

Admin Reports

Functional Specifications

Abstract

This document contains the functional specifications of the “admin reports” feature.

Diffusion: Public (CC BY-SA 3.0)

Status: DRAFT

Change log

When	Who	What
26/03/2020	Kevin	First draft of scope
26/03/2020	Remy	Quick review
05/04/2020	Kevin	Added report content for MFA onboarding report

Table of content

Introduction	3
Approach for reports implementation	3
Report list	4
Admin reports	4
User reports	6
Reports properties	7
Branding	7
Reports capabilities	7
Report types	7
Simple report	7
Combined report	7
Technical specifications	8
Prioritization	8
Reports content	9
MFA Onboarding report	9
Meta	9
Styleguide	10
Simple reports included	10
mfa-activated-users-count	10
mfa-activated-admins-count	11
mfa-non-activated-users-count	12
mfa-non-activated-users-list	13
Users Onboarding report	14
Meta	14
Styleguide	15
Simple reports included	15
activated-users-count	15
logged-in-once-users-count	16
never-activated-or-logged-in-users-count	17
non-activated-or-never-logged-in-users-list	18
Users login report	19
Meta	19
Styleguide	19
Simple reports included	20

users-login-daily-count	20
users-login-list	20
Technical note	21
Users churn report	21
Employee offboarding report	22
Meta	22
Styleguide	23
Simple reports included	24
user-resources-reach	24
user-resources-shared-with-count	24
user-resources-secrets-access-count	25
user-resources-personal-count	26
user-resources-secrets-access-list	26
user-resources-personal-list	27
user-groups-sole-manager-list	28
user-action-logs-list	29
Users passwords reach list report	30
Users resources personal	30
Shared resources secret last touches list	32
Overview report	33
Appendix1 : Competition analysis	34
Bitwarden	34
1Password	35
LastPass	37

Introduction

The goal of the feature is to provide administrators with reports about the credentials and activity inside their instance of passbolt. The aim of these reports is to provide a comprehensive overview of the health of a Passbolt instance and to inform the administrator(s) in case they need to take action.

Approach for reports implementation

The implementation will be done in 2 steps.

1. We will first focus on the admin reports

2. Then we will implement the individual users report

Report list

Admin reports

Name	Description
Overview report (Dashboard)	Inspired from 1Password reports: - User breakdown by status - Number of activated users - Number of inactive users (pending activation) - In recovery - Users that don't login (?)(future) - Deleted users - MFA enabled (?) - Item breakdown - Number of shared items - Number of private items - Number of groups - Number of devices (?)
Team reports	
Employee MFA onboarding report	List of all users who don't have 2FA enabled
Employee onboarding report	List of all users who have never activated their account, or never logged in
Employee churn report	List all users that don't use passbolt at least X times for Y duration.
Employee offboarding report	Report about - What passwords the employee had access to. - What passwords they solely own (and should be transferred)
Groups managers report	List of all the groups that do not have X administrators
Groups membership report	List all the groups and their membership composition
Group overview report	Number of: administrators, overall users, invited users, non-active users. Number of devices per user. Is 2FA enabled.

Users evolution report	Growth of all users / active users over time
Users log in report	List of all log-ins in the past month, with the device used.
Users activity report	List of all users activity logs for the past month (can be configurable later)
Usage reports	
Passwords reach reports	List of all users and the percentage of passwords reach they have. (Example: if there are 100 passwords in database, and I can access 10, I have 10% reach)
Solely owned passwords	Report about passwords that are solely owned by a user
Passwords quantity report	Number of passwords created and evolution over months
Shared Passwords activity report	List of all shared passwords activity logs over the past month (configurable)
Shared passwords last usage report	List of all shared passwords and the last time they have been used, ordered by last use for the past month (configurable)
Unused shared password report	List all shared password that have not been used since X time.
Shared password individual usage report	List of all shared passwords accessible by a given user, and the last time they have been used, ordered by last use.
Security reports	
Security overview report	Overview of security (inspired by lastpass). Risky items, with the number (and list) of concerned users. • Accounts not activated • Solely owned passwords • Inactive passwords • Weak passwords • Duplicate passwords • Exposed passwords • Insecure websites (non-https) • Data breached websites
Weak passwords report	List of all weak passwords, with their owner
Exposed passwords report	List of all exposed passwords and their owners

Re-used / duplicate passwords report	List of passwords that are used several times, with their owner.
Insecure websites report	List of all insecure websites (non https) with their owner
Data breach report	List of all websites with known data breaches
	Expired password / password that should be changed
	Password that don't respect the policy

User reports

These reports only concern a given user.

