



# SYMPLYNEBULA

USER GUIDE v.1.0.0

# CONTENTS

<b>Introduction</b>	<b>3</b>
Network Connectivity	3
Accounts and Roles	4
Setup Overview	4
<b>Sign-in</b>	<b>5</b>
My Account	7
<b>Bucket creation</b>	<b>8</b>
<b>Bucket deletion</b>	<b>10</b>
Super bucket deletion	11
<b>Policy creation</b>	<b>12</b>
<b>User creation</b>	<b>14</b>
<b>Generate keys</b>	<b>15</b>
Generate Keys for another user	15
Generate Keys for your account	16
<b>Assign Policies to Users</b>	<b>18</b>
Grant permissions	18
<b>New user setup</b>	<b>19</b>
<b>Test bucket access</b>	<b>22</b>
Application configuration	22

# INTRODUCTION

Welcome to SymplyNEBULA! This is a Quick Start Guide to get you up and running with Symply's cloud storage offering.

SymplyNEBULA is a cloud-based object storage service using the Simple Storage Service (S3) data model backed with public and hybrid infrastructures. SymplyNEBULA allows customers to store data across single or multiple geographical locations and can be used to distribute data as needed to the nearest endpoint to their desired delivery location.

An S3 bucket is a public cloud storage resource containing objects. Object storage data models use a flat data structure where there is no hierarchy of folders and subfolders, all objects are stored at the root of the bucket. Objects are identified by a combination of its bucket, full-name (a.k.a. object ID) and optional associated metadata.

*This guide assumes some familiarity with other AWS S3 compatible storage.*

## NETWORK CONNECTIVITY

SymplyNEBULA's S3 compatible object storage is accessible only over HTTPS (port 443). SymplyNEBULA can be used either Interactively or Programmatically.

### INTERACTIVELY

- Through the web UI used for admin console management and simplified data access and can be accessed through your custom URL: <https://symplynebula.com/signin?c=<accountname>>
- Using 3rd-party S3 compatible graphical and command line driven clients
  - e.g. awscli, CyberDuck, MountainDuck, Transmit, Archiware P5, etc...

### PROGRAMMATICALLY

- Through API calls using S3 compatible SDKs or libraries using Endpoint, Access key and Secret key credentials

## ENDPOINT ACCESS

Buckets are accessible through DNS-style or Virtual Host endpoint conventions, as well as via the web UI.

- DNS-style: [https://\\$bucketname.s3.symplynebula.com/\\$path/](https://$bucketname.s3.symplynebula.com/$path/)
- Virtual Host: [https://s3.symplynebula.com/\\$bucketname/\\$path](https://s3.symplynebula.com/$bucketname/$path)
- Native web UI: <https://symplynebula.com/signin>

### EXAMPLES

- bucketname = `myarchivedfiles`
- path = `/2022/02/08/nightly`

### DNS-STYLE

- <https://myarchivedfiles.s3.symplynebula.com/2022/02/08/nightly/>

### VIRTUAL HOST

- <https://s3.symplynebula.com/myarchivedfiles/2022/02/08/nightly/>

## ACCOUNTS AND ROLES

SymplyNEBULA has three (3) distinct roles for storage access:

### ROOT

- Initial account and main identity of the account.
- Can manage all aspects of the account.
- May generate key pairs for access.

*NOTE: The Root account cannot be deleted.*

### ADMIN

- Can manage all aspects of the account (bar the Root account).

### USER

- Can perform operations on Buckets (within the privileges set on those buckets by an Admin or Root user). Can change the User account's password, generate key pairs for access.

## SETUP OVERVIEW

A summary of the setup process is as follows:

- Sign-in
- Bucket creation
- Policy creation
- User creation
- Generate keys
- Assign Policies to Users
- New user setup
- Test bucket access

Already experienced with AWS S3 storage? Here's the very short version... If you are going to use root access with no additional users:

- Use the web GUI to generate a key set
- Create a bucket
- Configure your app with:
  - the end-point (<https://s3.symplynebula.com>)
  - your bucket name
  - the keys you generated
- Go!

*NOTE:*

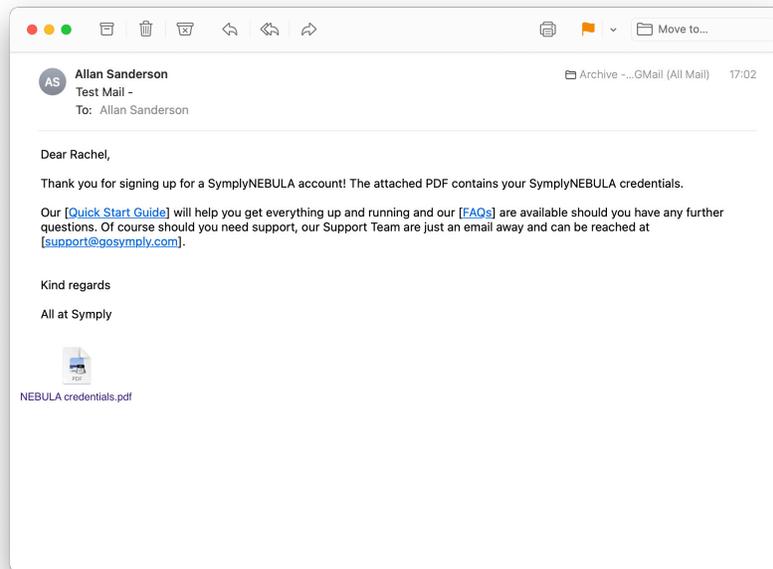
- *SymplyNEBULA does not use the concept of regions in the endpoint.*
- *We only support access on port 443, using TLS 1.2 or later.*

# SIGN-IN

When you sign up for a SymplyNEBULA account you will receive a Welcome email sent to the address provided to us with the details necessary to allow you to sign-in to your SymplyNEBULA management console and get started building your S3 storage.

