Borgmatic Director UI for professionals

Borgmatic Director UI - Professional Administration Guide

> This guide is intended for system administrators and IT professionals who need comprehensive knowledge of the Borgmatic Director UI application, its operating modes, configuration options, and administrative features.

Operating Modes

Borgmatic Director UI supports three operating modes for different deployment scenarios. Understanding these modes is essential for proper deployment planning.

Mode Comparison Matrix

Feature	Standalone	Client	Director
Manage local backups	✅	✅	✅ (via client proxy)
Full local web UI	✅	✅	✅
Connect to Director	✅	✅	✅
Manage multiple machines	✅	✅	✅
Approve client connections	✅	✅	✅
Deploy templates to clients	✅	✅	✅
Aggregate monitoring dashboard	✅	✅	✅

Feature	Standalone	Client	Director
Receive remote commands			

---

1. Standalone Mode (Default)

Standalone mode is the default operating mode. The instance operates independently, managing backups on a single server with no external connections.

Use Cases

- Single server deployments
- Home labs and personal servers
- Small businesses with one backup server
- Testing and development environments
- Air-gapped or isolated systems

Configuration

No additional configuration required. This is the default state after installation.

```
# Identity configuration file: /app/data/config/identity.json
{
  "mode": "standalone",
  "instance_id": "auto-generated-uuid",
  "instance_name": "My Backup Server"
}
```

Available Features

- Full backup job management (create, edit, delete, run)
- Repository management (local, SSH, S3, Rclone)
- Archive browsing and restore
- Schedule management
- SSH key management
- YAML configuration editor
- Real-time backup monitoring
- Notifications (email, webhooks, etc.)

---

2. Client Mode

Client mode allows the instance to be remotely managed by a central Director server while retaining full local functionality.

Use Cases

- Multiple servers managed by a central IT team
- Distributed infrastructure requiring unified management
- Managed Service Provider (MSP) client deployments
- Branch offices connected to headquarters

Configuration Steps

1. Navigate to **Settings → Operating Mode**
2. Click the toggle to switch from Standalone to Client mode
3. Configure connection settings:
   - **Client Name:** Human-readable identifier (e.g., "Production Web Server")
   - **Identification Phrase:** Secret phrase shown to Director admin for verification
   - **Director URL:** WebSocket URL (e.g., `wss://director.example.com`)
   - **Director Port:** Default is 9000
4. Save and initiate connection
5. Wait for Director admin to approve the connection request

Authentication Security

Client authentication uses Ed25519 cryptographic keypairs:

1. **Keypair Generation:** Client generates Ed25519 keypair on first setup
2. **Registration:** Client sends public key + identification phrase to Director
3. **Approval:** Director admin verifies phrase and approves connection
4. **Challenge-Response:** All subsequent connections authenticated via cryptographic challenge

```
Authentication Flow:
1. Client → Director: "Register me" + public key + phrase
2. Director Admin: Reviews request, verifies phrase
3. Director Admin: Clicks Approve (optionally locks IP)
4. Director → Client: Issues signed JWT token
5. Future connections:
   - Director: "Sign this random challenge: XYZ123"
   - Client: Signs with private key
   - Director: Verifies signature with stored public key
   - Connection established 
```

Connection Status Indicators

Status	Indicator	Meaning
Connected	□□ Green	Active connection to Director
Pending	□□ Yellow	Awaiting Director approval
Disconnected	□□ Red	No connection (network issue or Director offline)
Rejected	□ Blocked	Connection rejected by Director admin

Client Mode Features

- All Standalone features remain available
- Receives template deployments from Director
- Reports status and backup results to Director
- Can be monitored remotely via Director dashboard
- Automatic reconnection with exponential backoff

---

3. Director Mode

Director mode transforms the instance into a central management hub that can monitor and control multiple Client instances.

