

SFTP Transfer

Quick Start Guide

StableLogic SFTP Transfer is a business-grade SFTP gateway that runs entirely within your AWS account. Files transferred by your users land directly in your Amazon S3 bucket — no third-party storage, no data leaving your control. This guide walks you through launching the product from AWS Marketplace, configuring your Security Group, connecting your S3 bucket, creating SFTP users, and verifying your first connection.

i Prerequisites

AWS Account

Permissions to launch EC2 instances, create IAM roles, and access S3.

VPC & Subnet

A subnet where the instance will be launched.

Amazon S3 Bucket

The bucket that will store all SFTP-transferred files.

EC2 Key Pair

Required for first-time admin setup (generating the initial password over SSH on port 2222) and for ongoing instance management.

IAM ROLE — create before launching

- Create a role for the EC2 instance with: `s3:GetObject` , `s3:PutObject` , `s3:DeleteObject` , `s3:ListBucket` , `s3:AbortMultipartUpload` .
- If using a customer-managed KMS key: also add `kms:GenerateDataKey` and `kms:Decrypt` .

1 Subscribe and Launch

1. On the AWS Marketplace listing, click **Continue to Subscribe** and accept the terms.
2. Click **Continue to Configuration**, select your region, then **Continue to Launch**.
3. Choose **Launch from EC2** and select your instance type from the table below.
4. Select your VPC and subnet, attach the IAM role you created, and select your EC2 Key Pair.
5. Click **Launch**. The instance configures itself automatically — no further action needed.

Instance Sizing

Instance	Use Case	Concurrent Connections
t3.small	Development / Testing	Up to 10
t3.medium	Small Production (Recommended)	Up to 25
t3.large	Medium Production	Up to 50
c5.xlarge	High Volume	50–100+

2 Configure the Security Group

Add these inbound rules to the instance's Security Group:

Protocol	Port	Source	Purpose
TCP	22	SFTP client IP ranges	SFTP file transfers
TCP	2222	Your office / VPN IP only	SSH instance management
TCP	5173	Your office / VPN IP only	Admin portal

SECURITY NOTE

- Never open port 5173 or port 2222 to `0.0.0.0/0` — these are management ports and must be restricted to your office or VPN IP.
- For port 22, restrict to known IP ranges where possible; where clients have dynamic or varied IPs, use per-user IP allowlisting in the admin portal as an additional layer of control.

3 Access the Admin Portal

Once all EC2 status checks pass (allow 2–3 minutes from launch), generate your one-time administrator password. **Each instance generates its own unique password — there is no shared default, and no credentials are baked into the AMI.**

Generate the one-time admin password

1. SSH to the instance on **port 2222** using your EC2 Key Pair:

```
ssh -p 2222 ubuntu@<EC2-Public-IP>
```

2. Run the bootstrap command:

```
sudo stablelogic-sftp-bootstrap
```

3. The command prints a strong, randomly generated password **once**. Copy it now — it is not stored and will not be shown again.

Log in to the admin portal

URL	http://<EC2-Public-IP>:5173
Username	admin
Password	the one-time password generated above

SET A PERMANENT PASSWORD AFTER FIRST LOGIN

- After logging in, go to **Admin** → **Web Users**, open your account, and set a strong, unique password.
- Enable multi-factor authentication under **My Account** → **MFA** before granting access to anyone else.
- Lost the password before logging in? Re-run `sudo stablelogic-sftp-bootstrap --force` to generate a new one.

BUILT-IN SFTP admin ACCOUNT

The same one-time password is also applied to a built-in SFTP user named `admin`, created for initial verification. If you do not intend to use it, disable its password login or delete it from **Users** — the SFTP users you create in Section 5 are independent of it.

4 Connect Your S3 Bucket

1. In the admin portal, click **Cloud Connections** in the sidebar.
2. Enter your S3 bucket name and AWS region.
3. Select your encryption type:
 - **SSE-S3** — S3-managed encryption (default, no extra cost).

- **SSE-KMS** — your own KMS key. Enter the KMS Key ID that appears below the dropdown. The IAM role attached to the instance must have `kms:GenerateDataKey` and `kms:Decrypt` permissions on that key.

4. Click **Save**.

5 Create Your First SFTP User

1. Go to **Users** → **Add User**.
2. Set a username and either a password or an SSH public key.
3. Set a **Home Folder** — this maps the user to an S3 prefix (e.g. `uploads/client-a/`).
4. Assign read and/or write permissions as required.
5. Optionally set an IP whitelist to restrict which client IPs can connect as this user.
6. Click **Save**.

6 Test Your Connection

Connect using any SFTP client (FileZilla, WinSCP, Cyberduck, or the `sftp` command):

Host	<EC2-Public-IP>
Port	22
Username	<the user you created>
Auth	Password or SSH key

Upload a test file, verify it appears in your S3 bucket, then confirm the session appears under **SFTP Activity Log** in the admin portal.

YOU ARE LIVE

Your SFTP server is running. Share the hostname and credentials with your SFTP clients to start transferring files.

Security Checklist

- ☐ Initial admin password generated via one-time bootstrap, and a permanent password set after first login
- ☐ Built-in SFTP `admin` account secured — disabled or deleted if not in use
- ☐ MFA enabled on the admin account (My Account → MFA)
- ☐ Admin portal port 5173 restricted to office / VPN IPs only
- ☐ SSH management port 2222 restricted to office / VPN IPs only
- ☐ S3 bucket Block Public Access enabled
- ☐ Port 22 restricted to known SFTP client IP ranges
- ☐ Per-user IP whitelisting configured where possible
- ☐ S3 bucket encryption enabled (SSE-S3 or SSE-KMS)

Troubleshooting

Symptom	What to Check
Admin portal does not load	Instance may still be starting — wait 2–3 minutes. Verify port 5173 is open in the Security Group.
No admin portal password / can't find credentials	There is no default password. Generate one via SSH on port 2222: <code>sudo stablelogic-sftp-bootstrap</code> (see Section 3). If a previously generated one was lost, re-run with <code>--force</code> .
<code>bootstrap</code> reports "no such container"	Services are still starting — wait 2–3 minutes after launch, then run the command again.
SFTP connection refused	Port 22 not open in Security Group, or the user account does not exist.
Files not appearing in S3	IAM role missing S3 permissions, or incorrect bucket name in Cloud Connections.
Login fails with correct password	Account may be locked after repeated failures. Unlock it from the Users page in the admin portal.
SFTP connected but cannot write	User has read-only permissions — edit the user in the admin portal and enable write access.

Support

NEED HELP?

Email: sftpsupport@stablelogic.com

Support hours and SLAs depend on your subscription tier (Standard or Enterprise).