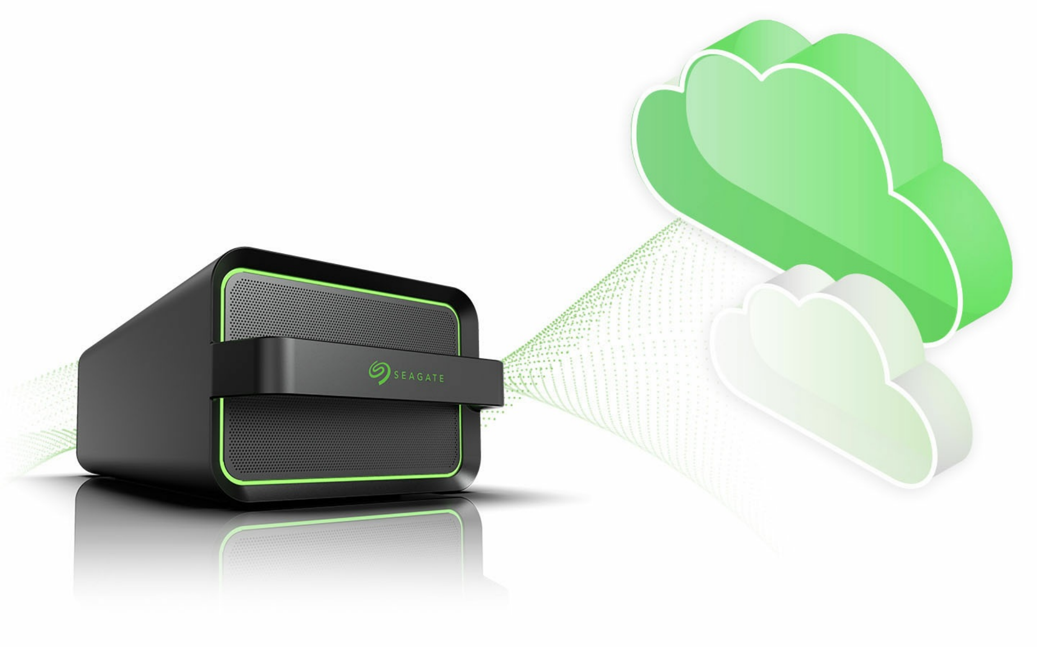
Cloud Import Service User Manual & Reference Guide



Clique aqui para acessar uma versão online atualizada
desse documento. Você encontrará o conteúdo mais recente, bem como ilustrações expansíveis, navegação mais fácil e recurso de pesquisa.

Contents

Lyve Mobile with Cloud Import

Lyve Mobile with Data Transfer from Seagate® is a high-capacity edge storage solution that enables businesses to aggregate, store, move, and activate their data. Scalable and modular, this integrated solution eliminates network dependencies so you can transfer mass data sets in a fast, secure, and efficient manner. With our new cloud import option, your data can be saved securely on the device and imported to the cloud destination of your choice.

The solutions are delivered as a service—you order and pay only for the devices you need, when you need them. Take a right-sized approach to your data transfer needs with flexible service plan options designed to optimize your budget. Adapt to changing business needs by adjusting your subscription at any time.

Cloud Import Process Overview

1. Sign in to Lyve Management Portal.

> ℹ If you do not have an account, register at lyve.seagate.com. Create a profile and an Org. See Getting Started in the Lyve Management Portal User Manual.

2. Create a Lyve Mobile subscription if one has not already been created for you. SeeLyve Mobile Subscriptions in the Lyve Management Portal User Manual.
3. Configure an import plan for the subscription. SeeConfigure a cloud import plan in the Lyve Management Portal User Manual.
4. Move data onto your Lyve Mobile Array(s).
5. Send Mobile Array(s) to a Seagate import site.
6. After completion of the import, verify your files in your cloud destination and confirm the import in Lyve Management Portal.
7. Device(s) are cryptographically erased. A confirmation document detailing the erasure is sent.

Security and Lyve Mobile with Cloud Import

You should always utilize best practices of ensuring encrypted data transfer protocols between Lyve Mobile and your cloud provider. Seagate provides a highly secure data center and network architecture that is built to meet the requirements of most security-sensitive organizations. Third-party agencies also regularly review and test the security of our systems, architecture, and processes. When storing your cloud destination credentials, all your information is transmitted and stored with industry standard encryption and access can only be requested by your device.

However, ensuring your data is protected is a shared responsibility that requires you to follow your organization’s security policies, maintain the sensitivity of your data, and align with applicable laws and regulations.

Key terms

Import destination—An import destination is a cloud and region where your data will be imported to.

Import plan—An import plan is tied to a Lyve Mobile subscription and contains the details which Seagate uses to import your data to your specified import destination. These details include credentials required to authenticate access to your cloud destination’s resources and services.

IP Address Access

If a firewall or IP restrictions are configured by your organization, you must list Seagate's Cloud Import services' IP address(es) as an allowed source.

Required IP addresses

i **Important**—If these IP addresses are not listed as allowed sources, Seagate cannot import your data.

Region	IP address(es) to allow
North America	192.55.6.251 4.15.22.254 134.204.253.248/29 192.55.8.248/29
Europe	134.204.250.248/29 91.242.219.5 185.212.46.5 134.204.255.250 193.242.211.16/28
Asia	192.55.20.248/29 134.204.251.248/29

File Naming Guidelines

Seagate follows general S3 file naming conventions.

> ! Folder names cannot contain forward slash `/` characters.

Safe characters	
Alphanumeric characters	
0-9	numerals
a-z	lowercase letters
A-Z	uppercase letters
Special characters	
*	asterisk
!	exclamation point
-	hyphen
(	parenthesis (open)
)	parenthesis (close)
.	period
'	single quote
_	underscore

Characters to avoid	
&	ampersand
	ASCII characters • ASCII ranges 00–1F hex (0–31 decimal) and 7F (127 decimal) • non-printable ASCII (128–255 decimal characters)

@	at sign
\	backslash
^	caret
:	colon
,	comma
{	curly brace (left)
}	curly brace (right)
$	dollar sign
=	equal sign
/	forward slash
`	grave
<	greater-than symbol
>	less-than symbol
%	percent sign
|	pipe or vertical bar
+	plus sign
#	pound character
?	question mark
"	quotation mark
;	semi-colon
	space - sequences with spaces, especially multiple spaces, may be lost
[	square bracket (left)
]	square bracket (right)

Be sure to check the file naming guidelines for your specific cloud destination:

- Naming guidelines for Amazon S3
- Naming guidelines for Google Cloud Storage
- Naming guidelines for IBM Cloud
- Naming guidelines for Microsoft Azure Blob Storage
- Naming guidelines for OVHcloud
- Naming guidelines for Seagate Lyve Cloud
- Naming guidelines for Wasabi S3

File Size Limitations

In general, Seagate does not recommend importing individual files larger than 5TB. Please refer to your cloud providers file size limitations and best practices.

Create a Cloud Import Plan

To configure a cloud import plan, you'll need the following:

Registered account	Access to a registered account and Org in the Lyve Management Portal. See Getting Started in the Lyve Management Portal User Manual.
Lyve Mobile subscription	A Lyve Mobile subscription with a month-to-month Project Plan service. See Lyve Mobile Subscriptions in the Lyve Management Portal User Manual.

Once you have access to your Lyve Mobile subscription, you can configure your cloud import plan. For details on configuring your import plan for your specific cloud destination, see the following:

- Import to Amazon S3
- Import to Google Cloud Storage
- Import to IBM Cloud
- Import to Microsoft Azure Blob Storage
- Import to OVHcloud
- Import to Seagate Lyve Cloud
- Import to Wasabi S3

Import to Amazon S3

Prerequisites

Before you can configure and submit your import plan, make sure to complete the following steps so that Lyve Import Service can securely access your specified Amazon S3 bucket to import your data.

AWS subscription—Set up an AWS account.

Amazon S3 bucket—Set up a dedicated bucket for your import. To learn more, seeCreating a bucket.

Seagate authorizations—Create an IAM role and supporting policy. To learn more, see Providing access to AWS accounts owned by third parties.

Seagate **requires** the following permissions to perform the import:

- s3:AbortMultipartUpload
- s3:CreateBucket
- s3:DeleteObject
- s3:GetAccelerateConfiguration
- s3:GetBucketLocation
- s3:GetObject
- s3:GetObjectAttributes
- s3:ListBucket
- s3:ListBucketMultipartUploads
- s3:ListMultipartUploadParts
- s3:PutObject

! **Important**—Failure to grant Seagate the permissions above will result in a failed import plan.

Recommendations

Seagate **strongly** recommends the following best practices:

- Create a bucket dedicated to your import plan.
- Block all public access for your bucket.
- Ensure bucket versioning is disabled.
- Ensure server-side encryption is enabled.
- Create an IAM Permission Policy.

- Create an IAM Role trusting Lyve Import Service, attaching the IAM policy you created.
- Disable or delete the role after the import plan has ended.
- Disable or delete the policy after the import plan has ended.

