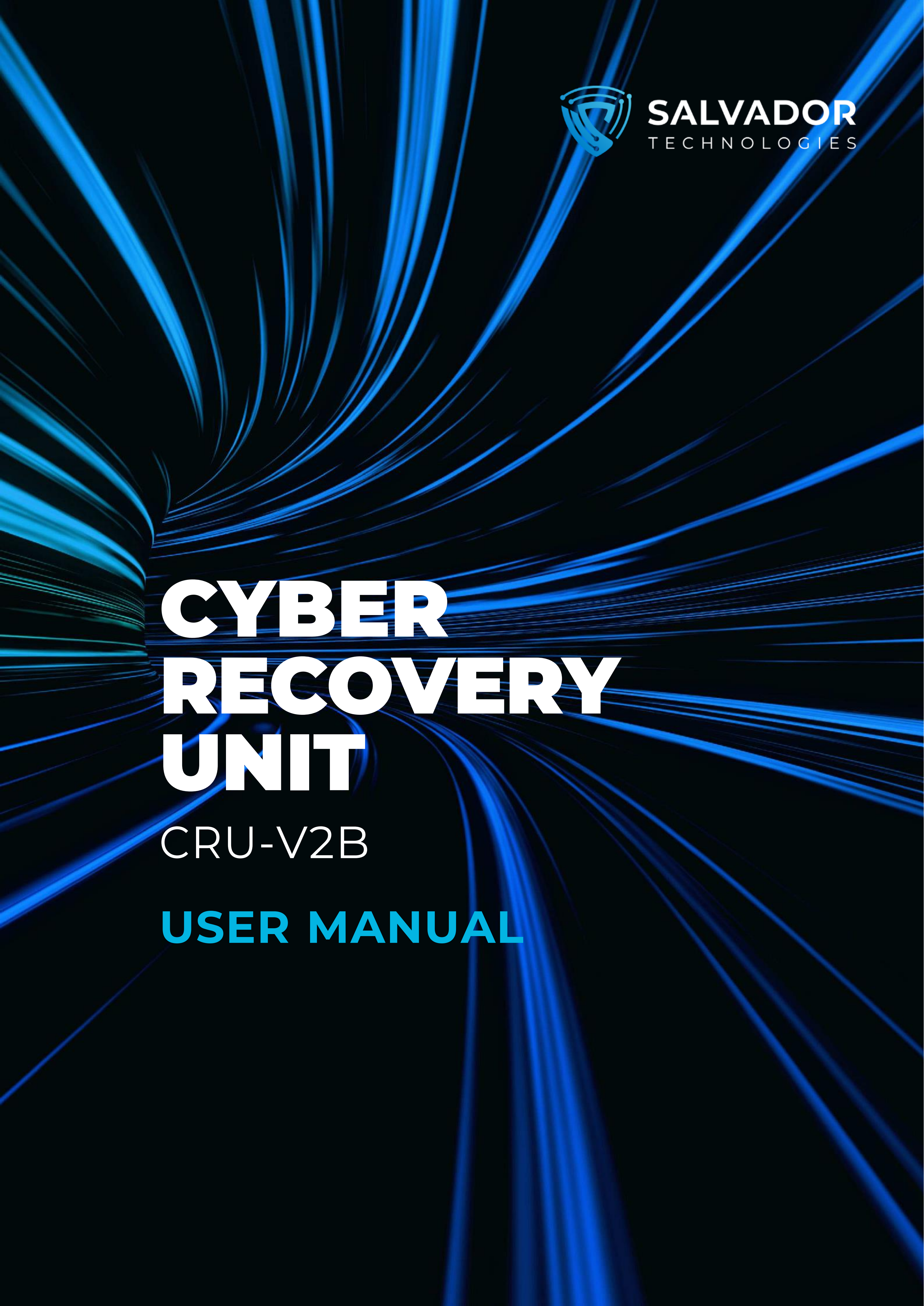
SALVADOR
TECHNOLOGIES



CYBER RECOVERY UNIT

CRU-V2B

USER MANUAL

TABLE OF CONTENTS

01 Introduction 3

1.1 Cyber Recovery Unit (CRU)

1.2 The Backup Software Agent

1.3 The Centralized Management System

1.4 Scheduled Backups Algorithm

02 Software Installation 4

2.1 Minimal Requirements

2.2 Prior to the Setups

2.3 Installation

03 Configure Backup Schedule 5

04 Restoration of the Computer 7

05 Full Recovery of the Internal Hard Drive........ 9

06 Additional Features 10

07 Cyber-Attacks Mitigation 10

08 VM Installation & Configuration 11

09 VMware Workstation Configuration 12

10 Scheduled Backups for Not-Administrator/Not-Logged-In Users 13

11 Advanced Features 15

12 Image Backup 17

13 Web Management System 20

14 Booting Salvador CRU on another computer/Server 26

15 Copying Specific Files From Salvador Backup Disk 26

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. Afterward, 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.
3. Direct link to the software agent: https://support.salvador-tech.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 back 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 during week 2, the NVMe-Previous will be created during week 3, NVMe-Current will be updated and 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 7/8/10/11
- Windows Server 2008/2012/2016/2019
  We currently do not support domain controller/active directory servers

Capacity: There are 3 CRU Versions:

CRU 512GB – please use only with disks up to

512GB

CRU 1TB - please use only with disks up to

1TB

CRU 2TB - please use only with disks up to

2TB

.NET 4.5 –

http://support.salvador-tech.com/Resources/DotNet%204.5.2%20installation.zip

512 disk sector size (4096 is not supported)

2.2 Before the Setup

1. Make sure that your computer/server can boot from a USB drive by properly configuring UEFI/BIOS (Enable boot from USB).
2. If the USB ports are disabled for the Antivirus/ DLP software, please add an exclusion for CRU hardware.

2.3 Installation

Connect the CRU unit to the computer using the supplied USB cable. If your computer has rear and front USB ports, it's better to connect it to the rear ports.

Direct link for the software agent:
https://support.salvador-tech.com/Resources/SalvadorBackupRecoveryLastVersion.zip

Install the software agent.

Note: *Make sure your power settings so the computer will not enter into "sleep" mode during backup*

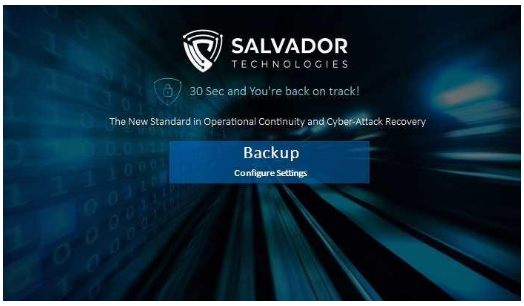
You can follow the nominal operation of the backup software by using the statistics in the software home screen or using the log file BackupLog.txt located in the installation folder.

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

https://support.salvador-tech.com/

3 | CONFIGURE BACKUP SCHEDULE

1. Run the software.

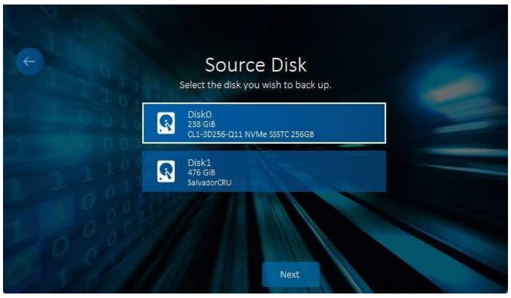


30 Sec and You're back on track!

The New Standard in Operational Continuity and Cyber-Attack Recovery

2. Click on the Backup button.

3. Select the source disk, which is the disk you wish to backup, usually Disk0.



Source Disk

Select the disk you wish to back up.

Disk0
238 GiB
CL1-3D256-Q11 NVMe SSSTC 256GB

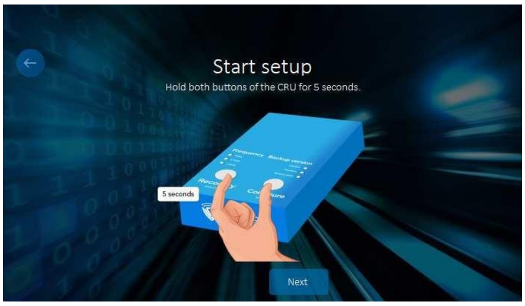
Disk1
476 GiB
SalvadorCRU

Click on the Next button.

