

StorageLink Web Administrator Guide

*This guide is for administrators who deploy, configure, and operate StorageLink. It covers the Web Admin Interface, the REST API, application properties, and server-side administration. For instructions you can share with your end users (the people uploading and downloading files), see the separate **StorageLink Web User Guide**.*

Table of Contents

1. [Introduction](#)
 2. [First Launch Experience](#)
 3. [Admin Web Interface](#)
 4. [Managing Folders](#)
 5. [Managing Users](#)
 6. [Settings: Cloud Credentials](#)
 7. [Settings: Identity Providers \(OIDC\)](#)
 8. [Settings: Theme Customizations](#)
 9. [Settings: Language](#)
 10. [Settings: Backup & Recovery](#)
 11. [Transfer Jobs](#)
 12. [Application Properties](#)
 13. [API Reference](#)
 14. [High Availability Deployment](#)
 15. [Server Administration](#)
 16. [Security Best Practices](#)
 17. [Troubleshooting](#)
 18. [Frequently Asked Questions](#)
-

Introduction

StorageLink is a cloud storage gateway that lets users move files in and out of cloud storage through a web browser. When a user uploads a file through the StorageLink web interface, that file is written immediately to your configured cloud storage backend (Amazon S3, Azure Blob Storage, Azure File Share, or Google Cloud Storage) — there is no intermediate staging area or sync process.

Key Benefits

- **No client software for end users.** Users connect with any modern browser.
- **Direct cloud writes.** Files land in cloud storage as users upload them.
- **Multi-cloud.** Connect to AWS S3, Azure Blob, Azure File Share, and GCS from a single instance — and mix providers within one user's view.

- **Centralized management.** Manage users, folders, and cloud credentials from a single Web Admin Interface.
- **API automation.** Programmatically upload files and manage configuration via REST API.
- **Identity provider integration.** OIDC SSO with Microsoft Entra ID, Google, Okta, Ping, AWS Cognito, and any standards-compliant IdP.

Architecture Overview



StorageLink stores its own configuration (users, folder structure, cloud credentials, audit logs) in a PostgreSQL database (embedded for single-instance, external for HA). Uploaded files are *not* stored on the StorageLink server — they go directly to your cloud storage. The server only needs disk space for the OS, the application, and rotated logs.

Two User Types

StorageLink has two distinct user types:

Type	What they can do	Sign-in URL
Admin User	Manage folders, Web Users, cloud credentials, IdPs, system settings	Web Admin Interface (the URL you go to)
Web User	Upload, download, rename, and delete files within their assigned folder	Same URL — the interface adapts based on role

Both types share the same sign-in page; what they see after sign-in differs.

First Launch Experience

The first time you launch a fresh StorageLink instance, you'll complete a one-time configuration — accessing the Web Admin Interface, signing in (or creating an admin account), and configuring a default cloud storage location. These steps happen in the browser; no SSH is required.

Accessing the Web Interface

After your StorageLink instance is provisioned, open a web browser and go to its public IP or hostname:

<https://<your-storagelink-ip>>

[?](#)

Finding the IP:

- **AWS:** In the CloudFormation console, open your stack and check the **Outputs** tab for the **Hostname** value.
- **Azure:** Open the VM in the Azure Portal and copy the **Public IP address** from the overview page.
- **Google Cloud:** Open Deployment Manager, find your StorageLink deployment, and click the **Site address** link.

If you land on the HTTP page first, click the **Click here** link to be redirected to HTTPS.

Bypassing the Self-Signed Certificate Warning

StorageLink ships with a self-signed SSL certificate, so your browser will display a security warning the first time you visit. Click **Advanced**, then **Proceed to <ip-address> (unsafe)** to continue. You can replace the certificate with your own later (see [SSL Certificates](#) under Server Administration).

Creating an Admin Account

The admin account flow differs by cloud:

- **AWS:** The admin account is created automatically using the **Web Admin Username** and **Web Admin Password** values you supplied to CloudFormation. You will be brought directly to the sign-in screen.
- **Azure / Google Cloud:** On the Welcome page, enter a username (e.g., **admin**) and a complex password (one uppercase, one lowercase, one digit, one special character, **at least 12 characters**), then click **Create Account**.

After creating or signing into the admin account, you'll be prompted to configure default storage.

Configuring Default Storage

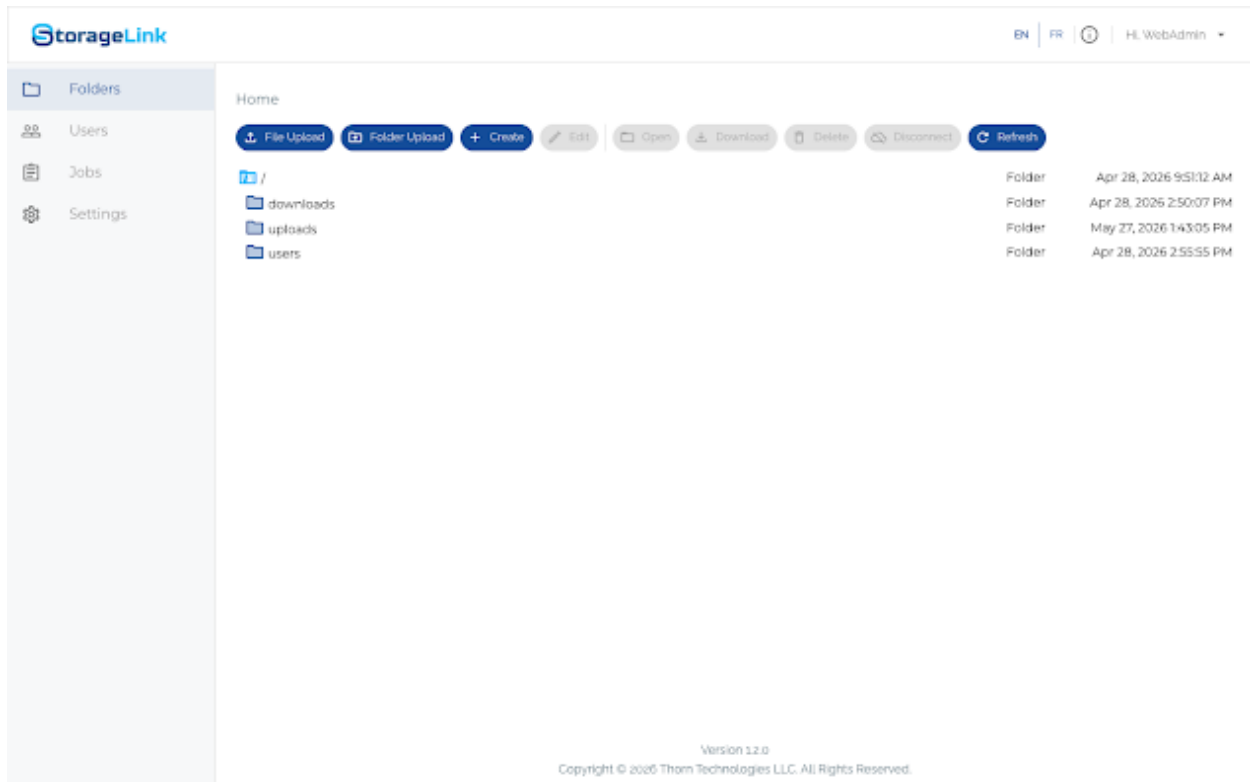
The default cloud storage location is associated with the root / folder. All other folders inherit from this unless you override them.

