SEAGATE

Lyve Client Software User Manual

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

Getting Started with Lyve Client Software

Welcome

Lyve Client lets you unlock and manage Lyve Mobile devices connected to your host computer.

Secure your devices—Industry-standard authentication key management lets you unlock your Lyve Mobile devices for use with a connected computer.

Your local data at a glance—View the status of connected Lyve Mobile devices, available storage capacities, and current data activities.

Workflow data management—Create worfklows to automate copying, moving, and deleting terabytes of data.

Lyve Management Portal credentials

To unlock and access Lyve Mobile devices connected to your computer, you must enter a username (email address) and password in the Lyve Client app. Your email address and password credentials were registered with Lyve Management Portal in one of two ways:

Account manager—You created a Lyve Management Portal account at lyve.seagate.com and set up your email address and password during registration.

Product admin or product user—You were identified as a product user for a project created in the Lyve Management Portal. An email was sent to you from the Lyve team inviting you to register your account.

If you haven't already registered your account, you should do so before attempting to unlock connected Lyve Mobile devices. The setup process allows you to:

- Create a password to manage your account and access connected Lyve Mobile devices.
- Establish 2-step verification for strong security.
- Register your account information with Lyve Management Portal.

If you can't remember your credentials or your email invitation period expired before you could register your account, visit lyve.seagate.com. Click **Sign in** and then click **Don't remember your password?**. If your email isn't recognized, contact your account manager. For further help, you can contact customer support using the Lyve Virtual Assist Chat at lyve.seagate.com.

Download and install Lyve Client Software

Install Lyve Client on any computer intended to connect to your Lyve Mobile device.

Links to the installer can be found on Lyve Management Portal:

1. Log in to lyve.seagate.com.
2. On the Home page, click **Downloads**.
3. At the prompt, click **Download** for either Windows® or macOS®.
4. Go the folder where you receive downloads and open the installer.
5. Follow the onscreen instructions to complete the setup and open Lyve Client.

You can also download Lyve Client installers from the support page at www.seagate.com/support/lyve-client.

Authorize host computers

Open Lyve Client on a computer intended to host your Lyve Mobile device.

> An internet connection is required when authorizing a host computer.

1. When prompted, enter your Lyve Management Portal email address and password.
2. Lyve Client authorizes the host computer to unlock and access Lyve devices and manage projects on the Lyve Management Portal.

> The host computer remains authorized for a period of time, during which you can unlock and access connected devices even without an internet connection. You'll need to periodically open Lyve Client on the computer and re-enter your credentials.

Key Terms

Host computer

A computer installed with Lyve Client used to access assigned Lyve Mobile devices.

Lyve Client

An app used to unlock specific Lyve Mobile devices. Lyve Client can be used to access devices using Lyve Portal Identity and/or Lyve Token Security.

Lyve Portal Identity

Security option that allows an end user to enter a username and password to authorize host computers to access connected Lyve Mobile devices. End users must have a Lyve user account. Internet connectivity is required during sign-in and when periodically reauthorizing a host computer. SeeAccessing Devices with Lyve Portal Identity.

Lyve Token file

An encrypted security token file authorizing a host computer to access specific Lyve Mobile devices.

Lyve Token Security

Security option that allows for use cases in which there is limited access to the internet when using Lyve Mobile Arrays. End users are not required to have a Lyve user account. Instead, the end user creates a registration file for the computer in Lyve Client and then sends it to the project administrator. The project administrator uses that registration file to generate a Lyve Token file in Lyve Management Portal and then sends it to the end user. Internet connectivity is required to download the installer for Lyve Client, but is not required when accessing devices with Lyve Token files. SeeAccessing Devices with Lyve Token Security.

Product admin

Administrator in the account permitted to:

- Register host computers.
- Assign Lyve Mobile devices to host computers.
- Issue Lyve Token files.

Product end user

End user accessing Lyve Mobile storage devices from a connected computer.

Registration file

A JSON file certifying Lyve Client on a specific host computer.

- A product end user downloads a registration file from Lyve Client running on the host computer.
- The registration file is sent to a product admin, who uses it to produce a Lyve Token file.

> **Registration files cannot be transferred between host computers or installations of Lyve Client.** If an end user uninstalls/reinstalls Lyve Client, they'll need to download new registration files to send to their product admin.

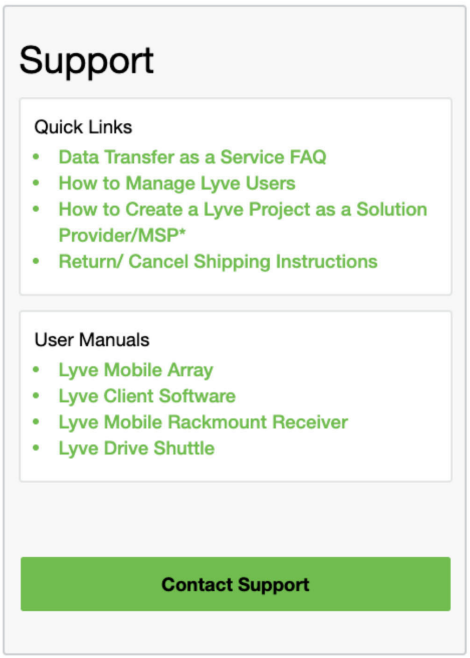
Unlocker

In Lyve Management Portal, an unlocker has the correct security permissions to unlock one or more Lyve Mobile Arrays. For example, an instance of Lyve Client installed on a host PC. Multiple Lyve Mobile Arrays can be assigned to a single unlocker, or to multiple unlockers.

Lyve Virtual Assistant

If you need to contact support, go to lyve.seagate.com and click on the Lyve Virtual Assistant icon to start a support session. Lyve Virtual Assistant is available throughout the Lyve Management Portal.

> You must upload a registration file and enter a name before you can click Seagate Virtual Assistant is only available during regional business hours of 8:00 AM-5:00 PM US Central Time and 8:00 AM-5:00 PM Central European Time.



Connection Types

Lyve Client can manage security for Lyve Mobile Arrays connected directly to the host PC or via the network using Lyve Mobile Rackmount Receiver.

> Make sure Lyve Mobile Array is powered on before connecting it to a computer.

Direct-Attached Storage (DAS) connections

USB and Thunderbolt

Lyve Mobile Array	Cable	Computer port
Host port (USB-C connector)	Thunderbolt™ 3	Thunderbolt 3 / Thunderbolt 4
Host port (USB-C connector)	USB-C to USB-C	USB 3.1 Gen 1 or higher
Host port (USB-C connector)	USB-C to USB-A	USB 3.0 or higher

For more connection details, see the following:

- Lyve Mobile Array User Manual

Lyve Mobile PCIe Adapter

Lyve Mobile PCIe Adapter	Cable
Ethernet port (device configuration)	Ethernet
PCIe NVMe 12Gb x2 SFF-8644 (data)	SFF-8644

For more connection details, see the following:

- Lyve Mobile Mount and PCIe Adapter User Manual
- Lyve Mobile Mount and PCIe Adapter - Front Loader User Manual

Rackmount Receiver connections

Lyve Mobile Rackmount Receiver	Cable
Ethernet port (device configuration)	Ethernet
FC 32Gb (data)	Fibre
FC 16Gb (data)	Fibre
iSCSI 25Gb (data)	Fibre (optical or copper)
iSCSI 10GbaseT (data)	Ethernet
SAS 12Gb (data)	SAS

For more connection details, see the following:

Lyve Mobile Rackmount Receiver User Manual
FC Network Setup for Windows
FC Network Setup for Linux (RHEL/CentOS 8)
FC Network Setup for Linux (Debian/Ubuntu)
iSCSI Network Setup for Windows
iSCSI Network Setup for Linux (RHEL/CentOS 8)
iSCSI Network Setup for Linux (Ubuntu/Debian)
SAS Network Setup for Windows
SAS Network Setup for Linux (RHEL/CentOS)
SAS Network Setup for Linux (Debian/Ubuntu)

IP addressing for networked and DAS connections

Make sure your anti-virus, firewall or VPN security settings allow port access to Lyve Client.

State	Access type	Port
Before device discovery	The application and device must be able to communicate via SLP.	UDP port 427

State	Access type	Port
After device discovery	The application and device must be able to communicate via SSH.	TCP port 22

In both states, it is assumed that the device has been assigned an IP address by a local DHCP server or has been assigned a static IP address.

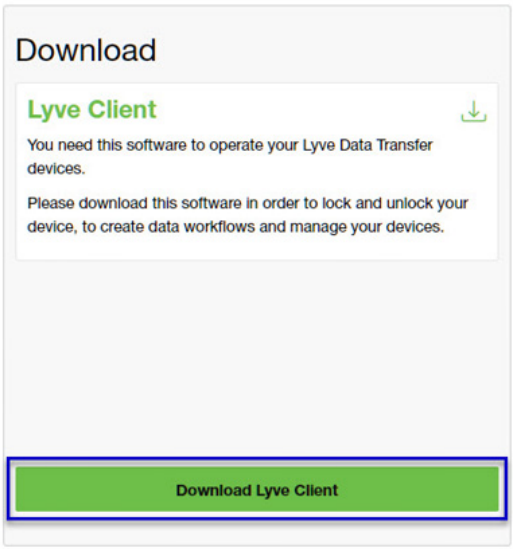
- All Lyve Mobile devices are in DHCP mode by default. If an IP is not assigned via DHCP, the device will generate its own IP address: 169.254.100.123.
- Any host on the same subnet can see the device and communicate with it using this address.
  - In DAS mode via a Thunderbolt/USB-C connection, this is the address that is used to communicate with the device.

Download and Install Lyve Client

Install Lyve Client on computers you intend to connect to your Lyve Mobile devices or manage on the network. Lyve Client is available for Windows and macOS.

