



# **Coronado Personal NAS Gateway**

## **Quick Start User Guide**

## Table of Contents

<b>Chapter 1: Theory of Operation.....</b>	<b>7</b>
<b>Chapter 2: Basic Installations.....</b>	<b>8</b>
2.1 Coronado Personal NAS Gateway Prerequisites .....	9
2.2 Installing the Virtual Machine .....	9
2.3 Coronado Personal NAS Gateway Disk Requirements.....	10
2.4 Turning on the Coronado Personal NAS Gateway for the first time .....	10
2.5 Configuring the Network.....	11
2.6 Configuring and Mounting a Cloud Bucket .....	15
<b>Chapter 3: Network Configuration.....</b>	<b>19</b>
3.1 Modify Network Configuration. ....	19
3.2 Test the Network Configuration .....	20
<b>Chapter 5: Changing the Password .....</b>	<b>21</b>
5.1 Changing the default password.....	21
<b>Chapter 6: Reboot/Shutdown/Upgrade.....</b>	<b>22</b>
6.1 Reboot, Shutdown or Upgrade the system.....	22
<b>Chapter 7: Connecting to the Gateway.....</b>	<b>23</b>
7.1 Connect over ssh .....	23
7.2 Connect over NFS .....	23
7.3 Connect over Windows .....	23

# SOFTWARE LICENSE AGREEMENT

**READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT (this "Agreement") CAREFULLY BEFORE USING THIS PRODUCT (the "Product"). THE PRODUCT IS COPYRIGHTED. THE SOFTWARE (AS DEFINED BELOW) IS LICENSED, NOT SOLD. BY USING THIS PRODUCT, YOU ARE ACCEPTING AND AGREEING TO THE TERMS OF THIS AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, YOU SHOULD IMMEDIATELY RETURN THIS PACKAGE WITH THE PRODUCT UNOPENED AND YOU WILL RECEIVE A REFUND.**

1. **License Grant.** BridgeSTOR, LLC ("Licensor") grants to you, and you accept, a non-exclusive license to use the software contained in the Product in machine-readable, object code form only (the "Software") as permitted by this Agreement. The Software may be used only in connection with the Product. You may not assign, sublicense or transfer any of your rights under this Agreement.
2. **Ownership.** You acknowledge Licensor has and will retain exclusive ownership of all proprietary rights to the Software, including all United States and international intellectual property and other rights such as patents, trademarks, and copyrights. You will have no interest in the Software except the right to use it as expressly set forth in this Agreement. You will (a) comply with all copyright, trademark, trade secret, patent, contract or other laws necessary to protect all of Licensor's rights in the Software and (b) not to challenge Licensor's ownership of (or the validity or enforceability of its rights in and to) the Software.
3. **License Fees.** The license fees paid by you are in consideration of the licenses granted under this Agreement.
4. **Term.** This Agreement is effective upon your opening this package and will continue until terminated. You may terminate this Agreement at any time by returning the Product to Licensor. Licensor may terminate this Agreement upon the breach by you of any term of this Agreement. Upon such termination by Licensor, you agree to return the Software and all user documentation to Licensor.
5. **Limited Warranty.** Licensor warrants, for your benefit alone, for a period of 90 days from the date of the commencement of this Agreement (the "Warranty Period") that the Software is free from defects in material and workmanship and that the Product will operate in substantial conformance with the functional specifications described in the user's manual. If a defect in the Software or Product occurs during the Warranty Period, you may return it to Licensor for replacement. This is your sole and exclusive remedy for any breach of representation or warranty by Licensor. EXCEPT FOR THE LIMITED WARRANTY SET FORTH ABOVE, THE PROGRAM AND THE SOFTWARE ARE LICENSED "AS IS" AND LICENSOR DISCLAIMS ANY AND ALL OTHER WARRANTIES, INCLUDING WITHOUT LIMITATION ANY EXPRESS, IMPLIED, OR STATUTORY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR GENERAL OR SPECIFIC USE.
6. **Limitation of Liability.** Licensor's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, actions, or causes of action arising from or relating to this Agreement will not exceed the license fee paid to Licensor for the use of the Software. In no event will Licensor be liable for any indirect, incidental, consequential, special, or exemplary damages or lost profits, even if Licensor has been advised of the possibility of such damages.
7. **Governing Law.** This Agreement will be governed under the laws of the State of Nevada, without regard to conflicts of law principles.
8. **Miscellaneous.** This Agreement contains the entire understanding of the parties with respect to the Software and supersedes any prior oral or proposals, representations, or understandings with respect to such subject matter and may not be modified or superseded, nor may any of its terms or conditions be waived, unless expressly agreed to by the parties in writing. Each provision of this Agreement will be valid and enforceable to the fullest extent permitted by law. If any provision of this Agreement or the application of the provision to any person or circumstance will, to any extent, be invalid or unenforceable, the remainder of this Agreement, or the application of the provision to persons or circumstances other than those as to which it is held invalid or unenforceable, will not be affected by such invalidity or unenforceability, unless the provision or its application is essential to this Agreement. You acknowledge that in the event of a breach of this Agreement, Licensor may suffer irreparable harm and will be entitled to injunctive relief as well as monetary remedies available at law or in equity. The failure of any party to require full performance of any provision of this Agreement will in no way affect the right of such party to enforce such rights at a later time. Headings are for reference purposes only.

