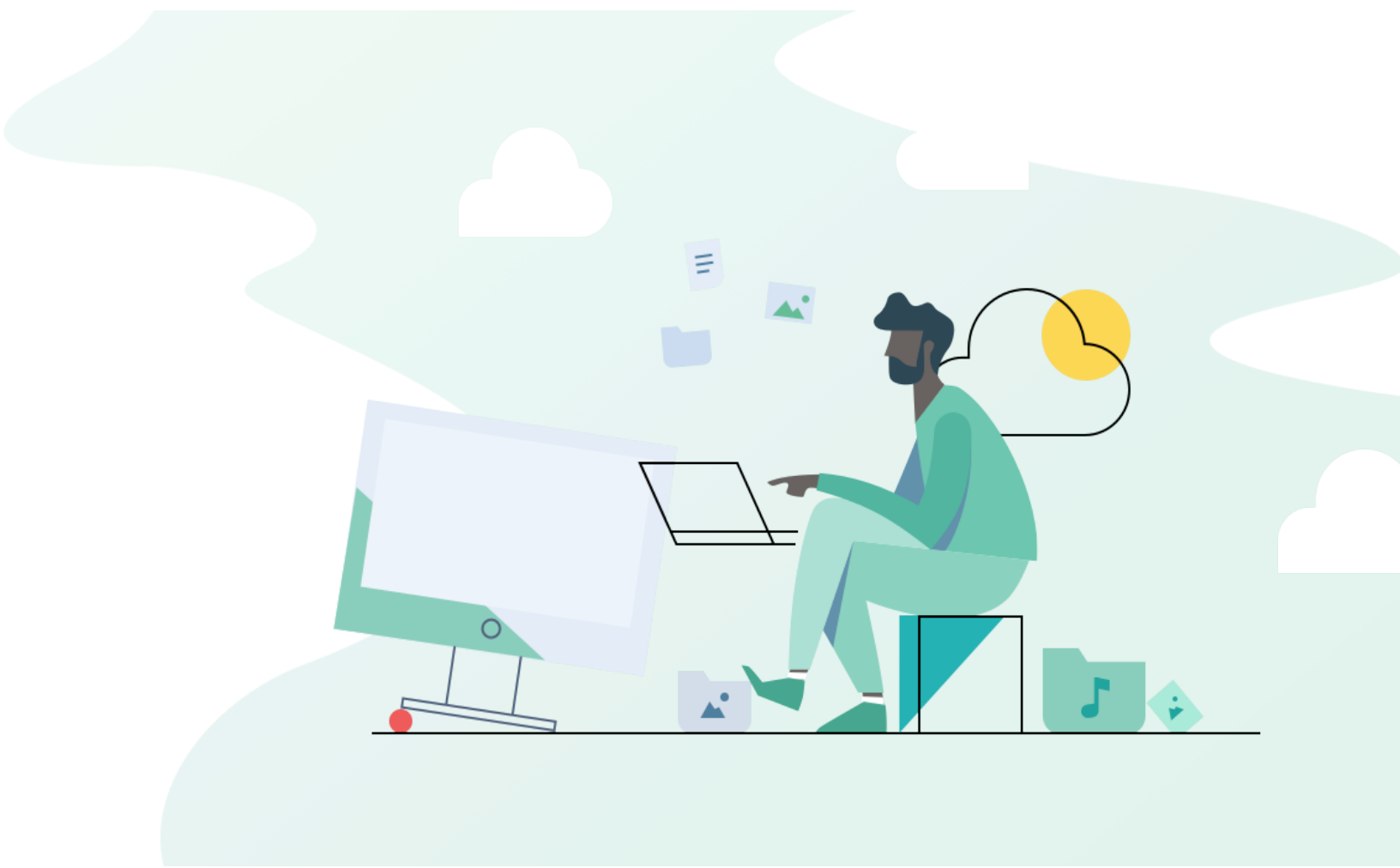




Installation, Backup, & Restore Guide.

Linux



Index

How to Install Cloudsafe	3
Getting Started	4
Logging into Your User Account	4
How to Create a Backup Plan	5
How to Create a Restore Plan	14
Contact Support	22

How to Install Cloudsafe

1. Download the installation package (the **.rpm** or **.deb** file) onto the system.



rh6_CloudAfrica_OnlineBackup_v2.3.0.12_20180305192509.rpm

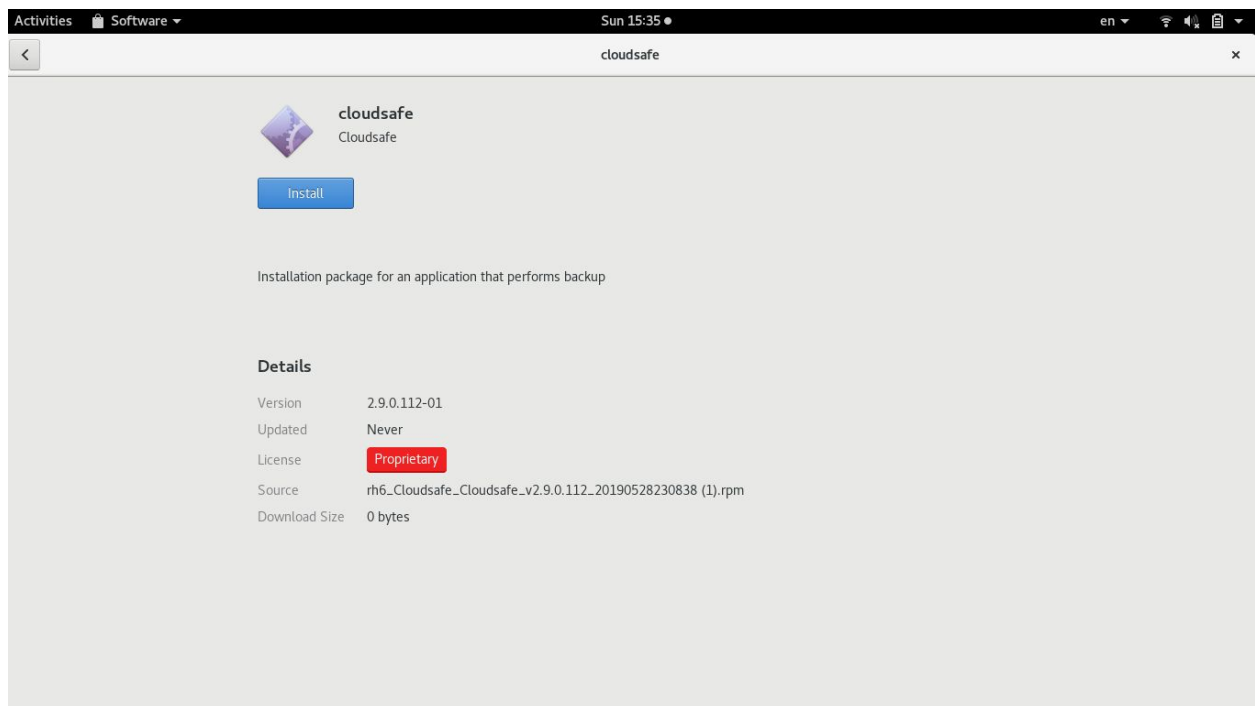
38.3 MB

12:38

2. Run the installation package by double-clicking on it.

4. **Fedora version 28 and up** open the terminal and run the following: `sudo dnf install -y libnsl`

3. Follow the installation instructions.



Getting Started

Once the Cloudsafe Installer has been completed go type the cloudsafe in the search bar. Run the application by clicking on it.