Name	Description
User overview report	Inspired from 1Password: • Groups the user belongs to • Number of items he owns • Number of items shared with him • Authorized devices • Recent activity
Security reports	
Weak passwords report	List of all weak passwords for the current user
Exposed passwords report	List of all exposed passwords for the current user
Re-used / duplicate passwords report	List of passwords that are used several times, with their owner.
Insecure websites report	List of all insecure websites (non https) with their owner
Data breach report	List of all websites with known data breaches

Reports properties

Branding

We believe it is important that the admins / users generating these reports feel a sense of ownership about them. When a report is printed and circulates in a company, having the company logo and name of the person who generated it would automatically give incentives to stakeholders to make it circulate.

In this purpose, each report should contain

- Name of the person who generated the report, email and date.
- Logo of the company (when white label feature will be available)

Reports capabilities

A user should be able to:

- Display a report on his screen
- Print a report (printer or pdf)

Report types

There will be 2 types of reports:

Simple report

A simple report is an atomic report. It contains a basic set of information, for instance:

- A count or a total
- A list of objects

The goal of a simple report is either:

- To be displayed individually as a widget (Could have)
- To be rendered individually as json (Must have)
- To be included in a combined report (Must have)

Combined report

A combined report is a collection of simple reports. It is the final result that a user will see in the UI.

The goal of a combined report is either:

- To be rendered as json (Must have)
- To be rendered in HTML (Must have)

Technical specifications

The technical specifications are available here:

<https://docs.google.com/document/d/1KE2wK6ENaqPOrMObsXMEtcHthGfdZKJyzi45za4GI8/e/dit?usp=sharing>

Prioritization

We will focus first on the reports that have the highest ROI in terms of value added for our users. Admin reports are the first priority.

Report name	Complexity (1- 5)	Release #
Overview report (Dashboard)	2	1
Team reports		
Employee MFA onboarding report	1	1
Employee onboarding report	1	1
Employee churn report	1	1
Employee offboarding report	1	1
Group manager report	1	
Group membership report	1	
Group overview report	2	
Users evolution report	2	
Users log in report	1	1
Users activity report	2	3
Usage reports		
Passwords ownerships report		

Solely owned passwords	1	
Passwords quantity report	2	
Shared Passwords activity report	2	
Shared passwords last usage report	1	2
Unused shared password report	1	2
Shared password individual usage report	3	2
Security reports		
Security overview report		
Weak passwords report	3	
Exposed passwords report	3	3
Re-used / duplicate passwords report	3	
Insecure websites report	2	3
Data breach report	2	

Reports content

MFA Onboarding report

Meta

Type	Combined
Name	Multi-factor authentication users onboarding
Status	Completed
Description	This report shows the onboarding metrics for multi-factor authentication in Passbolt, and the list of users who still have not activated MFA for their account.
Slug	mfa-users-onboarding
Route	/reports/mfa-users-onboarding
Route params	N/A

Filters	TBD
Contain	TBD
Sorts	TBD
Views	• Json • Html
Sub reports	• mfa-activated-users-count • mfa-activated-admins-count • mfa-non-activated-users-count • mfa-non-activated-users-list

Styleguide

HTML is defined in the style guide.

<https://gitlab.com/passbolt/passbolt-styleguide/-/tree/master/demo/reports>

Simple reports included

mfa-activated-users-count

Type	Simple
Name	MFA Activated Users Count
Status	Completed
Description	Provides the count of all Passbolt users that have activated MFA for their account.
Slug	mfa-activated-users-count
Route	/reports/mfa-activated-users-count
Route params	N/A
Filters	TBD
Contain	TBD
Sorts	TBD
Data	

	<pre>{ "mfa_activated_users_count": 10, "activated_users_count": 15, "data": { "status": "success", "percentage": "90", } }</pre>
Statuses	• 0 < 25%: fail • 25% > 75%: in-progress • 75% >= 100%: success
Visual representation	Type: Gauge (in percent) Text below the gauge: "Of the users have MFA configured"

mfa-activated-admins-count

Type	Simple
Name	MFA Activated Admins Count
Status	Completed
Description	Provides the count of all Passbolt admins that have activated MFA for their account.
Slug	mfa-activated-admins-count
Route	/reports/mfa-activated-admins-count
Route params	N/A
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre>{ "mfa_activated_admins_count": 10, "activated_admins_count": 15,</pre>

	<pre> { "data": { "status": "success", "percentage": "90", } } </pre>
Statuses	• 0 < 100%: fail • >= 100%: success
Visual representation	Type: Gauge (in percent) Text below the gauge: "Of the admins have MFA configured"

mfa-non-activated-users-count

Type	Simple
Name	MFA Non activated users count
Status	Completed
Description	This report provides the count of all Passbolt users that haven't activated MFA for their account
Slug	mfa-non-activated-users-count
Route	/reports/mfa-non-activated-users-count
Route params	N/A
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre> { "mfa_non_activated_users_count": 10, "activated_users_count": 15, "data": { "status": "success", "percentage": "90", } } </pre>

