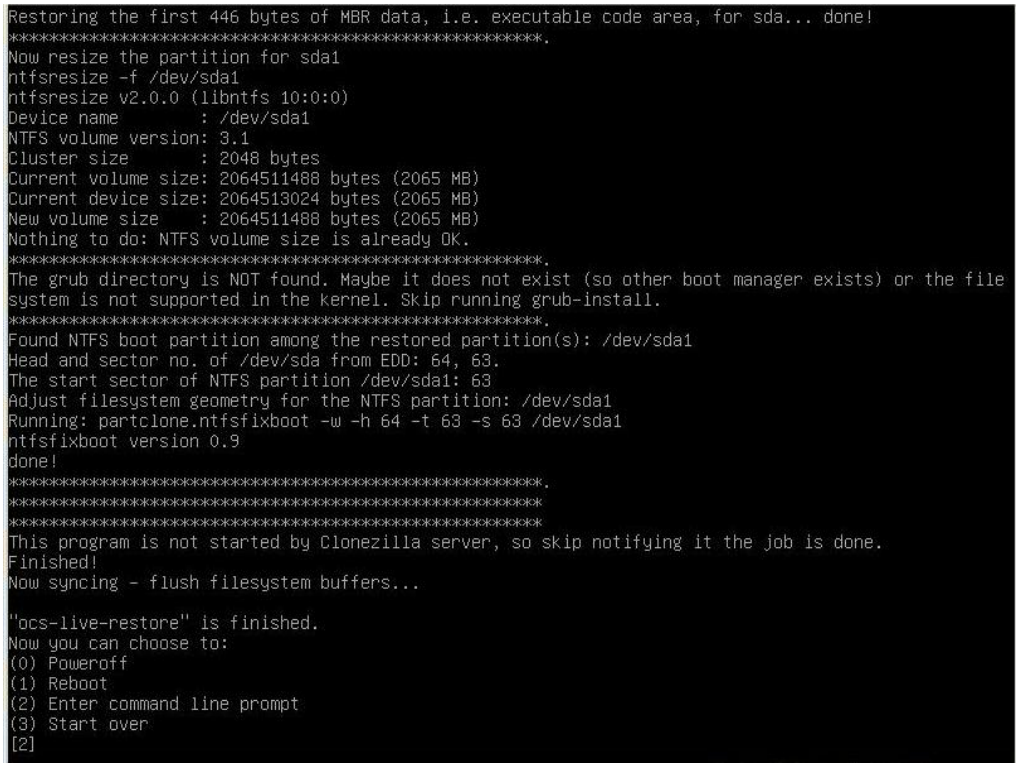
3. Enter **y** to continue.



4. Wait for the process to finish.



5. Select **(0) Poweroff** so that the computer will power off when the process is finished.



8

Proactive Monitoring

The V2201 series supports the "Moxa Proactive Monitoring" utility. See the "Moxa Proactive Monitoring Windows Software User's Manual" for details. The manual can be found on the product CD/DVD or downloaded from Moxa's website. Note that the V2201 does not support hardware relay.