Seagate Lyve Pilot User Guide

Abstract

This guide provides information about using Lyve Pilot software to manage an ecosystem of data and devices.

Part Number: 83-00007734-00-12
Revision: 1.8.0
Published: May 2022

Open Source Third Party Licenses and Code

Seagate storage products use open source software components. To view information about open source software licenses and open source code used in Seagate storage products, see www.seagate.com/support.

Contents

Overview

Lyve Pilot brings Seagate technologies together into an ecosystem for data management from endpoint to edge to core, enabling customer use cases for modern IT workflows. IoT devices generate much more data than current and near-term Internet capability can transport. Computing resources and storage are moving to the edge to process this data. As data is processed at the edge and needs to move to private or public clouds, portable shuttles or local cloud storage might be required to efficiently move this processed data.

Whether you are using Seagate or non-Seagate devices, your data is secured at rest, and using TLS connections, the data is secured in flight.

Lyve Pilot helps users manage data that needs to be moved. The key features of Lyve Pilot include:

- Monitors alerts, data activity, and device movement within your infrastructure
- Secures data through encryption and fingerprinting, uploading metadata to ensure data integrity
- Notifies the user and quarantines data when it has been modified, tampered with, or corrupted
- Works in a desktop browser

Lyve Pilot data

- Lyve Pilot data bundles combine customer data and metadata.
- Lyve Pilot bundles can be stored in file storage systems as well as object stores and allows you to move data freely between them.
- Lyve Pilot bundles contain a set of metadata upon import into the Lyve Pilot data domain. The metadata contains the initial state of all objects included and adds information about post-import changes, such as data moves or the addition of user-defined tags.
- As Lyve Pilot bundles move from device to device, the dynamic metadata is updated to track the chain of custody information.

Data security and provenance

- Seagate Secure or your own devices' encryption technology protects data at rest.
- Transport Layer Security (TLS)--the successor to Secure Sockets Layer (SSL)--protects data in motion.
- Lyve Pilot provides an end-to-end security solution.
- Lyve Pilot fingerprints data to ensure integrity.

Getting started

The account team will provide you with the credentials and URL for your account.

Obtain credentials

You only need to obtain one ID from the account team. After receiving the first Admin user credentials, you can create the rest of your users on your own.

Email: The email address for the first admin user. The email address is case sensitive.

Token: The token is a one-time use code used to log in for the first time and set your password. The email will contain an expiration date and time for this token.

Lyve Pilot URL: The URL starts with pilot.lyve.seagate.com and is followed by your customer ID. The customer ID is a unique, 22 character, alphanumeric string. Example: https://pilot.lyve.seagate.com/1abcde234fghi5jk6lmn7o8pq9/

Follow the Quick start: Endpoints guide to get up and running quickly.

Quick start: Endpoints

Seagate's Lyve Pilot software automates data flow and lets you manage and monitor data movement between devices in your environment, from endpoint to edge to core. A device can be a physical device or an endpoint. This quick start describes just one example how to complete a full circle of data transfer an endpoint to the core to the cloud.

Tasks

Perform the following tasks to complete your first data transfer cycle.

1. Obtain your Lyve Pilot URL and credentials and log in with your email address and token for the first time.

   See Manage users.

2. Follow the instructions to deploy Pilot Links on Kubernetes.

   See Deploy Pilot Links.

3. Add and link endpoints in the Lyve Pilot portal.

   See Manage Endpoints.

4. Import data to the endpoint of your data share.
   In the Lyve Pilot portal, import data and monitor the data activity.

   See Import Data.

5. Copy data to your server.
   In the Lyve Pilot portal, copy data to your edge server.

   See Copy data.

6. Export data to the cloud.
   In the Lyve Pilot portal, export data to the cloud (such as, AWS S3, or NFSv3).

   See Export data.

Dashboard overview

The Lyve Pilot dashboard provides one convenient place to view and manage all Lyve Pilot data, devices, and activity. The dashboard displays an event stream, known as the dashboard feed, which automatically posts new events at the top as they occur.

The notifications in the dashboard feed provide history for all Lyve Pilot events in the environment. You can tag and filter notifications on the feed to include only events of interest, and you can further inspect events to find details such as the history of a device, movement of data between devices, and any associated alerts. You can also perform actions on data and devices, as well as other types of events, directly from the dashboard feed.

NOTE When you log in to the portal, there might not be activity to display on the dashboard, so you see a welcome screen instead. You need to add a device to your Lyve Pilot domain to get started. If you or another user has already begun using the Lyve managed data ecosystem, the dashboard shows activity as described above.

Notification types

There are multiple notification types on the dashboard feed, each represented by icons which help you quickly identify the actions. To view the icons and the actions associated with each, see Icons in the interface.

- Device events
- Data activities
- System events
- Alerts

Device and endpoint events

Device events include any actions related directly to a physical device or Pilot Link, such as:

- A new device added to the domain
- A new volume detected on a device
- New data discovered on a managed volume
- A managed device disconnected or reconnected
- A Pilot Link connected to Lyve Pilot
- Storage has been removed from Lyve Pilot Management

The icons that appear with device notifications represent the device type, volume, or endpoint.

Data activities

Most feed items are data activities. These events include any type of action performed on the data within your secure domain, such as:

- Data imported into the domain from a connected device
- Data copied from one location to another within the domain
- Data exported outside the domain
- Data deleted from a device that is a member of the domain
- Data trusted that had been quarantined

System events

System events include issues related to the Lyve Pilot environment, such as:

- Service log generation
- New user creation
- New user log in

Alerts

Alerts in the dashboard feed warn you about unexpected events within the environment. Alerts stand out with a red bar icon. Events can generate alerts such as:

- A data operation resulted in quarantined files
- An operation failed for any reason (e.g., insufficient space)
- Other system failures

NOTE Be sure to review the alert notifications to determine the appropriate action, if any, to resolve the issue.

Actions from the dashboard feed

Actions are context-sensitive. When you hover over a notification, its related icons are displayed, if available. To view the icons and the actions associated with each, see Icons in the interface.

- **Cancel**: Stops an ongoing activity, such as an import, copy, or export. This action appears only while an action is in progress.
- **Copy**: Copies data from one location to another within the Lyve managed data ecosystem.
- **Export**: Exports data to a location outside the domain.
- **Import**: Imports data from a connected device or volume to the Lyve managed data ecosystem.
- **Inspect**: Opens a detail screen for more information about the notification. This action is available for most dashboard notifications.
- **Tag data**: Apply tags to data bundles in Lyve Pilot to add unique identification to your data.
- **Verify data**: Compares the data in this bundle with the Lyve metadata in order to verify that your data remains unchanged since your last operation. A successful verification will leave your data untouched, but a failed verification will trigger a quarantine of your data.

Icons in the interface

The tables below show the most common icons found in the notification feed on the Lyve Pilot dashboard and in the user interface and explain how they are used.

Table 1 Notification feed icons

Icon	Event	Description
ALERT	Alert	An unexpected event in the environment.
	Copy	Data copied between systems in your managed environment.
	Device	Device registered with the Lyve Pilot domain. The actual image varies depending on the device type.
	Export	Data exported outside the managed environment.
	Import	Data imported into the managed environment.
	Pilot Link	Pilot Link has been connected to or removed from Lyve Pilot Management
	Trust	A user trusted a quarantined data bundle.
	User management	A new user created, logged on for the first time, or similar user administration tasks.
✓	Verify	Data in a bundle verified against its metadata to ensure it is unchanged.
	Volume	A volume discovered by or removed from the Lyve managed data ecosystem.

Table 2 Action icons

Icon	Name	Use
⊕	Add	Adds assets, such as a new device, a new endpoint for exports, and new users.
⊕	Assign	Assigns a linked endpoint to a device.
✕	Close or Abort	Stops an operation that is in progress.

