SALVADOR
TECHNOLOGIES

CYBER RECOVERY UNIT

CRU-V2B

USER MANUAL

TABLE OF CONTENTS

1 | INTRODUCTION

1.1 Cyber Recovery Unit (CRU)

The backup & recovery unit consists of 3 NVMe disks with the following names:

NVMe-Current

NVMe-Previous

NVMe-Factory Reset

During the initial installation, you will be required to perform an initial configuration of the software and the hardware. Afterwards, the backups will be performed automatically according to the predetermined backup schedule and frequency (daily / 2 days / weekly).

1.2 The Backup Software Agent

The software performs the following tasks:

1. Scheduled backups according to the selected backup frequency.
2. Continuous monitoring of the backup data, including the autonomous ejection of the Salvador disk in case of a cyber-attack to.
3. Direct link to the software agent: https://support.salvadortech.com/Resources SalvadorBackupRecoveryLastVersion.zip

1.3 The Centralized Management System

The cloud-based centralized monitoring system provides remote real-time status of each of the backup devices. The system can be installed on premise (deployed as a virtual machine), or you can use the cloud-based version (https://support.salvador-tech.com/).

During the initial installation, you will be required to create a site administrator user account, and then you will be able to add devices by using their serial numbers (SN). The SNs are located on the backward of the hardware.

1.4 Scheduled Backups Algorithm

During each moment, just one of the backup disks is physically connected to the computer and receives electrical voltage; the other 2 disks are in a full air-gapped mode (not receiving electrical voltage).

During the initial installation, the first backup copy will be transferred to the NVMe-Factory Reset disk. After 24 hours of that transfer, this disk will be in an always air-gapped state, as it is the factory reset/ baseline version of the system.

The NVMe-Current and NVMe-Previous disks will be constantly updated by the software agent according to the selected frequency. For example, if you selected the daily backup frequency and installed the software on Monday, the following backups will be created during the first week:

- **Monday:** NVMe-Factory Reset will be created
- **Tuesday:** NVMe-Current will be created
- **Wednesday:** NVMe-Previous will be created
- **Thursday:** NVMe-Current will be updated
- **Friday:** NVMe-Previous will be updated
- **Saturday:** NVMe-Current will be updated
- **Monday:** NVMe-Previous will be updated

If you select the weekly frequency, the backup schedule will be similar to the previous example. During the initial installation, the NVMe-Factory Reset will be created. On week 1, the NVMe-Current will be created; on week 2, the NVMe-Previous will be created; on week 3, NVMe-Current will be updated, and it will continue according to the predetermined weekly frequency.

2 | SOFTWARE INSTALLATION

2.1 Minimal Requirements

- USB 2.0/3.0/3.1 hardware port
- Windows OS
  - Windows Server 2012/2016/2019/2022
  - Windows 7/8/10/11
  - BitLocker encryption disabled
- Capacity: Up to 2TB (depends on the capacity CRU hardware, there are 3 versions: 512GB/1TB/2TB).
- .NET 4.8

2.2 Prior to the Setup

1. Make sure that your computer/server is able to boot from a USB drive by properly configuring UEFI/BIOS (Enable boot from USB, disable secure boot).
2. If the USB ports are disabled the Antivirus/ DLP software, please add an exclusion for CRU hardware.
3. Make sure your internal hard drive (the disk you wish to backup) is not encrypted by Bitlokcer (otherwise decrypt it).

2.3 Installation

- Connect the CRU unit to the computer using the supplied USB cable.
- Use the installation file located in the device driver or download the installation file from our portal: https://support.salvador-tech.com/

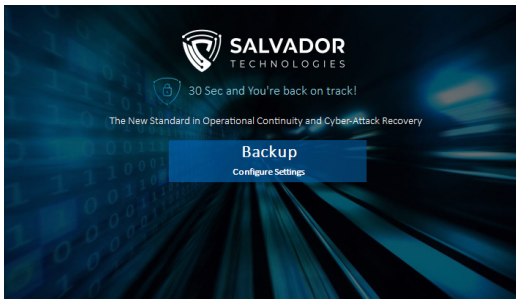
  Note: *If this is your first usage of the "centralized web management system", please register to create a company's administrator user.*

  Direct link for the software agent: https://support.salvadortech.com/Resources/SalvadorBackupRecover yLastVersion.zip
- Install the software agent.