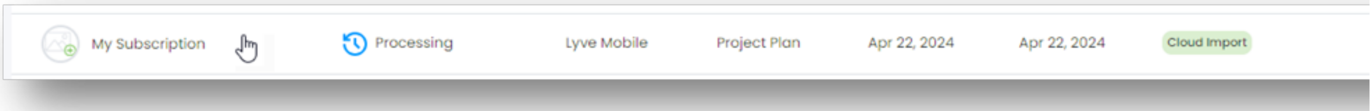
Amazon IAM Permission Policy example

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LyveMobilePolicyTemplate",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucketMultipartUploads",
                "s3:AbortMultipartUpload",
                "s3:GetObjectAttributes",
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:GetAccelerateConfiguration",
                "s3:DeleteObject",
                "s3:GetBucketLocation",
                "s3:ListMultipartUploadParts"
            ],
            "Resource": [
                "arn:aws:s3:::{bucketname}",
                "arn:aws:s3:::{bucketname}/*"
             ]
        }
    ]
}
```

Complete the prerequisites

- All devices within a subscription must be imported to the same destination and region.
- You will be required to enter and validate your bucket credentials.

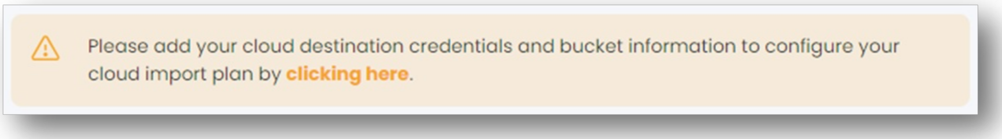
1. On your Home page, select a Lyve Mobile service subscription that includes a Cloud Import plan.



My Subscription	Processing	Lyve Mobile	Project Plan	Apr 22, 2024	Apr 22, 2024	Cloud Import

Alternatively, select the More icon in the 'Actions' column, and then select **View Subscription**.

2. Select **Import Plans** in the sidebar, or select the link at the top of the page:



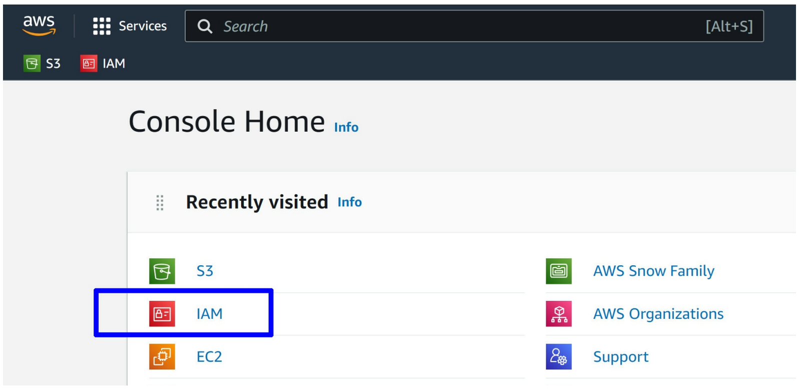
Please add your cloud destination credentials and bucket information to configure your cloud import plan by **clicking here**.

3. Confirm the Cloud Destination and Region. Select**Next**.
4. Complete the steps below so that Lyve Import Service can securely access your AWS S3 destination.

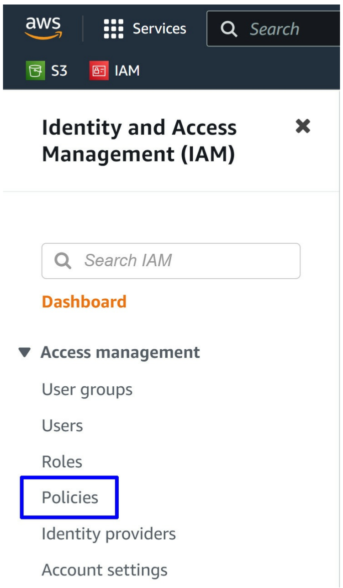
> i For helpful instructions related to each configuration step for your chosen cloud destination, select the Instructions link in Lyve Management Portal.
>
>
>
>

Create an IAM Permission Policy on your bucket

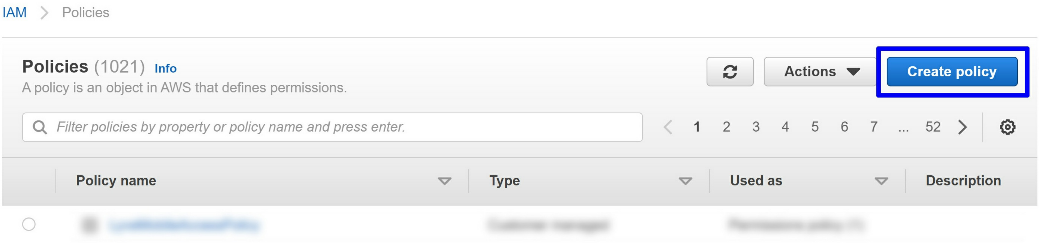
1. Log in to your AWS Console.
2. Enter the IAM service.



3. Select Policies.

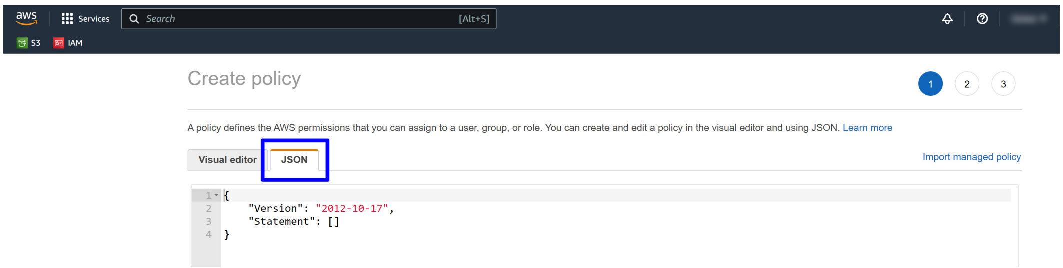


Click the **Create policy** button.



A policy is an object in AWS that defines permissions.

4. Click on the **JSON** tab.



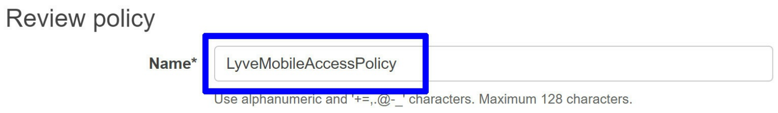
A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

```
{
    "Version": "2012-10-17",
    "Statement": []
}
```

5. Copy the provided JSON script below:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "LyveMobilePolicyTemplate",
         "Effect": "Allow",
         "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:ListBucketMultipartUploads",
            "s3:AbortMultipartUpload",
            "s3:GetObjectAttributes",
            "s3:CreateBucket",
            "s3:ListBucket",
                "s3:GetAccelerateConfiguration",
                "s3:DeleteObject",
                "s3:GetBucketLocation",
                "s3:ListMultipartUploadParts"
            ],
            "Resource": [
                "arn:aws:s3:::{bucketname}",
                "arn:aws:s3:::{bucketname}/*"
             ]
        }
    ]
}
```

6. Paste the copied text into the JSON editor.
7. Replace {bucketname} with the name of the bucket you want to import your data to.
8. Click the **Next: Tags** button.
9. Add tags (optional) and click the **Next: Review** button.
10. On the **Review policy** page, name the policy LyveMobileAccessPolicy.

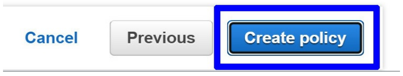


Review policy

Name* LyveMobileAccessPolicy

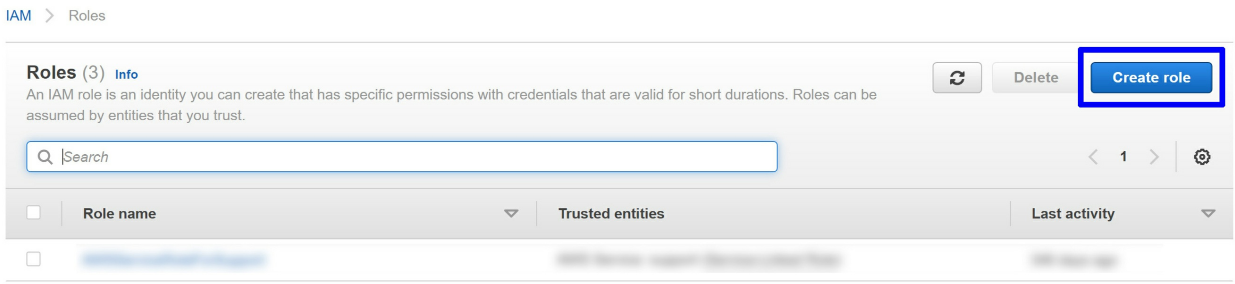
Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

11. .Click **Create policy**



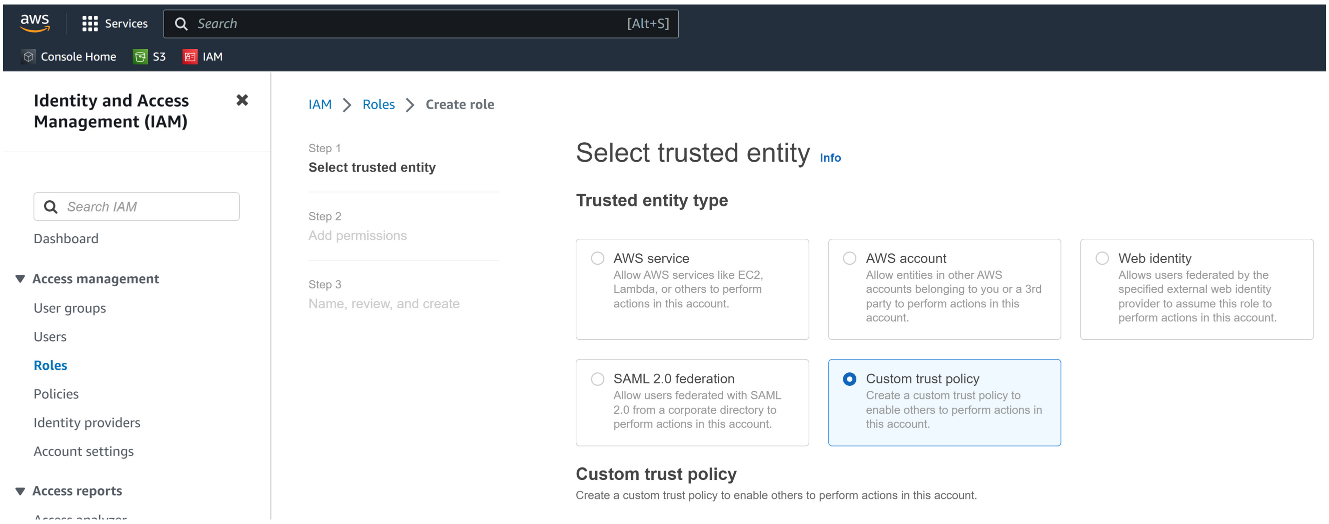
Create an IAM role trusting Lyve Import Service

1. In the sidebar, click **Roles**. Click the **Create role** button.



An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

2. On the **Select trusted entity** page, select **Custom trust policy**.



Services Search [Alt+S]

Console Home S3 IAM

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

○ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

● Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

3. Copy the provided trust policy below:

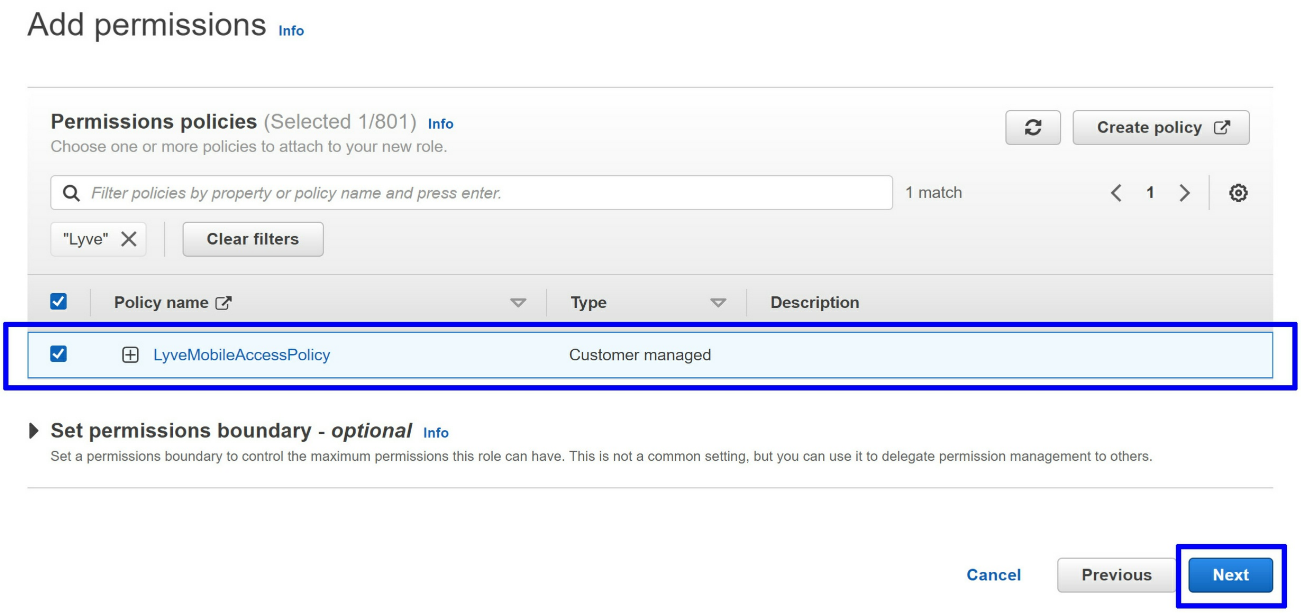
```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::{accountid}:root"
   },
   "Action": "sts:AssumeRole",
   "Condition": {
    "ForAnyValue:StringEqualsIfExists": {
     "sts:ExternalId": [
      "{externalid}"
     ]
    }
   }
  }
 ]
}
```

4. Paste the copied text into the JSON editor.
5. Replace {accountid} with the value you copied for Lyve's S3 Account ID. Replac{externalid} with the value you copied for External ID.
6. On the **Add permissions** page, add the **LyveMobileAccessPolicy** you created earlier and click **Next.**

