



# SEAGATE 45656 Lyve Mobile Security User Guide

[Home](#) » [Seagate](#) » SEAGATE 45656 Lyve Mobile Security User Guide 

## Contents

- [1 SEAGATE 45656 Lyve Mobile Security](#)
- [2 Overview](#)
- [3 Accessing Devices with a Lyve Token Software Unlocker](#)
- [4 End user initial tasks](#)
- [5 Viewing authorized devices](#)
- [6 File issue notifications](#)
- [7 Admin tasks](#)
- [8 Download Lyve Token file](#)
- [9 Documents / Resources](#)
  - [9.1 References](#)
- [10 Related Posts](#)



**SEAGATE 45656 Lyve Mobile Security**



## Overview

Lyve Mobile offers two ways for product end user admins to manage how product end users securely access Lyve Mobile storage devices:

- **Lyve Portal Identity**—Product end users authorize client computers to access Lyve Mobile devices using their Lyve Management Portal credentials. Requires an internet connection for initial setup and periodic reauthorization through Lyve Management Portal.
- **Lyve Token Security**—Product end users are provided with Lyve Token files that can be installed on certified client computers. Once configured, computers unlocking Lyve Mobile devices do not require access to Lyve Management Portal or the internet.

## 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. See [Accessing 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. See [Accessing 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.

## Register on 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.

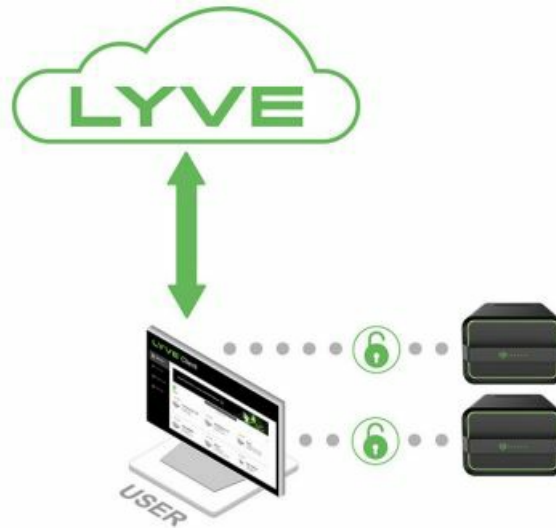
## Accessing Devices with Lyve Portal Identity

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://imp-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.

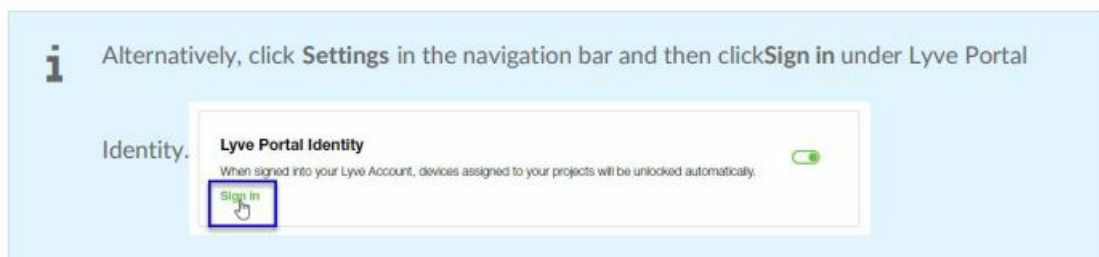
If you don't have a username and password, see Users with no username/password below.

- 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:



- 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.