Use Cases

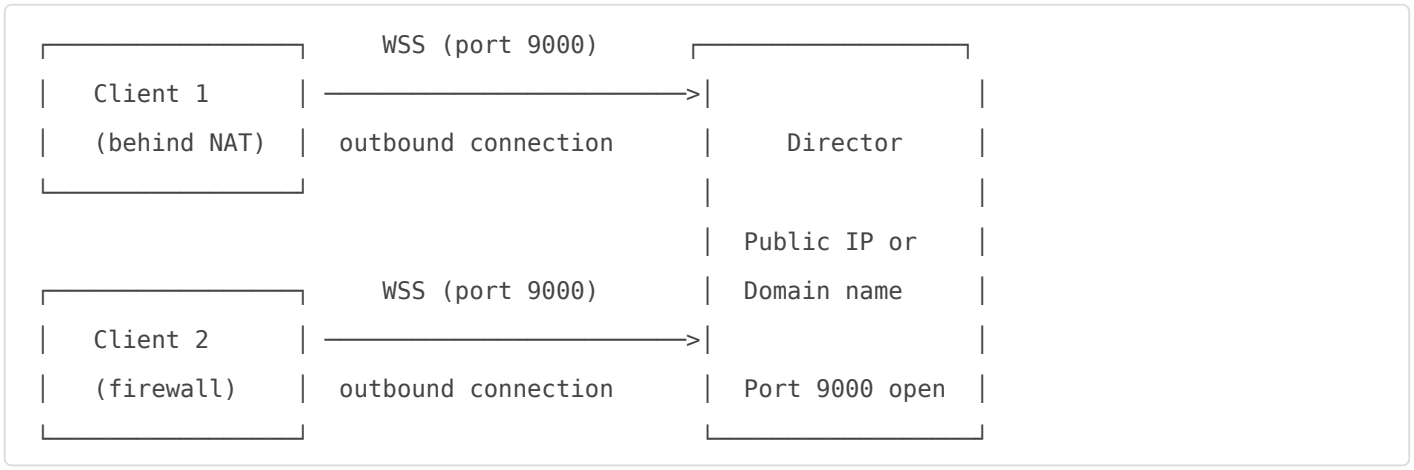
- Enterprise IT managing multiple servers
- Managed Service Providers (MSPs)
- DevOps teams managing infrastructure fleets
- Organizations requiring centralized backup oversight

Configuration Steps

1. Navigate to **Settings → Operating Mode**
2. Click "Switch to Director Mode"
3. Type "switch" to confirm (this is a significant change)
4. Configure Director settings:
   - **Listen Port:** WebSocket port for client connections (default: 9000)
   - **SSL/TLS:** Enable for production (recommended)
   - **Auto-Approve:** Automatically approve new clients (not recommended)
5. Restart the server if prompted

> **Note:** Switching to Director mode enables HTTPS and may require server restart. Switching back to Standalone clears all client data.

Network Requirements



- Director needs a public IP or domain name
- Director port 9000 (or configured port) must be accessible
- Clients initiate outbound connections (NAT-friendly)
- No port forwarding required on client machines
- Can use CloudFlare Tunnel or reverse proxy if Director is also behind NAT

Client Management Dashboard

The Director dashboard provides:

- **Connected Clients:** Real-time list of online clients with status
- **Pending Approvals:** New clients awaiting approval
- **Offline Clients:** Previously connected clients that are currently unreachable
- **Aggregate Statistics:** Total backups, repositories, success/failure rates

Client Approval Workflow

1. New client connects and appears in "Pending Approvals"
2. Admin reviews:
   - Client name
   - Identification phrase (verify this matches expected)
   - IP address
   - Public key fingerprint
3. Admin decides:
   - **Approve:** Client can connect and be managed
   - **Approve + Lock IP:** Only allow connections from current IP
   - **Reject:** Deny connection permanently

Managing Remote Clients

When in Director mode, a client selector appears in the navigation:

- Select a client to view/manage that client's backups, repositories, etc.
- All pages (Backups, Repositories, Archives, etc.) show data from selected client
- Actions performed affect the selected client

- "View All Clients" returns to the aggregate dashboard

Template Deployment

Directors can create and deploy templates to multiple clients:

- **Backup Templates:** Pre-configured backup job definitions
- **Schedule Templates:** Standardized backup schedules
- **Repository Templates:** Common repository configurations

Deployment options:

- Deploy to selected clients
- Deploy to client groups
- Deployed items are created as **inactive** for security (must be activated locally)

Mode Switching Reference

From	To	Data Impact	Action Required
Standalone	Client	None (non-destructive)	Toggle switch + configure Director URL
Client	Standalone	None (non-destructive)	Toggle switch
Standalone/Client	Director	Enables HTTPS, adds Director features	Type "switch" to confirm + restart
Director	Standalone	Clears all client connection data	Type "switch" to confirm

---

Dashboard

The Dashboard provides an at-a-glance overview of backup system health and recent activity.

