

Next Generation UTM

NU 系列

快速安裝手冊
QUICK
INSTALLATION
GUIDE

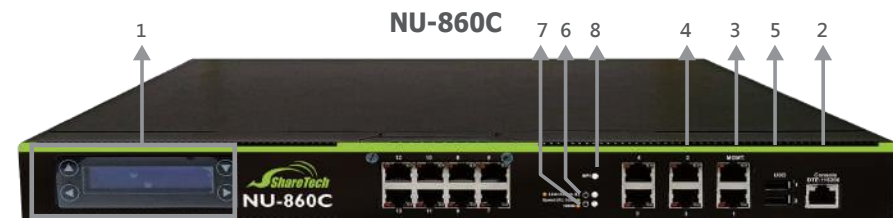
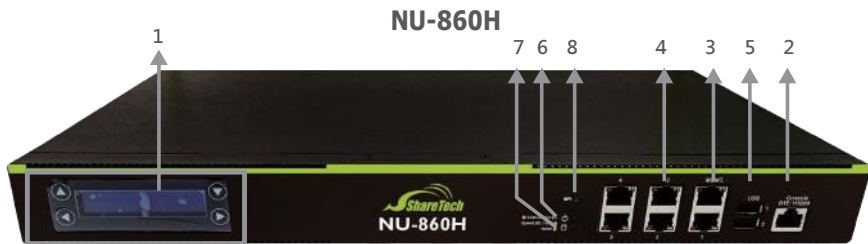
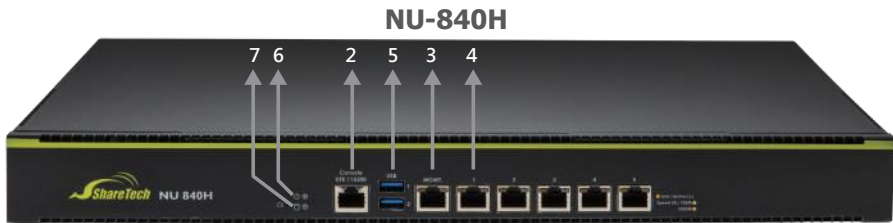
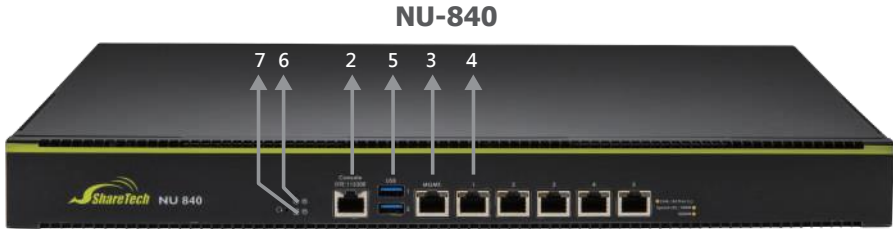
目錄 / Index

繁體版快速安裝指引	2
一、硬體介面	2
1. 硬體介面說明	2
2. 硬體連接設定	4
二、系統設定	5
簡易系統設定步驟	5
English QIG (Quick Installation Guide).....	11
I. Hardware Installation	11
1. Front panel	11
4. Deployment	14
II. System Setting	15
Easy system configuration steps.	15