Table 2 Action icons (continued)

Icon	Name	Use
⧉	Copy	Copies data between systems in your managed environment.
🗑	Delete	Deletes data from a device.
⏏	Disconnect endpoint	Disconnect from a linked endpoint.
⤓	Download	Downloads assets, such as a generated service log.
✎	Edit	Customizes display information for your devices and other elements in the interface.
↗	Export	Removes data from Lyve management and puts it outside the managed environment.
📄	Generate service log	Generates a service log for the Lyve managed data ecosystem that users can download for support issues.
↙	Import	Imports data into the managed environment.
🔍	Inspect	Opens a detail screen for more information on the item.
☰	List view	Toggles to show items in list view.
⋮	More	Expands the list of icons to reveal additional options.
⊕	Reconnect endpoint	Reconnect an endpoint to the managed environment
⊖	Remove	Remove data or endpoint from the managed environment
🏷	Tag data	Opens the Tag data dialog box where users can create and apply custom tags.
⊞	Tile view	Toggles to show items in tile view.
🤝	Trust data/bundle	Creates a new trusted bundle from a bundle that has quarantined data.
⊖	Unassign	Unassigns a linked endpoint from a device.
📋	Verify data/bundle	Compares data in a bundle with its metadata to ensure the data is unchanged.
🗀	View bundle	View bundle or bundle contents

Table 3 Status icons

Icon	Name	Use
✓	Good	Good status or action completed successfully.
!	Warning	Indication of an error or alert.
?	Question mark	Device or volume does not have a network connection from the current device.

Table 4 Pilot Links and Endpoint icons

Icon	Name	Use
●	Pilot Link	Pilot Link
NFS	NFSv3	NFSv3 endpoint
S3	S3	S3 Object Storage unmanaged data-endpoint
● S3	S3	S3 Object Storage linked endpoint
SMB	SMB	SMB unmanaged data-endpoint
● SMB	SMB	SMB linked endpoint

Security model

Lyve Pilot provides an easy and secure model for users to manage data across multiple devices. The security model creates a trusted ecosystem of storage devices that can securely and reliably transport data between remote content creation, typically performed at the edge, and storage devices, which can be in the user's private cloud or in a public cloud.

Lyve Pilot achieves this level of security through a combination of:

- Device trust establishment
- Communication privacy
- User data fingerprinting
- User data provenance
- Authentication and authorization

Device trust establishment

The Lyve managed data ecosystem establishes the trust aspect of the security model. The domain defines which devices are allowed to communicate and share data between each other.

The Lyve Pilot portal acts as the controller for the secure domain by defining the domain root-of-trust and acting as the gatekeeper for accepting new devices as domain members. When a Lyve-enabled device is placed under Lyve management, it is trusted by all other devices within the same domain.

The components of the Lyve managed data ecosystem are equipped with multiple cryptographic identities for authentication and signing purposes. The encryption key types and sizes follow National Institute of Standards and Technology (NIST) recommended best practices for security strength.

For information about how to register a new device to the secure domain, see Registering a device.

Communication privacy

Communication between devices in the Lyve managed data ecosystem can take place over public networks. To ensure communication privacy, all API and data transport connections in the Lyve managed data ecosystem are TLS encrypted.

In addition, the Lyve managed data ecosystem uses two-way certificate verification to facilitate automated orchestration actions. This system means that device connections aren't placed under Lyve management unless a valid certificate is received by both participants.

Two-way certificate verification between the domain and device allows access to the device without needing to enter user credentials after a device has been added to the domain. However, valid user authentication and authorization are required to register a device with the system.

User data fingerprinting

Data within the Lyve managed data ecosystem is secured with fingerprinting. When data is imported, a unique fingerprint is calculated for the import session. This fingerprint is calculated based on each imported file as well as on the metadata that describes the import session.

This fingerprint is then used to validate the consistency of that data on each device for as long as it resides within the secure domain. Fingerprints are calculated following NIST recommendations for secure cryptographic hashing.

User data provenance

Data provenance provides proof that data you import into the Lyve managed data ecosystem has not been manipulated or corrupted. Data fingerprinting alone is not sufficient to ensure provenance because it validates only that a given instance of the data is consistent with the stated fingerprint. The fingerprint itself could potentially be manipulated to match modified data.

Data provenance ensures that the fingerprint used for data consistency validation is the same fingerprint that was calculated on import. It also demonstrates that all devices handling the data are trusted.

Provenance in Lyve Pilot is achieved through a secure blockchain that includes the fingerprint for the original data along with its session metadata and an audit log that records every operation performed on the data within the domain. This information accompanies the data bundle as the data is copied and stored on different devices in the domain. If a validation error occurs, data is quarantined and you receive an alert notification on the dashboard.

Authentication and authorization

Authentication and authorization are the final pieces of the security model. These elements protect the Lyve managed data ecosystem from unwanted connections by users or devices. Authentication establishes a user or device’s identity. Authorization establishes that the user or device is permitted to access specific functionality.

Lyve Pilot supports:

- Local user authentication: This method uses Lyve Pilot's built-in authentication and authorization server.

Manage data

Lyve Pilot lets you efficiently and securely manage data across your enterprise. When you import data into the Lyve managed data ecosystem, the system generates unique metadata and fingerprinting, which is used to identify the data and ensure it remains intact and has not been tampered with or corrupted.

For an example workflow, see Quick start. The following pages describe in detail each of the actions you can perform on your data.

- Import data
- Copy data
- Export data
- Inspect data and data events
- Verify data
- Tag data
- Delete data
- Manage endpoints
- Manage orchestration mode

For information about working with devices and adding devices to the secure domain, see Manage devices. For more information about how Lyve Pilot secures data and devices, see Security model.

Import data

When you import data into the Lyve managed data ecosystem, Lyve Pilot adds encryption and fingerprinting to ensure data integrity, both at rest and in flight. The data is tracked and verified as it moves through the ecosystem.

NOTE The Import option appears only if unmanaged data exists on the managed or unmanaged volume.

You can access the Import action from:

- notifications on the dashboard feed for volumes with available data
- the volume table of a device detail screen
- the endpoint table of the Linked endpoint or Unmanaged-data endpoint screen

Import from unmanaged volume

You can import data from an external, unmanaged volume such as a USB device plugged into the shuttle.

1. Hover over the unmanaged volume and select Import .
2. Select the destination type of Device Volume or Device Endpoint.
3. Select the Volume or the Data endpoint.
4. Select **Next**.
5. From the Orchestration Mode drop-down menu, select one of the following:
   - Enterprise Security: Utilizes all security capabilities available to Lyve Pilot to track and protect your data as it moves through your Lyve environment.
   - Enterprise Performance: Trades file-level data protection for maximum performance during imports, copies, and exports of your data. Your data is still tracked and protected as a bundle.
6. If you want to verify the data integrity after the import is complete, select the **Verify data integrity after this import is complete** check box.

   NOTE If you select the **Verify data integrity** check box, the time to complete can increase significantly.

7. After Lyve Pilotvalidates the connection between your devices, **Import** to add the data to the managed volume.

   By default, Lyve Pilot deletes your original data after metadata has been written and your data is verified.

Import from unmanaged volume

You can import data from an external, unmanaged volume such as a USB device plugged into the shuttle.

1. Hover over the managed volume and select Import .
2. Select the destination type of Device Volume or Device Endpoint.
3. Select the Volume or the Data endpoint.
4. Select **Next**.
5. From the Orchestration Mode drop-down menu, select one of the following:

- Enterprise Security: Utilizes all security capabilities available to Lyve Pilot to track and protect your data as it moves through your Lyve environment.
- Enterprise Performance: Trades file-level data protection for maximum performance during imports, copies, and exports of your data. Your data is still tracked and protected as a bundle.

