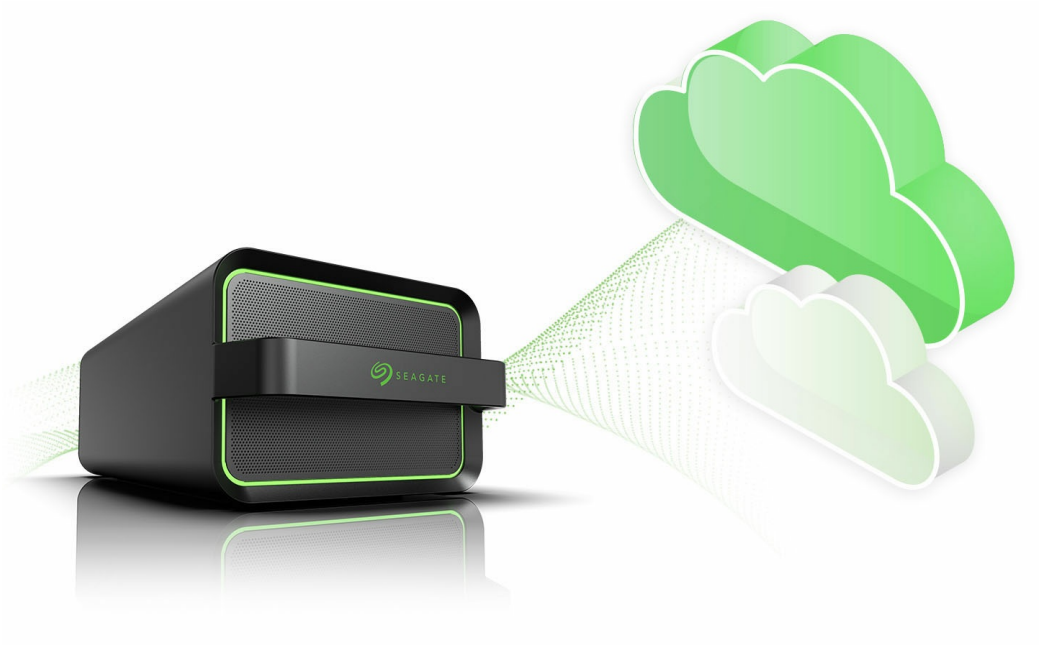
SEAGATE

Cloud Import Service

User Manual & Reference Guide



Hier klicken, um eine aktuelle Online-Version
dieses Dokuments aufzurufen. Auch finden Sie hier die aktuellsten Inhalte sowiеerweiterbare Illustrationen, eine übersichtlichere Navigation sowie Suchfunktionen.

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 project needs by adjusting your subscription at any time.

Cloud Import Process Overview

1. Sign in to Lyve Management Portal. If you do not have an account, register at lyve.seagate.com.
2. Create a Lyve Mobile with Cloud Import project.
3. Configure the import plan for your project.
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 project 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

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

Region	IP address(es) to allow
North America	20.253.219.114 38.100.210.253 38.104.105.74 67.200.249.173
Europe	91.242.219.6 149.5.114.11 185.212.46.0/29 193.242.211.16/28

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

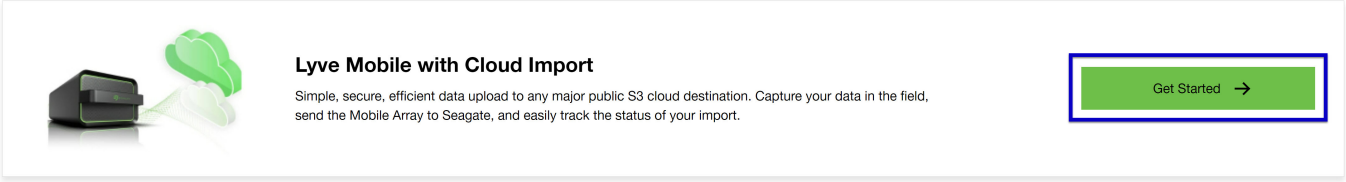
File Size Limitations

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 Project

> You must be a master account user or a sub user to create a project.

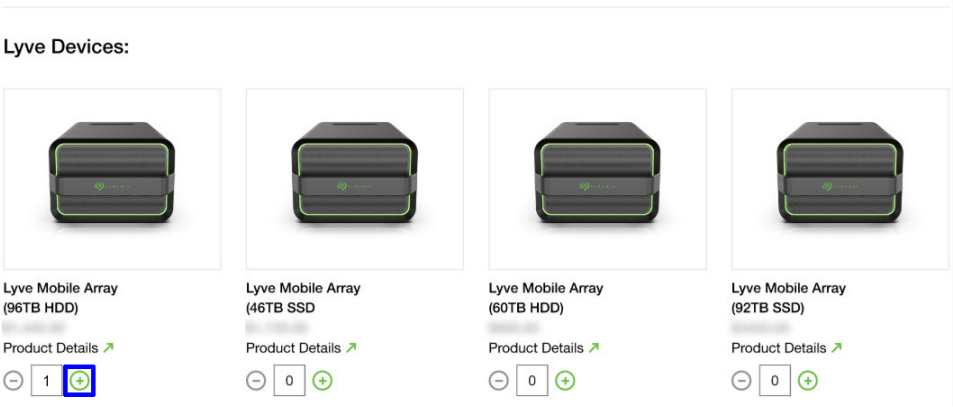
1. Go to lyve.seagate.com and sign in. Enter a verification code to continue to Lyve Management Portal.
2. On the Lyve Services page, click **Get Started** on the Lyve Mobile with Cloud Import card.



3. On the Service Plan page, review the Lyve service selected.
4. Review the associated rate plan selection for this service.

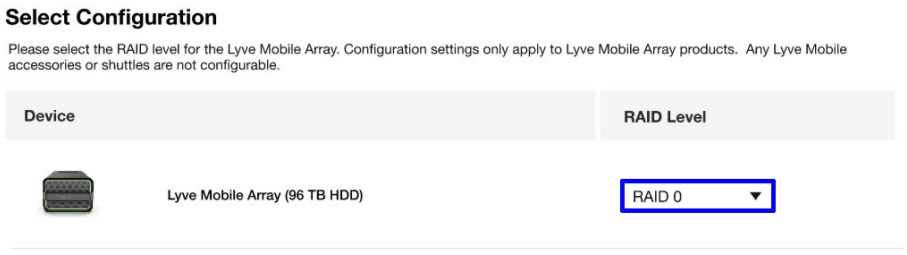
> A one-time import service charge is applied to each storage device in a project with a payment due at checkout.

5. Check the box to acknowledge that you have read and understand our Cloud Import Service User Manual & Reference Guide. Click **Continue**.
6. Add products to your subscription by clicking the Plus (+) icon or entering a quantity to the field below a product.



Click **Continue.**

7. Select the RAID level for each Mobile Array in your project. RAID options are RAID 0 and RAID 5 (default).

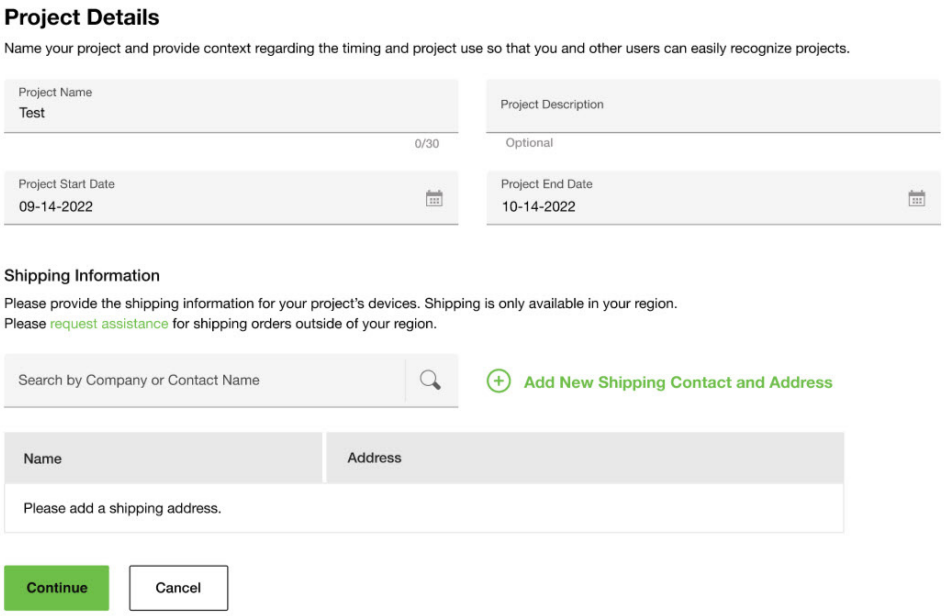


> Configuration settings are only displayed for configurable devices.

Click **Continue**.

8. Fill in project details:

- Project name
- Project start and end date
- Contact information
- Shipping information



Click **Continue**.

9. Select an import destination from the table. If there are no previous import destinations listed, or you need to add a new one, see Adding a new import destination below.

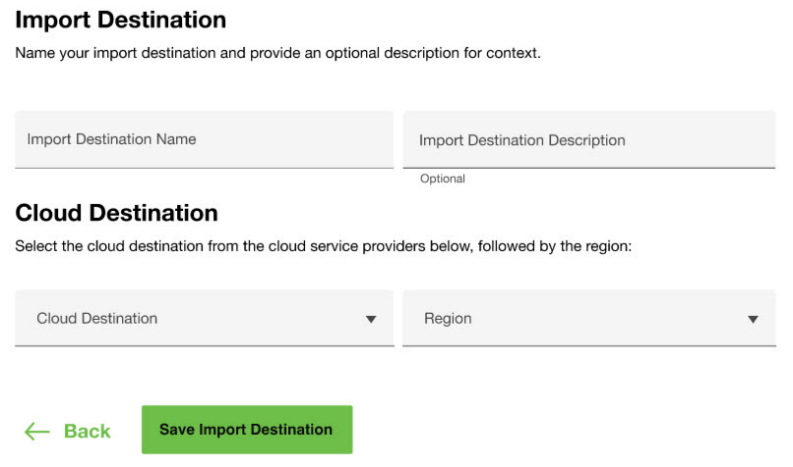
> All devices within a project use the same import destination. If you want some devices to use another cloud or region, you'll need to create a separate project.

Ensure that the correct import destination in the table is selected and that the information is accurate. Click **Continue.**

Adding a new import destination

Click **Add Import Destination** and enter the following destination details:

- Import destination name and (optionally) description.
- Cloud destination and region.

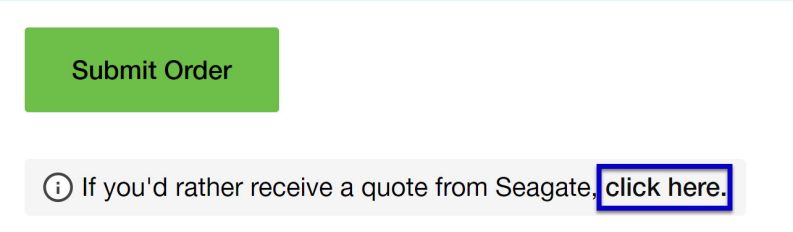


Each import destination must have a unique name, along with a unique cloud and region combination. You will configure the bucket/container and credentials later.

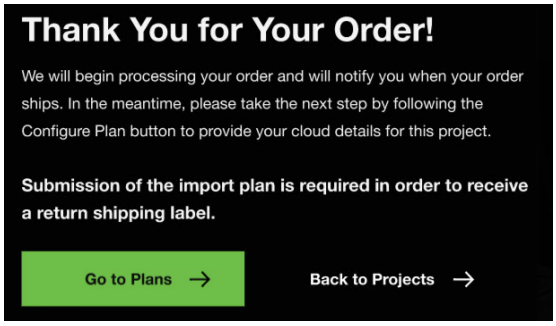
Click **Save Import Destination**.

10. Review your service plan, project details, shipping details, import destination, and devices. If you have a valid promo code, enter it in the order summary section.
11. Submit your order or request a quote from Seagate.

To receive a quote, click on the link at the bottom of the page.



