

# ENCRIPTING YOUR HARD DISK: A GUIDE

Developed by APC Tech for Global Encryption Day 2021



**APC**  
ASSOCIATION FOR  
PROGRESSIVE  
COMMUNICATIONS

# There is a lot of information around on securely protecting your communications, but how can you better protect your devices?

For the last decade encryption has been one of the main priorities for those working in technology. Even though its scientific meaning involves many words, all of us know that encrypting basically means exchanging and storing data in a secure way, away from prying eyes.

There are many protocols and implementations of these protection methods: there is the infamous WhatsApp “end to end” encryption, the “you must trust our company can’t see your data” encryption, the PGP/email encryption, and device encryption, among others.

In this article we will talk about the latter – device encryption – which is a very useful type of protection in case your device is seized, stolen or lost. Without the access code no one would be able to see anything on it!

When it comes to device encryption, there are mainly two options: encrypt external devices (thumb drives, SD cards, external hard drives,

etc.) or encrypt internal devices, most likely meaning the drive on which the operating system is running.

If you want to encrypt your hard disk, this needs to be done during the operating system installation. In recent GNU/Linux distributions, it's as easy as ticking a checkbox at the hard drive partition stage of the installation, and providing a passphrase that needs to be used every time the system boots.

The way the protection works once installed is that the system asks for a passphrase on boot. If you provide it, then everything is able to start normally. If you don't, then the whole content of the hard disk is completely inaccessible. So beware – if you forget this password you cannot access your device's content anymore! This guide contains detailed explanations for Linux operating system variants, with some recommendations for other systems.

We hope that you enjoy encrypting your devices so that we all work and live in a better protected world!

1. Installation guide for encryption in Linux operating systems
2. Installation guide for other external devices in Linux
3. Encryption on other operating system

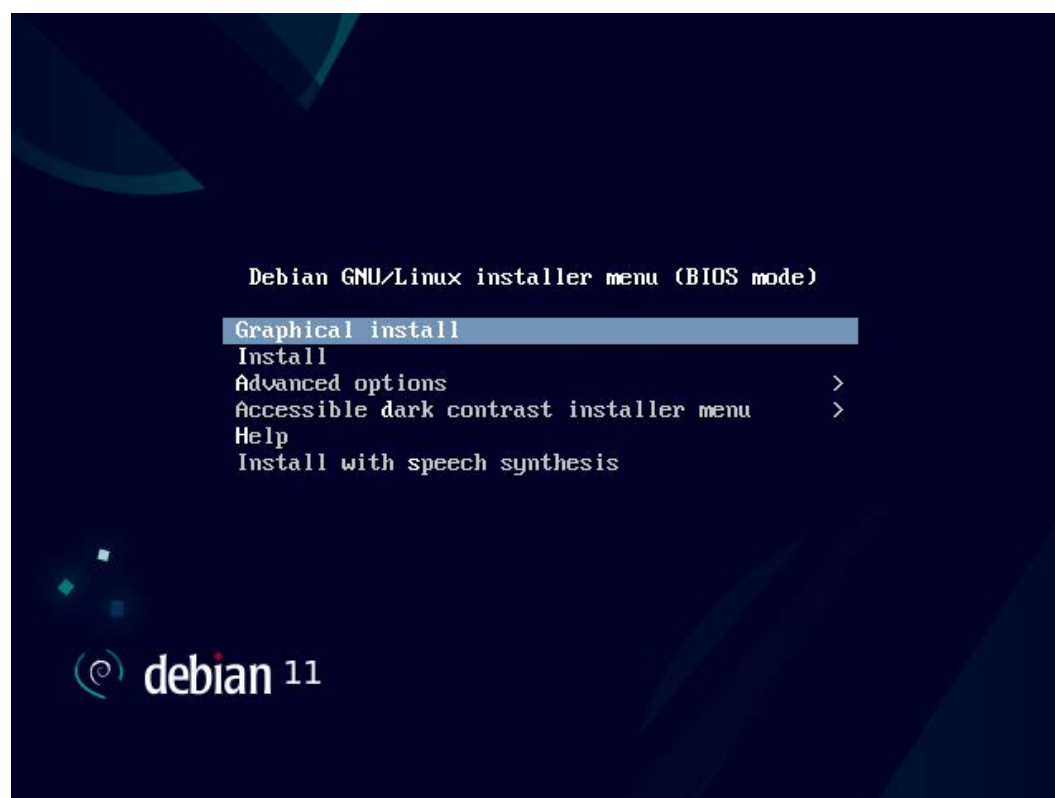
# 1. Installation guide for encryption in Linux operating systems

In order to encrypt your hard disk, it is better to start with a brand new device or hard disk, as all the information will be deleted.

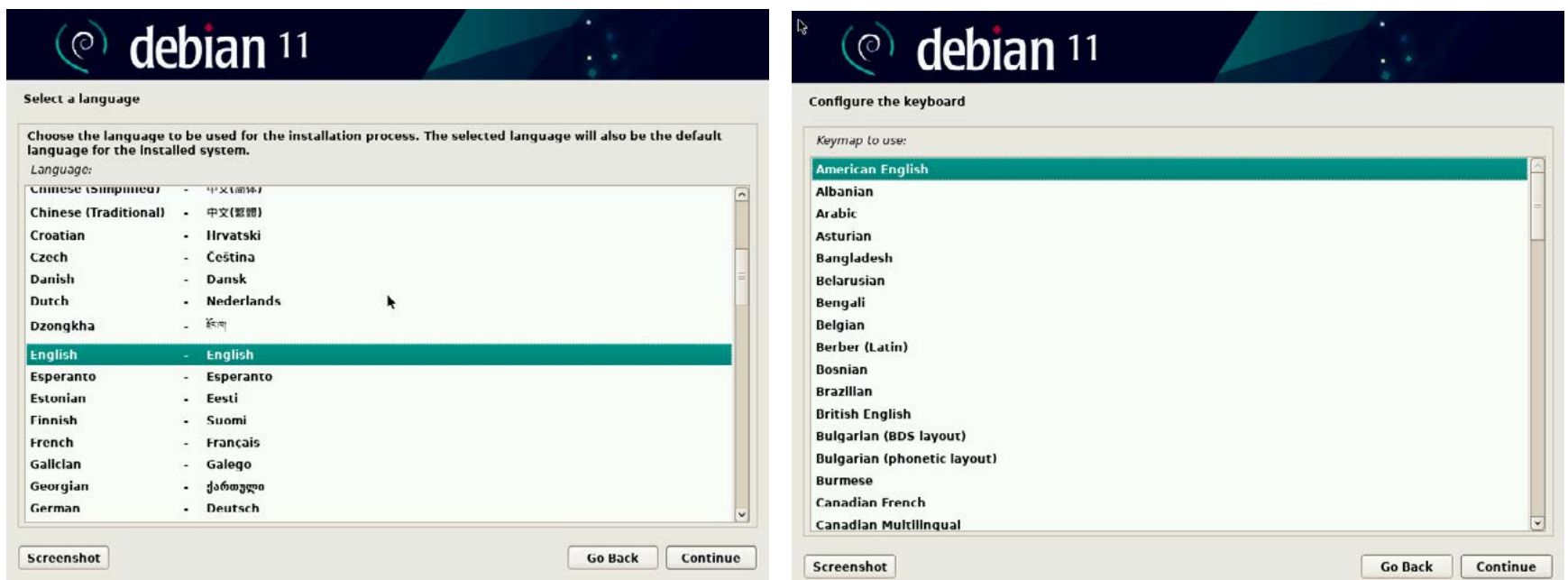
To assist you in the process, this guide includes sample screenshots of the full encrypted operating system (OS) installation process in Debian OS.

Before you start, you will need to download the desired operating system installation file(s).

1. This is the first installer screen. Go for “Graphical install”.



2. Then select the language – English is the default. Then the country (it would be great if there was no default for this!) and keyboard layout.



3. Next enter your computer's name. It can be anything, but no spaces or special characters are allowed.



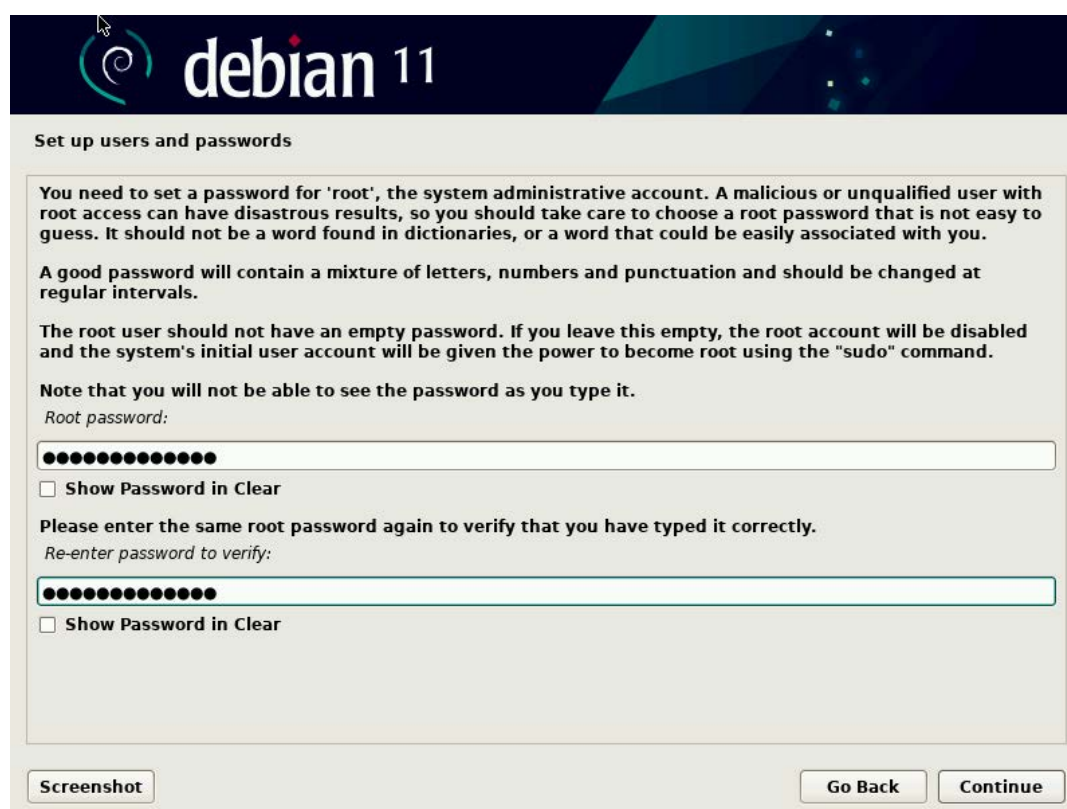


4. Since most of the GNU/Linux OS was initially developed thinking of the device being part of a network, setting a domain name is part of the installation process, but it can be left blank as needed.