4. <u>Hardware Setup -Factory Reset Backup Generation</u>

Press and hold both buttons of the CRU for 5 seconds, all the device's LEDs should blink for a second.

Nominal state: Under Frequency "Daily" LED is turned on, "Factory Reset" and SET buttons should be flickering.



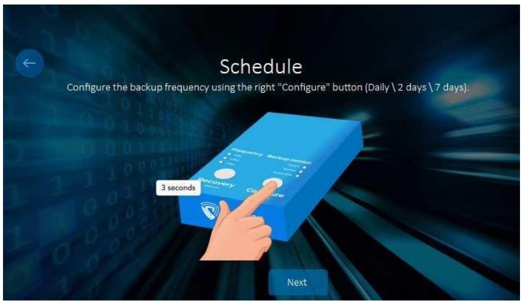
Start setup

Hold both buttons of the CRU for 5 seconds.

5. Click the Next button.

6. <u>Hardware Setup -Backup Frequency Configuration</u>

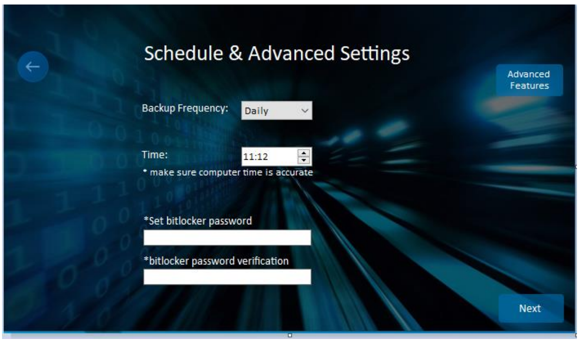
Skip this section if you would like to configure daily backup frequency. Otherwise, Configure the backup frequency by pressing the "SET" button for 3 seconds on the CRU device. There are 3 backup frequency options (Daily/2 Days/ Weekly)



Schedule

Configure the backup frequency using the right "Configure" button (Daily \ 2 days \ 7 days).

7. Select the same backup frequency in the software (according to the selection in the previous section, it should be the same as on the hardware)



Schedule & Advanced Settings

Backup Frequency: Daily

Time: 11:12

* make sure computer time is accurate

*Set bitlocker password

*bitlocker password verification

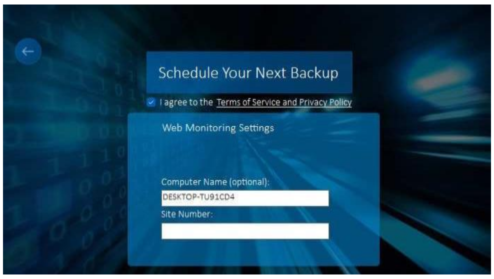
8. If BitLocker encryption is enabled on the computer, please set the encryption password which will be used to encrypt the "Salvador CRU" device.

9. Click on the "Next" button.

10. Read and agree to the Terms of Service and Privacy Policy.

11. Skip this section I you don’t want to use our cloud-based management system:

12. Enter https://support.salvador-tech.com/



Schedule Your Next Backup

☑ I agree to the Terms of Service and Privacy Policy

Web Monitoring Settings

Computer Name (optional): DESKTOP-TU91CD4

Site Number:

After successful registration, you will find the “site number” parameter

13. Skip this section if you don’t want to use our VM-based on-premise management system: You will find the full instructions in Chapter 8 (On-Prem Web Management Monitoring Installation).
14. Click on the “Start Backup” button.
15. After the first backup, the other backup tasks will be executed 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:

- You can minimize the software and find it in the tray icons.
- Future backups, at the scheduled time (in the background of your nominal operation).
- Make sure that your system will not enter a sleep mode during the backup operation, by changing the power settings accordingly.

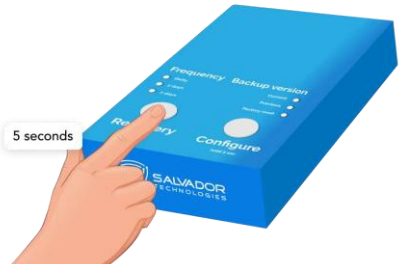
4 | RESTORATION OF THE COMPUTER

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

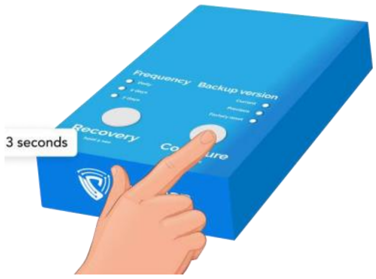
   Note: *This is important to avoid any corruption in the air-gapped recovery disk, as it will turn online during this section.*

2. Turn off the computer.

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



4. The selected disk is the "Current". If you would like to recover from a different disk ("Previous" or the "Factory Reset") hold the "SET" button for 3 seconds 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.

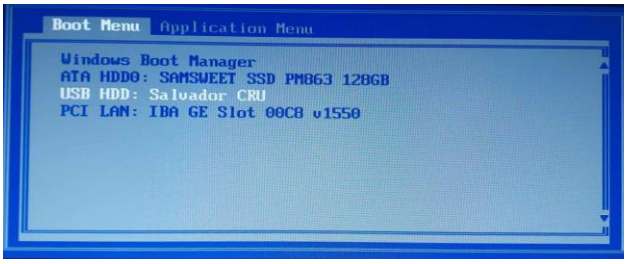
5. Turn on the computer.

6. 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 Menu Key
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

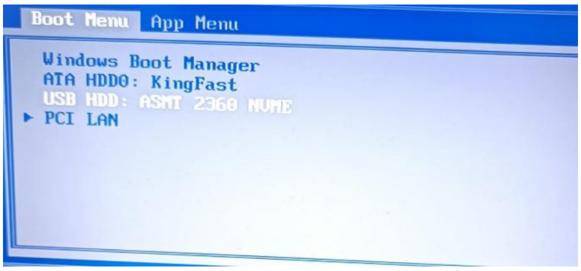
7. When using old legacy systems (MBR based), you must choose in the UEFI/BIOS- booting from "legacy mode".

8. Select a USB device (Salvador CRU or ASMT 2360 NVME)



```
Windows Boot Manager
ATA HDD0: SAMSWEET SSD PM863 128GB
USB HDD: Salvador CRU
PCI LAN: IBA GE Slot 00C8 v1550
```

9. Some of the computers, might recognize the CRU (Cyber Recovery Unit) as ASMT 2360 NVME, in this particular case, please choose to boot from this device:



```
Boot Menu   App Menu

  Windows Boot Manager
  ATA HDD0: KingFast
  USB HDD: ASMT 2360 NVME
▸ PCI LAN
```

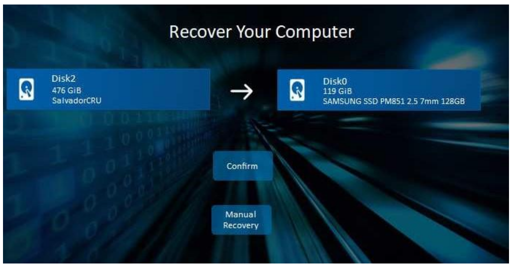
The computer will continue to operate from the selected backup version, replacing the main hard drive.
You can continue to operate in this mode as long as you need (days, weeks) before the full recovery process (mentioned in Chapter 5) is done.

Note: *No additional backups will be executed during the recovery mode.*

5 | FULL RECOVERY OF THE INTERNAL HARD DRIVE

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

2. The following recovery screen will appear automatically.



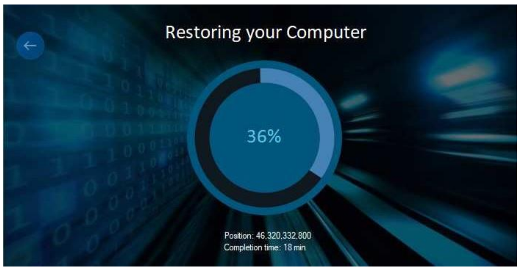
Recover Your Computer

Disk2
476 GiB
SalvadorCRU

→

Disk0
119 GiB
SAMSUNG SSD PM851 2.5 7mm 128GB

3. Click the Confirm button. The recovery process will be started.



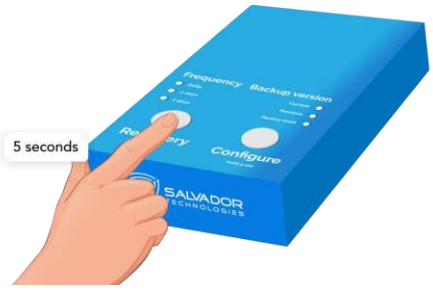
Restoring your Computer

36%

Position: 46,320,332,800
Completion time: 18 min

4. When finished, restart the computer and boot as usual from the main hard drive.

5. 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 continue your computer backups according to the schedule*

6 | ADDITIONAL FEATURES

To reset the internal timer of the CRU device, click and hold the “SET” 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.
  - One of the methods to mitigate APT malware is the “creation of a backup image file” (more details in chapter 12), the image file can run in a sandbox virtual environment. The virus can be deleted by using XDR/AV or forensics analysis, afterward, the VHD file can be transferred to a CRU device and booted on a physical machine.

