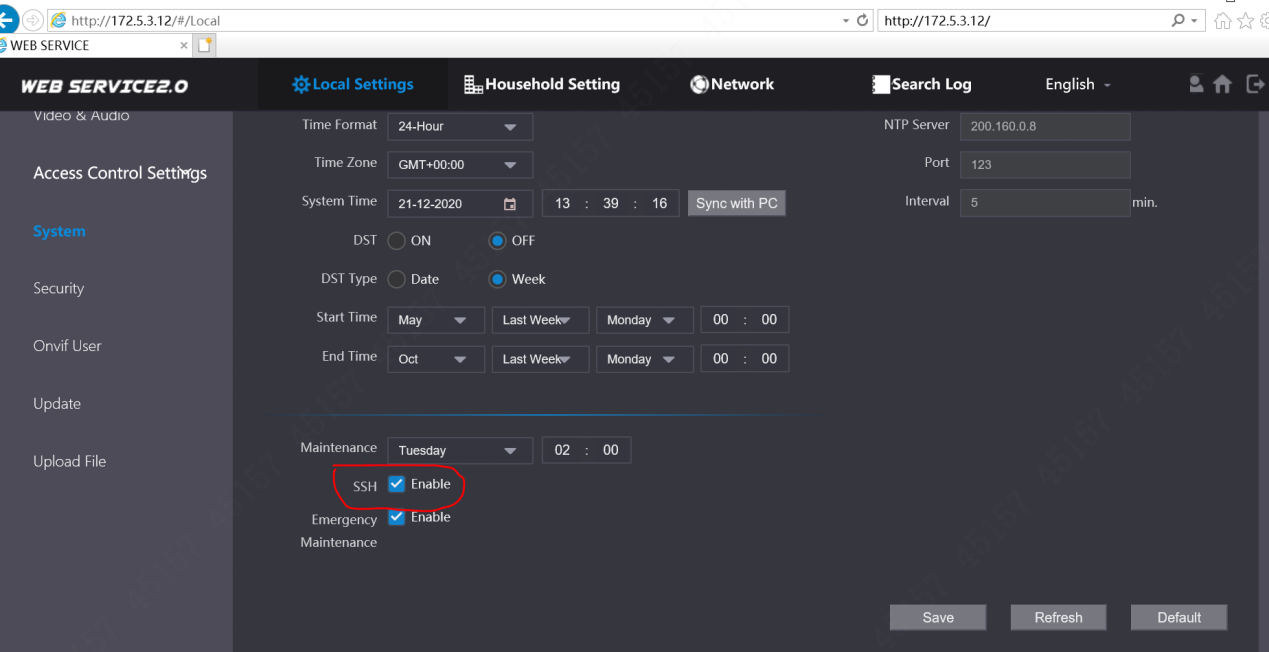
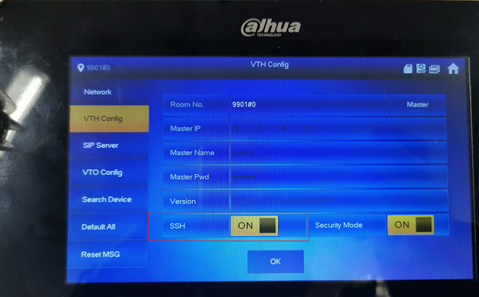
**Network Mount Capture**