5. There are at least two important passwords: root and user. In this case we'll have a third one – encryption. Even though they can be the same, it's advised for them not to be. You should at least add a small variation on each.

Please note that Root equals Admin on GNU/Linux systems.



You can use either your real full name or nickname, but it's different than your username, which is the one you'll use to log in/start session.



debian 11

Set up users and passwords

A user account will be created for you to use instead of the root account for non-administrative activities.

Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.

Full name for the new user:

Screenshot Go Back Continue

This is what you will use to identify yourself to the system. It cannot contain blank spaces or special characters.



debian 11

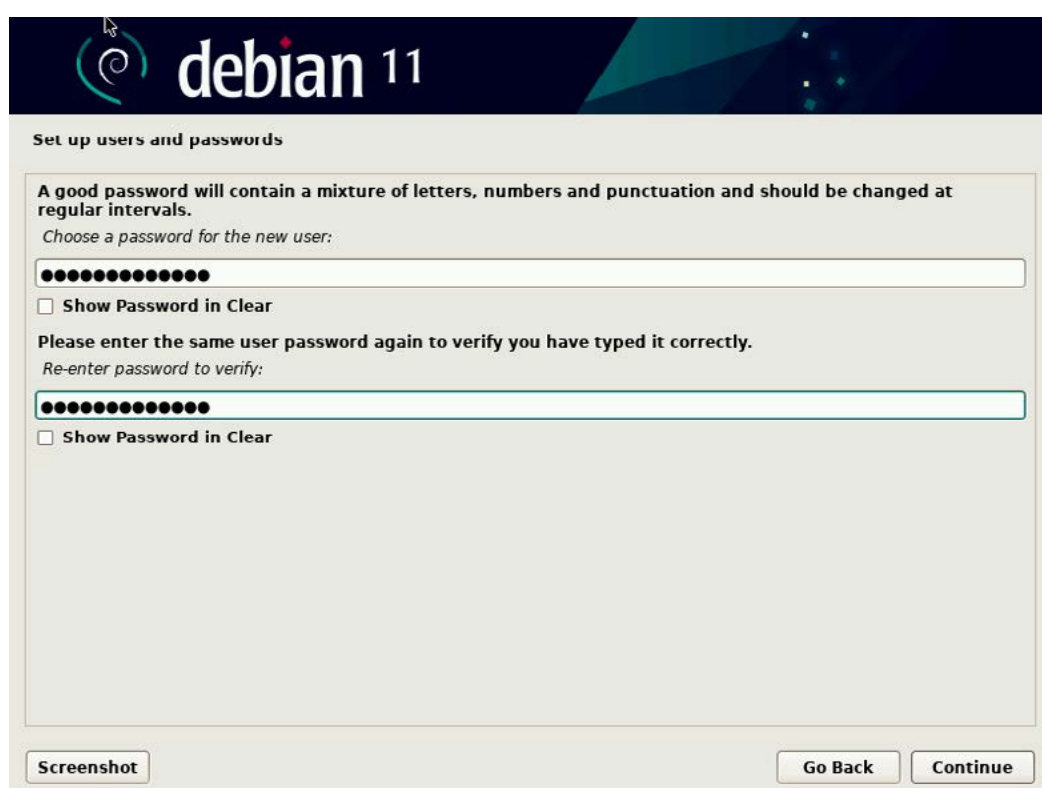
Set up users and passwords

Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.

Username for your account:

Screenshot Go Back Continue

And this is your user password. Again, try to avoid using the same as you set for Root.



debian 11

Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

Choose a password for the new user:

  
 Show Password in Clear

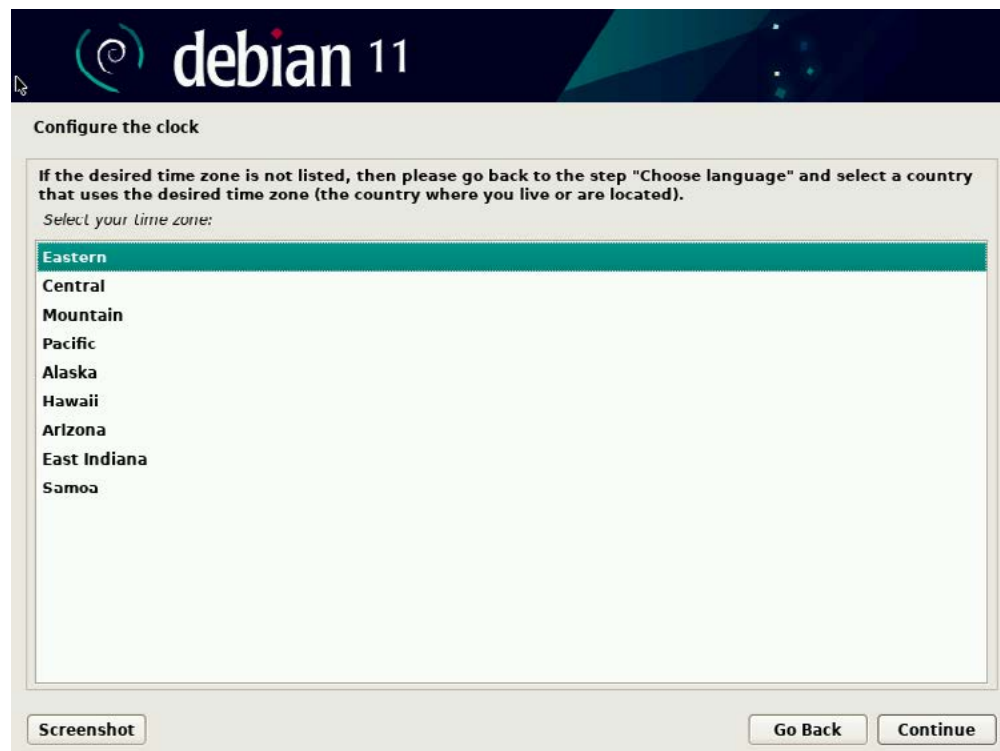
Please enter the same user password again to verify you have typed it correctly.

Re-enter password to verify:

  
 Show Password in Clear

Screenshot Go Back Continue

6. Now select the timezone (options are based on the country you previously selected).



7. Here's where we take the encryption branch of the road! If you want to explore all the options, select "Manual partition" and take a look, but most of the time you just want to use the "Guided entire disk encrypted LUKS" option, so go for it.

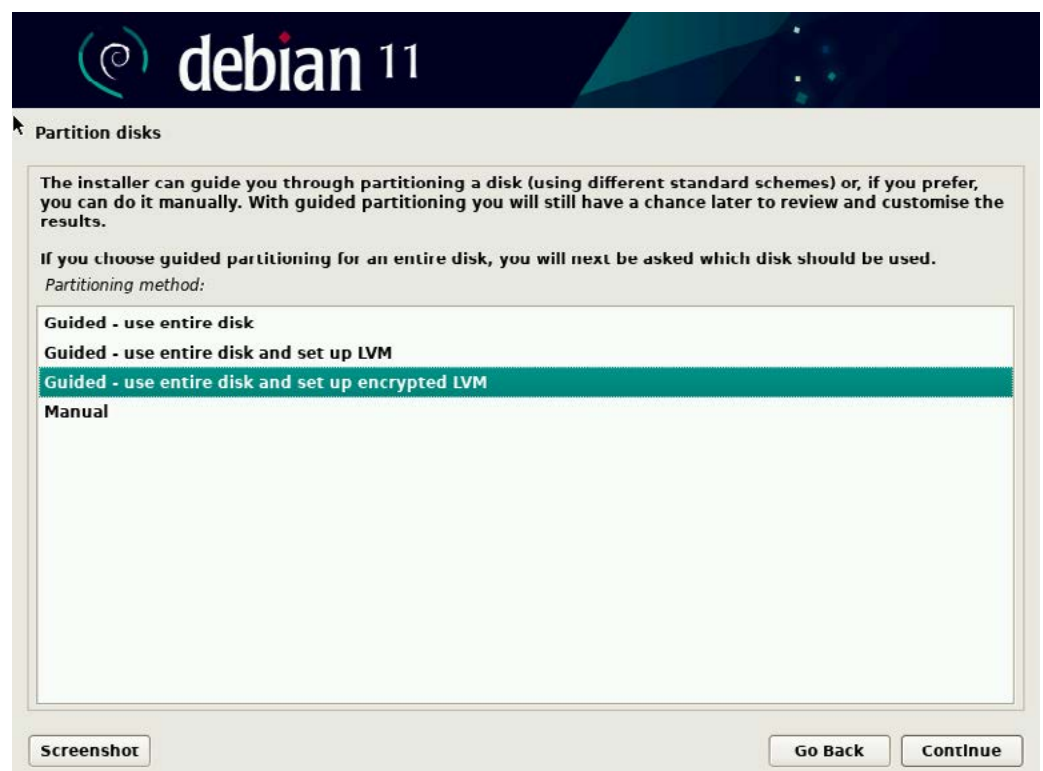




8. Unless you are installing on a brand new hard drive, you will actually not see this screen. The reason why is that it's about creating a partition table, which needs to be done only the first time a hard drive is used.



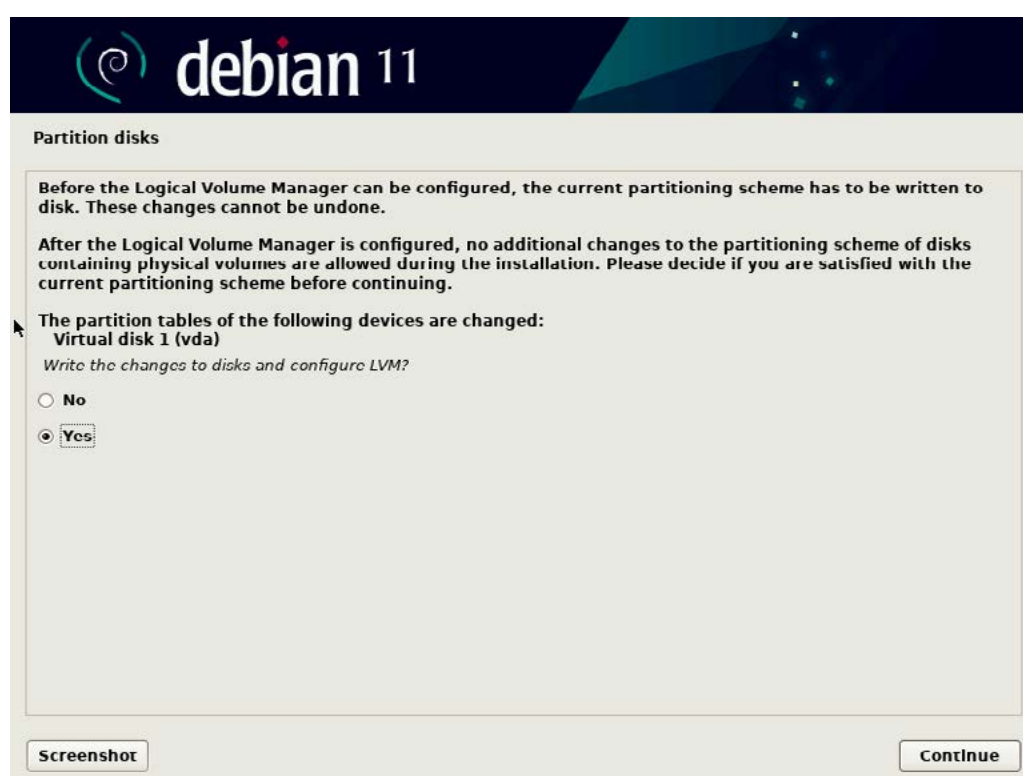
Don't let the installer call you "new user", or don't think of yourself as a newbie just for choosing the first option. It is true that for certain use cases it's advised to separate certain data into different partitions, but for non-server installation, having it all in the same one is just as good, so let's do it that way.



