passbolt

THIS DOCUMENT IS ARCHIVED IT IS REPLACED BY ANOTHER DOCUMENT:
https://docs.google.com/document/d/1gVpiU5ejVxgSmpWg6Tt0eZ_7s92RI7cfJhfiD_fiiDs/edit?usp=sharing

Password Rotation & Expiry

Requirements & specifications Part I

Abstract

This document describes a new feature that will be part of the version 3 of the software. It is aimed at stakeholders and passbolt staff to understand the goals and implementation details. The goal of the feature in a nutshell is to allow users to view which password should be changed as a consequence of offboarding users and/or set passwords as to be changed manually.

Status: ARCHIVED

Change history

Date	Author	Changes
03/03/2021	Remy	Initial version
13/03/2021	Remy	Finalize scope / first stories and wireframes
25/08/2021	Vivien	High fidelity wireframes

Index

Introduction

Password rotation is a controversial topic. One could argue that a blanket policy to rotate passwords every 60 days generally leads to poor password hygiene and/or places an additional burden on individuals and organizations alike. However it is still a requirement in many organizations that implement such policy, they see it as a way to reduce the window of opportunity for attackers in case of an undetected leak or basically just have to do it because of regulations.

Moreover there are some more clear legitimate cases for password rotation, mainly when a password was shared with a group of people and that the group composition has changed, typically when a user leaves a group or the organization. Or alternatively when a password is meant to be shared temporarily with someone (as a single use for example).

Included scope

The goal of this feature is to help support the use cases of password rotation as part of the off-boarding of users or when passwords are manually marked as expired, now or in the future.

In short this version includes:

- Setting and viewing expiry date on resource using the API.
- Setting and viewing expiry date on resource create / update dialog.
- Auto update of a resource expiry when a permission to a resource is removed (because of changes via a share, or via group membership, or when a user is deleted).
- Email notifications when a resource expires prompting owner to change and associated email notification settings and digests.

Excluded scope

This version of the functionality does not include:

- Setting expiry based on usage (ex. mark as expired if X accesses Y).
- Setting automatic expiry dates from administrators rotation policies.
- Reporting on the compliance of whether a given password rotation policy is met or not.
- Similarly it doesn't cater for the "share for a single time" use case.

All these different features will be part of a separate improvement, however the suggested design in this document aimed to take into account these requirements to enable them more easily in the future.

Functional specifications

High level requirements and Wireframes

Figma file:
https://www.figma.com/file/LbIziirnbUjSP4EWQMwky4/Password-Expiry?node-id=0%3A1

Resource dialog

When users create a new resource, in the create password dialog a new field named “Expires” is added.

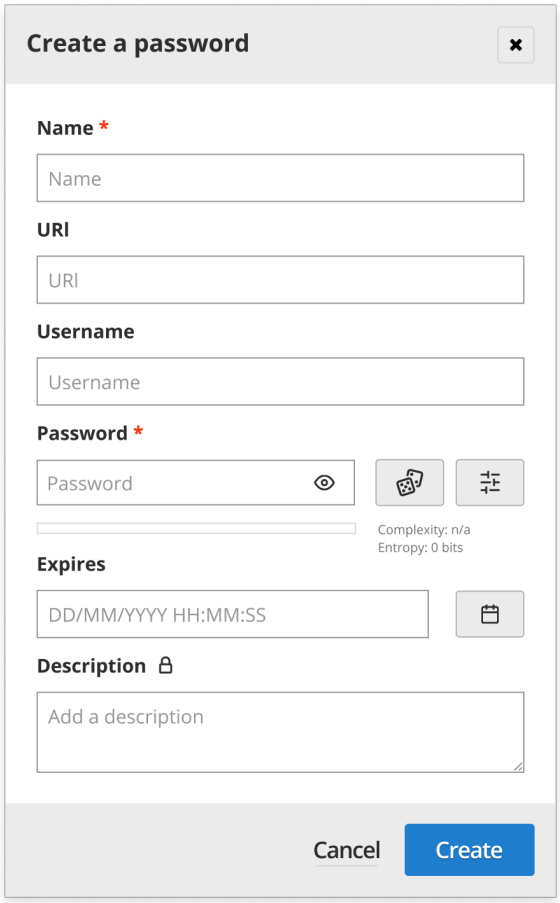

Fig. 1.0 Resource dialog with expiry date (source figma)

The placeholder depend on the policy selected by the administrator:

- Without a default password expiry period, the placeholder is “DD/MM/YYYY HH:MM:SS”

- With a default password expiry period set, the field is already filled with the selected policy

