

Quanta WiMAX Connection Manager Operator Guide

Version 1.1

Aug. 25, 2010



Federal Communication Commission Interference Statement

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an **uncontrolled environment**.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

SAR compliance has been established in typical laptop computer(s) with USB slot, and product could be used in typical laptop computer with USB slot. Other application like handheld PC or similar device has not been verified and may not compliance with related RF exposure rule and such use shall be prohibited.



Contents

| | | |
|--------|---|----|
| 1. | Introduction..... | 6 |
| 1.1. | Document Scope..... | 6 |
| 2. | Install and Un-install Windows Driver and Connection Manager..... | 7 |
| 2.1.1. | Un-installation of Windows Driver & Connection Manager..... | 7 |
| 2.1.2. | Execute InstallShield Wizard..... | 7 |
| 2.1.3. | Install with Second WiMAX device..... | 10 |
| 2.1.4. | Upgrade WiMAX Connection Manager..... | 10 |
| 3. | Configuration by WiMAX Connection Manager..... | 13 |
| 3.1. | Connection Mode..... | 14 |
| 3.1.1. | Auto Mode..... | 14 |
| 3.2. | Profile..... | 15 |
| 3.2.1 | Scanning Setting..... | 16 |
| 3.2.2. | User Authentication..... | 19 |
| 4. | How to Upgrade F/W..... | 20 |
| 5. | Trouble Shooting..... | 24 |
| 5.1. | Why I can't detect my device?..... | 24 |
| 5.2. | Why I can't find any base station?..... | 24 |
| 5.3. | Why I can't connect to base station?..... | 24 |
| 5.4. | How to log debug information and report it?..... | 25 |
| 5.5. | What does LED activity mean?..... | 26 |
| 6. | Appendix..... | 27 |
| 6.1. | Create Device Information *.IFO file..... | 27 |
| 6.2. | Device Authentication..... | 28 |
| 6.3. | User and Device Authentication..... | 29 |
| 6.4. | Functional Button..... | 30 |
| 6.4.1. | Profile..... | 31 |
| 6.4.2. | Scan..... | 32 |
| 6.4.3. | Network..... | 33 |
| 6.4.4. | Statistic..... | 34 |
| 6.4.5. | Tools..... | 34 |



Revision History

| Version | Release Date | Description |
|----------------|---------------------|--|
| 1.1 | Aug. 25, 2010 | Based on WU202 to update the document. |
| 1.0 | Apr. 30, 2009 | 1 st User Guide Release |



1. Introduction

The WiMAX dongle supports IEEE 802.16e-2005 state of the art Scalable OFDMA based Technology. It provides users a seamless broadband wireless access, video streaming at home, office or on the move. To protect information transmitting through wireless network, standard security Sublayer PKMv2 EAP based user authorization/authentication for data encryption is supported.

The following chapters will show you how to install the software package step by step.

1.1. Document Scope

This document has been written based on:

- WCM: 02.01.06
- OS: Windows 7 x86-based PC, English Version

2. Install and Un-install Windows Driver and Connection Manager

2.1.1. Un-installation of Windows Driver & Connection Manager

1. Please EXIT the WiMAX Connection Manager first.
2. Please click “Start * All Programs * WCM * Uninstall WCM” to remove it.

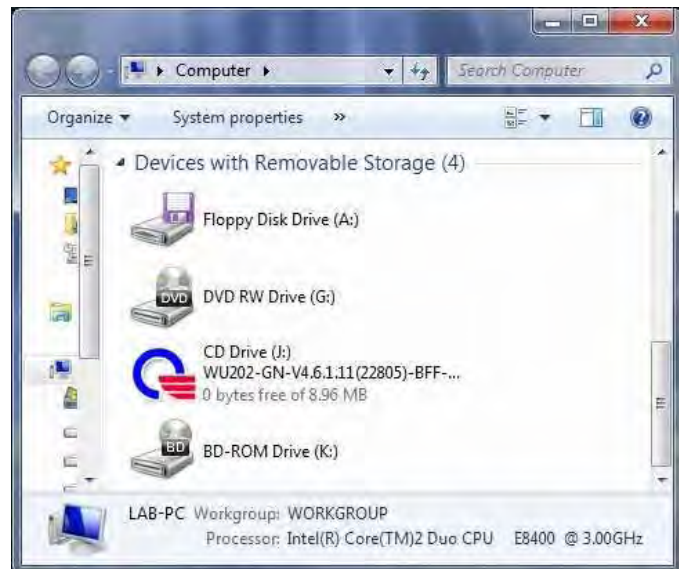


2.1.2. Execute InstallShield Wizard

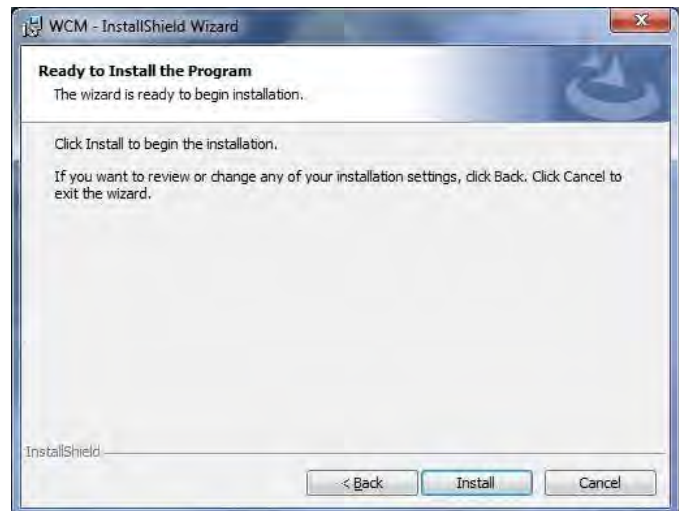
1. Please plug in WiMAX device into the laptop and execute InstallShield Wizard to install windows driver and connection manager.
2. Please click “Next” button.