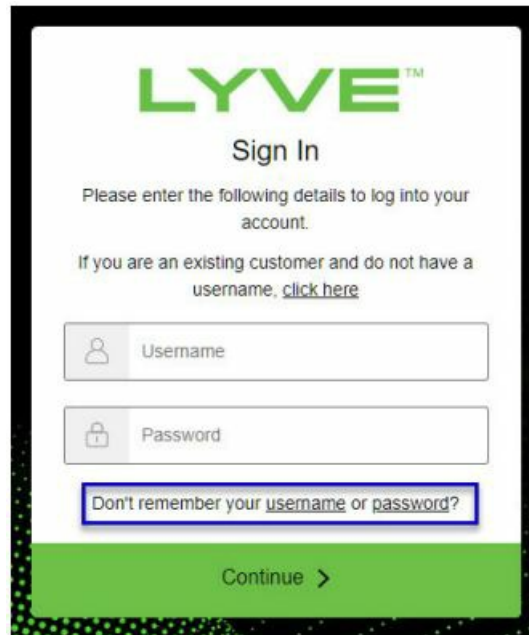
## Forgotten username and/or password

If you can't remember your username or password:

1. Go to [lyve.seagate.com](https://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 <a href="#">Resend an email invitation</a> below.

## Resend an email invitation

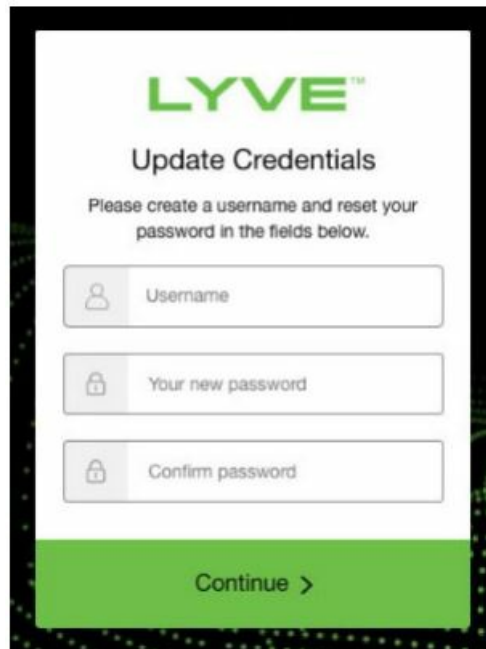
1. Go to [lyve.seagate.com](https://lyve.seagate.com).
2. Click Sign In in the navigation bar:



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

The image shows a mobile app screen for updating credentials. At the top is the LYVE logo. Below it is the title 'Update Credentials' and a prompt: 'Please create a username and reset your password in the fields below.' There are three input fields: 'Username' with a person icon, 'Your new password' with a lock icon, and 'Confirm password' with a lock icon. At the bottom is a green bar with a white 'Continue >' button.

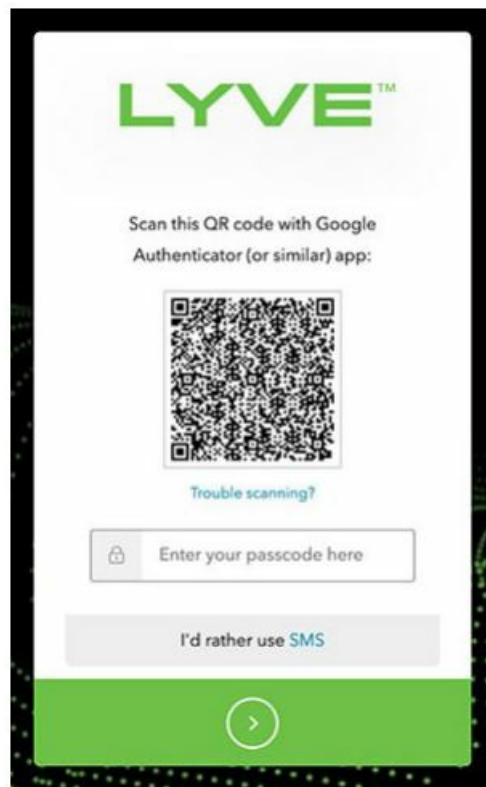
**LYVE™**

### Update Credentials

Please create a username and reset your password in the fields below.


[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.

