9: Passbolt - Team Password Management

Passbolt is an OpenPGP-based, self-hosted team password manager with strong security properties and a browser-extension-centric UX. For comprehensive configuration, hardening guidance, and usage documentation, see the official Passbolt documentation.

Prerequisites

- Traefik installed (Chapter 4) and domain configured (Chapter 4.5)
- Docker running (Chapter 3)
- Borgmatic installed (Chapter 5) for automated backups
- Subdomain ready, e.g., `pass.example.com`

Installation via Infinity Tools

Menu Installation

```
APPLICATIONS → Passbolt → Install
```

CLI Installation

```
sudo bash /opt/InfinityTools/Solutions/setup-passbolt.sh --install
# or with environment variables
export PB_DOMAIN="pass.example.com"
sudo -E bash /opt/InfinityTools/Solutions/setup-passbolt.sh --install
```

Configuration Overview

- **Deployment modes:** Traefik (recommended), standalone HTTPS (self-signed), or HTTP
- **Database:** MariaDB 10.11 managed alongside Passbolt
- **Data paths:** `/opt/speedbits/passbolt/` (GPG keys, JWT keys, DB data)

- **Version pinning:** Passbolt image version pinned for stability

Environment Parameters (examples)

```
# SSL + domain
export PB_DOMAIN="pass.example.com"        # FQDN for Passbolt
# Networking
export PROXY_NETWORK="proxy"               # Traefik network name
```

What the Installer Sets Up

- Creates directories under `/opt/speedbits/passbolt/` (GPG, jwt, db_data)
- Generates secure database credentials (`db_password.txt`)
- Runs Passbolt + MariaDB containers
- Configures Traefik labels for HTTPS routing (if selected)
- Outputs access URLs and image versions on completion

Post-Install Steps

1. Open the web UI: `https://pass.example.com`
2. Follow the onboarding to create the first admin user
3. Install the Passbolt browser extension (Chrome/Firefox) when prompted
4. Configure SMTP in the Passbolt UI for email notifications

Backup & Restore

- Passbolt data (GPG, jwt) and database live under `/opt/speedbits/passbolt/`
- Borgmatic file backups include `/opt/speedbits/` by default
- Database dumps are included in the high-frequency DB backups

Operational Checks

```
# Check container states
sudo docker ps | egrep 'passbolt|passbolt-db'


# View logs
```

```
sudo docker logs passbolt --since 10m
sudo docker logs passbolt-db --since 10m

# Show current config hints (paths)
ls -la /opt/speedbits/passbolt/
```

Troubleshooting

SSL / Routing

```
# Verify Traefik is running
sudo docker ps | grep traefik

# Check ACME events
sudo docker logs traefik | grep -i acme

# Confirm DNS
dig +short pass.example.com
```

Database Connectivity

```
# Check DB container
sudo docker logs passbolt-db --since 10m

# Exec into DB and test
sudo docker exec -it passbolt-db mysql -u passbolt -p
```

Passbolt Health

```
# Application logs
sudo docker logs passbolt --since 10m

# Restart services
cd /opt/speedbits/passbolt && sudo docker compose down && sudo docker compose up -d
```

Security Notes

- Restrict admin access to known IPs (Traefik middleware optional)
- Rotate database and JWT keys as part of change management
- Ensure regular backups and test restoration

Verification

- Web UI reachable via HTTPS
- First admin created and logged in
- Browser extension paired
- Borgmatic backups succeeding

For advanced configuration (SMTP, LDAP/SSO, security hardening), consult the official Passbolt documentation.

Revision #2
Created 31 October 2025 13:25:00 by bjoern
Updated 17 November 2025 16:36:38 by bjoern