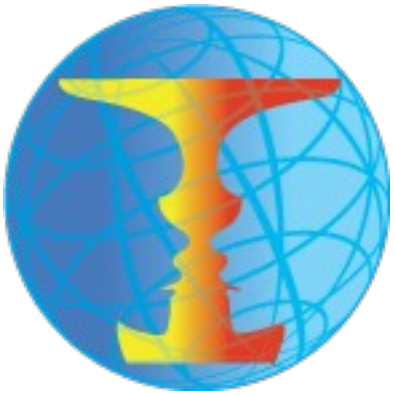


Dooble

A Web Browser

Table of Contents

Introduction

Dooble is an elegant, portable, and zero-dependency Web browser. The application should be functional on any operating system where the newest Qt is supported.

The source is readily available at https://github.com/textbrowser/dooble.

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.

Third-Party Session Rejections

The section contains links of third-party cookies which were rejected by Dooble.

Note: Defined domains also reside in a session container which is optimized for rapid (amortized O(1)) discovery. The special container contains all of the defined domains.

Note: The bundled Data directory contains the file dooble_accepted_or_blocked_domains.txt. An import feature is included in the Accepted / Blocked Domains window. An import will enable (Blocked or Accepted) existing domains.

Address Widget

The address widget contains the current page's URL. The present URL may be inserted in the Favorites container by pressing the favorites (star) tool button.

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 non-private certificate exception if a certificate exception has been previously accepted.

Note: All address widgets share a common history container. The container is optimized for rapid (amortized O(1)) discovery of history items and is required for displaying previously-accessed URLs in address widgets.

Note: Certificate exceptions are not available for private URLs. That is, if a certificate exception is accepted from a private window, the exception is only available within that window. Other non-private and private Dooble windows will not have insight into the accepted certificate exception.

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

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

Application Locking

A Dooble session may be locked via a tab’s context menu’s Lock Application action. The Lock Application action is disabled if credentials have not been prepared.

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 unless the parent window is a private window. For private windows, certificate exceptions exist only within such windows.

Overridden non-private 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: Dooble allows for a single certificate exception to be defined for a given URL. Future revisions may allow for multiple exceptions.

Note: Private windows will also interrogate permanent certificate exceptions. If a permanent certificate exception is discovered for the given private URL, the particular Web site will be loaded by the private page.

Clear Items

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

Command-Line Options

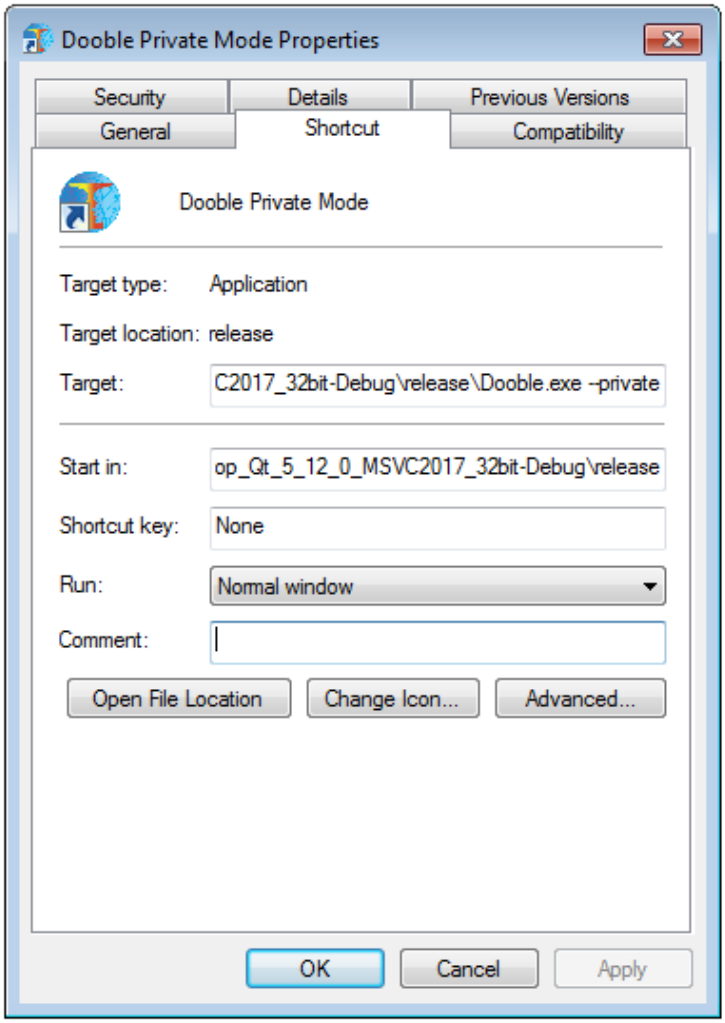
The command-line option --load-url is supported by Dooble. Multiple instances are allowed.

The command-line option --private is supported by Dooble. If provided, the first Dooble window will be a private window.

The command-line option --test-aes may be used to test the AES implementation. See also –test-aes-performance.