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 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).

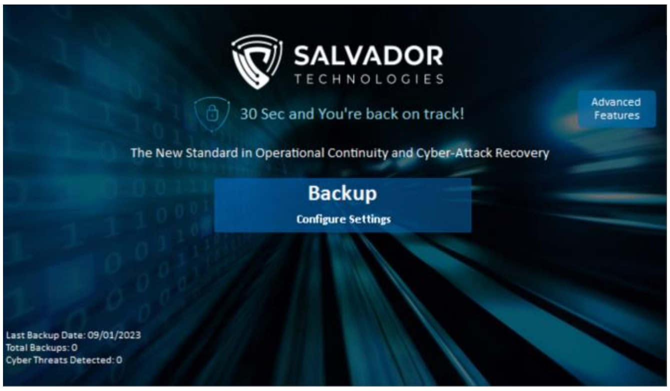
8 | VM Installation & Configuration

Download the on-premise “centralized web management” Ubuntu-based VM from: https://support.salvador-tech.com/Resources/Salvador_1_5_4_OVA.zip

1. Important notes for various hypervisors:
   - For ESXI, please delete any redundant CD-ROMs, Hard-Drives that are not related to the VMDK. Use “IDE” in the SCSI Controller.
2. Default admin password for the VM:
   SC056AJ!
3. Please configure static IP in the VM using the following user guide:

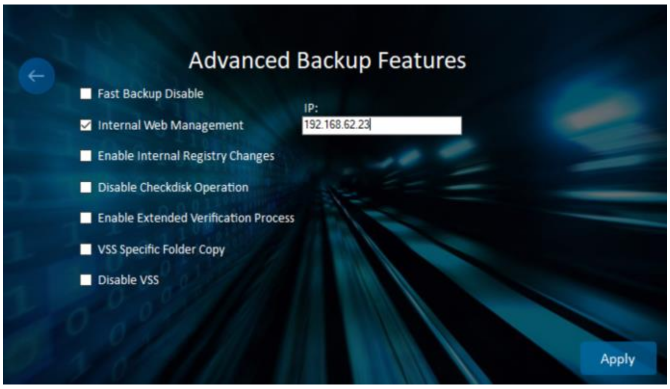
   https://linuxconfig.org/how-to-configure-static-ip-address-on-ubuntu-18-10-cosmic-cuttlefish-linux

   Configure the software agent to use the internal VM. Use the instructions in section 3. In the following screen enter “Advanced Settings”:
4. Enter the “Advanced Features” on the main screen


SALVADOR
TECHNOLOGIES
30 Sec and You're back on track!
Advanced Features
The New Standard in Operational Continuity and Cyber-Attack Recovery
Backup
Configure Settings

Last Backup Date: 09/01/2023
Total Backups: 0
Cyber Threats Detected: 0

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



Advanced Backup Features

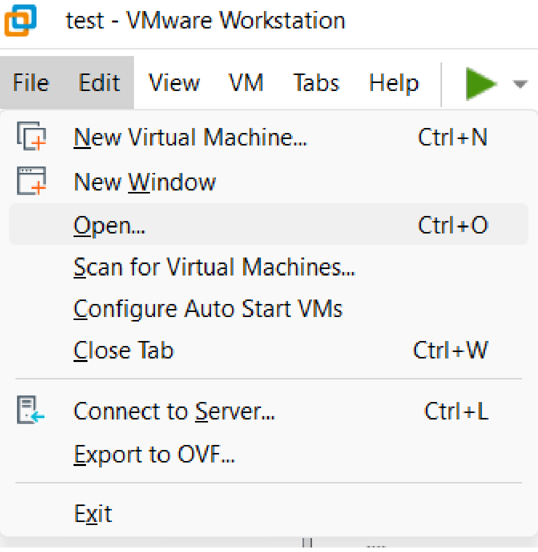
□ Fast Backup Disable
☑ Internal Web Management — IP: 192.168.62.23
□ Enable Internal Registry Changes
□ Disable Checkdisk Operation
□ Enable Extended Verification Process
□ VSS Specific Folder Copy
□ Disable VSS

6. Enter the web management system using your web browser using the Static IP:
7. Register a new user to the internal web management system

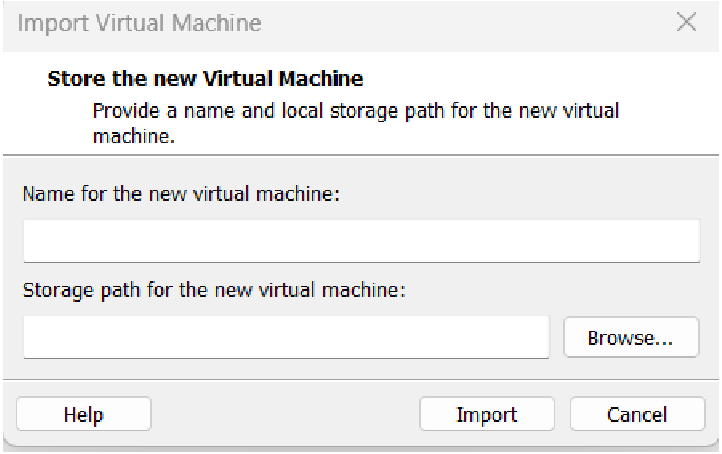
9 VMware Workstation Configuration

VMware Workstation

1. Open the OVA file:


test - VMware Workstation
File
Edit
View
VM
Tabs
Help
New Virtual Machine... Ctrl+N
New Window
Open... Ctrl+O
Scan for Virtual Machines...
Configure Auto Start VMs
Close Tab Ctrl+W
Connect to Server... Ctrl+L
Export to OVF...
Exit

2. Configure the name and the path of the virtual machines. Click on the "Import" button.


Import Virtual Machine

Store the new Virtual Machine

Provide a name and local storage path for the new virtual machine.

Name for the new virtual machine:

Storage path for the new virtual machine:

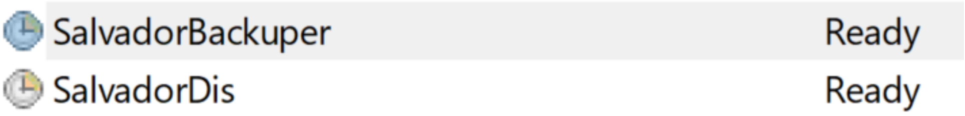
3. Run the VM

4. For more information regarding the VM configuration, please follow the instructions in the previous chapter "VM Installation & Configuration".