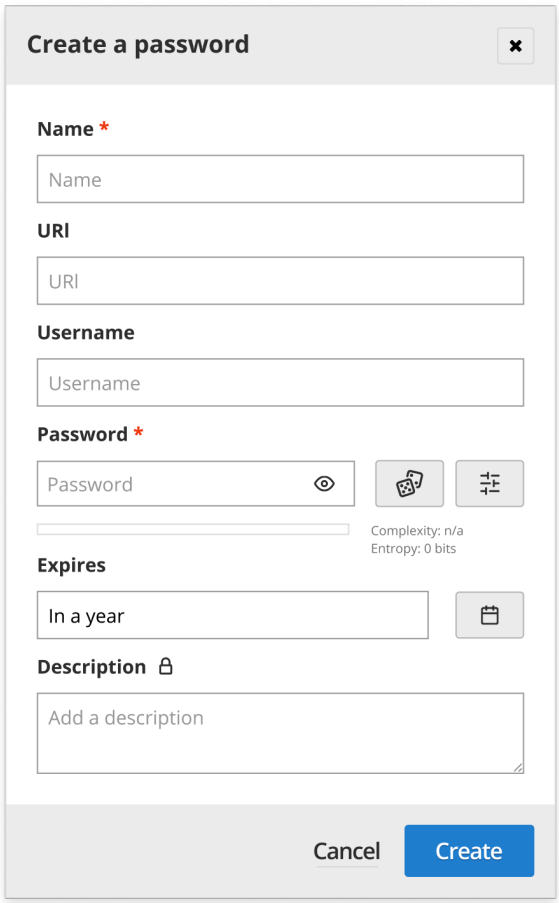

Fig. 1.1 Resource dialog with expiry date with policy (source figma)

When users click on the calendar button, a contextual menu shows a list of options.

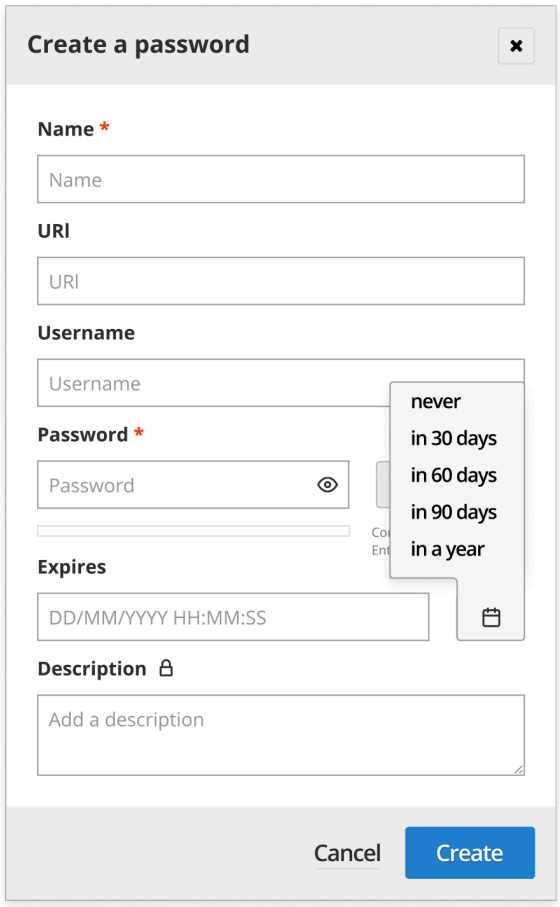

Fig. 1.2 Resource dialog with expiry menu (source figma)

When users edit a new resource with an expiry date due in less than a week, the colour of date in the field is set to @red.

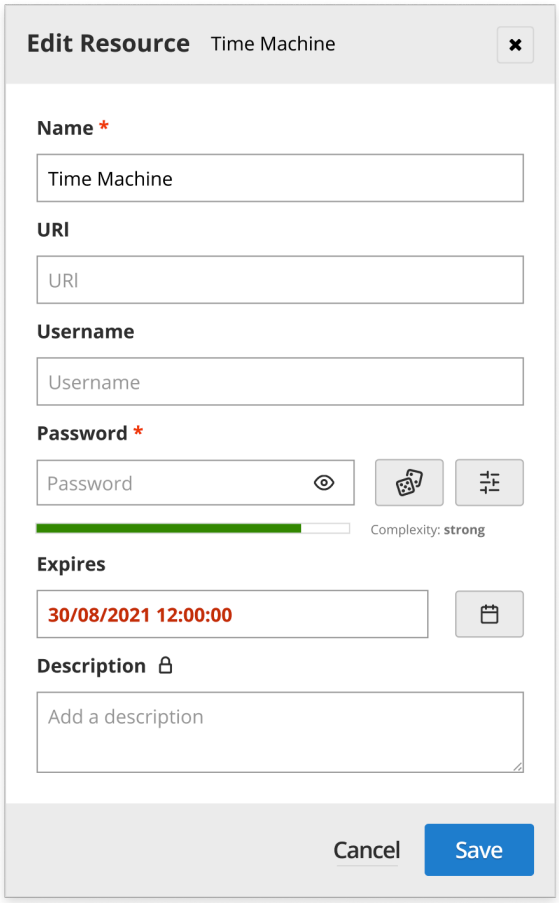

Fig. 1.3 Edit Resource dialog with expiry date (source figma)

Size issues options:

- Option 1. We reduce the overall size of all elements on all dialog by 10% on a smaller screen in order to produce more estate / prevent scroll without reducing usability.
- Option 2. Scroll inside the dialog so that create button is always visible (like on share permission lists)
- Option 3: scroll outside the dialog.