The command-line option --test-threefish may be used to test the Threefish implementation. See also –test-threefish-performance.

Windows users, please create a shortcut to the Dooble.exe file and add the --private option to the Target field.



Other command-line options are available via WebEngine. Please read https://peter.sh/experiments/chromium-command-line-switches/. The option disable-reading-from-canvas may be of interest.

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 on the main thread.

Debian

The Debian package may be GPG-signed. This section describes the process of verifying the digital signature.

First, create a special directory.

> mkdir 66E6A4C70DA51DCD

Next, install debsig-verify via aptitude.

> sudo apt install debsig-verify

Then, copy the bundled file Documentation/dooble.pol to 66E6A4C70DA51DCD.

> cp Documentation/dooble.pol 66E6A4C70DA51DCD

Import the bundled public key Documentation/dooble.asc.

> gpg --no-default-keyring --keyring 66E6A4C70DA51DCD/debsig.gpg --import Documentation/dooble.asc

Finally, verify the Debian package.

> debsig-verify --keyrings-dir . --policies-dir . ./Dooble-2019.01.15_amd64.deb

Results should be similar to the following.

debsig: Verified package from 'Dooble' (Text Browser)

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 provides a mechanism for restarting a canceled or interrupted download if the application is generated using Qt 5.10.x and newer. 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.

Close Tab

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

Open URL

Place focus on the URL widget.

Save

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

Print

A modal print dialog is displayed.

Print Preview

Display a preview of the current page.

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 from the local Visited Links file.

Find

Enables the Find panel.

Settings

Display the Settings window.

Vacuum Databases

Vacuum local SQLite databases.

Tools

Accepted / Blocked Domains

Display the Accepted / Blocked Domains window.

Certificate Exceptions

Display the Certificate Exceptions window.

Charts

Display a sub-menu of available charts. Charts are disabled if Dooble was built without the QtCharts module.

Cookies

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

Downloads

Display the Downloads window.

Favorites

Display the Favorites non-modal dialog.

Floating Digital Clock

Display a digital clock dialog.

History

Display the History window.

Inject Custom Style Sheet

Also available off of the address widget. Allows custom style sheets to be injected into individual pages.

Search Engines

Display the Search Engines window.

View

Show Full Screen

Disable or enable full-screen mode.

Show Status Bar

Hide or show the status bar.

History

Clear History

Clear the history.

History

Show the History window.

Help

About

Display the non-modal About dialog.

Documentation

Display this document in a Dooble tab.

Release Notes

Display Dooble’s release notes in a separate 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.

Note: Purged items are not automatically removed from the History window during a session. Subsequent sessions will represent the most current contents of dooble_history.db.

Miscellaneous

The environment variable DOOBLE_HOME is supported. If correctly set, Dooble files will reside in DOOBLE_HOME.

Performance and Security Considerations

- Accepted / Blocked domains are stored in a container that’s designed for rapid (amortized O(1)) discovery. The container is populated during the initialization of Dooble.
- Authentication may be interrupted.
- 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 are destroyed effectively.
- Dooble attempts to lock secret keys into RAM, if mman is available.
- Dooble populates icons of table items only when required. The software inspects respective views and determines the entries which require icons.
- History items are safely purged within a dedicated thread.
- Initial gathering of History data is performed by a thread.
- Processing large quantities of icon data will certainly burden most software applications. Dooble provides an innovative solution. Address widgets, the Favorites window, the History window, and the Search Engines window implement an intelligent algorithm which causes Dooble to load only the icon data of visible items. Once loaded, the icon data are cached. Also included are SQLite database indexes. This innovative solution produces exceptionally-smooth rendering of important data.
- Some SQLite database writes occur without synchronization. Future releases will introduce synchronization.
- 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:

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

While in private windows, Dooble does save:

- Downloads
- Favorites

Settings

This section describes some of the interesting 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.

UTC Time Zone

Set the environment variable TZ to UTC.

Web

Local Storage

Required for HTML5 storage.

User Agent

The user agent is sometimes used for content negotiation between the Dooble client and a server. The initial value is system-dependent. To reset, please clear the field and press the Apply button. Please reset the field whenever new Qt products are provided.

WebRTC Public Interfaces Only

Limits WebRTC to public IP addresses. If disabled, remote hosts may be able to detect local IP addresses.

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.

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

See QRandomGenerator.

Linux

See QRandomGenerator.

Windows

See QRandomGenerator.

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.

Web Page Features

Some pages may submit requests for accessing local devices. When a feature request is received by Dooble, a notification is displayed. A request may be accepted or denied. The URL and the policy are recorded after a transaction completes. Existing entries may be reviewed via the Web panel of the Settings window.

Please note that a notification is displayed only for the first received request for a given page during a page load. That is, received requests are not queued. If a request is received while a request is pending, the received request is denied and an entry is added to the Features Permissions panel of the Web section in the Settings window.

Windows Compilation

As of October 4, 2018, Qt 5.11.2 requires Windows Studio 2017. Please download the Community edition from https://visualstudio.microsoft.com/downloads/.