Logging into Your User Account

1. On the initial start you will be prompted to enter the user email and password you received in the welcome email.

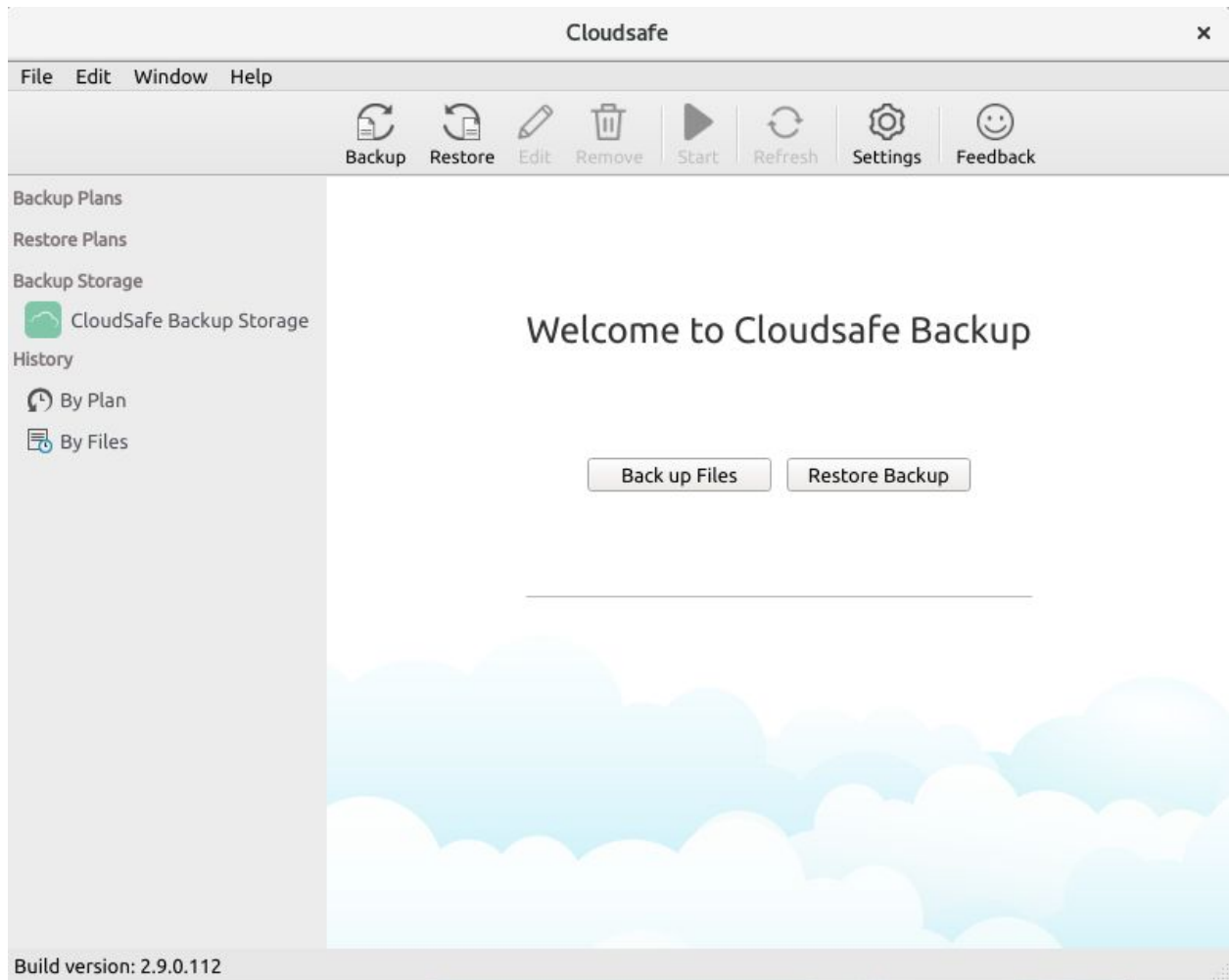


The screenshot shows a window titled "Cloudsafe" with a close button (X) in the top right corner. The window features the Cloudsafe logo at the top center. Below the logo, there are three input fields: "User Account:" with an empty text box, "Password:" with an empty text box, and "Product Edition:" with a dropdown menu currently set to "Desktop Edition". At the bottom right of the window, there is a blue link labeled "Proxy Settings" and a "Sign in" button.

2. Once your user email and password has been entered, click "**Sign in**".

How to Create a Backup Plan

1. Click "**Backup Files**" or the "**Clockwise Arrow**" on the toolbar to get started.



2. **Backup plan: Plan name** - Cloudsafe will automatically create a backup **plan name** based on the time and date. This name can be edited if you would like to create your own custom name.

Create backup plan

Backup plan: Plan name

Specify plan name

Plan name:

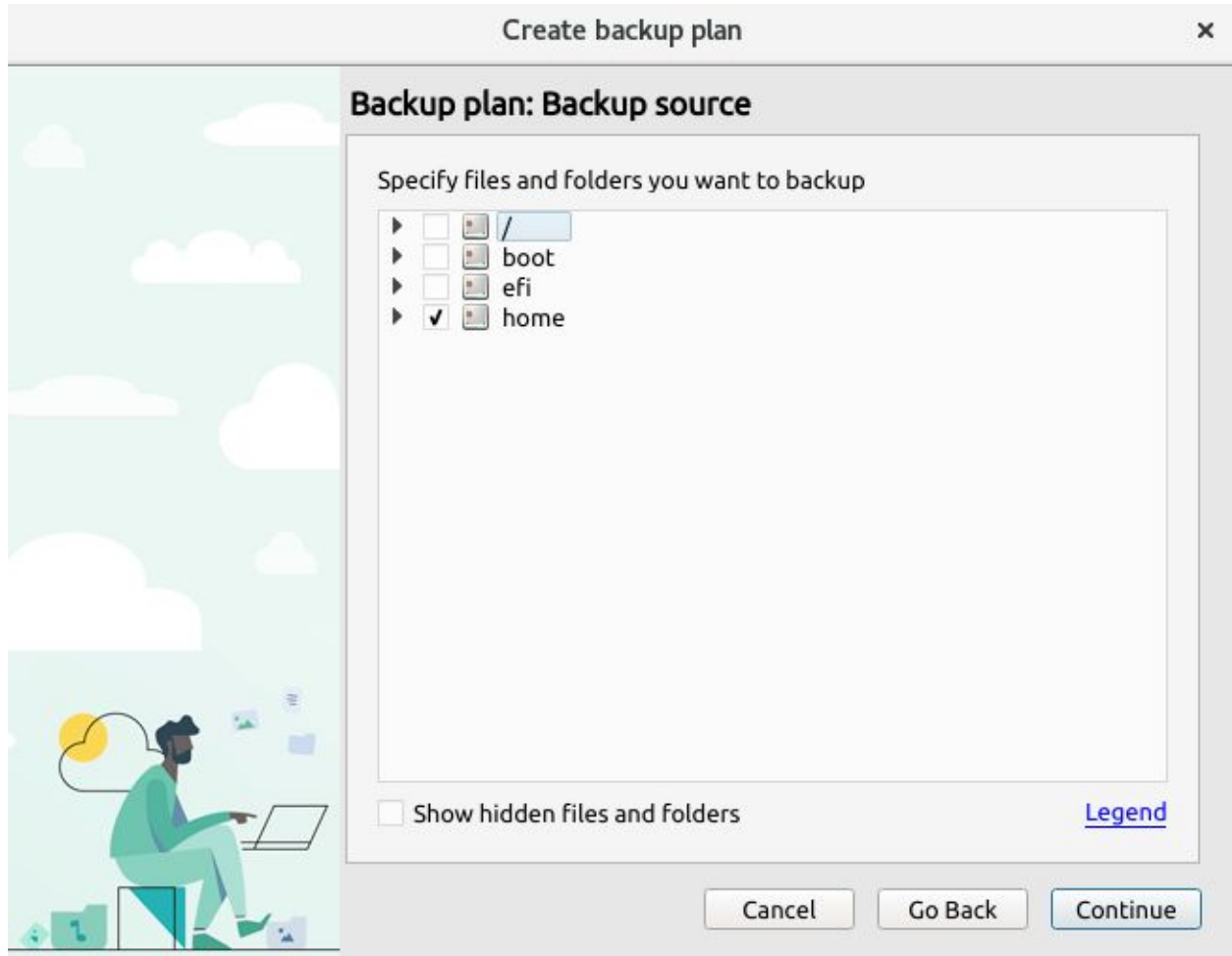
Use block level backup

Save backup plan configuration to the backup storage

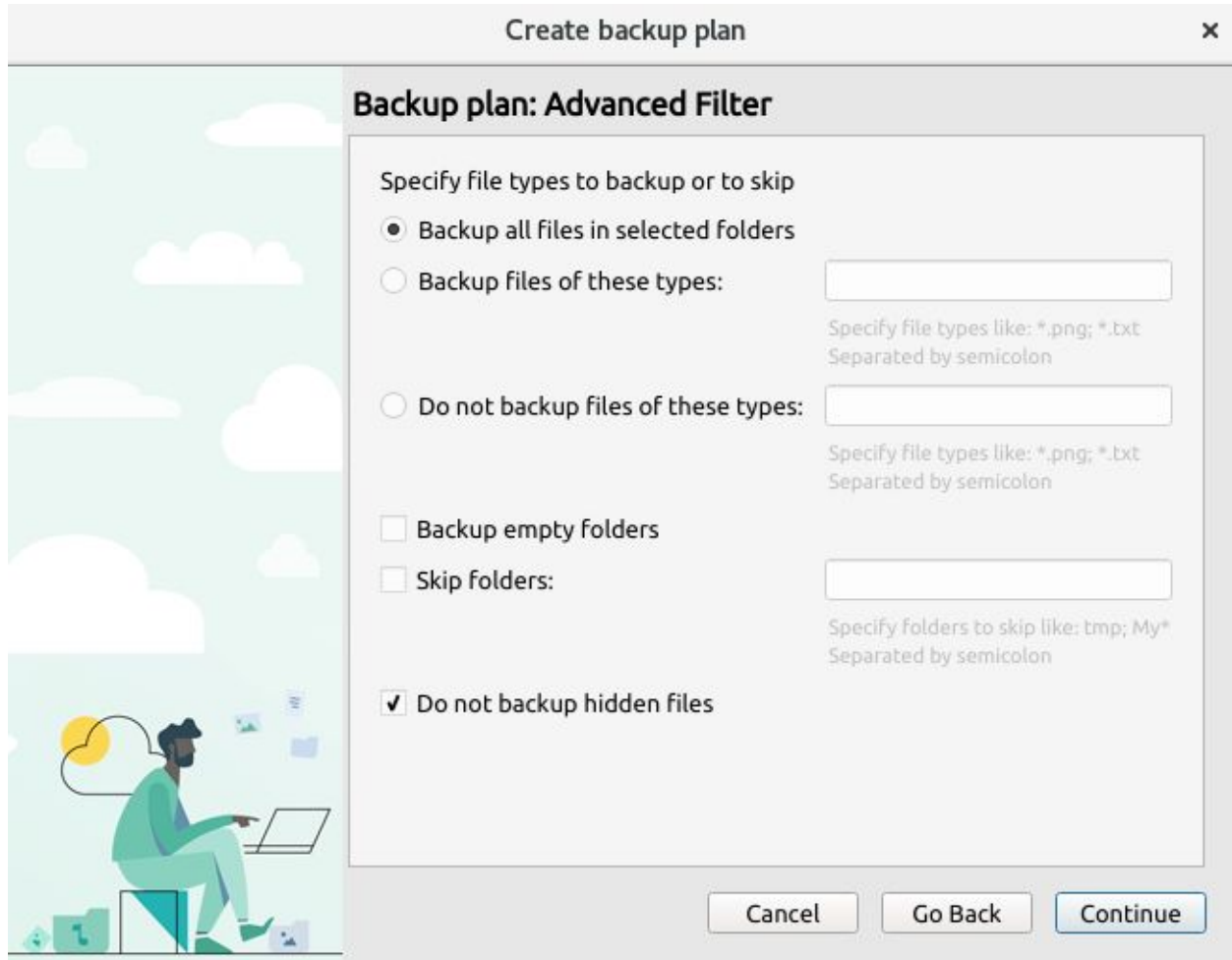
Note: If your plan has encryption, the encryption password will not be stored by security reason. You will have to specify the encryption password during restore.

Cancel Go Back Continue

3. Backup plan: Backup source - Select the folders/files you would like to backup.



4. Backup plan: Advanced Filter - Specify which file types you would like to backup in the folder you previously selected. By default it will backup all files (recommended).



5. Backup plan: Retention Policy - Here you are able to specify the retention policy for your backup plan. **“Use default”** if a custom retention plan is not needed.

Create backup plan

Backup plan: Retention Policy

Specify retention policy for backup files

Use default
Use default **options** specified for the whole product

Specify custom retention policy for backup plan


Delete versions older than
1 day from modified date

Always keep the last version

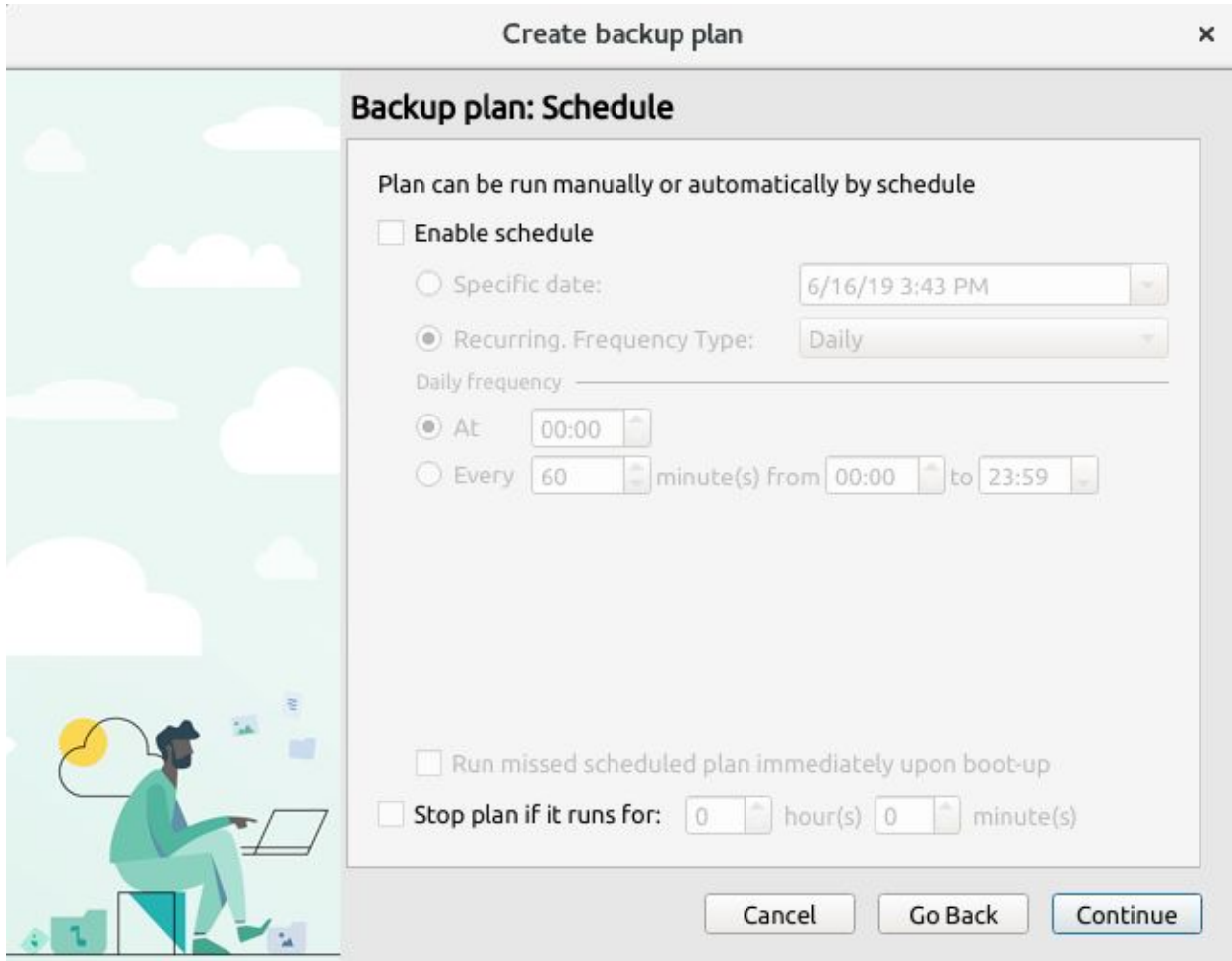
Keep number of versions (for each file)
Keep number of versions: 3

Delete files that have been deleted locally
Delete after: 30 days

Cancel Go Back Continue



6. Backup plan: Schedule - Here you can choose a custom schedule of when Cloudsafe will automatically create a backup of your files. If no schedule is set the backup will need to be run manually.



