

Introduction Help

Intro Help & Documentation

Learn how to use Borgmatic Director UI to manage your backups

Quick Links

[Overview](#)[Operating Modes](#)[Connecting Client](#)[Repositories](#)[Backup Jobs](#)[Schedules](#)[Restore](#)[Settings](#)

Overview - What is Borgmatic UI?

Borgmatic UI is a web-based interface for managing{' '} [BorgBackup](#){' '} through{' '} [Borgmatic](#). It provides an intuitive interface for configuring backups, managing repositories, scheduling automated backups, and restoring files.

Key Features

- Create and manage backup jobs with an easy-to-use wizard
- Configure repositories (local, SSH, SFTP, S3, Rclone)
- Schedule automated backups with cron-like scheduling
- Browse and restore files from any backup archive
- Multi-node management with Director mode
- Real-time backup monitoring and logging

Operating Modes

Borgmatic UI can operate in two main modes, depending on your needs:

Client / Standalone Mode

Run Borgmatic UI on a single machine to manage its local backups. This is the default mode and is perfect for individual servers or workstations.

Use when:

- You have a single server to back up
- You want a simple, self-contained backup solution
- You don't need centralized management

Note: A standalone instance can later connect to a Director to become a managed client.

Director Mode

A central management server that can monitor and control multiple client instances. The Director doesn't run backups itself – it manages others.

Use when:

- You have multiple servers to back up
- You want centralized monitoring and control
- You need to manage backups across your infrastructure

Features: Client management, templates, deployments, centralized passphrase vault.

Choosing Your Mode

You choose the operating mode during initial setup. The mode can be changed later in **Settings ? Operating Mode**, but this will reset mode-specific configurations.

Connecting a Client to a Director

To connect a Client (or Standalone instance) to a Director for centralized management:

- 1**
On the Director: Get Connection Details
In the Director's **Settings ? Connection Configuration**, find or create a **Connection Token**. Also note the Director's URL (e.g., `https://director.example.com:8000`).
- 2**
On the Client: Configure Connection
Go to **Settings ? Client Configuration**. Enter:
 - **Client Name:** A friendly name for this client (e.g., "Web Server 1")
 - **Director URL:** The full URL including port (use `https://`)
 - **Connection Token:** The token from the Director (leave empty if open access)
- 3**
Save and Connect
Click **Save Configuration**, then **Test Connection** to verify, and finally **Connect** to establish the connection.
- Connected!**
Once connected, the client will appear in the Director's dashboard and can be managed remotely. The connection uses WebSocket over SSL for real-time communication.

Troubleshooting Connection Issues

- **Connection refused:** Ensure the Director is running and the URL is correct (including https://)
- **Invalid token:** Double-check the connection token matches exactly
- **SSL errors:** Director mode automatically uses HTTPS – make sure to use https:// in the URL
- **Firewall:** Ensure port 8000 (default) is open between client and Director

Switching Between Clients (Director Mode)

When logged into a Director, you can switch between viewing the Director's own interface and any connected client's interface.

Using the Client Selector

In the top navigation bar, you'll see a dropdown showing "**Director**" or the currently selected client's name. Click it to:

- Switch to **Director** - View the Director dashboard with all connected clients
- Switch to a **Client** - View that client's backups, schedules, and settings as if you were logged in directly

Director View	
	<ul style="list-style-type: none">• See all connected clients• Manage templates and deployments• Configure the vault for passwords• View aggregated statistics

Client View	
	<ul style="list-style-type: none">• Manage backup jobs• View/restore archives• Configure schedules• Edit repositories

Quick Access from Dashboard

In the Director Dashboard, each connected client has a "View" button. Clicking it switches to that client's view and highlights the dropdown selector so you know where to switch back.

Setting Up Repositories

A **repository** is where your backup data is stored. Before creating backup jobs, you need to set up at least one repository.

Supported Repository Types

Local
Backup to a local directory or mounted drive

SSH/SFTP
Backup to a remote server via SSH

Borg Server
Connect to a dedicated Borg backup server

S3/MinIO

Amazon S3 or compatible object storage

Rclone

Use Rclone for cloud storage (Google Drive, Dropbox, etc.)