Links to the installer can be found on Lyve Management Portal:

1. Go to lyve.seagate.com and sign in.
2. On the Home page, click **Download Lyve Client.**



3. At the prompt, click **Download** for either Windows® or macOS®.

> You can also download Lyve Client installers from the support page at www.seagate.com/support/lyve-client

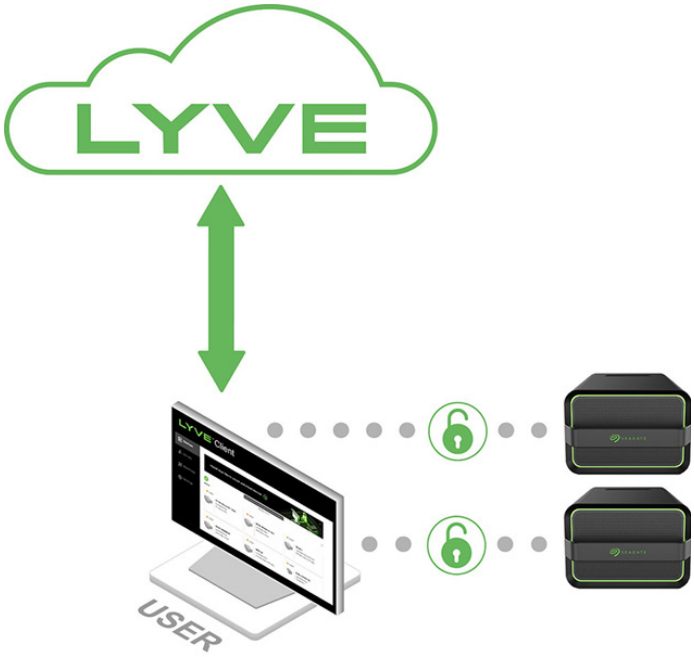
4. Go the folder where you receive downloads and open the installer.
5. Follow the onscreen instructions to complete the setup and open Lyve Client.

Accessing Devices with Lyve Portal Identity

The Lyve Portal Identity security option lets you unlock connected Lyve devices by entering a username and password in Lyve Client.

> An internet connection is required when signing in.

After you've signed in, Lyve Client is authorized to unlock and access assigned Lyve devices. Lyve Client remains authorized for up to 30 days of active use or 15 days of inactivity. Once the authorization period has elapsed, you must sign in again with your username and password to access connected devices.



Requirements

- Product admin has invited the product end user to be added to the account in Lyve Management Portal.
- Product admin set up projects, added devices to projects, and assigned the product end user to the same projects.
- Devices have been delivered to the product end user.
- End user has downloaded and installed Lyve Client on a computer they will use to unlock Lyve Mobile devices.

> **Important**—Lyve Portal Identity must be enabled in the Lyve Client settings. See Settings.

Important—If Lyve Client is used behind a proxy or firewall, ensure that the following domains are allow.

- https://lmp-prod.us.auth0.com/
- https://rest.lyve.seagate.com/
- https://lyve.seagate.com/

Sign in using Lyve Client

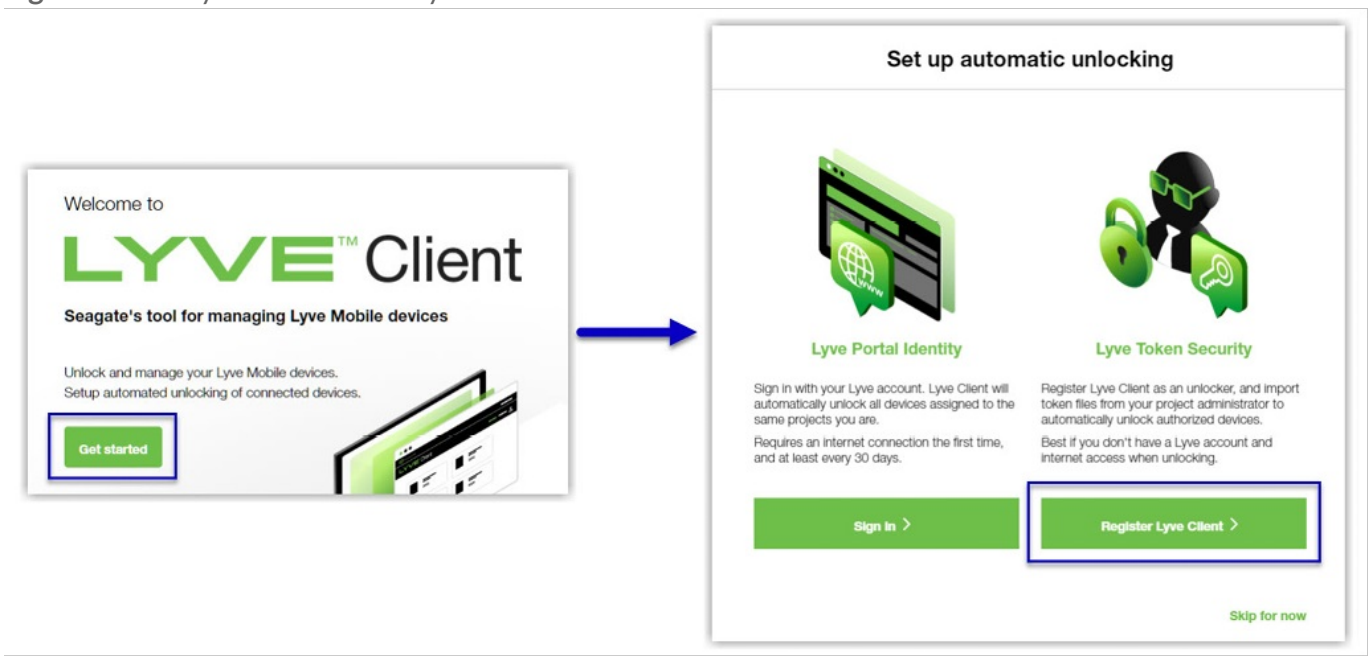
You created a username and password in Lyve Management Portal in one of two ways, depending on your role in the account:

Account creator—You set up an email address, username, and password when you initially created the account.

Other role—A user manager added your email address to an account, org, or project in Lyve Management Portal. An email was sent to you from Lyve Management Portal inviting you to set up your username and password.

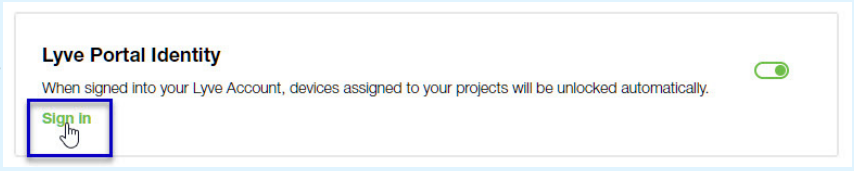
If you don't have a username and password, seeUsers with no username/password below

If you're opening Lyve Client for the first time, click**Get Started** on the Welcome screen, and then click **Sign in** under Lyve Portal Identity:

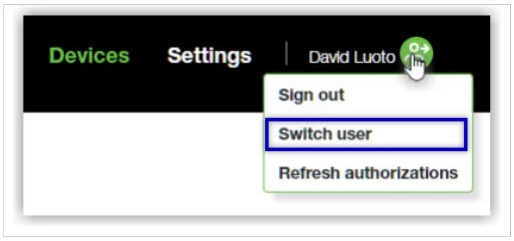


If Lyve Client has been opened previously but no user is currently signed in, click on the user icon in the navigation bar:

Alternatively, click **Settings** in the navigation bar and then click**Sign in** under Lyve Portal Identity.



If another user is currently signed in and you want to switch users, click on the user icon in the navigation bar and select **Switch user**:



Device locking

Lyve Client must be open and you must be signed in to access connected Lyve Mobile Arrays. A Lyve Mobile Array will lock when:

- The computer running Lyve Client goes to sleep.
- Lyve Mobile Array is ejected.
- Lyve Mobile Array is disconnected from the computer or network.
- Lyve Mobile Array is powered off.

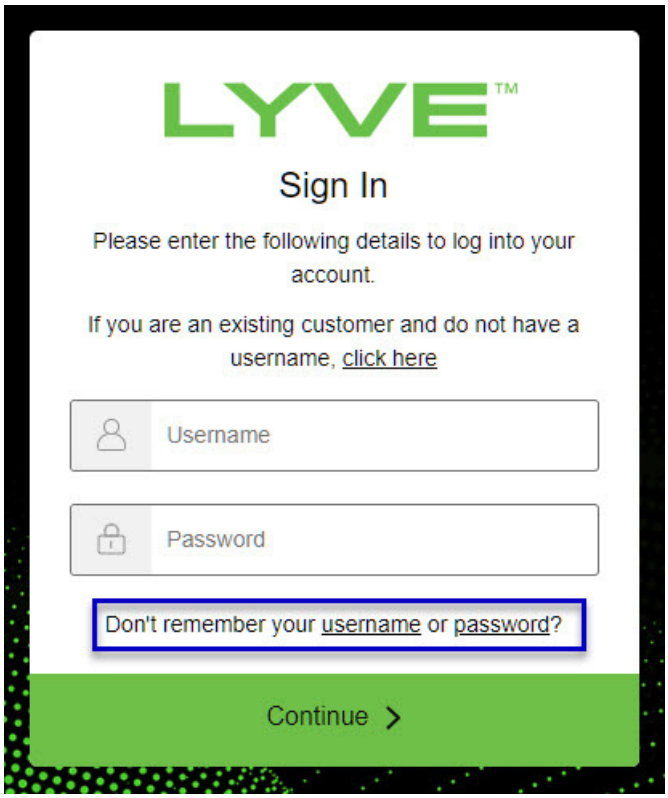
Use Lyve Client to unlock Lyve Mobile Array again once the computer has been awakened or the device has been reconnected and powered on.

Forgotten username and/or password

If you can't remember your username or password:

1. Go to lyve.seagate.com.
2. Click **Sign In** in the navigation bar:

3. In the Sign In dialog, click on the link for a forgotten username or password:



4. Follow the onscreen instructions for recovering your username or changing your password.

Users with no username and password

You need a username and password to unlock connected Lyve Mobile devices. The setup process lets you:

- Create a username/password connected to your email address.
- Establish 2-step verification for strong security.