	<pre>}</pre>
Statuses	Same as for mfa-activated-users-count, but inverted. • 0 < 25%: success • 25% > 75%: in-progress • 75% >= 100%: fail
Visual representation	Type: Gauge (Integer) Text below the gauge: “Users need to configure MFA”

mfa-non-activated-users-list

Type	Simple
Name	MFA Non activated users list
Status	Completed
Description	Provides the list of all Passbolt users that haven't activated MFA for their account
Slug	mfa-non-activated-users-list
Route	/reports/mfa-non-activated-users-list
Route params	N/A
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre>{ "users": [<userEntity> <userEntity>] }</pre>

	Each user entity must include: • User object (with is_mfa_configured field) • Profile object
Visual representation	Type: Table list Columns • Name • Username • Active since (xx days / months ago) • MFA? (Yes or No) • Role (User or Admin)

Users Onboarding report

Meta

Type	Combined
Name	Users onboarding
Status	In progress (Json should be done / Html to complete)
Description	This report shows the list of all who have never activated their account, or never logged in
Slug	users-onboarding
Route	/reports/users-onboarding
Route params	N/A
Filters	TBD
Contain	TBD
Sorts	TBD
Views	• Json • Html
Sub reports	• activated-account-users-count • logged-in-once-users-count

- never-activated-or-logged-in-users-count
- non-activated-or-never-logged-in-users-list

[Styleguide](#)

TODO

Simple reports included

[activated-users-count](#)

Type	Simple
Name	Activated Users Count
Status	In progress
Description	Count of all users with activated accounts compared to the total count of users.
Slug	activated-users-count
Route	/reports/activated-users-count
Route params	N/A
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre>{ "account_activated_users_count": 10, "total_users_count": 15, "change_over_time": 15, "data": { "status": "success", "percentage": "90", } }</pre> Total_users_count means the total number of non deleted accounts.

Statuses	• 0 < 25%: fail • 25% > 75%: in-progress • 75% >= 100%: success
Visual representation	Type: Gauge (in percent) Text below the gauge: "Of the users Have activated their account"

logged-in-once-users-count

Type	Simple
Name	Logged In Once Users Count
Status	In progress
Description	This report provides the count of all users that logged in at least once, compared with the total number of users.
Slug	logged-in-once-users-count
Route	/reports/logged-in-once-users-count
Route params	N/A
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre>{ "logged_in_once_users_count": 10, "total_users_count": 15, "data" : { "status": "in-progress", "percentage": 10, }, }</pre> Total_users_count means the total number of non deleted accounts.
Statuses	• 0 < 25%: fail

	• 25% > 75%: in-progress • 75% >= 100%: success
Visual representation	Type: Gauge (in percent) Text below the gauge: “Of the users have logged in at least once”

never-activated-or-logged-in-users-count

Type	Simple
Name	Never Activated Or Logged In Users Count
Status	In progress
Description	This report provides the count of all users that never activated their account or never logged in.
Slug	never-activated-or-logged-in-users-count
Route	/reports/never-activated-or-logged-in-users-count
Route params	N/A
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre>{ "logged_in_once_users_count": 15, "total_users_count": 15, "data": { "status": "success", "percentage": "90", } }</pre> Total_users_count means the total number of non deleted accounts.
Statuses	• 0 < 25%: success • 25% > 75%: in-progress

	75% >= 100%: fail
Visual representation	Type: Gauge (in percent) Text below the gauge: “Users have never used Passbolt”

non-activated-or-never-logged-in-users-list

Type	Simple
Name	Never Activated Or Never Logged In Users List
Status	In progress
Description	This report provides the list of all the users who never activated their account or never logged in.
Slug	never-activated-or-logged-in-users-list
Route	/reports/never-activated-or-logged-in-users-list
Route params	N/A
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre> { "users": [<userEntity> <userEntity>] }</pre> Each user entity must include: - User object (with active and last_log_in field) - Profile object
Visual representation	Type: Table list

	Columns • Name • Username • Active since (xx days / months ago) • Last login? (date or Never) • Role (User or Admin)
--	---

Users login report

Meta

Type	Combined
Name	Users login report
Status	Review
Description	This report shows the list of all users logins over a period of time
Slug	users-login
Route	/reports/users-login
Route params	N/A
Filters	• Date from: one month ago • Date to: today These filters will later become configurable
Contain	TBD
Sorts	TBD
Views	• Json • Html
Sub reports	• users-login-daily-count • users-login-list

[Styleguide](#)