# Preface

Welcome to the Coronado Personal NAS Gateway User Guide. This document provides a comprehensive discussion of the theory of operation, installation, configuration and usage of the Coronado Personal NAS Gateway and is intended for users who will install, operate and maintain the software.

## Prerequisites

Before proceeding, you should have a general understanding of the following:

- General networking concepts
- Minimal Linux command line knowledge
- Virtual Machine Management
- Cloud Storage Bucket, Policy and User Management

BridgeSTOR has created a Global File System that transfers files to 3<sup>rd</sup> party Cloud Storage for object access and availability anywhere in the world. To facilitate the Global File System, BridgeSTOR has developed its own Linux file system called CSFS (Cloud Storage File System). CSFS converts files to objects while transferring the new object to Cloud Storage. One of CSFS's unique capabilities is the ability to store files in Cloud Storage in a "Native Object" format. The "Native Object" format allows local files and Cloud Objects to have a 1 to 1 relationship allowing the local file and the Cloud Objects to be 100% identical. The "Native Object" is 100% compatible with other 3<sup>rd</sup> party tools and keeps the 5TB limit for a file.

One of the major issues of Cloud Storage is "*how to reduce latency*". Latency is measured by the amount of time it takes for the data to move from the local site to the Cloud. For example, San Diego to AWS in Oregon will be a minimum of 40 milliseconds. Latency is the Storage Administrators worst nightmare when sending data over the wire. The Coronado Personal NAS Gateway cannot remove the latency, but it can help hide the latency from the End User. Like an HTML proxy cache, HTTP S3 requests are sent into the local disk cache where the PUT data is written immediately to disk and a transaction is kept locally in the gateway. The Coronado Personal NAS Gateway has multiple background threads that will re-play the transaction file sending the data directly to the Cloud Storage. Using S3 Multipart upload API, each background thread also spawns multiple threads which sends the data into the cloud in a fast and efficient manner. When reading a file all data will be placed back into the local disk cache before returning the data to the application.

- DO:** Configure Networking using the Linux command line Interface nmtui.
- DO:** Use the BridgeSTOR GUI to configure the Coronado Personal NAS gateway host name.
- DO:** Before Installing, Create Cloud Storage Bucket(s) or Blob(s).
- DO:** Assign Policies and generate authentication keys.
- DO:** Feel free to download your data from the Native Bucket with any S3 tool.
- DO:** Change the default root and admin passwords of your Coronado Personal NAS Gateway before using the product.

## Document Organization

[Chapter 1, "Theory of Operation"](#) provides an overview of the Coronado Personal NAS Gateway and how it fits into an overall Global File System.

[Chapter 2, "Basic Installation"](#) explains how to install the Coronado Personal NAS Gateway using an ISO and how to use the BridgeSTOR GUI to configure basic networking.

[Chapter 3, "Network Configuration"](#) describes how to modify the Coronado Personal NAS Gateway networking after installation.

[Chapter 4, "Changing the Password"](#) explains how to change the default Brooklyn NAS Edge Cache GUI password.

[Chapter 5, "Reboot and Shutdown"](#) explains how to properly reboot or shutdown the Brooklyn NAS Edge Cache software.

Note on usage of upper case and typefaces:

- In addition to its normal use, upper case is used for the first letter of words that refer to specific Coronado Personal NAS Gateway elements; that is, words that have a special meaning, to distinguish them from common usage of the same terms.
- *Italics* is used in the text to distinguish a word or words from surrounding text, such as what the user needs to type into a data entry screen.
- **Bold** typeface is used for emphasis.

## **Customer Support**

The BridgeSTOR support is online only and available 9-5 PST. If you have paid for support a response will be returned with in 4 hours. Please submit a new case in the BridgeSTOR Website at [www.bridgestor.com](http://www.bridgestor.com).

## **Web Site**

For general information about BridgeSTOR and BridgeSTOR products and for all contact information refer to: [www.bridgestor.com](http://www.bridgestor.com)

## **Copyright Notice**

Coronado Gateway, Sydney Ransomware Gateway, Brooklyn NAS Edge Cache are trademarks of BridgeSTOR. Other names used in this document are the property of their respective owners.



# Chapter 1: Theory of Operation

BridgeSTOR has created a Global File System that allow corporations to store files and objects in 3<sup>rd</sup> party Cloud Storage locations while allowing all local corporate locations to securely view and access the file data. BridgeSTOR relies on the defacto standard S3 REST (Representational State Transfer) protocol developed by Amazon as the storage protocol to transfer data between locations.

There are multiple choices for 3<sup>rd</sup> Party Cloud Storage such as Amazon, Microsoft, Wasabi, RSTOR, Seagate and Backblaze. BridgeSTOR also supports local Object storage sold by Cloudian, IBM, Netapp, EMC and other vendors.