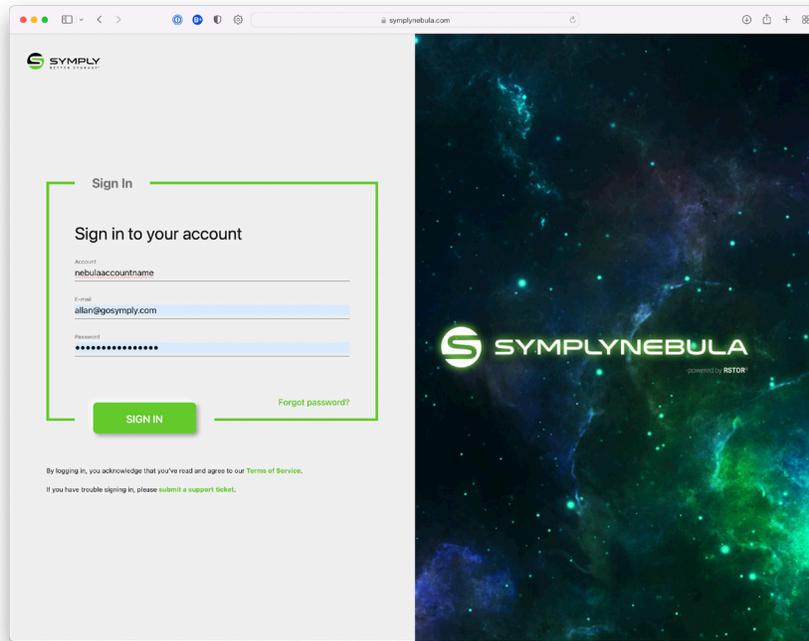
Those details are:

- Account: [nebulaaccountname](#)
- Admin Email: [signup@yourdomain.com](#)
- Admin Password: **\*\*\*\*\***
- URL: <https://symplynebula.com/signin?c=nebulaaccountname>



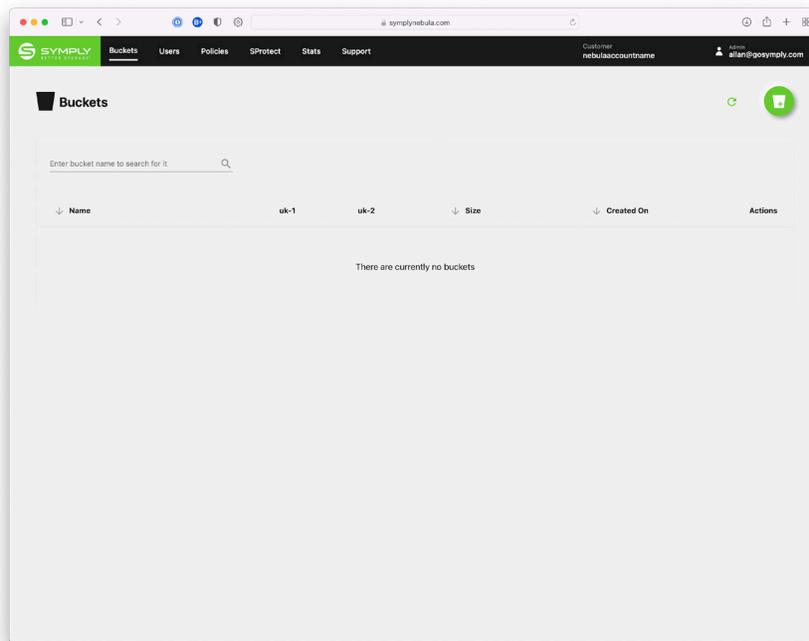
*Signup email (example)*

To sign-in for the first time click the link to the NEBULA URL.



*SymplyNEBULA sign-in page*

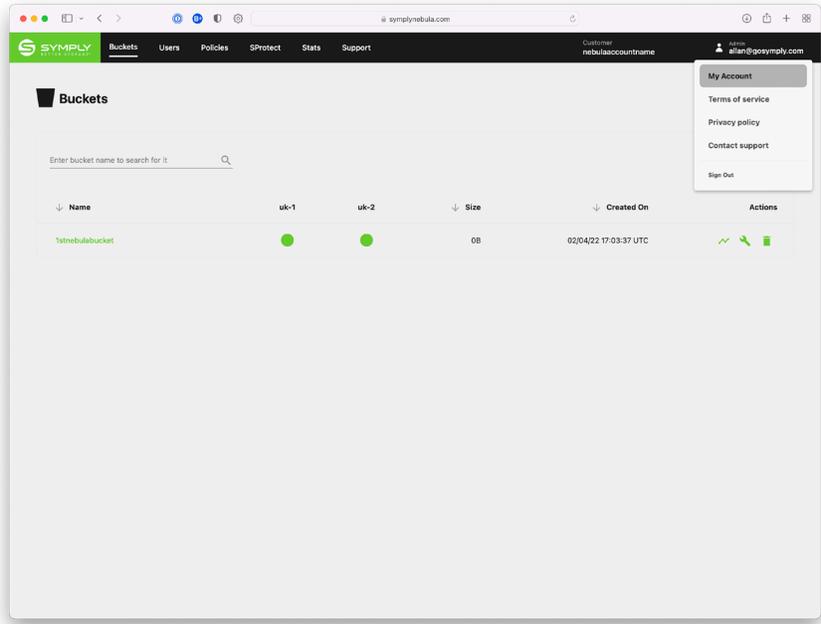
Enter your NEBULA Admin Email and NEBULA Admin Password then click SIGN IN. (The Account field should be populated with the custom URL).



*Admin console | Buckets tab*

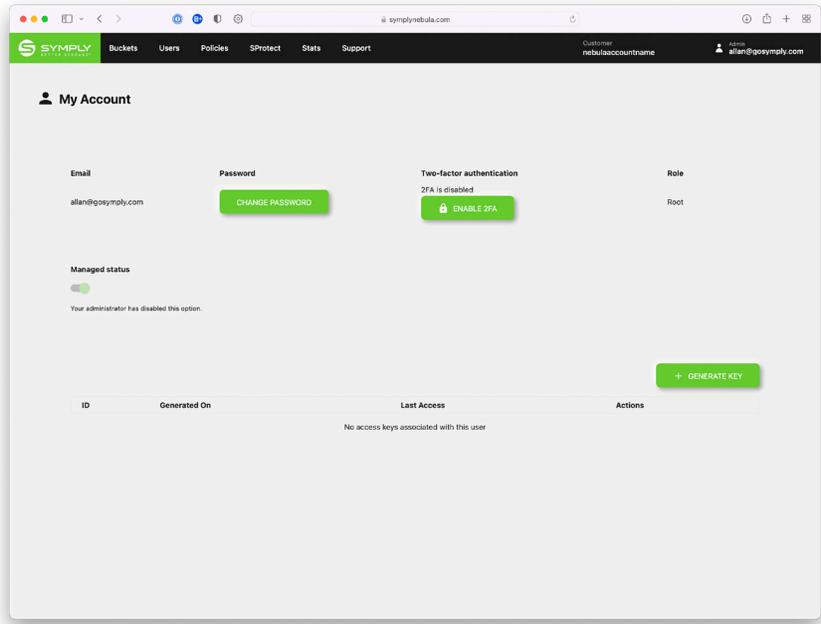
Once logged in to your SymplyNEBULA Admin Console, this is where you can create Buckets, Policies, Users, use SProtect to set whitelists for source IPs and view Stats of your SymplyNEBULA account usage.