Dashboard Widgets

System Status

- **Backup Tools Health:** Shows installed status and versions of Borg 1.x, Borg 2.x, Borgmatic, and Rclone
- **Last Health Check:** Timestamp of most recent tool verification

Backup Statistics

- Total backup jobs configured
- Active vs. inactive backups
- Last 24-hour success/failure count
- Currently running backups

Recent Activity

- List of recent backup runs with status
- Click to view detailed logs
- Filter by status (success, failed, running)

Repository Overview

- Total repositories configured
- Storage usage (if available)
- Repository health status

Backup Jobs

Backup Jobs define what data to back up, where to store it, and when to run.

Creating a Backup Job

Basic Settings

Field	Description	Required
Name	Human-readable identifier for the backup	Yes
Description	Optional notes about the backup purpose	No
Repository	Target repository for storing backups	Yes
Borg Version	Use Borg 1.x or Borg 2.x (must match repository)	Yes
Active	Enable/disable the backup job	Yes

Source Configuration

Field	Description	Example
Source Directories	Paths to back up	`/host/home`, `/host/var/www`
Exclude Patterns	Glob patterns to exclude	`*.tmp`, `**/node_modules/**`

Field	Description	Example
Exclude If Present	Skip directories containing these files	`.nobackup`, `CACHEDIR.TAG`

Advanced Options

Option	Description	Default
Compression	Compression algorithm and level	`zstd,3`
One File System	Don't cross filesystem boundaries	Enabled
Read Special	Read special files (devices, FIFOs)	Disabled
Numeric Owner	Store numeric user/group IDs	Disabled
No Atime	Don't store access time	Enabled

Retention Policy

Configure how many archives to keep:

Setting	Description	Recommended
Keep Hourly	Number of hourly archives	24
Keep Daily	Number of daily archives	7
Keep Weekly	Number of weekly archives	4
Keep Monthly	Number of monthly archives	6
Keep Yearly	Number of yearly archives	2

Hooks

Execute commands before/after backups:

Hook	When Executed	Use Case
Before Backup	Before archive creation starts	Database dumps, stop services
After Backup	After successful backup	Cleanup temp files, start services
On Error	When backup fails	Send alerts, cleanup

Running Backups

- **Manual Run:** Click the "Run" button on any backup job
- **Scheduled Run:** Automatically triggered by configured schedule
- **Stop Running:** Click "Stop" to abort a running backup

Backup Status

Status	Indicator	Meaning
Idle	○ Gray	Not currently running
Running	◫ Blue (spinner)	Backup in progress
Success	◫ Green	Last run completed successfully
Failed	◫ Red	Last run failed
Inactive	● Disabled	Backup job is disabled

Repositories

Repositories are the storage destinations for backup archives.

Repository Types

Local Repository

- **Path format:** `/path/to/repository`
- **Use case:** Local disk, mounted NAS, attached storage
- **Performance:** Fastest backup/restore speeds
- **Configuration:** Just specify the path

SSH/SFTP Repository

- **Path format:** `ssh://user@hostname:port/path`
- **Use case:** Remote backup servers, dedicated storage boxes
- **Authentication:** SSH key (recommended) or password
- **Configuration:**
  - Host, port, username
  - SSH key selection or password
  - Remote path (browse with file explorer)

S3/Cloud Storage (Rclone)

- **Providers:** Amazon S3, Backblaze B2, Wasabi, MinIO, Google Cloud, etc.
- **Storage Modes:**
  - **Local + Cloud Sync:** Fast local backups, automatic cloud sync
  - **Native Cloud (Borg 2.x):** Direct S3 writes, no Rclone needed
- **Configuration:**
  - Select Rclone remote (pre-configured in Rclone)

- Specify bucket/path
- Choose storage mode

Creating a Repository

1. Navigate to **Repositories → Create Repository**
2. Select repository type (Local, SSH, S3/Rclone)
3. Configure type-specific settings
4. Set Borg version (1.x or 2.x)
5. Enter encryption passphrase
6. Click **Create** to initialize the repository

> **Critical:** Save your repository passphrase securely! Without it, your backups cannot be accessed or restored.

Repository Actions

Action	Description	When to Use
Check	Verify repository integrity	Periodically or after errors
Compact (Borg 2.x)	Reclaim space from deleted archives	After pruning many archives
Update Passphrase	Change stored passphrase	If passphrase was entered incorrectly
Delete	Remove repository from UI	Optionally delete data on disk

---

Archives (View/Restore)

Archives are point-in-time snapshots stored in repositories.