7. Backup plan: Pre/Post Actions - Here you can specify what actions (if any) to take before and after backup.

Create backup plan ✕

Backup plan: Pre / Post Actions

Specify commands you want to be executed before and/or after the backup completes

Pre-backup action

...

Exit backup plan if pre-backup action failed

Continue backup plan if pre-backup action failed


Post-backup action

...

Execute action only if backup has been successfully

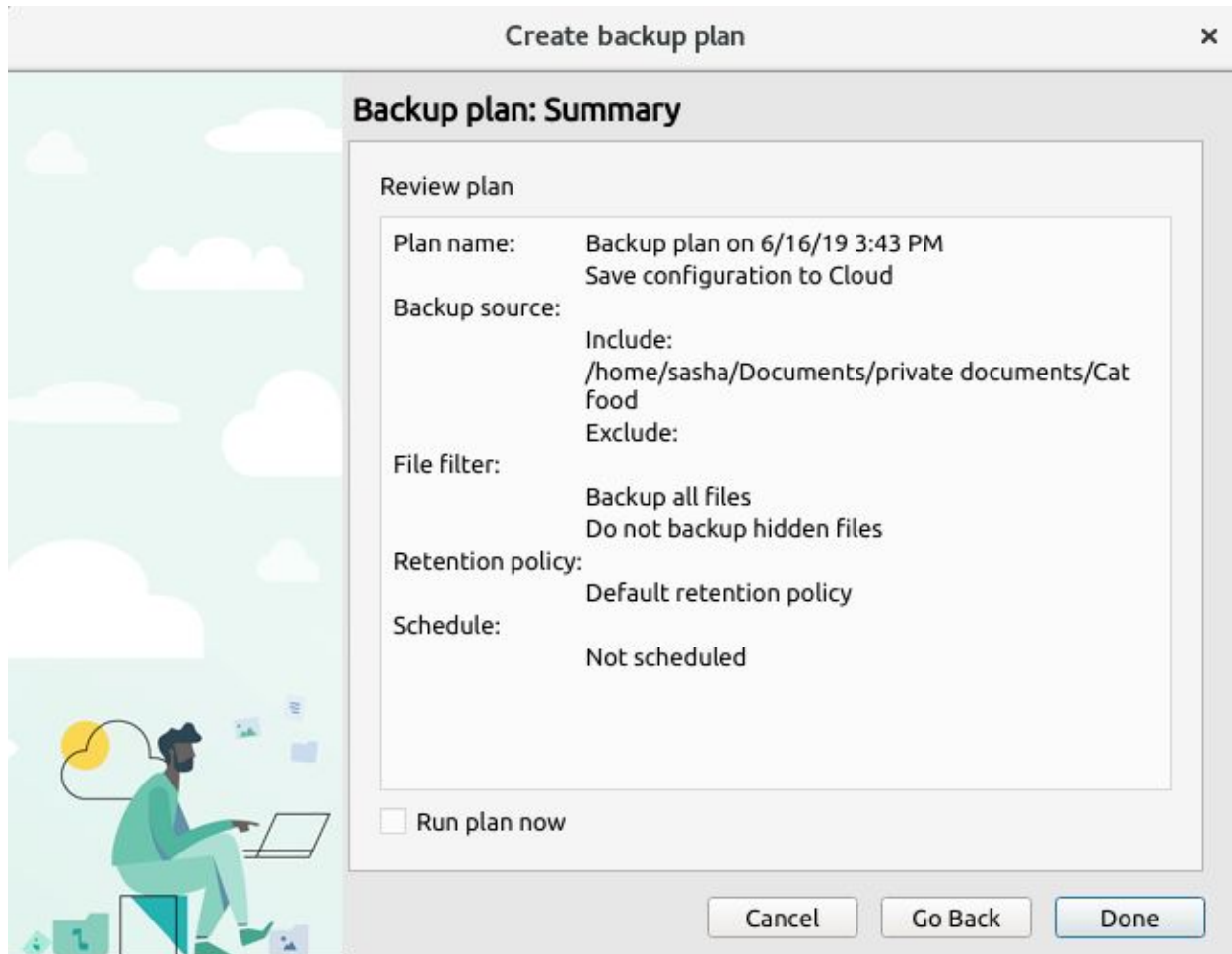
Execute action regardless of the backup result

Cancel Go Back Continue



8. Backup plan: Summary - The final step is to review a summary of your backup plan. This will include a breakdown of the configurations you selected in the previous steps. Once happy click on **Done** and the Wizard to create your backup plan will be complete.

NOTE: If you would like to run the plan immediately you can select **Run plan now** before clicking done. If **Run plan now** is not selected Cloudsafe will run the plan on the scheduled time/date that was specified previously or it will need to be run manually if no schedule was selected.



Create backup plan [X]

Backup plan: Summary

Review plan

Plan name: Backup plan on 6/16/19 3:43 PM
Save configuration to Cloud

Backup source:
Include:
/home/sasha/Documents/private documents/Cat food
Exclude:

File filter:
Backup all files
Do not backup hidden files

Retention policy:
Default retention policy

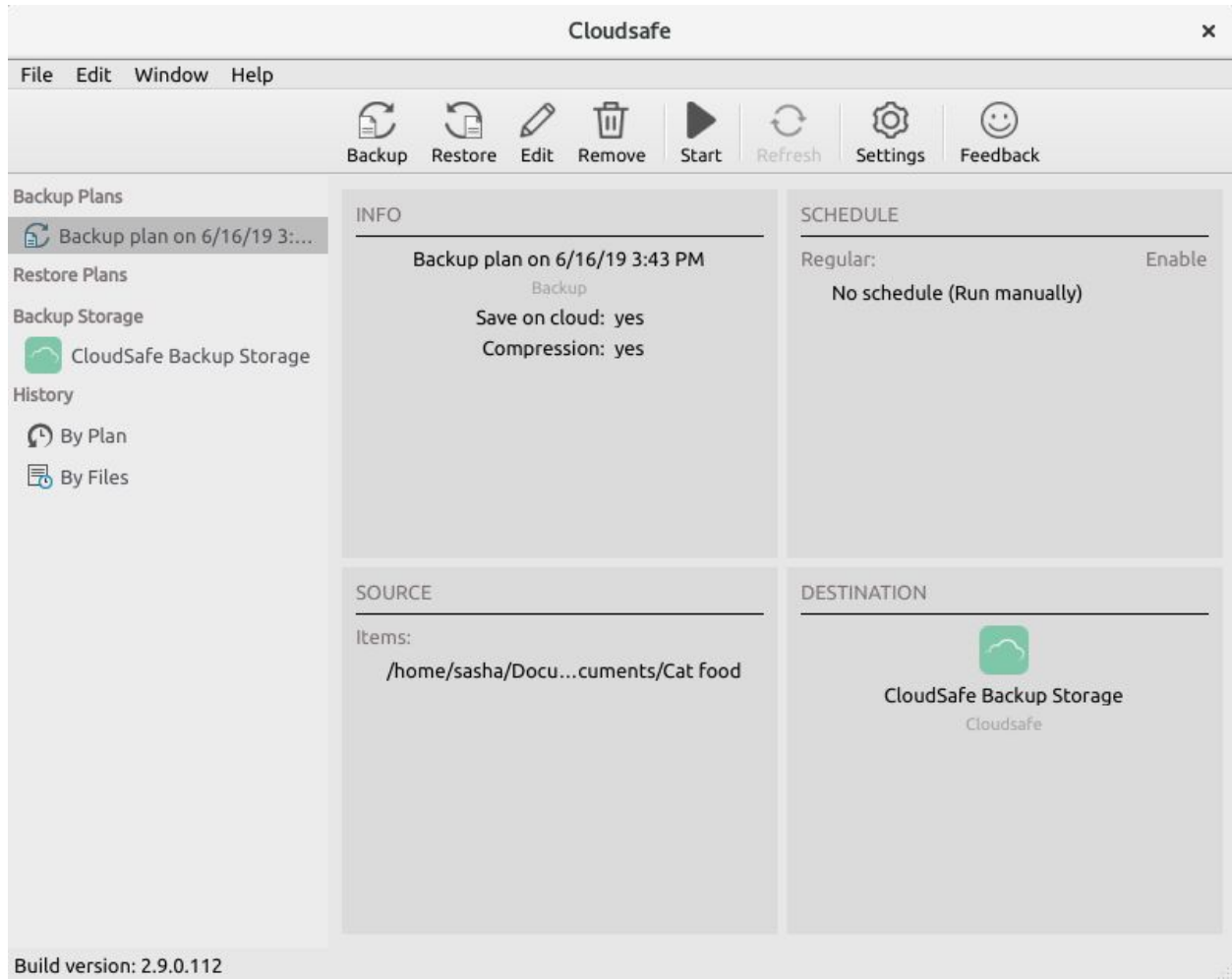
Schedule:
Not scheduled

Run plan now

Cancel Go Back Done

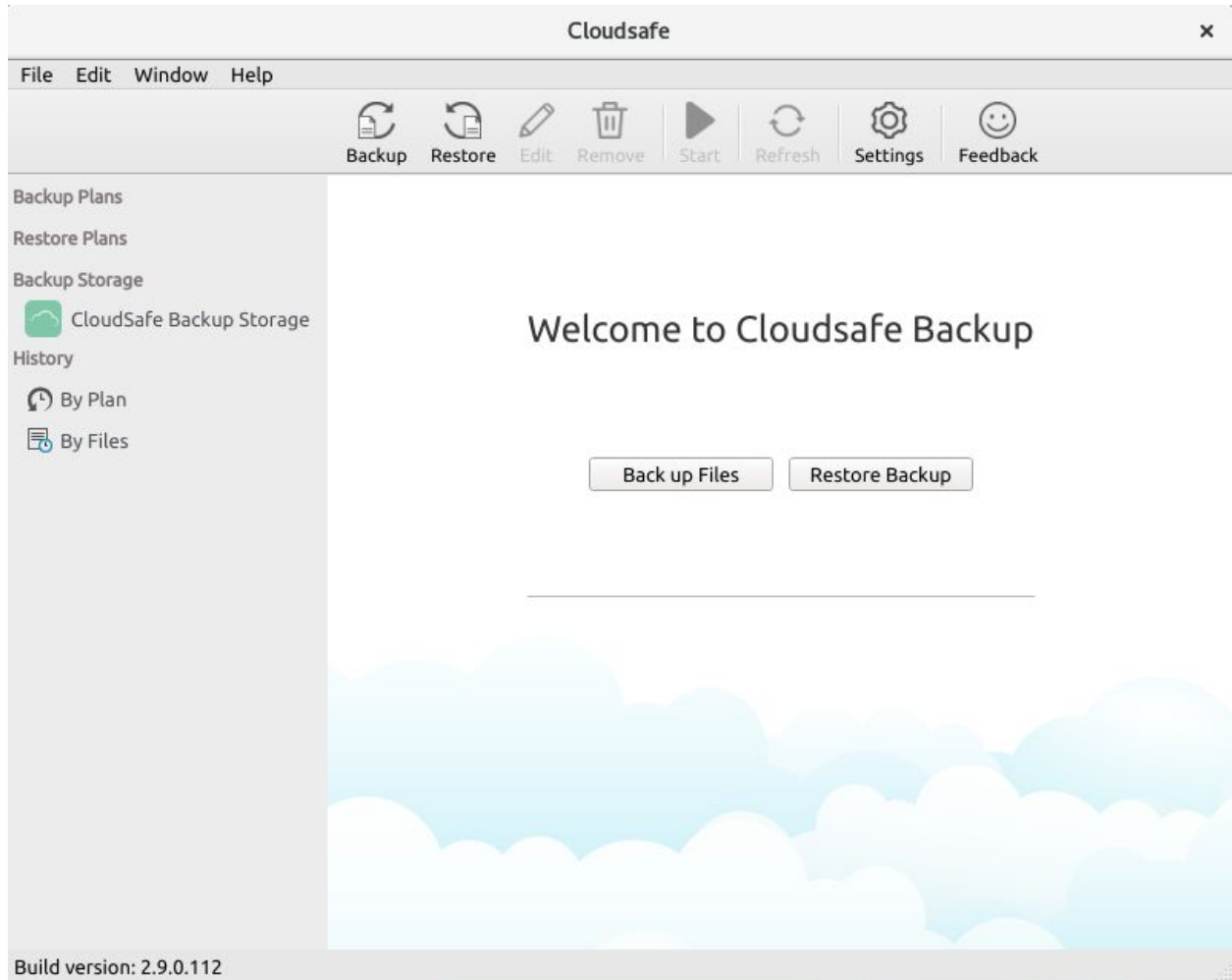
9. The backup plan you have just created will now be visible under “**Backup Plans**” on the left. Click on the backup plan name to see more details.

NOTE: If you would like to run the backup plan manually at any stage this can be done by clicking on “**Start**”.



How to Create a Restore Plan

1. Click **"Restore Backup"** or the **"AntiClockwise Arrow"** on the toolbar to get started.



2. Restore plan: Plan name - Next select whether you would like to run this restore plan just once or name and save it for future running or scheduling.

NOTE: If you choose to save a restore plan you will be prompted in a following step to schedule the restore plan.