繁體版 快速安裝指引

一、硬體介面

1. 硬體介面說明



NU-8700C



NU-8700F



NU-8700T



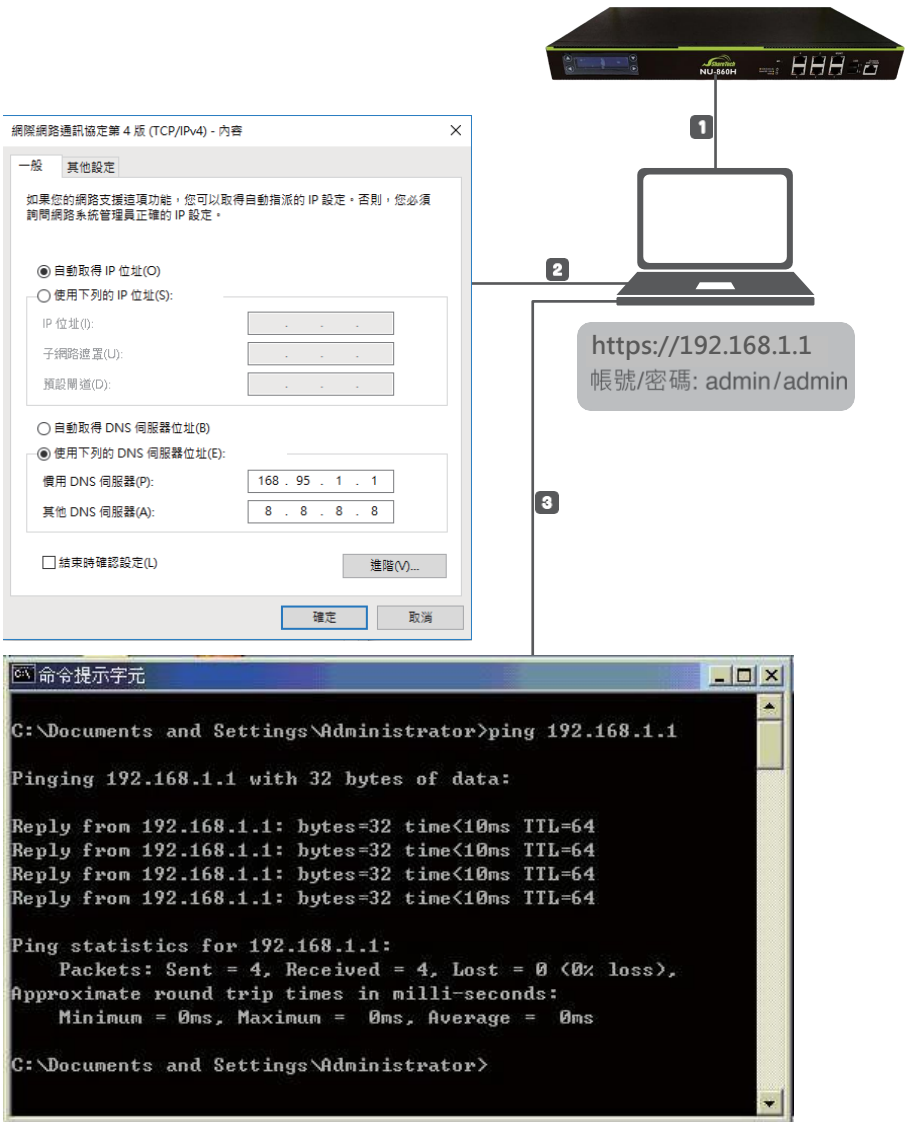
NU-8800T



1. LCM顯示板:	<p>主要顯示包含</p> <p>Status (IP/Mask/Model/CPU)</p> <p>Service (DHCP/DDNS /DNS/ClamAV/SPAM/IPSecVPN)</p> <p>Maintain (Start SSH/Reset Password/Reset IP/Reboot/Power Off)</p>
2. Console Port: DTE 115200	<p>主要的用途是查看系統內部網路介面設定和重置管理員密碼。</p>
3. MGMT. Port:	<p>NU 網路管理介面預設 IP 為 https://192.168.1.1</p>
4. Port :	<ul style="list-style-type: none"> ◆ 可自訂為內部網路介面：與內部交換器連接 ◆ 可自訂為外部網路介面：與外部路由器連接
5. USB Port:	<p>當設備發生意外狀況導致無法正常運作，可透過 USB 裝置進行設定檔快速復原。(USB災難救援功能)</p>
6. POWER LED:	<p>當LED亮綠色燈時，表示系統處於開機狀態。</p>
7. HDD LED:	<p>當LED閃爍綠燈時，表示系統正在讀取或存入資料到內建之硬碟。</p>
8. BP1 LED	<p>當LAN Bypass功能啟動時，會恆亮綠燈。</p> <p>(NU-860H、NU-860T、NU-860C Port4、5和NU-8700C、NU - 8700F、NU-8700T Port 1~4為具有LAN Bypass功能之網路孔)</p>