You might not have a username and password for one of the following reasons:

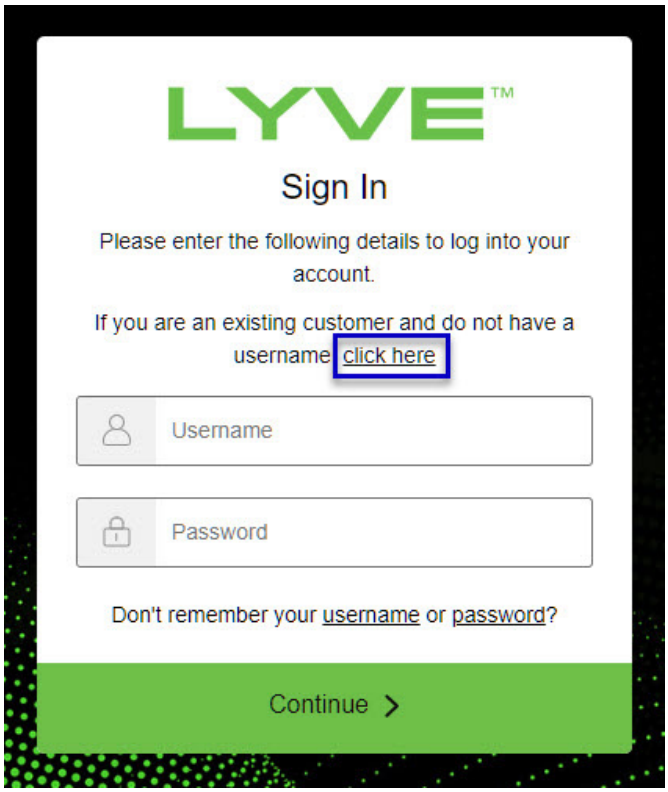
Issue	Resolution
A user manager in the account has not added you as a user.	Contact a user manager in the account and request to be added as a user.

Issue	Resolution
Your email invitation is expired.	If the email invitation sent to you expired before you could register as a user, you can have Lyve Management Portal resend an invitation. See Resend an email invitation below.

Resend an email invitation

1. Go to lyve.seagate.com.
2. Click **Sign In** in the navigation bar:

3. Click on the link for existing customers who do not have a username:

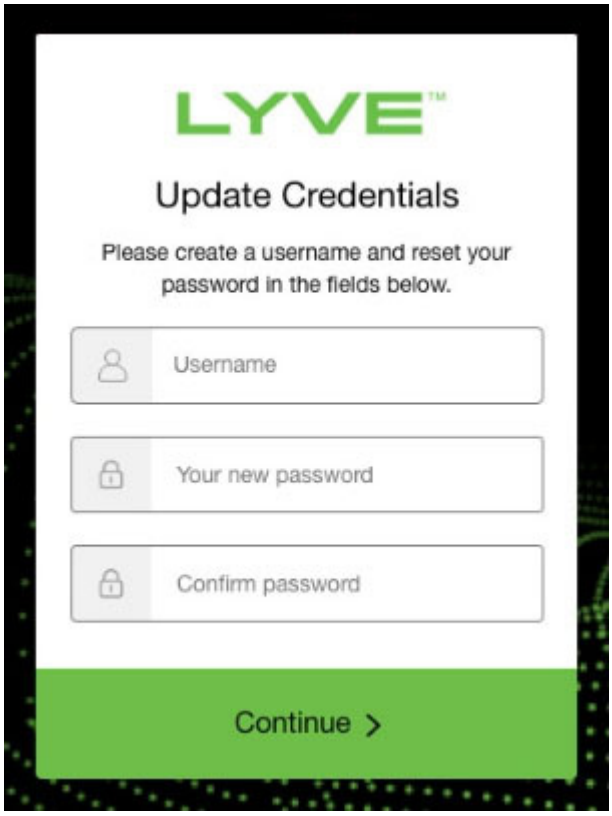


4. Enter your email address and click **Continue**. After a few minutes, Lyve Management Portal will send you a new email invitation. Check your inbox for the message.

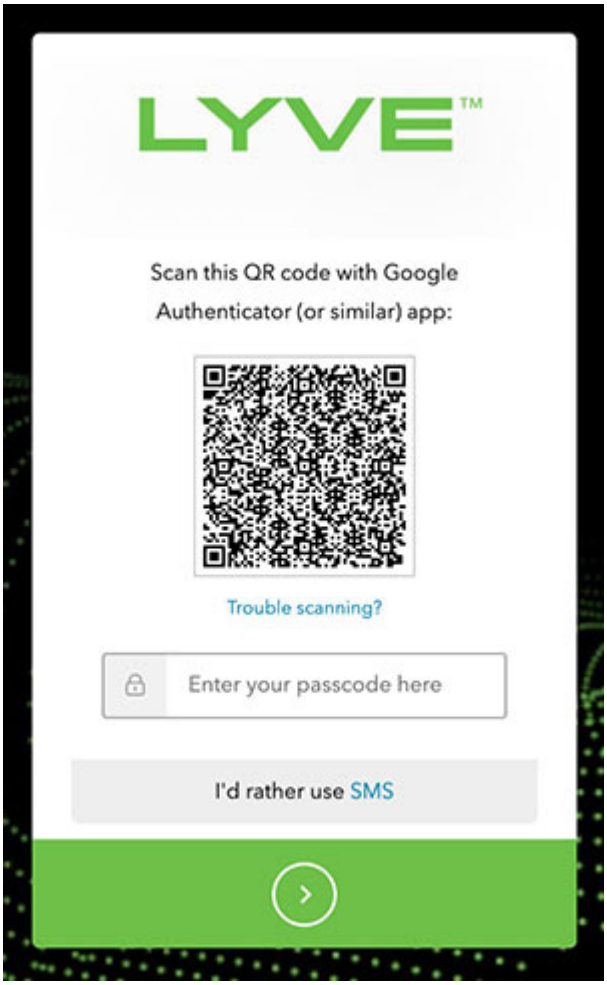
> If you didn't see the email in your inbox after a few minutes, check your spam folder. If you can't find it there, click **Resend Email** in Lyve Client. If you need to contact support, use the Lyve Virtual Assistant icon to start a support session.

5. Open the email and click on the **Register Your Account** button.

6. Enter a username and password. Confirm the password, and then click **Continue**.

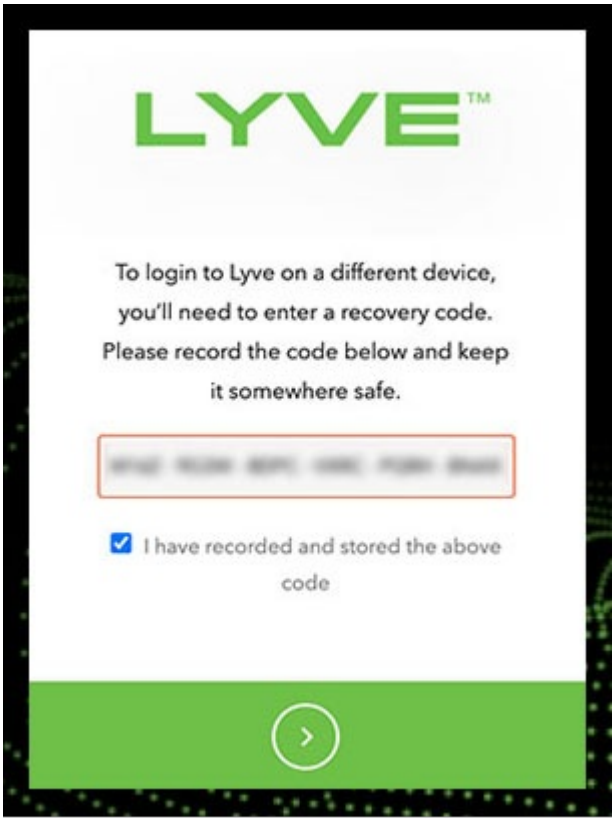


7. Use an authenticator app such as Google Authenticator or Microsoft Authenticator to scan the QR code and receive a passcode. Enter your passcode and click the icon to continue.



> Alternatively, you can receive a passcode via SMS. Click the **SMS** option and enter your phone number to receive the 6-digit verification code. Note that carrier charges may apply. Enter the verification code sent to your phone and click the icon to continue.

8. You're asked to record a recovery code. A recovery code lets you log in to Lyve Management Portal from other devices. Copy the recovery code and keep it in a safe place. Once it's recorded, check the confirmation box and click the icon to continue.



Refreshing authorizations

If the product end user's project/device assignments have been changed by a product admin in Lyve Management Portal, they can refresh their authorizations in Lyve Client.

> An internet connection is required when refreshing authorizations.

1. Open Lyve Client.
2. Click on the **Settings** tab.
3. Click **Refresh authorizations**.

Accessing Devices with Lyve Token Security

The Lyve Token Security option lets you configure a registered computer installed with Lyve Client to automatically unlock assigned Lyve Mobile devices. Once configured, Lyve Client will unlock devices, even when there's no access to Lyve Management Portal.

Requirements

- Product admin has set up projects and added devices to projects.
- Devices have been delivered to the product end user.
- End user has downloaded and installed Lyve Client on the computer they will use to unlock Lyve Mobile devices.

"

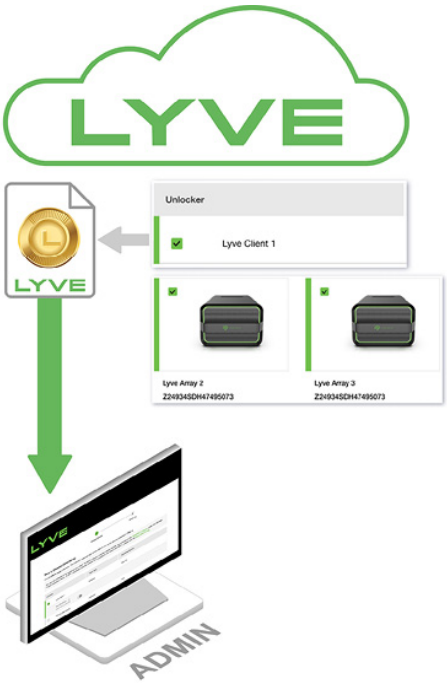
> **Important**—Lyve Token Security must be enabled in the Lyve Client settings. See Settings.

Process

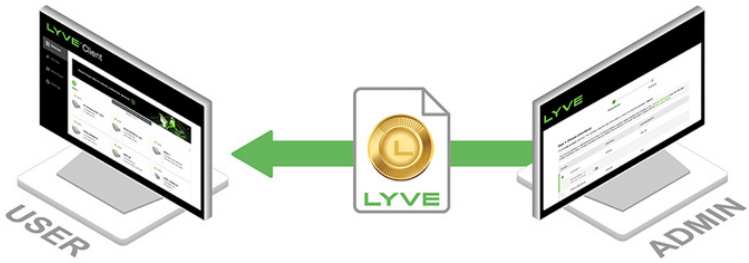
Product end user opens Lyve Client on a host computer and creates a registration file. End user sends the registration file to a product admin.

Admin uploads the registration file to the Lyve Management Portal and registers the Lyve Client installation as an unlocker.