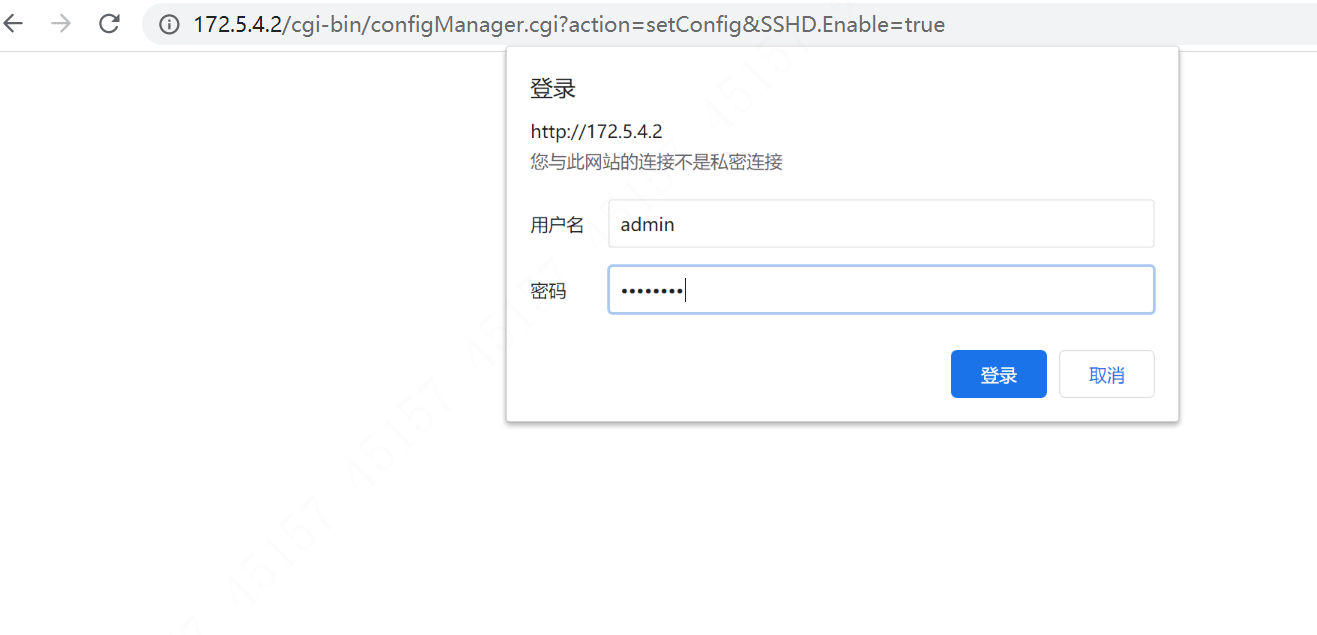
At present, we have the SSH enable item for the intercom devices, including VTH and VTO, we need to enable SSH first if this option is off. For VTH, we can enable SSH in VTH Config. And we can also find it on the web page for VTO, as shown below:

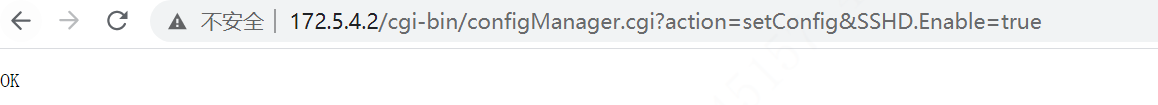




If it does not work, we can also use cgi command to enable SSH:

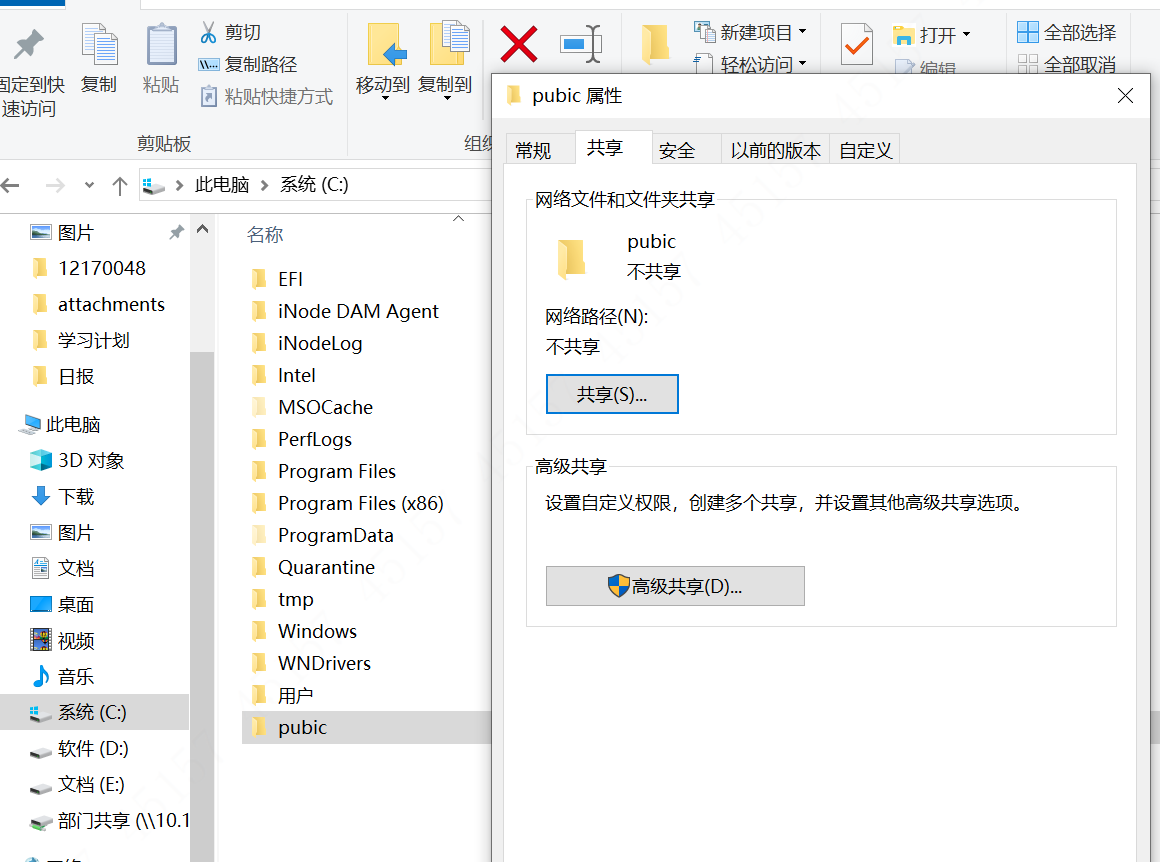
**http://device IP/cgi-bin/configManager.cgi?action=setConfig&SSHD.Enable=true**