2. 硬體連接設定

- 1 RJ45, Cat 5e, 連接設備MGMT.埠
- 2 電腦區域網路設定成 DHCP 模式，即可自動取得 192.168.1.x/24 同網段 IP。
- 3 IP 取得後，於設定電腦上 Ping 192.168.1.1



二、系統設定

簡易系統設定步驟

STEP 1

開啟瀏覽器

- IP : <https://192.168.1.1>
- 帳號/密碼 : admin / admin
- 選擇介面語系

STEP 2

設定安裝精靈

- LAN 設定
- WAN 設定
- URL 黑名單設定
- 防護設定
- 郵件管理

STEP 1. 開啟瀏覽器 (Chrome)

1.1 輸入遠端登入網址

打開Chrome 瀏覽器，於網址輸入 **https://192.168.1.1**



1.2 輸入登入帳號/密碼

在彈出的Chrome視窗再次輸入 **admin** (帳號) / **admin** (密碼) 後點選「系統登入」。並選擇介面語系，目前支援英語、繁體中文、簡體中文三種語系。



NU-840

帳號

密碼

記住登入帳號

繁體中文 ▾

系統登入

1.3 登入管理者介面後，將自動開啟安裝精靈，引導管理者完成設定流程。

註: 注意安裝精靈會先清除目前資料，再儲存新設定。



STEP2. 設定安裝精靈

管理者請按下下方右鍵按鈕，進行下一個安裝精靈步驟。

2.1 LAN 設定

請輸入IP 位址與網路遮罩。



2.2 WAN 設定

請按下箭頭選擇所需的連線模式，至少設定一個WAN才可繼續安裝精靈流程。

【STATIC】 需自訂IP位址、網路遮罩和閘道，預設網路遮罩255.255.255.0

【DHCP】 由上端設備主動配發，不需要設定IP位址、網路遮罩和閘道。

【PPPOE撥接】 由電信業者主動配發，不需要設定IP位址、網路遮罩和閘道。如果配發的是固定IP，也可先選STATIC。

The screenshot shows a configuration wizard titled "STEP 2 - 網路介面設置 WAN". At the top, a progress bar indicates six steps: 1 LAN, 2 WAN (current), 3 DSL Blacklist, 4 Security Settings, 5 Mail Management, and 6 Setup Completed. Below the progress bar, there are two tabs: "WAN1" (selected) and "WAN2". The configuration fields for "WAN1" are as follows:

啟用	STATIC
名稱	WAN1
IP 位址	192.168.186.97
網路遮罩	255.255.255.0
預設閘道	192.168.186.1
管理 IP	<input checked="" type="checkbox"/>

At the bottom right, there are three buttons: "取消" (Cancel), a left arrow, and a right arrow.

2.3 URL 黑名單設定

預設關閉，管理者可依照需求開啟此功能，選擇對比模式、輸入URL 或 IP黑名單，或勾選預設黑名單進行管理。

STEP 3 - URL 黑名單設定

1 LAN 2 WAN 3 URL Blacklists 4 Security Settings 5 Mail Management 6 Setup Completed

設定

URL 黑名單 ON

比對模式 完整 模糊

URL 黑名單

IP 黑名單

預設黑名單

<input checked="" type="checkbox"/> 經營暴力	<input checked="" type="checkbox"/> 線上影響	<input checked="" type="checkbox"/> 廣告
<input checked="" type="checkbox"/> 賭博	<input checked="" type="checkbox"/> 勒索	<input checked="" type="checkbox"/> 成人網站
<input checked="" type="checkbox"/> 代理連環彩	<input checked="" type="checkbox"/> 轉賣	<input checked="" type="checkbox"/> 澳門版式
<input checked="" type="checkbox"/> 不雅在網址	<input checked="" type="checkbox"/> 非法盜版	