Quickaccess

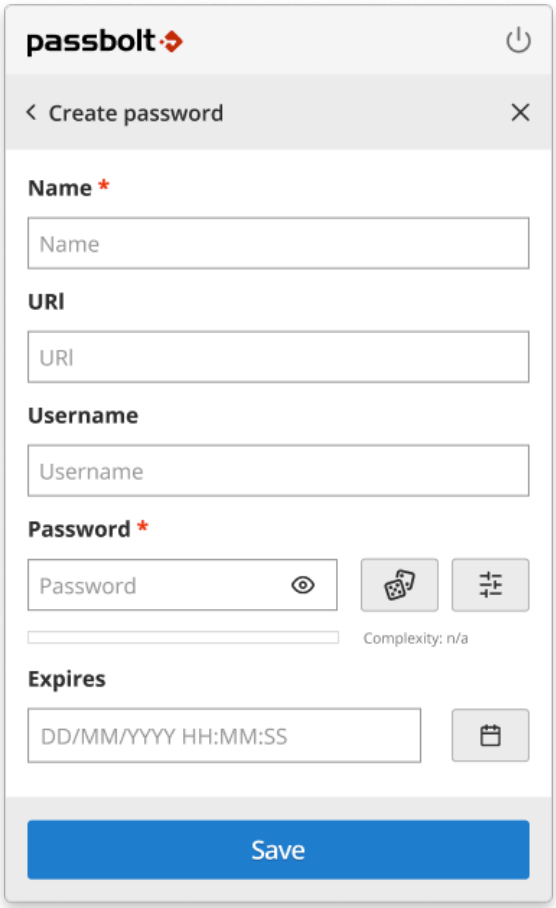

Fig. 5.0 Quick Access (source figma)

- Option1. for now we just don't include expiry as part of quick access? However we must apply the default expiry date if it is set as policy by admin.
- Option 2. Enable scrolling on quick access create in order to allow fitting expiry and description but below the fold. => consequence: must support encrypted description in quickaccess too.

Resource workspace

Users must be able to view the expiry time of each resource in the grid

Expired record dates for less than a week are shown with @red color, to put a visual emphasis that an action is needed.

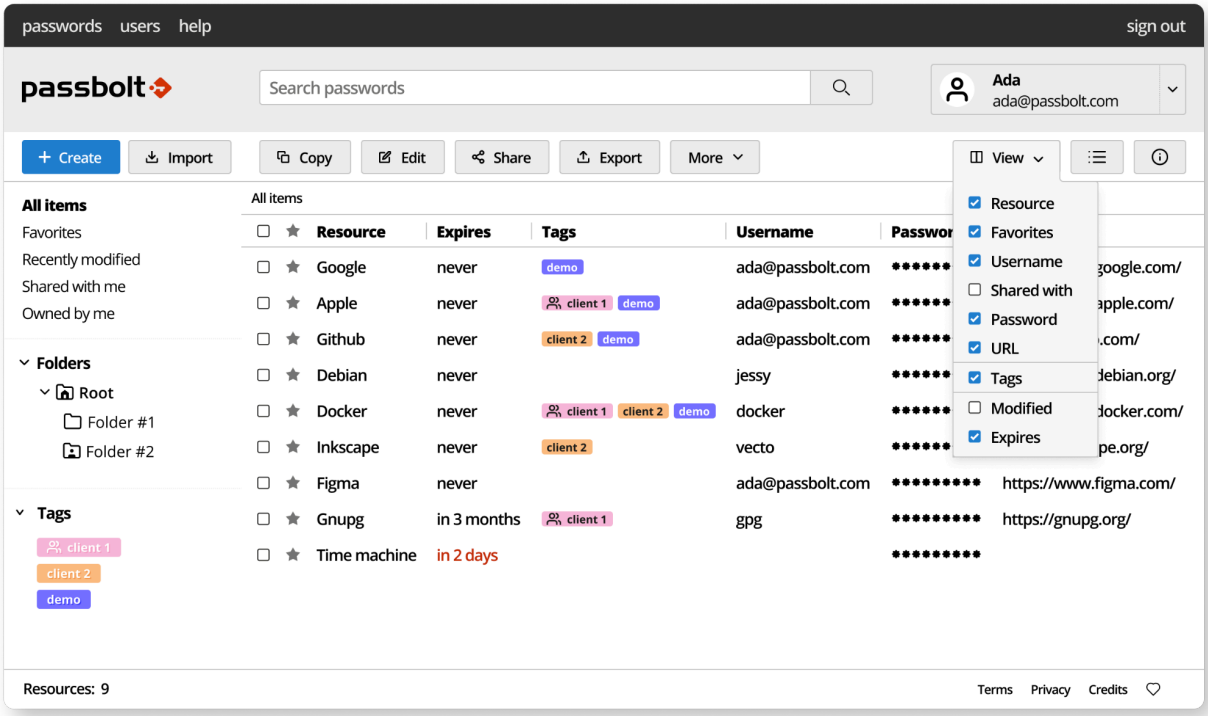

Fig. 2.0 Password workspace with expiry date (source figma)

Users can right click on a resource to reset the expiry date.