# MY ACCOUNT



### Where to find My Account

My Account is accessed from the top-right of the screen by clicking on the email address used to sign-in to SymplyNEBULA.



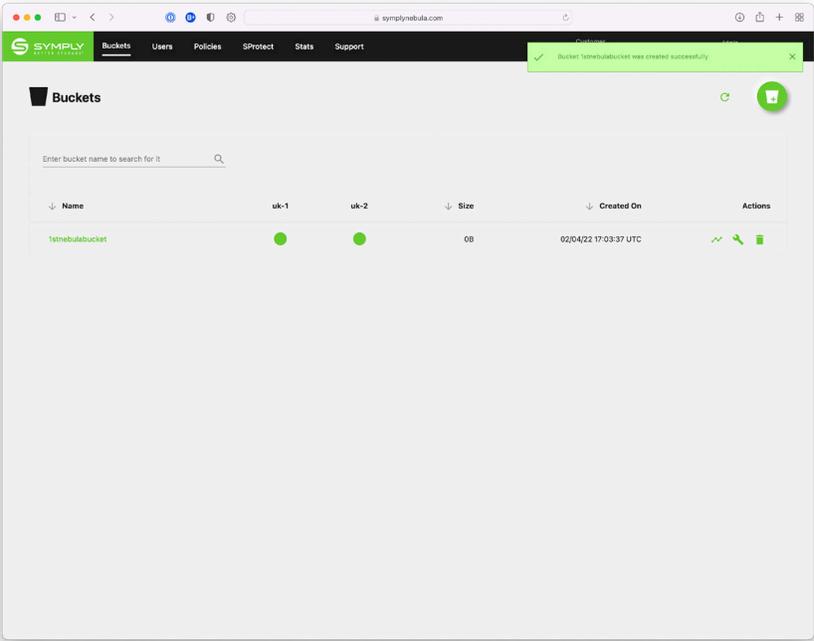
### My Account page options

A user can use this page to change their account password, setup MultiFactor Authentication (MFA) and generate key pairs for access.

# BUCKET CREATION

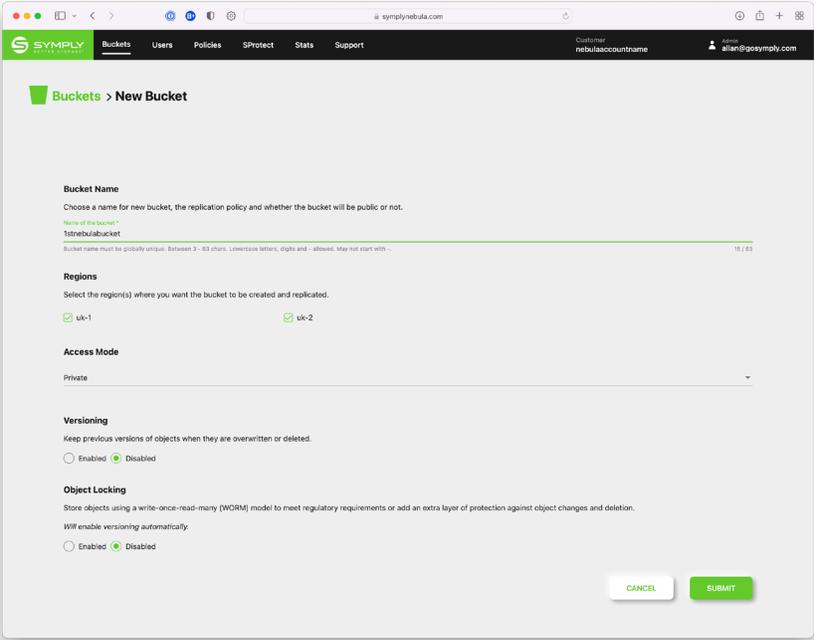
A bucket is a container for objects with a unique URL for use with S3 compatible software for storing data in your SymplyNEBULA cloud account.

The Bucket tab lists buckets associated with the account, the regions in which buckets are enabled (Replication), the bucket's Size, date Created On and an Actions column for managing the bucket.



Admin console | Buckets list

Create a bucket by clicking on the image of a bucket with a '+' symbol, found in the top right of the page.



New Bucket form

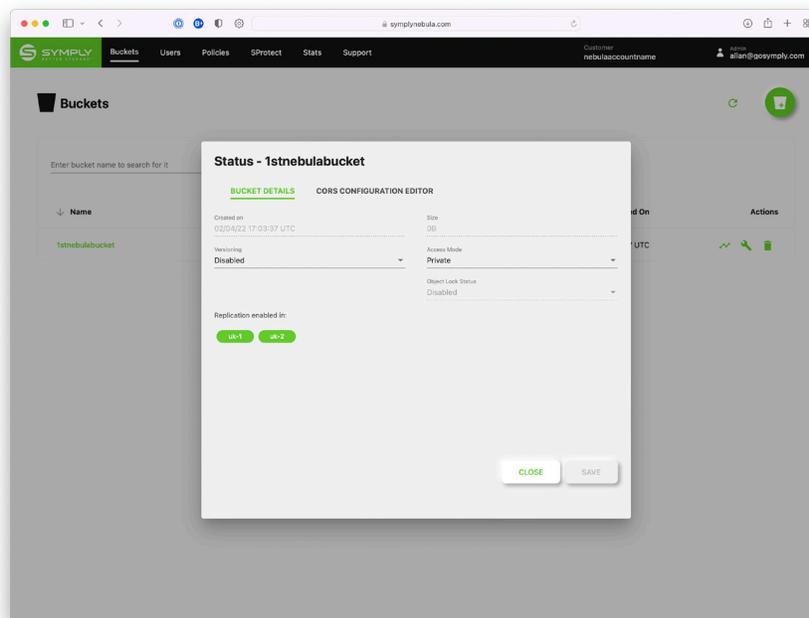
Creating a bucket is a case of:

- entering a Bucket Name
- selecting the replication Regions - defaulted to all available
- setting the Access Mode - defaulted to Private
- setting the Versioning option - defaulted to Disabled
- setting the Object Locking option - defaulted to Disabled
- clicking SUBMIT

Having clicked SUBMIT you are returned to the Buckets tab.