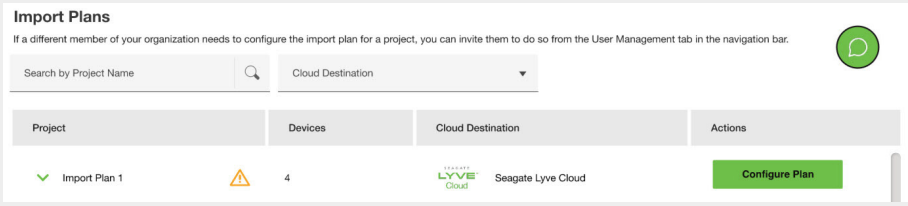
12. Once you submit your cloud import project, you'll see a confirmation page. Click the **Go to Plans** button to start your plan configuration. (**Note**—It may take a minute for your project to appear on the Import Plans page.) If you click **Back to Projects**, you can complete your import plan configuration at a later time. An import plan will remain in draft status until the details are configured and submitted.



You'll only see the confirmation screen above if you **submit a project**. If you **request a quote** or **register a deal**, you can configure your import plan after the quote/deal has been approved. There are two other ways to start configuring your import plan:

From the Import Plans page

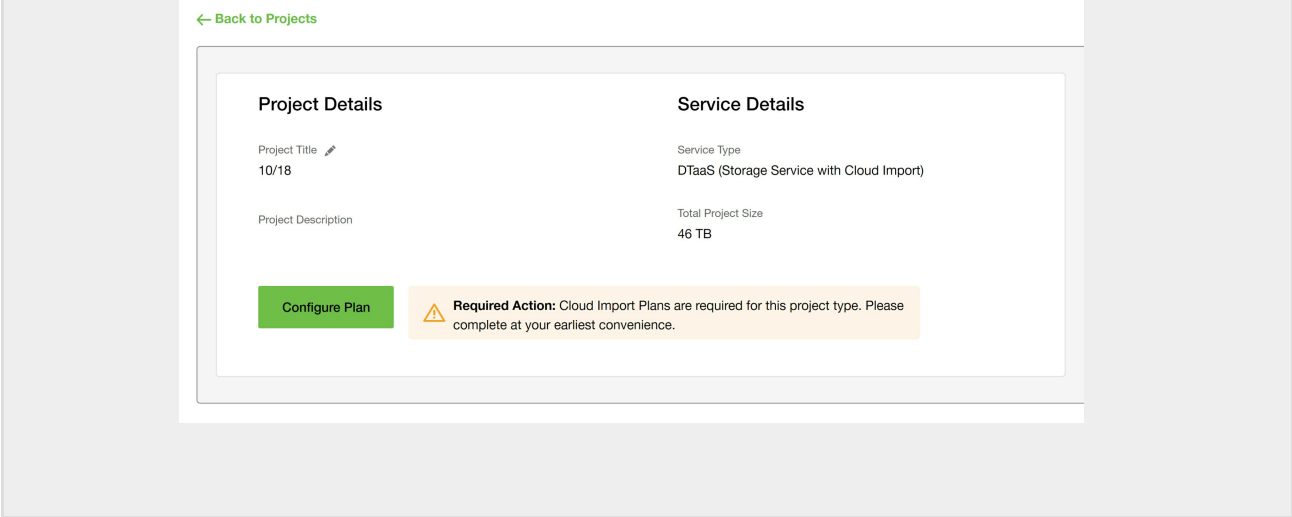
1. Go to lyve.seagate.com and sign in. Enter a verification code to continue to Lyve Management Portal.
2. On the Lyve Services page, go to the Lyve Mobile with Cloud Import card. Click on the **Manage Projects** dropdown and select **View Plans.**
3. In the Import Plans table, locate the project that you would like to configure the plan for and click the **Configure Plan** button in the Actions column.



Note—If you requested a quote or submitted a deal, you will be able to configure the plan once your project is approved and active.

From the Project Details page

1. Go to lyve.seagate.com and sign in. Enter a verification code to continue to Lyve Management Portal.
2. On the Lyve Services page, go to the Lyve Mobile with Cloud Import card. Click on the **Manage Projects** dropdown and select **View Projects.**
3. Click on the cloud import project that you would like to configure a plan for.
4. Click **Configure 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

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, see Creating 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 Lyve Import project.
- 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 cloud import project has ended.

- Disable or delete the policy after the cloud import project has ended.

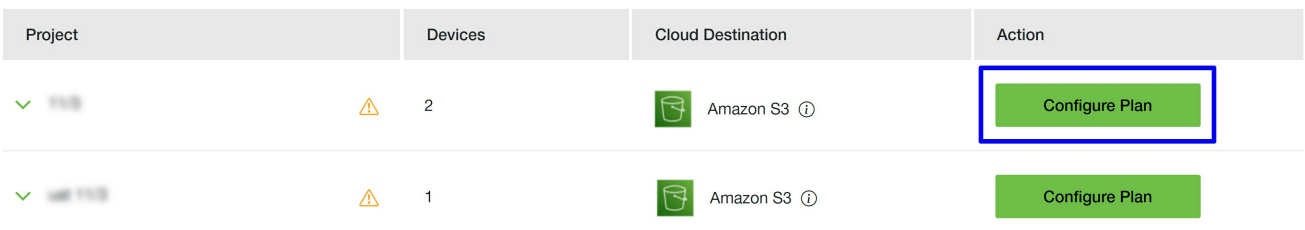
Amazon IAM Permission Policy example

```
{
   "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}/*"
          ]
      }
   ]
}
```

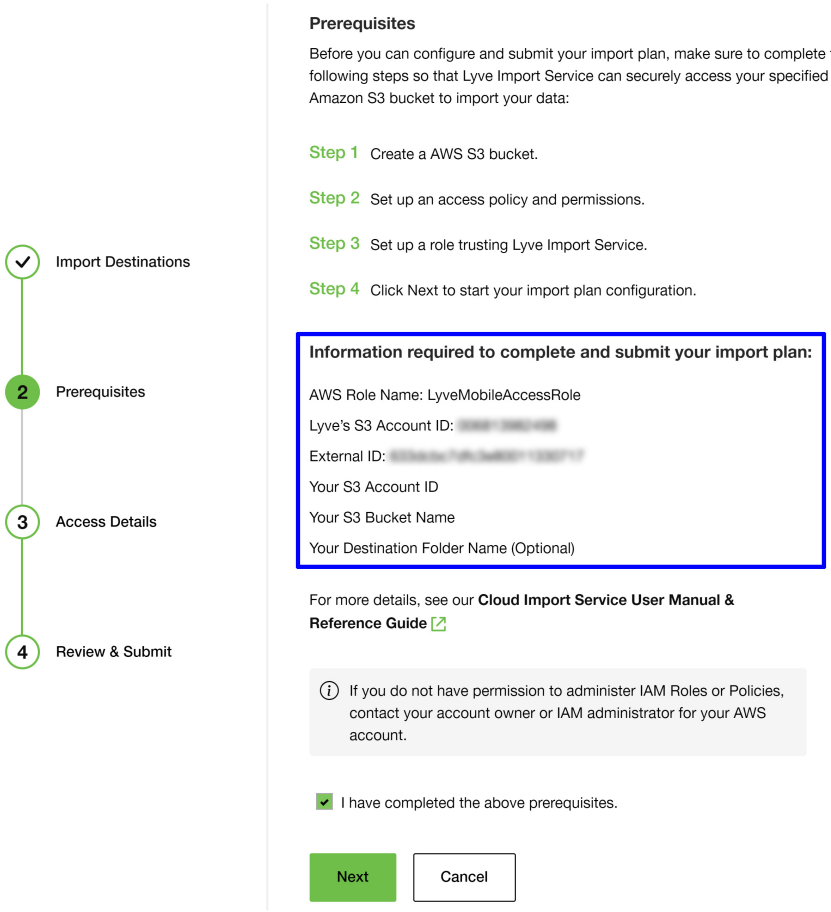
Complete the prerequisites

Gather information

1. Click **Import Plans** in the navigation bar. In the Import Plans table, locate the project that you would like to configure the plan for and click the**Configure Plan** button in the Actions column.**Note**—If you requested a quote or submitted a deal, you will be able to configure the plan once your project is approved and active.



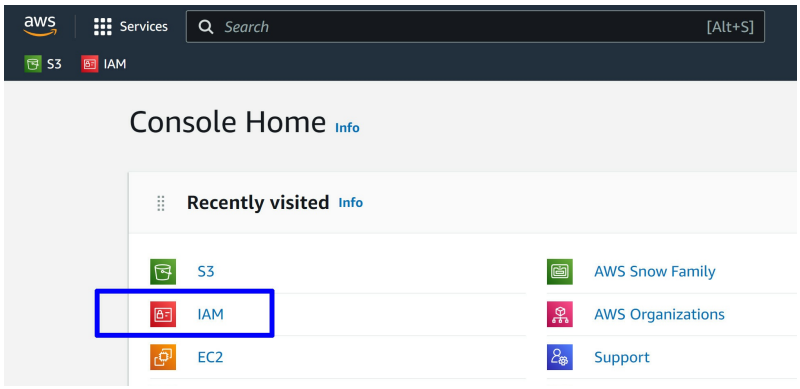
The plan confirguration wizard appears:



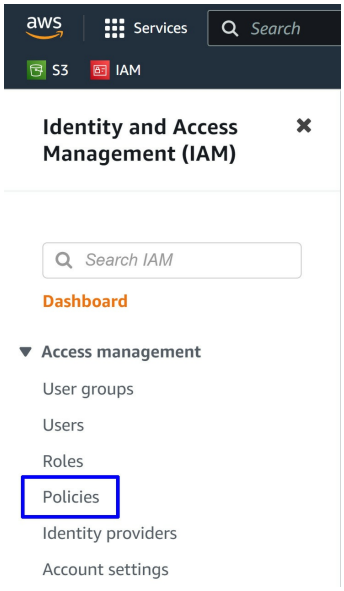
2. Copy the required information, taking note of **Lyve's S3 Account ID** and the **External ID.** You will need these in the steps that follow. (If you need to update the import destination first, click on the Import Destination step and edit.)

Create an IAM Permission Policy on your bucket

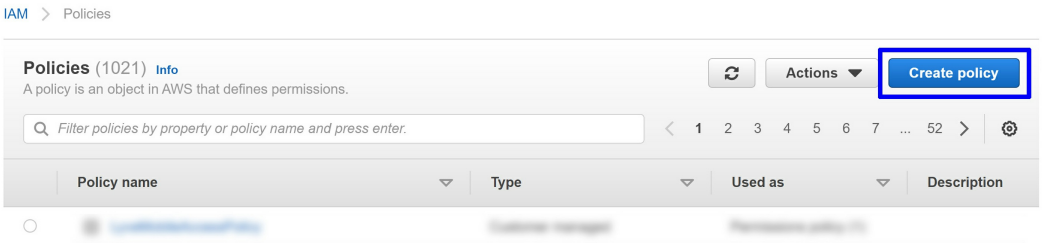
1. Log in to your AWS Console.
2. Enter the IAM service.



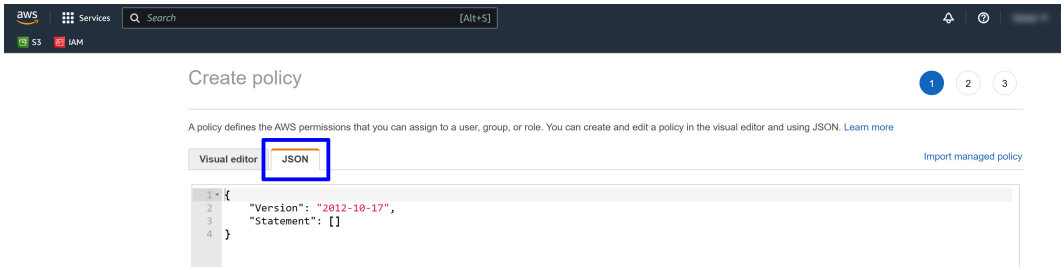
3. Select Policies.



Click the **Create policy** button.