Admin assigns devices to the unlocker and downloads an encrypted Lyve Token file authorizing the unlocker to access Lyve Mobile devices.



Admin sends the token file to the user.



User imports the token file into Lyve Client. Lyve Client is now authorized to unlock assigned Lyve Mobile devices with no connection to Lyve Management Portal.

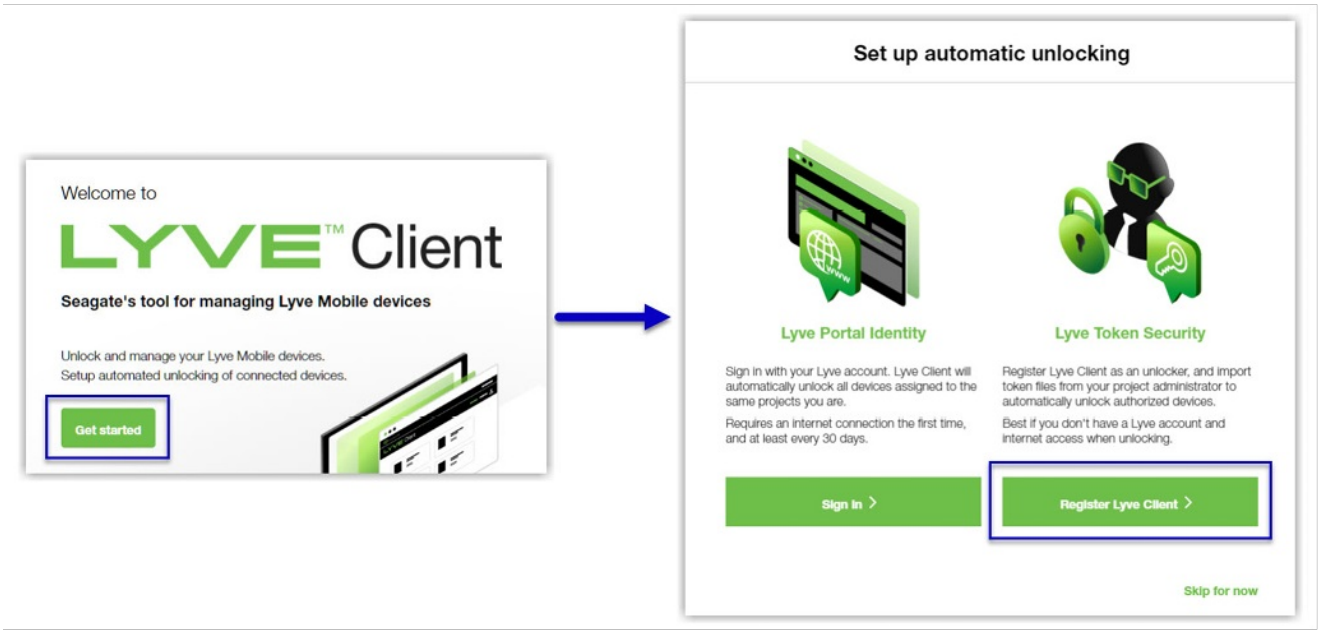
End user initial tasks

Create a registration file

You will need a registration file for each host computer/Lyve Client installation used to access Lyve Mobile devices.

1. Open Lyve Client.

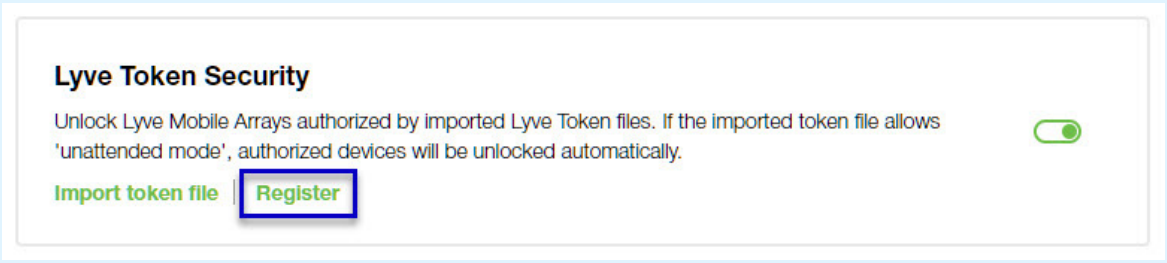
   If you're opening Lyve Client for the first time, click **Get Started** on the Welcome screen, and then click **Register Lyve Client** under Lyve Token Security.



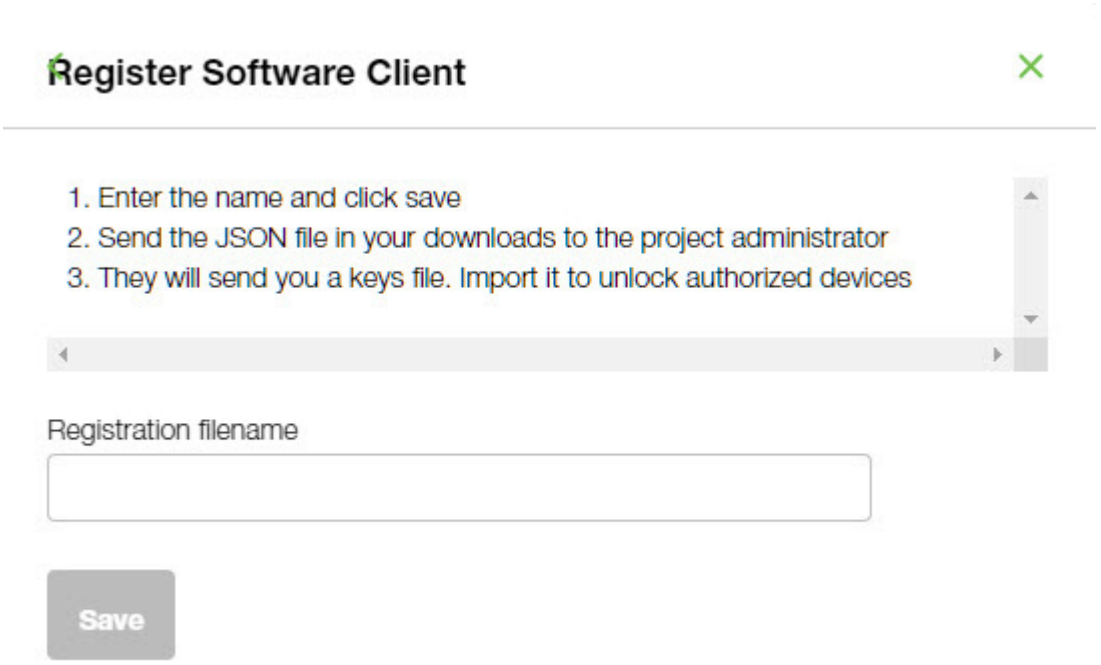
   If Lyve Client was opened previously, click on the **Devices** tab, and then click the banner:

Alternatively, click on the Settings tab and then click**Register**

.



2. In the dialog, enter a filename and click**Save**.



3. Confirm the location for the download and click**Save**. A JSON (.json) file is downloaded to the location you specified.

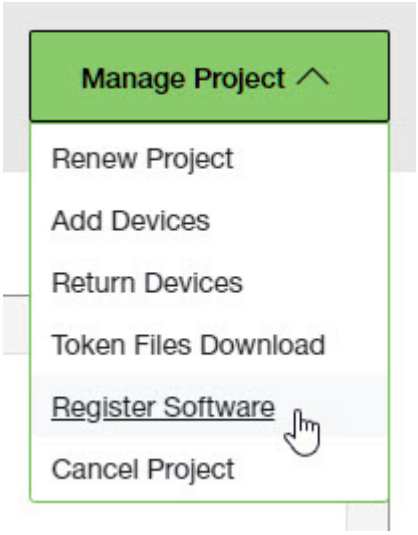
Send the registration file to your product admin

Using a file browser such as File Explorer or Finder, locate the downloaded registration file. Share it with your product admin using your preferred means of business communication (such as email, chat, or sending on a USB drive).

Admin tasks

Register the Lyve Client installation as an unlocker

1. Go to lyve.seagate.com and sign in.
2. Click **Projects** in the navigation bar.
3. Click on a project.
4. On the Project Details page, click on the **Manage Project** dropdown and select **Register Software**.



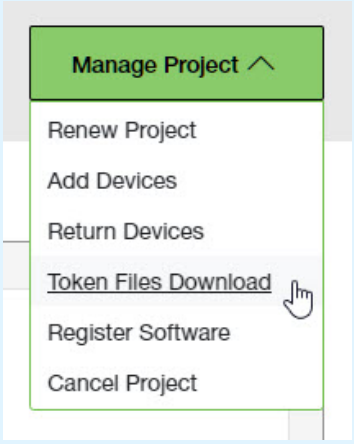
5. In the Register Software Client dialog, click **Attach File**.
6. Navigate to the location where you are storing the registration file you received from a product end user. Select the file and click **Attach File**.
7. Enter a name for the Lyve Client installation. Choose any friendly name that helps you differentiate one product end user/Lyve Client installation from another.
8. Click **Register**.
9. When the registration is completed, click **Close**.

> You must upload a registration file and enter a name before you can click **Register**.

Choose unlockers and assign devices

1. In the confirmation dialog, click the **Token Files Download** link.

If you're no longer viewing the confirmation dialog, go to the Project Details page and select **Token Files Download** from the **Manage Projects** dropdown.



2. Click checkboxes to select one or more unlockers. Selected unlockers will be permitted to unlock the devices you specify.

3. For each unlocker, use the **Save File to Unlocker** toggle to specify whether or not the product end user can store the unlocker in the Lyve Client app.
   - **Enabled**—Lyve Token file can be imported and stored in Lyve Client, allowing the host computer to unlock assigned devices whenever they're connected.
   - **Disabled**— Lyve Token file may only be used to unlock assigned drives for the current session. The file is not deleted from its location on the host computer, but it must be reselected each time the end user wants to use it.

4. Click checkboxes to select one or more devices. Selected devices can be unlocked by any of the unlockers selected in step 1.