10 |Scheduled Backups For Not-Administrator Users or Logged-Off Users

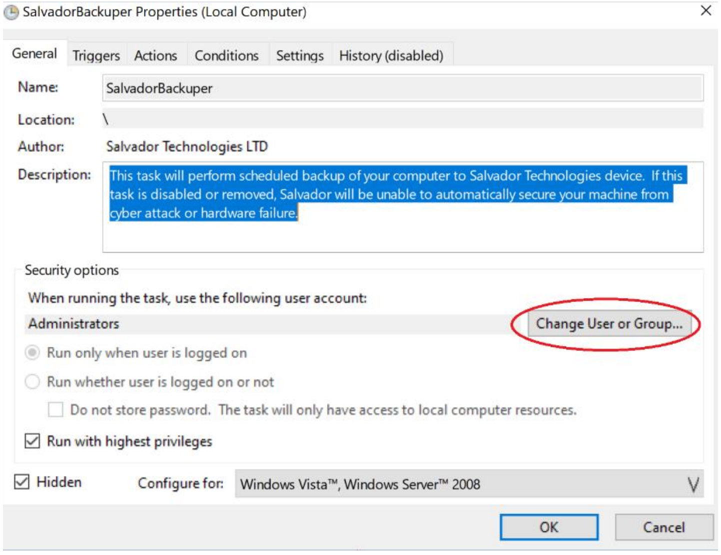
If you would like to run scheduled backups on a not-administrator account, or you have an organization policy that requires manual administrator password typing, please follow the instruction to enable automatic scheduled backups:

1. Enter the "Task Scheduler" using administrator credentials.
2. Locate the "SalvadorBackuper" task and double click:



SalvadorBackuper	Ready
SalvadorDis	Ready

3. On the following screen enter "Change User or Group"



SalvadorBackuper Properties (Local Computer)

Name: SalvadorBackuper

Location: \

Author: Salvador Technologies LTD

Description: This task will perform scheduled backup of your computer to Salvador Technologies device. If this task is disabled or removed, Salvador will be unable to automatically secure your machine from cyber attack or hardware failure.

Security options

When running the task, use the following user account:

Administrators

● Run only when user is logged on

○ Run whether user is logged on or not

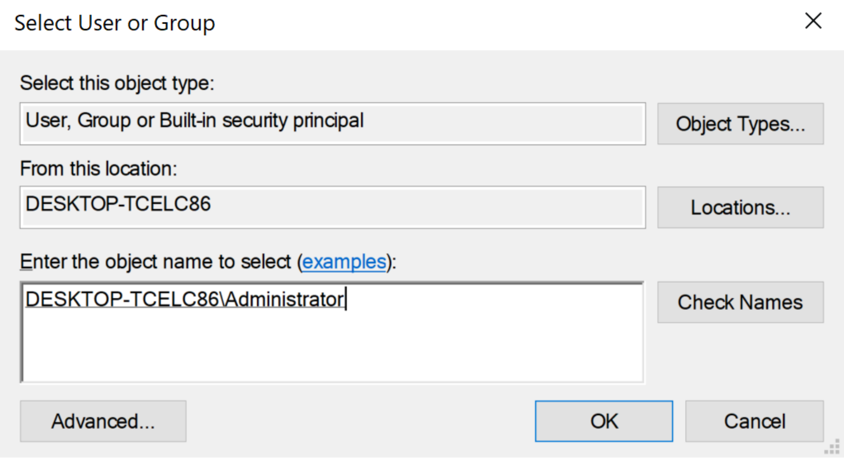
□ Do not store password. The task will only have access to local computer resources.

☑ Run with highest privileges

☑ Hidden

Configure for: Windows Vista™, Windows Server™ 2008

4. On the following screen select the local/domain administrator, and press OK:



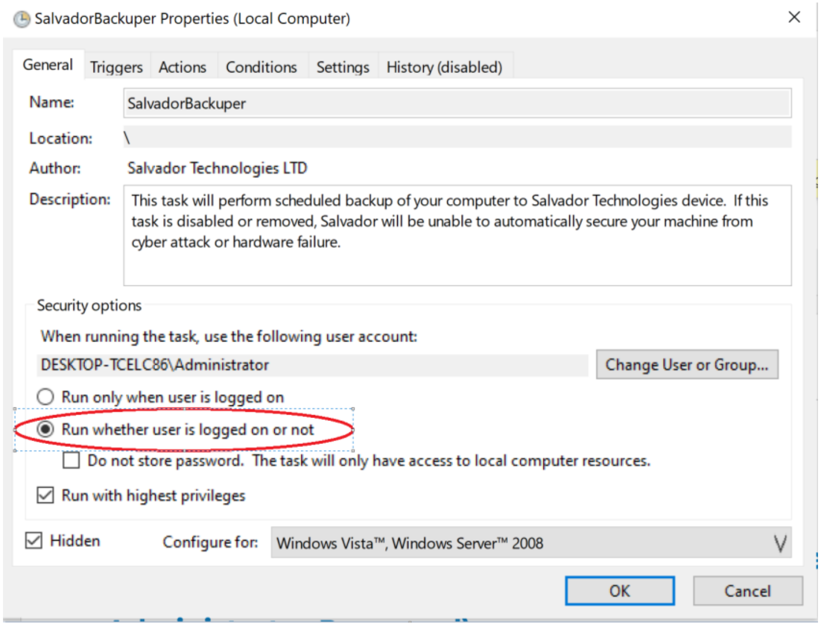
Select User or Group

Select this object type:
User, Group or Built-in security principal

From this location:
DESKTOP-TCELC86

Enter the object name to select (examples):
DESKTOP-TCELC86\Administrator

5. Select the second option “Run whether the user is logged on or not” and click OK.



SalvadorBackuper Properties (Local Computer)

Name: SalvadorBackuper

Location: \

Author: Salvador Technologies LTD

Description: This task will perform scheduled backup of your computer to Salvador Technologies device. If this task is disabled or removed, Salvador will be unable to automatically secure your machine from cyber attack or hardware failure.

Security options

When running the task, use the following user account:
DESKTOP-TCELC86\Administrator

○ Run only when user is logged on

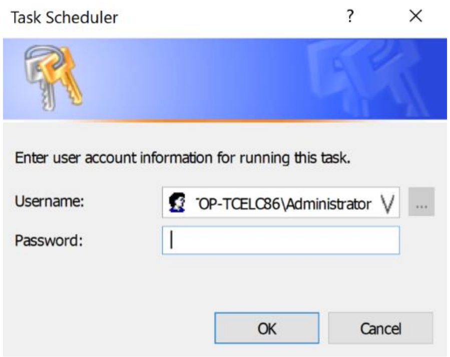
● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

☑ Run with highest privileges

☑ Hidden   Configure for: Windows Vista™, Windows Server™ 2008

5. Enter the administrator credentials:



Task Scheduler

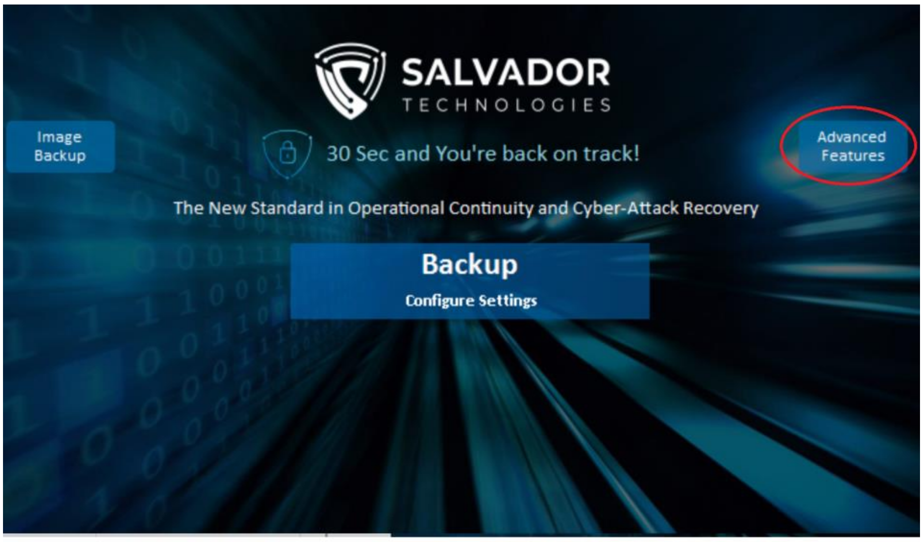
Enter user account information for running this task.