Create restore plan ✕

Restore plan: Plan name

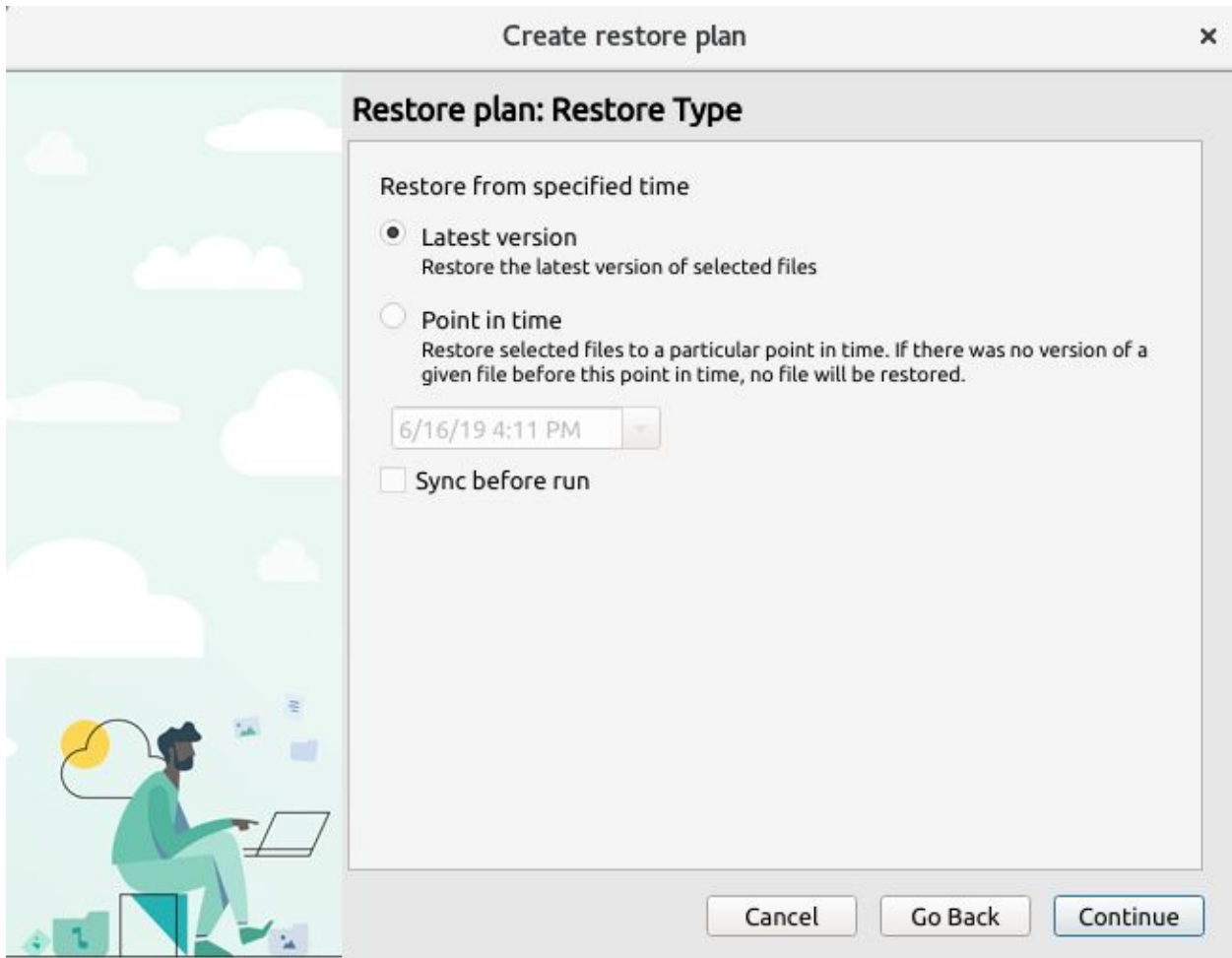
Specify plan name

- Run restore once
Run restore only once when press Finish button on the last wizard step. No schedule option is available
- Save restore plan
Save restore plan options for further running or scheduled restore

Plan name:

Cancel Go Back Continue

3. Restore plan: Restore Type - The next step will allow you to specify which backup version of your data you would like to restore. "**Sync before run**" will ensure Cloudsafe has the latest version of your backed up data (Optional).



Restore plan: Restore Type

Restore from specified time

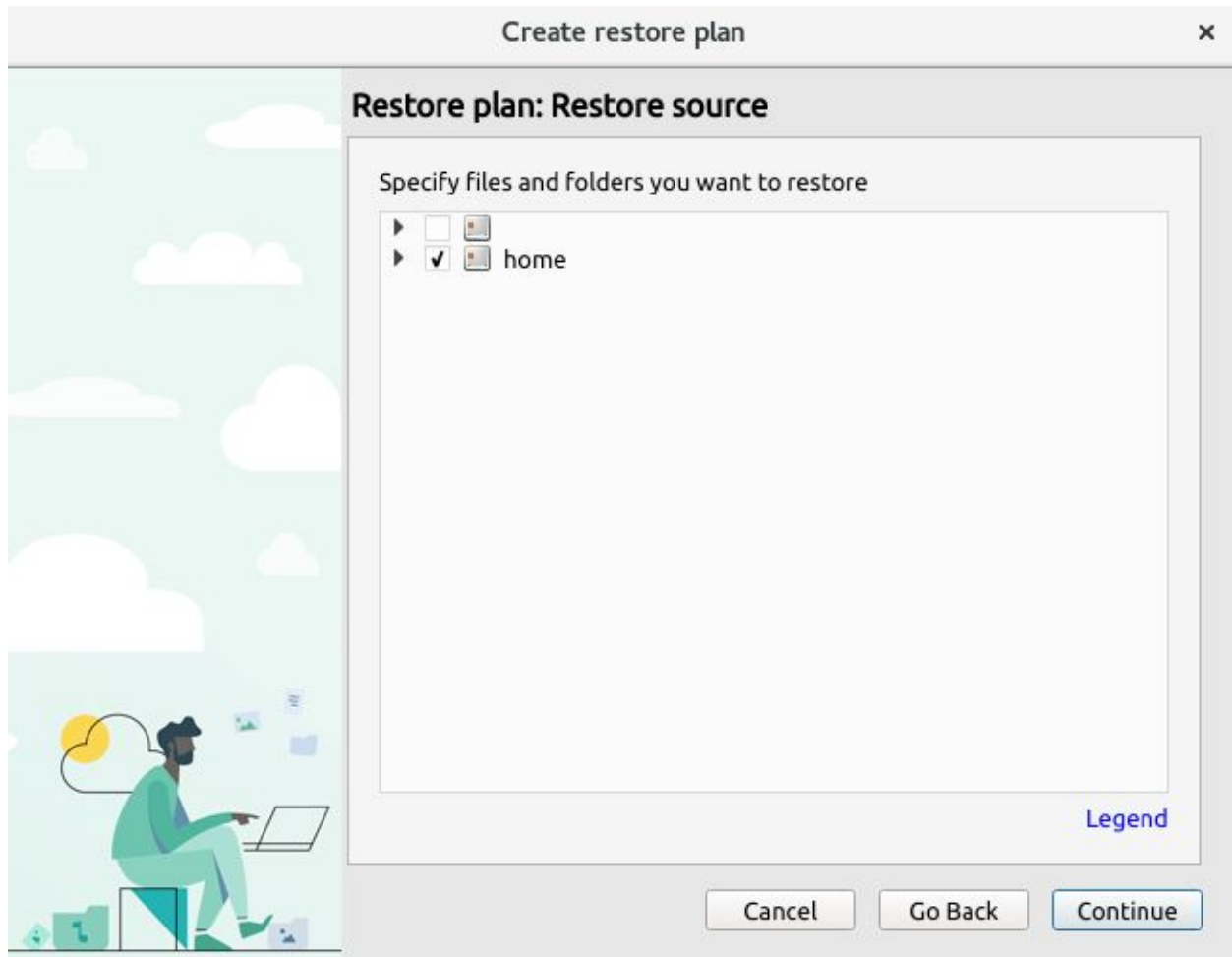
- Latest version
Restore the latest version of selected files
- Point in time
Restore selected files to a particular point in time. If there was no version of a given file before this point in time, no file will be restored.