   If you have multiple import plans to configure, add the external ID for each plan separated with a comma (,). For example:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::{accountid}:root"
   },
   "Action": "sts:AssumeRole",
   "Condition": {
    "ForAnyValue:StringEqualsIfExists": {
     "sts:ExternalId": [
      "{firstexternalid}",
          "{secondexternalid}",
          "{thirdexternalid}"
     ]
    }
   }
  }
 ]
}
```

7. Click **Next** to exit the JSON editor.
8. On the **Add permissions** page, add the **LyveMobileAccessPolicy** you created earlier and click **Next**.



Add permissions Info

Permissions policies (Selected 1/801) Info

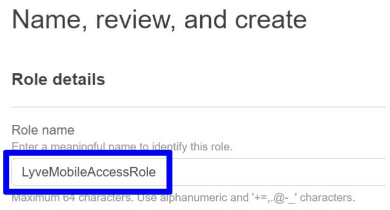
Choose one or more policies to attach to your new role.

☑	Policy name	Type	Description
☑	⊞ LyveMobileAccessPolicy	Customer managed	

Set permissions boundary - *optional* Info

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

9. On the **Name, review, and create** page, enter a **Role name**, for example,LyveMobileAccessRole.



Name, review, and create

Role details

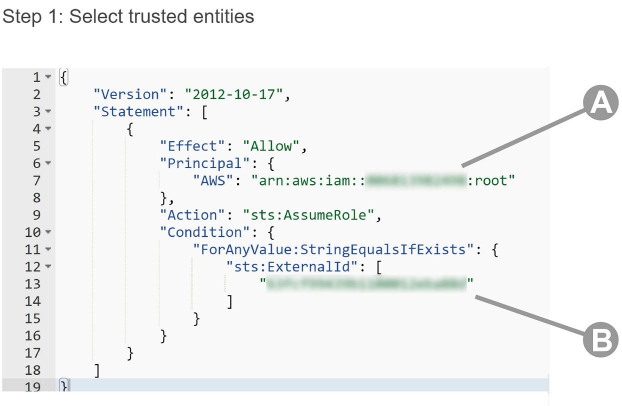
Role name

Enter a meaningful name to identify this role.

LyveMobileAccessRole

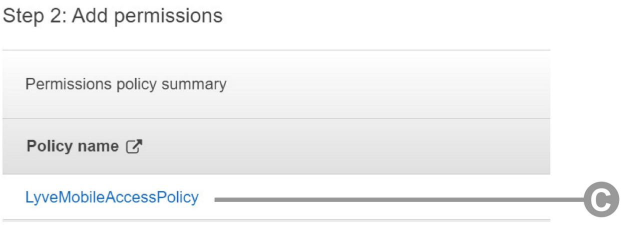
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

10. Review the trusted entity and permissions information:



Step 1: Select trusted entities

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::[redacted]:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ForAnyValue:StringEqualsIfExists": {
                    "sts:ExternalId": [
                        "[redacted]"
                    ]
                }
            }
        }
    ]
}
```



Step 2: Add permissions

Permissions policy summary

Policy name
LyveMobileAccessPolicy

Ensure the following

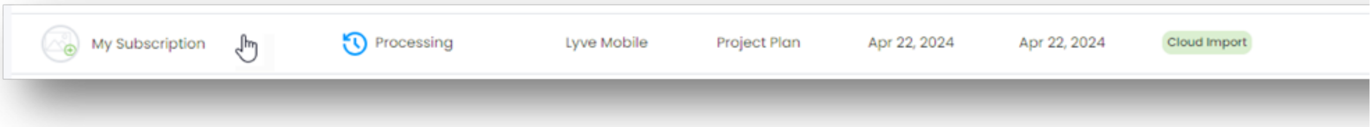
A. “AWS” is paired with the value you copied for Lyve’s S3 Account ID.
B. “sts:ExternalID” is paired with the value you copied for External ID.
C. The **Policy name** is the **LyveMobileAccessPolicy** you created earlier.

Configure your import plan

After you’ve completed the prerequisites above**,** return to Lyve Management Portal and enter your access details.

> You must successfully validate your access details and submit your plan before your return shipping label(s) are available for you to download.

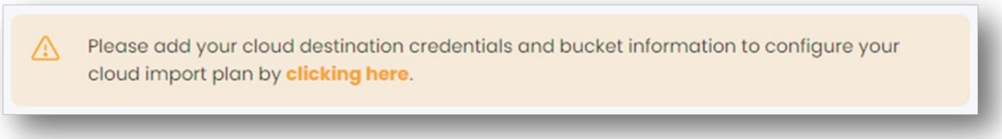
1. On your Home page, select a Lyve Mobile service subscription that includes a Cloud Import plan.



My Subscription	Processing	Lyve Mobile	Project Plan	Apr 22, 2024	Apr 22, 2024	Cloud Import

Alternatively, select the More icon in the 'Actions' column, and then select **View Subscription**.

2. Select **Import Plans** in the sidebar, or select the link at the top of the page:


⚠ Please add your cloud destination credentials and bucket information to configure your cloud import plan by **clicking here**.

3. Select the **+ Credentials** button in the upper right corner of the page.
4. Confirm your AWS S3 cloud destination and region, and then select **Next**.
5. Enter your Account ID and specify an existing bucket for the subscription. Select **Validate Credentials**.

> If the validation fails, check that the Account ID and Bucket entered are accurate, and then revalidate.

6. (Optional) Under 'Customized Path', provide the name of an existing folder or provide a folder name for Seagate to use to create a new folder for import. If you don’t provide a folder name, Seagate will create a folder based on the device serial number and date.

> Each storage device in your import plan will have a designated folder in your bucket. The device’s serial number will be automatically appended to the folder name at the time of import.
>
> - Provide a name for Seagate to use to create the folder(s) in your bucket on your behalf. (**Recommended**)
> - If you leave this field blank, Seagate will create a folder(s) for your files and will use the device’s serial number as its name.
> - Alternatively, if you have an existing folder within your bucket that you would like to import your files to, provide the name of this folder.
> - **Important**—Make sure that your bucket policy does not block folder creation. If you are providing a name for a new folder to be created, ensure that the name follows the Naming Guidelines.

7. To enable the checkbox, select the **IP Address Access Guide** link.
8. Check the checkbox, and then select **Submit**.

Inviting another user to configure an import plan

If a different member of your Org needs to configure the import plan for a Lyve Mobile subscription, you can invite them to do so in Lyve Management Portal.

- The person must be a member of the Org containing the Lyve Mobile subscription to which you want to add the import plan. See Manage Org members in the Lyve Management Portal User Manual.
- The member must be given the Manage Import Plans permission. See Manage subscription members in the Lyve Management Portal User Manual.

Naming guidelines

> ! Folder names cannot contain forward slash / characters.

Safe characters	
Alphanumeric characters	
0-9	numerals
a-z	lowercase letters
A-Z	uppercase letters
Special characters	
*	asterisk
!	exclamation point
-	hyphen
(	parenthesis (open)
)	parenthesis (close)
.	period
'	single quote
_	underscore

Characters to avoid	
&	ampersand
	ASCII characters • ASCII ranges 00–1F hex (0–31 decimal) and 7F (127 decimal) • non-printable ASCII (128–255 decimal characters)
@	at sign
\	backslash
^	caret

:	colon
,	comma
{	curly brace (left)
}	curly brace (right)
$	dollar sign
=	equal sign
/	forward slash
`	grave
<	greater-than symbol
>	less-than symbol
%	percent sign
|	pipe or vertical bar
+	plus sign
#	pound character
?	question mark
"	quotation mark
;	semi-colon
	space - sequences with spaces, especially multiple spaces, may be lost
[	square bracket (left)
]	square bracket (right)

Best practices

See the following knowledge base articles:

- Best practices for managing AWS access keys
- Security Best Practices for Amazon S3
- Access control best practices
- Creating Amazon S3 backups
- Restoring S3 data

Troubleshooting

See the following knowledge base article:

- Troubleshooting

Import to Google Cloud Storage

Prerequisites

Before you can configure and submit your import plan, make sure to complete the following steps so that Lyve Import Service can securely access your specified Google Cloud Storage bucket to import your data:

Google Cloud subscription—Set up an Google Cloud account.

Google Cloud project—Set up a Google Cloud project. To learn more, seeCreating and managing projects. Note—Make sure that billing is enabled for your Cloud project. To learn more, see Verify the billing status of your projects.

Google Cloud Storage bucket—Set up a dedicated bucket for your import. To learn more, see Create buckets.

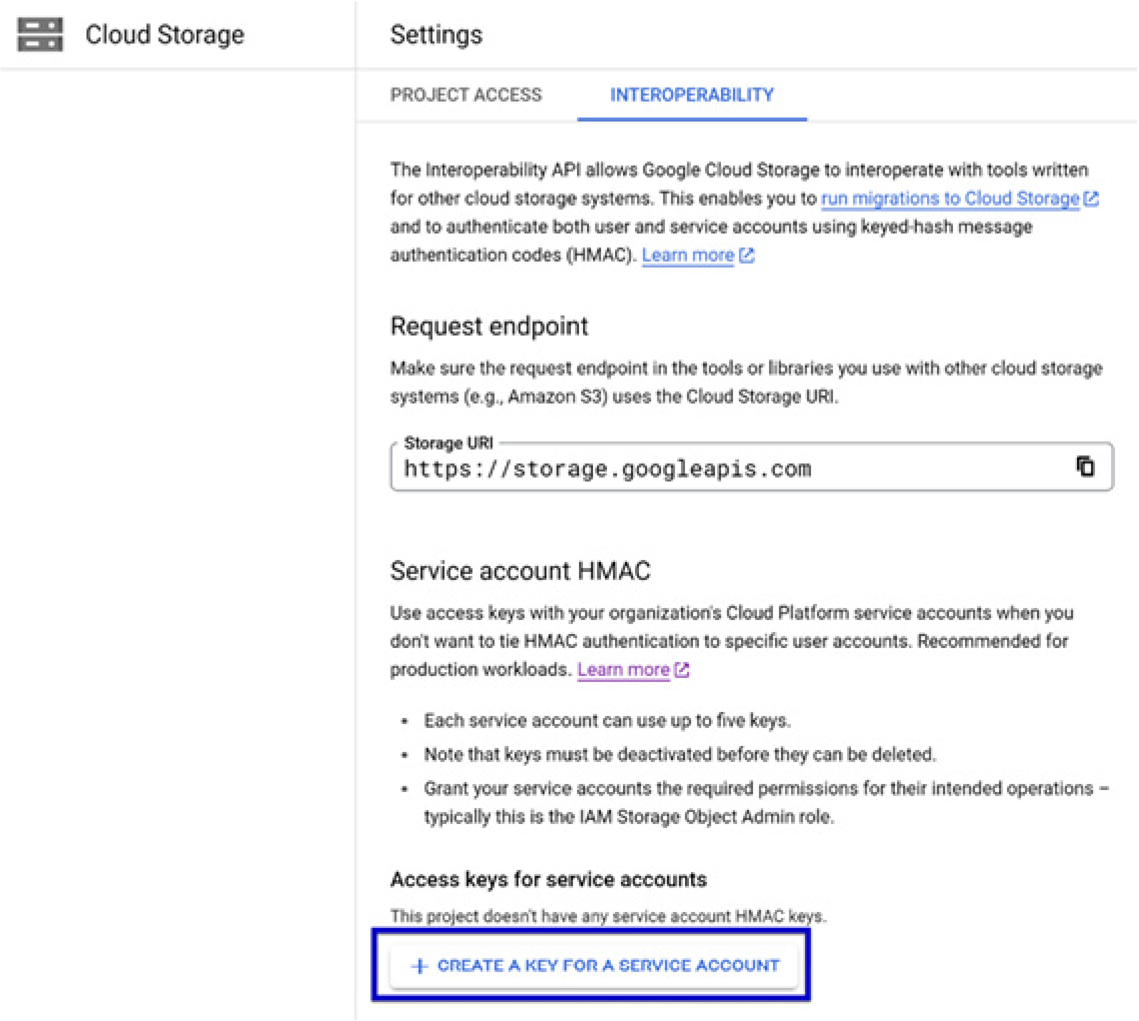
IP address access—If configured by your organization, list Seagate's IP address(es) as an allowed source. See IP Address Access.

Seagate authorizations—See below.

Seagate authorizations

Seagate requires permissions to read, write, and list to your bucket to perform the import. Hash-based message authentication code (HMAC) keys using an Access ID and Secret are required to authenticate requests to your cloud resources. To generate the HMAC keys, follow the steps below after creating your bucket:

1. Using the Google Cloud console, go to the Cloud Storage**Buckets** page and click**Settings**.
2. Click the **Interoperability** tab. Click **Create A Key For A Service Account**.



The Interoperability API allows Google Cloud Storage to interoperate with tools written for other cloud storage systems. This enables you to run migrations to Cloud Storage and to authenticate both user and service accounts using keyed-hash message authentication codes (HMAC). Learn more

Request endpoint

Make sure the request endpoint in the tools or libraries you use with other cloud storage systems (e.g., Amazon S3) uses the Cloud Storage URI.