- **AWS:** A default S3 bucket named **swiftgw-i-<ec2_instance_id>** is created and wired up automatically. To use your own bucket instead, edit the root / folder on the Folders page and change the S3 URL.
- **Azure / Google Cloud:** A **Configure Default Storage** popup appears. Click **OK** to open the **Add Azure Cloud Connection** or **Add Google Cloud Connection** form. Fill in the required fields, click **Test Connection**, and then **Save**.

A successful **Test Connection** returns three green checkmarks. If it fails, fix your settings before continuing — first-launch setup can't complete without a working default connection on Azure or GCP.

Admin Web Interface

After signing in as an Admin User, you'll land on the **Folders** page:



Layout

- **Sidebar (left):** Four navigation items, each with an icon — **Folders, Users, Jobs, Settings.**
- **Top bar:** EN / FR language toggle, info icon, and your username with a dropdown ("Hi, WebAdmin ▼") that contains **Change Password** and **Log Out.**
- **Main area:** Page content. Always has a **breadcrumb** at the top showing where you are.
- **Footer:** Version number (this guide is based on **1.2.0**) and copyright.

Sidebar Sections

Section	Purpose
Folders	Browse and configure the virtual file system, including cloud-storage mappings
Users	Create and manage Admin Users and Web Users
Jobs	View and manage in-progress and completed transfer jobs
Settings	Cloud credentials, identity providers, theme, language, backup/recovery

Managing Folders

How the Virtual File System Works

The **Folders** page shows a *virtual* file system that all your users (admins and web users alike) share a single view of. It is **not** a Linux filesystem — it's a structure stored in StorageLink's database. Every folder maps to either:

- a **Cloud Connection** (its own bucket / container / storage account), or
- the parent folder's Cloud Connection (**inherited**).

The root `/` folder must always have a Cloud Connection. Below that, you mix-and-match.

`[?]/` → Default Cloud Connection (e.g., Azure container "claude")
`/users/` → inherited from `/`
`/users/alice/` → inherited from `/users/`
`/shared-finance/` → override → Cloud Connection "Finance Bucket"

`[?]`

When you create a folder in StorageLink, it does **not** appear in cloud storage immediately. It only materializes when a Web User signs in and accesses it.

Toolbar

When you have a folder selected, the toolbar shows:

Creating a Folder

1. From the Folders page, click **Create**.
2. The Add Folder dialog opens:

3. Enter a **Name** (nested names with / are not allowed — create one level at a time).
4. Choose **User Permissions**. By default a new folder is "Only administrators can access this folder" — you'll grant Web User access via the user record or by editing the folder later.
5. Choose a **Cloud Connection** option:
 - **Inherit from Ancestor Folders** — the new folder uses the parent's cloud connection. The form shows the inherited path so you can confirm where files will land.
 - **Map to a specific provider** — pick AWS, Azure Blob, Azure File Share, or GCS and fill in the per-provider fields.
 - **Use Existing Cloud Credentials** — point to an existing saved Cloud Credential (set up under Settings).
6. Click **SAVE**.

Editing a Folder

Select a folder and click **Edit**. The same form appears, pre-populated. You can change:

StorageLink EN FR ⓘ Hi, WebAdmin ▾

Folders

Users

Jobs

Settings

Edit folder ?*
The root folder can't be renamed

User Permissions
Only administrators can access this folder.

Cloud Connection
Map to Azure Blob Storage ▾

Storage Account Name
dyspro

Container Name
claude/

☐ HNS is enabled

▸ **Advanced Options**

Cloud Credentials
Use Existing Credentials ▾

Saved Azure Storage Account Credentials
Azure creds - dyspro sa ▾

Test Connection

SAVE **CANCEL**

Version 1.2.0
Copyright © 2026 Thom Technologies LLC. All Rights Reserved.

Support + troubleshooting ✕

Edit Folder or File

A folder in StorageLink represents a folder in cloud storage. A file represents an object in cloud storage.

If editing a folder, you can edit the name, user permissions, and cloud connection. Please note that editing the name of a folder will take time depending on how many files are in the folder since the files will need to be copied in cloud storage.

If editing a file, you can edit the name of the file.

When finished, click **Save**. This will take you back to the File System page.

Folder Permissions

You can assign user permissions to folders within StorageLink. By default, permissions are inherited from the parent folder.

StorageLink supports the following permissions:

- **List:** List the contents of this folder
- **Download:** Download files
- **Upload:** Upload files and folders
- **Delete/Overwrite:** Delete or overwrite files and folders

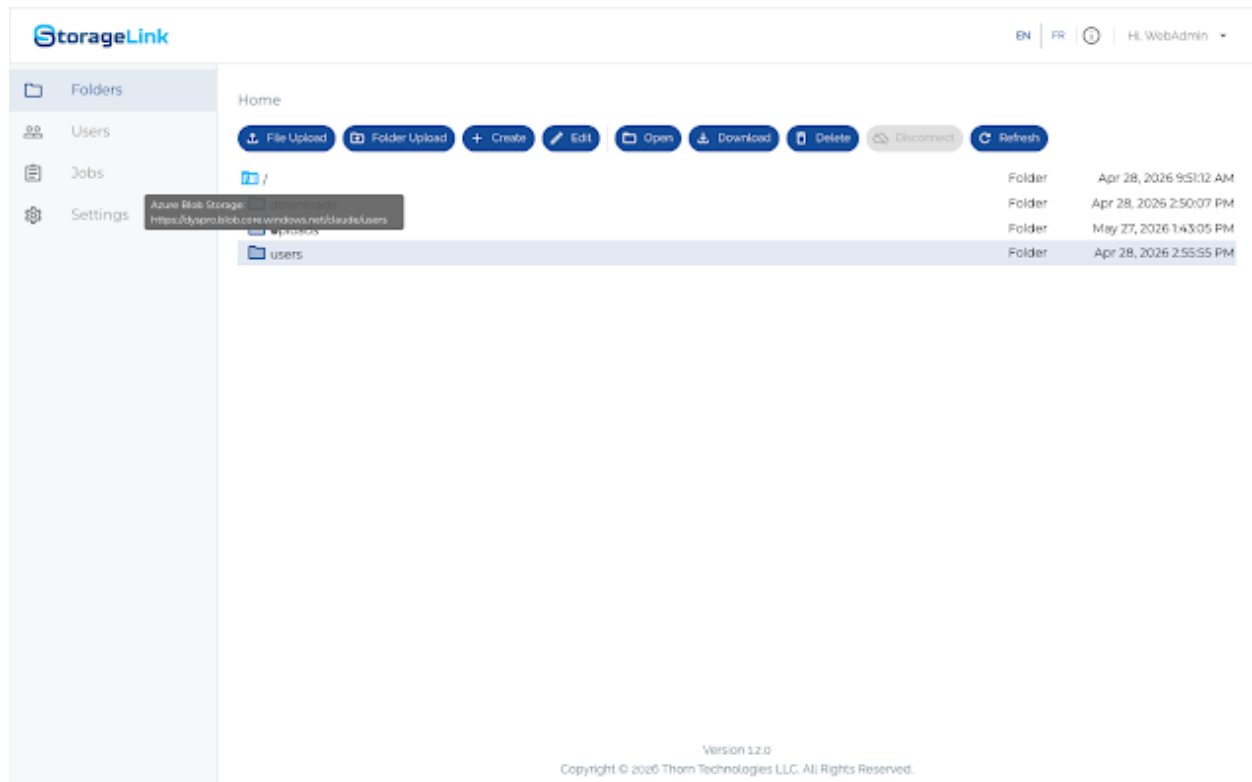
- **Name** (except for the root /, which can't be renamed or deleted)
- **User Permissions** for each user on this folder
- **Cloud Connection** — re-map, inherit, or switch to a saved credential
- **Advanced Options** (per-provider tuning — multipart sizes, region overrides, etc.)