Username: OP-TCELC86\Administrator

Password:

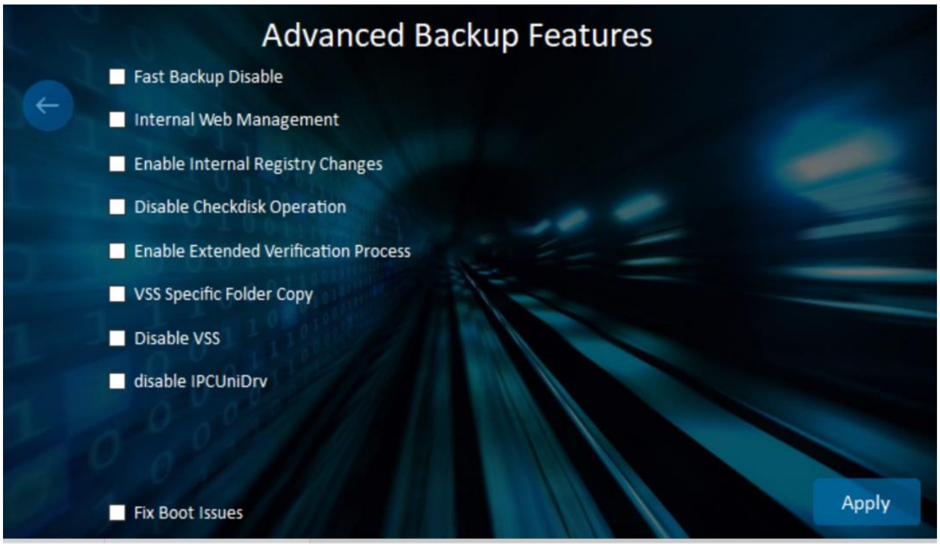
11 | Advanced Features

On the home screen, click on the advanced features button.



30 Sec and You're back on track!

The New Standard in Operational Continuity and Cyber-Attack Recovery



Advanced Backup Features

- □ Fast Backup Disable
- □ Internal Web Management
- □ Enable Internal Registry Changes
- □ Disable Checkdisk Operation
- □ Enable Extended Verification Process
- □ VSS Specific Folder Copy
- □ Disable VSS
- □ disable IPCUniDrv
- □ Fix Boot Issues

Advanced features details:

- Fast Backup Disable- option to prevent “optimization algorithms” during a nominal backup operation
- Internal Web Management – enable VM-based web management (described in section 8), after selecting this option, you need to enter the VM IP address.
- Enable Internal Registry Changes- in computers that block access to the USB disks (for example “DLP software” that cannot be bypassed). Internal registry changes might be required to allow boot from USB drives.
- Disable Checkdisk Operation- at the end of the verification process, the software runs automatically checkdisk algorithm, this feature can be disabled.
- Enable Extended Verification Process - in computers that block access to the USB disks (for

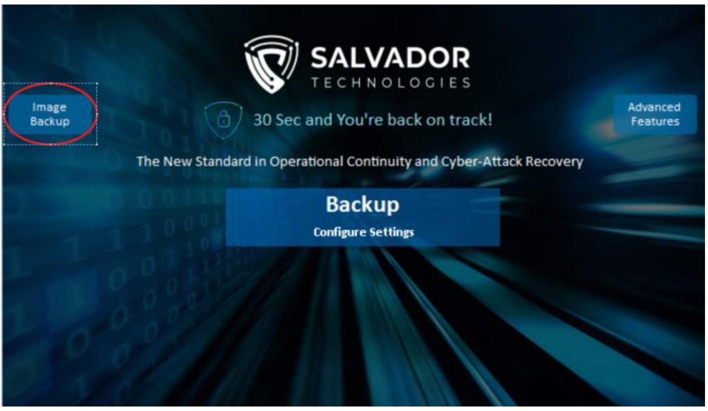
example "DLP software" that cannot be bypassed), extended verification might be required as the VSS verification algorithm might be blocked. m

- VSS Specific Folder Copy- implement VSS algorithm copy on a specific copy, more details regarding VSS algorithm https://learn.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service
- Disable VSS – disables the VSS algorithm
- Disable IPCUniDrv- "Industrial PC Siemens Driver" that cannot operate on computers with different hardware. Selecting this option, and clicking "Fix Boot Issues" will enable to transfer of the backup to a computer with a different hardware"
- "Fix Boot Issues" – if for some reason you experience any booting issues from the Salvador CRU. selecting this option while the device is connected might fix them (please wait for 1 minute for a "confirmation message" after selecting this option.

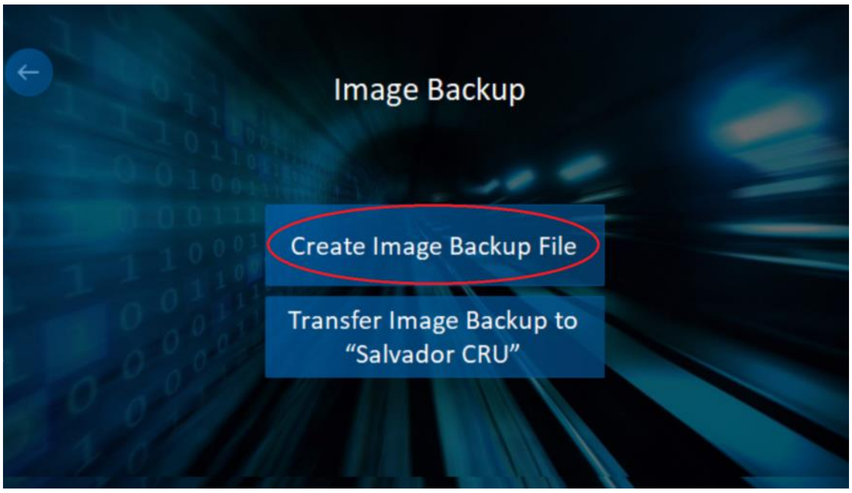
12| Image Backup

Before utilizing this feature, please read this note:
It is not feasible to duplicate a hard drive with a sector size of 512 bytes to a hard drive with a sector size of 4096 bytes. The target storage sector size should be 512 bytes.

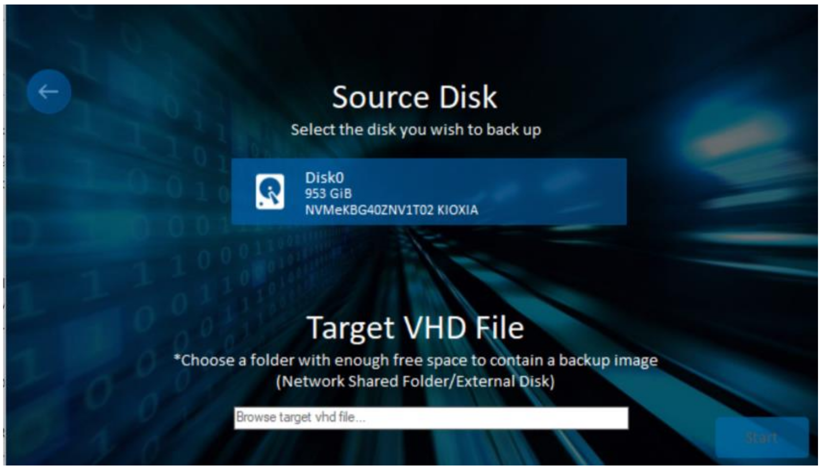
On the home screen, click on the image backup button.


SALVADOR
TECHNOLOGIES
Image Backup
30 Sec and You're back on track!
Advanced Features
The New Standard in Operational Continuity and Cyber-Attack Recovery
Backup
Configure Settings

Creation of Image Backup File:
On the following screen, click on Create Image Backup File



Select the "Source Disk" you wish to backup (can be the internal drive or Salvador CRU).
The target folder should have enough free space to contain a backup image (network shared folder/external drive



Source Disk

Select the disk you wish to back up

Disk0
953 GiB
NVMeKBG40ZNV1T02 KIOXIA

Target VHD File

*Choose a folder with enough free space to contain a backup image (Network Shared Folder/External Disk)

Browse target vhd file...

