7
Installing Whonix

In the last chapter, we focused on installing Tails and accessing the Deep Web with it. Whonix is designed for advanced security and privacy. It's a heavily reconfigured Linux Debian that runs inside multiple virtual machines, providing a substantial layer of protection from malware and IP address leaks.

Whonix is the only operating system designed to be run inside a VM and paired with Tor.

In this chapter, we'll learn how to install and use Whonix to browse the Deep Web.

We will discuss the following topics:

- What Whonix is
- Whonix installation and pre-requisites
- Using Tor Browser with Whonix

What is Whonix?

Whonix is another OS focused on security and privacy. It's open source, and hence free to download and use. It's based on Linux (Debian) and Tor is implemented into it, to force all network connections through Tor (or be blocked). This is done automatically and is virtually system wide. Whonix is the only OS to work this way, so far.

Whonix was designed with the concept of VMs in mind. Desktop applications come pre-installed and are pre-configured with safety in mind. (It's also possible to install custom applications)

Whonix has two parts: the Whonix-Gateway VM and the Whonix-Workstation VM. The first runs Tor processes and acts as a gateway, while the second runs applications on an isolated network. There are several benefits to this design:

- All connections are routed through Tor
- Applications and servers can be run anonymously over the internet
- DNS leaks are not possible
- Malware with root privileges can't detect the user's real IP address
- User errors that could lead to threats are minimized

Most of the pre-installed applications, which connect to networks, use a dedicated Tor SocksPort. This helps with stream isolation and helps prevent identity correlation. Applications using Tor's DNS and/or Transport can be optionally disabled.

Whonix can be installed on hypervisors such VirtualBox, KVM, and more interestingly, on Qubes OS, to enhance security and anonymity. According to the Whonix website, it can help to do the following:

- Disguise a user's IP address
- Prevent ISP spying
- Prevent websites from identifying the user
- Prevent malware from identifying the user
- Circumvent censorship

Whonix can do this by providing the following features (among others):

- Anonymous browsing, by using Tor Browser for internet browsing
- Anonymous instant messaging, using apps such as Tox and Ricochet, routed through Tor
- Anonymous file sharing with OnionShare (`https://www.whonix.org/wiki/Onionshare`)
- Hiding Host location (`https://www.whonix.org/wiki/Hosting_Location_Hidden_Services`)
- Sending anonymous emails without registration
- Anonymous Java/JavaScript
- Full IP/DNS protocol leak protection
- Hiding Tor and Whonix use from network observers
- Hiding installed software from network observers
- Preventing anyone from learning the user's IP address

- Protecting user privacy
- Almost any application is torified
- Can torify other operating systems (such as Qubes and Windows)
- Connecting to a proxy, VPN, or SSH before Tor or vice versa
- Tunneling to other networks through Tor, such as GNUnet, I2P, and more
- PGP-encrypted email with Mozilla Thunderbird, Enigmail, and TorBirdy

Whonix installation and prerequisites

The following are the supported platforms:

- Qubes
- KVM
- VirtualBox
- PC x86 compatible

The minimum hardware resource requirement is as follows:

- 1 GB free RAM
- 10 GB free hard drive space

The minimum (Qubes 4.X) requirements are as follows:

- A 64-bit Intel or AMD processor
- 4 GB RAM
- 32 GB disk space
- Legacy boot mode—required for R3.0 and earlier; UEFI is supported beginning with R3.1
- Intel VT-x with EPT (`https://en.wikipedia.org/wiki/Second_Level_Address_Translation#Extended_Page_Tables`) or AMD-V with RVI (`https://en.wikipedia.org/wiki/Second_Level_Address_Translation#Rapid_Virtualization_Indexing`)
- Intel VT-d or AMD-Vi (also known as AMD IOMMU)—required for effective isolation of network VMs

Whonix download

Whonix can be downloaded ready for the various supported hypervisors (Windows, Linux, OS X, and Qubes), from the following URL:

`https://www.whonix.org/wiki/Download`

Whonix installation

For this hands on installation, we'll use VirtualBox. You can find VirtualBox for download at the following URL:

`https://www.virtualbox.org/wiki/Downloads`

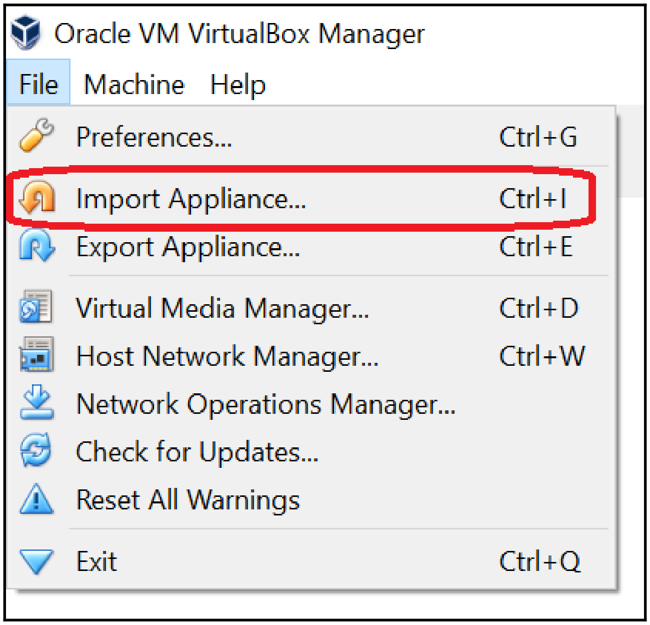
Perform the following steps to install Whonix:

1. Download the version that's appropriate for your host operating system and install it
2. Install VirtualBox in the manner that's appropriate for your host OS
3. Import the Whonix-Gateway and Whonix-Workstation OVA files into VirtualBox, as an appliance
4. Double-click on the Whonix-Gateway and Whonix-Workstation objects in VirtualBox to start them
5. Finish the configuration
6. Start Tor Browser

You can see the step-by-step instructions (for steps 3-6) here: `https://www.whonix.org/wiki/VirtualBox/CLI`

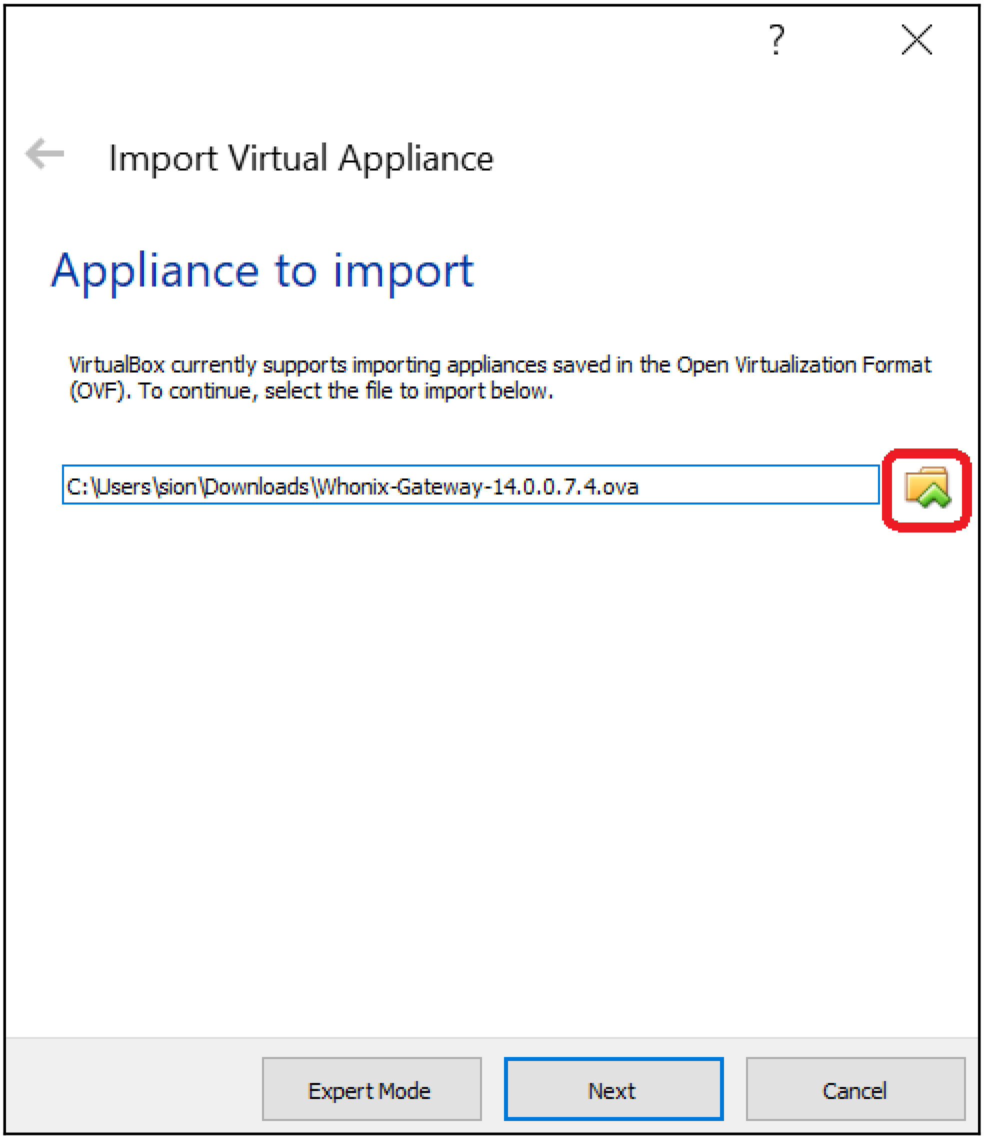
To import Whonix into VirtualBox, see the following:

1. In VirtualBox, Click **File | Import Appliance**:


Oracle VM VirtualBox Manager
File
Machine
Help
Preferences... Ctrl+G
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
Virtual Media Manager... Ctrl+D
Host Network Manager... Ctrl+W
Network Operations Manager...
Check for Updates...
Reset All Warnings
Exit Ctrl+Q

Import the virtual appliance

2. Click the Choose icon (it looks like a folder) and select the `Whonix-Gateway.ova` file, which you downloaded previously and then click **Open**:



Import Virtual Appliance

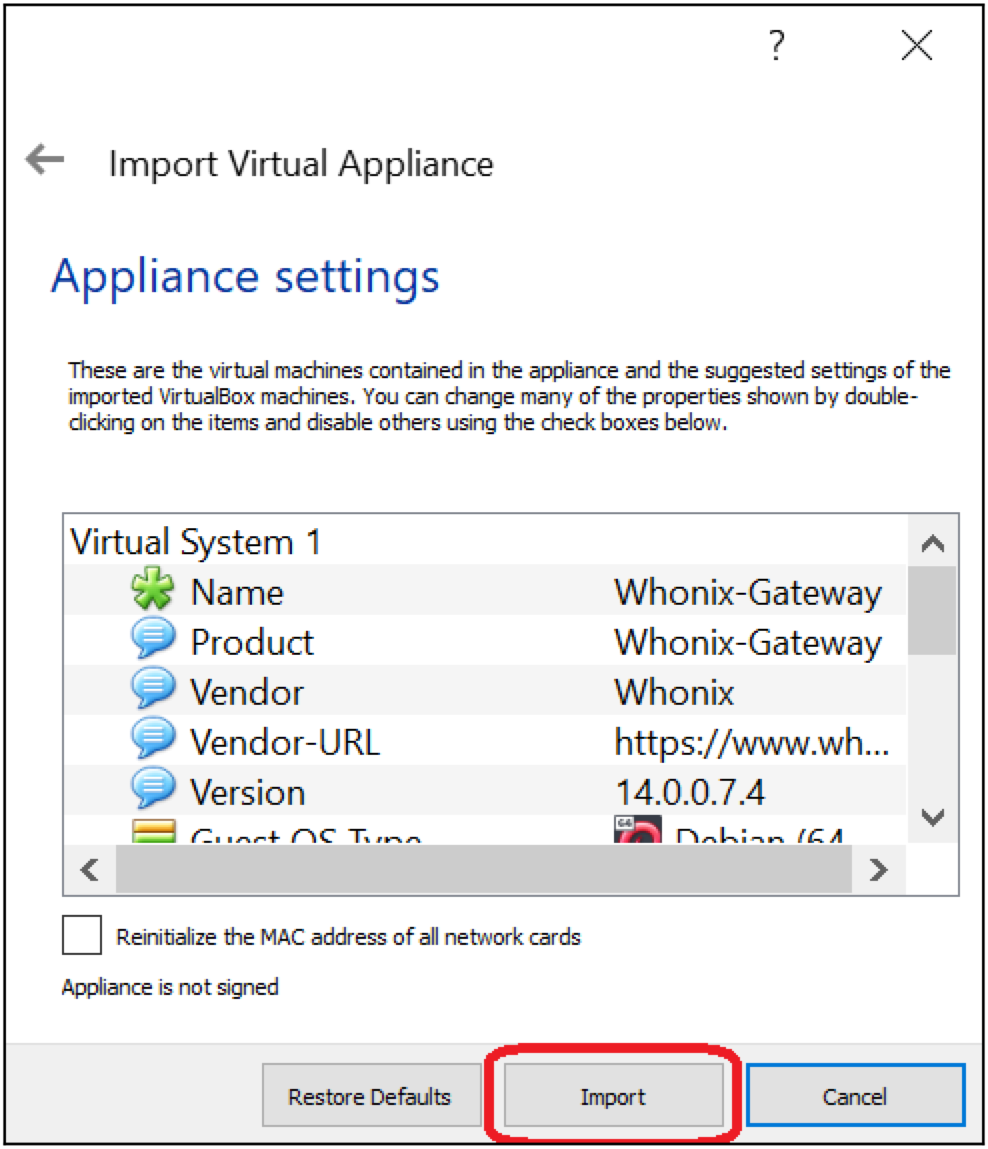
Appliance to import

VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

C:\Users\sion\Downloads\Whonix-Gateway-14.0.0.7.4.ova