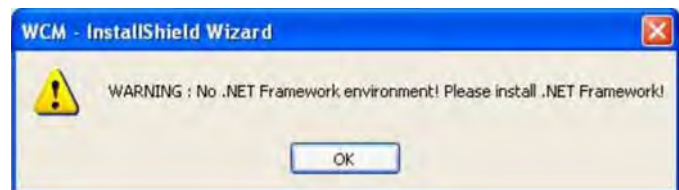
3. If the laptop is off auto-install feature for security reasons, please open “**CD Driver: WU202-GN...**” and run “**setup.exe**”.



4. Please click “**Install**” button to continue installation.



5. WCM InstallShield will pop out a message if your laptop doesn't install .NET Framework.
6. Please check if your Windows has .NET Framework 2.0 or plus, or WCM may not work properly.



7. Prepare to copy configuration file to C:\WiMAX.



8. Windows will find new hardware and guide you to complete installation.

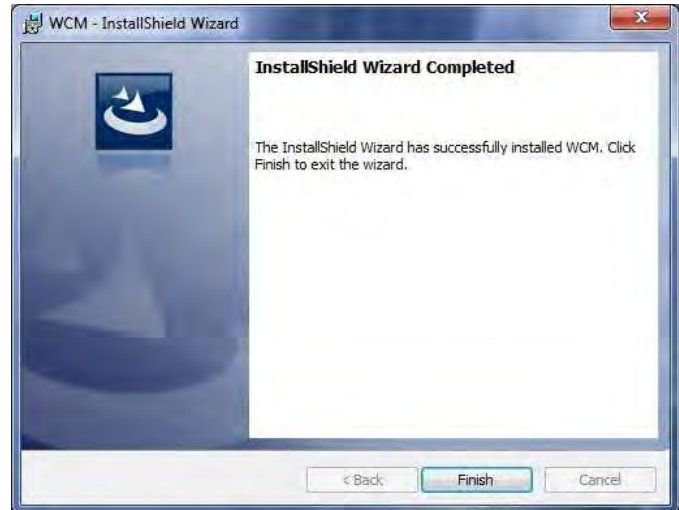


9. Please check “Always trust software from “Sequans Communications”.” and click “Install” button to continue installation.

10. It may take a few minutes to complete driver installation.



11. After InstallShield Wizard has successfully installed WCM and driver, windows will prompt a message.
12. Click “**Finish**” button to finish InstallShield Wizard.
13. You can run the WCM from the WiMAX Connection Manager icon on desktop or run WCM from “Start * All Programs * WCM * WiMAX Connection Manager”.

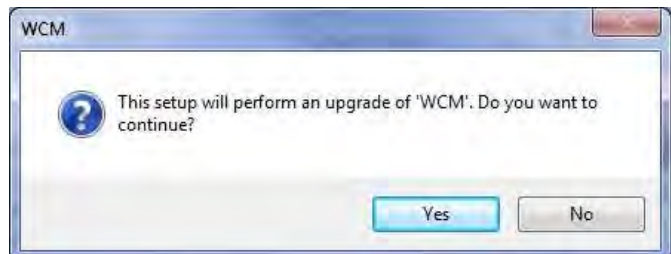


2.1.3. Install with Second WiMAX device

1. Each device is written with unique serial number in the flash, so windows will recognize each device as different one.
2. Once you plug in the second device, Windows will pop out “**Found New Hardware Wizard**” and install driver automatically.

2.1.4. Upgrade WiMAX Connection Manager

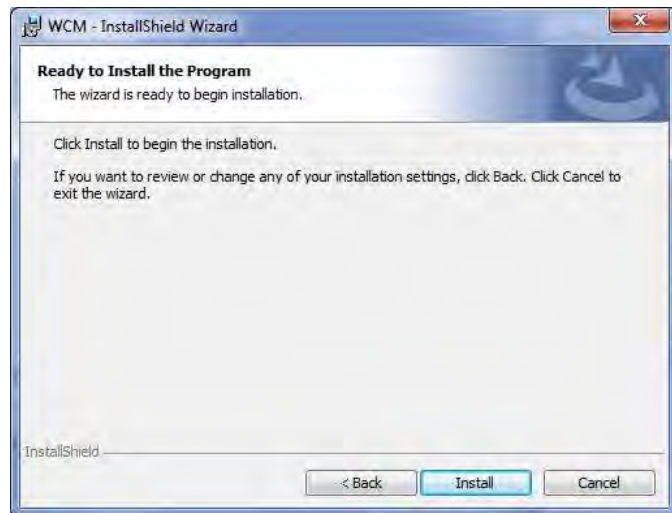
1. This section will guide you how to upgrade to latest software package in client side.
2. Please make sure to plug in your WiMAX device first.
3. Please execute InstallShield of new WCM, and click “**Yes**” button if you want to upgrade the WCM.



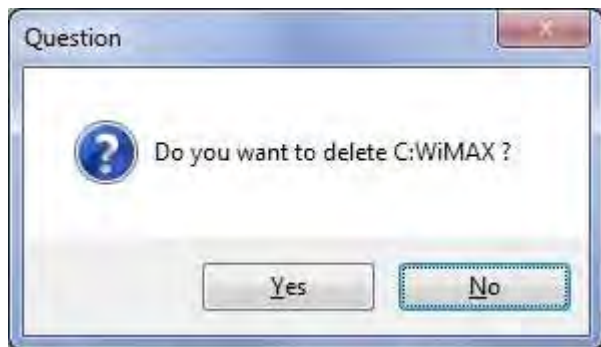
4. Click “**Next**” button to start installing WCM.