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



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",
```

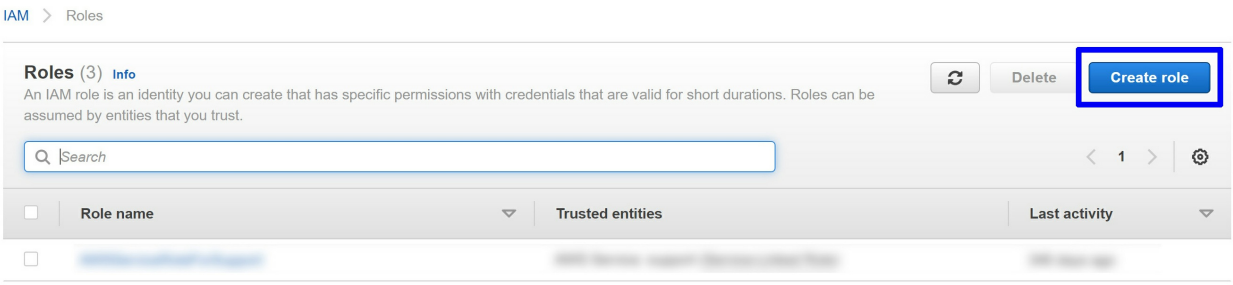
```
            "s3:GetAccelerateConfiguration",
            "s3:DeleteObject",
            "s3:GetBucketLocation",
            "s3:ListMultipartUploadParts"
        ],
        "Resource": [
            "arn:aws:s3:::{bucketname}",
            "arn:aws:s3:::{bucketname}/*"
        ]
    }
  ]
}
```

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.

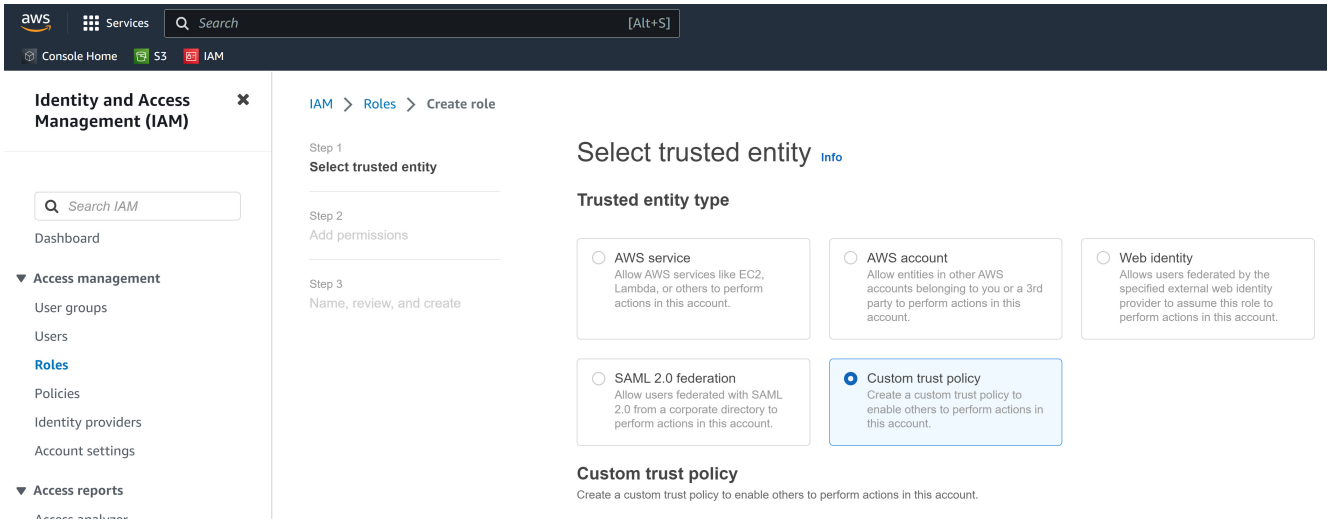
11. .Click **Create policy**

Create an IAM role trusting Lyve Import Service

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



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



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}"
     ]
    }
   }
  }
 ]
}
```

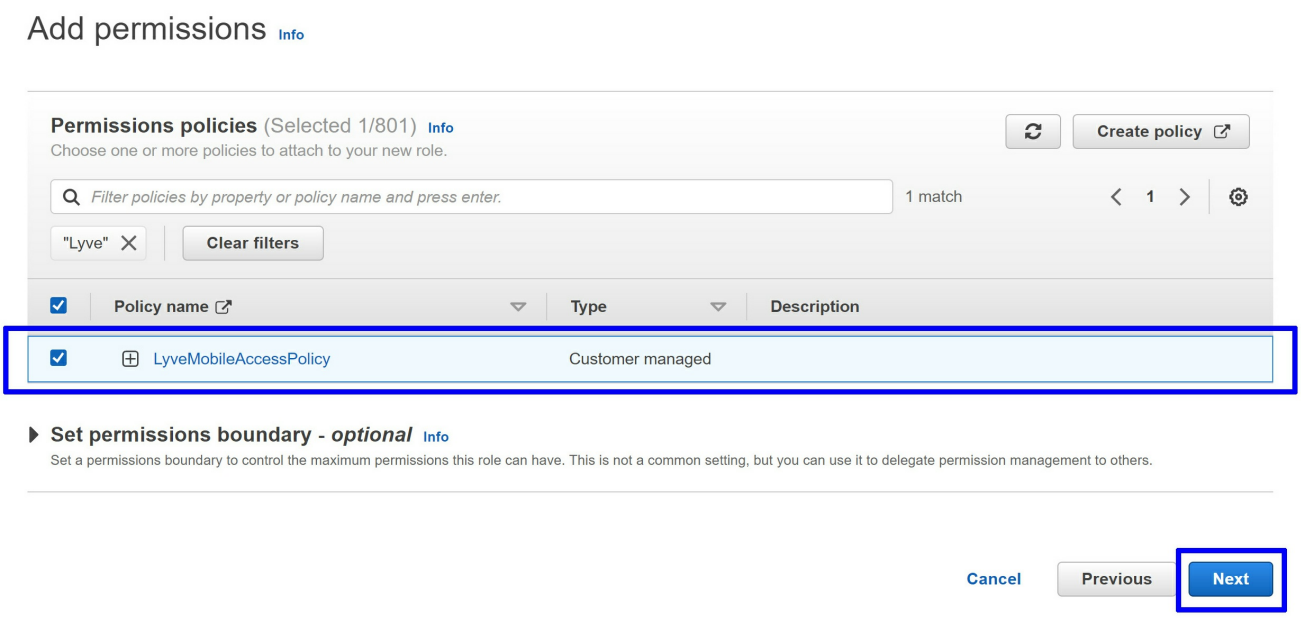
4. Paste the copied text into the JSON editor.
5. Replace {accountid} with the value you copied for Lyve's S3 Account ID. Replac{externalid} with the value you copied for External ID.
6. On the **Add permissions** page, add the **LyveMobileAccessPolicy** you created earlier and click **Next**.

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

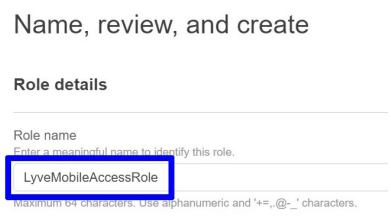
```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::{accountid}:root"
```

```
    },
    "Action": "sts:AssumeRole",
    "Condition": {
     "ForAnyValue:StringEqualsIfExists": {
      "sts:ExternalId": [
       "{firstexternalid}",
          "{secondexternalid}",
          "{thirdexternalid}"
      ]
     }
    }
   }
  ]
}
```

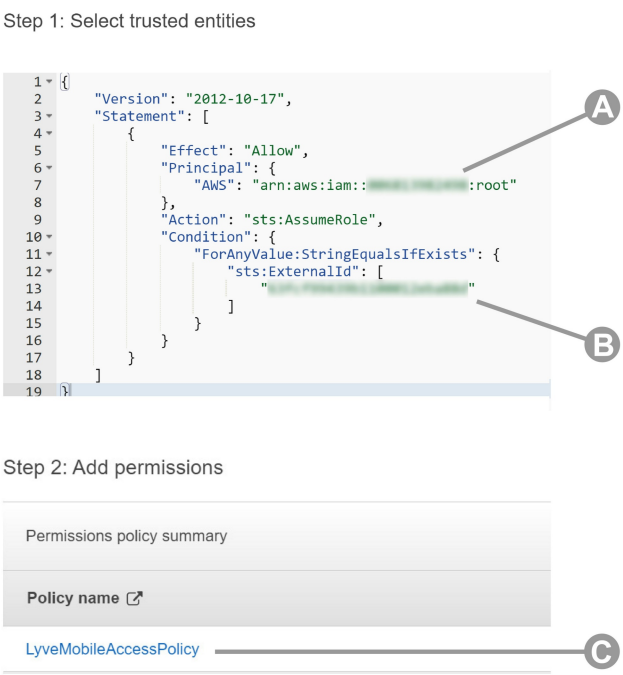
7. Click **Next** to exit the JSON editor.
8. On the **Add permissions** page, add the **LyveMobileAccessPolicy** you created earlier and click **Next**.



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



10. Review the trusted entity and permissions information:



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.

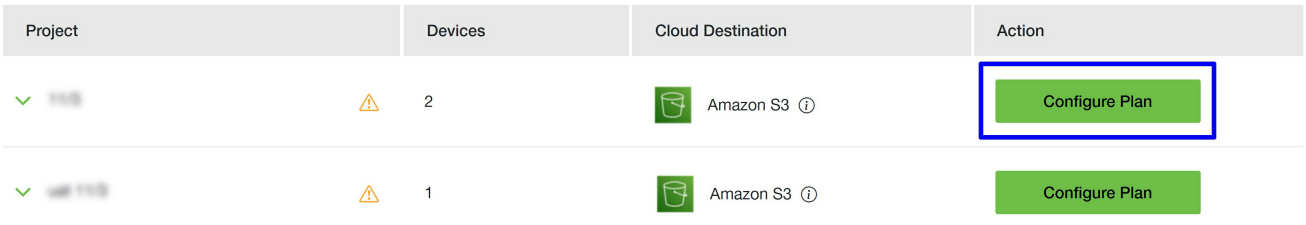
Configure your import plan

After you’ve completed the prerequisites, continue to the next step to enter your access details.

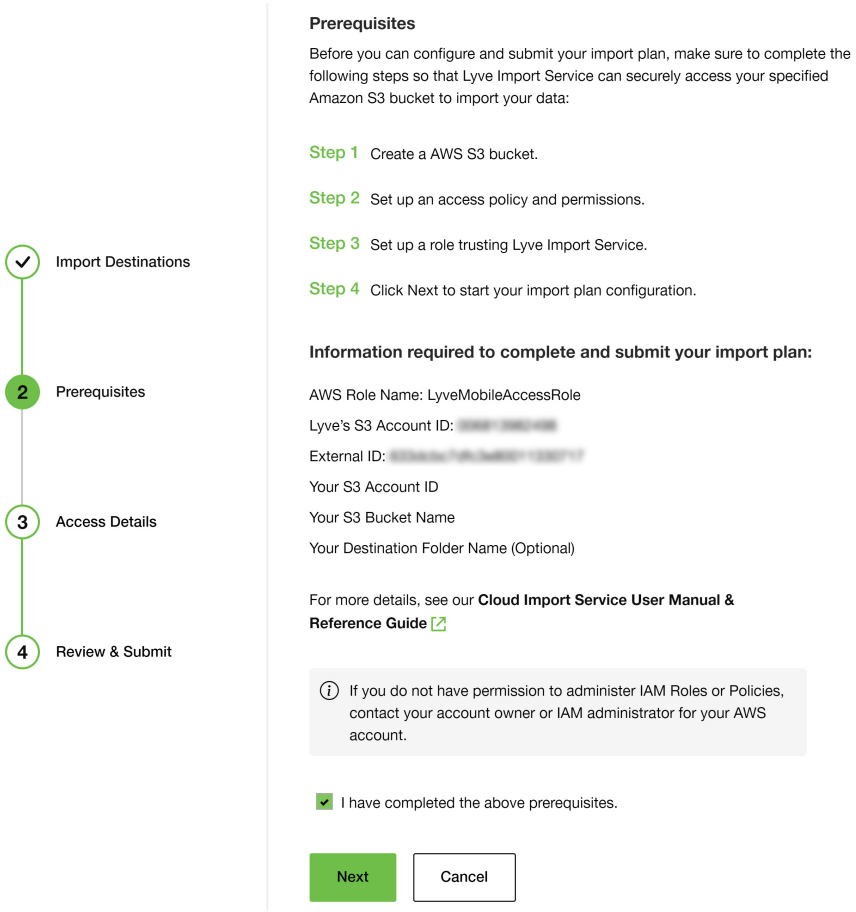
You must successfully validate your access details and submit your plan before your return shipping label(s) are available for you to download.

