



Admin Quick Start Guide

What you need to know to get started

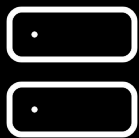
How do I get started?

This is what the setup looks like

Step 1. Gather **Your Credentials**



Websites



Servers



Cloud
Services



API keys



Databases



Other
credentials

- ✓ Gather your credentials
- ✓ Remove outdated, duplicate, or inactive credentials
- ✓ Remove what your team no longer uses

Step 2. Design Your **Folder Architecture**. Foundation of a successful rollout

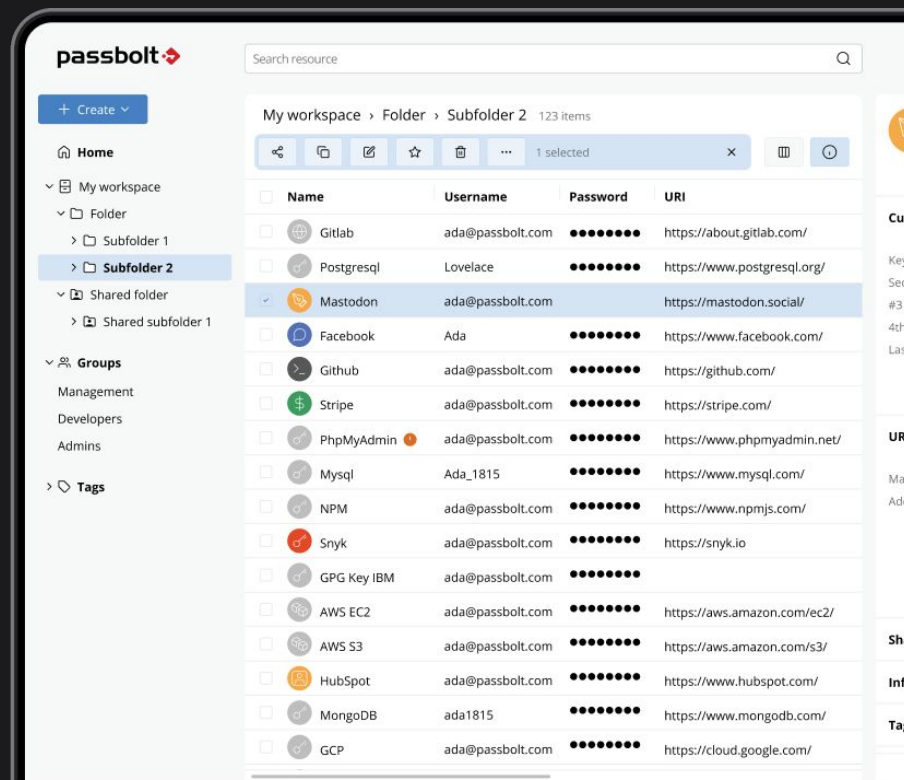
Mirror Your Organisation

Choose your folder structure to group passwords

- ✓ Department-Based / Project-Based / Client-Based / Business Unit-Based, etc.
- ✓ Nest folders to improve navigation. Avoid one massive catch-all folder.

Create groups (of users) that mirror your departments

- ✓ Group users based on shared access needs to simplify permissions.
- ✓ Strongly advise to import Active Directory groups (Pro feature).