Storage URI: `https://storage.googleapis.com`

Service account HMAC

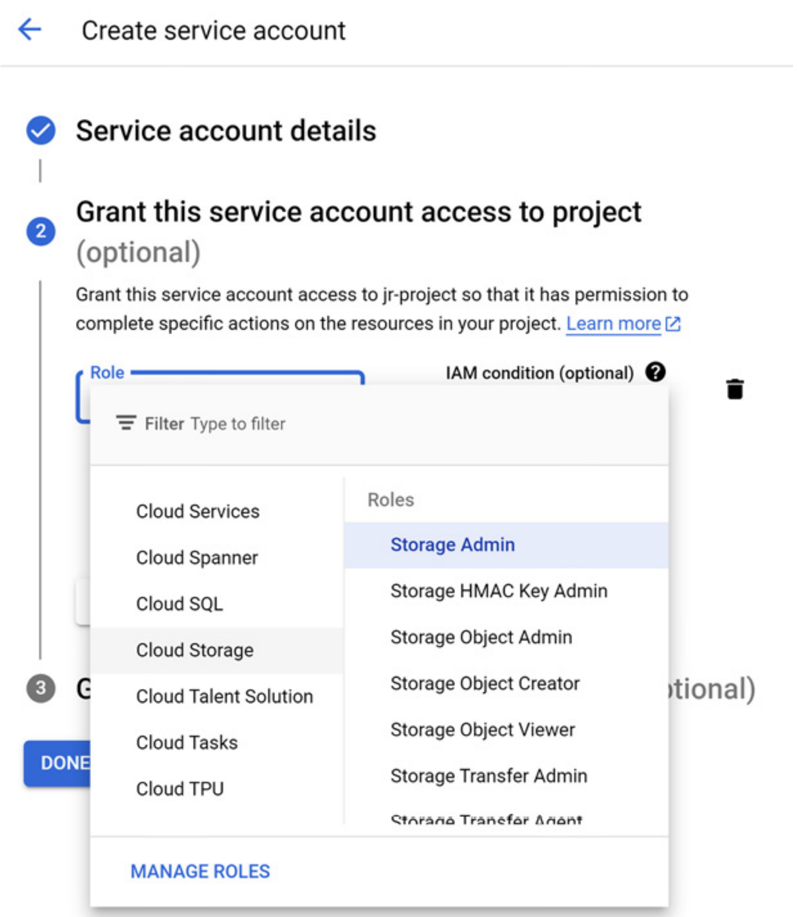
Use access keys with your organization's Cloud Platform service accounts when you don't want to tie HMAC authentication to specific user accounts. Recommended for production workloads. Learn more

- Each service account can use up to five keys.
- Note that keys must be deactivated before they can be deleted.
- Grant your service accounts the required permissions for their intended operations – typically this is the IAM Storage Object Admin role.

Access keys for service accounts

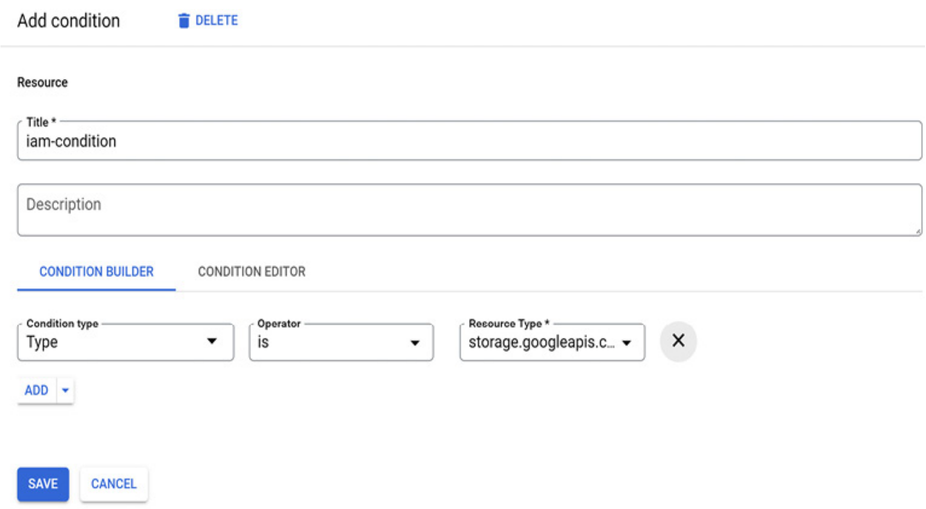
This project doesn't have any service account HMAC keys.

3. Select the service account you want the HMAC key to be associated with, or clicl**Create New Account** to create a new service account.
4. If creating a new service account, select**Storage Admin** for the role.



Grant this service account access to jr-project so that it has permission to complete specific actions on the resources in your project. Learn more

5. Add an IAM condition with the following selections:
   - **Condition type** = Type
   - **Operator** = is
   - **Resource Type** = storage.googleapis.com/Bucket.



Title * iam-condition

Description

Condition type: Type

Operator: is

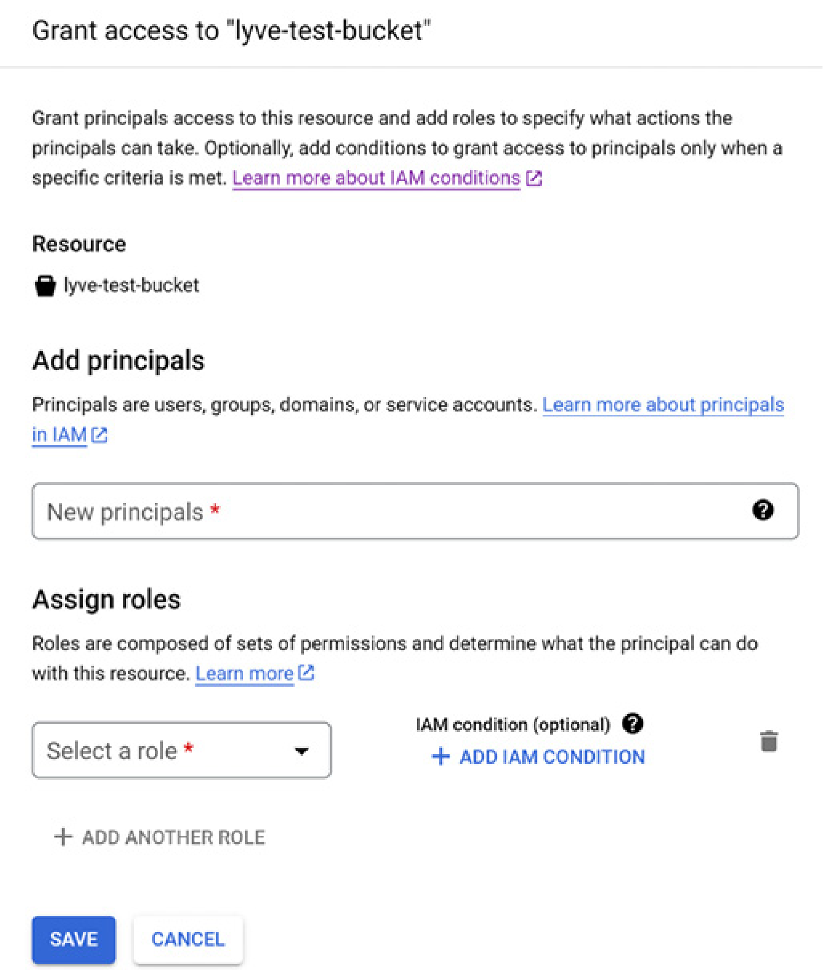
Resource Type *: storage.googleapis.c...

Click **Save**.

6. Record the service account HMAC key.
7. Navigate to the Cloud Storage **Buckets** page and locate the bucket to which you want to assign access for your import. Click the Bucket overflow menu ⋮) and select **Edit Access**.
8. Click **Add Principal**.
9. Enter the email address of the service account the HMAC keys are associated with**Note**—You can

find the service account email in the IAM console.

10. Select the **Storage Admin** role and click **Save**.



Grant access to "lyve-test-bucket"

Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. Learn more about IAM conditions

Resource

lyve-test-bucket

Add principals

Principals are users, groups, domains, or service accounts. Learn more about principals in IAM

New principals *

Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. Learn more

Select a role *

IAM condition (optional)

> To learn more, see HMAC keys.

Recommendations

Seagate **strongly** recommends the following best practices:

- Create a bucket dedicated to your import plan.
- When creating your bucket, select “Region” for location type.
- Block all public access for your bucket.
- Disable or delete the HMAC key after the import plan has ended.

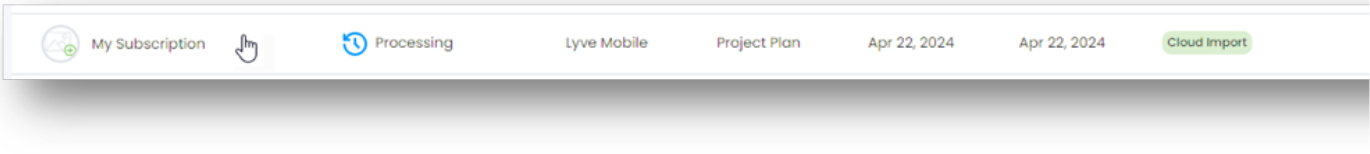
> **Important note on file sizes**—In general, Seagate does not recommend importing individual files larger than 5TB. Please refer to your cloud provider’s file size limitations and best practices.

Configure your import plan

Add your cloud destination credentials and bucket information to configure your cloud import plan.

- All devices within a subscription must be imported to the same destination and region.
- You will be required to enter and validate your bucket credentials.

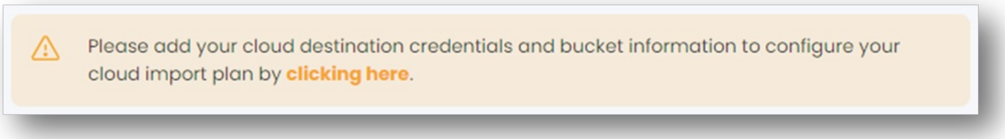
1. On your Home page, select a Lyve Mobile service subscription that includes a Cloud Import plan.



My Subscription	Processing	Lyve Mobile	Project Plan	Apr 22, 2024	Apr 22, 2024	Cloud Import

Alternatively, select the More icon in the 'Actions' column, and then select **View Subscription**.

2. Select the link at the top of the page:



Please add your cloud destination credentials and bucket information to configure your cloud import plan by **clicking here**.

3. Confirm the Cloud Destination and Region. Select**Next**.
4. Add the Access ID and Secret for your cloud destination. Specify an existing bucket for the subscription. Select **Validate Credentials** .

> If the validation fails, check that the Access ID, Secret, and Bucket entered are accurate, and then revalidate.

5. (Optional) Under 'Customized Path', provide the name of an existing folder or provide a folder name for Seagate to use to create a new folder for import. If you don't provide a folder name, Seagate will create a folder based on the device serial number and date.

Each storage device in your import plan will have a designated folder in your bucket. The device's serial number will be automatically appended to the folder name at the time of import.

- Provide a name for Seagate to use to create the folder(s) in your bucket on your behalf. (**Recommended**)
- If you leave this field blank, Seagate will create a folder(s) for your files and will use the device's serial number as its name.
- Alternatively, if you have an existing folder within your bucket that you would like to import your files to, provide the name of this folder.
- **Important**—Make sure that your bucket policy does not block folder creation. If you are providing a name for a new folder to be created, ensure that the name follows the Naming Guidelines.

6. To enable the checkbox, select the**IP Address Access Guide** link.
7. Select the checkbox, and then select**Submit**.

Inviting another user to configure an import plan

If a different member of your Org needs to configure the import plan for a Lyve Mobile subscription, you can invite them to do so in Lyve Management Portal.

- The person must be a member of the Org containing the Lyve Mobile subscription to which you want to add the import plan. SeeManage Org members in the Lyve Management Portal User Manual.
- The member must be given the Manage Import Plans permission. SeeManage subscription members in the Lyve Management Portal User Manual.