Review access details

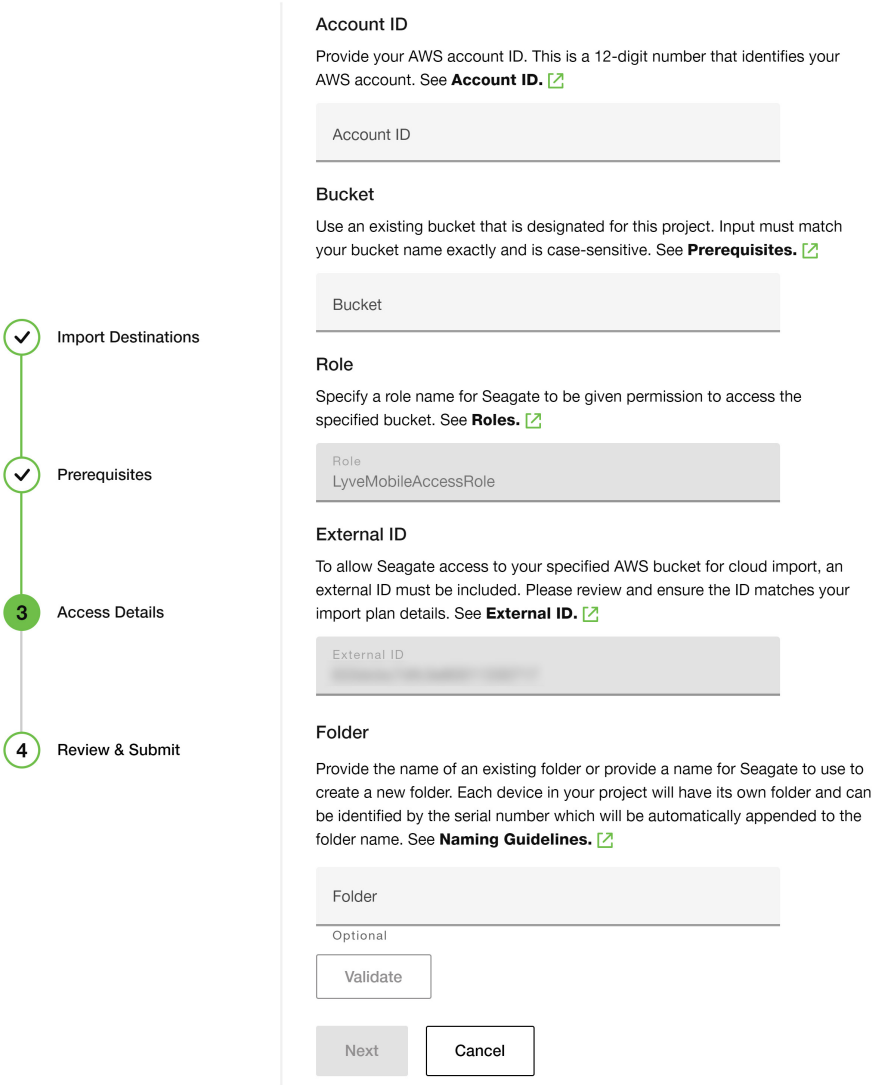
1. In Lyve Management Portal, click **Import Plans.** Click **Configure Plan** next to an Amazon S3 cloud destination.



2. Confirm that you’ve completed the prerequisites and click **Next.**



3. Enter access details:



A. Enter your AWS account ID.
B. Enter your bucket name. The name is case-sensitive and must match exactly.
C. Confirm the name of the IAM role you created in the prerequisite steps.
D. Confirm the External ID you created in the prerequisite steps.
E. (Optional) Enter a name for your folder.

Each storage device in your project 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.

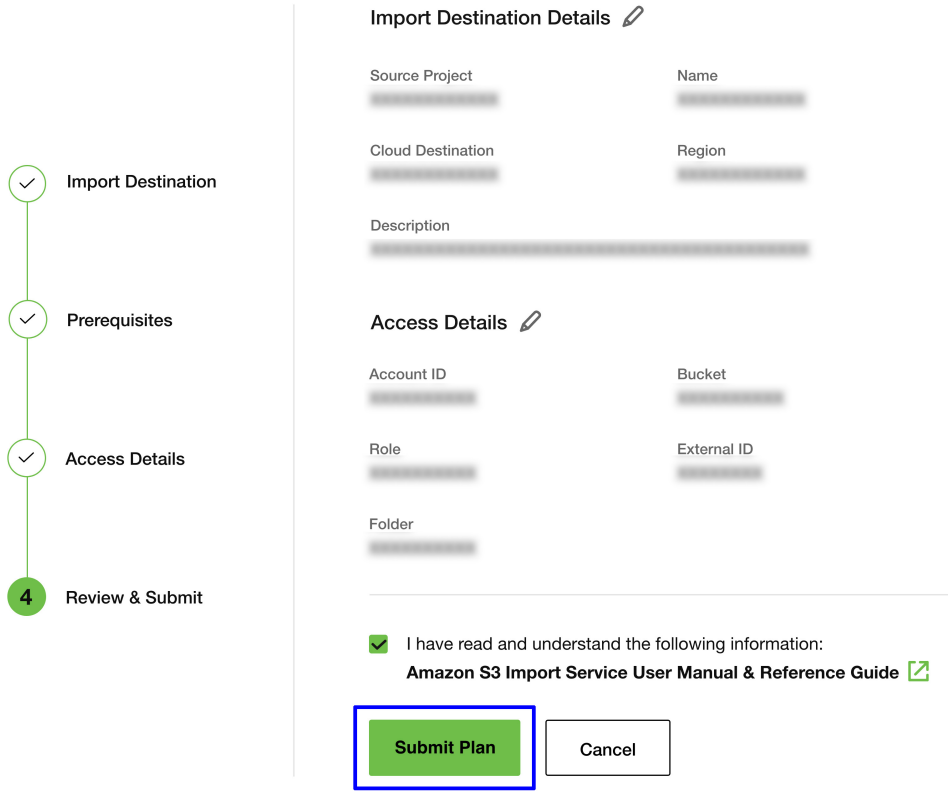
4. Click **Validate**.

> ! If the validation fails, check your AWS account ID, bucket name, IAM permission policy, and IAM role, and then revalidate.

5. Click **Next**.

Review and submit your import plan

1. Review your import destination and access details. If you need to make any changes, click the Edit icon.
2. Check the box to confirm that you've read and understand the information in this reference guide.
3. Click **Submit Plan.**



Inviting another user to configure an import plan

If a different member of your organization needs to configure the import plan for a project, you can invite them to do so in Lyve Management Portal. See Invite Another User to Configure an Import Plan.

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, see Creating 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.

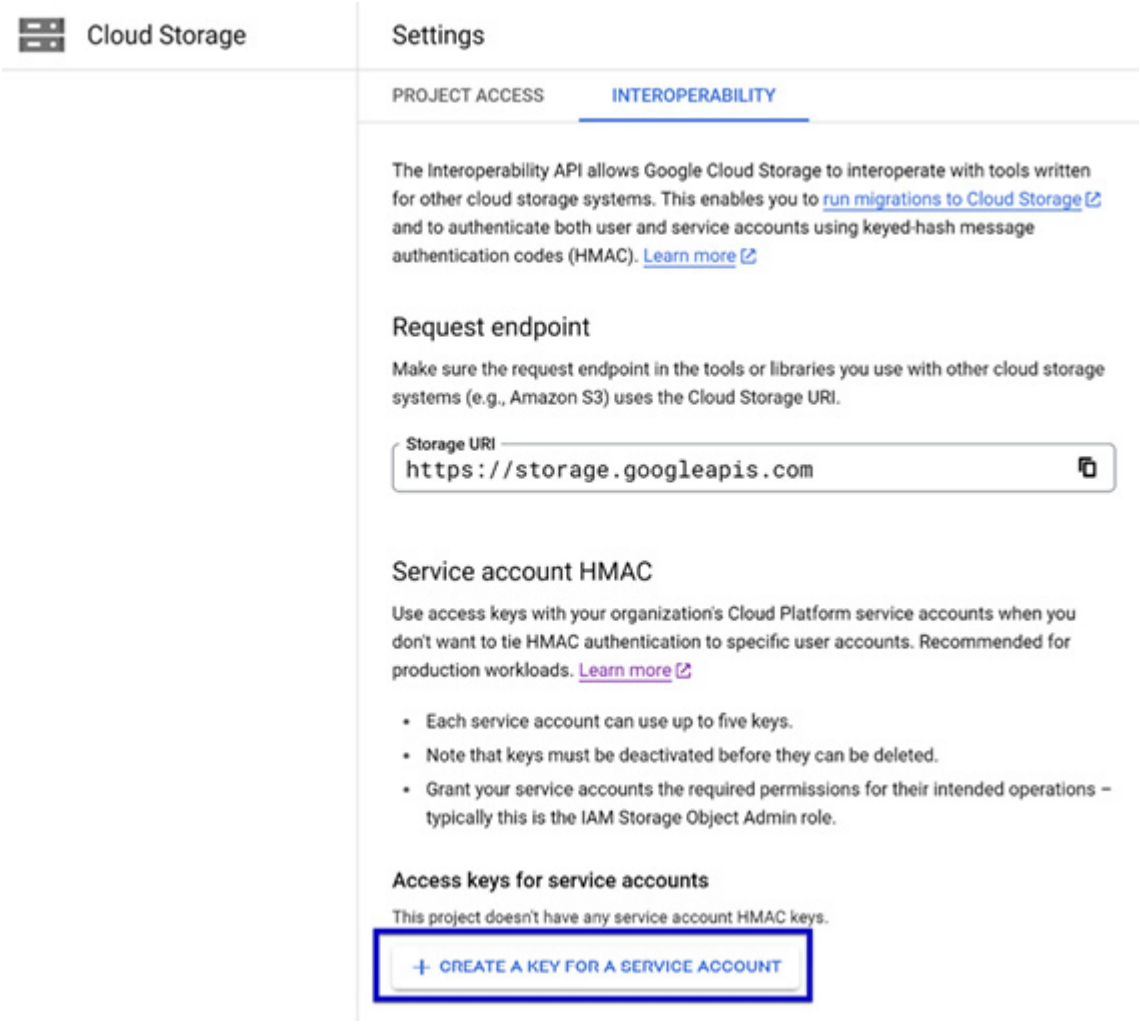
IP address access—If configured by your organization, list Seagate's IP address(es) as an allowed source. See IP Address Access.

Seagate authorizations—See below.

