Disk Encryption

This feature is available but is absolutely unsupported. If you choose to use it, you cannot expect support and WILL NOT get support in trying to recover your data.

NAS4Free can encrypt your hard drive (or RAID array) using the FreeBSD geom eli module. This feature will use a hardware crypto acceleration card if supported.

Warning: Creating an encrypted disk will erase ALL data on this disk.

You should configure the WebGUI to use HTTPS protocol before using this feature: The passphrase used for encrypting your disk must be protected when you send it to the WebGUI.

The encryption layer must take place between the hard drive (or RAID array) and the filesystem. **The High-Level process flow for encrypting simple disk is:**

1. Add Disks
2. Create your encrypted volume using the previously added disk : This step will automatically 'attach' this volume
3. Format this encrypted volume
4. Add a Mount Point using this encrypted volume

The High-Level process flow for encrypting software RAID array is:

1. Create your simple or complex RAID array (chapter 4.6) without formatting it at the end of this process.
2. Create your encrypted volume using the previously created software RAID array: This step will automatically 'attach' this volume
3. Format this encrypted volume
4. Add a Mount Point using this encrypted volume

At each reboot of NAS4Free, the mount point using encrypted disk cannot be mount automatically: You must enter your passphrase to 'attach' it.

Configure your WebGUI for using HTTPS

It's not a mandatory step, but a highly recommended step before you create an encrypted volume: This will prevent transferring your passphrase in clear on the network.

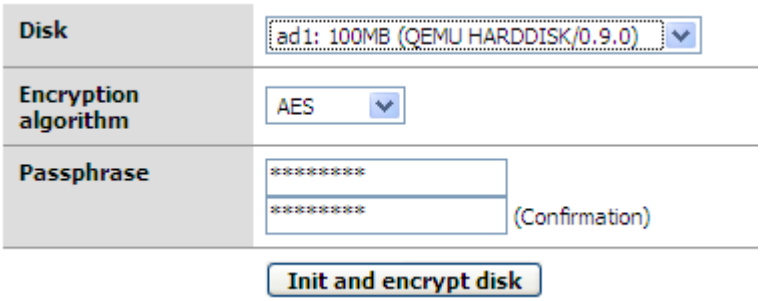
Refer to Chapter 5.1.4 for how to change this parameter.

Add your disk or create your software RAID array

In this example, I will use the disk 'ad1'. After adding this disk on the disk management page:

Create the encrypted volume

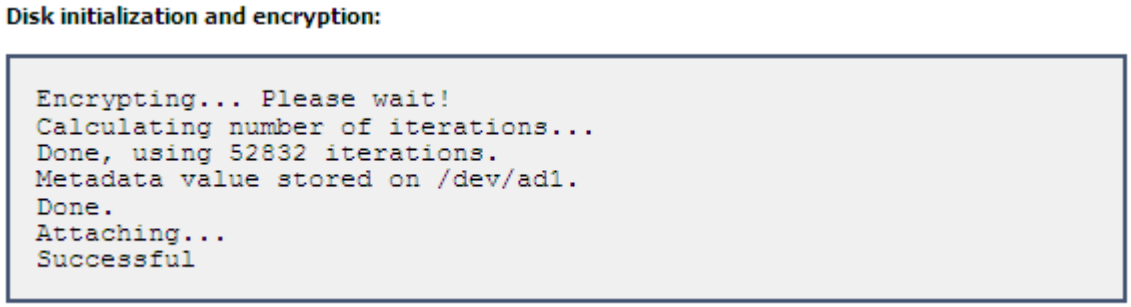
Open the Disk/Encryption page and click the ➕ icon on the right hand side.



1. Select the newly added disk/created RAID array on the disk menu.
2. Choose the Encryption Algorithm
3. Choose a strong pass phrase
4. Click on “Init and encrypt disk”, and confirm

Generating time for the encrypted volume is dependent on your disk size: It will fill your disk with random value.

You should obtain the following output:

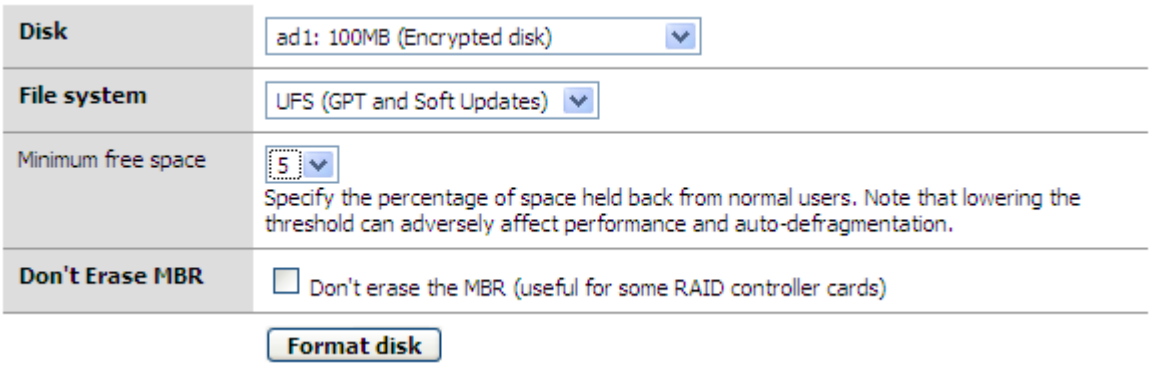


Then click on ‘encryption’ menu and ‘save’:

Format Encrypted disk

When the Status is ‘attached’, then the Encrypted disk must be formatted.