Lyve Mobile Array (96TB HDD)

NB26003C

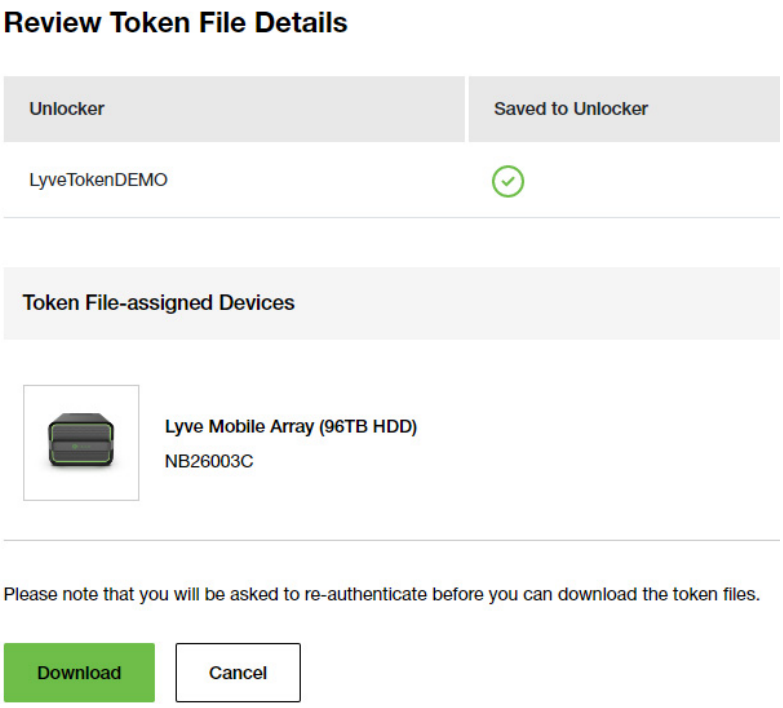
> If you don’t know a device’s serial number, you can find it by scanning the QR code on the left side of the Lyve Mobile Array handle.
>
> 
>
>
> Do not confuse the QR code on the handle with the QR code on the back of Lyve Mobile Array, which is clearly marked PSID. The PSID is not the same as the serial number.
>
> If the serial number on the handle is unreadable or doesn't work, use the Lyve Virtual Assistant icon to start a support session.

5. Click **Continue**.

Download Lyve Token files

> Note that in the following steps you’ll need to provide your Lyve Management Portal password and multifactor authentication before your Lyve Token files will be downloaded.

1. Review the details of the Lyve Token file you created.
2. Click **Download**.



3. At the prompt, enter your Lyve Management Portal password and click on the icon to continue.
4. A dialog informs you that the Lyve Token file has been downloaded. Click **Close**.
5. Using a file browser such as File Explorer or Finder, locate the file in the folder where you receive downloads.

> The filename is a unique identifier followed by the date it was created. Once the file is downloaded, you can rename the file.

Send the Lyve Token file to the product end user

Share the Lyve Token file you downloaded with the appropriate product end user using your preferred means of business communication (such as email, chat, or sending on a USB drive).

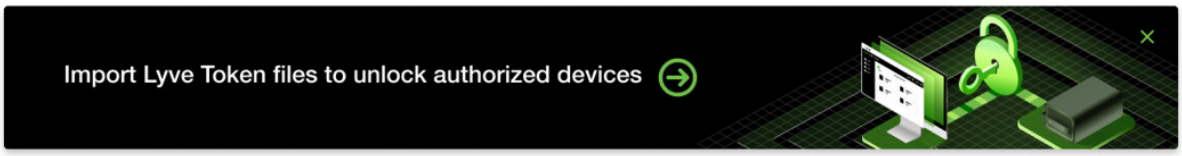
End user final tasks

Download the Lyve Token file

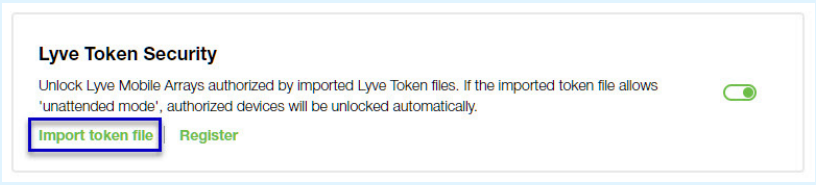
Download the Lyve Token file you received from yourproduct admin to the appropriate host computer that will be accessing Lyve Mobile devices.

Import Lyve Token file and/or unlock devices

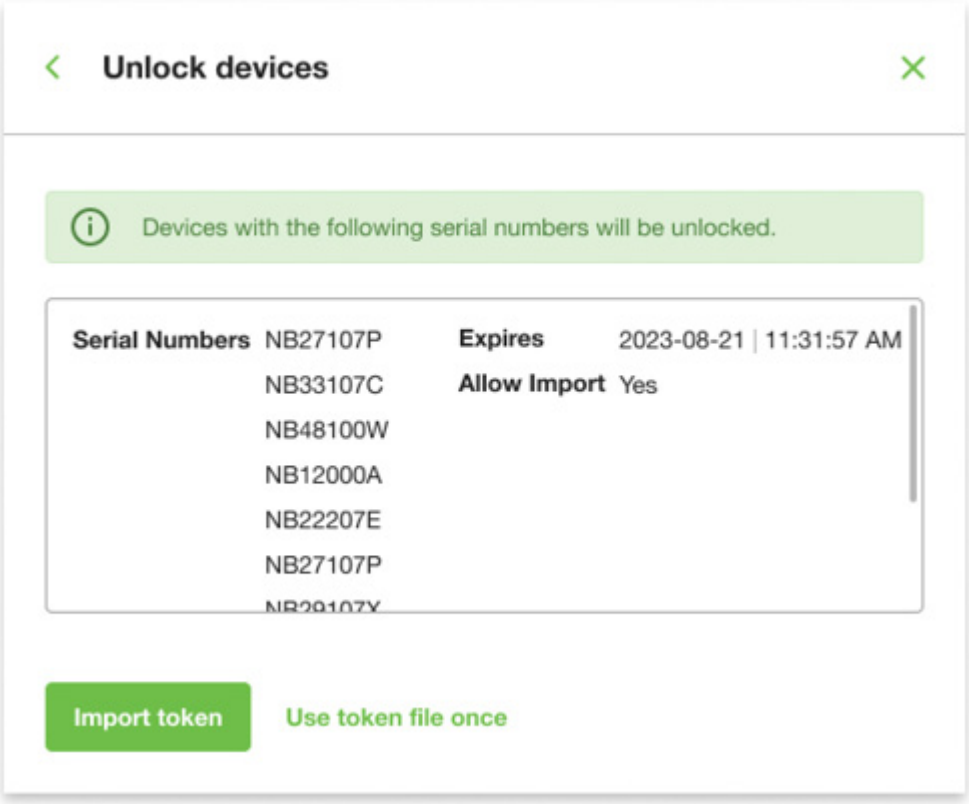
1. On the host computer, open the Lyve Client app.
2. Click on the **Devices** tab and then click the banner.



Alternatively, click on the Settings tab and then click Import token file:



3. Use the folder tree to find the location of the downloaded Lyve Token file (.json). Select the appropriate file and click **Inspect File.**
4. Review the details of the file:



The following information is available:

Detail	Description
Serial Numbers	Specific devices the Lyve Token file is permitted to unlock.
Expires	Date/time when the Lyve Token file becomes invalid.

Detail	Description
Allow Import	**Yes**—Lyve Token file can be stored in the Lyve Client app. **No**—Lyve Token file may only be used to temporarily unlock drives.

Check the serial numbers reported in Lyve Client correspond to the serial numbers of the Lyve Mobile Arrays you want to access. If you don't know a device's serial number, you can find it by scanning the QR code on the left side of the Lyve Mobile Array handle.

Do not confuse the QR code on the handle with the QR code on the back of Lyve Mobile Array, which is clearly marked PSID. The PSID is not the same as the serial number.

If the serial number on the handle is unreadable or doesn't work, use the Lyve Virtual Assistant icon to start a support session.

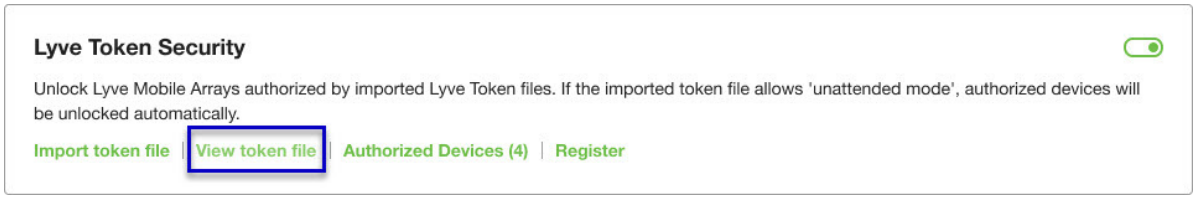
5. Click one of the following:

Import Lyve Token file	Imports the Lyve Token file to Lyve Client, allowing for automatic unlock of assigned devices. Once imported, the file is removed from its location and is no longer available for selection.
Use Lyve Token file once	Allows Lyve Client to unlock assigned devices for the current session. The file is not deleted from its location. You must reselect it each time you want to use it.

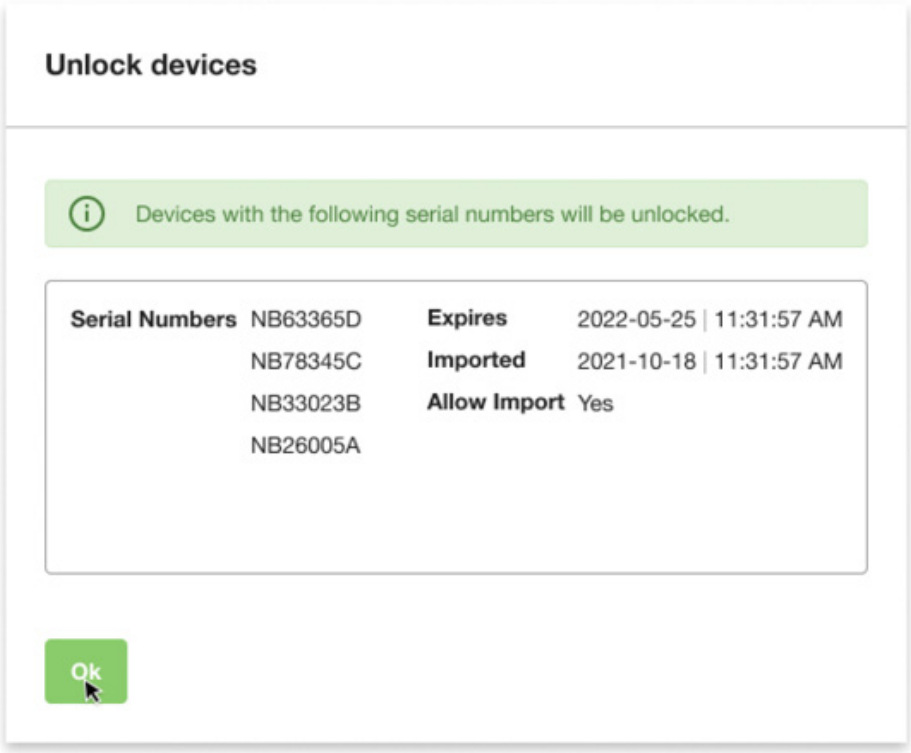
Viewing Lyve Token files

You can view an image of the most recent Lyve Token file imported into Lyve Client.