6. If you want to verify the data integrity after the import is complete, select the **Verify data integrity after this import is complete** check box.

NOTE If you select the **Verify data integrity** check box, the time to complete can increase significantly.

7. After Lyve Pilotvalidates the connection between your devices, **Import** to add the data to the managed volume.

   By default, Lyve Pilot deletes your original data after metadata has been written and your data is verified.

During the import operation, you can select Dashboard or Data to view the progress of the import.

Import from managed volume

You can import unmanaged data from a managed volume such as data that is newly added to an existing volume. In a shuttle environment, you can switch the shuttle to DAS mode, write data to that volume, then switch the shuttle back to Lyve Management mode to import the new data into the Lyve managed data ecosystem. In this environment, the volume contains both managed and unmanaged data. The unmanaged data is not encrypted and has not been assigned any metadata or tags.

1. Hover over the managed volume and select Import .
2. Select the destination volume.
3. Select **Next**.
4. From the Orchestration Mode drop-down menu, select one of the following:
   - Enterprise Security: Utilizes all security capabilities available to Lyve Pilot to track and protect your data as it moves through your Lyve environment.
   - Enterprise Performance: Trades file-level data protection for maximum performance during imports, copies, and exports of your data. Your data is still tracked and protected as a bundle.
5. If you want to verify the data integrity after the import is complete, select the **Verify data integrity after this import is complete** check box.

NOTE If you select the **Verify data integrity** check box, the time to complete can increase significantly.

6. On the Import table:
   - If there is only one managed destination volume available, the destination volume is automatically selected. Select **Import**.
   - If there are multiple managed destination volumes available, you have the option to import to the source volume or a different volume.
     - To import to the source volume:
       a. From the Import to drop-down menu, select **Source volume**.

          The destination volume is automatically selected.

       b. Select **Import**.

- To import to a destination volume:
    a. From the Import to drop-down menu, select **A different volume**.
    b. Select one of the destination volumes
    c. Select **Import**.

7. On the confirmation window, select **OK** to add the data to the managed volume.

   By default, Lyve Pilot deletes your original data once metadata has been written and your data is verified.

8. On the confirmation window, select **OK** to add the data to the unmanaged volume.

During the import operation, you can select Dashboard or Data to view the progress of the import.

Copy data

You can copy data around the Lyve managed data ecosystem from device to device or from a device to a linked endpoint. For example, you can copy data from your Lyve Mobile Shuttle to your Lyve Mobile Array device.

You can access the Copy action ⧉ from:

- Import, Copy, and Verify data notifications on the dashboard feed
- Import, Copy, and Verify data events on the Data screen
- a data detail screen for an Import, Copy, or Verify event
- the volume table of a device detail screen
- the assigned endpoints table of a device detail screen

You can select either a device volume or a data endpoint as a copy destination. The steps you follow are different depending on your choice.

Copy data to a data endpoint

1. Select **Copy**. As shown in the list above, this action can be accessed from multiple locations.
2. From the Select destination type drop-down menu, select **Data endpoint**.
3. Drill-down through the endpoints to find your data endpoint.
   - If there is only one linked endpoint available, the destination endpoint is automatically selected.
   - If there are multiple linked endpoints available, you have the option to import to several destination endpoints. Select one of the endpoints.
4. Select the **Pilot Link** from the drop-down menu.
5. If you want to verify the data integrity after the copy is complete, select the **Verify data integrity** check box.

   > (missing or bad snippet)If you select the **Verify data integrity** check box, the time to complete can increase significantly.

6. Select **Next**.
7. After a successful validation, select **Copy**.
8. On the confirmation window, select **OK** to copy the data to the data endpoint.

During the copy operation, you can select Dashboard or Data to view the progress of the import.

Copy data to a device volume

1. Select **Copy** ⧉. As shown in the list above, this action can be accessed from multiple locations.
2. From the Select destination type drop-down menu, select **Device volume**.
3. Select **Next**.
4. If you want to verify the data integrity after the copy is complete, select the **Verify data integrity** check box.

> **NOTE** If you select the **Verify data integrity** check box, the time to complete can increase significantly.

5. Select **Next**.
6. After a successful validation, select **Copy**.
7. On the confirmation window, select **OK** to copy the data to the data endpoint.

During the copy operation, you can select Dashboard or Data to view the progress of the import.

Copy data to a data endpoint

1. Select **Copy**. As shown in the list above, this action can be accessed from multiple locations.
2. From the Select destination type drop-down menu, select **Data endpoint**.
3. Drill-down through the endpoints to find your data endpoint.
   - If there is only one managed linked endpoint available, the destination endpoint is automatically selected.
   - If there are multiple managed linked endpoints available, you have the option to import to several destination endpoints. Select one of the endpoints.
4. Select the **Pilot Link** from the drop-down menu.
5. Select **Validate Connection**.
6. Select **Next**.
7. If you want to verify the data integrity after the copy is complete, select the **Verify data integrity** check box.

NOTE If you select the **Verify data integrity** check box, the time to complete can increase significantly.

8. Select **Next**.
9. After a successful validation, select **Copy**.
10. On the confirmation window, select **OK** to copy the data to the data endpoint.

During the copy operation, you can select Dashboard or Data to view the progress of the import.

Export data

You can export data from a managed endpoint or volume to an unmanaged location, such as a regular file system, NFS/SMB share, or an object store. You can choose from a list of unmanaged, external volumes seen by Lyve Pilot, or configure custom destination endpoints such as Amazon S3 or NFSv3.

Exported data is validated against the original imported file content as it is moved out of the Lyve Pilot domain, and the user can opt to have Lyve Pilot run a final, post-export validation of the data in its external location before it is released by Lyve Pilot. Additionally, the user can choose to export Lyve Pilot metadata to the provided location. Once exported out of the Lyve managed data ecosystem, the data is no longer tracked.

You can access the Export action from:

- the notification feed
- a data detail screen
- the volume table of a device detail screen

Export data to a device volume

You can export data to an unmanaged volume.

1. Hover over the data view and select **Export** .
2. From the Select a destination type drop-down menu, select **Device volume**.
3. Select a volume.
4. If you want to verify the data integrity after the export is complete, select the **Verify data integrity after this import is complete** check box.

NOTE If you select the **Verify data integrity** check box, the time to complete can increase significantly.

5. Select **Next** to test the connection to the endpoint.
6. After a successful validation, select **Export**.
7. On the confirmation window, select **OK**.

During the export operation, you can select **Dashboard** or **Data** to view the progress of the export.

Export data to an external endpoint

You can export data to a custom destination endpoint to any device such as Amazon AWS S3. To quickly create or edit endpoints, see Manage endpoints.

1. Hover over the data view and select **Export** .
2. From the Select a destination type drop-down menu, select **Data endpoint**.
3. Select a data endpoint.
4. If you want to verify the data integrity after the export is complete, select the **Verify data integrity after this import is complete** check box.

NOTE If you select the **Verify data integrity** check box, the time to complete can increase significantly.

5. Select **Next** to test the connection to the endpoint.
6. After a successful validation, select **Export**.
7. On the confirmation window, select **OK**.

During the export operation, you can select **Dashboard** or **Data** to view the progress of the export.

Inspect data and data events

You can view details about data activities and data bundles by using the Inspect action.

In Lyve Pilot, a bundle is a collection of data or data objects (e.g., files, S3 objects) added to the Lyve managed data ecosystem as a result of an import operation. During import, bundle data is fingerprinted and metadata is generated to describe the bundle contents. The combination of these assets gives a bundle a unique digital signature, and that signature is tracked and verified throughout the life of the data within the Lyve ecosystem.