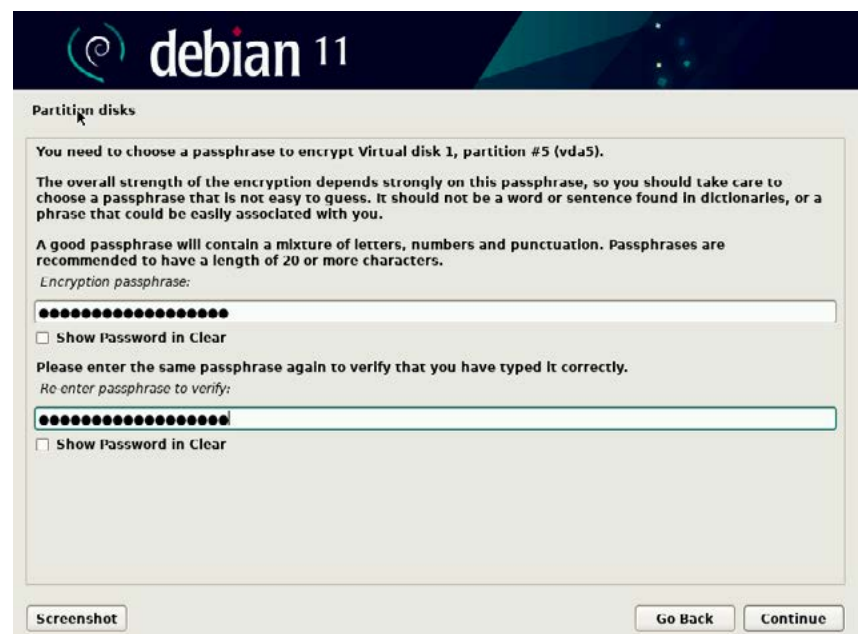
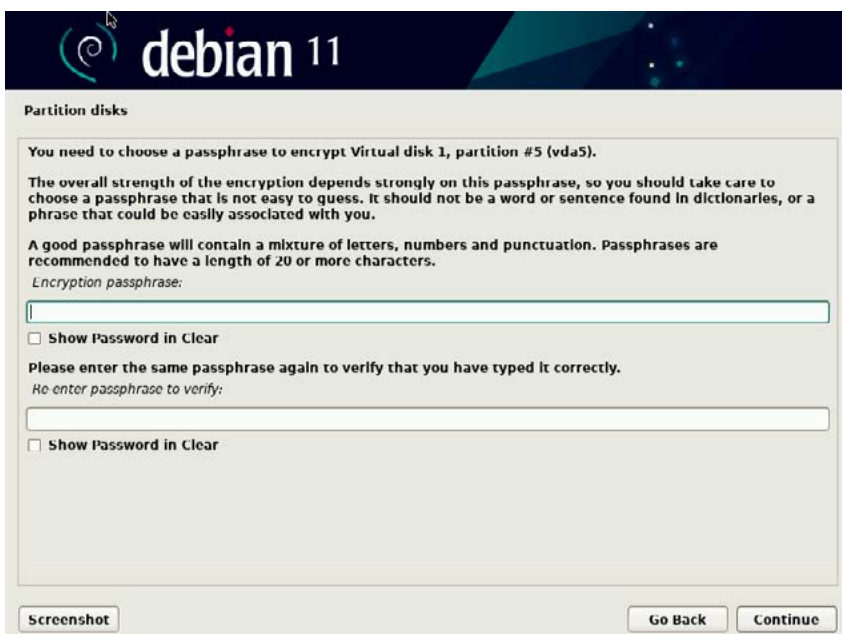
Since this is the step where all we've done before gets really written into the hard drive, and it makes whatever was stored on it before inaccessible (gone forever), the default option is "No", and you need to change it to "Yes" and continue.

And then confirm you know what you're doing.

This will take a while depending on whether you are installing on a solid state drive or in a conventional hard drive, and the size of it. So at this point you might want to take a break and think of all the kitty-cat videos you'll be able to safely keep in your new encrypted system.

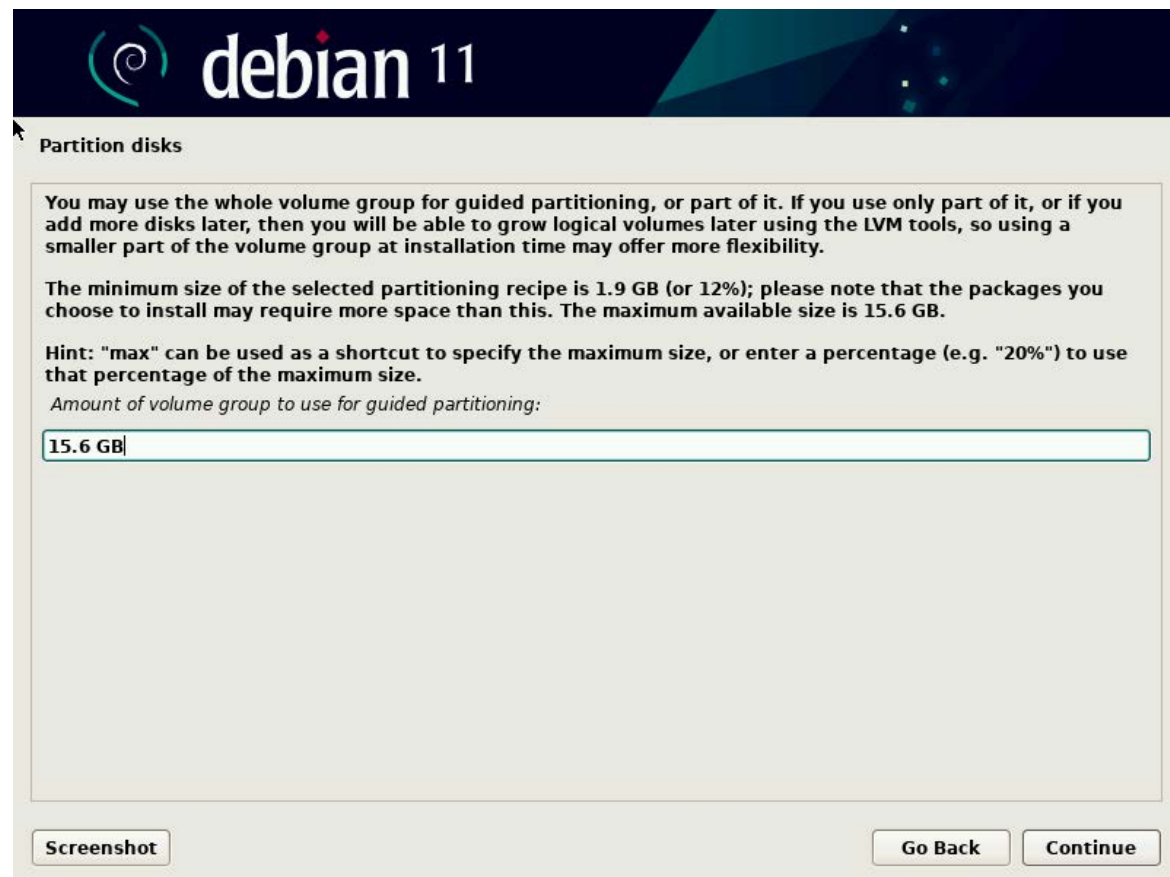


9. Once it's done writing random data in your drive, it will prompt you for a passphrase and you really need to make sure you don't forget it. Any half-experienced Linux systems administrator can easily bypass both the root and user passwords with a few commands if the system is not encrypted. However, the only way to bypass the encryption is through what is called a "brute force attack", and doing that can take decades if you used a strong one encryption password. So even if it's not advised to write down passwords, in this case it might be better than losing access to all of the data stored in your computer, so you should either consider doing that, or keeping it in a KeePass password safe.



Feel free to tick the "Show password in clear" checkbox to triple check you are typing what you think you are, and that the keyboard layout is the one you think it is.

10. The next step is defining the size of the partition and it defaults to all of the available space, which is fine in most cases, so feel free to go with it.