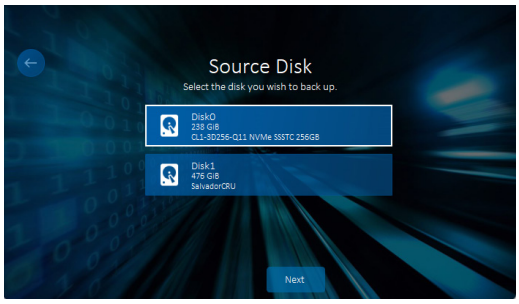
  Note: *Make sure your power settings so the computer will not enter into "sleep" mode during backup*
- You can follow the nominal operation of the backup software by using the statistics in the software home screen or using the log file BackupLog.txt located in the installation folder.

3 | CONFIGURE BACKUP SCHEDULE

1. Run the software again after restart.
   The main screen appears.

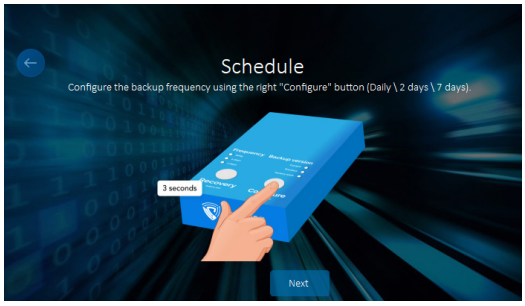


2. Click the Backup button.
3. Select the source disk, which is the disk you wish to backup, usually Disk0.

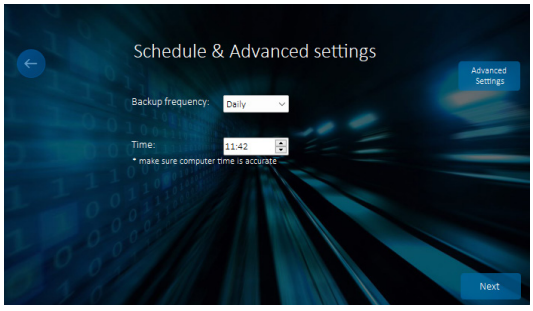


4. Click the Next button.
5. Press and hold both buttons of the CRU for 5 seconds. The “Current” LED will flicker on the CRU device.

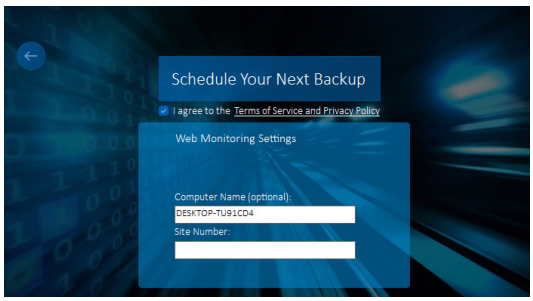
6. Click the Next button.
7. Skip this section if you would like to configure daily backup frequency. Otherwise Configure the backup frequency by pressing the “Configure” button on the CRU device (hold for 3 seconds). The corresponding LED will flicker: Daily / 2 days / Weekly (you must hold the button for at least 3 seconds)



8. Select the same backup frequency in the software (according to the selection in previous section)



9. Click the “Next” button.
10. Read and agree to the Terms of Service and Privacy Policy.



Skip this if you are not using the “centralized web monitoring system”

11. In order to use it, usage of the centralized web management system (not mandatory), in order to use the system you can register using cloud version https://support.salvador-tech.com. The web management can be installed on-prem using the instructions in chapter 8 (On-Prem Web Management Monitoring Installation)
12. After a successful registration, you will find your "site number" parameter, in the web management after successful registration:
13. Click the Schedule Your Next Backup button.
14. Install the software agent. The first backup will run immediately to create the "Factory reset" backup version.
15. After the first backup, the other backup tasks will be performed automatically according to the schedule you have just configured. (Frequency: daily / 2 days / weekly).

