

SecureNAS[®] CX-40KHD, CX-40KSD and CX-80KSD

Based on Linux ZFS



Before you start

Thank you for purchasing a Ciphertex Data Security® SecureNAS®

Your SecureNAS® is FIPS 140-2 (Level 3) Certified with its proprietary Ciphertex Protect® Encryption Key used for locking/unlocking encrypted volumes. Before setting up your new SecureNAS®, please check the package contents to verify that you have received the items below. Also, make sure you read the safety instructions carefully in order to avoid harming yourself or damaging your SecureNAS®.

	Ciphertex Secure NAS®
	Key (2) 
	Power Cable 
	Network Cable (2) 
	Ciphertex Protect® Encryption Key (2) 

Ciphertex SecureNAS® at a Glance



No.	Article Name	Description
A	Durable Handle	Unique portability feature
B	Power Button	Turns on/off device
C	LED Indicators	Monitor system status
D	LCD Display	Review SecureNAS settings
E	Key Lock	Locks/unlocks secure door
F	ESC Button	Returns to previous screen
G	Enter/Arrow Buttons	Navigates LCD display
H	Copy Button	Initiates One-Touch Copy
I	USB (Type-C Ports)	Connect peripheral devices
J	Drive Trays	Stores HDDs or SSDs
K	PCIe Extension	Available PCI Expansion Slot

No.	Article Name	Description
L	PCIe Extension	Available PCI Expansion Slot
M	DB15 Port	Connects device to computer
N	Cooling Fan	Prevents overheating
O	10GbE SFP+ Ports	Connects copper network cables
P	10G Ethernet Ports (4)	Connects fiber network cables
Q	RJ-45 Gigabit LAN	Power and data connection
R	USB 3.0 (Type-A Ports)	Type-A Ports
S	IPMI Port	For maintenance-use only
T	Power Connector	AC-line

All product specifications and data are subject to change without notice to improve security, reliability, function, design or otherwise.

(Optional)
SecureNAS®
Quick-Link
cable



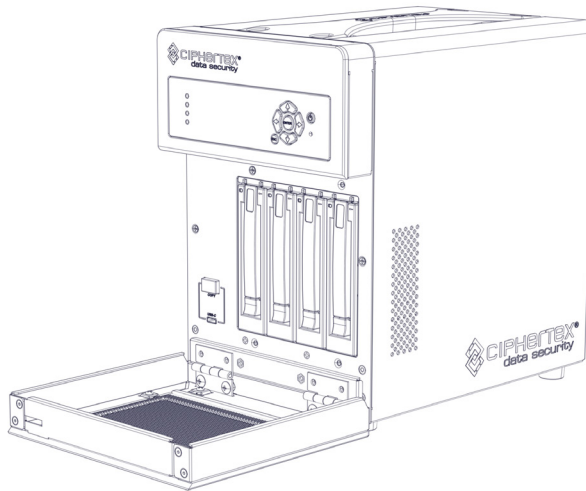
Ciphertex SecureNAS® Quick-Link (Optional)

- Easily connect your SecureNAS to any Windows, Mac, or Linux computer via a fast USB-3 connection
- Maintains all the same access as standard Ethernet without the hassles of setting up a formal network.
- Perfect for AD-HOC connections in the field or at the office
- Supports up to 10 computers when using the optional USB-3 add-in boards and cables

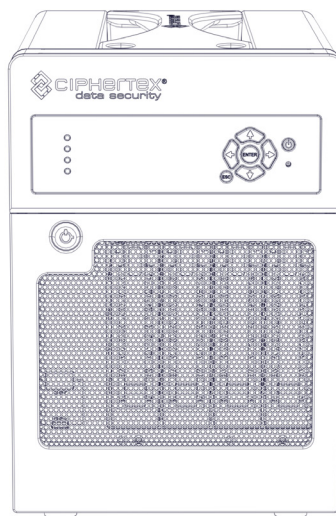
Hardware Design

Remove/Install Drives

1. Press the lower part of the drive trays to pop out the handle.



2. Pull the drive tray handles in the direction as indicated below to remove the respective drive tray (s).



Installing SecureNAS®

Starting/Shutting Down the SecureNAS®

1. Plug your Ciphertex SecureNAS® into AC power.
2. Connect to the network. Plug network cable into a **network port** (top right). Left for static IP, right for DHCP.
3. Press the power button on the front of the unit to power it on and start the boot process.
4. To shut down the unit, simply press the power button and the unit will begin the shutdown process.
5. If necessary, you can also press and hold the power button for at least 5 seconds to force the power off without going through the shutdown process.



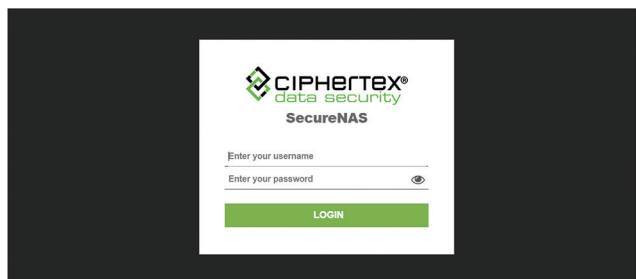
NOTE: Holding down the power button should **NOT** be done for expedience. Only force the power off in instances where SecureNAS® is unresponsive to the normal shutdown process. commands should you force a power off.

Obtaining an IP Address

1. During boot, your SecureNAS® will automatically obtain network information from a DHCP server if you plugged into the connector on the right. If you do not have a DHCP server and you plugged into the connector on the left, your SecureNAS® will default to the IP address 192.168.1.200.
2. After SecureNAS® obtains an IP address, the address will be displayed on the LCD screen on the front of the unit.

Logging in to the SecureNAS®

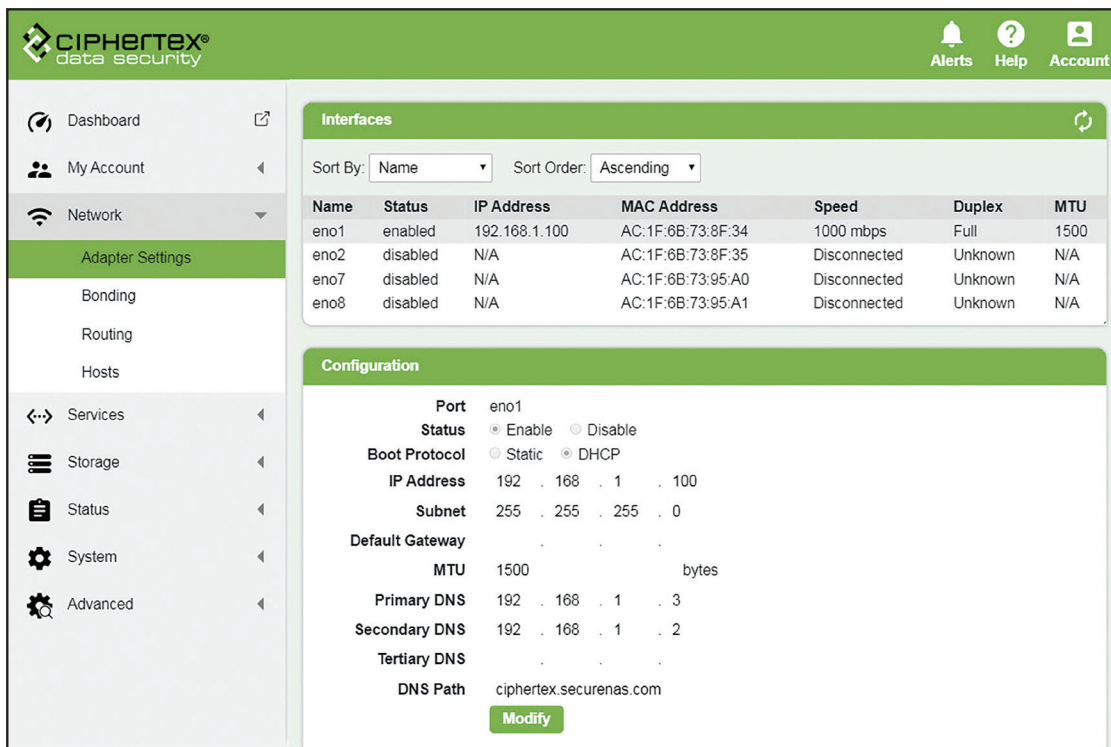
1. On a computer, use a web browser to connect to your SecureNAS®. In the address bar of the web browser, type `http://ip_address` (type in the unit's ip address in place of "ip_address").
2. You will be directed to the SecureNAS® login screen. Here, enter the default username and password of the built-in administrator account. For a new machine, the default username is "administrator" and the password is "password". Then press the LOGIN button.



3. Once you have logged in, you will see basic system information on the SecureNAS® dashboard.

Setting Up A Network

1. On the left-side of the screen, click on the Network menu item to expand the options.
2. Then select Adapter Settings under Network.



Interfaces

Sort By: Sort Order:

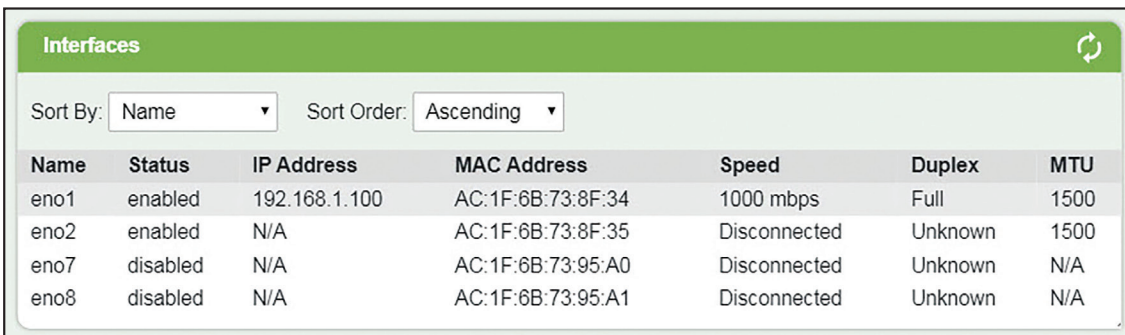
Name	Status	IP Address	MAC Address	Speed	Duplex	MTU
eno1	enabled	192.168.1.100	AC:1F:6B:73:8F:34	1000 mbps	Full	1500
eno2	disabled	N/A	AC:1F:6B:73:8F:35	Disconnected	Unknown	N/A
eno7	disabled	N/A	AC:1F:6B:73:95:A0	Disconnected	Unknown	N/A
eno8	disabled	N/A	AC:1F:6B:73:95:A1	Disconnected	Unknown	N/A

Configuration

Port: eno1
 Status: Enable Disable
 Boot Protocol: Static DHCP
 IP Address: 192 . 168 . 1 . 100
 Subnet: 255 . 255 . 255 . 0
 Default Gateway:
 MTU: 1500 bytes
 Primary DNS: 192 . 168 . 1 . 3
 Secondary DNS: 192 . 168 . 1 . 2
 Tertiary DNS:
 DNS Path: ciphertex.securenas.com

[Modify](#)

3. On the Adapter Settings page, select "eno1" from the Interfaces list. This will populate the Configuration information at the bottom of the page.



Interfaces

Sort By: Sort Order:

Name	Status	IP Address	MAC Address	Speed	Duplex	MTU
eno1	enabled	192.168.1.100	AC:1F:6B:73:8F:34	1000 mbps	Full	1500
eno2	enabled	N/A	AC:1F:6B:73:8F:35	Disconnected	Unknown	1500
eno7	disabled	N/A	AC:1F:6B:73:95:A0	Disconnected	Unknown	N/A
eno8	disabled	N/A	AC:1F:6B:73:95:A1	Disconnected	Unknown	N/A

4. After you have selected eno1 and the information is displayed in the Configuration area, click the Modify button.

Configuration

Port	eno1
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Boot Protocol	<input type="radio"/> Static <input checked="" type="radio"/> DHCP
IP Address	192 . 168 . 1 . 100
Subnet	255 . 255 . 255 . 0
Default Gateway
MTU	1500 bytes
Primary DNS	192 . 168 . 1 . 3
Secondary DNS	192 . 168 . 1 . 2
Tertiary DNS
DNS Path	ciphertex.securenas.com

[Modify](#)

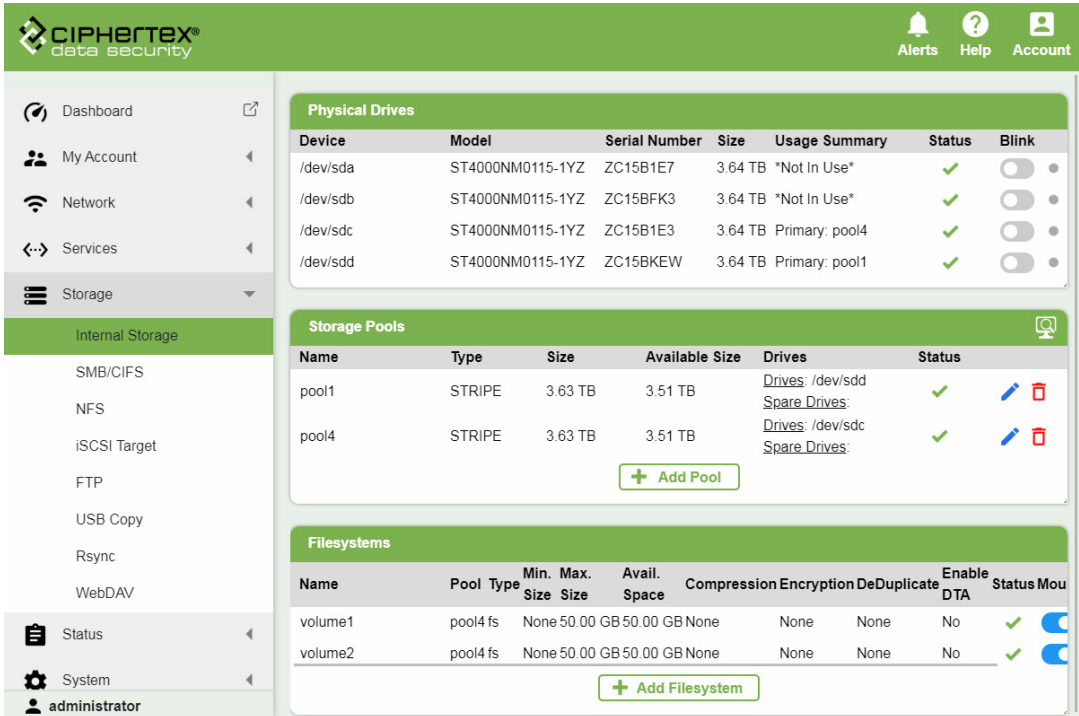
5. Fill out the configuration for eno1 for your network.
6. Click the Apply button when you have made the necessary configuration changes.

NOTE: Changes to network settings will require a system reboot.

Configuring Storage

Before taking advantage of the various features of SecureNAS, you need to set up at least one storage space. This section explains how to use the SecureNAS Management Console to configure and manage internal storage.

Storage Pools and Volumes



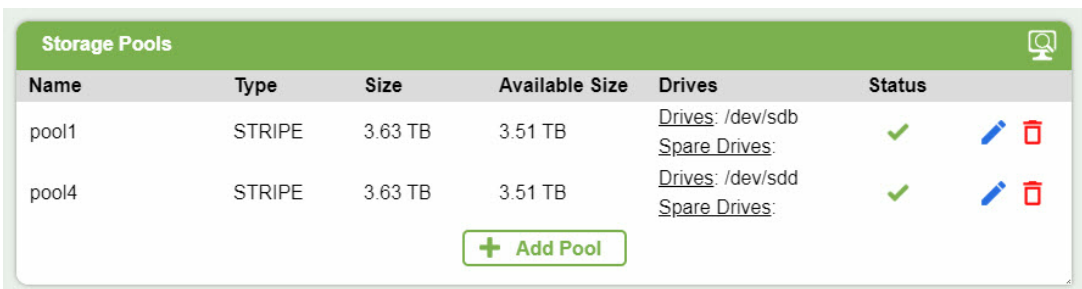
The screenshot shows the CIPHERTEX Management Console interface. The left sidebar contains navigation options: Dashboard, My Account, Network, Services, Storage (expanded to Internal Storage), Status, and System. The main content area is divided into three sections:

- Physical Drives:** A table listing four drives (sda, sdb, sdc, sdd) with columns for Device, Model, Serial Number, Size, Usage Summary, Status, and Blink. All drives are 3.64 TB and have a status of 'Not In Use' or are part of a pool.
- Storage Pools:** A table listing two pools (pool1, pool4) with columns for Name, Type, Size, Available Size, Drives, and Status. Both pools are STRIPE type, 3.63 TB size, and 3.51 TB available. Pool1 uses /dev/sdd and pool4 uses /dev/sdc.
- Filesystems:** A table listing two volumes (volume1, volume2) with columns for Name, Pool Type, Min. Size, Max. Size, Avail. Space, Compression, Encryption, DeDuplicate, Enable DTA, and Status. Both volumes are pool4 fs, 50.00 GB min/max, 50.00 GB avail, and have no compression, encryption, or deduplication.

Select the page under the Storage > Internal Storage menu item to configure storage pools and volumes. A volume is the basic storage space on your SecureNAS unit. A volume is created on a storage pool. Before creating a volume you must first create a storage pool.

Create Storage Pools

1. On the Internal Storage page in the Storage Pools section, click the **+ Add Pool** button to create a storage pool.



This close-up screenshot shows the Storage Pools table with two rows (pool1 and pool4) and a '+ Add Pool' button at the bottom. The table columns are Name, Type, Size, Available Size, Drives, and Status. Pool1 uses /dev/sdb and pool4 uses /dev/sdd.

2. On the Add Pool pop-up, fill in the following information and then click the Add button:

Add Pool

Pool Name:

Select Protection Level:

- None - STRIPE
- Mirror - MIRROR
- Single parity - RAIDZ-1
- Double parity - RAIDZ-2
- Triple parity - RAIDZ-3
- Striped mirror - STRIPED-MIRROR

Select Drives To Use:

/dev/sda (Size: 5.46 TB SN: ZAD9ERLA)
 /dev/sdb (Size: 5.46 TB SN: ZAD9E8TZ)
 /dev/sdc (Size: 5.46 TB SN: ZAD9FB2E)
 /dev/sdd (Size: 5.46 TB SN: ZAD9EMSE)

/dev/sda (Size: 5.46 TB SN: ZAD9ERLA)
 /dev/sdb (Size: 5.46 TB SN: ZAD9E8TZ)
 /dev/sdc (Size: 5.46 TB SN: ZAD9FB2E)
 /dev/sdd (Size: 5.46 TB SN: ZAD9EMSE)

Select Spare Drives:

/dev/sda (Size: 5.46 TB SN: ZAD9ERLA)
 /dev/sdb (Size: 5.46 TB SN: ZAD9E8TZ)
 /dev/sdc (Size: 5.46 TB SN: ZAD9FB2E)
 /dev/sdd (Size: 5.46 TB SN: ZAD9EMSE)

/dev/sda (Size: 5.46 TB SN: ZAD9ERLA)
 /dev/sdb (Size: 5.46 TB SN: ZAD9E8TZ)
 /dev/sdc (Size: 5.46 TB SN: ZAD9FB2E)
 /dev/sdd (Size: 5.46 TB SN: ZAD9EMSE)

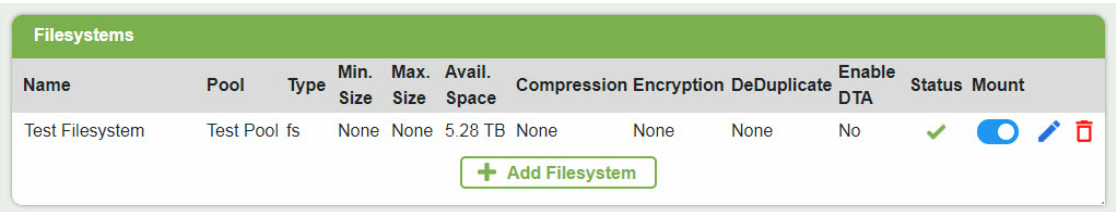
Pool Name	<p>The name for the storage pool that is being added. The only special characters allowed are hyphens(-) and periods(.). No spaces are allowed.</p> <p>Each pool name must be unique.</p>
Select Protection Level	<p>Select from the following:</p> <ul style="list-style-type: none"> None - STRIPE: The pool is configured for maximum speed, not to provide data protection. Any drive failure will result in data loss. Mirror - MIRROR: Data is striped across two mirrors. This type of RAID offers the best

	<p>performance for small random reads and writes.</p> <ul style="list-style-type: none"> • Single parity - RAIDZ-1: Data is striped across multiple single parity arrays, which can tolerate one drive failure without data loss. This type of RAID has faster performance than double and triple parity based RAIDs. • Double parity - RAIDZ-2: Data is striped across multiple double parity arrays, which can tolerate two drive failures without data loss. In most cases, double parity provides the best balance between data protection, performance, and storage capacity. • Triple parity - RAIDZ-3: Data is striped across multiple triple parity arrays, which can tolerate three drive failures without data loss. This type of RAID provides the maximum data protection. • Striped mirror - STRIPED-MIRROR: Data is protected by combining disk mirroring and disk striping, which can tolerate failure as long as one disk in each mirrored pair is functional. This requires a minimum of four disks and striped data across mirrored pairs.
Select Drives to Use	Select the drives to include in the storage pool.
Select Spare Drives	Select the drives to be used as spares. You can select any drives that are not currently in a storage pool.

Volumes/Filesystems

Create Filesystems

1. On the Internal Storage page in the Filesystems section, click the Add Filesystem button to create a filesystem.



Name	Pool	Type	Min. Size	Max. Size	Avail. Space	Compression	Encryption	DeDuplicate	Enable DTA	Status	Mount
Test Filesystem	Test Pool	fs	None	None	5.28 TB	None	None	None	No	✓	

[+ Add Filesystem](#)

2. On the Add Filesystem pop-up, fill in the following information and then click the Add button:

Add Filesystem

Name:	<input style="width: 95%;" type="text"/>
Pool:	Test Pool (5.28 TB) ▼
Type:	Filesystem ▼
Minimum Size:	No Minimum ▼
Maximum Size:	No Maximum ▼
Compression:	off ▼
Encryption:	off ▼
DeDuplicate:	off ▼
Enable DTA:	<input type="checkbox"/>

Add
Cancel

Name	<p>The name for the filesystem being added. The only special characters allowed are hyphens (-) and periods (.). No spaces are allowed.</p> <p>Each filesystem name must be unique.</p>
Pool	<p>Select from the available storage pools that are configured on your SecureNAS system.</p>
Type	<p>Select from:</p> <ul style="list-style-type: none"> • Filesystem • Raw

Minimum Size	Select the minimum size to be used for the filesystem: <ul style="list-style-type: none">• No Minimum• Max Size• Custom: Enter a size in the textbox. Then select the units (i.e. GB, TB, etc.). Note: This option is only available when type Filesystem is selected.
Maximum Size	Select the maximum size to be used for the filesystem: <ul style="list-style-type: none">• No Maximum• Max Size• Custom: Enter a size in the textbox. Then select the units (i.e. GB, TB, etc.). Note: This option is only available when type Filesystem is selected.
Size	Enter a size in the textbox. Then select the units (i.e. GB, TB, etc.). Note: This option is only available when type Raw is selected.
Compression	Choose from the options: <ul style="list-style-type: none">• off• lzjb• gzip-1• gzip-2• gzip-3• gzip-4• gzip-5• gzip-6• gzip-7• gzip-8• gzip-9• zle• lz4

Encryption	Choose from the options: <ul style="list-style-type: none">• off• aes-128-ccm• aes-192-ccm• aes-256-ccm• aes-128-gcm• aes-192-gcm• aes-256-gcm
DeDuplicate	Choose from the options: <ul style="list-style-type: none">• off• sha256• sha256-verify• sha512• sha512-verify• skein• skein-verify• edonr• edonr-verify
Enable DTA	Enable/Disable date time access timestamp tracking.

Mount a Filesystem

1. On the Internal Storage page in the Filesystems section, select the filesystem you want to mount. This will highlight the row. Then click on the toggle switch to mount the filesystem.

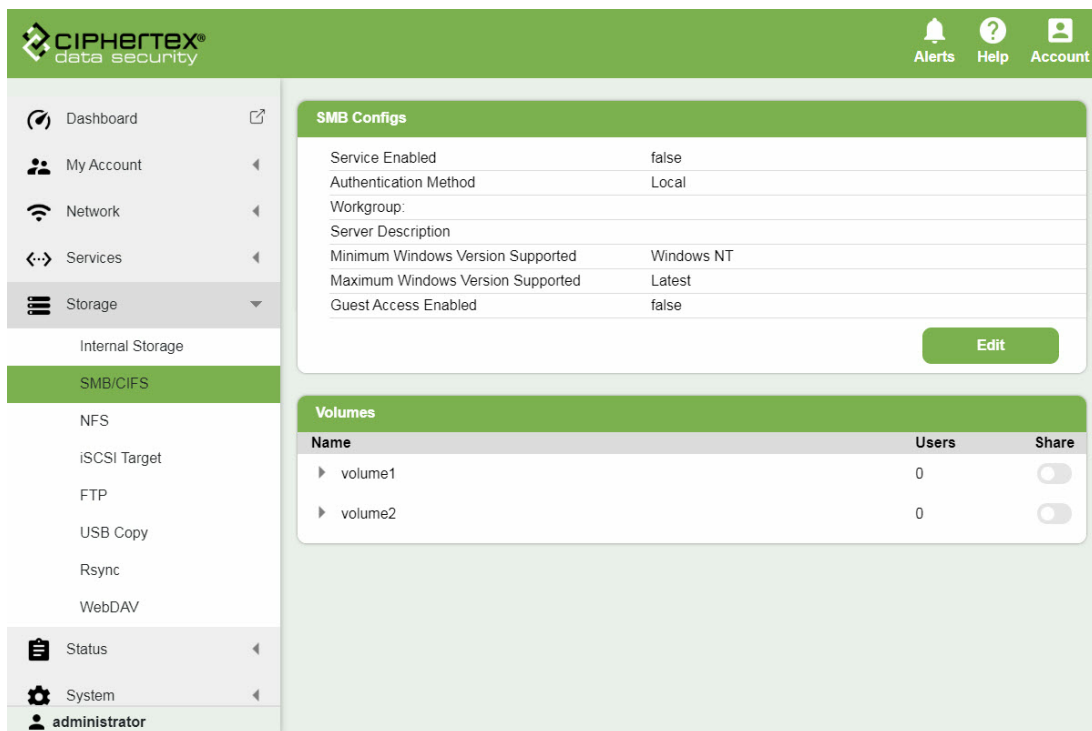
Note:

- To mount a filesystem that is encrypted with a SecureNAS Ciphertex Protect® Encryption Key, you must first unlock and then insert the SecureNAS Ciphertex Protect® Encryption Key in the SecureNAS unit.

SMB/CIFS

Configure SMB/CIFS

Select the page under the Storage > SMB/CIFS to configure settings for sharing volumes via SMB/CIFS.



The screenshot shows the CIPHERTEX web interface. The left sidebar contains navigation options: Dashboard, My Account, Network, Services, Storage (expanded), Internal Storage, SMB/CIFS (selected), NFS, iSCSI Target, FTP, USB Copy, Rsync, WebDAV, Status, System, and administrator. The main content area is titled 'SMB Configs' and contains a table with the following settings:

Service Enabled	false
Authentication Method	Local
Workgroup:	
Server Description	
Minimum Windows Version Supported	Windows NT
Maximum Windows Version Supported	Latest
Guest Access Enabled	false

An 'Edit' button is located at the bottom right of the SMB Configs section. Below this is a 'Volumes' section with a table:

Name	Users	Share
▶ volume1	0	<input type="checkbox"/>
▶ volume2	0	<input type="checkbox"/>

1. On the SMB/CIFS page in the SMB Configs section, click the Edit button to enable SMB/CIFS and modify the SMB configuration.
2. On the Modify SMB Configs pop-up, fill in the following information and then click the OK button:

Modify SMB Conigs

Service Enabled:


Authentication Method: Local Active Directory

Workgroup:

Server Description:

Minimum Windows Version Supported: Windows NT Windows Vista Windows 7
 Windows 8 Latest

Maximum Windows Version Supported: Windows NT Windows Vista Windows 7
 Windows 8 Latest

Enable Guest Access: 

Modify SMB Conigs

Service Enabled:

Authentication Method: Local Active Directory

Domain/Realm:

Domain Username:


Domain Password:

Confirm Domain Password:

Server Description:

Minimum Windows Version Supported: Windows NT Windows Vista Windows 7
 Windows 8 Latest


Maximum Windows Version Supported: Windows NT Windows Vista Windows 7
 Windows 8 Latest


Enable Guest Access: 

Service Enabled	Select this option to enable SMB/CIFS sharing.
Authentication Method	<p>Choose either Local or Active Directory.</p> <p>Local: Allow local users added in the SecureNAS Management Console to access the shares.</p> <p>Active Directory: Use your Active Directory to control access to the shares.</p>
Workgroup	<p>The name of the workgroup that the shares will show up with are grouped together.</p> <p>Optional.</p> <p>Note: This option is only available when the Authentication Method Local is selected.</p>
Domain/Realm	<p>The Active Directory domain or realm that will be joined.</p> <p>Note: This option is only available when the Authentication Method Active Directory is selected.</p>
Domain Username	<p>The Windows user account that will be used to authenticate with Active Directory to determine if SecureNAS has permission to join the domain.</p> <p>Note: This option is only available when the Authentication Method Active Directory is selected.</p>
Domain Password	<p>The password for the Windows user account that will be used to authenticate with Active Directory.</p> <p>Note: This option is only available when the Authentication Method Active Directory is selected.</p>
Confirm Domain Password	<p>Re-type the password for the Windows user account that will be used to authenticate with Active Directory.</p> <p>Note: This option is only available when the Authentication Method Active Directory is selected.</p>
Server Description	<p>Similar to server name, this is how SecureNAS will appear in your Local Networks.</p>
Minimum Windows Version Supported	<p>The earliest Windows version with which the share is to be compatible. Choose from:</p> <ul style="list-style-type: none"> • Windows NT

	<ul style="list-style-type: none"> • Windows Vista • Windows 7 • Windows 8 • Latest
Maximum Windows Version Supported	<p>The latest Windows version with which the share is to be compatible. Choose from:</p> <ul style="list-style-type: none"> • Windows NT • Windows Vista • Windows 7 • Windows 8 • Latest
Enable Guest Access	<p>Enabling this option will allow anyone to see the names of browsable shares.</p>

Choose Volumes to Share via SMB/CIFS

1. On the SMB/CIFS page in the Volumes section, find the volume that you want to share.
2. To share a volume via SMB/CIFS, click on the toggle switch  under the heading Share. When the switch is blue and positioned to the right, the volume is shared.

Volumes		
Name	Users	Share
▶ volume1	1	

Configure Volumes for SMB/CIFS

1. On the SMB/CIFS page in the Volumes section, select the volume that you want to share. This will expand the volume information.
2. Configure the volume according to the instructions below.
3. Click the Update button to save the changes and update the volume.

SMB/CIFS Volume Accounts

1. On the SMB/CIFS page in the Volumes section, select the volume that you want to share. This will expand the volume information.
2. Configure the volume according to the instructions below.
3. Click the Update button to save the changes and update the volume.

SecureNAS® Quick-Link

(Optional Accessory)

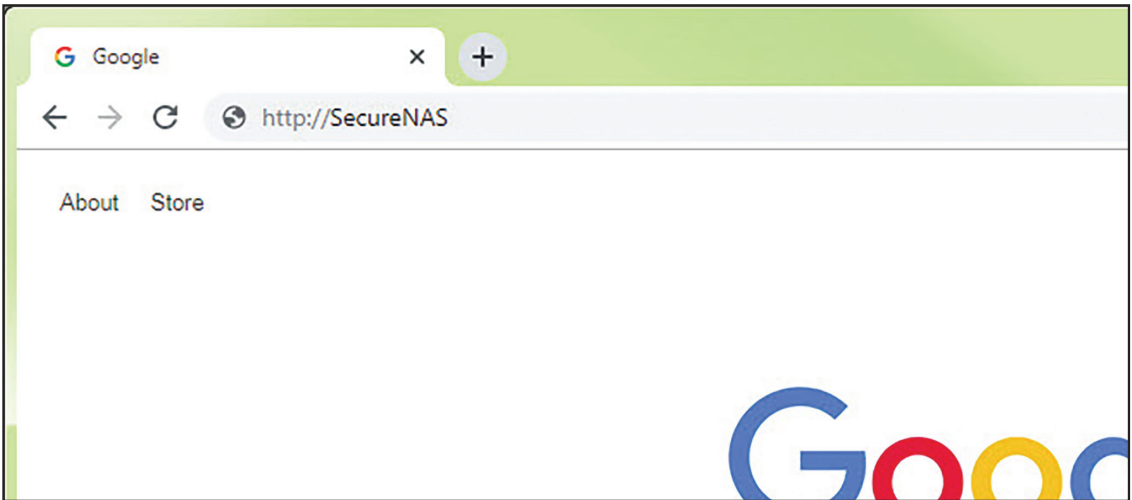
Setup

1. Take the SecureNas® Quick-Link cable and plug one end into any of the rear USB ports of the SecureNAS®. Plug the other end of the Quick-Link cable into any available USB port of your computer.
2. If you are using a Windows 10 computer, the necessary drivers will automatically be installed when the cable is connected.
 - a. For older versions of Windows, you will need to manually install the necessary driver.
3. Your SecureNAS® unit is now connected.



Manage SecureNAS®

1. To access the Management Console for the SecureNAS® unit, open a web browser on your computer and navigate to `http://<server_name>`.

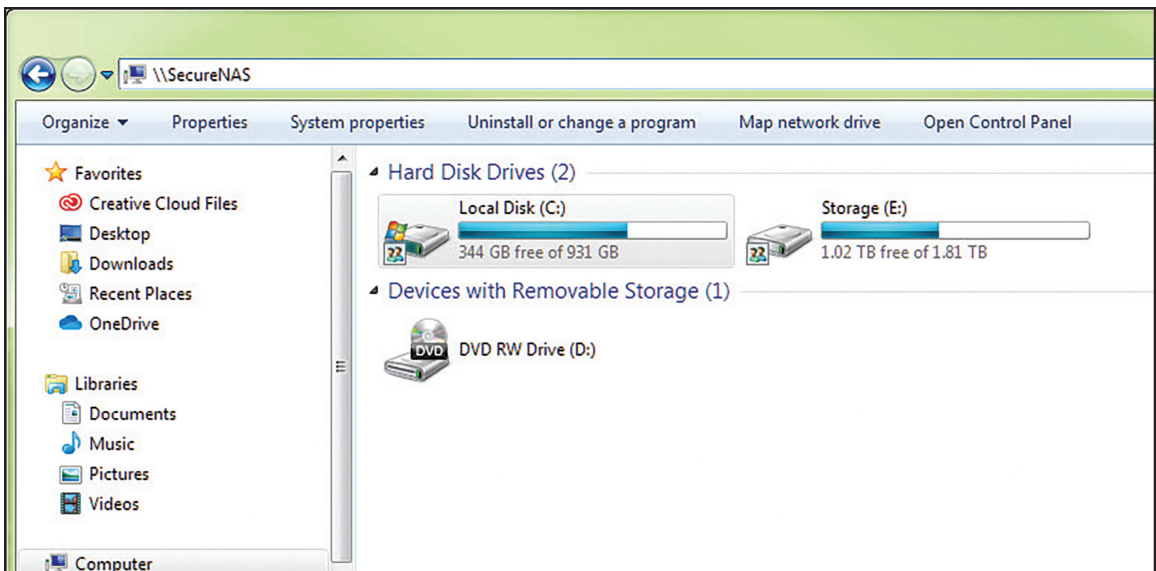


- a. Replace `<server_name>` with the name that appears on the front LCD screen of the SecureNAS® unit.
 - b. The server name automatically resolves to the correct IP Address.
2. You will be directed to the login screen for the SecureNAS® Management Console web UI.



Access Shares

1. First, you must configure shares on SecureNAS® using the Management Console.
2. To access shares via the SecureNAS® Quick-Link, open a file explorer on your computer and type \\<server_name> in the file explorer browser bar. Hit enter.
 - a. (Replace <server_name> with the name that appears on the front LCD screen of the SecureNAS® unit.)
 - b. The server name automatically resolves to the correct IP Address.



3. The SecureNAS® shared filesystems will be displayed in the file browser.



Ciphertex Protect® Encryption Key

Serial Number	Description	Status	Paired	Unlocked
10003354	John Smith key	✓	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
20000001	Fred Jottenhymer issued 2019-12-30	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>
31001133	Joan's key	✓	<input checked="" type="checkbox"/>	<input type="checkbox"/>
45451122	---	⚠	<input type="checkbox"/>	<input type="checkbox"/>
65827112	---	✓	<input type="checkbox"/>	<input type="checkbox"/>
69754121	Guest key from last week	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>
77000001	---	✓	<input type="checkbox"/>	<input type="checkbox"/>

Select the page under the **System > Protect Key** menu item to configure a Ciphertex Protect® Key to be used with the SecureNAS. At least one Protect Key must be paired and unlocked with a SecureNAS unit to allow use of secure encrypted storage.

The SecureNAS with Protect Key delivers FIPS 140-2 Level 3 validated, AES-256 compliance. The Protect Key protects sensitive data while at rest by preventing unauthorized access. It provides security and reliability without impacting drive performance.








WARNING!

IMPORTANT: It is very important that you always keep a paired Protect Key in a safe location and store the password for it in a known and safe location. If you render all of your paired Protect Key inoperable, you will lose access to all encrypted data on the Secure NAS. There is no way to recover from this situation.



STATUS OF A PROTECT KEY



A Protect Key entry can display three different statuses:

-  : The Protect Key is currently plugged into a USB port on the SecureNAS unit and connected to the system.
-  : The Protect Key is not plugged into a USB port on the SecureNAS unit.
-  : The Protect Key is currently plugged into a USB port on the SecureNAS unit, but has trouble and cannot be used.
-  : The Protect Key is currently plugged into a USB port on the SecureNAS unit, but is blocked due to exceeding incorrect password attempts.
-  : The Protect Key is currently plugged into a USB port on the SecureNAS unit, but might be currently paired to another SecureNAS unit.

Note:

- Do not attempt to use third-part applications to manipulate the configuration of the Protect Key. Doing so may render the Protect Key inoperable.
- When a Protect Key has been rendered inoperable, it can be removed from the system key list and then added back in as a new key assuming you have at least one paired Protect Key that can be unlocked.
- In order to create an encrypted filesystem, a Protect Key must be connected to a USB port on the SecureNAS unit, paired with the system, and unlocked.
- In order to mount an encrypted filesystem, a Protect Key must be connected to a USB port on the SecureNAS unit, paired with the system, and unlocked.
- Once you have mounted an encrypted filesystem, you can disconnect the Protect Key from the USB port and the filesystem will still be accessible.
- After the SecureNAS has been restarted, all encrypted filesystems will be unmounted. A Protect Key must be used to mount the filesystems for use.
- After the SecureNAS has been restarted, any inserted Protect Key will automatically be locked.
- Any Protect Key that has been disconnected from a USB port will be automatically locked.
- In order to pair additional keys to the NAS, a paired and unlocked key must be in the NAS.

CONFIGURE A PROTECT KEY FOR USE WITH SECURENAS

1. Insert a Protect Key into a USB port on the SecureNAS unit.
2. The Protect Key serial number will show up in the table on the **Protect Key** page
3. Ensure that there is a green check mark  under **Status** and that both the **Paired** and **Unlocked** toggle switches  are off.

4. Next, click on the **Paired** toggle switch for the Protect Key.
5. In the Pair Protect Key pop-op, fill out the following information and then click the **Pair** button.

Pair Protect Key

Serial Number	<input type="text" value="65827112"/>
Protect Key Password	<input style="width: 100%;" type="password"/>
Description	<input style="width: 100%;" type="text"/>
Override Pairing	<input type="checkbox"/>

Serial Number	The serial number for the selected Protect Key. This value is provided by the system and is not modifiable.
Protect Key Password	<p>The password to be used to unlock the Protect Key once connected to the SecureNAS unit. This password serves as a second factor of authentication when using your Protect Key for encryption.</p> <p>A password must be exactly 8 characters and only contain a-z, A-Z, 0-9, !, \$, #, %. No spaces are allowed.</p>
Description	<p>A description for the Protect Key. This is for informational purposes only.</p> <p>Optional. If the Description is left blank, it will be auto-filled with the date and time that the Protect Key was paired with the system.</p>
Override Pairing	If this option is selected, the Protect Key will be paired to this SecureNAS unit and will be unpaired

	<p>from the other SecureNAS unit that it is currently paired to.</p> <p>This option is only available when the Protect Key is currently paired to a different SecureNAS unit.</p> <p>Note: This will unpair the selected Protect Key from any other SecureNAS unit. If this Protect Key is the only key on the other SecureNAS unit, do Not override the pairing. This will make all data on the other Secure Nas unit unrecoverable.</p>
--	---

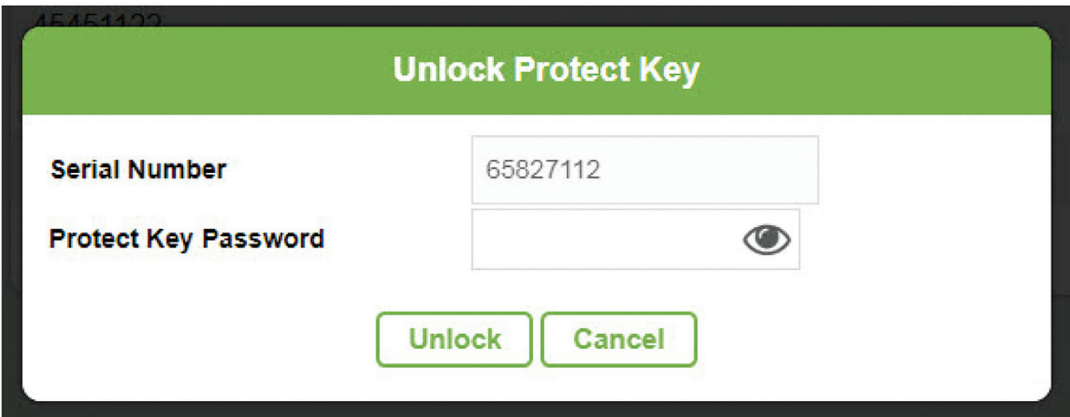
6. The Protect Key is now added to the system.

Note:

- You must have at least one unlocked Protect Key in order to create new encrypted filesystems and to mount encrypted filesystems.
- A Protect Key must be Unlocked for it to be used to create new encrypted filesystems and to mount an encrypted filesytem.

1. To unlock a paired Protect Key, click on the Unlocked toggle switch for the Protect Key.

2. In the Unlock Protect Key pop-up, fill out the following information and then click the Unlock button:



Serial Number	The serial number for the selected Protect Key. This value is provided by the system and is not modifiable.
---------------	---



Protect Key Password

The password that was chosen and entered when the Protect Key was paired with the SecureNAS unit.

When entering your password to unlock the Protect Key, you will have 5 tries to enter the correct password. If you fail 5 times consecutively, the Protect Key will be rendered unusable. When a correct password is entered, the error retry count is always set back to 5 tries.

LOCK A PROTECT KEY



Note:

- Locking a Protect Key prevents its use with the SecureNAS unit.
- Disconnecting a Protect Key from a USB port will automatically lock it.
- A Protect Key can remain inserted into a USB port while it is locked

1. Click on the Unlocked toggle switch for the Protect Key to move the toggle switch into the "off" position



UNPAIR A PROTECT KEY



Note:

- The Unpair Protect Key Operation cannot be undone. Once the Protect Key has been unpaired, it will not be usable with the SecureNAS unit unless it is paired again with a new password.
- To Unpair, the Protect Key does not need to be plugged into a USB port on the SecureNAS unit.

2. Click on the **Paired** toggle switch for the Protect Key.
3. In the pop-up, enter your login password and click the **Unpair** button.

Apply Firewall Rules

SecureNAS has a built-in firewall that can be enabled to further protect your system from internet threats.

1. From the menu on the left, select **Services > Firewall**.
2. On the Firewall page select the **Enable Firewall** checkbox.
3. Click the **Apply** button to apply these changes.

Model and Part Numbers

Model: SecureNAS® CX-40KHD

- P/N: SNCX40KH-32G-16T = 16TB
- P/N: SNCX40KH-32G-32T = 32TB
- P/N: SNCX40KH-32G-40T = 40TB
- P/N: SNCX40KH-32G-48T = 48TB
- P/N: SNCX40KH-32G-64T = 64TB
- P/N: SNCX40KH-32G-72T = 72TB

Model: SecureNAS® CX-40KSD

- P/N: SNCX-40KS-32G-4T = 4TB
- P/N: SNCX-40KS-32G-8T = 8TB
- P/N: SNCX-40KS-32G-15T = 15TB
- P/N: SNCX-40KS-32G-30T = 30TB
- P/N: SNCX-40KS-32G-60T = 60TB

Model: SecureNAS® CX-80KSD

- P/N: SNCX-80KS-32G-8T = 8TB
- P/N: SNCX-80KS-32G-15T = 15TB
- P/N: SNCX-80KS-32G-30T = 30TB
- P/N: SNCX-80KS-32G-60T = 60TB

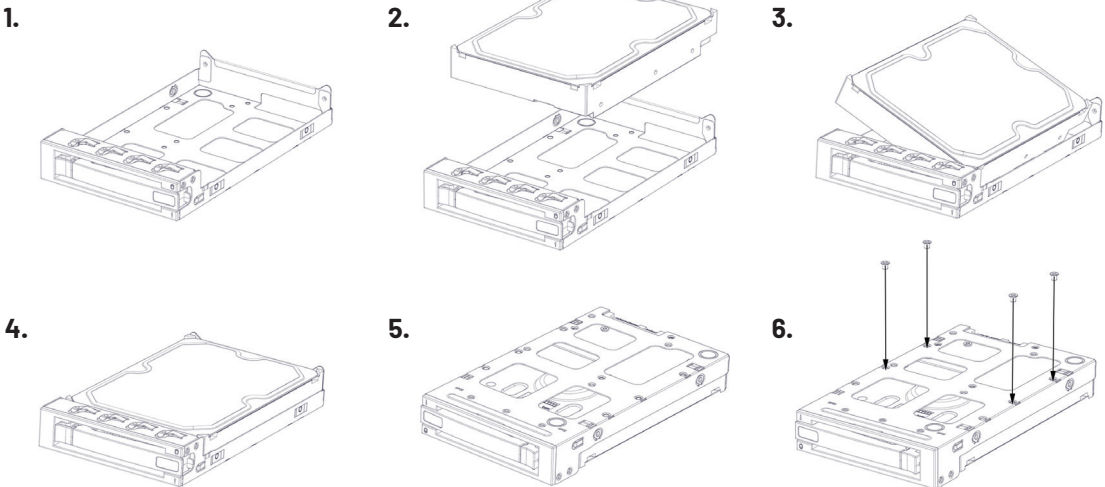
With optional Copper NIC append to Part Number

- -10G2 for 10Gbps 2 Port
- -10G4 for 10Gbps 2 Port
- -40G for 40 Gbps
- -50G for 50 Gbps

EXAMPLE:

A 16TB SecureNAS CX40KHD with a 10G Copper 2 Port Add-on is P/N: SNCX40KH-32G-16T-10G2

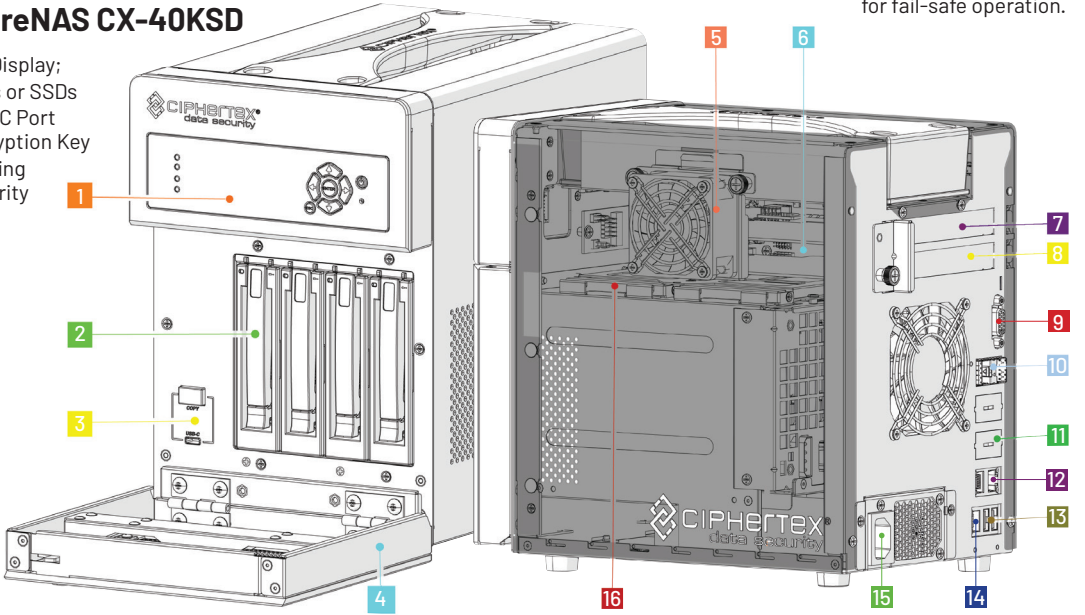
Hard Drive Assembly into the Tray



Mechanical Drawings

SecureNAS CX-40KHD SecureNAS CX-40KSD

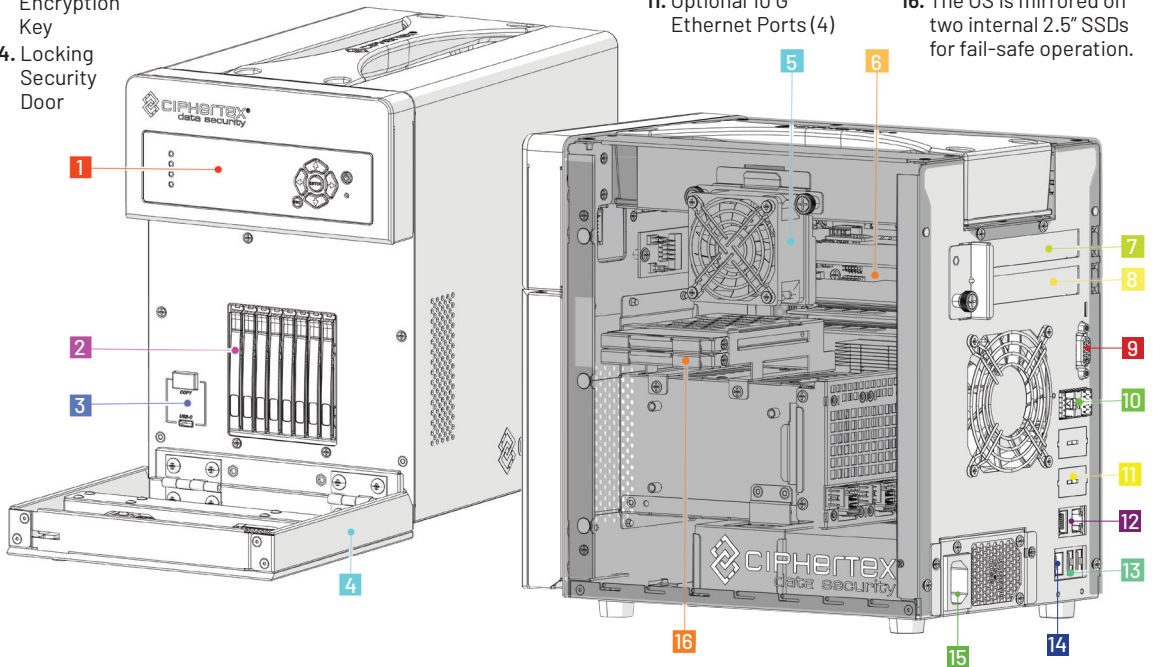
- 1. LCD Display;
- 2. HDDs or SSDs
- 3. USB-C Port Encryption Key
- 4. Locking Security Door



- 5. Cooling Fan
- 6. 7. 8. Expansion Slot
- 9. DB15 Port
- 10. 10GBE SFP+Ports
- 11. Optional 10 G Ethernet Ports (4)
- 12. RJ-45 Gigabit LAN
- 13. USB 3.0 (Type-A Ports)
- 14. IPMI Port
- 15. Power Connector
- 16. The OS is mirrored on two internal 2.5" SSDs for fail-safe operation.

SecureNAS CX-80KSD

- 1. LCD Display;
- 2. SSDs
- 3. USB-C Port Encryption Key
- 4. Locking Security Door



- 5. Cooling Fan
- 6. 7. 8. Expansion Slot
- 9. DB15 Port
- 10. 10GBE SFP+Ports
- 11. Optional 10 G Ethernet Ports (4)
- 12. RJ-45 Gigabit LAN
- 13. USB 3.0 (Type-A Ports)
- 14. IPMI Port
- 15. Power Connector
- 16. The OS is mirrored on two internal 2.5" SSDs for fail-safe operation.



SecureNAS® CX-40KHD

SecureNAS® CX-40KSD

SecureNAS® CX-80KSD



Ciphertex Protect®
Encryption Key



FCC CE COMPLIANCE - Designed and Manufactured and Software Development in the USA.
AS9100D with ISO 9001:2015 NSF-ISR

Made in the U.S.A.

V1.13.21