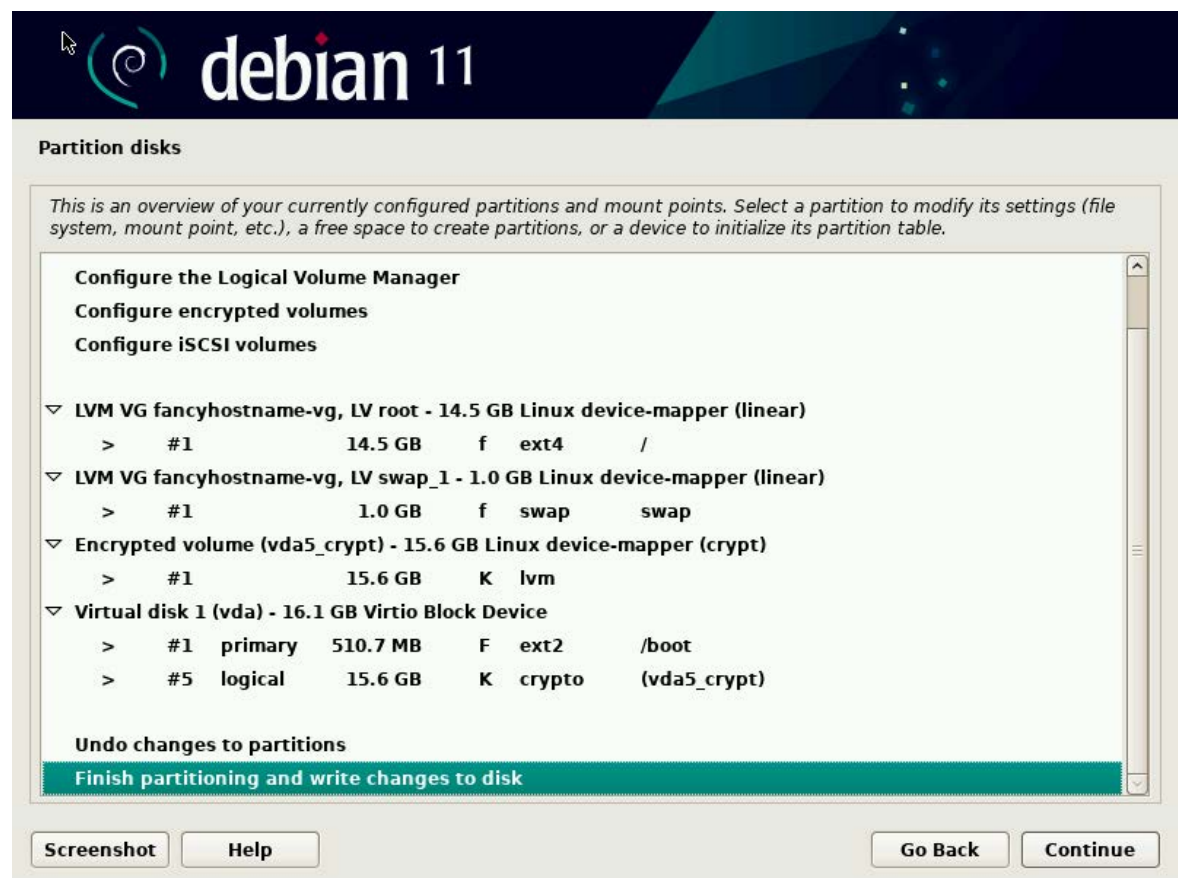
Then it will show you the final partition table, and you can read it from the bottom to the top.

Because we are installing this example in a virtual machine for the sake of this guide, the "Virtual disk" would actually be the "Physical disk" in a non-virtual machine installation, and it would have two partitions: the "/boot" one that is the one you'll use to decrypt the system on boot, and the "crypt" one, which is the one containing the logic volume manager (LVM) that contains the virtual RAM space (swap) and the "/" containing all of the files in the system.



11. Hit the “Continue” button so you can continue to the confirmation screen.

Tick on “Yes” and “Continue”.



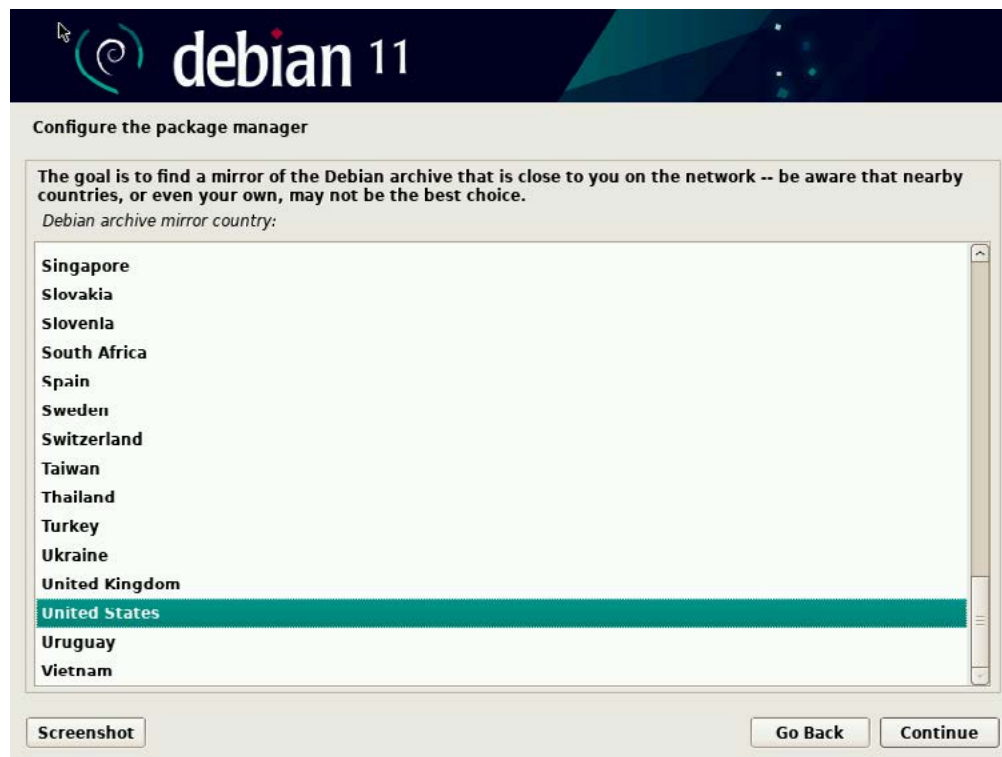
12. Now you only need to wait for the base system installation to be done.



When it is finished, it will ask if you have an additional installation media and “No” is fine to “Continue”.



13. Related to the country you selected when you installed the system: the installer will default to the closest data mirror, and unless you are planning to move somewhere else, you can stick with it and “Continue”, otherwise select a different one.



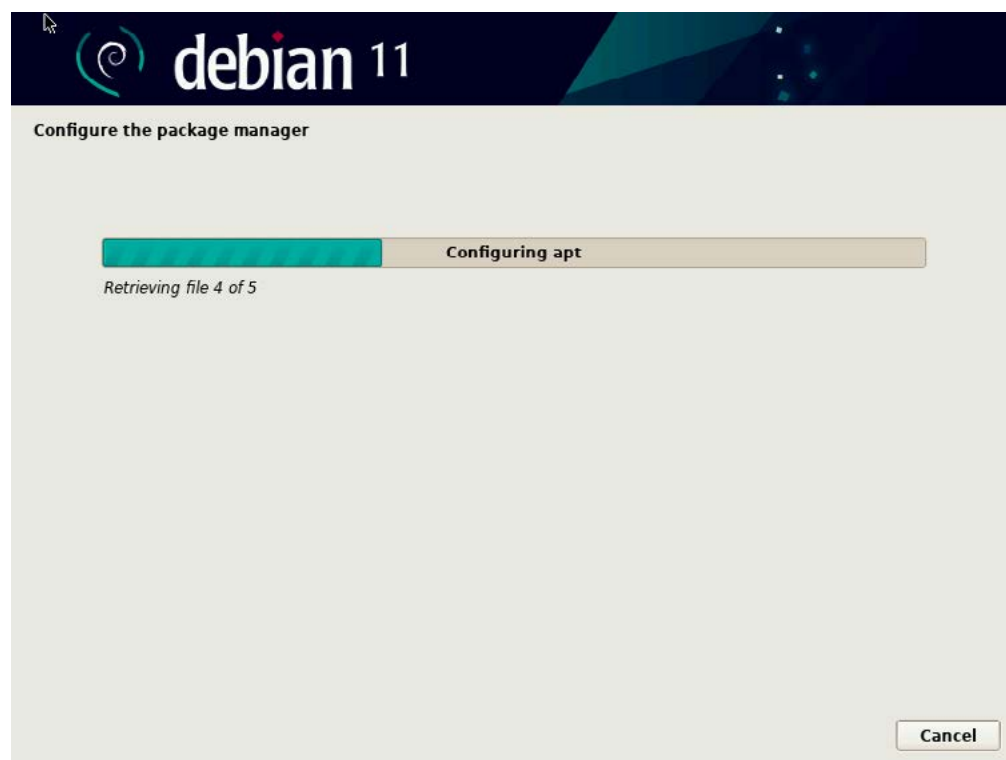
14. Same applies in this next step. (One tech team member has been using a Linux system for about two decades and doesn't remember choosing something other than the default on this screen, so unless you want to try something different, just go with it!)



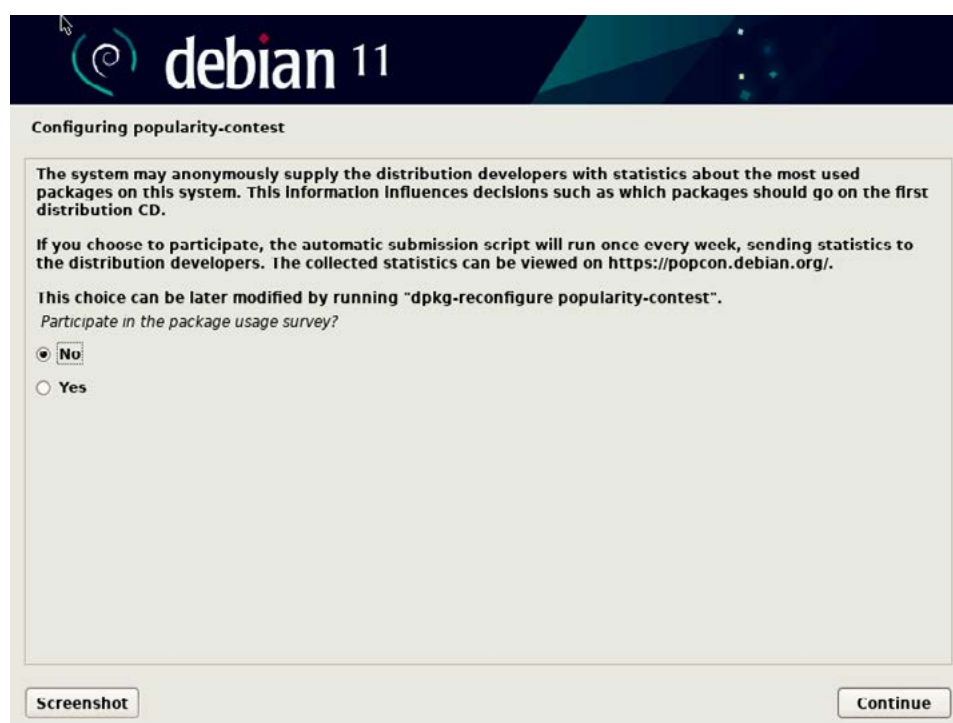
15. Then comes the proxy. You could use different proxies here to save bandwidth/time, but leaving it blank would work fine for a single installation.



Now give it a few seconds/minutes to install the package manager.