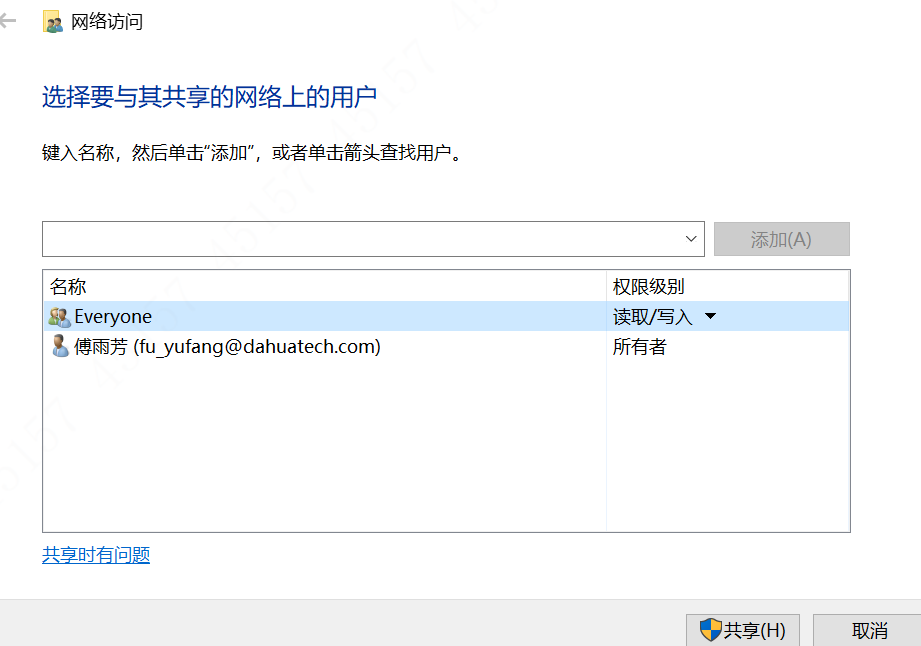


1. **Create Public Folder**

Then we start to set NFS configurations. First, we create a public folder---this folder is the output of NFS server. For example, we create the public folder in disk C. Right click the folder property, select “sharing”,

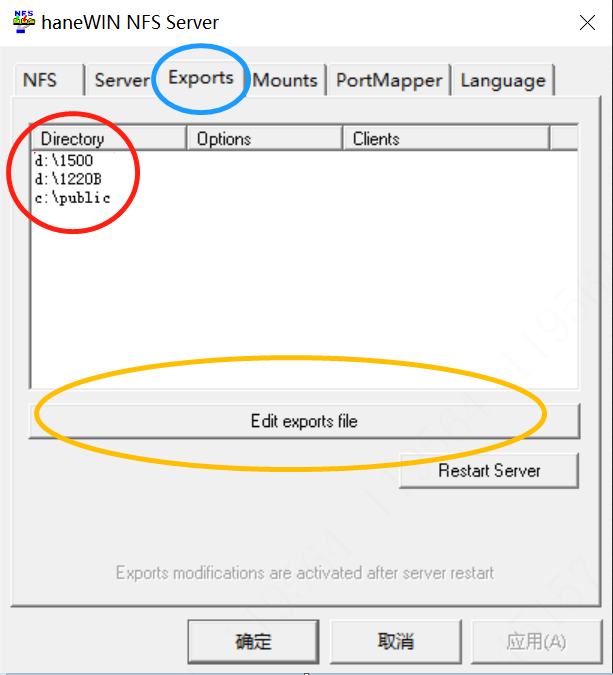


And then search for “everyone” in the user input, choose authorization level as “read/write”.



