9: Passbolt - Team Password Manager

Passbolt is a team-oriented, self-hosted password manager built on OpenPGP. It lets you securely store and share passwords with your team. For comprehensive usage instructions, browser extension setup, and advanced features, please refer to the official Passbolt documentation.

What is Passbolt? (Simple Explanation)

Passbolt helps teams store and share passwords securely. It uses strong encryption and a browser extension to keep your secrets safe and easy to use.

Why Passbolt is useful:

- **Team sharing** - Share secrets with specific people
- **Strong security** - OpenPGP-based encryption
- **Browser extensions** - Easy access in Chrome/Firefox
- **Self-hosted** - You control your data

Prerequisites

Before installing Passbolt, make sure you have:

- **Traefik installed** (from Chapter 4)
- **Docker running** (from Chapter 3)
- **Borgmatic installed** (from Chapter 5) - Your data will be automatically backed up (optional but recommended)
- **Subdomain ready** (from Chapter 4.5), e.g., `pass.yourdomain.com`
- **An email address** (for SSL certificates)

Why These Prerequisites Matter

Traefik: Provides secure HTTPS access

Docker: Runs Passbolt securely in containers

Borgmatic: Automatically backs up your Passbolt data and database

Subdomain: Easy, secure access for your team

Step 1: Start Infinity Tools

Connect via SSH and start Infinity Tools:

```
sudo infinity-tools
```

Using the Infinity Tools GUI

From the main menu, go to the **APPLICATIONS** section.

- **Clear categories** - Applications are grouped logically
- **Status indicators** - Shows if services are installed
- **Easy navigation** - Arrow keys + Enter

Step 2: Install Passbolt

1. Open **APPLICATIONS**
2. Select **Passbolt**
3. Choose **Install Passbolt**

What Happens During Installation

- Creates Passbolt and database containers
- Generates secure database passwords
- Configures SSL via Traefik (recommended)
- Sets up data directories in `/opt/speedbits/passbolt`

Step 3: Configure Passbolt

SSL & Domain

You'll be asked whether to use Traefik and for your domain. Recommended:

- Use Traefik: **Yes**
- Domain: e.g., `pass.yourdomain.com`

Admin Account

After installation, you'll finish setup in the browser by creating the first admin user and installing the Passbolt browser extension.

Step 4: Open Passbolt

Once installation completes:

- Go to `https://pass.yourdomain.com`
- Follow the on-screen setup wizard
- Install the Passbolt browser extension when prompted

Step 5: Verify and Basics

- **Service running:** Check **STATUS & HEALTH → STATUS**
- **Backup active:** Borgmatic will include Passbolt data automatically
- **Login works:** Use your admin account

Troubleshooting

Can't Access the Site

- Check Traefik is running: `docker ps | grep traefik`
- Make sure your subdomain points to your server
- Wait a few minutes for SSL certificates

Database Issues

- Check database container status in **STATUS & HEALTH → DOCKER INFO**
- Review logs: `docker logs passbolt`, `docker logs passbolt-db`

Quick Reference

Web UI: `https://pass.yourdomain.com`

Data directory: `/opt/speedbits/passbolt/`

Database credentials: `/opt/speedbits/passbolt/db_password.txt`

You're Ready!

Passbolt is now installed and ready for your team. Manage users and shared passwords from the web interface and browser extension.

Next: Add your team, create groups, and start sharing passwords securely. For how-to guides and best practices, see the official Passbolt documentation.

Revision #5
Created 30 October 2025 13:12:50 by bjoern
Updated 17 November 2025 16:42:34 by bjoern