*NOTE: When naming a bucket, be sure to follow these rules:*

- *Bucket name must be globally unique.*
- *Between 3 - 63 chars.*
- *Lowercase letters, digits and "-" allowed.*
- *May not start with "-".*

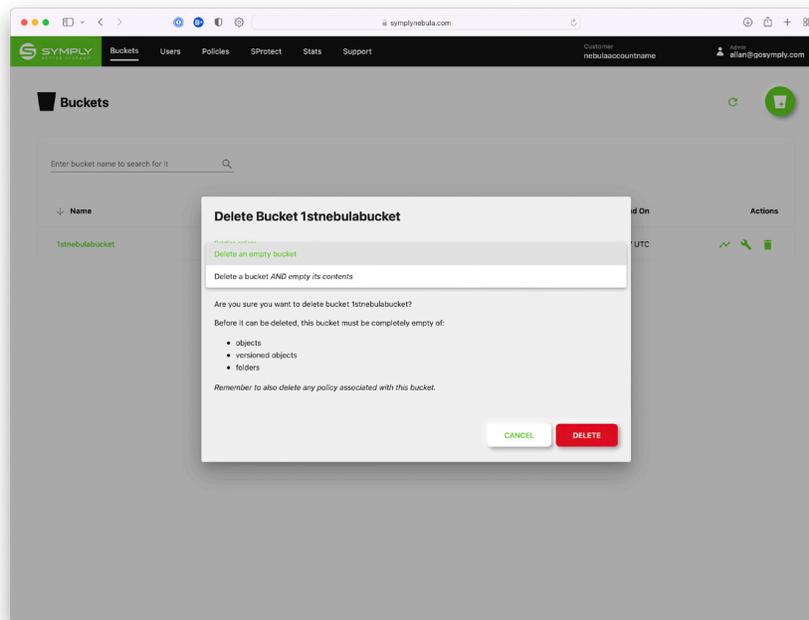


*Edit Bucket pop-up*

Should you wish to make changes to your bucket, this can be done by clicking on the wrench icon under Actions where you can alter:

- Versioning
- Access Mode

# BUCKET DELETION

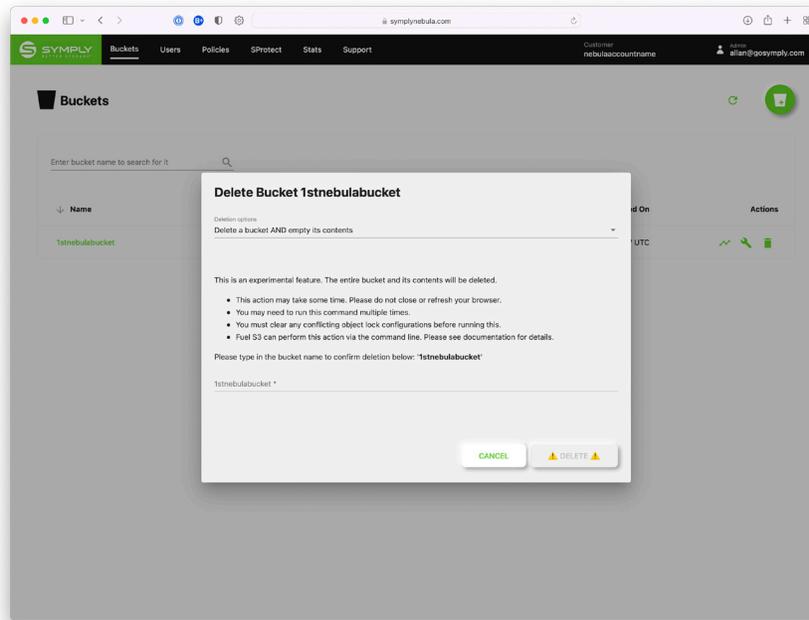


*Delete bucket pop-up*

The process to delete a bucket is as follows:

1. Empty the bucket of all contents
2. Detach all Policies attached to the bucket
3. Click the Trash icon under Actions associated with the bucket to be deleted.

# SUPER BUCKET DELETION



*SuperDelete bucket pop-up*

SymplifyNEBULA includes an experimental feature: SuperDelete that will delete all contents and associated Policies all at once. There are a number of caveats which should be noted when using this feature however:

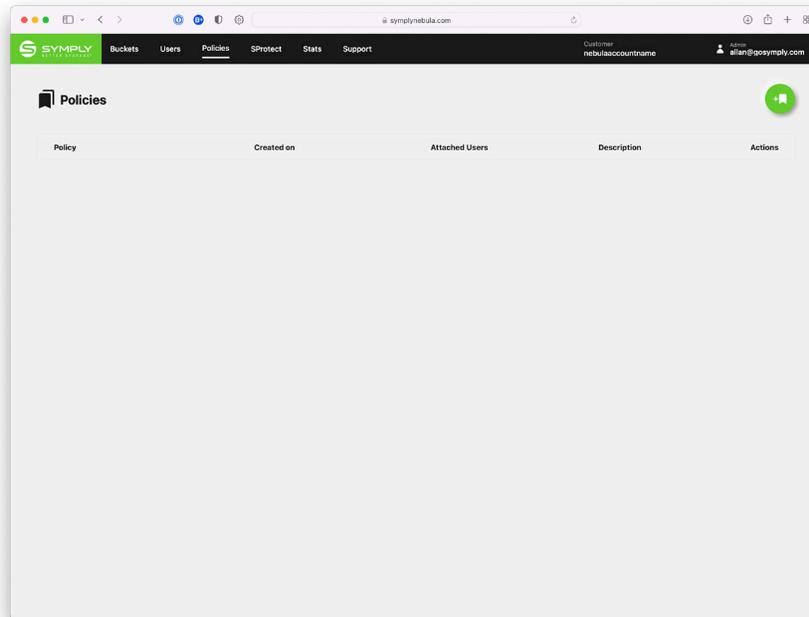
- This action may take some time. Please do not close or refresh your browser.
- You may need to run this command multiple times.
- You must clear any conflicting object lock configurations before running this.
- Fuel S3 can perform this action via the command line. Please see documentation for details.

# POLICY CREATION

Access to buckets and their contents is controlled through policies which are attached to buckets and users.