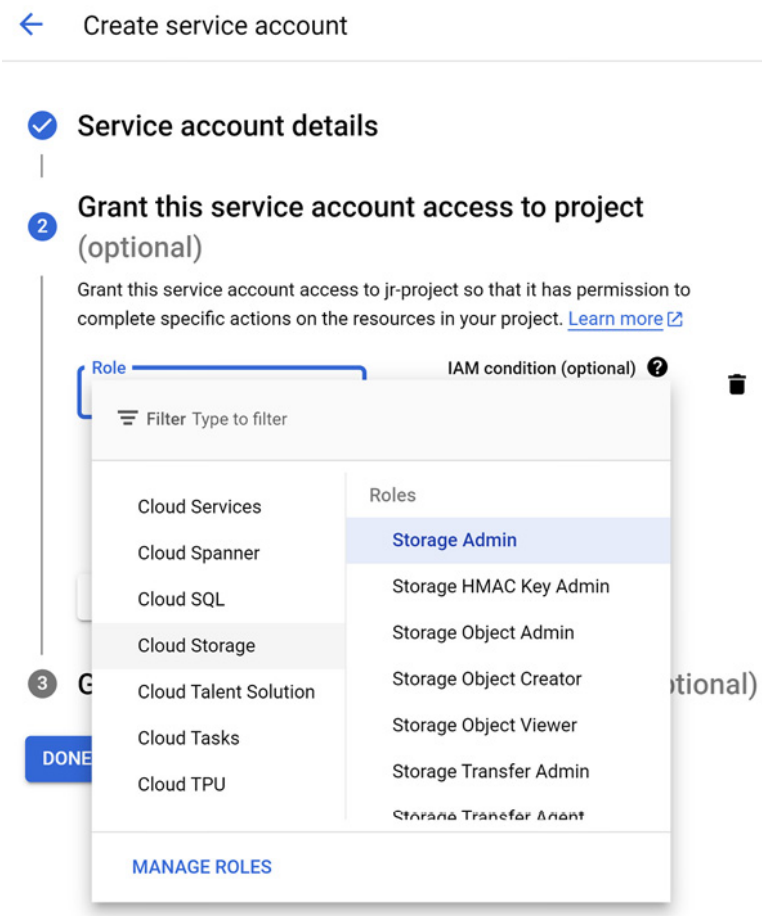
Seagate authorizations

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:

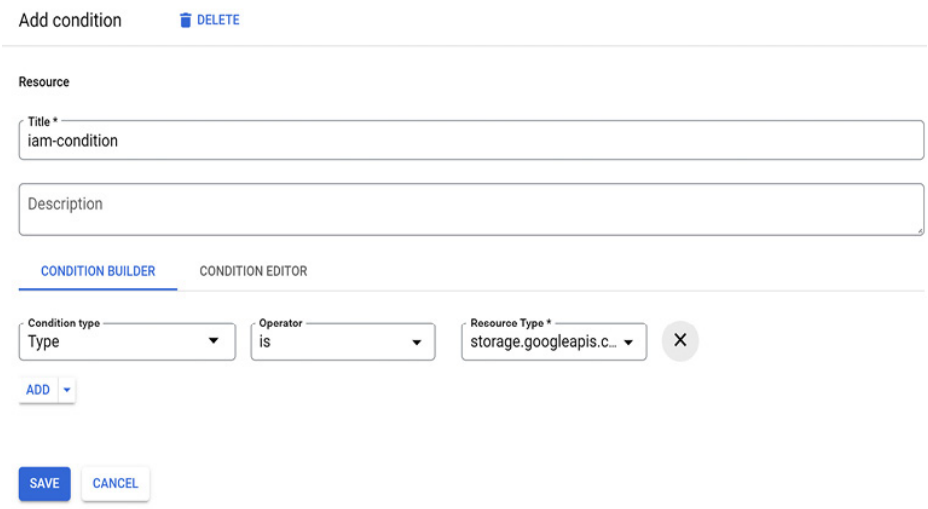
1. Using the Google Cloud console, go to the Cloud Storage **Buckets** page and click **Settings**.
2. Click the **Interoperability** tab. Click **Create A Key For A Service Account**.



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



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

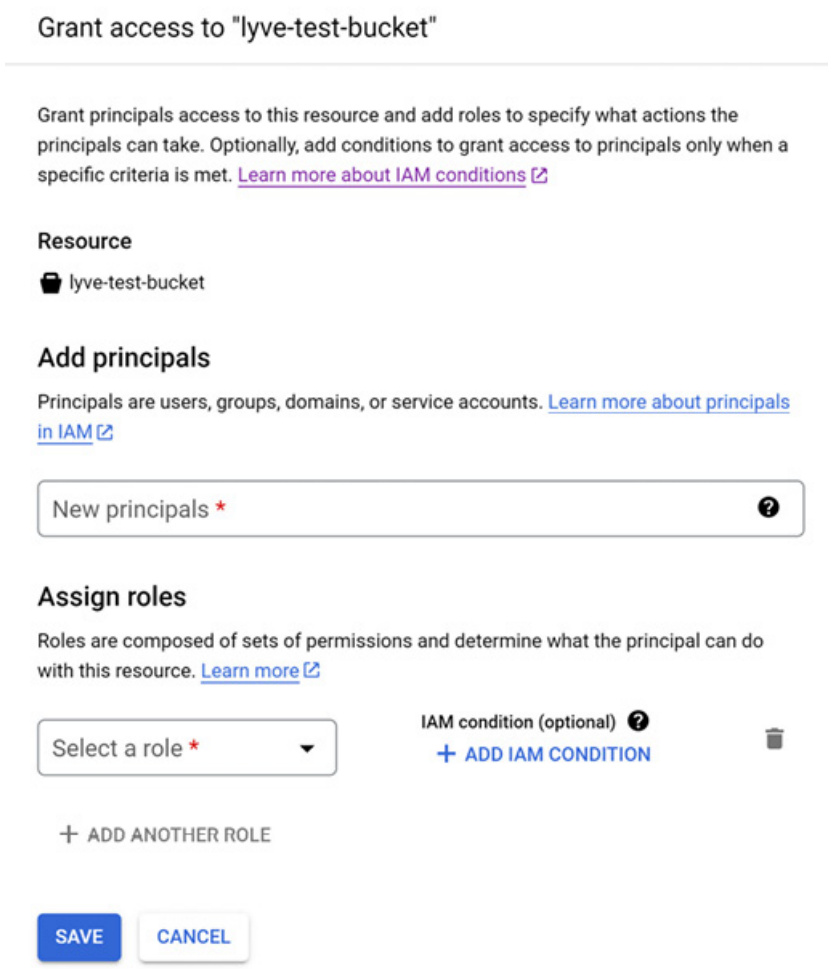


   Click **Save**.

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**.



> To learn more, see HMAC keys.

Recommendations

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

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

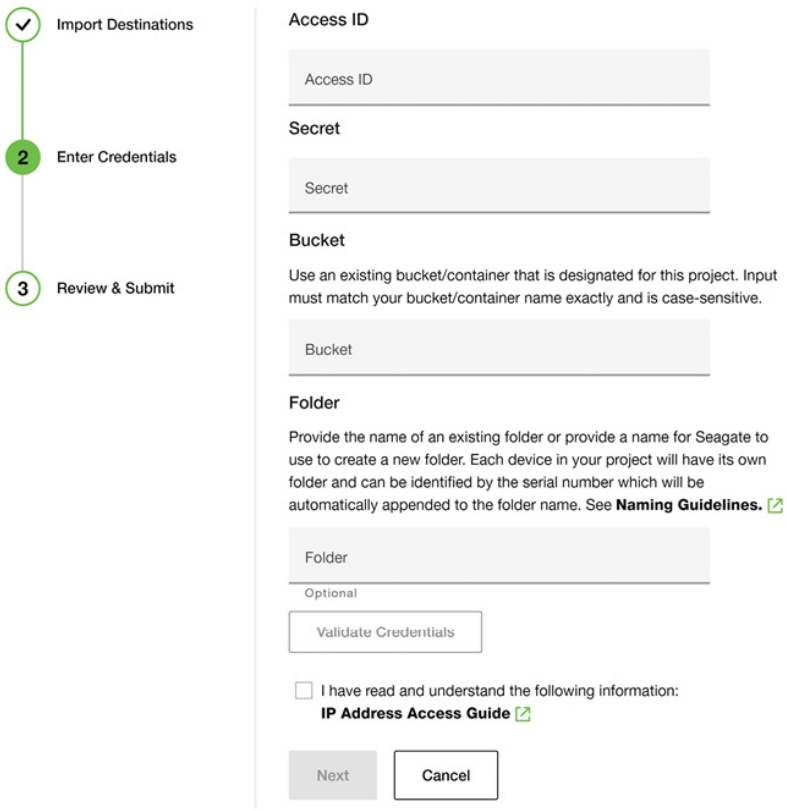
> **Important note on file sizes**—In general, Seagate does not recommend importing individual files larger than 5TB. Please refer to your cloud provider’s file size limitations and best practices.

Configure your import plan

Enter credentials

1. In Lyve Management Portal, click **Import Plans** in the navigation bar, and then click**Configure Plan**.
2. Enter your Access ID and Secret. (If you need to update the import destination first, click on the **Import Destinations** step and edit.)

> Characters you enter in these fields are always masked.



3. Enter your bucket name. The name is case-sensitive and must match exactly.
4. (Optional) Enter a name for your folder.

> Each storage device in your project 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.

5. Validate Credentials.

> **i** If the validation fails, check that the access ID, secret, and bucket name entered are accurate, and then revalidate.

6. Check the box to confirm that you have read and understand the details in IP Address Access.
7. Click **Next**.

Review and submit your import plan

1. Review your import destination and credential details.
2. Check the box to confirm that you've read and understand the information in this reference guide.
3. Click **Submit Plan**.

Inviting another user to configure an import plan

If a different member of your organization needs to configure the import plan for a project, you can invite them to do so in Lyve Management Portal. See Invite Another User to Configure an Import Plan.

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 the goog prefix.
- Bucket names cannot contain google or close misspellings, such as g00gle.

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, see Choosing a plan and creating an instance.

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

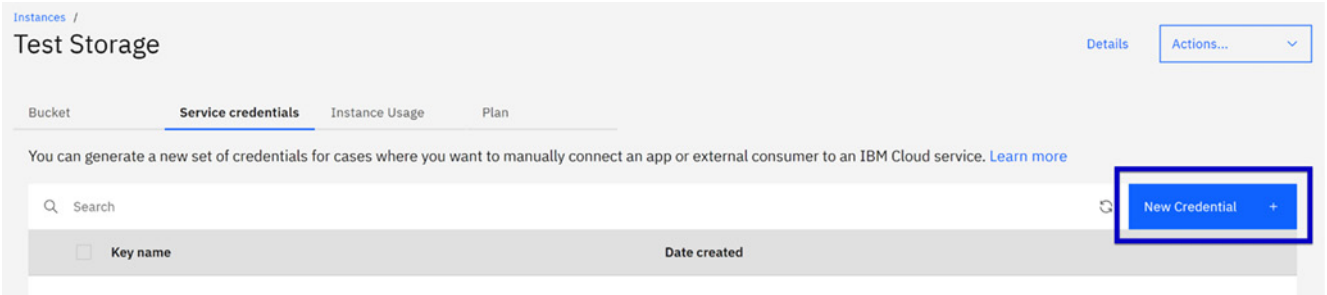
IP address access—If configured by your organization, list Seagate's IP address(es) as an allowed source. See IP Address Access.

Seagate authorizations—See below.