A single bundle can exist in multiple locations within the Lyve ecosystem, and each location of the bundle corresponds to a particular activity. You can view data through two views, which are represented by the following tabs on the data detail screen:

- **Activity:** Shows information about the data activity that created or acted upon a corresponding bundle
- **Bundle:** Shows information about the bundle that was created or acted upon by the corresponding activity

Access Inspect

When you hover over items on the dashboard, as well as entries on the Data screen, the **Inspect** icon appears.

Select **Inspect** to open a detailed view of the item.

Alerts

If the bundle currently includes quarantined data, you see an alert tile at the top of the detail page, above the Activity and Bundle tabs. The tile shows information about when the failure occurred to cause the quarantine, the operation that failed, and the specific error that caused the failure.

From the alert, you can select Inspect for more detail, including recommended recovery actions. In some cases, you can perform a **Trust data** operation to accept the quarantined data and create a new bundle.

Activity tab

The Activity tab provides detail about what took place during the data action.

> **NOTE** If you open a data detail screen while an action is in progress, this tab displays a progress bar that updates to show the status of the action. If the action completes while you're viewing the detail, the progress bar goes away and the detail screen shows the completed action statistics.

The header line on the detail screen explains the type of data action and shows the source or destination of the action. The types of data activity include:

- **Import**: Imports unmanaged data into the Lyve managed data ecosystem.
- **Copy**: Copies data from one location in the Lyve ecosystem to another.
- **Export**: Exports data from the Lyve ecosystem to an external destination.
- **Delete**: Removes data from the Lyve managed data ecosystem.

The other information on the detail screen varies based on the action type. The specific fields that might appear include:

- **Status**: Shows whether the indicated action succeeded or failed. If the action failed, the failure reason is shown as well, if it is known.
- **Size**: Shows the total size of the data in the action.

- **Number of files**: Shows the number of data files involved in the action.
- **Source**: Shows the source location of the data in the action.
- **Destination**: Shows the destination location of the data in the action.
- **Throughput**: Shows the rate of transfer of the data during the action; also shows the total amount of data transferred in the action and the time the action took to complete.
- **Activity initiated by**: Shows the username and role (admin or standard) for the user who initiated the operation.

NOTE Not all fields appear for each activity type. Only relevant data is displayed.

Start actions from the Activity tab

From this tab, you can initiate several actions. Actions are context-sensitive so that each action appears only on data items where the action is possible.

From the header tile, you might select from the following actions:

- **Copy**: Copies data from one volume location in the environment to another. See Copy data for more information.
- **Export**: Exports data to an external source. See Export data for more information.
- **Delete**: Removes data from the source location. See Delete data for more information.
- **Verify data**: Verifies the integrity of the underlying data bundle. See Verify data for more information

Bundle tab

The Bundle tab displays information and history about the current data bundle. The information on this tab is divided into sections.

General information

The top section displays basic information about the bundle:

- **Bundle name:** The header line uses the bundle ID to describe the bundle.
- **Date/time:** Displays the date and time for when the bundle was created.
- **Size:** Shows the total size of the bundle.
- **Files:** Shows the total number of files in the bundle.
- **Volume:** Displays the volume name for the location of the bundle.

When you hover over this top tile, action icons appear. Actions you can take from here include:

- **Inspect:** Opens the bundle detail screen that shows a table listing all the files in the bundle.
- **Copy:** Copies data from one volume location in the environment to another. See Copy data for more information.
- **Export:** Exports data to an external source. See Export data for more information.
- **Delete:** Removes data from the source location. See Delete data for more information.
- **Verify data**: Verifies the integrity of the bundle. See Verify data for more information

Tags

The Tags section lets you review, edit, and update tags associated with the bundle. Select **Edit** to open the Tags dialog box.

For information about creating and editing tags, see Tag data.

Orchestration mode

Displays whether the bundle was transferred under the Enterprise Security or Enterprise Performance Orchestration Mode.

Activity history

This section lists all the events or actions for this bundle. Activity is shown with the most recent activities at the top.

Operations that completed successfully show a green check mark on the right. If an operation resulted in quarantined data or encountered other errors, a red warning icon is shown on the right instead.

NOTE If an activity is in progress, the tile for that action shows the progress bar.

The tiles in this section let you access the Inspect action. Select this action to view details about the specific action.

Other locations

This section lists other instances of the original bundle across the Lyve managed data ecosystem. When you copy a bundle to a new storage location within the environment, it keeps the same bundle ID but with added metadata that shows the activity as well as the new location of the data.

Each time you move or copy data, it remains linked to every other copy through the bundle ID. This section of the Bundle tab lets you easily find where every version of that bundle resides within the Lyve managed data ecosystem.

Verify data

When you perform an action in Lyve Pilot such as a data copy or export, your data is automatically verified before the action is executed. If data has changed or been corrupted since the previous activity on that data, the activity results in a failure and the bundle gets quarantined.

Lyve Pilot also lets you manually verify the integrity of your data at any time. Manually performing verification provides peace of mind that your data remains intact, and that future actions will succeed.

The Verify data action compares the data in the bundle with the Lyve metadata to ensure the data is unchanged since your last operation. Successful verification leaves your data untouched. However, a failed verification triggers a quarantine of the data.

You can invoke a Verify data action from:

- an Import or Copy event, whether on the dashboard feed, the table on the Data screen, or the Inspect view for the event.
- a view of the bundle itself, such as on the Bundle tab of a data detail screen.

Verify your data

To verify data integrity:

1. Select **Verify data** on the bundle or data event you want to verify.

2. On the Verify data dialog box, select **Verify data** to start verification.

During the verify operation, you can select Dashboard or Data to view the progress of the verification. If you need to cancel the operation in progress, hover over the event, then select Cancel ✕ .

When the operation completes, the event tile updates to show status and statistics. Remember that if the verification fails, the data is quarantined, which generates an Alert notification.

Tag data

You can apply tags to data bundles in Lyve Pilot to add unique identification to your data. Tags are user-defined labels that you can use to filter events on the dashboard feed so that you can easily focus on related items.

About tags

Because tags are defined by users, you can use them for grouping data bundles into categories such as:

- Business-specific data workflows that describe how the data is used
- Data sources such as camera, sensors, or vehicle
- Data destination such as hardware type or cloud service
- Data types such as documents or media

You should create tags that make sense in your environment and are helpful to your users. For instance, you can apply tags to data bundles to reflect different workflows.

When you create and apply tags, note the following rules:

- No more than 32 characters in tag names
- No more than 8 tags on any bundle
- You can't apply the same tag more than once per bundle

> NOTE Although you apply tags through activities on the dashboard feed, tags are associated with the underlying data bundles. For example, if you open the tag action from a data import event on the feed, then apply tags, those tags are associated with the data bundle that was imported. Therefore, any other actions on the feed for that same bundle are simultaneously populated with the same tag or tags.

> NOTE Make sure the **Show tags** toggle is on (to the right) to create and apply tags and show assigned tags on the dashboard feed.
>
> Setting the **Show tags** toggle to off hides all tags from the UI, but this setting doesn’t delete tags from activities or bundles. When you turn **Show tags** on, previously applied tags are displayed again with their associated feed items.

How to create and apply tags

If an event is based on a data bundle, you can add tags to it. The tag action is represented by the Tag icon 🏷 when you hover over the event.

1. Select Tag 🏷.
2. In the Tag dialog box, enter the tag name.
3. Select the tag button at the right side of the field to create the tag. You can also select Enter or Tab on your keyboard.

   Tags display below the field as they are created.
4. Repeat the previous step for each tag you want to apply to the bundle.
5. Select **Done**.

Tags appear at the bottom of feed items.

How to remove tags from bundles

1. Select Tag 🏷.
2. In the Tag dialog box, select the X for any tag you want to delete.
3. Select **Done**.

> **NOTE** This process removes the tag from the associated data bundle. However, it does not delete the tag itself, which could be applied to other bundles.