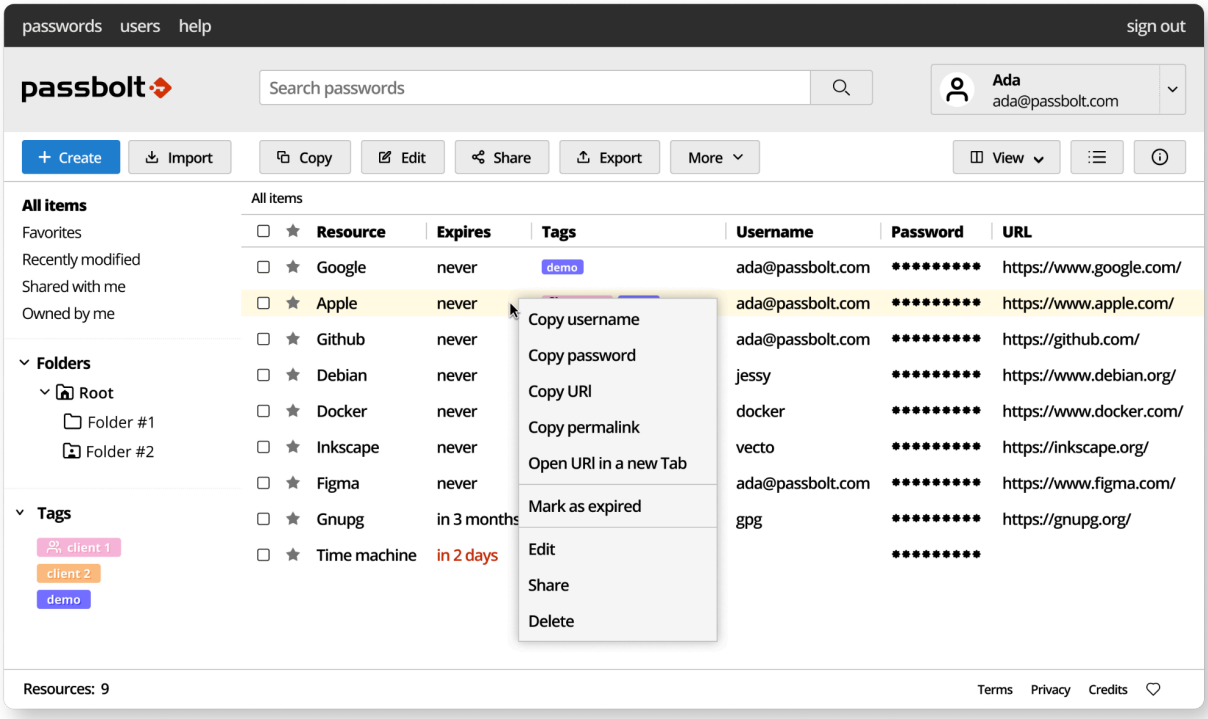

Fig. 2.2 Password workspace and contextual menu (source figma)

Users can right click on a resource to reset the expiry date.

Admin settings

Password policy

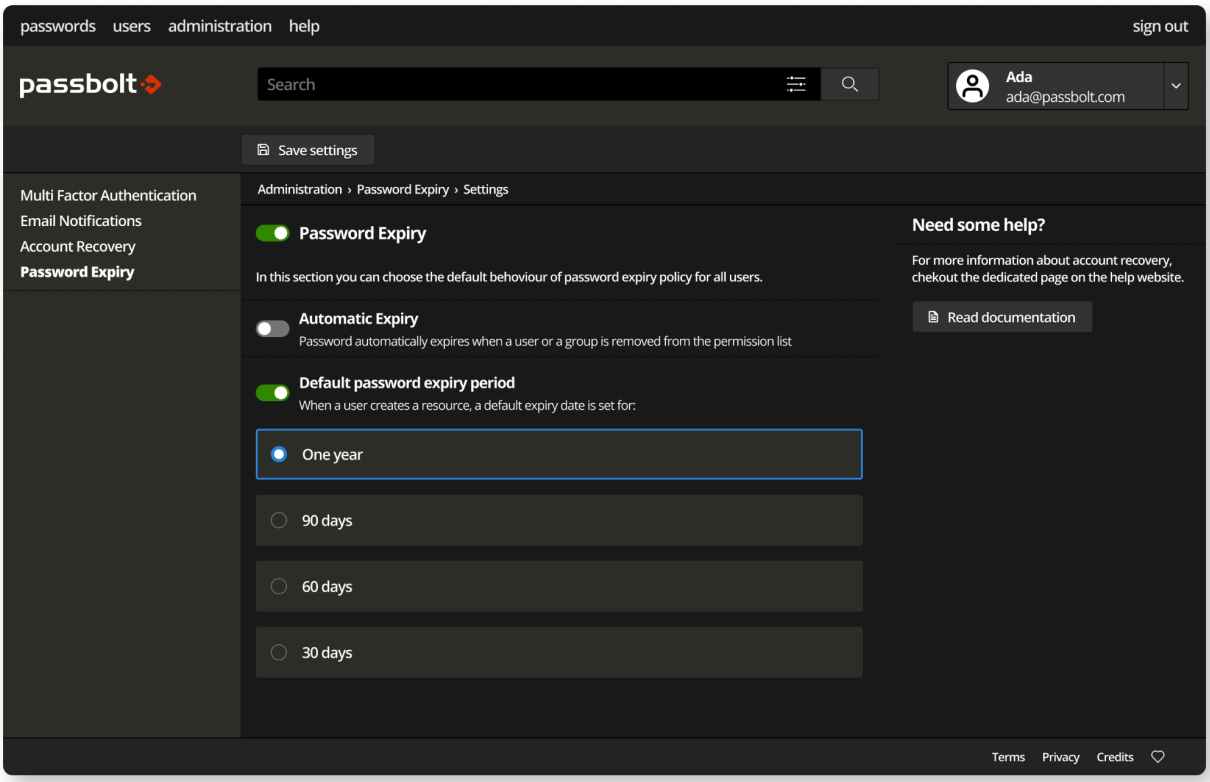

Fig. 3.1 - Admin Settings - Password Expiry (source figma)

In the administration workspace, A new “Password Expiry” section is available.