Naming guidelines

Bucket naming guidelines:

- Bucket names can only contain lowercase letters, numeric characters, dashes-, underscores _, and dots .. Spaces are not allowed. Names containing dots require verification.
- Bucket names must start and end with a number or letter.
- Bucket names must contain 3-63 characters. Names containing dots can contain up to 222 characters, but each dot-separated component can be no longer than 63 characters.
- Bucket names cannot be represented as an IP address in dotted-decimal notation (for example, 192.168.5.4).
- Bucket names cannot begin with thegoog prefix.
- Bucket names cannot contain google or close misspellings, such asg00gle.

Object naming guidelines:

- Object names can contain any sequence of valid Unicode characters, of length 1-1024 bytes when UTF-8 encoded.
- Object names cannot contain Carriage Return or Line Feed characters.

- Object names cannot start with .well-known/acme-challenge/.
- Objects cannot be named . or .. .

Avoid the Following in Object Names:

- Control characters that are illegal in XML 1.0 (#x7F–#x84 and #x86–#x9F): these characters cause XML listing issues when you try to list your objects.
- The # character: Google Cloud CLI commands interpret object names ending with #<numeric string> as version identifiers, so including # in object names can make it difficult or impossible to perform operations on such versioned objects using the gcloud CLI.
- The [,] , * , or ? characters: gcloud storage and gsutil interpret these characters as wildcards, so including them in object names can make it difficult or impossible to perform wildcard operations with those tools.
- Sensitive or personally identifiable information (PII): object names are more broadly visible than object data. For example, object names appear in URLs for the object and when listing objects in a bucket.

To learn more, see Object Naming Requirements.

Best practices

See the following knowledge base article:

- Best Practices for Cloud Storage

Troubleshooting

See the following knowledge base articles:

- Support
- Resources

Import to IBM Cloud

Prerequisites

Before you can configure and submit your import plan, make sure to complete the following steps so that Lyve Import Service can securely access your specified IBM Cloud bucket to import your data:

IBM Cloud subscription—Set up an IBM Cloud Platform account.

Object Storage instance—Set up a storage instance. To learn more, seeChoosing a plan and creating an instance.

IBM Cloud bucket— Set up a dedicated bucket for your import. To learn more, seeCreate some buckets to store your data.

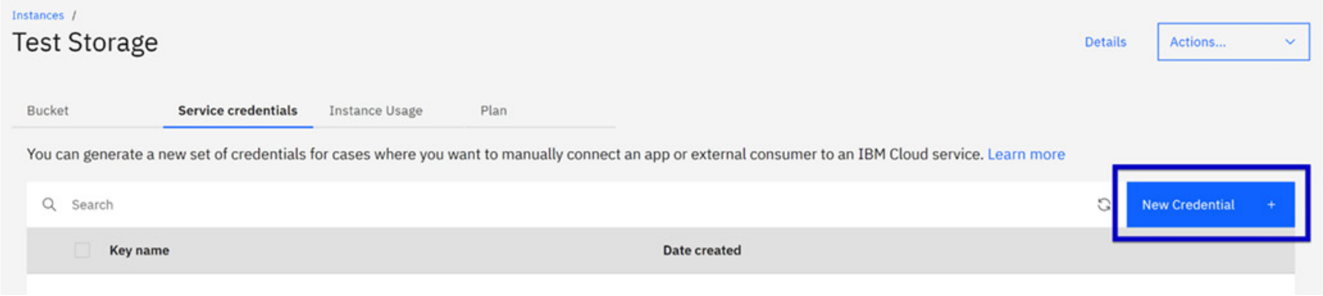
IP address access—If configured by your organization, list Seagate's IP address(es) as an allowed source. See IP Address Access.

Seagate authorizations—See below.

Seagate authorizations

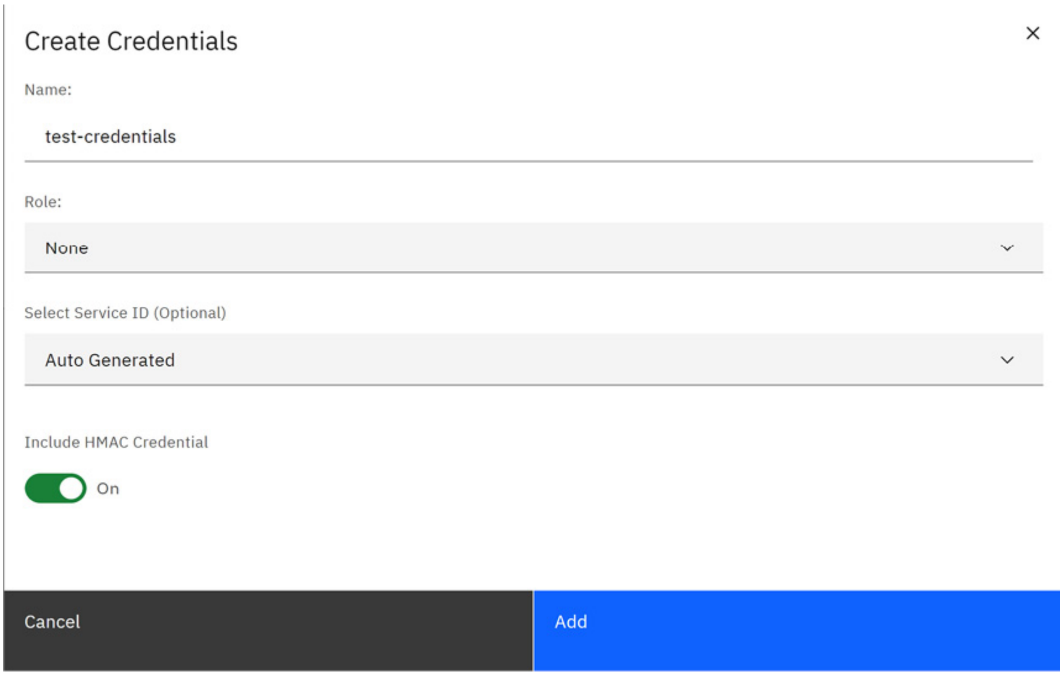
Seagate requires permissions to read, write, and list to your bucket to perform the import. Hash-based message authentication code (HMAC) keys using an Access Key ID and Secret Access Key are required to authenticate requests to your cloud resources. To generate the HMAC keys, follow the steps below after creating your bucket:

1. In your Object Storage instance, click the**Service credentials** tab.
2. Click the **New Credential** button.



You can generate a new set of credentials for cases where you want to manually connect an app or external consumer to an IBM Cloud service. Learn more

3. Name the credential and make the following selections:
   - **Role** = None
   - **Service ID** = Auto Generated
   - **Include HMAC Credential** = On



Create Credentials

Name: test-credentials

Role: None

Select Service ID (Optional): Auto Generated

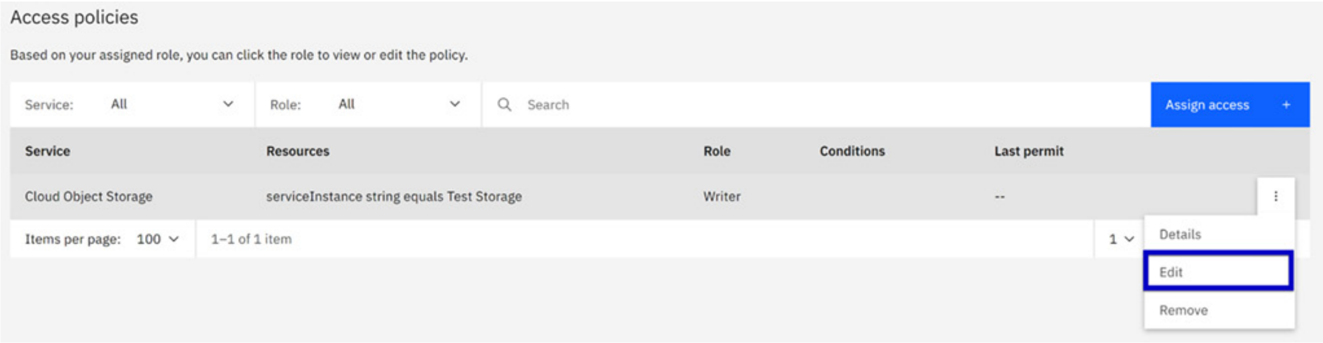
Include HMAC Credential: On

Click the **Add** button. Once added, you can expand the credentials to view the values for the Access Key ID and Secret Access Key.

> When these credentials are created, the underlying service ID has access to any bucket in your instance (if it was automatically generated). To limit access to a specific bucket or subset of buckets, you will need to edit the access policy of the service ID tied to these credentials.

Proceed through the steps below to edit the access policy for the service ID:

1. Navigate to the IAM console by clicking**Manage > Access (IAM)**. Click **Service IDs** in the side panel. Click on the service ID you want to edit.
2. Under **Access policies**, locate the role with the access policy you want to edit. Click the**Actions** icon and select **Edit**.



Access policies

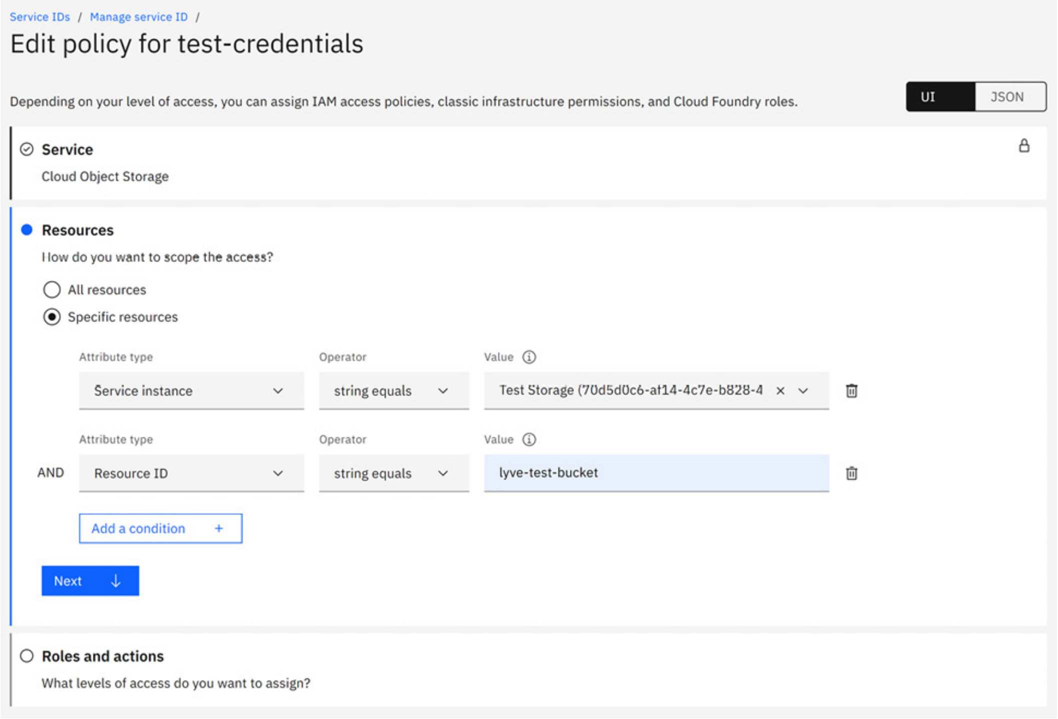
Based on your assigned role, you can click the role to view or edit the policy.

Service: All Role: All

Service	Resources	Role	Conditions	Last permit
Cloud Object Storage	serviceInstance string equals Test Storage	Writer		--

Items per page: 100 1–1 of 1 item 1

3. Click on the **Resources** tab and select **Edit**. Select **Specific resources** and add conditions to scope access to specific resources.


Service IDs / Manage service ID /

Edit policy for test-credentials

Depending on your level of access, you can assign IAM access policies, classic infrastructure permissions, and Cloud Foundry roles.

Service

Cloud Object Storage

Resources

How do you want to scope the access?

