

HyperBUNKER

Quick Start Guide and User Manual

HyperBUNKER LTD.

VERSION 1.0

Contents

1. Quick start guide 2
2. Introduction 3
   2.1 Device and Security Overview 3
   2.2 Safety Guidelines 4
   2.3 First Power-On Setup 4
   2.4 User account operations 5
   2.5 Admin account operations 6
   2.6 Backup Operation 6
   2.7 Restore Operation 7
   2.8 Security Lock & Alerts 9
   2.9 Best Practices 9
3. Technical Specifications 10
4. Install HyperBUNKER Client 10
   4.1. Windows client 10
      4.1.1. Installation Wizard Guide 10
   4.2. Linux client 12
      4.2.1. Installation Wizard Guide 12
   4.3 Common Issues and Solutions Windows client 13
      4.3.1 Repository not created 13
      4.3.2 HyperBUNKER Transitory unit Not Detected 13
      4.3.3 Files Not Transferring 13
      4.3.4 Task Scheduler Issues 13
   4.4 Common Issues and Solutions Linux client 14
      4.4.1 No USB devices detected 14
      4.4.2 Copy process not starting 14
      4.4.3 Permission issues 14
5 Monitoring system 14
   5.1 On screen monitoring 14
   5.2. Local network monitoring 15
   5.3. Monitoring server via API key – monitoring.hyperbunker.com – optional 15
6 Support 16
7 Disclaimer of Liability 16

1. Quick start guide

Thank you for choosing HyperBUNKER!

To quickly get your device up and running, follow the below outlined steps. For more information on the product, read the User Manual section.

- If you are mounting the device inside of a rack, ensure it is properly secured using 4 rack-mount screws and there is room for ventilation. Otherwise, ensure it is placed on a flat and stable surface, with no nearby obstructions

- Connect your main data connection cable USB situated on the right side of the device, ensure that is firmly seated and secure
    - Optionally, connect RJ45 connection into the left RJ45 port to enable local network monitoring

- Connect power cables to the dual power supply connectors on the back, ensure they are firmly connected

- Perform initial setup of the device

1.1 Set PIN/ Password for the User account

1.2 Select the backup schedule

- Ensure you store your PIN/Password in a safe place to prevent unauthorized access

After initial setup on HyperBunker is finished, HyperBUNKER logs in and appears in the outside world.

- On the user's side, make an installation of client so that HyperBUNKER can retrieve data.

The scheduled operation, the current operation, stats and its progress are displayed on the touch screen.

For additional information and instructions, refer to the User Manual section.

USER MANUAL

2. Introduction

HyperBUNKER, your last line of defense for critical data security. We appreciate your trust in our technology and are committed to ensuring that your essential data remains safe against any modern cybersecurity threat.
HyperBUNKER (HB) is a hardware-based data vault designed to protect your organization's most critical information from ransomware, hackers, and corruption. By storing immutable, AIR-gapped, offline backups in an isolated environment, HB ensures rapid recovery and long-term data integrity.

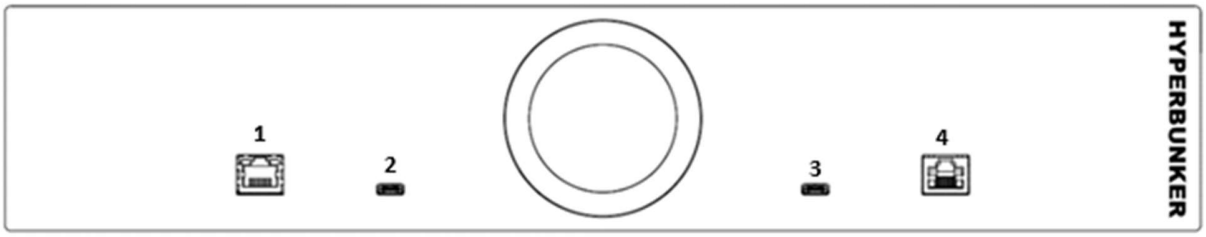
Key Advantages:

- Air-gapped, multi-drive immutable storage
- Rapid recovery of essential data
- Dual power supply unit redundancy for high availability
- Easy-to-use touchscreen interface which is also the only interact interface, ensuring maximum security