1. Open Lyve Client.
2. Click on the **Settings** tab.
3. Click **View token file**.



4. Review details of the recently imported file:



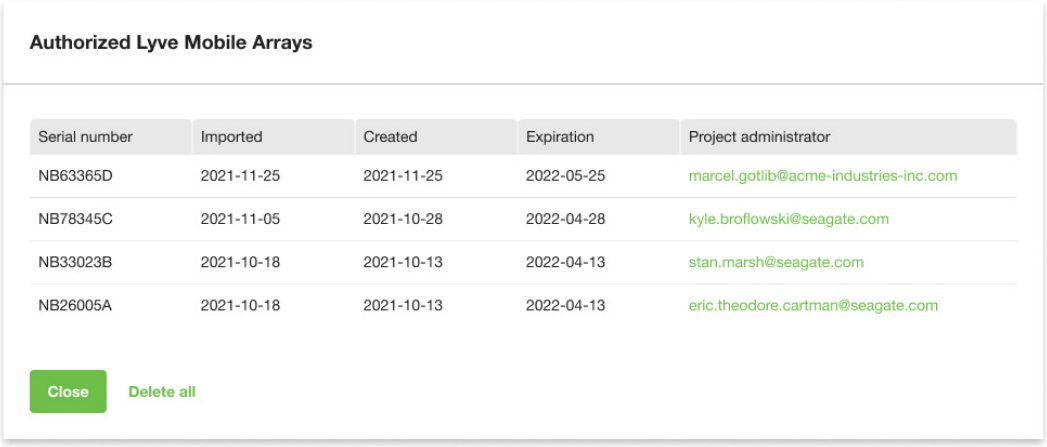
5. Click **OK**.

Viewing authorized devices

You can view an image of the most recent Lyve Token file imported into Lyve Client.

1. Open Lyve Client.
2. Click on the **Settings** tab.
3. Click **Authorized Devices**.

4. Review details of the devices Lyve Client is currently authorized to access:



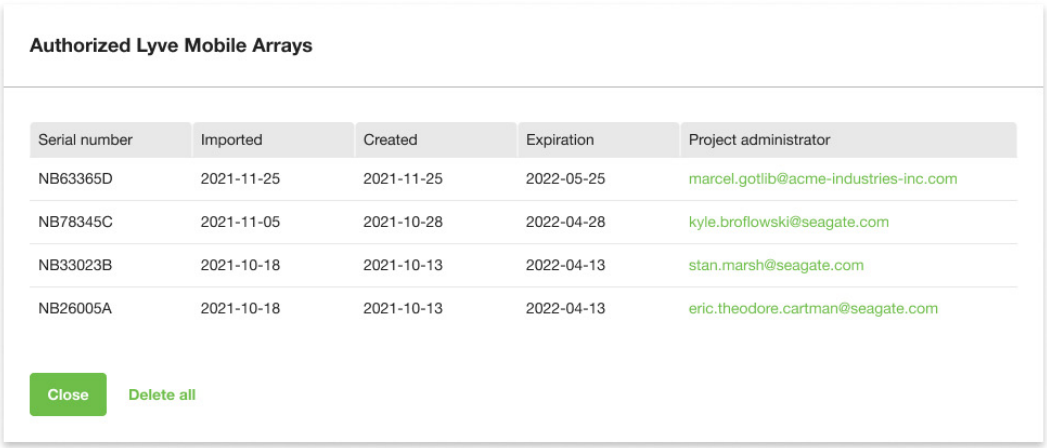
5. Click **Close**.

Deleting Lyve Token device authorizations

You can delete specific device authorizations from Lyve Client.

1. Open Lyve Client.
2. Click on the **Settings** tab.
3. Click **Authorized Devices**.

4. Review the list of devices Lyve Client is currently authorized to access:



5. Hover over the device and click the Delete icon.

> **i** Alternatively, if you want to delete all device authorizations, click**Delete all**.

6. Confirm that you want to continue with the deletion.
7. Delete additional devices, or click**Close**

File issue notifications

Issues with a Lyve Token file may prompt the following messages:

Message	Notes
Devices with the following serial numbers were found in the token file, but failed to unlock: [serial numbers]	A device or configuration issue is preventing the device from being accessed. Contact Lyve Mobile support using theLyve Virtual Assistant.
The file you've selected is corrupt or is not a token file at all. It cannot be imported or used to unlock devices.	Lyve Client does not recognize the file as a Lyve Token file. Select a different Lyve Token file or request a new Lyve Token file from your product admin.
The selected Lyve Token file cannot be used with this installation of Lyve Client. Select a different token file or register Lyve Client and request a new token file from your project administrator.	This Lyve Client installation is not designated as the unlocker in this Lyve Token file. Select a different Lyve Token file or request a new Lyve Token file from your product admin.
The selected Lyve Token file does not authorize Lyve Client to unlock this device. Devices with the following serial numbers will be unlocked.	The Lyve Token file you attempted to import is not authorized to unlock the selected device. Select a different Lyve Token file or request a new Lyve Token file from your product admin that assigns the device to this installation of Lyve Client.
This token file has expired. Request a new token file from your project administrator.	The Lyve Token file has passed its expiration date. Request a new Lyve Token file from your product admin.

Devices

Click on the **Devices** tab to view devices that have been added to Lyve Client.

Disk group management

A disk group is a combination of two or more physical drives that are presented to the operating system as a single device. Drives are combined into different configurations known as 'RAID levels'. RAID stands for *redundant array of independent disks*. A RAID level categorizes how data is written to the drives in the array.

The RAID level you choose depends on which storage attributes are most important to you:

Capacity	The total amount of data you can store.
Performance	The speed at which data is copied.
Protection	The number of disks that can fail before data is lost.

Lyve Mobile Array can be configured as RAID 0 or RAID 5. Both RAID levels offer advantages and disadvantages, described below.

RAID 0

In RAID 0, data is split into blocks that get written across all drives in the array. A minimum of two drives is required to create a RAID 0 array.

Advantages

Data is not duplicated across drives. This results in faster transfers and more storage, since the full capacity of all drives can be used to store unique data.

Disadvantages

RAID 0 lacks data protection. If a single drive fails, all data in the array is lost.

RAID 5

In RAID 5, data is also split into blocks that get written across all hard drives in the array. In addition, a redundant *parity* block is written for each data block. A minimum of three hard drives is required to create a RAID 5 array.

Advantages

RAID 5's strong advantage over RAID 0 is data protection. If one physical drive fails, the parity blocks can be used to rebuild the data on a spare drive. You still have access to all your data, even while the data is being rebuilt on the spare drive. For a configuration that does not include a spare drive, be sure to back up your data to another storage device. Contact customer support concerning the failed drive.

RAID 5 offers read performance that can approach RAID 0. However, write performance is slower because the parity data must also be calculated.

Additionally, you still have much of the storage capacity of a RAID 0 array, based on the total available hard drives and storage capacities. The equation for determining the storage is:

(The size of the drive with the smallest capacity in the array) * (Total hard drives minus 1)

Example: An array is assigned five 10TB hard drives for a total of 50TB. The equation is:

10TB * 4 = 40TB

Disadvantages

If one drive in the array fails, restoring the data by building a replacement drive may take hours, depending on the array's capacity. If another drive fails during this time, all data in the array is lost.

Creating a disk group

1. Click on the Devices tab.
2. Click on the card for a connected device.
3. Click Create disk group.

Lyve Client currently supports only one disk group. The Create disk group option is not displayed if another disk group already exists.

4. On the Edit screen, select a RAID configuration: RAID 0 or RAID 5.
5. Click on available drives to select/deselect the drives to be included in the array.
6. Click **Next**.
7. Select options for the array.

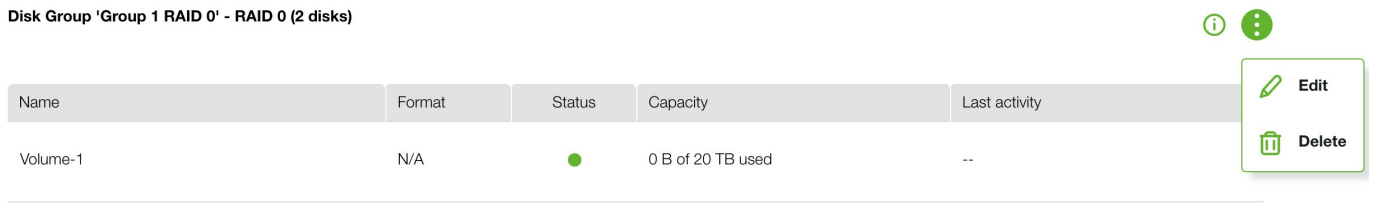
Volume Name	Enter a name for the volume.

Auto format	Automatically format the hard drives when creating a RAID array. Use the dropdown menu to select the format that is best for your operating system: exFAT (macOS and Windows), NTFS (Windows only), HFS+ (macOS only).
Disk cache	Enabling the cache optimizes performance, however, data is at risk since a power loss or system error clears all cached data. Disabling the cache prevents data loss in the event of power loss or system error but copy performance may be reduced.
Initialization	Fixes sector errors that can lead to corrupt data. Note that an initialization can run for hours, or days based on the array's capacity. You can use the device during an initialization, but it will prolong the time to complete it. Performance is degraded during an initialization..

8. Click **Save**.

Editing an existing disk group

1. Click on the Devices tab.
2. Click on the card for a connected device.
3. Locate the disk group you want to edit. Click on the More icon and selec**Edit**.



4. On the Edit screen, select a RAID configuration: RAID 0 or RAID 5.
5. Click on available drives to select/deselect the drives to be included in the array.
6. Click **Next**.
7. Select options for the array.