TODO

Simple reports included

users-login-daily-count

Type	Simple
Name	Users Login Daily Count
Status	Review
Description	This report provides the count of all daily logins over a period of time
Slug	users-login-daily-count
Route	/reports/users-login-daily-count
Route params	N/A
Filters	TBD
Contain	TBD
Sorts	N/A
Data	<pre>{ "2019-10-01": 10, "2019-10-02": 15, }</pre>
Visual representation	Type: Line Chart Chart title: Users login evolution

users-login-list

Type	Simple
Name	Users Login List
Status	Review
Description	This report provides the list of all users logins over a period of time
Slug	users-login-list

Route	/reports/users-login-list
Route params	N/A
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre>{ "action_logs": [<ActionLog> (with user object and profile), <ActionLog>] }</pre> ordered by created desc
Visual representation	Type: Table list Columns • Name • Username • Role (User or Admin) • Date

Technical note

It is currently not possible to know who logged in successfully from action_logs. For this report, we will need to fix this limitation.

We decided that the best technical approach to fix this is to add the user_id in the UserAction singleton after the login is successful.

Users churn report

Type	Simple
------	--------

Name	User resources Secrets Access
Status	In progress - Sort, filters and pagination missing
Description	This report provides the list of all the resources the user accessed the secret after modification
Slug	users-churn-list
Route	/reports/users-churn-list
Route Params	N/A
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre>[<UserEntity>, <UserEntity>, ...]</pre>
Visual representation	Type: Table list Columns: • Avatar • First name • Last name • Modified • Last logged in

Employee offboarding report

This report is user-dependent. It can only be displayed after selecting a user in the filters.

Meta

Type	Combined
Name	Employee offboarding report
Status	In progress - Sort, filters and pagination missing. Action log report

	missing
Description	This report gives important information to help with an employee offboarding such as • The resources reach percentage • The count of resources shared with the user • The count of resources secrets the user accessed since last rotation • The count of personal resources • The list of all the resources the user accessed the secret since last rotation • The list of personal resources • The list of groups the user is sole manager • The actions the user had done
Slug	employee-offboarding
Route	/reports/employee-offboarding/<USER_ID>
Route Params	• USER_ID: The target user to generate the report for
Filters	TBD
Contain	TBD
Sorts	TBD
Views	• Json • Html
Contain	• user: The target user the report has been generated for
Sub reports	• user-resources-reach • user-resources-shared-with-count • user-resources-secrets-access-count • user-resources-personal-count • user-resources-secrets-access-list • user-resources-personal-list • user-groups-sole-manager-list • user-action-logs-list

Styleguide

TODO

Simple reports included

user-resources-reach

Type	Simple
Name	User resources reach
Status	Done
Description	This report provides the resources reach of a user
Slug	user-resources-reach
Route	/reports/user-resources-reach/<USER_ID>
Route Params	• USER_ID: The target user to generate the report for
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre>{ "count": <integer> }</pre>
Visual representation	Type: Gauge Text: Resources shared with “user name”

user-resources-shared-with-count

Type	Simple
Name	User resources shared with count
Status	Done
Description	This report provides the count of resources that are shared with a user
Slug	user-resources-shared-with-count
Route	/reports/user-resources-shared-with-count/<USER_ID>

Route Params	USER_ID: The target user to generate the report for
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre>{ "count": <integer> }</pre>
Visual representation	Type: Gauge Text: Passwords shared with “user name”

user-resources-secrets-access-count

Type	Simple
Name	User resources secrets access count
Status	Done
Description	This report provides the number of secrets a user accessed
Slug	user-resources-secrets-access-count
Route	/reports/user-resources-secrets-access-count/<USER_ID>
Route Params	USER_ID: The target user to generate the report for
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre>{ "count": <integer> }</pre>
Visual	Type: Gauge

representation	Text: Accessed resources
----------------	--------------------------

user-resources-personal-count

Type	Simple
Name	User resources personal count
Status	Done
Description	This report provides the number of resources a user didn't share
Slug	user-resources-personal-count
Route	/reports/user-resources-personal-count/<USER_ID>
Route Params	USER_ID: The target user to generate the report for
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre>{ "count": <integer> }</pre>
Visual representation	Type: Gauge Text: Personal resources

user-resources-secrets-access-list

Type	Simple
Name	User resources Secrets Access
Status	In progress - Sort, filters and pagination missing
Description	This report provides the list of all the resources the user accessed the secret after modification
Slug	user-resources-secrets-access-list