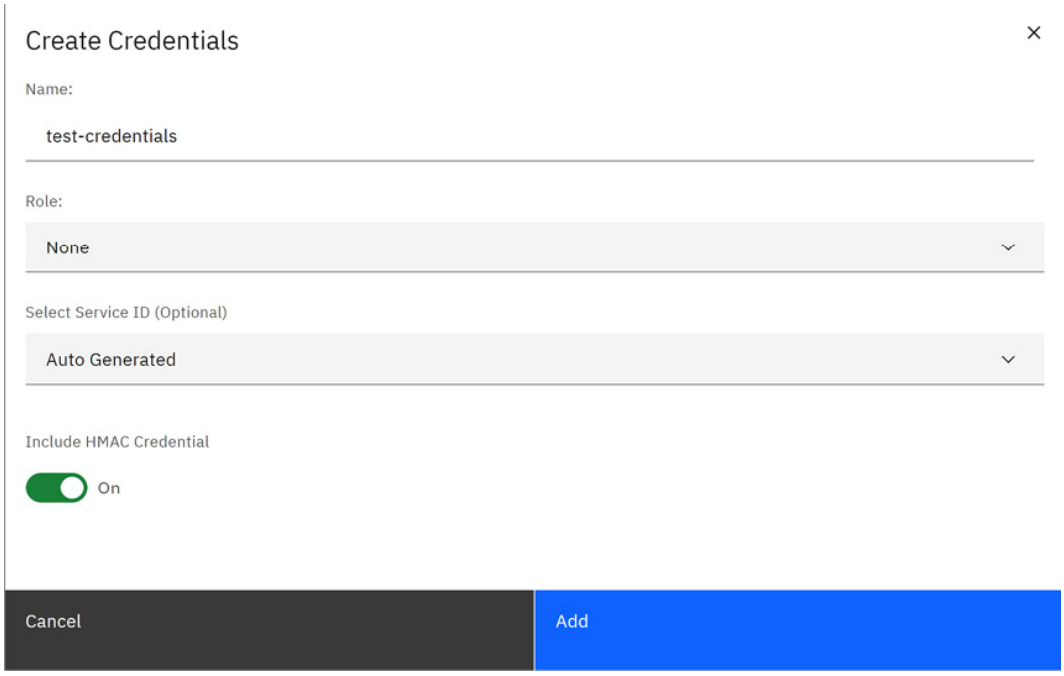
Seagate authorizations

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



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

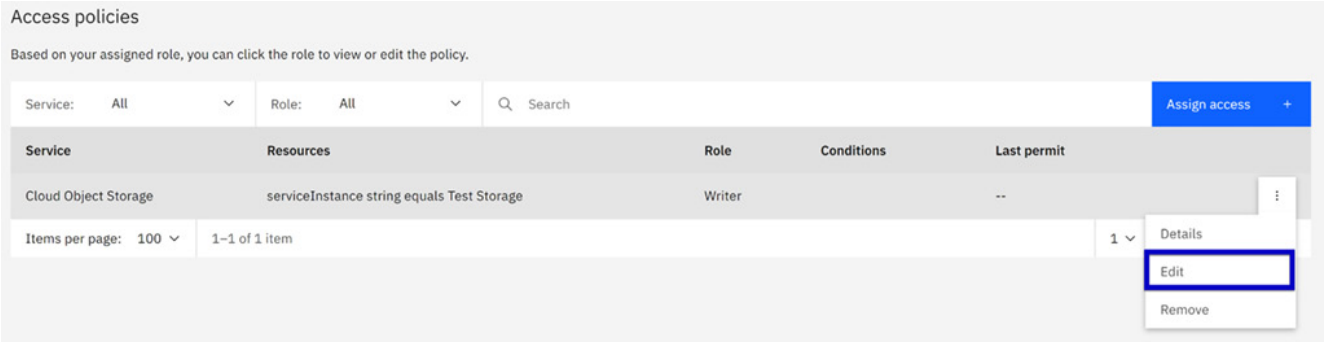


Click the **Add** button. Once added, you can expand the credentials to view the values for the access key ID and secret access key.

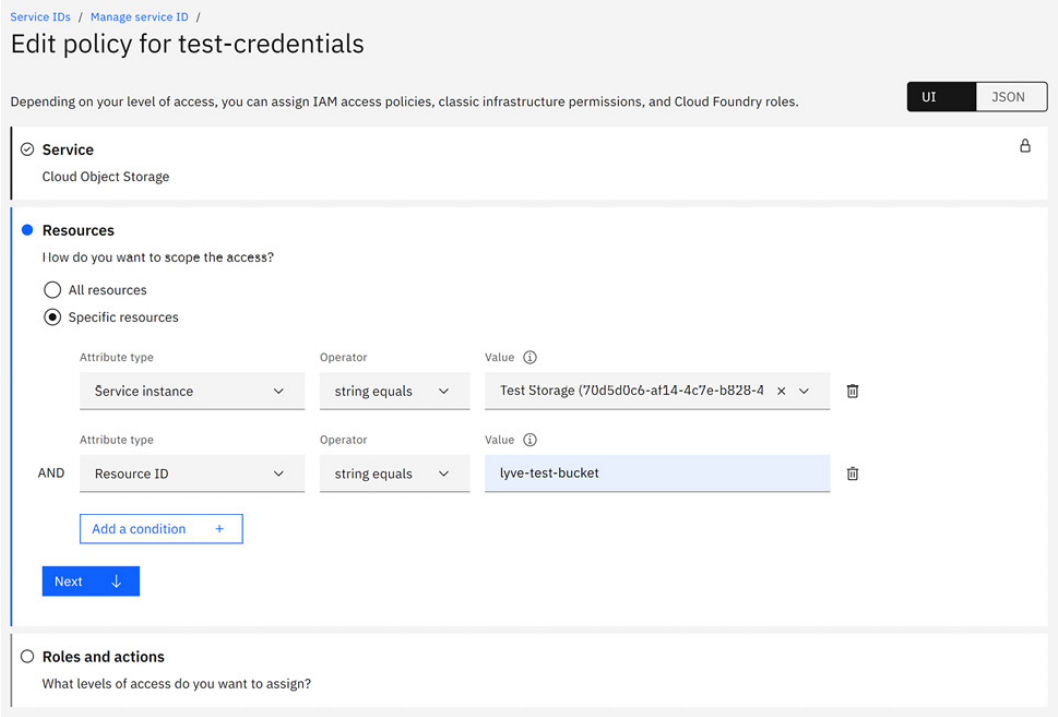
> When these credentials are created, the underlying service ID has access to any bucket in your instance (if it was automatically generated). To limit access to a specific bucket or subset of buckets, you will need to edit the access policy of the service ID tied to these credentials.

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

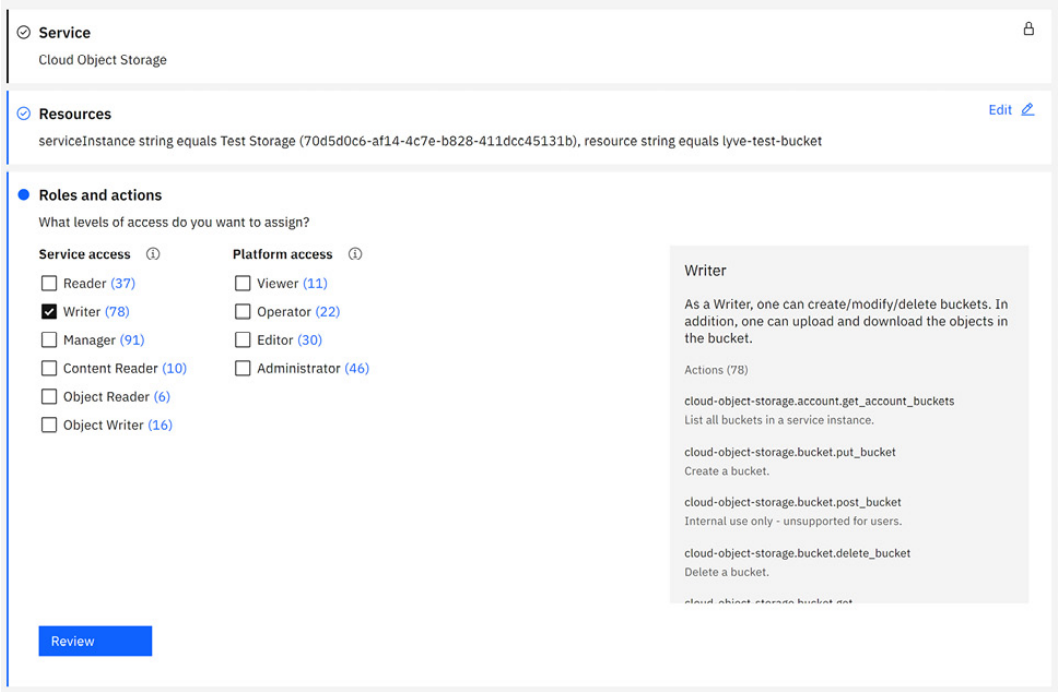
1. Navigate to the IAM console by clicking**Manage > Access (IAM)**. Click **Service IDs** in the side panel. Click on the service ID you want to edit.
2. Under **Access policies**, locate the role with the access policy you want to edit. Click the**Actions** icon and select **Edit**.



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



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



5. Click **Save**.

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

Recommendations

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

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

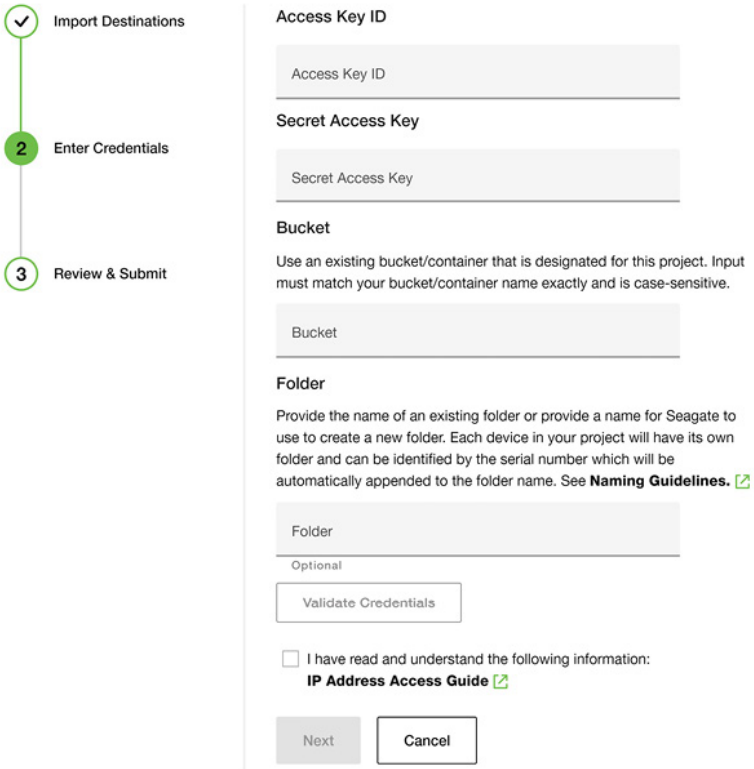
> **Important note on file sizes**—In general, Seagate does not recommend importing individual files larger than 5TB. Please refer to your cloud provider’s file size limitations and best practices.

Configure your import plan

Enter credentials

1. In Lyve Management Portal, click **Import Plans** in the navigation bar, and then click **Configure Plan**.
2. Enter your Access Key ID and Secret Access Key. (If you need to update the import destination first, click on the **Import Destinations** step and edit.)

> Characters you enter in these fields are always masked.



3. Enter your bucket name. The name is case-sensitive and must match exactly.
4. (Optional) Enter a name for your folder.

> **i** Each storage device in your project 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.

5. Click **Validate Credentials** .

> **i** If the validation fails, check that the access ID, secret, and bucket name entered are accurate, and then revalidate.

6. Check the box to confirm that you have read and understand the details in IP Address Access
7. Click **Next**.

Review and submit your import plan

1. Review your import destination and credential details.
2. Check the box to confirm that you've read and understand the information in this reference guide.
3. Click **Submit Plan**.

Inviting another user to configure an import plan

If a different member of your organization needs to configure the import plan for a project, you can invite them to do so in Lyve Management Portal. See Invite Another User to Configure an Import Plan.

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 Lyve project.