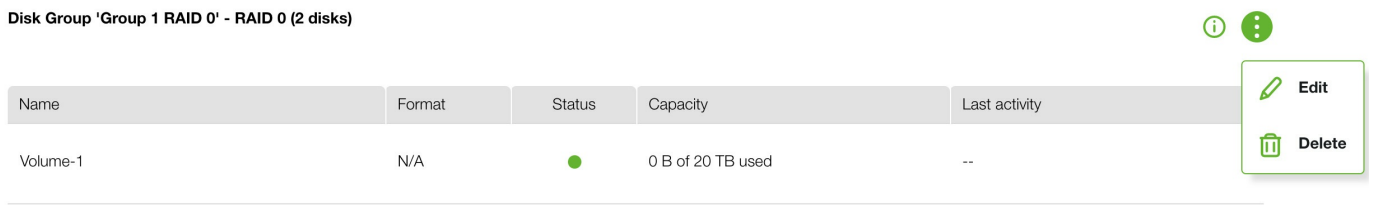
Volume Name	Enter a name for the volume.
Auto format	Automatically format the hard drives when creating a RAID array. Use the dropdown menu to select the format that is best for your operating system: exFAT (macOS and Windows), NTFS (Windows only), HFS+ (macOS only).

Disk cache	Enabling the cache optimizes performance, however, data is at risk since a power loss or system error clears all cached data. Disabling the cache prevents data loss in the event of power loss or system error but copy performance may be reduced.
Initialization	Fixes sector errors that can lead to corrupt data. Note that an initialization can run for hours, or days based on the array's capacity. You can use the device during an initialization, but it will prolong the time to complete it. Performance is degraded during an initialization..

8. Click **Save**.

Deleting a disk group

1. Click on the Devices tab.
2. Click on the card for a connected device.
3. Locate the disk group you want to delete. Click on the More icon and select **Delete**.



4. Confirm that you want to delete the disk group.

Identifying a connected Lyve Mobile device using the LED

Lyve Client can identify a connected Lyve Mobile device for you by having it temporarily flash its LED. This is useful if you have a large bank of connected Lyve Mobile devices and you need to identify a particular device.

1. Click on the **Devices** tab.
2. Hover your cursor over a Lyve Mobile device card and click on the Identify LED icon.

3. Observe the front faces of your devices to spot the one with the flashing purple LED.
4. Click the Identify LED icon a second time to turn off the identification.

Renaming a connected Lyve Mobile device

You can rename connected Lyve Mobile devices.

1. Click on the **Devices** tab.
2. Hover your cursor over a Lyve Mobile device card and click on the Edit icon.

3. Enter a new name for the device.
4. Click **Done**.

Viewing device details

To view device details:

1. Click on the **Devices** tab.
2. Hover your cursor over a device card and click on the Inspect icon.

Change a Lyve Mobile device's LED settings

You can turn a Lyve Mobile device's LED on or off and view the device's LED color legend. The Legend shows the definition of each LED color to a specific state.

1. Click on the **Devices** tab.
2. Click on the card for a connected device.
3. Hover your cursor over the LED card and click on the Edit LED icon.

4. Click on the toggle switch to turn the LED on or off.
5. Click on **Show LED Legend** to expand the legend.
6. Click **Done**.

Adding tags to a device

You can add metadata tags to your device.

Tags will be available for future use in searching and filtering devices. Filtering devices is currently not supported.

1. Click on the **Devices** tab.
2. Click on the card for a connected device.
3. Hover your cursor over the Tags card and click on the Edit icon.

4. Enter a tag in the edit field and press **Enter**.
5. Continue to enter tags in the edit field, pressing **Enter** after each entry.
6. When you're finished adding tags, click **Done**.

Crypto-erasing a Lyve Mobile device

A crypto-erase securely deletes all data on the Lyve Mobile device while keeping your device settings and password intact.

Data deleted during a crypto-erase cannot be recovered.

To securely erase your Lyve device, Lyve Client accesses all data on individual drives. Therefore, the RAID must be recreated after the crypto-erase is complete. Recreating the RAID requires an initialization that can take over 24 hours if the Lyve device is not in use. You can use your Lyve device during the initialization but performance will be degraded until it is complete. Also, using the device during an initialization will increase the time for it to complete. To avoid delays in completing the initialization, make certain that the host computer does not go to sleep until it is complete. If the computer goes to sleep, the initialization will be paused until it wakes up.

1. Click on the **Devices** tab.
2. Click on the card for a connected device.
3. Hover your cursor over the Device Settings card and click on the Erase icon.

4. Click **Erase**.

Viewing Lyve Mobile disk details and enabling dynamic spare disks

You can view Lyve Mobile device disk details, such as the status of each disk, it's capacity, and its RAID array setting. You can also allow disks that are unassigned to an array to act as a spare for any disk group

on the device.

1. Click on the **Devices** tab.
2. Click on the card for a connected device.
3. Hover your cursor over Disks and Spares icon and click on the Inspect icon.

4. (Optional) Click the Enable Dynamic Spares toggle switch.

Download log files for Lyve Mobile devices

To aid in troubleshooting, you can download device log files to your computer.

1. Click on the **Devices** tab.
2. Click on the card for a connected device.
3. Hover your cursor over the Device card and click on the Download Logs icon.

4. Select a download location on your computer.
5. Click **Download Logs**.

Viewing device volumes using a disk utility

You can quickly open Disk Management (Windows) or Disk Utility (Mac) to view device volumes.

1. Click on the **Devices** tab.
2. Click on the card for a connected device.
3. Hover your cursor over a row in the Device Volumes list and click on the Utility icon.

Viewing device volumes using a file browser

You can quickly open File Explorer (Windows) or Finder (Mac) to view the content of your volume.

1. Click on the **Devices** tab.
2. Click on the card for a connected device.
3. Hover your cursor over a row in the Device Volumes list and click on the Find icon.

View Lyve Mobile firmware details

You can view details about your Lyve Mobile device's firmware for use in troubleshooting.

1. Click on the **Devices** tab.
2. Click on the card for a connected device.
3. View the Firmware card.

Configure Disk Group (RAID)

A disk group is a combination of two or more physical drives that are presented to the operating system as a single device. Drives are combined into different configurations known as 'RAID levels'. RAID stands for redundant array of independent disks. A RAID level categorizes how data is written to the drives in the array.

The RAID level you choose depends on which storage attributes are most important to you:

Capacity	The total amount of data you can store.
Performance	The speed at which data is copied
Protection	The number of disks that can fail before data is lost

Lyve Mobile Array can be configured as RAID 0 or RAID 5. Both RAID levels offer advantages and disadvantages, described below.

RAID 0

In RAID 0, data is split into blocks that get written across all drives in the array.

Advantages

- Data is not duplicated across drives. This results in faster transfers and more storage, since the full capacity of all drives can be used to store unique data.
- Initialization takes only minutes.

Disadvantages

- RAID 0 lacks data protection. If a single drive fails, all data in the array is lost.

RAID 5

In RAID 5, data is also split into blocks that get written across all hard drives in the array. In addition, a redundant parity block is written for each data block.

Advantages

RAID 5's strong advantage over RAID 0 is data protection. If one physical drive fails, you still have access

to all your data.

> In the event a drive fails, you should immediately copy all your data to another storage device and contact customer support.

Disadvantages

- RAID 5 offers read performance that can approach RAID 0. However, write performance is slower because the parity data must also be calculated.
- You still have much of the storage capacity of a RAID 0 array, based on the total available hard drives and storage capacities. However, overall storage capacity is reduced slightly. The equation for determining the storage is:

  (The size of the drive with the smallest capacity in the array) * (Total hard drives minus 1)

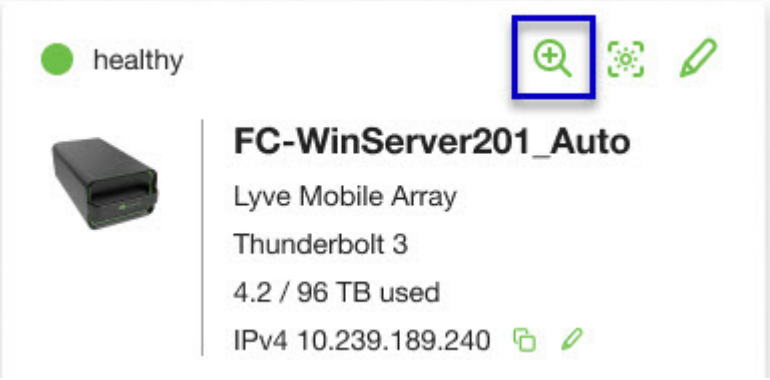
  Example: An array is assigned six 10TB hard drives for a total of 60TB. The equation is:

  10TB * 5 = 50TB

- Initialization may take up to 32 hours for an HDD device.