The Coronado NAS Gateways exports out industry standard protocols such as SMB or NFS allowing for the easy and fast transport of files into the Cloud. The Brooklyn NAS Edge Cache sits between the Coronado Gateway and the Cloud Storage creating a “*bump in the wire*” storing the most accessed data on a local disk and recording each transaction while backend threads replay the transactions and move the data into the cloud. These functions allow files to appear to be stored local, but they are really stored as objects in the Cloud Storage. All Brooklyn NAS Edge Caches have been designed to run on physical hardware or virtual machines (VM) running in VMware, Microsoft Hyper-V, Oracle Virtual Box or Linux KVM environments.

## Installing the Coronado Personal NAS Gateway

The Coronado Personal NAS Gateway is installed in two phases. The first phase requires Linux command line access. The gateway requires a static network address and this is installed with the Linux nmtui command. Once the system is up and running, the BridgeSTOR GUI may be used to setup additional Networking and defining Bucket Credentials. Once networking has been installed, ssh may also be used for remote management.

## Integration with Microsoft Active Directory

The Coronado Personal NAS Gateway does not support Active Directory.

# Chapter 2: Basic Installations

For security reasons BridgeSTOR will never create buckets in the Cloud Storage. Before installing have your Cloud Administrators create your bucket, set bucket policies and create your Access Key and Secret Key. Please review your Cloud Storage documentation on how to perform these tasks.

The sections of this chapter are organized as follows:

**Section 2.1** Coronado Personal NAS Gateway Prerequisites

**Section 2.2** Installing from a Virtual Machine

**Section 2.3** Coronado Personal NAS Gateway Disk Requirements

**Section 2.4** Turning on the Coronado Personal NAS Gateway for the first time

**Section 2.5** Configuring the Network

**Section 2.6** Configuring and Mounting a Cloud Bucket



## 2.1 Coronado Personal NAS Gateway Prerequisites

The Coronado Personal NAS Gateway supported as a virtual machine. Virtual machines may be deployed in VMware, Microsoft Hyper-V, Oracle Virtual Box or Linux KVM environments. All Coronado Gateway configurations allow integration with Microsoft Active Directory. The following are required to successfully set up the Coronado Personal NAS Gateway:

1. Network Connective to the Coronado Personal NAS Gateway.
2. Static IP Address and Internet Gateway Address.
3. An Active Bucket in the Cloud or Object Storage.
4. Valid Access Key and Secret Key for the Bucket.

## 2.2 Installing the Virtual Machine

The Coronado Personal NAS Gateway ships as a CentOS 7 image inside an OVA. Most hypervisor environments should easily recognize this format and easily import the image. If it does not, you may do the following:

- 1) An OVA image is nothing more than a compressed OVF image. Use the tar command below to decompress the image.

```
tar -xvf Personal.ova
```

- 2) Once uncompressed, you will see the following virtual disk files.

```
personal-disk1.vmdk  
personal-disk2.vmdk  
personal-file1.nvram  
personal.mf  
personal.ovf
```

- 3) Use these files to install as an OVF for your hypervisor.
- 4) If your hypervisor still not cannot install with the OVF, then you will have to create the virtual machine manually. Use coronado-disk1.vmdk as your boot disk

At this point, both images should be ready to be booted.

## 2.3 Coronado Personal NAS Gateway Disk Requirements

The Coronado Personal NAS Gateway ships with two virtual disks. One for the Operating System and the other for an ingest cache. The operating system disk is 128GB and BridgeSTOR recommends this disk be configured on SSD or flash. The ingest disk is 1 TB and is used when NFS or SMB protocols write data to and from the Gateway. Files are written to the ingest cache on input and flushed out of the cache once the data has been sent to the Cloud Storage or a Brooklyn NAS Edge Cache. BridgeSTOR recommends the ingest drive should be an SSD or flash and be larger than the maximum data sent to the Gateway at any time. If the drive is too small, users will receive disk full errors.

## 2.4 Turning on the Coronado Personal NAS Gateway for the first time

The Coronado Personal NAS Gateway ships as a CentOS 7 image and may be managed by a web-based GUI. Once your machine is turned on, you will be presented a Centos 7 login screen.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.el7.x86_64 on an x86_64