Appliance to import

3. Click **Next** and then **Import** without changing any settings:



Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1

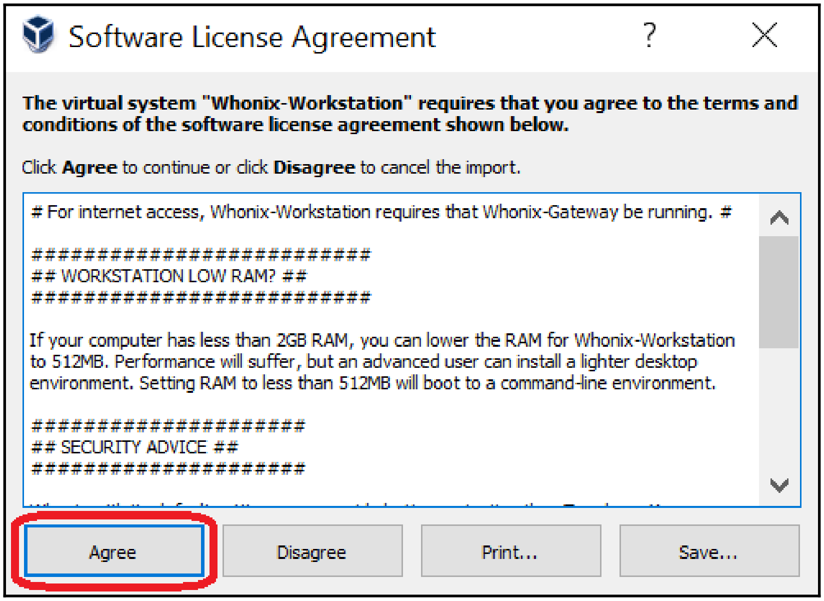
Name	Whonix-Gateway
Product	Whonix-Gateway
Vendor	Whonix
Vendor-URL	https://www.wh...
Version	14.0.7.4
Guest OS Type	Debian (64

□ Reinitialize the MAC address of all network cards

Appliance is not signed

Appliance settings

4. Click **Agree** when the **Software License Agreement** window appears:



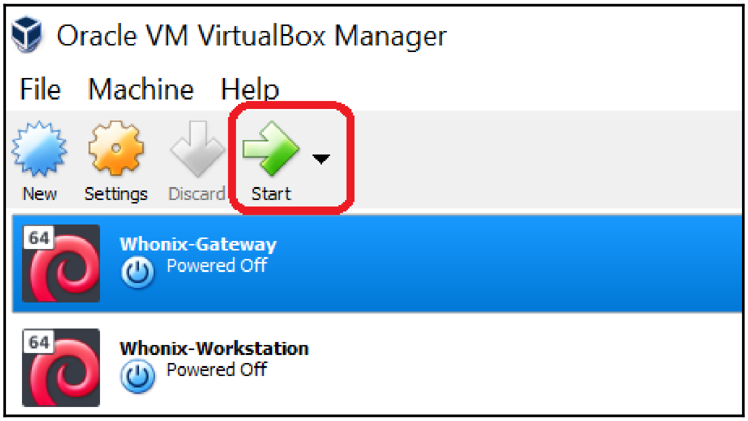
The virtual system "Whonix-Workstation" requires that you agree to the terms and conditions of the software license agreement shown below.

