RSTOR®

RSTOR Space

US Direct Customer Quick Start Guide

September 2021

Prepared by: RSTOR Support

Table of Contents

1 Introduction

RSTOR Space™ is RSTOR's core product offering that is **S3 compatible** with public and hybrid infrastructures. RSTOR Space allows customers to safely store their data with multi-copy geographically distributed data protection, immutability options and eventually consistent replication. RSTOR Space is hyper-scalable to serve the needs of varying workload types.

As an S3 compatible storage system, RSTOR Space can easily be integrated with existing S3 compatible applications.

An **S3 bucket** is a public cloud storage resource which contains objects. The Simple Storage Service **(S3)** data model uses a flat structure, there is no hierarchy of folders and subfolders, all objects are stored inside the root of the bucket. It is possible to filter objects using prefixes and delimiters to a subset of the bucket. An object is uniquely identified by its bucket, its full name (also known as object ID) and optionally the associated metadata.

1.1 Clients and Network Connectivity

RSTOR Space exposes an S3 compatible interface over HTTPS. The interface can be used in two ways:

Interactively:

- RSTOR's Native Web GUI, best for simplified management access (https://us.rstorcloud.io/signin)
- Third-Party S3 compatible GUI or CLI clients

Programmatically:

- Via API calls with S3 compatible SDKs or libraries with Endpoint, Access Key and Secret Key credentials

1.2 API Guide

The API Guide is accessible from the RSTOR Space Web GUI:

https://s3.us.rstorcloud.io/apidoc/index.html

RSTOR Space Object Storage has been tested against all major SDKs for S3 clients (including but not limited to boto python library, AWS SDK Go library, AWS SDK JS library), S3 GUIs (CyberDuck, S3browser), and various S3 capable applications. Please check with RSTOR for the compatibility listing, if you do not see one applicable to your needs, let us know.

1.3 The “Very” Quick Start

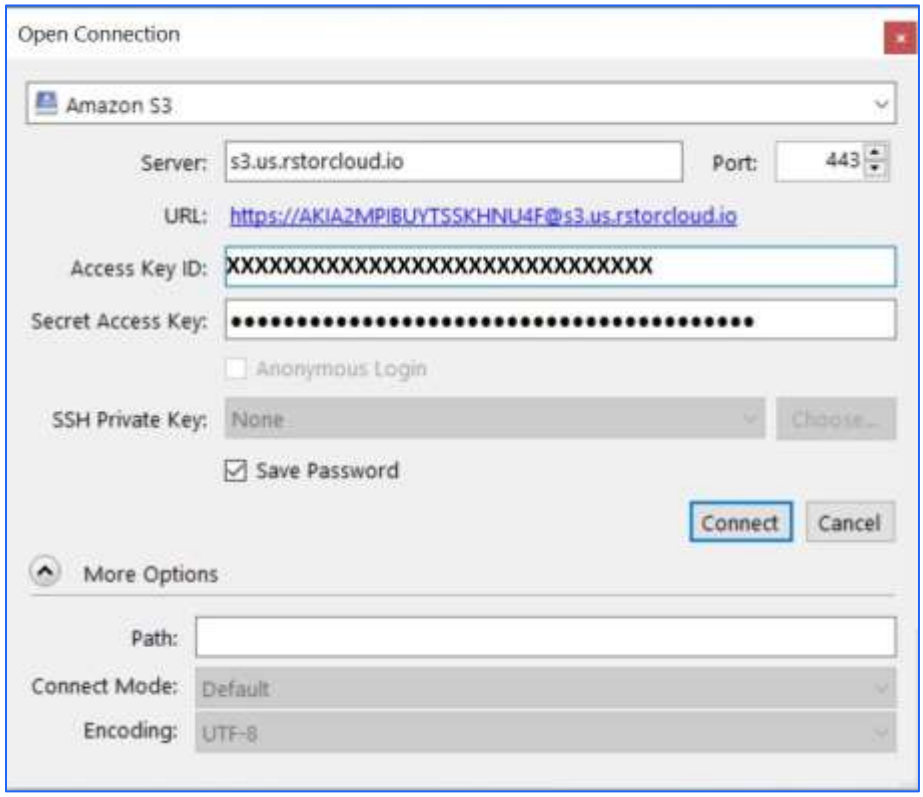
If you are going to use root access with no additional users:

- In the web GUI generate a key set for your user ID
- Create a bucket
- Use the keys you’ve generated, along with the endpoint, in your app (Cyberduck, etc.)
- Go!

