

Analysis Notes

[Test Environments](#)

[Notes](#)

[LastPass](#)

[1Pass](#)

[DashLane](#)

[Roboform](#)

[Chrome](#)

[Internet Explorer](#)

[Edge](#)

[Safari](#)

[Opera](#)

[Firefox](#)

[Bitwarden](#)

[KeePassX](#)

[KeePassXC](#)

Test Environments

Ubuntu 18.04.1 LTS

macOS Mojave Version 10.14

Windows 10 Education 17134.590

Notes

Obeys Autofill

LastPass - no

Dashlane - no

1Password - will after user interaction (as always)

RoboForm - will after user interaction (as always)

Bitwarden - yes if autofill enabled (or after interaction)

KeePass X - n/a

KeePass XC - will after user interaction (or if autofill enabled)

Chrome - no

Safari - with user interaction

Opera - no

Firefox - no

IE - no

Edge - no

Chrome

Interaction never required

http: default

https broken cert: disabled

Same Origin: default

Same Origin Hidden: disabled

Cross Origin: user interaction

Cross Origin Hidden: disabled

Invisible Login Form: default

Firefox

Interaction never required

Same Origin: Default

http: Default
https broken cert: Default
Same Origin Hidden: Default
Cross Origin: Default
Cross Origin Hidden: Default
Invisible Login: Default

Opera

Interaction never required
http: default
https broken cert: disabled
Same Origin: default
Same Origin Hidden: disabled
Cross Origin: user interaction
Cross Origin Hidden: disabled
Invisible Login Form: default

Edge

Interaction never required
http: user interaction
https broken cert: user interaction
Same Origin: default
Same Origin Hidden: default
Cross Origin: user interaction
Cross Origin Hidden: disabled (fills in user e-mail, but not pword)
Invisible Login Form: default

IE

Interaction never required
http: user interaction
https broken cert: user interaction
Same Origin: default
Same Origin Hidden: default
Cross Origin: user interaction
Cross Origin Hidden: disabled
Invisible Login Form: default

IE

Interaction never required

http: user interaction
https broken cert: user interaction
Same Origin: default
Same Origin Hidden: default
Cross Origin: user interaction
Cross Origin Hidden: disabled
Invisible Login Form: default

Remember E-mail

Bitwarden - default yes, didn't find option
Dashlane - default yes, didn't find option
RoboForm - default yes, didn't find option
LastPass - default yes, can toggle
1Password - default yes, didn't find option - only one that does not display your e-mail until you log in

System

Extensions

LastPass
Dashlane
OnePassword
RoboForm
KeePass XC

Thick apps (no autofill)

KeePass X
KeePass XC

Browsers

Chrome
Safari
Opera
Firefox
IE
Edge

Overview

1. Default settings / options / features
2. Cost? Different tiers?
3. One time passwords?
4. Security model
 - a. 2FA support
5. Subdomain behavior / passwords shared across domains

6. Security assessment tool
7. Cost
8. no external resources should be loaded from any third-party domains - third party content is a potential avenue for malicious actors - subresource integrity enforcement (<https://www.ctrl.blog/entry/migrating-to-bitwarden>)
9. Change mp to see if values change
10. Is it open source? DB location different operating systems?
11. Requirements for MP?
12. Clear clipboard? (browsers generally do not offer option to copy password - just to fill)
13. Auto-update passwords???
14. Cross-platform?
15. Check for software updates how often? Is it automatic?

Entropy / Password Generation

1. Calculate Score with Ur's tool and zxcvbn
2. Shannon entropy
3. Report basic statistics of letter frequencies
 - a. What are the character sets used
4. Get data for length 8, 12 and 20
5. Default configuration - options for modifying
6. Cronjob to clear /tmp after killing python/firefox processes - then relaunch (should relaunch on its own) - every 6-12 hours should do the trick
7. How do various password options influence entropy? (such as don't use lookalike characters or make human readable)

Databases

1. Any plaintext? Is everything encrypted?
2. Who can download? Any weaknesses?
3. What about metadata?

Autofill

1. Still vulnerable to hidden i-Frames?
2. Does it require user input by default? Configurable?
3. Behavior in presence of HTTP / HTTPS / Broken HTTPS
4. Iframe with login page on a different page of the same website that is vulnerable (same origin)
5. Iframes of other websites on landing page that is http rather than https
6. Login form with display: none;

LastPass

LastPass Premium is \$24 per year - \$26.22 with tax

\$48 for family 6 (you included)

Teams - \$48 per user per year / Enterprise - \$72 per user per year

Overview

Remembers email by default, but not password (why is remember password even an option?)

Uses 'Security Challenge' to encourage users to practice good password habits - enter your MP and it provides security score, percentile within LP and MP score as well as suggesting which passwords to strengthen. Provides detailed statistics of when passwords were last changed and their strength. Has option to check if any emails compromised in security breaches:

Want to know if your email addresses were leaked in known security breaches?[Check now.](#)

'Emergency Access' rights to trusted people so that they can request your vault in case of emergency - you set a time delay before they are sent the data and can revoke privileges

Multifactor not enabled by default

- Free version only allows one time code generators like Google Authenticator
- Premium includes YubiKey, fingerprint, smartcard,
- Enterprise includes salesforce

One time password - can generate one time passwords to login from public spaces if worried about keyloggers / shoulder surfing

Secure notes - can store notes / documents in a secure fashion

Sharing Center - can securely share specific notes / documents with other users

Trusted Devices - don't need to use multifactor authentication for 30 days

Mobile Devices - control what smartphones / tablets have access - tracks via UUID

Never URLs - add specific sites that LastPass should never function on

Equivalent domains - same password multiple domains can indicate that fact

URL limit - limit what urls are shown when attempting to login

Identities - create subvaults under each identity so that only items for current identity will be used



















History gives a detailed log of time/date, type of browser, etc for usage unless cleared

Bookmarklets - extension is better, but these are available - 'Lastpass Login!' (autofill and submit), 'Lastpass Fill!' (only fills) or 'LastPass Fill Forms!' (fills form data)

Form fills - autofill forms

LastPass Authenticator can generate one-time passwords for other websites or for LastPass - don't warn against using their authenticator for their own PWM. Must not require 2factor itself...

If you have different logins for different subdomains or paths, you can tell LastPass to treat each host or path in a domain as a separate login by setting up [URL Rules](#). Will not offer options for other subdomains if you set up the rules appropriately.

FEATURES	FREE	PREMIUM
 Emergency access		
 One-to-many sharing		
 Advanced multi-factor options		
 Priority tech support		
 LastPass for Applications		
 1 GB encrypted file storage		

MP Length requirement 8 letters at least - only requirement

Default Settings

Does not automatically logout when browsers are closed or idle after x time - reopen browser you are logged in (both can be configured) - while this increases usability, it is a security concern

Do not overwrite fields that are already filled unchecked by default

Automatically Fill Login Information checked

Clear filled fields on logout unchecked

Save a disabled One Time Password locally for Account Recovery checked

Poll Server for account changes set to 15 minutes (can be unchecked)

Respect AutoComplete = off; unchecked

Warn before filling insecure forms unchecked

Per Site

Require Password Reprompt (requires master password for this site) / Autologin / Disable Autofill are off by default

If choose site from LastPass extension, it will autologin even if autologin is not checked for that website

Clear clipboard only on Windows binary - not available in the extension

Entropy / Password Generation

Default: length 12, A-z/a-z/0-9 (no symbols), min 1 numeric, allow all character types checked, avoid ambiguous unchecked

Length range: 4-100

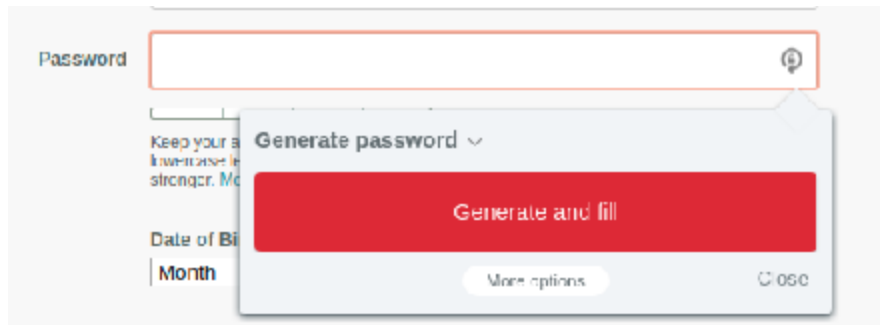
(online 1-50)

Persists changes to password generator settings after closing dialog

'Use Password' to autofill or 'Copy Password'

Symbol set: !\$/%@#

Requires user to click the icon in the far right in order to bring up the password generation menu:



Databases

stored in sqlite database - location depends on operating system and browser

For chrome - `~/.config/google-chrome/'profile'/databases/chrome-extension_id/'databases'`

All values in database encrypted - even preferences

Might leak number passwords based on size encrypted data? Yes, if you filter by 'accts' an account with more passwords has a noticeably larger encrypted blob than the one with less passwords (2 websites ~ 18502 char(s), 1 ~ 17666, 3 ~ 18950, 92 ~ 126k)

256-bit AES encryption

[AES](#) utilizing 256-bit keys as well as PBKDF2:

<https://helpdesk.lastpass.com/account-settings/general/password-iterations-pbkdf2/>

Have to enter master password to download a backup csv - when you download this way all values are unencrypted! Can get a raw csv file with all data. More

Options/Advanced/Export/Lastpass CSV File

Subdomain Behavior

Treats login.localhost, sub.localhost and localhost as 3 separate websites - never offers password for one of them for the others...even if no password yet saved for the others. Has this behavior changed since the below article??? Only appears to offer multiple login options if it is the same url with different credentials - like gmail's login

Even tried one.one.localhost and one.two.localhost - still did not offer multiple options

Also with heroku - by default LastPass recognizes the difference between 2 different heroku websites and does not offer password choice - https

utk.libapps.com does not have a match even though my.utk password saved - different top level domain....

accounts.google.com shows multiple options - but it is literally the same domain for each one

By default, LastPass uses the 2nd level domain name to decide if a site's credentials should be autofilled. For example, if you have saved a site with credentials for `www.acme.com`, then LastPass will consider all of the following URLs matches since they all have a 2nd level domain name of 'acme.com'.

`www.acme.com`




`acme.com`

`login.acme.com`

`secure.login.acme.com`

You can also choose to have LastPass only offer the logins saved to a particular URL. You can do this by setting a [URL Rule](#) with exact host matching. By setting this URL rule, LastPass will recognize any subdomains as part of the URL, and only offer the appropriate logins.

<https://lastpass.com/support.php?cmd=showfaq&id=3676>

Domain	Path	Host Matching	Port Matching	Type	Action
appspot.com		Yes	No	Default	
cloudaccess.net		Yes	No	Default	
google.com	/a/	No	No	Default	

Autofill

Fills plain text

Does not require user interaction by default (configurable)

Does not automatically submit by default

Will autofill login form with display: none; on another page

IFrame

Will autofill hidden IFrame on login page

Will autofill IFrame login page on another page of same origin even if display: none; or visibility: hidden; - however, for some reason once the page is cached it requires user interaction to autofill

Will not autofill IFrame from another origin - even if click LastPass icon within cross-origin IFrame only password suggested is for the current origin

HTTPS

Will autofill

HTTP

Won't autofill, but can fill by user interaction

Broken HTTPS

Won't autofill, but can fill via user interaction

CSRF Vulnerability for OTP

LastPass has added a CSRF token to their request, thereby fixing this vulnerability? They send 2 requests - one to /verifypassword.php and one to /otp.php each time OTP form is submitted. Only possible attack I could see is a replay attack if the attacker sees the user submit otp form and quickly uses the existing token to generate another otp - but would need to verify that is possible.

▼ Form Data view source view URL encoded

```
newkey: 1
xml: 1
hash: fa5cdf0cfa4275925b1711038af7e7f6d5f5380b8155187fac62b659e5355413
encrypted_otp: !40vov9slavItcraZM3diNA==|kmWPFG0mKPp9vwpa+Dbhl3FsbLQRglbrlu/S95GLrRESWu5I1Wf2Ej rVD/40mfwl
rand_encrypted_key: !dPhSTyLa0Cg92Zm343MBGg==|PEvTHH0HwR00lpM1TmzKshpWvknSClPjtqDP61hzlr0BqTAHwmiGbGkg0yFuPPBJ6GmzqiJA7PEB8ELPBj3J8kX1x5t+gXXj rxcwTt0
okg=
token: MTU0Nzkw0DEyNy45NzUyLZjZVM4J0nmDmYf+3Hv0SguKzPiyIQoL0nfXkdtSr806
method: web
ott: 8IA4Mieof4FimoHcm61Ssuox3BU3bFmXHL409VQ8BPqA=
```

Without page refresh the token remains identical:

▼ Form Data view source view URL encoded

```
newkey: 1
xml: 1
hash: 1cb220152f09b7a81ab343c5247fe7d9487f16dfc8c0a98af43e8fe8f04accfa
encrypted_otp: !zQrf+hrag+0WI3wF3YKfEQ==|7SVxlVl8nj8gbJhuJZ4g0QVzj1zYBf9k6mYFACVZwfZW/r7iGPjcdQ0ZnJ/MZyB
rand_encrypted_key: !dOV+X4Up9SagTR68whucEg==|l0flUyS290Peov25SYVU77uXBjHc+v08k7cxiVRBUzbljWG3koppZ8fopwXHf8v4nkKSAqh8MX8adj01VhkldNmsF
PbJMfw9dCnvY8qs rM4=
token: MTU0Nzkw0DEyNy45NzUyLZjZVM4J0nmDmYf+3Hv0SguKzPiyIQoL0nfXkdtSr806
method: web
ott: dfE6eB4236y4LtJg0BLpJ6pgBjaVFudMB0ALF41QTpA=
```

On page refresh the token is updated:

▼ Form Data
view source
view URL encoded

newkey: 1
xml: 1
hash: 06399ba5599fecdfbd197b599b812d4df68e8315f9136a65cfed3966681a0ac2
encrypted_otp: !nSbkTsXU08YD4VgyjVDpWw==|LfTniCuLVZd5ittjHRN9XsNJX/eEtdjl1FR+62kx8zuysNSs32QRk8RsykMtx+ch
rand_encrypted_key: !exmsQInn1oZq4HwPZITvkq==|j64Jw8ZUej5k6Yjr6T0wDo3dxs0SbY509n\5Q/pSyGvfjs8gya+/AbPM0\QRAhn\KULegmA/+ED9cgwQDmkWfX1x2G5QuhsvpzQ9qcybVwU=
token: MTU0NzkwOTQ2NS4zNy3Ns8px6byYFzIHeQGBScDPxjRG7mogJNe8fW0pxU0hvvg==
method: web
ott: 0mE6dm0ect+wlymwjhi581oxMC3gKHJEDR7uCR0\LOk=

In controller.js the extension also appears appears to fetch token from the server - presumably the actual vault is served this value whenever the page is loaded.

```

LPProxy.getToken = function (e, r) {
  if (void 0 === e) return X;
  null !== X ? e(X) : LPPatform.ajax({
    type: "POST",
    url: LPProxy.getBaseURL() + "getCSRFToken.php",
    data: {
      token: X
    },
    success: function (r) {
      e(X = r)
    },
    error: t(r)
  })
}

```

1Pass

Free Trial but no free version

\$36 per year personal / \$60 for family of 6 (you included)

Teams - \$48 per person per year / Business - \$96 per person per year / Enterprise no price listed

Overview

Far fewer options presented to the user, so in that sense probably easier to avoid getting into trouble

Unlike LastPass, the 1Pass icon does not appear in the form field until you select the field and does not indicate the number of passwords for that domain - usability question

<https://1password.com/files/1Password%20for%20Teams%20White%20Paper.pdf>

256 Bit AES End-to-End Encryption

Master Password + 128 Bit Secret Key (2SKD - two-secret key derivation)

Every time use new browser or device must enter Secret Key in addition to Master Password

PBKDF2 used to derive key from MP, thereby greatly reducing the efficacy of brute force attacks

'Watchtower' tells you if password has been compromised in breach so you can update it.

Also checks for weak passwords, unsecured websites, logins that support two factor and identity reuse. (Personal Security Suite - Security Audit)

Offers Secure Notes and Identities for form fills

Looks like there was a 1Click bookmark feature for Mac at some point - but bookmarklets are nowhere on the website or in the interface so not a supported feature

Has 2 factor authentication - 6 digit code when signing into account on new device - can use Authy or YubiKey

Can act as an authenticator app to generate one-time passwords for other websites - but recommended not to use as multifactor for itself...

Travel Mode - Travel Mode removes your sensitive information from your computers and mobile devices while you're traveling. If you're stopped for inspection, the only data on your devices will be data you've marked as safe for travel.

MP length requirement of 10 (no other requirements - used abcdefghij)

Default Settings

Automatically locks after 10 seconds or device goes to sleep

Automatically lock 1Password is selected

'Offer to fill and save passwords' and 'Show autofill menu on field focus' selected

App

Lock on sleep / when screen saver is activated

Lock when fast user switching

Lock after computer is idle for 5 minutes

Lock when main window is closed (not checked)

Clear clipboard contents after 90 seconds (seems to apply to the browser extension as well)

Subdomain Behavior

Password is saved for that specific subdomain - when I enter password for sub.localhost and localhost 1Pass only offers the password for that specific domain

Even for heroku sites it recognizes the difference between 2 subdomains by default - only suggest the password for that subdomain - https

this is an ongoing issue that it's difficult to solve in a way that benefits the small number of people like you who have twenty or thirty logins all for the same domain (different subdomains) while not either breaking things for or increasing complexity for the much larger contingent of users who have only one or at most a couple of logins for any given site. We're always looking into ways we can meaningfully improve the experience for our power-users who have edge cases while not degrading the experience for regular users, but so far a solution that works well for both groups in the case has proven elusive. Thanks for reporting, however!

<https://discussions.agilebits.com/discussion/89271/matching-sub-domains>

Entropy / Password Generation

Default to Length 20, Numbers and Symbols enabled, type 'Random Password' ('Memorial Password' or 'PIN Code' (numbers only) options also available)

Shows Password Generator history in a dropdown - very detailed - date created, password, website

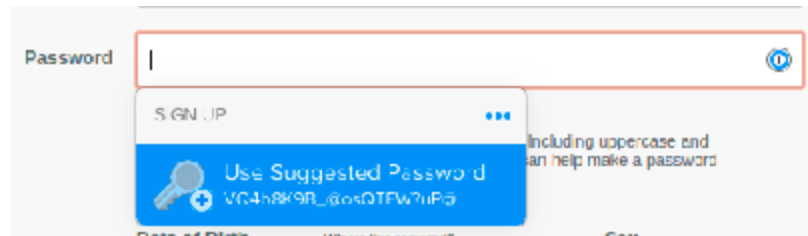
Range: 8-50

(online tool 8-100)

Persist changes to password generator settings after closing dialogue

Can copy password or select 'Fill' to fill the dialogue automatically

Suggested password dialog pops up and shows recommended password:



Databases

<https://discussions.agilebits.com/discussion/8591/onepassword-sqlite>

Using 1PassordX it appears to hit the server every time a password is updated. Cannot update without Internet connection.

192.16.414812574	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TCP	96.443 -> 51126 [SYN, ACK] Seq=0 Ack=1 Win=26787 Len=0 MSS=1440 SACK_PERM=1 TSval=732199002 TSecr=2865752573
195.16.443104344	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TCP	88.443 -> 51126 [ACK] Seq=1 Ack=518 Win=27904 Len=0 TSval=732199009 TSecr=2865752573
196.16.443843598	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TLSv1.2	1516 Server Hello
198.16.443940017	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TCP	1516 443 -> 51126 [ACK] Seq=1429 Ack=518 Win=27904 Len=1428 TSval=732199009 TSecr=2865752573 [TCP segment of
200.16.444159200	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TCP	1516 443 -> 51126 [ACK] Seq=2857 Ack=518 Win=27904 Len=1428 TSval=732199009 TSecr=2865752573 [TCP segment of
202.16.444159343	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TLSv1.2	1071 Certificate, Server Key Exchange, Server Hello Done
209.16.472180136	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TLSv1.2	346 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
210.16.472180475	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TLSv1.2	166 Application Data
213.16.474564905	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TCP	88.443 -> 51126 [ACK] Seq=5604 Ack=2646 Win=32000 Len=0 TSval=732199017 TSecr=2865752603
214.16.499089591	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TCP	88.443 -> 51126 [ACK] Seq=5604 Ack=3524 Win=34816 Len=0 TSval=732199023 TSecr=2865752603
215.16.501322189	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TLSv1.2	1256 Application Data
216.16.501322371	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TLSv1.2	126 Application Data
218.16.502606559	2000:1f18:60d5:4e02_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TLSv1.2	294 Application Data
221.16.553230017	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TCP	1516 443 -> 51126 [ACK] Seq=6810 Ack=3621 Win=34816 Len=1428 TSval=732199037 TSecr=2865752604 [TCP segment of
222.16.553230344	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TLSv1.2	389 Application Data
224.16.553230507	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TLSv1.2	126 Application Data
227.16.613175428	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TCP	1516 443 -> 51126 [ACK] Seq=8577 Ack=3739 Win=34816 Len=1428 TSval=732199052 TSecr=2865752715 [TCP segment of
228.16.613170807	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TLSv1.2	1423 Application Data
230.16.613178524	2000:1f18:60d5:4e04_	2000:1700:5010:4da0:fd05:d492:f86d:ecdb	TLSv1.2	126 Application Data

Also every time log in with master password hits the server and fetches application data. Can still access passwords without Internet and after clearing cache - def stored somewhere locally.

Posted question on support form - Assuming Chrome uses the same folder structure on Linux as they do on macOS you should find in the Chrome profile folder a folder titled IndexedDB and then inside of there a folder titled

chrome-extension_aeblfdkhhhdcdjpihfhhbdiojplfjncoa_0.indexeddb.levelddb . That's the extension folder created by Chrome where we can store data on the device.

The actual file ought to be given away by the file size as I'm not sure the name will be consistent between platforms or maybe even Chrome profiles.

Binary file located at:

~/config/google-chrome/[profile]/IndexedDB/chrome-extension_aeblfdkhhhdcdjpifhbbdiojplfncoa_0.indexeddb.leveldb/

embedded database, i.e. one you use directly in your programming language and it runs in the same process as your program.

Not certain how exactly this works...chrome uses custom comparator so can't open level db with normal python library without reimplementing that comparator

<https://support.1password.com/opvault-design/>

Appears settings are stored in the clear:

~/mozilla/firefox/djp50pju.default/webappsstore.sqlite

```
{"autoLockEnabled":true,"autoLockMinutes":10,"autoLockOnDeviceSleep":true,"autoSaveEnabled":true,"autoSaveExceptions":[],"ignoreAccounts":[],"inlineEnabled":true,"inlineShowAutomatically":true,"saveNewItemIn":"","showNotifications":true,"icon":"color-light","generator":{"passwordType":"characters","length":20,"requireDigits":true,"requireSymbols":true},{"passwordType":"words","length":4,"separatorType":"hyphens","capitalize":false},{"passwordType":"pin","length":4},{"passwordType":"syllables","length":5,"separatorType":"hyphens","capitalize":false}],activeGenType":"characters","syllables":false,"hibpEnabled":false,"language":"en-US","defaultPasswordManager":false,"shouldShowDefaultAutofillPrompt":true,"shouldShowImportPrompt":false,"showTags":true,"shouldShowBuildUpdateNotification":false}
```

On Mac

~/Library/Group Containers/2BUA8C4S2C.com.agilebits/Library/Application Support/1Password/Data/B5.sqlite (if download from app store)

All values are encrypted with A256GCM - it appears both master password (mp) and master key (mk) are encrypted and stored - iv, encryption method, data, ct, and kid stored

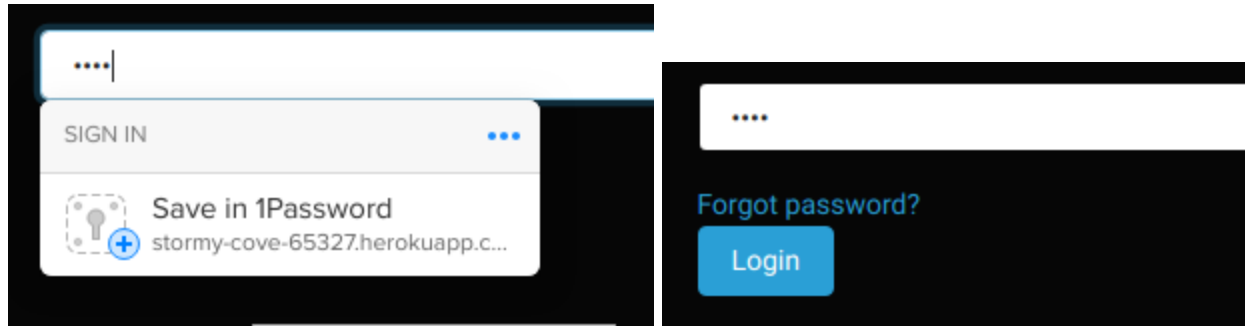
Passwords stored in the 'items' table and very obvious not using ECB when changing the password

Very easy to see how many passwords there are, but it's all encrypted

If change MP, the encrypted values for the passwords are changed

Autofill

Unlike LastPass does not prompt after form submission - provides a popup beneath the password field where you can choose to save in 1Pass - could be irritating if you just want to hit the enter button and continue and it partially covers it



To see the prompt to autofill have to click on the username or password input textbox

Fills plain text

requires user interaction by default

No autologin by default even after selecting to sign in

Won't autofill invisible login form (display: none;)

If you select website from vault, it will autofill on field focus - otherwise requires clicking dropdown

IFrame

Will autofill hidden IFrame on login page once user chooses to fill in main login form

Even if user interacts with visible IFrame will not fill in other IFrames on the same page that are hidden

Even if IFrame has website from other origin login suggested by 1Pass is only for current origin

IFrame

Thought about trying to click the iframe generated by 1Password to fill in a hidden login form, but it looks like basic cross origin policies prevent doing so.

```
< DOMException: Blocked a frame with origin "https://stormy-cove-65327.herokuapp.com" from accessing a cross-origin frame.  
  at HTMLIFrameElement.<anonymous> (snippet:///ClickJack:11:42)  
  at Function.each (https://stormy-cove-65327.herokuapp.com/js/jquery.js:33:34)  
  at w.fn.init.each (https://stormy-cove-65327.herokuapp.com/js/jquery.js:25:340)  
  at snippet:///ClickJack:1:13
```

Always requires user interaction...

DashLane

Business - \$48 per year per user

Free \$0	<i>Most popular</i> Premium \$4.99 /MO <i>billed annually</i>	Premium Plus \$9.99 /MO <i>billed annually</i>
Manage up to 50 passwords and autofill all your personal information on your favorite device, free for life.	Manage unlimited passwords on unlimited devices, plus Dark Web Monitoring and secure VPN.	Get added protection with credit monitoring and up to \$1 million in Identity Theft Insurance .
Get Free	Get Premium	Get Premium Plus
<ul style="list-style-type: none">✓ Store up to 50 passwords✓ Dashlane on one device✓ Instant form and payment autofill✓ Security alerts Learn more >	<ul style="list-style-type: none">✓ Unlimited password storage✓ Passwords and data automatically synced across devices✓ Instant form and payment autofill✓ Dark Web Monitoring with personalized security alerts✓ VPN for safe, private connection on unsecure WIFI networks✓ Secure storage for sensitive files Learn more >	<ul style="list-style-type: none">✓ Unlimited password storage✓ Passwords and data automatically synced across devices✓ Instant form and payment autofill✓ Dark Web Monitoring with personalized security alerts✓ VPN for safe, private connection on unsecure WIFI networks✓ Secure storage for sensitive files✓ Real-time credit monitoring✓ Identity restoration support✓ Up to \$1 million in Identity Theft Insurance coverage Learn more >

Overview

requires 2 factor auth by default on first login in new browser / device - code sent to email - subsequent logins do not require it even after closing browser

Multifactor can be required on every login, but by default only for new devices

Can use authenticator app - default is send code to e-mail

They do have own authenticator app

However, you cannot use Dashlane as an authenticator app to log into your Dashlane account. This would be the same as leaving your car keys in the car and locking them inside.

Option to keep session active for 14 days

From a user's Master Password, we derive a ciphering key using 10000 PBKDF2 iterations, and we use AES-256 to cipher

Secure Notes and Payments (credit/debit card info)

Manage Devices - if you delete a device from this list that has been given approval data will be deleted from that machine on the next login attempt

Icon showed up on LastPass's generator site for an input that had 'password' in the name but was not actually a password input.

```
<input value="12" name="length" class="lp-custom-range__number" step="1" id="lp-pg-password-length" type="number" min="0" max="100" data-kwimpalastatus="alive" data-kwimpalaid="1548784511044-3">
```

Password Length



```
<input type="text" id="passwordMirror" style="margin-top:40px;" data-kwimpalastatus="alive" data-kwimpalaid="1548793636410-4">
```



MP must meet certain criteria - 8 characters, 1 digit, one uppercase and one lowercase letter

Default Settings

Require Master Password before using unchecked (when saving password)

Use only on this subdomain unchecked (when saving password)



Store my data locally only

Dashlane stores an emergency web app backup of your Dashlane data. If you choose to store your data locally only, this encrypted copy will be deleted from our servers.

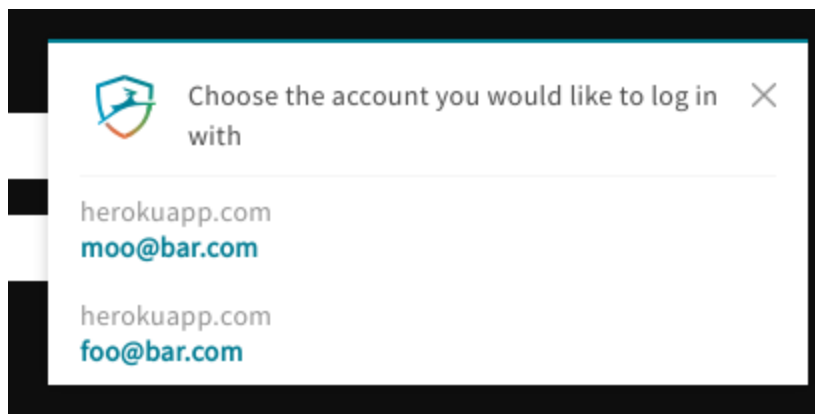
For each saved password - 'Always log me on to this website' checked, 'Always require Master Password' and 'For this subdomain only' not checked

There is a release note saying it clears the clipboard - but cannot find any setting and it does not clear clipboard by default - even after 5 minutes

Subdomain Behavior

HTTP: Treats login.localhost, sub.localhost and localhost as 3 separate websites - never offers password for one of them for the others...even if no password yet saved for the others.

Using heroku was able to see actual subdomain behavior - at least for https:



Password Generation

Default Length: 12 - Letters, Digits, Symbols, Avoid ambiguous characters all checked

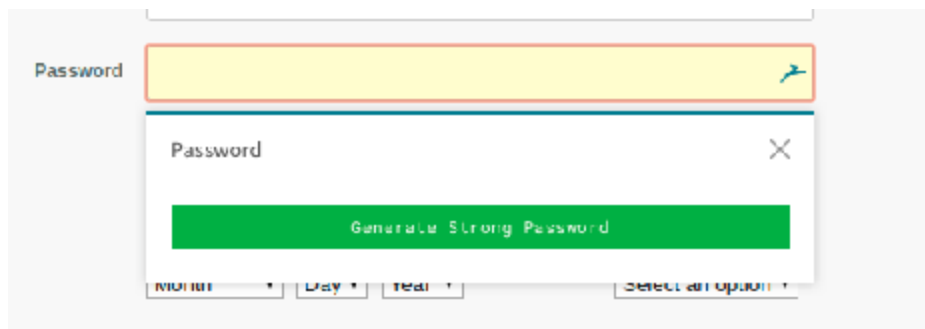
Range: 4-28

Online (4-40)

Generator always snaps back to default settings after closing - can select 'Save as Default' to update default configuration

Only option is 'Copy Password'

Offers dropdown when you click on password input to 'Generate Strong Password' - very noticeable and easy to use



Databases

stored locally and also on Dashlane servers for synchronization purposes

Modified sqlite file in ~/.config/Code/Local Storage/ and ~/.config/google-chrome/[profile]/Local Extension Settings/fdjamakpfbddfdjaooikfcpapjohcfmg folder

On MAC

~/Library/Application Support/Dashlane

Dashlane/www/Websites/ has images used as icons for the different websites - not encrypted - could be used to determine what websites user visits

Files all .aes - encrypted with AES Crypt - <https://www.aescrypt.com/>

Appears password is in profiles/[profile]/Personaldata/personaldataDatabase.aes - it does change when MP is changed

Autofill

After I selected 'only from this subdomain' and then deselected no longer autofilling / logging in - very odd. There are some inconsistencies in the behavior.

If you click on the website from the dashlane icon or within dashlane it will always automatically log you in, even if that option is disabled

Fills plain text

requires user interaction by default

automatically hits login button for you (can disable - sort of - if you ever select website from Dashlane it tries to autologin - doesn't if already cached - odd)
Will not autofill login form with display: none; on another page

IFrame

Autofills whichever IFrame grabbed first???

Will autofill visible IFrame if it is the first thing on the page

Will autofill hidden IFrame (display: none;) on login page for an alternate subdomain - fills it in with whichever login used last - dashlane logo still present in main login form

If multiple hidden IFrames, appears to fill whichever one loaded first - the ones that are not filled do not even get the dashlane logo in the input fields - appears a bit random which one is filled in???

Setting both websites to 'this subdomain only' solves the problem - neither hidden login form nor hidden IFrame is filled

What happens if no password for a hidden IFrame on another subdomain? Do you get the main password? Looks like the answer is no....

If you have hidden IFrame from another subdomain it will fill it in and submit that form rather than the one that is displayed once you select the value - will also autofill it when conditions appropriate - could steal credentials for a subdomain

Can prevent this simply by checking 'for this subdomain only'

Why is there not just a blanket rule against IFrames???

HTTPS

Autofills and logs in automatically if not cached - if cached only autofills

HTTP

Requires user interaction

Warning - 'This website is not secure. Information you enter here could be compromised'

Logs in as soon as you select password

Broken HTTPS

Will save it

Autofills and logs in automatically if not cached - if cached only autofills

If select the non-password field it will fill in the actual login form as well - could put an overlay over the actual password field and intercept the entry



The image shows a login interface with a dark background. At the top, there are two yellow input fields. The first field contains the email address "storm@storm.com" and has a small blue icon of a person running at the end. The second field contains five asterisks "*****" and also has the same blue icon. Below these fields, the text "Forgot password?" is visible. Underneath that is a blue button with the word "Login" in white. At the bottom, there is a label "Password Mirror" followed by a yellow input field containing the text "storm" and the same blue icon. This "Password Mirror" field is positioned directly over the actual password field, illustrating how it can intercept the user's input.

Roboform

Everywhere individual: \$23.88/year

Everywhere family: \$47.75/year

For business:

1 YEAR SUBSCRIPTION

1-10
\$39.95 / year / user

3 YEAR SUBSCRIPTION
15% DISCOUNT

11-25
\$35.95 / year / user

5 YEAR SUBSCRIPTION
25% DISCOUNT

26-100
\$34.95 / year / user

101-1000
\$29.95 / year / user

	Free	Everywhere
Unlimited Logins	✓	✓
Fill web forms	✓	✓
Multi-platform support	✓	✓
Strong encryption	✓	✓
Password audit	✓	✓
Securely send Logins	✓	✓
Receive Emergency Access	✓	✓
Application Logins	✓	✓
Sync across all devices		✓
Cloud backup		✓
Secure shared folder		✓
Grant Emergency Access		✓
Web access		✓
Email / phone support		✓

Overview

Only requires Master Password to login by default - does not require secret key or multifactor

Roboform icon does not appear in the input fields at all - chills up in the toolbar

Does offer popup dialog to save password after form submission

No popups on input field focus at all - you always have to go to the icon in the toolbar to select desired password

MP length requirement 8 - that's it - no warning if it is weak in popup (just has the bar - used abcdefgh)

Default Settings

Session timeout after 20 minutes / device enrollment period 1 year - requires Master Password every time browser closed / reopened

Password Generation

Default Length: 14

Range: 1-99 (Online: 1-99)

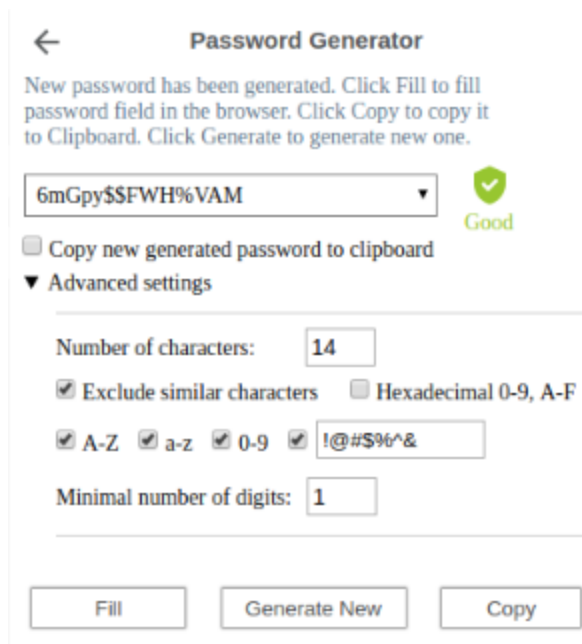
Always returns to default - no way to save a new default configuration

Symbol Set: !@#\$%^&

Copy or Fill

No history

Does not automatically popup when focus on password input - have to actually click on app icon in toolbar and generate password from there



The screenshot shows a 'Password Generator' window. At the top, a back arrow is on the left, and the title 'Password Generator' is in the center. Below the title, a message reads: 'New password has been generated. Click Fill to fill password field in the browser. Click Copy to copy it to Clipboard. Click Generate to generate new one.' A password field displays '6mGpy\$F\$WH%VAM' with a dropdown arrow on the right. To the right of the field is a green shield icon with a checkmark and the word 'Good' below it. Below the password field is a checkbox labeled 'Copy new generated password to clipboard'. Underneath is a section titled 'Advanced settings' with a downward arrow. This section contains several settings: 'Number of characters:' with a value of '14'; a checked checkbox 'Exclude similar characters' and an unchecked checkbox 'Hexadecimal 0-9, A-F'; a row of four checked checkboxes 'A-Z', 'a-z', '0-9', and a custom symbol set '!@#\$%^&'; and 'Minimal number of digits:' with a value of '1'. At the bottom, there are three buttons: 'Fill', 'Generate New', and 'Copy'.

Databases

On MAC: ~/Library/Application Support/RoboForm/.userdata/_user-data.rfo

It exposes your e-mail in _settings.rfo, but the rest is encrypted

Do have to use Master Password to view / access data

RoboForm V7 credentials were comprised of a User ID, Everywhere password, and Master Password. Juggling and differentiating the three proved to be very confusing for many users. As a result, we have simplified the process while also increasing security. RoboForm 8 uses SCRAM, the most modern and secure authentication scheme.

More info on the mechanism can be found here:

https://en.wikipedia.org/wiki/Salted_Challenge_Response_Authentication_Mechanism

<https://help.roboform.com/hc/en-us/articles/115001904532-One-File>

After MP changed the files where MP stored also change

Autofill

Fills plain text

requires user interaction by default

Chrome

Version 71.0.3578.98-1

Overview

With sync turned on, passwords are saved to google account. Otherwise, only stored locally on computer. If sync to another device, the passwords are then stored on that devices keychain even after the user has logged out of their account in the browser.

Option to export passwords

If you 'sync' passwords and login on new machine are your passwords stored locally on the device? Yes - even after logout.

Can lookup your passwords online at passwords.google.com - login first

Syncing pulls bookmarks, passwords and everything even after log out - though when you stop syncing there is the option to delete all artifacts from the device

Turn off sync and sign out?

This will sign you out of your Google accounts. Changes to your bookmarks, history, passwords, and other settings will no longer be synced to your Google Account. However, your existing data will remain stored in your Google Account and can be managed on [Google Dashboard](#).

Cancel

Turn off



Clear bookmarks, history, passwords, and more from this device



Supports multi-factor authentication for signing into your google account, but not specifically for the PWM

Default Settings

Offer to save passwords and Auto Sign-in enabled by default

Auto-signin quietly signs you into browser when you sign in to another google site

Does not appear to be any way to turn off autofill

Password Generation

If sync is turned on, right click password box and click 'Suggest Password' - it will autogenerate password and that password can be saved to the keychain by selecting 'Update Password'

Appears to attempt to discern the password policy - used no symbols for sites without policy, but did use symbols on a site with policy (master password creation for LastPass). Defaults to letters (lowercase and uppercase) and numbers and length 15. Seems to try to use as few symbols as possible. Would need further testing to verify.

<https://stackoverflow.com/questions/53062991/is-there-a-way-to-tell-chrome-password-generator-the-website-password-policy>

<https://security.stackexchange.com/questions/190796/chrome-generated-passwords-not-high-entropy>

Databases

Depends on what system you are on - but in any case it uses operating system functionality to encrypt the passwords on the local disk.

/.config/google-chrome/'profile'/'Login Data' - browser has lock when running - when I open with sqlite browser no data in the 'logins' table

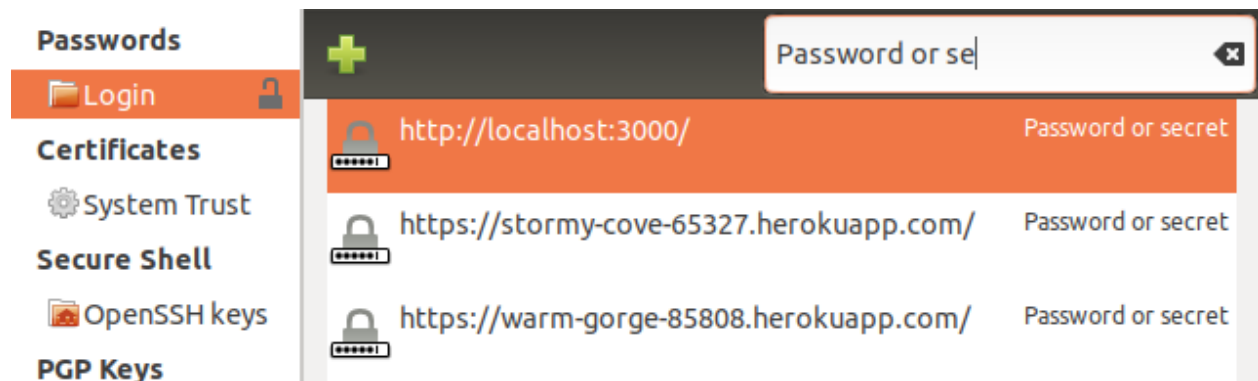
~/.config/opera/Web Data - sqlite database with list of website urls and number of times autofilled plus id of the input field filled in in the 'autofill' Table - not protected in any way (see Opera for image)

From 'man google-chrome':

--password-store=<basic|gnome|kwallet>

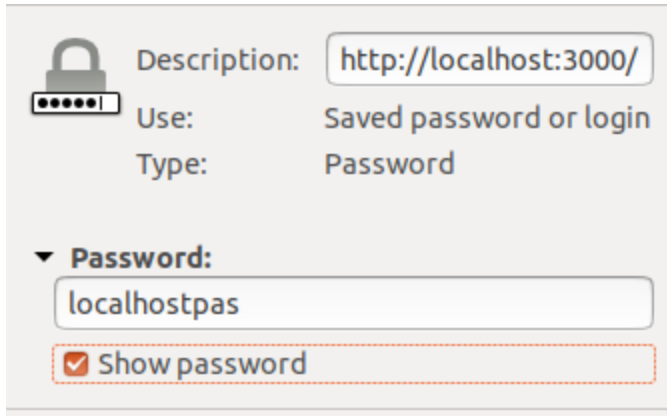
Set the password store to use. The default is to automatically detect based on the desktop environment. basic selects the built in, unencrypted password store. gnome selects Gnome keyring. kwallet selects (KDE) KWallet. (Note that KWallet may not work reliably outside KDE.)

Uses the GNOME keyring by default - go to 'Passwords and Keys':



If you can access the keyring you can view everything, including the password:

```
date_synced: 0
submit_element:
type: 0
avatar_url:
scheme: 0
action_url: http://localhost:3000/submit
username_value: foo@bar.com
blacklisted_by_user: 0
origin_url: http://localhost:3000/
application: chrome-5308494
signon_realm: http://localhost:3000/
form_data:
XAEAAAYAAAAFAAAATABvAGcAaQBuAAAAFgAAAGh0dHA6Ly9sb2NhbGhvc3Q6MzAwMC8
AABwAAABodHRwOi8vbG9jYWxob3N0OjMwMDAv3VibWI0AgAAAcAAAAAAAAEAAAAGk
AbgBwAHUAdABFAG0AYQBpAGwASABpAGQAZABIAG4AAAAAAUAAABlbWFpbAAAAAA
AAD///9/AAAAAAAAAAAAAAAAQAAAAEAAAABAAAAAAgAAAAAAAAAAAAAAAAAAAA
AgAAAAAAAAAAcAAAAAAAAAEwAAAGkAbgBwAHUAdABQAGEAcwBzAHcAbwByAGQASA
BpAGQAZABIAG4AAAAAAACAAAAHBhc3N3b3JkAAAAAP///38AAAAAAAAAAAAAAAABA
AAAAQAAAAEAAAACAAAAAAAAAAAAAAAAAAAAACUAAAAAAAAAQAAAAAAAE
AAAAbnVsbA==
username_element: inputEmailHidden
generation_upload_status: 0
times_used: 1
date_created: 13192908216241927
preferred: 1
display_name:
federation_url:
should_skip_zero_click: 1
password_element: inputPasswordHidden
```



The image shows a Chrome password manager entry. At the top left is a lock icon. To its right, the 'Description' field contains 'http://localhost:3000/'. Below this, the 'Use:' field is set to 'Saved password or login' and the 'Type:' field is set to 'Password'. A section titled 'Password:' with a dropdown arrow contains a text field with the value 'localhostpas'. Below the text field is a checkbox labeled 'Show password' which is checked.

"Chrome Safe Storage" in the Keychain is simply an application password that Chrome uses to encrypt/decrypt data in its secure information store.

Subdomain Behavior

Password is saved for that specific subdomain - when I enter password for sub.localhost and localhost chrome only autofills the password for that specific domain

Same for heroku - does not offer two options - automatically assumes the subdomain - https

Autofill

Appears to autofill after page load, but does not trigger onchange event until clicking on the page so that it is in focus

Fills plain text

Does not require user interaction

Does not automatically submit

Will autofill login form with display: none; on another page once the page itself is clicked and comes into focus

IFrame

Will not autofill hidden IFrame on login page unless user clicks on one of the form fields of the actual login

Will autofill IFrame login page on another page if it is visible, but not with display: none; or visibility: hidden; unless user clicks on one of the form fields in one of the other iFrames

Will not autofill IFrame login for another website (different origin) even if visible without user interaction (can if interact)

HTTPS

Will autofill

HTTP

Will autofill

Broken HTTPS

No engagement whatsoever - the key icon does not appear, no suggestion for username or password - does not offer to save password - nothing

Internet Explorer



Version: 11.523.17134.0
Update Versions: 11.0.105 (KB4480965)
Product ID: 00150-20000-00003-AA459

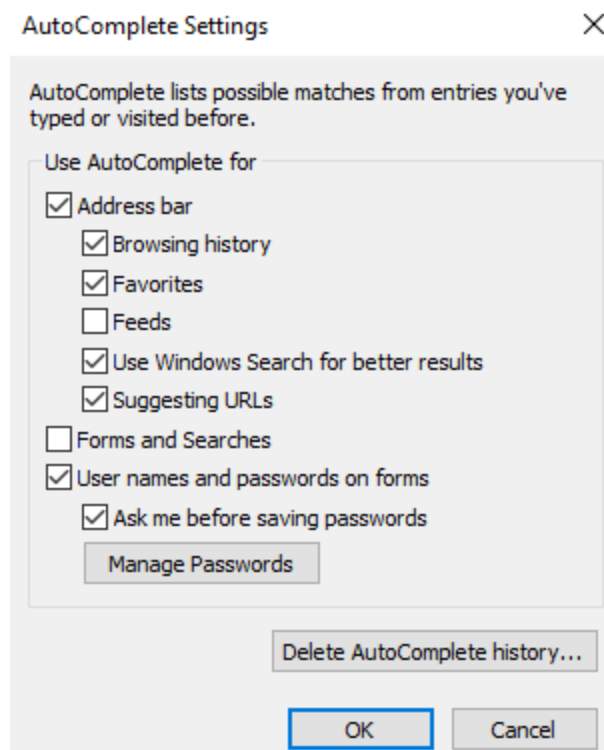
© 2015 Microsoft Corporation. All rights reserved.

Overview

No MP

Clicking 'Manage Passwords' takes you directly to Web Credentials

Default Settings



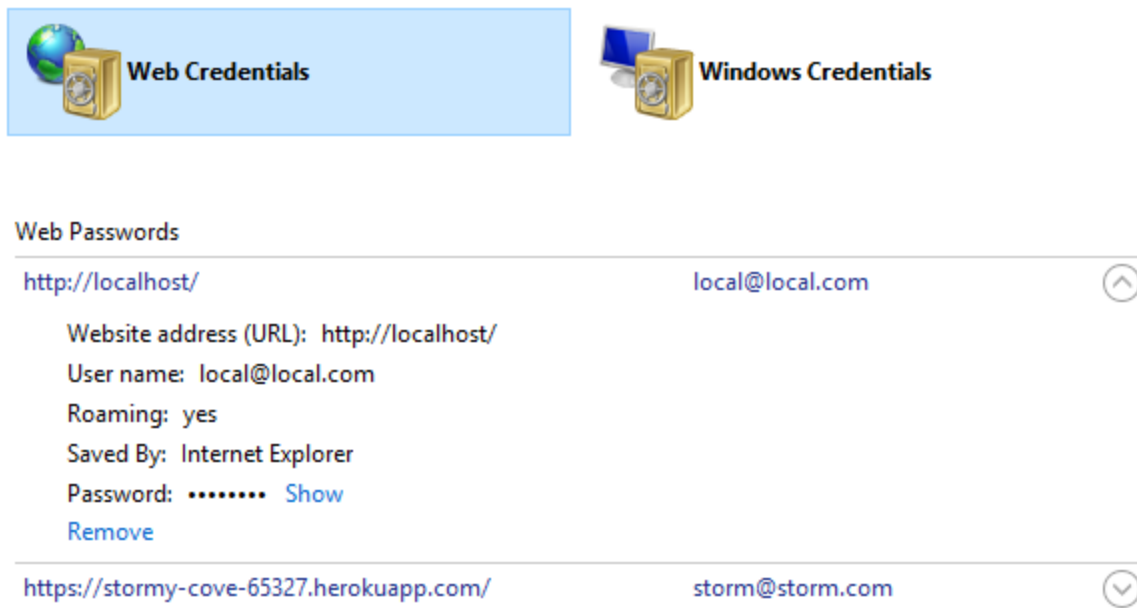
Subdomain Behavior

Only offers for that specific subdomain (heroku)

Password Generation

n/a

Databases



User password required to view in the clear

Autofill

Fills after page load (fires the onchange event)

Fills plain text

Does not require user interaction

Does not automatically submit

Will autofill login form with display: none; on another page

IFrame

Requires user interaction for IFrame, but with user interaction will fill in cross origin

Will only autofill hidden IFrame on login page for same origin if it is clicked on (even if clicked on while hidden, still works)

Will autofill hidden IFrame on another page for same origin - even if there are multiple

Will not autofill IFrame from another origin without user interaction - hidden or visible - on any page

HTTPS

Will autofill - appears to fill when page is loaded - no popup appears in response to onchange() event

HTTP

Won't autofill, but can fill by user interaction - click on user name input and select the appropriate item from dropdown

Broken HTTPS

Won't autofill, but can fill via user interaction

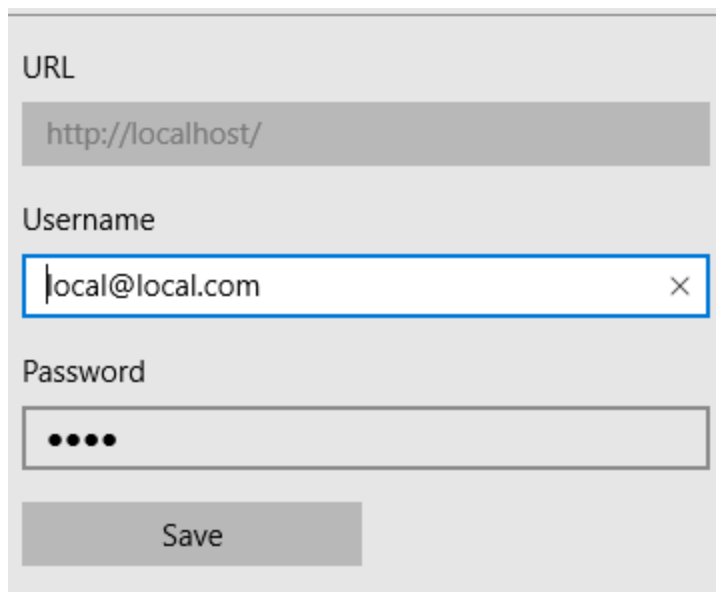
Edge

Microsoft Edge 42.17134.1.0

Overview

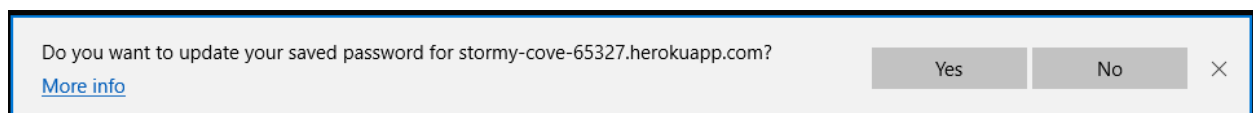
No Master Password

No way to 'copy' password - in fact, no way to view it in plain text using the UI - it just shows up as '*****'



A screenshot of a password save dialog box. It has a light gray background and a blue border. The dialog contains three input fields: 'URL' with the text 'http://localhost/', 'Username' with the text 'local@local.com', and 'Password' with five black dots. Below the fields is a 'Save' button. A small 'X' icon is visible in the top right corner of the dialog.

Very basic UI



A screenshot of a password update confirmation dialog box. It has a light gray background and a blue border. The dialog contains the text 'Do you want to update your saved password for stormy-cove-65327.herokuapp.com?' and a link 'More info'. To the right are 'Yes' and 'No' buttons, and a small 'X' icon in the top right corner.

Default Settings

Under Advanced/Autofill settings - 'Save passwords' enabled, 'Save form entries' enabled, 'Save cards' enabled - can click 'Manage passwords' to view sites with saved passwords

Subdomain Behavior

Does not suggest multiple passwords for the heroku websites

Password Generation

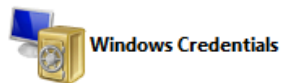
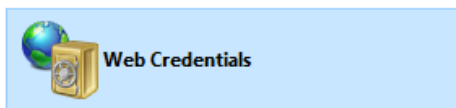
n/a - none by default - there are apps for windows / extensions, but none by default

Databases

Uses your Windows Credentials to store the passwords and requires password to view them in plain text

Manage your credentials

View and delete your saved login information for websites, connected applications and networks.



Web Passwords

http://localhost/

local@local.com



Website address (URL): http://localhost/

User name: local@local.com

Roaming: yes

Saved By: Internet Explorer

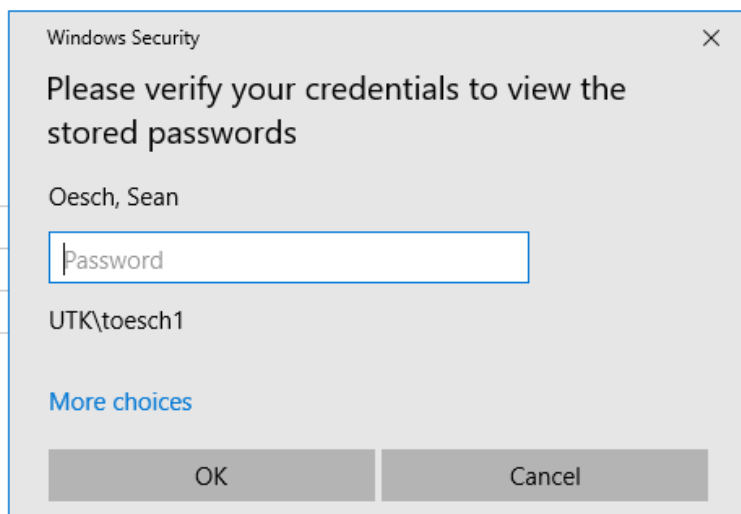
Password: [Show](#)

[Remove](#)

<https://localhost/>

<https://stormy-cove-65327.herokuapp.com/>

<https://warm-gorge-85808.herokuapp.com/>



Autofill

Fills plain text

Does not require user interaction by default (configurable)

Does not automatically submit

Will autofill login form with display: none; on another page

IFrame

Requires user interaction for IFrame, but with user interaction will fill in cross origin

Will autofill hidden IFrame on login page for same origin

Will autofill hidden IFrame on another page for same origin - even if there are multiple

In fact, if there are multiple and you embed an IFrame on the login page for another origin, you can get the password for another origin within that IFrame (for example: login page for stormy with embedded IFrame for warm - place multiple of those hidden on the same page and one of them will have credentials for warm)

Will not autofill IFrame from another origin without user interaction - hidden or visible - on any page

HTTPS

Will autofill - appears to fill when page is loaded - no popup appears in response to onchange() event

HTTP

Won't autofill, but can fill by user interaction - click on user name input and select the appropriate item from dropdown

Broken HTTPS

Won't autofill, but can fill via user interaction

Safari

Version 12.0 (14606.1.36.1.9)

Overview

Passwords are locked on a user by user basis (to view the 'Passwords' menu in Preferences, must enter user password)

No MP - uses your user account to lock credentials

Can use iCloud Keychain to sync across devices

Default Settings

AutoFill is checked by default

There are no other options :)

Subdomain Behavior

For heroku only offers password for that subdomain - if visit heroku.com to login still does not offer either of the subdomain passwords

Password Generation

iCloud keychain

Databases

Stores the user credentials in the Keychain - under 'Local Items' - can view password by entering the keychain password (on Mac)

Autofill

The [just-released iOS 11.3](#) requires Safari users to tap in web pages to AutoFill their user names and passwords. This means extra work for you, but it's also more secure.

<https://www.cultofmac.com/538447/ios-11-3-safari-security/>

Fills plain text

Does require user interaction

Does not automatically submit

Will not autofill login form with display: none; on another page once the page itself is clicked and comes into focus

IFrame

Will not autofill hidden IFrame on login page unless user clicks on one of the input form fields of the actual login

Will not autofill IFrame login page on another page if it is visible, but not with display: none; or visibility: hidden; unless user clicks on input form fields for a login

Will not autofill IFrame login for another website (different origin) even if visible without user interaction (can if interact)

HTTPS

Will not autofill - does offer popup on field focus

HTTP

Will not autofill - does not offer popup on field focus - have to click the key icon at the far right of the input field

Broken HTTPS

Safari requires user password to visit a site with broken https...

Will not autofill on broken https - does not offer popup - have to click on key to instantiate popup

Opera

Opera-stable_58.0.3135.47_amd64.deb

Uses code from the Chromium project but designed to use less memory than chrome

Automatically loads data - including passwords - from chrome:

<https://blogs.opera.com/desktop/2014/06/opera-developer-update-silent-import/>

<https://productforums.google.com/forum/#!topic/chrome/l2S8pRqdqnl>

Overview

Has built-in VPN that is free - disabled by default

Can view passwords by going to settings/passwords without entering any credentials

No master password option in the latest version

Offers sync by creating Opera account, but no specific website to view passwords from another browser

No multifactor????

Default Settings

Auto Sign-in option checked by default - if uncheck will be asked before credentials entered (I unchecked this option and cleared cache and closed browser, but it still autofilled passwords for saved websites)

Offer to save passwords selected by default - disabling it does prevent opera from offering to remember passwords, but nothing keeps it from autofilling?

Subdomain Behavior

Password is saved for that specific subdomain - when I enter password for sub.localhost and localhost 1Pass only offers the password for that specific domain

Password Generation

None without add-on

Databases

Same as Chrome - stores in the keychain on Linux and has the Login Data file for other operating systems - relies on operating system for encryption.

~/.config/opera/Login Data - sqlite file - browser has a lock on it while running - tables appear empty when opening with SQLite Browser

~/.config/opera/Web Data - sqlite database with list of website urls and number of times autofilled plus id of the input field filled in in the 'autofill' Table - not protected in any way

Table:

autofill

New Record

Delete Record

	name	value	value_lower	date_created	date_last_used	count
	Filter	Filter	Filter	Filter	Filter	Filter
1	inputEmailHidden	foo@bar.com	foo@bar.com	1548423912	1548423912	2
2	inputEmailHidden	foo@moon.com	foo@moon....	1548424545	1548426333	4
3	inputEmailHidden	foo@speed.com	foo@speed....	1548424661	1548424661	2

Autofill

Appears to autofill after page load, but does not trigger onchange event until clicking on the page so that it is in focus

Fills plain text

Does not require user interaction

Does not automatically submit

Will autofill login form with display: none; on another page once the page itself is clicked and comes into focus

IFrame

Will not autofill hidden IFrame on login page unless user clicks on one of the input form fields of the actual login

Will autofill IFrame login page on another page if it is visible, but not with display: none; or visibility: hidden; unless user clicks on input form fields for a login

Will not autofill IFrame login for another website (different origin) even if visible without user interaction (can if interact)

HTTPS

Will autofill

HTTP

Will autofill

Broken HTTPS

Will not autofill on broken https

Gives the option with user interaction to enter the username, but does not offer to fill in password in any way

Firefox

Firefox Quantum 64.0

Overview

By default does not use Master Password - can be enabled in Preferences/Privacy & Security/Use a master password (checkbox)

Without Master Password, anyone with access to your computer can view your passwords

Suggest using capital letter, symbol and one or more digits - password meter to indicate strength - 'easy for you to remember and hard for someone else to guess'

Master Password has nothing to do with how the data is encrypted - it only prevents other users from viewing your passwords in plaintext in the web interface

Use master password to view logins and enter it again to view actual passwords in plain text

Example of User who def should have used PWM instead of firefox's built in one:

<https://support.mozilla.org/en-US/questions/1232056>

SHA-1 is used to hash master password (insecure):

<https://nakedsecurity.sophos.com/2018/03/20/nine-years-on-firefoxs-master-password-is-still-insecure/>

Can sync passwords across devices by enabling sync, but does not have a specific website to which you can go from another browser to view passwords

Recently implemented multifactor - We chose to implement this feature using the well-known authentication standard **TOTP** (Time-based One-Time Password). TOTP codes can be generated using a variety of authenticator applications. For example, Google Authenticator, Duo and Authy all support generating TOTP codes.

<https://blog.mozilla.org/services/2018/05/22/two-step-authentication-in-firefox-accounts/>

Subdomain Behavior

Steps to reproduce:

1. Erase all passwords saved for *.deviantart.com.
2. Go to www.deviantart.com and log in. Save the password when prompted.
3. Log out
4. Return to the Deviantart homepage.
5. Click Log On. The saved password does auto-populate. (Do not complete login.)
6. Go to any artist's subdomain site (artistname.deviantart.com).
7. Click Log On. The saved password does not auto-populate.

https://bugzilla.mozilla.org/show_bug.cgi?id=589628

Password Generation

Does not generate passwords without extensions

Gives this advice on how to create strong passwords:

<https://support.mozilla.org/en-US/kb/create-secure-passwords-keep-your-identity-safe>

Step 1: Choose a phrase

Step 2: Add special characters

Step 3: Associate it with a website

Examples

#Hihas4ei:AmZ for Amazon

fCb#Hihas4ei: for Facebook

#Hihas4ei:YtB for YouTube

dRm#Hihas4ei: for Drumbeat

Databases

it is encrypted but metadata not encrypted - ~/.mozilla/firefox/[profile]/logins.json. Encryption key stored in ~/.mozilla/firefox/[profile]/key4.db (sqlite3). Can view usernames and passwords by going to Preferences/Privacy & Security/Saved Logins in plain text. Appears to use 3DES.

<https://dxr.mozilla.org/mozilla-release/source/security/nss/doc/html/pk12util.html>

```
{"nextId":4,"logins":[{"id":1,"hostname":"http://localhost:3000","httpRealm":null,"formSubmitURL":"http://localhost:3000","usernameField":"","passwordField":"","encryptedUsername":"MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECMStf2gttTH2BBD0wgK2YI5E0Xgg/wwgHGiO","encryptedPassword":"MDIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECKi6d/hnjd/HBAhFWCQUtubTUA==","guid":"{34c89f67-cd9d-4ab7-b78f-321724fa7f32}","encType":1,"timeCreated":1548290511308,"timeLastUsed":1548290511308,"timePasswordChanged":1548290511308,"timesUsed":1}]}
```

No difference to encrypted values after applying Master Password

Autofill

Browser prevents alert(); from iframe showing up in parent? No - it looks like Firefox literally fills in the fields as the page is rendered so that the onchange event is never fired - whoa - confirmed, alert(val) on page load has the password already filled in even for hidden iframe from another origin

Fills plain text

Does not require user interaction by default

Does not automatically submit by default

Will autofill login form with display: none; on another page

IFrame

Will autofill hidden IFrame on login page

Will autofill IFrame login page on another page

Will autofill IFrame login for another website (different origin), even if hidden

HTTPS

Will autofill

HTTP

Will autofill

Broken HTTPS

Will autofill

Bitwarden

Free	Premium
FREE forever	\$10 /year
We believe that security is important for everyone. The core features of Bitwarden are 100% free.	Upgrade your personal account to premium and unlock some great additional features.
Everything from a free account, plus:	Everything from a free account, plus:
<ul style="list-style-type: none">✓ Access & install all Bitwarden apps✓ Sync all of your devices, no limits!✓ Store unlimited items in your vault✓ Logins, secure notes, credit cards, & identities✓ Two-step authentication (2FA)✓ Secure password generator✓ Self-host on your own server (optional)	<ul style="list-style-type: none">✓ 1GB encrypted file storage✓ Two-step login with YubiKey, FIDO U2F, & Duo✓ Password hygiene & vault health reports✓ TOTP authenticator key storage & code gen.✓ Priority customer support
Create a FREE Account	★ Upgrade to Premium

PERSONAL USE		BUSINESS USE	
Free	Families	Teams	Enterprise
FREE forever	\$1 /month	\$5 /month	\$3 per user /month
share with a spouse or friend upgradeable at any time	includes 5 users sharing for family & friends	includes 5 users additional: \$2 per user /mo.	All teams features, plus:
<ul style="list-style-type: none">✓ Sharing for 2 users✓ Limit 2 collections✓ Unlimited shared items	<ul style="list-style-type: none">✓ Share with 5 users✓ Unlimited collections✓ Unlimited shared items✓ 1GB enc. file storage✓ Self-hosting (optional)	<ul style="list-style-type: none">✓ Unlimited users✓ Unlimited collections✓ Unlimited shared items✓ 1GB enc. file storage✓ Priority tech support	<ul style="list-style-type: none">✓ User groups✓ Directory sync✓ On-premise hosting✓ Event/audit logs✓ MFA with Duo Security✓ Users get premium
Create Account	Start Free Trial	Start Free Trial	Start Free Trial

Overview

Code completely open source (neat)

Encryption with end-to-end AES-256 bit, salted hashing and PBKDF2 SHA-256

Offers to save Card info / Identity / Secure Note

Can Sync Vault

Requires MP be length 8 - will give you a warning popup if the password is weak

Appear not to have a security assessment tool though the community is interested - <https://community.bitwarden.com/t/password-hygiene-report/206>

Default Settings

Autofill not enabled by default

Locks on Browser Restart by default - can set it to 'Immediately', 'Never', or anywhere from 1 min to 4 hours in intervals - can also click 'Lock Now' and lock yourself out :)

Two-step Login - security key, authenticator app, SMS, phone call or e-mail (with Premium - YubiKey, FIDO U2F, and Duo)

Fingerprint phrase (ex: alligator-transfer-laziness-macaroni-blue) - never changes and can be used to verify a new user before adding them to organization (verify end-to-end encryption securely initiated and nothing has been tampered with...)

Password Generation

Passwords

Default: length 14, A-Z/a-z/0-9 checked, !@#\$%^&* unchecked, Minimum Numbers 1, Minimum Special 1, Avoid Ambiguous Characters checked

Range: 5-128

You can 'Copy Password' but no 'Fill option' - no popup in the field either

Remember whatever settings it had last when you close / reopen - no 'save as default' option

Passphrase (ex: exclusive-galley-sprig)

Default: Number of Words 3, Word Separator - (can make this character whatever you want - just type it in)

Range: 3-20 with the widget (can get it to go as low as 1 by typing - entering 0 gives you 20 - entering huge number gives you 20)

Subdomain Behavior

For heroku apps only offers password for the full domain name

For the actual subdomain only offers one option (on localhost - sub.localhost.com, mail.localhost.com) - but if you go to the top level domain - localhost.com - offers multiple options

Databases

On Mac

Stores data in ~/Library/Application Support/Bitwarden/data.json

JSON file with key value pairs - the keys are mostly not encrypted, but the values are... Leaks your user e-mail by default in 'rememberedEmail' field for your bitwarden account. The last time the password was revised and last time vault synced is also stored in the open.
name/username/password/uri all encrypted.

When change the MP fields are updated - accessToken, some of the passwords (but not all) - have a diff of changes saved

Autofill

Not enabled by default - 'WARNING: This is currently an experimental feature. Use at your own risk'

Fills plain text

Does not require user interaction once enabled

Does not automatically submit - even if select site from within the extension

Will not autofill login form with display: none; on another page

IFrame

Will not autofill hidden IFrame on login page from another origin or for the same origin when there is already login form present

Will autofill IFrame login page on another page if visible for same origin and if invisible or visible for another origin (but it uses current origins credentials)

Will not autofill IFrame login for another website (different origin), even if hidden, with that sites credentials

HTTPS

Will autofill

HTTP

Will autofill

Broken HTTPS

Will autofill

KeePassX

KeePassX 2.0.3 - libgcrypt 1.7.3 / Qt 4.8.7

Overview

(passfoo)

Browser extensions / add-ons such as KeePass Tusk enable the use of KeePassX files in the browser with autofill - do not require KeePassX to be on the machine

Provide master key when create new database - file type .kdbx

No requirements for the master password and no master password meter

Very clear documentation about exactly how encryption works

Can use a 'keyfile' rather than an MP - however, they warn that while this may be a stronger key it is generally harder to keep secret

Does KeePassXC support two-factor authentication (2FA) with YubiKeys?

Yes and no. KeePassXC supports YubiKeys for securing a database, but strictly speaking, it's not two-factor authentication. KeePassXC generates a challenge and uses the YubiKey's response to this challenge to enhance the encryption key of your database. So in a sense, it makes your password stronger, but technically it doesn't qualify as a separate second factor, since the expected response doesn't change every time you try to decrypt your database. It does, however, change every time you save your database.

Default Settings

By default passwords do not expire, but can set expiration date

Can modify icon

Has Uuid, created, modified, accessed dates

Lock databases after inactivity of Not checked

Show passwords in cleartext by default not checked

Clear clipboard after ...10 sec checked

Password Generation

On MAC

Default Length: 16

A-Z,a-z,0-9 checked

Symbols unchecked

Exclude look-alike characters checked

Ensure the password contains characters from every group checked

Can define your own character sets...

If you change settings and reopen it remembers your changes - no default or 'set as default'
However, if you close the entire program and reopen it goes back to default

Databases

Encrypts whole database - not only passwords - .kdbx

Stores files wherever you choose - produces .kdbx file and a .kdbx.lock file (MAC) - some documentation said lock file not normal for 2.x

Lock file contains process id, name of the machine and string 'keepassx' - lock file vanishes when keepassx is closed

Changed MP and the encrypted file contents also changed

AES / Rijndael 256 bit encryption (NIST FIPS 197)

ChaCha20 256 bit (RFC 7539)

HMAC-SHA-256 hash of ciphertext (Encrypt-then-MAC scheme)

Autofill

N/A

KeePassXC

KeePassXC 2.3.4 - libgcrypt 1.8.3 / Qt 5.11.1

Overview

(XC1 - ab)

Cross-platform and Open Source

Very tight coupling between the browser extension and the Desktop client

Browser Extension

When connected extensions to keepassxc desktop receive an 'association request' for a generated key - must give it a unique name - your browser settings are then stored in your keepassxc .kdbx file (whichever one you are connected to when you establish the link)

Desktop client must be running for the extension to receive the passwords - Cannot receive generated password. Is KeePassXC running?

Client provides a popup directing you to the extension icon in order to change credentials - directs user to appropriate action

Creates separate group for browser passwords within the database

Does not offer a popup to save password - have to actually click on the extension icon

Default Settings

Desktop UI

Clear clipboard after 10 sec checked

Lock database after inactivity of Unchecked

Lock database when session is locked or lid is closed checked

Hide passwords in the preview panel checked

Not Checked

Lock database after minimizing window

Don't require password repeat when it is visible

Show passwords in cleartext by default

Use Google as fallback for downloading website icons

Browser

Inherits desktop settings for PW generator and others

Activate password generator checked - adds button for generating new password - remains there even if password already exists

Automatically retrieve credentials checked - when tab loaded grabs credentials from desktop client

Automatically fill in single-credential entries - not checked - 'Warning! Using auto-fill is not safe. Use at your own risk' highlighted in red

☐ Automatically fill in single-credential entries.

Let KeePassXC-Browser automatically fill in credentials if it receives only a single entry.

Warning! Using auto-fill is not safe. Use at your own risk.

Activate autocomplete for username fields checked

Show notifications checked - these notifications actually appear on desktop client rather than as browser popups

Save domain only checked - when saving credentials - save only the domain instead of the full URL - it does includes subdomain when it saves

Check for updates - every 3 days checked (every week, month, never also options)

Automatically fill in HTTP Basic Auth dialogs and submit them not checked

Sites on this page have special handling methods associated with them.

To ignore new/modified credentials on a specific site, add them below or click the blinking KeePassXC-Browser icon and select *Never ask for this page*.

If a site is fully ignored (*Disable all features* is selected), then the plugin will do nothing when visiting that site.

Username-only detection allows KeePassXC-Browser to fill in login details on websites with separate pages for username and password.

Add URL manually:

Page URL	Ignore	Username-only Detection	Delete
No ignored sites found.			

Subdomain Behavior

Does distinguish between subdomains (heroku)

Password Generation

Provides entropy value and strength meter

On Windows

Default Length: 16

A-Z,a-z,0-9 checked

Symbols unchecked

Exclude look-alike characters checked

Pick characters from every group checked

Extended ASCII option

Can also generate Passphrase

Default word count: 7

Can define custom word separator - default is space

If you change settings and reopen it remembers your changes - no default or 'set as default'

Still remembers even if you close entire program and reopen

Online password generator uses the same generation settings as the desktop client - can 'Generate', 'Copy', or 'Fill and Copy'

The icon in the far right of the password input box is a green key - it only generates passwords - it does not offer the available login options (which is what most other PWMs do - this could be a bit confusing)

Databases

Encrypts whole database - not only passwords - .kdbx

Stores files wherever you choose - produces .kdbx file but no lock file

Changed MP and the encrypted file contents also changed

The complete database is always encrypted with the industry-standard AES (alias Rijndael) encryption algorithm using a 256 bit key.

Autofill

Off By Default

Off

Can select the username field and click on option from dropdown menu or click the extension icon and select

If click the extension icon and select, it will fill in a hidden iFrame with the same username / password - even one from another domain

Won't fill in iFrames or invisible login

On

Will not autofill invisible login

Will not autofill hidden iFrame on login page for another domain (if login form visible)

Will autofill hidden iFrames for same origin and other origins on other webpages with the appropriate credentials