

# QUICK START GUIDE

Your SMiD device ensures that the information you store in the cloud remains safe, secure and private. This manual will help you get started with SMiD. Please read it thoroughly.

## BOX CONTENTS

- SMiD device
- USB power supply
- Startup key
- Ethernet cable with RJ45 connector

## SETUP

1. Insert the startup key into the SMiD USB. Connect the SMiD device to your local network using the RJ45 Ethernet cable, and then connect the SMiD to a power supply.
2. Open a browser in your PC, tablet or smartphone and enter the URL <https://smid>.
  - (A) If the SMiD main page does not open, use the SMiD finder application available from <http://smidcloud.com/software/> to find your SMiD, and then double click on it.
  - (B) LINUX USERS: install the package nss-winbind and add "wins" in the Hosts section of the file /etc/nsswitch.conf
3. A wizard will walk you through initialization. If what you want to do is restore your device from a previous SMiD, click the link that asks you if you want to do this, and you will be led through the corresponding operation.

Follow the steps indicated to configure your SMiD device. You will be asked to set an **Administrator Password**. Once your SMiD is configured, the Administration panel will appear.

## ADMINISTRATION PANEL

From the Administration panel, you can configure the following parameters:

- **Add a user account** (*Administration -> Users*).

At least one account must be assigned in order to access the SMiD network device.
- **Add a cloud storage account** (*Administration -> Storage Providers*).

At least one storage account must be configured in order to store encrypted files. You can use accounts like Dropbox, Amazon S3, DAV servers, Google Drive, or FTP.
- **Safeguard your SMiD** (*Administration -> SMiD Safeguard*).

You will be prompted by the system to perform a SMiD Safeguard right away. The operation creates a copy of SMiD's internal configuration and cryptographic keys, which are essential to restoring your SMiD in the event of an incident. Two high quality USB keys are required to perform the operation. They should be stored in a secure location, since you cannot restore your SMiD with only one of the USBs. If you want to save additional pairs of SMiD Safeguard USBs, simply repeat the process.
- **Initialize the file system**.

Once you have added a user and at least one cloud service provider account, the local file system can be initialized and opened by clicking on the icon. You will need to click in this icon each

time you start up the system to allow user's access:



## FILE MANAGEMENT

Each SMiD connected to the Local Area Network appears as a separate network storage unit, accessible through your file explorer. Your user name and password are required to access SMiD storage.

There are two folders in your SMiD: one with your username that is accessible only by you and other called SMiD\_Shared that is shared with the other SMiD users.

Every folder also contains the subfolders **\_\_SMID\_ENC** and **\_\_SMID\_DEC**, which you can use to manually encrypt or decrypt your SMiD-stored files. Simply drag and drop a file to its respective folder to perform the operation (ENC to encrypt and DEC to decrypt).

Encrypted files maintain the file name they have when unencrypted, but will have a **.smid.txt** extension.

[info@smidcloud.com](mailto:info@smidcloud.com)

[www.smidcloud.com](http://www.smidcloud.com)