

# Troubleshooting: FindIT v. 2.1.1 Probe Software for the Raspberry Pi

## Objective

This article shows the steps for a successful fresh install of FindIT v. 2.1.1 Probe Software with the Raspberry Pi OS Buster version.

## Applicable Devices | Software Version

FindIT | 2.1.1

## Introduction

Let's talk about FindIT 2.1.1 Probe Software when using a Raspberry Pi and the Raspberry Pi OS Buster version.

Are you about to do a fresh install, or have you tried to do a fresh install and received error messages and a failed download? Are you using a Raspberry Pi as a FindIT probe?

For most installations with Raspberry Pi and FindIT, you simply flash a software image onto a micro SD card, put it into the Pi, and run the installer. Upgrades are snap as well.

Unfortunately, there is a little bump in the road when you do a fresh install of FindIT v. 2.1.1 with the Raspberry Pi OS Buster version.

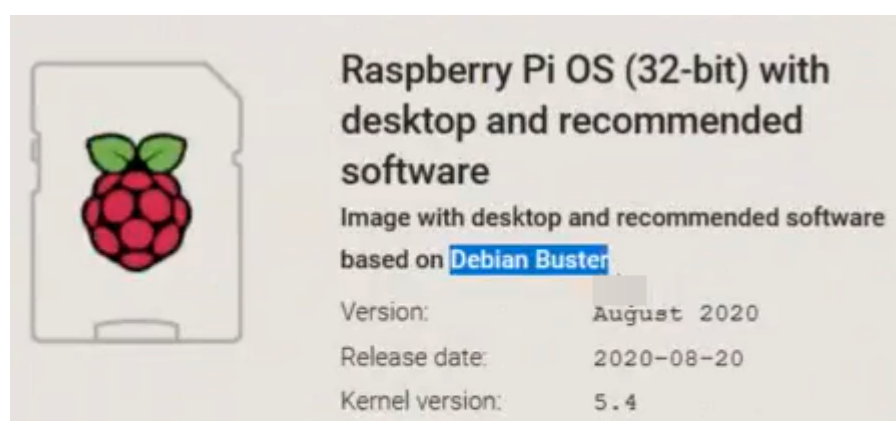
Whether this is your first attempt or you had a failed installation, you must follow these instructions. If your installation failed, the permissions changed so you essentially have to start over. I know, it's a bummer, but just follow these steps for success.

## Download and Flash the Image

### Step 1

Navigate to [Raspberry Pi Downloads](#) and download the appropriate version for your operating system. Open the download and unzip if needed. Flash the image to the micro SD card of the Raspberry Pi using a utility such as [etcher](#).

If you already have this installed, you do not need to install this a second time, but you should confirm you have the correct software.



## Step 2

Download [FindIT Network Probe 2.1.1 all languages installer for Raspberry Pi \(Debian Buster\)](#).

Cisco FindIT Network Probe 2.1.1 all languages installer for  
Raspberry Pi (Raspbian Buster)  
finditprobe-2.1.1.20200521-raspbian-buster\_armhf.signed.sh

01-Jun-2020

12.42 MB



By default, Secure Shell (SSH) is disabled with a fresh Raspberry Pi OS image. It can be enabled by using the command **sudo raspi-config** and then use the menus to enable it. An alternate option would be to create a shortcut by creating a blank file called **ssh** on the memory card before you insert it into the Pi. If you use the second option, make sure there is no file extension in the file name.

## Step 3

Put the micro SD card into the Raspberry Pi and power it up.

## Step 4

Open the command prompt on your computer. Ping the IP address of the Pi to test for connectivity. When you see the reply messages, you can proceed.

```
Command Prompt - ping 10.0.0.200 -t
Microsoft Windows [Version 10.0.17134.1667]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\j...>ping 10.0.0.200

Pinging 10.0.0.200 with 32 bytes of data:
Reply from 10.0.0.102: Destination host unreachable.
Request timed out.
Request timed out.
Request timed out.

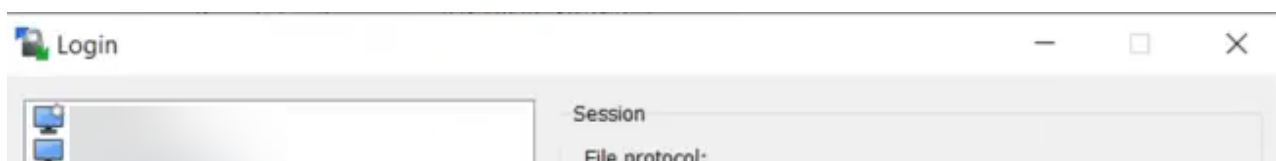
Ping statistics for 10.0.0.200:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),

C:\Users\j...>ping 10.0.0.200 -t

Pinging 10.0.0.200 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 10.0.0.200: bytes=32 time=8ms TTL=64
Reply from 10.0.0.200: bytes=32 time=1ms TTL=64
Reply from 10.0.0.200: bytes=32 time=2ms TTL=64
Reply from 10.0.0.200: bytes=32 time=2ms TTL=64
Reply from 10.0.0.200: bytes=32 time=4ms TTL=64
Reply from 10.0.0.200: bytes=32 time=2ms TTL=64
Reply from 10.0.0.200: bytes=32 time=1ms TTL=64
```