Archive Browser

The Archive Browser provides file-system navigation of backup contents:

- **Directory Navigation:** Click folders to explore
- **Breadcrumb Trail:** Navigate back to parent directories
- **Search/Filter:** Filter files by name
- **File Preview:** View text file contents directly
- **Selection:** Check items for restore/download

Restore Options

Option	Description	Best For
Restore to New Location	Extract to a specified folder	Safest - review before replacing
Download	Download to your browser (ZIP for folders)	Small files, quick access
Restore to Original Location	Put files back where they were	Full disaster recovery

Restore History

Each archive tracks its last restore operation:

- Destination path or "Downloaded"
- Timestamp of restore
- Persisted across sessions

Archive Actions

Action	Description
Browse	Open archive in file browser
Info	View archive metadata (size, file count, etc.)
Delete	Permanently remove archive from repository

Schedules

Schedules automate backup execution at specified intervals.

Schedule Configuration

Field	Description	Example
Schedule Type	Preset or custom cron	Daily, Weekly, Custom
Time	When to run	02:00
Day (weekly)	Day of week for weekly schedules	Sunday
Cron Expression	Custom cron for advanced scheduling	`0 */6 * * *`
Timezone	Timezone for schedule evaluation	Europe/Berlin

Cron Expression Reference

```
# Format: minute hour day-of-month month day-of-week
#         0-59   0-23 1-31         1-12  0-6 (0=Sunday)

0 2 * * *      # Daily at 2:00 AM
0 */6 * * *    # Every 6 hours
0 3 * * 0      # Weekly on Sunday at 3:00 AM
0 4 1 * *      # Monthly on the 1st at 4:00 AM
*/30 * * * *   # Every 30 minutes
```

Common Schedule Patterns

Pattern	Cron	Use Case
Daily at 2 AM	`0 2 * * *`	Standard daily backup
Every 6 hours	`0 */6 * * *`	Frequently changing data
Weekdays at 6 PM	`0 18 * * 1-5`	End of business day
Sunday at 3 AM	`0 3 * * 0`	Weekly full backup

SSH Key Management

SSH keys enable secure, passwordless authentication to remote servers.

Key Operations

Import Existing Key

1. Click **Import SSH Key**
2. Provide a name for the key
3. Paste the private key content, OR
4. Click **Select from Server** to browse server filesystem, OR
5. Click **Upload Key File** to upload from your computer
6. If key is encrypted, enter the passphrase
7. Click **Create**

Generate New Key

1. Click **Generate SSH Key**

2. Provide a name
3. Select key type (Ed25519 recommended, RSA for compatibility)
4. Click **Generate**
5. Copy the public key to remote server's `~/.ssh/authorized_keys`

Test Connection

1. Click the test icon on a key
2. Enter remote host, username, and port
3. Click **Test Connection**
4. Verify connection succeeds and Borg is detected

Supported Key Types

Type	Format Header	Recommendation
OpenSSH	`-----BEGIN OPENSSH PRIVATE KEY-----`	Recommended (modern)
RSA PEM	`-----BEGIN RSA PRIVATE KEY-----`	Good (legacy compatible)
EC PEM	`-----BEGIN EC PRIVATE KEY-----`	Good
PKCS#8	`-----BEGIN PRIVATE KEY-----`	Good

Key Security

- Private keys are stored encrypted in the database
- Passphrase-protected keys are supported
- Temporary key files are created with mode 0600
- Temporary files are cleaned up immediately after use

YAML Editor

The YAML Editor provides direct access to Borgmatic configuration files.

Features

- **Syntax Highlighting:** YAML-aware editor with color coding
- **Validation:** Real-time syntax and schema validation
- **Backup/Restore:** Automatic backups of config changes
- **File Browser:** View all configuration files in `/etc/borgmatic.d/`

Use Cases

- Advanced configuration not exposed in UI
- Bulk editing of multiple options
- Importing existing Borgmatic configs
- Troubleshooting configuration issues

> **Caution:** Manual YAML edits may conflict with UI-managed settings. Use the UI for standard configurations.

Logs

The Logs page provides access to backup execution logs and system events.

Log Types

Log Type	Content	Location
Backup Logs	Individual backup execution output	Per-backup log files
Borgmatic Logs	Borgmatic wrapper output	System logs
Application Logs	Borgmatic UI application events	Container stdout/stderr

Log Features

- **Real-time Streaming:** Watch backup progress live
- **Search:** Find specific entries
- **Filter by Level:** Info, Warning, Error
- **Download:** Export logs for analysis

Settings

General Settings

Setting	Description
Instance Name	Display name for this server

Setting	Description
Theme	Light or dark mode
Timezone	Default timezone for schedules

Operating Mode

See the Operating Modes section above.