Route	/reports/user-resources-secrets-access-list/<USER_ID>
Route Params	• USER_ID: The target user to generate the report for
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre>[{ "resource": <ResourceEntity>, "accessed": <Date>, }, ...]</pre>
Visual representation	Type: Table list Columns: • Name • Username • Uri • Modified • Personal • Accessed

user-resources-personal-list

Type	Simple
Name	User resources personal
Status	In progress - Sort, filters and pagination missing
Description	This report provides the list of resources a user didn't share
Slug	user-resources-personal-list
Route	/reports/user-resources-personal-list/<USER_ID>
Route Params	• USER_ID: The target user to generate the report for
Filters	TBD

Contain	TBD
Sorts	TBD
Data	<pre>[<ResourceEntity>, <ResourceEntity>,]</pre>
Visual representation	Type: Table list Columns: • Name • Username • Uri • Modified

user-groups-sole-manager-list

Type	Simple
Name	User groups sole manager list
Status	In progress - Sort, filters and pagination missing
Description	This report provides the list of groups a user is sole manager but not the sole member
Slug	user-groups-sole-manager-list
Route	/reports/user-groups-sole-manager-list/<USER_ID>
Route Params	• USER_ID: The target user to generate the report for
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre>[{ "group": <GroupEntity>, "members_count": <integer>, }]</pre>

	<pre> }, ...] </pre>
Visual representation	Type: Table list Columns: • Name • Members count • Modified

user-action-logs-list

Type	Simple
Name	User action logs
Status	Todo
Description	This report provides the list of action logs for a user
Slug	user-action-logs-list
Route	/reports/user-action-logs-list/<USER_ID>
Route Params	• USER_ID: The target user to generate the report for
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre> [<ActionLogEntity>, <ActionLogEntity>, ...] </pre>
Visual representation	Type: Table list Columns: • TBD

Users passwords reach list report

Type	Simple
Name	Users resources reach list
Status	In progress - Sort, filters and pagination missing
Description	This report provides the list of users resources reach
Slug	users-resources-reach-list
Route	/reports/users-resources-reach-list
Route Params	N/A
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre>[{ "user": <UserEntity> "reach": <float> }]</pre> ordered by reach desc
Visual representation	Type: Table list Columns • Name • Username • Role (User or Admin) • Reach

Users resources personal

Type	Simple
------	--------

Name	Users resources personal
Status	In progress - Sort, filters and pagination missing
Description	This report provides the list of resources all users didn't share
Slug	users-resources-personal-list
Route	/reports/users-resources-personal-list/<USER_ID>
Route Params	USER_ID: The target user to generate the report for
Filters	TBD
Contain	TBD
Sorts	TBD
Data	<pre> { "resources": [<ResourceEntity>, <ResourceEntity>, ...], "users": [<UserEntity>, <UserEntity> ...] "users_resources": [{ "user_id": <UUID>, "resource_id": <UUID>, }, { "user_id": <UUID>, "resource_id": <UUID>, }, ...] }</pre>
Visual representation	Type: Table list Columns: - Name - Username - Uri

	• Modified • User name • User role
--	--

Shared resources secret last touches list

Type	Simple
Name	Shared resources secret last touches list
Status	In progress - Sort, filters and pagination missing
Description	This report provides the list of all the resources secret last touches. When and what was the last operation that manipulated them.
Slug	shared-resources-secrets-last-access-list
Route	/reports/shared-resources-secrets-last-access-list
Route Params	N/A
Filters	TBD
Contain	• user: to get the user who perform the associated operation • user.profile: to get the user profile • resource: to get the resource • action_log: to get the action log associated to the operation
Sorts	TBD
Data	<pre>[<ResourceSecretTouchDto>, <ResourceSecretTouchDto>, ...]</pre>
Visual representation	Type: Table list Columns: • Name • Username • Uri • User full name • Last touch • Touch context (Resource create, secret update, share ...)

Overview report

TODO

Appendix1 : Competition analysis

Bitwarden

See all screenshots there: <https://bitwarden.com/blog/post/vault-health-reports-released/>

TOOLS

- Password Generator
- Import Data
- Export Vault

REPORTS

- Exposed Passwords Report**
- Reused Passwords Report
- Weak Passwords Report
- Unsecured Websites Report
- Inactive 2FA Report
- Data Breach Report

Exposed Passwords Report

Exposed passwords are passwords that have been uncovered in known data breaches that were released publicly or sold on the dark web by hackers.