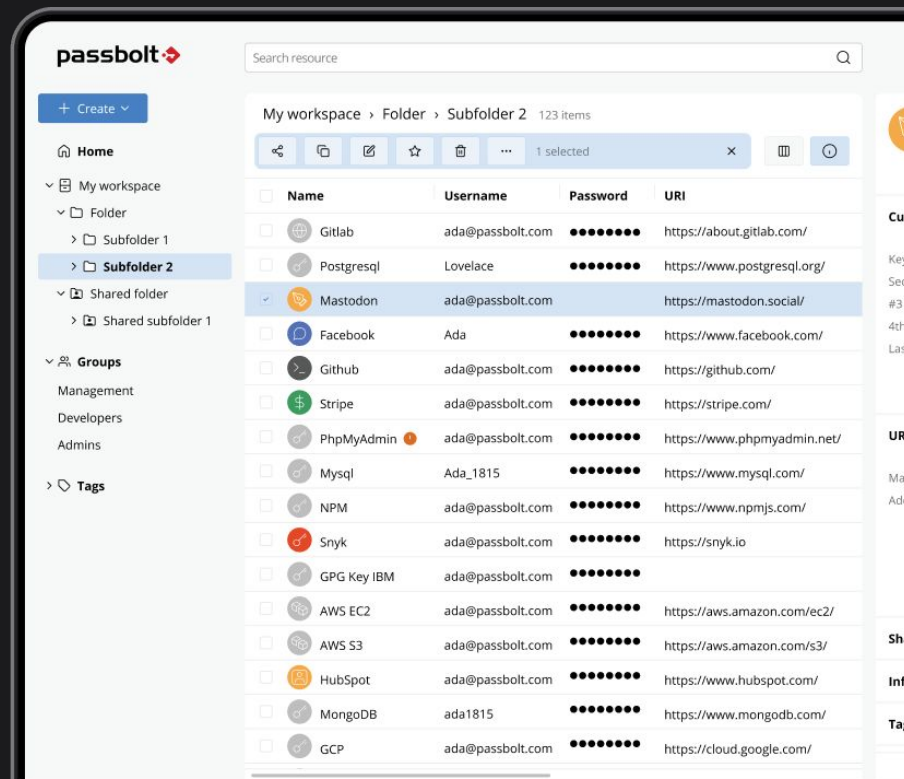
Step 2. Design Your **Folder Architecture**. Foundation of a successful rollout

Strongly advise respecting the Principle of Least Privilege

When your folder structure and groups are set up correctly, least privilege happens naturally. Each user sees only what they need, nothing more.

The principles to follow:

- ✓ Permissions will be assigned at the group level (recommended); sharing with an individual should only ever be an exception.
- ✓ Share a folder with several groups when more than one team genuinely needs it, rather than duplicating folders.
- ✓ Give each group only the permission it requires, such as Read-Only or Update.
- ✓ Choose carefully which group(s) own a folder, since owners can add or remove users and groups.



Step 3. Import **Your Credentials**

**TIP: IT Department owns
the initial import**

gather the initial credential setup

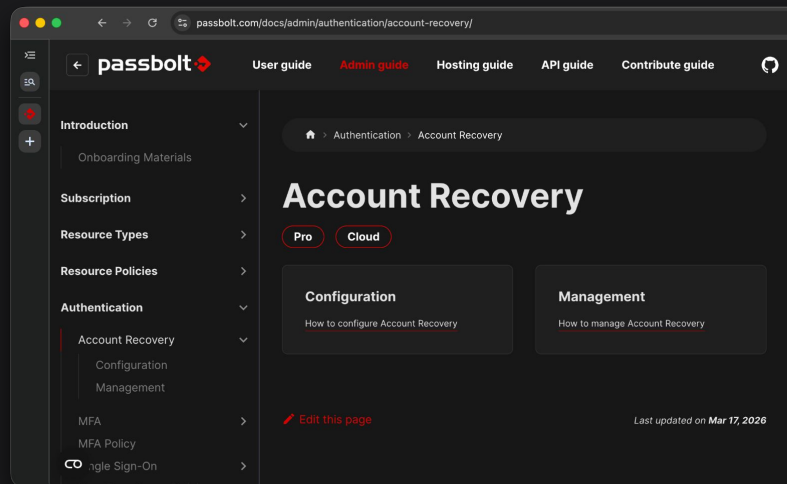
*Import the CSVs or the KeePass file
within the relevant folder structure
defined in step 2.*



Step 4. Setting Up the **Organisation Recovery Key** before importing users!

Ensure users can regain access if they lose their **private key** or **passphrase**

1. Configure your Organisation Recovery Key. Select **Prompt** (recommended). New users will be automatically prompted to enrol during account setup.
2. If a user loses access click "Help, I lost my passphrase" on the login screen to start recovery process.
3. You also have the possibility to create a role and assign non-admin user to perform account recovery (for a support team for example).



TIP: Good timing to also configure your Security Baseline

- ✓ Resources policies, expiry, and secret history.
- ✓ Authentication policies, Single Sign-on (SSO), Passphrase policies, and Multi-Factor Authentication (MFA).
- ✓ Notifications and more information about role-based access control in the next slide.

Step 5. Setting Up Role Based Access Control

Ensure specific actions are forbidden for regular users and/or create custom roles to allow specific actions for a portion of your users.

1. Remove the possibility for your users to export credentials.
2. Give your support team the possibility of performing account recoveries.
3. Hide the user workspace.
4. Disable the possibility to configure phone or desktop app, etc.