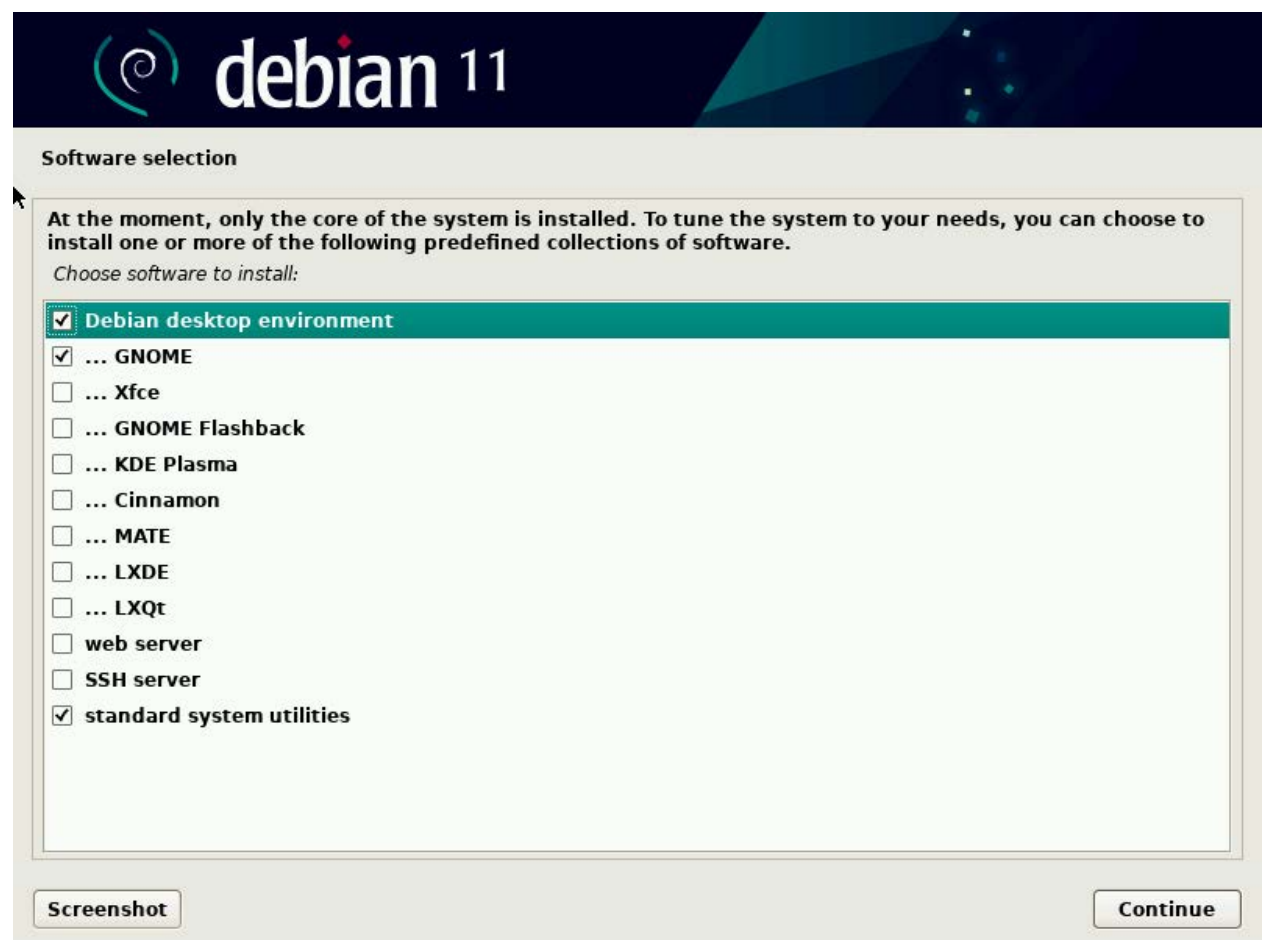


16. Once that's done you will need to answer one of the toughest questions of the whole installation process: would you like to share anonymous statistics about the packages you install in your system?



On one hand, from the privacy point of view, we don't want to share any information from our system, even in an anonymous way (in this case we do trust it's anonymised). On the other hand, in terms of free and open source software, this information helps developers better use their energy on the packages that are being installed the most, or those that have been uninstalled the most. And since it's always hard to answer that question, we will leave it up to you!

17. We are getting closer to the end, but before that we need to choose what packages we want to have when the system first boots. If you are an experienced user or want to try different desktop managers, just tick different boxes. I'll choose Gnome because at the end of this guide we'll rely on Gnome's file manager (Nautilus) to also encrypt an external storage device (USB drive).

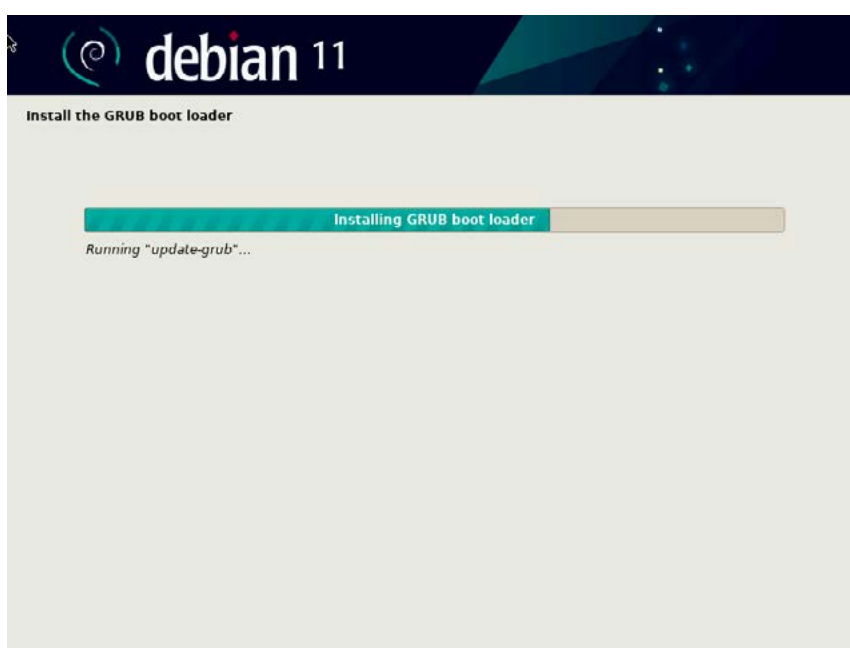


And hit "Continue".

18. The last two steps are if you want to install the GRUB loader in the primary driver and where, but please note that since we are using a virtual machine to document the process, it say “/dev/vda”. If the installation process is done in a physical machine, the primary drive would either be “/dev/sda” or “/dev/hda” (if the computer is very old).



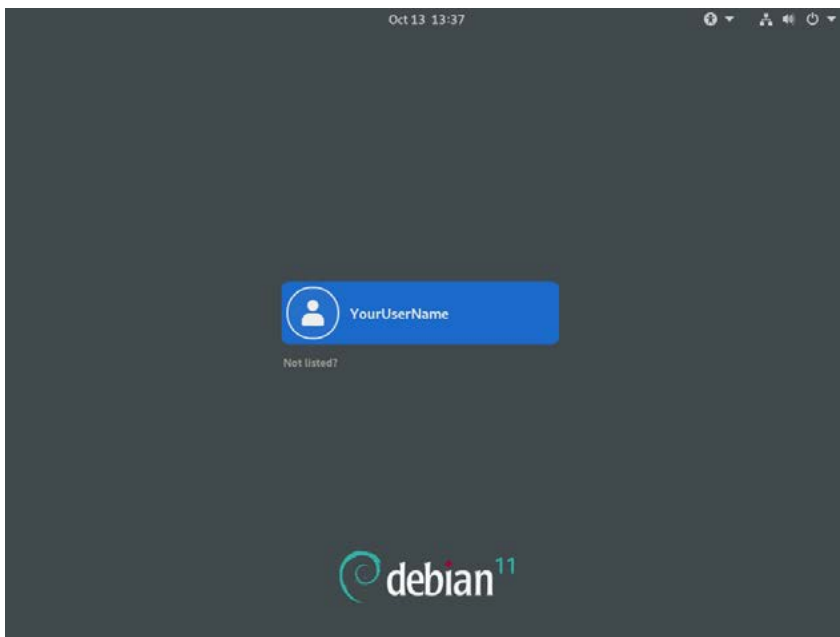
19. This is the very last step of the GRUB installation! And when it's done you can hit “Continue” to finalizse it and reboot the computer.



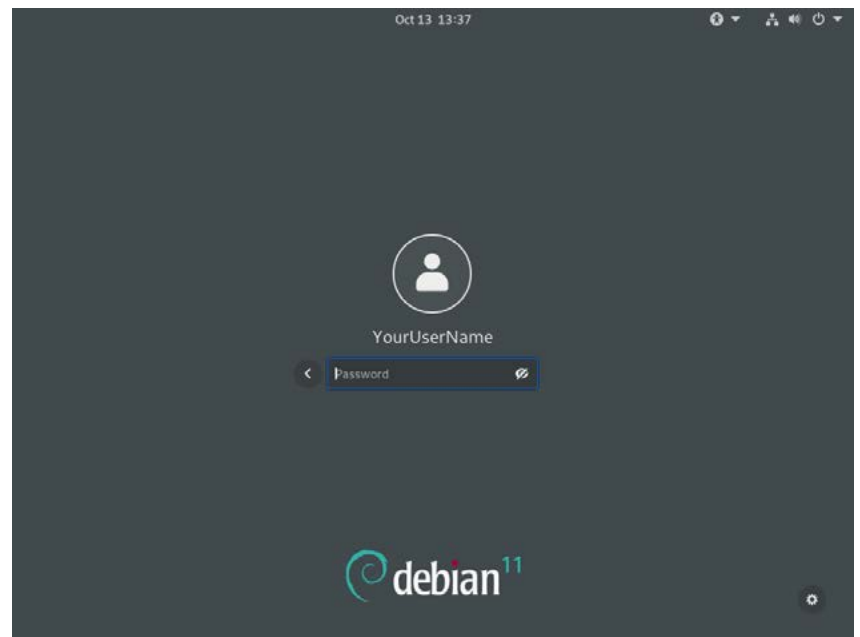


20. Once it has rebooted you will be prompted to enter the encryption passphrase.

```
Volume group "fancyhostname-vg" not found
Cannot process volume group fancyhostname-vg
Volume group "fancyhostname-vg" not found
Cannot process volume group fancyhostname-vg
Please unlock disk vda5_crypt: _
```



And then to select the user you want to start the session with.



And then enter the user password to log in.

Amazing! Your Linux operating system has been installed to run on an encrypted hard disk. Congratulations! But we cannot repeat it enough times: do not forget the passphrase, or you will not be able to access your data ever again!