The image shows a mobile app screen for QR code authentication. At the top is the LYVE logo. Below it is the text 'Scan this QR code with Google Authenticator (or similar) app:'. In the center is a QR code. Below the QR code is a link 'Trouble scanning?'. There is an input field 'Enter your passcode here' with a lock icon. Below that is a button 'I'd rather use SMS'. At the bottom is a green bar with a white circular arrow icon.

**LYVE™**

Scan this QR code with Google Authenticator (or similar) app:



[Trouble scanning?](#)

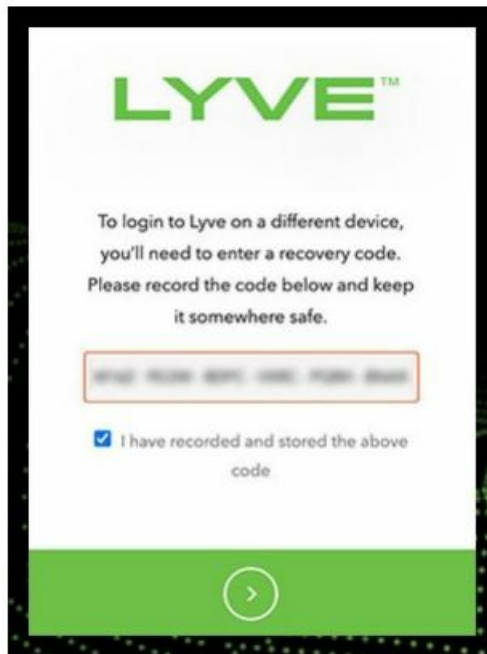
[I'd rather use SMS](#)

[>](#)

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 Porta 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 authorization

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.



## Lyve Token Security – Overview

With Lyve Token Security, product end user admins provide product end users with Lyve Token files that authorize unlockers to access assigned Lyve Mobile devices. Unlockers can unlock assigned Lyve Mobile devices without access to Lyve Management Portal or the internet.

There are two types of unlockers:

- **Software unlocker**—A client computer installed with a Lyve Client app that has been certified to access assigned Lyve Mobile devices.
- **Hardware unlockers** —A Lyve Mobile Padlock that has been certified to access assigned Lyve Mobile devices.

For details on unlocker configuration and usage, see the following:

- [Accessing Devices with a Lyve Token Software Unlocker](#)
- [Accessing Devices with a Lyve Token Hardware Unlocker](#)

## Accessing Devices with a Lyve Token Software Unlocker

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

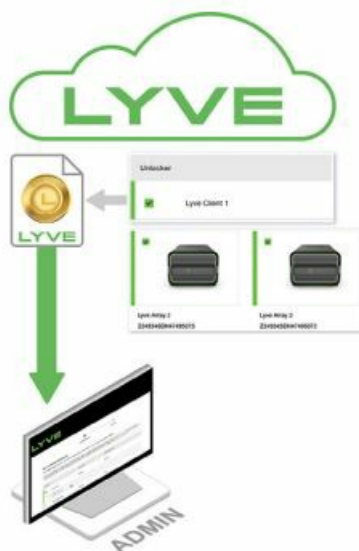
[Product end user](#) opens Lyve Client on a [host computer](#) and creates a [registration file](#). End user sends the registration file to a [product admin](#).



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 file [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 registered on file

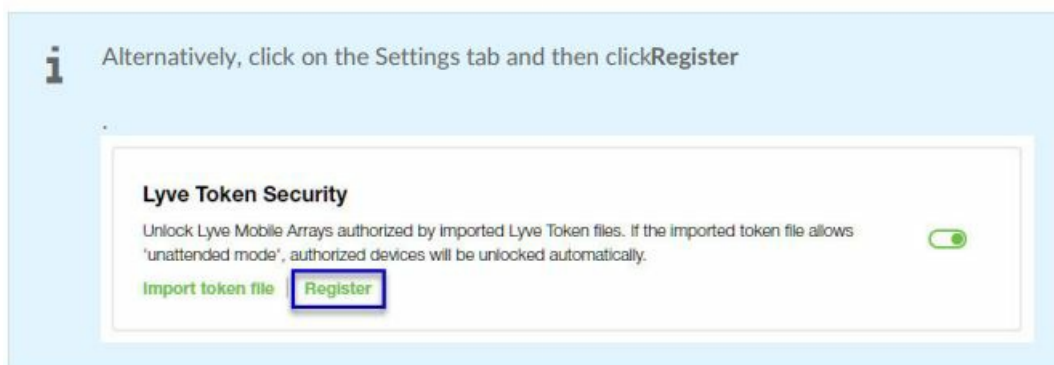
You will need a registration file for each host computer/Lyve Client installation used to access Lyve Mobile devices.