## Step 5

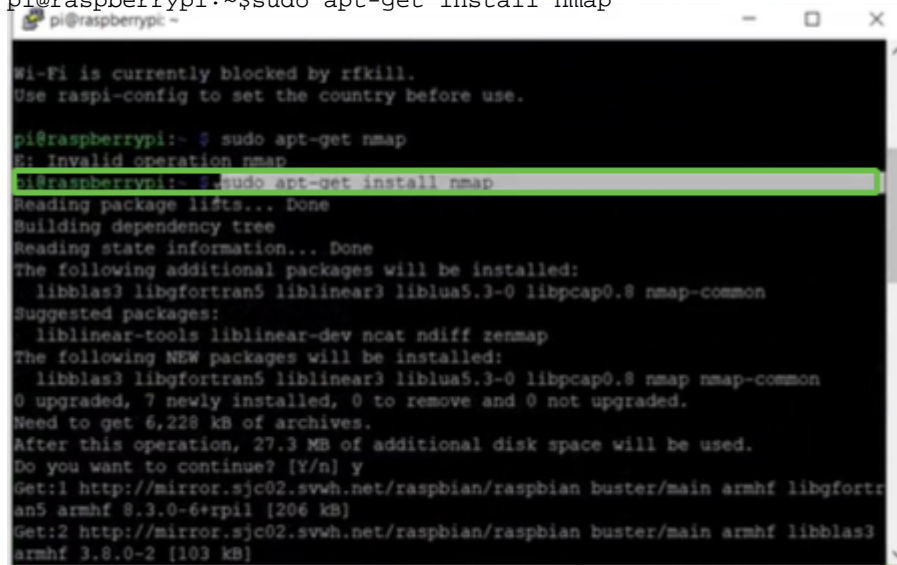
Use an SFTP client, such as WinSCP, to access the Raspberry Pi. The default password is *raspberrypi*.



## Step 6

Enter the following command. Keep in mind that it takes some time between each of these steps. Be patient, it's worth it!

```
pi@raspberrypi:~$sudo apt-get install nmap
```

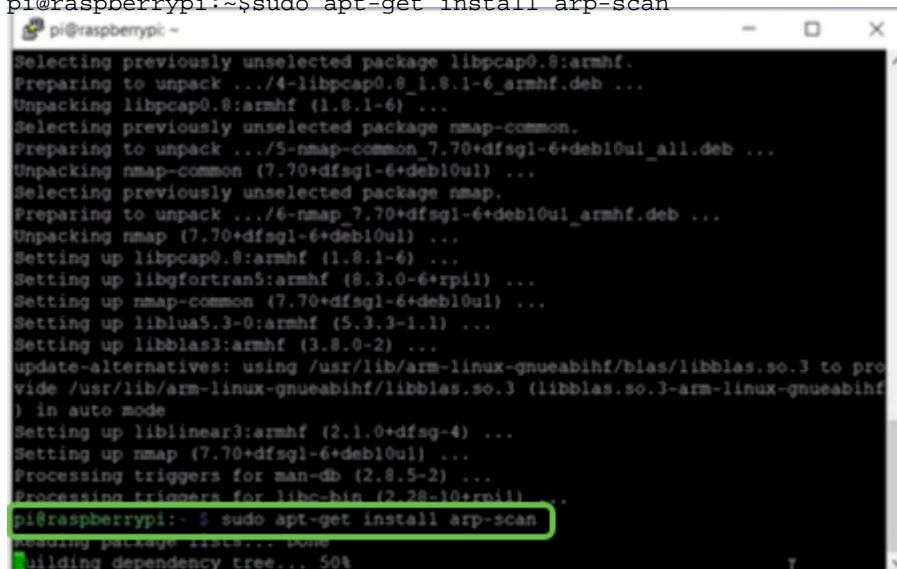


```
pi@raspberrypi:~$ sudo apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libblas3 libgfortran5 liblinear3 liblua5.3-0 libpcap0.8 nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 libgfortran5 liblinear3 liblua5.3-0 libpcap0.8 nmap nmap-common
0 upgraded, 7 newly installed, 0 to remove and 0 not upgraded.
Need to get 6,228 kB of archives.
After this operation, 27.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://mirror.sjc02.svwh.net/raspbian/raspbian buster/main armhf libgfortran5 armhf 8.3.0-6+rpi1 [206 kB]
Get:2 http://mirror.sjc02.svwh.net/raspbian/raspbian buster/main armhf libblas3 armhf 3.8.0-2 [103 kB]
```

## Step 7

Enter the following command.