The right-hand panel ("Support + troubleshooting") shows contextual help.

Caution: Deleting a folder that maps to its own Cloud Connection deletes the underlying cloud objects. To remove a StorageLink folder *without* deleting the data, switch its Cloud Connection to **Inherited** first (or use **Disconnect**), then delete.

Drilling In

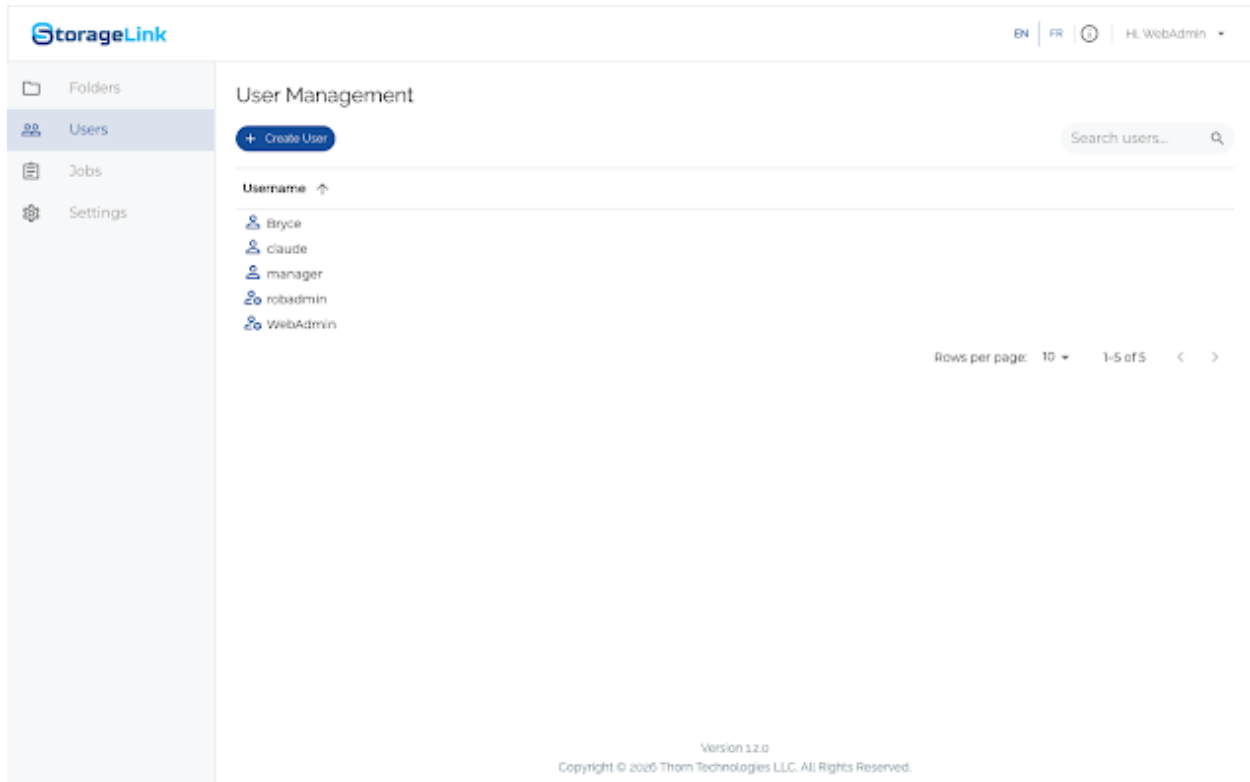
Double-click a folder row (or select it and click **Open**) to navigate into it. Use the breadcrumb to navigate back up:



Managing Users

User Management Page

Click **Users** in the sidebar to reach **User Management**:



The icon next to each username indicates the role:

-  plain person icon — **Web User**
-  person with a cog — **Admin User**

You can search by username, click a row to edit, or click **Create User** to add a new account.

Creating a User

Click **+ Create User** to open the New User form:

StorageLink

EN

FR

Hi, WebAdmin

Folders

Users

Jobs

Settings

Add User

Username

Enter unique username

Role

Web User

Notes

Enter notes about the user (optional)

0/1000

Password

Enter Password

Suggest password

Force User to choose new password at sign in

Home Folder

Users/

BROWSE

The user's access will be restricted to this home directory and its subdirectories.

Home Folder Permissions

List files

Upload

Download

Delete/Overwrite/Rename

Cloud Connection

Inherit from Ancestor Folders

Inherited Cloud Connection From Path

/

Cloud Provider

azure

Resolved Cloud Connection

https://tyspro.blob.core.windows.net/claude/users

SAVE

CANCEL

Support + troubleshooting

Create User

There are two main types of users. A web user is a regular user that can transfer files. An admin user can do the same, but also has the ability to manage users and settings.

In the **Username** field, type in the name of the user. Usernames are case-sensitive, so try to avoid using uppercase letters, as well as symbols.

For the **Password**, type in a complex password that meets the following requirements:

- Mixed case
- Contains a number
- Contains a special character
- Has at least 8 characters

Setting a password is not required and may be omitted if using an Identity Provider.

- if not specifying a password and using an Identity Provider, the user will log in to this user account if the Username matches the configured name attribute for the identity provider.
- if specifying a password and using an Identity Provider, the user will need to use the password upon first login via the Identity Provider.
- if not specifying a password, the

Version 1.2.0

Copyright © 2026 Thom Technologies LLC. All Rights Reserved.

Fields:

Field	Description
Username	Must be unique. Case-sensitive at sign-in.
Role	Web User or Admin User
Notes	Optional free-text
Password	One-Time Password. The user will be required to change it on first sign-in. Must meet complexity requirements (12+ chars, mixed case, digit, special char).

Field	Description
Home Folder	Default is <code>/users</code> (StorageLink will auto-create <code>/users/<username></code>). You can specify a custom path instead.
Home Folder Permissions	Four checkboxes: List files , Upload , Download , Delete/Overwrite/Rename .
Cloud Connection	Default Inherit from Ancestor Folders — the user's home folder uses the parent's cloud connection. Or map it to its own connection.

The form shows the resolved cloud connection path so you can confirm where the user's files will land.

Default home folder isolates users. With the `/users/<username>` default, each user lands in their own sibling directory under `/users/`. Each user is chrooted to their home folder — even if Alice knew the path to Bob's folder, she couldn't navigate up out of `/users/alice/`.

Editing a User

Click the user row in the User Management list to open the Edit User form (same fields as Create User). The form includes a **DELETE** button at the bottom to remove the user:

StorageLink

EN

FR

Hi, WebAdmin

Folders

Users

Jobs

Settings

Edit User

Username

claude

Role

Web User

Notes

Enter notes about the user (optional)

0/1000

Password

Password is set

Suggest password

Force User to choose new password at sign in

Home Folder

/users/claude

BROWSE

The user's access will be restricted to this home directory and its subdirectories.

Home Folder Permissions

List files

Upload

Download

Delete/Overwrite/Rename

Cloud Connection

Inherit from Ancestor Folders

Inherited Cloud Connection From Path

/

Cloud Provider

azure

Resolved Cloud Connection

https://tyspro.blob.core.windows.net/claude/users/claude

SAVE

CANCEL

DELETE

Support + troubleshooting

Edit User

There are two main types of users. A web user is a regular user that can transfer files. An admin user can do the same, but also has the ability to manage users and settings.

In the **Username** field, type in the name of the user. Usernames are case-sensitive, so try to avoid using uppercase letters, as well as symbols.

For the **Password**, type in a complex password that meets the following requirements:

- Mixed case
- Contains a number
- Contains a special character
- Has at least 8 characters

Setting a password is not required and may be omitted if using an Identity Provider.

- if not specifying a password and using an Identity Provider, the user will log in to this user account if the Username matches the configured name attribute for the identity provider.
- if specifying a password and using an Identity Provider, the user will need to use the password upon first login via the Identity Provider.
- if not specifying a password, the

Version 1.2.0

Copyright © 2026 Thom Technologies LLC. All Rights Reserved.

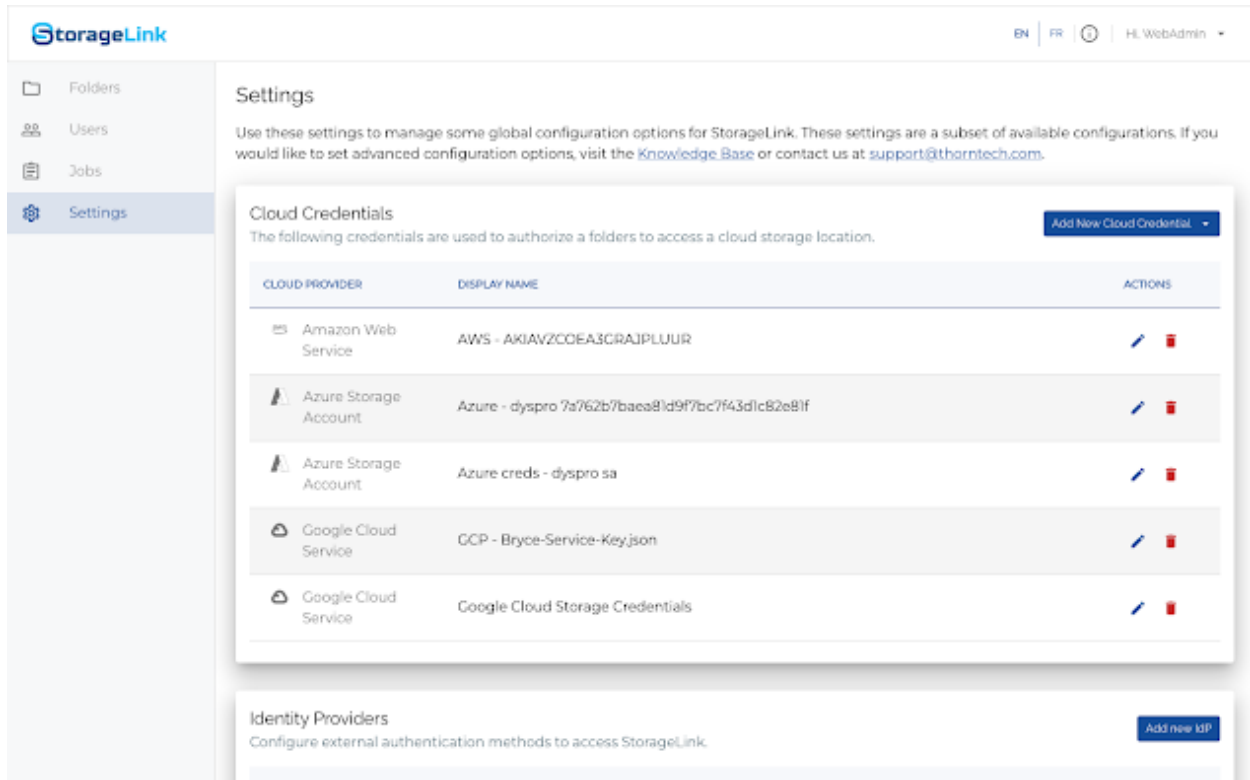
Deleting a Web User removes the StorageLink account. The folders the user had access to remain, and the files in cloud storage are not touched. To delete the user's data, do it from the cloud-storage console.

First Sign-In for a New User

When a user signs in for the first time with the One-Time Password you set, they're sent to an Update Password page where they must set their own password. The Web User Guide walks through this — share that guide with new users.

Settings: Cloud Credentials

The **Settings** page is a single long scrolling page with multiple sections:



The **Cloud Credentials** section lists all the saved cloud-storage credentials available to map folders to. Each row shows:

- **Cloud Provider** icon (AWS, Azure Storage, Azure File Share, GCS)
- **Display Name** — friendly name you assign
- **Actions** — edit and delete

Click **+ Add New Cloud Credential** to add another. A dropdown lets you pick the provider:

- **Amazon Web Service** (S3)
- **Azure Storage Account** (Blob)
- **Google Cloud Service** (GCS)

(Azure File Share is configured via the Azure Storage Account flow with the appropriate share name.)

The per-provider form asks for the fields appropriate to that cloud:

Amazon S3

Field	Description
Connection Name	Friendly name
S3 URL	s3://bucket or s3://bucket/prefix/
Region	Optional; uses server's region if blank. Populate for cross-region setups.
S3 Encryption	SSE-S3, KMS, or No Encryption
Credentials	Use instance profile credentials (recommended on AWS) or Use unique credentials

Azure Blob Storage

Field	Description
Connection Name	Friendly name
Storage Account Name	e.g., mystorageaccount
Container Name	Lowercase. Optionally append a path: container/prefix/.
HNS Enabled	Check if the storage account has Hierarchical Namespace (Data Lake Gen2) enabled.
Credentials	Managed Identity (uses VM's identity) or Connection String (from Azure Portal)

Google Cloud Storage

Field	Description
Connection Name	Friendly name
GCS URL / Bucket Name	The GCS bucket, optionally with a path
Credentials	Attached Service Account (simplest on GCP) or Service Account JSON Key File

The service account needs `storage.objects.create`, `delete`, `get`, `list`. The **Storage Object Admin** role grants all four.

Testing the Connection

Every Add/Edit form has a **Test Connection** button. A passing test returns three green checkmarks. Failed tests are usually:

- Typo in the bucket / container name
- Missing IAM / RBAC permission on the cloud side
- Wrong region (for S3 cross-region setups)
- HNS-enabled / HNS-disabled mismatch on Azure

For S3 with SSE-KMS, the test also verifies that the KMS key is accessible and that the credentials have `kms:GenerateDataKey` and `kms:Decrypt`. (*KMS-aware testing added in v1.2.0.*)

Settings: Identity Providers (OIDC)

OIDC connections let you delegate sign-in to an external identity provider (Entra ID / Azure AD, Google, Okta, Ping, AWS Cognito, or any standards-compliant OIDC IdP). MFA, password complexity, and account lifecycle are then managed at the IdP.

The Identity Providers section of the Settings page lists configured providers and has an **+ Add New IdP** button:

The screenshot shows the StorageLink web interface. The top navigation bar includes the StorageLink logo, language options (EN, FR), a user icon, and the text 'Hi, WebAdmin'. The left sidebar contains links for Folders, Users, Jobs, and Settings (which is highlighted). The main content area is titled 'Settings' and includes a descriptive paragraph. Below this, there are two main sections: 'Cloud Credentials' and 'Identity Providers'. The 'Cloud Credentials' section has a table with columns for Cloud Provider, Display Name, and Actions. It lists five credentials: Amazon Web Service, two Azure Storage Accounts, and two Google Cloud Services. Each entry has edit and delete icons. The 'Identity Providers' section is partially visible at the bottom.

CLOUD PROVIDER	DISPLAY NAME	ACTIONS
Amazon Web Service	AWS - AKIAVZCOEASCRAPLUUR	[Edit] [Delete]
Azure Storage Account	Azure - dyspro 7a762b7baea81d9f7bc7f43d1c82e81f	[Edit] [Delete]
Azure Storage Account	Azure creds - dyspro sa	[Edit] [Delete]
Google Cloud Service	GCP - Bryce-Service-Key.json	[Edit] [Delete]
Google Cloud Service	Google Cloud Storage Credentials	[Edit] [Delete]

Clicking **Add New IdP** opens a full-page form:

StorageLink

EN | FR | ⓘ | Hi, WebAdmin ▾

Folders

Users

Jobs

Settings

Add Identity Provider

☒ Allow login for users that do not yet exist in StorageLink?

Identity Provider Display Name

Enter unique name

Name used to identify this identity provider

Default User Role

Web User

Role given to new users created from this identity provider

Notes

Enter notes (optional)

Notes about this identity provider

0/1000

Issuer URI

Enter issuer URI

Enter issuer URI

Client ID

Enter client id

Enter the client ID from the IdP

Client Secret

Enter client secret

Enter the client secret from the IdP

Username Attribute

Enter username attribute

Set the attribute name used to access the user's name from the user info response. This attribute is used to match an existing user or to create a new user.

Registration Id

Enter registration id

Set registration id

Scopes

openid

Set a list of extra OpenID Connect scopes separated by comma or space. The 'openid' scope is always included.

Prompt

Controls the OIDC prompt parameter sent during login. Determines whether the identity provider shows an account picker, forces re-authentication, etc.

SAVE

CANCEL

Fields for Identity Provider

Provide these fields when appropriate during configuration of OIDC on the identity provider.

Authorized JavaScript Origin

https://104.41.135.141 ⓘ

Authorized Redirect URI / Callback URL

Provide registration id to view Redirect URI ⓘ

Front-channel Logout URI / Sign out URL

https://104.41.135.141 ⓘ

Version 12.0

Copyright © 2026 Thom Technologies LLC. All Rights Reserved.

Required fields:

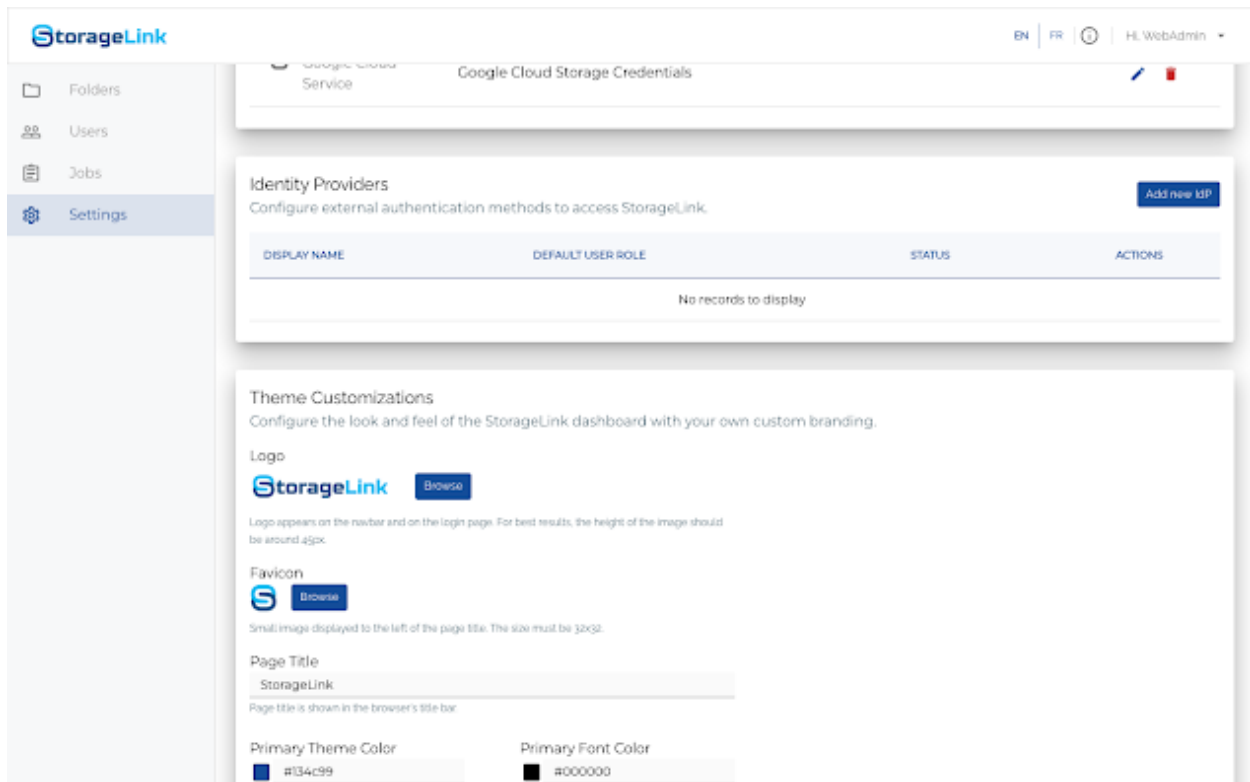
Field	Description
Allow login for users that do not yet exist?	If checked (default), OIDC sign-in auto-provisions a new StorageLink user. Uncheck to require pre-provisioning.
Identity Provider Display Name	Shown on the sign-in page button
Default User Role	Web User or Admin User
Notes	Optional
Issuer URI	Discovery URL from your IdP
Client ID	From your IdP
Client Secret	From your IdP
Username Attribute	Attribute on the IdP user-info response to use as the StorageLink username
Registration Id	Unique ID for this provider in StorageLink
Scopes	Defaults to openid . Add more if your IdP requires them.
Prompt (v1.2.0)	Controls the OIDC prompt parameter (e.g., force re-auth, force account picker). A recommended value is suggested for known providers like Google and Microsoft.

The form's footer shows the **Authorized JavaScript Origin** and **Front-channel Logout URI** values you'll need to paste into your IdP configuration — copy them with the icon next to each.

Credential error alerts (v1.2.0): When SSO credentials expire or become invalid, the Identity Providers list shows an error indicator. Users see a clear error message instead of a generic login failure.

Settings: Theme Customizations

The Theme Customizations section lets you replace the default StorageLink branding:



- **Logo** — upload an image (PNG/SVG) to replace the StorageLink word-mark in the top-left
- **Favicon** — upload an image for the browser tab icon
- **Page Title** — replaces "StorageLink" in the browser title bar
- **Primary Theme Color / Primary Font Color** — main colors (buttons, links)
- **Secondary Theme Color / Secondary Font Color** — accents

Click **SAVE** to apply. **RESET TO DEFAULT** restores the StorageLink branding.

Settings: Language

The screenshot displays the 'Settings: Language' page in the StorageLink admin portal. The page is divided into three main sections:

- Page Title:** A text input field containing 'StorageLink'. A note below states 'Page title is shown in the browser's title bar'.
- Theme and Font Color Settings:** Four color pickers are arranged in a 2x2 grid:
 - Primary Theme Color: #134c99
 - Primary Font Color: #000000
 - Secondary Theme Color: #27b2fa
 - Secondary Font Color: #546e7aButtons for 'SAVE', 'CANCEL', and 'RESET TO DEFAULT' are located at the bottom of this section.
- Language Settings:** A section titled 'Language Settings' with the subtitle 'Configure the available languages and the default language for StorageLink'. It includes:
 - Available Languages:** Two checkboxes, 'English' and 'French (Français)', both of which are checked.
 - Default Language:** A dropdown menu currently set to 'English'.
 - A 'SAVE' button at the bottom.
- Backup & Recovery:** A section at the bottom with the title 'Backup & Recovery' and the subtitle 'Import and export YAML artifact files for backup and recovery.'.

StorageLink ships with **English** and **French** localizations throughout the admin portal, the Web User file browser, and contextual help. Administrators can:

- **Available Languages** — check which languages are offered to users
- **Default Language** — the language a user sees if their browser/locale doesn't match a configured option

If only one language is checked, the EN/FR selector is hidden in the UI. Users can switch language manually at any time when more than one is available.

Settings: Backup & Recovery

The screenshot displays the StorageLink web interface. On the left is a sidebar with navigation links: Folders, Users, Jobs, and Settings (which is highlighted). The main content area is divided into three sections. The top section, titled 'Page Title', shows 'StorageLink' as the current title and includes input fields for 'Primary Theme Color' (#134c99), 'Secondary Theme Color' (#27b2fa), 'Primary Font Color' (#000000), and 'Secondary Font Color' (#546e7a), with 'SAVE', 'CANCEL', and 'RESET TO DEFAULT' buttons. The middle section, 'Language Settings', allows configuring available languages (English and French (Français) are both checked) and setting the default language to English. The bottom section, 'Backup & Recovery', is partially visible and mentions importing and exporting YAML artifact files.

This section exports and imports StorageLink **configuration** — users, folders, admin users, and cloud connections — as a YAML file. **It does not include the files themselves**; those live in cloud storage.

Export

Click **Export Backup File** to download a YAML file. Store it securely — it contains your configuration (and references to credentials, though not the secret values themselves). Many admins schedule regular exports for disaster recovery.

Import

Drag-and-drop or browse to your YAML file. Status messages indicate what was imported, with four categories:

Category	Meaning
Error	Property failed to import — check the message for the line and cause
Warning	Imported but with caveats

Category	Meaning
Skipped	Property already exists on the target server; left as-is
Success	Imported cleanly

Import does not overwrite existing items. If a user already exists, their settings in the backup are skipped even if they differ. Import is intended for fresh instances (migrations, disaster recovery, cloning to staging) — not ongoing sync between two live instances.

Transfer Jobs

Transfer Jobs were introduced in v1.2.0.

A Transfer Job is a copy, move, or rename operation that runs in the background. Users and admins can submit jobs and walk away; failed operations are retried automatically.

The Jobs Page

Click **Jobs** in the sidebar to see your jobs:

[EN](#)
[FR](#)
[🔔](#)
[Hi, WebAdmin](#)

📁

Folders

👤

Users

📋

Jobs

⚙️

Settings

My Jobs

+ Create Job

ID	Operation	Source	Destination	Status	Progress	Started	Completed	Created ↕
13	Move	/Azure Files	/downloads&3/uploads/Test Directory	Completed	100%	4/28/2026, 2:50:56 PM	4/28/2026, 2:50:59 PM	4/28/2026, 2:50:30 PM
1	Copy	/Azure Files	/downloads	Completed	100%	4/28/2026, 2:48:51 PM	4/28/2026, 2:48:54 PM	4/28/2026, 2:48:22 PM

Rows per page: 10 ▾

1-2 of 2

< >

Version 12.0

Copyright © 2026 Thorn Technologies LLC. All Rights Reserved.

The page title is **My Jobs**. Columns: ID, Operation (Copy / Move / Rename), Source, Destination, Status (Pending / Running / Completed / Failed / Canceled), Progress, Started, Completed, Created.

The **+ Create Job** button at the top lets you submit a new transfer job manually (most jobs are created implicitly when a user copies/moves/renames in the file browser).

Job Lifecycle

- **PENDING:** Queued, waiting for a worker thread.
- **RUNNING:** In flight. Status shows transfer rate and bytes transferred.
- **COMPLETED:** Finished successfully. Records are retained for one year by default.
- **FAILED:** Exhausted retries. Look at per-file errors to diagnose.
- **CANCELED:** A user or admin canceled the job mid-flight.

Failed operations retry up to **three times** by default (`features.transfer-jobs.max-retry-count`).

Tuning

Configured via application properties (see next section):

Property	Default	Purpose
<code>features.transfer-jobs.worker-thread-count</code>	10	Concurrent worker threads (restart required)
<code>features.transfer-jobs.completed-job-retention-days</code>	365	How long completed job records are kept
<code>features.transfer-jobs.max-retry-count</code>	3	Retries before marking failed
<code>features.transfer-jobs.cleanup-interval-hours</code>	6	How often the cleanup job runs

Application Properties

Application properties configure settings that aren't exposed in the Web Admin Interface. They control password policy, API rate limiting, transfer-job tuning, and tracking metadata.

Configuration File Location

`[?]/opt/swiftgw/application.properties`



After editing, restart the StorageLink service:

`sudo systemctl restart swiftgateway`

Password Policy

The default policy is **stricter than 8 characters** — the deployed minimum is **12 characters** and the system enforces a previously-used-password block:

`password.policy.require-upper=true`
`password.policy.require-lower=true`
`password.policy.require-digit=true`
`password.policy.require-special=true`
`password.policy.required-upper-count=1`
`password.policy.required-lower-count=1`
`password.policy.required-digit-count=1`
`password.policy.required-special-count=1`
`password.policy.min-length=12`
`password.policy.prevent-previously-used-password-count=5`
`password.policy.word-file=classpath:100k-most-used-passwords-NCSC.txt`



The Update Password form shows live validation against these rules — green checkmarks for satisfied rules, red X for failed rules, with a strength meter.

Token Lifetime

`features.api.access-token-time-to-live-seconds=28800` # 8 hours

API Rate Limiting (v1.2.0)

`features.api.api-rate-limit-per-second=200` # per authenticated user



Exceeding returns HTTP 429 with a **Retry-After** header. Set to 0 to disable. Unauthenticated requests are not rate-limited.

Tracking Metadata (v1.2.0)

Write tracking information to cloud-object metadata so uploads can be traced back to the user and session:

`features.file-system.metadata.enable-correlation-id=false`
`features.file-system.metadata.enable-username=false`
`features.file-system.metadata.enable-remote-address=false`

CORS Origin (v1.2.0)

`features.api.cors-allowed-origin-pattern=*` # default; restrict in production

❓ Disabling Admin Access

For a public-facing instance with no admin interface:

❓ `features.api.admin-enabled=false`

❓ Preserving Upload Timestamps

❓ `features.api.preserve-file-timestamp-on-upload-enabled=true`

❓

API Reference

StorageLink exposes a REST API for programmatic uploads and configuration management.

Why Use the API

- **Automation** — provision users when new partners are onboarded, upload files on a schedule
- **Bulk operations** — migrate hundreds of users without manual entry
- **Scheduled backups** — automate YAML exports
- **Integration** — connect StorageLink to ticketing or workflow systems

Authentication

OAuth 2.0 with client credentials + password grant. You need four values:

1. `security.client-id`
2. `security.client-secret`
3. Web Admin username
4. Web Admin password

Client ID and secret are in `/opt/swiftgw/application.properties` on the server:

❓ `grep security.client /opt/swiftgw/application.properties`

❓ Obtaining a Bearer Token

POST `https://<host>/backend/login`

Use **Basic Auth** with the client ID and secret. Send `x-www-form-urlencoded` body with `grant_type=password`, `username`, and `password`.

The response includes an `access_token` to use as a Bearer token in subsequent requests. Default lifetime is 8 hours.

Uploading a File

POST <https://<host>/backend/1.0.0/filesystem/<path>>

Body: **form-data** with key **data** (type **File**). Successful response: **204 No Content**. The path after **/filesystem/** is the virtual path in StorageLink.

Listing and Downloading

Same [/backend/1.0.0/filesystem/](#) prefix. List responses are paginated.

Logout

POST [/backend/1.0.0/logout](#) revokes the current token.

API Documentation

Full OpenAPI (Swagger) spec:

<https://thorn-tech-public-documents.s3.amazonaws.com/storagelink/KB/storagelink-api-documentation-swagger.json>

Paste into <https://editor.swagger.io/> for a browseable view. The knowledge base has Python and bash example scripts.

Network

API calls hit port 443. Ensure your client machine is allowed through the security group / firewall rule.

High Availability Deployment

A single StorageLink instance is a single point of failure. For workloads that require 24/7 availability or have SLAs tied to file delivery, deploy in HA mode.

Architecture

[Web Browser](#) → Load Balancer → Auto-scaling group (N StorageLink instances)



PostgreSQL (RDS / Azure DB / Cloud SQL)



Cloud Storage (shared)

[?](#)

Because StorageLink keeps state in PostgreSQL and uploaded files in cloud storage, there is no local state to synchronize. Any instance can serve any user.

Component	Single Instance	HA
User accounts & config	Embedded Postgres	External Postgres (RDS / Azure DB / Cloud SQL)
Uploaded files	Cloud storage	Cloud storage
Audit & application logs	Local disk	Local disk (centralize via cloud logging)

Load Balancer

- **AWS:** Network Load Balancer (NLB) from the CloudFormation template. Add an ALB in front for SSL termination and Cloud Armor / WAF integration if desired.
- **Azure:** Standard Load Balancer with TCP rules, or Application Gateway for SSL termination.
- **GCP:** TCP/UDP Network Load Balancer, or Application Load Balancer with Cloud Armor.

Forward port 443 (and 80 for HTTP→HTTPS redirect) to the instances.

Health Checks

- **Protocol:** HTTPS
- **Port:** 443
- **Path:** `/backend/actuator/health`
- **Interval:** 30 seconds
- **Threshold:** 2–3 failures before marking unhealthy

AWS HA Deployment

Subscribe to StorageLink on the AWS Marketplace and use one of:

- **StorageLink (High Availability — New Network)** — provisions VPC, subnets, NLB, RDS, ASG
- **StorageLink (High Availability — Existing Network)** — deploys into your existing VPC/subnets

Key stack parameters: Bucket Access (`restricted` vs `open`), EC2 Type, Disk Volume Size, Key Pair, Desired Capacity, VPC IP Range, Web/SSH Input CIDRs, Web Admin Username/Password, DB Class.

Azure / GCP HA

Use the ARM, Terraform, or Deployment Manager reference templates from the knowledge base. Both Azure and GCP provision a Standard Load Balancer, a managed PostgreSQL, and a VM Scale Set / managed instance group running StorageLink.

Custom Deployments

For environments where you can't provision some of the underlying resources, the `launch_config` mechanism lets you plug into an existing database:

```
[?] ARCHITECTURE=HA
CLOUD_PROVIDER=aws # or azure, gcp
DB_HOST=<database-hostname>
[?]
```

Drop these into `/opt/swiftgw/launch_config.env` on each instance. The `ARCHITECTURE=HA` flag tells StorageLink to use the external database instead of the embedded Postgres.

For premier support on custom templates, contact support@thorntech.com.

Server Administration

This section covers tasks that require SSH access to the StorageLink VM.

SSH Access

Port	Purpose	Users
22	SSH admin	Administrators
80	HTTP (redirects to 443)	Web Users
443	HTTPS (Web Admin + Web User)	Everyone

Connect with the key pair specified at deployment:

```
[?] ssh -i /path/to/key.pem ec2-user@<server-ip> # AWS Amazon Linux
ssh -i /path/to/key.pem azureuser@<server-ip> # Azure Ubuntu
ssh -i /path/to/key.pem <user>@<server-ip> # GCP Ubuntu
```

[?] Service Management

StorageLink runs as a systemd service named `swiftgateway`:

```
[?] sudo systemctl status swiftgateway
sudo systemctl restart swiftgateway
sudo journalctl -u swiftgateway -f
```

Memory Settings

JVM heap is sized at boot from VM RAM. If you resize the VM, update `-Xmx` in `/opt/swiftgw/swiftgateway-*.conf` manually:

VM RAM	Recommended <code>-Xmx</code>
32 GB	22014m
16 GB	9937m
8 GB	3900m
4 GB	1903m
2 GB	1024m

Restart the service to apply.

Log Files

File	Purpose
<code>/opt/swiftgw/log/application-*.log</code>	Java application events and errors
<code>/opt/swiftgw/log/audit-*.log</code>	Sign-in, upload, download, delete
<code>/var/log/swiftgw/cloudinit.log</code>	First-launch / bootstrap issues

Retention is **30 days or 3 GB**, whichever comes first. In HA, centralize via CloudWatch / Log Analytics / Cloud Logging.