Notifications

Configure alerts for backup events:

Provider	Configuration
Email (SMTP)	SMTP server, credentials, recipients
Webhook	URL to POST events to
Slack	Webhook URL
Discord	Webhook URL
Gotify	Server URL and token
Ntfy	Topic and server URL

Security Settings

Setting	Description
Change Password	Update admin password
Session Timeout	Auto-logout after inactivity
API Tokens	Generate tokens for API access

Factory Reset

Completely reset the instance:

- Removes all configurations
- Clears all credentials
- Optionally regenerates secret key
- Requires typing "RESET" to confirm

> **Warning:** Factory reset is irreversible. Backup your data first!

Environment Variables

Configure the application via environment variables:

Variable	Default	Description
`NODE_ENV`	production	Environment mode (production/development)
`PORT`	3000	HTTP server port
`JWT_SECRET`	(auto-generated)	Secret for JWT token signing
`ADMIN_USERNAME`	admin	Default admin username
`ADMIN_PASSWORD`	admin	Default admin password
`DATA_DIR`	/app/data	Persistent data directory
`TZ`	UTC	Container timezone
`DIRECTOR_PORT`	9000	WebSocket port (Director mode)
`RESTORE_ALLOWED_ROOTS`	/host,/tmp,/data	Allowed restore destination paths
`DEBUG_REPOSITORIES`	false	Enable verbose repository logging

Docker Deployment

Basic Docker Compose

```
version: '3.8'

services:
  borgmatic-ui:
    image: borgmatic-ui:latest
    container_name: borgmatic-ui
    restart: unless-stopped
    ports:
      - "8080:3000"      # Web UI
      - "9000:9000"      # Director WebSocket (if using Director mode)
```

```
    volumes:
      - ./data:/app/data                    # Persistent data
      - ./borgmatic.d:/etc/borgmatic.d      # Borgmatic configs
      - /:/host:ro                          # Host filesystem access
      - ./borg-cache:/root/.cache/borg      # Borg cache
    environment:
      - ADMIN_PASSWORD=change-me-please
      - TZ=Europe/Berlin
```

Volume Mounts Explained

Mount	Purpose	Required
`/app/data`	Application data, credentials, SSH keys	Yes
`/etc/borgmatic.d`	Generated Borgmatic YAML configs	Yes
`/:/host`	Access to host filesystem for backups	Yes (for local backups)
`/root/.cache/borg`	Borg cache (improves backup speed)	Recommended

Troubleshooting

Common Issues

Problem	Cause	Solution
"Cannot connect to server"	Backend not running or port blocked	Check container logs, verify port mapping
"Authentication failed" (SSH)	Wrong key or not in authorized_keys	Verify public key on remote server
"Passphrase wrong"	Incorrect repository passphrase	Update passphrase in repository settings
"Repository locked"	Previous backup didn't finish	Wait or use "Break Lock" action
Backup stuck at 0%	Network issue or SSH timeout	Check connectivity, test SSH connection
Director: Client not connecting	Firewall, wrong URL, or DNS issue	Verify port 9000 accessible, check client logs

Debug Mode

```
# Enable verbose logging
docker run -e DEBUG_REPOSITORIES=true ...

# View container logs
docker logs -f borgmatic-ui

# Check real-time backup output
# (visible in the UI during backup execution)
```

API Access

Borgmatic Director UI provides a REST API for automation and integration.

Authentication

```
# Login to get JWT token
POST /api/auth/login
Content-Type: application/json
{
  "username": "admin",
  "password": "your-password"
}

# Use token in subsequent requests
Authorization: Bearer <token>
```

Key Endpoints

```
# Backups
GET  /api/backups              # List all backup jobs
POST /api/backups/:id/run      # Trigger backup
POST /api/backups/:id/stop     # Stop running backup

# Repositories
GET  /api/repositories         # List repositories
POST /api/repositories/:id/check  # Check integrity
```

```
# Archives
GET  /api/archives/:repo       # List archives
GET  /api/archives/:repo/:archive/browse  # Browse contents

# Health
GET  /api/dashboard/health     # System health
GET  /api/dashboard/tools-health  # Tool versions
```

> **Need more help?** Check the container logs (`docker logs borgmatic-ui`) for detailed error messages. Most issues are related to SSH connectivity, passphrases, or file permissions.

Revision #2
Created 17 January 2026 08:12:26 by Admin
Updated 17 January 2026 08:24:47 by Admin