### 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:



In the dialog, enter a filename and click Save.



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

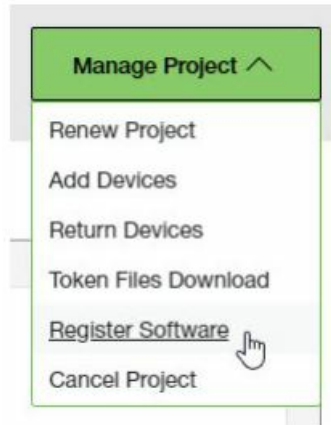
Using a file browser such as File Explorer or Finder, locate the downloaded registration file. Share it with your

[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](https://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

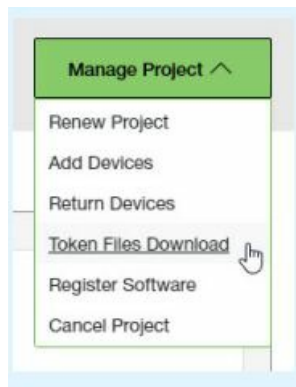
### Choose unlockers and assign devices

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.



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



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.



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.


**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.

**Review Token File Details**

Unlocker	Saved to Unlocker
LyveTokenDEMO	

---

**Token File-assigned Devices**



Lyve Mobile Array (96TB HDD)  
NB26003C

---

Please note that you will be asked to re-authenticate before you can download the token files.

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 your [product 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.



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

**Lyve Token Security**

Unlock Lyve Mobile Arrays authorized by imported Lyve Token files. If the imported token file allows 'unattended mode', authorized devices will be unlocked automatically.

[Import token file](#) [Register](#)

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:

< Unlock devices

Devices with the following serial numbers will be unlocked.

Serial Numbers	NB27107P	Expires	2023-08-21   11:31:57 AM
	NB33107C	Allow Import	Yes
	NB48100W		
	NB12000A		
	NB22207E		
	NB27107P		
	NB29107Y		

Import token

Use token file once

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	<b>Yes</b> —Lyve Token file can be stored in the Lyve Client app.
	<b>No</b> —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.

**Click one of the following:**

<b>Import Lyve Token file</b>	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.
<b>Use</b>	
<b>Lyve Token file</b>	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.
<b>once</b>	

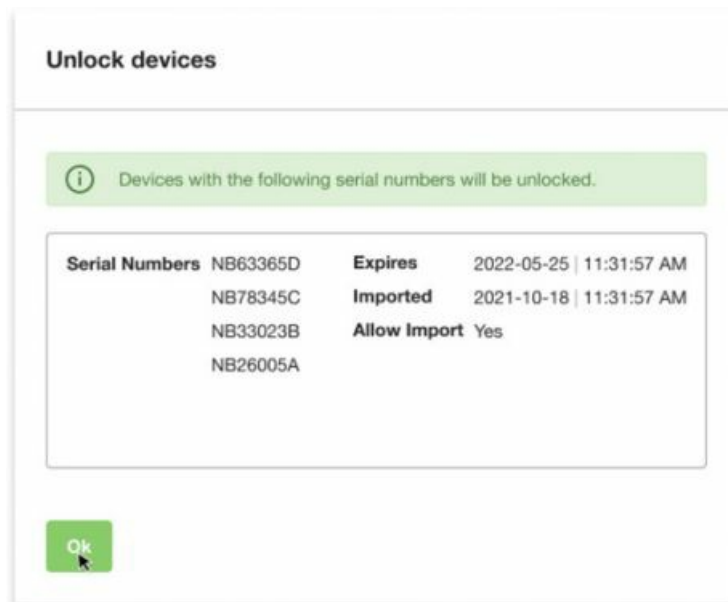
## Viewing Lyve Token files

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:

Authorized Lyve Mobile Arrays				
Serial number	Imported	Created	Expiration	Project administrator
NB63365D	2021-11-25	2021-11-25	2022-05-25	marcel.gotlib@acme-industries-inc.com
NB78345C	2021-11-05	2021-10-28	2022-04-28	kyle.broflowski@seagate.com
NB33023B	2021-10-18	2021-10-13	2022-04-13	stan.marsh@seagate.com
NB26005A	2021-10-18	2021-10-13	2022-04-13	eric.theodore.cartman@seagate.com

Close Delete all

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.

**Lyve Token Security**

Unlock Lyve Mobile Arrays authorized by imported Lyve Token files. If the imported token file allows 'unattended mode', authorized devices will be unlocked automatically.

[Import token file](#) | [View token file](#) | **Authorized Devices (4)** | [Register](#)

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

Authorized Lyve Mobile Arrays

Serial number	Imported	Created	Expiration	Project administrator
NB63365D	2021-11-25	2021-11-25	2022-05-25	marcel.gotlib@acme-industries-inc.com
NB78345C	2021-11-05	2021-10-28	2022-04-28	kyle.broflowski@seagate.com
NB33023B	2021-10-18	2021-10-13	2022-04-13	stan.marsh@seagate.com
NB26005A	2021-10-18	2021-10-13	2022-04-13	eric.theodore.cartman@seagate.com

Close

Delete all

5. Hover over the device and click the Delete icon

NB78345C	2021-11-05	2021-10-28	2022-04-28	kyle.broflowski@seagate.com	
NB33023B	2021-10-18	2021-10-13	2022-04-13	stan.marsh@seagate.com	<div><div></div></div>
NB26005A	2021-10-18	2021-10-13	2022-04-13	eric.theodore.cartman@seagate.com	

Delete authorization to unlock this device

i

Alternatively, if you want to delete all device authorizations, clickDelete 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 the Lyve 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.

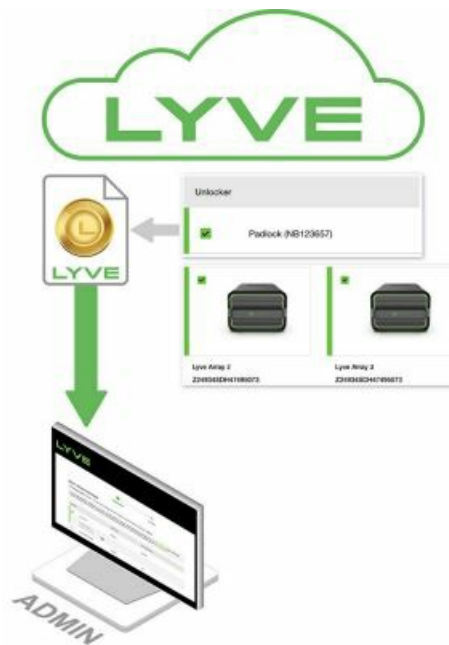
## Accessing Devices with a Lyve Token Hardware Unlocker

### Requirements

- Product end user admin has set up projects and added devices to projects, including Lyve Mobile storage devices and a Lyve Mobile Padlock.
- Devices have been delivered to the product end user.

### Process

1. In Lyve Management Portal, admin selects the Lyve Mobile Padlock as a hardware unlocker and assigns devices to it. Admin downloads an encrypted Lyve Token file that authorizes the unlocker to access Lyve Mobile devices.



2. Admin sends the token file to the product end user



3. User downloads the Lyve Token file to a USB external drive



4. User connects the USB external drive to a USB 3.0 port on Lyve Mobile Padlock. Lyve Mobile Padlock can now unlock assigned Lyve Mobile devices with no connection to Lyve Management Portal or the internet.