Click **Agree** to continue or click **Disagree** to cancel the import.

```
# For internet access, Whonix-Workstation requires that Whonix-Gateway be running. #

##########################
## WORKSTATION LOW RAM? ##
##########################

If your computer has less than 2GB RAM, you can lower the RAM for Whonix-Workstation
to 512MB. Performance will suffer, but an advanced user can install a lighter desktop
environment. Setting RAM to less than 512MB will boot to a command-line environment.

#####################
## SECURITY ADVICE ##
#####################
```

Whonix Software License Agreement

- Wait for the progress bar to complete the import
- Repeat these steps for the `Whonix-Workstation.ova` file
- Now, start the Whonix-Gateway followed by Whonix-Workstation:



Whonix-Gateway
Powered Off

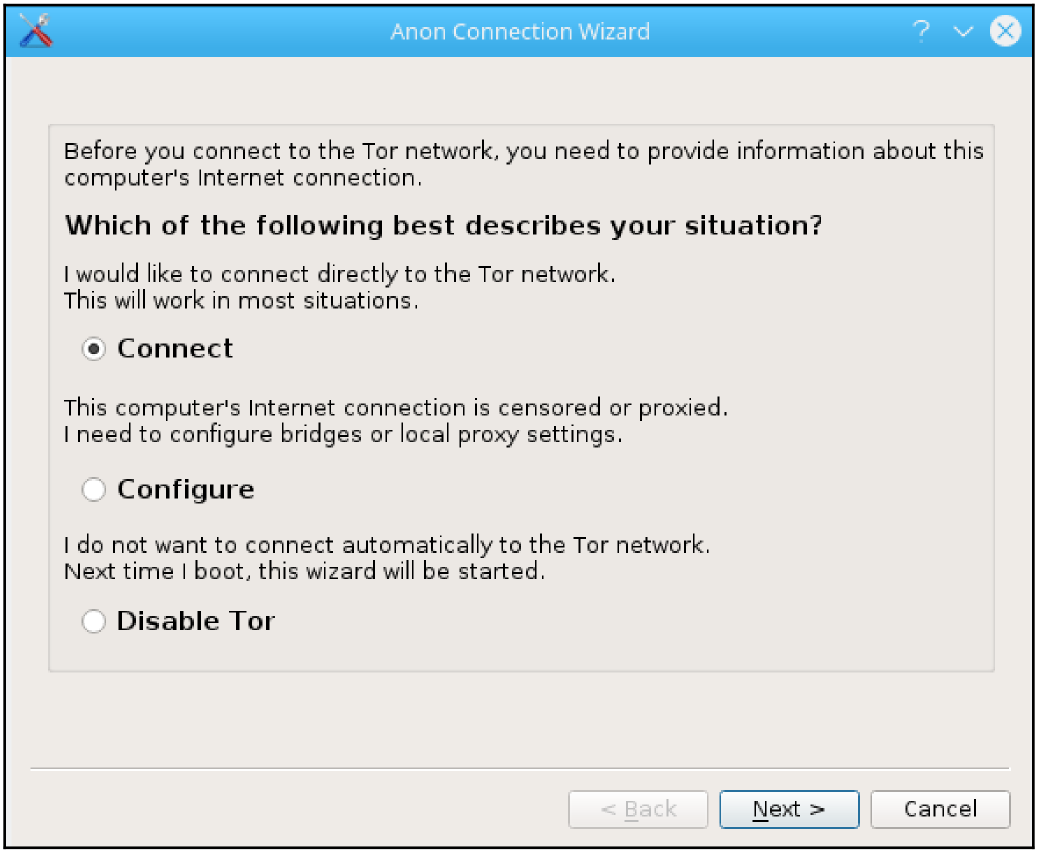
Whonix-Workstation
Powered Off

Start Whonix VMs

If you need to log on, these are the default credentials:

- **Username**: `user`
- **Password**: `changeme`

5. Configure network connectivity in Whonix-Gateway:



Before you connect to the Tor network, you need to provide information about this computer's Internet connection.

Which of the following best describes your situation?

I would like to connect directly to the Tor network.
This will work in most situations.

● Connect

This computer's Internet connection is censored or proxied.
I need to configure bridges or local proxy settings.