Open the *Disk:Format* menu and choose the newly created Encrypted disk:



Leave the Type as UFS (GPT and Soft Updates), click the Format Disk button and confirm.

A display similar to this should be output:

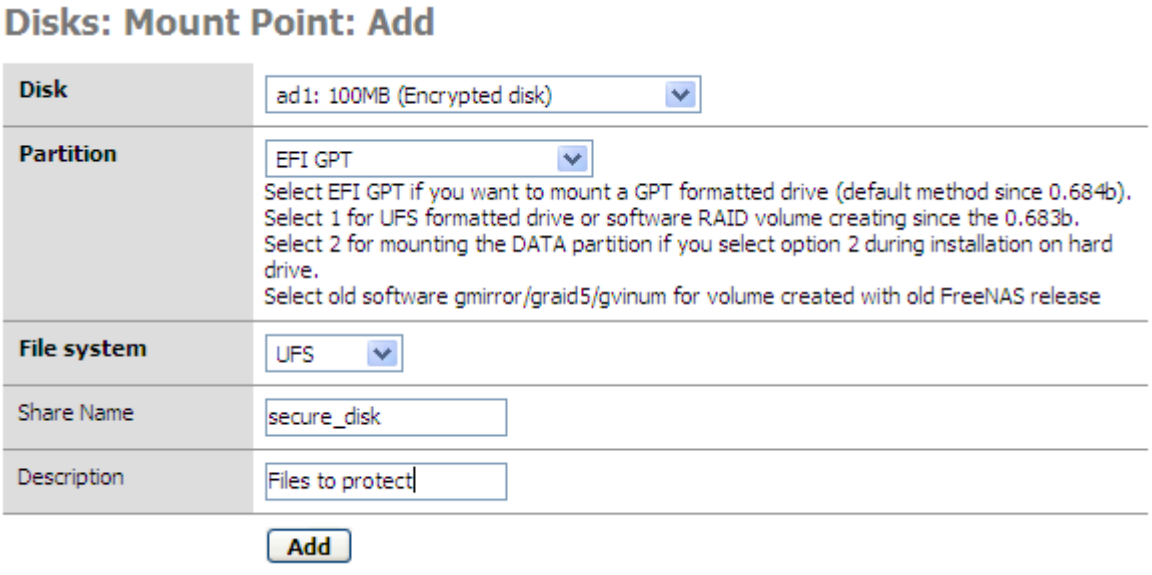
Disk initialization details:

```
Erasing MBR and all partitions.
Destroying old GPT information:
Creating GPT partition:
/dev/ad1.elip1 added
Creating filesystem with 'Soft Updates':
/dev/ad1.elip1: 100.0MB (204732 sectors) block size 16384, fragment size 2048
        using 4 cylinder groups of 25.00MB, 1600 blks, 3200 inodes.
        with soft updates
super-block backups (for fsck -b #) at:
 160, 51360, 102560, 153760
Done!
```

Create the mount point for encrypted disk

Once the Encrypted volume is created and formatted, all that is left is to create the mount point.

Open the Disk/Mount Point page and click the ➕ icon on the right hand side.

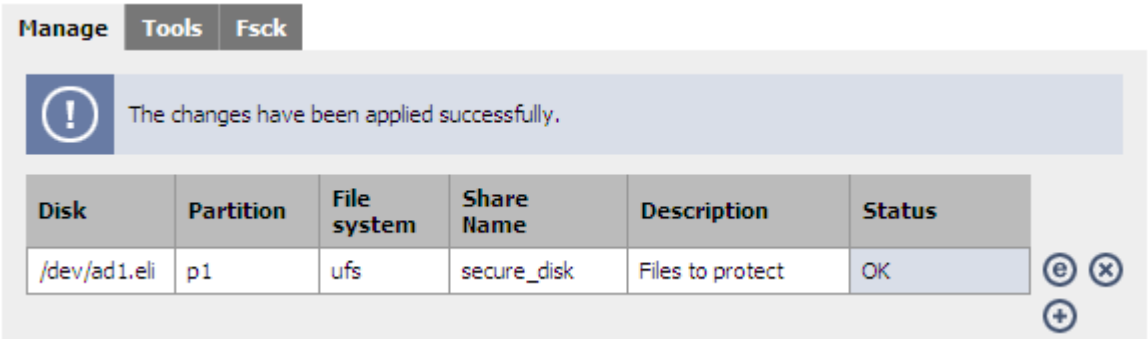


From the Disk drop down, select the Encrypted disk. The Encrypted disk name you previously configured is visible.