> **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

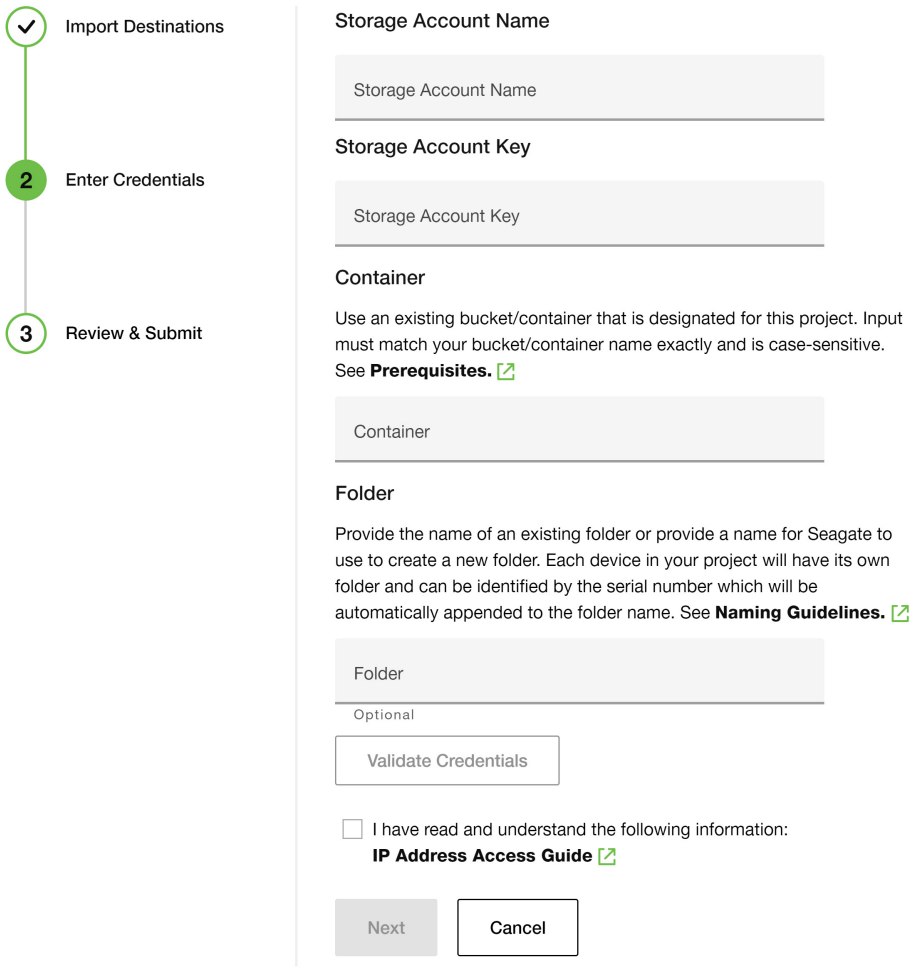
Enter credentials

The storage account name and storage account key are required to authenticate requests to your cloud resources. Access keys can be found in the Azure portal under the Security + networking tab in your storage account.

1. In Lyve Management Portal, click **Import Plans** in the navigation bar, and then click **Configure Plan**.

1. In Lyve Management Portal, click **Import Plans** in the navigation bar, and then click **Configure Plan**.
2. Enter your storage account name and storage account key. (If you need to update the import destination first, click on the Import Destination step and edit.)

> Characters you enter in security-related fields are always masked.



> **Important**—If you rotate your account access keys at any point, make sure that the import plan for your Lyve project is updated with the new credentials.

3. Enter your container name.
4. (Optional) Enter a name for your folder.

   Each storage device in your project 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.

5. Click **Validate Credentials** .

If the validation fails, check that the storage account name, storage account key, and container entered are accurate, then revalidate. If you have a key expiration policy in place, ensure that the access key provided has not expired. See Manage storage account access keys.

6. Check the box to confirm that you have read and understand the details in IP Address Access.
7. Click **Next**.

Review and submit your import plan

1. Review your import destination and credential details. If you need to make changes to the credentials provided, click the Edit icon.
2. Check the box to confirm that you've read and understand the information in this reference guide.
3. Click **Submit Plan**.

Inviting another user to configure an import plan

If a different member of your organization needs to configure the import plan for a project, you can invite them to do so in Lyve Management Portal. See Invite Another User to Configure an Import Plan.

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, see Creating 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 ID and secret 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 Lyve Import project.
- Block all public access for your container.
- Disable or delete the HMAC key after the cloud import project has ended.

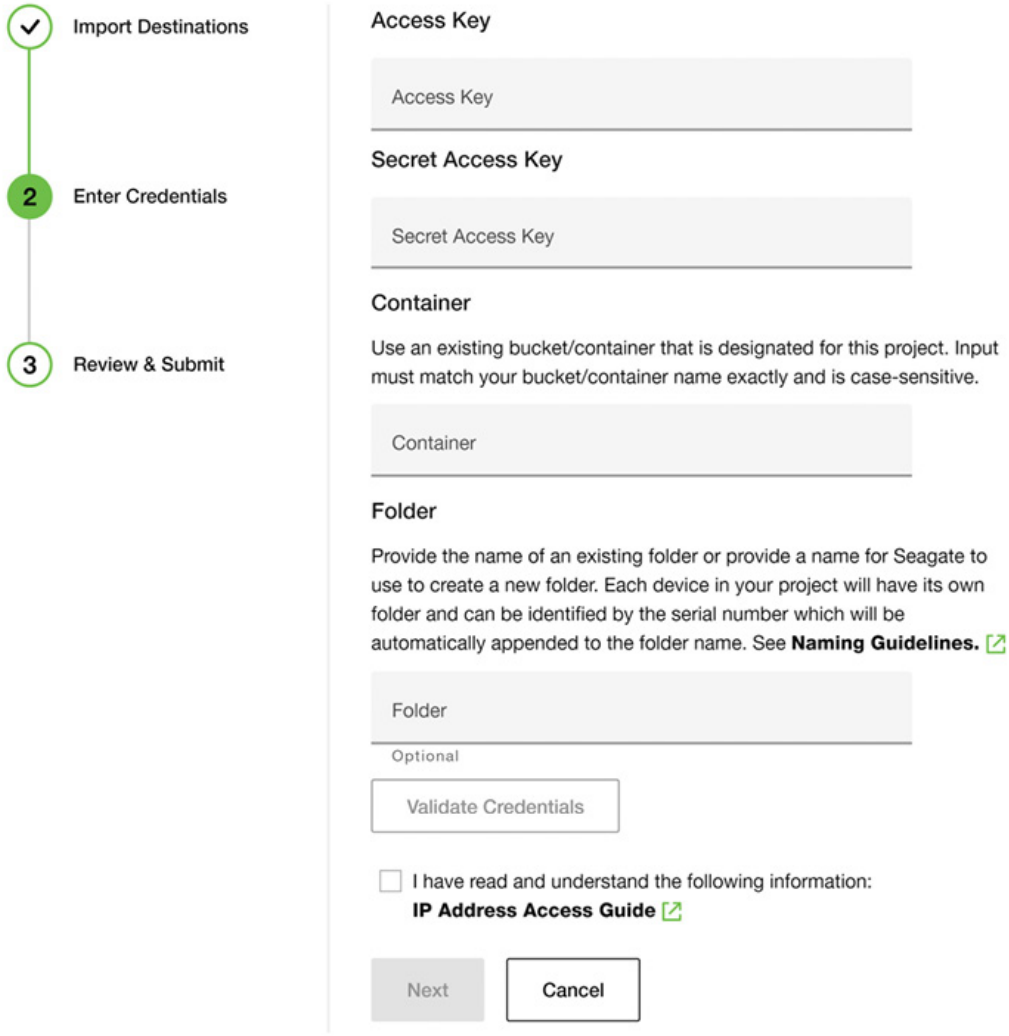
Important note on file sizes—In general, Seagate does not recommend importing individual files larger than 5TB. Please refer to your cloud provider's file size limitations and best practices.

Configure your import plan

Enter credentials

1. In Lyve Management Portal, click **Import Plans** in the navigation bar, and then click **Configure Plan**.
2. Enter your Access Key and Secret Access Key. (If you need to update the import destination first, click on the **Import Destinations** step and edit.)

> Characters you enter in these fields are always masked.



3. Enter your container name. The name is case-sensitive and must match exactly.
4. (Optional) Enter a name for your folder.

> Each storage device in your project 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.

5. Click **Validate Credentials** .

> If the validation fails, check that the access, secret access key, and container name entered are accurate, and then revalidate.

6. Check the box to confirm that you have read and understand the details in IP Address Access.
7. Click **Next**.

Review and submit your import plan

1. Review your import destination and credential details.
2. Check the box to confirm that you've read and understand the information in this reference guide.
3. Click **Submit Plan**.

Inviting another user to configure an import plan

If a different member of your organization needs to configure the import plan for a project, you can invite them to do so in Lyve Management Portal. See Invite Another User to Configure an Import Plan.

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, see Managing 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 Lyve project.

> **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.

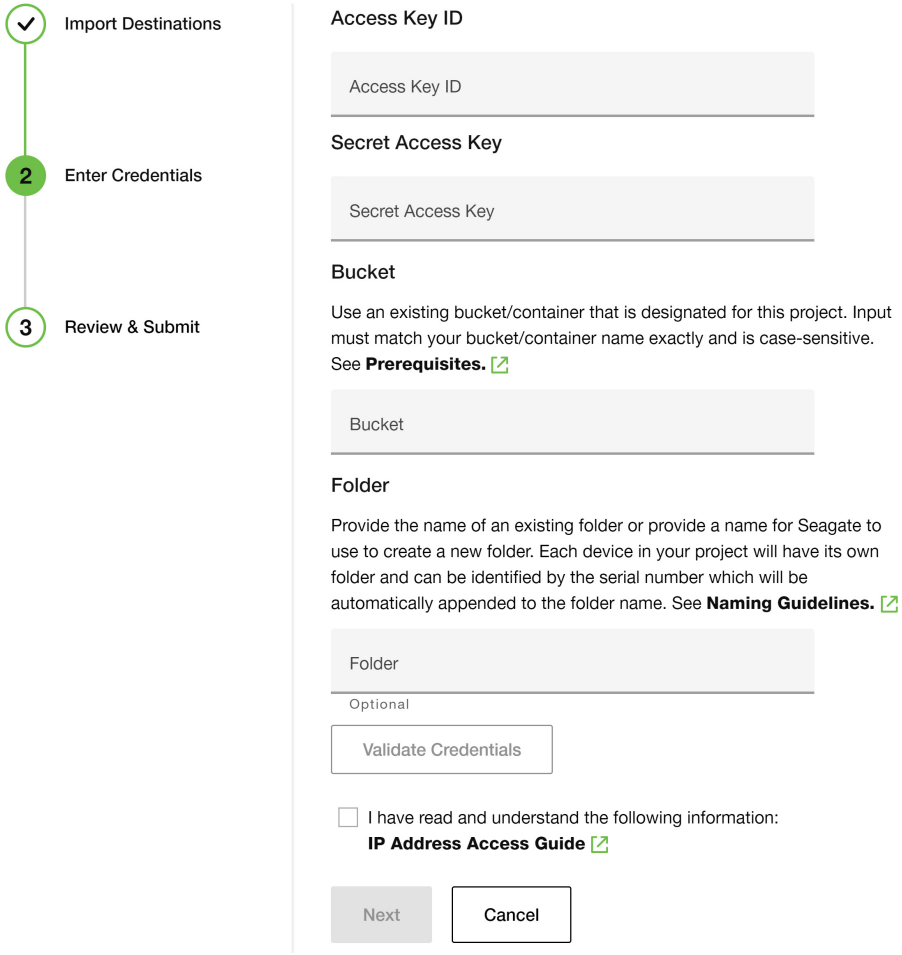
Configure your import plan

Enter credentials

An access key and secret key are required to authenticate requests to your cloud resources. To learn more, see Manage service account.

1. In Lyve Management Portal, click **Import Plans** in the navigation bar, and then click **Configure Plan**.
2. Enter your access key and secret key. (If you need to update the import destination first, click on the Import Destination step and edit.)

Characters you enter in security-related fields are always masked.



3. Enter your bucket name.
4. (Optional) Enter a name for your folder.

   Each storage device in your project 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.

5. Click **Validate Credentials** .

> ! If the validation fails, check that the access key, secret key, and bucket name entered are accurate, then revalidate.

6. Check the box to confirm that you have read and understand the details in IP Address Access.
7. Click **Next**.

Review and submit your import plan

1. Review your import destination and credential details. If you need to make changes to the credentials provided, click the Edit icon.
2. Check the box to confirm that you've read and understand the information in this reference guide.
3. Click **Submit Plan**.

Inviting another user to configure an import plan

If a different member of your organization needs to configure the import plan for a project, you can invite them to do so in Lyve Management Portal. See Invite Another User to Configure an Import Plan.

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

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, see Working 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 and Secret Key that are generated in a safe place.