← Organisation settings

Home > Role-Based Access Control

Role-Based Access Control

In this section you can define access controls for each user role. [Add role](#)

	Admin	User	Group Admin
API Permissions			
Group management			
Create a group	Allow	Deny	Allow
Account recovery request			
Account recovery request view	Allow	Deny	Deny
Account recovery request index	Allow	Deny	Deny
Account recovery request review	Allow	Deny	Deny
UI Permissions			
Resources			
Import/Export			
Can import	Allow	Allow	Allow
Can export	Allow	Allow	Allow
Password			
Can preview	Allow	Allow	Allow
Can reset	Allow	Allow	Allow

[Role-Based Access Control](#) [Save](#)

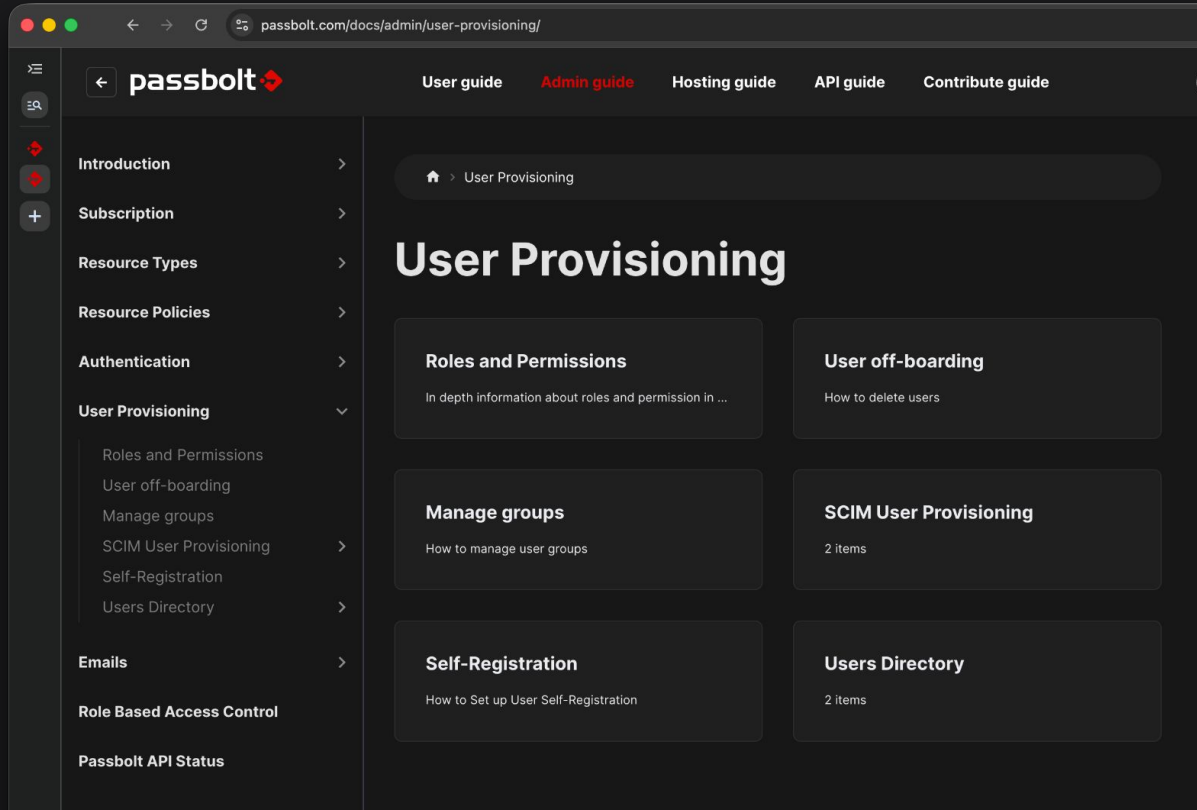
Internationalisation

Step 6. Bring your team onboard **User & Group Sync**

**Deploy progressively
(recommended)**

Import your users/groups

- ✓ LDAP sync (Pro)
- ✓ SCIM (Pro/Cloud)