edge login: _
```

The Coronado Personal NAS Gateway ships with two internal users; one user for the Centos 7 system called “root”, and another for BridgeSTOR administration called “admin”. Refer to the table below for usernames, passwords and descriptions.

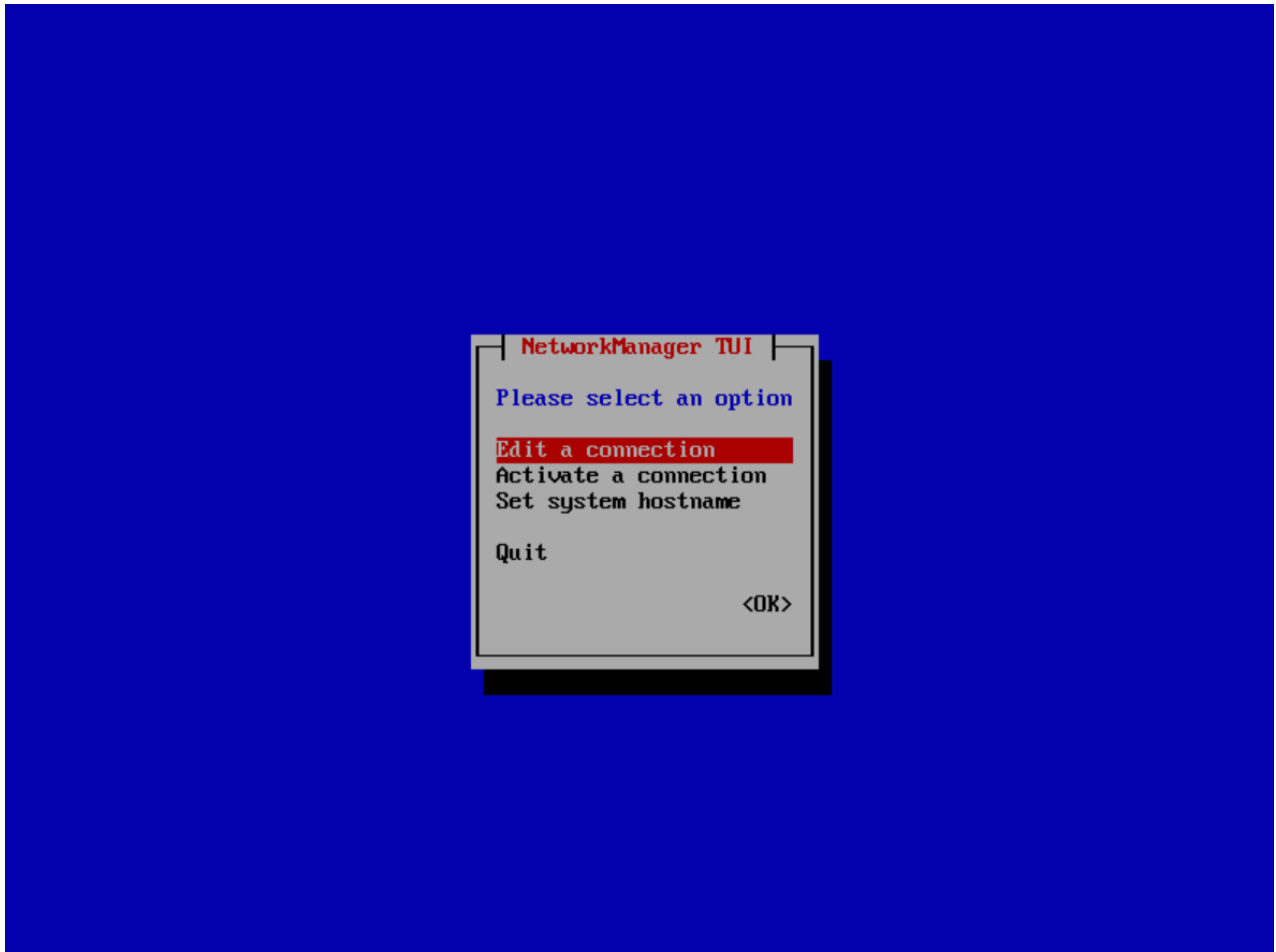
<b>Username</b>	<b>Password</b>	<b>Description</b>
root	Bstor1234	Super user login access for setting networking and general management tasks
admin	Bstor1234	Web based credentials for BridgeSTOR configuration and as a default login for SMB or NFS

## 2.5 Configuring the Network

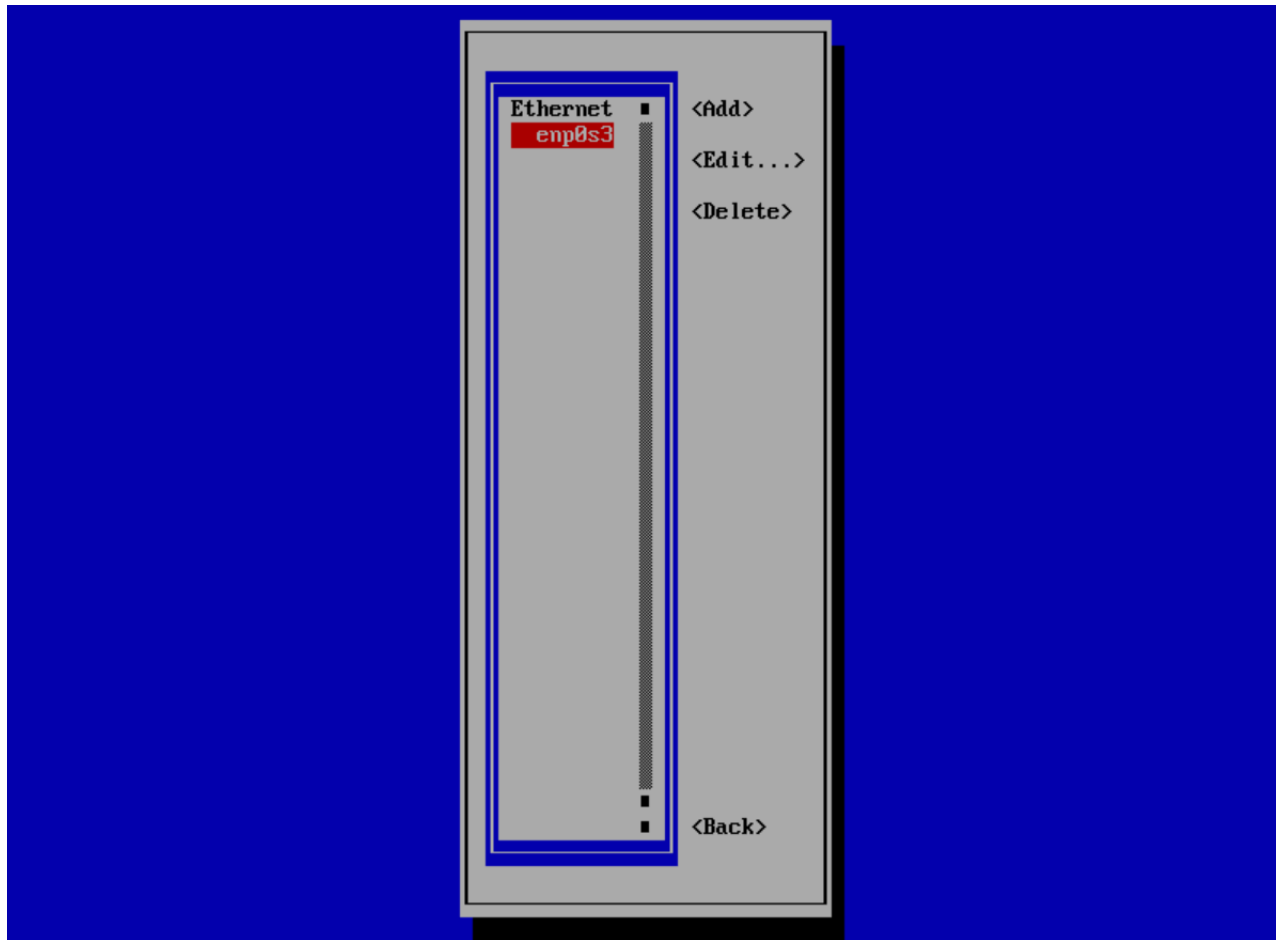
Login to the system as root using the password above and then execute the following command.

**nmtui**

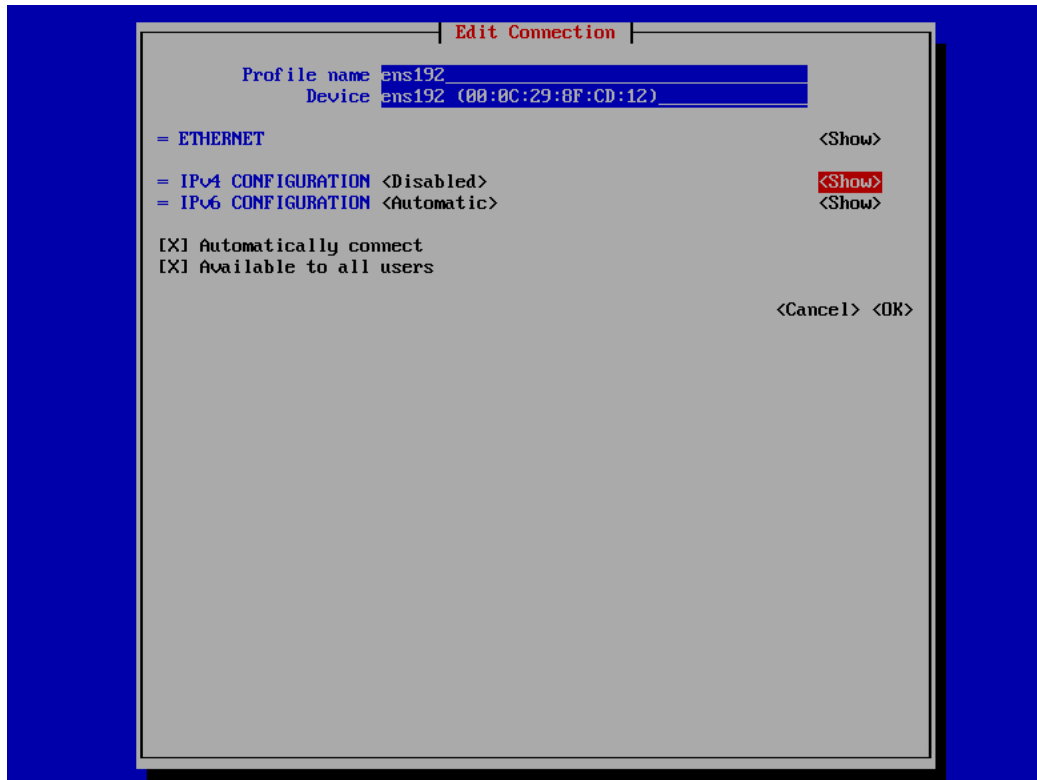
The following screen should appear.



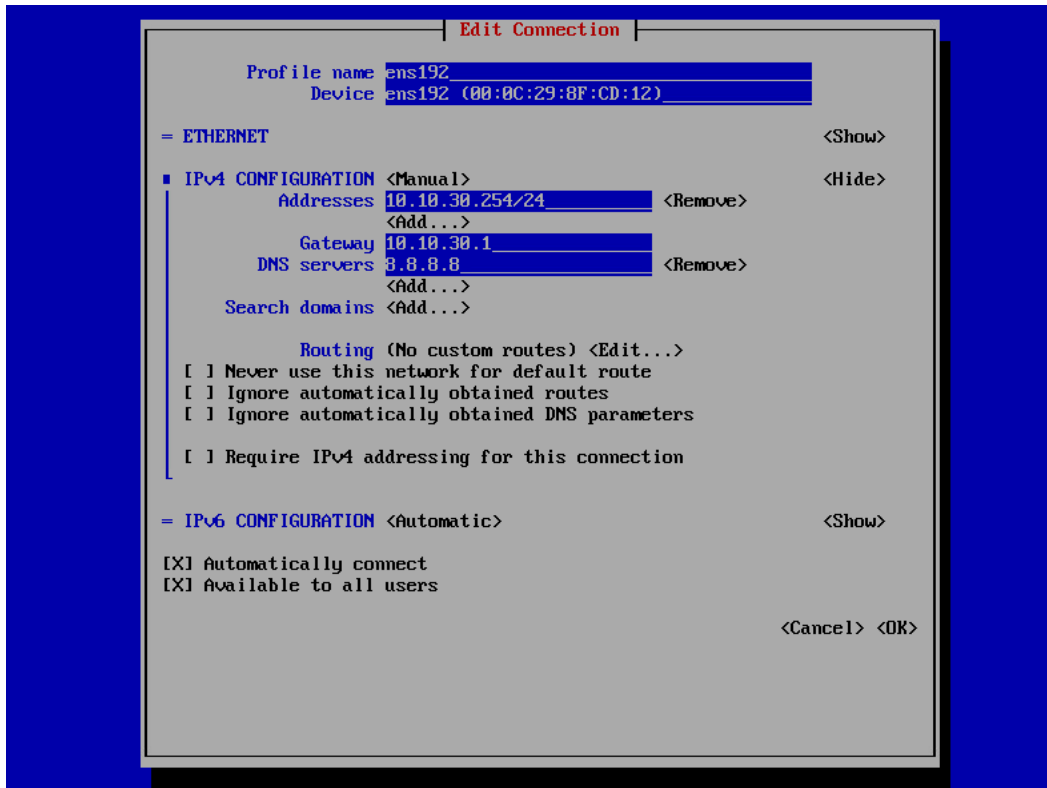
Select "Edit a connection" and press return. This will allow you to modify the network addresses of the network connection. The following screen will appear.