Recommendations

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

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

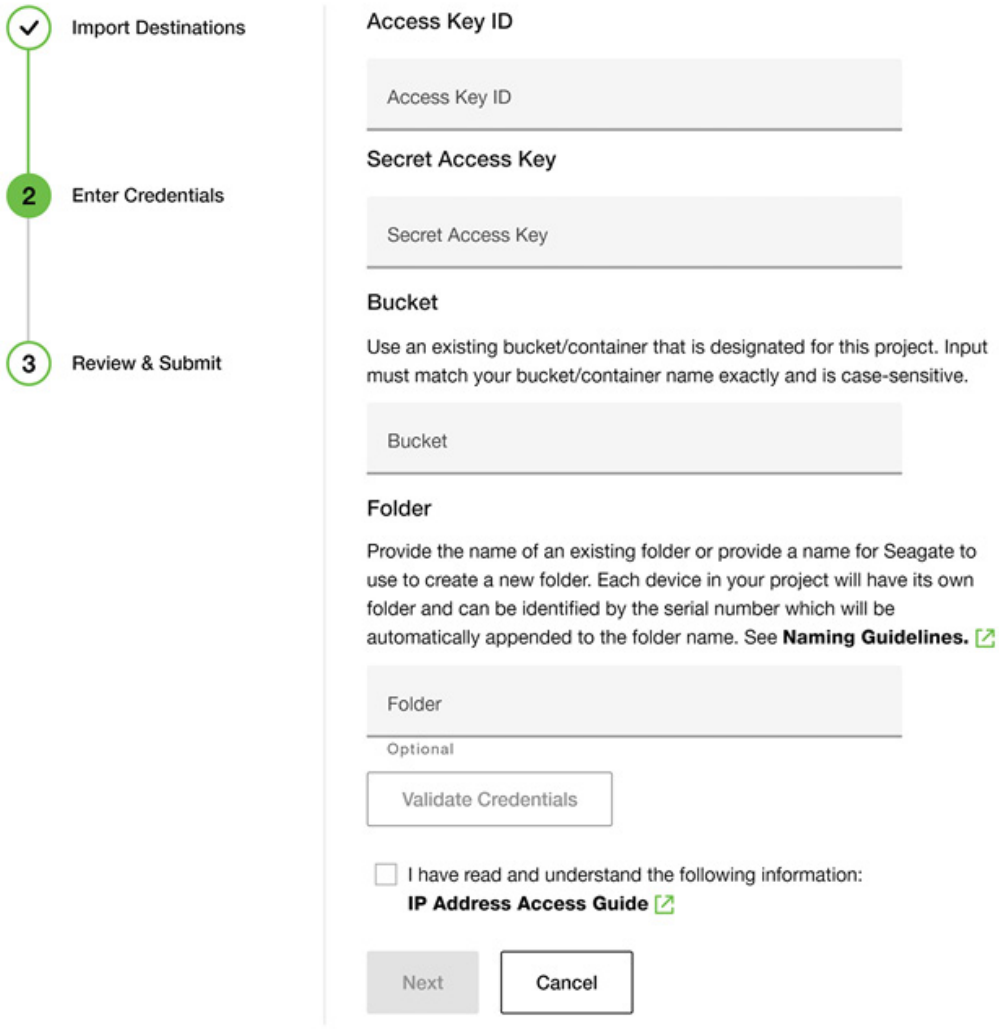
> **Important note on file sizes**—In general, Seagate does not recommend importing individual files larger than 5TB. Please refer to your cloud provider's file size limitations and best practices.

Configure your import plan

Enter credentials

1. In Lyve Management Portal, click **Import Plans** in the navigation bar, and then click **Configure Plan**.
2. Enter your Access Key ID and Secret Access Key. (If you need to update the import destination first, click on the **Import Destinations** step and edit.)

> Characters you enter in these fields are always masked.



3. Enter your bucket name. The name is case-sensitive and must match exactly.
4. (Optional) Enter a name for your folder.

> Each storage device in your project 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.

5. Click **Validate Credentials** .

> If the validation fails, check that the access ID, secret, and bucket name entered are accurate, and then revalidate.

6. Check the box to confirm that you have read and understand the details in IP Address Access.
7. Click **Next**.

Review and submit your import plan

1. Review your import destination and credential details.
2. Check the box to confirm that you've read and understand the information in this reference guide.
3. Click **Submit Plan**.

Inviting another user to configure an import plan

If a different member of your organization needs to configure the import plan for a project, you can invite them to do so in Lyve Management Portal. See Invite Another User to Configure an Import Plan.

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 User to Configure an Import Plan

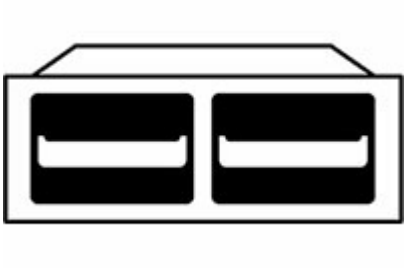
If a different member of your organization needs to configure the import plan for a project, you can invite them to do so in Lyve Management Portal.

1. Go to lyve.seagate.com and sign in. Enter a verification code to continue to Lyve Management Portal.
2. Click on the Account icon in the navigation bar and select **User Management.**
3. Click on the **Quick Action** dropdown menu and select **Add User**. Alternatively, click **Add User** in one of the user role descriptions.
4. Provide details for the new user such as their name and contact information.
5. Select the project(s) that you would like to assign to this user.
6. Select the import destination(s) that this user can view and add to import plans.

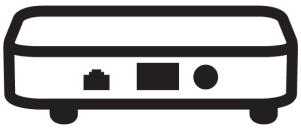
The invited user will receive an email with a link to register their account. The user will need to complete the account registration in order to configure the plan.

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

Sending a Lyve Mobile Array to a Seagate import site is a separate process from other types of hardware returns:

Returning a Lyve Mobile accessory— If you need to return an accessory, see How do I return a device? in the **Lyve Management Portal User Manual**.

Returning a Lyve Mobile Array for another reason—There may be situations in which you need to return a device for non-import reasons, for example, the device needs to be replaced. Contact your sales representative or customer success manager or, use the Lyve Virtual Assistant 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 Lyve Services page, go to the Lyve Mobile with Cloud Import card. Click on the **Manage Projects** dropdown and select **View Plans.**
3. From the Import Plans table, click on a project to expand the row and view the Mobile Arrays within that project.
4. Find the Mobile Array you would like to send to a Seagate import site and click **Send for Import**. This will initiate a cloud validation process which may take several minutes.

A cloud validation process is initiated. The process may take several minutes.

5. Once the validation is complete, click Print Shipping Label to view and print your shipping label in a separate browser tab.

Issues preventing successful validation

The validation may fail if there were issues with the following:

Security credentials provided in the import plan —You are prompted to edit the credentials and revalidate the import plan. In the Actions column, click the **Edit Credentials** button for the applicable project.

Connecting to the cloud destination—In the Actions column, click the **Troubleshoot** button for the applicable project. Follow the onscreen instructions.

Track Import Status

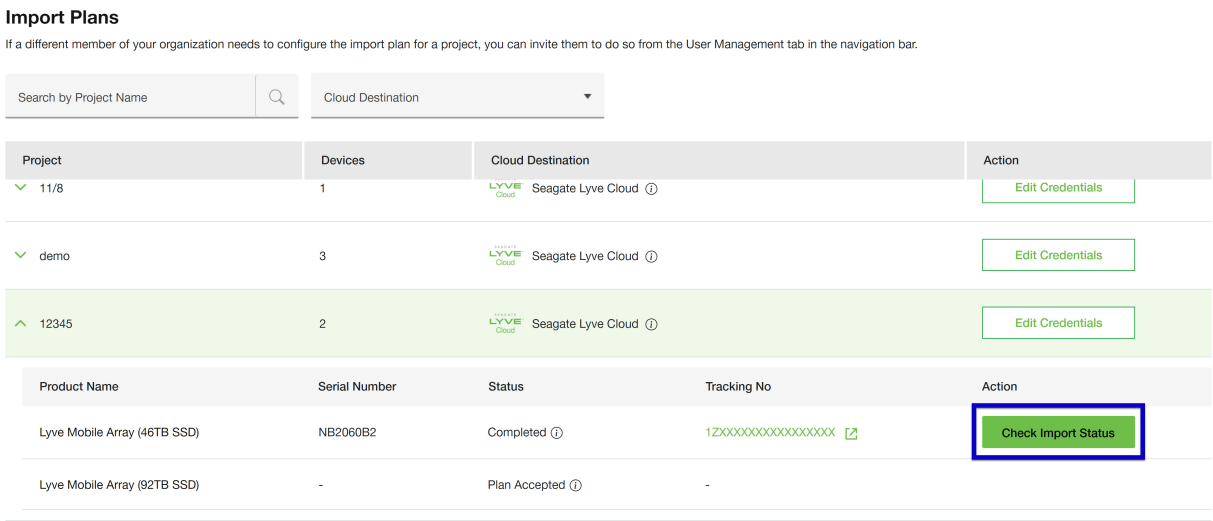
The status of your import plan(s) can be tracked in Lyve Management Portal.

1. Go to lyve.seagate.com and sign in. Enter a verification code to continue to Lyve Management Portal.
2. On the Lyve Services page, go to the Lyve Mobile with Cloud Import card. Click on the **Manage Projects** dropdown and select **View Plans.**
3. Find your project in the Import Plans table and click to expand it.
4. View the status of the import plan in the Status column. You can also hover over the infographic icons to see more information about a status.

> Projects with the orange warning icon contain import plan(s) that require one or more actions to be taken. Click the project to expand it and view the action(s) required.

Once a device has been received at the import site, you can track the status of the import by doing the following:

1. Click on a project to expand it.
2. Click the **Check Import Status** button next to a device.



Confirm Import Completion

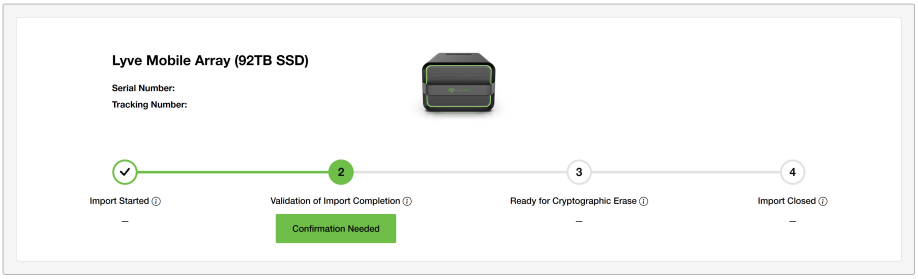
Upon completion of your cloud import, verify that your files have been successfully imported to your cloud destination.

> **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.

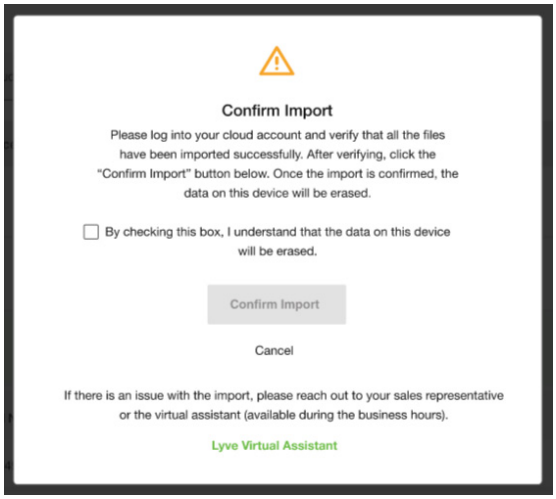
After verifying the files in your cloud destination, confirm the import in Lyve Management Portal.

> **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.

1. Go to lyve.seagate.com and sign in. Enter a verification code to continue to Lyve Management Portal.
2. On the Lyve Services page, go to the Lyve Mobile with Cloud Import card. Click on the **Manage Projects** dropdown and select **View Plans.**
3. Find your project in the Import Plans table and click to expand it.
4. Find the import plan for the applicable device and click **Check Import Status**.
5. Click **Confirmation Needed**.



6. Check the box to confirm your understanding of the device erasure.
7. Click **Confirm Import**.



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