All of these are discussed in much greater detail below.

1.4 Application Configuration

Most S3 compatible applications are configured in the same manner. RSTOR Space does not use the concept of regions in an end-point configuration, so it is ok to leave it using the defaults. Here is an example of an S3 Browser style application called Cyberduck (Cyberduck does not use concept of regions).



2 Getting Started

Customers may access their buckets through a DNS-style or Virtual-Host convention, as well as through the web GUI:

- DNS style uses https://$bucketname.$endpoint/$path/
- Virtual-Host style uses https://$endpoint/$bucketname/$path
- https://us.rstorcloud.io/signin

Where $endpoint is:

- s3.rstorcloud.io
- We support access only on port 443, using TLS v1.2 or later.

2.1 Roles and Types (Account Identities)

There are three distinct roles for those who access the RSTOR Space system:

Role	Description
Admin	Can manage users and policies, with the exception of the Root account.
Root	The initial and main identity of the customer account. Direct customer Root identities can also create access/secret key pairs for access. **The Root account cannot be deleted.*
User	Can perform operations on buckets according to the policies that are attached. It can change its own password, create access/secret key pairs for access.

The Root identity is assigned to the owner of the RSTOR Space account.

2.2 Access and Configuration

To access the account, use the following URL: https://us.rstorcloud.io/signin.

*If resetting the password, the user must wait 1 minute before repeating a password reset request. No error is returned if the user does not respect the minimum interval between requests.

Once logged in, the account page gives access to options such as configuring MFA (multifactor authentication), changing the account password, and generating keys. Click on your profile in the upper right corner of the navigation bar to locate "My Account".

2.3 Create a Bucket

RSTOR Space leverages the concept of buckets: each bucket is a container for objects. To create a bucket, complete the following steps.

1. Go to "Buckets" using the top navigation bar.
2. Click on the "Add New Bucket" icon in the upper right corner.
3. A popup will appear where you can fill in the necessary information to make a bucket. You can select which sites you would like your bucket to be replicated to.

   **If this option is not available, please contact your overarching admin as they may have disabled this setting.*

4. Through Access Mode, buckets can be set as "Private", "Public", or "Custom". Check the boxes for the permissions that you want to provide. All new buckets are private by default. To grant access to your bucket to the general public (everyone in the world), select "Public" under Access Mode. Granting public access permissions means that anyone can access files in the bucket.

   The format for accessing a public bucket is: https://bucketname.endpoint.path where there is case sensitivity in the letters. Such as:

   https://s3.us.rstorcloud.io/samplefiles/createrandomfiles.sh*

   All new buckets are private by default.

   To change the access mode for an existing bucket:

   1. Go to "Buckets" using the top navigation bar.
   2. Select the wrench icon under the "Actions" column for that bucket to change the Access Mode (Private or Public) or change versioning.

2.4 Delete a Bucket

To delete a bucket, typically you have to empty all of its objects, folders, etc., and delete all of its associated policies. However, RSTOR offers a SuperDelete feature that deletes the bucket and its entire contents for you at once.

To use either of these, do the following:

1. Navigate to the “Buckets” home screen.
2. On the far right, beneath the “Actions” column, click on the “Trash” icon.
3. Here you will have the option to delete your bucket using one of the two methods talked about above. Use the dropdown menu to choose your deletion option. Remember that if you decide to proceed with SuperDelete, you should *not* close or refresh your browser and the command may need to be run several times.

2.5 Create Users

To create a new user, follow the next steps.