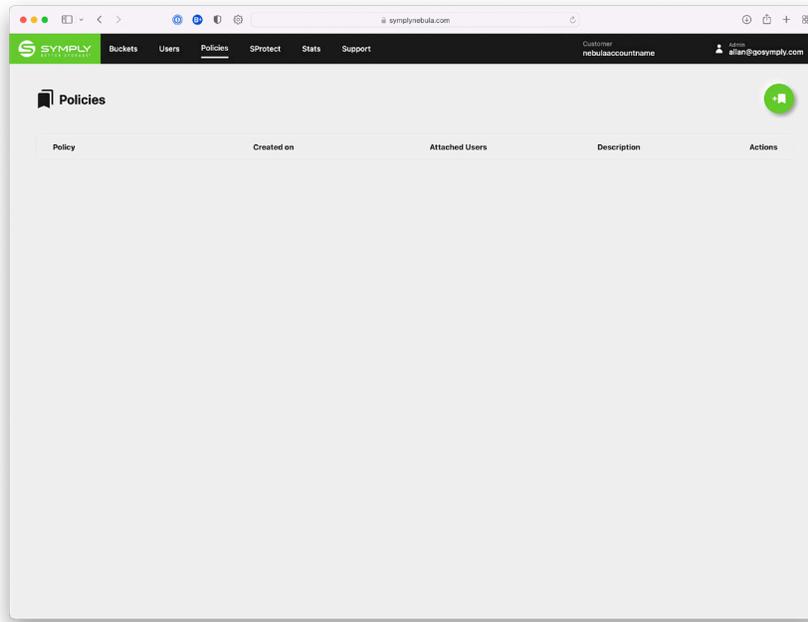
These controls are:

- Read
- Write
- List
- Delete



*Admin console | Policies tab*

Create a policy by clicking on the new policy icon in the top right of the page. This opens the new policy page.



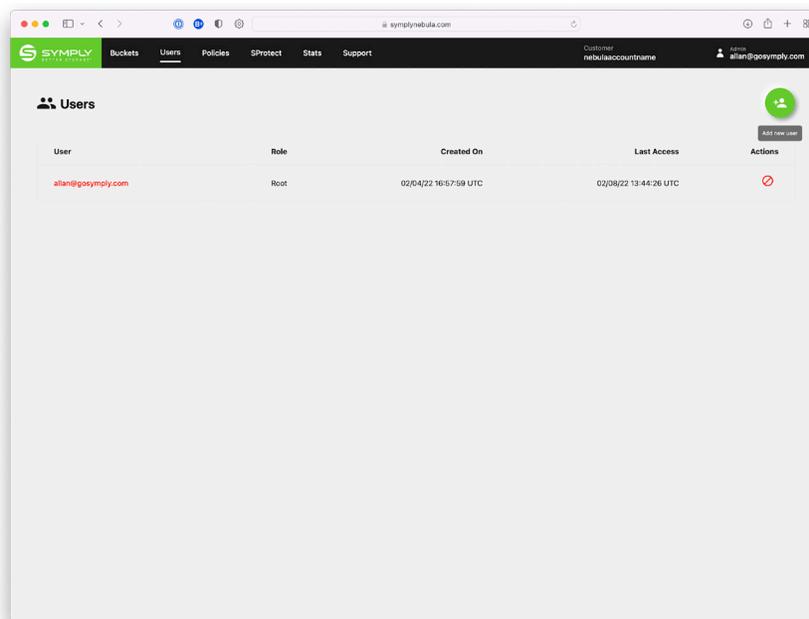
*New Policy form*

Creating a Policy is a case of entering the following details:

- Policy Name
- Policy Description
- Select Bucket – specific bucket or All Buckets
- Set Permissions
- Click SAVE

In order to complete the granting of permissions to a bucket, create a user and attach a policy to the user.

# USER CREATION

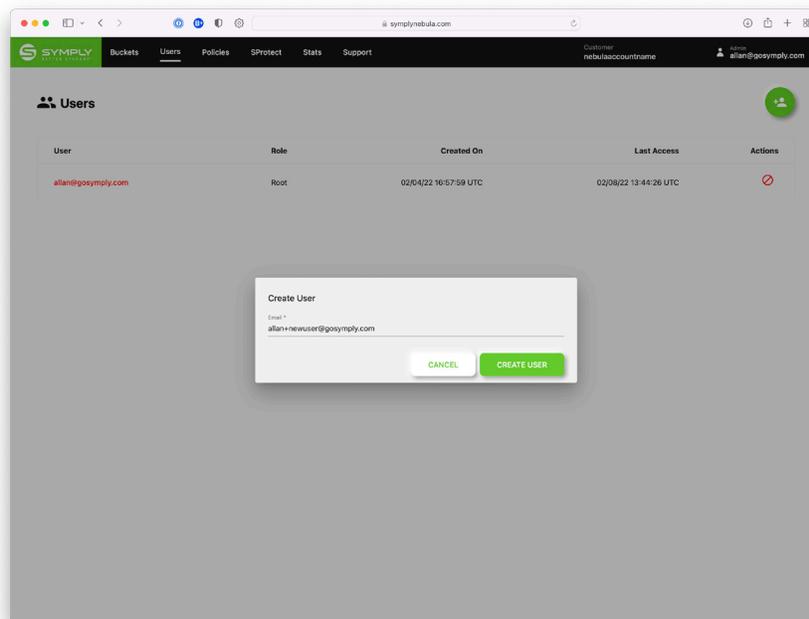


Admin console | User tab

Create new users by following these steps:

1. Go to the Users tab on the top of the page
2. Click the new user icon at the top right of the page
3. Enter the user's email address.

*NOTE: the email address is not validated and is only used for login purposes and to send password reset links*



Enter new user email

4. Click CREATE USER which opens the new user setup page where it is possible to send a RESET PASSWORD link, attach policies and generate key pairs for access.

# GENERATE KEYS

The Access Key acts as a Username and the Secret Key as a Password. All S3 compatible software will require these credentials.

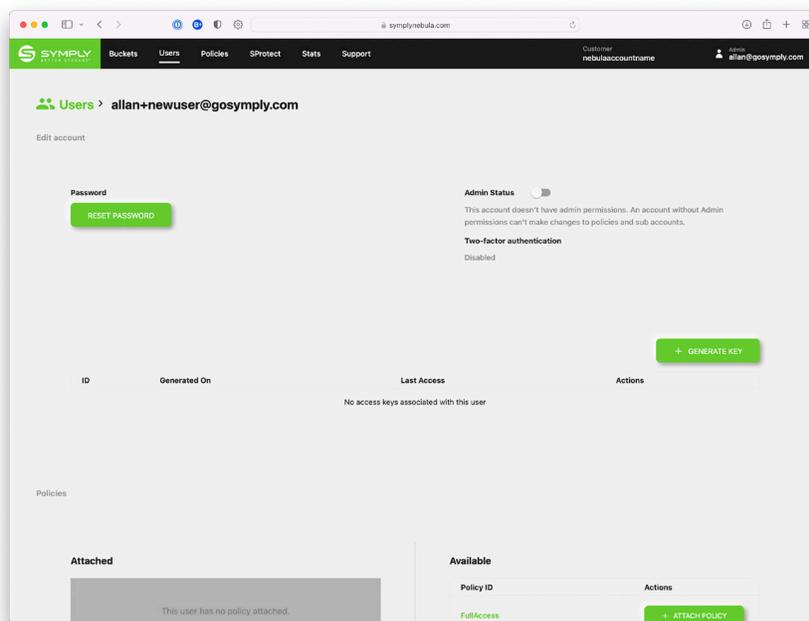
Admin and Root accounts can generate key pairs for other users, and those with the User role can generate their own keys.