5. Click “**Install**” button to start install WCM.



6. It will pop out a Question window. If you want to keep the configuration settings, please click “**No**” button.



7. It will show the message “**Found USB/ PCIe Device**”.
8. It may take a few minutes to complete driver installation.



9. Please click “**Finish**” button to exit the Wizard.



3. Configuration by WiMAX Connection Manager

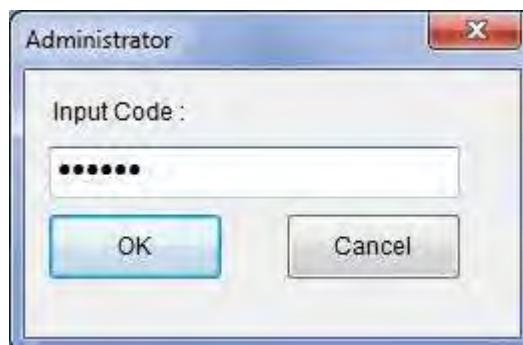
1. Please open WiMAX Connection Manager firstly.



2. Please move the mouse on the WCM and press “**Ctrl + Alt + F9**” to show the “**Advanced**” button for advance settings. Please click “**Advanced**” button and input the code “**admin2**”.



3. Once you switch to Advanced View, WCM will keep staying at Advanced View till you exit WCM or minimize to system tray.



4. Please plug in WiMAX device and wait for WCM detects device.
5. After WCM detects WiMAX device, you can start to set up the profile settings and EAP parameters.



3.1. Connection Mode

3.1.1. Auto Mode

1. If you have well setup frequency, bandwidth and the other EAP settings. Please keep the “**Auto Mode**” setting as “**On**” on “**Profile**” tab, this button will let device always try to automatically connect with BS.
2. If “**Auto Mode**” is to “**On**” and the BSs information are listed in **Pre-defined List** or in **History List** on “**Scan**” tab, MS will automatically connect with BS.
3. Please note that if you ever double clicked the **NAP ID** in the **Base Station Scan List** on “**Scan**” tab, it means you didn’t want to automatically connect with BS and the “**Auto Mode**” will be “**Off**”.



- Please remember to keep the “**Auto Mode**” as “**On**” to let device automatically connect with BS.

3.2. Profile

The user profile “WiAMXd.cfg” is stored in the directory “C:\WiMAX”.

- Please plug in WiMAX device and wait for WCM detects device as depicted in the right screenshot.
- When WCM detects WiMAX device, you can start to set up the EAP parameters.
- Please input all the information on “**Profile**” tab, including PKM, Authentication, EAP Method, NWG, Inner EAP, and so on.
- Please click “**Save Setting**” button to save your setting.
- You also can re-set the “**Operator Password**” for advance setting.