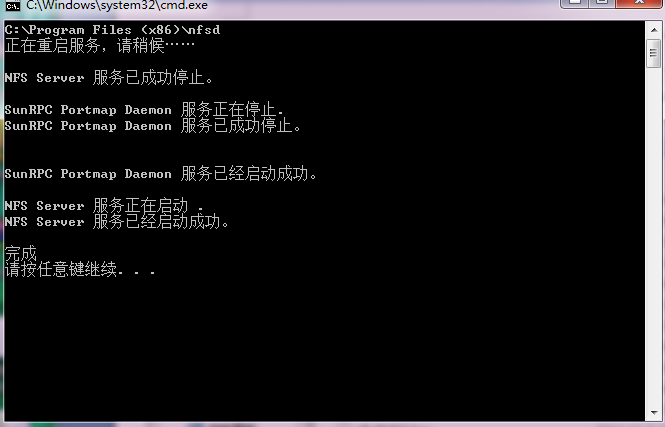
1. **Install NFS Server**

Then we install nfs1169.exe (choose default installation--- just click “next” until it shows finish). , we run it as an administrator and select “output” in the navigation bar.

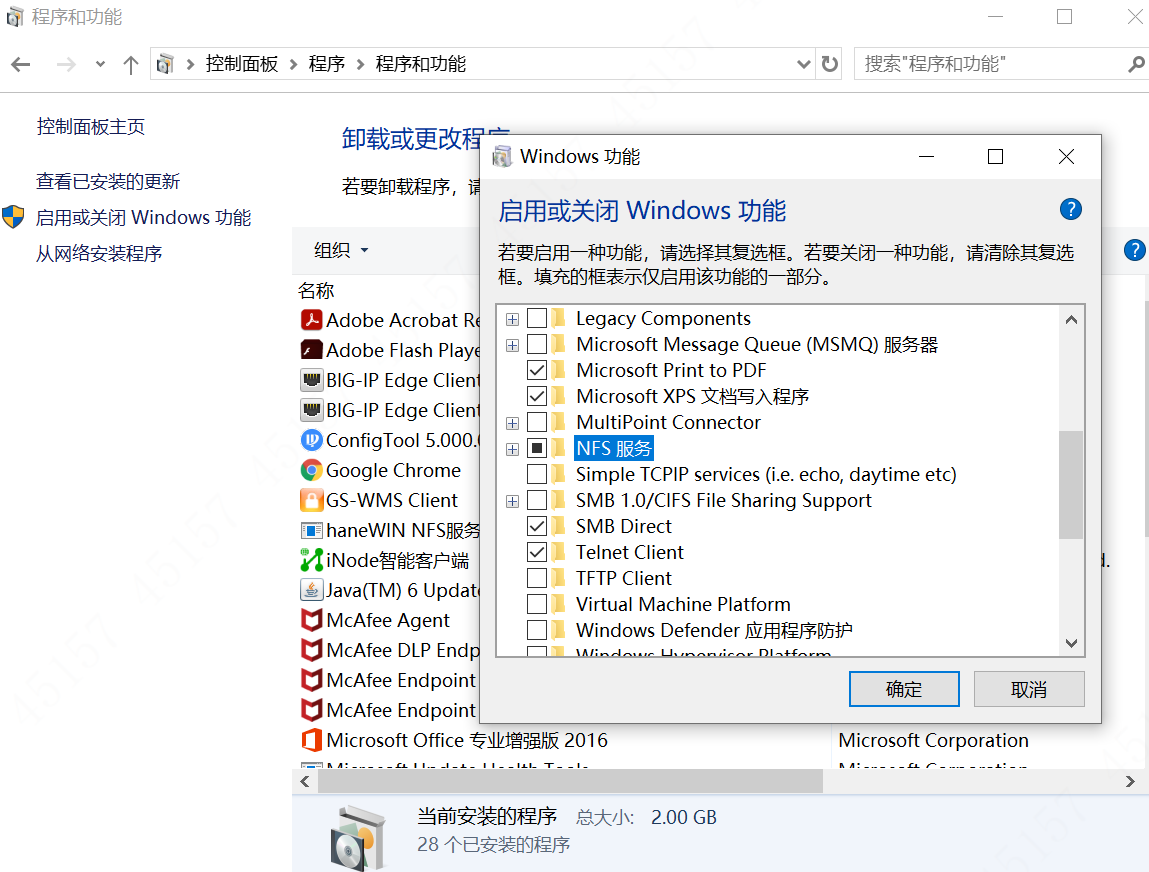


Click “Edit output file” and modify the path (for e.g. c:\public here, same as the public folder we create) in the popup and save.