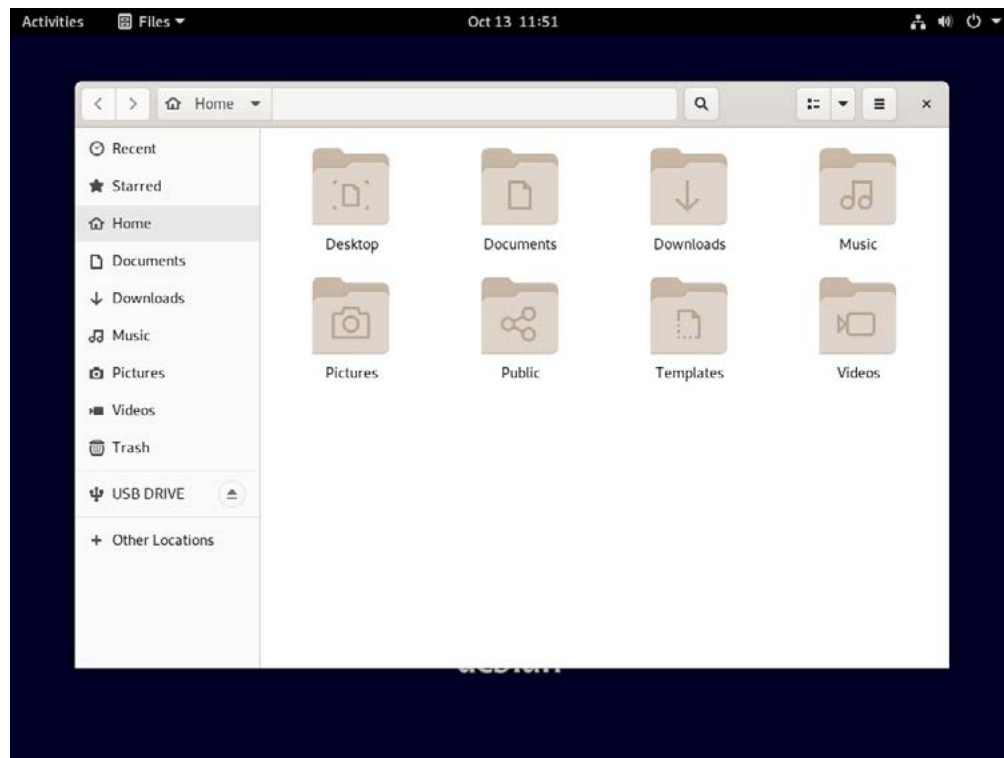
## 2. Installation guide for other external devices in Linux

Besides encrypting the hard disk where the operating system is located, we can also encrypt any external storage device, like a USB flash drive. Please note the same method applies for external hard drives and even secondary internal hard drives. Installing encryption means formatting, so all pre-existing data will be lost!

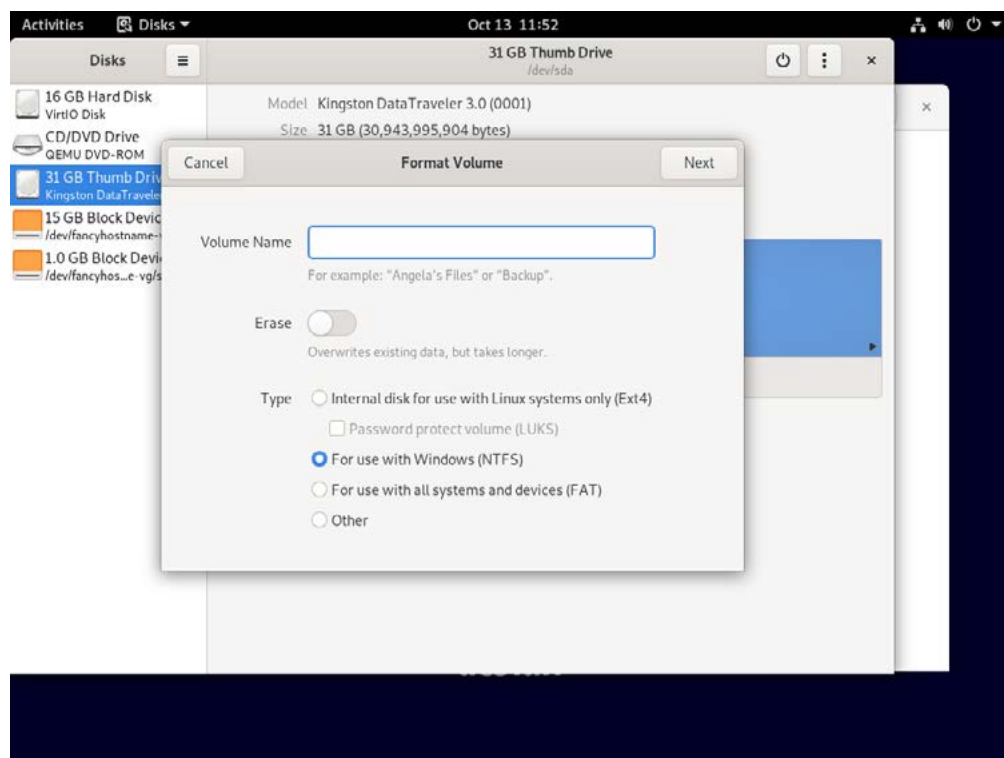
This example is running on Debian OS.

1. Start by opening Nautilus (the default Gnome file manager) found in the left side dock of the screen. The dock is not displayed by default but it will show up if you hit the Super key on your keyboard (sometimes also known as the Windows key).

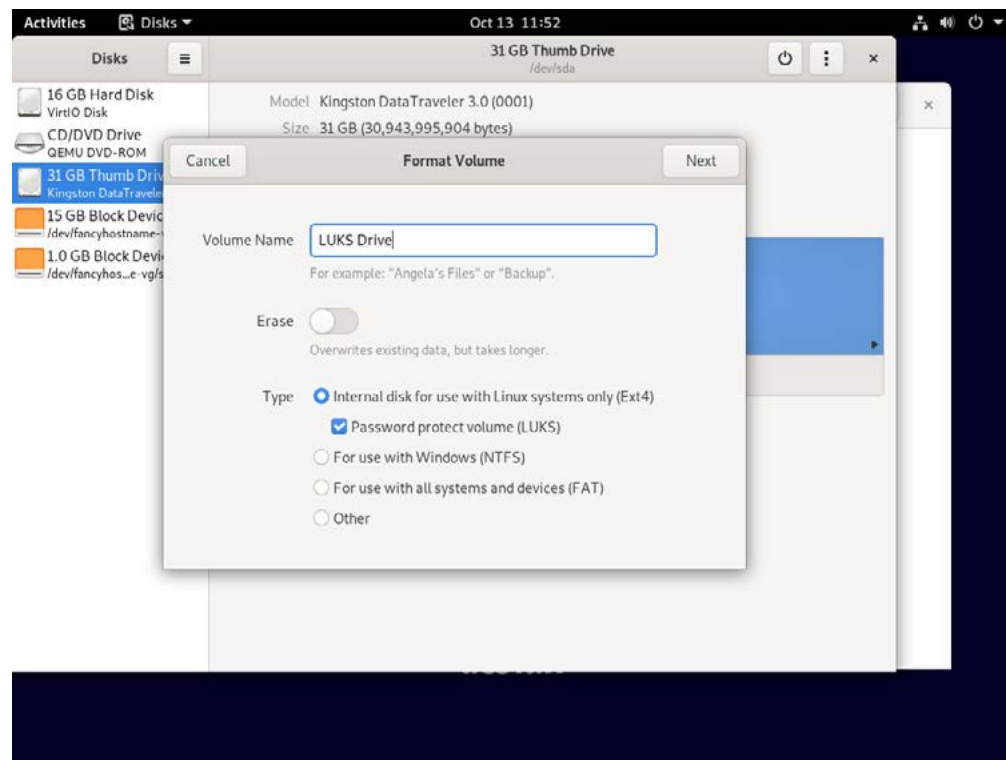
2. Either plug in the USB drive or, if it's plugged in already, find it on the left side bar and right click on it to get the contextual menu, then click on the "Format" option in it.



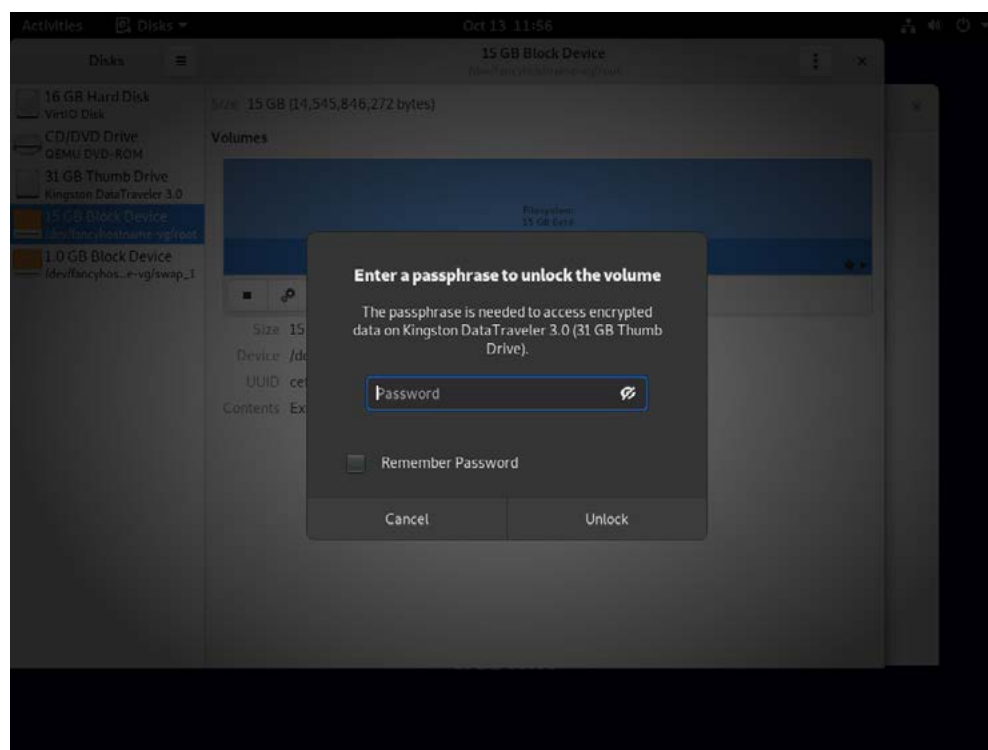
3. It will open the Disks manager, where for compatibility's sake the NTFS file system will be selected.



4. Since we want to use LUKS Encryption, you need to change the partition type and select Ext4 + Password protected volume (LUKS).