Password Expiry is by default disabled and it can be enabled via a toggle button.

In this section, an administrator can view the policy with two main options:

- “Automatic Expiry”, if toggled then Password automatically expires when a user or a group is removed from the permission list.

An owner of a password is notified via email when resources need to be changed.

- “Default password expiry period”, this is the default policy that fills the field described in Fig. 1.1 Resource dialog with expiry date with policy

A list of options is presented and the administrator can select the default period for the expiry date.

Notification settings

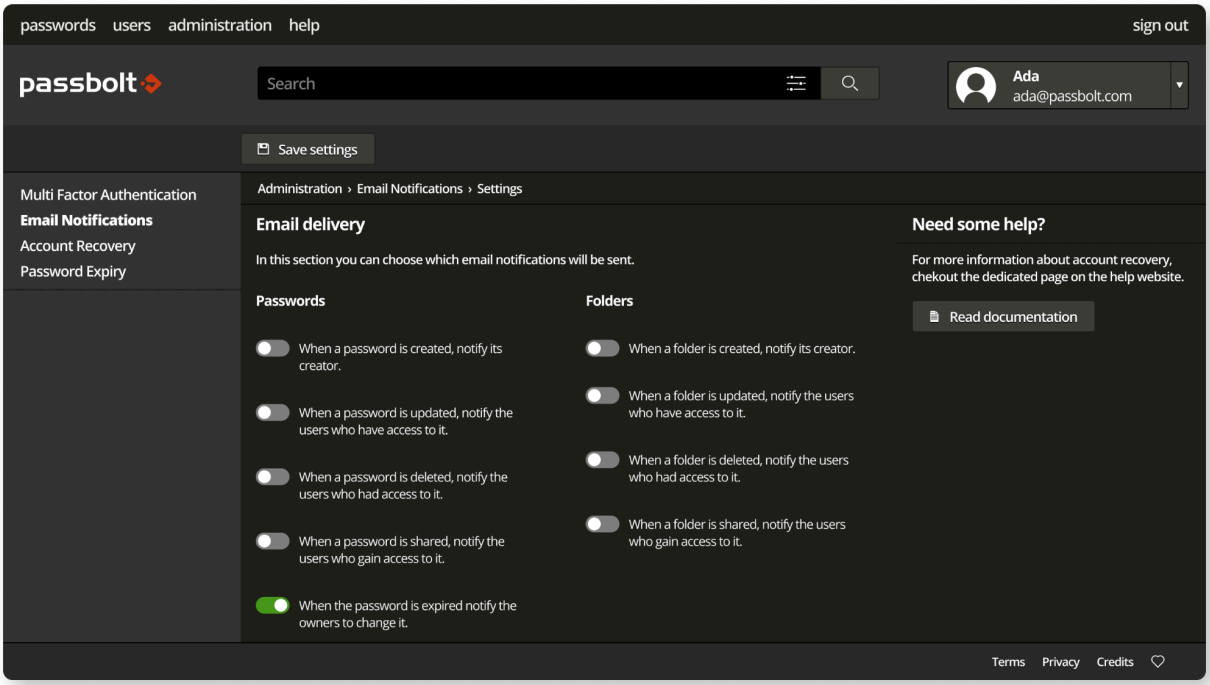

Fig. 3.2 - Admin Settings - Email notifications (source figma)

In the email Email notification section, a new option is available to notify the owners when a password has expired and they need to change it.

Email content

Single email

An owner of a password is notified via email when resources need to be changed.

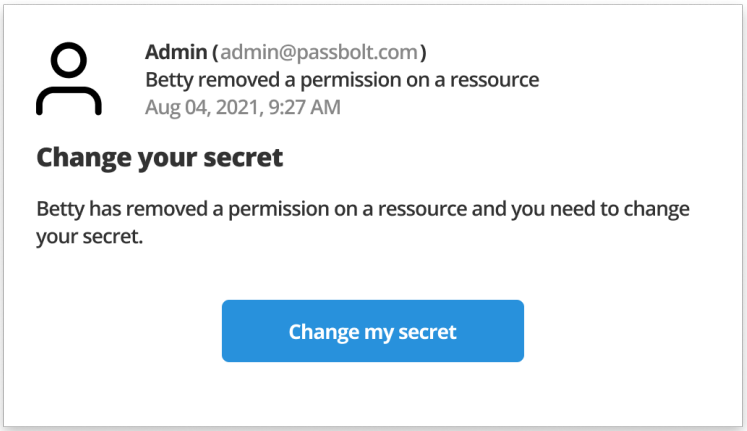

Fig. 4.1.1 Email notification (source figma)

When a resource expires in less than 48 hours, an email is sent to the users.

