Tails HVM - Community Guides - Qubes OS Forum

3-4 minutes ⋮ 8/15/2023

Tails 29 stands for The Amnesic Incognito Live System. It is a live operating system that aims to preserve your privacy and anonymity. Tails is intended to be booted off of a live CD and leave no trace on the computer it is run on, but using Tails this way requires the user to restart their computer every time they want to switch from their installed OS to Tails. Despite this, in case that method becomes cumbersome, Tails can be used inside virtualization software and Qubes.

To run Tails under Qubes:

1. Read about creating and using HVM qubes 42

2. Download and verify Tails from 29https://tails.boum.org 29 in a qube, (saved as `/home/user/Downloads/tails.iso` on qube “isoVM” for purposes of this guide).

3. Create a HVM

   - In Manager, click “VM menu” and select “Create VM”
   - Name the new qube - “Tails”
   - Select “HVM”
   - Set “initial memory” and “max memory” as the same (official documentation 7 recommends at least 2048 MB)
   - Configure networking
   - Click “OK” to create new HVM.

4. Open dom0 Konsole and start Tails:

   ```
   qvm-start Tails --cdrom=isoVM:/home/user/Downloads/tails.iso
   ```

5. Configure Tails at start up.

6. Once the Tails qube has started, configure networking in the qube.

   - Check the IP address allocated to the qube - either from GUI Manager, or `qvm-ls -n Tails` in Konsole. (E.g. `10.137.1.101` with gateway `10.137.1.1`)
   - In the Tails qube, open systems menu in top-right corner. Select “Wired Settings”, and change IPv4 configuration from “Automatic (DHCP)” to “Manual”.
   - Enter the Address: `10.137.1.101` in our example.
   - Enter the Netmask: `255.255.255.0`
   - Enter the Gateway: `10.137.1.1` in our example.
   - Enter DNS: `10.137.1.1` in our example.
   - Click “Apply”. You should now see “Connected”.

7. Use Tails as normal.

Security

You will probably want to implement MAC spoofing 59.

There are added security concerns for Tails users when running it in a virtual machine. If you intend to do this, you should read the warnings 42 from the Tails team about it. While the Qubes security model mitigates most of the risks identified, traces of the Tails session may remain on the disk. Live booting Tails, though less convenient, is always more secure than using it inside virtualization software or Qubes, because you don't run the added risk of the virtualization software or Host OS being compromised. Depending on your threat model, this might induce too much risk.

Troubleshooting

See the Tails Troubleshooting guide 20.

▼ This document was migrated from the qubes-community project

- Page archive 1
- First commit: 08 Dec 2020. Last commit: 08 Dec 2020.
- Applicable Qubes OS releases based on commit dates and supported releases: 4.0
- Original author(s) (GitHub usernames):
- Original author(s) (forum usernames):
-