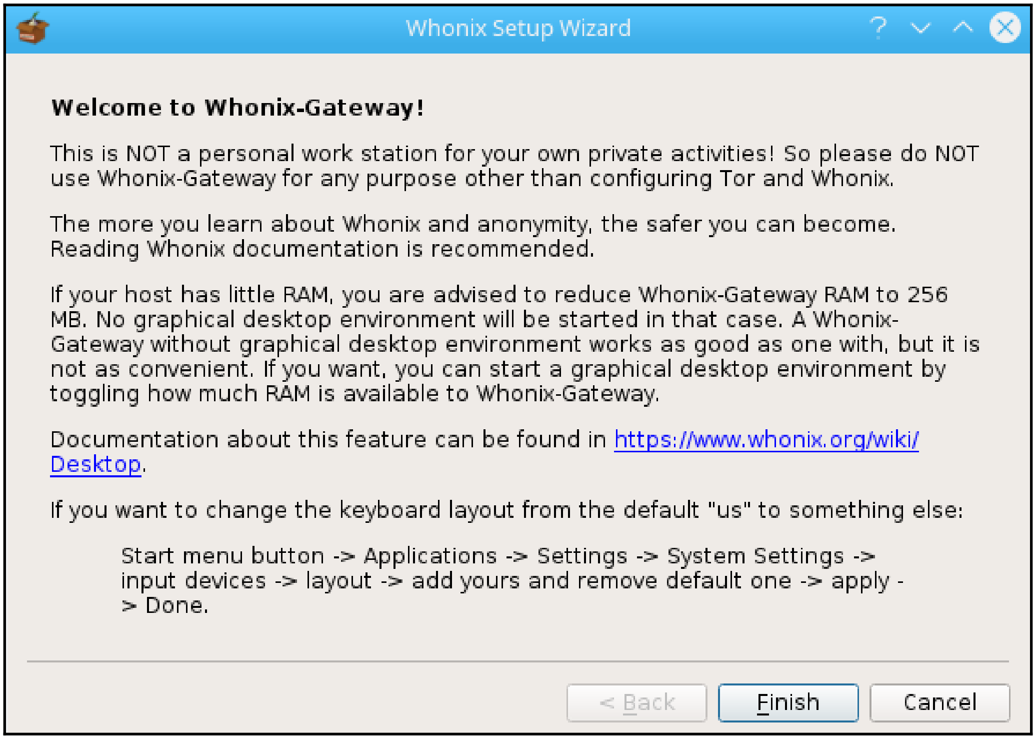
○ Configure

I do not want to connect automatically to the Tor network.
Next time I boot, this wizard will be started.

○ Disable Tor

Anon Connection Wizard

6. After the **Anon Connection Wizard** finishes, you'll continue the setup process, until Tor is fully configured:



Welcome to Whonix-Gateway!

This is NOT a personal work station for your own private activities! So please do NOT use Whonix-Gateway for any purpose other than configuring Tor and Whonix.

The more you learn about Whonix and anonymity, the safer you can become. Reading Whonix documentation is recommended.

If your host has little RAM, you are advised to reduce Whonix-Gateway RAM to 256 MB. No graphical desktop environment will be started in that case. A Whonix-Gateway without graphical desktop environment works as good as one with, but it is not as convenient. If you want, you can start a graphical desktop environment by toggling how much RAM is available to Whonix-Gateway.

Documentation about this feature can be found in https://www.whonix.org/wiki/Desktop.

If you want to change the keyboard layout from the default "us" to something else:

Start menu button -> Applications -> Settings -> System Settings -> input devices -> layout -> add yours and remove default one -> apply -> Done.

Finish Whonix installation

It's highly recommended to change passwords on both Whonix-Gateway and Whonix-Workstation for both the user and root accounts. (Qubes-Whonix users can skip this section.)

To do so,

1. Open Console, the Whonix terminal, by going to the following: **Start menu** | **Applications** | **System** | **Terminal**.
2. Log in as `root` by running the following:

```
sudo su
```