5. Click on "Next" and you will be prompted to enter the external device encryption passphrase (twice).

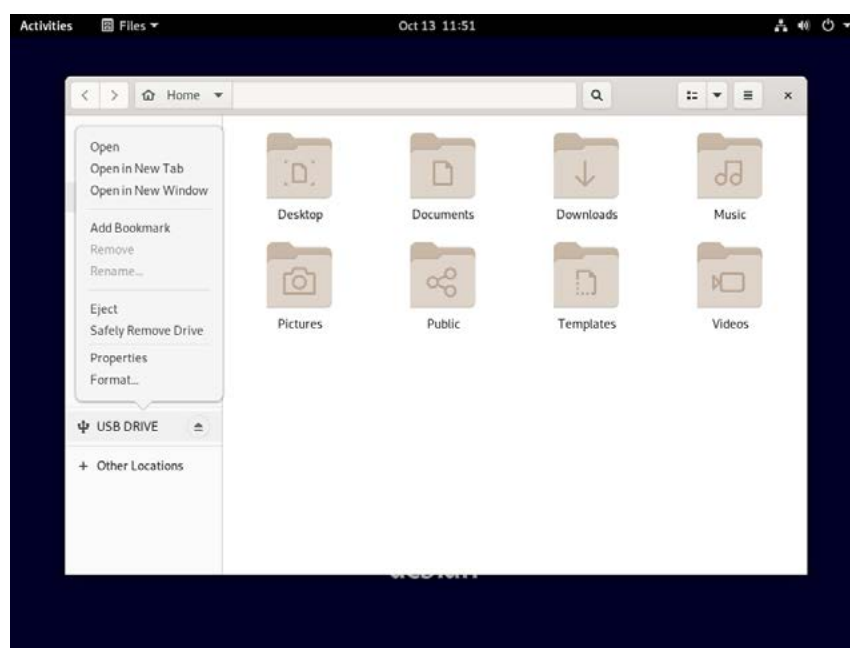
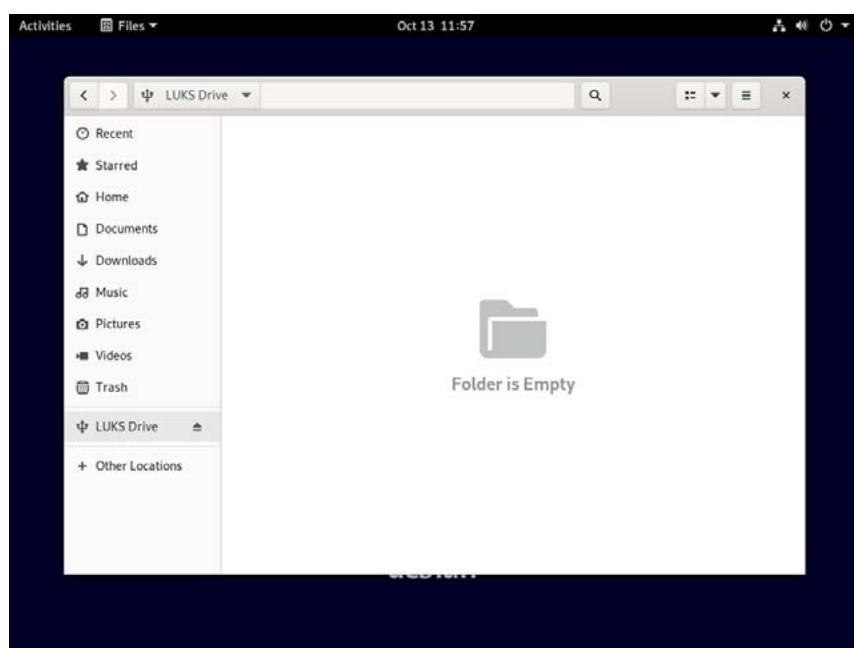


Your device has been formatted in an encrypted way and is ready to store your confidential data!

Remember: The next time you want/need to use that storage device, you just need to plug it in and you will be prompted for the passphrase.

Again, please keep in mind that the only way to recover access to that device in case you lose/forget the passphrase is through a brute force attack (that can take decades), and unlike the base system encryption passphrase that you will be typing pretty often, weeks or months can pass before you use a certain USB drive. This means the chances of you forgetting it are higher, and ticking the “Remember Password” box is a good option, but it doesn’t replace the need for keeping the passphrase in a safe and reliable place.

Once the drive has been decrypted it will act exactly the same way as a regular one, and you can save and delete files from it normally.





# 3. Encryption on other operating systems

If you would like to set up encryption on a non-GNU/Linux operating system, take a look at this [Windows tutorial](#) or this one for [Mac OSX](#).