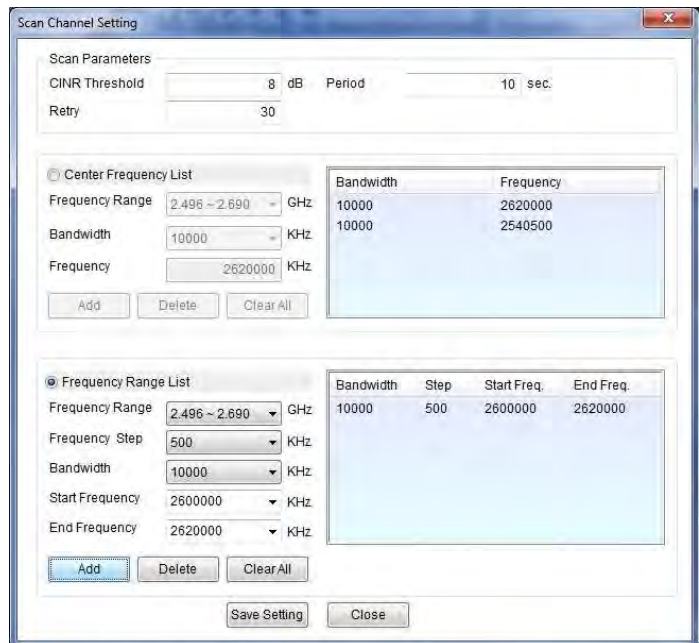


3.2.1 Scanning Setting

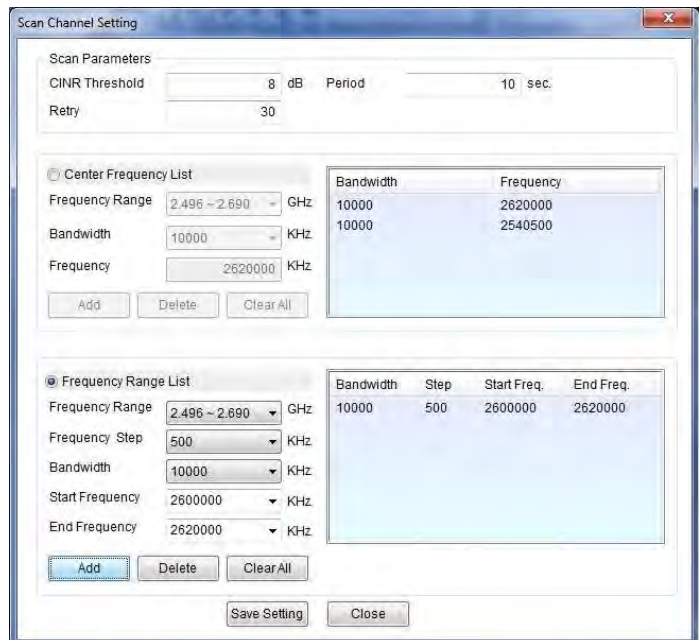
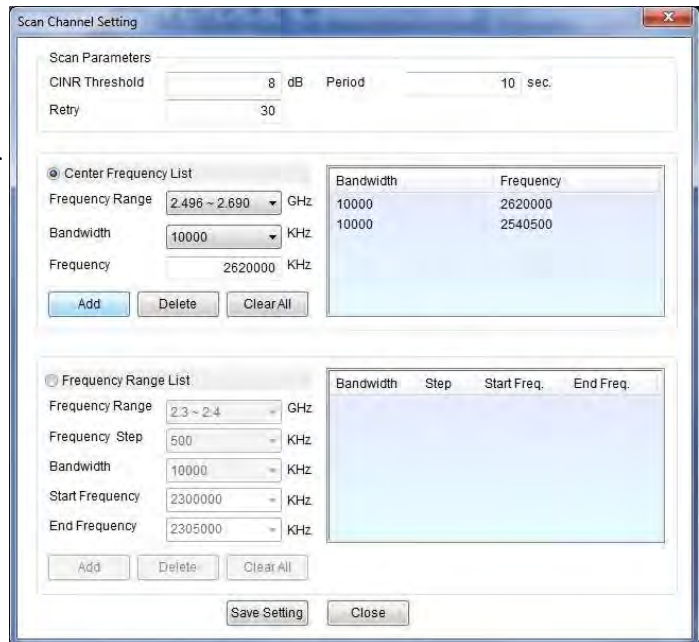
1. Please click “Scan Setting” button to enter setting page.



2. In the **Scan Channel Setting** field, you can set up some searching criteria.
3. **CINR Threshold** filter: searching BS if and only if CINR is higher than specified value (dB). Minimum: -20, and maximum: 40.
4. **Period** setting: *Period (0)* which is initial period in second after which the terminal restart scanning procedure. Minimum: 0, and maximum: 255.
5. **Retry** setting: *(n) configurable maximum value* of the countdown procedure. Minimum: 0, and maximum: 50.



6. In the **Center Frequency List** field, you can set up some specified frequency you want.
7. **Frequency Range:** please select your target and frequency range according to what kind of WiMAX device you used.
8. **Bandwidth:** please select your preferred bandwidth in KHz. WCM supports mix-bandwidth scanning mechanism.
9. **Frequency:** please input your preferred frequency in KHz according to what kind of WiMAX device you used.
10. Please click **Add** button to add it into frequency list.
11. Please select frequency from frequency list and click **Delete** button to remove it from the list.
12. You can click **Clear All** button to clear all setting of **Center Frequency List**.
13. In the **Frequency Range List** field, you can set up some specified frequency range you want.
14. **Frequency Range:** please select your target frequency range according to what kind of WiMAX device you used.
15. **Frequency Step:** please select increasing step.
16. **Bandwidth:** please select your preferred bandwidth in KHz. WCM supports mix-bandwidth scanning mechanism.
17. **Start Frequency:** please select starting frequency in KHz according to what kind of WiMAX device you used.
18. **End Frequency:** please select ending frequency in KHz according to what kind of





WiMAX device you used.

19. Please click **Add** button to add it into frequency list. **WCM supports maximum up to three sets of frequency range list.**
20. Please select frequency from frequency list and click **Delete** button to remove it from the list.
21. You can click **Clear All** button to clear all setting of **Center Frequency List.**
22. If you have confirmed all your setting, please click **Save Setting** button.
23. This device will auto-reboot in order to make your settings become effective.

3.2.2. User Authentication

This section only guide you to connect with BS by User Authentication, for Device Authentication and User and Device Authentication, please refer to chapter 6.

1. Please enable PKM by selecting the “PKMv2_EAP” option.
2. Please select “User Authentication” as your authentication method. WCM will select EAP Method as “EAP-TTLS”.
3. Please select inner EAP method, such as PAP, CHAP, MSCHAP and MSCHAPV2.
4. Please input postfix (Realm) of “Outer Identity”.
5. Please load your CA Certificate.
6. Please input “User ID”.
7. Please input “User Password”.
8. Please select NWG spec as R1.0, Draft or No Decoration.
9. Please click “Save Setting” button to save all authentication settings.
10. If you want to reset to default setting, please click “Reset” button.
11. Now, you can start connecting to BS successfully after setting scanning method through scan setting button as shown in [section 3.1](#).