1. Click on the “Users” tab on the side bar at the bottom of the window then click the round icon in the top right corner to add a user.
2. Provide the email you would like to give access to. The email address is not validated, and is only used for login purposes or to send password reset links.
3. After that has been provided, press “Create User”.
4. Once created, you can edit what permissions the new sub-user has by clicking on their email in the Users page. The notification is not sent to the user automatically. The user should be notified separately, though in the case of a password reset there is an option to send the link to the user email used in the account credentials.

2.6 Create Policies

To create policies in your RSTOR Space bucket, begin by accessing the Policies menu from the main bar.

1. Click the create policies button in the top right corner. This will open up a screen that will allow you to input a name and description for your new policy.
2. The option to select a bucket is located underneath the naming schema. Once a bucket is selected you will have the option to control what permissions to apply to that bucket.
3. Once the options are selected, press save, and those permissions will now apply to the bucket.

2.7 Generate Access Keys

It is important to note the following about access keys.

- A ROOT user without an {AccessKeyID, SecretAccessKey} pair cannot generate a pre-signed link. The request will not send a valid credentials object and will fail.
- The current user cannot generate a pre-signed link without an {AccessKeyID, SecretAccessKey} pair.
- The ROOT user of an account does not have an {AccessKeyID, SecretAccessKey} pair generated for them by default.

1. To create application credentials (access/secret key pairs) for the account, go to the RSTOR Portal and click on your name in the upper right corner. From there choose “MY ACCOUNT”.
2. Select “+ GENERATE KEY” in the bottom right corner.
3. Download the CSV key and manage as you normally would, such as with a password manager.
4. Once downloaded, use your favorite .csv compatible application (Excel, Google Sheets, Numbers) to view the contents. For a onetime view, select the “eye” icon for the secret key.

   *Note that multiple key pairs may be created for an account.

2.8 Set Up Multifactor Authentication

1. To begin set up for multifactor authentication, access your accounts page by clicking on the top right corner of the UI where your name is listed and choosing “My Account.”

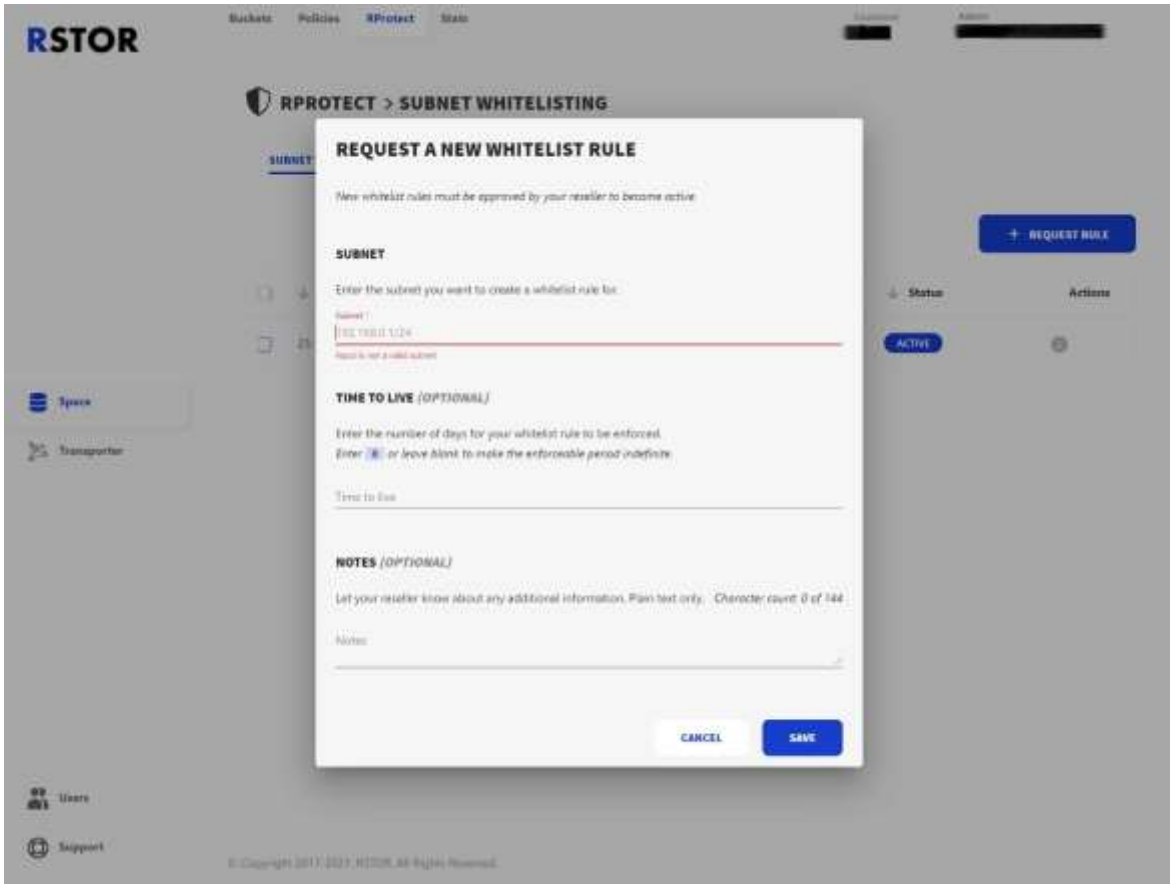
2. Next, press the “ENABLE 2FA”.