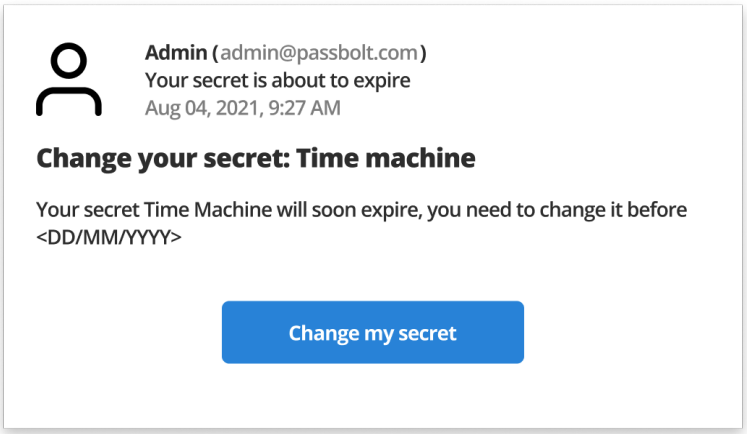

Fig. 4.1.2 Email notification (source figma)

Email digest

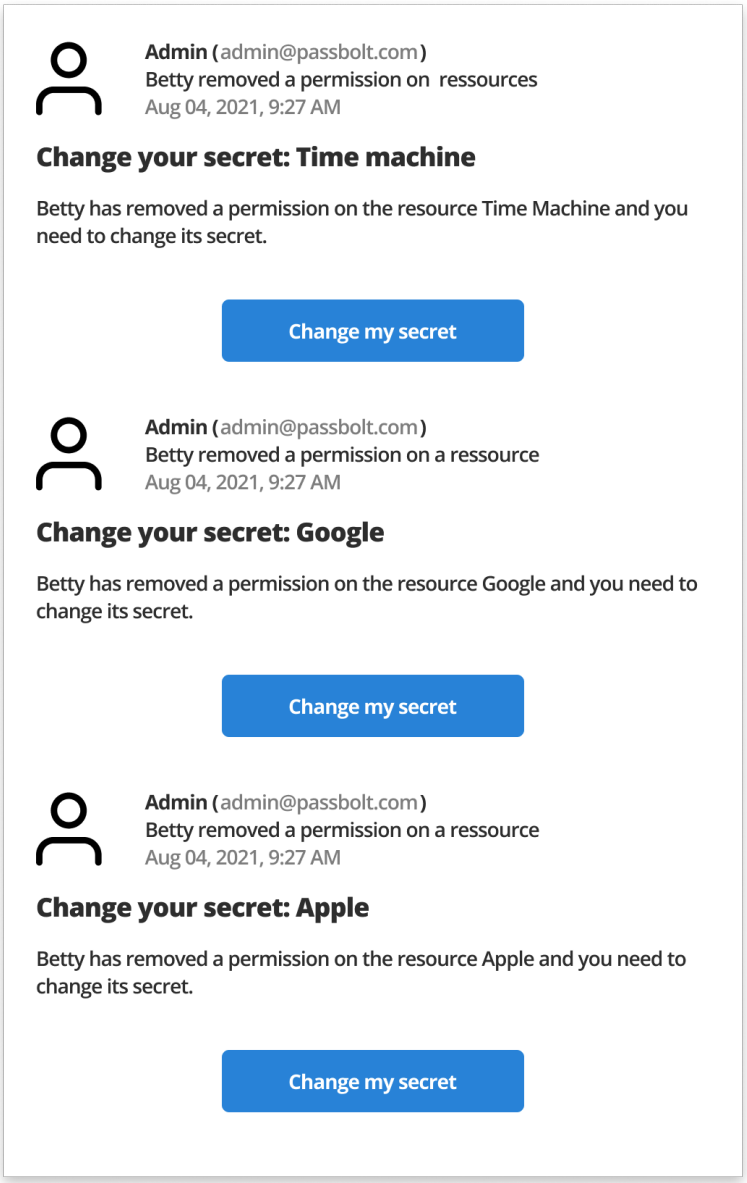

Fig. 4.2 Email digest (source figma)

User stories

Password create / edit dialog

As a logged in user I can optionally set the expiry date when creating a resource

```
Given I am a logged in user on the password workspace
And   I am on the create resource dialog
Then  I can see the option with label “Expires”
And   I can see a datetime input field
And   I can see a button to show preset dates
When  I click on the button to show preset dates
Then  I can see the multiple options such as “Next week” and “Next year”
When  I click on “Next year”
Then  I see the expiration date is set one year in the future
When  I set a title and password
And   I click save
Then  I can see a notification that the resource was saved
And   I can see the resource in the grid
```

Error message

```
Given I am a logged in user on the password workspace
And   I am on the create resource dialog
When  I enter an invalid expiry date
And   I press enter
Then  I can see an validation error
```

As a logged in user I can set the expiry date when editing a resource

```
Given I am a logged in user on the password workspace
And   I am editing a resource I own
When  I set an expiry date
And   I click save
Then  I can see a notification that the resource was edited
And   I can see the resource with the in the grid
```