This manual provides comprehensive guidance for setup and operation of the HyperBUNKER system

2.1 Device and Security Overview

Physical Layout:



Front Panel:

- Circular HD Touchscreen – main control interface
- LAN Port (1) - used for monitoring
- USB-C Port (2) - service port – *not in use*
- USB-C Port (3) - main data connection
- LAN Port (4) - used for HyperLINK – *not in use*

Rear Panel:

- Dual redundant PSU ports – ensures continuous power
- Power switch – in future versions – *not in use*

Form Factor:

- 2U rack mountable or standalone desktop/server room installation

Security Features:

- Immutable Backups – no data modification once written
- No self-execution of scripts allowed on Cold Storage units
- Multi-user control – Admin and User roles with password/PIN access
- Buzzer Alerts – system halts and displays QR code, support contact instructions on errors
- Transitory R/W Storage always cleared between operations; no residual files present at any point in time

2.2 Safety Guidelines

- Always use both power supplies for redundancy, connected to two separate power circuits
- Do not block ventilation holes; allow for adequate cooling
- The device contains anti-tamper protections. Any attempt to force access will trigger an alarm and will disable operation of device
- Ensure that the PIN/Password is stored in a secure physical location
- Service, repair, or internal maintenance of the HyperBUNKER may only be performed by an authorized partner approved by the manufacturer

2.3 First Power-On Setup

Placement:

- Install inside a server rack (2U space required) or on a stable surface with no nearby obstructions to ensure adequate airflow
- Secure the device using 4x rackmount screws and cage nuts

Power Connection:

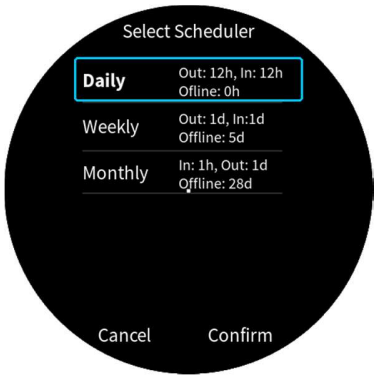
- Connect two PSU cables to redundant power supplies
- HB initiates boot sequence and display progress bar

Initial Configuration (Touchscreen Wizard):

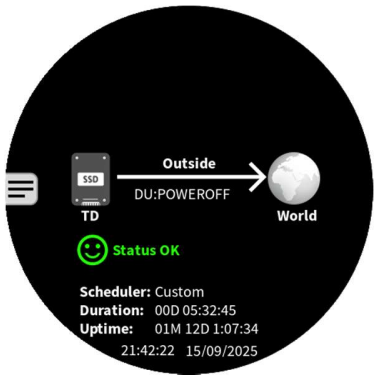
- Create User PIN/Password



- Configure Backup Schedule Mode (daily, weekly, monthly, or custom on request)



- HB confirms initialization and starts in outside world



Initial Configuration on client side:

- OS supported with HyperBUNKER client – Windows/Linux
- Setup HyperBUNKER Client – see page 9.
- User can use their own software solution for sync data to HyperBUNKER

2.4 User account operations

- User-level access is limited to ensure system integrity, and has the following functionality:
  - Change user password
  - Perform backup and restore operations
  - Input licence code
  - Change LCD Brightness
- Every touchscreen interaction requires PIN/password verification

2.5 Admin account operations

- Admin-level access has the following functionality:
  - Change User Password
  - Perform restore operations
  - Input licence code
  - Change LCD Brightness
  - Pause System / Stop all operations
  - Setup Date & Time
  - Setup Custom Scheduler
  - Register Format and mount Cold Storage and Transitory R/W Disk after replacement
  - Reset HB to factory defaults
  - DU Power – only in error status
- Every touchscreen interaction requires PIN/password verification

2.6 Backup Operation

How Backups Work:

- HB copies data from designated repository into AIR-gapped immutable storage using Transitory R/W Storage
- Transitory R/W Storage automatically clears its contents after storing them onto Cold Storage drives
- If any of the Cold Storage drives is not available during operation, HB displays an error and continues its operation; skipping the affected drive

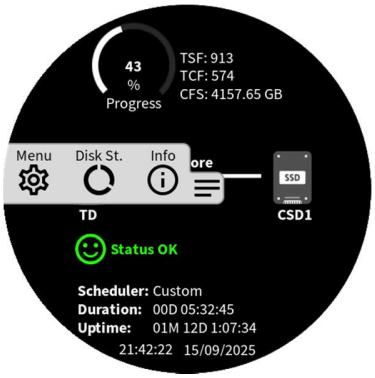
Monitoring:

- All stats displayed on touchscreen
- Last successful backup time in Disk Info is shown on touchscreen
- When a LAN cable is connected to the LAN1 port on the front, web monitoring is enabled and can be accessed via web browser from a device on the same network HB is connected to
- At the user's request, we can activate sending logs to the monitoring server.
- Errors or interruptions trigger buzzer alerts and monitoring server send info on e-mail (if activated).

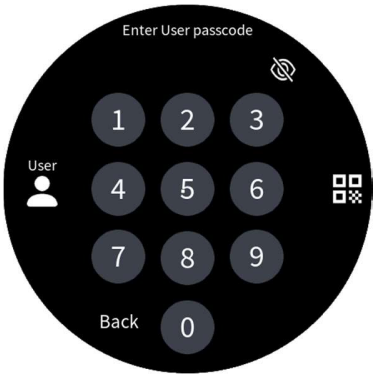
2.7 Restore Operation

Restore procedure:

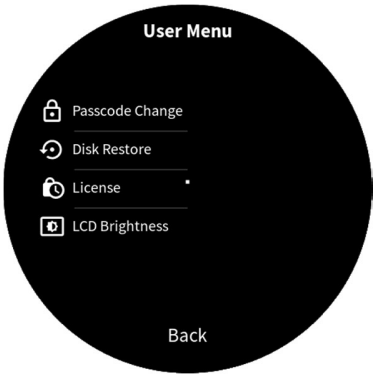
- Activate Menu on touchscreen and click on Menu



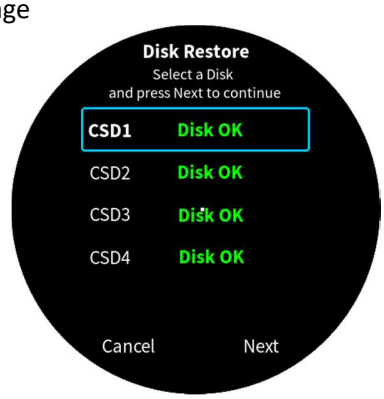
- Enter PIN/Password



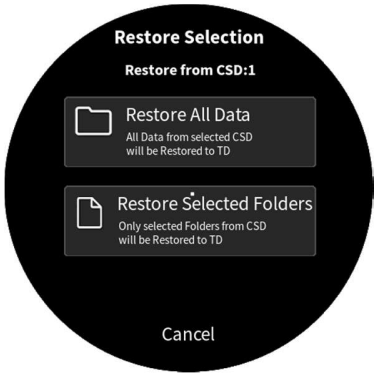
- Select Disk Restore



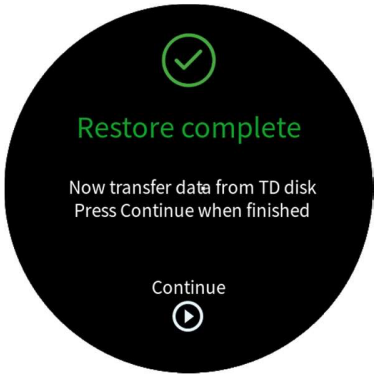
- Choose available Cold Storage



- Select restore type:



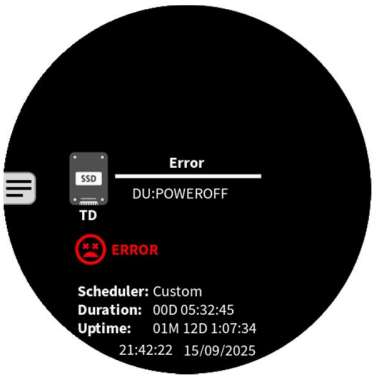
- Restore All data – restores all data from selected cold storage
- Restore Selected Folders, in 2 minutes folder list appear on touchscreen, select one or more folders and click next
- After retrieving data from selected Cold Storage drive, Transitory R/W Unit appears on the connected client's device with recovered data as an external drive
- When Transitory R/W Unit is connected in outside world all Cold Storages turned off
- HB remains in Restore Mode until operator confirm Return to Backup Mode



Returning to Backup Mode:

- Touchscreen command resets time scheduler
- HB resumes the backup procedure
- HB connect to outside world

2.8 Security Lock & Alerts



On critical errors:

- HB stops the backup process
- Buzzer activates
- Screen displays Error, click on error show error message
- Device requires unlock/reset procedure to continue operating
- When someone tries to open HyperBUNKER, the device locks and stops all operations, reactivation of the device with a new license is required

---

2.9 Best Practices

- Always store PIN/password offline and in a safe and secure space
- Test restores at least once a month to confirm backup integrity
- Keep both power supply units connected to separate power circuits
- Monitor and address Cold Storage alerts immediately

2.10 Troubleshooting

- On Error Screen scan QR code and send message to support@hyperbunker.com



---

3. Technical Specifications

- Size - 2U Rackmount
- Storage Capacity - 1TB, 2TB, 4TB
- Storage Type - Flash storage
- Connectivity - USB-C for data transfer, RJ45 for monitoring
- Power Supply - 100-240V AC, 50-60Hz, 2 power supply units
- Cooling System - active cooling, case fans
- Security - air gap isolation, only physical access via touch screen, PIN/passwords as well as separate accounts for User and Admin, tamper detection
- Monitoring & control - monitoring available via web interface if connected, control and monitoring via touch screen
- Supported OS - compatible with all major operating systems
- Operating environment - 10 - 35°C with adequate room for ventilation

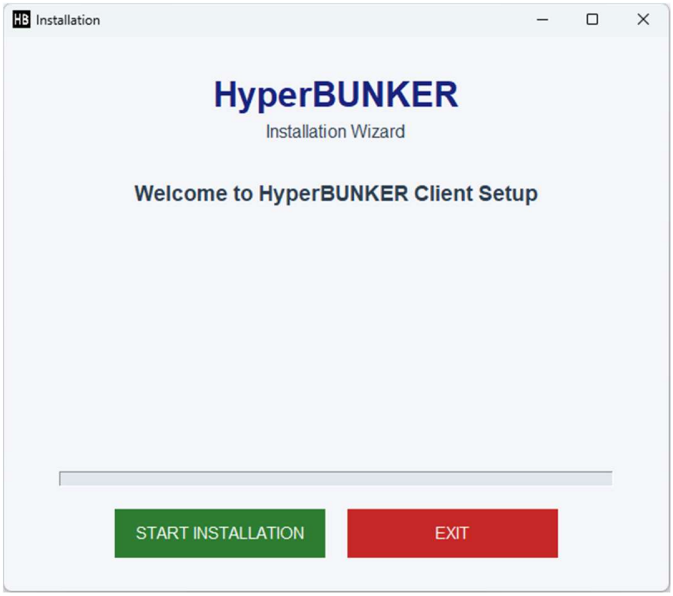
4. Install HyperBUNKER Client

4.1. Windows client

- HyperBUNKER must be connected via USB and in Outside world
- temporarily disable Antivirus, or allow file in Antivirus software as exception
- Run “setup.exe” installation wizard with “Run As Admin”

4.1.1. Installation Wizard Guide

- Click “START INSTALLATION” to begin



- Select or create Repository folder for Critical data
    - Use the "Browse for Folder" button to select or create a repository folder
    - This repository folder will be the location from which HyperBUNKER Client monitors and copies files to Transitory unit
    - Click “Continue” once you have selected your repository folder
    - NOTE: Recommended name for repository folder: PrintUpStair, PrintDownStair, OldPrinter, OldPrinterLogs, PrinterJobArchive, PrinterSysBackup etc…

- Select HyperBUNKER device
    - The installer will display a list of detected drives
    - Each drive will be shown with its drive letter and volume name
    - Select the USB drive that is recognized as connected HyperBUNKER Transitory unit “Transitory HB Disk”

- Enter extension which want to transfer from Repository
    - Use comma-separated format (e.g., *.dat, *.bak, *.zip) for specific file extension
    - Use *.* to transfer all files from repository folder
    - Extensions should be entered with wildcards (*)
    - Examples of valid inputs:
        - *.dat, *.bak, *.bkf, *.zip
        - *.doc, *.docx, *.pdf
        - *.jpg, *.jpeg, *.png, *.gif
        - or any extension that need to be transferred

- Setup finish - The window will automatically close after 20 seconds
- If data already prepared in repository, reconnect HyperBUNKER USB to start backup, otherwise scheduled backup will start next time when HyperBUNKER appears in the outside world

---

4.2. Linux client

- Ensure the Hyper BUNKER is connected via USB, mounted and in Outside world
- Copy installer and make executable
  - copy install_hyperbunker_linux_client.sh
  - chmod +x install_hyperbunker_linux_client.sh
- Run the installer as root or with sudo
  - sudo ./install_hyperbunker_linux_client.sh

4.2.1. Installation Wizard Guide

```
[Step 1/5] Select Repository Folder
Enter the path for your repository folder (This is location from where Hyper BUNKER
take data): e.g. /home/user/repoHyperBUNKER
```

- Repository Folder Selection:
  - Enter the full path where your files will be stored
  - If the folder doesn't exist, the installer will offer to create it
  - This is the folder that HyperBUNKER client will monitor for files to copy

```
[Step 2/5] Select Your HyperBUNKER
Scanning for USB devices...
Available USB devices:
1. /dev/sda1 (900G) UUID=1bbe3057-017e-4d35-ab51-3b0c8a0d991d [test] mounted on
/media/user/test
```

- HyperBUNKER Selection
- Shows all available USB devices with their:
  - Device path
  - Size
  - UUID (unique identifier)
  - Label (if any)
  - Mount point
- Select your device by entering its number

```
[Step 3/5] Enter File Extensions
Enter file extensions you want to mark for transfer (comma-separated, e.g.,
*.dat,*.bak,*.zip or *.* for all): *.*
```

- File Extension Configuration
  - Specify which file types to copy
  - Use comma-separated list (e.g., *.dat,*.bak,*.zip)
  - Use *.* to copy all files
  - Extensions are case-sensitive

```
[Step 4/5] Creating Scripts and Rules
[Step 5/5] Installation Complete
```

- Script and Rule Creation is automatic
  - Creates necessary scripts and udev rules
  - Sets up automatic HyperBUNKER detection
  - Configures copy operations
  - Displays complete configuration summary
- Final message to inform the user the installation is completed

4.3 Common Issues and Solutions Windows client

4.3.1 Repository not created

- If you receive an error about folder creation, verify you have write permissions for the selected location
- If the Continue button remains disabled, ensure you have properly selected a folder
- You can always select a different folder by clicking the "Browse for Folder" button again

4.3.2 HyperBUNKER Transitory unit Not Detected

- Verify the volume name matches the installation configuration
- Try reconnecting the HyperBUNKER device
- Check Windows Device Manager for drive issues
- Repository not created

4.3.3 Files Not Transferring

- Verify the repository folder contains files
- Check that file extensions match the configured patterns
- Review error.log for specific issues

4.3.4 Task Scheduler Issues

- Open Task Scheduler and verify "HyperBunkerCopyTask" is present and enabled
- Check that the task has proper permissions
- Verify the event log "Microsoft-Windows-DriverFrameworks-UserMode/Operational" is enabled

4.4 Common Issues and Solutions Linux client

4.4.1 No USB devices detected

- Ensure the HyperBUNKER is properly connected
- Check if the device is formatted and has a UUID
- Verify the device is mounted

4.4.2 Copy process not starting

- Check if the HyperBUNKER matches the configured UUID
- Verify the repository folder exists
- Check error logs in `/root/.config/hyperbunker/logs/error.log`

4.4.3 Permission issues

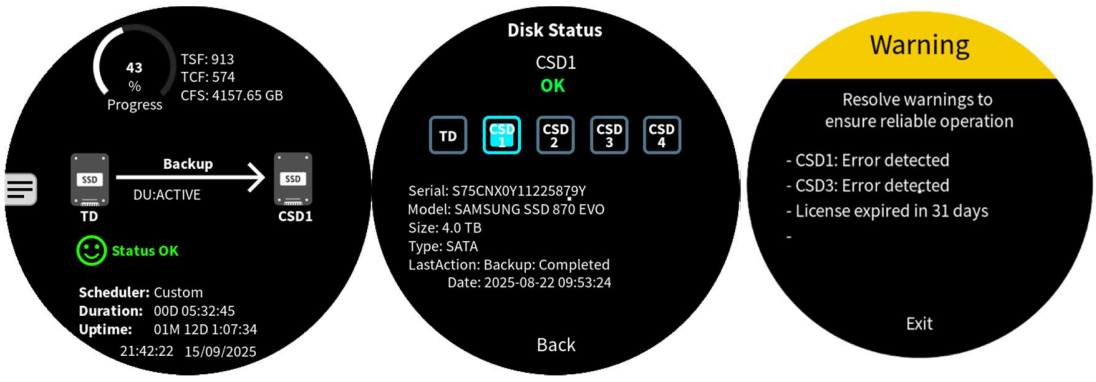
- Ensure the script is run with root privileges
- Check folder permissions in repository directory

---

5 Monitoring system

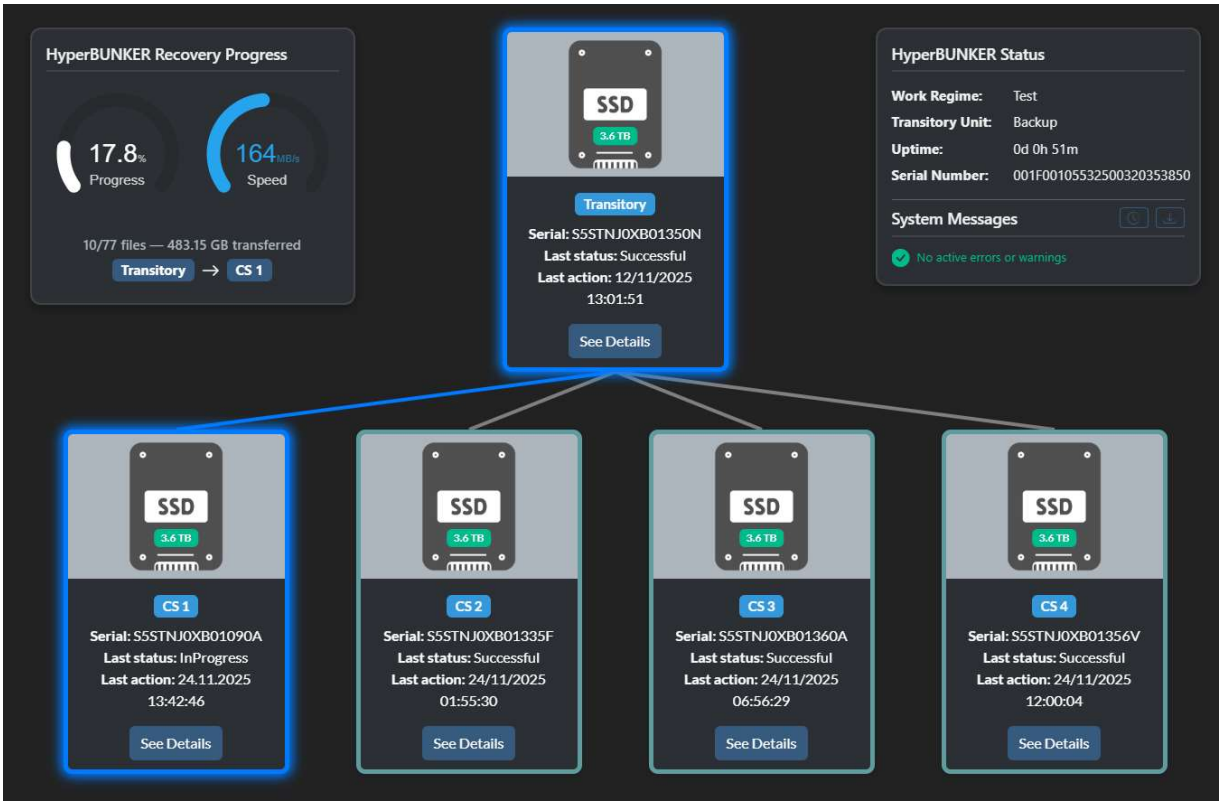
HyperBUNKER have optional 3 levels of Monitoring system

5.1 On screen monitoring

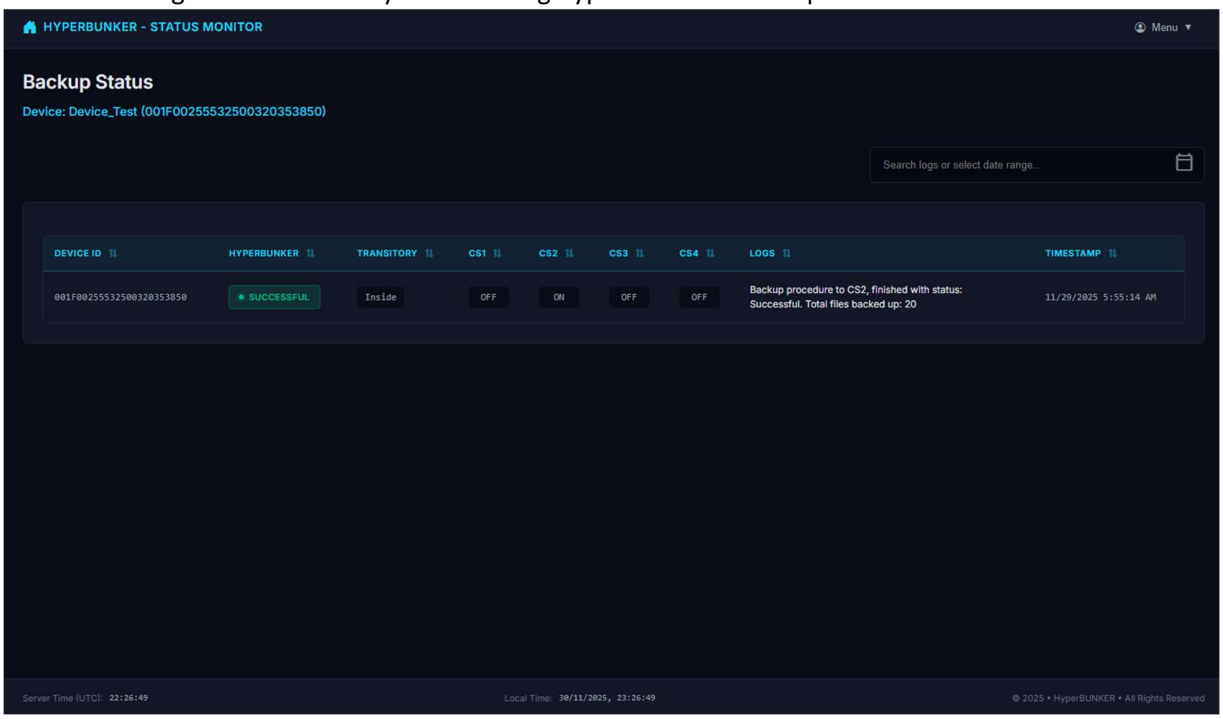


- HyperBUNKER inside or outside world connected
- Backup on which ColdStorage or Restore from which ColdStorage
- Status – number of files, percentage progress of copy and size copied
- Disk informations with last backup status and last backup time on selected Cold Storage
- Warning display with warning info
- Error display with error info

5.2. Local network monitoring



5.3. Monitoring server via API key – monitoring.hyperbunker.com – optional



6 Support

For technical assistance:
Email: support@hyperbunker.com
Website: www.hyperbunker.com

7 Disclaimer of Liability

The manufacturer, developers, and partners of HyperBUNKER disclaim all liability for any loss, damage, data corruption, downtime, business interruption, or other consequences arising directly or indirectly from the use or misuse of this device.

By using HyperBUNKER, the user acknowledges and agrees that:

- The responsibility for securing recovery keys, unlock codes, and passwords lies solely with the user or organization
- The manufacturer is not responsible for failures caused by improper installation, unauthorized modifications, misuse, or failure to follow the instructions provided in this manual
- The manufacturer is not liable for data loss, business interruption, or financial damages, even if advised of the possibility of such damages

Use of HyperBUNKER constitutes acceptance of this disclaimer and recognition that ultimate responsibility for data integrity, system operation, and risk management rests with the user or operating organization.