SMID BUSINESS ADMINISTRATOR MANUAL

VERSION 1.3

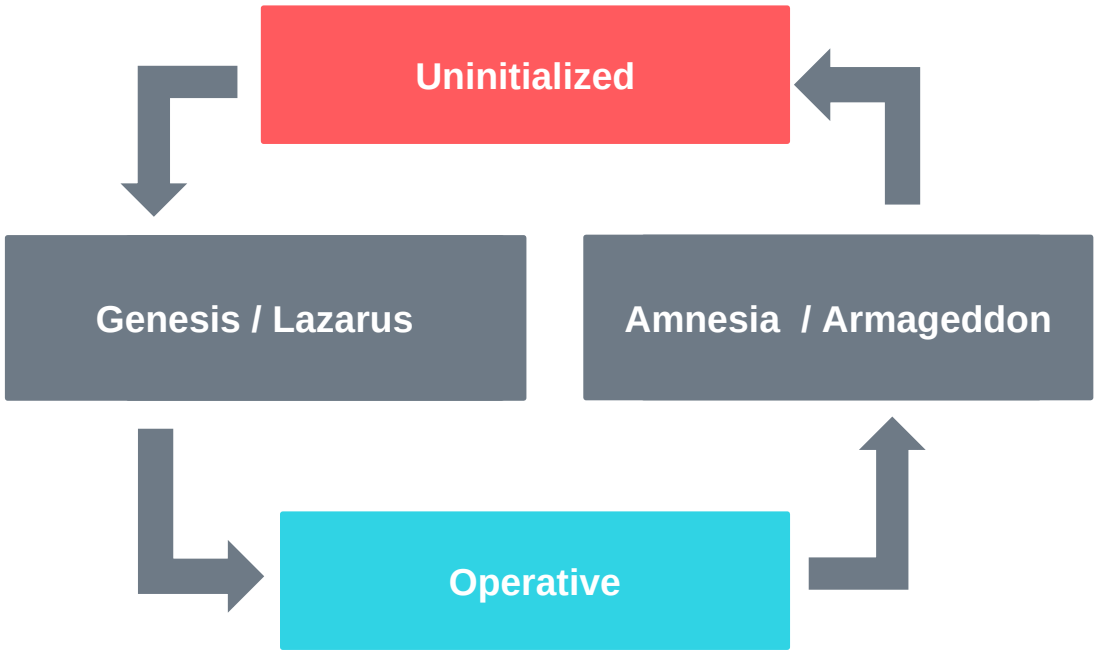
TABLE OF CONTENTS

1. Introduction

SMiD is a plug & play privacy device that allows you to keep all the information you store with external storage providers absolutely private and secure. When a SMiD device is initialized, it internally generates cryptographic keys that are totally unique to the device. This highly confidential information is only used inside the device, so only that particular SMiD device can access and use it. The keys are used to encrypt, decrypt, and authenticate your cloud-stored files.

This manual explains all operations of the SMiD Administration panels and provides you with the information you need to manage your SMiD device. SMiD can be managed from any terminal connected to the same Local Area Network (LAN) as the device.

The four main SMiD operations – Genesis, Lazarus, Amnesia, and Armageddon – follow the lifecycle of any SMiD device, from SMiD's uninitialized factory state to its operative state. SMiD Safeguard is an additional operation that creates a copy of your SMiD's internal configuration and cryptographic keys so you can restore the device in the event of an incident.



2. THE SMiD CRYPTOGRAPHIC LIFECYCLE

2.1. Genesis

This operation initiates SMiD setup and generates a set of cryptographic keys.

2.2. SMiD Safeguard

This operation creates a copy of your SMiD internal configuration and cryptographic keys. It should be performed as soon as possible.

You will need two high quality USB drives to perform a SMiD Safeguard. After the operation, the USB drives should be stored in different and secure locations, since both are required to restore your SMiD. If you want to save additional pairs of SMiD Safeguard USB drives, simply repeat the process.

2.3. Lazarus

This operation allows you to restore the configuration of a previous SMiD, using the two USB drives that contain previously safeguarded SMiD internal content.