Password expiry “auto” changes

As a resource owner when I remove the access of a user to a shared resource, the resource is marked as to be changed.

```
Given I am a logged in user on the password workspace
```

```
And   I am sharing a resource I own
When  I remove a user from the permission list
And   I click save
Then  I can see a notification that the resource was edited
And   I can see the resource is marked as expired
```

As a group manager when I remove a user from a group the resources the user had access to is now marked as to be changed.

```
Given I am a logged in user on the user workspace
And   I a group manager with shared resources
When  I remove a user from the group list
And   I click save
Then  I can see a notification that the group was edited
When  I go to the password workspace
Then  I can see the resources the group has access are marked as expired
```

As an administrator when I delete a user from the organization, the resources the user had access to are marked as to be changed.

```
Given I am a logged in administrator on the user workspace
When  I delete a user who has access to shared resources
Then  I can see a notification that the user was deleted
When  I go to the password workspace
Then  I can see the resources the user had access to are marked as expired
```

Password grid / workspace

As a user on the password workspace I can see in the grid which resources need to be changed, and sort them by expiry date.

```
Given I am a logged in user on the password workspace
And   resources I have access to resources that are expired
When  I look at the grid
And   I can see an “Expires” column with the date in friendly format
And   I see “Never” column of the resources that are not expired
When  I click on “Expires” column
Then  I see the resource sorted by expiration date ascending
When  I click on “Expires” column again
Then  I see the resource sorted by expiration date descending
```

As a user on the password workspace I see expiry info in the resource sidebar.

```
Given I am a logged in user on the password workspace
And   resources I have access to resources that are expired
When  I click on a resource
Then  I see the resource sidebar
And   I see the “Expires” with the date in friendly format
When  I click on a resource that is not expired
Then  I see the “Expires” set to “Never”
```

As a user on the password workspace I can filter the grid by expired resources.

```
Given I am a logged in user on the password workspace
And   resources I have access to resources that are expired
When  I click on the “Expired” filter on the left side
Then  I can see the grid filtered by resources that are expired
And   I can’t see the one that are not expired
```

Quickly/multi mark as expired/reset expiry

As a user on the password workspace I can mark one resource as expired using the contextual menu.

```
Given I am a logged in user on the password workspace
When  I select a resource that I can update that is not expired
And   I right click on the resource
Then  I can see the contextual menu
And   I see “Mark as expired” in the menu
When  I select “Mark as expired”
And   I see the “Expires” column in the grid set to “A few seconds ago”
And   I see the “Expires” in the resource sidebar set to “A few seconds ago”
```

As a user on the password workspace I can mark one or more resources as expired using the action menu.

```
Given I am a logged in user on the password workspace
When  I select multiple resources that I can update that is not expired
And   I click on the more button in the action bar
Then  I can see the “Mark as expired” option
When  I click on the “Mark as expired” option
And   I see the “Expires” date as been updated to “A few seconds ago”
```

As a user on the password workspace I can reset the expiration date date using the contextual menu.

```
Given I am a logged in user on the password workspace
When  I select a resource that that is expired
And   I right click on the resource
Then  I can see the contextual menu
And   I see “Reset expiry date” in the menu
When  I click “Reset expiry date”
And   I see the “Expires” column in the grid set to “Never”
And   I see in the activity log that I have edited the resource last
```

As a user on the password workspace I can mark one or more resources as to be changed using the action menu.

```
Given I am a logged in user on the password workspace
When  I select multiple resources that I can update that are expired
And   I click on the more button in the action bar
Then  I can see the “Reset expiry date” option
When  I click on the “Reset expiry date” option
And   I see the “Expires” date as been updated to “Never”
```

Import / Export

As a user on the password workspace I can import password expiry date from KDBX files.

```
Given I am a logged in user on the password workspace
And   I have a KDBX file with three resources one expired, one not expired
and one where the expiry date is not set
When  I import the KDBX file
Then  I can see the resource that is not expired in the grid
And   I can see the resource that is expired in the grid
And   I can see the resource that have expiry date not set in the grid
```

As a user on the password workspace I can import password expiry date from KDBX files.

```
Given I am a logged in user on the password workspace
And   I own three resources one expired, one not expired and one where the
expiry date is not set
When  I selected the resources
And   I export the resources as KDBX file
And   I open the file in Keepass
Then  I can see the resource that is not expired in the grid
And   I can see the resource that is expired in the grid
```

```
And   I can see the resource that have expiry date not set in the grid
```

Email notifications

As a user owner of a password, I'm notified when resources need to be changed.

```
Given I am a logged in user in my mail client
And   Another user removed a permission on a resource
And   email notification settings are enabled
Then  I can see an email notification
And   the email is prompting me to change the secret
And   there is a link to open passbolt
When  I click on the link
Then  I can see the edit dialog for this resource
```

As a user I can receive an email digest when several secrets need to be changed.

```
Given I am a logged in user in my mail client
And   Another user removed a permission on several resources
And   email notification settings are enabled
And   email digest is enabled
Then  I can see an email notification
And   the email is prompting me to change the multiple secret
And   there is a link to open passbolt
When  I click on the link
Then  I can see the password workspace filtered on "Expired"
```

As an administrator I can set if email notification on resource expiry

```
Given I am a logged in administrator on the administration workspace
When  I click on "Email notification" settings
Then  I see the "password" section a notification
And   I see the "When the password is expired notify the owners to change
it."
And   I see the email notification is on by default.
```