In order to access buckets and their contents a user must have the following:

- Endpoint URL - <https://s3.symplynebula.com>
- Bucket name - supplied to them by an admin
- Be assigned a policy granting them appropriate permissions
- Access Key & Secret Key pairs

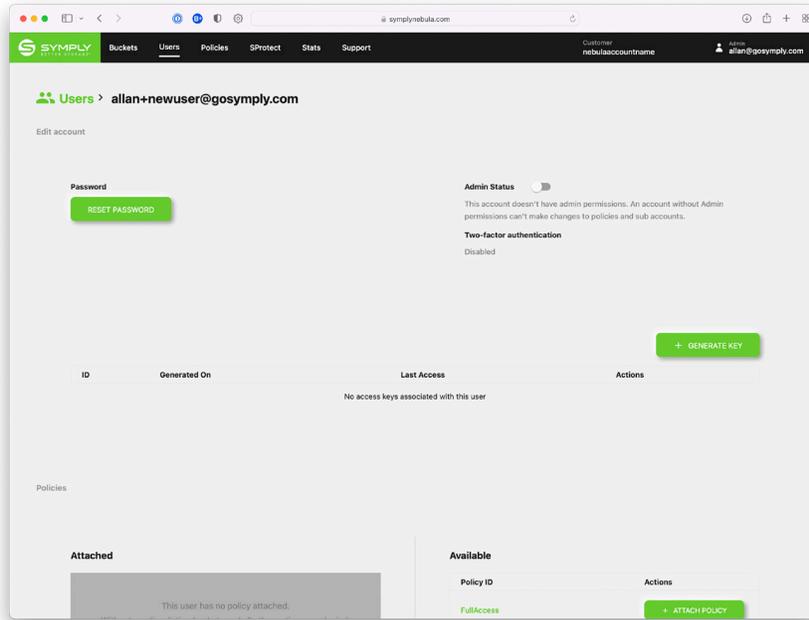
## GENERATE KEYS FOR ANOTHER USER

1. Go to the Users tab and click the pencil icon under the Actions column to enter the Edit Account page



Admin console | Users | Edit Account

2. Click + GENERATE KEY button to generate the key pair

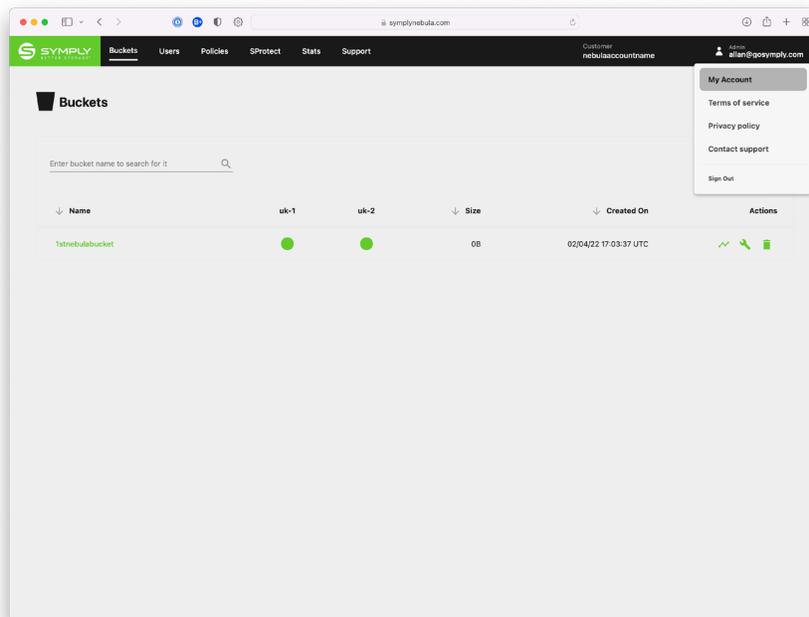


Admin console | Users | Generate Keys

3. It is advisable to use the option to Download as CSV and then keep this in a safe and secure area, preferably in an encrypted vault such as a password manager as it cannot be retrieved again from the system
4. For a one-time view, select the eye icon for the Secret Key