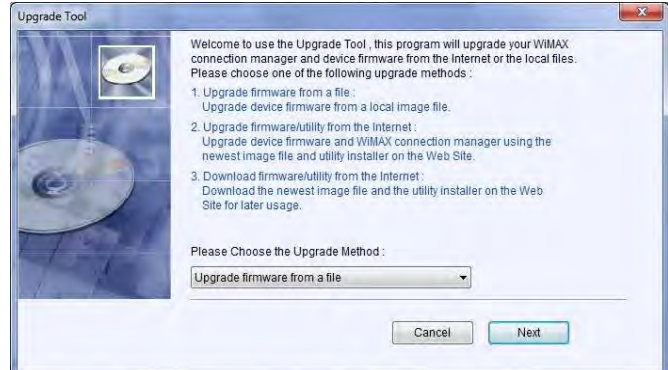


4. How to Upgrade F/W

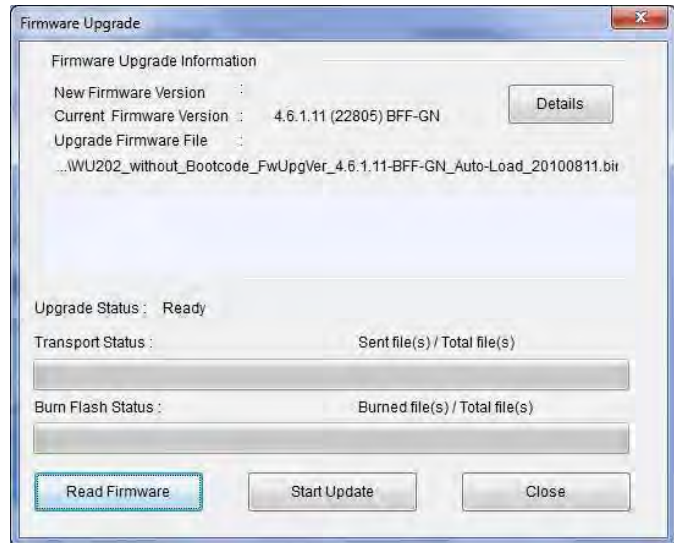
1. This section will guide you how to upgrade the F/W of the device.
2. Please click “**Upgrade**” button on “**Tools**” tab to start the F/W upgrade wizard.



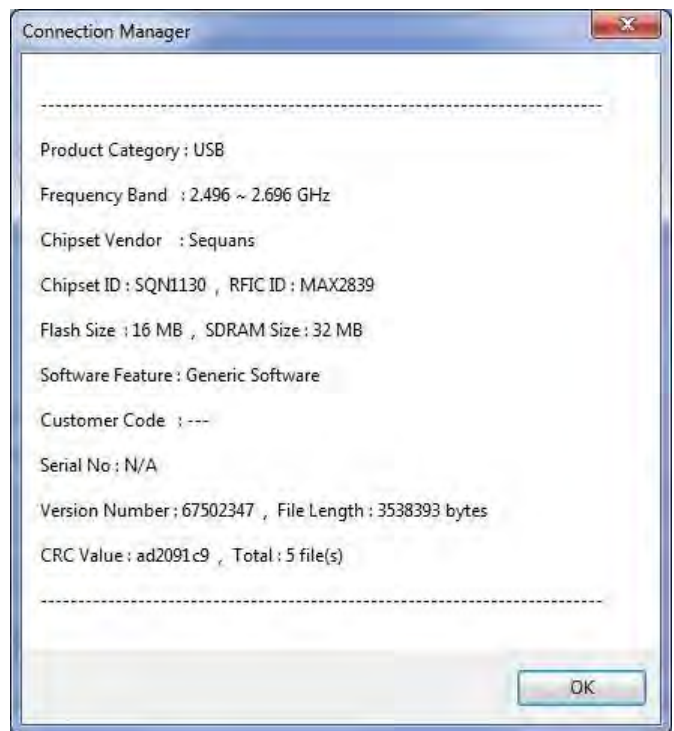
3. Please choose “**Upgrade firmware from a file**”, and then click “**Next**” button.



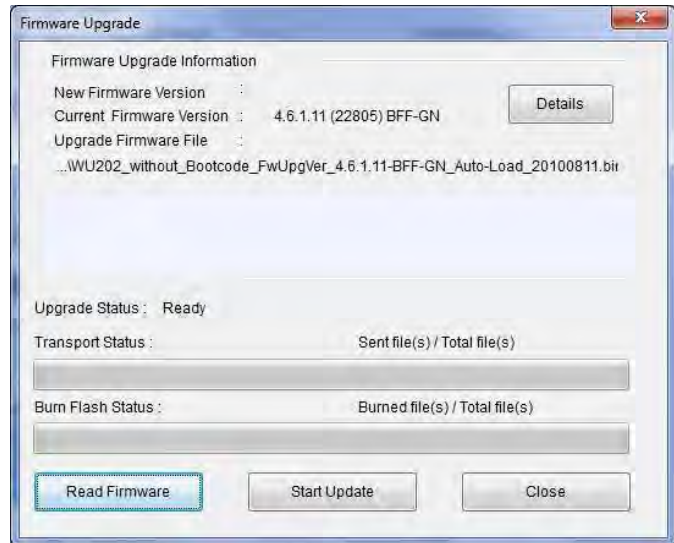
- Click “**Read Firmware**” button to browse the new F/W file.



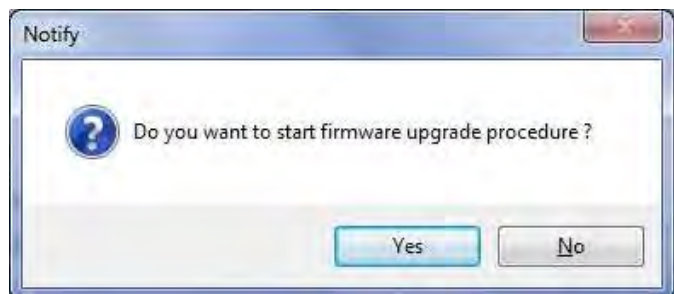
- Please browse the new F/W file and then click the “**Open**” button.
- Please click “**Details**” button if you want to check the new F/W information.