- ✓ Self registration



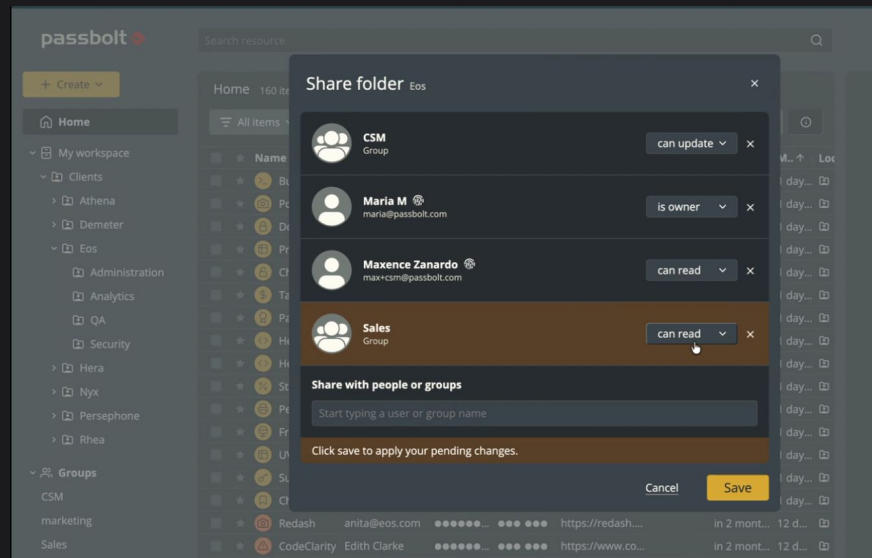
Step 7. Start secure collaboration **Folder Sharing & Permission**

Apply the "One-to-Many" Rule

- ✓ Link folders to groups
- ✓ Manage permissions tier at the folder level. (The sub-folders and passwords will inherit the upper-permission rights unless you modify them)
- ✓ Avoid assigning access user by user

Permission Tier	Capabilities	Can Share?
Can Read	View and use credentials only	No
Can Update	Create, Edit, and Delete items (folders, resources) in a folder	No
Is Owner	Full rights + Permission management	Yes

Passbolt requires every folder to have at least one owner at all times to prevent data from becoming orphaned



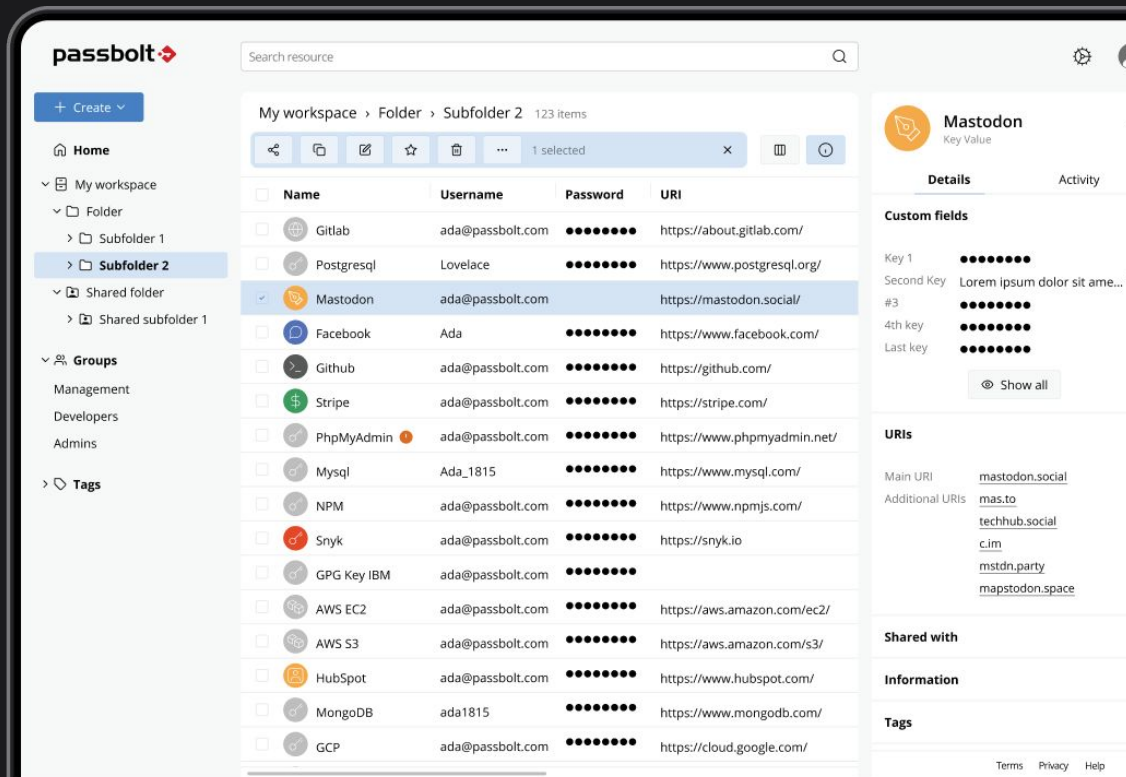
⚠ Avoid sharing passwords directly with individual users. Always go through groups. It makes (on/off)boarding and permission changes much easier