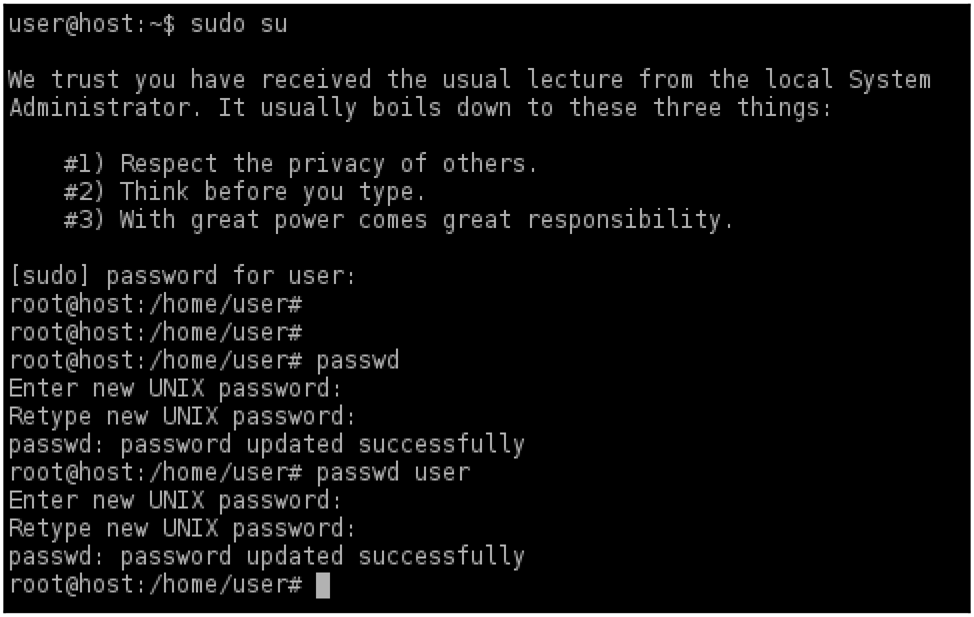
3. Then, run the following:

```
passwd
```

4. And then run the following command:

```
passwd user
```

Let's look at the following output:

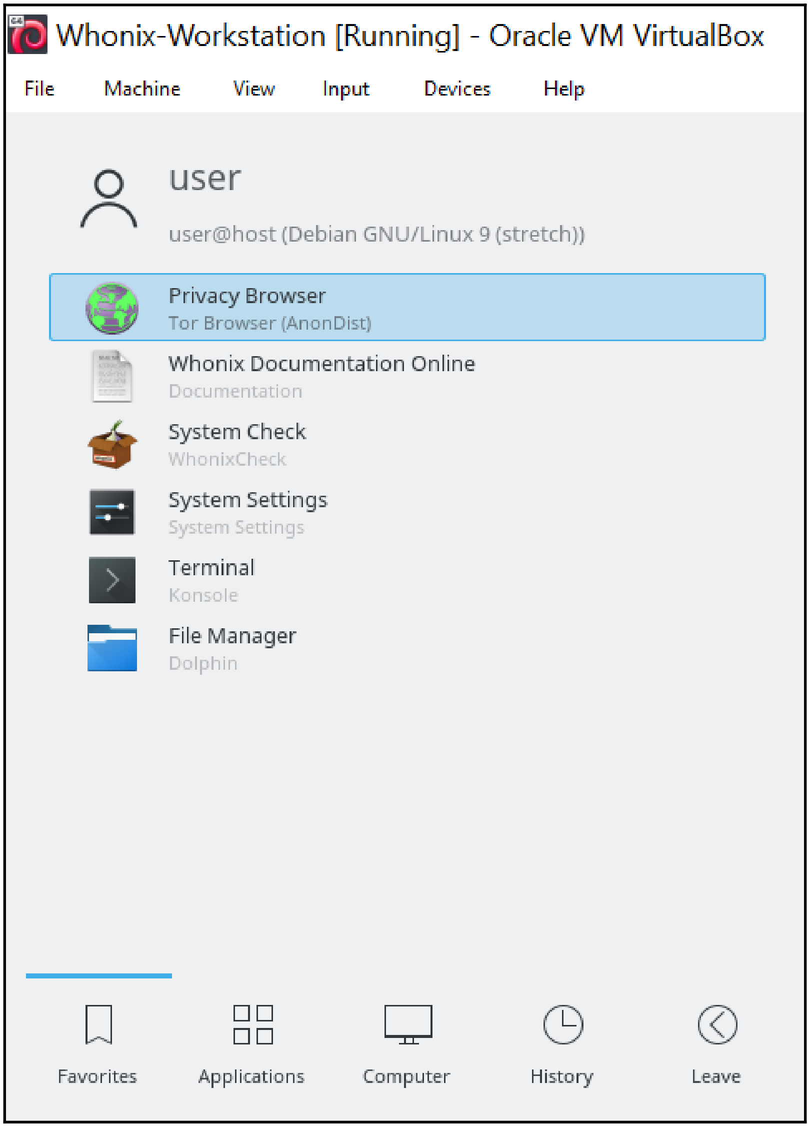


```
user@host:~$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for user:
root@host:/home/user#
root@host:/home/user#
root@host:/home/user# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@host:/home/user# passwd user
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@host:/home/user#
```