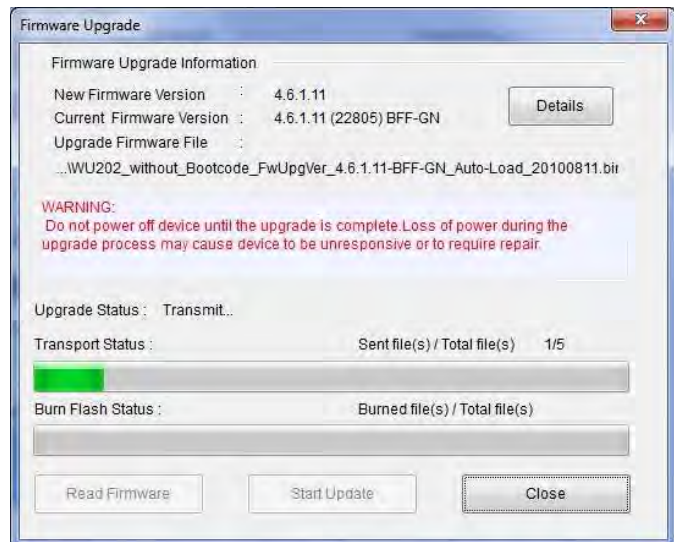
- It will show the file name of new F/W in the window, then click **“Start Upgrade”** button to start upgrade procedure.



- The message is to notify you to start the upgrade procedure.



- The device will auto reboot and then start to upgrade new F/W. Please don't power off device during the upgrade procedure.
- In the upgrade procedure, the LED will display **“Green Flashing”** light
- There are total 5 files to transport and burn to flash, it will take a few minutes to do this.



12. After all files are burned success, the device will reboot automatically and display a successful message.
13. Please click “Close” button to exit the F/W upgrade wizard.



14. Please click on “Device” tab to check if the F/W version is the same with new F/W version.





5. Trouble Shooting

5.1. Why I can't detect my device?

1. If there is a yellow exclamation point on WiMAX Network Adapter, please re-install the driver from
C:\Program Files\WCM\Driver\USB.
2. Please check if you have installed software package successfully. If not, please uninstall WCM, reboot your computer and reinstall it again.
3. Please check if LED function is OK on your device,
 - I. if YES,
 - i. Please uninstall WCM
 - ii. Please reinstall software package again.
 - II. if NO,
 - i. Please unplug and plug device and check it again.
4. **Hibernation mode issue:** In order to avoid an issue caused by Microsoft Vista when operating system recovers from hibernate mode, please update the hotfix provided by Microsoft website.
<http://support.microsoft.com/kb/KB946723>
5. **Blue Screen issue:** In order to avoid abnormal situation caused by Microsoft XP SP2, when user uses configure editor, please update the hotfix provided by Microsoft website.

5.2. Why I can't find any base station?

1. Please check if your BS is still alive or not?
2. Please check your bandwidth and frequency setting is correct.
3. If your setting is correct and you still can not find any BS, please reboot your computer and try it again.
4. If you still can't find BS, please report it and contact your support team.

5.3. Why I can't connect to base station?

1. Please check if your BS is still alive or not?
2. Please check if WCM detects your device and LED function of device works.
3. If WCM can't detect your device, please refer to 5.1.
4. If WCM can detect your device and also find BS, but you can't connect to BS, please check if your profile setting is correct, including user ID, password, CA, and etc.
5. If you still can't connect to BS, please exit WCM and unplug and plug your device and try it again.
6. If you still can't connect to BS, please report it and contact your support team.

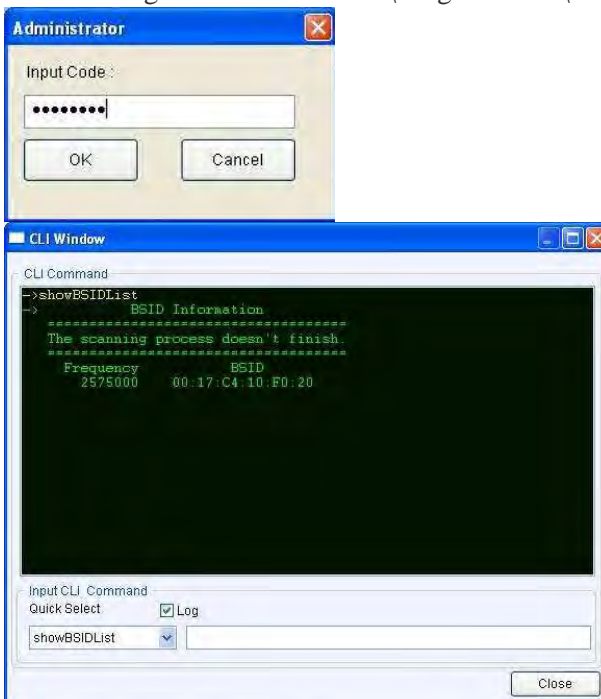
5.4. How to log debug information and report it?

Please open WCM and click on “Tools” tab.



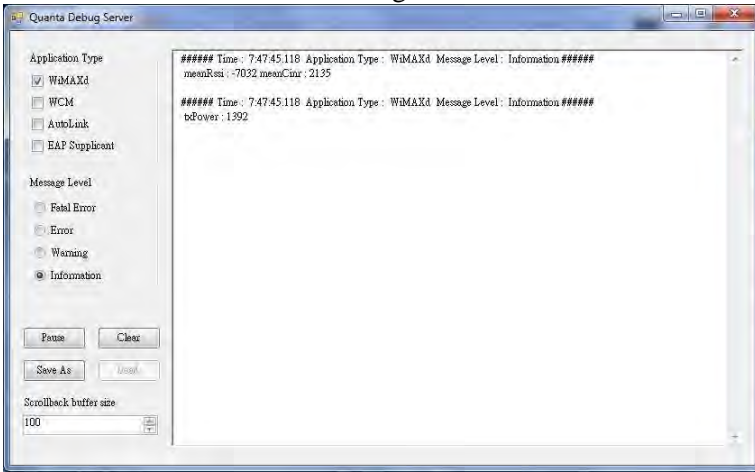
1. For CLI window:

- I. Please click “Popup CLI window” button and input the administrator code “22822281”.
- II. You can run the CLI command and get the response in this window.
- III. The log file is stored in “C:\Program Files\WCM\WiMAXlog.txt”.