How to filter information by tags

When dashboard items and data bundles have tags, you can use those tags to filter the information presented in the view.

To use tag filters:

- Select a tag or multiple tags to immediately view content that meets tag filter criteria.
- Deselect any tag to remove it from the filter criteria and view the resulting filter criteria, or view all feed items if all tags are removed.

Filtering by multiple tags shows only items that include all tags that you've selected.

> **NOTE** If any filter is applied, you are not able to use the **Show tags** toggle to hide tags from view. The toggle is disabled as long as filters are active.

Delete data

At some point, you might want to delete data bundles from the Lyve managed data ecosystem. For instance, the files could be outdated or quarantined, or you could have copied a bundle to a different volume or device in the ecosystem and want to free space from the source location.

A Delete 🗑 action can be accessed from:

- the Data screen
- a data detail screen

The Delete action is available only for items that have data that can be deleted.

1. Select **Delete** 🗑. This icon appears when you hover over elements that have data that can be deleted.
2. In the confirmation window, select **Delete**.

   This dialog box includes information such as the location of the data to be deleted and the size of the bundle to ensure you are deleting the correct data.

While the action is in progress, an event with a progress bar is generated on the Lyve Pilot Dashboard. When the operation completes, the event displays details for the delete action.

Deploy Pilot Links

A Pilot Link is a Data Mover Service that runs in Kubernetes and can be instructed via the Lyve Pilot Cloud service to import, copy, and export data between different types of storage.

Pilot Links must be deployed prior to moving data into and around the managed environment.

The Pilot Link platform consists of the following components:

1. The Pilot Link deployment scripts and helm charts.
2. The Pilot Link Controller, responsible for managing the Pilot Link Data Services.
3. The Pilot Link Data Service, responsible for connecting with the Lyve Pilot Cloud service and conducting requested data operations.

For the most complete, up-to-date information on Pilot Links, visit the following URL:

https://github.com/Seagate/uds-deploy-k8s/blob/integration/README.md

Manage devices

Lyve Pilot creates a security domain of trusted devices and users so that you can securely manage and monitor your data. When you register a device with Lyve Pilot, that device is trusted by all other members of the managed domain. With trusted devices, you can import data into the ecosystem and copy data between devices securely.

The hardware currently supported with Lyve Pilot is:

- Lyve Mobile Shuttle
- Lyve Mobile Array
- Pilot Link

The following pages show how to add a device to your secure domain and describe other hardware management tasks.

- Register a device
- Inspect devices and device activity
- Remove a device from Lyve management

For information about importing data and working with data in your managed domain, see Manage data. For more information about how Lyve Pilot secures data and devices, see Security model.

Register a device

You must register each device to be part of the Lyve Pilot managed environment.

Pilot Links must be deployed prior to moving data into and around the managed environment.

View the Pilot Link

Prior to completing this section, a controller and data service pod must be created.

1. Select **Devices** from the menu.
2. Select the **Inspect** icon.
3. To edit the **Pilot Link** name, select the **Edit** icon.
4. On the **Device volume** tab, any storage that was provisioned in Kubernetes displays along with the volume name, status, unmanaged data, capacity, and Last Activity. After Last activity, the icons are displayed to allow Import, Copy, and Export of data to and from the device volume.

   After Last activity, the icons are displayed to allow Import, Copy, and Export of data to and from the device volume.

5. On the **Assigned endpoints** tab, the Name or Volume ID of the Linked endpoint displays along with the Type, URL, Connected to, Status, Capacity, and Last Activity.

   After Last activity, the icons are displayed to allow you to Disconnect or Unassign the endpoint and Copy or Export data.

   Above the table, is the Assign a Linked endpoint icon where you can assign a new or existing linked endpoint.

Register a Lyve Mobile Shuttle

Follow the steps on the display of the Lyve Mobile Shuttle to securely register and encrypt your device and authenticate and connect to Lyve Pilot.

1. Follow the instructions in the Lyve Mobile Shuttle User Manual to power on your Lyve Mobile Shuttle by connecting the power cable.
2. From the display, follow the onscreen instructions to complete the setup.
3. When "Lyve Shuttle is Ready" displays, tap the menu icon, then **Lyve Pilot Connect**.
4. On the Connect screen, tap **Next**.
5. On the Upgrade screen, select the check box to delete all data, then select **Next**.
6. From a computer or tablet, sign in to Lyve Pilot.

   For additional instructions, see Managing users.

7. On the Lyve Mobile Shuttle, select **Next**.
8. Follow the instructions on the Identifier Token screen to add a device in the Lyve Pilot portal.
9. From the Lyve Pilot portal menu, select **Devices**, then select Add device to Lyve Pilot ⊕.
10. Enter the identifier token from the Lyve Mobile Shuttle, then select **Next**.
11. Enter the Lyve Pilot Token from the Lyve Pilot portal into the Lyve Mobile Shuttle, then select **Next**.
    The shuttle is formatted and encrypted. When the device successfully connects to the Lyve Pilot domain, you receive a notification in the portal. On the dashboard, you see that the device is placed under Lyve management, disconnected, and reconnected when the formatting finishes.

Inspect devices and device activity

The Inspect action in Lyve Pilot provides details about data and devices. For device items, details include information about the type of device, what data and volumes are on the device, available capacity of the device, and similar relevant information.

Access Inspect

When you hover over items on the dashboard, as well as entries on the Data and Devices screens, the **Inspect** icon appears.

Select **Inspect** to open a detailed view of the item.

Review device information

The device detail screen provides information about hardware in the Lyve managed data ecosystem. The device detail screen is divided into four sections:

- General information
- Data allocation
- Activities section
- Volume information
- Device information

General information

This section displays general information about the physical hardware. The header is the name of the device. When you add a device, Lyve Pilot inserts its recognized name. You can customize the name here on the detail screen:

1. Click the Edit icon that appears beside the name on hover.
2. Enter your new name in the field.
3. Select Enter or Tab to apply the change.

Every place where the device name displays updates automatically to the new name.

> NOTE As a best practice, choose a naming scheme that is meaningful, consistent, and easy to remember, then apply your own names to devices so that they are easy to recognize by all users. For instance, your names might include information about where devices are located or what they are used for.

Other information displayed in this upper section includes:

- **Type of device**: For example, *Lyve Shuttle*, *Lyve Client*, and *Lyve Mobile Array* are types of devices.

  > NOTE The device icon represents the device type. Different device types in your environment are easily distinguished by different images.

- **Connection status**: The indicator dot shows whether the connection to the device is healthy (green) or disconnected (gray). Hover over the dot for a pop-up that shows when the device was last synced to the domain.
- **Managed files**: Shows the number of files from the device that are part of the Lyve managed data ecosystem.

Data allocation

The upper-right section displays live data utilization information for the device. The arc graph gives a visualization of the total storage space available along with the amount of data on the device that is managed as well as unmanaged, if any.

Below the graph, the same information is listed as numerical data for total available space, managed data, and unmanaged data, including the percentage of available space represented by each.

Activities section

When activities related to the device are in progress, tiles for those activities are added temporarily to the center portion of the detail screen. These tiles are essentially the same as those on the dashboard feed.

Tiles in this section show a progress bar for the ongoing activity and information about what the activity is (copy, export, and so forth) and when it started. The tile also lets you take actions:

- **Cancel:** Stops the ongoing activity
- **Inspect:** Loads a detail screen with more information about the ongoing activity

When an activity completes, the tile closes out from the activities section. If no actions are ongoing, no tiles are present in this section.

Volume information

This section displays information about volumes on the device and lets you drill down to examine data within those volumes. The table includes two tabs:

- **Managed volumes**: Displays information about the volumes that have been registered and authenticated to the Lyve managed data ecosystem. Typically, these volumes are the partitioned storage volumes that are internal to the connected device.
- **Unmanaged volumes**: Displays information about volumes recognized by the device that have not been registered and authenticated to the Lyve managed data ecosystem. These volumes can be external volumes, such as SD cards, USB cards, or external NAS/DAS attached storage volumes.

