



AC650 Wireless Dual Band USB Adapter

Quick Start Guide



Foreword

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	June 2024

Table of Contents

Foreword.....	I
1 Product Introduction	1
1.1 Product Description.....	1
1.2 Product Features	1
1.3 Application Topology.....	1
2 Installation and configuration.....	3
2.1 Hardware Installation	3
2.2 Software Installation.....	3
Appendix 1 Hardware Specifications.....	5
Appendix 2 Security Commitment and Recommendation.....	6

1 Product Introduction

1.1 Product Description

The AC650 Wireless Dual Band USB adapter, using the USB2.0 interface, the application of IEEE802.11ac standard design, while backward compatible with 802.11a/b/g/n wireless devices. It adopts 1×1 MIMO (multiple input and output) architecture and supports 2.4GHz or 5GHz wireless dual-band connectivity. 5G(802.11ac) speeds up to 433Mbps and 2.4G(802.11ac) speeds up to 200Mbps. As a result, there is no need to worry about signal interference from nearby wireless devices and home appliances, ensuring high-quality connectivity to applications such as high-definition video and online games, giving you a purer wireless environment. Support WPS one-key encryption, just press the WPS button, you can quickly and easily transfer encrypted data to the wireless network, thereby preventing the intrusion of illegal users.

1.2 Product Features

- 2.4GHz or 5GHz dual frequency band wireless connection.
- Compatible with IEEE802.11ac standard, backward compatible with 802.11a/b/g/n.
- Support 64/128bit WEP, WPA and WPA2 advanced security encryption.
- USB 2.0 interface.
- Support Windows XP/Vista/7/8/10, Mac, Linux operation system.

1.3 Application Topology

The AC650 Wireless Dual Band USB adapter connects wirelessly to a desktop or laptop computer within the area of an existing LAN.



NOTEThe icon is a small, stylized graphic of an open book with two pages visible.

This wireless card only supports Windows X/Vista/7/8/10, Mac, and Linux operating systems.

2 Installation and configuration

2.1 Hardware Installation

AC650 wireless dual-band USB wireless network card hardware installation is as follows:

- Step 1 Connect the wireless NIC to any USB port.
- Step 2 Install the wireless NIC driver.
- Step 3 Connect to the wired network.

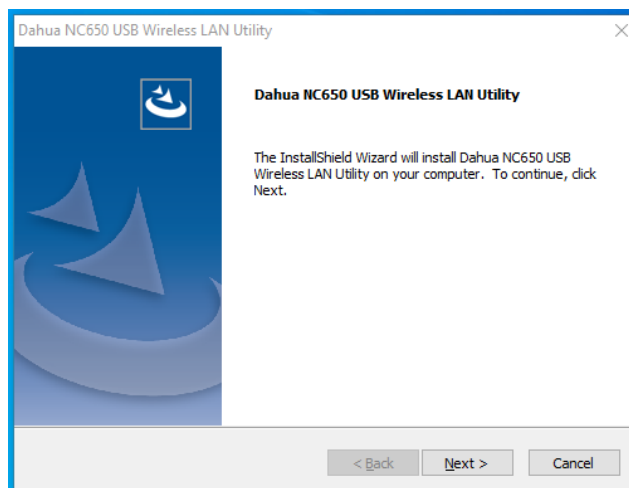
2.2 Software Installation

This section uses Windows10 as an example to describe how to install the wireless NIC driver.

- Step 1 Enter the website "<https://transmission.dahuasecurity.com/en/support/Downloads>", select download "Dahua NC650 USB wireless network card driver" to the computer.
- Step 2 Select the installation package, select the "Setup" application, and then double-click to open the following icon.