2. For Debug Message

- I. Please click “**Debug Message**” button that will pop out another window to have scanning, network link status and EAP log.



Please check application type and message level you want to filter messages. You can click “**Pause**”, “**Start**”, “**Clear**”, “**Save As**”, and “**Load**” button to control tracking messages.

5.5. What does LED activity mean?

The different state information for WU series is as follows:

1. USB dongle:

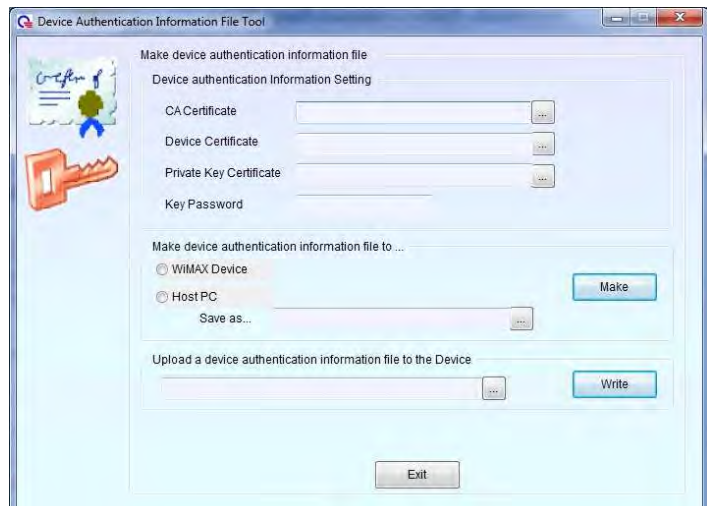


| Device Activity | LED Status |
|------------------|------------------|
| Initialized | Green |
| Firmware Upgrade | Green (Flashing) |
| No Connection | Green |
| Normal Operation | Blue |

6. Appendix

6.1. Create Device Information *.IFO file

1. If you would like to set up a WCM with security, especially Device Authentication and User + Device Authentication, please use WCM to generate the Device Authentication Information file firstly.
2. WCM will import all your necessary certificates and generate a file named *.ifo format.
3. Please enable PKM by selecting **PKMv2_EAP**.
4. Please select “**Device Authentication**” as your authentication method.
5. Please choose “**Host PC**” item and click “**Create New**” button from “**Get Device Authentication Information File from...**” field.
6. Please select your Certificate files.
CA Certificate file
Device Certificate file
Private Key Certificate file
7. Enter your Key Password. If there is no password for authentication, please keep it empty.
8. Select the directory you want to place the *.IFO file. Please choose “**Host PC**” item. “**WiMAX Device**” item is for feature.
9. Click “**Make**” button to generate *.ifo file.
10. You have created **Device Authentication Information File** successfully.



6.2. Device Authentication

1. Please follow [section 6.1](#) to create Device Authentication Information File before you set up device authentication.
2. Please enable PKM by selecting the “PKMv2_EAP” option.
3. Please select “**Device Authentication**” as your authentication method. WCM will select EAP Method as “EAP-TLS”.
4. Please check the “**Outer Identity**”, it should be “0017C4XXXXXX”.
5. 0017C4XXXXXX is the MAC address of your device. Please type ipconfig/all in the DOS command window to check whether it matches your MAC address or not.
6. Please input postfix (Realm) of “Outer Identity”.
7. Please load your CA Certificate.
8. Please load your Device Authentication Information File from your local hard disk.
9. You can click “**Create New**” button to create new one used for device authentication.
10. Please select NWG spec as R1.0 or Draft or No Decoration.
11. Please click “**Save Setting**” button to save all authentication settings.
12. If you want to reset to default setting, please click “**Reset**” button.
13. If the “Outer Identity” is empty, please exit this WCM and take out your WiMAX device.
14. You must plug in your WiMAX device firstly



before you configure device authentication, otherwise WCM can NOT detect and get your device MAC address and can NOT put its MAC address as outer identity for device authentication.

15. Once you have plugged in your WiMAX device, please open WCM and wait for 5 seconds for WCM to initialize your device and get MAC address. Then you can start to configure device authentication.
16. Now, you can connect to base station successfully.

6.3. User and Device Authentication

1. Please follow [section 6.1](#) and [section 6.2](#) to create Device Authentication Information File before you set up user and device authentication.
2. Please enable PKM by selecting the “PKMv2_EAP” option.
3. Please select “**User and Device Authentication**” as your authentication method. WCM will select EAP Method as “**EAP-TTLS**”
4. Please select Inner EAP, such as PAP, CHAP, MSCHAP and MSCHAPV2.
5. Please input postfix (Realm) of “Outer Identity”.
6. Please load your CA Certificate.
7. Please input “**User ID**”.
8. Please input “**User Password**”.
9. Please load your Device Authentication





Information File from you local hard disk.

10. You can click “**Create New**” button to create new one used for device authentication.
11. Please select NWG spec as R1.0 or Draft or No Decoration.
12. Please click “**Save Setting**” button to save all authentication settings.
13. If you want to reset to default setting, please click “**Reset**” button.
14. If the “Outer Identity” is empty, please exit this WCM and take out your WiMAX device.
15. You must plug in your WiMAX device firstly before you configure device authentication, otherwise WCM can NOT detect and get your device MAC address and can NOT put its MAC address as outer identity for device authentication.
16. Once you have plugged in your WiMAX device, please open WCM and wait for 5 seconds for WCM to initialize your device and get MAC address. Then you can start to configure device authentication.
17. Now, you can connect to base station successfully.