3. This will display a QR code along with a secret key in a popup menu. Most MFA apps will ask to scan this QR code. Your MFA app will then provide a token that needs to be entered into the available space below the QR code to confirm the setup.

4. Once setup is completed, a handful of recovery keys will be given in case you lose access to your MFA device. Please make sure to copy these down. This will be the only way to recover your locked account. Popular MFA apps are Authy and Google Authenticator.

2.9 RProtect

RSTOR Space uses whitelisting as part of our security. To add an IP address range to our whitelist use the RProtect tab in the web GUI.



The only required information is the IP/range. Please keep the IP ranges requested as small as possible. Requests are approved automatically for our customer production accounts.

3 Appendix

3.1 Statistics of Transfer

In the RSTOR Space portal, you can display statistics of your account along with the storage and transfer rates. It will also display a graph with the total used space (GB), number of objects stored, egress and ingress traffic, all aggregated by day. This can give insight into when your users seem to be using the most bandwidth.

The admin can choose the date interval to display and can export the data to csv for easier processing using third-party programs.

1. To view the statistics, click on “Stats” in the top navigation bar.

Information on how to obtain the same data in a programmatic way is available in the API documentation.

3.2 Support

Through the RSTOR Space Support portal, you can receive further support through accessing our API documentation or contacting us. Access the Suport portal by clicking on the tab labelled “Support” on the lower left of the GUI window, then clicking the “CONTACT US” link.

3.3 Troubleshooting

The following are some troubleshooting tips for the most common problems we have encountered. Please contact your account team for additional assistance.

1. If you are unable to connect to the RSTOR Space web portal using the password reset URL provided with your credentials, please contact RSTOR for a new reset URL. There is a time limit in which these URLs are able to be used.

2. If you have obtained a new password reset URL and are still unable to connect to the RSTOR Space web portal, please make note of the error you are receiving.

    a. “invalid Account, E-mail address or Password” – check these match the credentials you were sent.

    b. “Your IP address (xxx.xxx.xxx.xxx) is not allowed. Make sure you are connected to the correct network and try again.” – check that your IP is the

same as was submitted to RSTOR for whitelisting. To obtain your IP address you can go to https://whatsmyip.com/

1. If you can connect to the RSTOR Space web portal but can not connect using a client such as Cyberduck, please verify you are using the correct server and URL. These are not the same as the RSTOR Space web portal.

    a. Server Example: s3.us.rstorcloud.io

    b. URL Example: HTTPS://s3.us.rstorcloud.io/