○ All resources

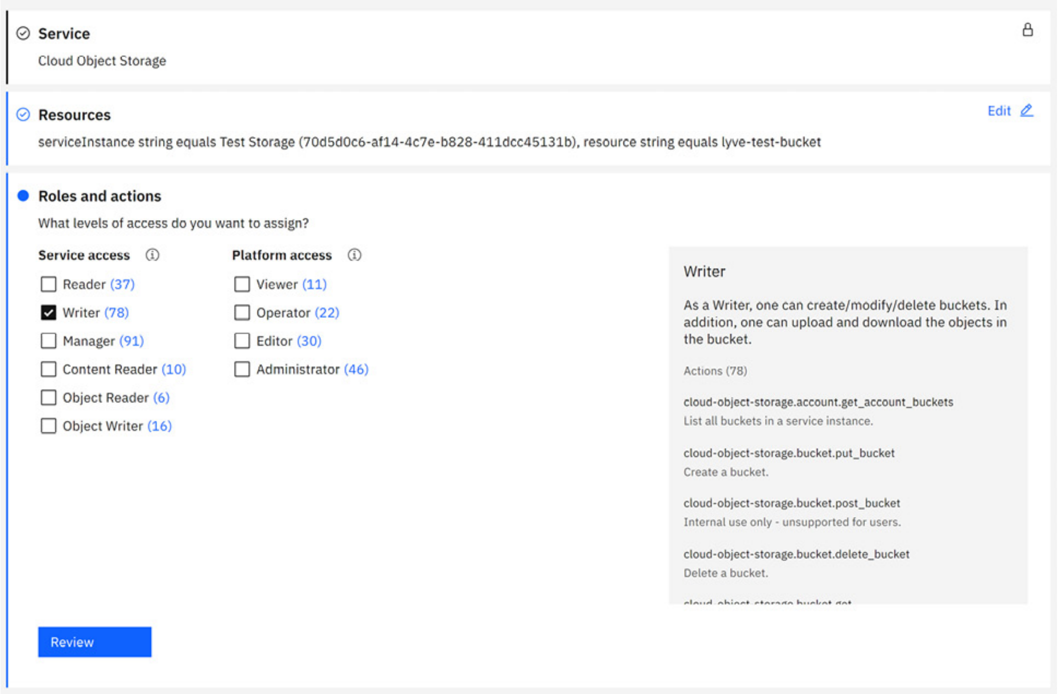
● Specific resources

	Attribute type	Operator	Value
	Service instance	string equals	Test Storage (70d5d0c6-af14-4c7e-b828-4
AND	Resource ID	string equals	lyve-test-bucket

Roles and actions

What levels of access do you want to assign?

4. Click **Next** to continue to the **Roles and actions** tab. In the **Service access** column, assign the **Writer** role. Click **Review**.


Service

Cloud Object Storage

Resources

serviceInstance string equals Test Storage (70d5d0c6-af14-4c7e-b828-411dcc45131b), resource string equals lyve-test-bucket

Roles and actions

What levels of access do you want to assign?

Service access	Platform access
□ Reader (37)	□ Viewer (11)
☑ Writer (78)	□ Operator (22)
□ Manager (91)	□ Editor (30)
□ Content Reader (10)	□ Administrator (46)
□ Object Reader (6)	
□ Object Writer (16)	

Writer

As a Writer, one can create/modify/delete buckets. In addition, one can upload and download the objects in the bucket.

Actions (78)

cloud-object-storage.account.get_account_buckets
List all buckets in a service instance.

cloud-object-storage.bucket.put_bucket
Create a bucket.

cloud-object-storage.bucket.post_bucket
Internal use only - unsupported for users.

cloud-object-storage.bucket.delete_bucket
Delete a bucket.

5. Click **Save**.

> **i** To learn more, see Assigning access to an individual bucket.

Recommendations

Seagate **strongly** recommends the following best practices:

- Create a bucket dedicated to your import plan.
- When creating your bucket, select “Regional” for resiliency.
- Block all public access for your bucket.
- Disable or delete the HMAC key after the import plan has ended.

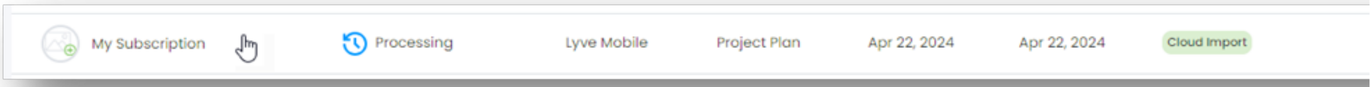
> **Important note on file sizes**—In general, Seagate does not recommend importing individual files larger than 5TB. Please refer to your cloud provider’s file size limitations and best practices.

Configure your import plan

Add your cloud destination credentials and bucket information to configure your cloud import plan.

- All devices within a subscription must be imported to the same destination and region.
- You will be required to enter and validate your bucket credentials.

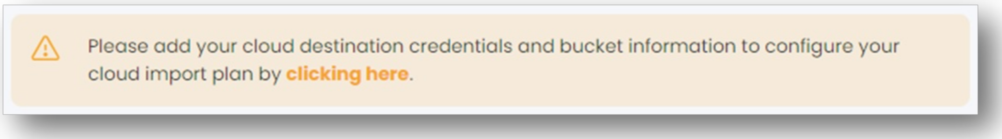
1. On your Home page, select a Lyve Mobile service subscription that includes a Cloud Import plan.



My Subscription	Processing	Lyve Mobile	Project Plan	Apr 22, 2024	Apr 22, 2024	Cloud Import

Alternatively, select the More icon in the 'Actions' column, and then select **View Subscription**.

2. Select the link at the top of the page:



⚠ Please add your cloud destination credentials and bucket information to configure your cloud import plan by **clicking here**.

3. Confirm the Cloud Destination and Region. Select**Next**.
4. Add the Access Key ID and Secret Access Key for your cloud destination. Specify an existing bucket for the subscription. Select**Validate Credentials** .

> If the validation fails, check that the Access Key ID, Secret Access Key, and Bucket entered are accurate, and then revalidate.

5. (Optional) Under 'Customized Path', provide the name of an existing folder or provide a folder name for Seagate to use to create a new folder for import. If you don’t provide a folder name, Seagate will create a folder based on the device serial number and date.

Each storage device in your import plan will have a designated folder in your bucket. The device’s serial number will be automatically appended to the folder name at the time of import.

- Provide a name for Seagate to use to create the folder(s) in your bucket on your behalf. (**Recommended**)
- If you leave this field blank, Seagate will create a folder(s) for your files and will use the device’s serial number as its name.
- Alternatively, if you have an existing folder within your bucket that you would like to import your files to, provide the name of this folder.
- **Important**—Make sure that your bucket policy does not block folder creation. If you are providing a name for a new folder to be created, ensure that the name follows the Naming Guidelines.

6. To enable the checkbox, select the**IP Address Access Guide** link.
7. Select the checkbox, and then select**Submit**.

Inviting another user to configure an import plan

If a different member of your Org needs to configure the import plan for a Lyve Mobile subscription, you can invite them to do so in Lyve Management Portal.

- The person must be a member of the Org containing the Lyve Mobile subscription to which you want to add the import plan. SeeManage Org members in the Lyve Management Portal User Manual.
- The member must be given the Manage Import Plans permission. SeeManage subscription members in the Lyve Management Portal User Manual.

Naming guidelines

Bucket naming guidelines:

- Must be unique across the whole IBM Cloud Object Storage system.
- Do not use any personal information (any part of a name, address, financial or security accounts or SSN)
- Must start and end in alphanumeric characters (3 to 63)
- Characters allowed: lowercase, numbers and nonconsecutive dots and hyphens
- Avoid using these characters: / \ “ ? < > 1 . This will not cause issues with IBM Cloud Object Storage but may cause issues with your applications.

Object naming guidelines:

- Object keys can be up to 1024 characters in length, and it’s best to avoid any characters that might be problematic in a web address. For example,? , = , < , and other special characters might cause unwanted behavior if not URL-encoded.

Troubleshooting

See the following knowledge base articles:

- FAQ
- Support

Import to Microsoft Azure Blob Storage

Prerequisites

Before you can configure and submit your import plan, make sure to complete the following steps so that Lyve Import Service can securely access your specified Azure container to import your data:

Azure subscription—Set up an Azure free account.

Azure storage account—Set up an Azure storage account. To learn more, see Create an Azure storage account.

Azure container—Set up a dedicated container for your import. To learn more, see Create a container.

Seagate authorizations—Ensure that Seagate is authorized to read, write, and list to an existing container.

IP address access—If configured by your organization, list Seagate's IP address(es) as an allowed source. See IP Address Access.

Additionally, see How to configure the Azure Storage Firewall.

Recommendations

Seagate recommends creating a container dedicated to your import plan.

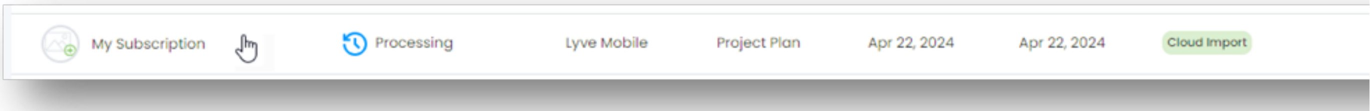
> i **Important note on file sizes**—In general, Seagate does not recommend importing individual files larger than 5TB. Please refer to your cloud provider's file size limitations and best practices.

Configure your import plan

Add your cloud destination credentials and container information to configure your cloud import plan.

- All devices within a subscription must be imported to the same destination and region.
- You will be required to enter and validate your container credentials.

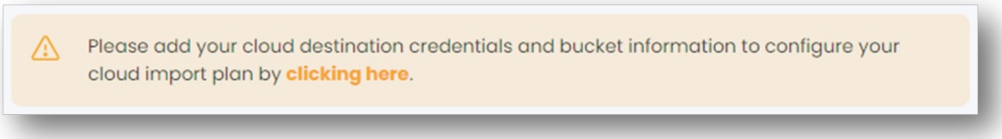
1. On your Home page, select a Lyve Mobile service subscription that includes a Cloud Import plan.



My Subscription	Processing	Lyve Mobile	Project Plan	Apr 22, 2024	Apr 22, 2024	Cloud Import

Alternatively, select the More icon in the 'Actions' column, and then select **View Subscription**.

2. Select the link at the top of the page:



Please add your cloud destination credentials and bucket information to configure your cloud import plan by **clicking here**.

3. Confirm the Cloud Destination and Region. Select**Next**.
4. Add the Storage Account Name and Storage Account Key for your cloud destination. Specify an existing container for the subscription. Select**Validate Credentials** .

> If the validation fails, check that the Storage Account Name, Storage Account Key, and Container entered are accurate, and then revalidate.

5. (Optional) Under 'Customized Path', provide the name of an existing folder or provide a folder name for Seagate to use to create a new folder for import. If you don't provide a folder name, Seagate will create a folder based on the device serial number and date.

> Each storage device in your import plan will have a designated folder in your container. The device's serial number will be automatically appended to the folder name at the time of import.
>
> - Provide a name for Seagate to use to create the folder(s) in your container on your behalf. (**Recommended**)
> - If you leave this field blank, Seagate will create a folder(s) for your files and will use the device's serial number as its name.
> - Alternatively, if you have an existing folder within your container that you would like to import your files to, provide the name of this folder.
> - **Important**—Make sure that your container policy does not block folder creation. If you are providing a name for a new folder to be created, ensure that the name follows the Naming Guidelines.

6. To enable the checkbox, select the**IP Address Access Guide** link.
7. Select the checkbox, and then select**Submit**.

Inviting another user to configure an import plan

If a different member of your Org needs to configure the import plan for a Lyve Mobile subscription, you can invite them to do so in Lyve Management Portal.

- The person must be a member of the Org containing the Lyve Mobile subscription to which you want to add the import plan. SeeManage Org members in the Lyve Management Portal User Manual.
- The member must be given the Manage Import Plans permission. SeeManage subscription members in the Lyve Management Portal User Manual.

Naming guidelines

Note the following naming guidelines:

- Every folder within a container must have a unique name.
- A folder name can contain any combination of characters.
- For blobs in Azure Storage, a folder name must be at least one character long and cannot be more than 1,024 characters long.
- Folder names are case-sensitive.
- Reserved URL characters must be properly escaped.
- Avoid folder names that end with a dot `.` , a forward slash `/` , or a sequence or combination of the two.

For additional information on naming folders, see Naming and Referencing Containers, Blobs, and Metadata.