2.4. Amnesia

This operation permanently erases your SMiD configuration as well as the entire memory of the SMiD, and leaves your SMiD-stored files encrypted in the cloud. Amnesia does not require physical access to the SMiD device and can be performed remotely.

***IMPORTANT*: Once Amnesia is performed, you will only be able to decrypt SMiD-stored files if you have previously executed SMiD Safeguard (which saves a set of your cryptographic keys in two USB drives). Without both copies, the decryption of all your encrypted files stored in the cloud is computationally impossible.**

2.5. Armageddon

This operation permanently erases your SMiD configuration as well as the entire memory of the SMiD, including all files in the cloud that are encrypted by SMiD. Armageddon does not require physical access to the SMiD device and can be performed remotely.

***IMPORTANT*: Armageddon is an irreversible action. If you perform this operation, you will erase not only the configuration of your SMiD, but the entire memory of the SMiD, including all files in the cloud that are encrypted by SMiD.**

3. System Setup: Genesis

The first time you start up a non-initialized SMiD device, a wizard will appear in your browser when you connect to SMiD.

The screen prompts you to perform Genesis, the initialization process.

The Genesis wizard initiates SMiD setup and generates a set of cryptographic keys. Click ‘Next’ to start the initialization process.

Note: To restore your SMiD to the configuration of another SMiD, click on the link that asks you if you want to do this, and you will be directed to the Lazarus wizard, which handles this process.

You will be prompted to type a password for the Administrator account. This password must contain at least 8 characters and a combination of lowercase and uppercase letters, numbers and/or symbols. Once you have selected your password and typed it into the field, click ‘Finish’ to go to the next screen.

4. Web Administration

4.1. Setup

The first time you open the Web Administration, a small wizard will take you through the 3 steps necessary to set up your SMiD device:

1. Add a cloud storage provider account (Dropbox, Amazon S3, WebDAV, FTP, etc.).
2. Add at least one user account so SMiD can be accessed as a network storage service.
3. Perform the **SMiD Safeguard** process if you want to ensure you are prepared to restore your SMiD if necessary.

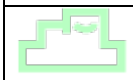
4.2. Top Navigation Bar

There are several useful items in the top navigation bar, which is accessible from every screen.

4.2.1. System Status Icon

In the top navigation bar there is an icon that shows the general state of the SMiD system.

Possible system states, as indicated by the system status icon:

	Status init	Default value during the setup.
	Status clean	The system is clean. There is no file in either SMiD or in the cloud.
	Status ok	The system is protected. If there are files on the SMiD device, all of them are safely encrypted.
	Status warning	There are files in clear text form stored on the SMiD device. It is normal to see this icon, since it appears when users are working in files that are stored on the SMiD.
	Status fail	SMiD detects an error. This icon may appear for an instant and then disappear. If it disappears, SMiD no longer detects an error, but if the icon remains, contact SMiD technical support at support@smidcloud.com or visit: https://forum.smidcloud.com/.
	Status stop	A shutdown or reboot is in process. All administrative functions have been disabled.

4.2.2. The Local Area Network Access Icon

Also in the top navigation bar there is an icon that indicates whether or not the SMiD device is reachable from the LAN.

Not accessible. The SMiD device is not LAN accessible. This is always the default state after a SMiD boot. To make the device LAN accessible, switch the icon to green by clicking it. You will

be prompted to enter your administration password.

Accessible. The SMiD device is LAN accessible. Any user with a valid account for the device can access it. To disable access, switch the LAN access icon to red by clicking it.

4.2.3. Enable/disable Help functionality

To make the administration panel as easy to use as possible, Help tooltips appear by default, The Help functionality can be switched on or off at any time by clicking the question mark icon that appears in the top menu bar.

4.2.4. Admin user

From the Admin icon at the far right-hand side of the top navigation bar, you can change the account password, shut down or reboot the SMiD device, or log out. When you click on the Admin icon, a pop-up menu displays the following options:

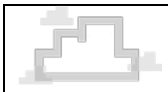
1. Change account password
2. Power: Shutdown or Reboot
3. Log out

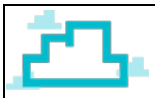
4.3. Dashboard

The dashboard presents four system information panels.