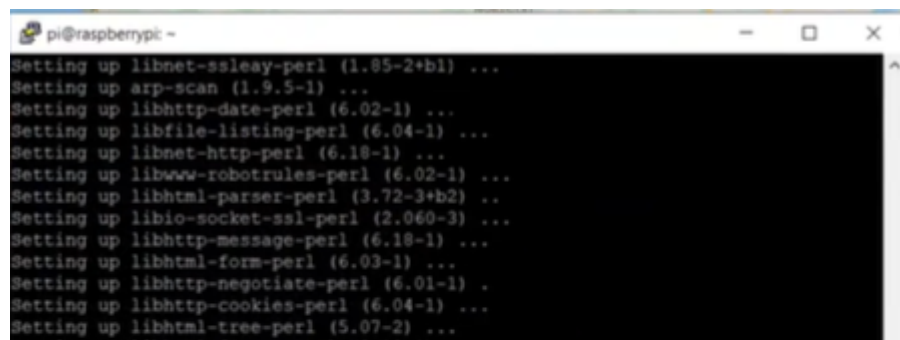
```
pi@raspberrypi:~$sudo apt-get install arp-scan
```



```
pi@raspberrypi:~$ sudo apt-get install arp-scan
Selecting previously unselected package libpcap0.8:armhf.
Preparing to unpack .../4-libpcap0.8_1.8.1-6_armhf.deb ...
Unpacking libpcap0.8:armhf (1.8.1-6) ...
Selecting previously unselected package nmap-common.
Preparing to unpack .../5-nmap-common_7.70+dfsg1-6+deb10u1_all.deb ...
Unpacking nmap-common (7.70+dfsg1-6+deb10u1) ...
Selecting previously unselected package nmap.
Preparing to unpack .../6-nmap_7.70+dfsg1-6+deb10u1_armhf.deb ...
Unpacking nmap (7.70+dfsg1-6+deb10u1) ...
Setting up libpcap0.8:armhf (1.8.1-6) ...
Setting up libgfortran5:armhf (8.3.0-6+rpi1) ...
Setting up nmap-common (7.70+dfsg1-6+deb10u1) ...
Setting up liblua5.3-0:armhf (5.3.3-1.1) ...
Setting up libblas3:armhf (3.8.0-2) ...
update-alternatives: using /usr/lib/arm-linux-gnueabi/libblas.so.3 to provide /usr/lib/arm-linux-gnueabi/libblas.so.3 (libblas.so.3-arm-linux-gnueabi) in auto mode
Setting up liblinear3:armhf (2.1.0+dfsg-4) ...
Setting up nmap (7.70+dfsg1-6+deb10u1) ...
Processing triggers for man-db (2.8.5-2) ...
Processing triggers for libc-bin (2.28-10+rpi1) ...
pi@raspberrypi:~$ sudo apt-get install arp-scan
Reading package lists... Done
Building dependency tree... 50%
```

## Step 8 (Optional)

Enter the following command if you would like to see a list of the files in the current directory. If you know the file name, you can skip to Step 9.

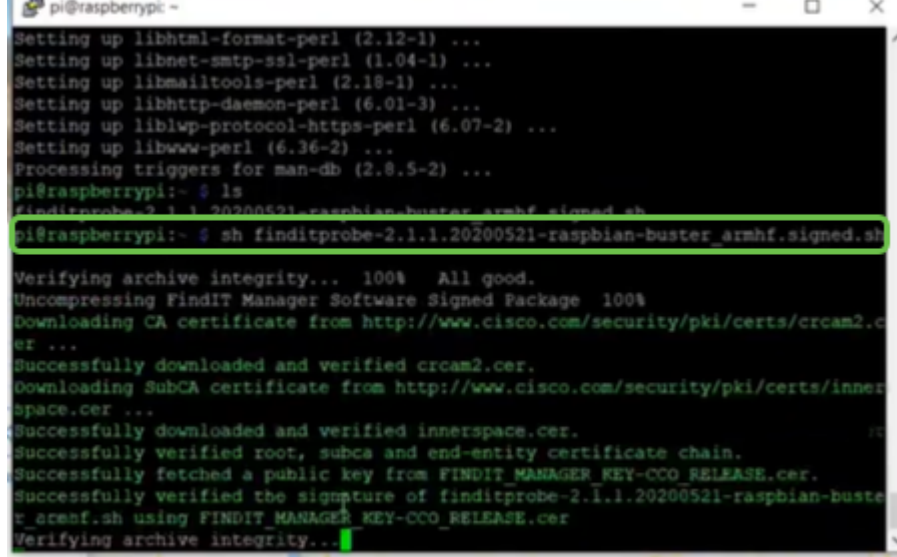


```
pi@raspberrypi:~$ sudo apt-get install arp-scan
Setting up libnet-sslseay-perl (1.05-2+b1) ...
Setting up arp-scan (1.9.5-1) ...
Setting up libhttp-date-perl (6.02-1) ...
Setting up libfile-listing-perl (6.04-1) ...
Setting up libnet-http-perl (6.18-1) ...
Setting up libwww-robotrules-perl (6.02-1) ...
Setting up libhtml-parser-perl (3.72-3+b2) ...
Setting up libio-socket-ssl-perl (2.060-3) ...
Setting up libhttp-message-perl (6.18-1) ...
Setting up libhtml-form-perl (6.03-1) ...
Setting up libhttp-negotiate-perl (6.01-1) ...
Setting up libhttp-cookies-perl (6.04-1) ...
Setting up libhtml-tree-perl (5.07-2) ...
```