RCRCD47h+smFB5HQiPDXU9sqNGu/2pYGPYHdvM+jUJDv1Gv+ka15DeVMevxfY4ktjg1TeRF5sR7VYN3XZG50aafOBYK0mAl0At9CDjRQMg6ourDe6Sl-1Hu6EzwVI+IHLD7dPCGmHLB8YRvRULvKlnBLwwwCS1l32HGPeYbynq1bJsLNQjSPY/LejwzHgLvS3IzeC5XoBZZRb6zlk804XBBBwOmRLHLHYMh3Vt-4G5LjpwOXfs6r0RrTxUDrArwmIQV5zG41SBm5Nev4SXPkDe12AoIdqdja7u0Bh9Kixj2MiOStp6CltpfNF70l2ziHwHSpl2d1ULIHlvvwyuFJrDXf/Q3wJmhd-9Bac2dwOMtvbz30LVCX7LkQpwFg1kllnSRVK/  
usFDBJnUHGXxXul3PfoVzf9a2gf+i7Bpd5TXiEkKQDZhATUrO7UEriDmrd8XESoah7LNEalDcAjwaD5vp8JlPqO1l7L+IepQEGdzv0sEMer7as1a5f/bIrT6Y- H2at1vsLEOxYo6eg1vBPUIRSdLKW8UYIdCo7gQOZdlqhq6s39DZbh7SchzCeKhvCUZbCY99hJ0eIAHf64e9zEvZiAw5Ve63Dax1YjFVqkORhxx4Rqi4px- O3XrTyEXfVVVWd6nE5GnOWVDRwYeouGrGw/1DrNZE/yaRy/KaQ358l7zEt4jJODgdzpz+bte93UDmeAY0gTAXaxX7eqO3Ad7jQeqli6AZ- zA5CXJuj8hEI4y+UEtftpB6ND8LQ7eOTyW8+U2lTUuwyJp0t16jSKNGJzo0JLdzLrHLMtKyv+onCyv+yuJitLkDXHEsPfuIaUSABQAQDHFimG8zUKTOPJx6e- ICT2sSlNfCkdwSRGuKcNzaIo6rR4/5RoS0y3irKrY9rATue9V6i6nFntJ0ilaXO3t44uIEa+TDwgEi0Rc8nuGf+ydGwAXmvgXyihvwoREzXOPThz9LN- QKUGWnkEk0KL7Jo/  
FqR1xnllm6/8N53XhmxK5iysiHmq145bpXp0HaUwBBb3xJIWoeZqi+rJjRao+D1XfAlaFjICf1lM8KgknANiB5OYjXBUMgGhichxyIPtAromCJZgGaVd0qsgp- 1WkvQhN6GN3nGb/FGU7FoOUx+dITfS0X/9O2XNu06+JDPy5Pk4C2G1Dmurs45Iz/93QzPOkh65pmkDMExUj6OD6qQI599wMP+BitXLbujtdi4RMb- 4gYTB5Zoz/ZR9z1DvVSDCS3/dRty9CDcbfYgCmXFqog7wnq2chDhwci5SK8uuyK4nkGBXlYl2ZgdajFclQGk8WYyTBSw6qfT1qYzH8ppxH41SoF9Cwy90d- 4HuXa+tNOhBhI0ze9DcJn7XwBs6FZGgN3mY3Qb3d2wQQvDw2sQTnUDYCpvaDyGb52MCYSAZgee5Bh/mpB5s9y5ISNsij6ESqfu/  
TDFqpImigkXFmHg0nWdkqLO4VwZNF7cxd83L65bxcJ/V4s8noajTr+bM6I8OQM+Q3C9bwhvThjXgKwCmYjluUXdgMoDPSGbwZqrOSjS8uLyZMWYgwc- bJhm2jG4Rqg4VjvhRX1pjVizR+9VDwlB+XiPDo/lXcib2Xmqu7bHGgiYtJoNH0D7mBQwJ/NcsYcJ85N5miy5M+xsx9TXmYHQ/ogBIIMR6DN7PThn- m7XL+Umghx19eGvVDCPM8cyIdz4rRHuhGVeh2yfe4T+XUHWopmPU7dBRgCra3Qp3VzTC/+VcXI2fhCmO+yHRen2M1JcnpXIMiCCfnh/0hLlfjNhG- 6NYrvf5uNe78U6c96ShYBq0/u3oB1Mi+QgEw0hu2uRAYDoO/72BH7LpNcG/  
A2US9xc6UZfxAXbxBWYkLgyqSCliATmDAIAYiTig8GxyJ7HCRSP4JKTGcut79tj1zahbx8PsaG2LwEvSKN3hkfnjTcglgftx4TAd+XvqlJf1vKxMmc0EGsV- vbm34ry9EYhBTRey6VM7AA5ggij/lHbzKw/NUgwJnhy52B6LAOSCBUv/QtGe5n60NqV4HZwjmzqZfcgNbDoWhRainRoxiScLFr65RbIm2b6YVx- 358mgU2N3D8MO5SbecZdh6OLgpcVZ4+hDOAx6YfutHgoe00dB67RPqviCUtdk0BI4n2XyvfK1N3/hIEnzHBZWth5ejux5Xmvbh3f3RbFITS2yC9h9Qdkk- K78HFzxAfEbZys6DHxjQnmfxwEXK2m+OewUYyCUxOfu4/  
iH0KHtWBHsqu+7/9e7I4nLnJkmQ8q4yhyllC22e9shwB+xEg8Fjz8yB83wSs2grNkK/4sb+GLy+IavdWbBD0ayFrUrdj5FdQy9Ejgp73kRXQRix/AK0Ev- 9fbT2WW6ybFdxYc/QbK1TdsB10Wson54LEdEEahujokm2Y40MxFru3j62b3IPEkSGh7vCuLxDnVoqvoWnp1ZuhQbPt52fN8xllJxWMnCiQxOoFMyza3H- HJBFQ10YvmLEclPSmQzVRPMnIoIrrF7EYbVxcSzblbBQLaLLJk/l9oJpmGVUjsPowLBLBENCWKZ0b35SpOT5t3RGxCBKEwKeBSGGENHJrIpst/vNW- liKFF3mSVozjgSS35LtucltDyUPl+MhaCJeKZ6Fbv//fXBaY3pOz+GQE8g6k5XGpzYjqQNOlO4HGEuzs9+mHrwWtOe76Pa0dgI2MakUgkNywLzFi/  
TsRNOFmQ2NLGkZ/chgp4x39ijXKaEPePrxY6jUGAcZ/o66ryu18HvXgXNaYQbtbFPPhcQAefgRuAxwBlcAf+3ftidray5kmNjCUdcM6hZOHJAa5xyMMrnLI- noMEM248tDNLf+7setWkla/mt/IP7pfOWL2OTeaz6p4hZAItOQtVdlyMjxJPO3vCPLBCNaLzMjT3MyPIAEJjQv9k+popDdc4wbXM5LBrWIn8LzLkPmS- jklE+anna8jiJvBlrgFXN/75AotkF3Y78XY4CfuX1tnWxm0Jlhc9F4VtFBYOSDylFbvHOhHzfQkFpKXusmyWgGYjFG8ad1ynxWJlcyXnT3NtPfZLPL70SGgkXx- dXP5dBiSpQ1QbUUZLrQjoyawULXuSxD37PewSHysKVtQwQeoHYUXS7yes3hx+S4fFHmyvN3vDdpb1sFixs3nzJB7b/NiT7/EYHQ/  
FOT8YbY5wYQZhv4PQWmhUCRBcUBiBSfc/Wx5lraZFFR0snjSY5JWWb776yN2QtKi36C0EHSg1syrQJDj3o/GaycRv6duA82j8J6ZVxkLA5eug1REFBxVfuA- 75psCc8AKJbInIHPkaCAToydNiUDl3tfArnxpianjZsR7a8RD9ThjS6yS8TpDQoANjnVy2ZGTxYTotMLBmsazT9YpnTVQel1Acf9xEvaknAbTPbEcNjK86Pjsd- 1pafmHmUs4q3uVbvKmfUom8Gug3g8qvMtFceUh1+rgw7BuQepZtKCRdRVgIKAZuRjJGaAk7xCGDmfK8SqYcCvMuOm3AmN3Jy/H4+Pyr7mcvzSTUBP- wa2XWKIBFBv8C4S01zmwCfHZpabnqHWDkcRM5JbZeM4BEF6khXnH+Ofu7N8G5eBA1Gcd+iyxMxIcD6kfsK/sDVDTPvKHPLqjM9d+dY/  
P86Esraaf3h0Z/ht93rQeucZ/mvJIVURHzf1MNIECgnPSlrKM7gCeGwMh7KtlhveZwhM3TEbTf/suUfXM88HYVUZoSo4e9BPGhhUeTsEbG2EzFeFHCMo- 6OsXLHA4M/cxRl3SZ56mcyIXgbRXgc2Qel09rTJjXEKpvxKF29nxhZVjxbumI2th4+q1lnu9gAkRLcEDQB2gUXW7mWbahrkriYcpFHCKVS60wYbuU- W7m6bnZweUXxfqhgG0oShTYB5c/ZtBW77X+F2ZOmqaeUSIvCBP75VcFez+OB1+A5oS27Kyh4cMUL8isRaAYWw5Rj+Oa7yscrYy6m7jTE2IdSp1Qfj2E- 2Hb8TC7ma/KYhjLYPtvCpKXTEYgayktoCdrCkGmoK55NyG7gT78IVQyt5R/  
No4VKBtXNIGl5jczdkxwoLWfu4i6YUctfB4HXBVn1pZuqBgjTEG9NsYsqN3Ft5LXyc+wewGX7VDndyn1fkRCGYL9fQEMf9s+4IUiHkAkPwHD+vZZIv3Ix- kelmFLUr1uBRTjla0zosbYVZ1kGqAHQt85nmTI3mHlvh4ooEye3830b01WIJ06xgRT82Xw1hgBlHHhHnt+v2mgyn9szRVJZDlxlyWodoXqkX2h1El+5ZqdvX- uDA0H12GZbuswB8TOSN2EzXXXJ9VYlbsPOj65k1rDKEtDntO38nofLkq/yQ5pKn8zfhr7aZvGXcqKgzoUNk6Eyf96XgLKKIqOat+Js5UL8OX2GGM3bu- Gorqfv2NeKUAbpuX5DmmRB0mOlhFu989VgVzePwGwzOt4JeFa7nOvb2dtzfqplJyyu6Sd9DnXF1bCwXQwzysYePxeTnNQNx41q8sxVerQ6bPngk4bD3qi- 2Lupo2WtTwEko2HAIGP+wxC/  
iCQ1x6ncv1UHfq5eOM5zUYfYnJS6g0E8zjCcDrN7ytPHpx44huFnLGOpCY6cdlAwAWOWHYB+qMTegvkdze8Na/87m7yGipRjk32j3wOIj7f7pGZju- 7VbhZFiqQnYLBph4JXdzsi3MJjRnc/4gsj2Dx2K2yDZNxNwiwuK95jMYpfs3eSGm49iTtZhr0/2truYRGbSwOeOpDqjighfjKyIV9+UZsugrTi- WU4n3b35TzYZ4Q6spwhbgl94rXYM6DYlQVhnK9N3yHXic6WnAi4qAhwbITis+bHPQuUvNcsvEsu5CP6mFfK6fQfZZjvX3H51BPj2xGxfAaveH1hSe9esRnu- ERZSCDoG94Y0REpgJNjN0olkwyDWelYvy16rfrbEFIsnvw7ONvoLfDVuA8Aqg+omSD2n67xKekTF/  
nFkYdxqmYEi6qrxzYyzU59OQ1R9gc9M2VhWDzUkCpZ1LJeJltxe9I+xF3mDwnj23fmLRNcIuOFTB3B0PUNj7nB894YT1oj5e9kN70ccL2hvAY+yB- 8Z5di+Ka7ptB8p1Xf0DQeKMGozk14Yuz4dq1tVA17gGgjlNkjWgl9u5vsMiqqOa3dGvKO4Ljzpmz2ACY4xPXYBDg5spBXzjTpnmelojX3Lpo07y- L++FF7ZUfGj9E/QtmFhq9F/7vzz4ropvzLi9uRCrat9+ii1jwSLdke+14m2Gz+hQtMQ88tvdHbJH2vjtSDaLzuGDkXeaYZHS1hEzE0+nwUmEWiORPWJx5C- qdw1ugFVMMy2zmA/IO8XBaiMbZgg9xggwWf/20IRyNYgzVa9utCKXDL1MNfTF4tqICm+V3/  
aYvdcYew54lfYN6OIvuNgDIVCinPdNsN6ippzBgyJpl3A7DtnmmHoKvRmQEurHuoTszaNvr+VrW7kp9gWxK7TEM09a/gIwf2uEh7WPR6l52gXhIRVuRnI- pRVj9Is8DxpXPOMqcqw5NPIT0Wf5kVQ7W3mcXNLxDHkEUjPGNCBy+N79Z+vCD3fuesHM02/rUaSS74/cpI7e6h2G136OvWclpwL3IbIdYVn/  
rs5451SHUBwnrTvDhK9boMSPLzxN+5qLv796DbRXjtFtaL5bPFze2Rruc/zGR4LK5CLaPcdI5BbNA+1L/R7wRtDAAwZy0k+EWBrj2Clf7+/JeikB- jQtqkvQ45vRyxsKojHG/cGW4BXyXMUvkYNWUKJAXKTS6O3HAptlyFBq02taeZRd86j9RQS8iVsrgVvYQDpd0GEaHNZs76nQTet29rJeOrxxzn/49t- MqMuh1SAlJI9lW4tkjmwbn5aBnRuJaDklefZoCrpnWlx9Keb6cSa0J/Zkd01nUkR5RioawWcFehq/dzFJMB46v+ZXCT1HfCeHjq+ToiLVAA4H3UNfMIvlt0e- JwhwNbP3Bp4Oxjiic1dKorifyKmmVsrSyVoizuUCuCK7PTY5kFlbn3+rVkyBm5CtkAfkaHjkjDRZuWeUeDFBxG5vDXr+hTvDacjllAl0CooAVvoTskFygegwR- 9wMu5JBL5tIxaaF9la6oxFdynOOOnKaQD55zpd2dPXapDFoi1N0LkE51jCeZq5VF+ywaX56xLTmIjx39VKX52VdwLBbuYs5IqRa2Ge+ZM5nFcG8XX3wwDf- WruUdn2HG+hwyppzkQw4cVGl1jaTcfxiURvW3qC5Y5GwBrkTM4Cl72OLHzgZAjcAIK99oKkD0sv0k+zxZ1wdsrQBeAv2pCyCEVUMFBAQKEPwNg8h6VYP- j0+ny02+rPSNNalHMUMEQT2tXdCv+LvmB7NQwruI6gcEcdRmwhxD+xYXREOIohHfFnL68nFGLDQU7uYJ0q9TvdCwyuvx+Ah1dkuHOEsbnN9w5T- 24Fm40y8XXVe5laxztMRG3pY/EB3A7j+pxbUrK5aXPxDWuH0NFzcV9+xUUeSgywYvyECTh6/  
slLnaDjiYVS5Zc6iKecfec4g9HKRX8wiNYReL8UU3e1+1PrHOVeq8J7HPKPUDsbpH6OVzIeyGoPflwzZxoF0T4DfP17zZ/M14cZ0gAOKMw0IP1Di- 8Wyo4rEyz+9kC2x/M9RshpEoF6UC+qISConwdZ72fiVpC3KcME87Fi3tmDaTuDQRIDwB5LOEbZuOxmVN3qbni6z9WB7OqIfFyfV+ZDH1cCi9ZD- IYAZ8WHh+LtQIKe0xhys6lVUM0ihCgFcy//JjLQREDIxXUi+15ejtUlzhNu68T6clxUYCm9CG7V3ncQLxouYJawZ2RgwTQYwJo2KakQfb3kQ7MfrMX- WrQWwRKzzmjOhri0yoNjgNiTxKHclDR6LriGq9sM5EFNAHpcGvbfFwxP7KiMI7tGgVYDRZ9SzCkAvKe8K31pP+e4RuYo3XBCMKSDfvt0TgZjbOO853t- M3hucpLcUaQUQ93N//  
NVs9Gsv+xd0j3eKEo25Cq2COHHS+0PumSH4Q4Ru8Psjwe0qawVKBS1OubrluVVB0d79nH3CL7rXcNor+IueJkm2v5O6cWiiaraRyqgeTbHTWsoYsBsjLs- gieayLLmGkWfgV+gGZDSUGeoM+tGuoVIjVvUvqLi1Ah3OcFnPbQg5NnJoEi9YuqrGVTM36MHBGkl6L7DP+z9GQxsl+JSE2IMNofjzwx94Npbt1v0wk2LL- t3yzMWtTmozRZG0htlcGCEdjfJokBL+efVZz4HxaH689Pnv4yxOEannscrB+sHvvU0C0SRVJUGXJ7QzTvS+O8i2Sm+obtVsuWGTvFa5nd0x- g1ke551YcsQf3eRe0l+2uimcWru/wsXg8eHAa1hEHpVNI5kytLXFDQPNE5h6pZqjJhVrANyg3/f7je9pYsP2D8kgaf/