4.3.1. System Status

This is a detailed version of the system status icon that appears in the top navigation bar. The icons differ just a bit, but represent the same set of system conditions as described above under System status icon.

	Status init	Default value during the setup.

	Status clean	The system is clean. There is no file in either SMiD or in the cloud.
	Status ok	The system is protected. If there are files on the SMiD device, all of them are safely encrypted.
	Status warning	There are files in clear text form stored on the SMiD device. It is normal to see this icon, since it appears when users are working in files that are stored on the SMiD.
	Status fail	SMiD detects an error. This icon may appear for an instant and then disappear. If it disappears, SMiD no longer detects an error, but if the icon remains, contact SMiD technical support at support@smidcloud.com or visit: https://forum.smidcloud.com/.
	Status stop	A shutdown or reboot is in process. All administrative functions have been disabled.

4.3.2. Resource Monitor

This panel graphically represents network, CPU, RAM, and disk usage, as well as the internal storage space used

4.3.3. Current Connections

A list of all users currently connected to the SMiD device

4.3.4. Recent Logs

Displays the last five log registers during the past 24 hours

4.4. STATISTICS

From Statistics, you can view SMiD activity graphically. You can select Current Statistics or Historical Statistics from the left menu.

4.4.1. Current Statistics

Cache

The Cache tab shows the evolution in real time of the number of files in each cache, or designated area. There are three SMiD caches:

1. The red cache is a designated area in SMiD that stores unencrypted files
2. The black cache is a designated area in SMiD that stores encrypted files
3. The blue cache contains your cloud storage accounts

Resources

The Resources tab of Current statistics shows network, CPU, RAM, and disk usage. If you see that the CPU, RAM or disk usage are running too high, you may want to stop uploading files until the system has stabilized.

4.4.2. Historical statistics

This section shows you the evolution of the number of files during different time periods.

4.5. ADMINISTRATION

In the Administration section accessible from the top navigation bar you can configure the settings of your SMiD device. Use the left menu bar to navigate.

4.5.1. System

From the System tab you can view and modify the name of your SMiD device. If you change the name, you must type the new name into the browser address bar after restarting your SMiD. Please take into account that some routers take time to register a name change, so you might need to access your SMiD through the assigned IP address until your router recognizes it. If you do not know the IP address, you can use SMiD tools[1] to locate it.

In the System area of the Administration section, you can also check to see if a SMiD update is available and view a log of the SMiD safeguard processes performed since system initialization (Genesis).

1 http://smidcloud.com/software/ Versions for Windows, MacOS, Linux and Android.

We recommend performing at least one SMiD Safeguard so you are fully prepared for a system restore.

To edit a field, click the pencil icon. 

Once the selected field has been edited, click the green check mark icon to update the system. 

4.5.2. Network

From the Network tab you can change the configuration of the network adapter, the proxy and the NTP servers.

4.5.3. Users

From the Users tab you can add and delete users. Users have access to the SMiD device and have their own file storage folder. Users can change their passwords by accessing the web using their existing credentials. To add a new user, click *Add new user*, assign a username and password, and click *Register user*. User passwords must be at least eight characters long.

You can limit the number of users you want to see when viewing your list of users, by selecting from the dropdown at the top right-hand side of the screen. The same is true anywhere a log of multiple entries appears, including when you are viewing your list of cloud providers, files in the trash bin, etc.

4.5.4. Current connections

From the Current connections tab, you can view users connected to the SMiD device. To see who is connected in real time, click the *Real time* button.

4.5.5. Providers

You can manage your providers from the Providers tab. Before adding your first

provider account, you will need to specify a folder name. A folder with this name will be generated for each provider you add. For example, if you name this folder “SMiD,” then a folder named “SMiD” will appear within each cloud provider you add, and all files encrypted by your SMiD device will be stored inside the folder “SMiD”.

Once a provider has been added, the storage space used and number of files stored will be visible. An icon appears next to a provider’s logo if the provider is out of service.