[Check Exposed Passwords](#)

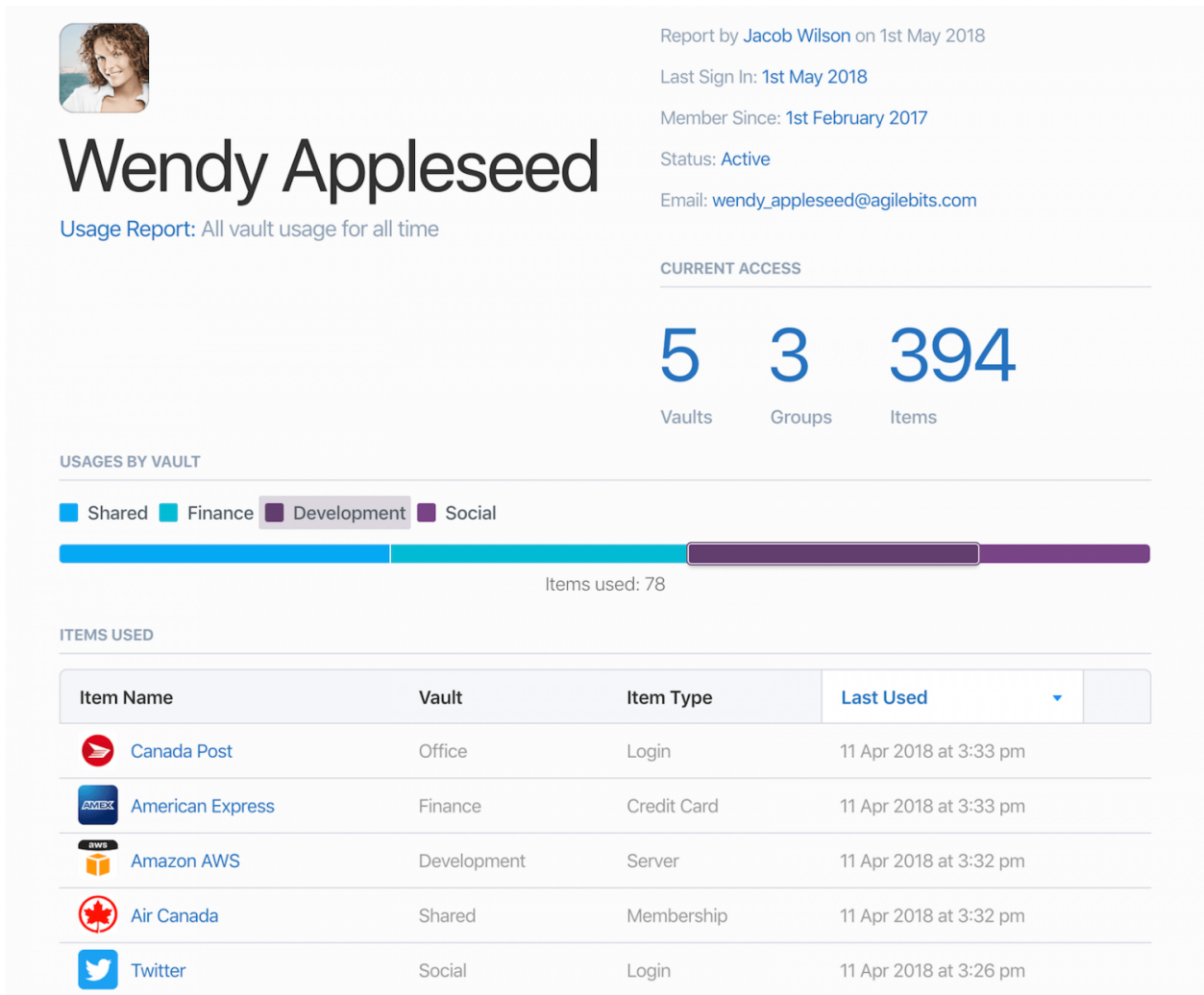
⚠️ EXPOSED PASSWORDS FOUND

We found 7 items in your vault that have passwords that were exposed in known data breaches. You should change them to use a new password.

Website	Username	Exposed Times
fidelity.com	john.smith	Exposed 557 time(s)
dashboard.stripe.com	testuser	Exposed 22,390,492 time(s)
codepen.io	testuser	Exposed 37,768 time(s)
schwab.com	jsmith	Exposed 8,409 time(s)
Facebook	hello@bitwarden.com	Exposed 925 time(s)
eBay	john.smith	Exposed 925 time(s)
EverBank	john.smith	Exposed 925 time(s)

Fig. Exposed passwords reports in Bitwarden

1Password



User Usage report



Business Tools

Vault Report: everyone's usage for the last 3 months

Report by [Khad Young](#) on January 17, 2020

Created: [June 12, 2018](#)

Last Updated: [January 16, 2020](#)

CURRENT ACCESS

13

People

3

Groups

ITEMS USED

Item Name	Item Type	Last Used	Used by
 Citrix	Login	2020-01-16 at 5:36:51 PM	 Khad Young
 DigitalOcean	Login	2019-11-20 at 8:47:06 PM	 Khad Young
 Zoom	Login	2019-11-15 at 3:03:48 PM	 Rob Hanslip

Vault report

PEOPLE

Active	36	Invitations	1
Suspended	0	Pending Confirmation	0
Guests	0	In Recovery	0