Beyond the setup

Two useful practices before rolling out

Onboarding Check

- ✓ **Verify user access** and sharing logic with test users
- ✓ **Recovery Check.** Test the Organisation Recovery Key and Recovery process



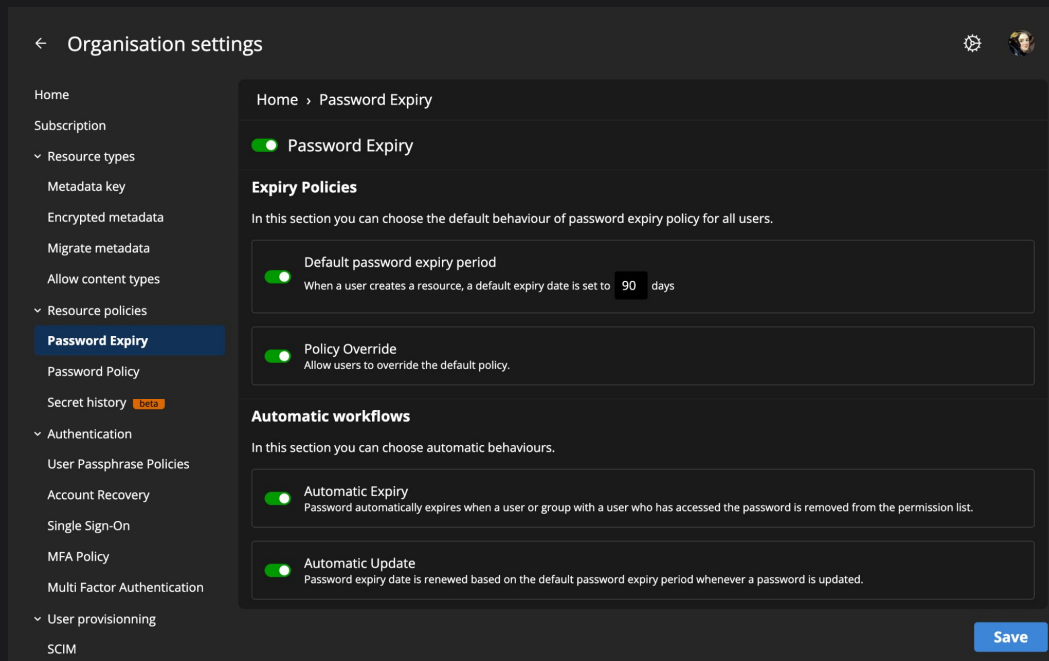
Offboarding Check and Credential Cleanup

Managing Password Expiry.

When a user is removed from a group, access is revoked immediately.

But credentials they previously accessed will be marked as (!) **expired** and should be rotated to maintain good security hygiene.

If a user is **sole owner** of elements (passwords, folders, groups), a pop-up will be displayed at the deletion of the user to **transfer** the ownership to another user.