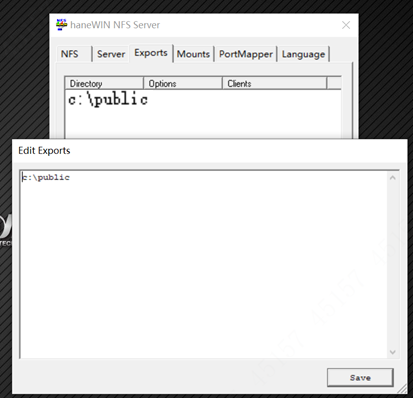
Next, we need to look for the installation direction for nfs server, it is “C:\Program Files (x86)\nfsd” by default, run “RestartService.bat” as an administrator, as shown below:



If it does not work, we need to restart NFS service manually through “control panel”—“service” to find the NFS service.

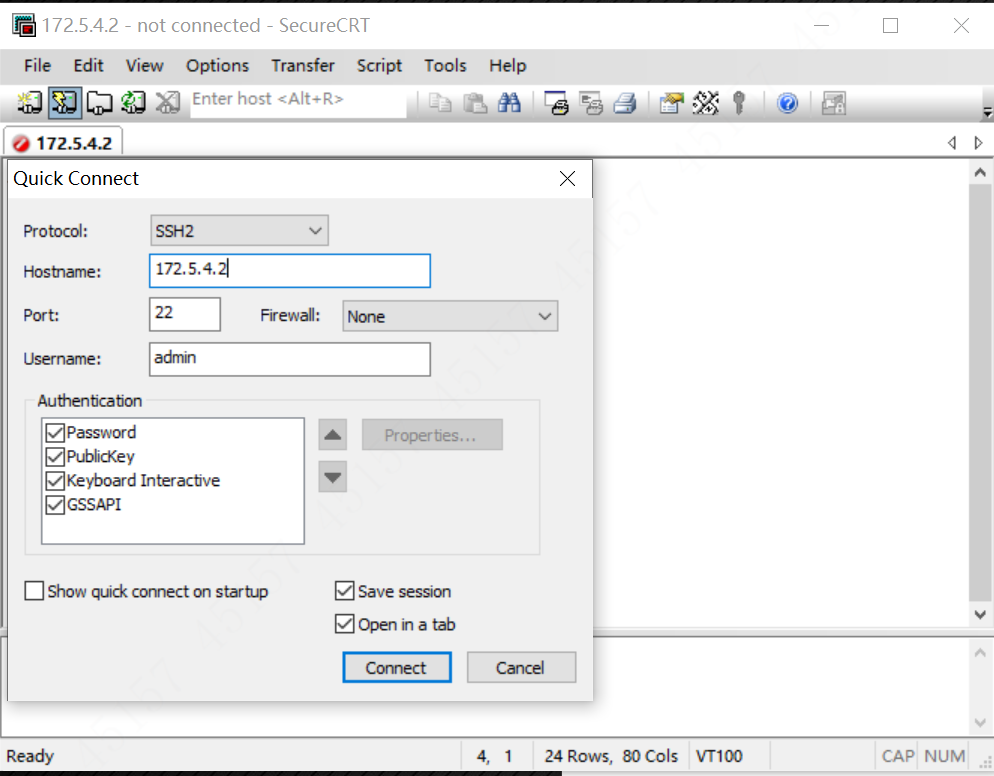


After restarting the service, check if the output is changed.