Change passwords

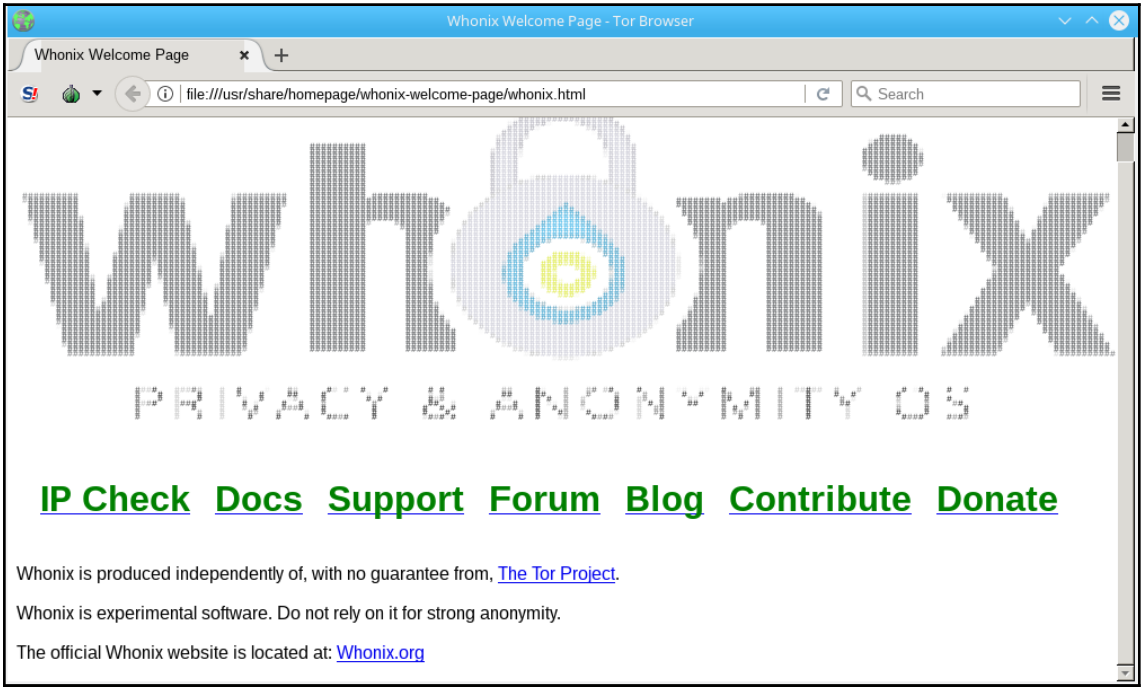
Using Tor Browser with Whonix

To start browsing the Dark Web, you can start Tor Browser, by going to **Start Menu** | **Favorites**| **Privacy Browser**, as can be seen in the following:



Start Tor Browser in Whonix

Then, you'll see the Whonix Tor Browser window:



Whonix is produced independently of, with no guarantee from, The Tor Project.

Whonix is experimental software. Do not rely on it for strong anonymity.

The official Whonix website is located at: Whonix.org

Whonix Tor Browser

Browsing is done as usual, by entering the URL of `.onion` sites.

Summary

In this chapter, we talked about Whonix, how to install it, and its basic use. We discussed what makes Whonix unique, and how it helps protect the user's privacy and security. We saw how easy it is to access the Dark Web using Whonix since it was developed for that purpose. There's no need to install or configure anything after installing the OS.

As we've discussed, Whonix works with two VMs, one acting as the gateway and securing the traffic, and the other as the workstation, providing a desktop interface for the user. Always remember to start Whonix-Gateway first, to verify that the traffic is going through it, and then turn on the Whonix-Workstation.

Questions

1. What makes Whonix unique?
2. What other operating systems are designed to work with Whonix?

Further reading

The following resource might be of interest if you'd like to go deeper into the issues discussed in this chapter:

- `https://www.whonix.org/wiki/Main_Page`