ITEMS AND VAULTS

Private Items	284	Private Vaults	65
Shared Items	153	Shared Vaults	12

GROUPS AND DEVICES

Groups	9	Secure Files	4
Devices	163	Storage Used	370 KB

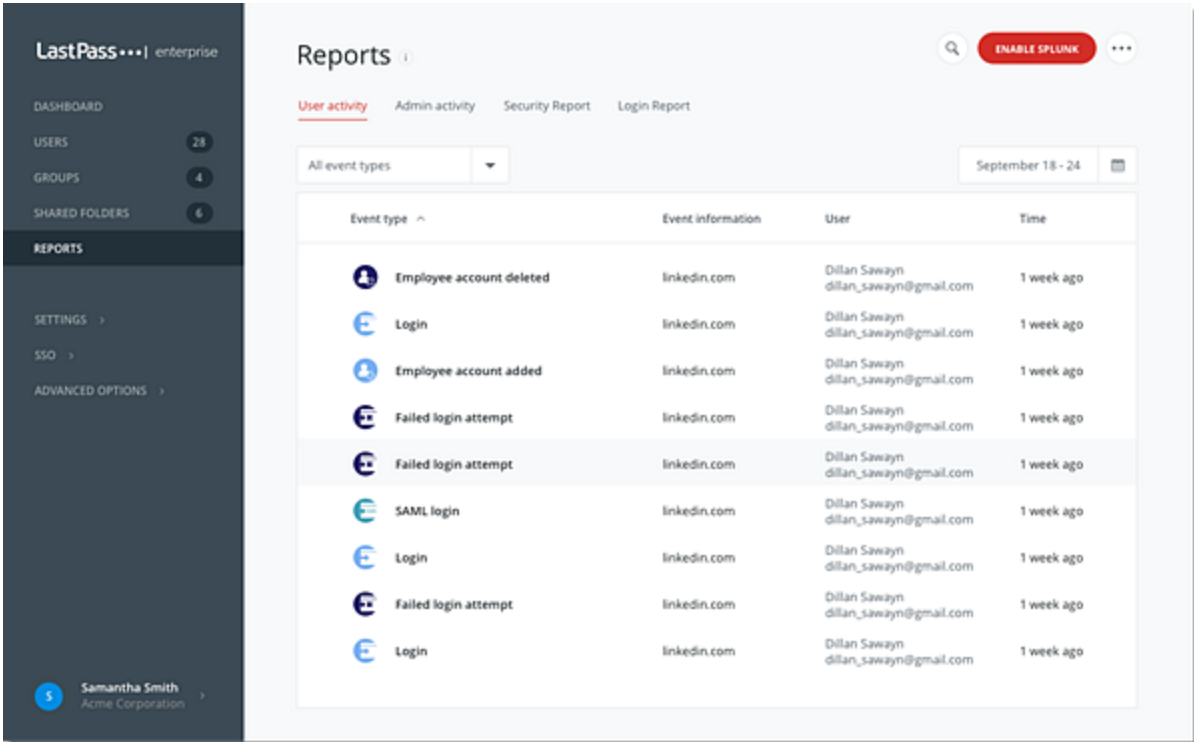
SECURE FILE STORAGE

Usage overview report

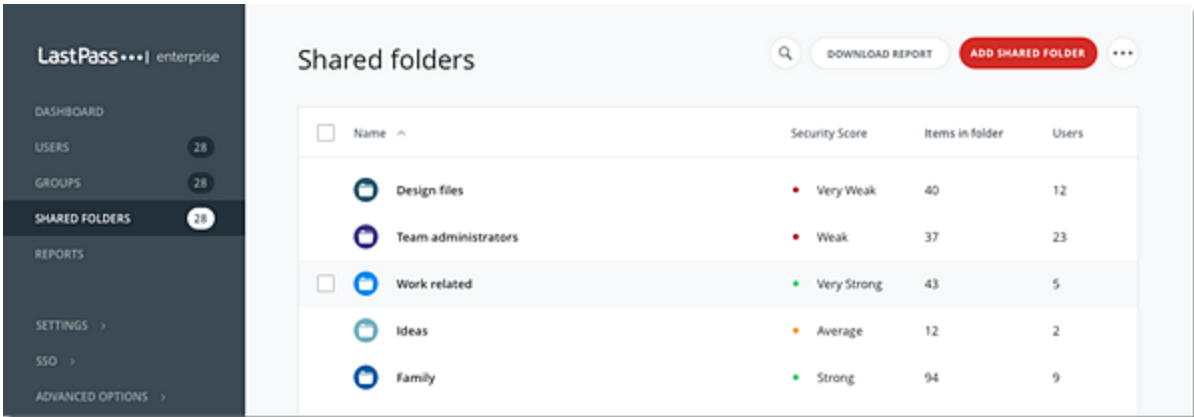
LastPass

Blog article with screenshots can be found here:
<https://blog.lastpass.com/2017/02/enhanced-reporting-features-for-lastpass-enterprise-admins.html/>

Overview



Reports dashboard



Shared folders report

LastPass... enterprise

DASHBOARD

USERS28

GROUPS28

SHARED FOLDERS28

REPORTS

SETTINGS

SSO

ADVANCED OPTIONS

Reports

User activity

Admin activity

Security Report

Risk name

Invitation not accepted

Account not activated

No sharing key

Inactive

Number of sites

No linked account

Weak Master Password

Reused Master Password

Weak security challenge

Weak passwords

Average password strength

Duplicate passwords

Duplicate password sites

Low number of Form Fill Profiles

Shows users who have less than 1 Form Fill Profile in their vault. To set up an automated email for this list, please go to the email notifications area in the Admin Console settings.

Export report

Set 'X' value (the value in the description above)

Users affected

D

Dillan Sawayn

dillan_sawayn@gmail.com

E

Emanuel Brakus

emmanuel_brakus@yahoo.com

G

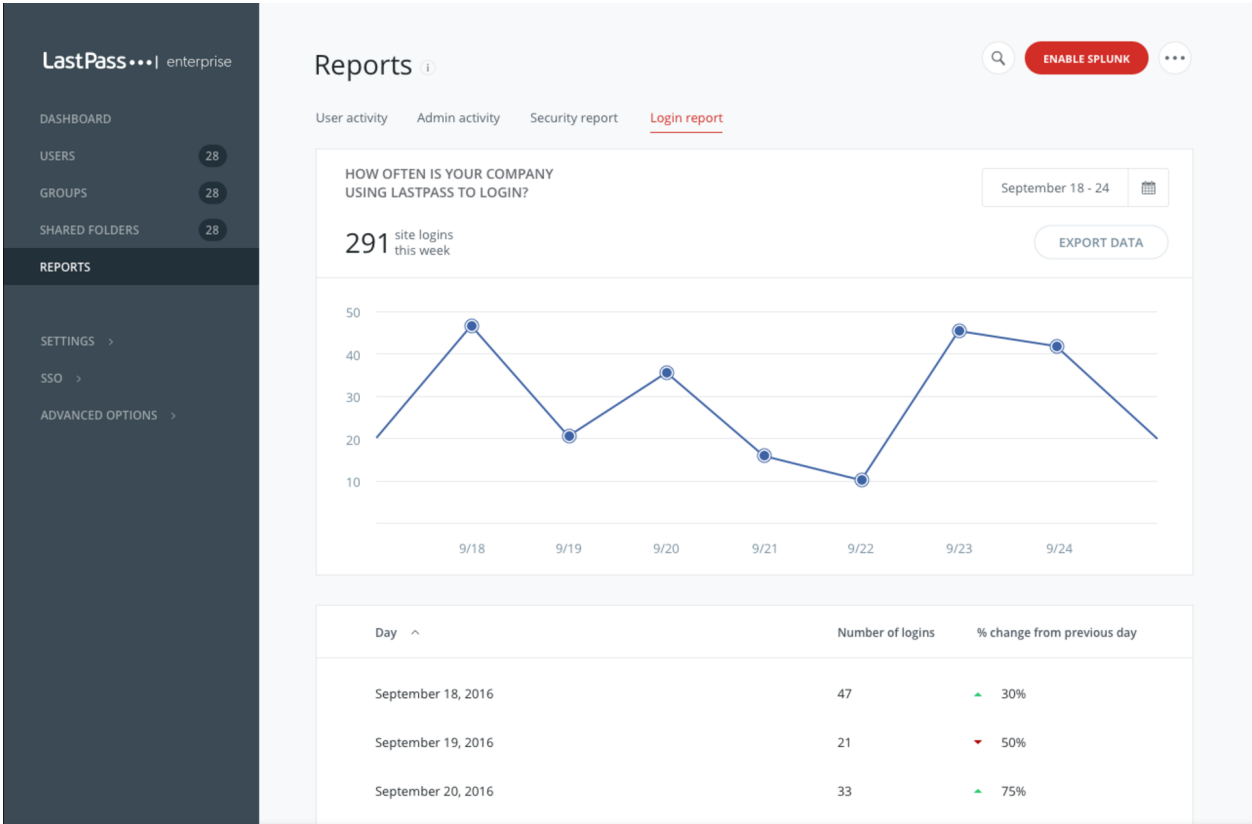
Goodwin Hassie

goodwin_hassie@gmail.com

Security report

PUBLIC

39/40



Login report