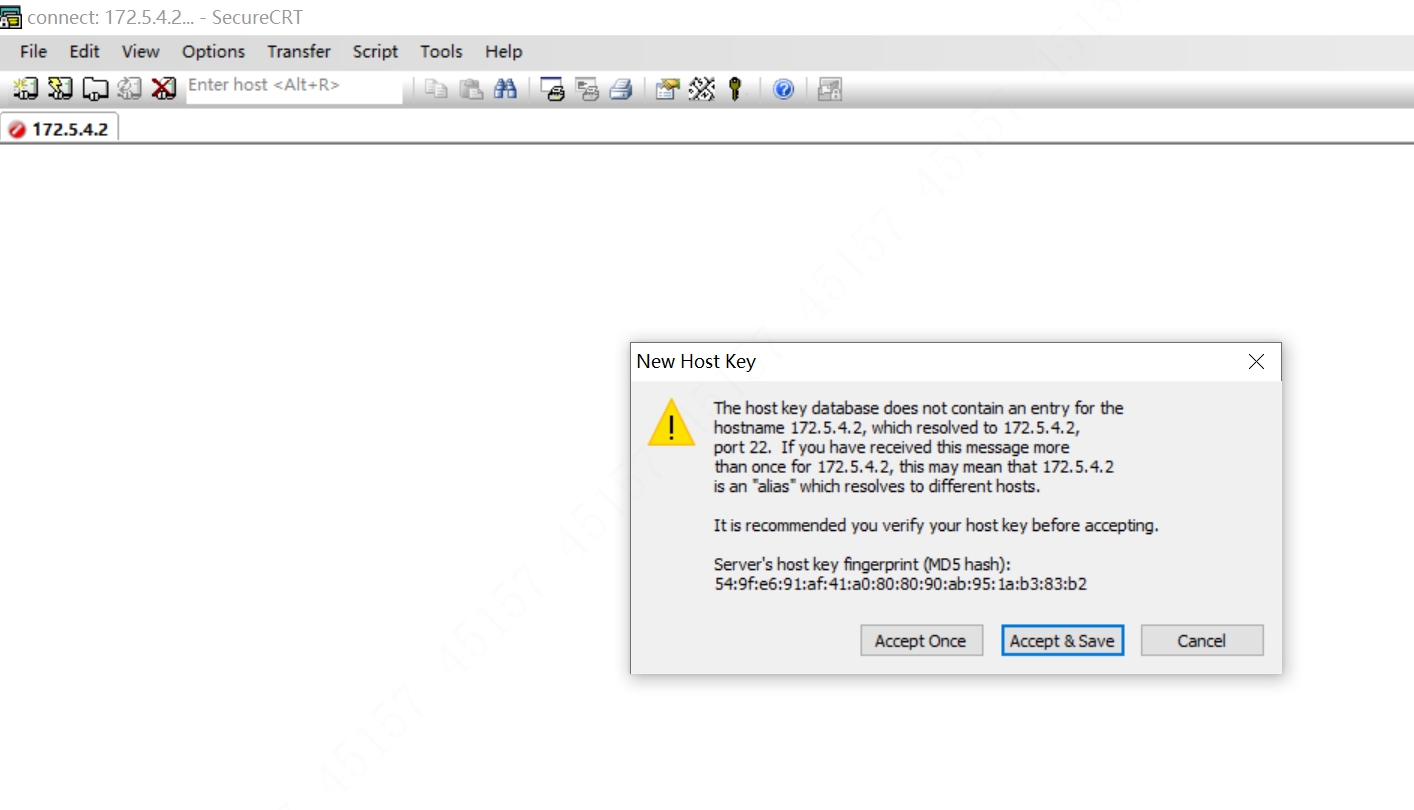
1. **Log in the Device through CRT**

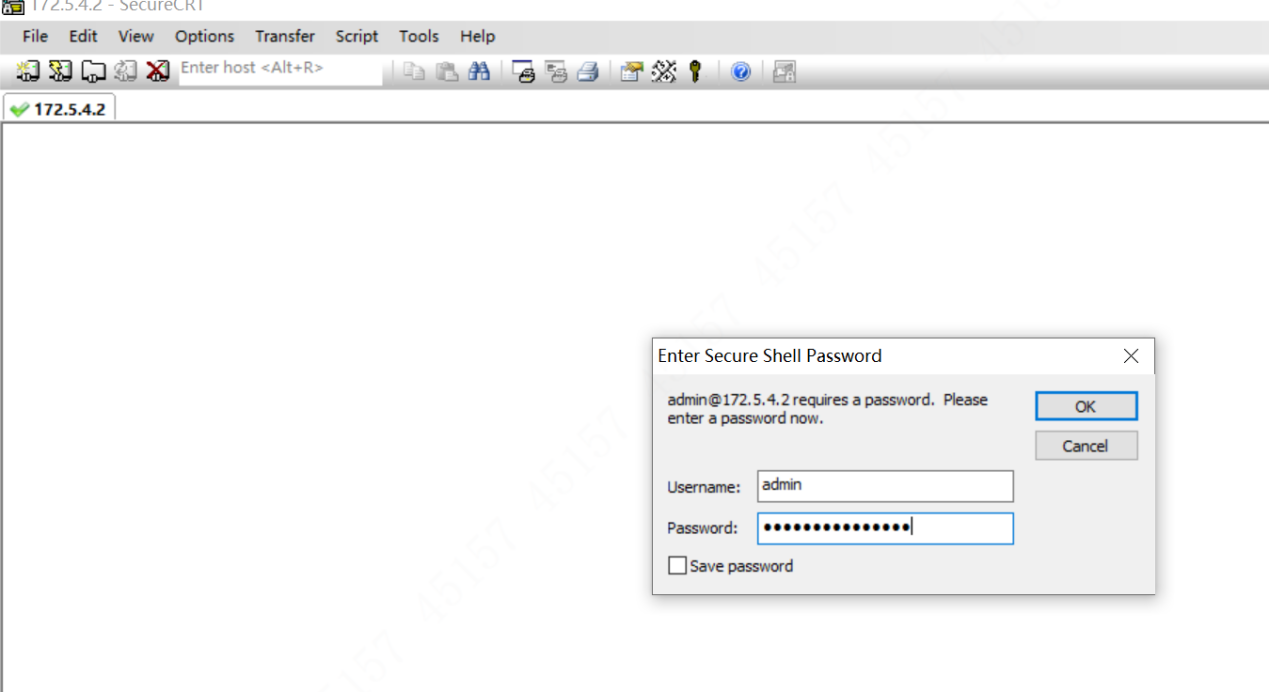
Then we log in secure CRT via SSH2.



Click “connect” button and input the user name and password---**7ujMko0+device password**

