

# Borgmatic Director UI for beginners

## Borgmatic Director UI - Beginner's Guide

Welcome to Borgmatic UI! This guide will help you understand the basics of backing up your data using this powerful yet easy-to-use backup management interface.

### Understanding Key Concepts

Before diving in, it's important to understand the terminology used throughout the application. These terms come from the underlying backup tools (Borg and Borgmatic) and understanding them will make everything much clearer.

#### ?? Repository

**What is it?** A **Repository** is the *destination* where your backups are stored. Think of it as a secure vault or storage container that holds all your backup data.

**Key points:**

- A repository is created once and can hold many backups over time
- Repositories are encrypted by default - you'll set a passphrase when creating one
- You can have multiple repositories (e.g., one local, one remote)
- Repositories can be stored locally (on your server) or remotely (SSH server, cloud storage)

**Important:** Never lose your repository passphrase! Without it, your backup data cannot be recovered.

# ? Backup (Backup Job)

**What is it?** A **Backup** (or Backup Job) is a *configuration* that defines:

- **What** to back up (which files and folders)
- **Where** to store it (which repository)
- **How** to back it up (compression, exclusions, etc.)
- **When** to run (if scheduled)

**Example:** You might create a backup job called "Website Backup" that backs up `/var/www` to your remote repository every night at 2 AM.

---

# ? Archive

**What is it?** An **Archive** is a single *snapshot* of your data at a specific point in time. Every time a backup job runs successfully, it creates a new archive.

**Key points:**

- Archives are stored inside repositories
- Each archive has a unique name (usually including a timestamp)
- Archives are deduplicated - only changed data is stored, saving space
- You can browse, restore, or delete individual archives

**Analogy:** If a Repository is a photo album, then Archives are individual photos. Each photo captures a moment in time, and the album holds them all together.

---

# ? Schedules

Schedules allow you to automate your backups so they run without manual intervention.

## How Schedules Work

- Schedules are attached to backup jobs
- You can set backups to run hourly, daily, weekly, or with custom cron expressions
- Scheduled backups run automatically in the background
- You'll see the status and history of scheduled runs in the dashboard

## Common Schedule Patterns

Pattern	Description	Best For
Daily at 2:00 AM	Runs once per day during low-activity hours	Most use cases
Every 6 hours	Runs 4 times per day	Frequently changing data
Weekly on Sunday	Runs once per week	Large, stable datasets

## ? SSH Keys

SSH Keys are used for secure, passwordless authentication when connecting to remote servers for backup storage.

## Why Use SSH Keys?

- **Security:** More secure than passwords
- **Automation:** Required for scheduled backups to remote servers (no password prompts)
- **Convenience:** No need to enter passwords repeatedly

## How to Set Up SSH Keys

1. Go to **SSH Key Management** in the sidebar
2. Either **Generate** a new key pair or **Import** an existing key
3. Copy the **public key** to your remote server's `~/.ssh/authorized_keys`
4. Test the connection to verify it works

**Tip:** When importing a key, you can select a file from the server or upload from your computer using the buttons in the import dialog.

## ?? Storage Types

When creating a repository, you can choose from several storage types depending on where you want to store your backups.

## Local Repository

**Path format:** `/path/to/repository`

- Stored on the same server or a mounted drive
- Fastest backup and restore speeds
- Best for: Quick backups, staging before cloud sync

## SSH/SFTP Repository

**Path format:** `ssh://user@hostname/path/to/repository`

- Stored on a remote server via SSH
- Requires SSH key or password authentication
- Best for: Off-site backups, dedicated backup servers

## Cloud Storage (with Rclone)

For cloud storage like Amazon S3, Backblaze B2, Google Drive, etc.

### Option 1: Local + Cloud Sync (Recommended)

- Backups are stored locally first
- Automatically synced to cloud after each backup
- Faster backups, cloud redundancy

### Option 2: Native Cloud (Borg 2.x only)

- Borg 2.x can write directly to S3-compatible storage
  - No Rclone required
  - Simplest cloud setup
- 

## ? How to Restore (Retrieve) Backups

Restoring your data is just as important as backing it up. Here's how to retrieve files from your backups.

### Step 1: Navigate to Archives

1. Go to **Archives** in the sidebar
2. Select the repository containing your backup
3. You'll see a list of all archives (snapshots) in that repository

### Step 2: Browse the Archive

1. Click on an archive to open the **Archive Browser**
2. Navigate through folders just like a file explorer
3. Preview text files directly in the browser

## Step 3: Restore Files

You have three options when restoring:

Option	Description	Use Case
<b>Restore to New Location</b>	Extract files to a folder you choose	Safest option - review before replacing
<b>Download</b>	Download files to your computer (folders are zipped)	Quick access, small files
<b>Restore to Original Location</b>	Put files back where they came from	Full restore after data loss

**Caution:** "Restore to Original Location" will overwrite existing files. Use with care!

## ? Quick Start Guide

Ready to create your first backup? Follow these steps:

### 1. Create a Repository

1. Go to **Repositories** → **Create Repository**
2. Choose a storage type (Local is easiest to start)
3. Set a path (e.g., `/host/backups/my-repo`)
4. Enter a strong passphrase and save it somewhere safe!
5. Click **Create**

### 2. Create a Backup Job

1. Go to **Backups** → **Create Backup**
2. Give it a name (e.g., "My Documents")
3. Select your repository
4. Add source paths (what to back up)
5. Optionally set a schedule
6. Click **Create**

## 3. Run Your First Backup

1. Find your backup job in the list
2. Click the **Run** button
3. Watch the progress in the dashboard
4. Once complete, you'll have your first archive!

## 4. Verify Your Backup

1. Go to **Archives**
2. Select your repository
3. Click on the archive to browse its contents
4. Confirm your files are there

---

## ? Tips for Beginners

- **Start small:** Begin with a small folder to test the process
- **Use descriptive names:** Name your backups and repositories clearly
- **Test restores:** Regularly practice restoring files to ensure your backups work
- **Multiple destinations:** Consider both local and remote repositories for redundancy
- **Monitor the dashboard:** Check regularly that scheduled backups are running
- **Keep passphrases safe:** Store repository passphrases in a password manager

---

## ? Glossary

Term	Definition
<b>Borg</b>	The underlying backup program that handles deduplication and encryption
<b>Borgmatic</b>	A wrapper around Borg that simplifies configuration and automation
<b>Deduplication</b>	Only storing unique data chunks, saving significant storage space
<b>Archive</b>	A single backup snapshot at a point in time
<b>Repository</b>	The storage location containing all your archives
<b>Passphrase</b>	The password used to encrypt/decrypt your repository
<b>Rclone</b>	A tool for syncing files to cloud storage providers

Term	Definition
<b>SSH Key</b>	A cryptographic key pair for secure, passwordless server authentication
<b>Retention</b>	Rules for how long to keep old archives before pruning them
<b>Pruning</b>	Removing old archives according to retention rules to save space

**Congratulations!** You now have a solid understanding of Borgmatic UI. Remember: a backup is only as good as its last successful restore test. Happy backing up! ☐☐

Revision #3

Created 17 January 2026 08:02:33 by Admin

Updated 17 January 2026 08:14:14 by Admin