Change the *Partition* to *EFI-GPT*

Enter a useful Share name and click the Add button.

The Status should display as configuring, and then click the Apply Changes button and the Status should update to UP:

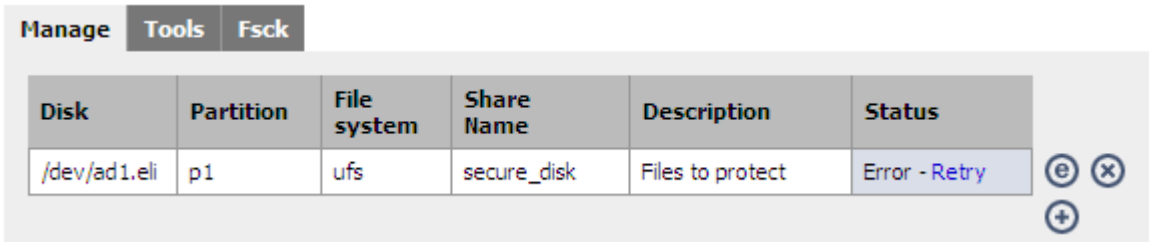


Now you can use your encrypted disk. Try to put some files on it, and we will check the comportment after a reboot:

Reboot for checking your passphrase

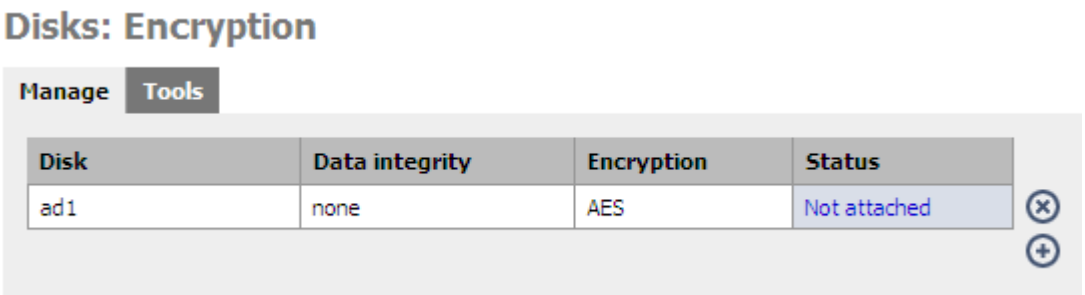
Reboot your NAS4Free server, and open the Disk/Mount Point page.

You should see an error because NAS4Free can't mount this encrypted disk without the passphrase:

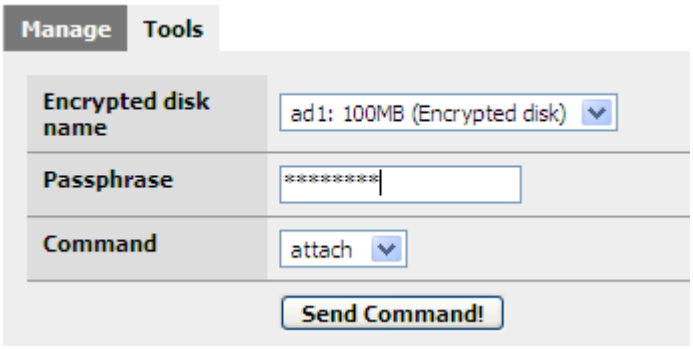


Now open the Disk/Encryption page

You should see this encrypted disk with the status 'Not attached':



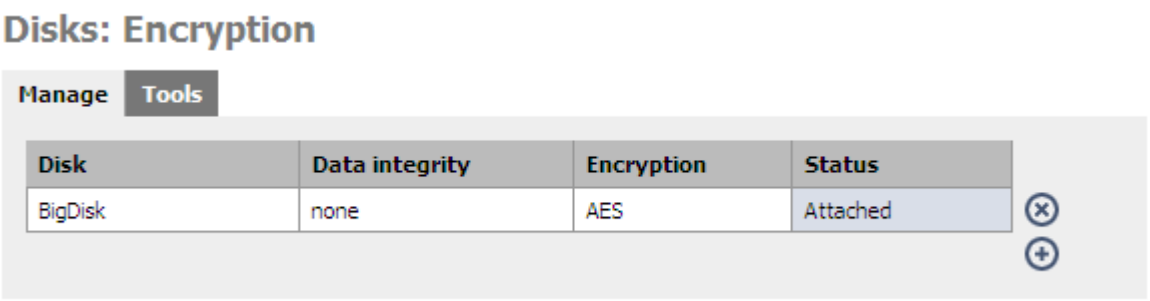
You must enter your passphrase by opening the Disk/Encryption/Tools page:



Enter you Pass phrase, select command ‘attach’ and click on ‘Send Command!”

It should display:

Now the state of this disk should be ‘attached’:



And the mount point status should be ‘OK’ now: