CIPHERTEX®
data security

Ciphertex SecureNAS® User Guide

CIPHERTEX®
OS
OPERATING SYSTEM

SecureNAS®

by Ciphertex Data Security

PROUDLY MADE IN THE USA

FIPS Level 3 Certified 140-2

GSA Contract Holder
Contract GS35F-487DA

Ciphertex Data Security | 9301 Jordan Avenue, #105A | Chatsworth, CA 91311 **USA** | 877.977.8878 | 818.773.8989
www.ciphertex.com

Ciphertex SecureNAS® User Guide

This document is for information use only and is subject to change without prior notice. Ciphertex Data Security® assumes no responsibility for neither any errors that may appear in this document, nor for incidental or consequential damages resulting from the furnishing, performance or use of this material.

Absent a written agreement signed by Ciphertex Data Security® (Ciphertex®) or its authorized representative to the contrary, Ciphertex explicitly disclaims any express and implied warranties and indemnities of any kind that may, or could, be associated with this document and related material. Any user of this document or related material agrees to such disclaimer as a precondition to receipt and usage hereof.

Each user of this document or any product referred to herein expressly waives all guarantees and warranties of any kind associated with this document any related materials or such product, whether expressed or implied, including without limitation, any implied warranty of merchantability or fitness for a particular purpose or non-infringement. Each user of this document or any product referred to herein also expressly agrees Ciphertex shall not be liable for any incidental, punitive, indirect, special, or consequential damages, including without limitation physical injury or death, property damage, lost data, loss of profits or costs of procurement of substitute goods, technology, or services, arising out of or related to this document, any related materials or any product referred to herein, regardless of whether such damages are based on tort, warranty, contract, or any other legal theory, even if advised of the possibility of such damages.

This document and its contents, including diagrams, schematics, methodology, work product, and intellectual property rights described in, associated with, or implied by this document, are the sole and exclusive property of Ciphertex. No intellectual property license, express or implied, is granted by Ciphertex associated with the document recipient's receipt, access and/or use of this document or the products referred to herein; Ciphertex retains all rights hereto.

This document and Ciphertex communications to the user associated therewith, shall be treated as Ciphertex LLC's proprietary and confidential information, protected by the recipient as such, and used by the recipient only for the purpose authorized in writing by Ciphertex LLC. This document shall be covered as Ciphertex LLC's confidential information under all applicable nondisclosure agreements between the recipient and Ciphertex LLC.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Ciphertex and the Ciphertex logo are registered trademarks or trademarks of Ciphertex LLC or its affiliates in the United States and/or other countries. Product specifications subject to change without notice. Pictures shown may vary from actual products. Not all products are available in all regions of the world.

TABLE OF CONTENTS

1 | INTRODUCTION

1 Introduction

Welcome to Ciphertex SecureNAS®, version 1.0.

1.1 Contact Info

Ciphertex Data Security®
www.ciphertex.com

HEADQUARTERS

9301 Jordan Ave, #105A
Chatsworth, CA 91311

CALL US

877.977.8878
818.773.8989

1.2 About This Guide

This guide describes how to configure, monitor, and maintain the Ciphertex SecureNAS®, sometimes referred to as the system in these instructions.

INTENDED AUDIENCE

This guide is intended for administrators and operators. The information in this guide assumes afamiliarity with computing terminology and with network connectivity protocols.

USER INTERFACE

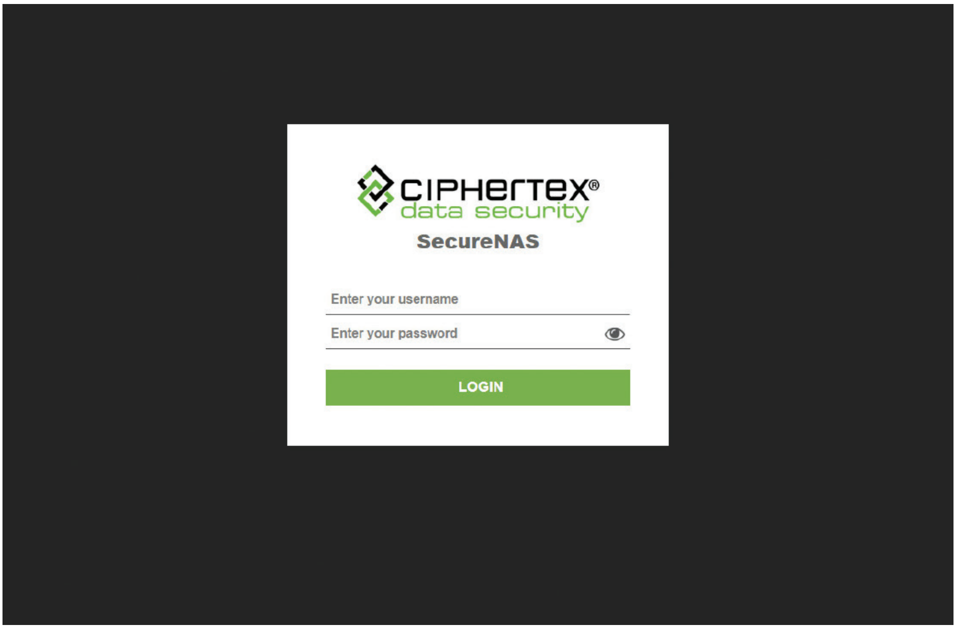
The SecureNAS® Management Console user interface changes over time as new features are added orother modifications are made. Therefore, the screens included in this user guide may differ from thosethat you see in your SecureNAS Management Console user interface.Some features are only available to admin users.

2 Getting started with SecureNAS.

Learn how to log into the SecureNAS Management Console for the firsttime, shutdown the system, and change the default password.

2.1 Login

After setting up and powering on your SecureNAS unit, you can log into the SecureNAS Management. Console using any supported web browser on your computer.



TO LOG INTO SECURENAS MANAGEMENT CONSOLE

1. Make sure your computer is connected to the same network as the SecureNAS.
2. Open a web browser on your computer. Chrome appears to provide the best user experience.
3. The IP address of your SecureNAS is displayed on the LCD screen on the front of the unit. Navigate to the SecureNAS Management Console login page by typing the SecureNAS unit IP address in the url bar as follows:
    a. **http://SecureNAS_IP** (replace **SecureNAS_IP** with IP address that is displayed on the LCD screen on the front of the unit).
    b. Press **Enter.**
4. On the **Enter your username** line, type your username. If this is the first time that the SecureNAS Management Console is being set up, type the default username: **administrator**.
5. On the **Enter your password** line, type your password. If this is the first time that the SecureNAS Management Console is being set up, type the default password: **password**.
6. Click the **Login** button to log into the SecureNAS Management Console.

Click on the eyeball icon on the right side of the Enter your password line to have the password you typed appear as plain text.

Supported Browsers

- Chrome
- Firefox
- Internet Explorer 11
- Safari 12 or later
- Brave

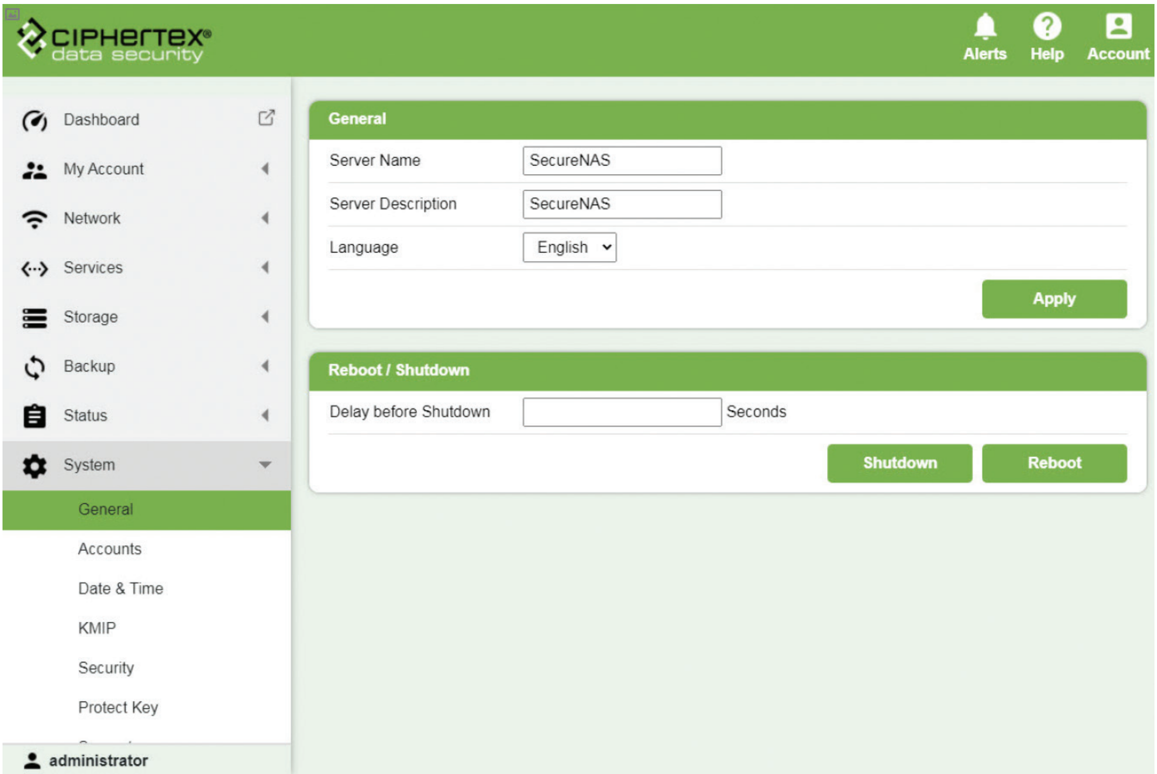
2.2 Shutdown, Restart, or Logout

SHUTDOWN

Use the SecureNAS Management Console web interface to shutdown the SecureNAS unit.

1. From the menu on the left, select **System > General.**
2. To shutdown the SecureNAS unit, click the **Shutdown** button near the bottom of the page in the Reboot/Shutdown section.

If you would like to delay the shutdown, type a number into the Delay before Shutdown textbox. This is the number of seconds to wait to shutdown the SecureNAS unit after the Shutdown button has been clicked.



Server Name	SecureNAS
Server Description	SecureNAS
Language	English

Delay before Shutdown ______ Seconds

REBOOT

Use the SecureNAS Management Console web interface to reboot the SecureNAS unit.

1. From the menu on the left, select **System > General**.
2. To reboot the SecureNAS unit, click the **Reboot** button near the bottom of the page in the Reboot/Shutdown section.

LOGOUT

1. At the top of the SecureNAS Management Console web interface, click on the **Account** icon 👤
2. Select **Logout** from the drop-down menu. You will be logged out.

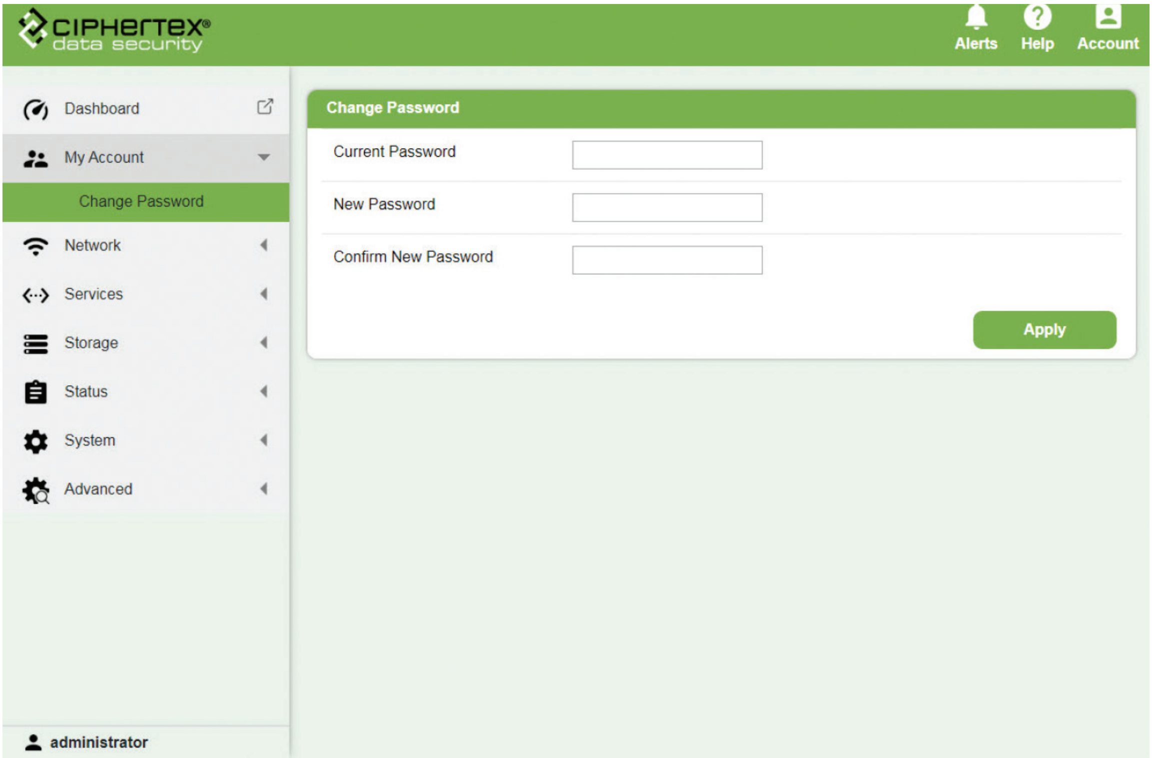
2.3 Change Password

Password Requirements:

- The password is case sensitive.
- The password can be 0-128 characters including: letters, numbers, and symbols.

CHANGE YOUR PASSWORD

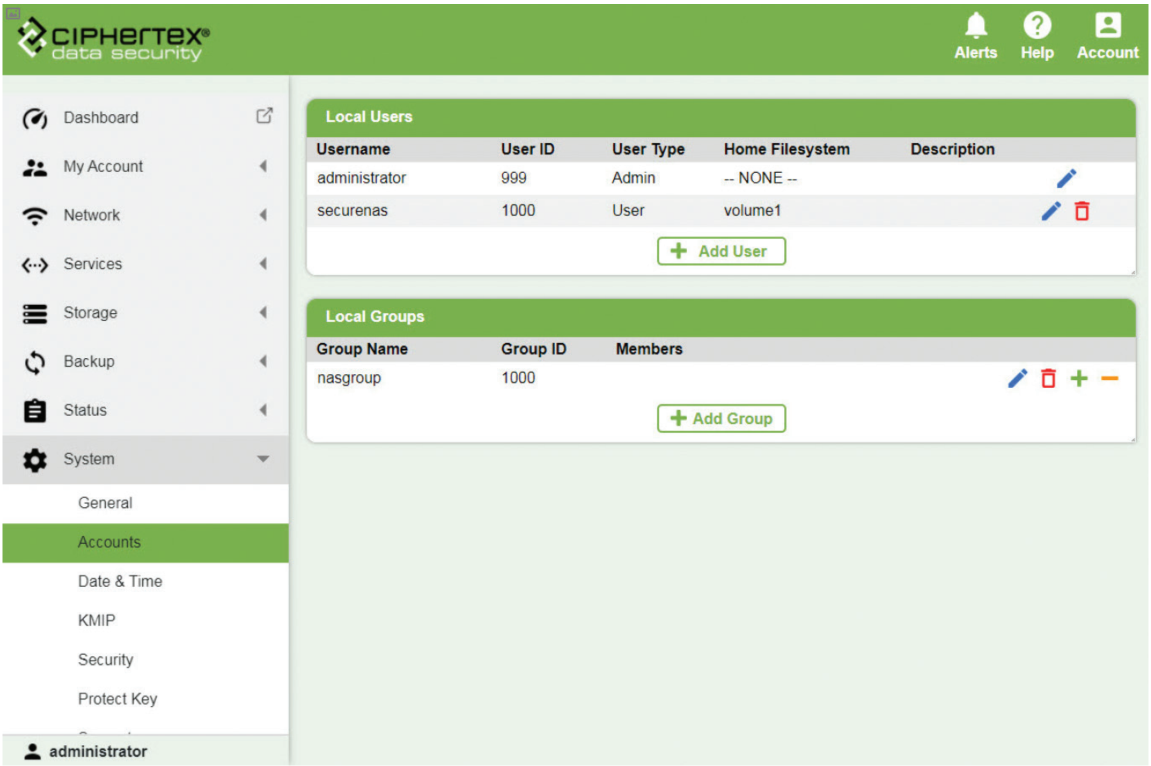
1. Log into the SecureNAS Management Console.
2. From the menu on the left, select **My Account > Change Password**.
3. On the Change Password page, fill in the password textboxes with the appropriate information.
    - a. **Current Password:** the correct current password for your account.
    - b. **New Password:** the new password to set for your account.
    - c. Confirm **New Password:** re-type the New Password that you have chosen.
4. Click the **Apply** button to apply your password change.



CHANGE THE PASSWORD FOR ANY USER

Only users who are part of the Admin group can change the password of other users.

1. From the menu on the left, select **System > Accounts**.
2. In the Local Users section, select the user whose password you want to change. Then click on the blue pen icon ✎ to edit that user's details and change password.
3. In the window that pops up, fill in the password textboxes with the appropriate information.
    - a. **Password**: the new password to set for the account.
    - b. **Confirm New Password**: re-type the New Password that was chosen.
4. Click the **Save** button to apply the password changes.



Local Users

Username	User ID	User Type	Home Filesystem	Description
administrator	999	Admin	-- NONE --	
securenas	1000	User	volume1	

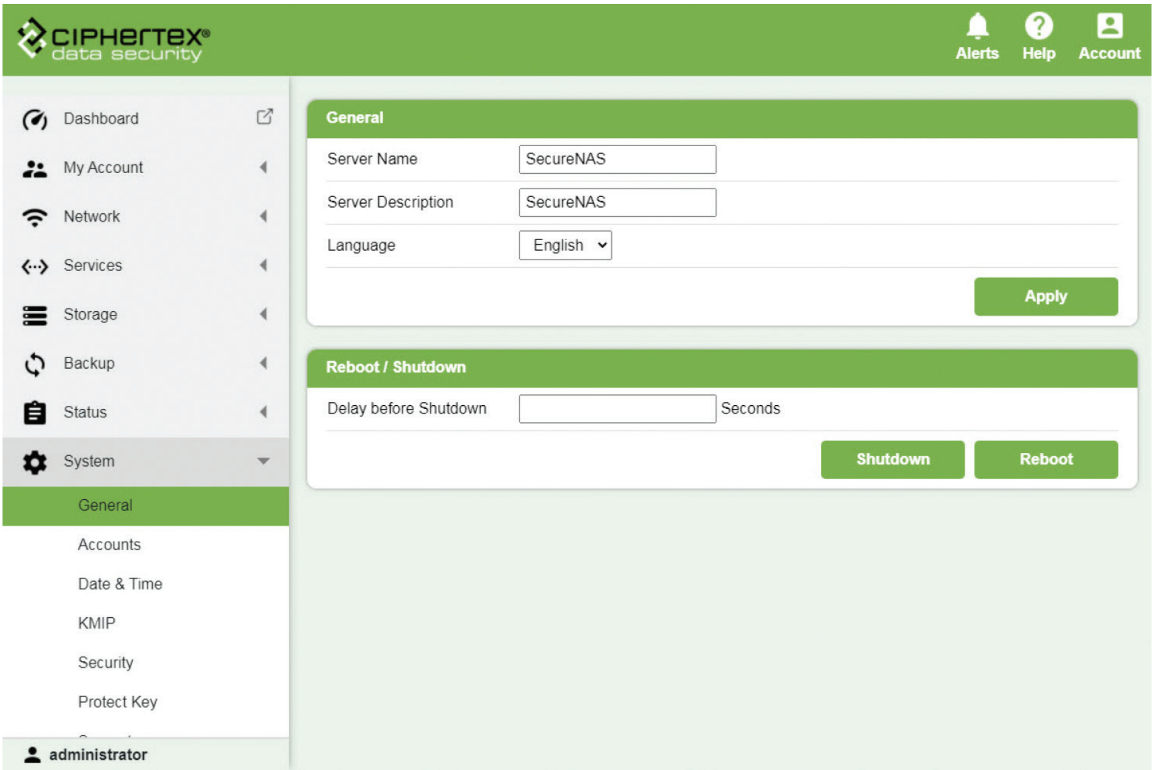
Local Groups

Group Name	Group ID	Members
nasgroup	1000	

3 Manage System Settings

After you have connected to the SecureNAS Management Console, users with the user type Admin can modify basic system settings.

3.1 General Settings



Server Name: SecureNAS

Server Description: SecureNAS

Language: English

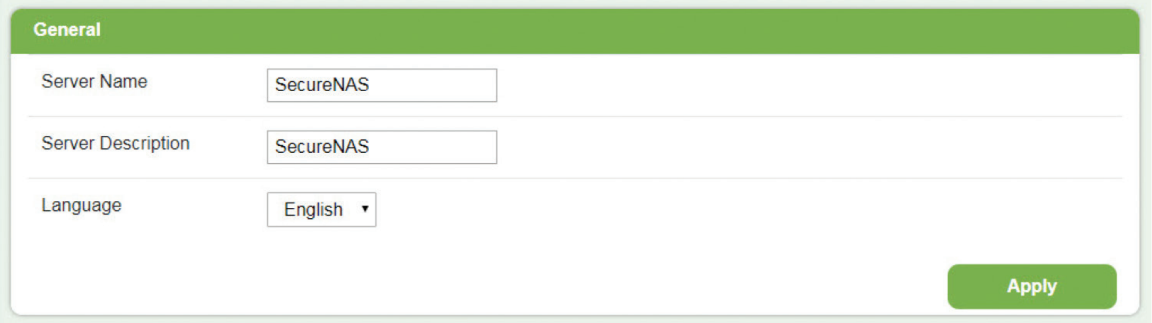
Delay before Shutdown: Seconds

Modify general system settings such as server name, description, and SecureNAS Management Console language.

Select the page under the **System > General** menu item to modify general system settings.

MODIFY GENERAL SYSTEM SETTINGS

1. From the General Settings page in the General section, modify the following information and then click the **Apply** button:



Server Name: SecureNAS

Server Description: SecureNAS

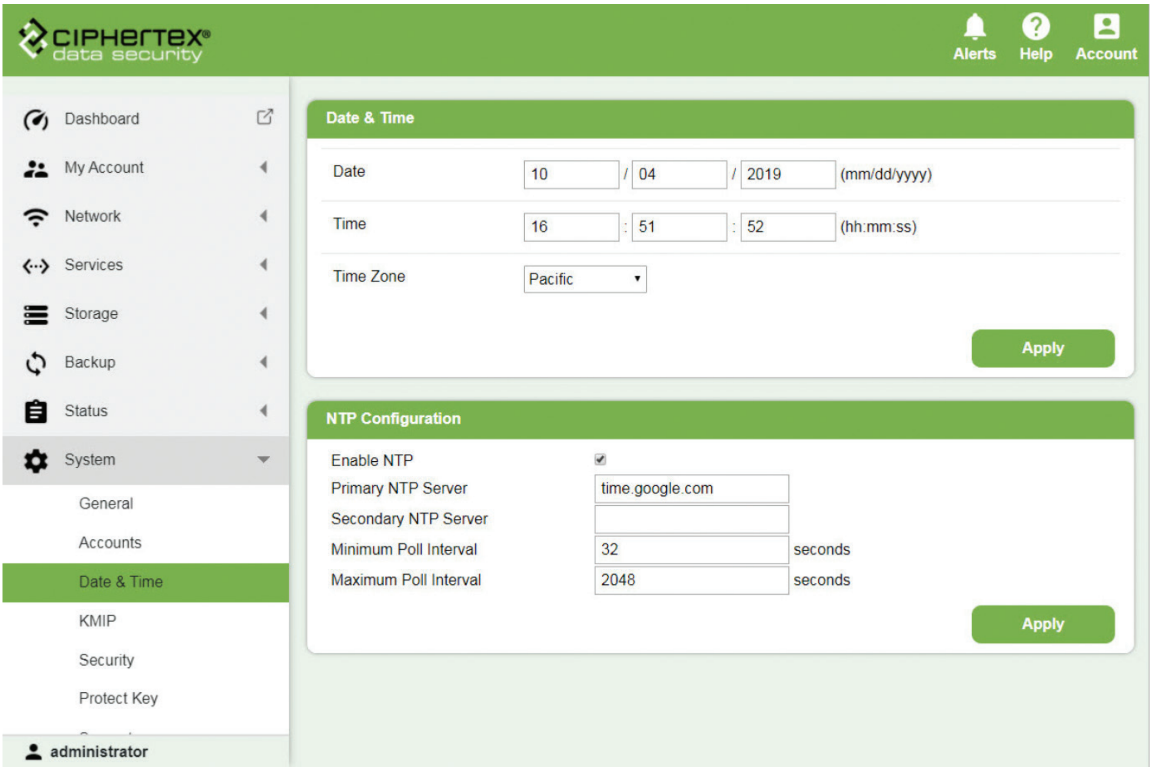
Language: English

Server Name	The name to use for the SecureNAS unit. This is the name that will be used as the hostname.
Server Description	The description to use for the SecureNAS unit.
Language	The language to use for the SecureNAS Management Console web interface. **Note:** At this time, only English is available.

Note:

- After changes have been made in the General settings, a system reboot is required for those changes to take effect.

3.2 System Date and Time



Date & Time

Date 10 / 04 / 2019 (mm/dd/yyyy)

Time 16 : 51 : 52 (hh:mm:ss)

Time Zone Pacific ▾

Apply

NTP Configuration

Enable NTP ☑

Primary NTP Server time.google.com

Secondary NTP Server

Minimum Poll Interval 32 seconds

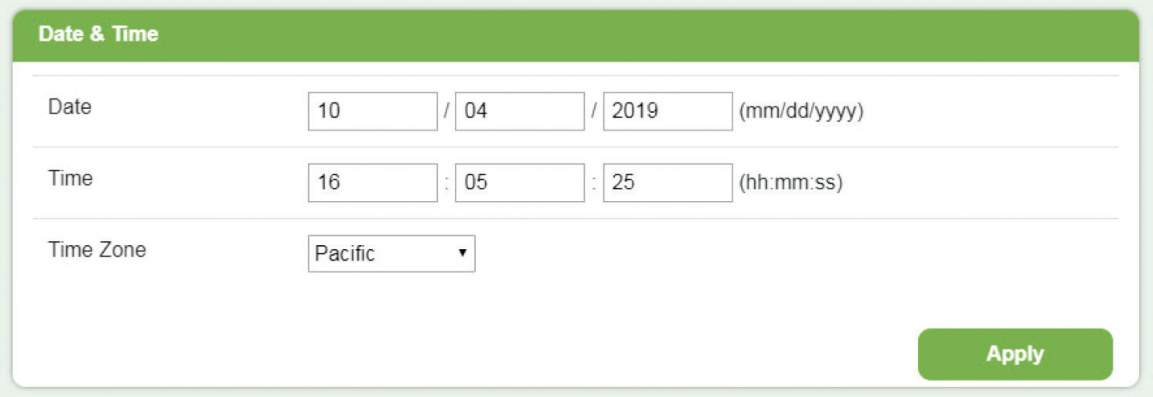
Maximum Poll Interval 2048 seconds

Apply

Select the page under the **System > Date & Time** menu item to modify system date and time settings.

MANUALLY SET SYSTEM DATE AND TIME

1. From the Date & Time page in the **Date & Time** section, modify the following information and then click the **Apply** button:



Date & Time

Date 10 / 04 / 2019 (mm/dd/yyyy)

Time 16 : 05 : 25 (hh:mm:ss)

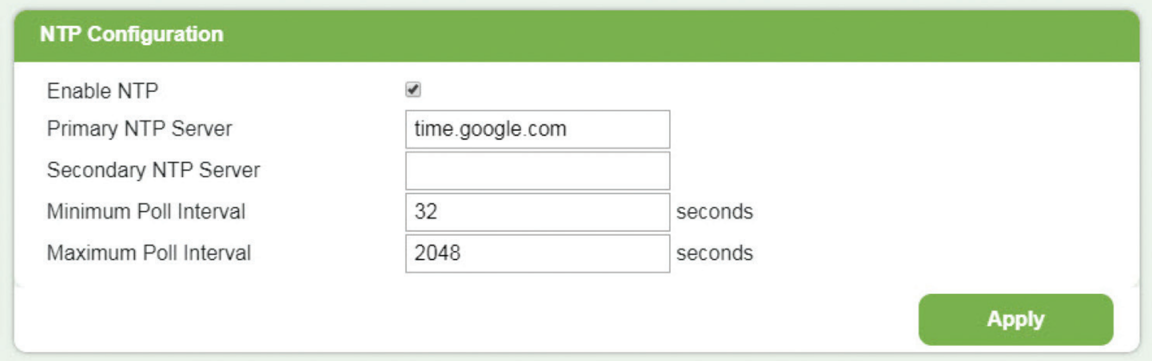
Time Zone Pacific

Date	The time for the SecureNAS unit in the format mm/dd/yyyy. In the first text box, type the two digit month (01-12). In the second text box, type the two digit day (01-31). In the third textbox, type the four digit year.
Time	The time for the SecureNAS unit in the format hh: mm:ss. In the first text box, type the two digit 24-hour clock hour (00-23). In the second text box, type the two digit minute (00-59). In the third textbox, type the two digit seconds (00-59).
Time Zone	Select the correct time zone from the choice pull-down menu.

3.2.1 NTP Configuration

CONFIGURE THE SYSTEM TO USE AN NTP SERVER

1. From the Date and Time page in the **NTP Configuration** section, modify the following information and then click the **Apply** button:

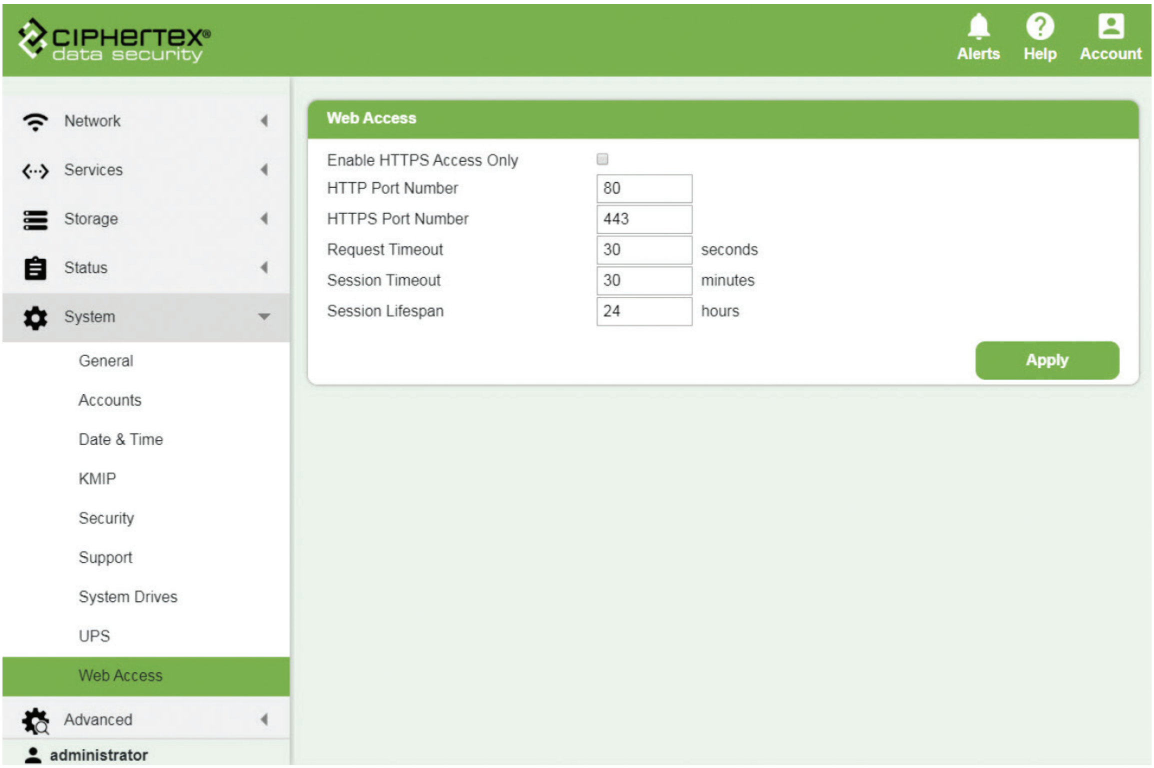


NTP Configuration

Enable NTP	☑
Primary NTP Server	time.google.com
Secondary NTP Server	
Minimum Poll Interval	32 seconds
Maximum Poll Interval	2048 seconds

Enable NTP	Enable this option to have SecureNAS synchronize time with the indicated NTP server.
Primary NTP Server	The server address of the NTP server to use for synchronizing.
Secondary NTP Server	A fallback NTP server if the first option is not available. The server address of the NTP server to use for synchronizing.
Minimum Poll Interval	The minimum amount of seconds between polling for time synchronization.
Maximum Poll Interval	The maximum amount of seconds between polling for time synchronization.

3.3 Web Access Settings



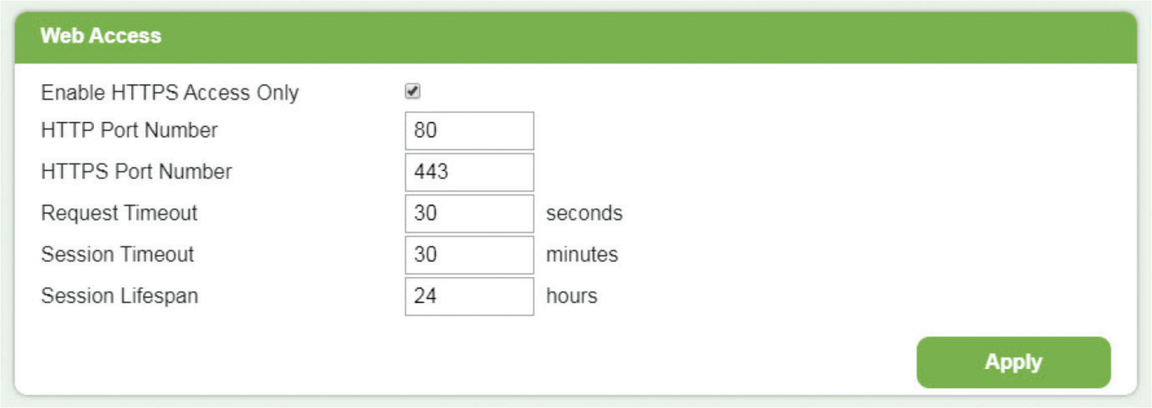
Web Access

Enable HTTPS Access Only	□	
HTTP Port Number	80	
HTTPS Port Number	443	
Request Timeout	30	seconds
Session Timeout	30	minutes
Session Lifespan	24	hours

Select the page under the **System > Web Access** menu item to modify the settings that control web access to the SecureNAS Management Console. Settings such as session timeout, SSL certificates, and HTTP/HTTPS port numbers can be configured here.

CONFIGURE WEB UI SETTINGS

1. Modify the following information and then click the **Apply** button:

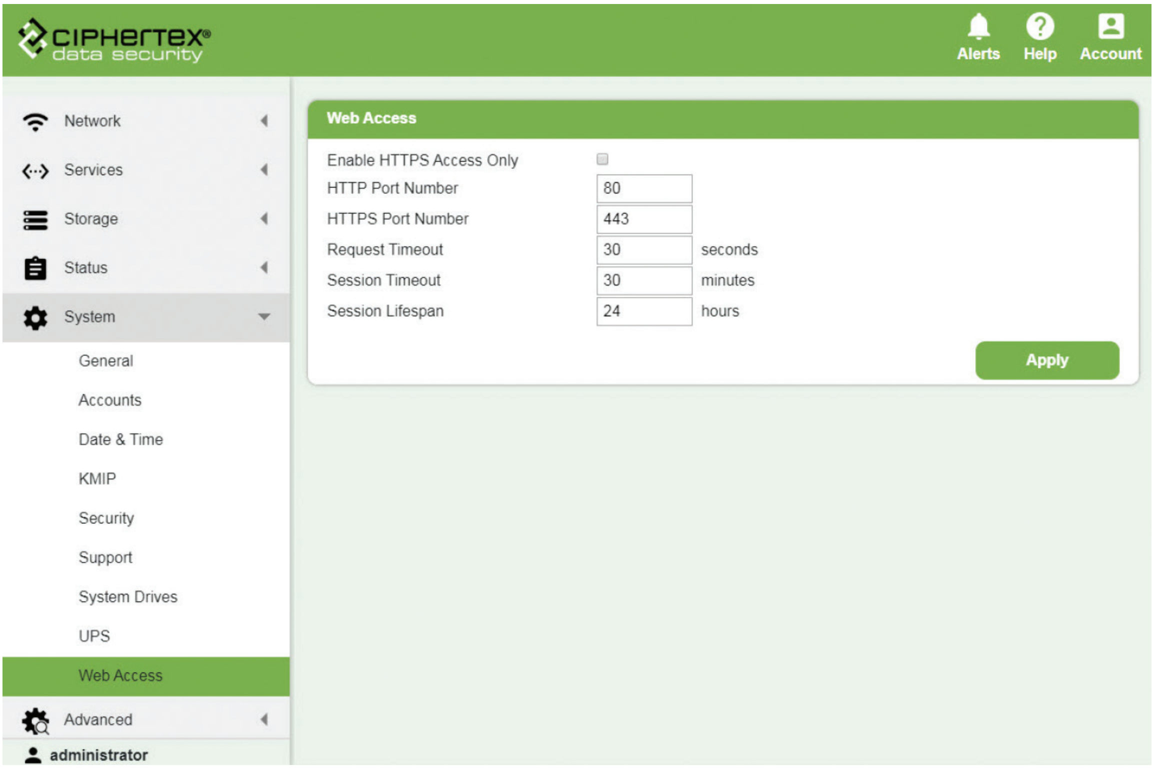


Web Access

Enable HTTPS Access Only	☑	
HTTP Port Number	80	
HTTPS Port Number	443	
Request Timeout	30	seconds
Session Timeout	30	minutes
Session Lifespan	24	hours

Enable HTTPS Access Only	If enabled, you will only be able to access the SecureNAS Management Console via a secured HTTPS connection. **Note:** If this feature is grayed out and not modifiable, you must first add a SSL certificate to your system in order to activate this feature.
HTTP Port Number	The port number to use for an HTTP connection.
HTTPS Port Number	The port number to use for an HTTPS connection.
Request Timeout	The length of time, in seconds, allowed before a request times out.
Session Timeout	The length of time, in minutes, that a single web session in the SecureNAS Management Console will stay active without any user interaction. After this length of time, the user will be logged out automatically.
Session Lifespan	The length of time, in hours, that a single web session in the SecureNAS Management Console will stay active. Even with user interaction, if the total length of time of the session exceeds this setting, the user will be logged out automatically.

3.3.1 SSL Certificate



Web Access

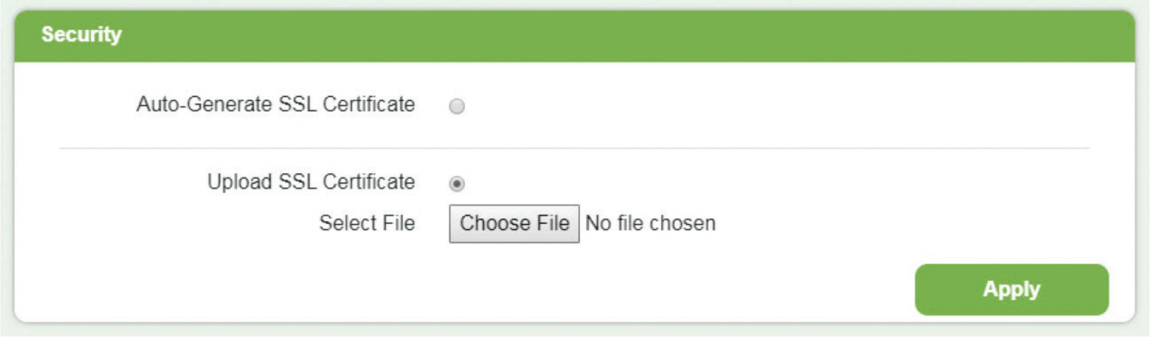
Enable HTTPS Access Only	□	
HTTP Port Number	80	
HTTPS Port Number	443	
Request Timeout	30	seconds
Session Timeout	30	minutes
Session Lifespan	24	hours

Select the page under the **System > Security** menu item to modify the security settings for accessing the SecureNAS Management Console web interface. SecureNAS allows you to either upload your own SSL certificate or choose to have one auto-generated.

CONFIGURE SSL CERTIFICATES

SecureNAS is not shipped with an SSL certificate. Use the following instructions to configure an SSL certificate for your system.

1. Choose from the following options and then click the **Apply** button:



Security

Auto-Generate SSL Certificate ○

Upload SSL Certificate ●

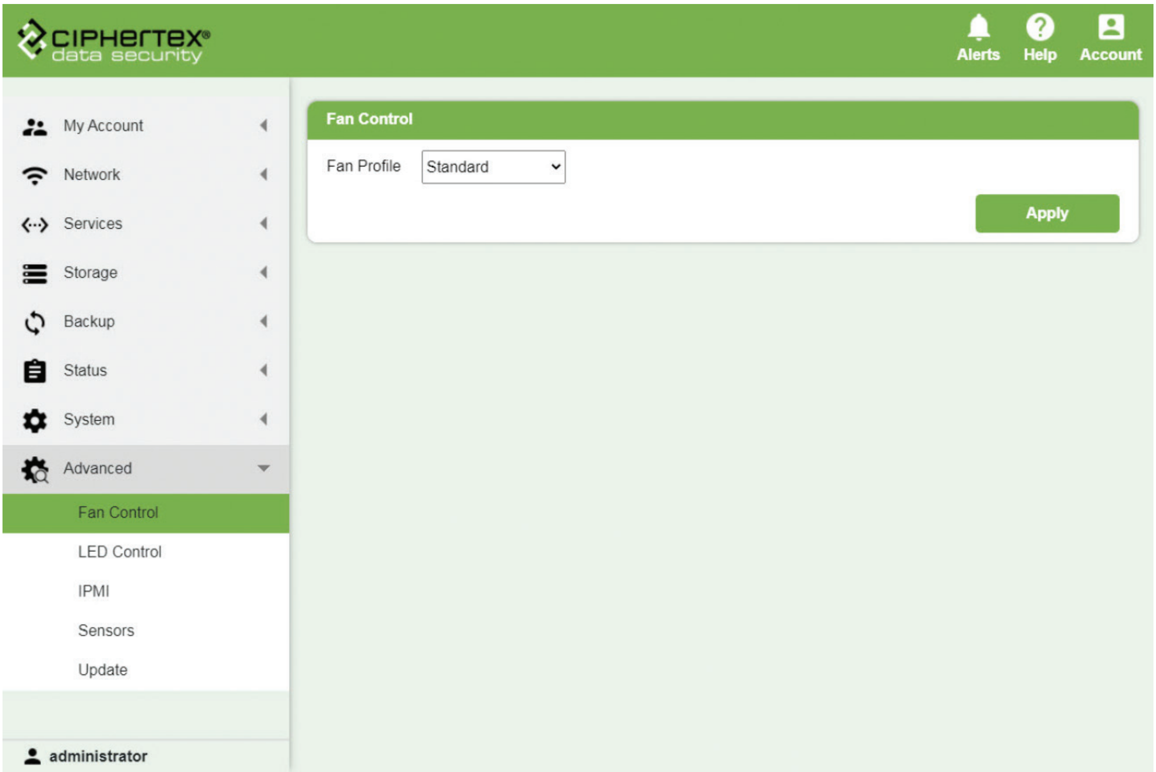
Select File: No file chosen

Auto-Generate SSL Certificate	Select this option to have the SecureNAS Management Console auto-generate a non-signed SSL certificate to use with your system. **Note:** Because this auto-generated certificate is not signed, you must pass a security check every time you attempt to access the SecureNAS Management Console or when you attempt to transfer data.
Upload SSL Certificate	Select this option to upload and install a signed, trusted SSL certificate. The certificate must be in PEM format and contain both the private key and the certificate.

3.4 Hardware Control

The SecureNAS Management Console web interface allows you to control some basic hardware functionality such as fan speed profiles and LED light settings.

3.4.1 Fan Speed Control


Fan Control

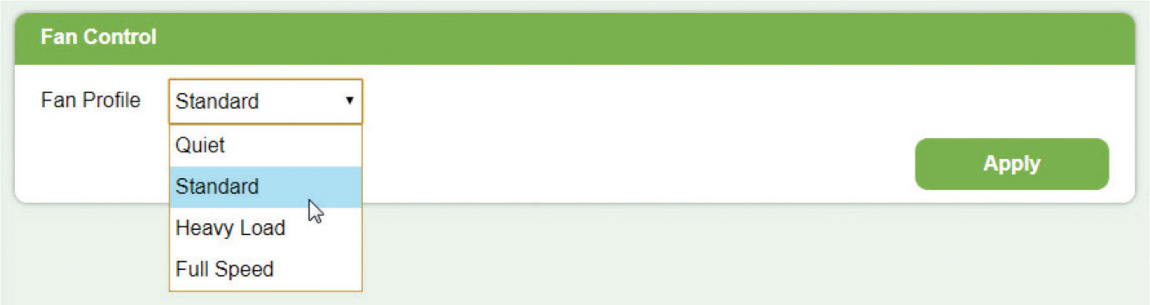
Fan Profile: Standard

Select the page under the **Advanced > Fan Control** menu item to modify the fan speed profiles. This setting let's you manually adjust fan speed and noise to suit environmental conditions.

Note:
Internal hardware fans will always automatically increase speed as required for adequate cooling.

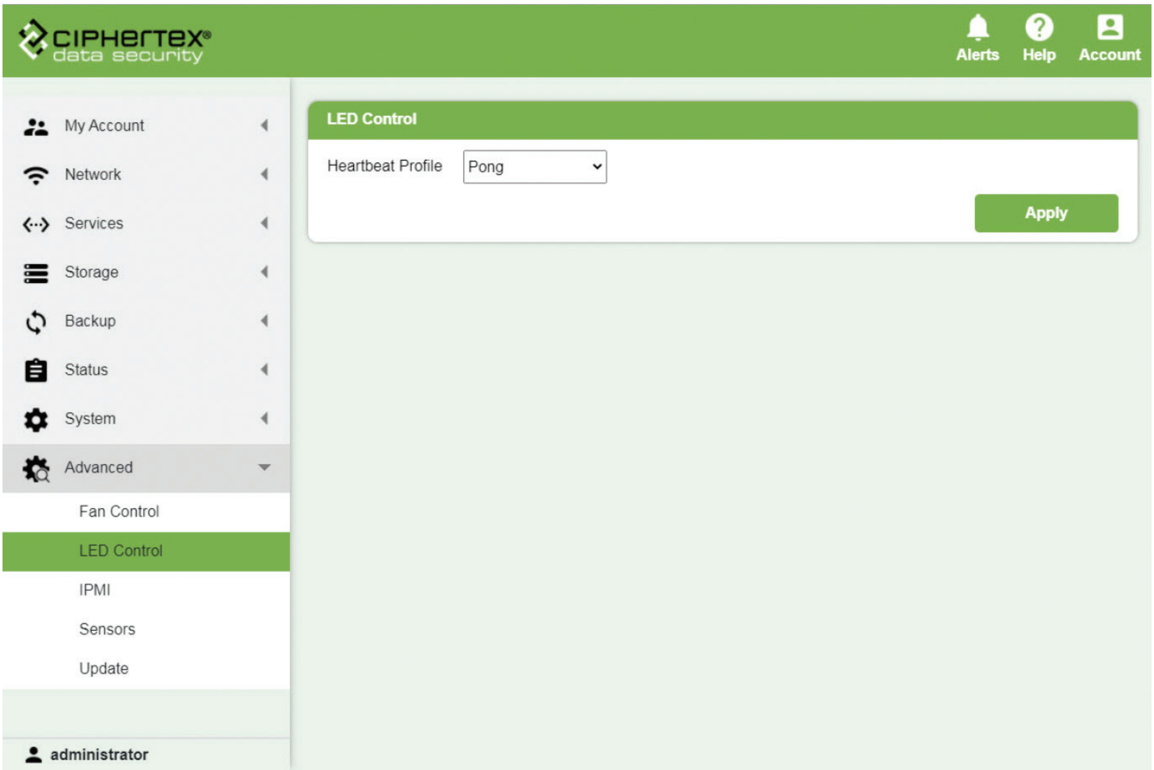
ADJUST FAN CONTROL

1. On the Fan Control page, choose from the following options and then click the Apply button:



Quiet	This profile will keep fan speed and noise low if environmental conditions allow.
Standart	This profile will keep fan speed at a normal rate for conditions.
Heavy Load	This profile will keep fan speed at a higher rate than normal.
Minimum Poll Interval	The minimum amount of seconds between polling for time synchronization.
Full Speed	This profile will keep fan at full speed at all times.

3.4.2 Front LED Settings



Heartbeat Profile: Pong

Select the page under the **Advanced > LED Control** menu item to modify the pattern for the amber-colored LEDs on the front of the SecureNAS unit. These amber-colored LEDs blink as a "heartbeat" for the system.

Note:

• The three amber-colored LEDs blink as a "heartbeat" for the system. They are not indicative of any problems.

•The top LED is used to indicate system status:

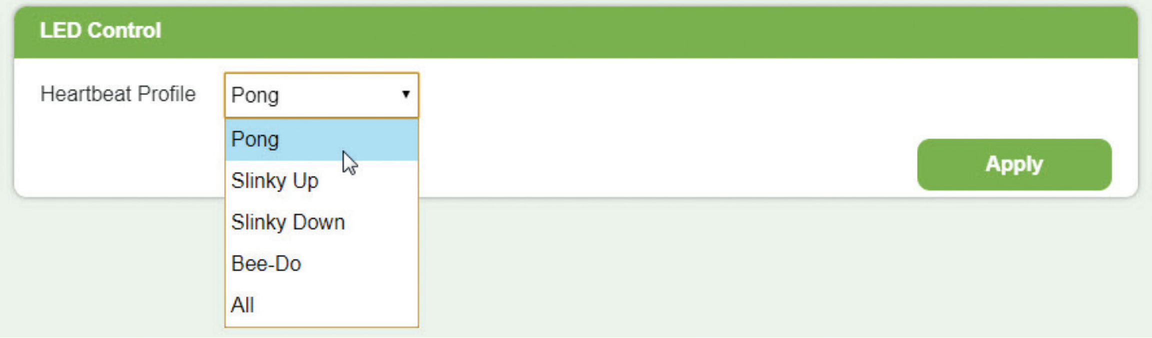
o Solid Green: everything is ok.

o Alternating Green/Red: there is at least one critical alert to view.

o Solid Red: there is a hardware failure that needs immediate attention.

CHANGE LED BLINKING PATTERN

1. On the LED Control page, choose from the following options and then click the Apply button:

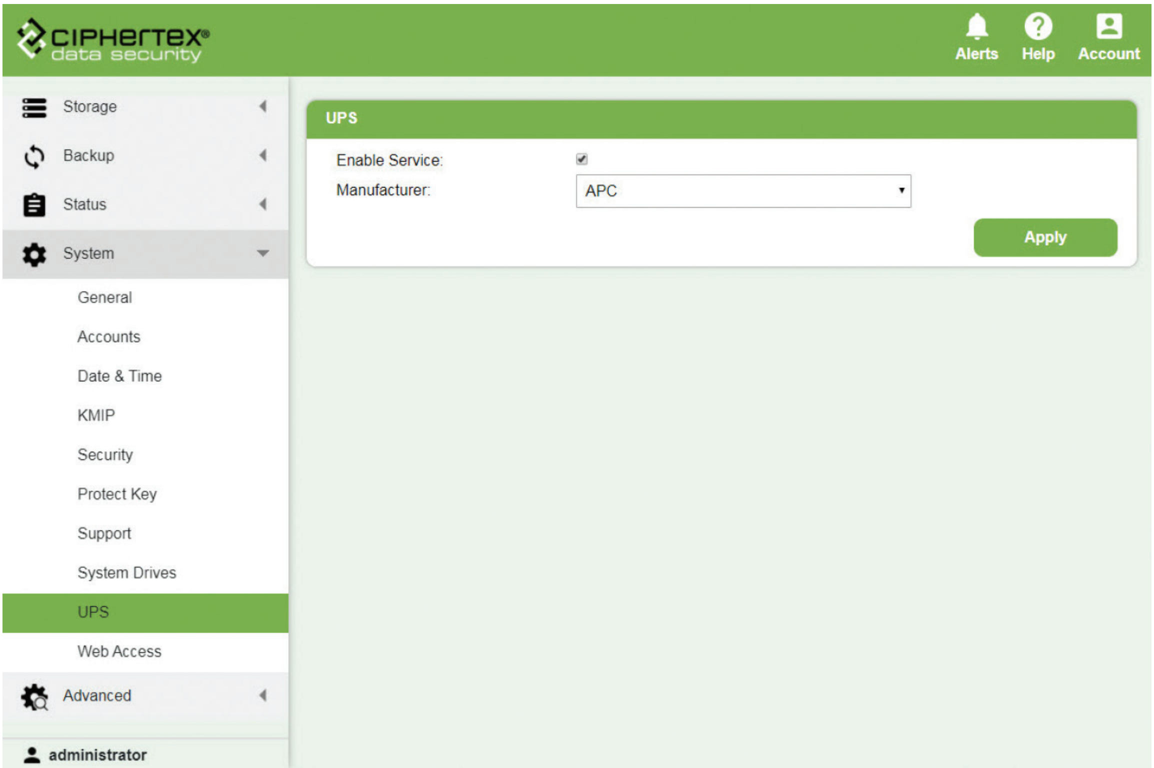


LED Control

Heartbeat Profile: Pong

Pong	LEDs will alternate blinking in a pattern going up and down.
Slinky Up	LEDs will alternate blinking in a pattern going up.
Slinky Down	LEDs will alternate blinking in a pattern going down.
Bee-Do	LEDs will alternate blinking in a pattern of top/bottom then middle.
All	All patterns will be cycled through.

3.5 UPS



Enable Service: ☑

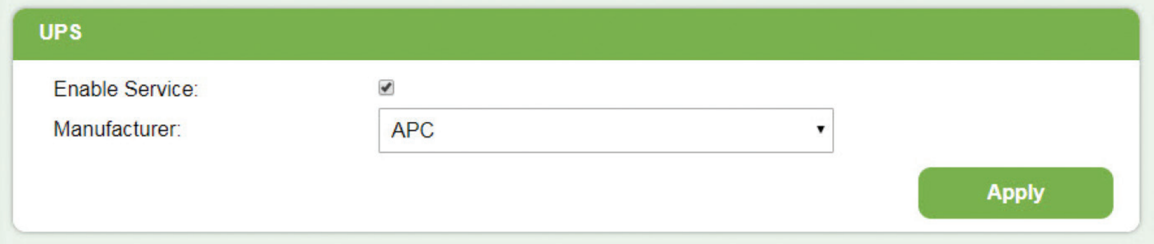
Manufacturer: APC

Select the page under the **System > UPS** menu item to modify UPS settings. UPS (Uninterruptible Power Supply) is a backup power device that allows the SecureNAS unit to continue operating for a period of time in the event of a power failure.

> **Note:**
> SecureNAS only supports USB connected UPS devices.

USE A UPS

1. On the UPS page, modify the following settings and then click the Apply button:

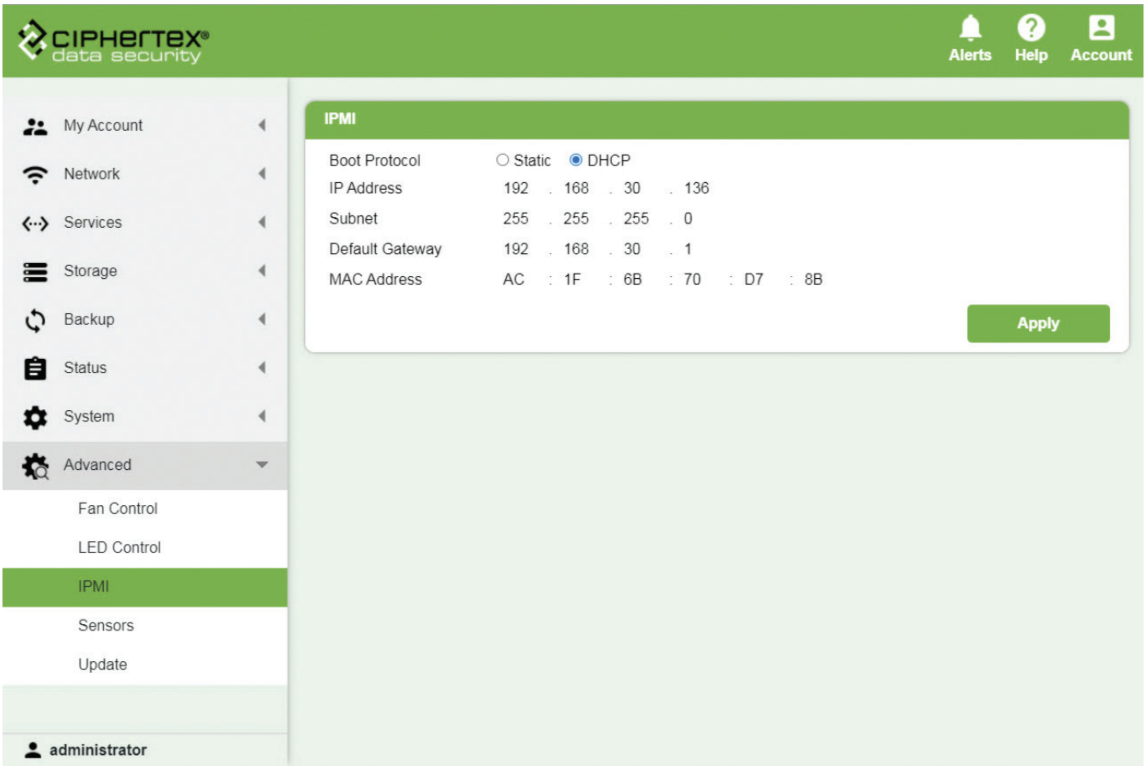


Enable Service: ☑

Manufacturer: APC

Enable UPS	Enable/disable the use of a UPS with SecureNAS.
MANUFACTURER	Choose the UPS manufacturer from the list.

3.6 Set Up IPMI



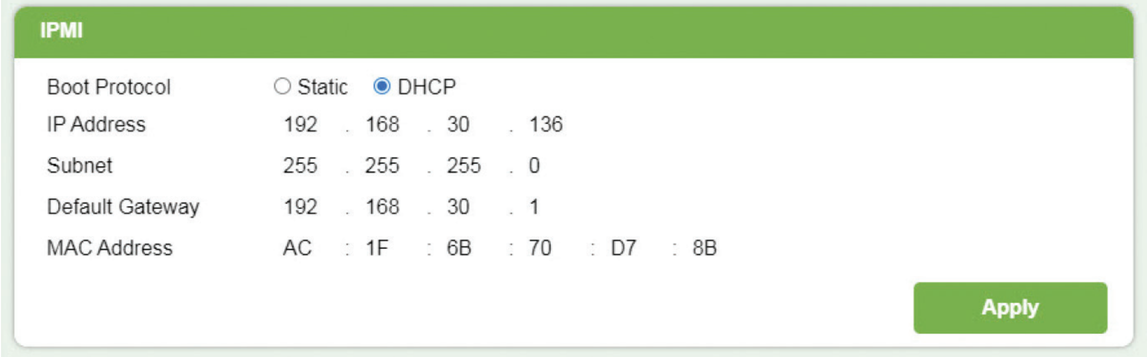
Boot Protocol ○ Static ● DHCP

IP Address	192 . 168 . 30 . 136
Subnet	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 30 . 1
MAC Address	AC : 1F : 6B : 70 : D7 : 8B

Select the page under the **Advanced > IPMI** menu item to modify IPMI settings.

CONFIGURE IPMI SETTINGS

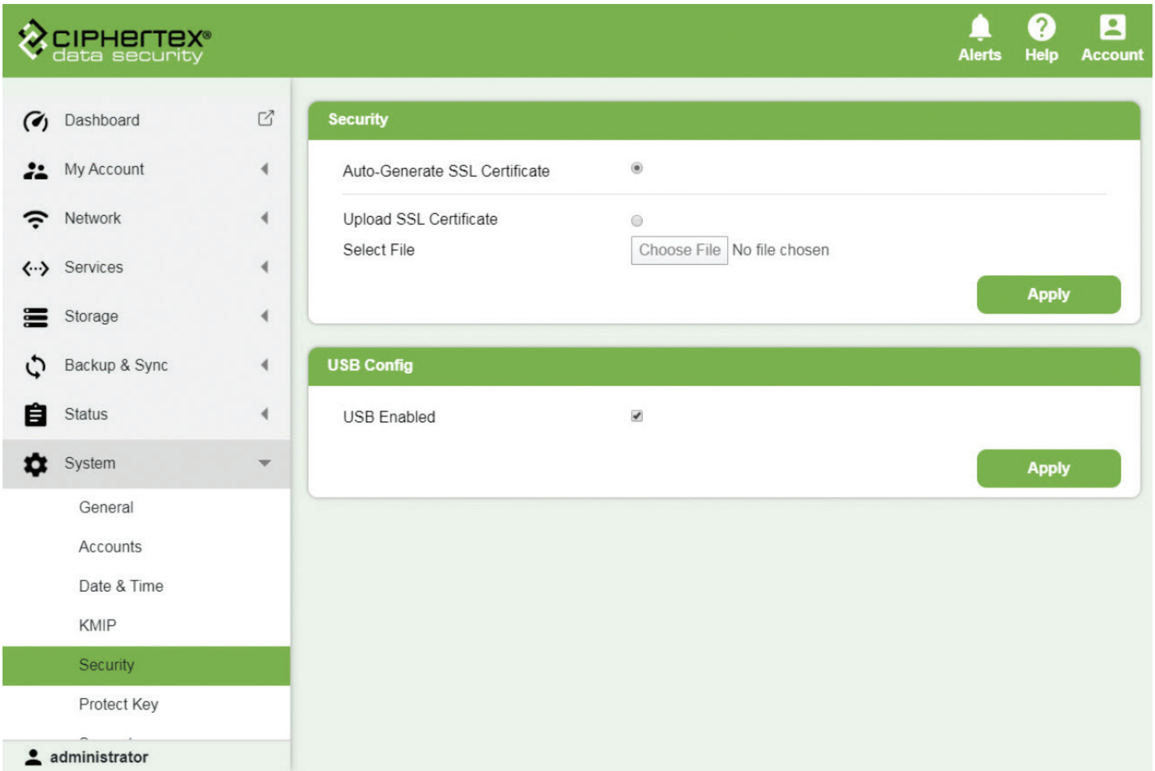
1. On the IPMI page in the IPMI section, select Static or DHCP and complete the settings as necessary.
2. After configuring IPMI, click the **Apply** button:



IPMI

Boot Protocol	○ Static	● DHCP				
IP Address	192	168	30	136		
Subnet	255	255	255	0		
Default Gateway	192	168	30	1		
MAC Address	AC	1F	6B	70	D7	8B

3.7 Disable All USB Ports



Security

Auto-Generate SSL Certificate ●

Upload SSL Certificate ○

Select File Choose File No file chosen

USB Config

USB Enabled ☑

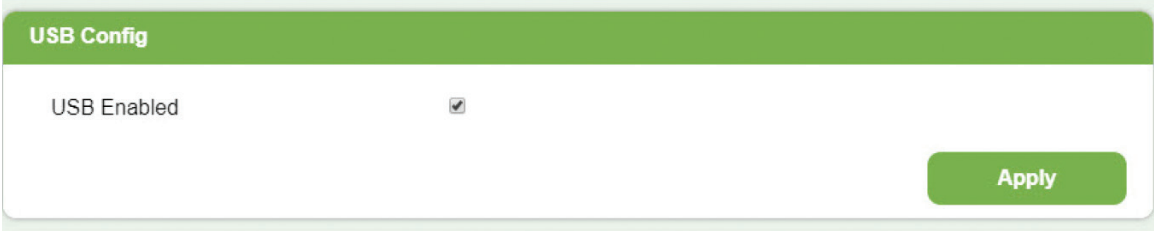
Select the page under the **System > Security** menu item to modify the settings for USB connectivity with the SecureNAS.

Note:

- If USB is disabled, all USB ports will be disabled. This means that USB storage sharing, USB copy, and Quick-Link USB connection will all be disabled and not available for use.

ENABLE/DISABLE USB

1. Select the USB Enabled checkbox to enable/disable USB connectivity from from all USB ports on the SecureNAS unit.
2. Click the **Apply** button to save the setting changes.



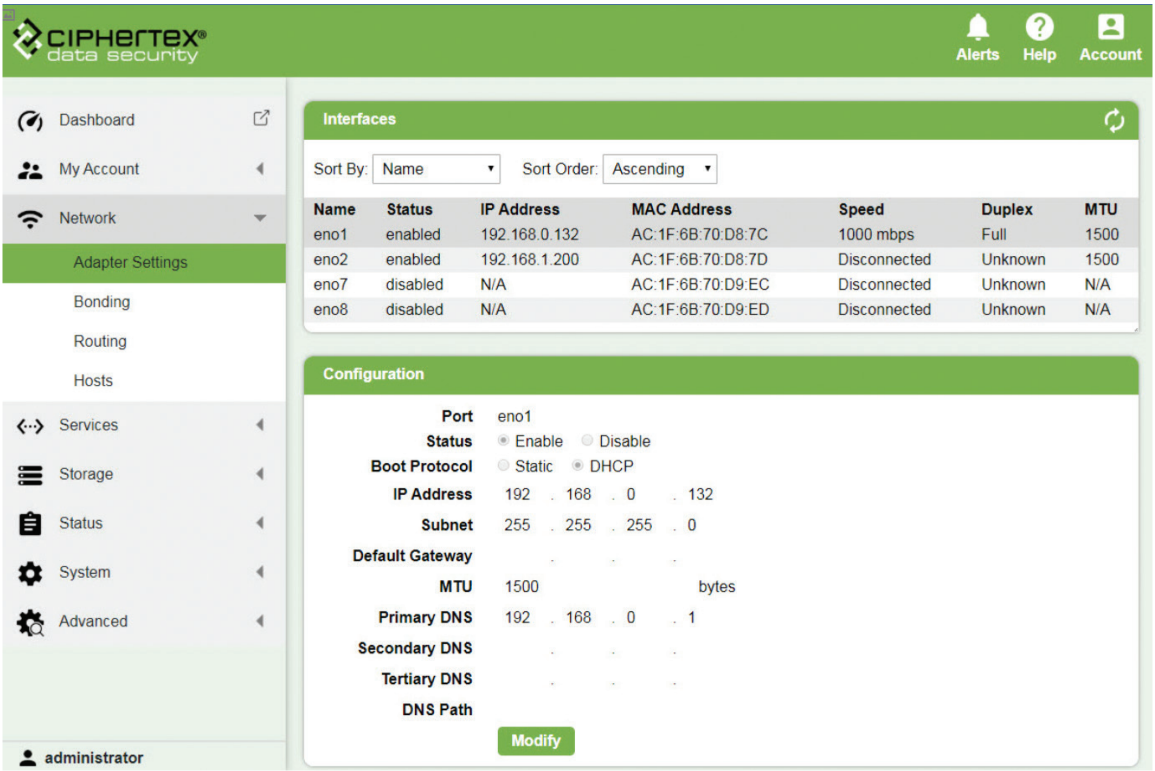
USB Config

USB Enabled ☑

4 Change Network Settings

Use the pages under the **Network** menu item to configure ethernet ports, change DNS settings, manage routes and bonding, and add/delete network hosts.

4.1 Change Adapter Settings



Sort By: Name ▾ Sort Order: Ascending ▾

Name	Status	IP Address	MAC Address	Speed	Duplex	MTU
eno1	enabled	192.168.0.132	AC:1F:6B:70:D8:7C	1000 mbps	Full	1500
eno2	enabled	192.168.1.200	AC:1F:6B:70:D8:7D	Disconnected	Unknown	1500
eno7	disabled	N/A	AC:1F:6B:70:D9:EC	Disconnected	Unknown	N/A
eno8	disabled	N/A	AC:1F:6B:70:D9:ED	Disconnected	Unknown	N/A

Port	eno1
Status	● Enable ○ Disable
Boot Protocol	○ Static ● DHCP
IP Address	192 . 168 . 0 . 132
Subnet	255 . 255 . 255 . 0
Default Gateway	. . .
MTU	1500 bytes
Primary DNS	192 . 168 . 0 . 1
Secondary DNS	. . .
Tertiary DNS	. . .
DNS Path	

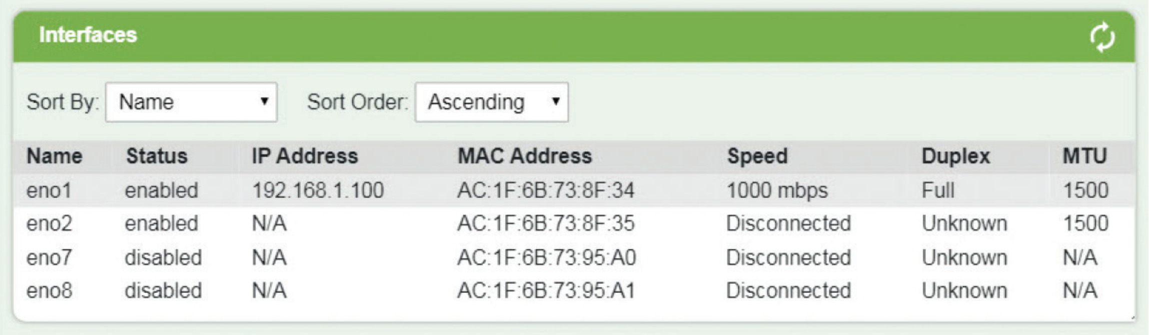
Select the page under the **Network > Adapter Settings** menu item to edit and configure the IP addressing of the Ethernet ports in the SecureNAS unit.

Note:

- You can create one or more network connections to the system.
- You can configure link aggregation for better performance.
- You can only use the SecureNAS unit management port to access the SecureNAS Management Console web interface. You cannot use this port for data transfer.

CONFIGURE THE MANAGEMENT PORT

1. On the Adapter Settings page in the **Interfaces** section, select **eno1** by clicking on the row in the table. This will display the configuration for eno1 in the Configuration section.



Interfaces

Sort By: Name ▾ Sort Order: Ascending ▾

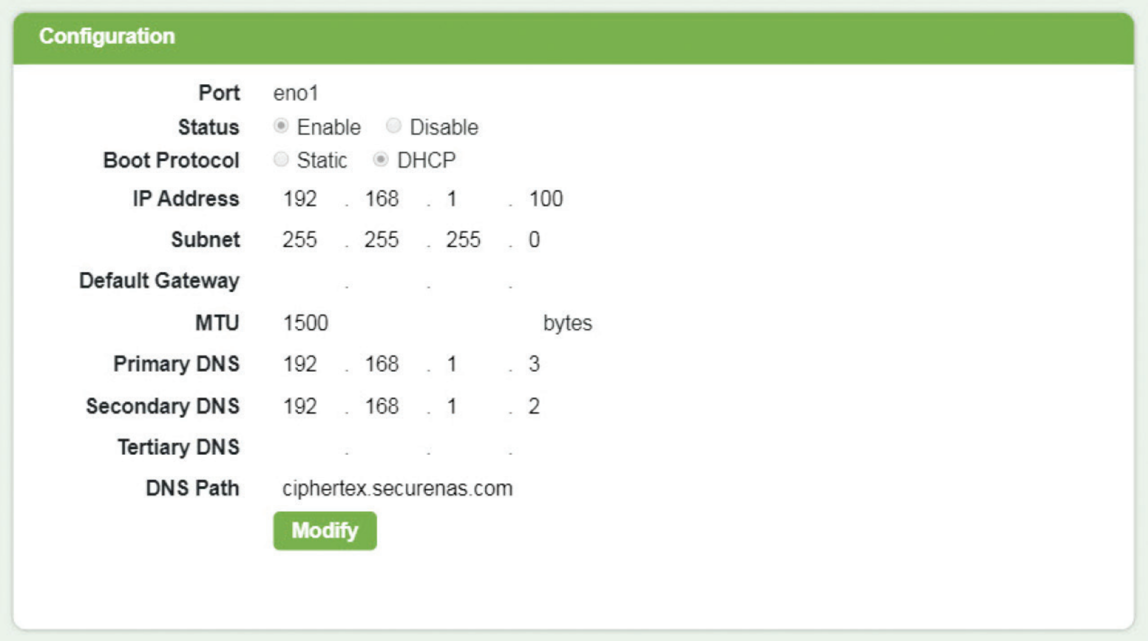
Name	Status	IP Address	MAC Address	Speed	Duplex	MTU
eno1	enabled	192.168.1.100	AC:1F:6B:73:8F:34	1000 mbps	Full	1500
eno2	enabled	N/A	AC:1F:6B:73:8F:35	Disconnected	Unknown	1500
eno7	disabled	N/A	AC:1F:6B:73:95:A0	Disconnected	Unknown	N/A
eno8	disabled	N/A	AC:1F:6B:73:95:A1	Disconnected	Unknown	N/A

2. Click on the **Modify** button to change the configuration.

3. Select **DHCP** to configure the system to automatically acquire an IPv4 address using DHCP.

4.To configure a static IP address, select Static.

5. Fill in the following information and then click the **Apply** button:



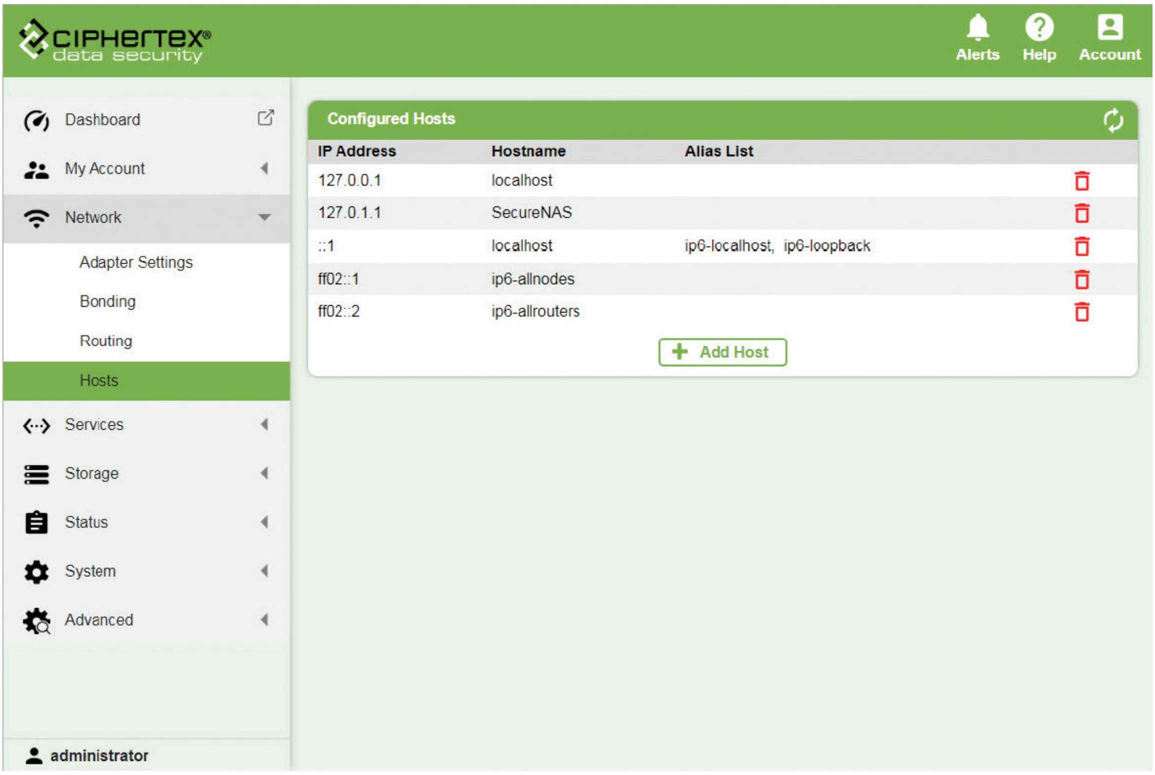
Configuration

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

Status	Enable or Disable.
Boot Protocol	Static: Set a static IP address. DHCP: SecureNAS unit will dynamically acquire an IPv4 address.
IP Address	Enter a valid IPv4 address. **Note:** If you selected DHCP, you cannot enter an IP address and this option will be unavailable for input.
Subnet	Enter the subnet mask. **Note:** If you selected DHCP, you cannot enter a subnet and this option will be unavailable for input.
Default Gateway	The gateway entered for the last configured IPv4 connection sets the default gateway for the SecureNAS unit. **Note:** If you selected DHCP, you cannot enter a default gateway and this option will be unavailable for input.
MTU	Default is 1500. Only change this value if you are sure that your switch configuration supports larger MTU settings, as well as all of the hosts on the network.
Primary DNS	The IP address of the primary DNS. **Note:** If you selected DHCP, this option may be unavailable for input. If DHCP is selected and this option is blank, you can fill it in. **Optional.**
Secondary DNS	The IP address of the primary DNS. **Note:** If you selected DHCP, this option may be unavailable for input. If DHCP is selected and this option is blank, you can fill it in. **Optional.**

Tertiary DNS	The IP address of the tertiary DNS. In a case where there is a problem with the primary DNS and the secondary DNS, the tertiary DNS will be used. **Note:** If you selected DHCP, this option may be unavailable for input. If DHCP is selected and this option is blank, you can fill it in. **Optional.**
DNS Path	This is the resolvable domain name for the primary DNS. **Note:** If you selected DHCP, this option may be unavailable for input. If DHCP is selected and this option is blank, you can fill it in. **Optional.**

4.2 Configure Network Hosts

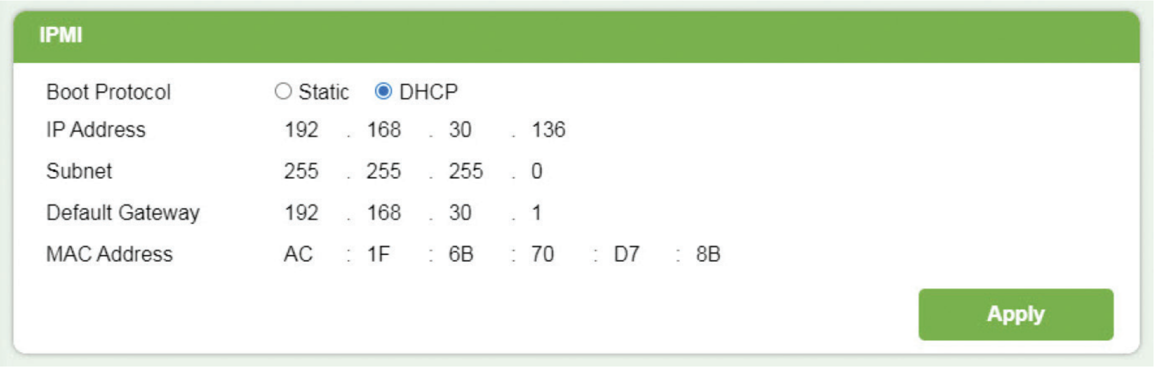


IP Address	Hostname	Alias List
127.0.0.1	localhost	
127.0.1.1	SecureNAS	
::1	localhost	ip6-localhost, ip6-loopback
ff02::1	ip6-allnodes	
ff02::2	ip6-allrouters	

Select the page under the **Network > Hosts** menu item to edit and configure network hosts.

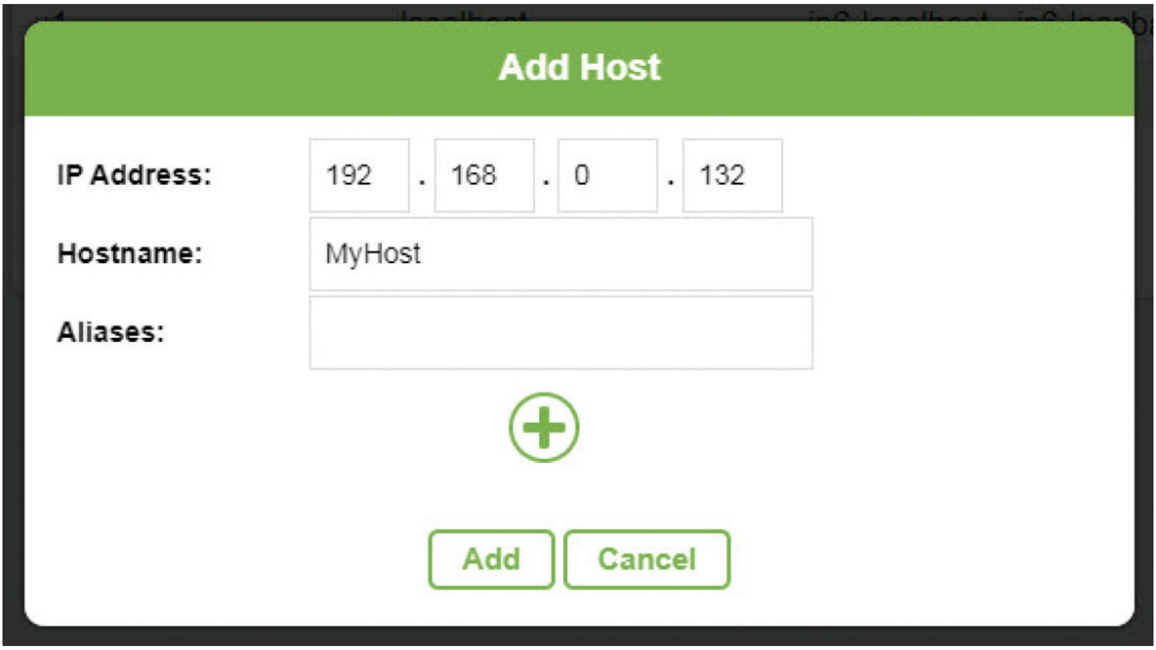
ADD HOST

1. On the Hosts page in the **Configured Hosts** section, click the ✚ Add **Host** button to add a new network host



Boot Protocol	○ Static ● DHCP
IP Address	192 . 168 . 30 . 136
Subnet	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 30 . 1
MAC Address	AC : 1F : 6B : 70 : D7 : 8B

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



IP Address: 192 . 168 . 0 . 132

Hostname: MyHost

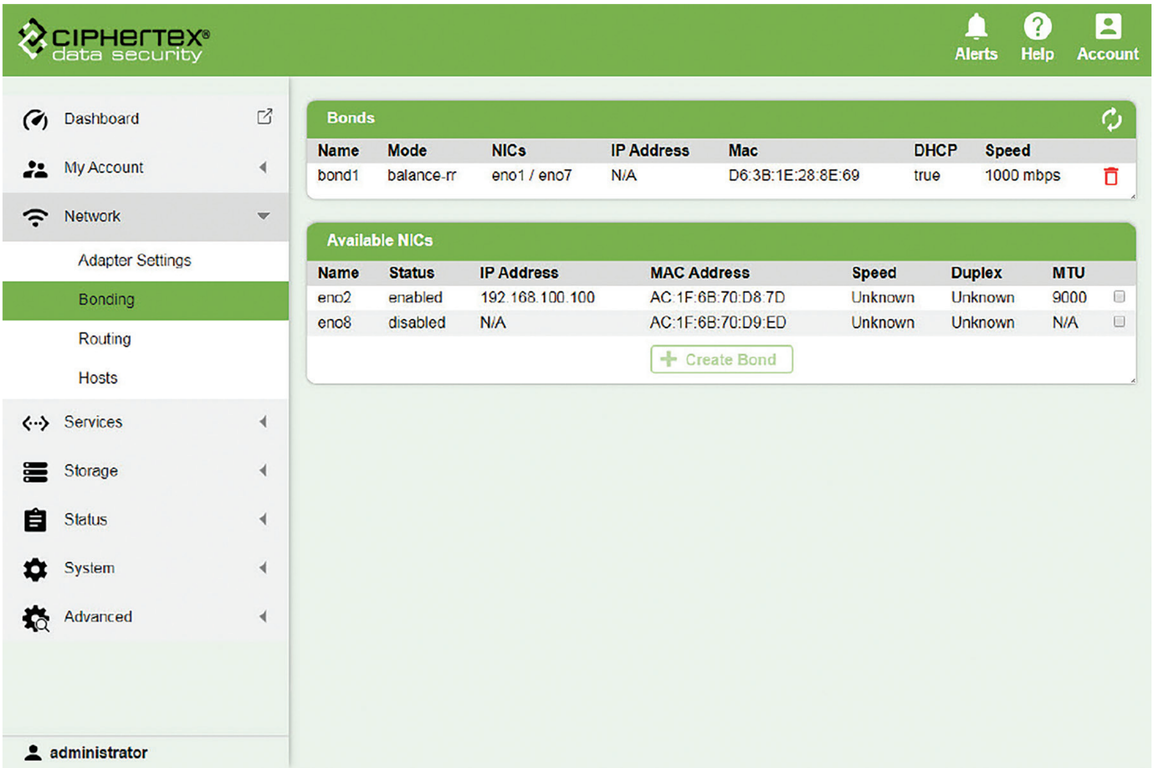
Aliases:

IP Address	The IP address of the network host being added.
Hostname	The hostname of the network host being added. The hostname may only contain the characters a-z, A-Z, 0-9, hyphens ("-"), and periods ("."). No other special characters or spaces are allowed.
Aliases	The alias for the network host being added. An alias can be used for a name change, alternate spellings, or shorter hostnames. Optional.

Delete HOST

1. On the Hosts page in the Configured Hosts section, elect the host that you want to delete. This will highlight the row. Then click on the red trashcan icon 🗑 to delete that host.

4.3 NIC Bonding



Bonds

Name	Mode	NICs	IP Address	Mac	DHCP	Speed
bond1	balance-rr	eno1 / eno7	N/A	D6:3B:1E:28:8E:69	true	1000 mbps

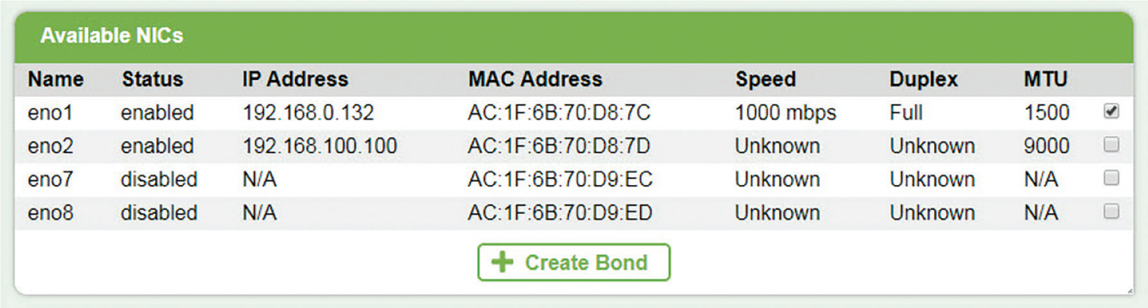
Available NICs

Name	Status	IP Address	MAC Address	Speed	Duplex	MTU	
eno2	enabled	192.168.100.100	AC:1F:6B:70:D8:7D	Unknown	Unknown	9000	□
eno8	disabled	N/A	AC:1F:6B:70:D9:ED	Unknown	Unknown	N/A	□

Select the page under the **Network > Bondings** menu item to edit and configure network hosts.

CREATE BOND

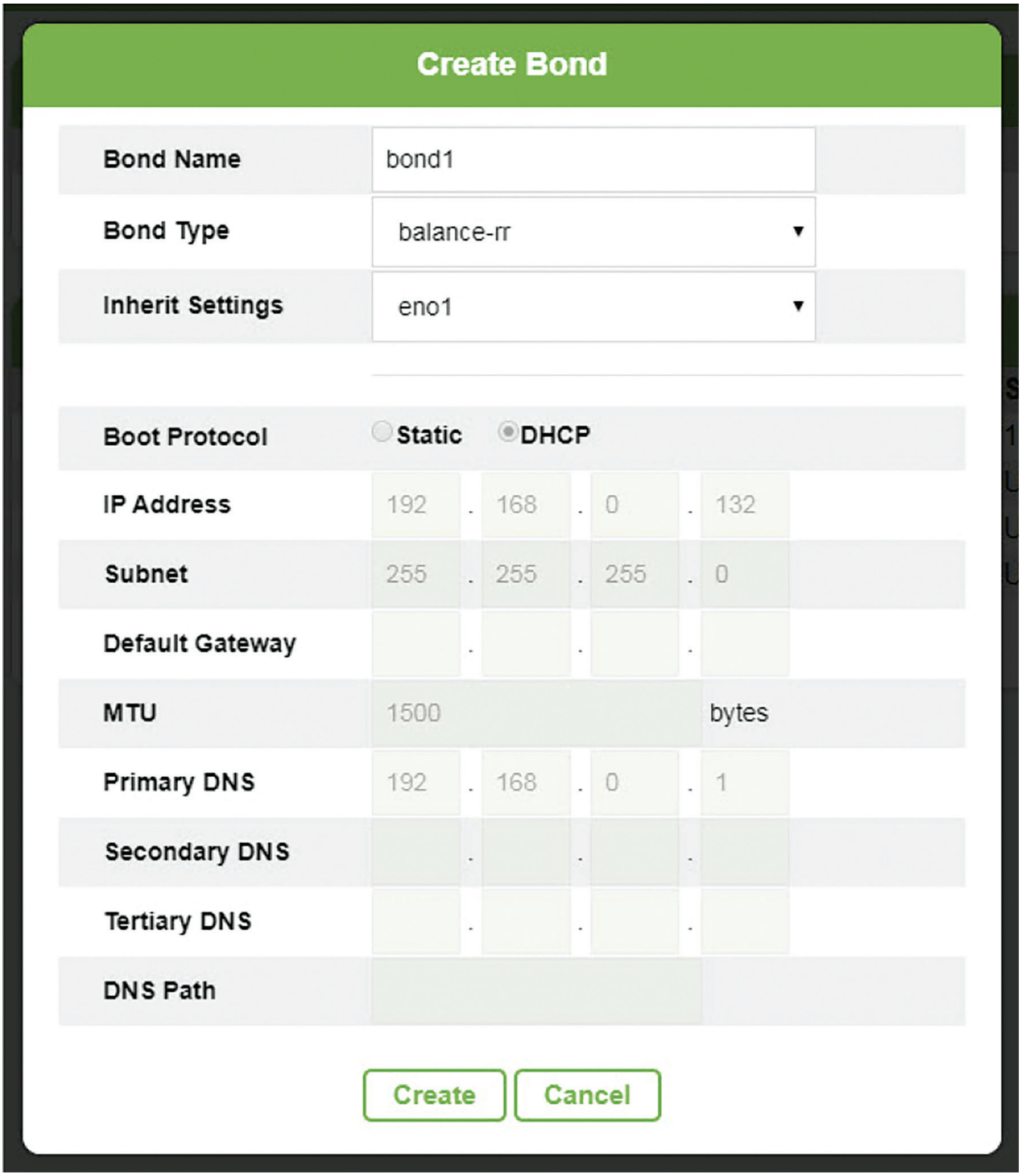
1. On the Bonding page in the **Available NICs** section, select the NICs to bond by selecting the checkbox at the end of the row.



Available NICs

Name	Status	IP Address	MAC Address	Speed	Duplex	MTU	
eno1	enabled	192.168.0.132	AC:1F:6B:70:D8:7C	1000 mbps	Full	1500	☑
eno2	enabled	192.168.100.100	AC:1F:6B:70:D8:7D	Unknown	Unknown	9000	□
eno7	disabled	N/A	AC:1F:6B:70:D9:EC	Unknown	Unknown	N/A	□
eno8	disabled	N/A	AC:1F:6B:70:D9:ED	Unknown	Unknown	N/A	□

2. Click on the **Create Bond** button to create a bond.
3. Fill in the following information and then click the **Create** button:



Create Bond

Bond Name	bond1
Bond Type	balance-rr ▾
Inherit Settings	eno1 ▾
Boot Protocol	○ Static ● DHCP
IP Address	192 . 168 . 0 . 132
Subnet	255 . 255 . 255 . 0
Default Gateway	. . .
MTU	1500 bytes
Primary DNS	192 . 168 . 0 . 1
Secondary DNS	. . .
Tertiary DNS	. . .
DNS Path	

Bond Name	The name of the bond that is being created.
Bond Type	The type of bond being created. Choose from: balance-rr, active-backup, balance-xor, broadcast, 802.3ad, balance-tlb, or balance-alb.

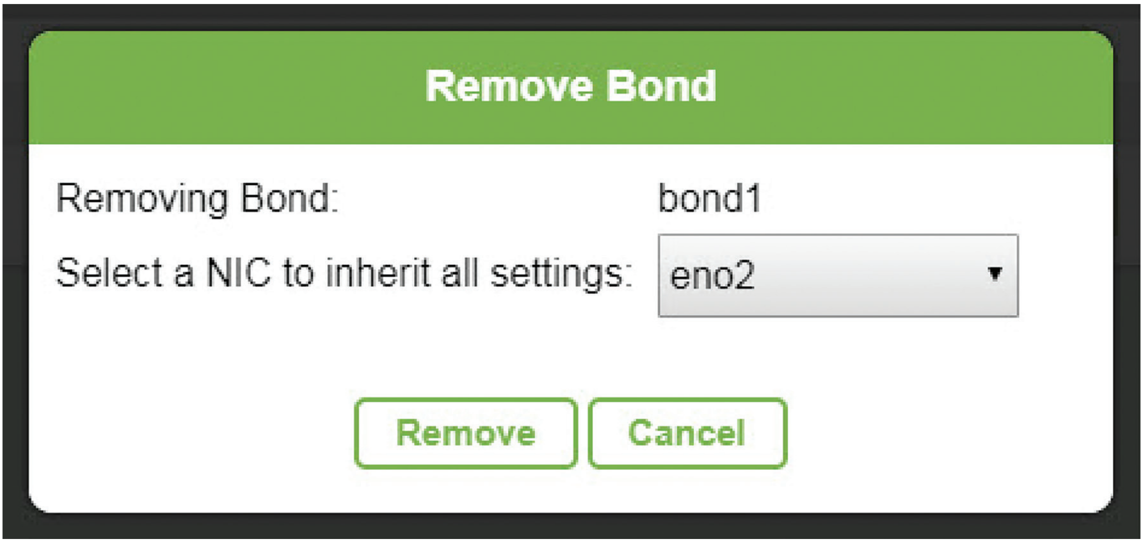
Inherit Settings	Choose a NIC to inherit settings from or choose Custom to input your own settings. **Note:** If you choose to inherit settings from an existing NIC, the rest of the bond settings will not be modifiable.
Boot Protocol	Choose between Static and DHCP.
IP Address	Enter a valid IPv4 address.
Subnet	Enter the subnet mask.
Default Gateway	The gateway entered for the last configured IPv4 connection sets the default gateway for the SecureNAS unit.
MTU	Default is 1500. Only change this value if you are sure that your switch configuration supports larger MTU settings, as well as all the hosts on the network.
Primary DNS	The IP address of the primary DNS. **Optional.**
Secondary DNS	The IP address of the secondary DNS. In a case where there is a problem with the primary DNS, the secondary DNS will be used. **Optional.**
Tertiary DNS	The IP address of the secondary DNS. In a case where there is a problem with the primary DNS and the secondary DNS, the tertiary DNS will be used. **Optional.**
DNS Path	This is the resolvable domain name for the primary DNS. **Optional.**

Note:

- Creating new bonds will require a system reboot.
- Be cautious when creating new NIC bonds. Incorrect configurations could cause SecureNAS to become unreachable.

DELETE BOND

1. On the Bonding page in the **Bonds** section, find the bond that you want to delete. Then click on the red trashcan icon 🗑 to delete that bond.



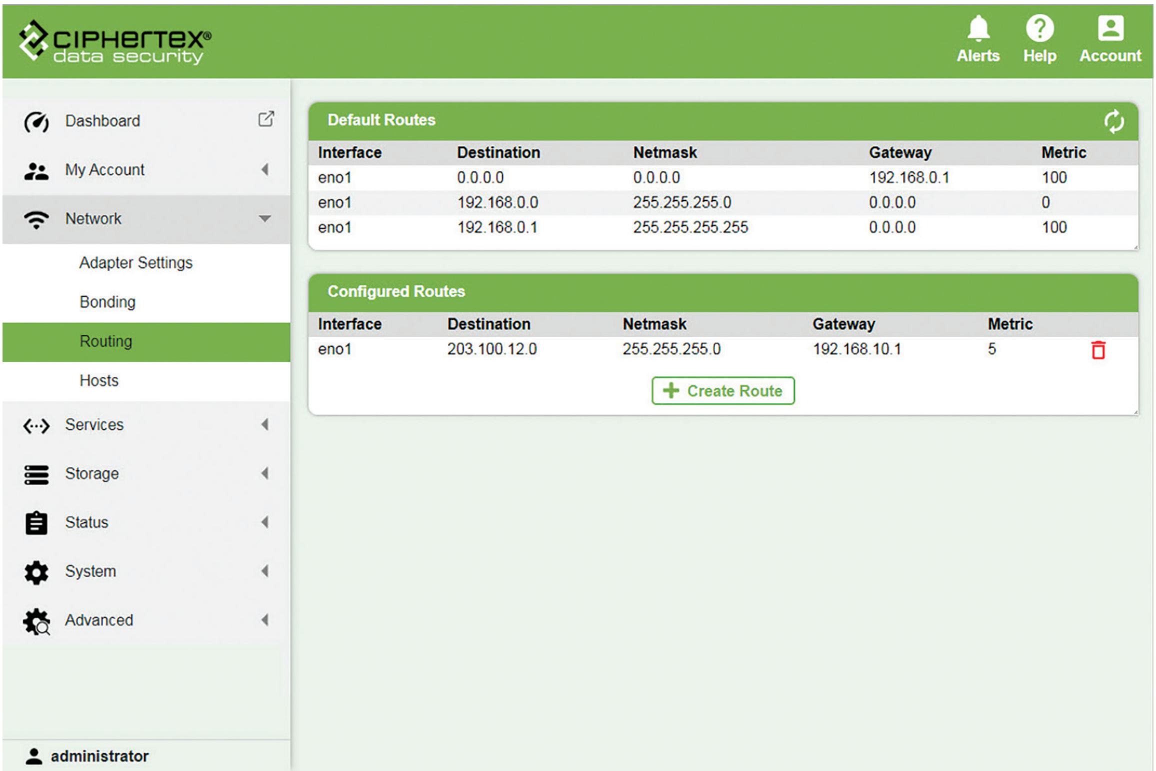
Remove Bond

Removing Bond: bond1

Select a NIC to inherit all settings: eno2

2. In the Remove Bond pop-up, select the NIC to inherit settings.
3. Click the **Remove** button.

4.4 Static Routes



Default Routes

Interface	Destination	Netmask	Gateway	Metric
eno1	0.0.0.0	0.0.0.0	192.168.0.1	100
eno1	192.168.0.0	255.255.255.0	0.0.0.0	0
eno1	192.168.0.1	255.255.255.255	0.0.0.0	100

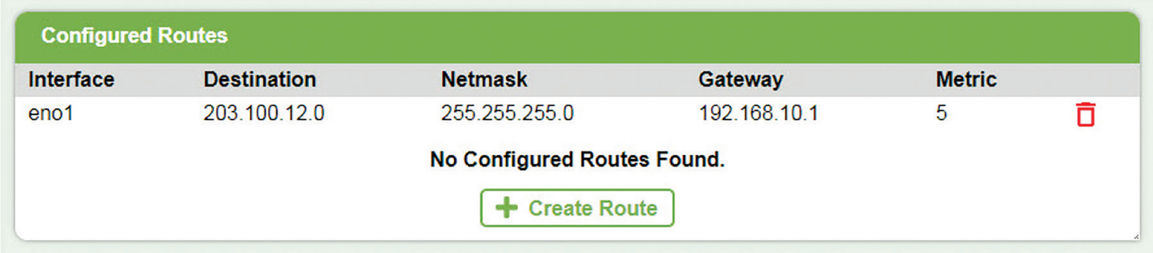
Configured Routes

Interface	Destination	Netmask	Gateway	Metric
eno1	203.100.12.0	255.255.255.0	192.168.10.1	5

Select the page under the **Network > Routing** menu item to configure static routes.

CONFIGURE STATIC ROUTES

1. On the Routing page in the **Configured Routes** section, click the **Create Route** button.

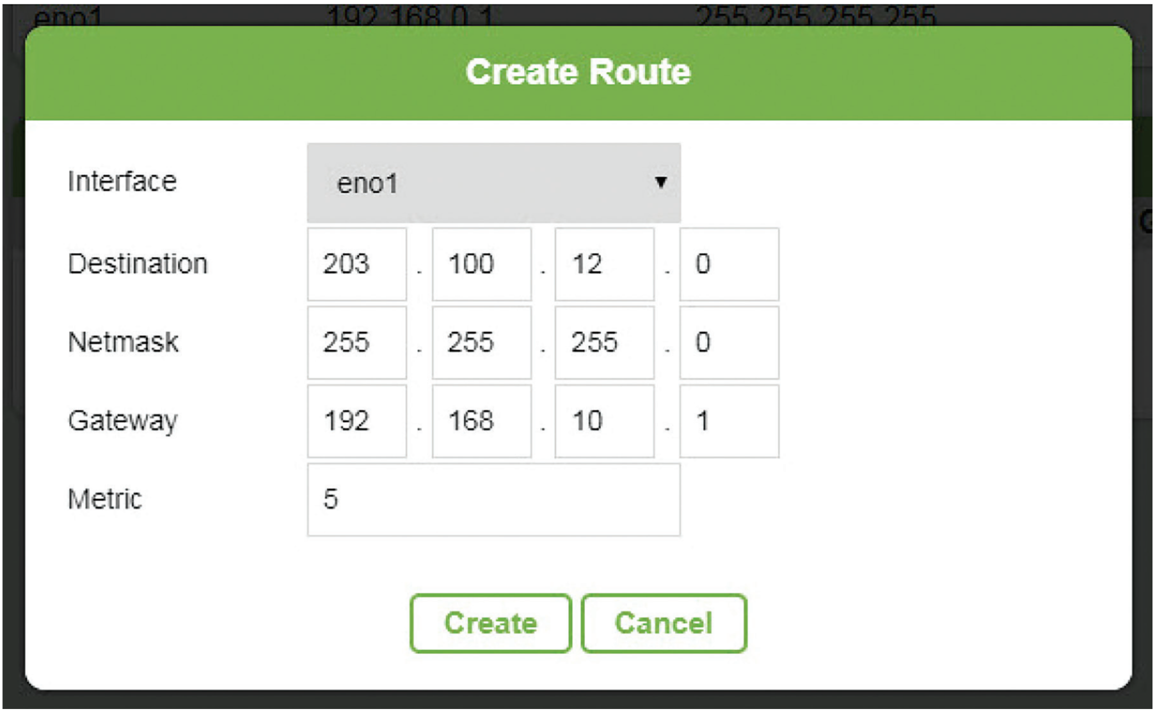


Configured Routes

Interface	Destination	Netmask	Gateway	Metric
eno1	203.100.12.0	255.255.255.0	192.168.10.1	5

No Configured Routes Found.

2. Fill in the following information and then click the Create button:



Create Route

Interface: eno1

Destination: 203 . 100 . 12 . 0

Netmask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 10 . 1

Metric: 5

Interface	The NIC/Interface port for the route.
Destination	The destination to be used for the route. Enter a valid IPv4 address.
Netmask	The netmask to be used for the route.
Gateway	The gateway to be used for the route. Enter a valid IPv4 address.
Metric	The metric for the route. The metric is used to decide which route to take. A lower number represents the better route.

Note:

- Configuring new routes may require a system reboot.

DELETE ROUTE

1. On the Routing page in the **Configured Routes** section, find the route that you want to delete. Then click on the red trashcan icon 🗑 to delete that route.

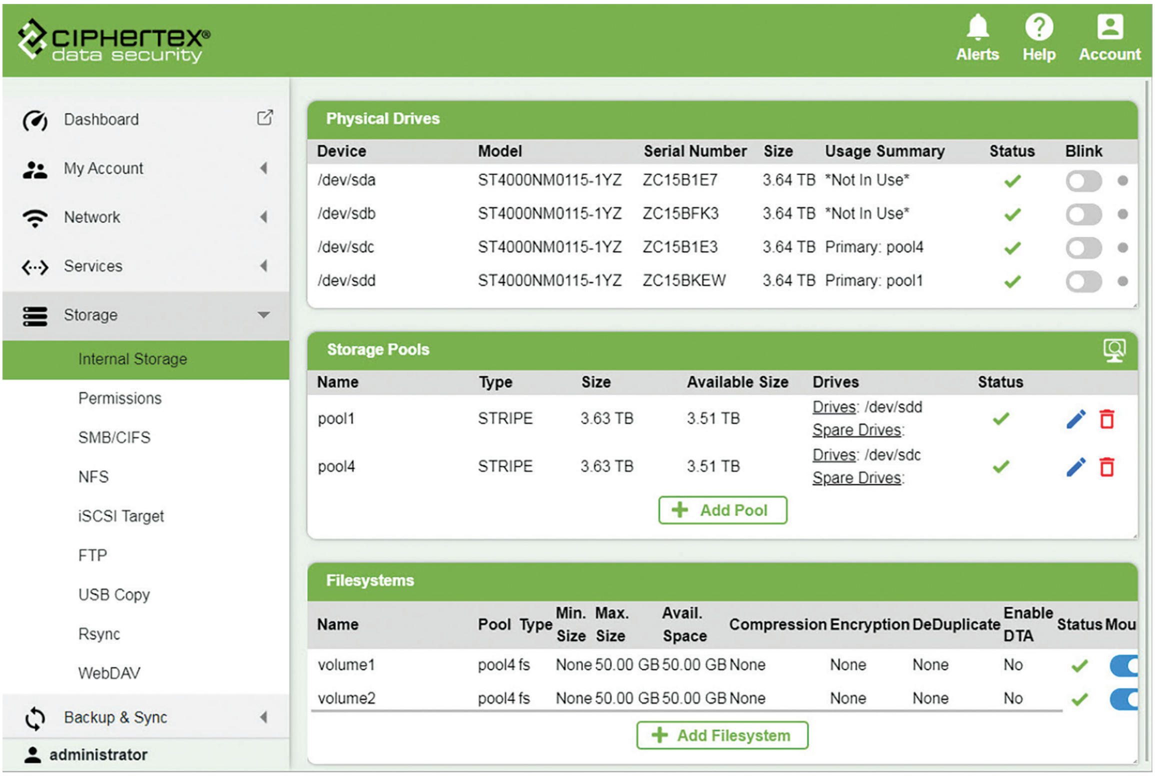
Note:

- Deleting routes may require a system reboot.

5 Configure 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.

5.1 Storage Pools and Volumes



Physical Drives

Device	Model	Serial Number	Size	Usage Summary	Status	Blink
/dev/sda	ST4000NM0115-1YZ	ZC15B1E7	3.64 TB	*Not In Use*	✓	
/dev/sdb	ST4000NM0115-1YZ	ZC15BFK3	3.64 TB	*Not In Use*	✓	
/dev/sdc	ST4000NM0115-1YZ	ZC15B1E3	3.64 TB	Primary: pool4	✓	
/dev/sdd	ST4000NM0115-1YZ	ZC15BKEW	3.64 TB	Primary: pool1	✓	

Storage Pools

Name	Type	Size	Available Size	Drives	Status
pool1	STRIPE	3.63 TB	3.51 TB	Drives: /dev/sdd Spare Drives:	✓
pool4	STRIPE	3.63 TB	3.51 TB	Drives: /dev/sdc Spare Drives:	✓

Filesystems

Name	Pool	Type	Min. Size	Max. Size	Avail. Space	Compression	Encryption	DeDuplicate	Enable DTA	Status	Mou
volume1	pool4	fs	None	50.00 GB	50.00 GB	None	None	None	No	✓	
volume2	pool4	fs	None	50.00 GB	50.00 GB	None	None	None	No	✓	

Select the page under the **Storage > Internal Storage** menu item to configure storage pools and volumes.

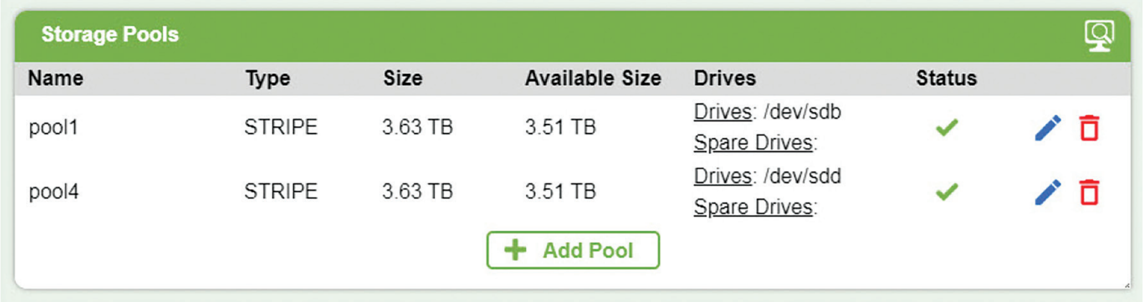
A volume is the basic storage space on your SecureNAS unit. A volume is created on a storage pool. Before creating a volume, you must first create a storage pool.

5.1.1 Storage Pools

Use the pages under the Network menu item to configure ethernet ports, change DNS settings, manage routes and bonding, and add/delete network hosts.

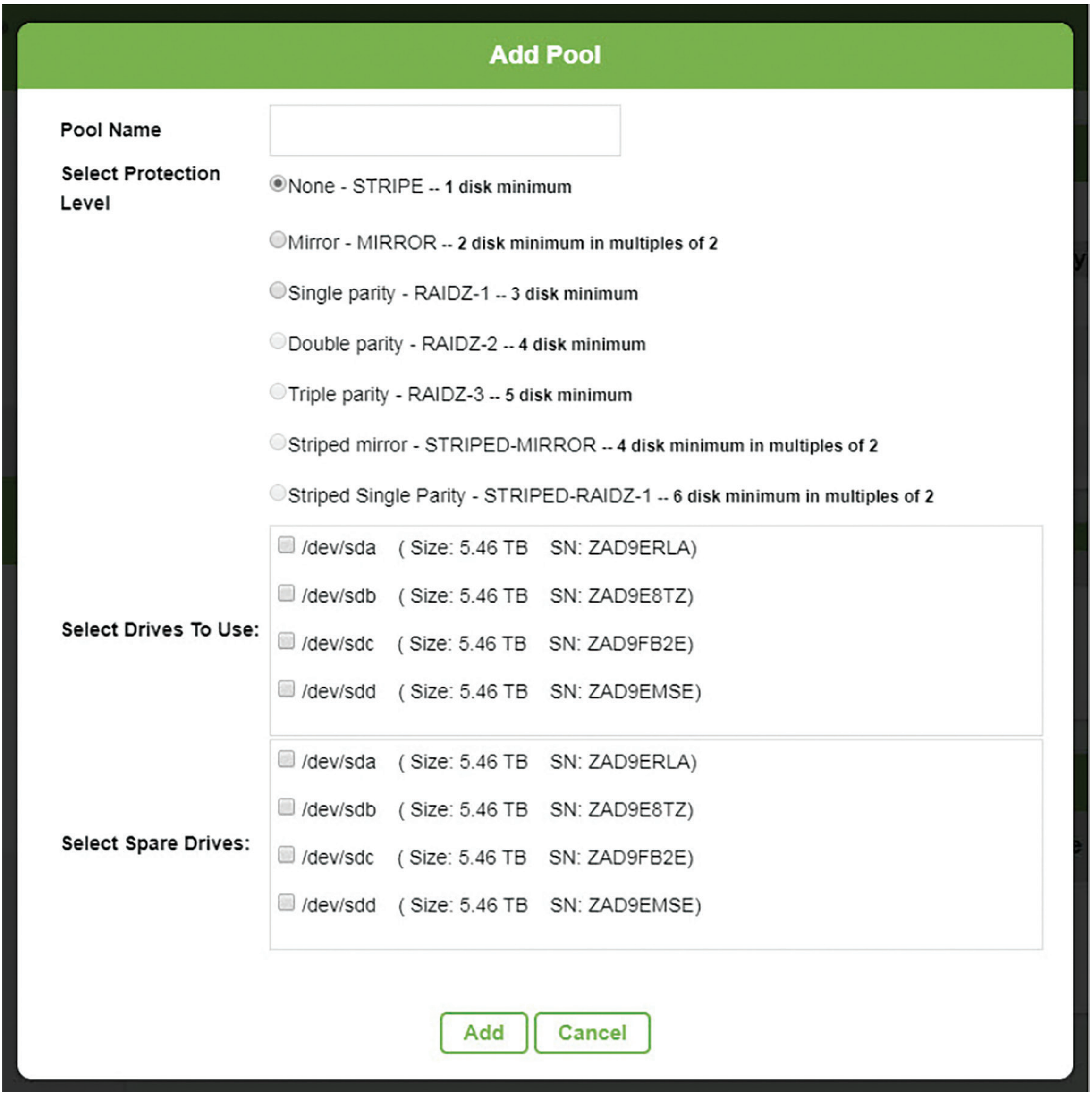
CREATE STORAGE POOLS

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



Storage Pools

Name	Type	Size	Available Size	Drives	Status	
pool1	STRIPE	3.63 TB	3.51 TB	Drives: /dev/sdb Spare Drives:	✓	✎ 🗑
pool4	STRIPE	3.63 TB	3.51 TB	Drives: /dev/sdd Spare Drives:	✓	✎ 🗑



Add Pool

Pool Name

Select Protection Level

● None - STRIPE -- 1 disk minimum

○ Mirror - MIRROR -- 2 disk minimum in multiples of 2

○ Single parity - RAIDZ-1 -- 3 disk minimum

○ Double parity - RAIDZ-2 -- 4 disk minimum

○ Triple parity - RAIDZ-3 -- 5 disk minimum

○ Striped mirror - STRIPED-MIRROR -- 4 disk minimum in multiples of 2

○ Striped Single Parity - STRIPED-RAIDZ-1 -- 6 disk minimum in multiples of 2

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)

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)

Pool Name	The name for the storage pool that is being added. The only special characters allowed are hyphens (-) and periods(.). No spaces are allowed. Each pool name must be unique.
Select Protection Level	Select from the following: • None - STRIPE: 1 disk minimum. The pool is configured for maximum speed, not to provide data protection. Any drive failure will result in data loss. Can be expanded in one drive increments.

	• Mirror - MIRROR: 2 disks. Data is mirrored across two drives. This type of RAID offers the best performance for small random reads and writes. Can tolerate a single drive failure without data loss. Cannot be expanded. • Single parity - RAIDZ-1: 3 disk minimum. Data is written across multiple drives with parity. Can tolerate one drive failure without data loss. This type of RAID has faster performance than double and triple parity based RAIDs. Can be expanded in one drive increments. • Double parity - RAIDZ-2: 4 disk minimum. Data is written across multiple drives with parity. Can tolerate two drive failures without data loss. In most cases, double parity provides a very good balance between data protection, performance, and storage capacity. Can be expanded in one drive increments. • Triple parity - RAIDZ-3: 5 disk minimum. Data is written across multiple drives with parity. Can tolerate three drive failures without data loss. This type of RAID provides the maximum data protection. Can be expanded in one drive increments. • Striped mirror - STRIPED-MIRROR: 4 disk minimum, in multiples of 2. Data is protected by striping data across mirrors of 2 drives. Can tolerate failure as long as one drive in each mirrored pair is functional. Performance is best of supported configurations at the expense of needing the highest drive count. Can be expanded in two drive increments. • Striped single parity - STRIPED-RAIDZ-1: 6 disk minimum, in multiples of 2. Data is protected by striping data across two RAIDZ-1 arrays. Can tolerate one drive failure in each RAIDZ-1 array. Provides the best balance between data protection, performance, and storage capacity for supported configurations. Can be expanded in two drive increments.
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.

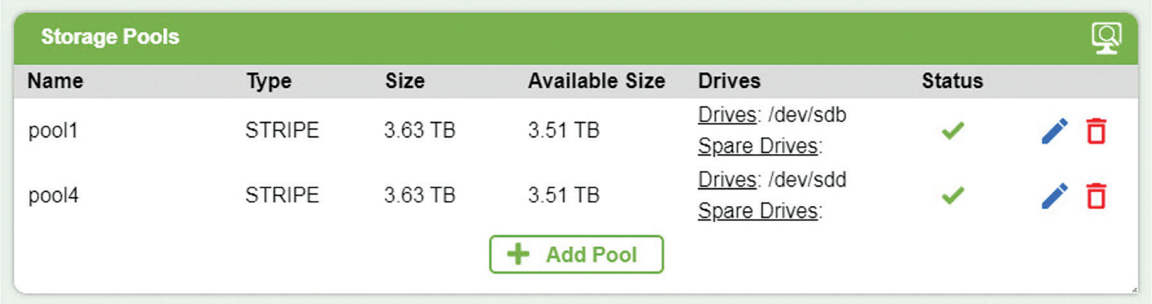
DELETE STORAGE POOLS

1. On the Internal Storage page in the **Storage Pools** section, select the storage pool you want to delete. This will highlight the row. Then click on the red trashcan icon 🗑 to delete that storage pool.
2. You will be required to input your login password to confirm that you want to delete this storage pool. Type your login password into the password textbox and then click the **Delete** button.

5.1.2 Add/Remove Drive from Storage Pool

ADD DRIVE TO STORAGE POOL

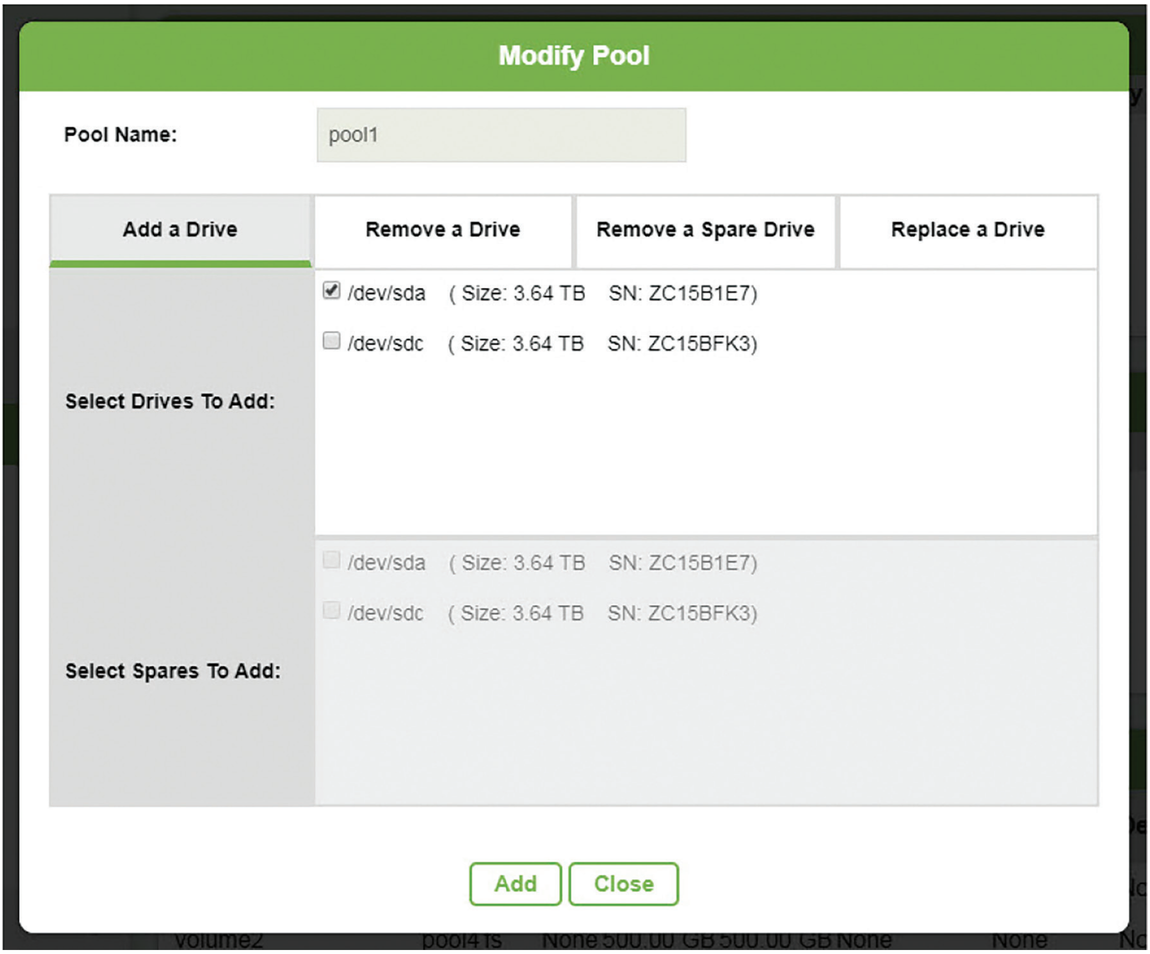
1. On the Internal Storage page in the **Storage Pools** section, click blue pen icon ✏ to modify that storage pool.



Storage Pools

Name	Type	Size	Available Size	Drives	Status	
pool1	STRIPE	3.63 TB	3.51 TB	Drives: /dev/sdb Spare Drives:	✓	✏ 🗑
pool4	STRIPE	3.63 TB	3.51 TB	Drives: /dev/sdd Spare Drives:	✓	✏ 🗑

2. On the Modify Pool pop-up, select Add a Drive from the tabs at the top.
3. Select a drive by clicking on the checkbox next to the name.
4. Click the Add button to add the selected drive to the storage pool.



Pool Name: pool1

Select Drives To Add:

☑ /dev/sda (Size: 3.64 TB SN: ZC15B1E7)

□ /dev/sdc (Size: 3.64 TB SN: ZC15BFK3)

Select Spares To Add:

□ /dev/sda (Size: 3.64 TB SN: ZC15B1E7)

□ /dev/sdc (Size: 3.64 TB SN: ZC15BFK3)

REMOVE DRIVE FROM STORAGE POOL

1. On the Internal Storage page in the **Storage Pools** section, click blue pen icon ✎ to modify that storage pool.
2. On the Modify Pool pop-up, select **Remove a Drive** from the tabs at the top.
3. Select a drive by clicking on the checkbox next to the name.
4. Click the **Remove** button to remove the selected drive from the storage pool.

REMOVE SPARE DRIVE FROM STORAGE POOL

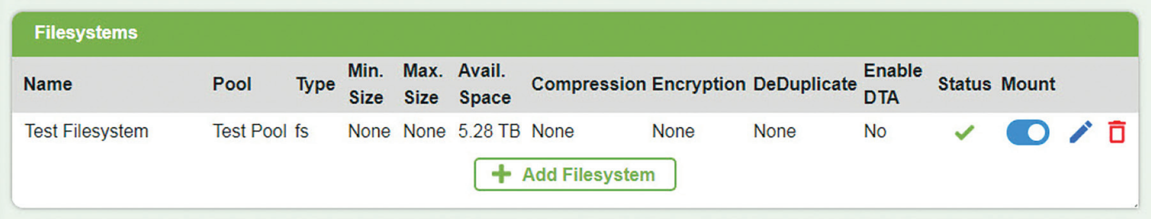
1. On the Internal Storage page in the **Storage Pools** section, click blue pen icon ✎ to modify that storage pool.
2. On the Modify Pool pop-up, select **Remove a Spare Drive** from the tabs at the top.
3. Select a drive by clicking on the checkbox next to the name.
4. Click the **Remove** button to remove the selected spare drive from the storage pool.

5.1.3 Volumes/Filesystems

CREATE FILESYSTEMS

> **Note:**
> - To create a filesystem that is encrypted, you must first insert a paired Ciphertex Protect® Key into the SecureNAS unit and then unlock it.

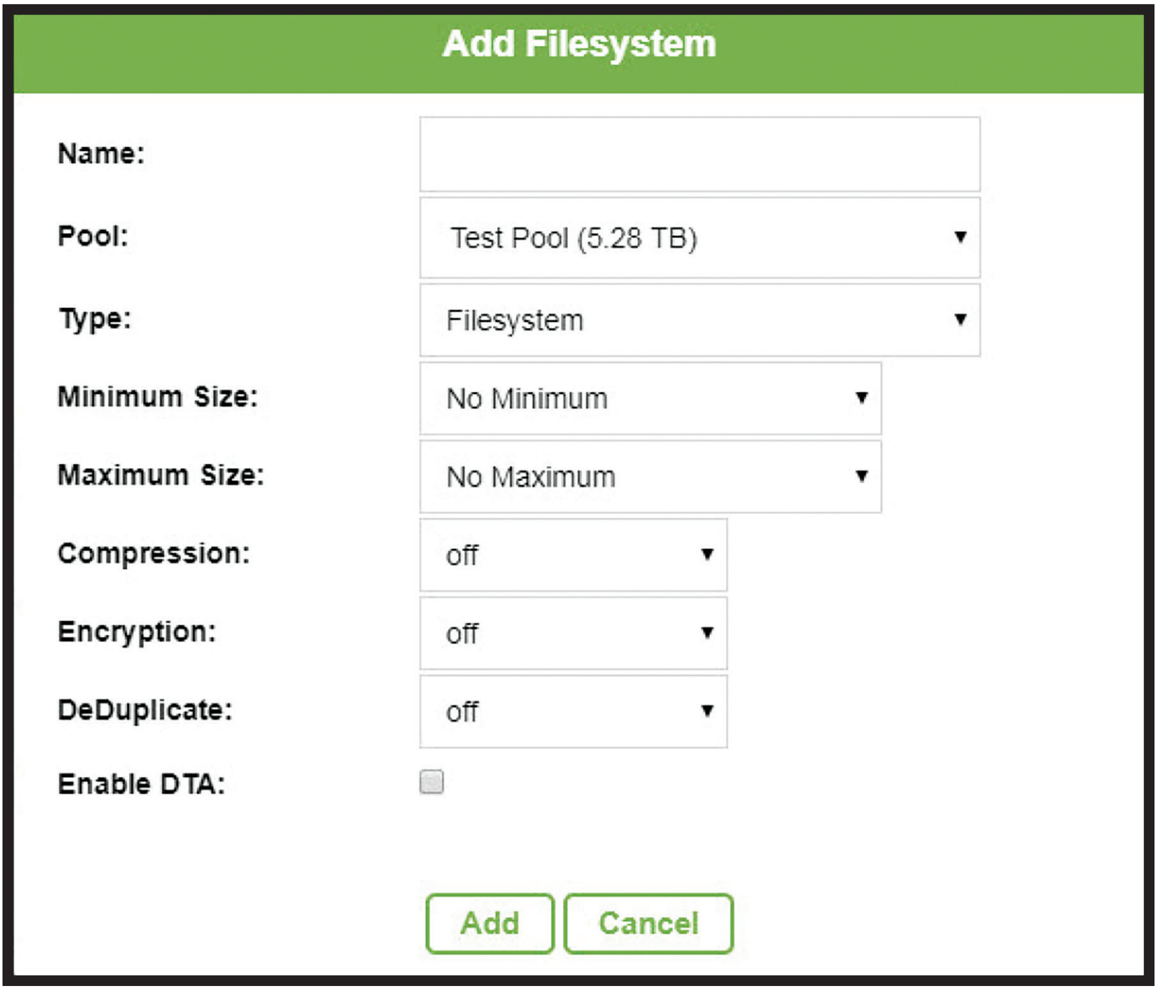
1. On the Internal Storage page in the **Filesystems** section, ✚ **Add Filesystem** button to create a filesystem.



Filesystems

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	✓	●	✎ 🗑

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



Add Filesystem

Name:	
Pool:	Test Pool (5.28 TB) ▾
Type:	Filesystem ▾
Minimum Size:	No Minimum ▾
Maximum Size:	No Maximum ▾
Compression:	off ▾
Encryption:	off ▾
DeDuplicate:	off ▾
Enable DTA:	☐

Name	The name for the filesystem being added. The only special characters allowed are hyphens (-) and periods(.). No spaces are allowed. Each filesystem name must be unique.
Pool	Select from the available storage pools that are configured on your SecureNAS system.
Type	Select from: • Filesystem • Raw
Minimum Size	Select the minimum size to be used for the filesystem: • 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: • 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: • 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: • off • aes-128-ccm • aes-192-ccm • aes-256-ccm • aes-128-gcm • aes-192-gcm • aes-256-gcm
DeDuplicate	Choose from the options: • off • sha256 • sha256-verify • sha512 • sha512-verify • skein • skein-verify • edonr • edonr-verify
Enable OTA	Enable/Disable date time access timestamp tracking.

MODIFY FILESYSTEMS

1. On the Internal Storage page in the **Filesystems** section, select the filesystem you want to modify. This will highlight the row. Then click on the blue pen icon ✏ to edit that filesystem.
2. Fill in and modify the information that you want to change.

Note:

- The filesystem name, pool name, filesystem type, and encryption type are not modifiable.

3. Click the **Save** button to save the changes for that filesystem.

DELETE FILESYSTEMS

1. On the Internal Storage page in the **Filesystems** section, select the filesystem you want to delete. This will highlight the row. Then click on the red trashcan icon 🗑 to delete that filesystem.
2. You will be required to input your login password to confirm that you want to delete this filesystem. Type your login password into the password textbox and then click the **Delete** button.

MOUNT/UNMOUNT 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 that filesystem.

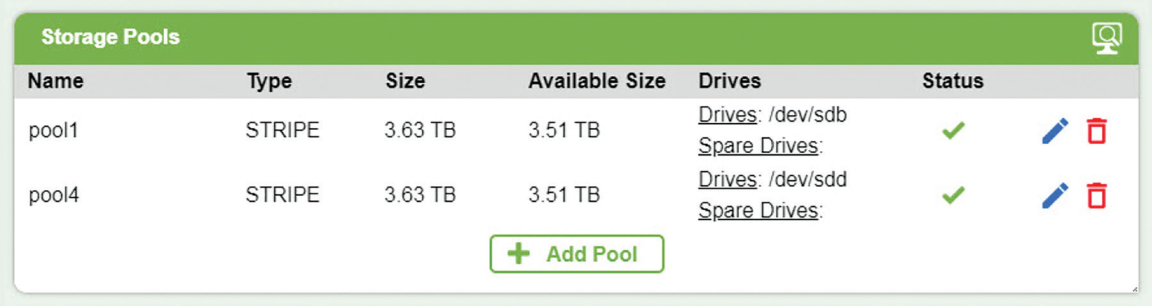
2.To unmount a filesystem, click on the toggle switch.

> **Note:**
>
> • To mount a filesystem that is encrypted, you must first insert a paired Ciphertex Protect® Key into the SecureNAS unit and then unlock it.

5.2 Replace a Drive

REPLACE DRIVE IN POOL

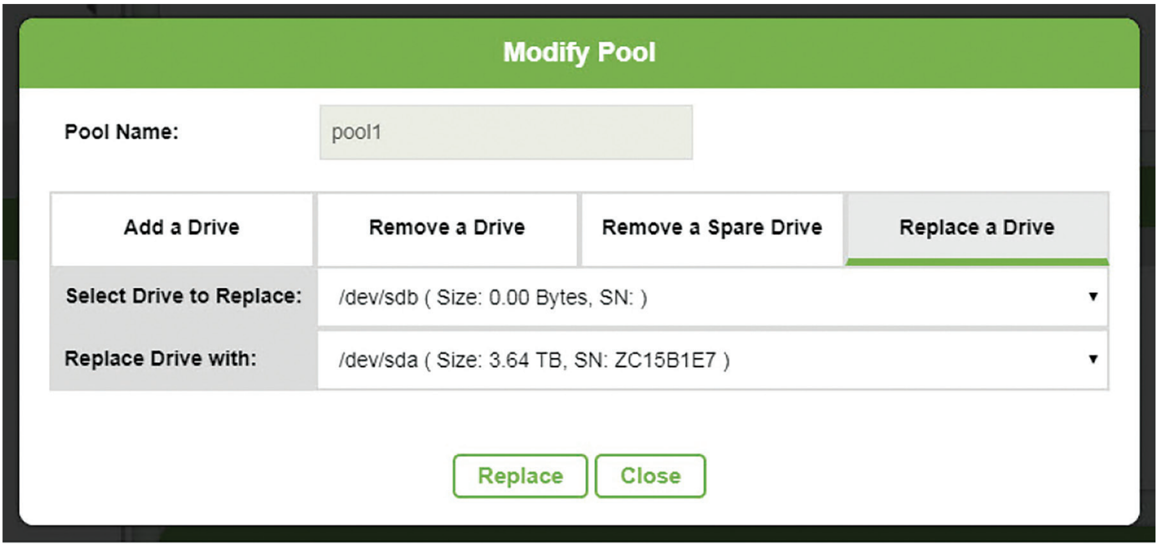
1. On the Internal Storage page in the **Storage Pools** section, click blue pen icon ✏ to modify that storage pool.



Storage Pools

Name	Type	Size	Available Size	Drives	Status	
pool1	STRIPE	3.63 TB	3.51 TB	Drives: /dev/sdb Spare Drives:	✓	✏ 🗑
pool4	STRIPE	3.63 TB	3.51 TB	Drives: /dev/sdd Spare Drives:	✓	✏ 🗑

2. On the Modify Pool pop-up, select **Replace a Drive** from the tabs at the top.
3. Select the drive to replace from the drop-down menu.
4. Select the replacement drive from the Replace Drive with drop-down menu.
5. Click the **Replace** button to replace the selected drive in the storage pool.



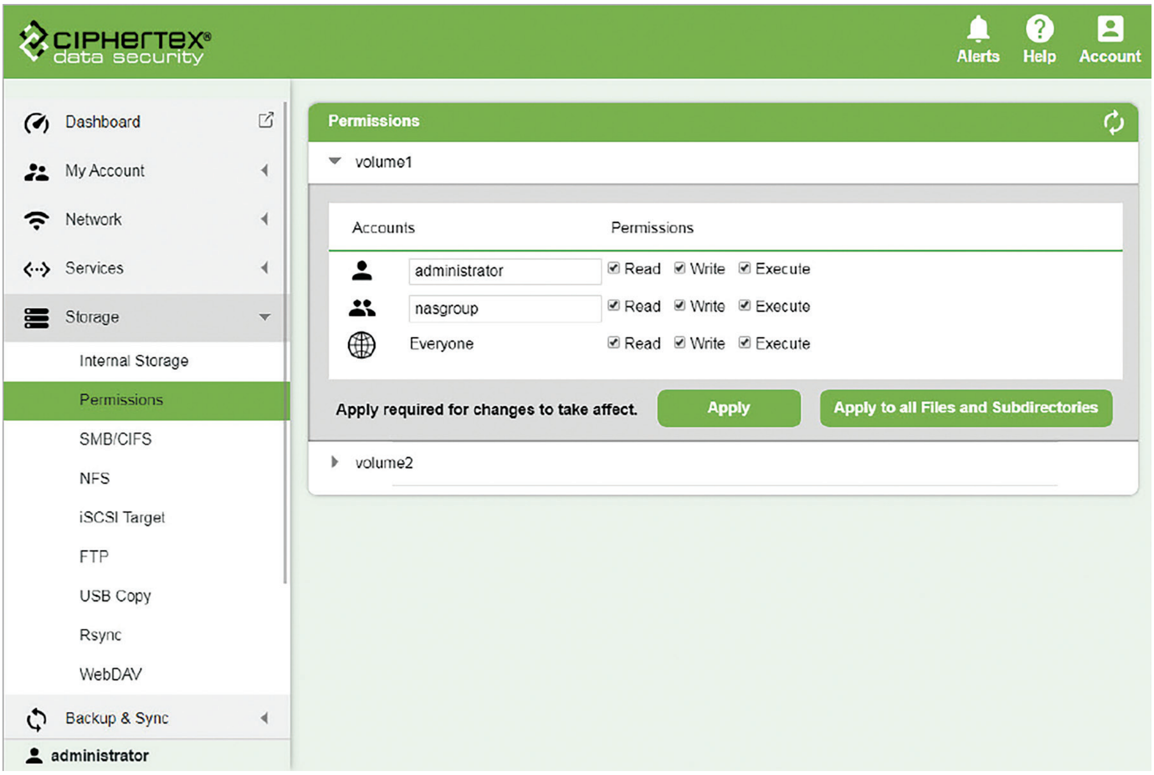
Modify Pool

Pool Name: pool1

Select Drive to Replace: /dev/sdb (Size: 0.00 Bytes, SN:)

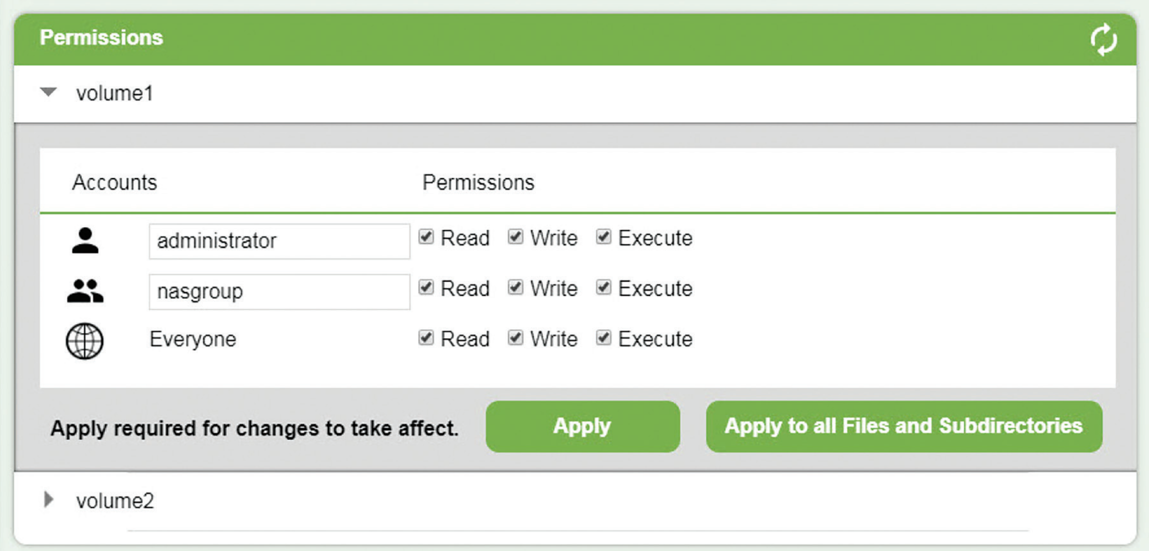
Replace Drive with: /dev/sda (Size: 3.64 TB, SN: ZC15B1E7)

5.3 Permissions for Volumes



Accounts	Permissions
administrator	☑ Read ☑ Write ☑ Execute
nasgroup	☑ Read ☑ Write ☑ Execute
Everyone	☑ Read ☑ Write ☑ Execute

Apply required for changes to take affect.



Accounts	Permissions
administrator	☑ Read ☑ Write ☑ Execute
nasgroup	☑ Read ☑ Write ☑ Execute
Everyone	☑ Read ☑ Write ☑ Execute

Apply required for changes to take affect.

CHANGE VOLUME OWNER & PERMISSIONS

1. On the Permissions page in the **Permissions** section, select the volume for which you want to edit permissions. This will expand the volume permissions information.
2. Click in the owner textbox 👥 to change the owner of the volume.
3. On the Set Owner pop-up, select the owner from the list of SecureNAS users.
4. Click the Set button.
5. Select the accompanying checkboxes to set the permissions for the owner.
6. Click the **Apply** button to save the changes and update the volume. Or click the **Apply to all Files and Subdirectories** button to apply the permissions changes to all files and directories on the selected volume.

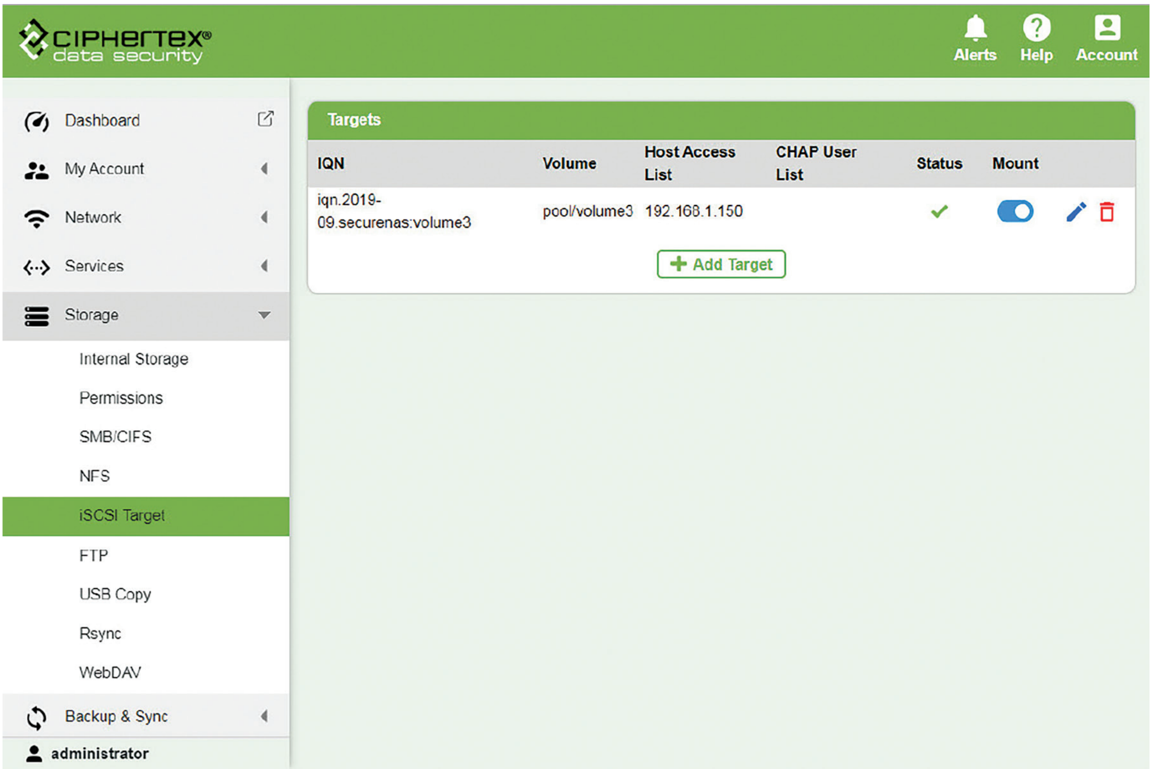
CHANGE VOLUME GROUP & PERMISSIONS

1. On the Permissions page in the **Permissions** section, select the volume for which you want to edit permissions. This will expand the volume permissions information.
2. Click in the owner textbox 👥 to change the group for the volume.
3. On the Set Group pop-up, select the group from the list of SecureNAS groups.
4. Click the Set button.
5. Select the accompanying checkboxes to set the permissions for the group.
6. Click the **Apply** button to save the changes and update the volume. Or click the **Apply to all Files and Subdirectories** button to apply the permissions changes to all files and directories on the selected volume.

CHANGE EVERYONE PERMISSIONS

1. On the Permissions page in the Permissions section, select the volume for which you want to edit permissions. This will expand the volume permissions information.
2. Select the accompanying checkboxes next to the Everyone 🌐 label to set the permissions everyone.
3. Click the A**pply** button to save the changes and update the volume. Or click the **Apply to all Files and Subdirectories** button to apply the permissions changes to all files and directories on the selected volume.

6 Manage iSCSI Targets

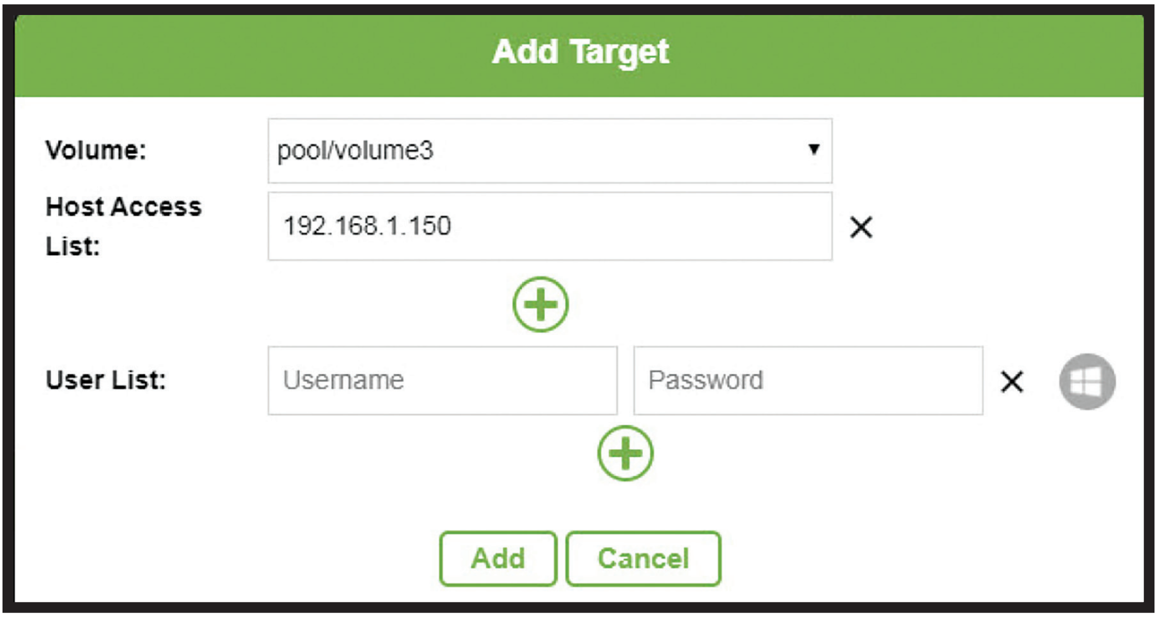


IQN	Volume	Host Access List	CHAP User List	Status	Mount
iqn.2019-09.securenas:volume3	pool/volume3	192.168.1.150		✓	●

Select the page under the **Storage > iSCSI Target** menu item to configure an iSCSI Target.

CONFIGURE ISCSI TARGETS

1. On the iSCSI Target page in the **Targets** section, click the **Add Target** button:



Volume: pool/volume3

Host Access List: 192.168.1.150

User List: Username Password

Volume	Select the volume to be configure as an iSCSI target.
Host Access List	Enter the IP address or servername of the host to be granted access. Click the green plus icon ➕ to add more hosts to the list.
User List	Enter the username and password of users to be granted access. Click the green plus icon ➕ to add more users to the list. **Note:** These users must be CHAP compliant. When the Windows icon on the right turns green, the password is CHAPS compliant.

Note:

- Only filesystems or volumes created as Raw Blocks can be used as iSCSI targets.
- Use the toggle switch ⏽ to mount and unmount an iSCSI target.

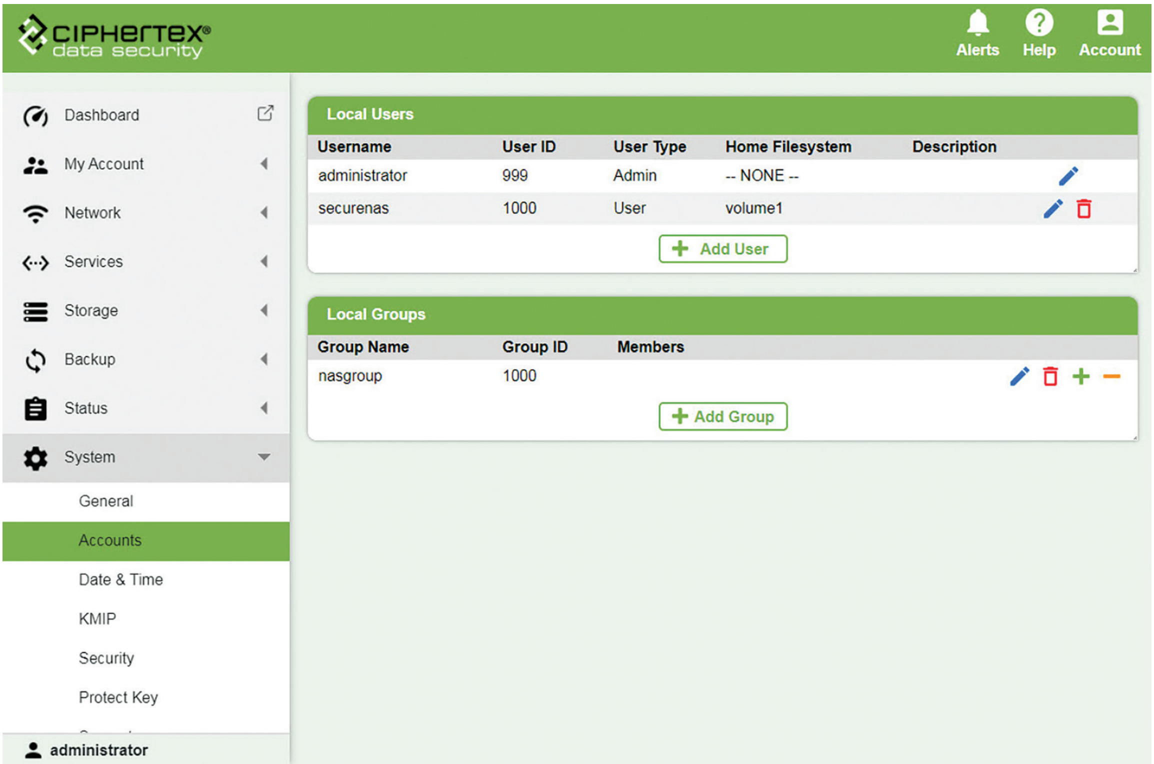
MODIFY ISCSI TARGET

1. On the iSCSI Target page in the **Targets** section, find the iSCSI target in the list that you want to modify. Then click on the blue pen icon ✏ to modify that target.
2. On the Modify Target, modify the information and then click the **Modify** button. Refer to the table above for field information.

DELETE ISCSI TARGET

1. On the iSCSI Target page in the **Targets** section, find the iSCSI target in the list that you want to delete. Then click on the red trashcan icon 🗑 to delete that target.

7 Manage Users and Groups



Local Users

Username	User ID	User Type	Home Filesystem	Description
administrator	999	Admin	-- NONE --	
securenas	1000	User	volume1	

Local Groups

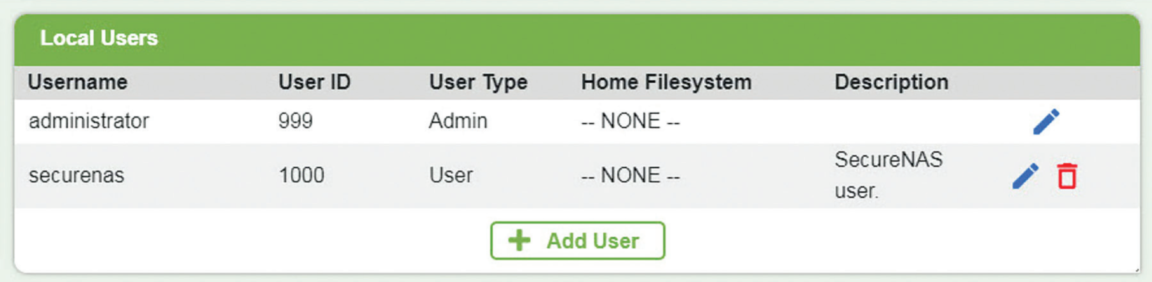
Group Name	Group ID	Members
nasgroup	1000	

Select the page under the **System > Accounts** menu item to manage users or groups.

7 Local Users

CREATE USERS

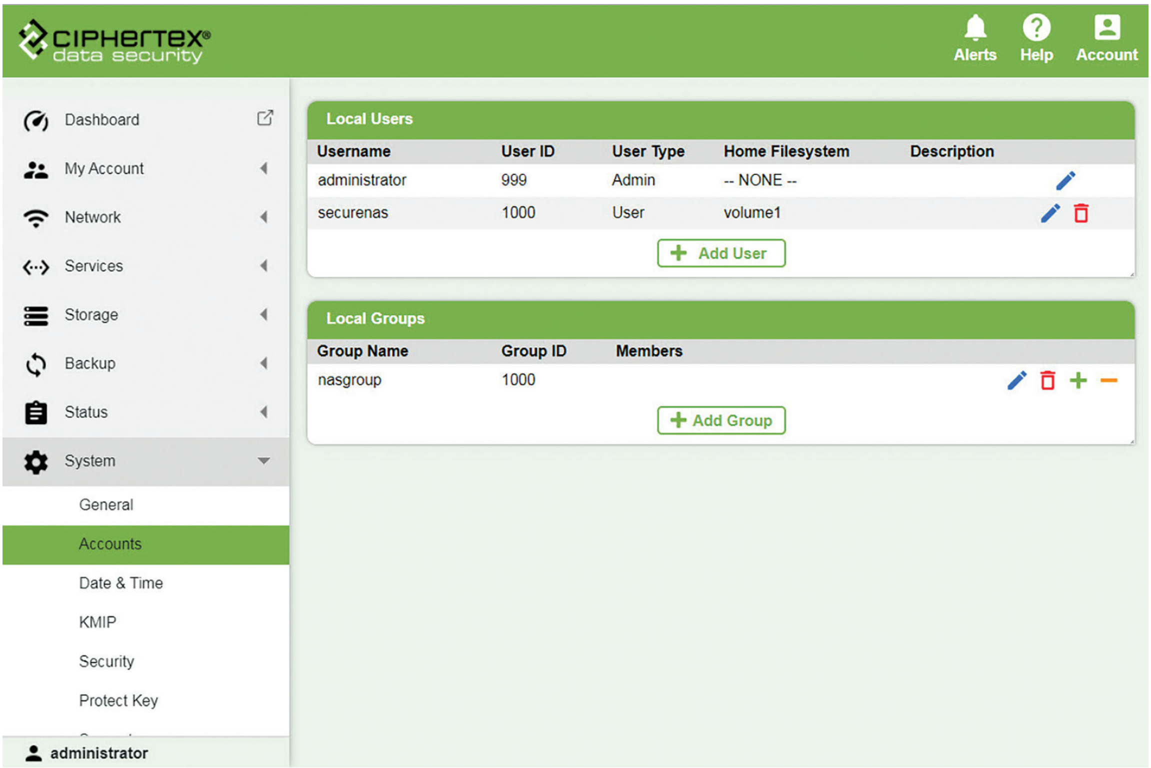
1. On the Accounts page in the **Local Users** section, click the + **Add User** button to create a user account. The user can log in to edit their account info after the user account has been established.



Local Users

Username	User ID	User Type	Home Filesystem	Description
administrator	999	Admin	-- NONE --	
securenas	1000	User	-- NONE --	SecureNAS user.

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



Local Users

Username	User ID	User Type	Home Filesystem	Description
administrator	999	Admin	-- NONE --	
securenas	1000	User	volume1	

Local Groups

Group Name	Group ID	Members
nasgroup	1000	

Username	The username for the user that is being added. A username must be between 1-31 characters and only contain a-z, A-Z, 0-9. No special characters or spaces are allowed.
User ID	Select **Auto-assign** to have SecureNAS assign an available user id. De-select Auto-assign to choose your own user id. Values must be between 1000-64999.
User Type	Choose between User, Power User, and Admin. **User:** A regular user. Will not be permitted to make changes or view settings in the SecureNAS Management Console. **Power User:** A user with privileges for viewing and editing a limited amount settings in the SecureNAS Management Console. **Admin:** A user with privileges to view and edit all settings in the SecureNAS Management Console.

Home Filesystem	Choose between None and the available filesystems. This home filesystem will be accessible only by this user. **Note:** Certain services, such as FTP, require a home filesystem. If None is selected, the user will be unable to use those services.
Description	General information about the user account. This field can contain things like the user's real name, phone number, etc.
Password	The password for the user account. **Note:** The user can log in to change their own password after their account is established.
Confirm Password	Re-type the password for the user account.

EDIT USER ACCOUNTS

1. On the Accounts page in the **Local Users** section, select the user whose account information you want to modify. This will highlight the row. Then click on the blue pen icon ✎ to edit that user's details.
2. On the Edit User pop-up, modify the information and then click the **Update** button. Refer to the table above for field information.

Note:

- The username and user id is not modifiable.
- If the user's home filesystem is changed, the old home filesystem will remain until it is removed by an admin user.
- If the Password fields are left blank during an edit, the password will be unchanged and will remain as the previously set password.

DELETE USER ACCOUNTS

1. On the Accounts page in the Local Users section, select the user whose account you want to delete. This will highlight the row. Then click on the red trashcan icon 🗑 to delete that user's account.

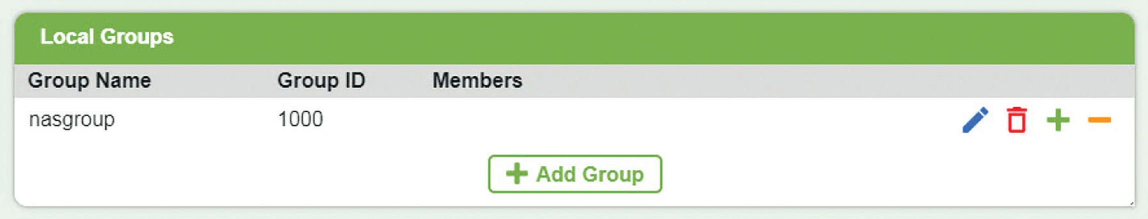
Note:

- The user's home filesystem will remain until it is removed by an admin user.
- The default administrator user cannot be deleted.

7.2 Local Groups

CREATE GROUPS

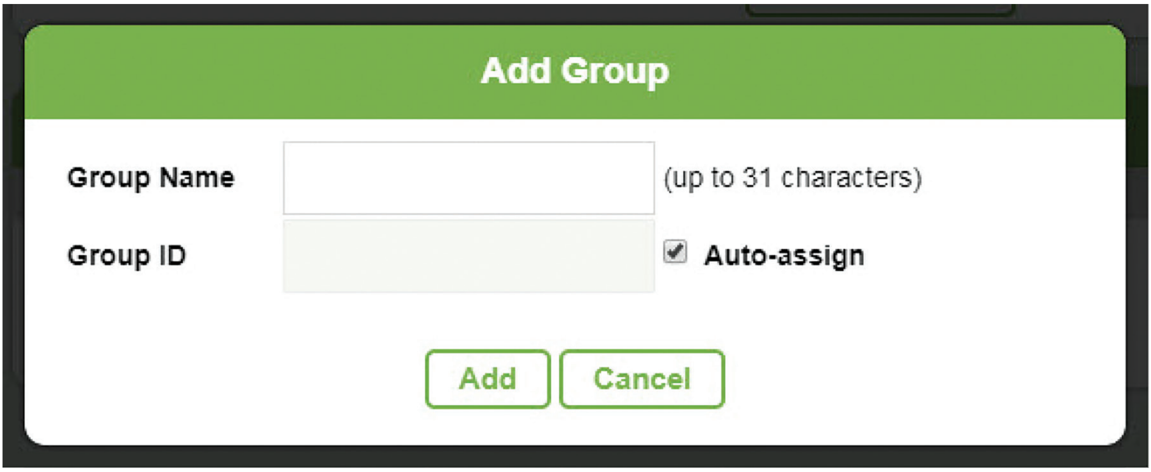
1. On the Accounts page in the **Local Groups** section, Click the ➕ **Add Group** button to create a new group.



Local Groups

Group Name	Group ID	Members
nasgroup	1000	

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



Add Group

Group Name (up to 31 characters)

Group ID ☑ Auto-assign

Group Name	The group name for the group that is being added. A group name must be between 1-31 characters and only contain a-z, A-Z, 0-9. No special characters or spaces are allowed.
Group ID	Select **Auto-assign** to have SecureNAS assign an available group id. De-select Auto-assign to choose your own group id. Values must be between 1000-64999.

ADD MEMBERS TO A GROUP

1. In the **Local Groups** section, select the group to which to add members. This will highlight the row.
2. Click on the green plus icon ➕ to add members to that group.
3. On the Add Members pop-up, select users from the available users list.
4. Click the **Add** button to add the selected members to the group.

> **Note:**
>
> • If no users are listed, you must add one or more new user accounts.

REMOVE MEMBERS FROM A GROUP

1. On the Accounts page in the Local Groups section, select the group from which to remove members. This will highlight the row. Then click on the orange minus icon ➖ to remove members from that group.
2. On the Remove Members pop-up, select users from the available users list.
3. Click the **Remove** button to remove the selected members from the group.

> **Note:**
>
> • If no users are listed, there are currently no members for that group.

DELETE GROUPS

1. On the Accounts page in the **Local Groups** section, select the group that you want to delete. This will highlight the row. Then click on the red trashcan icon 🗑 to delete that group.

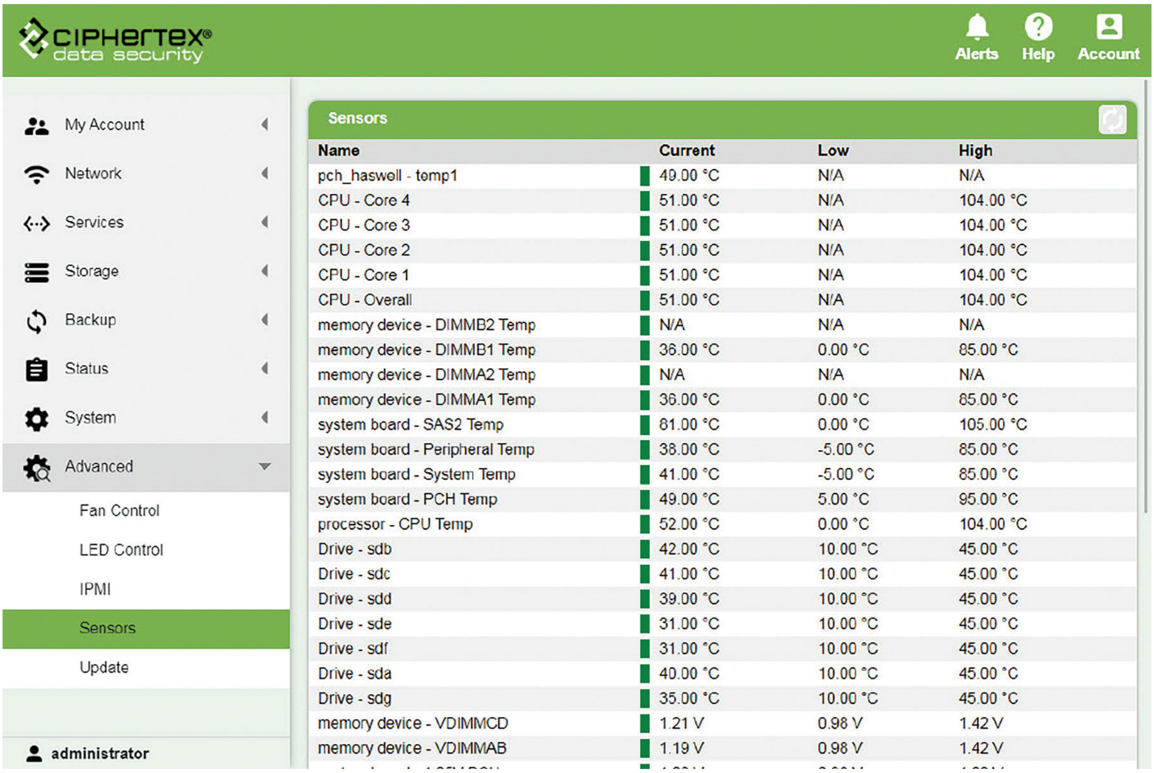
8 Upload and Access Files

SecureNAS can be a file sharing center within the local network or over the internet. Users can access files from anywhere, at anytime.

This section explains how to enable the support for file sharing protocols for different platforms, set up shared folders, and allow or deny access to the shared folders.

8.1 View System Information

8.1.1 Monitor Hardware Sensors



Name	Current	Low	High
pch_haswell - temp1	49.00 °C	N/A	N/A
CPU - Core 4	51.00 °C	N/A	104.00 °C
CPU - Core 3	51.00 °C	N/A	104.00 °C
CPU - Core 2	51.00 °C	N/A	104.00 °C
CPU - Core 1	51.00 °C	N/A	104.00 °C
CPU - Overall	51.00 °C	N/A	104.00 °C
memory device - DIMMB2 Temp	N/A	N/A	N/A
memory device - DIMMB1 Temp	36.00 °C	0.00 °C	85.00 °C
memory device - DIMMA2 Temp	N/A	N/A	N/A
memory device - DIMMA1 Temp	36.00 °C	0.00 °C	85.00 °C
system board - SAS2 Temp	81.00 °C	0.00 °C	105.00 °C
system board - Peripheral Temp	38.00 °C	-5.00 °C	85.00 °C
system board - System Temp	41.00 °C	-5.00 °C	85.00 °C
system board - PCH Temp	49.00 °C	5.00 °C	95.00 °C
processor - CPU Temp	52.00 °C	0.00 °C	104.00 °C
Drive - sdb	42.00 °C	10.00 °C	45.00 °C
Drive - sdc	41.00 °C	10.00 °C	45.00 °C
Drive - sdd	39.00 °C	10.00 °C	45.00 °C
Drive - sde	31.00 °C	10.00 °C	45.00 °C
Drive - sdf	31.00 °C	10.00 °C	45.00 °C
Drive - sda	40.00 °C	10.00 °C	45.00 °C
Drive - sdg	35.00 °C	10.00 °C	45.00 °C
memory device - VDIMMCD	1.21 V	0.98 V	1.42 V
memory device - VDIMMAB	1.19 V	0.98 V	1.42 V

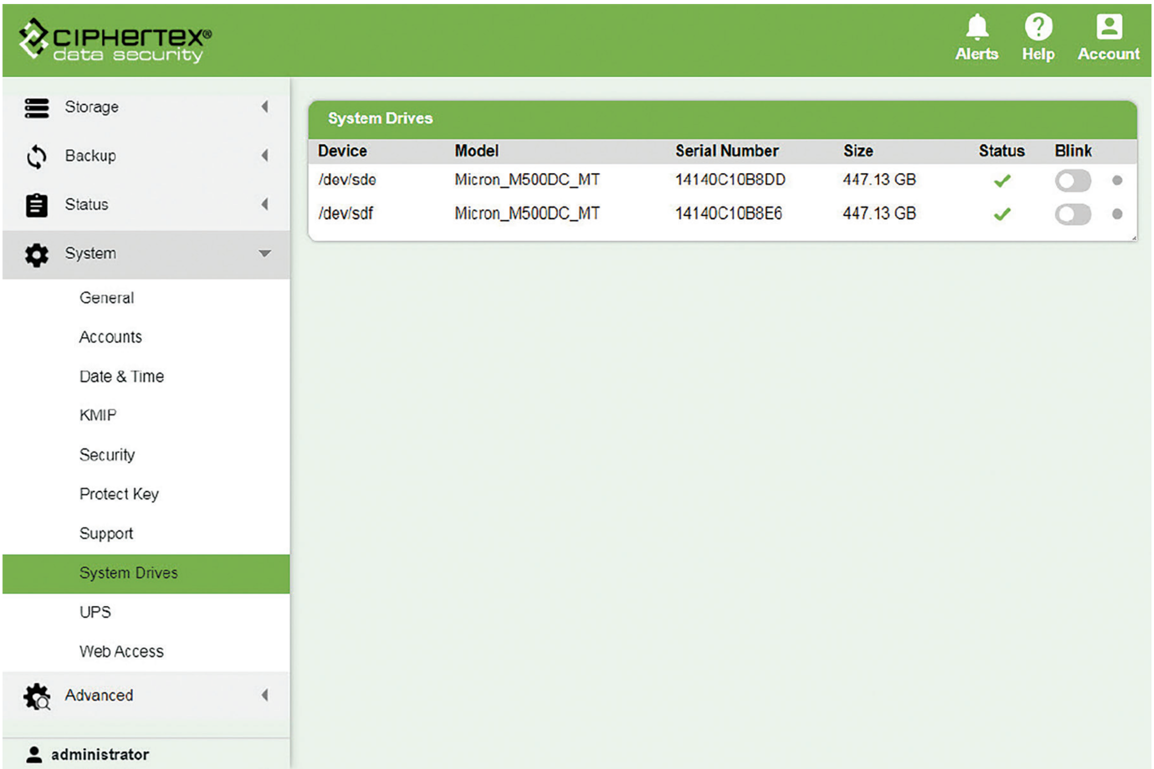
Select the page under the **Advanced > Sensors** menu item to view information about the hardware sensors in the SecureNAS unit. This page is for a view of system information and for diagnostic purposes.

SENSORS

1. View a list of sensors inside the SecureNAS unit. Use the table below to interpret data.
2. To enable continuous refresh of the information, click the refresh button in the upper right corner.

Name	The name of the sensor.
Current	The current reading of the sensor. This can be temperature, speed, etc. **Note:** A green indicator next to the Current value indicates a good status. Any other color indicates a value that is either out of range or getting close to being out of range.
Low	The minimum operating value recommended for the sensor.
High	The maximum operating value recommended for the sensor.

8.1.2 View Physical Drive Information



System Drives

Device	Model	Serial Number	Size	Status	Blink
/dev/sde	Micron_M500DC_MT	14140C10B8DD	447.13 GB	✓	○
/dev/sdf	Micron_M500DC_MT	14140C10B8E6	447.13 GB	✓	○

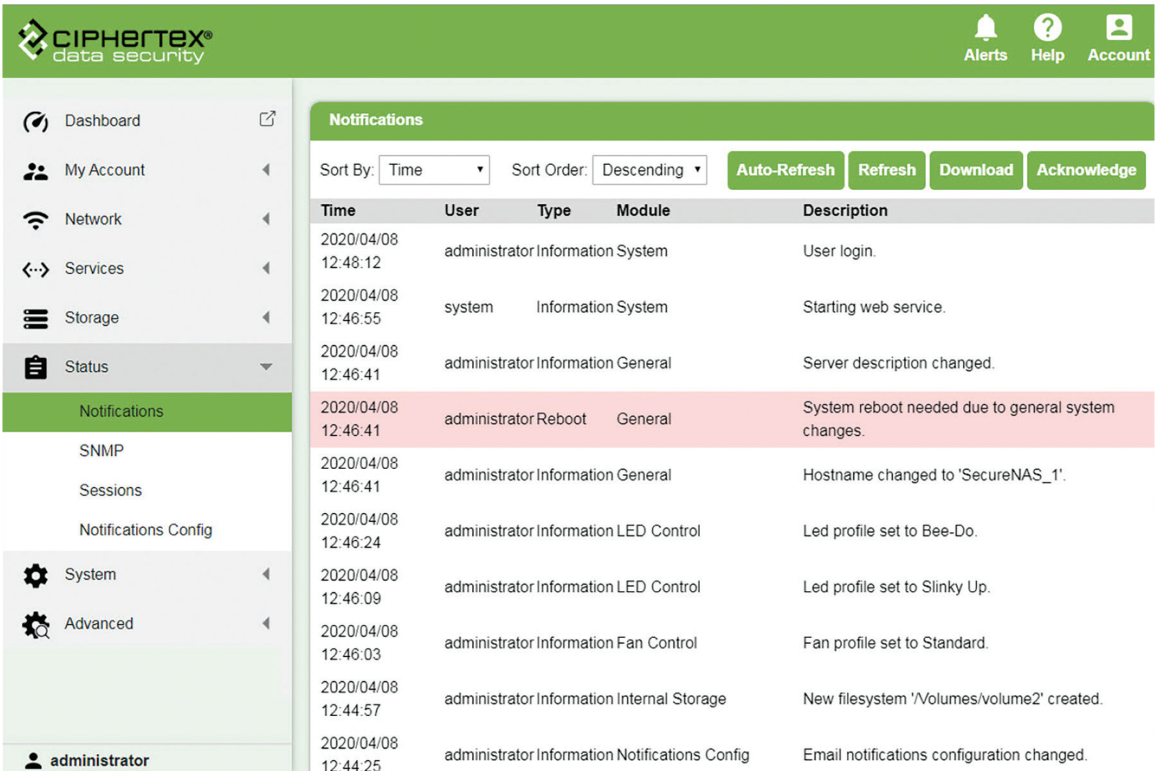
Select the page under the **System > System Drives** menu item to view information about the physical drives in the SecureNAS unit. These are the non-removable drives inside of the SecureNAS unit.

SYSTEM DRIVES

1. This is a list of the non-removable physical drives inside the SecureNAS unit. This information is for diagnostic purposes. Explanations for the list entries are in the table below.
2. Click the Blink toggle switch to have the blue LED blink above the selected drive.

Device	The name of the device.
Model	The model of the drive.
Serial Number	The serial number of the drive. The serial number will be included in any notifications pertaining to a failure of the drive.
Size	The total size of the drive.
Status	The green check icon ✓ indicates an "all good" status. For any other icon, see system notifications for any warnings and information.
Blink	Click the Blink toggle switch to have the blue LED light blink above the selected drive on the SecureNAS unit.

8.1.3 System Logs and Notifications



Sort By: Time Sort Order: Descending

Time	User	Type	Module	Description
2020/04/08 12:48:12	administrator	Information	System	User login.
2020/04/08 12:46:55	system	Information	System	Starting web service.
2020/04/08 12:46:41	administrator	Information	General	Server description changed.
2020/04/08 12:46:41	administrator	Reboot	General	System reboot needed due to general system changes.
2020/04/08 12:46:41	administrator	Information	General	Hostname changed to 'SecureNAS_1'.
2020/04/08 12:46:24	administrator	Information	LED Control	Led profile set to Bee-Do.
2020/04/08 12:46:09	administrator	Information	LED Control	Led profile set to Slinky Up.
2020/04/08 12:46:03	administrator	Information	Fan Control	Fan profile set to Standard.
2020/04/08 12:44:57	administrator	Information	Internal Storage	New filesystem '/Volumes/volume2' created.
2020/04/08 12:44:25	administrator	Information	Notifications Config	Email notifications configuration changed.

Select the page under the **Status > Notifications** menu item to view and acknowledge system notifications.

VIEW SYSTEM NOTIFICATIONS

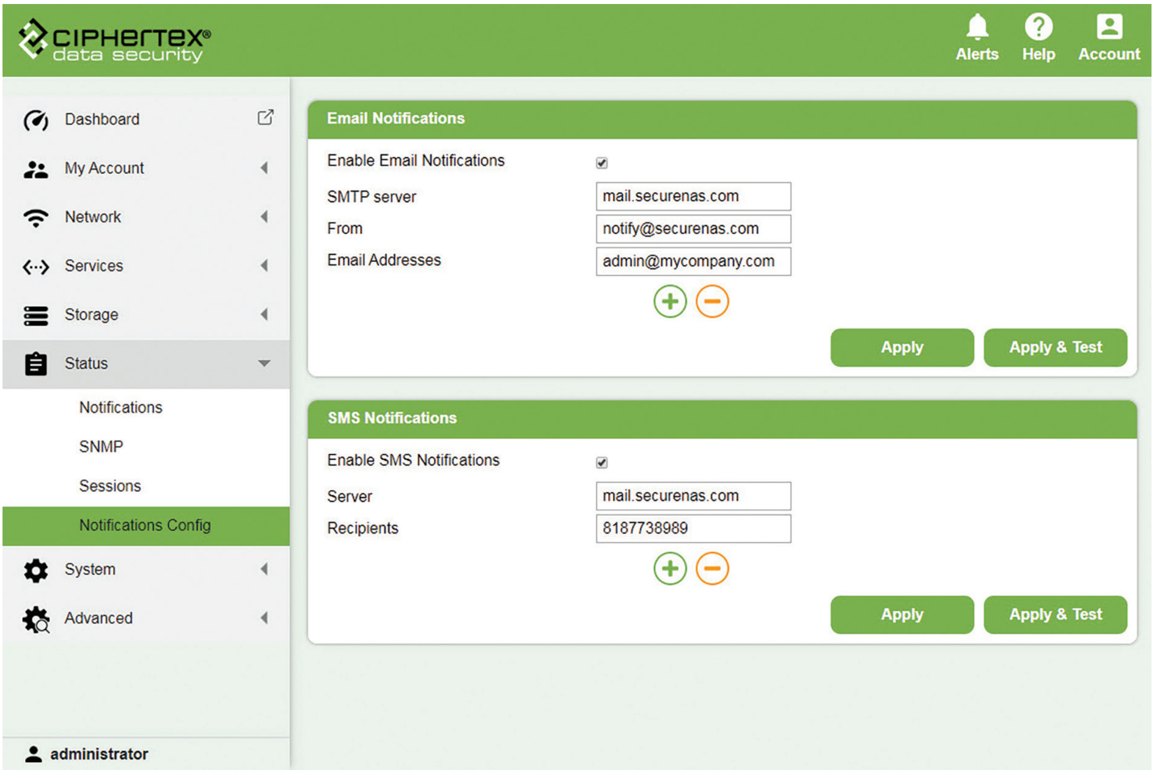
1. View a list of system notifications on the **Status > Notifications** page. Use the table below to interpret data.

Time	The time and date that the notification was given.
User	The username of the user logged in when the notification was given.
Type	The type of notifications: Information, Warning, Critical, and Reboot. **Note**: Critical and Reboot notifications are highlighted in red.
Module	The module that generated the notification.
Description	A short description of the notification.

Note:

- Select the Auto-Refresh button to continuously refresh the notifications page.
- Click the the Refresh button to refresh the notifications page once.
- Click the Download button to download the system notifications to a file.
- Click the Acknowledge button to dismiss any Alerts or critical messages.

8.1.3.1 Configure Notification Methods



Email Notifications

Enable Email Notifications	☑
SMTP server	mail.securenas.com
From	notify@securenas.com
Email Addresses	admin@mycompany.com

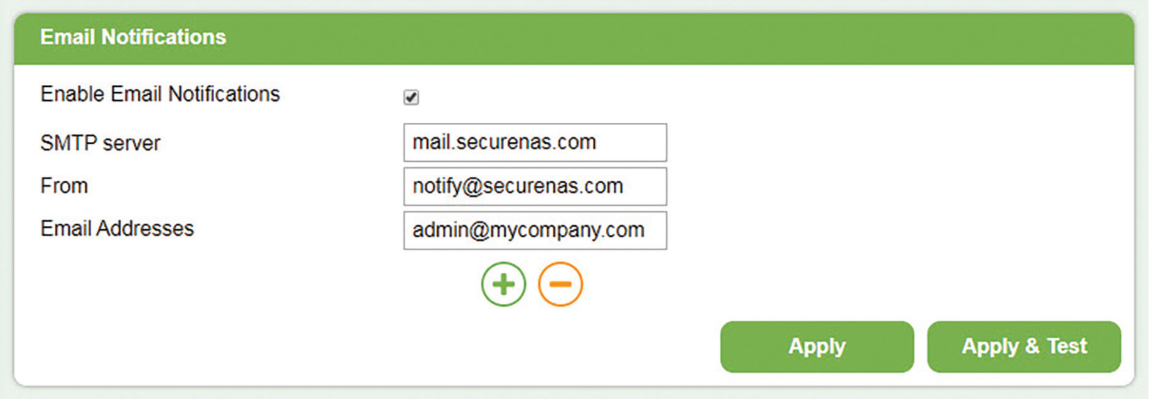
SMS Notifications

Enable SMS Notifications	☑
Server	mail.securenas.com
Recipients	8187738989

Select the page under the **Status > Notifications** Config menu item to manage system notification methods. Notifications are only sent out for Critical and Reboot notification types. To see all notifications and logs, go to the Status > Notifications page.

EMAIL NOTIFICATIONS

1. On the Notifications Config page in the **Email Notifications section**, fill out the Email Notifications section on the Notifications Config page. Then click the **Apply** button.
2. Click the Apply & Test button to save the settings and also send a test email to each email address in the list.



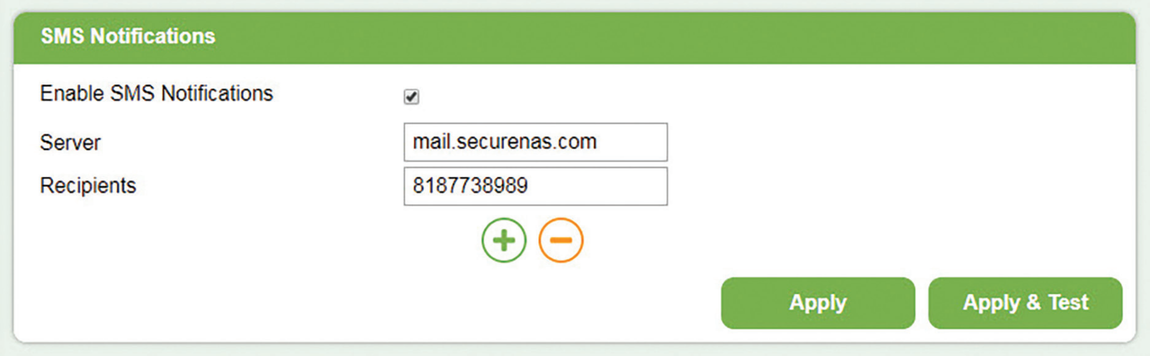
Email Notifications

Enable Email Notifications	☑
SMTP server	mail.securenas.com
From	notify@securenas.com
Email Addresses	admin@mycompany.com

Enable Email Notifications	Enable/disable notifications being sent via email.
SMTP Server	The SMTP server to be used to send email notifications.
From	The name/email address that will appear in the "from" section of the email.
Email Address	The email address of each recipient of the notification email. Click the green plus icon ➕ to add more recipients. Click the orange minus icon ➖ to delete recipients.

SMS NOTIFICATIONS

1. On the Notifications Config page in the **SMS Notifications** section, fill out the SMS Notifications section on the Notifications Config page. Then click the **Apply** button.
2. Click the **Apply & Test** button to save the settings and also send a test sms text message to each cell phone number in the recipient list.

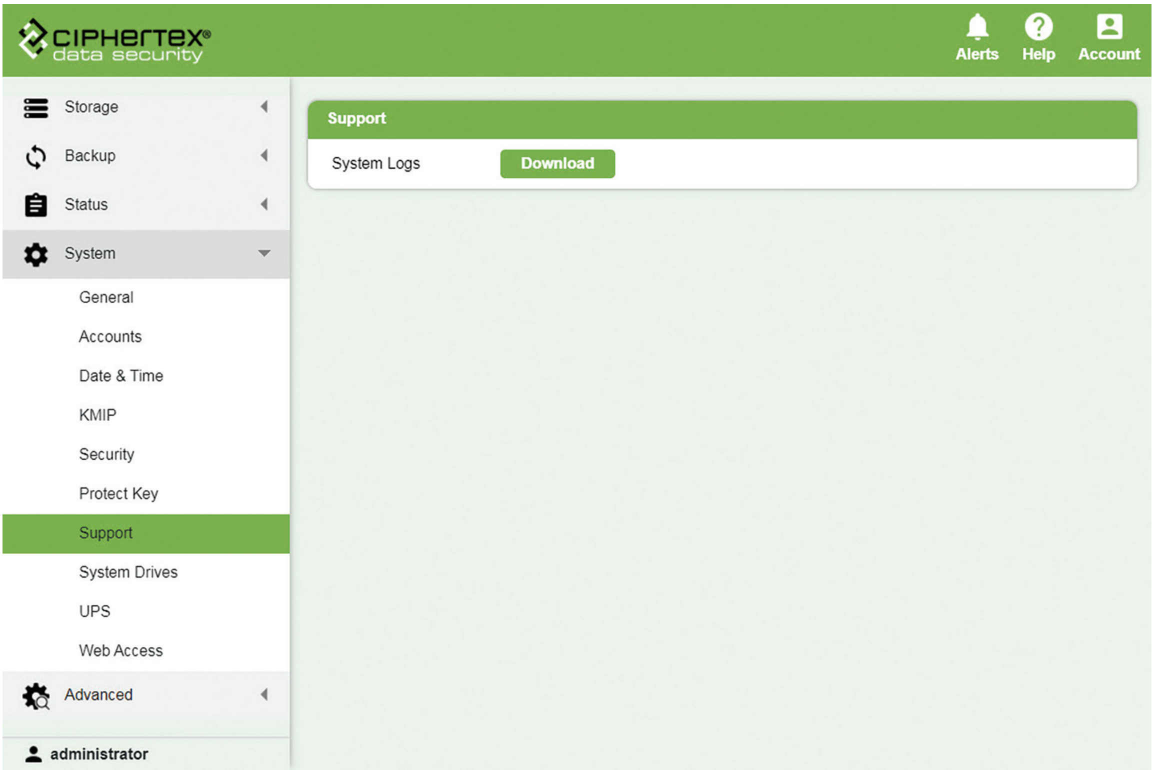


SMS Notifications

Enable SMS Notifications	☑
Server	mail.securenas.com
Recipients	8187738989

Enable SMS Notifications	Enable/disable notifications being sent via sms text message.
Server	The server to be used to send sms notifications. Note: This server must to have the ability to send email in order for sms notifications to function properly.
Recipients	The cell phone number of each recipient for the notification SMS text message. Click the green plus icon + to add more recipients. Click the orange minus icon − to delete recipients. **Note:** Cell phone numbers should be entered as numbers only.

8.1.3.2 Download All System Logs

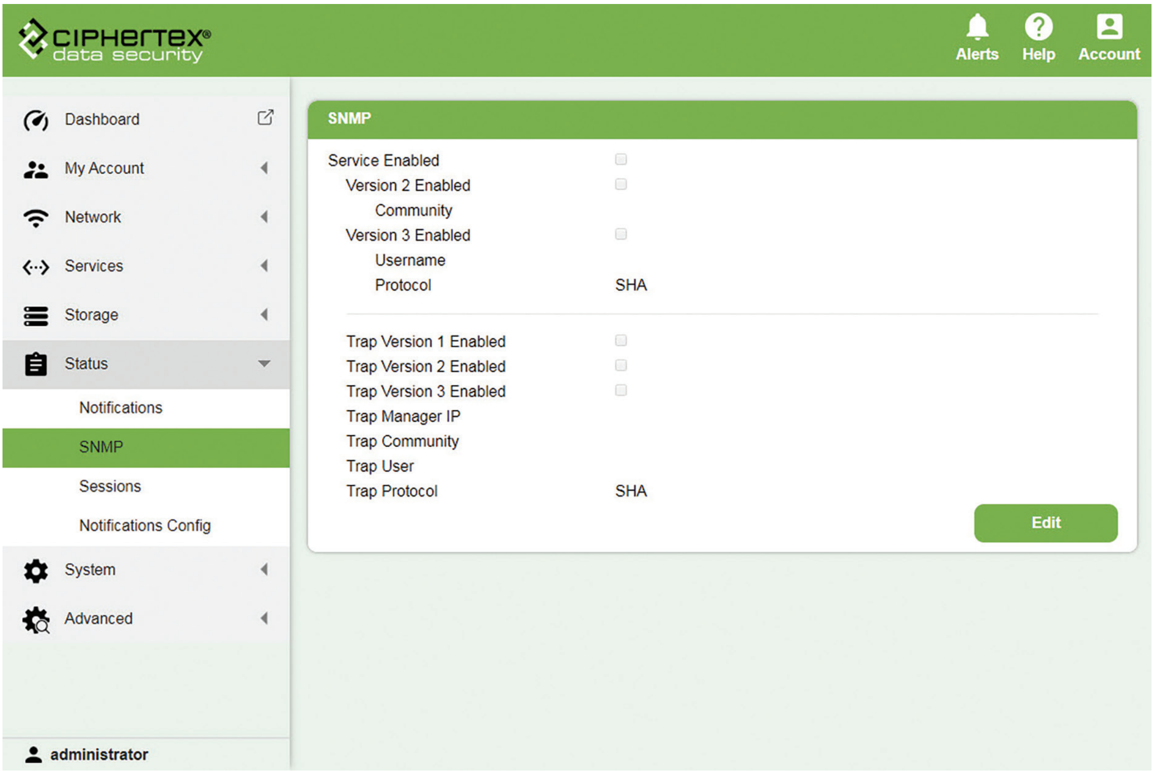


Select the page under the **System > Support** menu item to download all of the system logs to one zip file. These logs are used for diagnostic purposes and include information that is not presented on the Notifications page.

DOWNLOAD LOGS FOR SUPPORT

1. In the Support section of the Support page, click the **Download** button to download a zip file containing all of the system logs.

8.1.4 SNMP



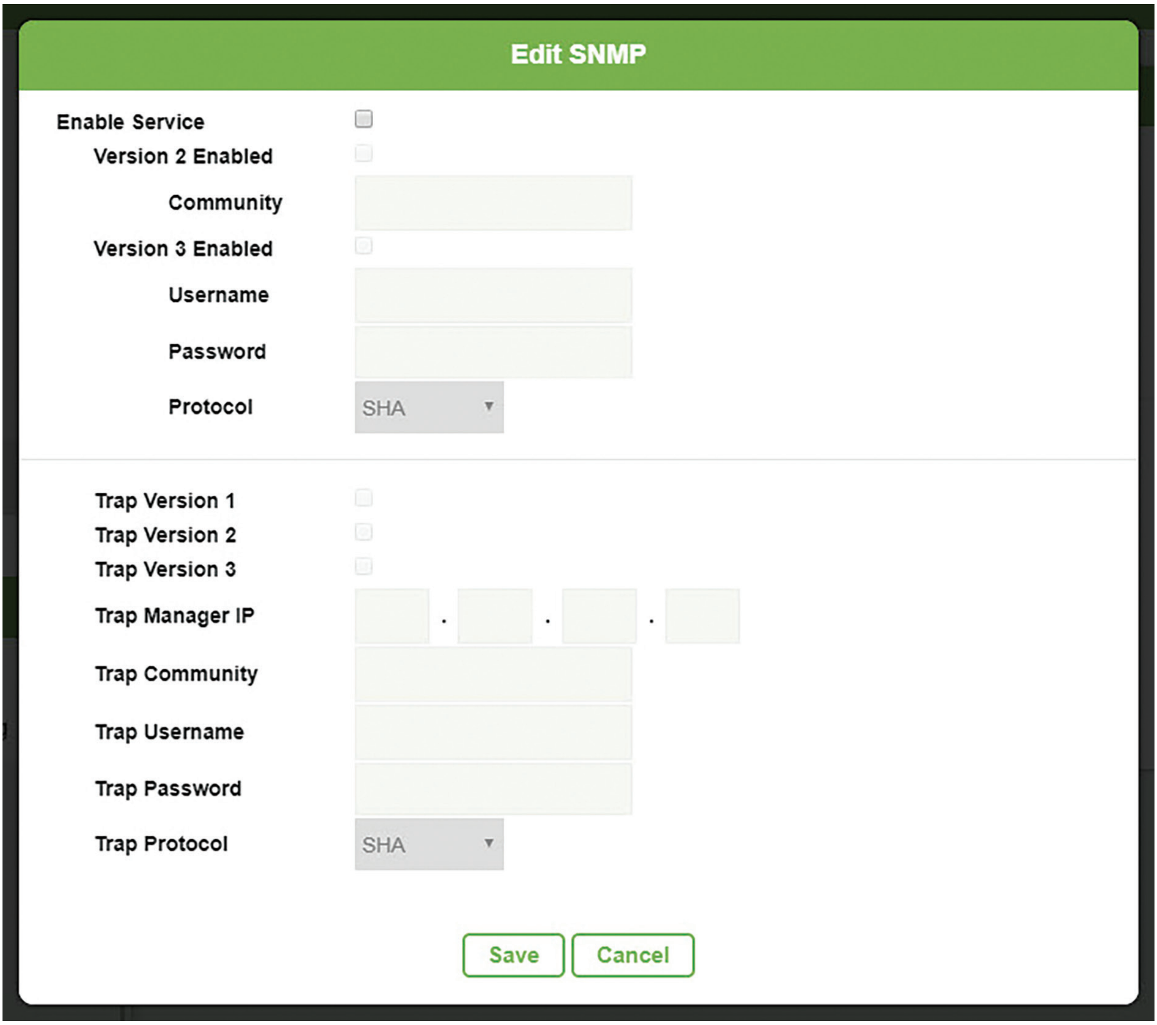
SNMP

Service Enabled	□
Version 2 Enabled	□
Community	
Version 3 Enabled	□
Username	
Protocol	SHA
Trap Version 1 Enabled	□
Trap Version 2 Enabled	□
Trap Version 3 Enabled	□
Trap Manager IP	
Trap Community	
Trap User	
Trap Protocol	SHA

Select the page under the **Status > SNMP** menu item to manage SNMP configurations.

SNMP CONFIGURATION

1. In the SNMP section, click the **Edit** button.
2. On the Edit SNMP pop-up, fill out the settings according to your SNMP monitoring tools requirements.
3. Click the **Save** button.



Edit SNMP

Enable Service □

Version 2 Enabled □

Community

Version 3 Enabled □

Username

Password

Protocol SHA ▾

Trap Version 1 □

Trap Version 2 □

Trap Version 3 □

Trap Manager IP . . .

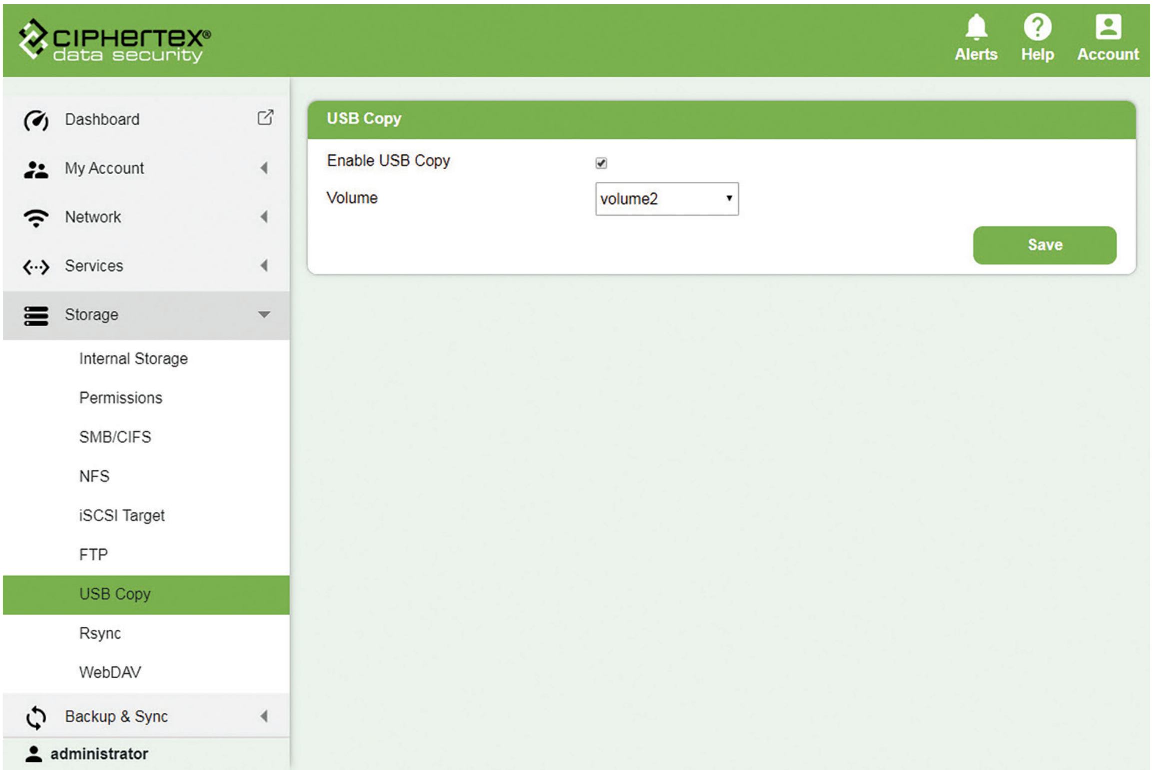
Trap Community

Trap Username

Trap Password

Trap Protocol SHA ▾

8.2 Upload Files from USB



Enable USB Copy ☑

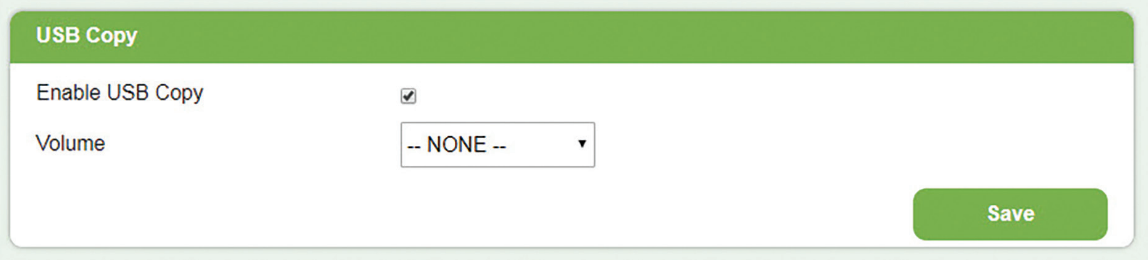
Volume: volume2

Select the page under the **Storage > USB** Copy to configure settings for copying from a USB storage device.

With SecureNAS, you can have files and data automatically copied and uploaded from an attached USB storage device. Simply plug a USB storage device into the front of SecureNAS unit and push the Copy button.

CONFIGURE USB COPY SETTINGS

1. On the **USB Copy** page in the USB Copy section, fill in the following information and then click the **Save** button:



Enable USB Copy ☑

Volume: -- NONE --

Enable USB Copy	Select this option to enable automatic upload/copy of data from an attached USB storage device.
Volume	Select from the list of available volumes. When files/ data are copied from the USB storage device, they will be stored on the selected Volume. **Note:** The data will be stored at this path: <Volume>/USB_Copy/ <device_name>_<date_time>

Note:

- You must first disable USB Copy before inserting a USB device for sharing.
- If USB Copy is enabled and a USB device is inserted into a USB port on the SecureNAS unit, SecureNAS will copy the contents of the USB device instead of showing it as a shareable volume.

COPY FILES FROM ATTACHED USB STORAGE DEVICE

1. Plug a USB storage device into the front USB slot of the SecureNAS unit.
2. While the USB storage device is plugged in, press the USB Copy button on the front of SecureNAS unit.
3. During the copy/upload process, all three amber LEDs will blink simultaneously. Message is displayed on the LCD, "USB Copy in Progress".
4. When the amber LEDs return to their normal heartbeat pattern, the copy is complete and you may remove the USB storage device.

8.3 USB Share

SHARE A USB DEVICE

1. Insert a USB device into one of the USB ports on the back of the SecureNAS unit.
2. The USB device will automatically show as a volume to share in SMB/CIFS and NFS.

Note:

- You must first disable USB Copy before inserting a USB device for sharing.
- If USB Copy is enabled and a USB device is inserted into a USB port on the SecureNAS unit, SecureNAS will copy the contents of the USB device instead of showing it as a shareable volume.

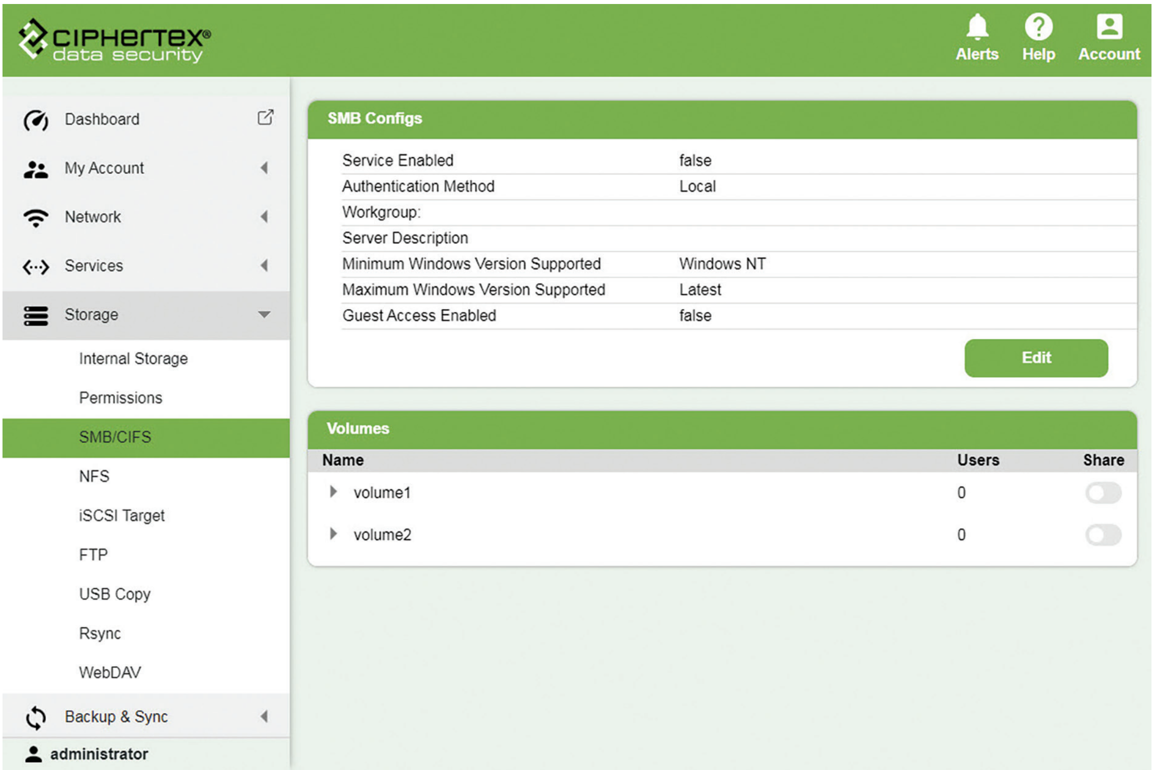
8.4 USB Quick Link (Optional)

The SecureNAS Quick-Link is an optional accessory that allows easy USB connectivity between the SecureNAS unit and your computer.

SET UP USB QUICK-LINK

1. Plug one end of the Quick-Link cable into one of the rear USB-3 ports on the SecureNAS unit.
2. Plug the other end of the Quick-Link cable into the USB port on your computer.
3. If you are using a Windows 10 computer, the necessary drivers will automatically be installed when the cable is connected.
4. For older versions of Windows, any Mac, or any Linux, you may need to manually install the necessary RNDIS network driver.

8.5 SMB/CIFS



SMB Configs

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

Volumes

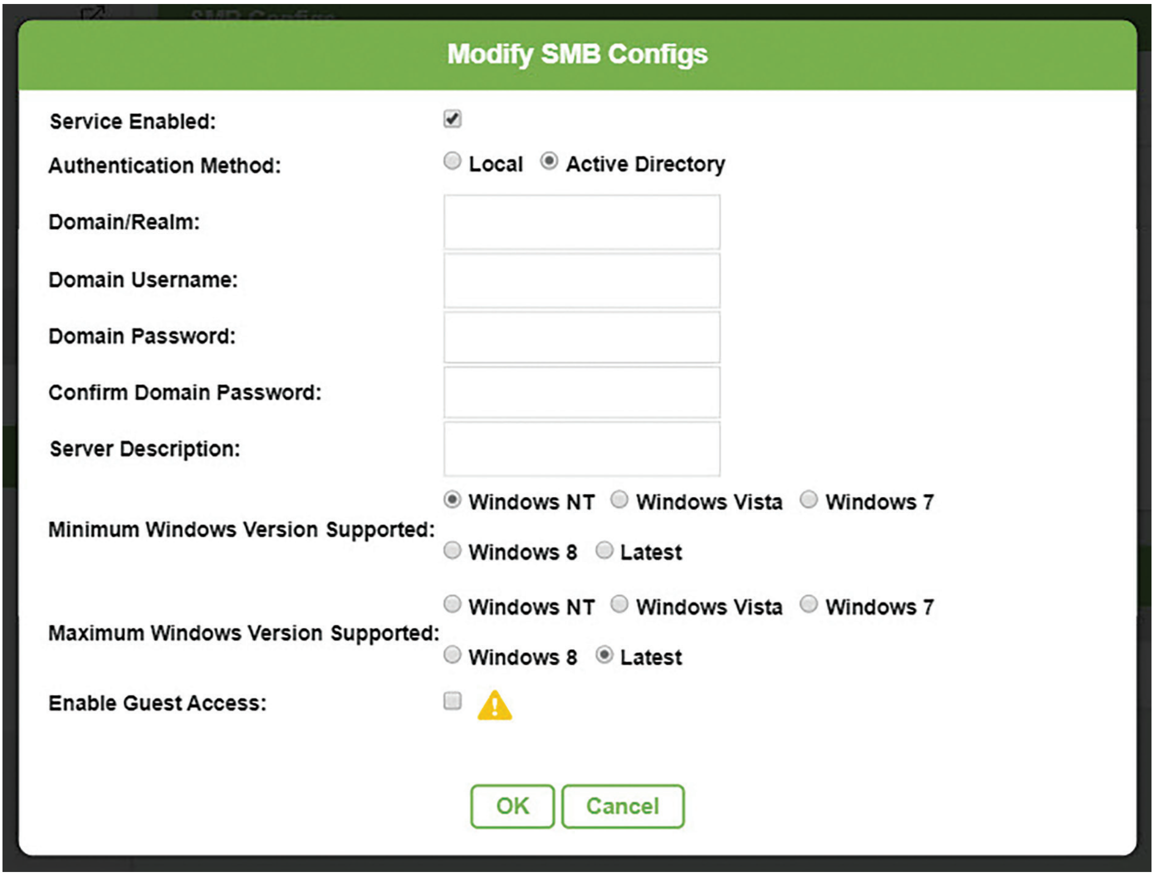
Name	Users	Share
volume1	0	○
volume2	0	○

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

CONFIGURE SMB/CIFS

1. On the SMB/CIFS page in the **SMB Configs** section, click the Edit button to enable SMB/CIFS and modify

2. On the Modify SMB Configs pop-up, fill in the following information and then click the **OK** button:



Modify SMB Configs

Service Enabled: ☑

Authentication Method: ○ Local ● Active Directory

Domain/Realm:

Domain Username:

Domain Password:

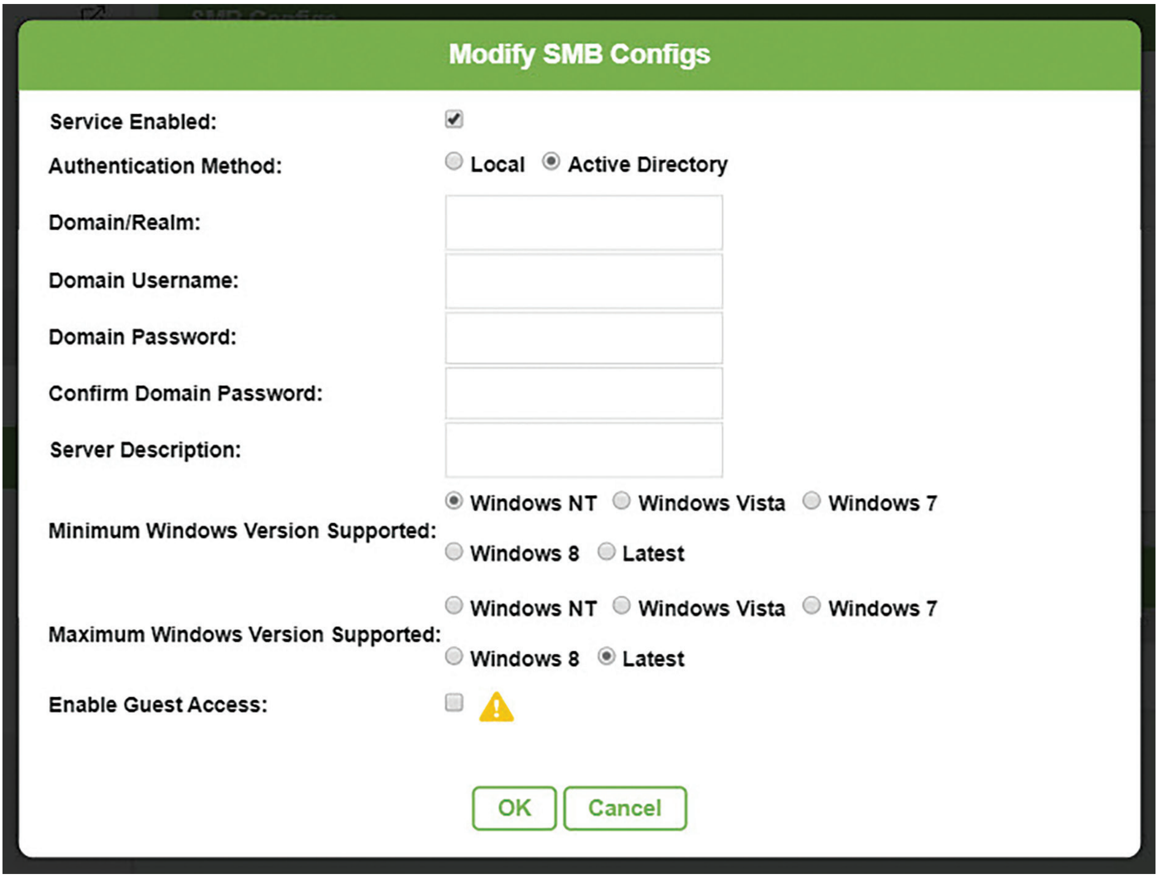
Confirm Domain Password:

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: □ ⚠



Modify SMB Configs

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

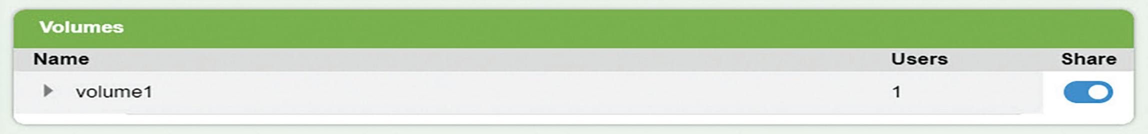
Enable Guest Access: □ ⚠

Service Enabled	Select this option to enable SMB/CIFS sharing.
Authentication Method	Choose either Local or Active Directory. Local: Allow local users added in the SecureNAS Management Console to access the shares. Active Directory: Use your Active Directory to control access to the shares.
Workgroup	The name of the workgroup that the shares will show up with are grouped together. Optional. **Note:** This option is only available when the Authentication Method Local is selected.
Domain/Realm	The Active Directory domain or realm that will be joined. Note: This option is only available when the Authentication Method **Active Directory** is selected.

Domain Username	The Windows user account that will be used to authenticate with Active Directory to determine if SecureNAS has permission to join the domain. **Note:** This option is only available when the Authentication Method **Active Directory** is selected.
Domain Password	The password for the Windows user account that will be used to authenticate with Active Directory. **Note:** This option is only available when the Authentication Method **Active Directory** is selected.
Confirm Domain Password	Re-type the password for the Windows user account that will be used to authenticate with Active Directory. **Note:** This option is only available when the Authentication Method **Active Directory** is selected.
Server Description	Similar to server name, this is how SecureNAS will appear in your Local Networks.
Minimum Windows Version Supported	The earliest Windows version with which the share is to be compatible. Choose from: • Windows NT • Windows Vista • Windows 7 • Windows 8 • Latest
Maximum Windows Version Supported	The latest Windows version with which the share is to be compatible. Choose from: • Windows NT • Windows Vista • Windows 7 • Windows 8 • Latest
Enable Guest Access	Enabling this option will allow anyone to see the names of browsable shares.

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

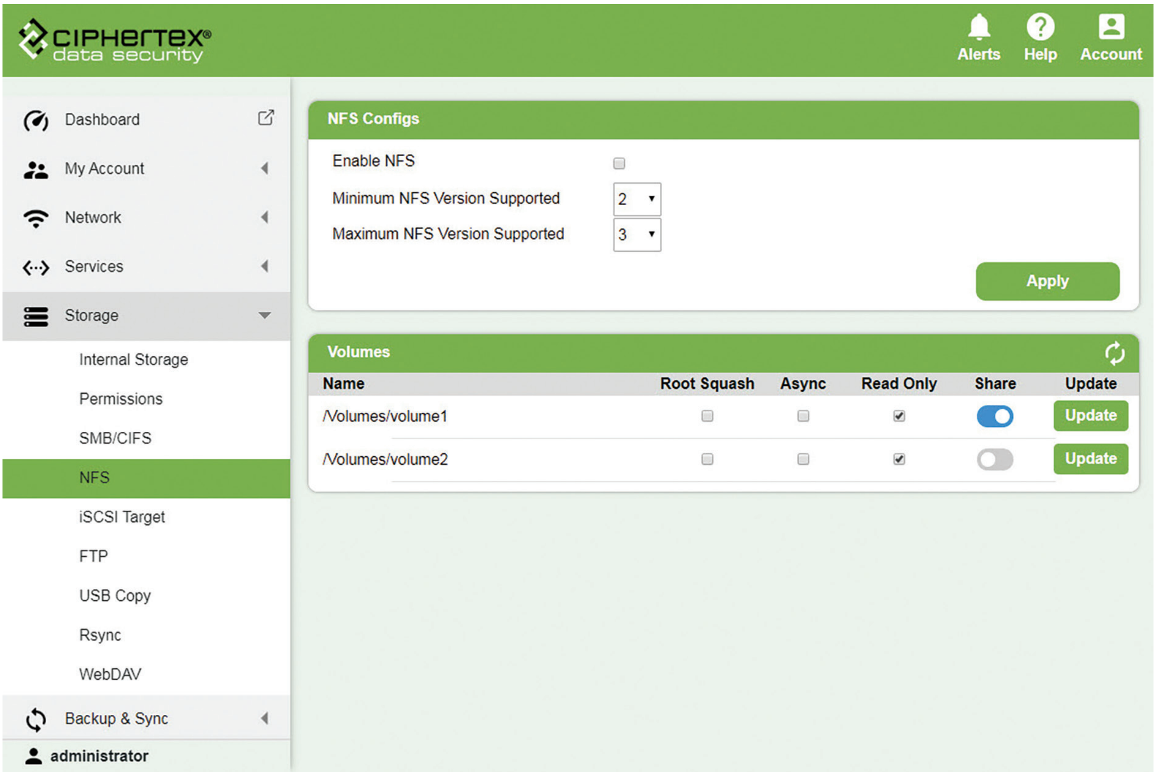
1. To add accounts that can access the volume via SMB/CIFS, click the **Add Accounts** button.
2. From the Add Accounts pop-up, select the accounts to add and then click the Add button.
3. Select permissions for the added account: Read, Write, or None.
4. Delete an account by clicking on the red trashcan icon 🗑 next to the account.

SMB/CIFS Volume Configuration

1. Click the Edit button to edit the configuration for the volume.
2. From the Edit Configuration Accounts pop-up, configure the following options and click the Ok button.

Browsable	Enable/disable the browsable option for SMB/CIFS. This controls whether or not this share is seen in the list of available shares in a network view.
Allow Guest	Enable/disable the allow guest option for SMB/CIFS. If enabled, then no password is required to connect to this volume.
Comment	Enter a comment. This is for note purposes only.

8.6 NFS



NFS Configs

Enable NFS □

Minimum NFS Version Supported: 2

Maximum NFS Version Supported: 3

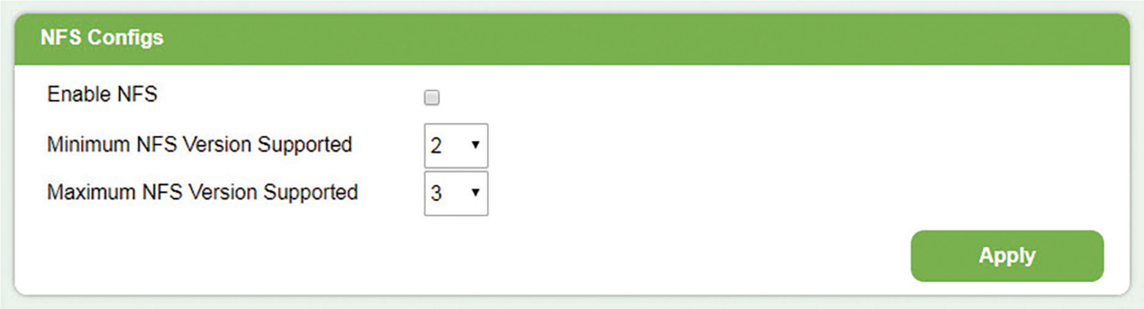
Volumes

Name	Root Squash	Async	Read Only	Share	Update
/Volumes/volume1	□	□	☑	●	Update
/Volumes/volume2	□	□	☑	○	Update

Select the page under the **Storage > NFS** to configure settings for sharing volumes via NFS.

CONFIGURE NFS (NETWORK FILE SYSTEM)

1. On the NFS page in the **NFS Configs section**, select to enable/disable NFS. Then select NFS versions.
2. After configuring NFS, click the **Apply** button:



NFS Configs

Enable NFS □

Minimum NFS Version Supported: 2

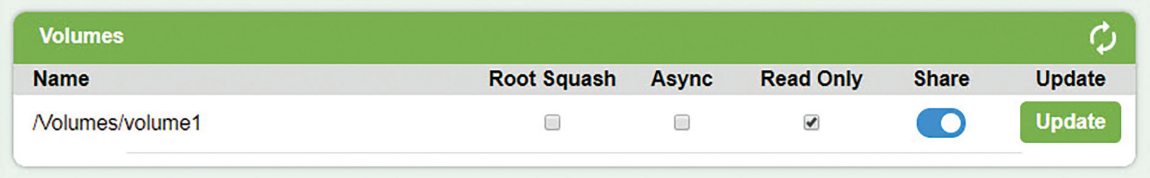
Maximum NFS Version Supported: 3

Enable NFS	Select this option to enable or disable NFS (Network File System).
Minimum NFS Version Supported	This is the minimum version of NFS that can be used with SecureNAS. Choose from version 2, 3, or 4.
Maximum NFS Version Supported	This is the maximum version of NFS that can be used with SecureNAS. Choose from version 2, 3, or 4.

CHOOSE VOLUMES TO SHARE VIA NFS

1. On the NFS page in the **NFS Configs** section, find the volume that you want to share.

2. Enable/Disable the following options and then click the **Update** button.

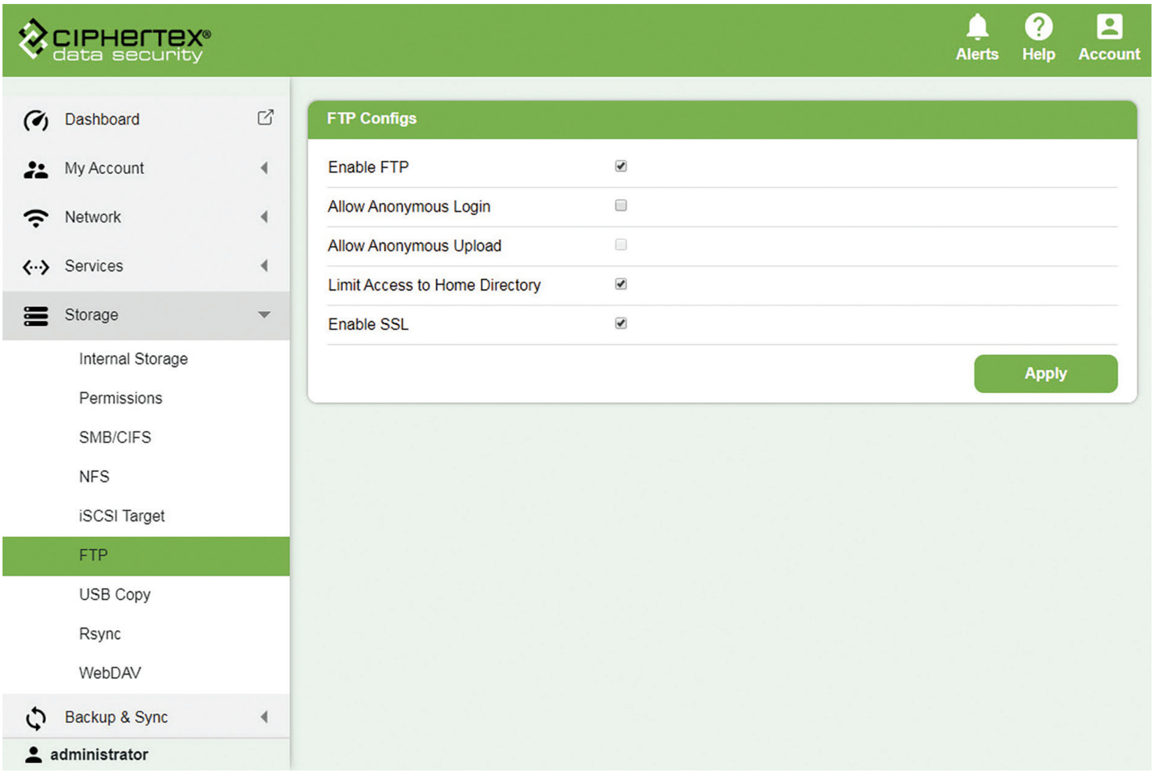


Volumes

Name	Root Squash	Async	Read Only	Share	Update
/Volumes/volume1	☐	☐	☑	●	Update

Name	The name of the volume. **Note:** The volume name is not editable from this list.
Root Squash	Enable/disable root squash for NFS. This will map the root user to "nobody".
Async	Enable/disable async for NFS. This option can be used to optimize performance.
Read Only	Enable/disable the read only for NFS. If enabled, users will only have read access to the volume.
Share	Enable/disable the volume share by clicking on the toggle switch ● . When the switch is blue and positioned to the right, the volume is shared.

8.7 FTP



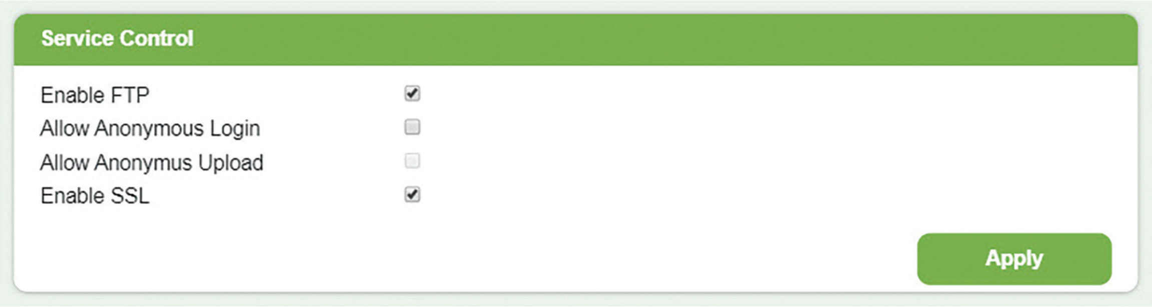
FTP Configs

Enable FTP	☑
Allow Anonymous Login	□
Allow Anonymous Upload	□
Limit Access to Home Directory	☑
Enable SSL	☑

Select the page under the **Storage > FTP** to configure settings for sharing volumes via FTP.

ACCESS FILES VIA FTP

1. On the FTP page in the Service Control section, enable/disable the following options and then click the Apply button:

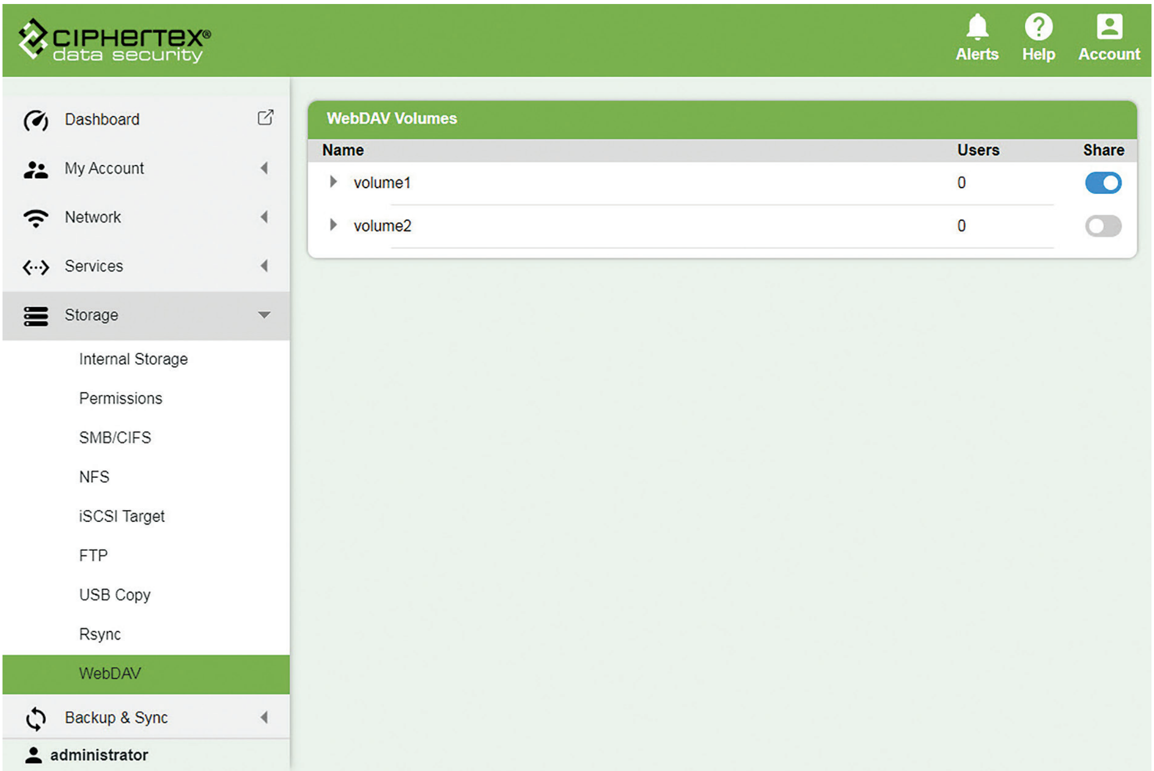


Service Control

Enable FTP	☑
Allow Anonymous Login	□
Allow Anonymus Upload	□
Enable SSL	☑

Enable FTP	Select this option to enable FTP access for SecureNAS.
Allow Anonymous Login	This option allows access to SecureNAS via FTP without a user account or authentication.
Allow Anonymous Upload	This option allows file/data uploads to SecureNAS via FTP without a user account or authentication.
Limit Access to Home Directory	This option will jail the user to their home directory. This means they will only have read/write access to their home directory and not all volumes.
Enable SSL	Select this option to use an encrypted SSL connection when viewing/sharing files via FTP. **Note:** This option is only available when there is a valid SSL Certificate installed on SecureNAS.

8.8 WebDAV



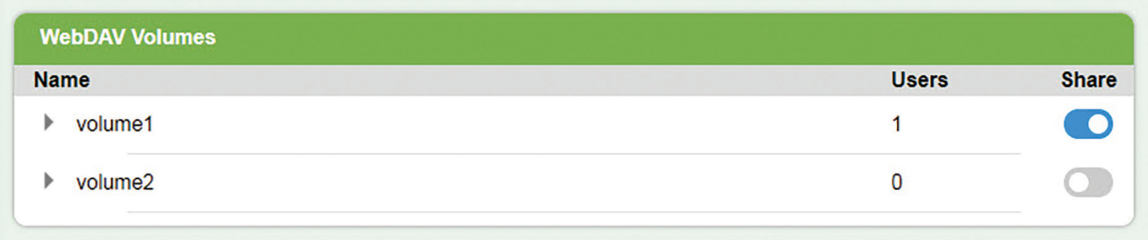
WebDAV Volumes

Name	Users	Share
volume1	0	●
volume2	0	○

Select the page under the **Storage > WebDAV** to configure settings for sharing and accessing volumes via WebDAV.

CHOOSE VOLUMES TO SHARE VIA WEBDAV

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



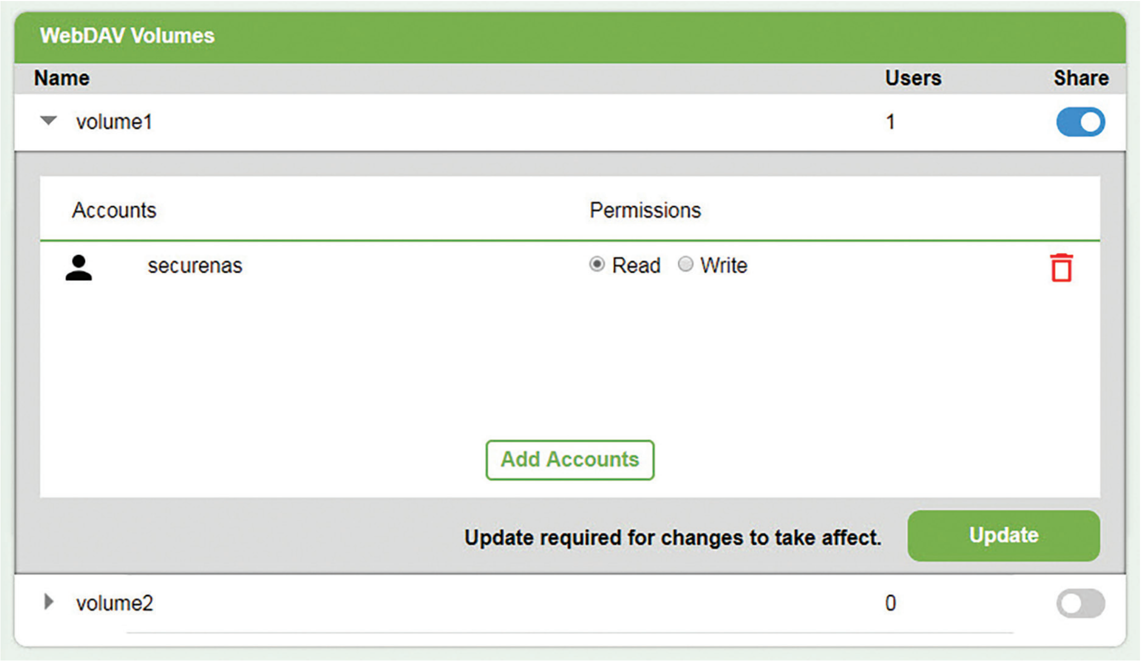
WebDAV Volumes

Name	Users	Share
▸ volume1	1	●
▸ volume2	0	○

> **Note:**
> - WebDAV on SecureNAS is configured to use port 5110.
> - If an SSL certificate is already added via the SecureNAS Management Console, WebDAV will be configured to use port 5113.

CONFIGURE VOLUMES FOR WEBDAV

1. On the WebDAV page in the **WebDAV 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.



WebDAV Volumes

Name	Users	Share
▾ volume1	1	● on
▸ volume2	0	○ off

Accounts	Permissions
securenas	● Read ○ Write

Update required for changes to take affect.

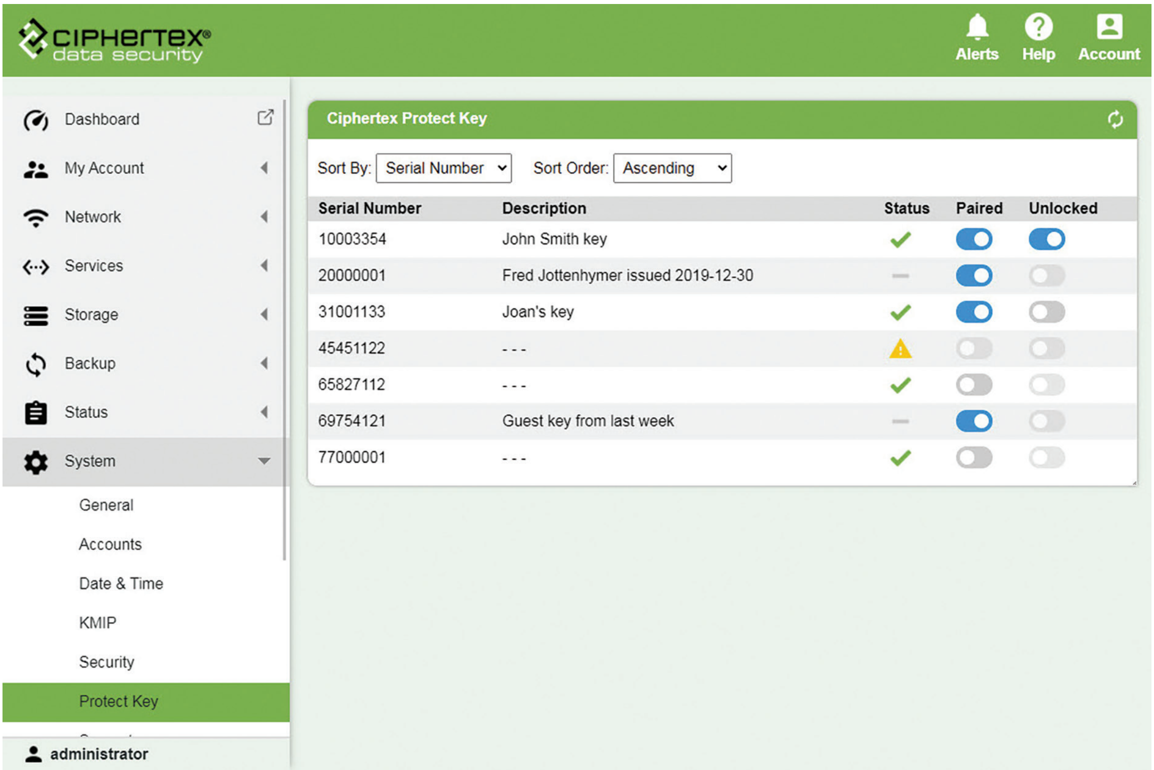
WebDAV Volume Accounts

1. To add accounts that can access the volume via WebDAV, click the **Add Accounts** button.
2. From the Add Accounts pop-up, select the accounts to add and then click the **Add** button.
3. Select permissions for the added account: Read or Write.
4. Delete an account by clicking on the red trashcan icon 🗑 next to the account.

9 Enhance Security

If your SecureNAS is reachable on the internet, you must safeguard it against any attacks. You can use the SecureNAS Management Console to set up the built-in firewall and also schedule antivirus scans.

9.1 Ciphertex-Protect® Encryption Key



Ciphertex Protect Key

Sort By: Serial Number   Sort Order: Ascending

Serial Number	Description	Status	Paired	Unlocked
10003354	John Smith key	✓	●	●
20000001	Fred Jottenhymer issued 2019-12-30	—	●	○
31001133	Joan's key	✓	●	○
45451122	- - -	⚠	○	○
65827112	- - -	✓	○	○
69754121	Guest key from last week	—	●	○
77000001	- - -	✓	○	○

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 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 or in transit 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 encryped 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.

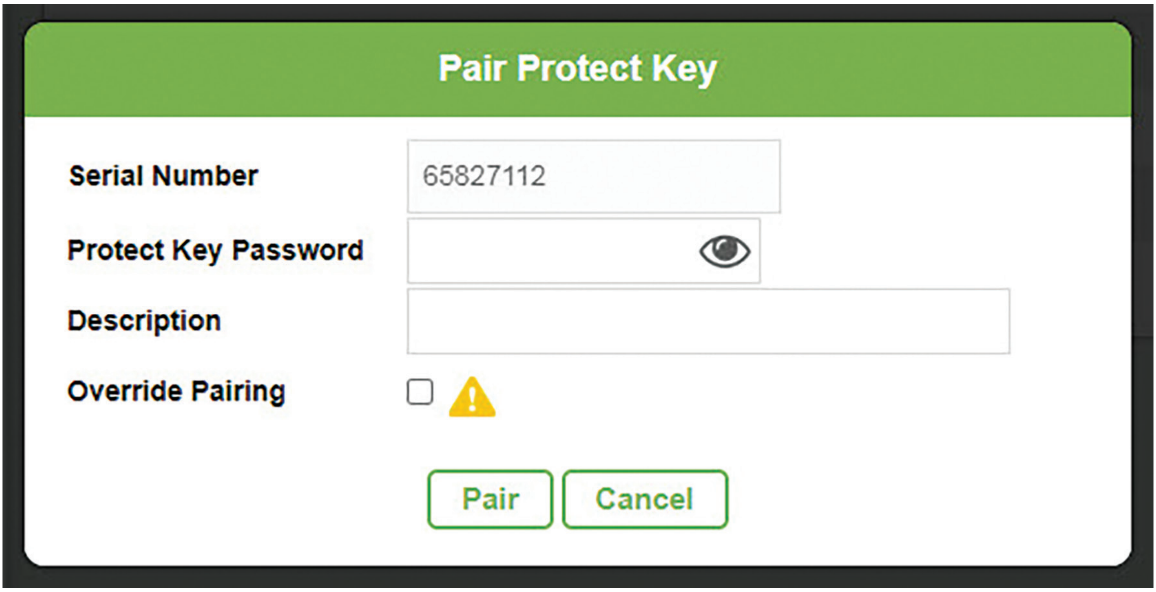
🔗 The Protect Key is currently plugged into a USB port on the SecureNAS unit, but might be currently paired to another SecureNAS unit.

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.

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-up, fill out the following information and then click the **Pair** button:



Pair Protect Key

Serial Number	65827112
Protect Key Password	
Description	
Override Pairing	□

WARNING!

IMPORTANT: The Ciphertex-Protect® hardware key for encryption authentication included with your Ciphertex SecureNAS®, and any additional keys you may have ordered from Ciphertex, contain proprietary code linking them to the SecureNAS® product family. This code further enhances the ultra-high level of data security you enjoy with your SecureNAS®. While you may be able to obtain a similar or identical hardware key from another source, that key will not contain the Ciphertex code, thus voiding your Ciphertex warranty, but more importantly opening your data to the potential of loss and/or theft.

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 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. A password must be exactly 8 characters and only contain a-z, A-Z, 0-9, !, $, #, %. No spaces are allowed.
Description	A description for the Protect Key. This is for informational purposes only. **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.
Override Pairing	If this option is selected, the Protect Key will be paired to this SecureNAS unit and will be unpaired from the other SecureNAS unit that it is currently paired to. This option is only available when the Protect Key is currently paired to a different SecureNAS unit. **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 SecureNAS unit unrecoverable.

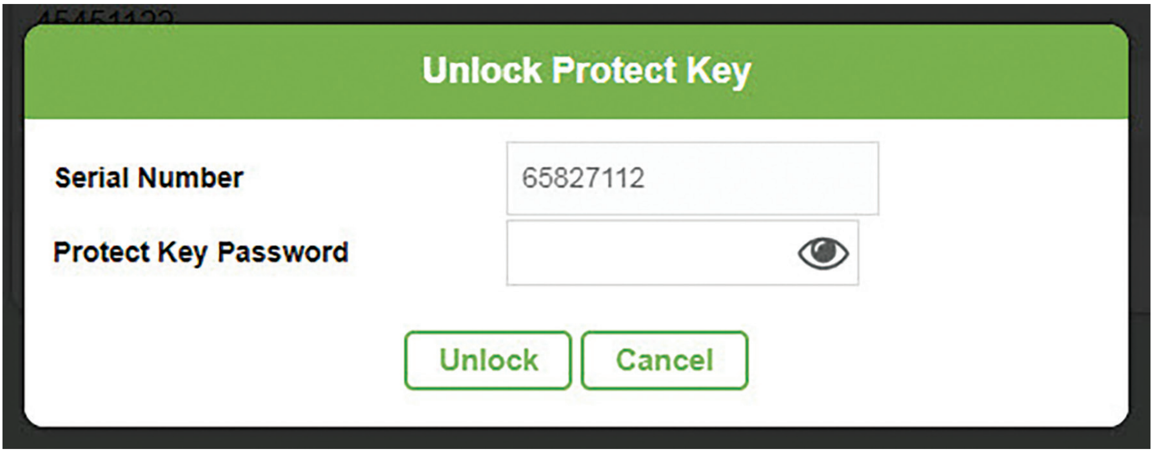
8. The Protect Key is now added to the system.

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 filesystem.

UNLOCK A PROTECT KEY

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:



Unlock Protect Key

Serial Number: 65827112

Protect Key Password:

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:**

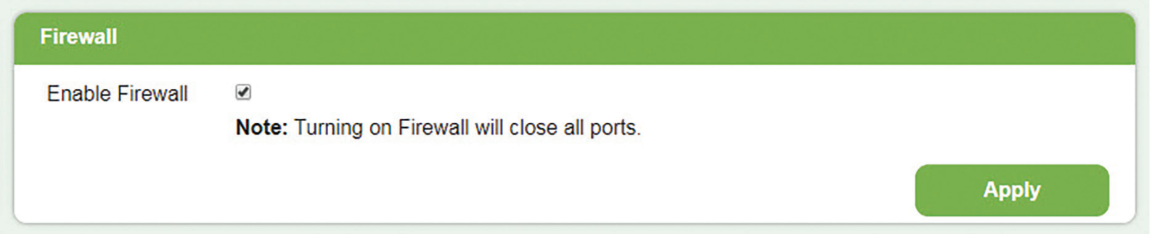
- The Unpair Protect Key operation cannot be undone. Once the Protect Key has been unpaired, it will no be usable with the SecureNAS unit unless it is paired again with a new password.
- To Unpair, the Protect Key does not need to be plugged into a USB port on the SecureNAS unit.

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.

9.2 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**.



Firewall

Enable Firewall ☑

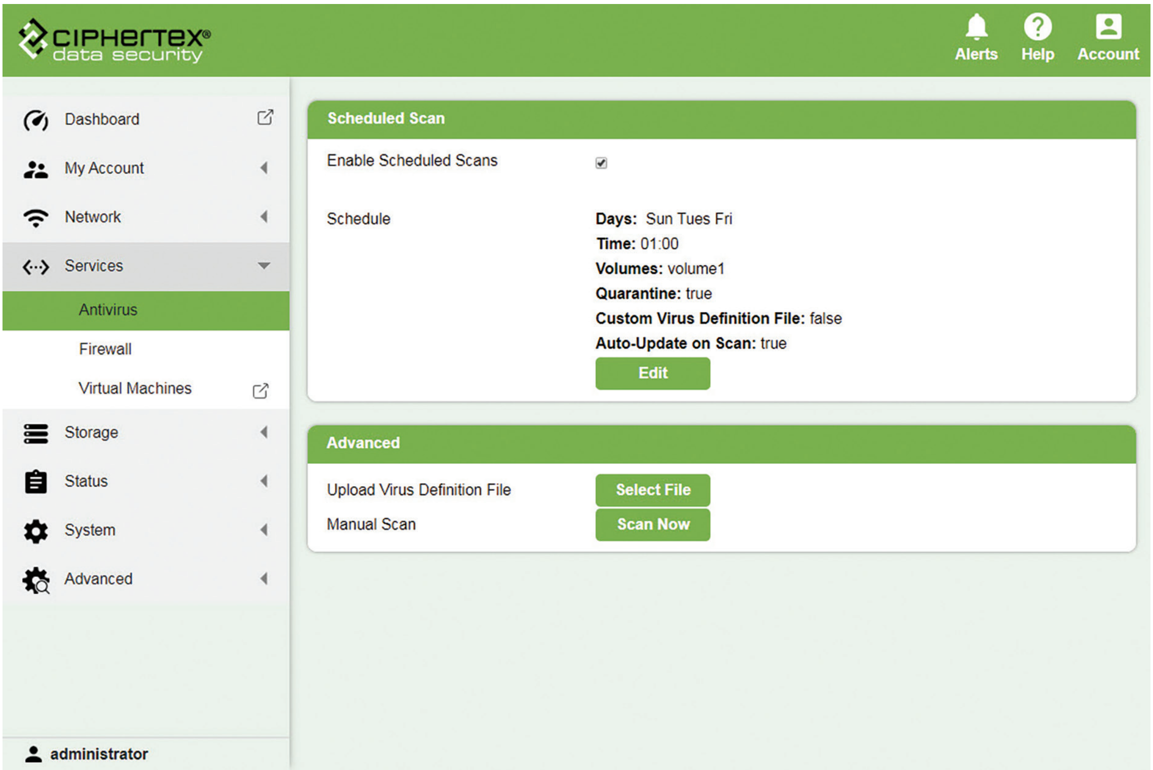
Note: Turning on Firewall will close all ports.

2. On the Firewall page select the **Enable Firewall** checkbox.
3. Click the **Apply** button to apply these changes.

Note:

- Turning on the Firewall will close all ports.

9.3 Schedule Antivirus Scans



Scheduled Scan

Enable Scheduled Scans ☑

Schedule

Days: Sun Tues Fri
Time: 01:00
Volumes: volume1
Quarantine: true
Custom Virus Definition File: false
Auto-Update on Scan: true

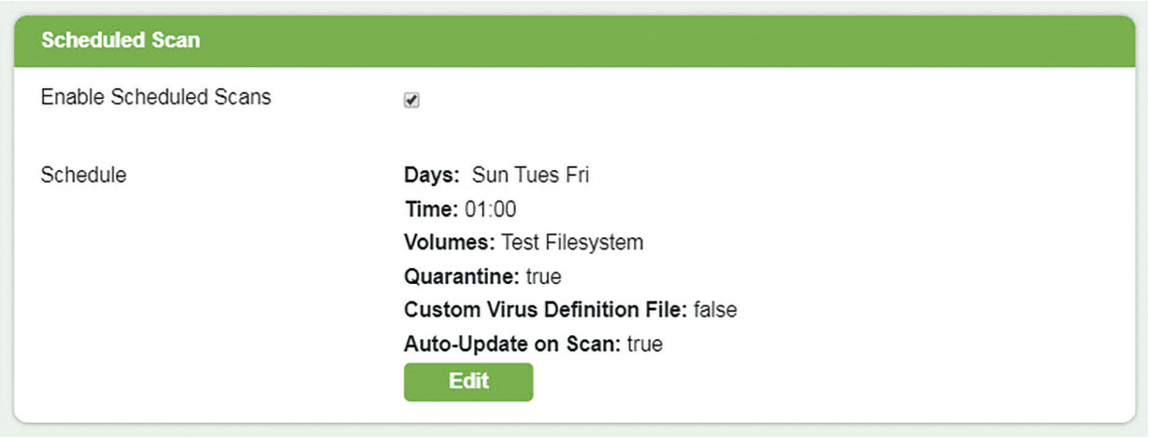
Advanced

Upload Virus Definition File

Manual Scan

Select the page under the **Services > Antivirus** menu item to set up and schedule antivirus scans.

SET UP ANTIVIRUS



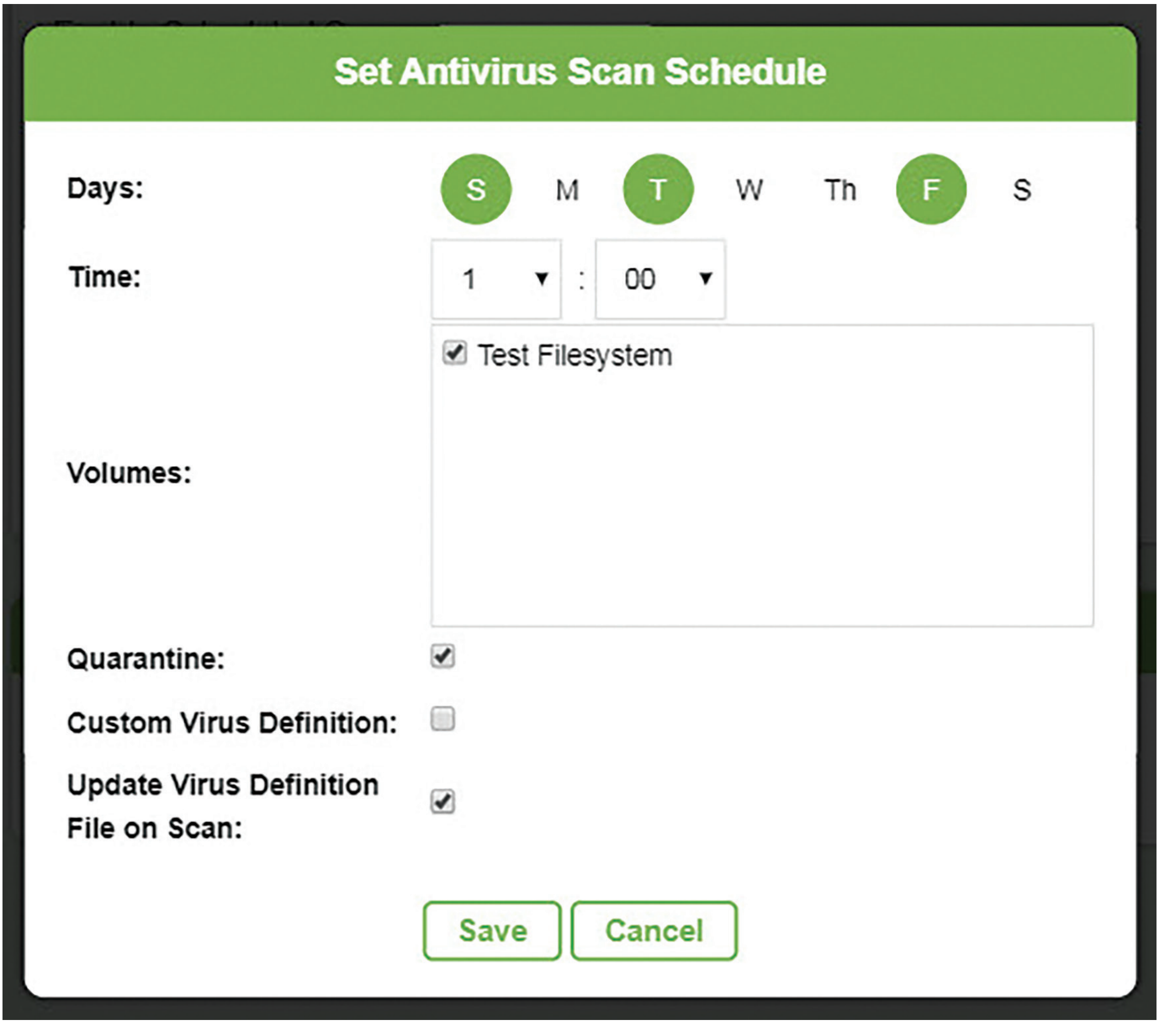
Scheduled Scan

Enable Scheduled Scans ☑

Schedule

Days: Sun Tues Fri
Time: 01:00
Volumes: Test Filesystem
Quarantine: true
Custom Virus Definition File: false
Auto-Update on Scan: true

1. To set up a schedule for antivirus scans, navigate to **Services > Antivirus** from the menu on the left.
2. In the **Scheduled Scan** section, click the checkbox for **Enable Scheduled Scan**s.
3. On the Set Antivirus Scan Schedule pop-up, fill in the following information and then click the **Save** button:



Set Antivirus Scan Schedule

Days: ● S M ● T W Th ● F S

Time: 1 ▾ : 00 ▾

Volumes: ☑ Test Filesystem

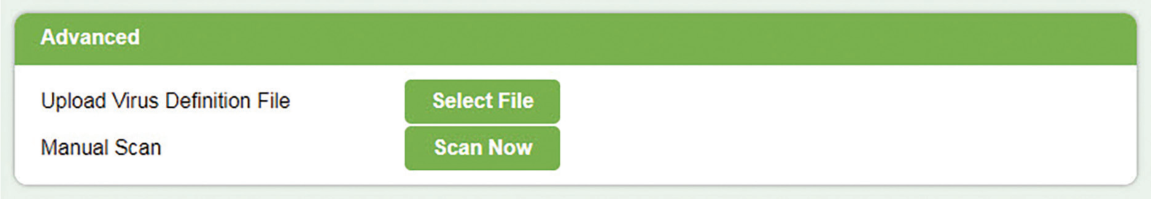
Quarantine: ☑

Custom Virus Definition: □

Update Virus Definition File on Scan: ☑

Days	Select the day(s) to perform a scan by clicking on the corresponding letters: Sunday (S), Monday (M), Tuesday (T), Wednesday (W), Thursday (Th), Friday (F), Saturday (S)
Time	Select the time of day to perform a scan. Use the the first drop-down box to select an hour on a 24 hour schedule. Use the second drop-down box to select the minute.
Volumes	This area will show a list of available volumes/filesystems. Choose which volumes/filesystems to scan by selecting the checkbox next to the corresponding name.
Quarantine	Select this option to enable Quarantine. This will place potential threats inside of a quarantine folder located at the root of the filesystem in which the scan was started.
Custom Virus Definition	Select this option to upload and use your custom virus definition file. **Note:** This option is not available for use until you have uploaded your own virus definition file in a separate step.
Update Virus Definition File on Scan	Select this option to make sure the virus definition file is always updated before the start of a scan.

OTHER ANTIVIRUS OPTIONS

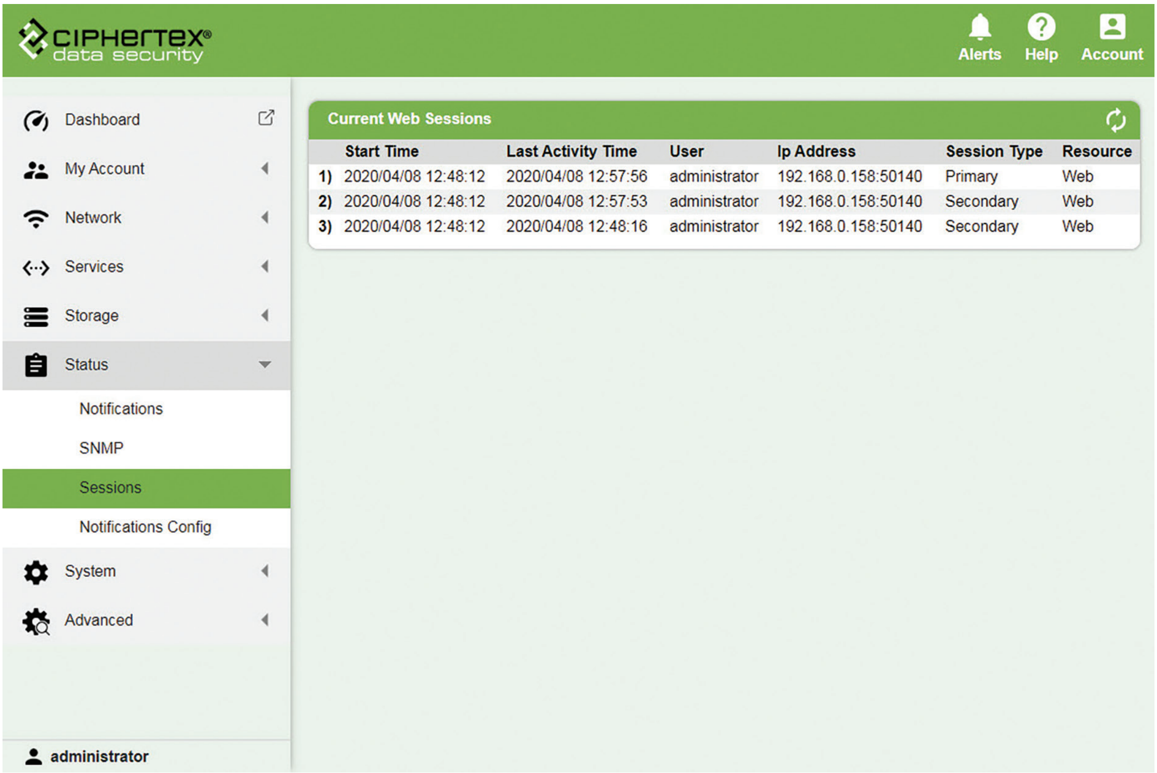


1. In the **Advanced** section on the Antivirus page, you can select more antivirus options.
2. Click the **Select File** button to upload a **Custom Virus Definition File**.
    a. After adding your own custom virus definition file, edit the scheduled scan by clicking the **Edit** button in the Schedule scan section of the Antivirus page.
    b. On the Set Antivirus Scan Schedule pop-up, you can now enable the option **Custom Virus Definition**.
    c. Click the **Save** button to save the changes.

Note:

- To manually start an antivirus scan at any time, click the **Scan Now** button in the Advanced section of the Antivirus page.

9.4 View Current Sessions



Current Web Sessions

	Start Time	Last Activity Time	User	Ip Address	Session Type	Resource
1)	2020/04/08 12:48:12	2020/04/08 12:57:56	administrator	192.168.0.158:50140	Primary	Web
2)	2020/04/08 12:48:12	2020/04/08 12:57:53	administrator	192.168.0.158:50140	Secondary	Web
3)	2020/04/08 12:48:12	2020/04/08 12:48:16	administrator	192.168.0.158:50140	Secondary	Web

Select the page under the **Status > Sessions** menu item to view current web sessions for the SecureNAS.

VIEW WEB SESSIONS

1. View a list of web sessions on the **Status > Sessions** page. Use the table below to interpret data.

Start Time	The time the session began.
Last Activity Time	The last time the session had any activity. This may be from a user navigating through a menu, refreshing a page, changing settings, etc.
User	The username of the user that is logged in for that session.
IP Address	The IP Address of the user that is logged in for that session.
Session Type	The type of session: Primary or Secondary. **Primary:** The initial and main session created when a user logs in. **Secondary:** The secondary session can be for background services that are running such as notifications. A secondary session can also be created if a user opens up a duplicate web page into the SecureNAS Management Console. **Note:** Each session will have a Primary/Secondary pair.
Resource	The resource associated with the session.

10 Backup Data

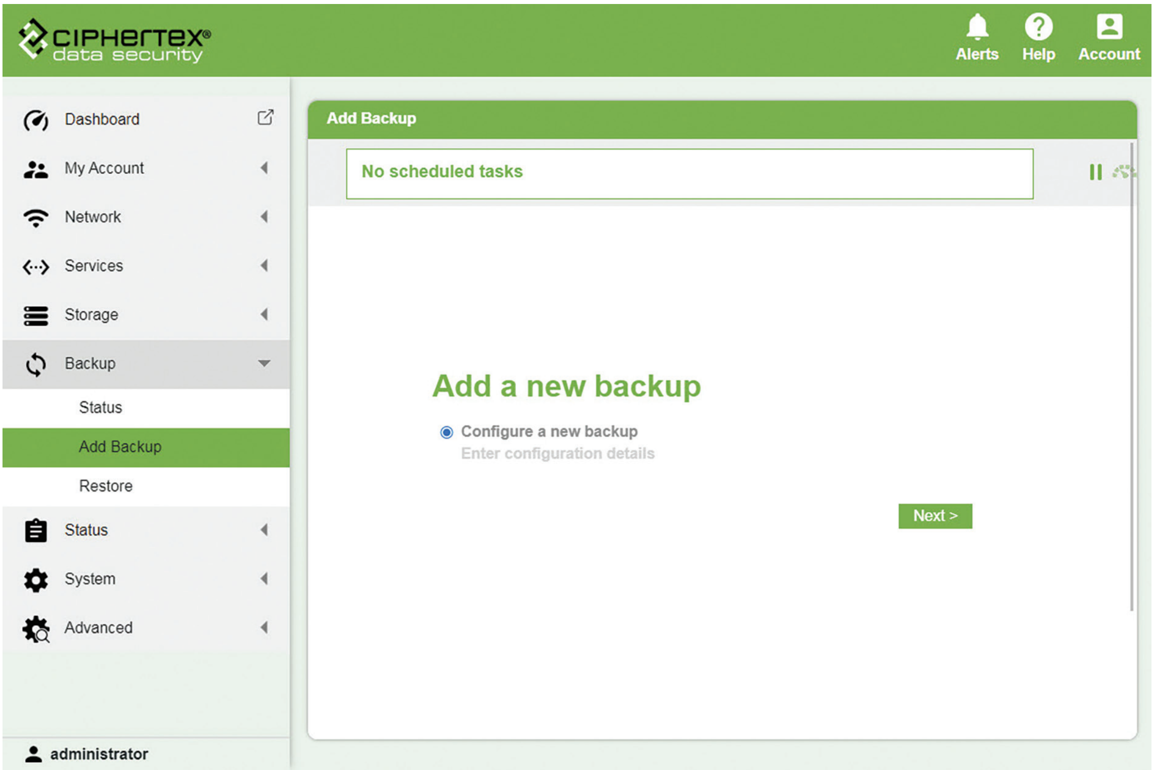
SecureNAS offers comprehensive and efficient backup solutions for your data. System administrators can configure different backup jobs to run on a defined schedule.

Use the pages under the **Backup** menu item to configure and manage backup jobs for SecureNAS.

Note:

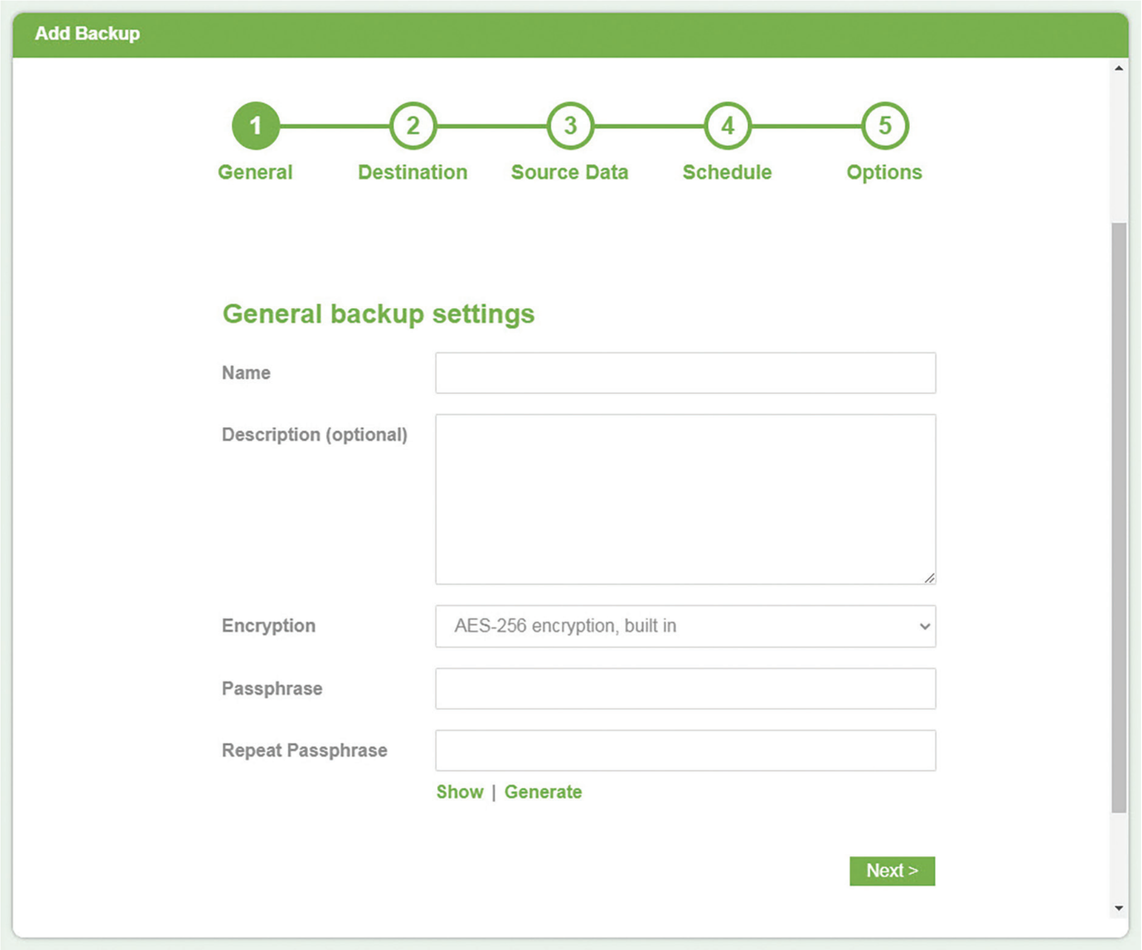
- SecureNAS utilizes Duplicati 2.0 for its backup offerings. You can refer to the Duplicati manual for more in-depth information about some features.

10.1 Create New Backup Job



CREATE BACKUP JOBS

1. Select the page under the **Backup > Add Backup** menu item to create and schedule backup jobs to run.
2. In the Add a new backup section, select the **Configure a new backup** option.
3. Click the **Next** button to continue with creating a new backup job.
4. On the **General** page, fill out the following information and then click the Next button:



General backup settings

Name

Description (optional)

Encryption: AES-256 encryption, built in

Passphrase

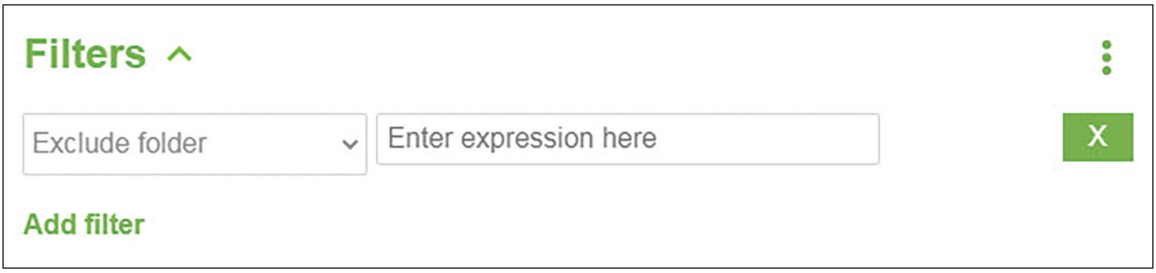
Repeat Passphrase

Name	A descriptive name for the backup job.
Description (optional)	A description of the backup job. **Optional**.
Encryption	Choose the encryption type for the backup job: • No encryption • AES-256 encryption, built in • GNU Privacy Guard, external
Passphrase	The encryption key/passphrase to be used for the backup job. **Note:** Click the Generate button to have the SecureNAS generate a strong encryption key.
Repeat Passphrase	The encryption key/passphrase that was entered above.

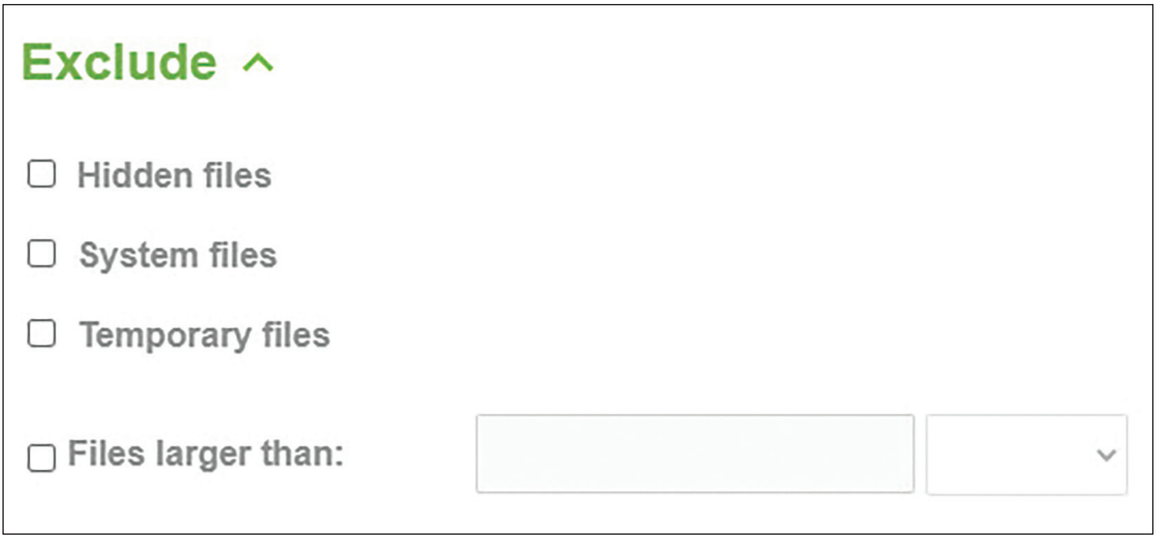
Note:

- Losing your encryption key will render your backup files useless and makes restore operations impossible. Always store your encryption key in a safe place and separate from your backup files.

5. On the **Destination** page, select the Storage Type.
6. For the selected storage type, fill out the destination information with accurate information for that choice.
7. Click the **Test connection** button to verify that the entered information is correct.
8. Once the information is verified, click the **Next** button to continue.
9. On the **Source Data** page, use the folder navigation area to expand Volumes.
10. Click on the box next to a volume in the tree to select that volume. A green checkbox will appear in the box next to the volume name.
11. Optional: Click on the **Filters** header to expand the filters area and add a filter.



12.Optional: Click on the **Exclude** header to expand the exclude area and select options.



□ Hidden files

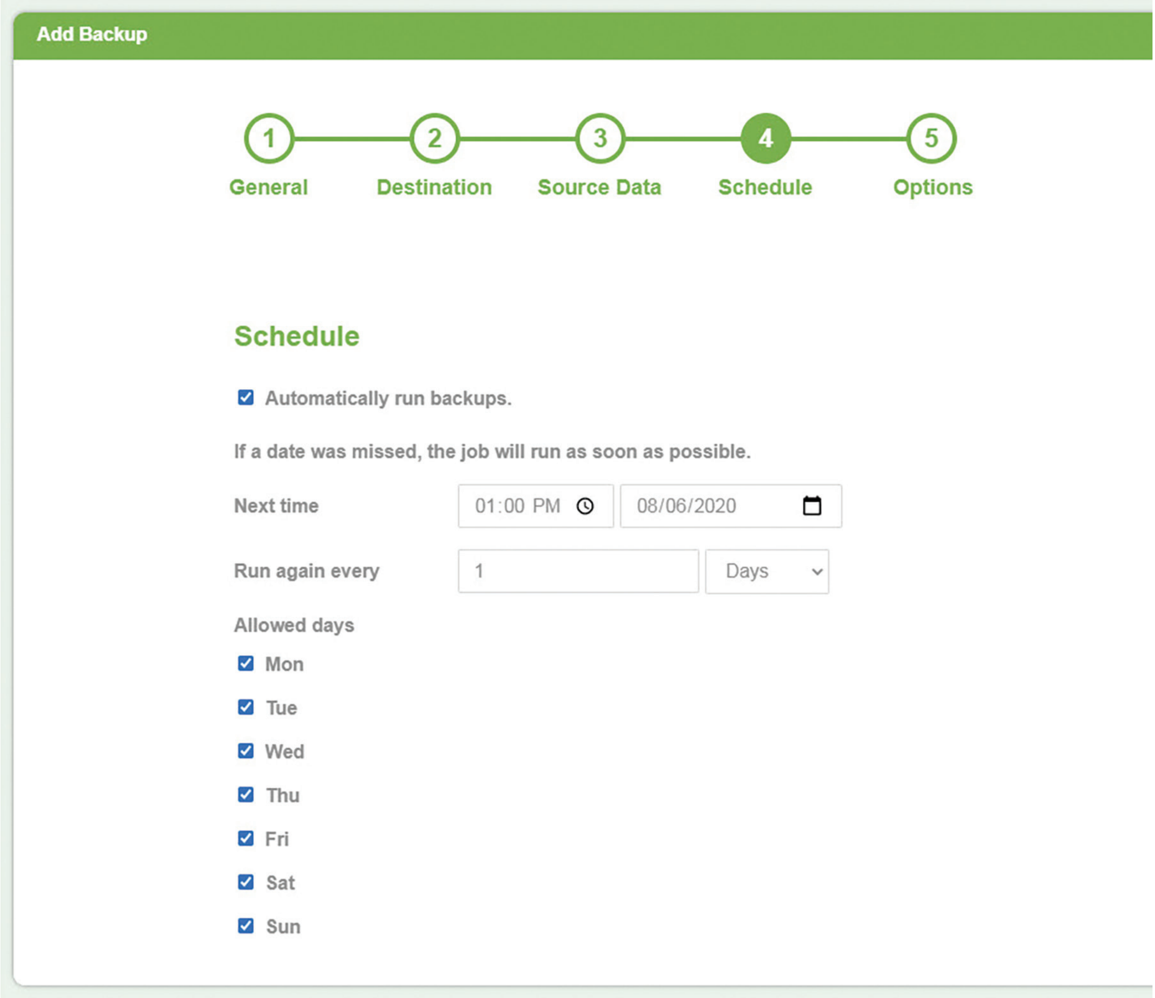
□ System files

□ Temporary files

□ Files larger than:

13. Click the **Next** button to continue.

14. On the **Schedule** page, fill out the following information and then click the Next button:



Schedule

☑ Automatically run backups.

If a date was missed, the job will run as soon as possible.

Next time: 01:00 PM 08/06/2020

Run again every: 1 Days

Allowed days

☑ Mon

☑ Tue

☑ Wed

☑ Thu

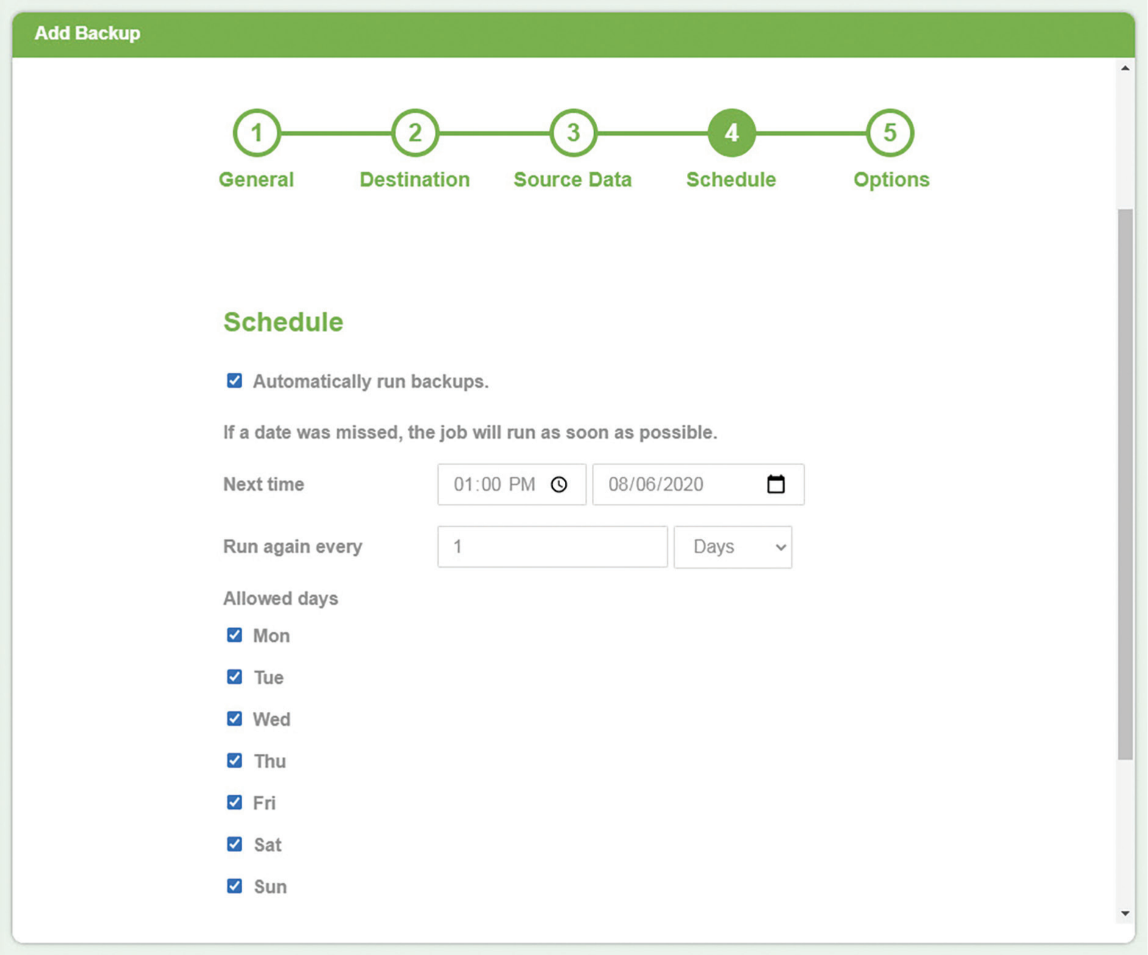
☑ Fri

☑ Sat

☑ Sun

Automatically run backups	Select this option to specify how frequently and at what time the backup job should run. **Note**: If this option is disabled, the backup job can be run manually instead of using a schedule.
Next time	The time and date at which to start running the backup job.
Run again every	How often to run the backup job.
Allowed days	The days of the week that the backup job will be allowed to run.

16. On the **Options** page, select the **Remote volume size** and set the **Backup retention** option.



Schedule

☑ Automatically run backups.

If a date was missed, the job will run as soon as possible.

Next time: 01:00 PM 08/06/2020

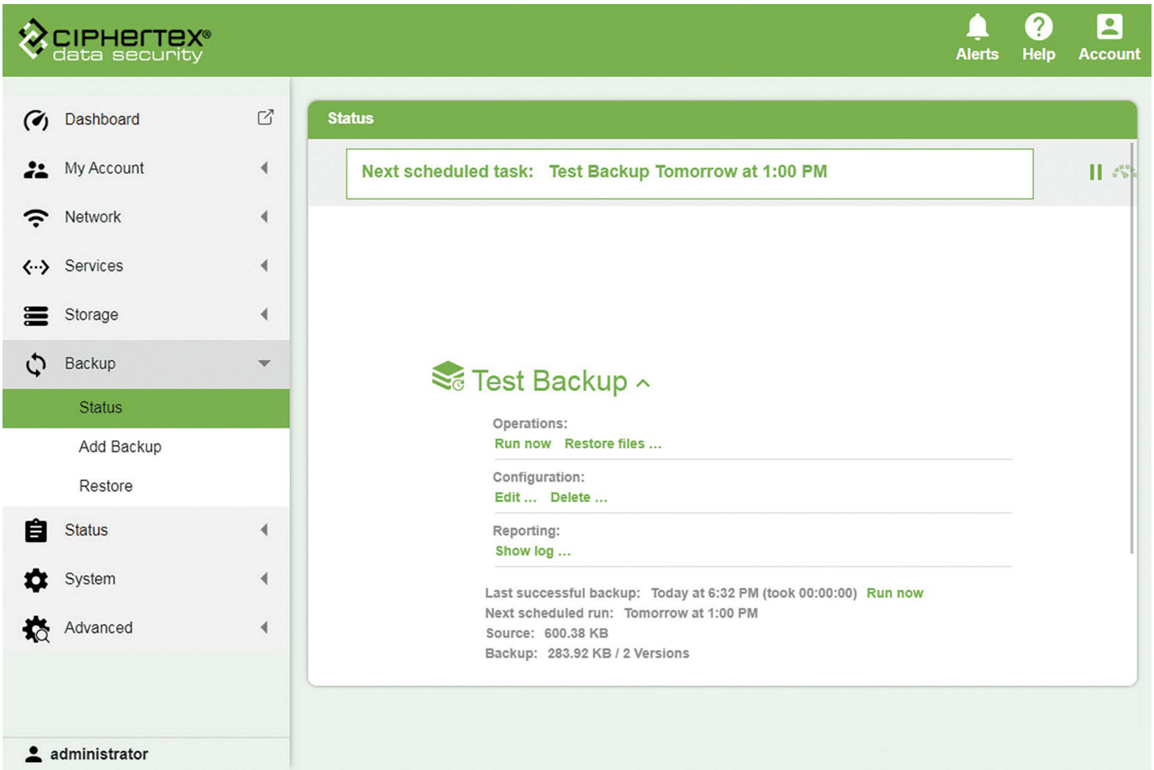
Run again every: 1 Days

Allowed days

☑ Mon
☑ Tue
☑ Wed
☑ Thu
☑ Fri
☑ Sat
☑ Sun

17. Click **Save** to save the backup job.
18. After the job has been saved, navigate back to the **Backup > Status** page to view the newly saved job.

10.2 Manage Backup Jobs



Next scheduled task: Test Backup Tomorrow at 1:00 PM

Test Backup

Operations:
Run now Restore files ...

Configuration:
Edit ... Delete ...

Reporting:
Show log ...

Last successful backup: Today at 6:32 PM (took 00:00:00) Run now
Next scheduled run: Tomorrow at 1:00 PM
Source: 600.38 KB
Backup: 283.92 KB / 2 Versions

VIEW THE STATUS OF A BACKUP JOB

1. Select the page under the **Backup > Status** menu item to view the status of currently configured backup jobs.
2. All currently configured backup jobs will be listed on this page.

RUN BACKUP JOB NOW

1. On the **Backup > Status** page, click on the name of the backup job that you want to run.
2. In the expanded job information under Operations, click on **Run now** to start that job.

EDIT A BACKUP JOB

1. On the **Backup > Status** page, click on the name of the backup job that you want to edit.
2. In the expanded job information under Configuration, click on **Edit**.
3. Edit the configuration settings for the job. These settings options are the same that were set when the job was created.
4. After going through each page using the Next button, click **Save** on the final page to save the new configuration.

DELETE A BACKUP JOB

1. On the **Backup > Status** page, click on the name of the backup job that you want to delete.
2. In the expanded job information under Configuration, click on **Delete**.
3. If you want to use this backup job later, choose to export the configuration first.
4. Click the **Delete backup** button to delete this backup job.

PAUSE A BACKUP JOB

Note:

- With the Pause button, you can temporarily stop a backup job from running.

1. Find a job in the list of currently scheduled jobs.
2. Click on the pause ⏸ icon next to the job that you want to pause.
3. On the Pause options window, select an amount of time to stop the job from running.
4. Click the Ok button to pause the job.

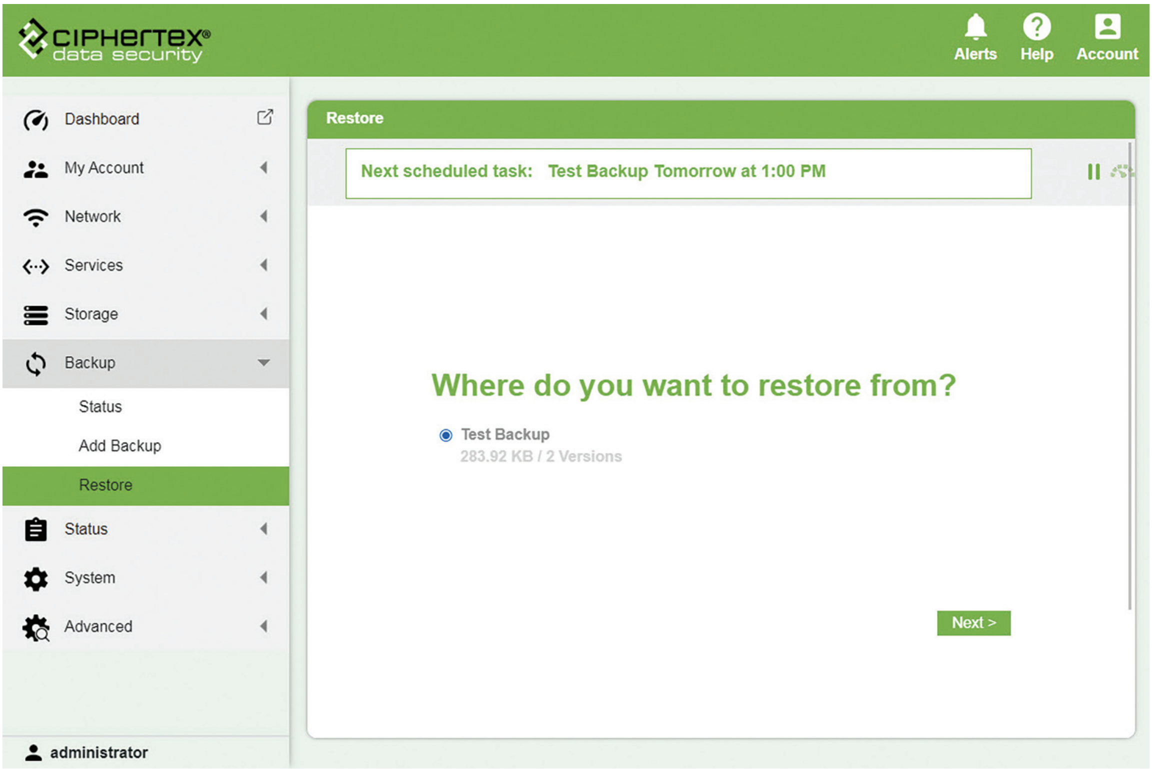
THROTTLE A BACKUP JOB

Note:

- With the Throttle button, you can limit the bandwidth used during a backup job.

1. Find a job in the list of currently scheduled jobs.
2. Click on the throttle icon next to the job that you want to throttle.
3. On the Throttle settings window, click the box next to **Max upload speed** to enable this option.
4. Enter a number in the box for the max upload speed.
5. On the Throttle settings window, click the box next to **Max download speed** to enable this option.
6. Enter a number in the box for the max download speed.
7. Click the Ok button to apply the throttle settings for the job.

10.3 Restore Data



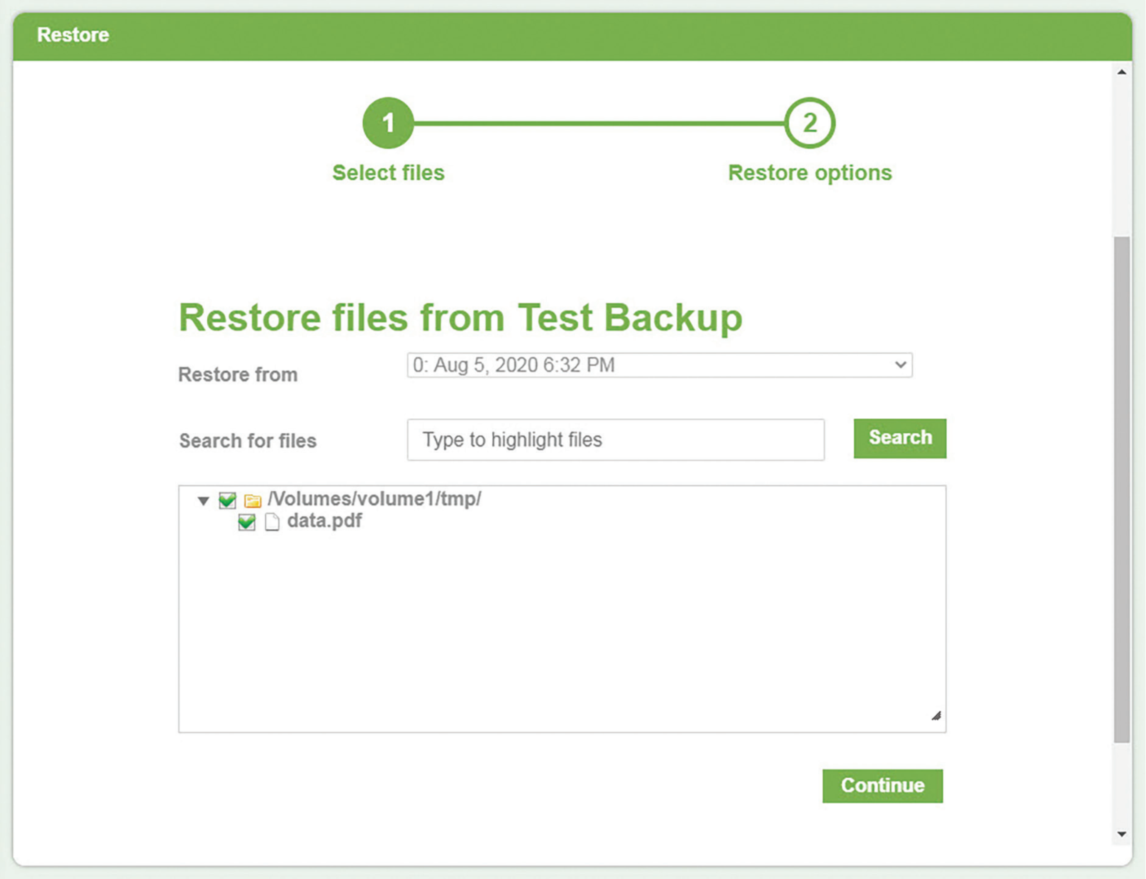
Next scheduled task: Test Backup Tomorrow at 1:00 PM

Where do you want to restore from?

● Test Backup
283.92 KB / 2 Versions

DIRECT RESTORE

1. Select the page under the **Backup > Restore** menu item to choose data to be restored.
2. Select name of the backup job from which you want to restore data.
3. Click the **Next** button.
4. On the **Select files Restore options** page, use the **Restore from** drop down menu to select a version of data to restore.
5. Use the Volumes tree to navigate and select the data to restore. A green check mark will appear next to the data that is selected for restore.



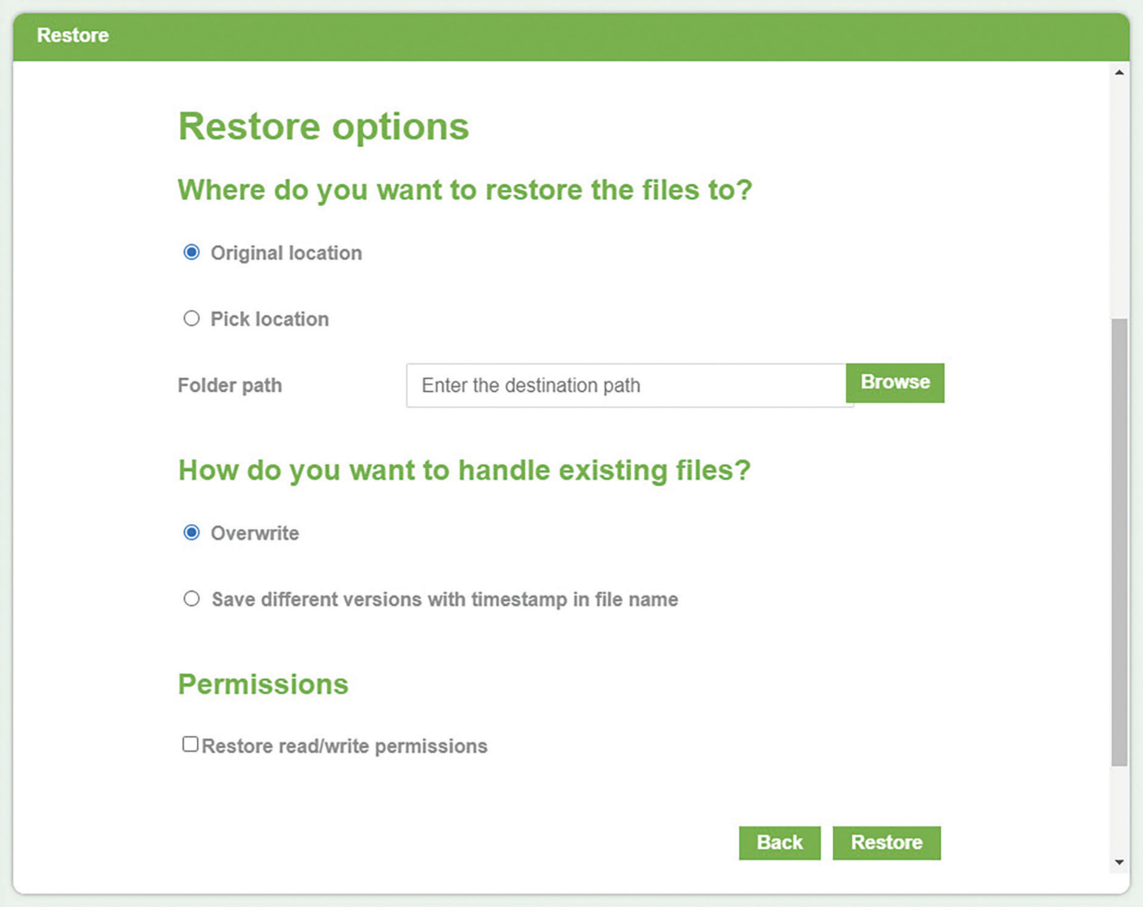
Restore files from Test Backup

Restore from: 0: Aug 5, 2020 6:32 PM

Search for files: Type to highlight files

- ☑ /Volumes/volume1/tmp/
  - ☑ data.pdf

6. Click the **Continue** button to go to the next page.
7. On the final page for restore options, choose where to restore files: **Original Location or Pick Location**.



Restore

Restore options

Where do you want to restore the files to?

● Original location

○ Pick location

Folder path: Enter the destination path

How do you want to handle existing files?

● Overwrite

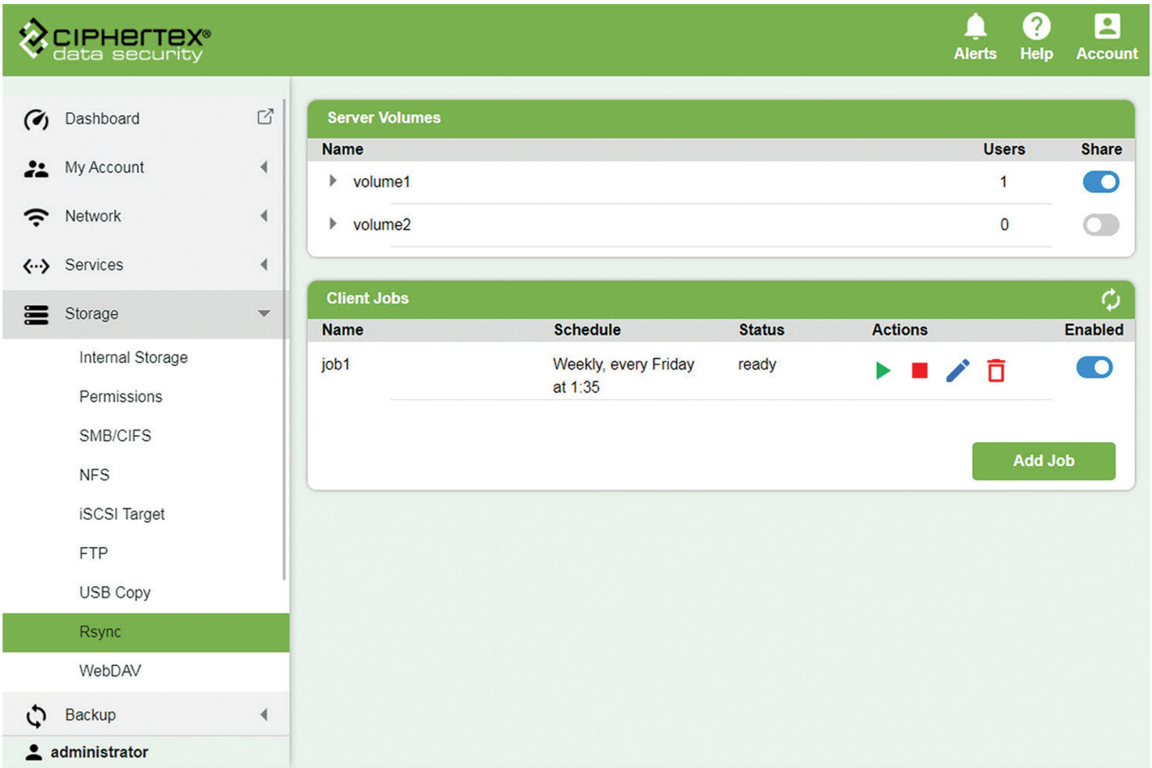
○ Save different versions with timestamp in file name

Permissions

□ Restore read/write permissions

8. If you chose to pick a new location to restore, click the Browse button to enter a destination.
9. If you chose to restore to the original location, you now have to choose how to handle file collisions with existing files (the file already exists in the restore location). Overwrite will remove the file in the destination and replace it with the restored version. Or you can choose to save the restored file by using the timestamp in the filename which will preserve the file that already exists in the destination.
10. Next, select or deselect the Restore read/write permissions to choose how to restore file access permissions. This is disabled by default because selecting this option might prevent access to the files that are being restored.
11. Click the **Restore** to start the restore operation for your data.

11 Rsync Remote Backup



Server Volumes

Name	Users	Share
volume1	1	●
volume2	0	○

Client Jobs

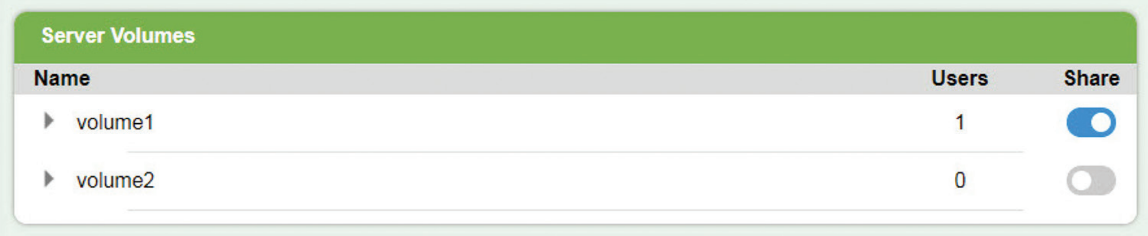
Name	Schedule	Status	Actions	Enabled
job1	Weekly, every Friday at 1:35	ready	▶ ■ ✎ 🗑	●

Select the page under the Storage > Rsync to configure settings for sharing and remote syncing volumes via Rsync.

11.1 Set Up Rsync Server

ENABLE REMOTE REPLICATION WITH RSYNC

1. On the Rsync page in the Server Volumes section, find the volume that you want to share for remote replication.
2. To share a volume via Rsync, click on the toggle switch ● under the heading **Share**. When the switch is blue and positioned to the right, the volume is shared.

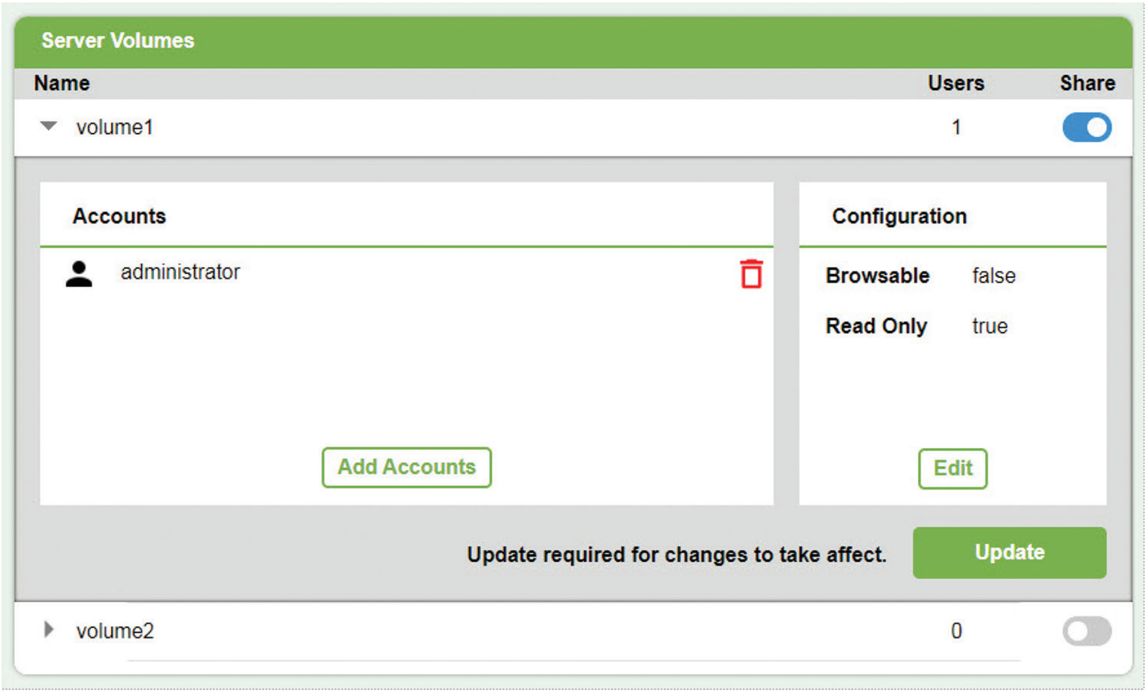


Server Volumes

Name	Users	Share
volume1	1	●
volume2	0	○

CONFIGURE VOLUMES FOR RSYNC

1. On the Rsync page in the Server 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.



Browsable false

Read Only true

Update required for changes to take affect.

RSYNC VOLUME ACCOUNTS

1. To add accounts that can access the volume via Rsync, click the Add Accounts button.
2. From the Add Accounts pop-up, select the accounts to add and then click the **Add** button.

RSYNC VOLUME CONFIGURATION

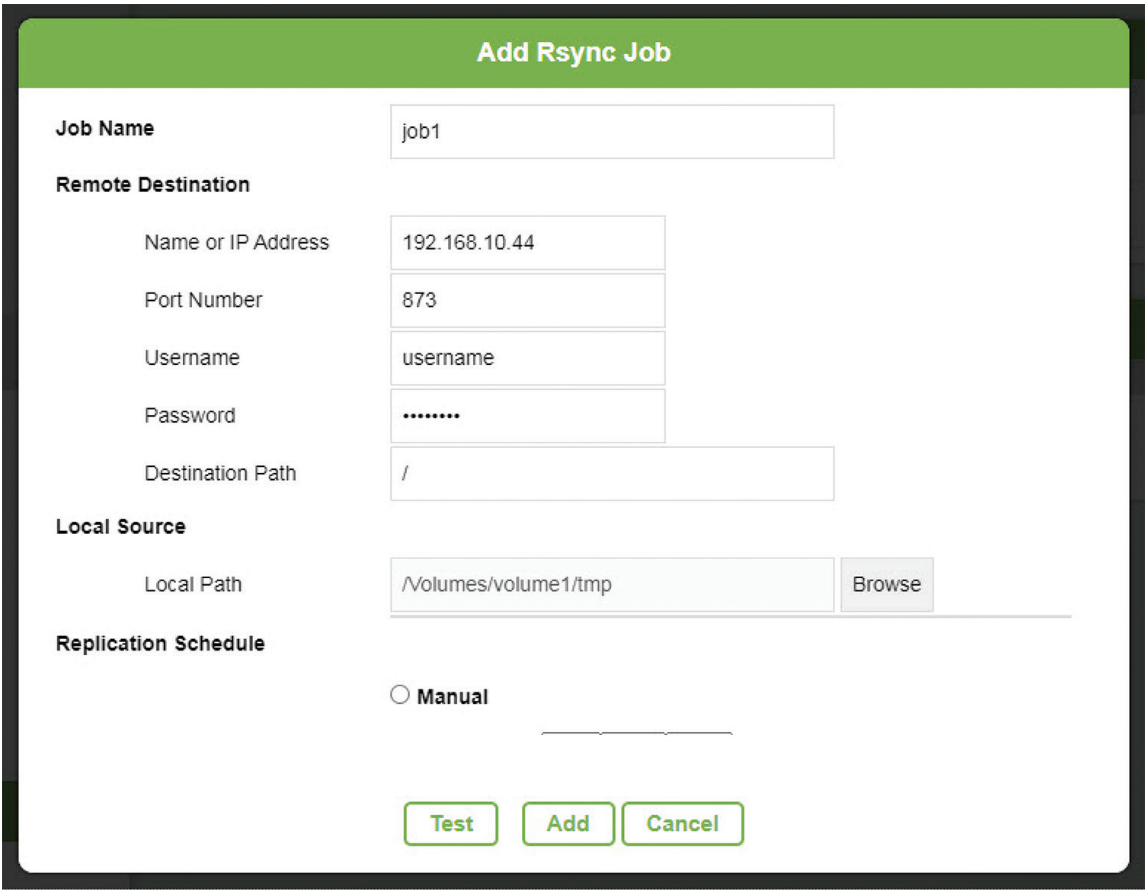
1. Click the Edit button to edit the configuration for the volume.
2. From the Edit Configuration Accounts pop-up, configure the following options and click the **Ok** button.

Browsable	Enable/disable the browsable option for Rsync. This controls whether or not this share is seen in the list of available shares in a network view.
Read Only	Enable/disable read only access to the volume.

11.2 Create Rsync Backup Jobs

ADD RSYNC JOBS

1. Select the page under the **Storage > Rsync** menu item to create and schedule rsync jobs to run.
2. In the Client Jobs section, click the **Add Job** button.
3. In the Add Rsync Job pop-up, fill out the following information and then click the **Add** button:



Add Rsync Job

Job Name: job1

Remote Destination

Name or IP Address: 192.168.10.44

Port Number: 873

Username: username

Password: •••••••••

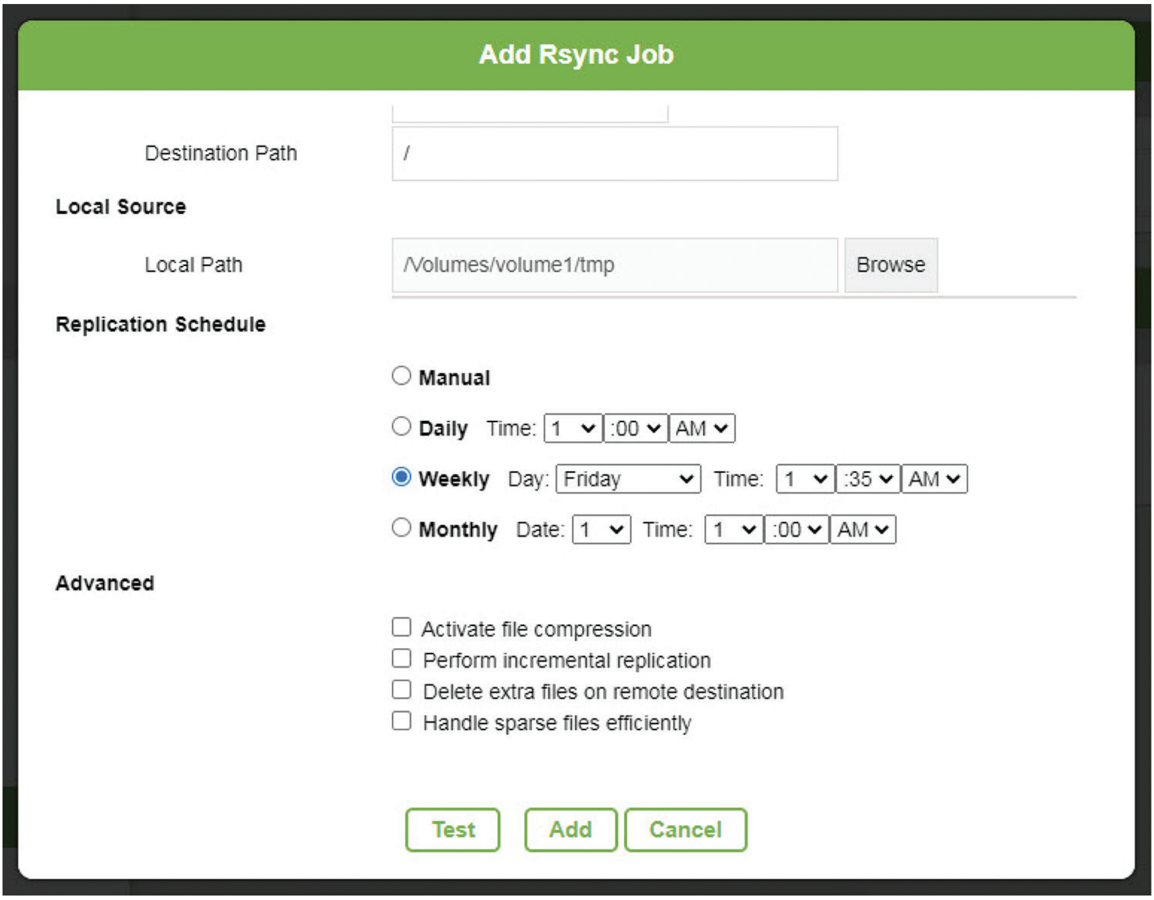
Destination Path: /

Local Source

Local Path: /Volumes/volume1/tmp

Replication Schedule

○ **Manual**



Add Rsync Job

Destination Path /

Local Source

Local Path /Volumes/volume1/tmp

Replication Schedule

○ **Manual**

○ **Daily** Time: 1 :00 AM

● **Weekly** Day: Friday Time: 1 :35 AM

○ **Monthly** Date: 1 Time: 1 :00 AM

Advanced

□ Activate file compression
□ Perform incremental replication
□ Delete extra files on remote destination
□ Handle sparse files efficiently

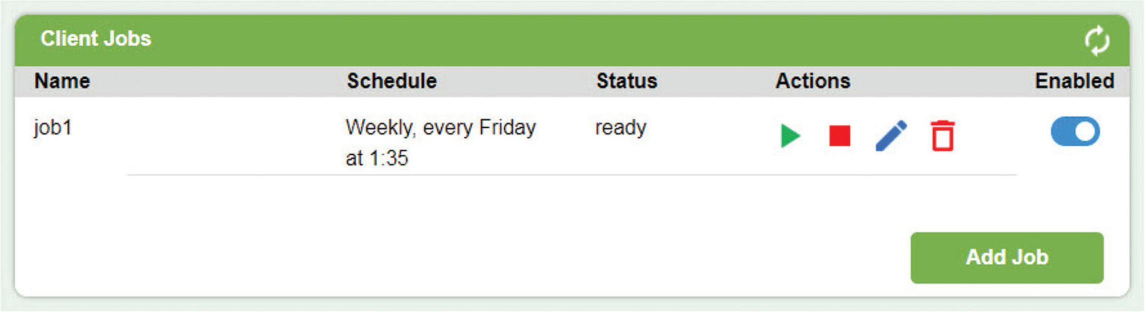
Job Name	A descriptive name for the rsync job.
Remote Destination	
Name or IP Address	The name or IP address of the remote destination to which the data will be replicated.
Port Number	The port number of the remote destination to which the data will be replicated. Optional. If left blank, the default port number 873 will be used.
Username	The username used to log in to the remote server. Optional.
Password	The password used to log in to the remote server. Optional.

Destination Path	The pathname or destination directory where data will be replicated.
Local Source	
Local Path	The pathname for the data on the SecureNAS that will be replicated. Click the **Browse** to select a directory on the SecureNAS.
Replication Schedule	• Manual - Run this job manually using the play button on the Rsync screen. • Daily - Run this job every day at the specified time. Use the Time drop-downs next to Daily to specify a time of day. • Weekly - Run this job one day a week on the specified day at the specified time. Use the Day drop-down to select a day of the week and use the Time drop-downs to specify a time of day. • Monthly - Run this job once a month on the specified day of the month. Use the Date drop-down to select which day of the month and use the Time drop-downs to specify a time of day.
Advanced	
Activate file compression	Allow file compression during data transfer to the remote destination. Use this option for low bandwidth environments.
Perform incremental replication	Only backup the files that have changed since the previous backup. Files that have not changed in the local source path will not be replicated after the initial backup.
Delete extra files on remote destination	Sync the local source and destination by removing files in the remote destination that no longer exist in the local path.
Handle sparse files efficiently	Reduce the time required to replicate sparse files from the local path.

Note:

- Click the **Test** button to test the remote destination connection information for this job.

11.3 Manage Rsync Jobs



Client Jobs

Name	Schedule	Status	Actions	Enabled
job1	Weekly, every Friday at 1:35	ready	▶ ■ ✎ 🗑	●

ENABLE A RSYNC JOB

1. On the Rsync page in the Client Jobs section, find the job that you want to enable for remote replication.
2. To enable a Rsync job, click on the toggle switch ● under the heading **Enabled**. When the switch is blue and positioned to the right, the job is enabled and will run according to the job schedule.

START A MANUAL RSYNC JOB

1. On the Rsync page in the Client Jobs section, find the job that you want to start now.
2. Click the green play button ▶ under Actions to start that job now.

Note:

- Only jobs with a "Manual" schedule can be run using the green play button.

STOP A RSYNC JOB

1. On the Rsync page in the **Client Jobs** section, find the job that you want to stop from running now.
2. Click the red stop button ■ under Actions to stop that job now.

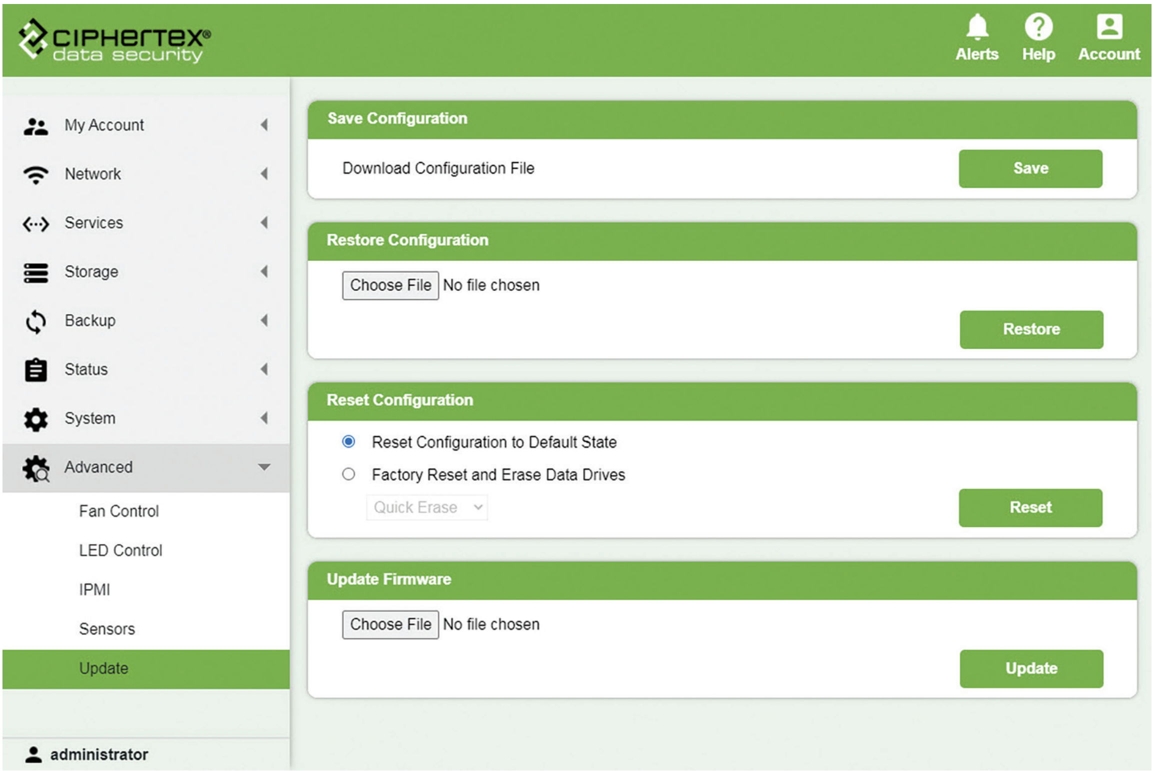
EDIT A RSYNC JOB

3. On the Rsync page in the **Client Jobs** section, find the job whose configuration you want to edit.
4. Click the blue edit pencil button ✎ under Actions to edit the job configuration.
5. On the Edit Rsync Job pop-up, edit and change the information. Job Name is not editable.
6. Click the **Save** button to save the job configuration changes.

DELETE A RSYNC JOB

7. On the Rsync page in the **Client Jobs** section, find the job that you want to delete.
8. Click the red trash can button 🗑 under Actions to delete that job now. This operation cannot be undone.

12 Update SecureNAS



Save Configuration

Download Configuration File

Restore Configuration

Choose File No file chosen

Reset Configuration

● Reset Configuration to Default State

○ Factory Reset and Erase Data Drives

Quick Erase

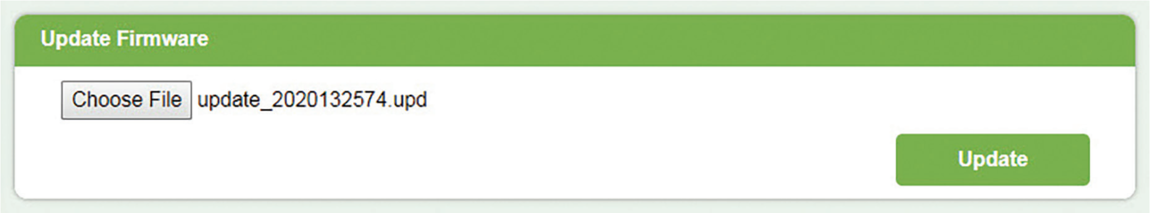
Update Firmware

Choose File No file chosen

Select the page under the **Advanced > Update** menu item to update SecureNAS firmware, save the SecureNAS configuration, restore the SecureNAS from a saved configuration, or reset the SecureNAS to original manufacturer settings.

12.1 Update Firmware

UPDATE SECURENAS FIRMWARE



Update Firmware

Choose File update_2020132574.upd

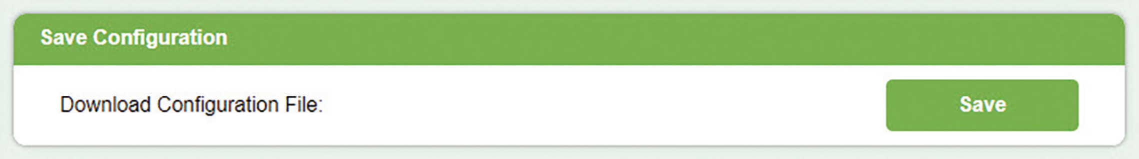
1. Select the page under the **Advanced > Update** menu item to update the SecureNAS firmware.
2. On the Update page in the **Update Firmware** section, click the **Choose File** button.
3. In the file browser window that pops-up, choose the SecureNAS update file (.upd) and click Open.
4. Verify that the update file is now listed in the Update Firmware section.
5. Click the **Update** button to start the update process.

Note:

- Before starting an update, it is highly advised to first save the configuration to retain as a backup.

12.2 Save and Restore Configuration

SAVE SECURENAS CONFIGURATION



Save Configuration

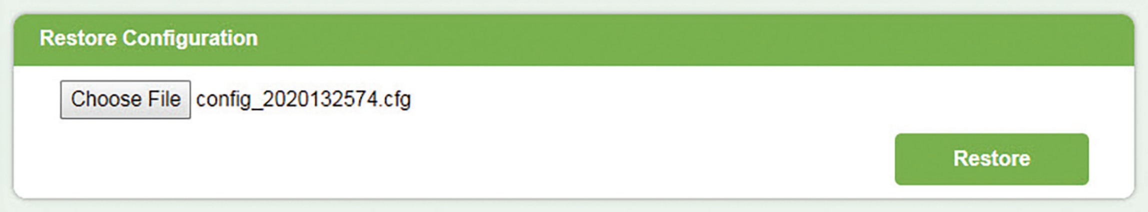
Download Configuration File:

1. Select the page under the **Advanced > Update** menu item to save the current SecureNAS configuration.
2. In the Save Configuration section, click the **Save b**utton. This will download a configuration file (.cfg).

Note:

- Before starting an update, restoring a previous configuration, or manufacturer reset to defaults, it is highly advised to first save the configuration to retain as a backup.

RESTORE SECURENAS CONFIGURATION



Restore Configuration

Choose File config_2020132574.cfg

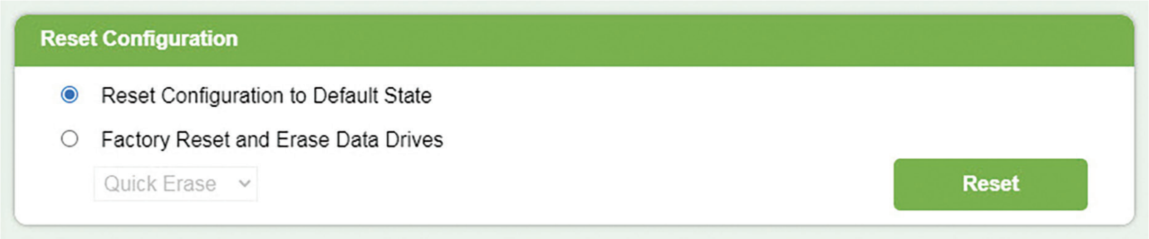
1. Select the page under the **Advanced > Update** menu item to restore the SecureNAS configuration to a previously saved configuration.
2.In the Restore Configuration section, click the **Choose File** button.
3. In the file browser window that pops-up, choose the SecureNAS configuration file (.cfg) and click Open.
4. Verify that the configuration file is now listed in the Restore Configuration section.
5. Click the **Restore** button.
6. You will be prompted to enter login credentials to proceed with the restore. Enter your login password and click Confirm to begin the restore process.

Note:

- Before restoring a previous configuration, it is highly advised to first save the configuration to retain as a backup.

12.3 Reset and Erase

RESET SECURENAS TO MANUFACTURER DEFAULTS



Reset Configuration

● Reset Configuration to Default State

○ Factory Reset and Erase Data Drives

1. Select the page under the **Advanced > Update** menu item to restore the SecureNAS to manufacturer defaults.
2. In the **Reset** Configuration section, select **Reset Configuration to Default State**.
3. Click the **Reset** button.
4. You will be prompted to enter login credentials to proceed with the reset. Enter your login password and click Confirm to begin the reset process.

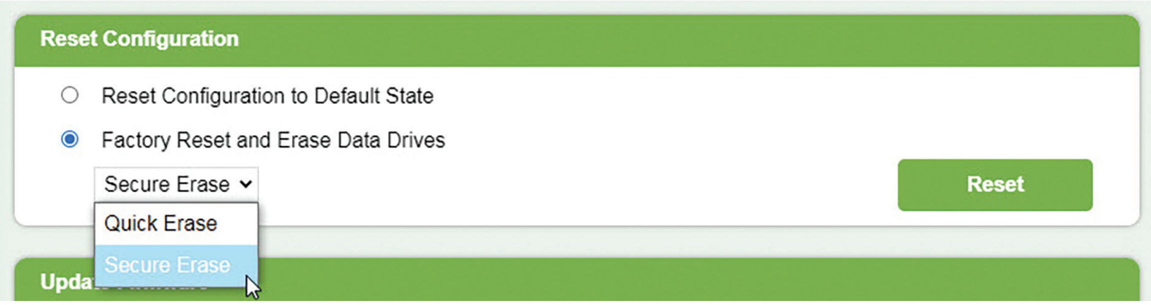
Note:

- Resetting the configuration will only set the SecureNAS back to manufacturer default settings. All storage will remain in place.
- Before resetting to manufacturer defaults, it is highly advised to first save the configuration to retain as a backup.

FACTORY RESET AND ERASE

IMPORTANT:

- A factory reset can take between 20 minutes and 6 hours depending on options chosen and the amount of data on the SecureNAS. Your SecureNAS unit will not be available for use during that time.
- SAS drives can perform Instant Secure Erase.



Reset Configuration

○ Reset Configuration to Default State

● Factory Reset and Erase Data Drives

Secure Erase

1. Select the page under the **Advanced > Update** menu item to factory reset the SecureNAS and erase data drives.
2. In the Reset Configuration section, select either **Quick Erase or Secure Erase**.

Note:

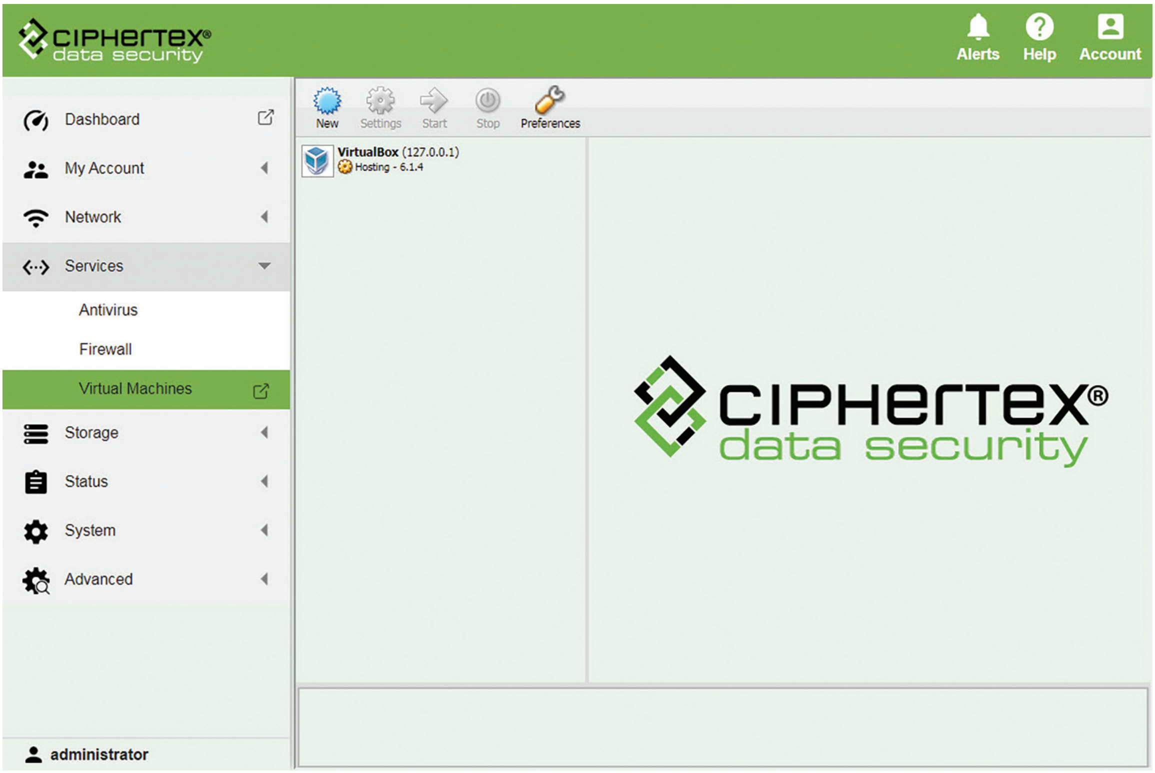
- **Quick Erase:** This option will erase installed data drives during the factory reset. After a quick erase, data could still be recoverable using certain data recovery services.
- **Secure Erase:** This option will completely and securely erase installed data drives during the factory reset. **This will erase all of your data and data will not be recoverable**. This option amounts to electronic data shredding and all installed user data drives will be completely erased of all user data. Your SecureNAS will not be available for use until the secure erase has been completed.

3. Click the **Reset** button.
4. You will be prompted to enter login credentials to proceed with the reset. Enter your login password and click Confirm to begin the reset and erase process.
5. The SecureNAS unit will run the internal fans at full speed during the factory reset process to keep the system cool. Once the process is complete, the SecureNAS will automatically shutdown.

Note:

- Before performing a factory reset and erase, it is highly advised to first save the configuration to retain as a backup. You may also want to create a backup of any data that you do not want permanently deleted.

13 Virtual Machines



Select the page under the **Services > Virtual Machines** menu item to configure virtual machines that will be stored on SecureNAS.

SecureNAS utilizes Oracle® VM VirtualBox® for its virtual machine offerings. All virtual machines configured through the SecureNAS Management Console will be stored on SecureNAS volumes.

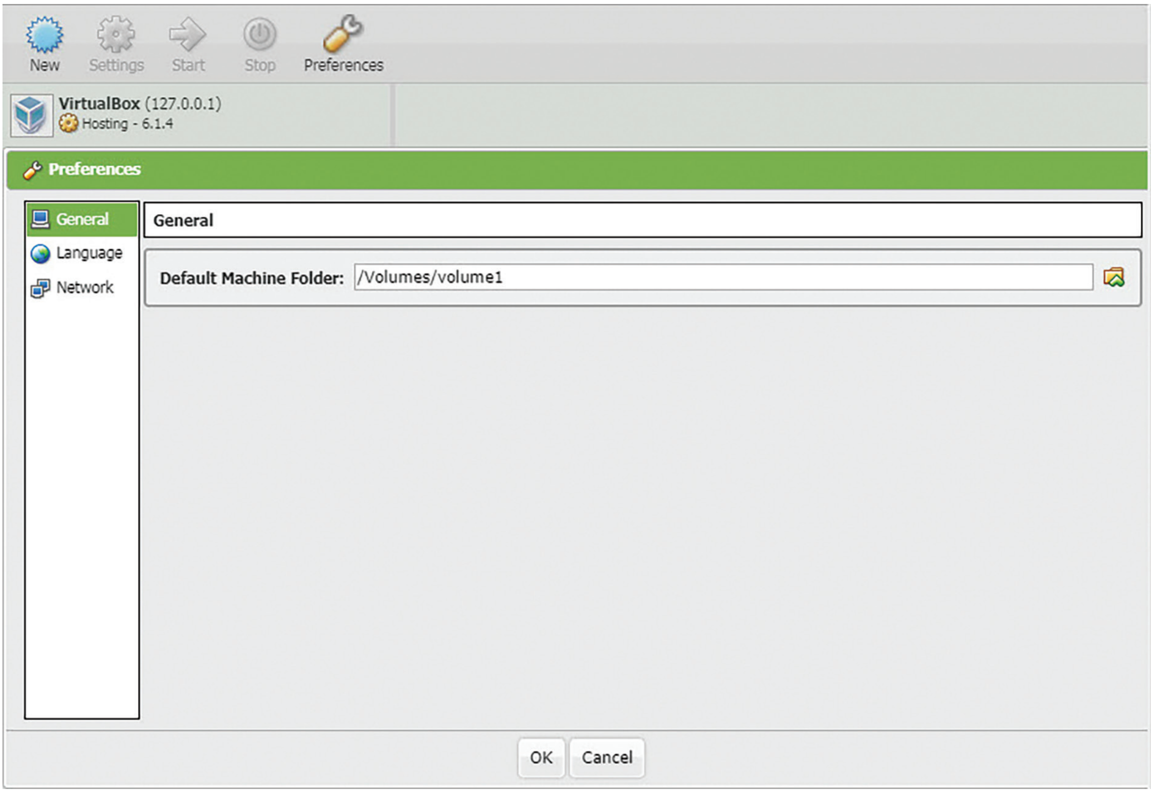
13.1 Configure Virtual Machine Default Preferences

CONFIGURE VIRTUAL MACHINE DEFAULT PREFERENCES

IMPORTANT:

- If this is the first time that you are creating a virtual machine, you must first configure the virtual machine settings.

1. On the Virtual Machines page, click the **Preferences** button to configure settings.
2. In the Preferences section, select **General**.
3. In the General section, click the folder icon to choose a default folder/volume for the virtual machines.
4. Click **OK** to save the settings.machines.



Default Machine Folder: /Volumes/volume1

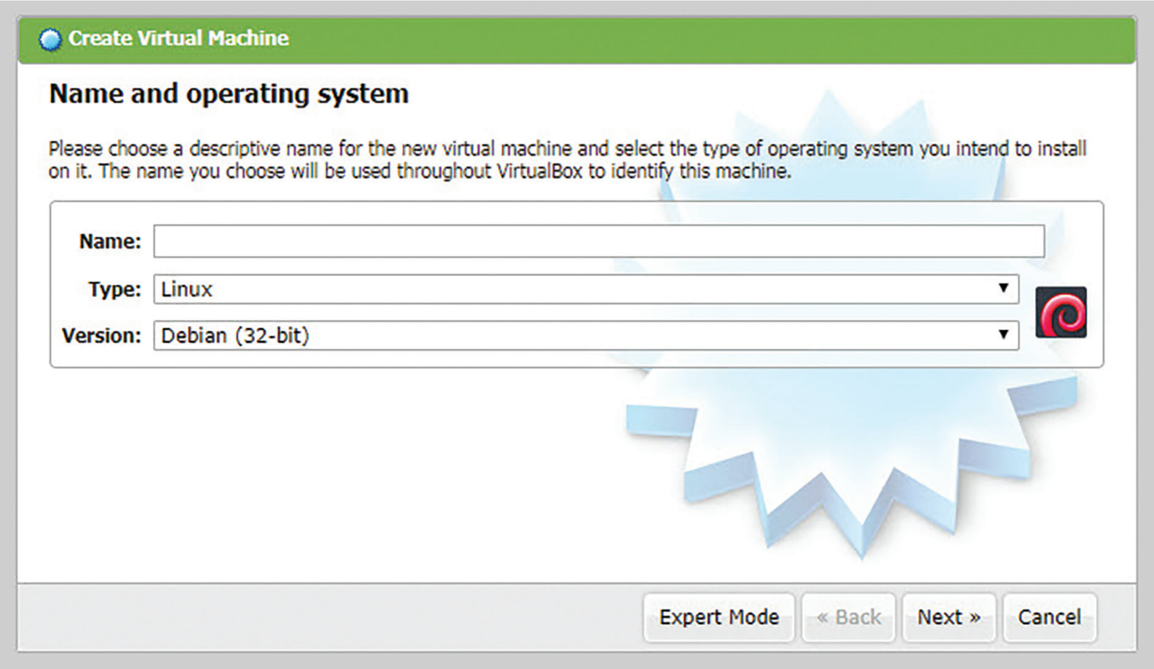
13.2 Create a Virtual Machine

CREATE A VIRTUAL MACHINE

Note:

- If this is the first time that you are creating a virtual machine, you must first configure the virtual machine settings.

1. On the Virtual Machines page, click the ✹ **New** button to create a virtual machine.
2. On the Name and operating system pop-up, fill in the following information and then click the **Next** button:



Create Virtual Machine

Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

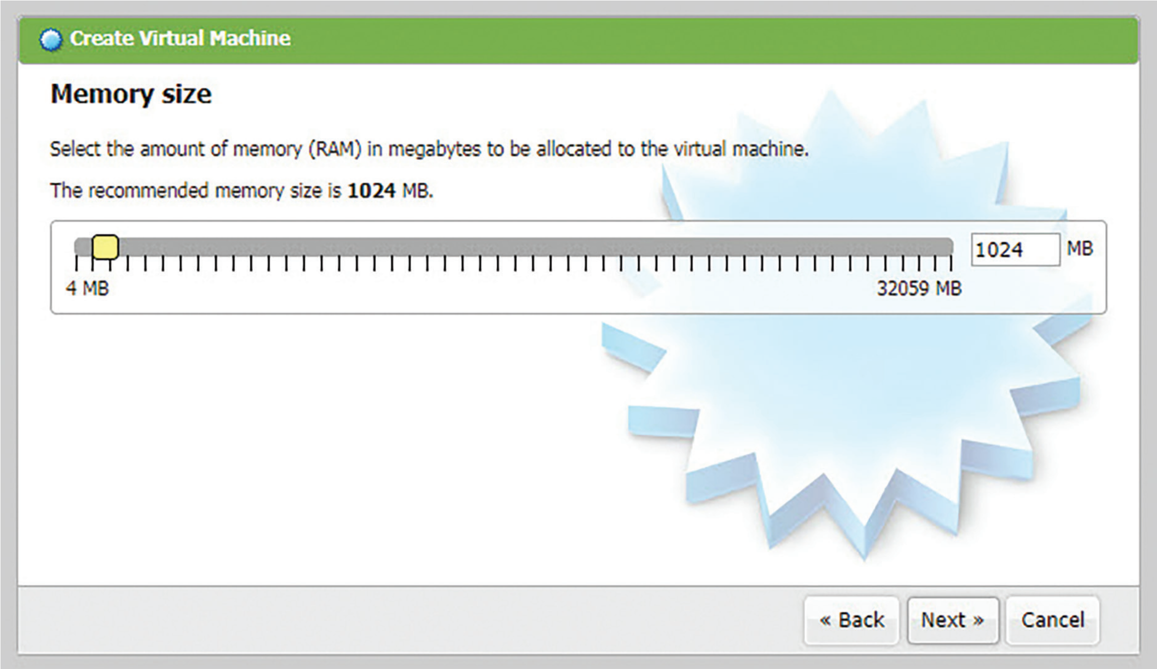
Name:

Type: Linux

Version: Debian (32-bit)

Name	The name of the virtual machine. This is the name that will be shown in the machine list on the Virtual Machines page. Be sure to assign each virtual machine an informative name that describes the operating system and software running on the virtual machine.
Type	The operating system type that you want want to install. The supported operating systems are grouped in the drop-down list. Certain virtual machines settings will be enabled/disabled depending on your selection. **Note:** If you want to install something very unusual, select Other.
Version	The version of the type of operating system that you want to install. These values will change depending on the Type of operating system that was selected above.

3. On the Memory size window, select the amount of memory (RAM) in megabytes to be allocated to the virtual machine and then click the **Next** button.



Create Virtual Machine

Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

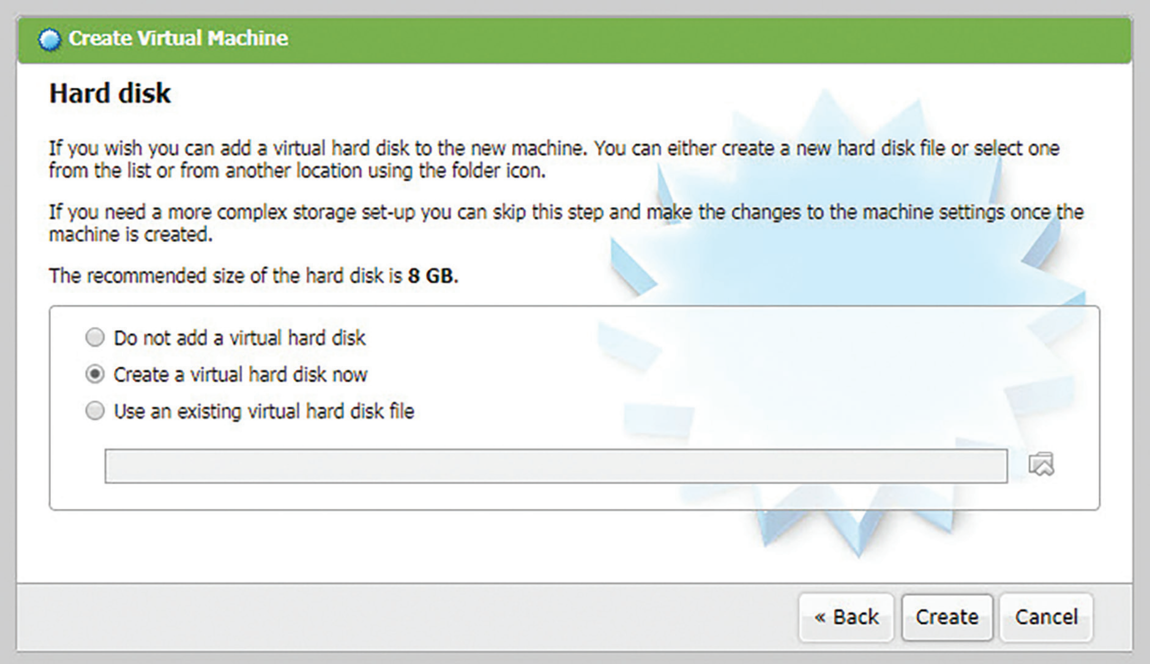
The recommended memory size is **1024** MB.

1024 MB

Note:

- Choose the memory setting carefully. The amount of memory given to the virtual machine will not be available to SecureNAS while the virtual machine is running. So do not allocate more than you can spare.

4. On the Hard disk window, select **Create a virtual hard disk now** and then click the **Create** button. This will begin the process of creating a virtual hard disk.



Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

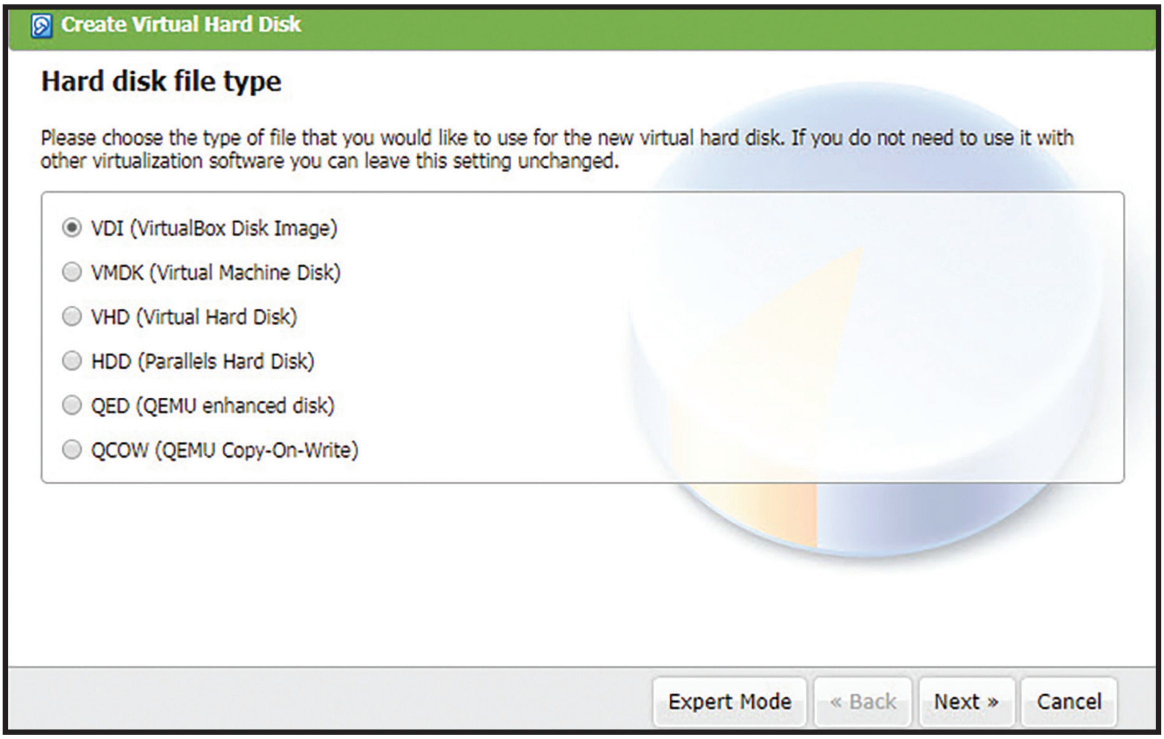
The recommended size of the hard disk is **8 GB**.

○ Do not add a virtual hard disk

● Create a virtual hard disk now

○ Use an existing virtual hard disk file

5. On the Hard disk file type window, select **VDI (VirtualBox Disk Image)** and then click the **Next** button.



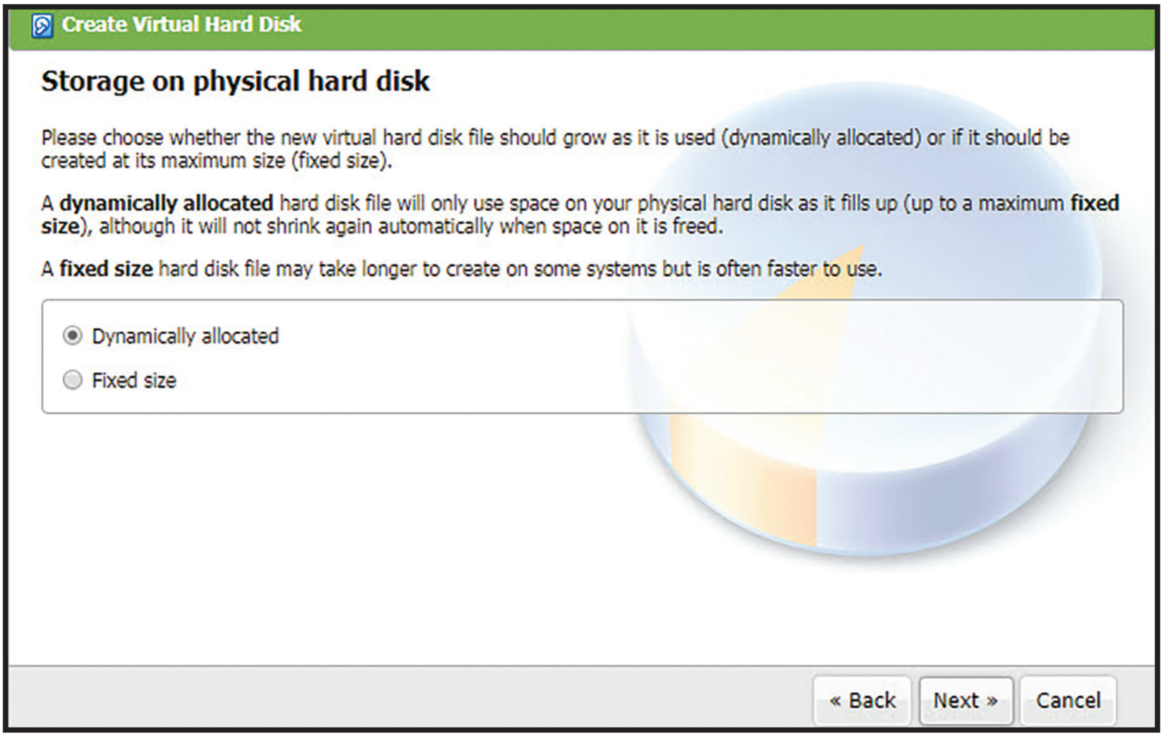
Create Virtual Hard Disk

Hard disk file type

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

● VDI (VirtualBox Disk Image)
○ VMDK (Virtual Machine Disk)
○ VHD (Virtual Hard Disk)
○ HDD (Parallels Hard Disk)
○ QED (QEMU enhanced disk)
○ QCOW (QEMU Copy-On-Write)

6. On the Storage on physical hard disk window, choose between Dynamically allocated and Fixed size for the new virtual hard disk file. Then click the **Next** button.



Create Virtual Hard Disk

Storage on physical hard disk

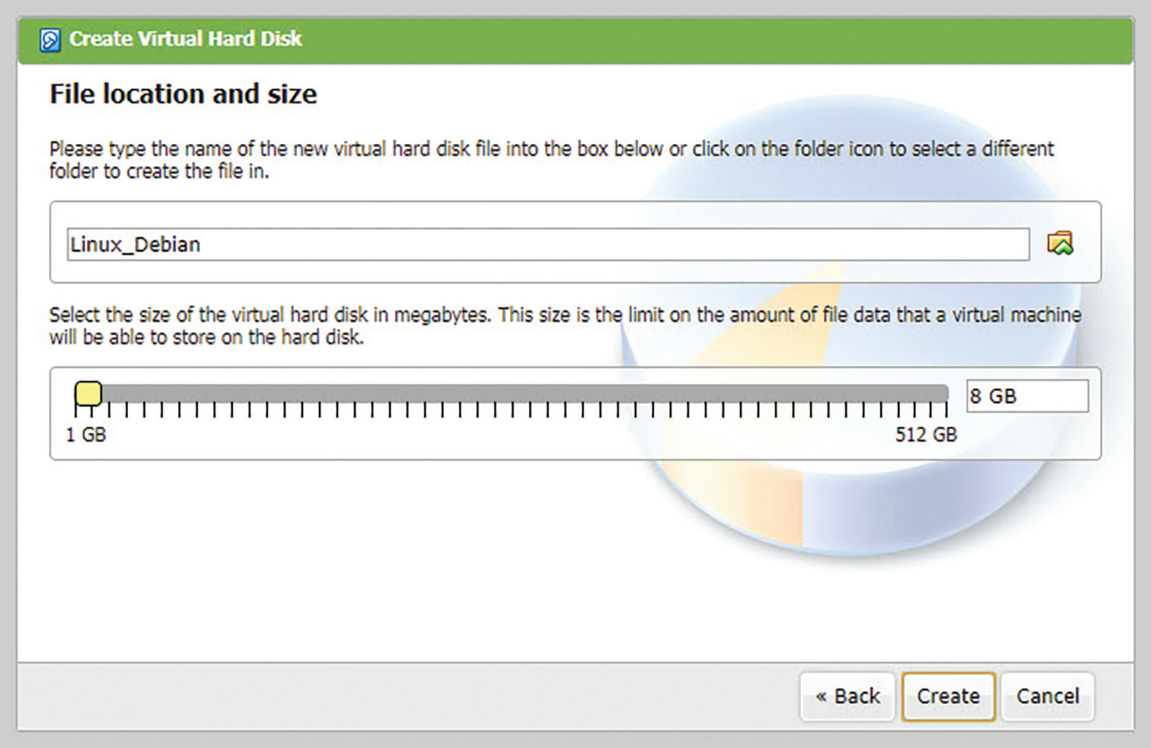
Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

● Dynamically allocated
○ Fixed size

7. On the File location and size window, click the folder icon to select a volume for the new virtual hard disk file and select the size to be used. Then click the **Create** button.



Create Virtual Hard Disk

File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

Linux_Debian

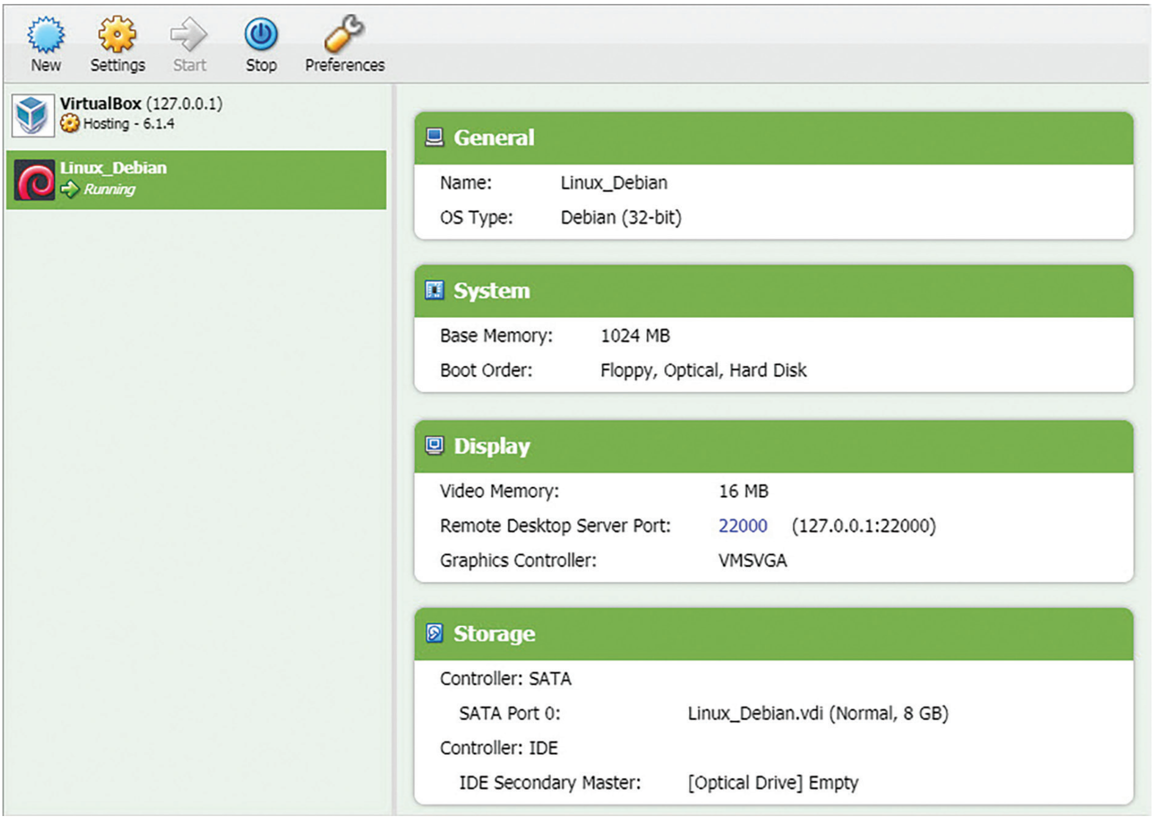
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

8 GB

13.3 Manage Virtual Machines

VIEW VIRTUAL MACHINE SETTINGS

1. On the Virtual Machines page, select a virtual machine from the list to view the general settings.



General

Name: Linux_Debian
OS Type: Debian (32-bit)

System

Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk

Display

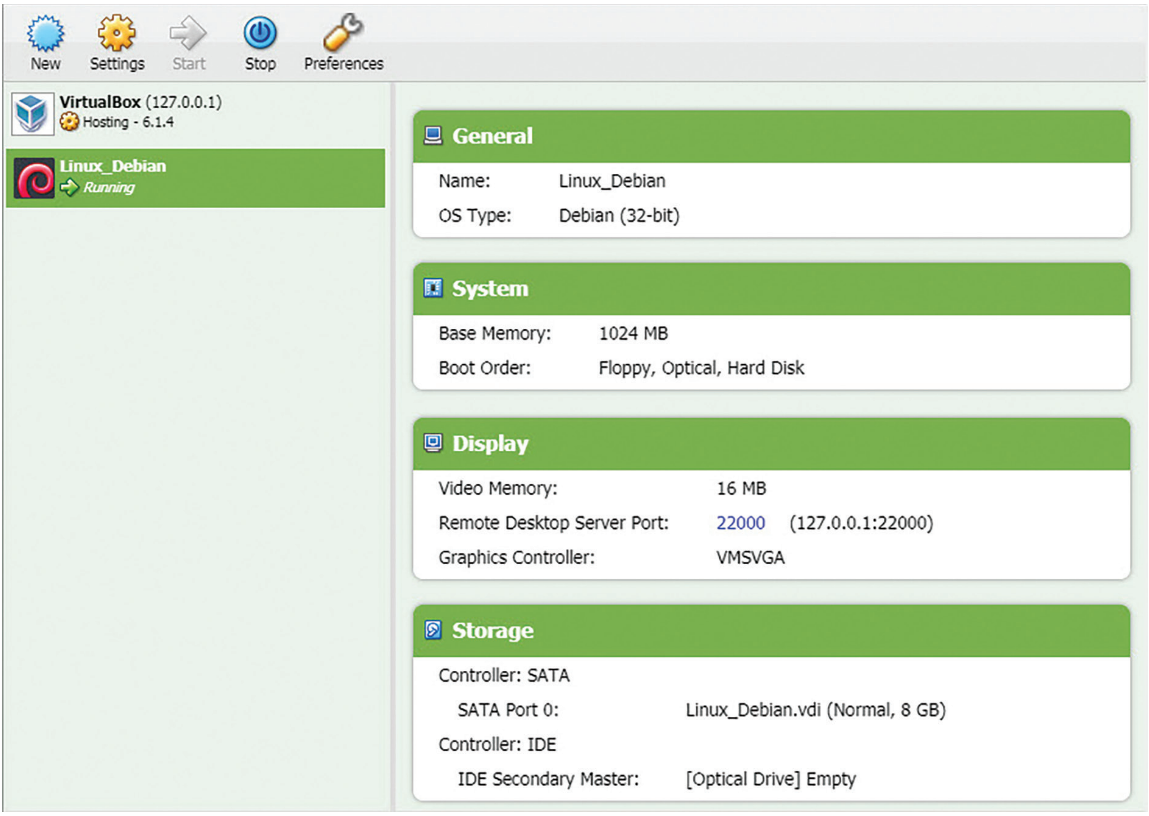
Video Memory: 16 MB
Remote Desktop Server Port: 22000 (127.0.0.1:22000)
Graphics Controller: VMSVGA

Storage

Controller: SATA
SATA Port 0: Linux_Debian.vdi (Normal, 8 GB)
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty

CHANGE VIRTUAL MACHINE SETTINGS

1. On the Virtual Machines page, select a virtual machine from the list.
2. Click the ⚙ **Settings** icon and then choose Settings from the drop-down menu to change the settings for the selected virtual machine.
3. Click **OK** to save the settings changes.



General

Name: Linux_Debian

OS Type: Debian (32-bit)

System

Base Memory: 1024 MB

Boot Order: Floppy, Optical, Hard Disk

Display

Video Memory: 16 MB

Remote Desktop Server Port: 22000 (127.0.0.1:22000)

Graphics Controller: VMSVGA

Storage

Controller: SATA

SATA Port 0: Linux_Debian.vdi (Normal, 8 GB)

Controller: IDE

IDE Secondary Master: [Optical Drive] Empty

13.4 Start/Stop Virtual Machines

START A VIRTUAL MACHINE

1. On the Virtual Machines page, select a virtual machine from the list.
2. Once the virtual machine is selected and highlighted, click the ➡ **Start** icon.
3. The virtual machine will now say "Running" under the name.

STOP A VIRTUAL MACHINE

1. On the Virtual Machines page, select a virtual machine from the list.
2. Once the virtual machine is selected and highlighted, click the ⏻ **Stop** icon.
3. Choose **Power Off** from the drop-down menu.
4. In the pop-up window, click the Power Off button to confirm that you want to stop the virtual machine.
5. The virtual machine will now say "Powered Off" under the name.

13.5 Virtual Machine

REMOVE A VIRTUAL MACHINE

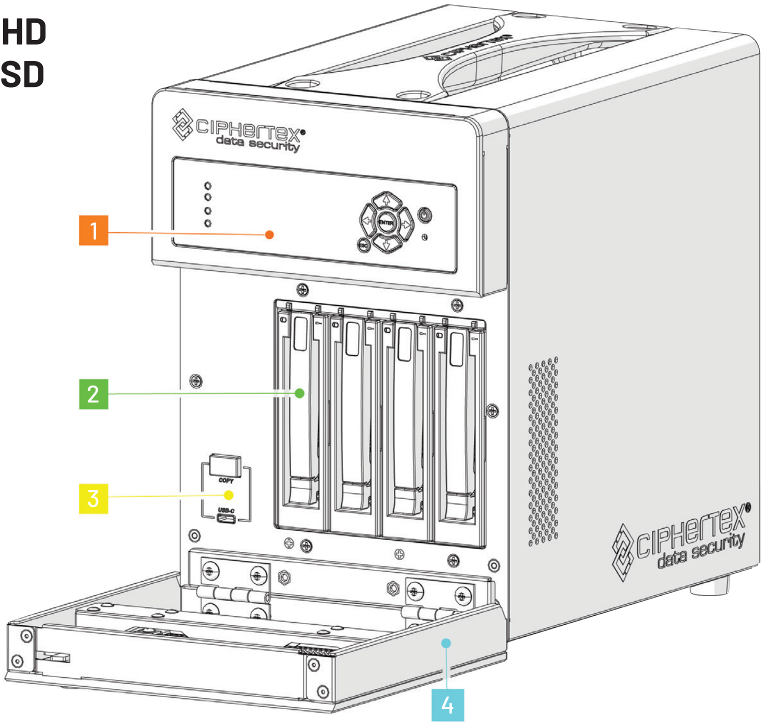
1. On the Virtual Machines page, select a virtual machine from the list.
2. Right-click on the name of the virtual machine and select **Remove** from the drop-down menu.
3. On the pop-up window, select either **Delete all files** or **Remove only**.

Note:

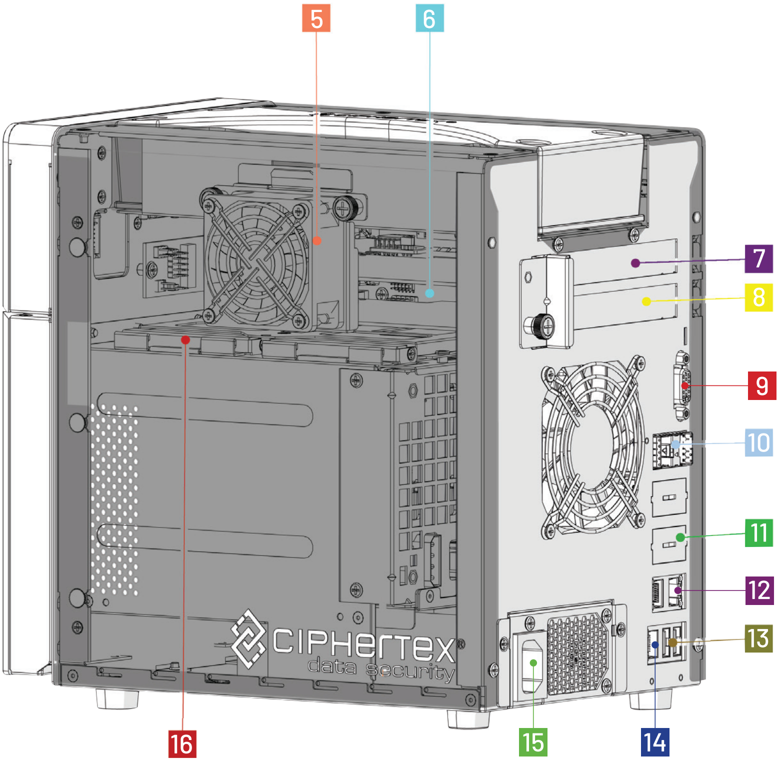
- If this is the first time that you are creating a virtual machine, you must first configure the virtual machine settings.

SecureNAS CX-40KHD
SecureNAS CX-40KSD

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

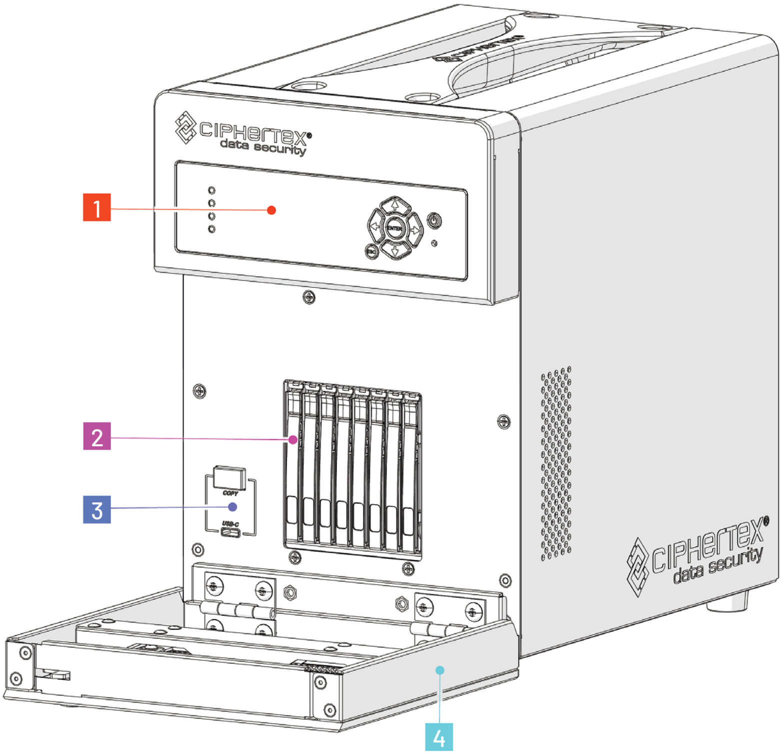


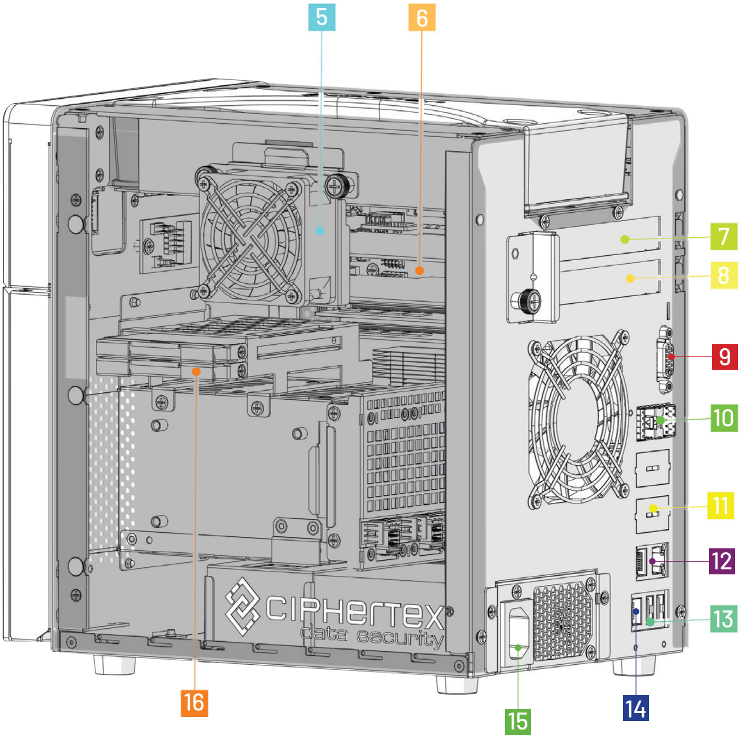
5. Cooling Fan
6. 7. 8. Expansion Slot
9. DB15 Port
10. 10GBE SFP+Ports
11. Optional 10 G
Ethernet Ports (4)
12. RJ-45 Gigabit LAN
13. USB 3.0 (Type-A Ports)
14. IPMI Port
15. Power Connector
16. The OS is mirrored on
two internal 2.5″ SSDs
for fail-safe operation.



SecureNAS CX-80KSD

1. LCD Display
2. SSDs (8)
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-80KHD-X
SecureNAS CX-80KSD-X
SecureNAS CX-120KHSD-X

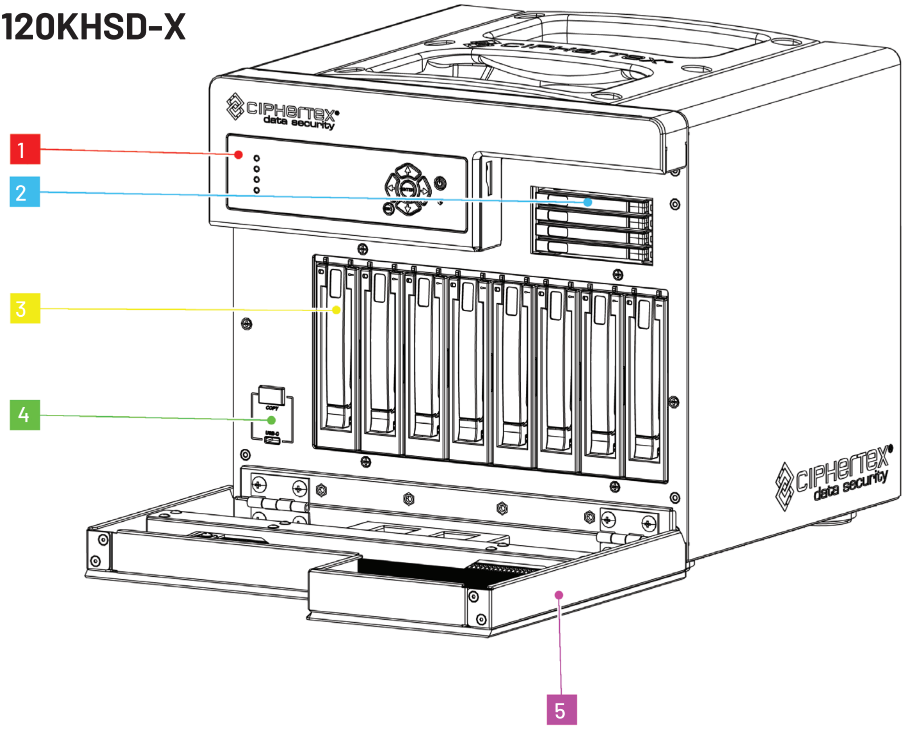
1. LCD Display

2. 4-SSD Drives (Only Model CX-120KHSD-X)

3. 8-HDDs or SSDs

4. USB-C Port Encryption Key

5. Locking Security Door



6. PCIe Extension

7. PCIe Extension

8. DB1 Port

9. 10 GbE SFP+Ports

10. 10 G Ethernet Ports (4)

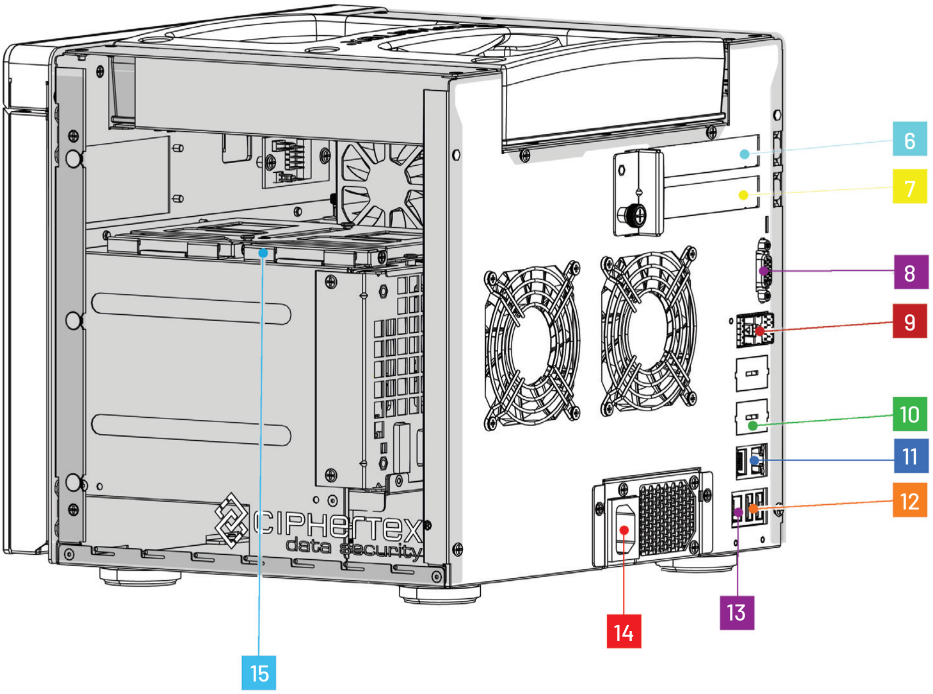
11. RJ-45 Gigabit LAN

12. USB 3.0 (Type A Ports)

13. IPMI Port

14. Power Connector

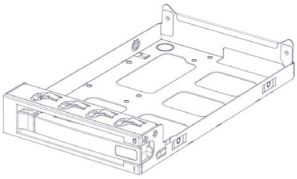
15. The OS is mirrored on two internal 2.5" SSDs for fail-safe operation.



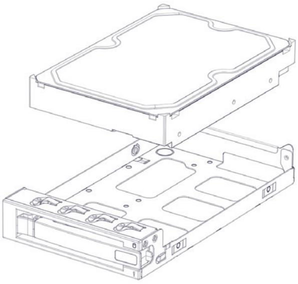
14 | MECHANICAL DRAWINGS

14.1 Hard Drive Assembly into the Tray

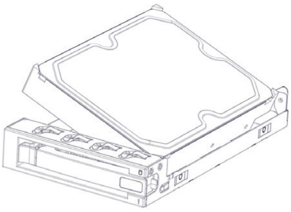
1.



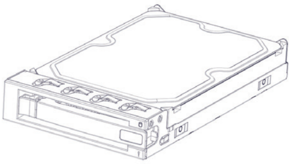
2.



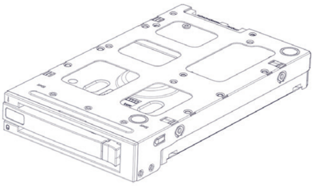
3.



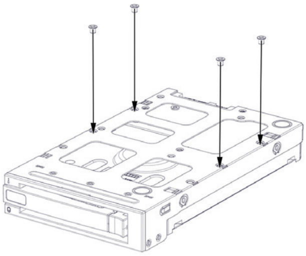
4.



5.



6.



15 | 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
- P/N: SNCX40KH-32G-80T = 80TB

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

Model: SecureNAS® CX-80KHD-X

- P/N: SNCX80KH-32G-32T = 32TB
- P/N: SNCX80KH-32G-64T = 64TB
- P/N: SNCX80KH-32G-80T = 80TB
- P/N: SNCX80KH-32G-96T = 96TB
- P/N: SNCX80KH-32G-128T = 128TB
- P/N: SNCX80KH-32G-144T = 144TB
- P/N: SNCX80KH-32G-160T = 160TB

Model: SecureNAS® CX-80KSD-X

- P/N: SNCX-80KSX-32G-8T = 8TB
- P/N: SNCX-80KSX-32G-15T = 15TB
- P/N: SNCX-80KSX-32G-30T = 30TB
- P/N: SNCX-80KSX-32G-60T = 60TB
- P/N: SNCX-80KSX-32G-120T = 120TB

Model: SecureNAS® CX-120KHSD-X

- P/N: SNCX120K-32G-150T = 150TB
- P/N: SNCX120K-32G-159T = 159TB
- P/N: SNCX120K-32G-174T = 174TB

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

INDEX

CIPHERTEX®
data security

FIPS Level 3 Certified 140-2

AES ENCRYPTION 256

TAA COMPLIANT

ANAB ACCREDITED ISO/IEC 17021

GSA Contract Holder
Contract GS-35F-487DA

PROUDLY MADE IN THE USA

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.

V1.11.23

Ciphertex Data Security | 9301 Jordan Avenue, #105A | Chatsworth, CA 91311 **USA** 877.977.8878 | 818.773.8989

www.ciphertex.com