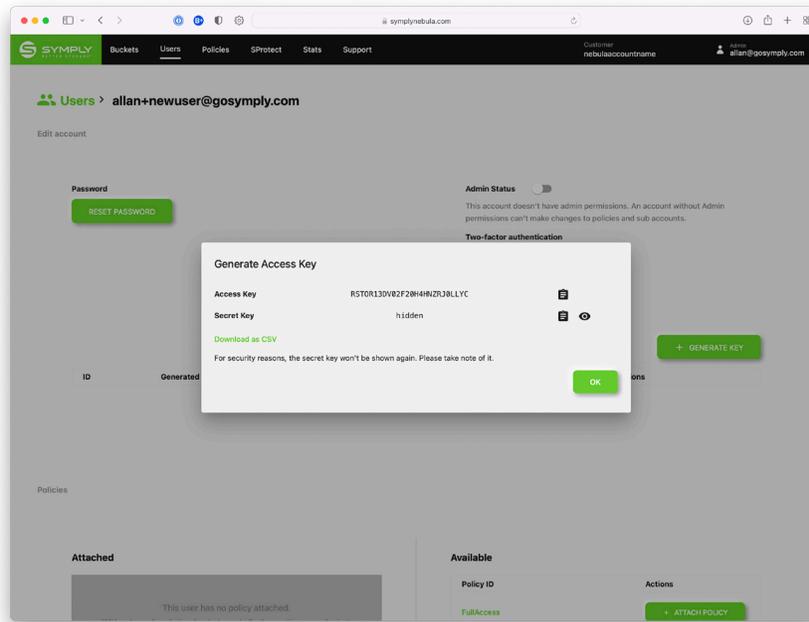
## GENERATE KEYS FOR YOUR ACCOUNT

1. Go to My Account by clicking on your email address in to the top right



Where to find My Account

2. Click + GENERATE KEY button to generate the key pair



*My Account | Generate Keys*

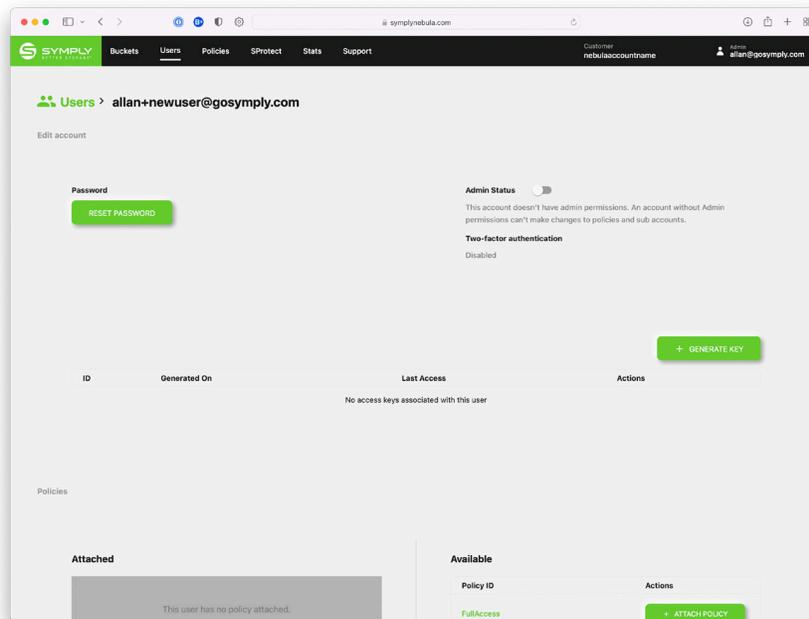
3. Click Download as CSV and store the file securely - preferably using a password manager as it cannot be retrieved again from the system. The Secret Key can be viewed once by clicking the eye icon.

It is important to note the following about key pairs:

- Any user without a key pair cannot generate a pre-signed link to share with anyone without a SymplyNEBULA user in their account. The request will not send a valid credentials object and will fail.
- Key pairs are not generated automatically for any user, so must be generated by a user with Admin or Root role or by the user themselves.

# ASSIGN POLICIES TO USERS

## GRANT PERMISSIONS



*Admin console | Users | Edit Account*

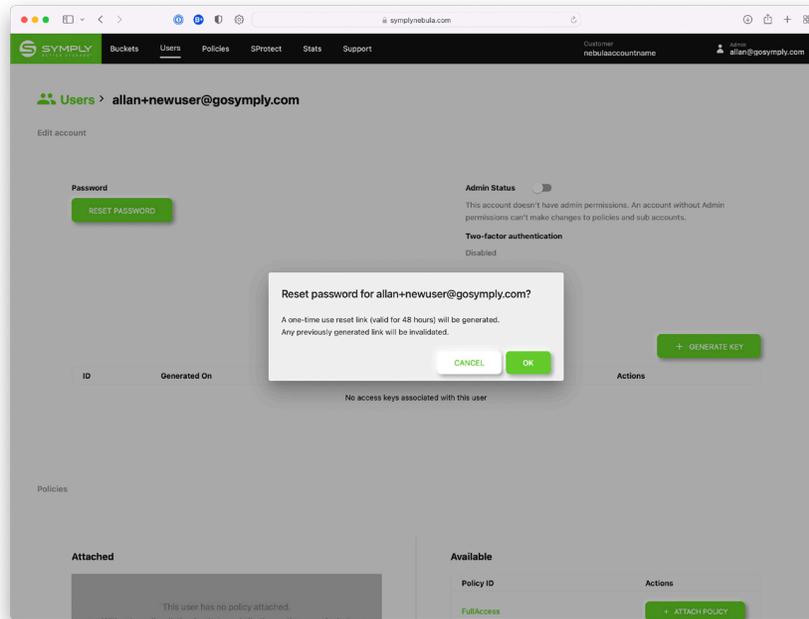
With a user created, attach the desired policy by clicking on the pencil icon next to their email address under the Actions column within the Users tab. If you have just completed creating a user, then you will already be in the Edit Account page.

Available Policies are listed at the bottom right of the page.

Simply click the + ATTACH POLICY button of the policy/policies desired.

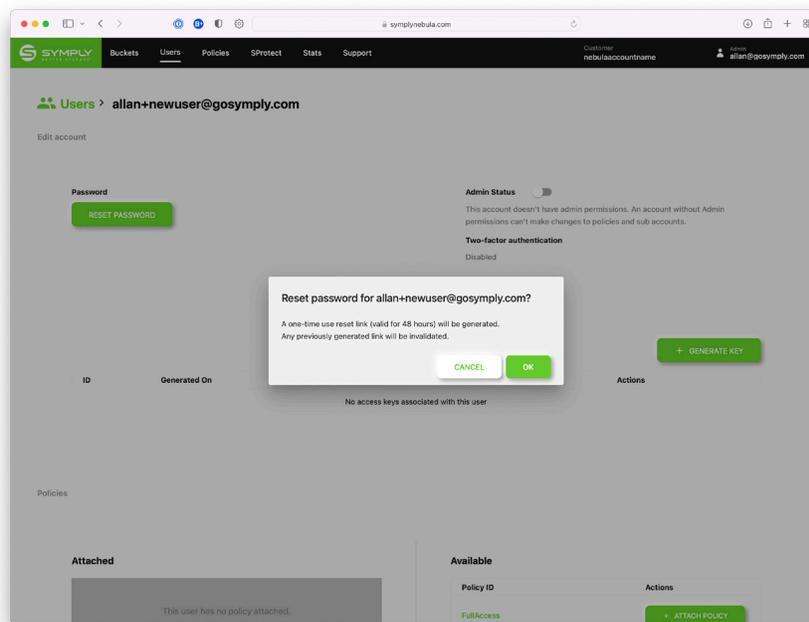
# NEW USER SETUP

SympleNEBULA will not automatically notify the user of their new account, in order for a new user to be able to sign-in they will need a RESET PASSWORD link sent to their email address from within the Edit Account page for their account.



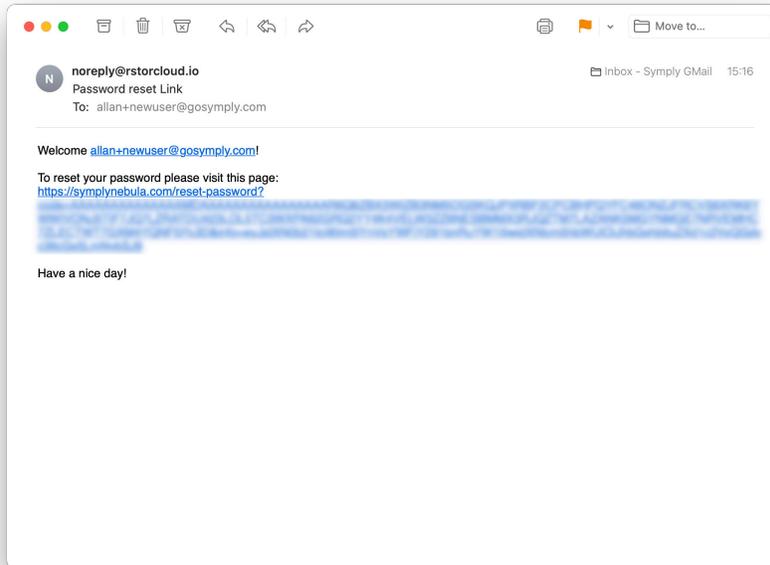
## *RESET PASSWORD button*

1. In the Users tab, click the pencil icon under Actions next to their account.
2. Click the RESET PASSWORD button in the top left
3. Click OK in the information pop-up



