Fosdem 2024

Passbolt: the open source password manager for teams

Lightning talks
Hello, I’m Remy,
Co-founder of passbolt

$ whoami

/passbolt
@stripthis

@passbolt@mastodon.social

passbolt, mailvelope, open social, cakephp cakefest, 05f5.com…
20 years ago? Throwback from the past...
Passbolt founders at fosdem with Jon 'Maddog' Hall
Anyone not using a password manager at work?
The open source credential manager built for collaboration

Go ahead share your secrets...
Quick access & in form menu

Fast & furious cautious!
Android and iOS
Your credentials on the go.
Retrieve, store, and share passwords programmatically with the JSON api.

Automate recurring tasks with CLI.

Use with Ansible collection, Gitlab, etc.

And **terminals** near you

Via official or community maintained CLIs, libraries, etc. or just Curl and Gpg

```
$> export SECRET=`
curl --location --request GET '${PASSBOLT_URL}'
--header 'Authorization: ${ACCESS_TOKEN}'
--header 'Content-Type: application/json'
| jq -j '.body.data'
| gpg -q --no-tty
```

```
$> passbolt get 664735b2-4be7-36d9-a9f8-08d42998faf8
------BEGIN PGP MESSAGE------

$> passbolt get \
$(passbolt find | awk '/server/ { print $NF }')\
| gpg -q --no-tty
```

```
$> passbolt get \
$(passbolt find | awk '/server/ { print $NF }')\
| gpg -q --no-tty
```

```
$> export SECRET=`
curl --location --request GET '${PASSBOLT_URL}'
--header 'Authorization: ${ACCESS_TOKEN}'
--header 'Content-Type: application/json'
| jq -j '.body.data'
| gpg -q --no-tty
| jq -j '.password'
```
Got trust issues? Host it yourself!

Works in air-gapped environments or on a Raspberry Pi

- Docker images (rootless / distroless)
- Debian / Ubuntu packages
- RPM packages (RHEL, Centos, etc.)
- Helm charts
- AWS AMI, Digital Ocean, etc.
How does passbolt compare with...

TL;DR; passbolt focus on secure online collaboration

**Keepass**
- ✗ Synced across devices
- ✗ Nested permissions
- ✗ User management
- ✗ JSON API
- ✗ Browser integration
- ✗ Audit logs
- ✓ Encrypted metadata
- ✓ Offline mode
- ✓ Files / more content types

**warden**
- ✗ Random private key
- ✗ Mandatory browser extension
- ✗ Challenge-based authentication
- ✗ Nested folders with flexible permissions
- ✗ 100% open source (not “source available”)
- ✗ Secret and password manager all in 1
- ✓ External share (Send)
- ✓ Offline mode
- ✓ Files / more content types
What happened in 2023?
Single Sign On

SSO OpenID will be coming soon in CE!
Collaborative management of TOTPs
Both on mobile and web extension
Passbolt.exe

If you are into blue screens... 😊
And also…

- Performance improvements
- Improved grid
- Improve filters & search (mobile)
- Key export/transfer (mobile)
- RBAC for UI
- Suspend user
- Password policies
- Passphrase policies
- MFA policies
- User self-registration
- 4 security audits
What’s cooking in 2024?
Password expiry

Fix automatically marking accessed items as expired when a user is deleted, leaves a group, lose a permission, etc.
Redesigned admin panel
And also...

- SSO ADFS
- Performance improvements
- Search improvements
- Icons / Custom fields
- File attachments
- More content types (notes, cards)
- Manifest V3 rollout
- New help site (admin, dev, user)
- Biometric login (web)
- Admin reports
- 7+ babies
What is it made of?

(the secret ingredient is love)
Three main application layers.

- **Styleguide**, **Browser Extension**, **Web API**

**User Interface**
Interactions, Styling

**Sensitive operations**
Crypto, validation, API calls

**JSON API**
(Some HTML content)

**Baseline services**
LAMP or similar

---

- **Webextension / Styleguide (React / Less)**
- **Webextension background Page (JS)**
- **Passbolt API (Cakephp / PHP)**
- **OpenPGP.js**
- **GnuPG**
- **Nginx / Apache**
- **File / Redis / etc.**
- **Mariadb / Postgresql / Etc.**
- **GNU/Linux**
Passbolt JSON API (CakePHP)

https://help.passbolt.com/api

API Documentation

View one resource

It is possible to get data for a single resource identified by the unique UUID. All you need is to make a GET request to /resources/<resourceId>.json.

GET /resources/<resourceId>.json

Possible responses

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Response includes the resource metadata object.</td>
</tr>
<tr>
<td>400</td>
<td>Bad Request</td>
</tr>
<tr>
<td></td>
<td>The resourceId supplied is not a valid UUID</td>
</tr>
<tr>
<td>403</td>
<td>Authentication Failure</td>
</tr>
<tr>
<td></td>
<td>The user making the request is not authenticated</td>
</tr>
<tr>
<td>404</td>
<td>Not Found</td>
</tr>
<tr>
<td></td>
<td>The resource either does not exist or the user does not have access permission.</td>
</tr>
</tbody>
</table>

Examples

Success response

For another perspective on the API you browse the OpenAPI 2.0 specifications using the dedicated API reference site (Swagger UI).

API Reference

You can also find the latest OpenAPI 2.0 specifications directly on the dedicated repository.

OpenAPI Specs repository
Passbolt styleguide (Storybook)

https://passbolt.github.io/passbolt_styleguide

Welcome to passbolt user interface design kit.

Visit our website  Follow on github
Questions? 🍅 ?
Thank you Fosdem ❤️

See you at the bar at 14:00 for some swag & 🍺