6/16/19 4:11 PM

Sync before run

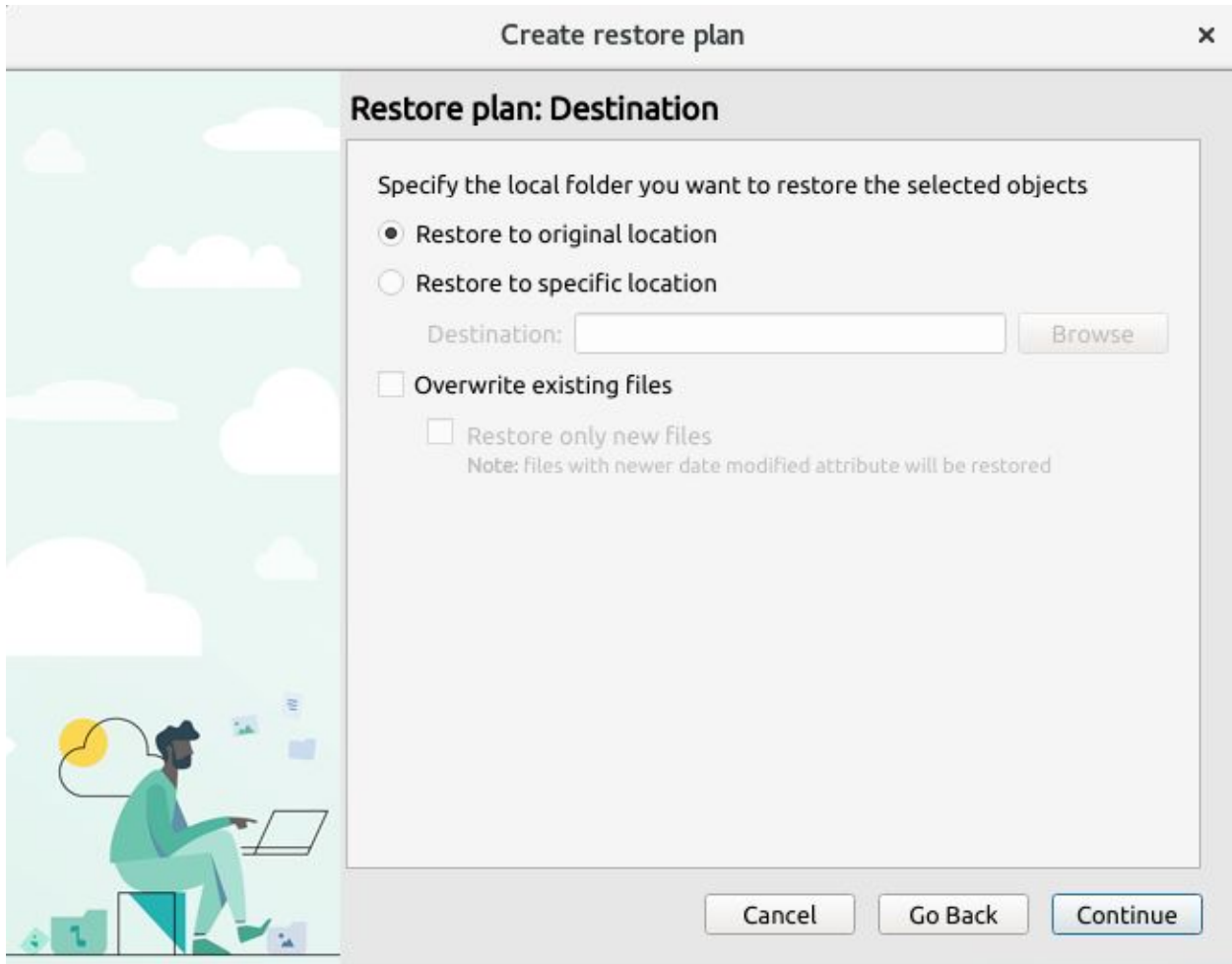
Cancel Go Back Continue

4. Restore plan: Restore source - Select the files and folders you would like to restore.

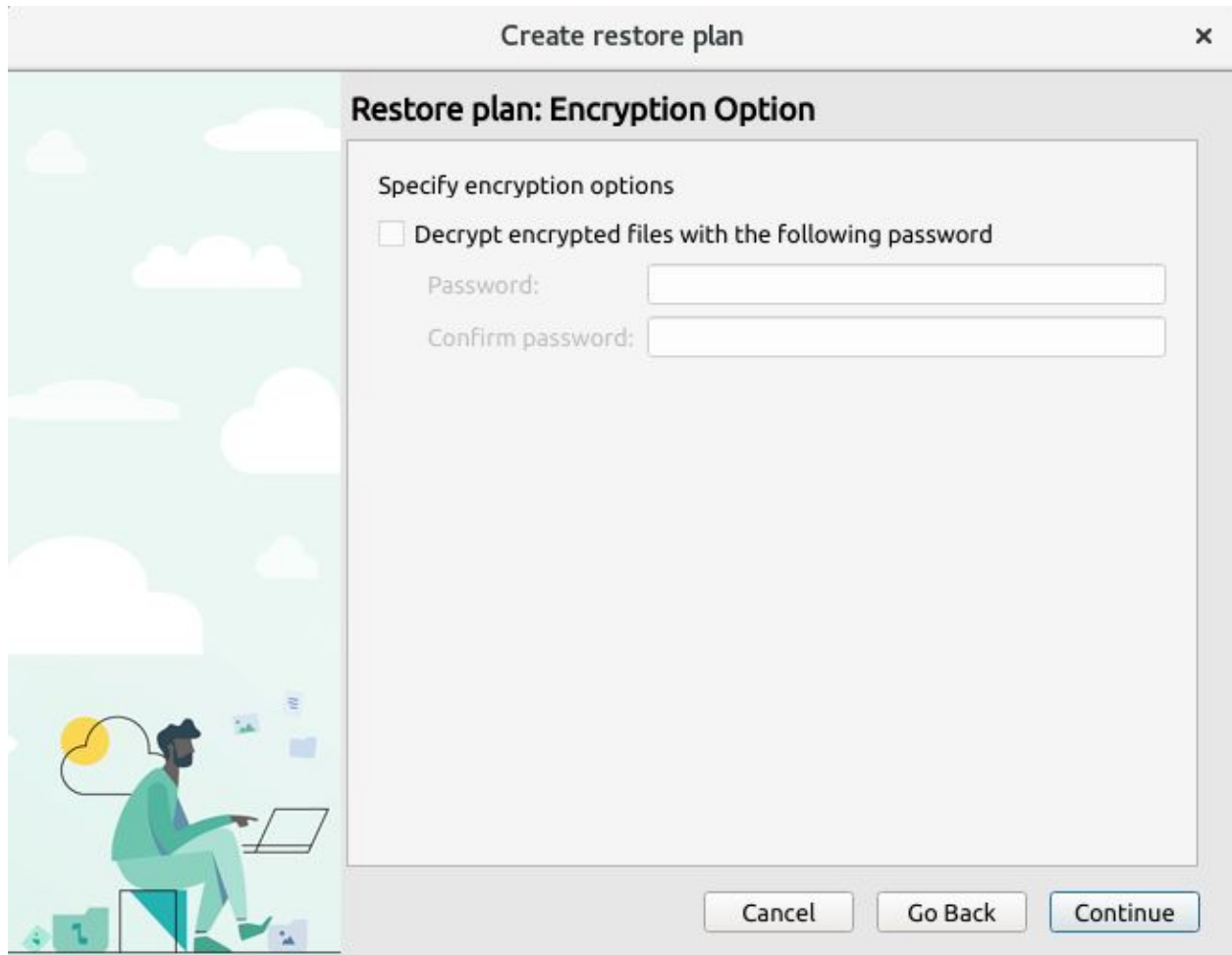


5. Restore plan: Destination - Here you are able to specify where your restored files will be placed.

NOTE: If the originally backed up files or folders still exists in the chosen destination the restore will fail unless **“Overwrite existing files”** is selected.



6. Restore plan: Encryption Option - This step will allow you to specify a password to decrypt files if you had an encrypted backup. If your backup was not encrypted you can skip this step and click continue.