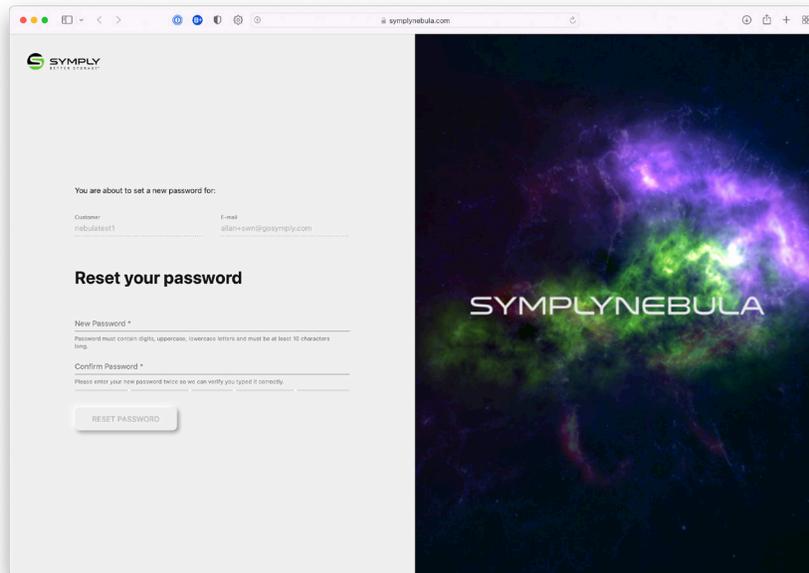
*Send email link to user*

4. Click the SEND LINK VIA E-MAIL button



*Reset password link email from SymplyNEBULA*

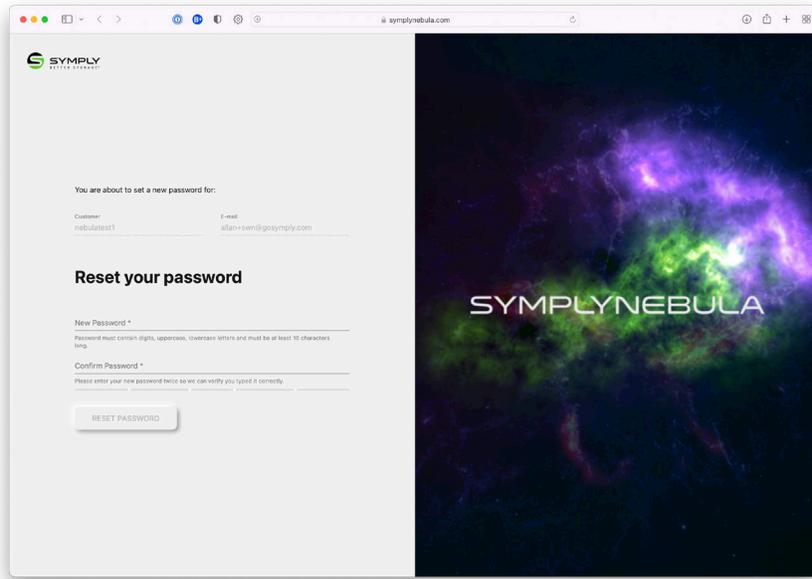
5. The user receives an email with the reset password link - valid for 48 hours. Clicking the link opens the SymplyNEBULA Reset Password page.



*Reset password page*

6. The user creates their password and clicks the RESET PASSWORD button

7. Once you've set your password, you'll be redirected to the SymplyNEBULA sign-in page. Enter your details and click SIGN IN.



*SymplyNEBULA sign-in*

# TEST BUCKET ACCESS

In order to access buckets and their contents a user must have the following:

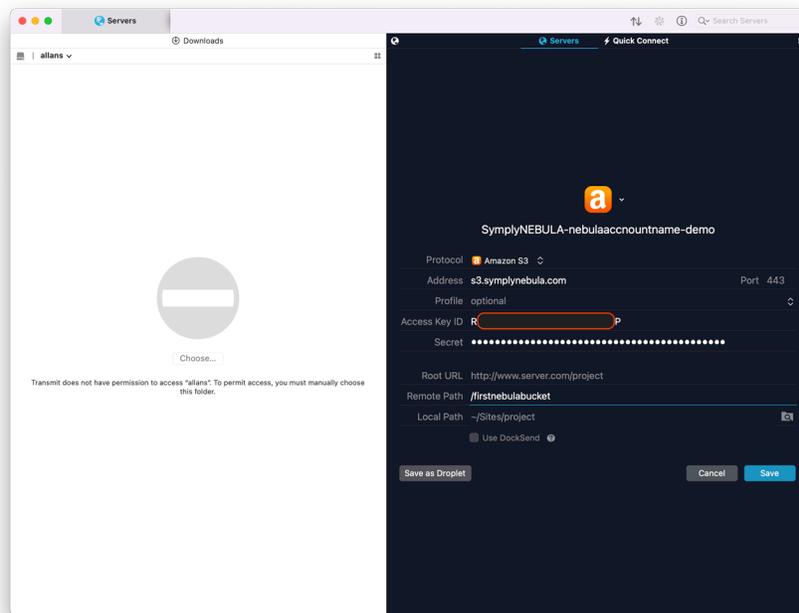
- Endpoint URL – <https://s3.symplynebula.com>
- Bucket name (supplied to them by an admin)
- Be assigned a policy granting them appropriate permissions
- Access Key & Secret Key pairs

## APPLICATION CONFIGURATION

Most S3 compatible applications are configured in the same manner, supplying:

- Endpoint URL
- Bucket name
- Access Key
- Secret Key
- Path (optional)

SymplyNEBULA does not use the concept of regions in its endpoint URL, therefore please leave any mention of regions as the default in the application.



*Transmit S3 configuration*

This is an example configuration using Transmit from Panic Software for macOS.



[www.gosymply.com](http://www.gosymply.com)  
[support.gosymply.com](mailto:support.gosymply.com)  
[hello@gosymply.com](mailto:hello@gosymply.com)