The ethernet name is highlight in red. Your name may be different depending on the system. Use the tab key to move to the "Edit" button. The current selection will always be in red. Press the Return key and the following screen should open.



Use the tab key again to move to <show> next to "IPv4 CONFIGURATION <Disabled>". Press the enter key to enter you network configuration. Below is an example of a completed entry for the screen.



First, change the field next to "IPV4 CONFIGURATION" from Disabled to Manual. This will turn on the network port. Next change the "Addresses" field, in this example we gave the address of 10.10.30.254 with a netmask of 255.255.255.0. The netmask is configured by the /24 or the CIDR. If you are not using 255.255.255.0 then replace the /24 with /xx for your correct CIDR. Finally change your network Gateway and DNS Servers. If you will be configuring Active Directory the first DNS entry must be the Active Directory DNS server. The second may be any DNS server that you prefer. Once everything is selected tab to the <OK> button and hit return.

You will return the previous menu. Use the tab key and select the <back> button and press return. This will bring you back to the first screen of nmtui. Use the tab key to select "Edit a connection". Then use the down arrow to select "Quit". This will exit you from the program.

At this point, reboot the system and login. Use ping or any other network tool to verify that you network connection is valid. Please do not continue with 2.8 until you have a valid network connection.

## 2.6 Configuring and Mounting a Cloud Bucket

At this point, the server or virtual machine has been configured. The remaining install portion of the installation may be done with the BridgeSTOR GUI. The system will be installing SSL Certificates in the background. This can take up to 20 minutes. You may review the status by logging into the system and running the following command.

`systemctl status bstor_gui`