Administration settings

As an administrator I can set when automatic expiry is triggered

```
Given I am a logged in administrator on the administration workspace
When  I click on "Password policies" in the left side menu
Then  I see a page with a "Expiry policy" section
```

```
And   I see a toggle button “Password automatically expires when a user or a
group is removed from the permission list”.
And   the toggle button is on by default
When  I click on the toggle button
And   I click save
Then  I can see the settings have been saved
```

As an administrator I can set the default expiry period.

```
Given I am a logged in administrator on the administration workspace
When  I click on “Password policies” in the left side menu
Then  I see a page with a “Expiry policy” section
And   I see a “Default password expiry period” label
And   a radio list with multiple options such as “60 days” or “One year”
And   the radio list is set to “never” by default
When  I select “60 days”
And   I click save
Then  I can see a notification saying the settings have been save
When  I go to the user workspace
And   I create a password
Then  I can see the expiry date is set to 60 days.
```

Technical Specifications

Passbolt Server

Data model changes

We propose to introduce an additional field “expired” to the data model on resources.

Name	Type	Description
expires	Datetime | null	Date at which the resource secret is considered expired.

API Endpoints

Resources Read

Additionally to existing fields, the API will return the expiry date. Example:

```
{
  "header": {
    "id": "bc8a85a7-bde8-48d5-8749-827c9185db15",
    "status": "success",
    "servertime": 1554907370,
    "title": "app_resources_view_success",
    "action": "83bb8bd8-2006-5546-a3bb-9319ae6e8f9d",
    "message": "The operation was successful.",
    "url": "/resources/ecf0ed85-3bfc-5f45-b11d-74e9a86aa313.json",
    "code": 200
  },
  "body": {
    "id": "ecf0ed85-3bfc-5f45-b11d-74e9a86aa313",
    "name": "Grogle",
    "username": "gustave",
    "uri": "http://fr.groland.wikia.com/wiki/Grogle",
    "description": "",
    "created": "2019-04-04T12:05:58+00:00",
    "modified": "2019-04-08T09:16:09+00:00",
    "expires": "2020-04-08T09:16:09+00:00",
    "created_by": "f848277c-5398-58f8-a82a-72397af2d450",
    "modified_by": "f848277c-5398-58f8-a82a-72397af2d450"
  }
}
```

Resources Index

Same as for the read endpoint, the API will return the expiry date as part of the resource. Additionally we implement the following filters:

Param	Description	Required	Type
filter[is-expired]	Return only the resources where expired date <= now.	No	Boolean

Resources Create

The create endpoint will support passing the expiry date as a parameter. It is possible to both give an expiry date in the past and the future. This will allow supporting multiple use cases. For example:

```
POST /resources.json?api-version=v2
{
  "name": "<uuid>",
  "resource_type_id": "<uuid>",
  "expires": "<datetime>",
  "secrets": [...]
}
```

Example of request and response with validation issues:

```
POST /resources.json?api-version=v2
{
    "name": "test",
    "resource_type_id": "965c9f17-18ae-48fd-a36e-e42f04a30442",
    "expires": "not a date",
    "secrets": [...]
}

{
    "header": {
        "id": "965c9f17-18ae-48fd-a36e-e42f04a30442",
        "status": "error",
        "servertime": 1554907648,
        "title": "app_resources_add_error",
        "action": "ad8bbc35-6435-538e-b1a7-80b87bcedb6a",
        "message": "Could not validate resource data.",
        "url": "\/resources.json",
        "code": 400
    },
    "body": {
        "expired": {
            "_datetime": "A valid expiry date is required."
        }
```

```
    }
}
```

Resources Update

Similar to the resource create endpoint it is possible to update a resource with an expiry date.

Resources share

The share endpoint does not change per se. However additional server side treatments are added to make sure records are expired and email notifications are sent when someone is removed from the permission list.

Group update

Similarly additional server side treatments are added to make sure records are expired and email notifications are sent when someone is removed from a group, if that group had access to shared secrets that is.

User delete

Similarly additional server side treatments are added to make sure records are expired and email notifications are sent when someone is deleted from the organization.

Cakephp implementation

- Add feature flag to settings whitelist
- Add a migration to add a datetime expires field to the resource table, default null.
- Add resource index controller expired filter and order.
- Add resource find table/trait filter and order options.
- Add expired date logic when someone or a group is removed from a resource permission list (direct share, group membership, user delete).
- Add email notification when a resource is marked as expired.
- Add email digests when multiple resources are marked as expired.
- etc.

AppJS changes

- Add feature flag “canIUse” make sure it disabled when it’s not present or set to disabled (to allow easier cloud rollout)
- Add email notification setting
- Add new password policy section
- etc.

Passbolt WebExtension

Front end

- Add feature flag “canIUse” make sure it disabled when it’s not present or set to disabled (to allow easier cloud rollout)
- Update create / update resource dialog
- Update dialog page and unit tests
- Add column to grid
- Add muti-select actions
- Add
- etc.

Background page

- Add feature flag as part of settings
- Update resource entity
- Update resource entity unit tests
- etc.

Security considerations

Risk analysis

Residual risks:

- User can override expiry without actually changing password

White paper update needed.