取消 ← →

2.4 防護設定

預設開啟，管理者可依照需求對於異常IP進行紀錄、通知或阻擋。

STEP 4 - 防護設定

1 LAN 2 WAN 3 URL Blacklists 4 Security Settings 5 Mail Management 6 Setup Completed

防火牆功能

防火牆防護設定 ON

異常IP分析

異常IP分析 記錄 通知 阻擋

SMTP: Password SHOW

Mail server 需要驗證 OFF TLS OFF

收件者

阻擋動作 10 分

內網防護

偽造者偵測: IP ON

偽造者偵測: MAC ON

取消 ← →

2.5 郵件管理設定

預設開啟，管理者可依照需求選擇是否關閉。

STEP 5 - 郵件管理

1 LAN 2 WAN 3 URL Blacklists 4 Security Settings 5 Mail Management 6 Setup Completed

郵件過濾及記錄設定

郵件過濾與記錄 ON

郵件防毒

啟動郵件防毒 ON

使用防毒引擎 ClamAV

取消 ← →

2.6 設定完成

最後顯示設定清單，確認後請按下儲存鍵，請稍後120秒，安裝精靈將儲存此設定。

STEP 6 - 設定完成

1 LAN 2 WAN 3 URL Blacklists 4 Security Settings 5 Mail Management 6 Setup Completed

列表

LAN 啟用: **STATIC** IP: 192.168.1.68 / 255.255.255.0

WAN1 啟用: **STATIC** IP: 192.168.166.97 / 255.255.255.0 預設網道: 192.168.166.1

WAN2 啟用: **OFF**

URL 黑名单設定 **OFF**

防竊設定 防火牆功能: **ON**

異常IP分析: 記錄 **ON** 通知 **OFF** 阻擋 **OFF**

內網防護: 偽造者偵測: IP **ON** 偽造者偵測: MAC **ON**

郵件管理 郵件過濾及記錄設定 **ON** 郵件防毒 **ON**

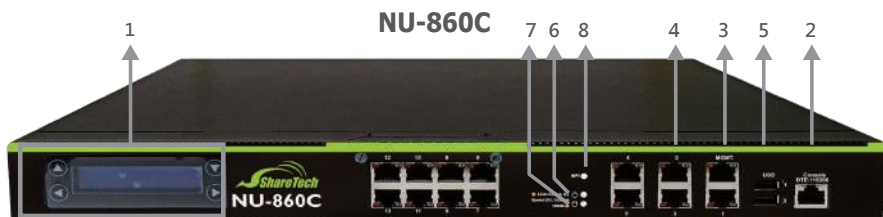
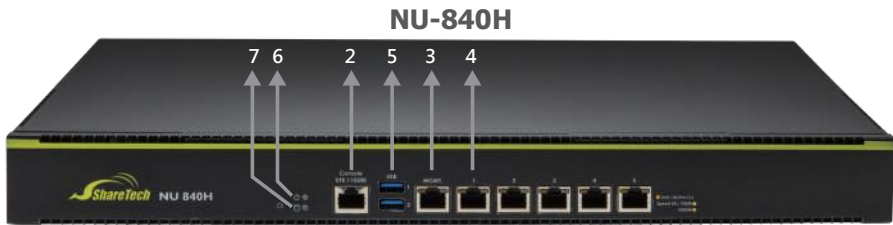
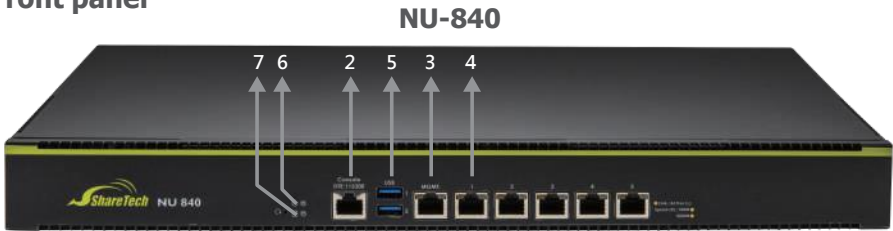
下次不要再出現此視窗

取消 ← 儲存

English QIG (Quick Install Guide)