```
root@edge bstorl# systemctl status bstor_gui
■ bstor_gui.service - BridgeSTOR GUI
   Loaded: loaded (/etc/systemd/system/bstor_gui.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2021-06-03 22:15:23 UTC; 7min ago
 Main PID: 1033 (start.sh)
    CGroup: /system.slice/bstor_gui.service
            └─1033 /bin/bash /etc/bstor/gui/start.sh
              └─8586 sleep 10

Jun 03 22:15:23 edge systemd[1]: Started BridgeSTOR GUI.
Jun 03 22:15:33 edge bash[1033]: waiting on diffie helman pem
Jun 03 22:15:43 edge bash[1033]: waiting on diffie helman pem
Jun 03 22:15:53 edge bash[1033]: waiting on diffie helman pem
Jun 03 22:16:03 edge bash[1033]: waiting on diffie helman pem
Jun 03 22:21:14 edge bash[1033]: waiting on diffie helman pem
root@edge bstorl#
```

The line “waiting on Diffie helman pem” will occur. When this changes to “Start bstor\_gui”, the process has completed, and you may enter the GUI.

Use your favorite browser and enter in your IP Address for the Brooklyn NAS Edge Cache. The system uses a self-signed certificate so you may see a warning about entering the site. Just acknowledge the certificate and continue to the site. You will be prompted with a login screen.



Please enter the Brooklyn system password

Password:

login

Enter the default password “Bstor1234”. This will allow you to enter into the system. Once logged in, you should see the following screen.



Version:2.0.1.7		Cloud Share Credentials			Mon Oct 04,2021 9:24 PM
Cloud Share Credentials	Network Configuration	Change Password	Reboot/Shutdown/Upgrade	Logout	

Select	Mount Point	Bucket Name	Access Key	Mounted
<input type="radio"/>	/C00			no

Notice on the mount point screen. You are allowed one Cloud mount points, with the Bucket Name, Access Key and Secret Key.

### a) Configure your Bucket Parameters

Click on the radio button for Mount Point /c00 and select "edit credentials". The "edit credentials" screen allows you to define your cloud bucket. The following screen should be displayed.

Version:2.0.1.7		Credentials for Cloud Share 0			Mon Oct 04,2021 9:26 PM
Cloud Share Credentials	Network Configuration	Change Password	Reboot/Shutdown/Upgrade	Logout	

**Bucket Settings**

Bucket Name:   
 Bucket Endpoint:  Use SSL: ☒  
 Access Key:   
 Secret Key:   
 Destination Address:  Start:  End:   
 NFS Enabled: ☐  
 SMB Enabled: ☐

### b) Install Your Bucket Credentials

To complete a proper bucket installation, each bucket requires 5 items.

- 1) **Bucket Name.** This is the bucket name of your Cloud or Object Storage. This bucket name must exist in your Cloud or Object Storage. For security purposes, BridgeSTOR will not create this bucket.
- 2) **Bucket Endpoint.** This is the URL address of the bucket location. For example.

*s3.amazonaws.com* points to Amazon east coast.

If you are using a region other than Amazon east coast enter the region of the bucket in the URL. For example,

*s3-us-west-2.amazon.aws.com* is the Oregon region.

For other providers, use their URL defined in their documentation. After defining the URL, please select if you would like to use https:// by selected the "Use SSL" box. If this is not clicked, the system will use the http protocol.

- 3) **Access Key.** Enter the Access Key for the bucket defined in your Cloud Storage for Microsoft, enter the "Storage Account" name.
- 4) **Secret Key.** Enter the Secret Key assigned to the bucket. For Microsoft enter the Access key assigned to the storage account.
- 5) **Destination Address.** This is the URL or IP Address of the bucket. Most of the time it will be the same address as #2 above. For Object Storage, it will be a local address of the Object Storage head. A port range is also available for use. If supported by an Object Storage system, the BridgeSTOR system will use a Round Robin approach to multiple Storage Nodes for redundancy and performance.
- 6) **NFS Enabled.** Allow NFS connectivity to this bucket. After the system has been mounted, users may mount an NFS mountpoint to the bucket.
- 7) **SMB Enabled.** Allow SMB connectivity to this bucket. After the system has been mounted, users may map a drive letter to this bucket.

Once all the data has been entered, press the "apply" button. This will not only save the data to the system but will verify if the data entered is correct with the Cloud or Object Storage bucket. If an error occurs, please check your input and try again.

### **c) Mounting the Bucket**

Before the bucket may be accessed, it must be mounted by the system. Return to the main menu of the system. Click the radio button of the /c00 Mount Point and then press the “mount” button.

# Chapter 3: Network Configuration

The Brooklyn NAS Edge Cache requires proper networking to operate. After installation if you need to change the network configuration the BridgeSTOR GUI allows modification to the IP Address information.

## 3.1 Modify Network Configuration.

At this point all networking should be functional. Login to the Brooklyn NAS Edge Cache with your web browser by entering the IP address. Select the "Network Configuration" from the main menu. The following screen will appear:

BridgeSTOR  
We Make Cloud Storage Accessible

Coronado Personal Edition NAS Cloud Gateway

Help

Version:2.0.1.7

Network Configuration

Change Password

Reboot/Shutdown/Upgrade

Logout

Mon Oct 04, 2021 9:27 PM

Cloud Share Credentials

Network Configuration

Change Password

Reboot/Shutdown/Upgrade

Logout

IP Address Settings

Host Name:

IP Address:

Netmask:

Gateway Address:

Domain DNS IP Address:

Secondary DNS IP Address:

apply

Ping Test

Ping IP Address:

apply


1. **Editing the IP Address Settings.** These series of input allow the IP Settings to be modified. Once the edits have been completed, press enter to update the system. If you want to cancel at any time press another option from the main menu and the information will not be saved.
  - a) **Host Name.** Enter the host name of the system. The Host Name should be a unique name for the Brooklyn NAS Edge Cache.
  - b) **IP Address.** This field sets the static IP Address of the Brooklyn NAS Edge Cache.
  - c) **Netmask.** Enter the netmask for the IP Address. The name may be up to 8 characters and may not contain spaces. If mirrored pairs are not required, this field may be left blank.

- d) **Gateway Address.** The Internet Gateway IP address.
- e) **Domain DNS Address.** The address to locate domain names. If Active Directory is required, then this first address must point to the Active Directory DNS server.
- f) **Secondary DNS Address.** This field allows a failover DNS address in case the first address fails.

Press "apply" and the system will save the parameters and return to the Brooklyn NAS Edge Cache Menu.

## 3.2 Test the Network Configuration

This screen includes a "Ping Test" screen which allows you to test the network. Type a Network Address in the "Ping IP Address" field and press "enter". This will attempt to contact the server entered.



Coronado Personal Edition NAS Cloud Gateway

Help

<jmatze@bridgestor.com> Sent: Monday, October...

Version: 2.0.1.7	Ping Results				Mon Oct 04, 2021 9:28 PM
Cloud Share Credentials	Network Configuration	Change Password	Reboot/Shutdown/Upgrade	Logout	