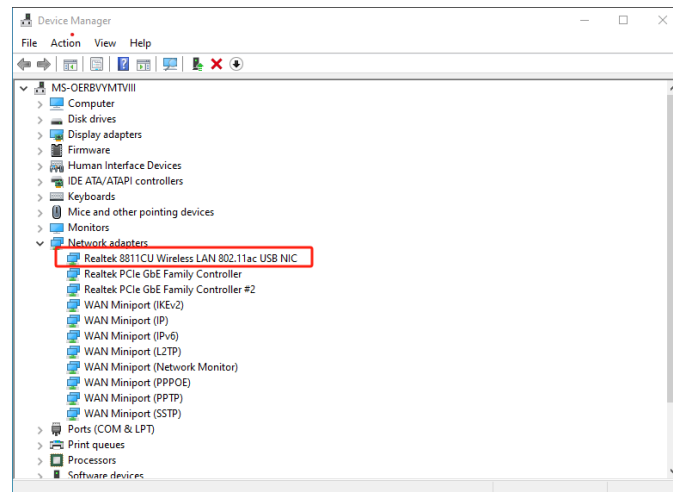
- Step 3 Click the installation wizard to start installing the driver.



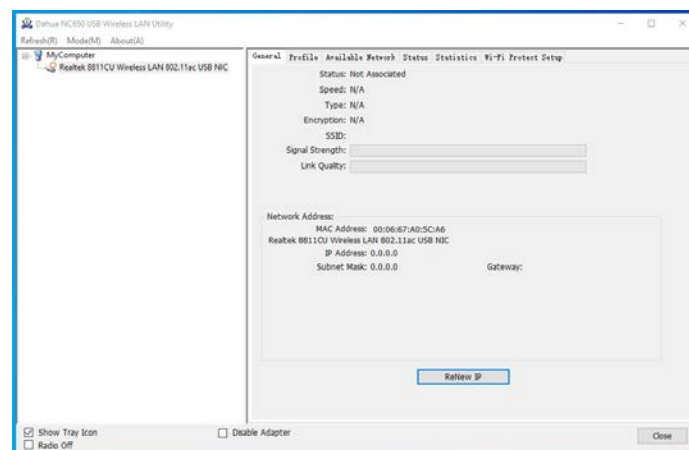
- Step 4 After the driver is installed, click "Finish" to display the following icon.



- Step 5 After the driver is successfully installed, choose "Device Manager" > "Network Adapters", and check whether the NIC driver is successfully installed.



Step 6 Open the  icon, in the "Available Network", select a wired network connection to access the Internet.



Appendix 1 Hardware Specifications

Hardware Specifications	
Standards and Protocols	IEEE 802.11a, IEEE 802.11b ,IEEE 802.11g, IEEE 802.11n, IEEE802.11ac
Operating Frequency	2.4GHz&5GHz
Signal Rate	2.4GHz up to 200Mbps 5G Hz up to 433Mbps
Modulation	IEEE 802.11b: CCK, QPSK, BPSK IEEE 11g/a: OFDM IEEE 11n: QPSK, BPSK,16-QAM,64-QAM IEEE 11ac: BPSK, QPSK,16QAM,64QAM,256QAM
Transmit Power	2.4GHz: 20dBm 5GHz: 20dBm
Interfaces	USB 2.0,USB1.1 Standard
Antenna	1*2dBi 2.5&5G built-in antennas
Dimensions (L* W*H)	15.6*7.4*18.8mm
Environment	Operating Temperature: 0°C~40°C Storage Temperature: -40°C~70°C Operating Humidity: 10%~90%RH non-condensing Storage Humidity: 5%~90%RH non-condensing

Appendix 2 Security Commitment and Recommendation

Dahua attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua's official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

1. Account Management

1.1 Use complex passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters: upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use repeating characters, such as 111, aaa, etc.

1.2 Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

1.3 Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

1.4 Enable account lockout function

The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

1.5 Set and update password reset information in a timely manner

Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

2. Service Configuration

2.1 Enable HTTPS

It is recommended that you enable HTTPS to access Web services through secure channels.

2.2 Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, we recommend you to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

2.3 Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up complex passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.

2.4 Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

3. Network Configuration

3.1 Enable Allow list

It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.

3.2 MAC address binding

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3.3 Build a secure network environment

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;

According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;

Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

4. Security auditing

4.1 Check online users

It is recommended to check online users regularly to identify illegal users.

4.2 Check device log

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

4.3 Configure network log

Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

5. Software Security

5.1 Update firmware in time

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

5.2 Update client software in time

We recommend you to download and use the latest client software.

6. Physical protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188