

Sophos SG105

The Sophos SG105 comes pre-installed with the (older) UTM 9 firmware, the XG105 comes pre-installed with the (newer) XG Firewall firmware. Both version are being maintained by Sophos. I purchased the SG105 and activated a home use license for UTM 9.4, and then later upgraded to the XG Firewall. Both are not trivial as Sophos does not allow to activate or install a home use license on Sophos hardware appliances (something I did not realize when I ordered the appliance), but I found workarounds for both, which are explained below.

I purchased the device from [Corporate Armor](#) in the USA and had it shipped to a US address. Currently, the price is 340 USD.

Initial Setup with existing UTM9 firmware

The fastest way is to utilize the installed firmware, but note that the firmware does not allow to be activated with a free home use license. Follow the guide below for a work around.

If you are a home user, buy the SG105 without any license. This is called a “basic license” in Sophos terms, but make sure your supplier provides an activation key. After setting up your base license, you need to get SSH access or connect a terminal, before you can register a home use license. Here are the necessary steps:

1. Download the firmware for [Sophos UTM Home Edition](#) and install it in a VM to test
2. Go to the [MyUTM](#) portal, create a MyUTM Account, and login
3. After login, click “Create a new License”, then “Create and use contact set”, after which you can create a home use license
4. To activate the SG105 appliance hardware (or any other Sophos hardware), you need to do the same but create a license by entering your activation key “ACT-SGHxxx-xxx”
5. After saving the license files, navigate to the appliance at <https://192.168.0.1:4444>, which will take you through the initial setup wizard
6. Upload the license file created for the SG105
7. Enable SSH access and create the passwords for “root” and “loginuser”
8. Open an SSH connection to the appliance and rename the file “/etc/asg” to eg. “/etc/asg-basic”
9. Reconnect to <https://192.168.0.1:4444> and upload the license file created for home use

Initial Setup clean install with XG Firewall firmware

Activation for XG Firewall is fundamentally different from the one for UTM9:

1. Download the firmware for [Sophos XG Firewall Home Edition](#) and install it in a VM to test
2. Create a VM with dynamic size equal or slightly smaller than the SSD which comes with the appliance. In my SG105 is a Transcend SSD370, the size is slightly larger than 61057 MB, so I created the VM with size 61057 MB.
3. Enable all 4 network adapters, but you can leave them as “not attached”
4. Connect the firmware iso and boot into the installer. When the installation is finished, the installer asks to detach the installation iso and reboot. **DO NOT REBOOT AT THIS TIME**, just

power off the VM.

5. Connect the SSD of the hardware appliance to the computer running the VM, make sure that the host does not utilize this SSD, and attach the SSD to the VM. Make sure that the VM harddisk and the SSD are attached to a SATA controller. For this to work on a Windows host you need to run the VM as administrator. For VirtualBox you need to open a CLI as administrator and run the following command, other Virtualizers such as VMware allow to attach a raw drive in their UI.

```
VBoxManage internalcommands createrawvmdk -filename  
"C:\Users\\VirtualBox VMs\\.vmdk"  
-rawdisk \\.\PhysicalDrive#
```

Find the PhysicalDrive# from Control Panel -> Administrative Tools -> Computer Management

6. Attach any live linux distro iso to the DVD drive of the VM, and boot into the live linux system and enter a CLI.
7. Verify that the live linux recognizes the VM drive with the pre-installed XG Firewall as sda and the raw attached SSD as sdb (use fdisk -l)
8. Copy the entire VM drive to the SSD with

```
dd if=/dev/sda of=/dev/sdb bs=1m
```

9. If you want to avoid to attach the SSD of the appliance to the VM. you can alternatively do the following: Copy the entire VM drive to a file on a USB drive with

```
dd if=/dev/sda of=/mount/point/of/usb/sophosfw bs=1m
```

then create a bootable USB with any live linux distro on it and plug it into the SG105 and boot into a CLI and enter

```
dd if=/mount/point/of/usb/sophosfw of=/dev/sda bs=1m
```

This takes longer but leads to the same result.

10. After the firmware is copied to the SSD, boot the SG105, and follow the [Getting Started Guide](#) for a Sophos Firewall Software Appliance. There is a note in the guide, that "SF OS using Software Appliance ISO can be installed on SG and XG series appliances after deleting hard drive partitions from the devices.", but this seems to work only with paid subscriptions, not with the home use license.

Links

Sophos

- [MyUTM for UTM 9 appliances](#)
- [MySophos for XG Firewall appliances](#)
- [Getting Started Guide](#)
- [Sophos XG Firewall Administrator Guide v15.01.0](#)

Community

- [Change loginuser/root passwords and login to SSH on UTM/Astaro Security Gateway](#)
- [free private license for appliance](#)
- [Home Use License on UTM appliance?](#)
- [Converting A VMware Image To A Physical Machine](#)
- [Using a Physical Hard Drive with a VirtualBox VM](#)

From:

<https://wiki.condrau.com/> - **Bernard's Wiki**

Permanent link:

<https://wiki.condrau.com/net:sg105>

Last update: **2016/09/22 16:11**