6.4. Functional Button

The following Configuration File parameters affect the WCM behavior.

6.4.1. Profile

1. “**Auto Mode**” On/Off, select on to enable automatic connection.
2. “**NWG R1.0.0**” option, use decoration with the format {am=1} preceding outer identity.
3. “**NWG Draft**” option, use decoration with the format {1} preceding outer identity.
4. “**No Decoration**” option, use no decoration preceding outer identity.
5. “**Save Setting**” button, click to save current setting into active profile.
6. “**Reset**” button, click to reset current setting to default.
7. “**Generate**” button, click to generate random outer identity.
8. “**Static Outer Identity**” option, check it to use static outer identity as user defined one.
9. “**Save**” button, click to save operator password once you change it.
10. “**Scan Setting**” button, click to open scan setting.



6.4.2. Scan

1. “**Disconnect**” button, click it to disconnect with current base station. If your WCM is in “Auto Mode On” state, WCM will reconnect to BS automatically. This action of “Disconnect” button will not cause WCM to switch off Auto Mode.
2. “**Scan Base Station**” button, click it to do manual scanning. This function is valid if and only if you switch “Auto Mode” off.
3. “**Start/Stop**” button, click it to start/stop the WiMAX RF.
4. “**Operator Allowed List**” button, click it to add, delete, and clear allowed operator list.
5. “**Add**” button, click it to add new operator ID into allowed list.
6. “**Clear All**” button, click it to clear all allowed list.
7. “**Load Default**” button, click it to load default allowed list.
8. “**Save Setting**” button, click it to save current operator allowed list.
9. “**Close**” button, click it to close current window.

Ex.,

Target BS group1 (HEX format)

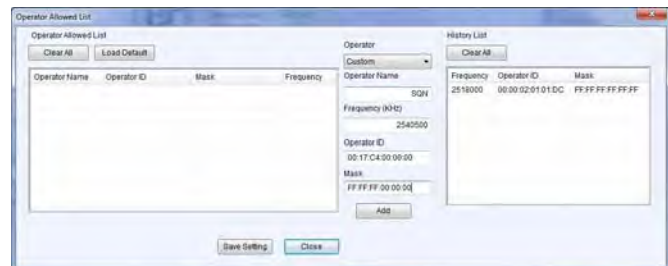
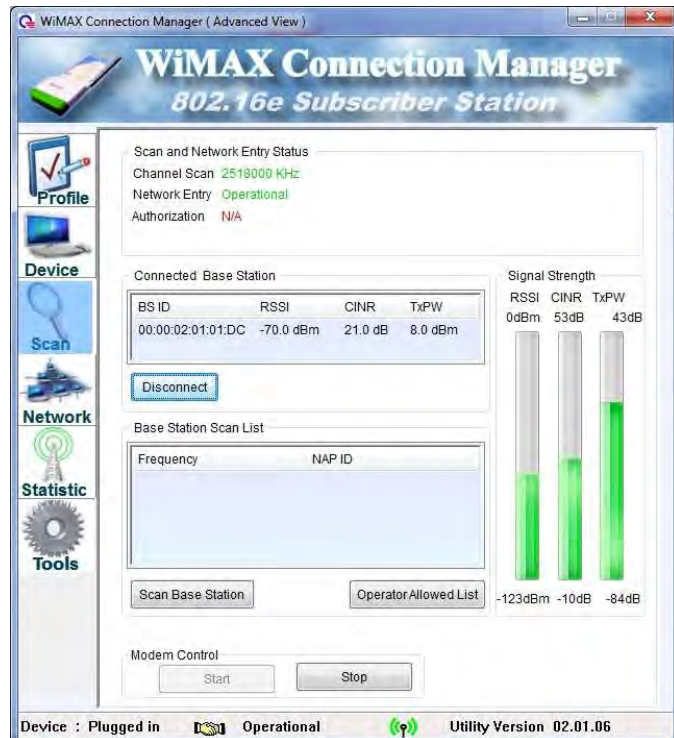
00:00:17:10:21:14

00:00:17:10:21:15

00:00:17:10:21:16

00:00:17:10:21:17

So, you can define the Start Operator ID and mask1



as

Start Operator ID = 00:00:17:10:21:14

mask1 = FF:FF:FF:FF:FF:FC

Target BS group2 (HEX format)

00:00:18:10:11:11

00:00:18:10:xx:yy

So, you can define the Start Operator ID and mask2

as

Start Operator ID = 00:00:18:10:11:11

mask2 = FF:FF:FF:FF:00:00

6.4.3. Network

1. “**IP Release**” button, click it to release current IP address.
2. “**IP Renew**” button, click it to renew the lease time of current IP address.

NOTICE:

IP release/renew buttons are for you to manually release/renew IP address. Basically, you don't need to do that, unless MS can not release/renew IP address. However if MS enters network entry and gets IP address successfully. Once if you click IP release button, BS will deregister MS and force MS to do network entry procedure.



6.4.4. Statistic

1. “Service Flow Refresh” button, click it to refresh the status of service flow.



6.4.5. Tools

1. “Popup CLI Window” button, click it to show a CLI window for CLI commands.
2. “Upgrade” button, click it to open upgrade wizard.
3. “Debug Message” button, click it to open Debug Message window.
4. IOT block, set IOT mode for different BS.
5. Debug Setting block:

Debug Port: UDP port “1234”

Debug IP: IP address “127.0.0.1”.

Enable debug message: Enable to show the debug messages in Debug Message tool.

Save Debug Setting: Save the debug settings.