## Admin tasks

### Choose unlockers and assign devices

1. Sign in to [lyve.seagate.com](https://lyve.seagate.com). Enter a verification code to continue to Lyve Management Portal.
2. Click Projects in the navigation bar.

3. Click on a project.
4. On the Project Details page, click on the Manage Projects dropdown and select Token Files Download.



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

Unlocker	Client Type	Operating System
<input checked="" type="checkbox"/> Padlock (NB123657)	Hardware	N/A

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



If you don't know a device's serial number, you or the device user can find it by scanning the QR code on the left side of the Lyve Mobile Array handle.



Click Continue.

## Download Lyve Token file

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 the Continue icon.
4. A dialog informs you that the Lyve Token file has been downloaded. Click Close.
5. Using a file browser such as Files Explorer or Finder, locate the file in the folder where you receive downloads.

### Send the Lyve Token file to the product end user

Send the Lyve Token file you downloaded to the appropriate product end user.

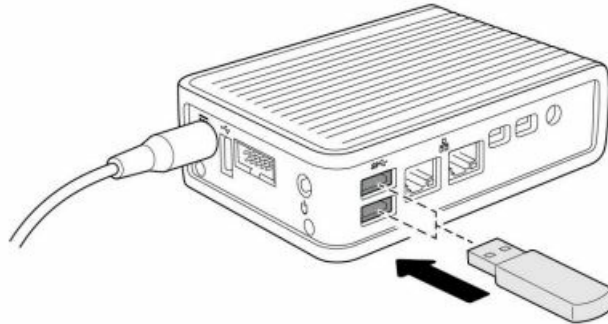
### End user tasks

#### Download Lyve Token files


Download the Lyve Token file you received from your admin and copy it to a storage device capable of connecting via a USB Type A connector. The Lyve Token file must be copied to the root level of the USB storage device to be detected by Lyve Mobile Padlock.

### Connect USB drive to Lyve Mobile Padlock

Connect the USB external drive containing the Lyve Token file to one of the USB 3.0 ports on Lyve Mobile Padlock.







### Documents / Resources

	<a href="#">SEAGATE 45656 Lyve Mobile Security</a> [pdf] User Guide 45656 Lyve Mobile Security, 45656, Lyve Mobile Security, Mobile Security, Security
---	---

### References

- [Auth0: Secure access for everyone. But not just anyone.](#)
- [Welcome - Lyve Management Portal](#)
- [Welcome - Lyve Management Portal](#)
- [Ultra Touch | Seagate US](#)
- [Lyve Management Portal User Manual - Project Management | Seagate US](#)
- [Lyve Management Portal User Manual - Project Management | Seagate US](#)
- [Lyve Management Portal User Manual - Project Management | Seagate Australia / New Zealand](#)
- [Lyve Management Portal User Manual - Project Management | Seagate US](#)
- [Lyve Mobile Security User Guide - Key Terms | Seagate Australia / New Zealand](#)
- [Lyve Mobile Security User Guide - Key Terms | Seagate Australia / New Zealand](#)
- [Lyve Mobile Security User Guide - Key Terms | Seagate US](#)
- [Lyve Mobile Security User Guide - Key Terms | Seagate US](#)
- [Lyve Mobile Security User Guide - Key Terms | Seagate US](#)
- [Lyve Mobile Security User Guide - Accessing Devices with Lyve Portal Identity | Seagate Australia /](#)

## [New Zealand](#)

-  [Lyve Mobile Security User Guide - Accessing Devices with Lyve Portal Identity | Seagate US](#)
-  [Lyve Client Software User Manual - Download and Install Lyve Client | Seagate US](#)
-  [Lyve Client Software User Manual - Lyve Virtual Assistant | Seagate US](#)
-  [Lyve Client Software User Manual - Settings | Seagate US](#)
- [User Manual](#)