The volume information tables includes five columns:

- **Name**: The recognized name for the volume.
- **Status**: A colored dot that indicates the health of the volume: healthy (green) or disconnected (gray). Hover over the dot for a pop-up to view the state of the volume (e.g., online/offline) along with other relevant information.
- **Capacity**: Shows the amount of data on the volume and the total storage available on the volume.
- **Unmanaged data**: (for managed volumes only) Shows the amount of unmanaged data on the volume—that is, data that hasn't yet been imported into the Lyve managed data ecosystem.
- **Last activity**: Displays information about the most recent activity on the volume: the type of action as well as the date and time when it took place. If an action is in progress, you will see an in-progress indicator here.

Device information

This section displays information about Lyve Client devices and lets you drill down to examine devices and data within these volumes. The table includes three tabs:

- **Managed devices**: Displays information about the devices that have been registered and authenticated to the Lyve managed data ecosystem through Lyve Client.

- **Unmanaged devices**: Displays information about the devices that have not been registered and authenticated to the Lyve managed data ecosystem through Lyve Client.
- **Unmanaged volumes**: Displays information about volumes recognized by the device that have not been registered and authenticated to the Lyve managed data ecosystem. These volumes can be external volumes, such as SD cards, USB cards, or external NAS/DAS attached storage volumes.

Start actions from the device detail screen

From the device detail screen, you can initiate several actions.

For managed volumes, select from the following actions:

- **Import**: Imports data to the Lyve managed data ecosystem. See Import data for more information.

> **NOTE** The Import option is available only if unmanaged data exists on the managed volume. A disabled (gray) import icon indicates that no data is available to import.

- **Copy**: Copies data from one location in the environment to another. See Copy data for more information.
- **Export**: Exports data to an external source. See Export data for more information.

For unmanaged volumes, the only action available is Import, which lets you add data to the Lyve managed data ecosystem.

While an action is in progress, an event with a progress bar is generated on the Lyve Pilot dashboard and that event also appears in the center of the device detail screen. When the operation completes, the event tile closes out from the device detail screen, while the event on the dashboard displays details for the completed action.

Review endpoint information

The device detail screen provides information about hardware in the Lyve managed data ecosystem. The device detail screen is divided into four sections:

General information

This section displays general information about the endpoint. The header is the name of the endpoint. When you add an endpoint, Lyve Pilot inserts its recognized name. You can view the status of the Pilot Link and customize the name here on the detail screen:

1. Click the Edit ✎ icon that appears beside the name on hover.
2. Enter your new name in the field.
3. Select Enter or Tab to apply the change.

Every place where the device name displays updates automatically to the new name.

> **NOTE** As a best practice, choose a naming scheme that is meaningful, consistent, and easy to remember, then apply your own names to devices so that they are easy to recognize by all users. For instance, your names might include information about where devices are located or what they are used for.

Other information displayed in this upper section includes:

- **Type of device**: For example, *Pilot Link*, *Lyve Shuttle*, *Lyve Client*, and *Lyve Mobile Array* are types of devices.

> **NOTE** The device icon represents the device type. Different device types in your environment are easily distinguished by different images.

- **Connection status**: The indicator dot shows whether the connection to the device is healthy (green) or disconnected (gray). Hover over the dot for a pop-up that shows when the device was last synced to the domain.
- **Capacity**:Shows the amount of data on the volume and the total storage available on the volume.

Volume and endpoint information

This section displays information about device volumes and assigned endpoints lets you drill down to examine data within these areas. The table includes two tabs:

- **Device volumes**: Displays information about the volumes that have been registered and authenticated to the Lyve managed data ecosystem. Typically, these volumes are the partitioned storage volumes that are internal to the connected device.
- **Assigned endpoints**: Displays information about endpoints that have been assigned to devices, shares, or S3 objects.

Activities section

When activities related to the device are in progress, tiles for those activities are added temporarily to the center portion of the detail screen. These tiles are essentially the same as those on the dashboard feed.

Tiles in this section show a progress bar for the ongoing activity and information about what the activity is (copy, export, and so forth) and when it started. The tile also lets you take actions:

- **Cancel:** Stops the ongoing activity
- **Inspect:** Loads a detail screen with more information about the ongoing activity

When an activity completes, the tile closes out from the activities section. If no actions are ongoing, no tiles are present in this section.

Device volumes information table

The device volume information table includes five columns:

- **Name**: The recognized name for the volume.
- **Status**: A colored dot that indicates the health of the volume: healthy (green) or disconnected (gray). Hover over the dot for a pop-up to view the state of the volume (e.g., online/offline) along with other relevant information.
- **Unmanaged data**: (for managed volumes only) Shows the amount of unmanaged data on the volume—that is, data that hasn’t yet been imported into the Lyve managed data ecosystem.
- **Capacity**: Shows the amount of data on the volume and the total storage available on the volume.
- **Last activity**: Displays information about the most recent activity on the volume: the type of action as well as the date and time when it took place. If an action is in progress, you will see an in-progress indicator here.

Assigned endpoints information table

The assigned endpoints volume information table includes seven columns:

- **Name or Volume ID**: The recognized name for the endpoint.
- **Type**: The type of share such as S3, SMB, or NFS.
- **URL**: Shows the URL of the share..
- **Connected to**: Shows the name of the Pilot Link.
- **Status**: A colored dot that indicates the health of the volume: healthy (green) or disconnected (gray). Hover over the dot for a pop-up to view the state of the volume (e.g., online/offline) along with other relevant information.
- **Capacity**: Shows the amount of data on the volume and the total storage available on the volume.
- **Last activity**: Displays information about the most recent activity on the volume: the type of action as well as the date and time when it took place. If an action is in progress, you will see an in-progress indicator here.

Remove a device from Lyve management

You can remove a registered device from the Lyve managed data ecosystem. If you do, the device is no longer seen by the Lyve environment and can't be used as a target for import or data copy actions.

> **IMPORTANT** Removing a Lyve Mobile Shuttle from the Lyve managed data ecosystem immediately causes a secure erase of the data on the device. Your data on the device is destroyed, so be certain you have a backup elsewhere or you no longer need the data before you remove a Lyve Mobile Shuttle from Lyve management.

> **NOTE** Only Admin users can perform a Remove device action. Standard users don't see this option. For information about user access levels, see Manage users.

How to remove a device

1. From the Device screen, select **Inspect** on the device you want to remove.
2. Hover over the top section of the device's detail screen, then select **Remove**.
3. On the Remove device dialog box:
   - If you are removing a Lyve Mobile Shuttle:
     1. Select the check box to acknowledge that you know you will erase your data from the device.

        > **IMPORTANT** Removing a Lyve Mobile Shuttle from the Lyve managed data ecosystem immediately causes a secure erase of the data on the device. Do not take this action unless you are sure you don't need this data.

     2. Select **Remove device**.
   - If you are removing a different type of device:
     1. Select **Remove device**.

        > **NOTE** Data on the device is not deleted but it will no longer be part of the Lyve managed data ecosystem.

If you want to use a device with Lyve Pilot again after removing it, you need to follow the registration process to add it as a new device. The Lyve system will see it as a new device from that point. For information about adding devices, see Register a device.

Manage endpoints

Endpoints are storage locations outside of Lyve Pilot. These endpoints are destinations where you can copy and export your Lyve Pilot data. You can create and edit custom endpoints in the Endpoints menu. Once endpoints are created, you can register and assign a Pilot Link which provides the ability to import, copy, and export data in a hybrid cloud environment.

There are two types of endpoints, linked endpoints and unmanaged-data endpoint.