SSL Certificates

To install a paid certificate (e.g., GoDaddy):

1. Copy your key + bundled cert to `/etc/nginx/ssl/`.
2. Edit the nginx config (`/etc/nginx/conf.d/website.conf` on AWS, `/etc/nginx/sites-available/website.conf` on Azure/GCP).
3. Point `ssl_certificate` and `ssl_certificate_key` at your files; set `server_name` to your domain.
4. `nginx -t && service nginx restart`.

For free certificates with auto-renewal, use **Let's Encrypt with DNS validation** — see the Let's Encrypt article in the knowledge base.

Web Admin Password Reset

If you forget the Web Admin password and have no other admin to fall back on, run the password-reset script via SSH. The script is published at <https://thorntech-products.s3.amazonaws.com/storagelink/create-admin-user-script/New-Admin-Storagelink.sh>. Download, chmod, and run with a new username and password.

Upgrade Process

Recommended path is **export-and-import**, not in-place:

1. On the old instance: Settings → Backup & Recovery → Export Backup File
2. Deploy a new StorageLink instance from the marketplace
3. On the new instance: Settings → Backup & Recovery → Import and upload the YAML

The new instance picks up all users, folders, admin users, and cloud connections. Verify the import counts (Success / Skipped / Warning / Error), then point clients at the new instance.

Security Best Practices

- **Restrict SSH (port 22) to admin IPs.** Never leave 22 open to 0.0.0.0/0 in production.
- **Restrict the Web Admin Interface where possible.** If your Web Users are a known IP range, lock down 80/443 to them. If not, accept that 80/443 must be public and lean on strong passwords + OIDC + MFA.
- **Use OIDC + MFA for admins.** Configure MFA at the IdP — it applies automatically at StorageLink sign-in.
- **Use instance profile / managed identity credentials.** Avoid embedding static access keys in Cloud Connections. Instance-level credentials rotate automatically.
- **Principle of least privilege.** Don't give the StorageLink instance broad cloud permissions. Scope it to the buckets it actually serves.
- **Monitor audit logs.** Stream `/opt/swiftgw/log/audit-*.log` to a central log system. Watch for repeated sign-in failures, off-hours uploads, and unexpected IPs.
- **Enable tracking metadata (v1.2.0).** Turn on `enable-correlation-id`, `enable-username`, and `enable-remote-address` so each uploaded object carries a breadcrumb back to user and session.
- **Set a CORS allowed origin (v1.2.0).** If you've built a custom front-end, scope `features.api.cors-allowed-origin-pattern` to that origin instead of `*`.
- **Configure API rate limiting (v1.2.0).** The 200 req/s default is generous — lower it if you know your workload.
- **Back up configuration regularly.** Schedule YAML exports.
- **Stay current.** Apply OS patches and StorageLink upgrades promptly. Release notes call out security fixes explicitly.

- **Replace the self-signed certificate.** Install a real SSL cert (or terminate at a load balancer with a managed cert). This removes the browser warning and avoids training users to click through certificate warnings.

Behind a Proxy or WAF

If StorageLink sits behind a load balancer, reverse proxy, or WAF, configure the upstream to pass through **X-Forwarded-For** so audit logs and tracking metadata capture the real client IP (v1.1.1+).

Troubleshooting

Can't Reach the Web Interface

- Confirm the instance is running (cloud console).
- Confirm the security group / NSG / firewall allows your IP on port 443.
- Confirm DNS resolves (if using a domain).
- Try `curl -k https://<host>/` from a known-allowlisted network. HTML response = app is up.

Test Connection Fails

- **Bucket / container name typo.** Spelling and case matter.
- **Missing IAM / RBAC.** The service principal needs read, write, list, delete. For S3+KMS, also `kms:GenerateDataKey` and `kms:Decrypt`.
- **Wrong region.** Populate the Region field for S3 cross-region.
- **HNS mismatch on Azure.** The HNS Enabled checkbox must match the storage account.

Files Aren't Showing Up in Cloud Storage

- Check the folder's **Resolved Cloud Connection** in the Edit dialog — that's the actual path files land in.
- Folders created in StorageLink only materialize in cloud storage after a Web User signs in and accesses them.

Sign-In Issues

- **Web Users:** confirm the user is enabled; username and password are case-sensitive.
- **Admin Users:** if no admin can sign in, use the SSH-based password reset script.
- **OIDC:** check the Identity Providers list for credential-error indicators (v1.2.0+). Expired client secrets are the most common cause.

Slow Uploads

- Bandwidth is bottlenecked by the slowest link between client and cloud storage. Test from the StorageLink VM itself (`curl / aws s3 cp`) to isolate.
- For high concurrency, increase `features.transfer-jobs.worker-thread-count` and the cloud-concurrency settings.
- For very large files, check multipart settings.

Out-of-Memory Errors

Application logs show `OutOfMemoryError` → heap too small for workload. Raise `-Xmx` in `/opt/swiftgw/swiftgateway-*.conf` and restart. See [Memory Settings](#).

Frequently Asked Questions

Q: What cloud storage providers does StorageLink support? A: Amazon S3, Azure Blob Storage, Azure File Share, Google Cloud Storage.

Q: Do Web Users need any software installed? A: No. Any modern browser works.

Q: Are files stored on the StorageLink server? A: No. Files are written directly to cloud storage. The instance only needs disk for OS, app, and rotated logs.

Q: How do I check what version of StorageLink I'm running? A: The footer of the Web Admin Interface shows the version (e.g., **Version 1.2.0**).

Q: When do folders show up in cloud storage? A: When a Web User first signs in and accesses them — not when you create them in the admin UI.

Q: Can I mix cloud providers? A: Yes. You can have folders within one StorageLink instance that point to S3, Azure Blob, and GCS simultaneously. Users can drag-and-drop files between them.

Q: How do I reset a Web User's password? A: Edit the user in the User Management page and set a new One-Time Password. The user will be required to change it on first sign-in.

Q: How do I reset a Web Admin's password? A: From the Web Admin Interface (if another admin can still sign in), edit the admin user. Otherwise use the SSH-based password reset script.

Q: Can I restrict a user to specific IP addresses? A: Not per-user in the current version — IP restriction happens at the security group / firewall level. Use OIDC + MFA for per-user protection.

Q: Can I share a folder between multiple users? A: Yes. Either (1) set multiple users' home folder to the same path, or (2) give each user their own home folder and add a sub-folder in each that maps to a shared Cloud Credential. The second pattern is generally cleaner.

Q: How is StorageLink priced? A: Software charge per hour (confirm the current rate on the marketplace listing) plus a 30-day free trial. Cloud infrastructure (EC2/VM, storage, data transfer) is billed by your cloud provider separately.

Q: What VM size should I use? A: For testing, **t3.medium** (AWS), **B1ms** (Azure), or **e2-medium** (GCP). For production, step up to **m5.large** / D-series / **n2-standard-2** or larger. **Do not** use **e2-small** on GCP — CPU is inadequate.

Getting Help

- **Knowledge base:** help.thorntech.com
- **Support:** support@thorntech.com
- **API documentation:** [OpenAPI / Swagger JSON](#) — paste into <https://editor.swagger.io/> for a browseable view

StorageLink is developed by Thorn Technologies. For the latest documentation, visit help.thorntech.com.