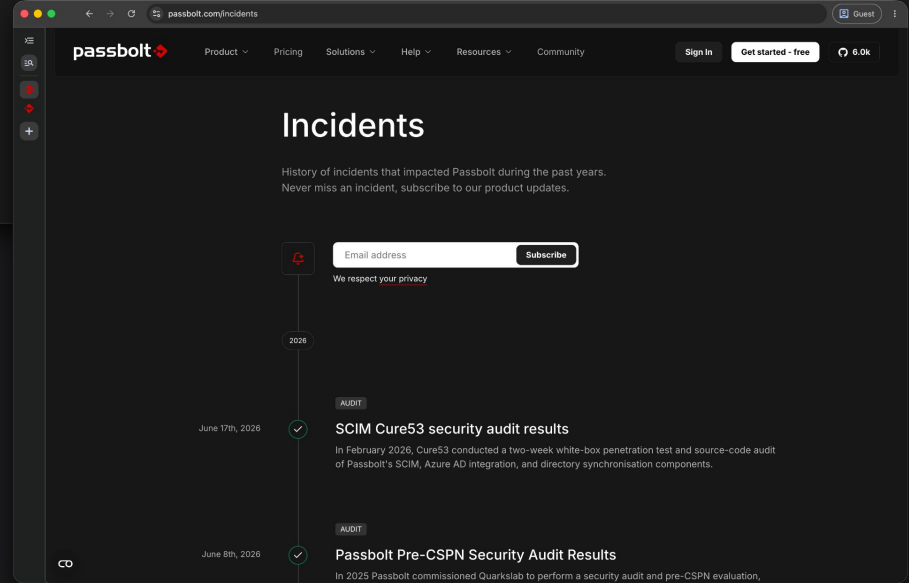
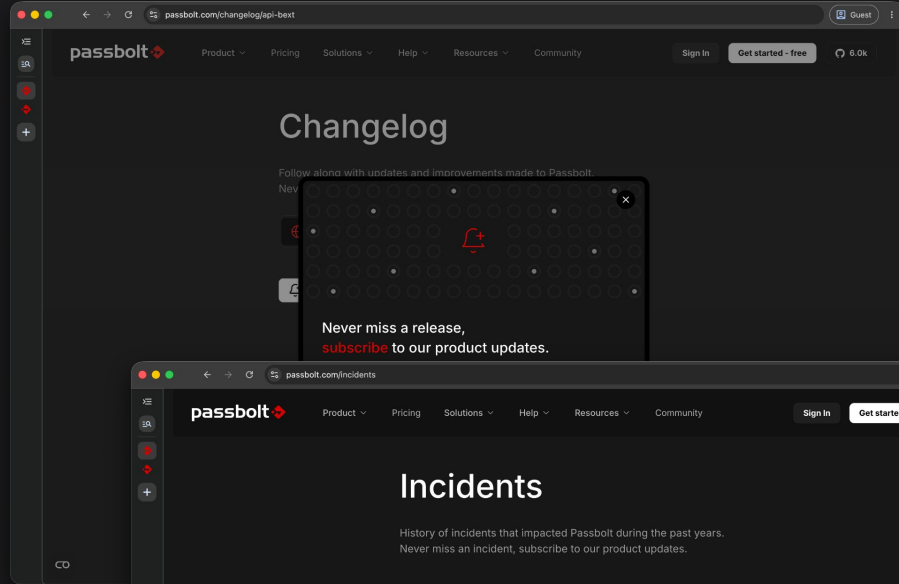
- ✓ **Flagged (!) credentials** were accessed, rotate these first
- ✓ Unflagged credentials were shared but never accessed, need no action

Useful resources

Where to learn more and get help

Subscribe to Updates and Alerts

- ✓ Subscribe to our monthly release updates to stay informed about new features
- ✓ Subscribe to incidents to stay informed about any security incidents



Browse the **admin guide**. Learn more about the other functionalities on the official documentation.

The screenshot shows a web browser window at `passbolt.com/docs/admin/`. The page has a dark theme. At the top, there's a navigation bar with the Passbolt logo and links for [User guide](#), [Admin guide](#) (highlighted in red), [Hosting guide](#), [API guide](#), and [Contribute guide](#). A search bar is on the right. A left sidebar contains a table of contents with items like Introduction, Subscription, Resource Types, etc. The main content area has a breadcrumb `Introduction` and a large heading `Welcome to the Admin Guide!`. Below this is a section titled `Admin guide` with a gear icon. The section `What is the Admin Guide?` explains that the documentation is divided into several sections accessible from the top navigation bar, listing the Admin Guide, Hosting Guide, User Guide, API Guide, and Contribute Guide.

passbolt.com/docs/admin/

passbolt

User guide Admin guide Hosting guide API guide Contribute guide

Search

Introduction

Onboarding Materials

Subscription

Resource Types

Resource Policies

Authentication

User Provisioning

Emails

Role Based Access Control

Passbolt API Status

Introduction

Welcome to the Admin Guide!