The first provider account you add is considered the Master Account by default. An star icon appears next to the Master Account provider’s logo. An encrypted backup of your system configuration is periodically stored in the Master Account. When you have two or more provider accounts, you will be able to select which account you want to be the Master Account.

4.5.6. Advanced Settings

From the Advanced Settings tab of the Administration section, you can change the configuration of timers or change the SSL digital identity of your SMiD device.

Timers

SMiD uses three timers:

Clear text file timer: Defines the amount of time a file stays in clear text format in the SMiD file system. Once the time limit is up, the file is automatically encrypted and queued to be uploaded into the cloud, and the clear text form is deleted.

Encrypted file timer: Defines how long an encrypted file copy is stored in the SMiD device. When the time limit up, the local encrypted copy is deleted.

Trash timer: Defines how long a file that has been deleted from the SMiD file system will remain in the trash bin before it is permanently deleted.

SSL Identity

If you have your own Certificate Authority, you can change the SSL digital identity of your SMiD. You can do this two ways:

- Upload a PEM file that contains both the private key and the certificate.
- Request a CSR, sign it with your CA, and upload the PEM file with the signed certificate.

The PEM file cannot be password-protected and must contain only one certificate and one private key.

Since these are critical elements of the security configuration, we recommend you not to change these options unless you are an expert user.

Crypto Operations

From the Crypto Operations tab you have access to three operations. A wizard walks you through each one:

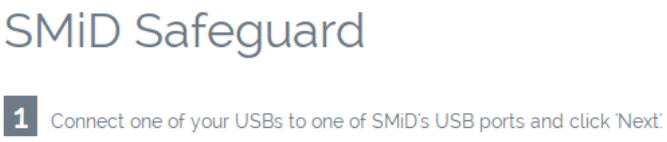
SMiD Safeguard

Amnesia

Armageddon

- ***SMiD Safeguard***

This operation generates a copy of your SMiD internal configuration and cryptographic keys that you can use to restore your SMiD in the event of an incident. You will need two high quality USB drives to perform the SMiD Safeguard.
The USB drives should be stored in different and secure locations, since you cannot restore your SMiD with only one of the USB drives. If you want to save additional pairs of SMiD Safeguard USB drives, simply repeat the process.



Disconnect this USB drive and connect the other USB drive to the SMiD device and click *Next* to finalize the backup process.

- ***Amnesia***

This operation permanently erases your SMiD configuration and leaves your SMiD-stored files encrypted in the cloud. **Once the wizard finalizes Amnesia, you will only be able to decrypt SMiD-stored files if you have previously executed SMiD Safeguard (which saves a set of your SMiD internal configuration and cryptographic keys to a USB drive) and perform the Lazarus operation. If Amnesia is not performed exactly as indicated in the wizard, you will not be able to decrypt any of your cloud-stored files.**

When prompted, enter the administrator password and click *Next* to launch the Amnesia process.

Allow the wizard to completely finalize the operation. SMiD will reboot automatically. If after 4 minutes the page has not refreshed, use SMiD Tools[2]. It is possible that your device has changed its IP address. Remember that when you perform Amnesia, any new name you have used for your SMiD is erased, so the device name will simply be “SMiD”.

- ***Armageddon***

This operation permanently erases your SMiD configuration as well as the entire memory of the SMiD, including all files in the cloud that are encrypted by SMiD. If there is a large number of files stored, the process may take time.

Armageddon is an irreversible action. If you perform this operation, you will erase not only the configuration of your SMiD, but the entire memory of the SMiD, including all files in the cloud that are encrypted by SMiD.

When prompted, enter the administrator password and click *Next* to launch Armageddon.

Allow the wizard to completely finalize the process, remember that it may take time if there is a large number of files stored in the SMiD device. SMiD will reboot automatically. If after 4 minutes the page is not refreshed, use SMiD Tools[2]. It may be that your device has changed its IP address. Remember that when you perform Armageddon, any new name you have used for your SMiD is erased, so the device name will simply be “SMiD.”

[2] http://smidcloud.com/software/

Trash

The Trash tab provides a list of all files deleted from SMiD. You can either retrieve files here or erase them permanently. Restored files are returned to their original locations.