Create restore plan ×

Restore plan: Encryption Option

Specify encryption options

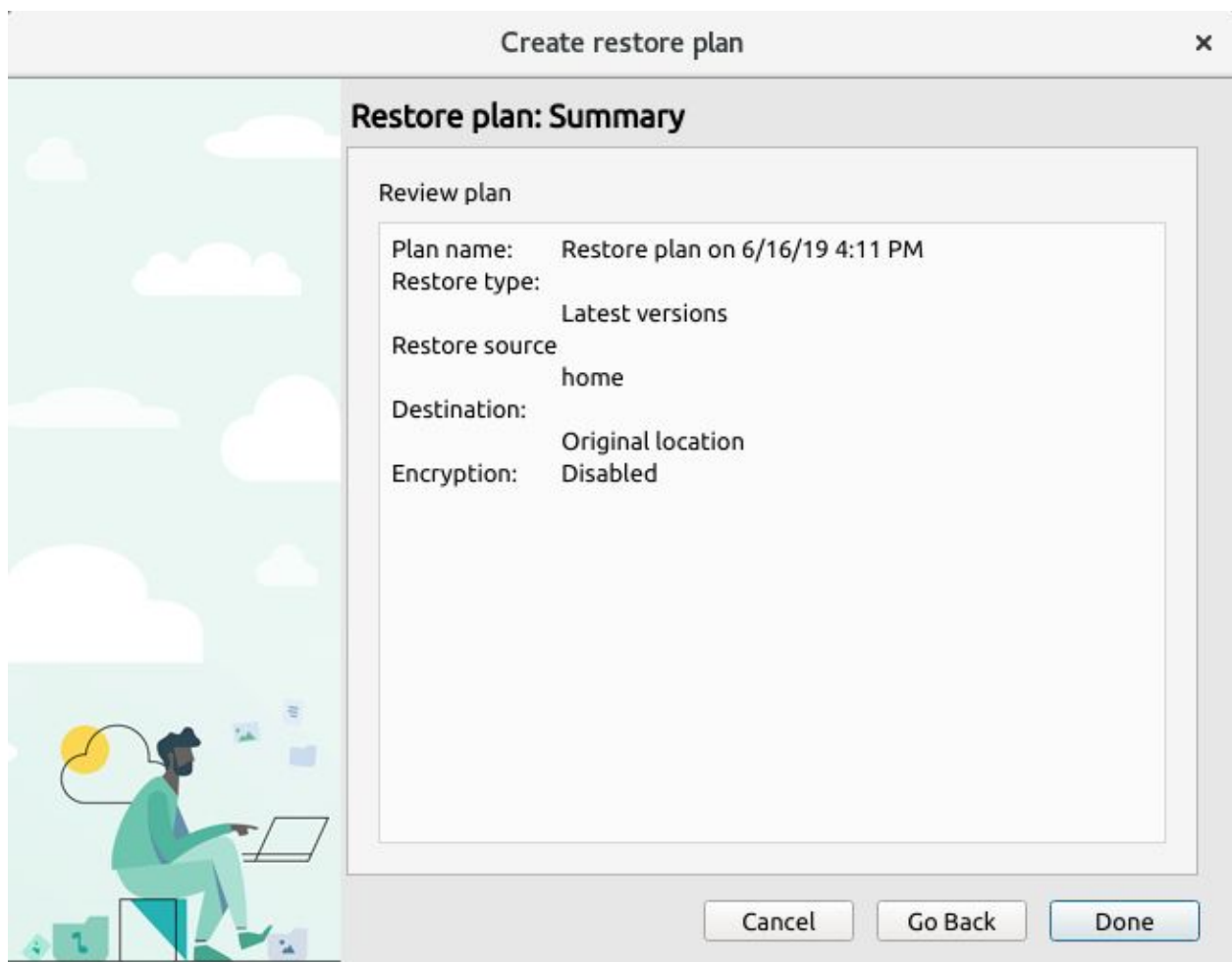
Decrypt encrypted files with the following password

Password:

Confirm password:

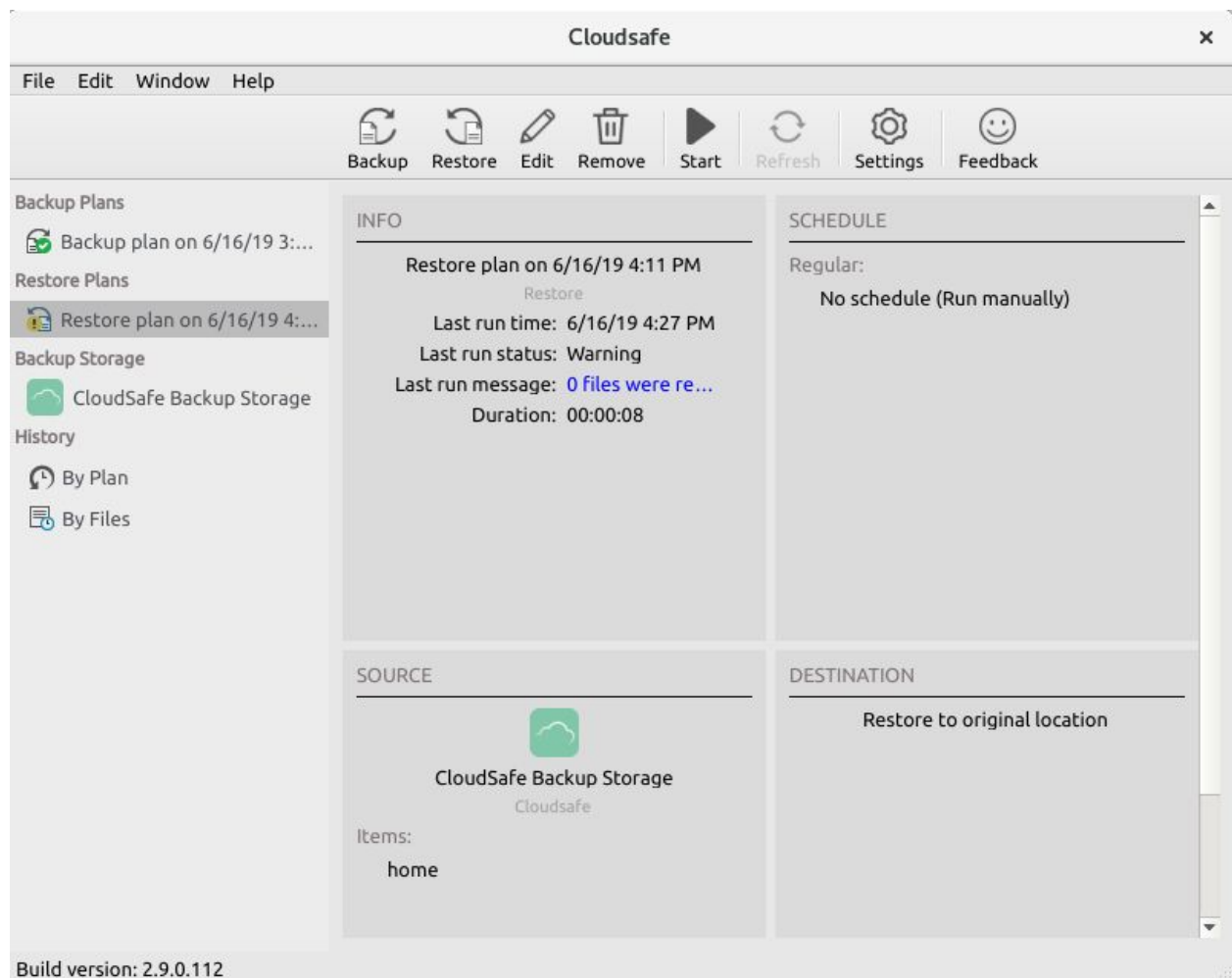
Cancel Go Back Continue

7. Restore plan: Summary - The final step is to review a summary of your restore plan. This will include a breakdown of the configurations you selected in the previous steps. Once happy click on **“Done”** and the Wizard to create your restore plan will be complete.



8. The restore plan you have just created will now be visible under “**Restore Plans**” on the left. Click on the restore plan name to see more details. If you chose to “**Run restore once**” in step 3 the restore plan will run automatically once it has been created. A scheduled plan will restore based on your defined schedule.

NOTE: If you would like to run the restore plan manually at any stage this can be done by clicking on “**Start**”.



9. Your data will now be restored once the **Restore Plan** has run.

Contact Support

Should you have any problems or issues with any of the above, please feel free to contact our support department who will be happy to help resolve the issue.

Cloudsafe Support - support@cloudsafe.me