Admin guide

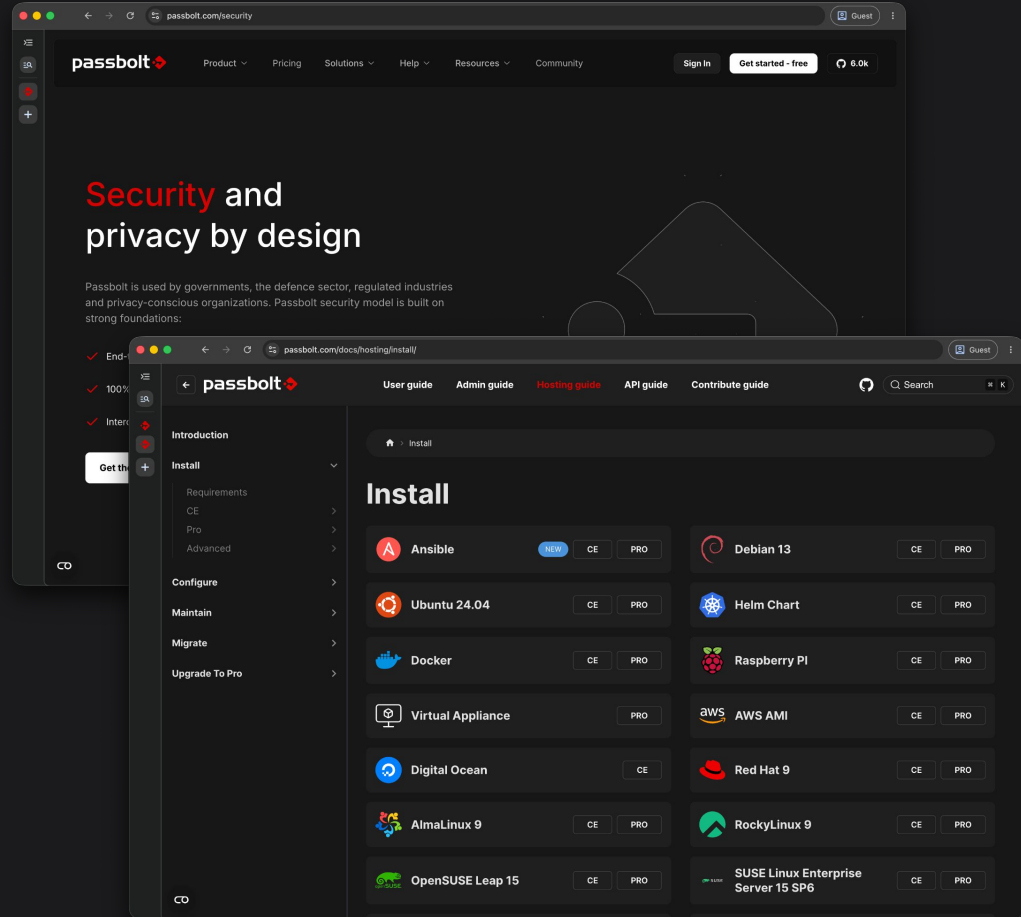
What is the Admin Guide?

The documentation for Passbolt contains several main sections, all accessible from the top navigation bar:

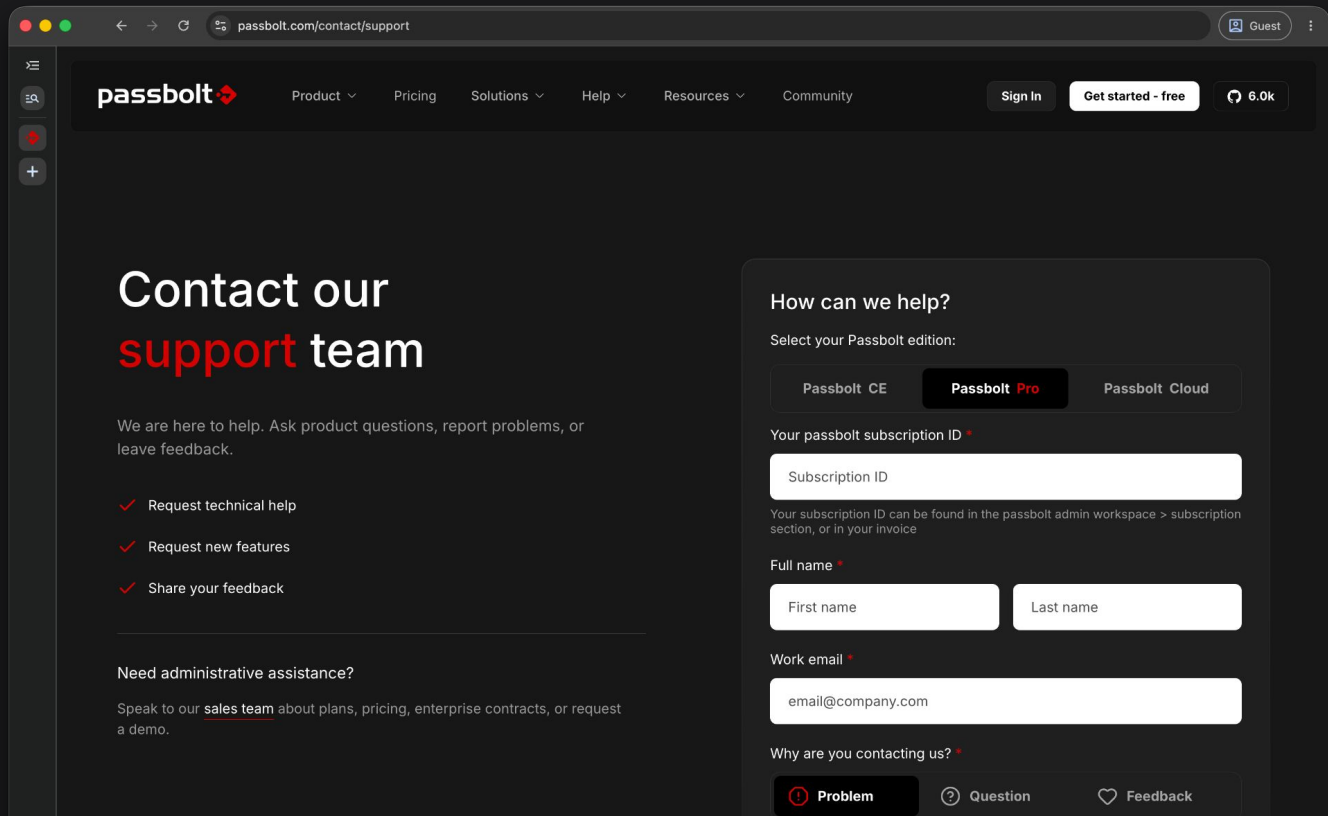
- The [Admin Guide](#) that you're currently reading contains all the information for users with the administrator role, e.g. all about the user and admin workspaces.
- The [Hosting Guide](#) contains all the technical information related to the setup and update of your passbolt self-hosted server.
- The User Guide contains all about the functionalities available to every user.
- The [API Guide](#) contains low-level and detailed information related to the different endpoints of the backend API.
- The [Contribute Guide](#) contains information about how you can contribute to passbolt in different ways.

Passbolt Pro Edition Additional Resources

- ✓ Security White Paper Risk mitigation, residual risks, and security best practices checklist
- ✓ Check the Hosting guide Installation, configuration, high availability, backup, and patching



If you are stuck you can always look in the passbolt community forum or ask our tech support.

A screenshot of a web browser showing the Passbolt support page. The browser's address bar displays 'passbolt.com/contact/support'. The page has a dark theme. At the top, there is a navigation bar with the Passbolt logo, links for Product, Pricing, Solutions, Help, Resources, and Community, and buttons for Sign In, Get started - free, and a 6.0k user count. On the left side, there is a sidebar with icons for menu, search, and a plus sign. The main content area is divided into two columns. The left column has a large heading 'Contact our support team' with 'support' in red. Below it, a paragraph states 'We are here to help. Ask product questions, report problems, or leave feedback.' followed by three bullet points: 'Request technical help', 'Request new features', and 'Share your feedback'. The right column has a heading 'How can we help?' and a section 'Select your Passbolt edition:' with three buttons: 'Passbolt CE', 'Passbolt Pro' (highlighted), and 'Passbolt Cloud'. Below this is a form for 'Your passbolt subscription ID' with a text input field. A note explains that the subscription ID can be found in the admin workspace or invoice. Further down is a 'Full name' section with two input fields for 'First name' and 'Last name'. This is followed by a 'Work email' section with a single input field containing 'email@company.com'. At the bottom, there is a 'Why are you contacting us?' section with three radio button options: 'Problem' (selected), 'Question', and 'Feedback'.

Connect with us on github & social media



<https://github.com/passbolt>



<https://mastodon.social/@passbolt>



<https://www.linkedin.com/company/passbolt/>