Dooble Web Browser

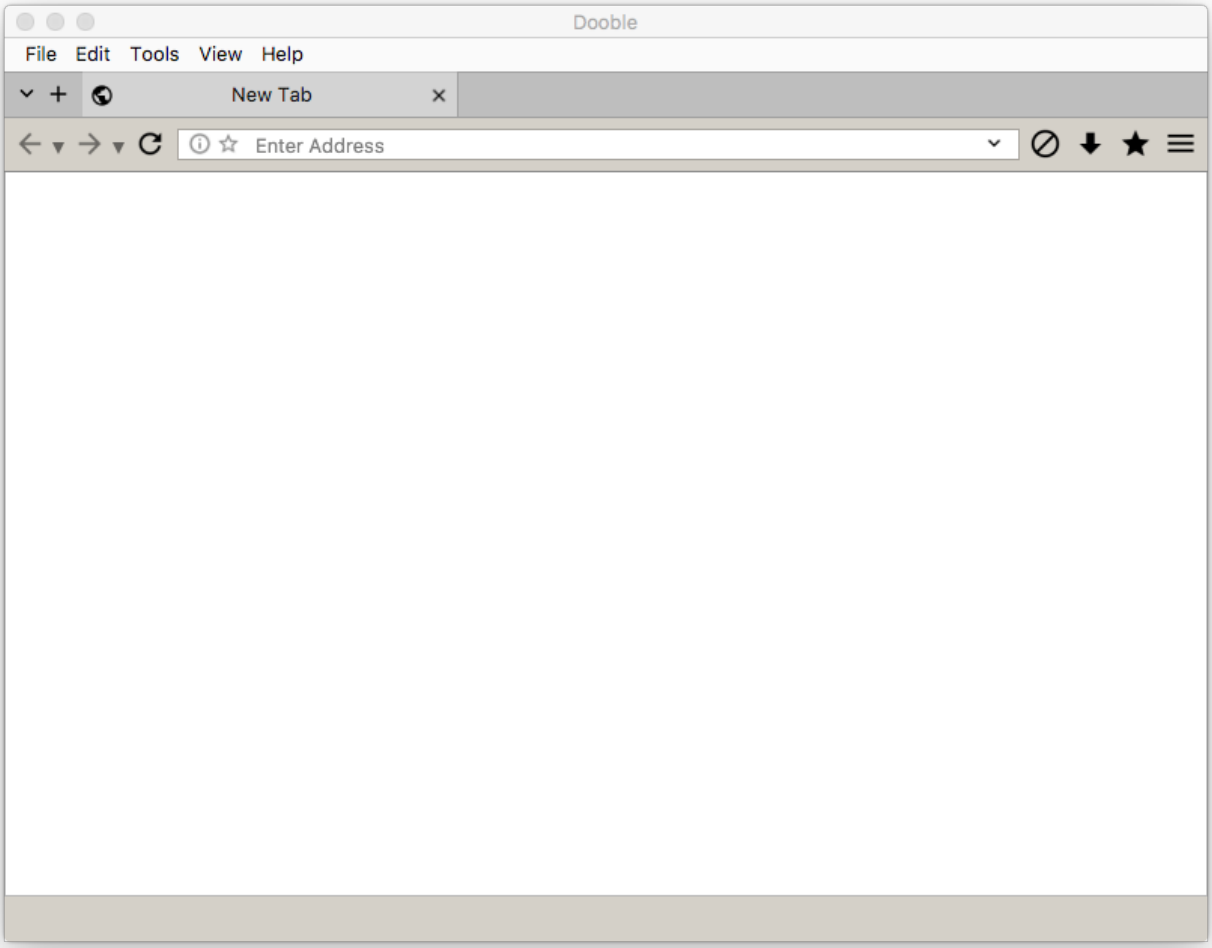
Version 2.2 (2017.12.25)

Table of Contents

Introduction

An elegant, simple, and zero-dependency Web browser. Dooble should be functional on any operating system where Qt 5.9.x is supported.

The source is readily available at https://github.com/textbrowser/dooble/tree/master/2.x.



AES Implementation

The AES implementation is derived from the guidelines provided by http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf. The implementation is independent of architecture.

Accepted / Blocked Domains

Dooble supports the accepting and blocking of specific domains. The Accepted / Blocked Domains window allows for the defining of domains which are to be accepted or blocked. Domains are stored in the SQLite database dooble_accepted_or_blocked_domains.db. An operating mode may also be prepared within this window. Supported operating modes are defined below.

Accept Mode

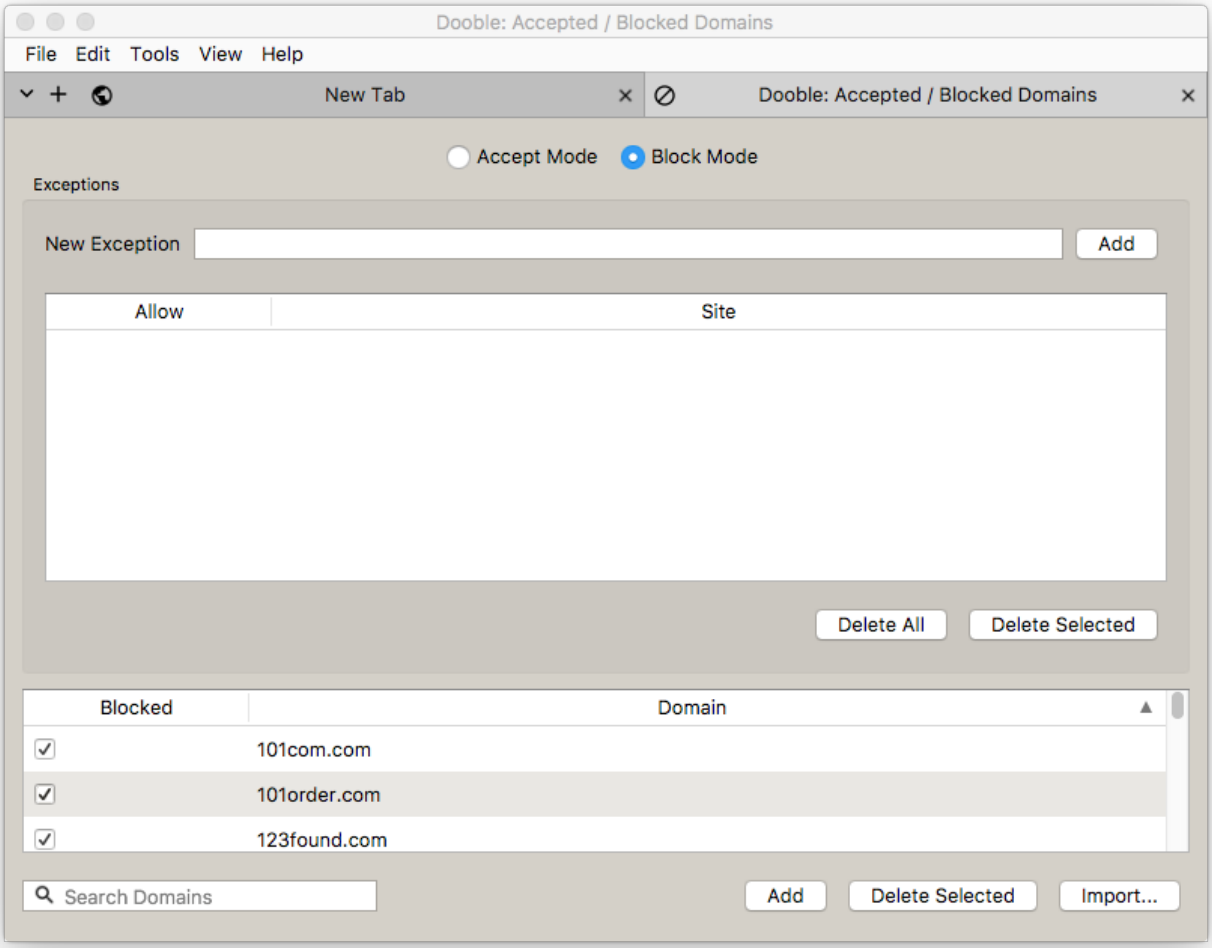
Only the specified domains may be accessed either directly or indirectly.

Block Mode

The specified domains are blocked. While in this mode, Dooble will prevent direct and indirect access to the listed domains.

Note: Defined domains reside in a container which is optimized for rapid (amortized O(1)) discovery.

Note: The bundled Data directory contains the file dooble_accepted_blocked_domains.txt. An import feature is included.


Dooble: Accepted / Blocked Domains
File Edit Tools View Help
New Tab
Dooble: Accepted / Blocked Domains
Accept Mode
Block Mode
Exceptions
New Exception
Add
Allow
Site
Delete All
Delete Selected
Blocked
Domain
101com.com
101order.com
123found.com
Search Domains
Add
Delete Selected
Import...

Address Widget

The address widget contains the current page’s URL. The present URL may be inserted in the Favorites container.

The current site’s cookies may be accessed via a context menu. The context menu also allows for the removal of the current site’s certificate exception, if one has been previously accepted.

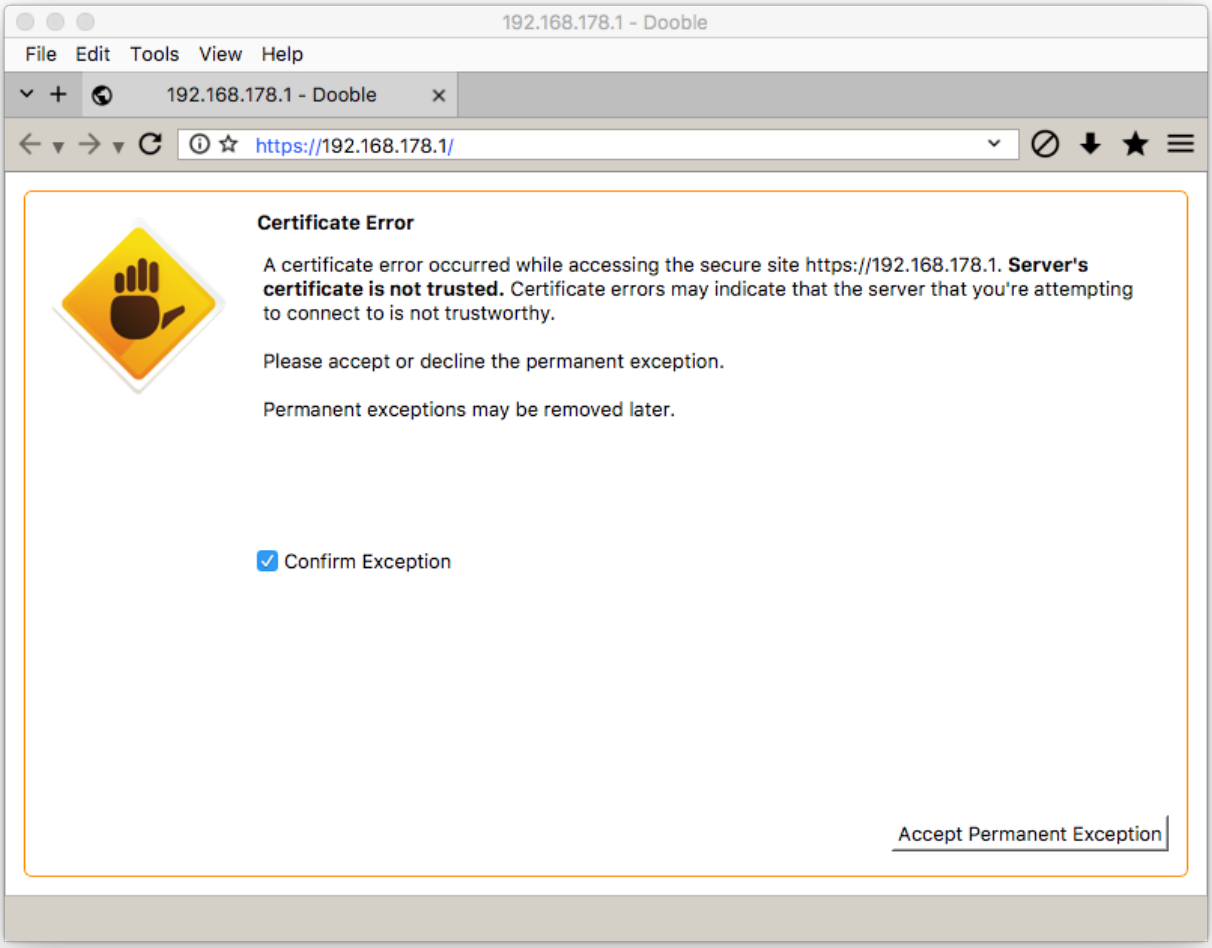
Note: All address widgets share two common history containers resulting in memory reduction and rapid (amortized O(1)) discovery of history items. The containers are required for displaying previously-accessed URLs in address widgets.

Note: Dooble applies the Levenshtein Distance algorithm during the history discovery process.

Note: Private windows record visited links in the internal history containers.

Certificate Exceptions

Web sites may raise SSL/TLS certificate errors. Some of these certificate errors may be overridden.

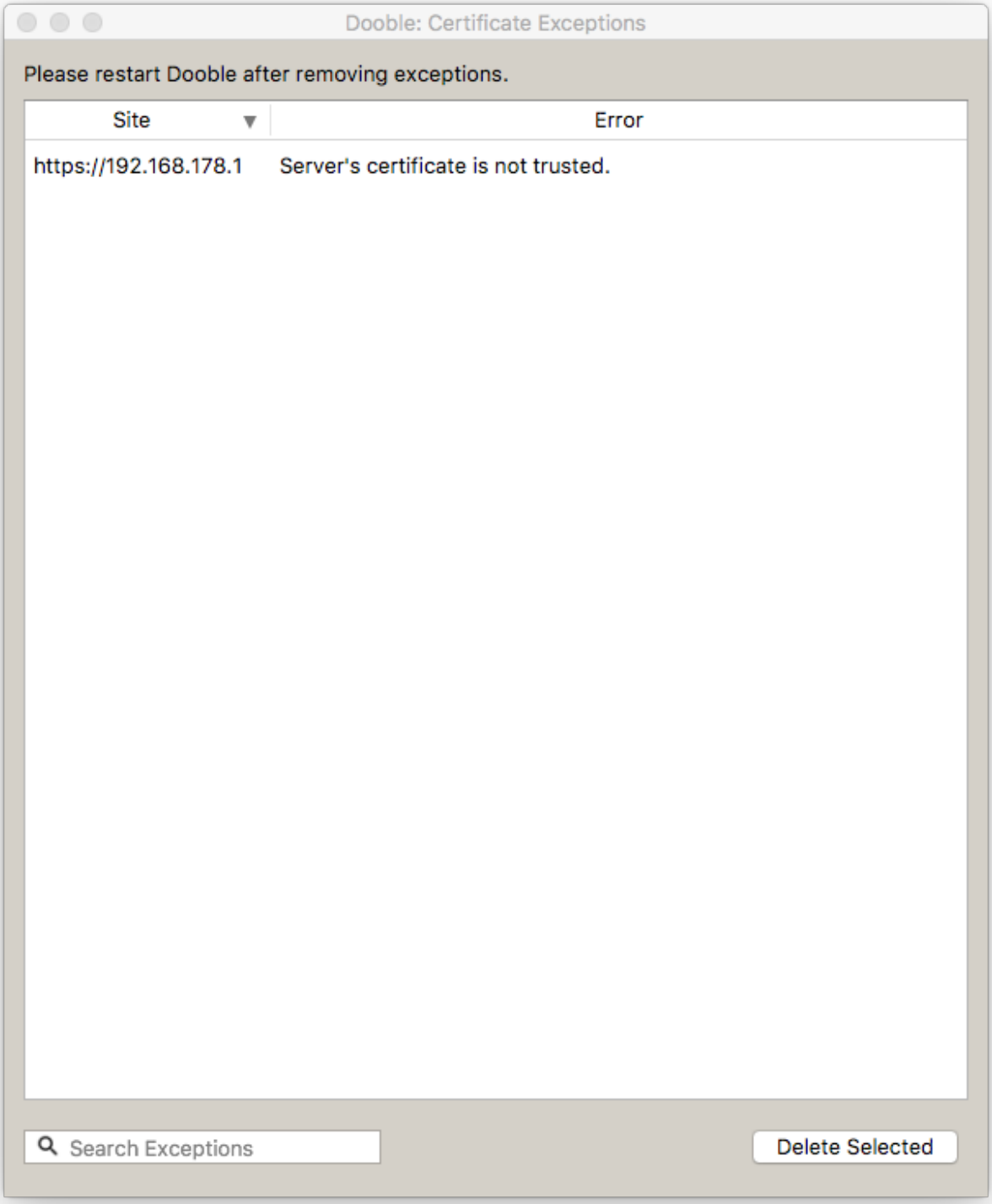


Once overridden, the Web site and the certificate error are recorded in the SQLite database dooble_certificate_exceptions.db.

Overridden sites are presented in the Certificate Exceptions window. Within this window, exceptions may be revoked.

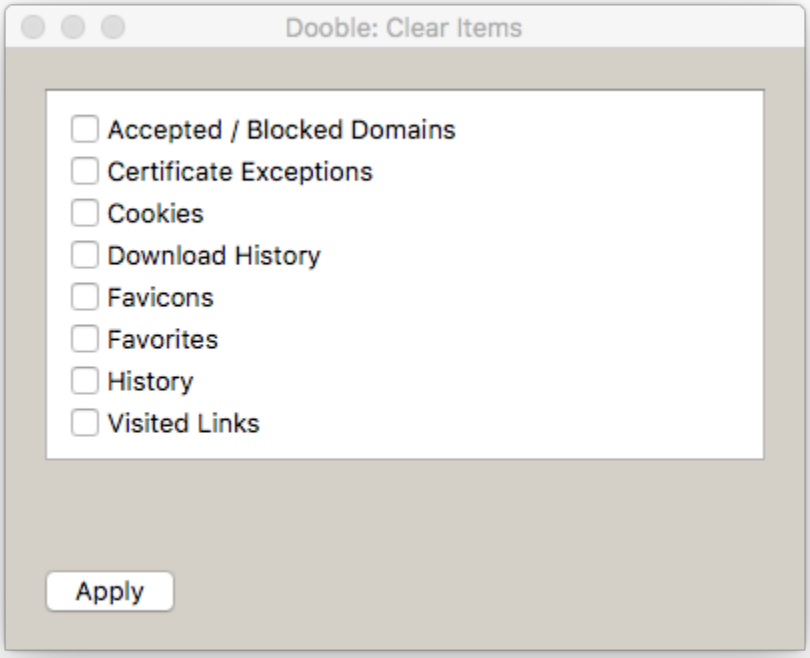
Note: Certificate errors may be raised by third-party requests.

Note: Version 2.00 of Dooble allows for a single certificate exception to be defined for a given URL. Future revisions may allow for multiple exceptions.


Dooble: Certificate Exceptions
Please restart Dooble after removing exceptions.
Site
Error
https://192.168.178.1
Server's certificate is not trusted.
Search Exceptions
Delete Selected

Clear Items

The Clear Items modal dialog may be used to remove an assortment of content.


Dooble: Clear Items
Accepted / Blocked Domains
Certificate Exceptions
Cookies
Download History
Favicons
Favorites
History
Visited Links
Apply

Cookies

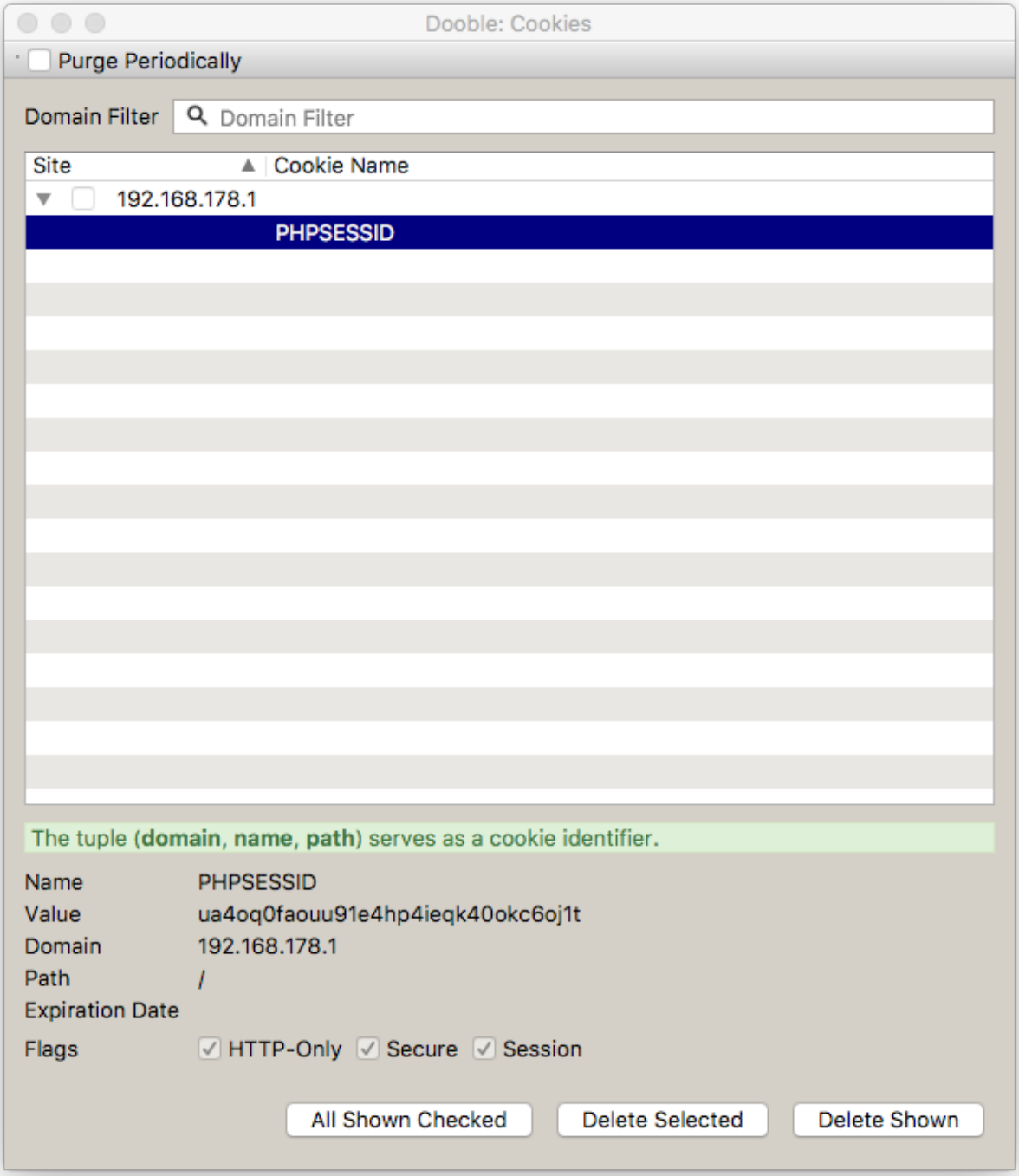
The Cookies window depicts Dooble’s current cookies. The SQLite database dooble_cookies.db contains cookie data.

Domain Filter

If set, only the specified domain's cookies are displayed.

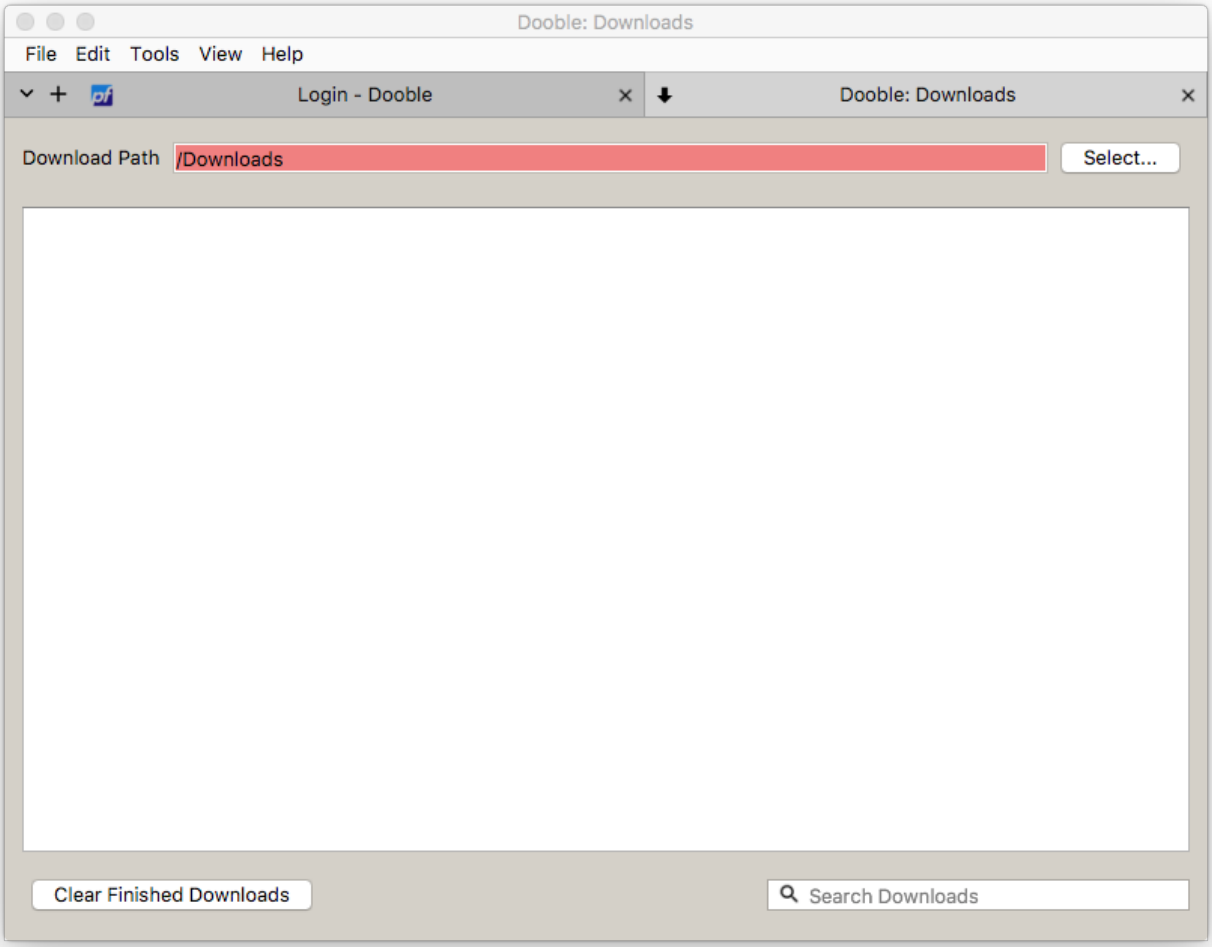
Purge Periodically

If enabled, unchecked domains will be purged every 15 seconds. Purging occurs in the main thread.


Dooble: Cookies
Purge Periodically
Domain Filter
Domain Filter
Site
Cookie Name
192.168.178.1
PHPSESSID
The tuple (domain, name, path) serves as a cookie identifier.
Name
PHPSESSID
Value
ua4oq0faouu91e4hp4ieqk40okc6oj1t
Domain
192.168.178.1
Path
/
Expiration Date
Flags
HTTP-Only
Secure
Session
All Shown Checked
Delete Selected
Delete Shown

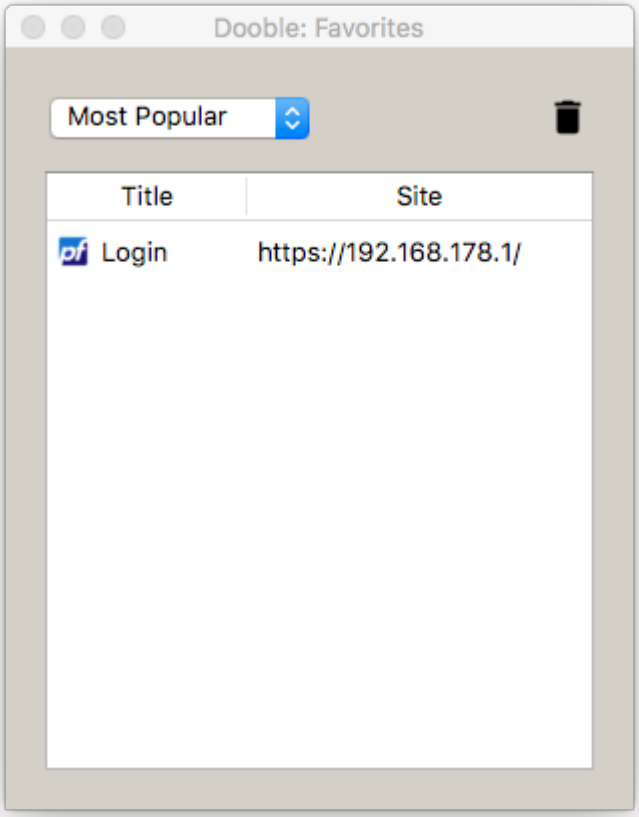
Downloads

Dooble supports the downloading of data. Active and inactive downloads are depicted in the Downloads window. Active downloads may be canceled. Files associated with canceled downloads are discarded. Dooble does not provide a mechanism for restarting a canceled or interrupted download. Downloads data are stored in the SQLite database dooble_downloads.db.



Favorites

Favorites are replacements of bookmarks. Included in the Favorites non-modal dialog are various sort options. Favorites, along with history items, are stored in the SQLite database dooble_history.db.



File Menus

Dooble offers a traditional menu bar. The menu bar's visibility may be configured via the Display panel in the Settings window. If the menu bar is permanently hidden, its visibility may be modified via the F10 key. Some menu options include mnemonics and shortcuts.

File

The File menu includes several basic functions.

Authenticate

If permanent credentials are defined, this option is enabled. An authentication dialog is displayed if the option is selected. If credentials are correctly authenticated, global containers are populated. Please note that interface components must be populated via the main thread and this activity may burden Dooble.

New Private Window

Open a new private window. Please also read the **Private Windows** section for details on private browsing.

New Tab

A new tab is appended to the end of the tab widget.

New Window

Open a new window.

Save

Save the current page. The action invokes a download request. A file-selection dialog is not displayed.

Close Tab

Close the current tab. If the current tab is the only Dooble tab and active downloads exist, a confirmation prompt is displayed.

Print

A modal print dialog is displayed.

Print Preview

Not implemented. Permanently disabled.

Exit Dooble

Exit Dooble. A confirmation prompt is displayed if active downloads exist.

Edit

Clear Items

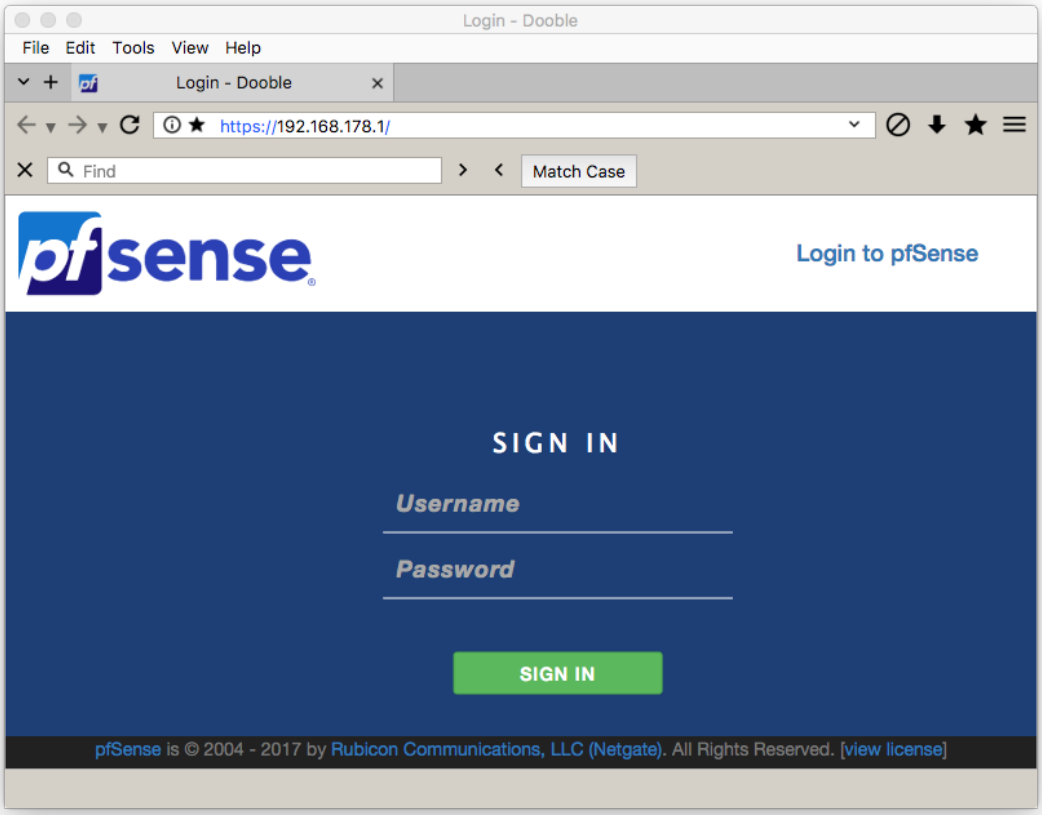
Display an instance of the modal Clear Items dialog.

Clear Visited Links

Remove contents of the local Visited Links file.

Find

Enables the Find panel.



Settings

Display the Settings window.

Tools

Accepted / Blocked Domains

Display the Accepted / Blocked Domains window.

Certificate Exceptions

Display the Certificate Exceptions window.

Cookies

Display the global Cookies window. If the window is a private window, the private window's cookie container is displayed.

Downloads

Display the Downloads window.

Favorites

Display the Favorites non-modal dialog.

History

Display the History window.

View

Show Full Screen

Disable or enable full-screen mode.

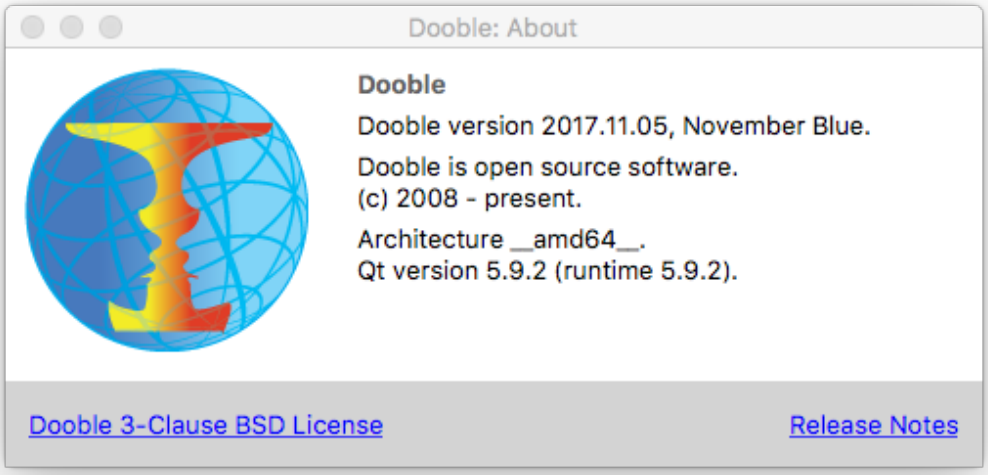
Show Status Bar

Hide or show the status bar.

Help

About

Display the non-modal About dialog.

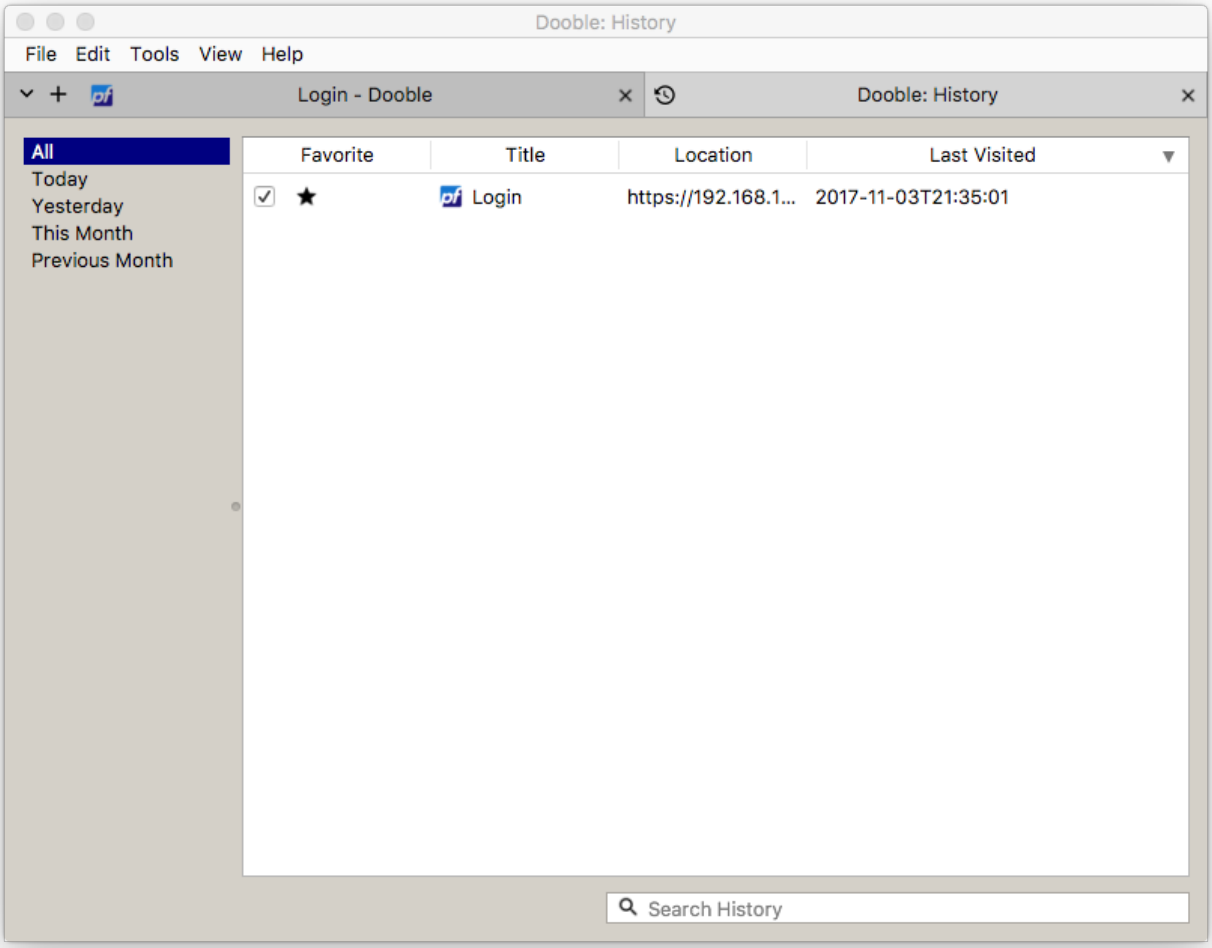


Documentation

Display this document in a Dooble tab.

History

The History window is a general-purpose container depicting Dooble’s browsing history. A simple search is included. Selected items may be removed via a context menu. The SQLite database dooble_history.db contains history data, along with favorites data.


Dooble: History
File Edit Tools View Help
Login - Dooble
Dooble: History
All
Today
Yesterday
This Month
Previous Month
Favorite
Title
Location
Last Visited
Login
https://192.168.1...
2017-11-03T21:35:01
Search History

Performance and Security Considerations

- Accepted / Blocked domains are stored in a container that’s designed for rapid (amortized O(1)) discovery.
- Authentication is interruptible.
- Constant byte-by-byte comparisons are implemented wherever cryptographic digests are involved.
- Cryptographic keys are zeroed on destruction. Sensitive fields are cleared after use. Please note that these processes do not guarantee that sensitive data is destroyed effectively.
- Dooble does not exercise secure memory.
- History items are safely purged within a dedicated thread.
- The AES and Threefish implementations are not designed to be thread-safe.
- The process of preparing credentials may be interrupted.

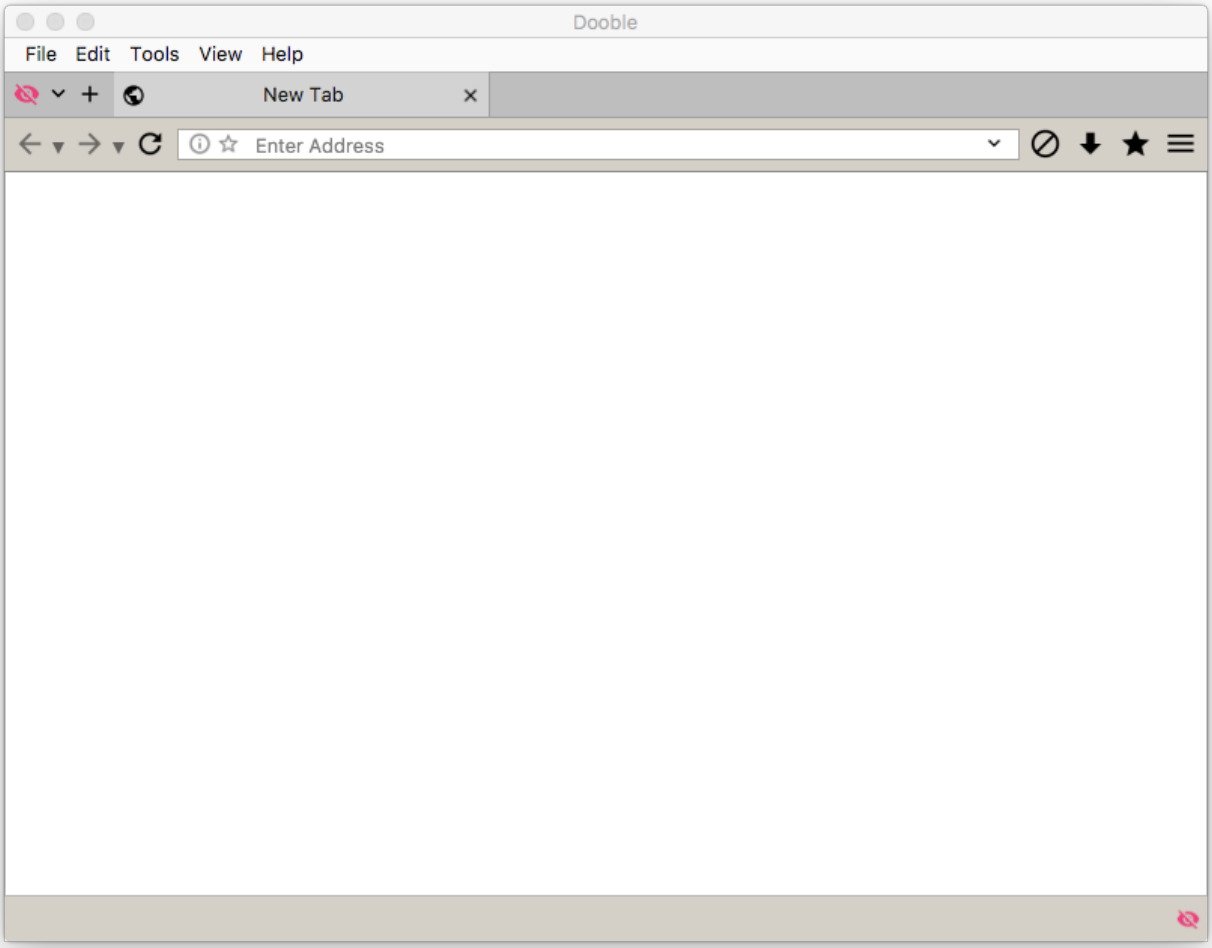
Private Windows

When browsing in private windows, Dooble does not save the following data:

- Cookies
- Favicons
- History
- Temporary Files
- Visited Links

While in private windows, Dooble does save:

- Downloads
- Favorites



Settings

This section describes some of the areas of the Settings window. Settings values are stored in the SQLite database dooble_settings.db.

Display

Pin Windows

Some support windows may be pinned. Pinning is the process of embedding support windows within a Dooble window.

History

A dedicated thread determines if browsing history has expired. The thread is also responsible for removing expired history data. The thread is safely canceled upon termination of Dooble.

Privacy

Credentials

Dooble provides a process of storing authentically-encrypted data in various databases. This process is completely optional. Three separate modes are included:

Disabled

This is the default mode. In this mode, Dooble stores data in cleartext.

Enabled with a Password

Dooble shall permanently store data in authentically-encrypted containers using credentials generated via the provided password.

Enabled without a Password

Dooble shall store private data in authentically-encrypted containers using session credentials. The data will not be available in future sessions.

Additional specifics are listed bellow.

CBC is the preferred cipher mode of operation.

SHA3-512 is the favored hash algorithm.

The password must contain at least 1 character.

The process is interruptible.

The pseudo-random password salt is composed of 64 bytes.

Web

Local Storage

Required for HTML5 storage.

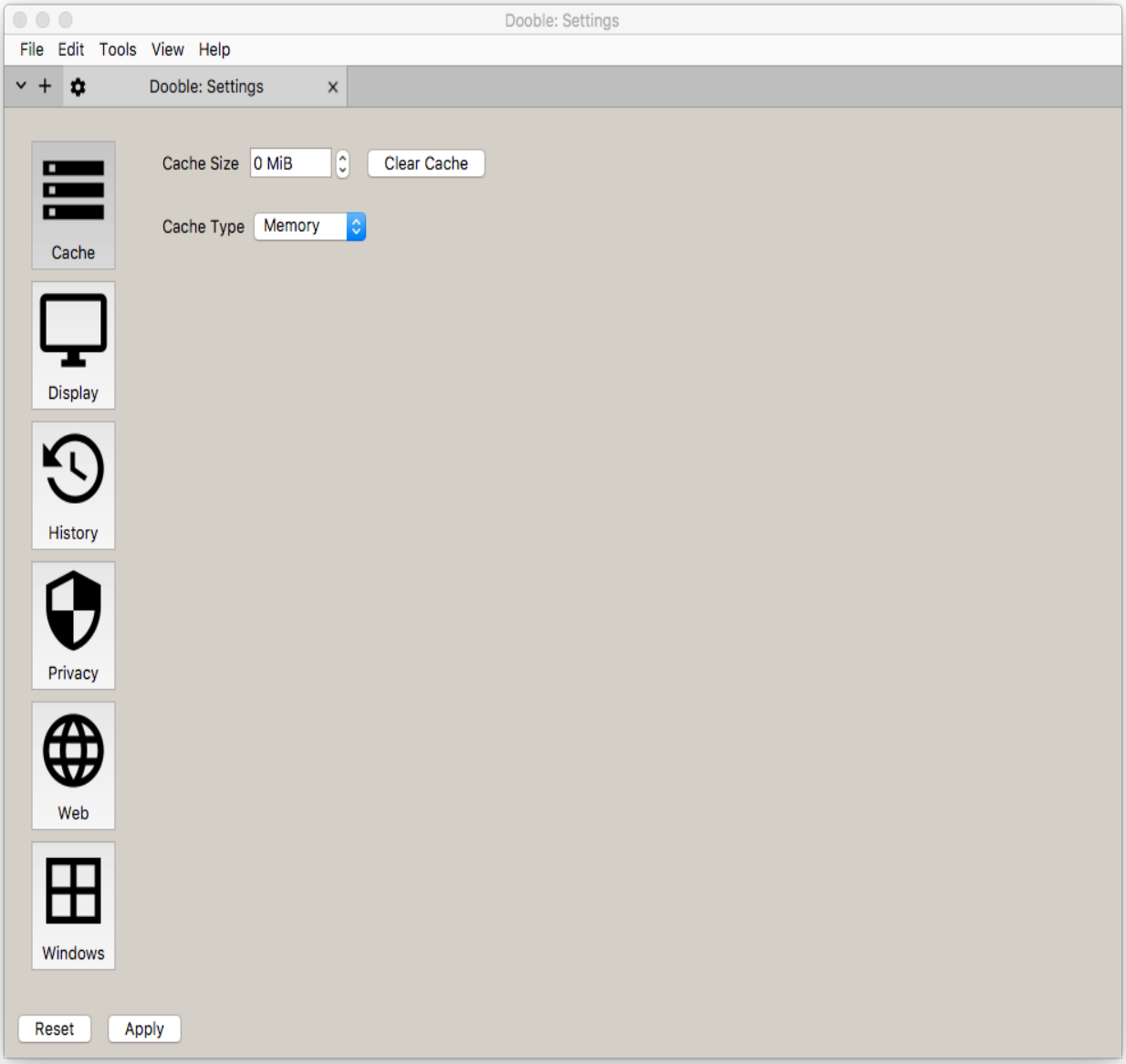
User Agent

The user agent is sometimes used for content negotiation between the client and server. The initial value is system-dependent. To reset, please clear the field and press the Apply button.

XSS Auditing

Per Qt’s documentation, XSS Auditing monitors load requests for cross-site scripting attempts. Suspicious scripts are blocked.

Note: Dooble does not remove the local WebEnginePersistentStorage directory during a reset. Please remove this directory after a reset completes.


Dooble: Settings
File Edit Tools View Help
Dooble: Settings
Cache
Display
History
Privacy
Web
Windows
Cache Size 0 MiB
Clear Cache
Cache Type Memory
Reset
Apply

Sources of Randomness

Dooble requires data streams of random data for an assortment of cryptographic algorithms. This section briefly describes the sources of these data streams for various operating systems.

BSD

BSD-like systems acquire pseudo-random data from the /dev/random device.

Linux

Linux systems acquire pseudo-random data from the /dev/urandom device.

Windows

Please read https://msdn.microsoft.com/en-us/library/windows/desktop/aa379942(v=vs.85).aspx.

Supported Protocols

Dooble supports the FILE, FTP, GOPHER, and HTTP(S) protocols.

Threefish Implementation

The Threefish implementation is derived from the guidelines provided by http://www.skein-hash.info/sites/default/files/skein1.1.pdf. The implementation is independent of architecture.

Translations

Translations are incomplete. Translating Dooble is quite simple. Please download and install Qt from https://download.qt.io, download Dooble's source, and become an expert in Qt's Linguist. Linguist documentation exists at https://doc.qt.io/qt-5/qtlinguist-index.html.