```

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
 64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=16.8 ms
 64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=15.0 ms

--- 8.8.8.8 ping statistics ---
 2 packets transmitted, 2 received, 0% packet loss, time 1001ms
 rtt min/avg/max/mdev = 15.060/15.937/16.814/0.877 ms

```

[Continue](#)

# Chapter 5: Changing the Password

The BridgeSTOR GUI allows you to change the admin GUI password. This is original set to “admin” from the default install.

## 5.1 Changing the default password.

Select “Change Password” from the main menu. The following menu will appear.

BridgeSTOR  
We Make Cloud Storage Accessible

Coronado Personal Edition NAS Cloud Gateway

Help

Version:2.0.1.7

Change Coronado Personal Edition Password

Mon Oct 04, 2021 9:29 PM

Cloud Share Credentials

Network Configuration

Change Password

Reboot/Shutdown/Upgrade

Logout

Old Password:

New Password:

Retype New Password:

apply

- a) **Old Password.** Enter the current password for the system.
- b) **New Password.** Enter a new password.
- c) **Retype New Password.** Re-enter the password to confirm accuracy.

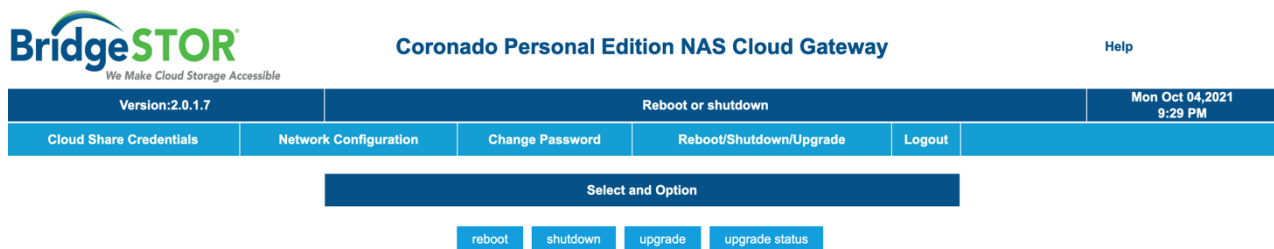
After entering these fields, press “apply” and the system will take a few seconds before giving you a response.

# Chapter 6: Reboot/Shutdown/Upgrade

The BridgeSTOR GUI allows you to reboot or shutdown the system.

## 6.1 Reboot, Shutdown or Upgrade the system.

Select "Reboot/Shutdown" from the main menu. The following menu will appear.



- Reboot.** Click "reboot" to reboot the system.
- Shutdown.** Click "Shutdown" to shut down the system.
- Upgrade.** Click "upgrade" to upgrade the system. Wait a few minutes and then press the "upgrade status" button and it will show if the upgrade has been completed.

The system will take a few seconds before giving you a responding.



# Chapter 7: Connecting to the Gateway

The BridgeSTOR Gateway allows users to connect over NFS, SSH or Windows. The gateway defaults with a user called admin, unless Active Directory is used, use admin and the default password.

## 7.1 Connect over ssh

Use whatever ssh tool that you prefer. Simply supply the BridgeSTOR Gateway address to your ssh program and use the "root" login name with the "Bstor1234" password to connect. Please change the "root" password once logged into the system.

## 7.2 Connect over NFS

The BridgeSTOR Gateway supports both NFS 3 and NFS 4. From your NFS machine, use your normal nfs mount command and create a mount point to the NFS gateway. The mountpoint will be based on the bucket that you have mounted. From the main GUI screen, you will see /c00, /c01, /c02, /c03 next to your bucket. This is the nfs mount point. For example, the first bucket would use /c00 and mount to the BridgeSTOR Gateway as:

```
mount -t nfs 10.10.30.254:/c00 /mnt/nfs
```

## 7.3 Connect over Windows

The BridgeSTOR Gateway supports Windows connective using the Samba protocol allowing Windows users to connect to the BridgeSTOR Gateway over a standard windows share. Users may login with either the BridgeSTOR Gateway "admin" user or if the BridgeSTOR Gateway has connected with Active Directory an active directory user.

Map a network drive the BridgeSTOR Gateway. For example: From File Explorer, right click on the "This PC" and use the "Map network drive" and to login into the Gateway. Select the drive letter and enter the share name. The share name is the BridgeSTOR Gateway address followed by the share name. The Windows share name is based on the bucket from the main GUI screen. You will see /c00 /c01 /c02 or /c03 next to your bucket. The name of the first bucket is /c00 so the share name would be \\10.10.30.254\c00. Select "Connect using a different credential" and then press Finish and you will be prompted to enter the username and password. Enter the username and password and press "OK". If correct, the drive will show up in File Explorer.