I. Hardware Installation

1. Front panel



NU-8700C



NU-8700F



NU-8700T



NU-8800T



1. LCM Display:	Mainly displays Status (IP / Mask / Model / CPU) Service (DHCP / DDNS / DNS / ClamAV / IPSec VPN) Maintain (Start SSH / Reset Password / Reset IP / Reboot / Power Off)
2. Console Port: DTE 115200	A console port for inspecting settings or, if needed, resetting the device to factory default.
3. MGMT. Port:	Connects to your computer directly at beginning. The default IP address is https://192.168.1.1.
4. Port:	<ul style="list-style-type: none"> ◆ It can be defined as LAN port and connects to the internal switch. Even though servers located in the internal allow external access, they still receive security protection from NU UTM. ◆ It can be defined as WAN port and connect to the perimeter router.
5. USB Port:	Performs an instant recovery using USB sticks during system suspend.
6. POWER Indicator:	Green light means the power is ON.
7. HDD Indicator:	Blinking green lights means the system is accessing data on the built-in HD
8. BP1 Indicator:	Green light means LAN Bypass is on. (NU-860H, NU-860T, NU-860C port 4&5 and NU-8700C、NU-8700F、NU-8700T Port 1~4 equip with LAN Bypass function.)

2. Deployment

- 1** Connect LAN (RJ45), and Cat. 5e to the device MGMT. Ethernet Port.
- 2** Configure a LAN with DHCP and you'll obtain 192.168.1.x/24(IP segment) automatically.
- 3** After getting the IP, ping 192.168.1.1 to ensure network connection.

The diagram illustrates the deployment process. A switch (MGMT. Ethernet Port) is connected to a laptop. Step 1 shows the physical connection. Step 2 shows the laptop configuration window with the following details:

Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

Alternate DNS server: 8 . 8 . 4 . 4

Advanced...