Log

From the Log tab you can read all log messages generated during SMiD operation. Filters allow you to view them by level of importance (Info, Warning, Error or Critical).

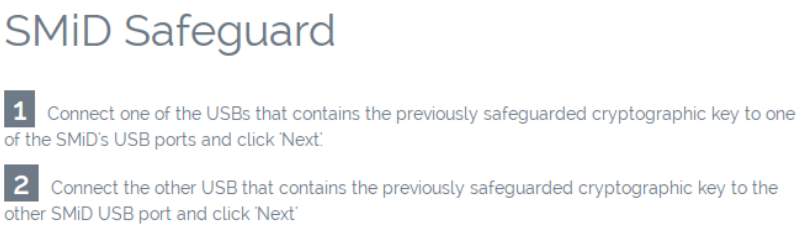
5. SYSTEM RESTORE: LAZARUS

This operation allows you to restore the configuration of a previous SMiD, using the two USB drives that contain previously safeguarded SMiD keys and configuration.

When you start up a non-initialized SMiD device, a wizard will appear in your browser when you connect to SMiD. To restore your SMiD to the configuration of another SMiD, click on the link that asks you if you want to do this, and you will be directed to the Lazarus wizard, which handles this process.

Follow the steps in the wizard to perform Lazarus.

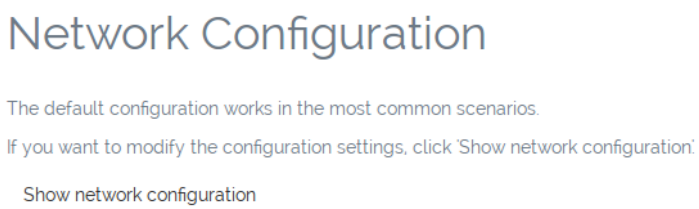
Connect one of the two USB drives and click ***Next***.



Connect the other USB drive and click ***Next***.

Select a password for the administrator and click ***Next***.

Your SMiD device must be connected to the Internet in order to perform Lazarus. If you need to change the configuration of your network adapter, click ***Show Network Configuration*** and modify the configuration to connect your device to the Internet.



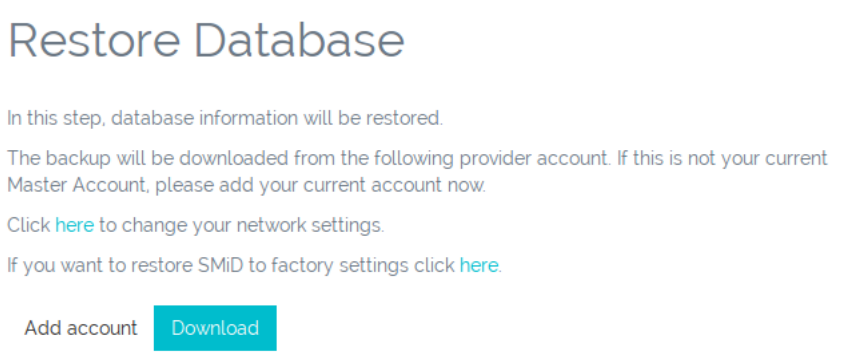
Note: If you change the network configuration, the device will reboot. Once the device is restarted, enter your administrator credentials and continue with the process.

To finalize Lazarus, you must be sure that your device is connected to the Internet and that the current provider Master Account matches the Master Account used during the last system backup, since the system will reconstruct your SMiD using the database from the original Master Account selected.

If you have not changed your Master Account, simply click Download, then Next and the system will restore your device correctly.

If you have changed your Master Account, however, you will need to inform the system of this change so that it performs the Lazarus operation correctly. To do this, click Add Account, and indicate the account that is your current Master Account and click Download. Check the date displayed to be sure the selected database is the most current, and then click Next, to finalize the process.

If you no longer have access to the Master Account you used when performing your SMiD Safeguard, you will not be able to fully restore SMiD.



Once the operation is complete, reboot SMiD. If after 4 minutes the page is not refreshed, use SMiD Tools, as your device may have changed its IP address during the process.