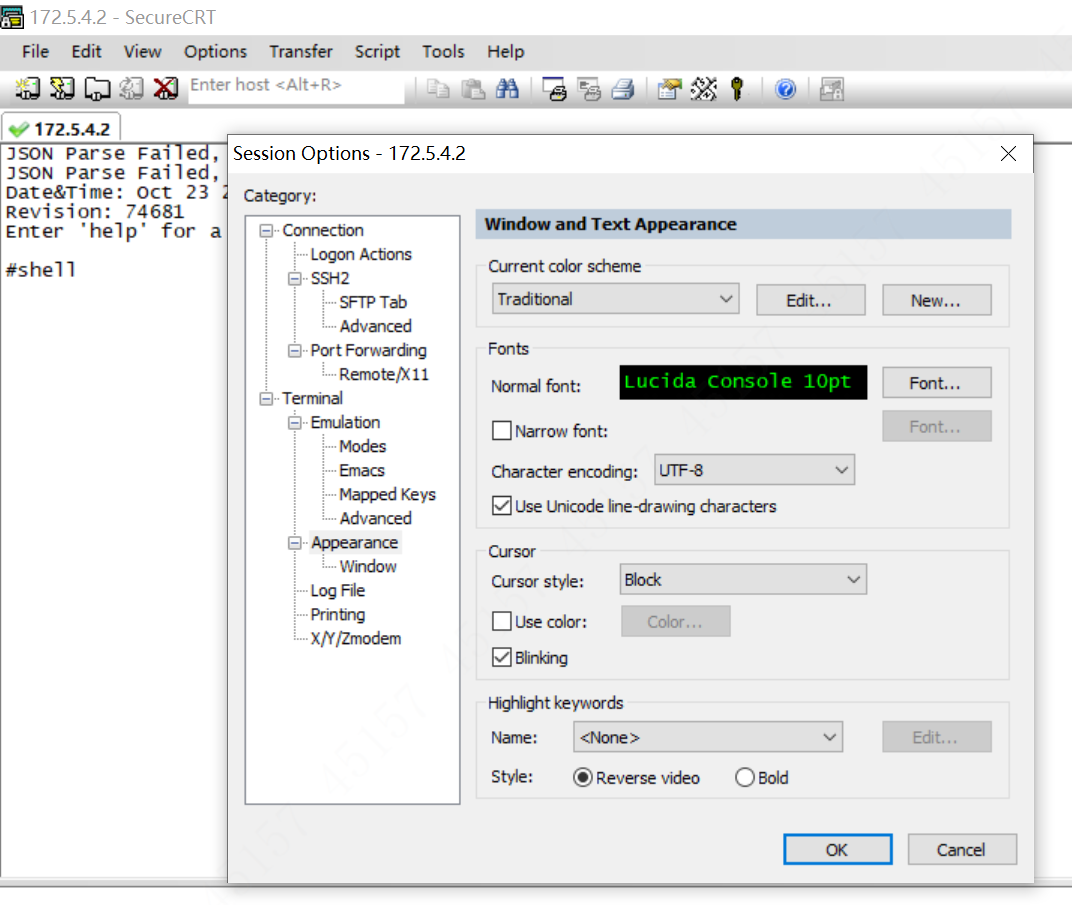
(For example, if the VTO password is admin123, so the password is **7ujMko0admin123;** For VTH or VTS, if the project password is 123456, then the password is **7ujMko0123456** ).