- A linked endpoint is an endpoint that uses a Pilot Link to provide Lyve Pilot services to this location, including import, copy, and storage of managed data. The Pilot Link can help perform operations on the linked endpoint and apply metadata tracking. You must have at least one Pilot Link set up and operating on your network to be able to create a linked endpoint. A linked endpoint can only connect to a Pilot Link that it is assigned to and can only connect to a single Pilot Link at a time. The Pilot Link works as an agent for the endpoint providing capacity information and updates as well as working to orchestrate data operations at that endpoint.
- An unmanaged-data endpoint sits outside of Lyve Pilot and cannot track or manage data. It works only as a source to import data into the Lyve managed data ecosystem or as a destination for exporting data from the Lyve managed data ecosystem.

Add a linked endpoint

1. From the Lyve Pilot portal menu, select **Endpoints**.
2. Select Linked endpoints.
3. Select Add endpoint ⊕.
4. Enter the endpoint name you want to display in Lyve Pilot.
5. Select endpoint type **S3** or **SMB**.
6. For S3 Object Storage,
   - Enter the URL.
   - Enter the Access key ID.
   - Enter the Secret access key.
7. For SMB,
   - Enter the URL.
   - Enter the Domain.
   - Enter the Username.
   - Enter the Password.
8. Under Pilot Link assignments, select the Pilot Link to associate with this endpoint.

   A green dot next to a Pilot Link indicates a good status.
9. Select **Connect**.

   A confirmation message is displayed indicating that your request has been initiated and this may take some time. You can track the progress of this activity in your dashboard notification feed.

   Lyve Pilot will attempt to find a Pilot Link to connect with from the list of assigned Pilot Links. If it can establish a connection with one of these, the endpoint information is saved in the database and the endpoint is connected to that Pilot Link. If it does not find a Pilot Link or cannot establish a connection with one of them, the endpoint is not created or saved.

Add an Unmanaged-data endpoint

1. From the Lyve Pilot portal menu, select **Endpoints**.
2. Select Unmanaged-data endpoints.
3. Select Add endpoint ⊕.
4. Enter the endpoint name.
5. Select endpoint type **S3**, **Amazon S3**, **SMB**, or **NFSv3**.
6. For S3 Object Storage,
   - Enter the URL.
   - Enter the Access key ID.
   - Enter the Secret access key.
7. For Amazon S3,
   - Enter the URL.
   - Enter the IAM AWS Access key ID.
   - Enter the IAM AWS Secret access key.
8. For SMB,
   - Enter the URL.
   - Enter the Domain.
   - Enter the Username.
   - Enter the Password.
9. For NFSv3,
   - Enter the URL.
10. Select **Connect**.
    A confirmation message is displayed indicating that your create/edit request has been initiated and this may take some time. You can track the progress of this activity in your dashboard notification feed.

Edit an endpoint

1. From the Lyve Pilot portal menu, select **Endpoints**.
2. Select Linked endpoints or Unmanaged-data endpoints.
3. Hover over the endpoint row and select **Edit** ✎.
4. Select **Disconnect**.

   If the endpoint is a linked endpoint, it must be in a disconnected state before editing the URI and credential details.
5. Select Edit to update any of the fields you need to change.
6. If you need to re-enter your credentials, select **Optional: re-enter credentials** and edit or update the any of the fields you need to change.
7. Select **Save**.

Assign a linked endpoint

1. You can assign a linked endpoint on the Devices or the Endpoints menu:
   - From the Lyve Pilot portal menu, select **Devices**, hover over the device row, and select **Assign**⊕.
   - From the Lyve Pilot portal menu, select **Endpoints** and select **Assign**⊕.
2. To assign a new Linked endpoint to a device:
   - From the **Devices** menu, select the appropriate device from the device list.
   - From the **Assigned endpoints** tab, select **Assign Linked endpoint**⊕.
   - For an existing endpoint, select the Linked endpoint.
   - For a new endpoint, select **New** and enter the endpoint name.
   - Select the endpoint type **S3** or **SMB**.
   - For an S3 endpoint, enter the URL, Access key Id, and Secret access key.
   - For an SMB endpoint, enter the URL, Domain, Username, and Password.

Remove an endpoint from Lyve management

1. To remove an endpoint Linked endpoint from Lyve management,
   - From the Lyve Pilot endpoint menu, select Linked endpoints, hover over the endpoint row, and select **Remove** ⊖.
   - From the Lyve Pilot endpoint menu, select Unmanaged-data endpoints, hover over the endpoint row, and select **Remove** ⊖.
2. Read the message for endpoint type and select **Delete**.
   - For the Linked endpoint, "Do you want to remove linked-endpoint-1 from Lyve management?"
   - For the Unmanaged-data endpoint, "You are about to delete this unmanaged-data endpoint. Your credentials will be removed from the system and you will no longer have access to this endpoint. Are you sure you want to continue?"

Manage settings

Lyve Pilot lets you efficiently and securely manage data across your enterprise. When you import data into the Lyve managed data ecosystem, the system generates unique metadata and fingerprinting, which is used to identify the data and ensure it remains intact and has not been tampered with or corrupted.

The following pages describe in detail the settings for Lyve Pilot.

- Manage users
- Manage orchestration mode

For information about working with devices and adding devices to the secure domain, see Manage devices. For more information about how Lyve Pilot secures data and devices, see Security model.

Manage users

Lyve Pilot supports two types of users: Admin and Standard. A deployment must always contain at least one Admin and there can be an unlimited number of users. Admins can create users and reset passwords for other users.

Log in using email and token

1. Obtain the credentials and web address for your account.

   You will receive an email with the email address for the administrator, a one-time-use numeric token, and a URL for your site.

2. Open a web browser.

   Currently, Chrome is the preferred browser.

3. Enter the URL.

   The URL starts with pilot.lyve.seagate.com followed by your customer ID.

   The application uses the standard https port 443.

   ```
   https://pilot.lyve.seagate.com/customerID/
   ```

4. If necessary, accept the self-signed certificates.
5. Select **Sign in using a token**.
6. Enter the Email and Token.

   The email address is case-sensitive.

   The password token must be entered prior to the expiration date and time.

7. Select **Validate token** to complete the initial log in.
8. Read and accept the Terms & Conditions, Privacy Policy, and End User License Agreement. Select **Next**.
9. Enter and confirm your new password.

   Passwords must be 8-64 characters in length. There are no required character types. However, password complexity is enforced. A pop-up window next to the password field shows password strength and gives suggestions for making stronger passwords. A password must be rated somewhat strong or better to enable the **Apply password** button.

10. Select **Apply password** to create the password and log in to the portal.
11. Complete your user profile details and select **Save user**.

    A welcome message is displayed on the dashboard and you can start to inspect, track, and manage data using notifications on the dashboard.

Log in using email and password

You must enter your username and password to access the system.

1. Open a web browser.
2. Enter the URL.

   The application uses the standard https port 443.

   ```
   https://pilot.lyve.seagate.com/customerID/
   ```

3. If necessary, accept the self-signed certificates.

4. Enter the Email and Password.
5. Select **Login** to log in to the portal.

View users

Users with a Standard or Admin role can view a list of all users.

1. From the Lyve Pilot portal menu, select **Settings**.
2. On the Users tile, select Inspect 🔍 to view the current user tile and a list of all users.
3. Hover over a user tile and select Inspect 🔍 to open a detailed view of a user.

Create a new user

You must have admin privileges to create a new user. When you create a new user, you receive a password token. This token should be shared with the new user and will be required for their initial login.