Creating a Repository

1. Go to **Repositories** in the sidebar
2. Click **Add Repository**
3. Select the repository type and fill in the details:
 - **Name:** A friendly name for reference
 - **Path/URL:** Where the repository will be stored
 - **Encryption:** Choose encryption mode (repokey-blake2 recommended)
 - **Passphrase:** A strong password to encrypt your backups
4. Click **Create & Initialize** to create the repository

Important: Save Your Passphrase!

The repository passphrase is required to access your backups. If you lose it, your backup data will be **permanently inaccessible**. Store it securely (e.g., in a password manager).

Creating Backup Jobs

A **backup job** defines what to back up and where. Each job specifies source directories, a target repository, and optional exclusions.

Creating a Backup Job

1. Go to **Backup Jobs** in the sidebar
2. Click **Create Backup Job**
3. Fill in the backup configuration:
 - **Job Name:** A descriptive name (e.g., "Daily Website Backup")

- **Source Directories:** Paths to back up (e.g., /var/www, /home)
- **Repository:** Select a configured repository
- **Exclusions:** Patterns to exclude (e.g., *.log, node_modules/)

4. Click **Save** to create the job

Running Backups

	Manual Backup Click the Run Now button on any backup job to start an immediate backup. Progress is shown in real-time.		Scheduled Backup Set up a schedule (see next section) to run backups automatically at specified times.
--	---	--	--

Backup Archives

Each time a backup runs, it creates an **archive** – a point-in-time snapshot. Borg uses deduplication, so subsequent backups only store changed data, making them fast and space-efficient.

Setting Up Schedules

Schedules automate your backups by running them at specified times. You can create multiple schedules for different backup jobs.

Creating a Schedule

1. Go to **Schedules** in the sidebar
2. Click **Add Schedule**
3. Configure the schedule:
 - **Backup Job:** Select which job to run

- **Frequency:** Daily, Weekly, Monthly, or Custom (cron)
- **Time:** When to run the backup
- **Days:** For weekly schedules, select which days

4. Click **Save** to activate the schedule

Schedule Examples

Daily at 2:00 AM	0 2 * * *
Every Sunday at midnight	0 0 * * 0
Every 6 hours	0 */6 * * *
First of every month at 3 AM	0 3 1 * *

Best Practices

- Run backups during low-activity periods (e.g., night)
- Stagger multiple backup jobs to avoid resource contention
- For critical data, consider running backups multiple times per day
- Monitor backup logs to ensure schedules are running successfully

Viewing and Restoring Archives

The **View/Restore** page lets you browse your backup archives and restore files when needed.

Browsing Archives

1. Go to **View/Restore** in the sidebar
2. You'll see a list of your repositories
3. Click on a repository to expand it and see archives grouped by backup job
4. Each archive shows:

- Creation date and time
- Size (original and deduplicated)
- Number of files

Restoring Files

1	Select an Archive Click the View button on the archive you want to restore from.
2	Browse Files Navigate through the archive's directory structure to find the files you need.
3	Select Files to Restore Check the files or directories you want to restore. You can select individual files or entire folders.
4	Choose Restore Location Specify where to restore the files: <ul style="list-style-type: none">• Original location: Restore files to their original paths• Custom location: Restore to a different directory
5	Start Restore Click Restore and wait for the process to complete. Progress is shown in real-time.

Restore Tips

- Restoring to the original location will overwrite existing files
- For safety, consider restoring to a temporary location first
- Large restores may take time – don't close the browser window
- Check file permissions after restore if needed

The **Settings** page contains various configuration options depending on your operating mode.

Operating Mode

View and change your current mode (Client/Standalone or Director). Changing modes will reset mode-specific configurations.

Client Configuration

Configure connection to a Director server. Set client name, Director URL, and connection token.

Connection Configuration

(Director only) Manage connection tokens and security settings for client connections.

Domain & Security

Configure custom domains, SSL certificates, and security settings for your installation.

Vault

(Director only) Securely store and manage repository passphrases for connected clients.

System Settings

Configure backup timeouts, concurrent backup limits, log retention, and other system-wide settings.

User Management

(Admin only) Create and manage user accounts, reset passwords, and configure permissions.