Transfer Image Backup To Salvador CRU

On the following screen, click on Transfer Image Backup to Salvador CRU

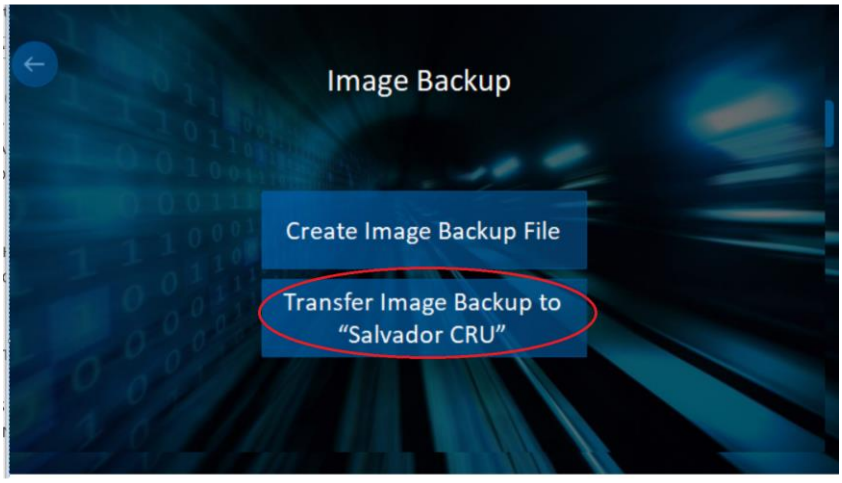
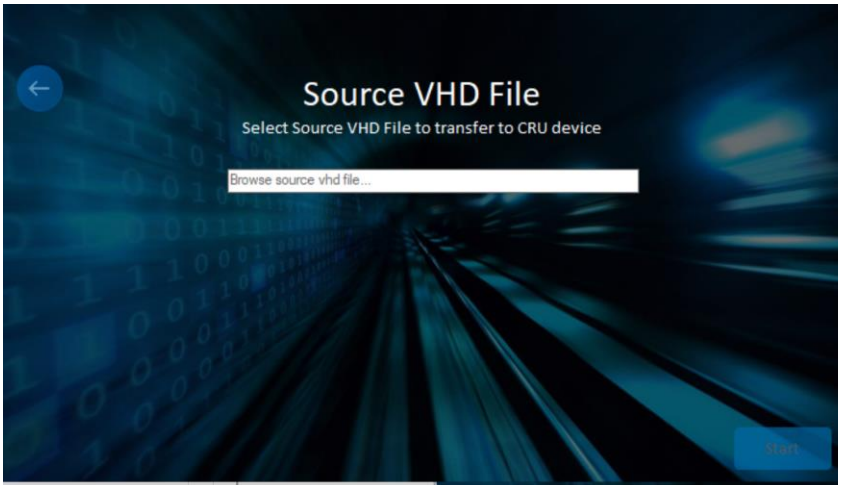


Image Backup

Select the VHD source file that you wish to transfer to the "Salvador CRU" device.



Source VHD File

Select Source VHD File to transfer to CRU device

Browse source vhd file...

Run Salvador Image VHD file as a virtual machine (virtual restoration test/Sandbox).

Important note: this feature is not supported in legacy OS such as Windows 7/ Windows Server 2008

One of the main advantages of image backup files is the ability to run them in a virtual environment. It's possible to test the backup by using the following hypervisors,

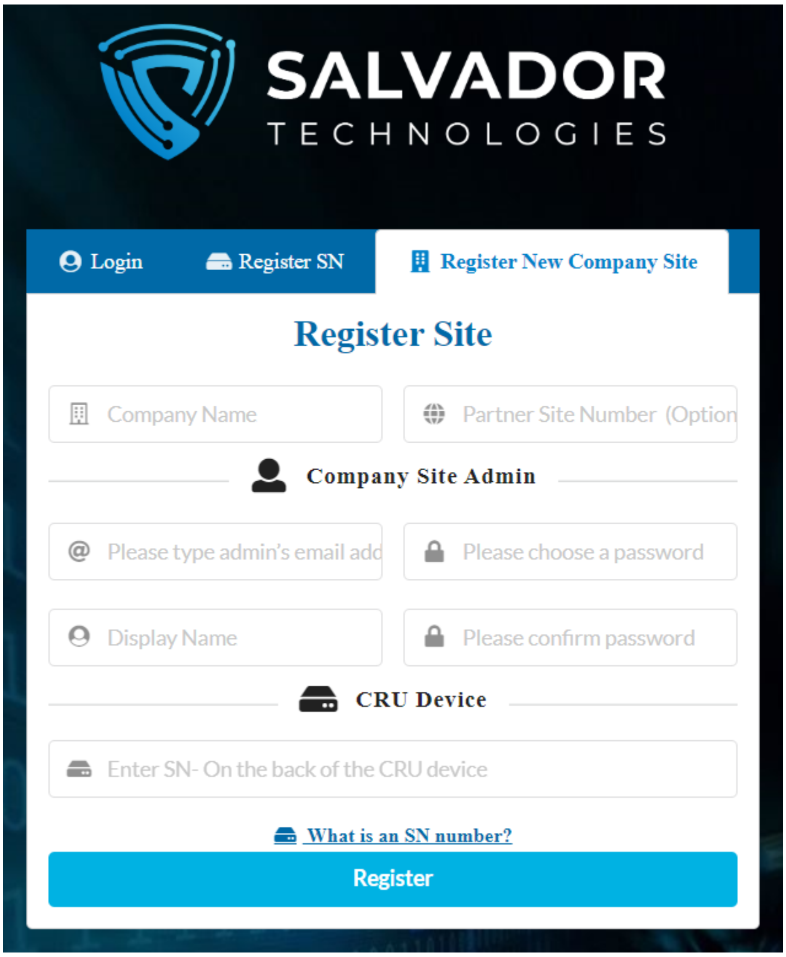
- "Oracle Virtual Box" - https://www.sysprobs.com/how-to-open-run-microsoft-vhd-files-on-virtualbox-pre-installed-vhd-images
- "Microsoft Hyper-V" http://reflect.macrium.com/help/v5/how_to/imgtovhd/using_a_vhd_with_microsoft_hyper-v_or_virtual_pc.htm

In a virtual environment, you can do the following things:

1. Virtual restoration test - check if the backup is running properly.
2. Sandbox- analyze the backup in the sandbox environment before booting it on a physical machine. This method can be used for forensics and the deletion of APT malware (advanced persistent threat).

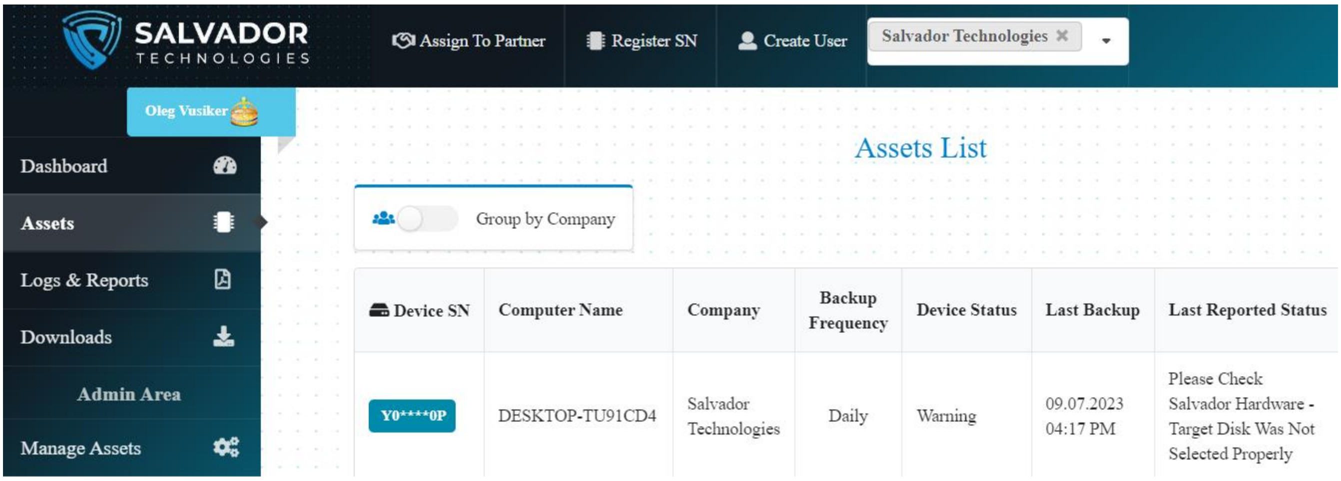
13| Web Management System

1. Enter to the cloud-based management system: https://support.salvador-tech.com/ or use the on-premises VM.
2. Click on "Register New Company Site" .
3. If your company has several physical sites, it may be worth considering registering each of them separately to establish clear segmentation between the sites. Alternatively, you can opt to register only one site and view all the company's assets on a single screen.
4. Important notes:
   a. Using the "Partner Site Number" field is optional. Only fill it out if you have acquired the product through a reseller or distributor and are aware of their site number.
   b. The SN is physically located on the back of the CRU hardware device.