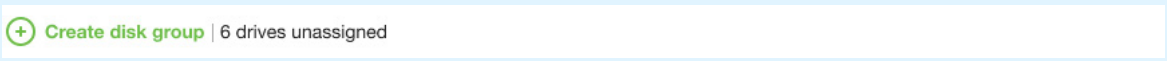
Change RAID configuration

1. Click on the **Devices** tab.
2. Hover your cursor over a device card and click on the Inspect icon.

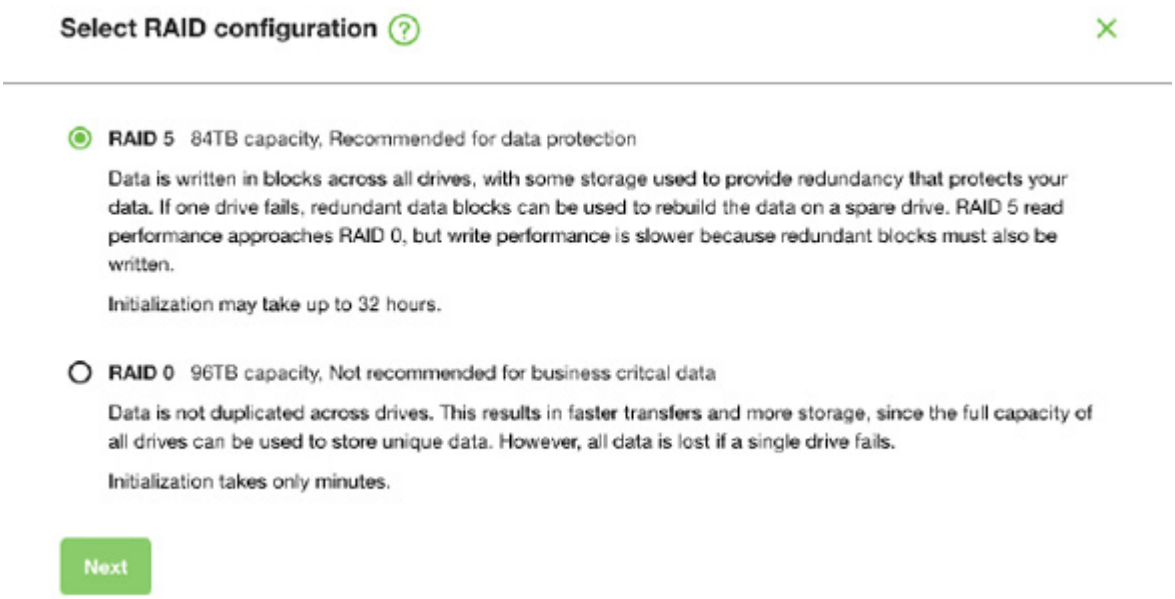


3. If the device is currently configured with a disk group (RAID array), click on the Wrench icon on the disk group volume card:

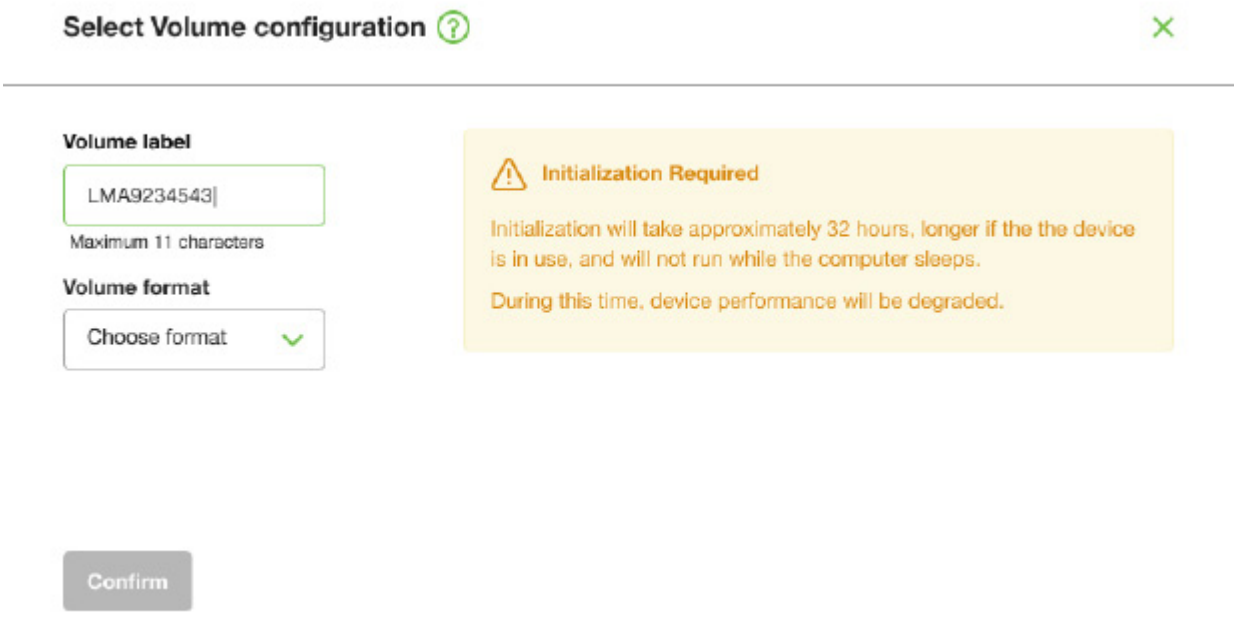
If the device is not currently configured with a disk group, scroll down and click **Create disk group**.



4. Select a RAID configuration: **RAID 5** or **RAID 0**. Click **Next**.

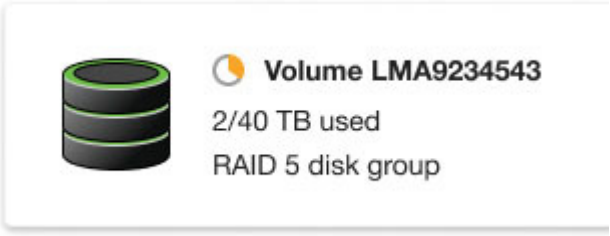


5. Select a volume configuration.



A. Enter a volume label.
B. Select a volume format:
   - Lyve Client for windows: **NTFS** or **exFAT**
   - Lyve Client for windows: **HFS+** or **exFAT**
C. Click **Confirm**.

The volume is displayed on the Device Details page with an amber status icon while the disks are being initialized.



Cryptographic Erase

A cryptographic erase securely deletes all data on the Lyve Mobile device while keeping your device settings intact.

> **!** Data deleted during a cryptographic erase cannot be recovered.

To securely erase your Lyve Mobile device, Lyve Client accesses all data on individual drives. The RAID must be recreated after the crypto-erase is complete.

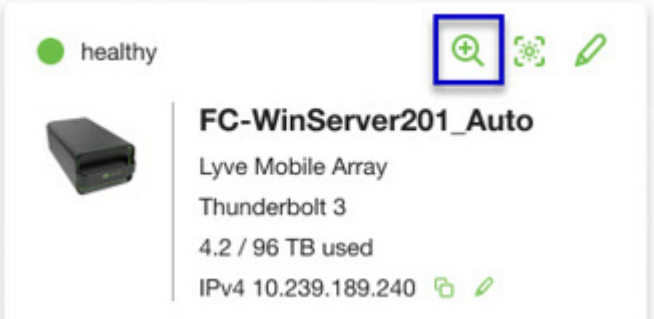
> **!** Recreating the RAID requires an initialization that can take over 24 hours if the Lyve device is not in use.

Recreating the RAID requires an initialization that can take over 24 hours if the device is not in use. You can use your device during the initialization but performance will be degraded until it is complete.

> **i** Using the device during an initialization will increase the time for it to complete. To avoid delays in completing the initialization, make certain that the host computer does not go to sleep until it is complete. If the computer goes to sleep, the initialization will be paused until it wakes up.

Initiating the erasure

1. Click on the **Devices** tab.
2. Hover your cursor over a device card and click on the Inspect icon.



3. On the Cryptographic Erase card, click on the Erase icon.

> **!** Data deleted during a cryptographic erase cannot be recovered.

4. Click **Confirm** to confirm the cryptographic erase.
5. Click **Erase all data** to proceed with the operation.
6. When the process has completed, click**Certify** to view a certificate with the details of the erasure.

Settings

Click on the **Settings** tab to control application and update settings:

Launch Lyve Client at startup—Check if you want Lyve Client to automatically open whenever you start your computer.

Auto-update Lyve Client—Check if you want Lyve Client to automatically check for new updates when connected to the internet.

Network Requirements

Make sure your anti-virus, firewall or VPN security settings allow port access to Lyve Client.

State	Access type	Port
Before device discovery	The application and device must be able to communicate via SLP.	UDP port 427
After device discovery	The application and device must be able to communicate via SSH.	TCP port 22

In both states, it is assumed that the device has been assigned an IP address by a local DHCP server or has been assigned a static IP address.

- All Lyve Mobile devices are in DHCP mode by default. If an IP is not assigned via DHCP, the device will generate its own IP address.
- Any host on the same subnet can see the device and communicate with it using this address.
  - In DAS mode via a Thunderbolt/USB-C connection, this is the address that is used to communicate with the device.

Dashboard

Use the Dashboard to view notifications relating to Lyve Mobile devices connected to the host computer. Dashboard information includes:

- Device connection types.
- Drive capacities and statuses.
- Import activities and progress.
- Event dates and timestamps.

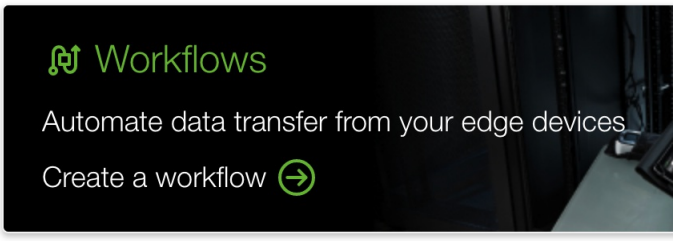
Viewing devices on the Dashboard

Lyve Client automatically adds devices for inclusion in Lyve Client workflows and device management. To view device details, hover your cursor over a device card and click on the Inspect icon.

This is a shortcut to clicking on the **Devices** tab and viewing device details.

Creating a workflow

A **workflow** is a set of rules that allow you to automate file imports from one device to another. It can be **invoked** manually or automatically to start a **data activity** such as moving, copying, and deleting files. To create a workflow, click on the Continue icon at the top of the Dashboard.



This is a shortcut to clicking on the **Workflows** tab and creating a new workflow.

Viewing activities on the Dashboard

To view details of workflow activities, hover your cursor over an activity card and click on the Inspect icon.

Dashboard notifications

Default

Activity	Notification
Connection lost	[device] connection lost
Copy - in progress, complete	Copy from [source volume] to [destination volume]
Delete - in progress, complete	Delete files from [source volume]
Device added	[device] was added
Device connected	[device] connected
Device disconnected	[device] disconnected
Device locked	[device] locked
Device unlocked	[device] unlocked
Tag - in progress, complete	Tag files from [source volume]

RAID

Activity	Notification
Initialization	RAID Initialization, [device]
Maintenance	RAID Maintenance, [device]
Rebuild	RAID Rebuild, [device]
Warning	Array Failed, [device]

Workflows

Activity	Notification
Workflow actions finished	[workflow name] actions finished
Workflow created	[workflow name] was created
Workflow deleted	[workflow name] was deleted
Workflow edited	[workflow name] was edited

Workflow in progress	[workflow name] underway
Workflow turned on	[workflow name] was turned on
Workflow turned off	[workflow name] was turned of

Workflow triggers

Activity	Notification
Workflow trigger - automatic	[workflow name] trigger set to automatic
Workflow trigger - manual	[workflow name] trigger set to manual
Workflow trigger - prompt	[workflow name] trigger set to prompt
Workflow trigger - scheduled	[workflow name] trigger set to scheduled