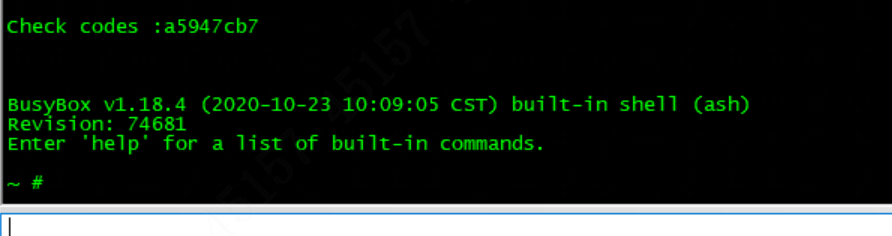


1. **Mount and Capture**

Then we are able to connect the device. Input shell, press enter and input domain account and password. Before press Enter, modify the option—appearance—character encoding as UTF-8. Otherwise, it may appear as nonsense coding.



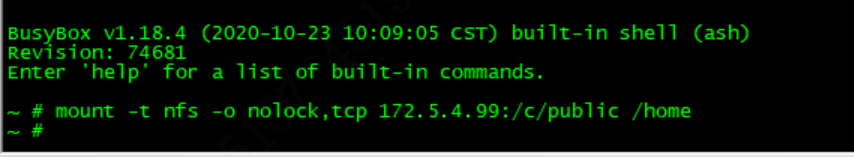
And then press Enter and you will see a QR code, scan it and enter your domain password, you will get the check codes. Input the code and log in device background by SSH successfully.



Note: do not hesitate for too long, or the code can be invalid. Once error occurs, just enter shell again and scan the new QR code.

“~ #” means log in successfully.

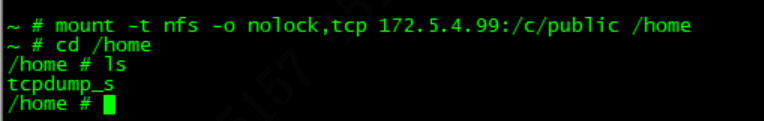
Then input the mount command: **mount –t nfs –o nolock,tcp 172.5.4.99:/c/public /home** (Note that here we need our PC’s IP)



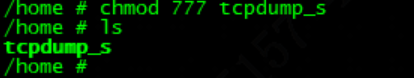
After entering this command, it shows "#" which means success.

Note that the mounting is always valid if we do not reboot the device. If we need to restart the mounting service or changing output direction we need to restart the server. If the mounting does not work, check if all firewalls are off.

Then we will start capturing the packet Here we take “**tcpdump\_s**” as an example. Copy tcpdump\_s(for security baseline firmwares) into the public folder. On terminal, go to home folder path by”**cd /home** ” and check if there is tcpdump\_s file by “**ls**”



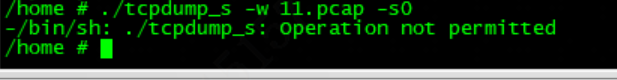
And then we give it authorization using the command: **chmod 777 tcpdump\_s**



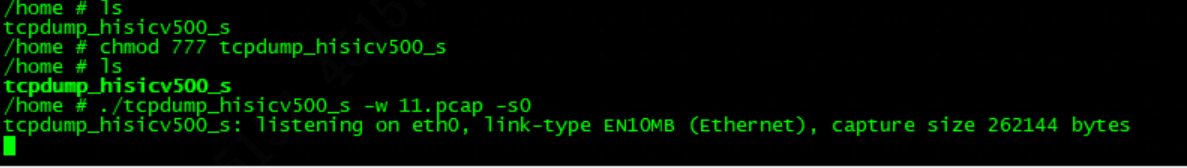
Now we have finished mounting and we are ready to listen.

Enter :”**./tcpdump\_s -w 11.pcap -s0**”

If it shows the operation is not allowed, like this:



Just change another tcp file and try it again.



When finish capturing, input **ctrl+z** to stop. You can see the wireshark file in the public folder.