Best practices

See the following knowledge base articles:

- Security recommendations for Blob storage
- Best practices for monitoring Azure Blob Storage

Troubleshooting

See the following knowledge base articles:

- Monitor, diagnose, and troubleshoot Microsoft Azure Storage
- Troubleshoot Azure RBAC
- Azure Blob Storage FAQ
- Microsoft Q&A question page
- Azure Storage on Stack Overflow

Import to OVHcloud

Prerequisites

Before you can configure and submit your import plan, make sure to complete the following steps so that Lyve Import Service can securely access your specified OVHcloud container to import your data:

OVHcloud subscription—Set up an OVHcloud account.

OVH Public Cloud project—Set up a OVHcloud Public Cloud project. To learn more, seeCreating your first OVHcloud Public Cloud project.

OVHcloud container—Set up a dedicated object container for your import. To learn more, see Object Storage - Creating a bucket.

OVHcloud Public Cloud instance—Set up an instance. To learn more, see Creating an instance.

IP address access—If configured by your organization, list Seagate's IP address(es) as an allowed source. See IP Address Access.

Seagate authorizations—Seagate requires permissions to read, write, and list to your container to perform the import. Hash-based message authentication code (HMAC) keys using an Access Key and Secret Access Key are required to authenticate requests to your cloud resources. To generate the HMAC keys, select an existing user or create a new user to link to your container. Set Read and write access to your container for this user. Once the user has been created and added to your container, you will see the credentials.

To learn more, see Object Storage - Identity and access management.

Recommendations

Seagate **strongly** recommends the following best practices:

- Create a container dedicated to your import plan.
- Block all public access for your container.
- Disable or delete the HMAC key after the import plan has ended.

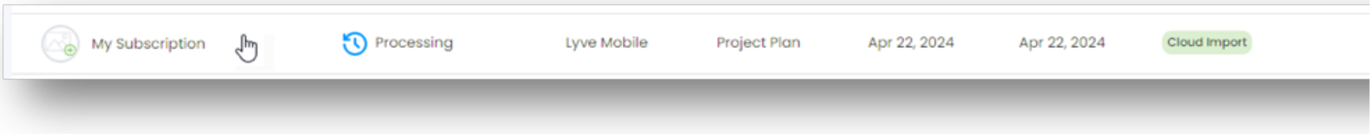
Important note on file sizes—In general, Seagate does not recommend importing individual files larger than 5TB. Please refer to your cloud provider's file size limitations and best practices.

Configure your import plan

Add your cloud destination credentials and bucket information to configure your cloud import plan.

- All devices within a subscription must be imported to the same destination and region.
- You will be required to enter and validate your bucket credentials.

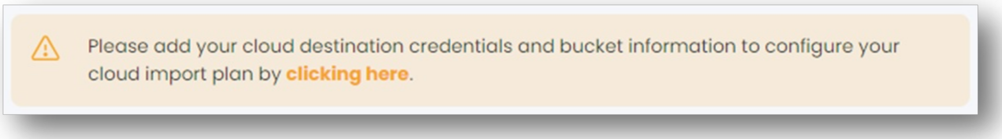
1. On your Home page, select a Lyve Mobile service subscription that includes a Cloud Import plan.



My Subscription	Processing	Lyve Mobile	Project Plan	Apr 22, 2024	Apr 22, 2024	Cloud Import

Alternatively, select the More icon in the 'Actions' column, and then select **View Subscription**.

2. Select the link at the top of the page:



Please add your cloud destination credentials and bucket information to configure your cloud import plan by **clicking here**.

3. Confirm the Cloud Destination and Region. Select**Next**.
4. Add the Access Key and Secret Access Key for your cloud destination. Specify an existing container for the subscription. Select**Validate Credentials** .

If the validation fails, check that the Access Key, Secret Access Key, and Container entered are accurate, and then revalidate.

5. (Optional) Under 'Customized Path', provide the name of an existing folder or provide a folder name for Seagate to use to create a new folder for import. If you don't provide a folder name, Seagate will create a folder based on the device serial number and date.

> Each storage device in your import plan will have a designated folder in your container. The device’s serial number will be automatically appended to the folder name at the time of import.
>
> - Provide a name for Seagate to use to create the folder(s) in your container on your behalf. (**Recommended**)
> - If you leave this field blank, Seagate will create a folder(s) for your files and will use the device’s serial number as its name.
> - Alternatively, if you have an existing folder within your container that you would like to import your files to, provide the name of this folder.
> - **Important**—Make sure that your container policy does not block folder creation. If you are providing a name for a new folder to be created, ensure that the name follows the Naming Guidelines.

6. To enable the checkbox, select the**IP Address Access Guide** link.
7. Select the checkbox, and then select**Submit**.

Inviting another user to configure an import plan

If a different member of your Org needs to configure the import plan for a Lyve Mobile subscription, you can invite them to do so in Lyve Management Portal.

- The person must be a member of the Org containing the Lyve Mobile subscription to which you want to add the import plan. SeeManage Org members in the Lyve Management Portal User Manual.
- The member must be given the Manage Import Plans permission. SeeManage subscription members in the Lyve Management Portal User Manual.

Naming guidelines

Container naming guidelines:

- Must be between 3 and 63 characters long.
- Must begin and end with lower case alphanumeric characters (a to z and 0 to 9).
- Must be unique within the same OVHcloud region.
- May contain the following punctuation marks:. and - .
- Must not contain multiple punctuation marks in a row .. or -. or .- or --).
- Must not look like an IP address (for example, 192.168.1.1).

Best practices

See the following knowledge base article:

- Best practices

Troubleshooting

See the following knowledge base articles:

- Object Storage - Technical Limitations
- FAQ Public Cloud OVHcloud

Import to Seagate Lyve Cloud

Prerequisites

Before you can configure and submit your import plan, make sure to complete the following steps so that Lyve Import Service can securely access your specified Lyve Cloud bucket to import your data:

Lyve Cloud account—Work directly with a Lyve Cloud Expert to create your Lyve Cloud account.

Lyve Cloud bucket—Set up a bucket for your import. To learn more, seeManaging buckets.

Bucket permissions—To learn more, see Managing bucket access permissions.

Seagate authorizations—Ensure that Seagate is authorized to read, write, and list to an existing bucket.

Service account—To learn more, see Managing service accounts.

IP address access—If configured by your organization, list Seagate's IP address(es) as an allowed source. See IP Address Access.

Recommendations

Seagate recommends creating a bucket dedicated to your import plan.

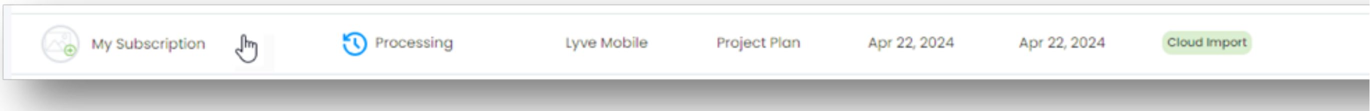
> i **Important note on file sizes**—In general, Seagate does not recommend importing individual files larger than 5TB. Please refer to your cloud provider's file size limitations and best practices.

Configure your import plan

Add your cloud destination credentials and bucket information to configure your cloud import plan.

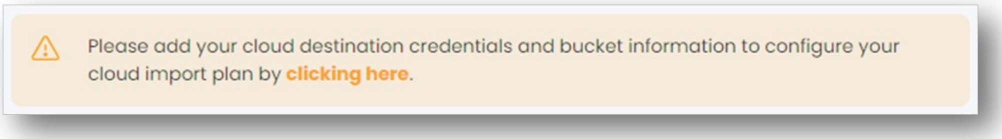
- All devices within a subscription must be imported to the same destination and region.
- You will be required to enter and validate your bucket credentials.

1. On your Home page, select a Lyve Mobile service subscription that includes a Cloud Import plan.


My Subscription | Processing | Lyve Mobile | Project Plan | Apr 22, 2024 | Apr 22, 2024 | Cloud Import

Alternatively, select the More icon in the 'Actions' column, and then select **View Subscription**.

2. Select the link at the top of the page:


Please add your cloud destination credentials and bucket information to configure your cloud import plan by **clicking here**.

3. Confirm the Cloud Destination and Region. Select**Next**.
4. Add the Access Key ID and Secret Access Key for your cloud destination. Specify an existing bucket for the subscription. Select**Validate Credentials** .

> **i** If the validation fails, check that the Access Key ID, Secret Access Key, and Bucket entered are accurate, and then revalidate.

5. (Optional) Under 'Customized Path', provide the name of an existing folder or provide a folder name for Seagate to use to create a new folder for import. If you don’t provide a folder name, Seagate will create a folder based on the device serial number and date.

> **i** Each storage device in your import plan will have a designated folder in your bucket. The device’s serial number will be automatically appended to the folder name at the time of import.
>
> - Provide a name for Seagate to use to create the folder(s) in your bucket on your behalf. (**Recommended**)
> - If you leave this field blank, Seagate will create a folder(s) for your files and will use the device’s serial number as its name.
> - Alternatively, if you have an existing folder within your bucket that you would like to import your files to, provide the name of this folder.
> - **Important**—Make sure that your bucket policy does not block folder creation. If you are providing a name for a new folder to be created, ensure that the name follows the Naming Guidelines.

6. To enable the checkbox, select the**IP Address Access Guide** link.
7. Select the checkbox, and then select**Submit**.

Inviting another user to configure an import plan

If a different member of your Org needs to configure the import plan for a Lyve Mobile subscription, you can invite them to do so in Lyve Management Portal.

- The person must be a member of the Org containing the Lyve Mobile subscription to which you want to add the import plan. SeeManage Org members in the Lyve Management Portal User Manual.
- The member must be given the Manage Import Plans permission. SeeManage subscription members in the Lyve Management Portal User Manual.

Naming guidelines

Safe characters	
Alphanumeric characters	
0-9	numerals
a-z	lowercase letters
A-Z	uppercase letters
Special characters	
*	asterisk
!	exclamation point
-	hyphen
(	parenthesis (open)
)	parenthesis (close)
.	period
'	single quote
_	underscore

Characters to avoid	
&	ampersand
	ASCII characters • ASCII ranges 00–1F hex (0–31 decimal) and 7F (127 decimal) • non-printable ASCII (128–255 decimal characters)

@	at sign
\	backslash
^	caret
:	colon
,	comma
{	curly brace (left)
}	curly brace (right)
$	dollar sign
=	equal sign
/	forward slash
`	grave
<	greater-than symbol
>	less-than symbol
%	percent sign
|	pipe or vertical bar
+	plus sign
#	pound character
?	question mark
"	quotation mark
;	semi-colon
	space - sequences with spaces, especially multiple spaces, may be lost
[	square bracket (left)
]	square bracket (right)

Note the following additional requirements:

- An object name matching a prefix is not supported. For example, an object with the name /A/B, where A is a prefix and B is the object name, should not be imported with another object named A.
- A standalone period `.` in the prefix folder is not supported.
- A standalone period `.` as an object name is not supported.

Best practices

See the following knowledge base article:

- Frequently asked Questions

Troubleshooting

See the following knowledge base articles:

- Troubleshooting Guide
- Release Notes

Import to Wasabi S3

Prerequisites

Before you can configure and submit your import plan, make sure to complete the following steps so that Lyve Import Service can securely access your specified Wasabi bucket to import your data:

Wasabi subscription—Set up a Wasabi account.

Wasabi bucket—Set up a dedicated bucket for your import. To learn more, seeWorking with Buckets and Objects.

IP address access—If configured by your organization, list Seagate's IP address(es) as an allowed source. See IP Address Access.

Seagate authorizations—See below.

Seagate authorizations

Seagate requires permissions to read, write, and list to your bucket to perform the import. Hash-based message authentication code (HMAC) keys using an Access Key ID and Secret Access Key are required to authenticate requests to your cloud resources. To generate the HMAC keys, follow the steps below after creating your bucket:

1. Using Wasabi's console, create a policy.
2. Copy the provided JSON script below to paste into your policy document:

```
{
 “Version”: “2012-10-17”,
 “Statement”: [
  {
   “Effect”: “Allow”,
   “Action”: “s3:*”,
   “Resource”: [
    “arn:aws:s3:::{yourbucketname}”,
    “arn:aws:s3:::{yourbucketname}/*”
   ]
   “Condition”:{}
  }
 ]
}
```

3. Replace {yourbucketname} with your actual S3 bucket name. Click**Create Policy**.
4. Create a user with programmatic access and attach the policy you created to this user. To learn more,

see Creating a User Account and Access Key.