    The backup status will appear on the screen. When finished, the window will close automatically.

Important Notes:

- Don't close the software by the X button, as a "Factory reset" backup will not be generated. You can minimize the software and see it in the tray icons.
- Future backups will run in the background, at the scheduled time.
- Make sure that your system will not enter into sleep mode during the backup, by changing the power settings accordingly.

4 | RESTORATION OF THE COMPUTER SCHEDULE

1. In case of a cyber-attack, disconnect the LAN cable and turn off the computer.

   Note: *This is important to avoid any corruption to the air-gapped recovery disk, as it will turn online during this section.*

2. On the CRU device, press the “Recovery” button and hold the button for 5 seconds.
   The “Recovery” and “Current” LEDs will start flickering.

3. The selected disk is the “Current”. If you would like to recover from a different disk (“Previous” or the “Factory Reset”) hold the “Configure” button for 3 seconds in order to select the backup version you wish to recover from:

   - Current: the most updated backup version.
   - Previous: the latest air-gapped protected backup version.
   - Factory reset: always air-gapped backup version (generated once, during backup configuration at the previous chapter).

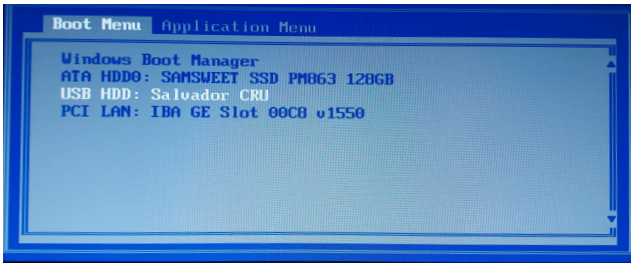
4. Turn on the computer.

5. During the computer startup, instantly press the Boot Menu key to enter UEFI/BIOS fast boot screen. Use the following table to determine the key for the “fast boot menu.”

Manufacturer	Boot Men
ACER	Esc, F12, F9
ASUS	Esc or F8
COMPAQ	Esc, F9
DELL	F12
HP	Esc, F9
INTEL	F10
LENOVO - desktop	F12, F8, F10
LENOVO - laptop	F12
SAMSUNG	F12, Esc
SONY	F11
SONY	F10
TOSHIBA	F12

6. When using old legacy systems (MBR based), you must choose in the UEFI/BIOS- booting from “legacy mode

7. Select USB device (Salvador CRU).

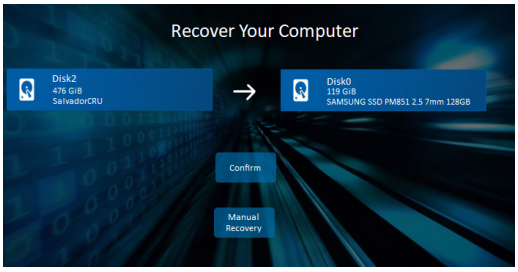


The computer will continue to operate from the selected backup version, replacing the main corrupted hard drive.
You can continue to operate in this mode as long as you need (days, weeks) before the recovery process is done. See the next section for more information.

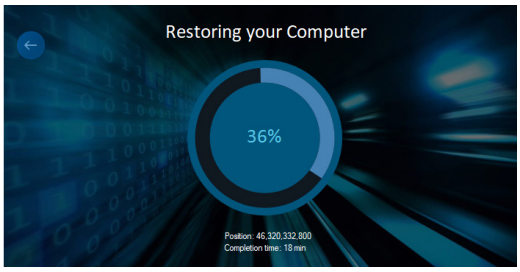
Note: *No additional backups will be performed in this case.*

5 | FULL RECOVERY OF THE DATA

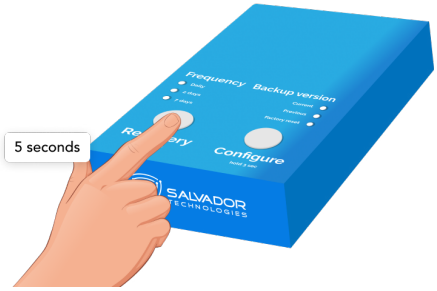
1. After booting from Salvador Technologies CRU, in order to return to nominal operation from the “main internal hard drive”, please run “Salvador Backup & Recovery” software. The recovery can be done in the background of the nominal operation The recovery screen will appear.