OK Cancel

Step 3 shows the command prompt output:

```
C:\Documents and Settings\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

A callout box indicates the URL and credentials: `https://192.168.1.1` Account/Password: admin/admin

II. System Setting

Easy system configuration steps

STEP 1

Start Browser

- <https://192.168.1.1>
- Acct./PW :admin / admin
- Select a preferred language

STEP 2

Setup Wizard

- Setup LAN
- Setup WAN
- URL Blacklist
- Security Setting
- Mail Management

STEP 1. Start Browser (Chrome)

1.1 Open the web browser and enter **https://192.168.1.1** in the address bar.



1.2 Enter login Account / Password

Chrome will pop up for authentication, please enter **admin** (account) / **admin** (password) to log in. And select a preferred language for interfaces, currently available in English/ Traditional Chinese / Simplified Chinese.



NU-840

Account

Password

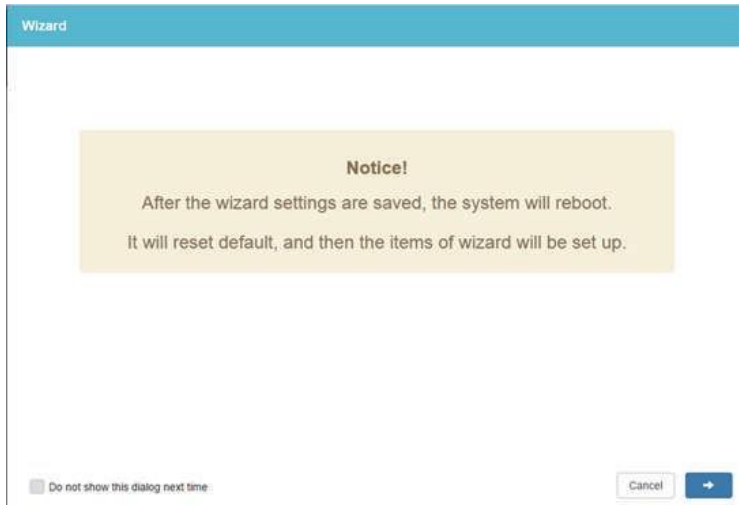
Remember account and password

English ▾

Login

1.3 Login completed. The wizard will automatically pop up to guide you through the configuration.

NOTE: A step-by-step wizard will wipe all your data and settings before saving new settings.



STEP2. Setup Wizard

2.1 Setup LAN

Please enter your IP address and Subnet mask.

The screenshot shows the 'STEP 1 - Network Interface LAN' configuration screen. At the top, a blue progress bar contains six steps: 1 LAN, 2 WAN, 3 URL Blacklists, 4 Security Settings, 5 Mail Management, and 6 Setup Completed. The 'LAN' step is currently selected.

Below the progress bar, the 'LAN' interface is shown with the following settings:

- Enable: STATIC
- Name: LAN
- IP address:
- Subnet mask:

At the bottom right, there are 'Cancel', 'Previous' (left arrow), and 'Next' (right arrow) buttons.

2.2 Setup WAN

Administrators can click on the drop-down arrow to select preferred connection methods. One WAN port must be enabled to proceed.

STATIC: IP address, subnet mask, and default gateway are required to configure WAN setting. The default gateway is 255.255.255.0

DHCP: A connection method that IP address is assigned by a router/switch in the perimeter. IP address, subnet mask, and default gateway are not required.

PPPOE: DSL providers typically use this option. Please enter the account and password provided by your ISP to gain access to the Internet. If your ISP provides you a set IP address, you are able to select STATIC.

STEP 2 - Network Interface WAN

1 LAN 2 WAN 3 URL Blacklists 4 Security Settings 5 Mail Management 6 Setup Completed

WAN1 WAN2

Enable: STATIC

Name: WAN1

IP address: 192.168.186.97

Subnet mask: 255.255.255.0

Default gateway: 192.168.186.1

Management IP:

Cancel + -

2.3 Setup URL Blacklists

URL Blacklist is switched off by default. Administrators can enable the function, select match level, enter blacklisted URL or IP, or select default categories.

STEP 3 - Uri blacklists

1 LAN 2 WAN 3 URL Blacklists 4 Security Settings 5 Mail Management 6 Setup Completed

Setting

URL Blacklist ON

Match level Exact Fuzzy

Blacklisted URL:

Blacklisted IP:

Default Blacklist

<input checked="" type="checkbox"/> Aggressive	<input checked="" type="checkbox"/> Audio-video	<input checked="" type="checkbox"/> Drugs
<input checked="" type="checkbox"/> Gambling	<input checked="" type="checkbox"/> Hacking	<input checked="" type="checkbox"/> Porn
<input checked="" type="checkbox"/> Proxy	<input checked="" type="checkbox"/> Redirector	<input checked="" type="checkbox"/> Spyware
<input checked="" type="checkbox"/> Suspect	<input checked="" type="checkbox"/> Warez	

Cancel

2.4 Setup Security Settings

Security settings are switched on by default. Administrators can select actions taken on detected anomalies.

STEP 4 - Security settings

1 LAN 2 WAN 3 URL Blacklists 4 Security Settings 5 Mail Management 6 Setup Completed

Firewall Protection

Firewall protection ON

Anomaly Detection

Anomaly Detection Log Notify Block

SMTP: Password

Mail server Authentication TLS

Recipient

Blocking actions:

Intranet Protection

Collision detection : IP ON

Collision detection : MAC ON

Cancel

2.5 Setup Mail Management

Filtering log and anti-virus are switched on by default. Administrators can choose manually to switch off if it is not required.

STEP 5 - Email management

1 LAN 2 WAN 3 URL Blacklists 4 Security Settings 5 Mail Management 6 Setup Completed

Filter Log

Filter log ON

Anti-Virus

Anti-virus ON

Virus engine ClamAV

Cancel

2.6 Setup Completed

To save your configuration settings, click the Save button in the lower right corner. Please wait for the Setup Wizard to finish. This could take up to 120 seconds.

STEP 6 - Setup Completed

1 LAN 2 WAN 3 URL Blacklists 4 Security Settings 5 Mail Management 6 Setup Completed

List

LAN Enable : STATIC IP : 192.168.1.1 / 255.255.255.0

WAN1 Enable : STATIC IP : 192.168.186.97 / 255.255.255.0 Default gateway : 192.168.186.1

WAN2 Enable : OFF

Url blacklists ON

Security settings Firewall Protection : ON

Anomaly Detection : Log ON Notify OFF Block OFF

Intranet Protection : Collision detection : IP ON Collision detection : MAC ON

Email management Filter Log ON Anti-Virus ON

Do not show this dialog next time

Cancel