## Step 9

Enter the following command.

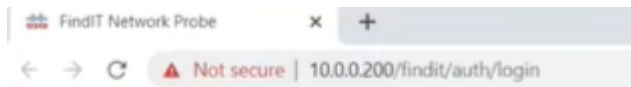
```
pi@raspberrypi:~$sh finditprobe-2.1.1.20200521-raspbian-buster_armhf.signed.sh
```



```
pi@raspberrypi:~$sh finditprobe-2.1.1.20200521-raspbian-buster_armhf.signed.sh
Setting up libhtml-format-perl (2.12-1) ...
Setting up libnet-smtp-ssl-perl (1.04-1) ...
Setting up libmailtools-perl (2.18-1) ...
Setting up libhttp-daemon-perl (6.01-3) ...
Setting up liblwp-protocol-https-perl (6.07-2) ...
Setting up libwww-perl (6.36-2) ...
Processing triggers for man-db (2.8.5-2) ...
pi@raspberrypi:~$ ls
finditprobe-2.1.1.20200521-raspbian-buster_armhf.signed.sh
pi@raspberrypi:~$ sh finditprobe-2.1.1.20200521-raspbian-buster_armhf.signed.sh
Verifying archive integrity... 100% All good.
Uncompressing FindIT Manager Software Signed Package 100%
Downloading CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully downloaded and verified crcam2.cer.
Downloading SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully downloaded and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from FINDIT_MANAGER_KEY-CCO_RELEASE.cer.
Successfully verified the signature of finditprobe-2.1.1.20200521-raspbian-buster_armhf.sh using FINDIT_MANAGER_KEY-CCO_RELEASE.cer
Verifying archive integrity...
```

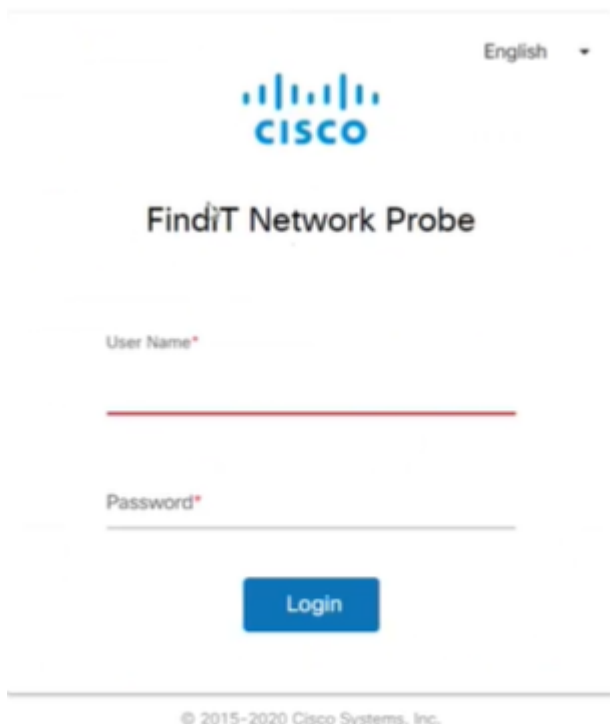
## Step 10

Once everything has loaded, enter the IP address of the Pi into a web browser.



## Step 11

Log into the probe. The default username and password, *cisco/cisco*, should be entered.



## Step 12

You will be asked to change the password.

---



**Change Password**

User Name `cisco`

Old Password\*

---

New Password\*

---

Retype New Password\*

---

## Conclusion

There you have it, now you have your Raspberry Pi working as a probe to help manage your network. Enjoy!