1. From the Lyve Pilot portal menu, select **Settings**.
2. On the Users panel, select Inspect 🔍 to view the current user and a list of all users.
3. Select Add user ⊕.
4. Enter the Email address.
5. If the user should have admin privileges, select the Admin user check box.
6. Enter the Full name.
7. Optional. Enter the Phone number.
8. Optional. Enter the Location.
9. Select **Create user** to create the new user.
10. On the confirmation window, select **OK**.

    This dialog box includes the email address, password token, and the expiration date and time of the token.

⚠ **CAUTION** The user must create a password and activate their account by the expiration deadline, or a reset password will need to be issued.

Reset a user password

A person with the Admin role can initiate a password reset for another user.

1. From the Lyve Pilot portal menu, select **Settings**.
2. On the Users tile, select Inspect 🔍 to view the current user tile and a list of all users.
3. Hover over a user tile and select Inspect 🔍 to open a detailed view of a user.
4. Select **Reset password**.
5. On the confirmation window, select **Reset password**

6. Confirm the password reset.
7. Send the password token to the user requesting the reset.

⚠ **CAUTION** The user must reset the password by the expiration deadline.

Manage orchestration mode

Lyve Pilot supports two orchestration modes: Enterprise Security and Enterprise Performance. Orchestration modes allow you to tune the level of performance and security in Lyve Pilot. The orchestration mode setting will apply to your data for its entire lifetime within the Lyve data environment. You can override the default orchestration mode for any individual import.

Enterprise Security mode is the highest level of security and utilizes all security capabilities available to Lyve Pilot to track and protect your data as it moves through your Lyve environment.

- Recommended for environments where data security is the highest priority.
- Files are digitally fingerprinted with a cryptographic hash to guarantee individual authenticity as they move through your Lyve environment.
- A private blockchain is applied to each file to record file history and support recognition of data corruption or tampering at the individual file level.

Enterprise Performance mode is the highest level of performance and trades file-level data protection for maximum performance during imports, copies, and exports of your data. Your data is still tracked and protected as a bundle.

- Recommended for environments orchestrating data movement of small files, or for environments where file corruption and tampering are highly unlikely events.
- Data is digitally fingerprinted at the bundle container level so you can verify that bundle structure is not altered while moving through your Lyve environment.

Set default orchestration mode

Users with a Standard or Admin role can view a list of all users.

1. From the Lyve Pilot portal menu, select **Settings**.
2. On the Orchestration mode tile, select Inspect ⊕ to view the current default orchestration mode.
3. Select the Enterprise Security or Enterprise Performance tile.

Troubleshoot

This table lists possible errors seen when data is being imported, copied, or exported and recommended actions to resolve the problems.

Data mismatch	**Alert:** Data has been quarantined due to data mismatch
	Details: During a copy or export activity, one or more of your destination files was detected as inconsistent with its bundle metadata and therefore is no longer trusted data. This situation is most likely to happen due to a write error during the activity.
	Recommendations: Retry this activity using a trusted copy of this data. In many cases, repeating the activity will lead to successful completion. After you have successfully completed your activity without quarantine failure, you can safely delete the data that was quarantined.
Not enough space	**Alert:** There is not enough available space to perform the requested activity
	Details: The destination volume specified in this activity has run out of space. This activity fails, and the data is deleted from the destination volume.
	Recommendations: Verify that your destination has enough available space to complete the activity successfully. Delete unnecessary data from the destination volume or choose a different destination device or volume before retrying the activity.
Failed transfer	**Alert:** At least one item failed to transfer during this activity
	Details: One or more files were not successfully transferred to the destination volume, resulting in an incomplete bundle. The activity will be marked as failed.
	Recommendations: Verify connectivity between your source and destination device, then retry the activity. Also verify that both source and destination devices are online and operational. The incomplete bundle left behind by this failed activity is safe to delete at any time.
Inaccessible destination or source	**Alert:** An activity failed because the destination or source storage device is inaccessible
	Details: Either your source volume or destination is unreachable at this time. This situation is most likely to occur because of network or cabling issues.
	Recommendations: Verify connectivity between your source and destination device, then retry the activity. It is important to note that even though the portal is connected to both source and destination devices, network or cabling problems can keep the devices from connecting to one another, which is required for the activity to succeed. Make sure both source and destination devices are online and operational.
Validation failure	**Alert:** Data has been quarantined due to a pre-check validation failure
	Details: You have requested an activity be performed on source data that failed pre-check bundle validation. Either your bundle metadata is corrupt or missing, or your data does not match the bundle manifest. Your source data cannot be validated and thus cannot be trusted to be copied or exported to another location.
	Recommendations: Re-establish consistent metadata and source data for this data bundle by finding a trusted copy of this data and copying it to this device. If this data was imported from an external volume, it will need to be re-imported in order to establish a valid bundle. When you have a valid bundle, you can safely delete the data that was quarantined.
Missing file	**Alert:** Data has been quarantined because at least one file is missing
	Details: At least one file listed in your bundle metadata is not present in your bundle, so your bundle has been quarantined.
	Recommendations: Re-establish consistent metadata and source data for this data bundle by finding a trusted copy of this data and copying it to this device. If this data was imported from an external volume, it will need to be re-imported in order to establish a valid bundle. When you have a valid bundle, you can safely delete the data that was quarantined.

Glossary

A

add device

The process of authenticating and authorizing new hardware to the Lyve managed data ecosystem.

B

bundle

A collection of data or data objects added to the Lyve managed data ecosystem as a single import operation.

D

device

The physical hardware that you connect (register) to the Lyve managed data ecosystem.

device health

The current known status of the hardware device; for example, Healthy or Disconnected.

F

fingerprinting

The process of deriving a unique value for data, typically a hash that represents the content of the data over which it is calculated.

I

identifier token

A number that is randomly generated and shown on the device display or web client and that is required to be entered in the Lyve Pilot portal to complete authentication of that device.

inspect

An action in Lyve Pilot that lets you view detailed information about devices, data, and activities.

inspect a device

An action in Lyve Pilot that lets you view detailed information about a registered storage device.

inspect data

An action in Lyve Pilot that lets you view detailed information about a data event.

L

Lyve Client

Desktop-based Windows, Mac, or Linux client for configuration and management of Lyve Mobile devices. Lyve Pilot uses Lyve Client as a proxy to manage data orchestration for Lyve Mobile devices.

Lyve managed data

Data that has been imported into the Lyve managed data ecosystem and secured with unique metadata and fingerprinting.

Lyve managed data ecosystem
The security domain established when devices register and authenticate to the Lyve Pilot portal.

M

managed data
Data that has been imported into the Lyve managed data ecosystem and secured with unique metadata and fingerprinting.

managed volume
A volume on a device that has been registered and authenticated to the Lyve managed data ecosystem.

metadata
Data recorded for each data bundle imported into the Lyve managed data ecosystem that tracks the initial state of all objects included and adds information about post-import changes, such as data moves or the addition of user-defined tags.

P

Pilot Link
A device that links your data endpoints for the purposes of data orchestration and runs inside a Kubernetes container. Provides the ability to import, copy, and export data to any storage device in a hybrid cloud environment.

provenance
Security principle that seeks to demonstrate that data imported into the Lyve managed data ecosystem, including its generated fingerprint, has not been manipulated or corrupted at any point.

R

register device
The process of authenticating and authorizing new hardware to be placed under Lyve management.

T

tag
A user-defined label assigned to a data bundle as metadata, and which can be used for sorting and filtering data within Lyve Pilot.

tagging data
The process of assigning user-defined labels to bundles that can identify business processes, data origin, and other information.

U

undiscovered volume
A volume on a device that has been registered and authenticated to the Lyve managed data ecosystem but has not made a network connection to the source device when you attempt a Copy operation.

unmanaged data
Data that is accessible on or through a managed volume but that has not been imported into the Lyve Managed Data ecosystem.

unmanaged volume

A volume that is accessible through the Lyve Managed Data ecosystem but is not part of the managed ecosystem.