5. Login to the web management using your credentials.

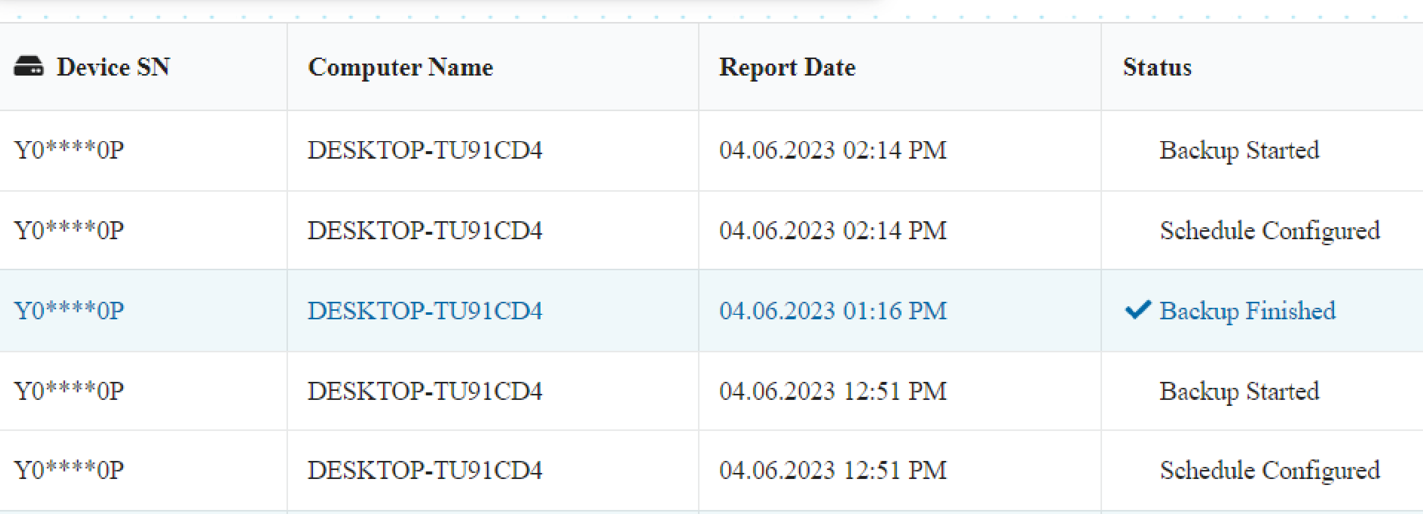
6. You can watch the entire assets of the "Company Site" by entering to the "Assets List" (on the left)



Assets List

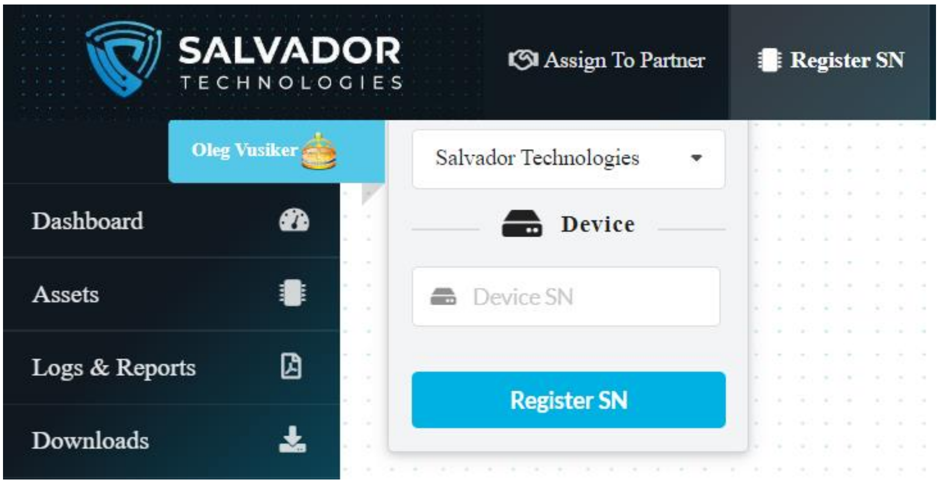
Device SN	Computer Name	Company	Backup Frequency	Device Status	Last Backup	Last Reported Status
Y0****0P	DESKTOP-TU91CD4	Salvador Technologies	Daily	Warning	09.07.2023 04:17 PM	Please Check Salvador Hardware - Target Disk Was Not Selected Properly

7. Clicking on a specific Device SN will show the recent history of this device



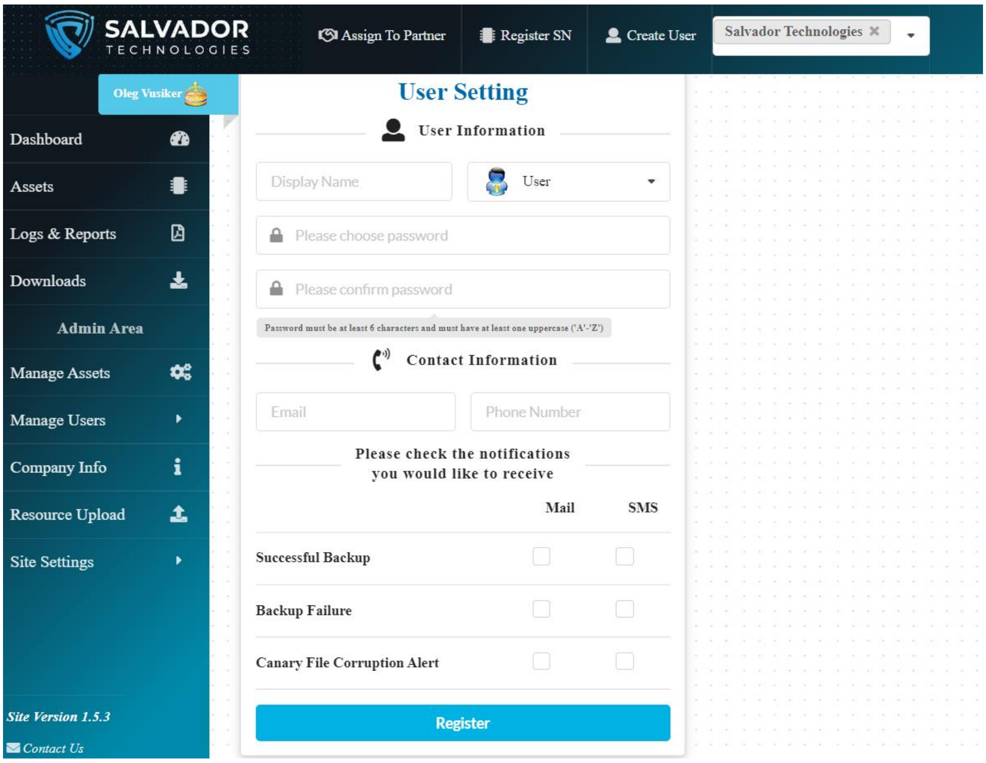
Device SN	Computer Name	Report Date	Status
Y0****0P	DESKTOP-TU91CD4	04.06.2023 02:14 PM	Backup Started
Y0****0P	DESKTOP-TU91CD4	04.06.2023 02:14 PM	Schedule Configured
Y0****0P	DESKTOP-TU91CD4	04.06.2023 01:16 PM	✓ Backup Finished
Y0****0P	DESKTOP-TU91CD4	04.06.2023 12:51 PM	Backup Started
Y0****0P	DESKTOP-TU91CD4	04.06.2023 12:51 PM	Schedule Configured

8. To add a new device to your "Company Site", please click on the "Register SN" . The device will be added automatically to the "Assets" table.



Salvador Technologies

9. To add a new user to your "Company Site", please click on "Create User", you can choose if the user will be site administrator, or a regular user. You can also select if the specific user will receive email alerts regarding the backups (Successful Backup Alerts, Backup Failure, Canary File Corruption Alert)



Salvador Technologies

User

Password must be at least 6 characters and must have at least one uppercase ('A'-'Z')

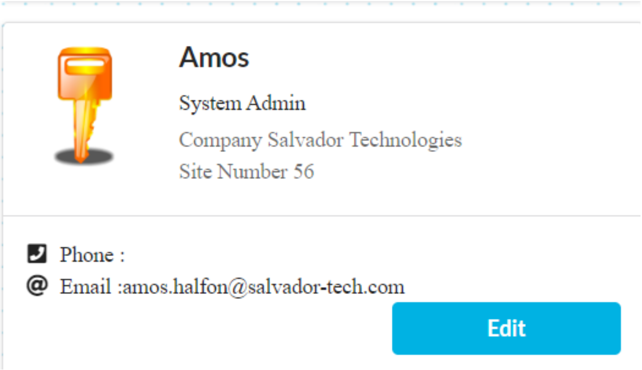
Please check the notifications you would like to receive

	Mail	SMS
Successful Backup	□	□
Backup Failure	□	□
Canary File Corruption Alert	□	□

10. To add a new user to your "Company Site", please click on "Create User", you can choose if the user will be site administrator, or a regular user. You can also select if the specific user will receive email alerts regarding the backups.