5. Record the Access Key ID and Secret Access Key that are generated in a safe place.

Recommendations

Seagate **strongly** recommends the following best practices:

- Create a bucket dedicated to your import plan.
- Block all public access for your bucket.
- Disable or delete the HMAC key after the import plan has ended.

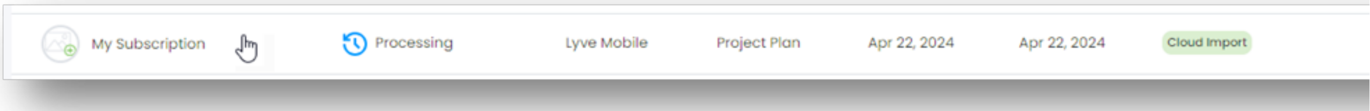
Important note on file sizes—In general, Seagate does not recommend importing individual files larger than 5TB. Please refer to your cloud provider's file size limitations and best practices.

Configure your import plan

Add your cloud destination credentials and bucket information to configure your cloud import plan.

- All devices within a subscription must be imported to the same destination and region.
- You will be required to enter and validate your bucket credentials.

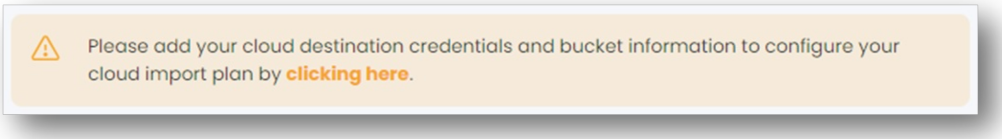
1. On your Home page, select a Lyve Mobile service subscription that includes a Cloud Import plan.



My Subscription	Processing	Lyve Mobile	Project Plan	Apr 22, 2024	Apr 22, 2024	Cloud Import

Alternatively, select the More icon in the 'Actions' column, and then select **View Subscription**.

2. Select the link at the top of the page:



Please add your cloud destination credentials and bucket information to configure your cloud import plan by **clicking here**.

3. Confirm the Cloud Destination and Region. Select**Next**.
4. Add the Access Key ID and Secret Access Key for your cloud destination. Specify an existing bucket for the subscription. Select**Validate Credentials** .

> i If the validation fails, check that the Access Key ID, Secret Access Key, and Bucket entered are accurate, and then revalidate.

5. (Optional) Under 'Customized Path', provide the name of an existing folder or provide a folder name for Seagate to use to create a new folder for import. If you don’t provide a folder name, Seagate will create a folder based on the device serial number and date.

> i Each storage device in your import plan will have a designated folder in your bucket. The device’s serial number will be automatically appended to the folder name at the time of import.
>
> - Provide a name for Seagate to use to create the folder(s) in your bucket on your behalf. (**Recommended**)
> - If you leave this field blank, Seagate will create a folder(s) for your files and will use the device’s serial number as its name.
> - Alternatively, if you have an existing folder within your bucket that you would like to import your files to, provide the name of this folder.
> - **Important**—Make sure that your bucket policy does not block folder creation. If you are providing a name for a new folder to be created, ensure that the name follows the Naming Guidelines.

6. To enable the checkbox, select the**IP Address Access Guide** link.
7. Select the checkbox, and then select**Submit**.

Inviting another user to configure an import plan

If a different member of your Org needs to configure the import plan for a Lyve Mobile subscription, you can invite them to do so in Lyve Management Portal.

- The person must be a member of the Org containing the Lyve Mobile subscription to which you want to add the import plan. SeeManage Org members in the Lyve Management Portal User Manual.
- The member must be given the Manage Import Plans permission. SeeManage subscription members in the Lyve Management Portal User Manual.

Naming guidelines

Bucket naming guidelines:

- The name must be unique across all existing bucket names in Wasabi.
- A bucket name must:
- Be a valid DNS-compliant name
- Begin with a lowercase letter or number, and
- Consist of 3 to 63 lowercase letters, numbers, periods, and/or dashes.
- The name cannot contain underscores, end with a dash, have consecutive periods, or use dashes

adjacent to periods.
- The name cannot be formatted as an IP address (for example, 123.45.678.90).

Characters to avoid:

- % (percent)
  < (less than symbol)
  > (greater than symbol)
  \ (backslash)
  # (pound sign)
  ? (question mark)
- Certain file names may have non-ASCII characters that are 4 byte UTF8 characters (such as emojis). Wasabi does not support these characters and will return a 400 error message to an application that tries to write a file with 4 byte UTF characters in the file name. We recommend renaming the affected files, if possible.

Troubleshooting

See the following knowledge base articles:

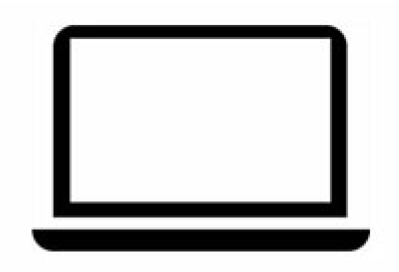
- FAQs
- Troubleshooting

Invite Another Member to Configure an Import Plan

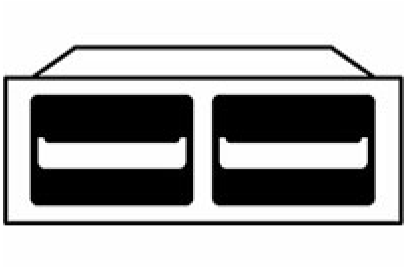
If a different member of your Org needs to configure the import plan for a Lyve Mobile subscription, you can invite them to do so in Lyve Management Portal.

- The person must be a member of the Org containing the Lyve Mobile subscription to which you want to add the import plan. SeeManage Org members in the Lyve Management Portal User Manual.
- The member must be given the Manage Import Plans permission. SeeManage subscription members in the Lyve Management Portal User Manual.

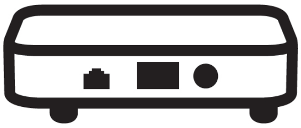
Move Data to a Lyve Mobile Array



Lyve Mobile Array can be used as direct-attached storage. See the Lyve Mobile Array user manual.



Lyve Mobile Array can also support connections via Fibre Channel, iSCSI and Serial Attached SCSI (SAS) connections using the Lyve Rackmount Receiver. For details, see the Lyve Rackmount Receiver user manual.



For high-speed mobile data transfers, connect Lyve Mobile Array using the Lyve Mobile PCIe Adapter. See the Lyve Mobile Mount and PCIe Adapter user manual or Lyve Mobile Mount and PCIe Adapter - Front Loader user manual.

Send a Lyve Mobile Array to a Seagate Import Site

Send your Lyve Mobile Array for cloud import after you have completed the following:

- Created a cloud import plan in Lyve Management Portal
- Configured the import plan with your cloud service credentials
- Moved data to your Lyve Mobile Array

See Return devices in the Lyve Management Portal User Manual.

Track Import Status

The status of your import plan(s) can be tracked in Lyve Management Portal.

1. Go to lyve.seagate.com and sign in. Enter a verification code to continue to Lyve Management Portal.
2. On the Home page, select an active Lyve Mobile subscription with a cloud import plan. (Alternatively, select the More icon in the 'Actions' column, and then select **View Subscription**).
3. In the sidebar, select **Import Plans**.
4. In the 'Import Plans' list, locate the import you're tracking. (If the list is long, use the search field to locate a device by its serial number.)
5. For information on the import:
   - View the status of the import in the 'Status' column.
   - Select the link in the 'Tracking Number' column to display tracking information in a new tab. (The tracking number is only available after the device has been returned for import.)
   - Select the More menu, and then select **View Plan Details**. View the following on the details screen:

Source	Device name, serial number, tracking number.
Cloud Destination	Destination type and region.
Path	Bucket and folder name.
Cloud Import Status	Add Credentials / Send for Import / Import to Cloud / Cryptographic Erase / Plan Close
Required Actions	Actions required for the import plan.
Cloud Import Timeline	List of import activities by date.

Confirm Import Completion

Upon completion of your cloud import, verify that your files have been successfully imported to your cloud destination.

> **!** **Important**—Ensure that all your files have been successfully imported to your cloud destination. **If there's an issue with your import, do not confirm it** Contact your sales representative or use the Lyve Support Center to report the issue.

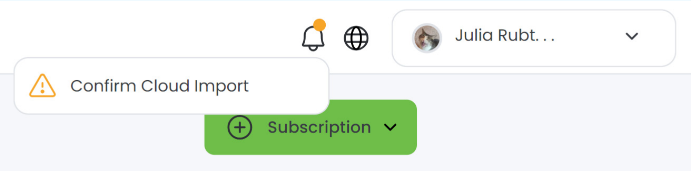
After verifying the files in your cloud destination, confirm the import in Lyve Management Portal.

> **!** **Important**—Confirmation of the import plan is required. Once you confirm the import in Lyve Management Portal, Seagate will purge the AES encryption key used to write data to the drive, making the data irretrievable. This erasure follows NIST SP 800-88 r1 standards.

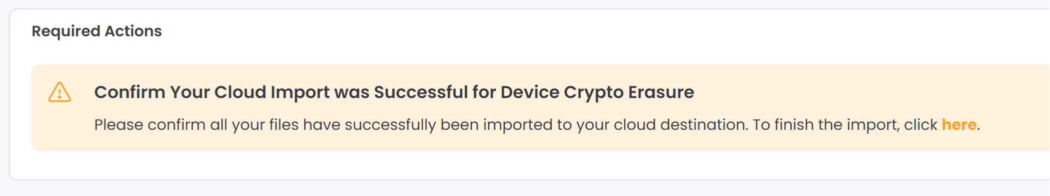
The status of your import plan(s) can be tracked in Lyve Management Portal.

1. Go to lyve.seagate.com and sign in. Enter a verification code to continue to Lyve Management Portal.
2. On the Home page, select an active Lyve Mobile subscription with a cloud import plan. (Alternatively, select the More icon in the 'Actions' column, and then selec**View Subscription**).
3. In the sidebar, select **Import Plans**.
4. In the 'Import Plans' list, locate the import with an 'Awaiting Confirmation' status. (If the list is long, use the search field to locate a device by its serial number.) Select the More icon in the 'Actions' column, and then select View Plan Details.

> **i** You can also select the Notifications icon in the upper right corner of the page and then select a **Confirm Cloud Import** alert in the list.



5. In the 'Required Actions' section, select the link in the alert banner.



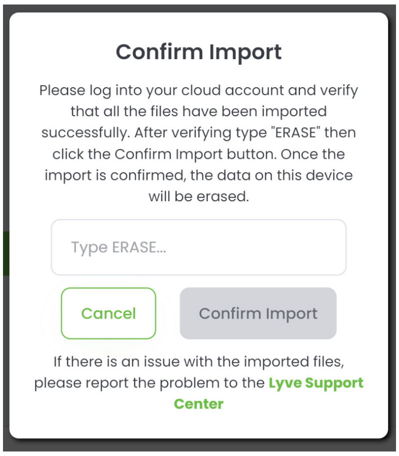
Required Actions

⚠ **Confirm Your Cloud Import was Successful for Device Crypto Erasure**

Please confirm all your files have successfully been imported to your cloud destination. To finish the import, click here.

6. Log into your cloud account and verify that your cloud import was successful and that there are no issues with the imported files.

> If there are issues with your imported files, discontinue the confirmation process. Contact your sales representative or use the Lyve Support Center to report the issue.



Confirm Import

Please log into your cloud account and verify that all the files have been imported successfully. After verifying type "ERASE" then click the Confirm Import button. Once the import is confirmed, the data on this device will be erased.

If there is an issue with the imported files, please report the problem to the **Lyve Support Center**

7. In the dialog, type **ERASE** in the field. Select **Confirm Import**.

After the device has been cryptographically erased, Seagate will send a certificate confirming the erasure of the device.