2. Click the Confirm button. Recovery Process will begin.



3. When finished, restart the computer and boot as usual from the main hard drive.
4. On the CRU device press the Recovery (hold for 5 seconds) button. The Recovery LED will be turned off, and you will return to a nominal backup operation.



Note: *This will keep your computer backups as scheduled.*

6 | ADDITIONAL FEATURES

To reset the internal timer of the CRU device, click and hold the “Configure” right button for 10 seconds when the device is in Backup mode.

To confirm the action, all the LEDs will light up for a few seconds.

7 | CYBER-ATTACKS MITIGATION

To prevent the reinfection of the computer after the recovery, we recommend that you temporarily disconnect the recovered computer from the network.
Connect the computer back to the network only if the following conditions are met:

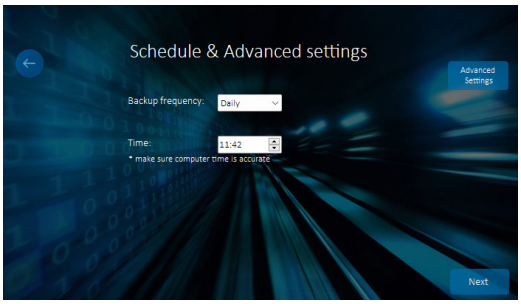
- The cyber-attack is fully isolated (infected computers are not connected to the network).
- The source of the attack was detected and blocked successfully. For example: if the attack occurred due to a Windows OS vulnerability, please fix it first.
- APT (Advanced Persistent Threat) means that the attacker stayed for a long period in your network before the execution.

To mitigate an APT cyber-attack:

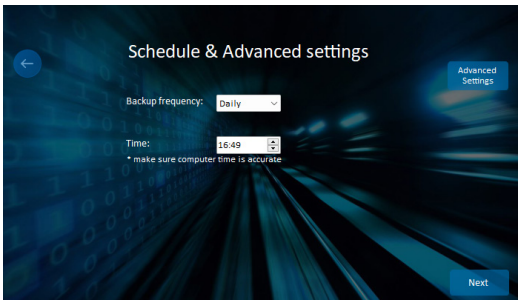
- Use the “Factory reset” version.
- Boot from the “Factory reset” version and complete a full recovery of the main hard drive (sections 4 and a full).
- After full recovery (section 4), copy the specific updated files from the “Current” or “Previous” backup versions, for example, an updated configuration file. using the instructions in Chapter 9 - “Copying specific files from Salvador backup disk” (Make sure you are not copying the APT malware file).

8 | CYBER-ATTACKS MITIGATION

1. Download the on-premise “centralized web management” VM from: https://support.salvador-tech.com/Resources/Salvador-tech.zip
2. Default admin password for the VM: **SC056AJ!**
3. Please configure static IP in the VM using the following user guide: https://linuxconfig.org/how-to-configure-static-ip-address-on-ubuntu-18-10-cosmic-cuttlefish-linux
4. Configure the software agent to use the internal VM. Use the instructions in section 3. In the following screen enter the “Advanced Settings”:



5. Select “Internal Web Management” and Enter the VM Static IP



6. Enter the web management system http://static IP address.
7. Register users who will have an access to the centralized web management under the “Register Company” tab.

9 | COPYING SPECIFIC FILES

Access to Salvador disks is blocked by default if “Salvador software agent” is installed.
In order to copy a specific file from the backup, simply connect Salvador’s hardware to another computer without performing a “Salvador software agent” installation.

SALVADOR
TECHNOLOGIES

www.salvador-tech.com

+972-73-2209-444

info@salvador-tech.com