11. Within the "Manage User" section, you can supervise and edit all users associated with your:

    By selecting the "edit" option, you have the ability to modify a range of settings, including: Password, Email alert preferences, and Contact Information.



Amos

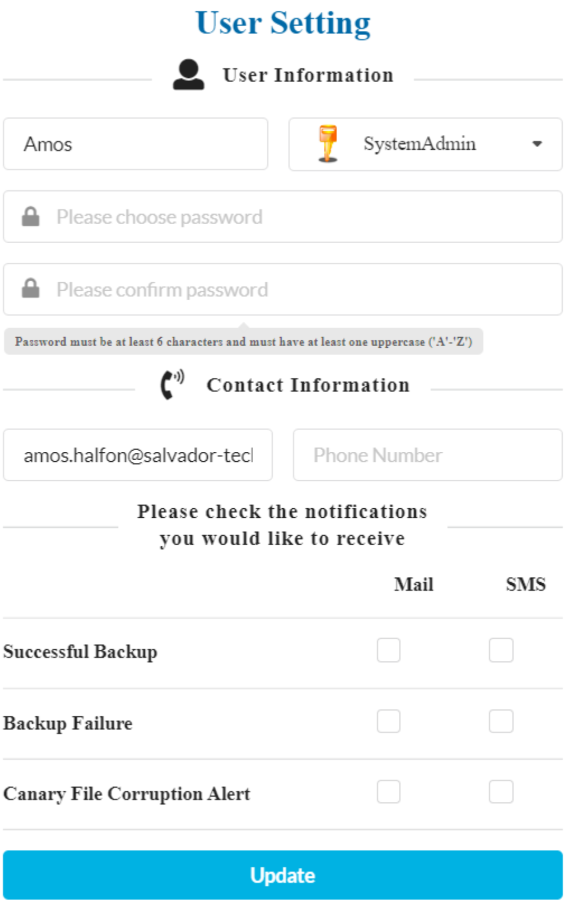
System Admin

Company Salvador Technologies

Site Number 56

☎ Phone :

@ Email :amos.halfon@salvador-tech.com



User Setting

User Information

Amos

SystemAdmin

Please choose password

Please confirm password

Password must be at least 6 characters and must have at least one uppercase ('A'-'Z')

Contact Information

amos.halfon@salvador-tecl

Phone Number

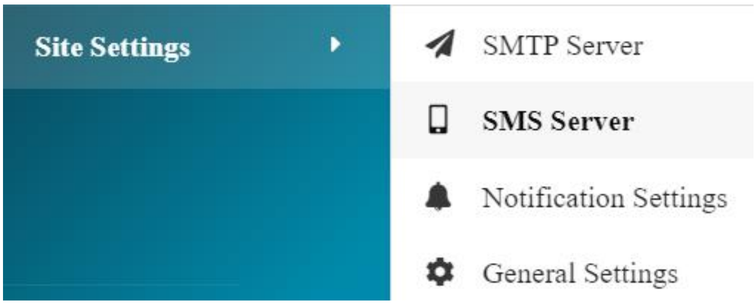
Please check the notifications you would like to receive

	Mail	SMS
Successful Backup	□	□
Backup Failure	□	□
Canary File Corruption Alert	□	□

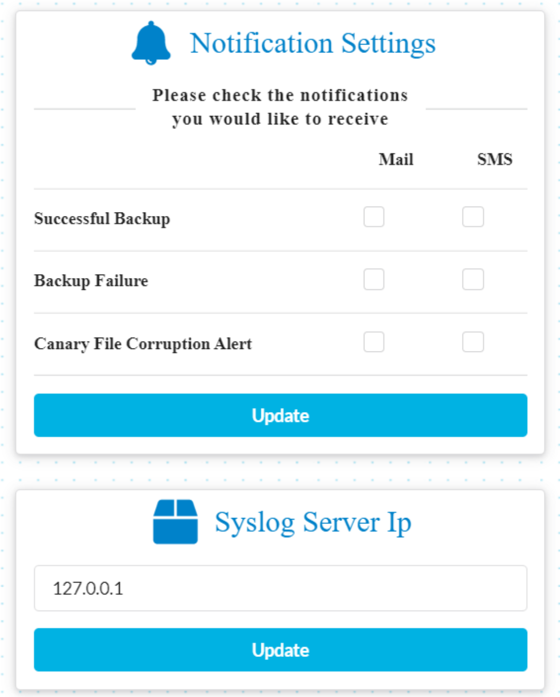
12. To add a new user to your "Company Site", please click on "Create User", you can choose if the user will be site administrator, or a regular user. You can also select if the specific user will receive email alerts regarding the backups.

13. In the "Site Settings" section, you can modify the following settings:

    - SMTP Server– Customize your server settings (replace the default configuration).
    - SMS Server– Customize your server settings (replace the default configuration).
    - Notification Settings- change general notification settings (will be elaborated in the next sections)
    - General Settings- various settings, will be elaborated in the next section.



14. In the "Notifications" section, you can modify which notification will be sent to the users, In addition you can configure that syslog alerts will be sent automatically to SIEM/SOC server:

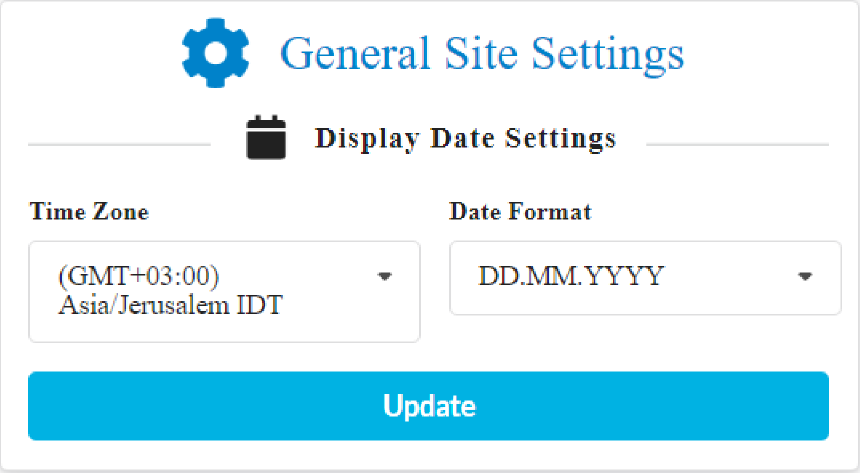


Please check the notifications you would like to receive

	Mail	SMS
Successful Backup	□	□
Backup Failure	□	□
Canary File Corruption Alert	□	□

127.0.0.1

15. In "General Settings" you can change the "Time Zone' and Date Format.



General Site Settings

Display Date Settings

Time Zone: (GMT+03:00) Asia/Jerusalem IDT

Date Format: DD.MM.YYYY

14 | Booting CRU on another physical computer/server

it’s possible to transfer the “Salvador CRU” device to another hardware and boot from it, please consider the following limitations.

Supported OS

Windows 10/11
Windows Server 2016/2019/2022

Windows 7 Important Notes:

- Windows 7 does not include native USB boot support by Microsoft.
- Windows 7 drivers OS are not automatically adapted to a new machine.
- Currently it’s not supported to transfer CRU to another machine on Windows 7

MBR/GPT Important Notes

- If your computer uses BIOS (legacy boot), the device can be transferred exclusively to other computers that also support MBR legacy boot, typically found in older systems.
- In the case of UEFI GPT boot on your computer, the device is compatible solely with computers that support UEFI GPT boot, which is more common in newer machines.

15 | COPYING SPECIFIC FILES FROM SALVADOR BACKUP DISK (USAGE AS A DISK ON KEY)

Access to Salvador disks is blocked by default, if “Salvador software agent” is installed.
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