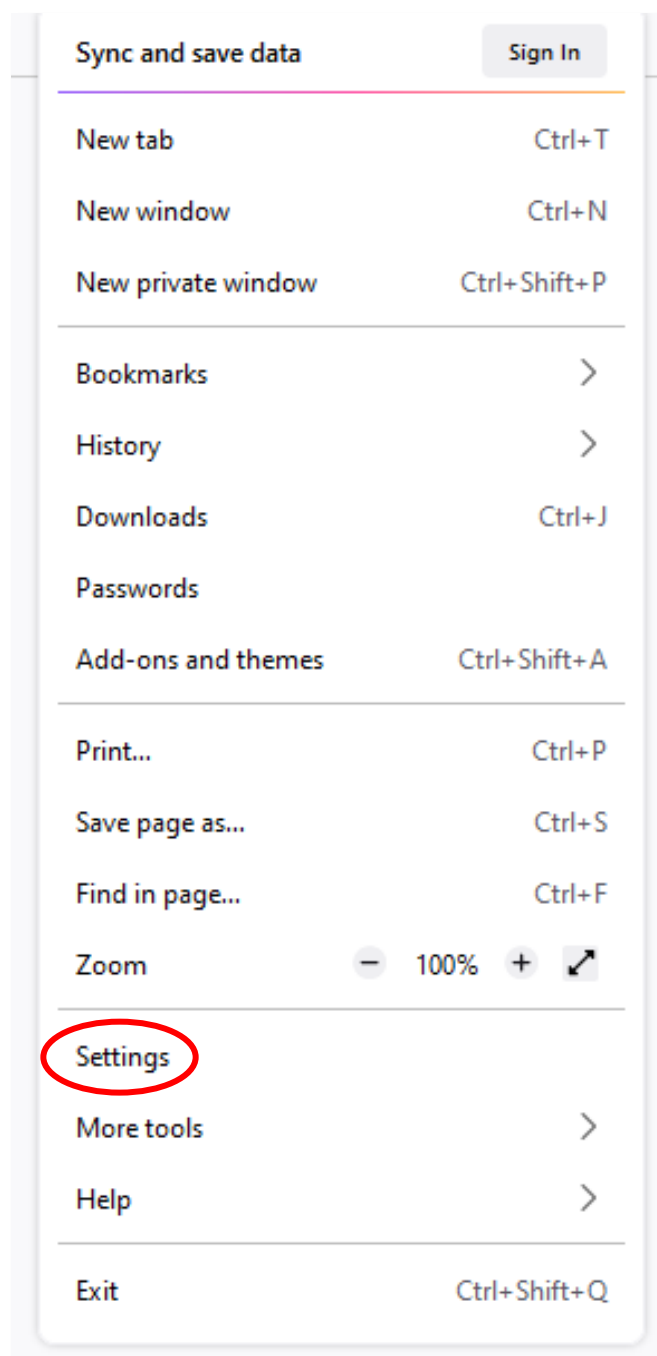
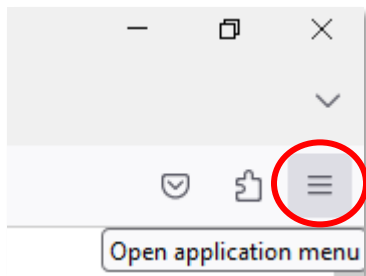




PRIVACY SETTINGS FOR FIREFOX

In Firefox from Mozilla, you can adjust the appropriate settings via **Open application menu > Settings > Privacy and Security**.





So, for example for **Tracking Protection**.

Here it is set to **Standard**, but you can set it yourself, for example to strict or custom.

Browser Privacy

Enhanced Tracking Protection

Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts. [Learn more](#)

Standard

Balanced for protection and performance. Pages will load normally.

Firefox blocks the following:

- Social media trackers
- Cross-site cookies in all windows
- Tracking content in Private Windows
- Cryptominers
- Fingerprinters

Includes Total Cookie Protection, our most powerful privacy feature ever

Total Cookie Protection contains cookies to the site you're on, so trackers can't use them to follow you between sites. [Learn more](#)

Strict

Stronger protection, but may cause some sites or content to break.

Custom

Choose which trackers and scripts to block.



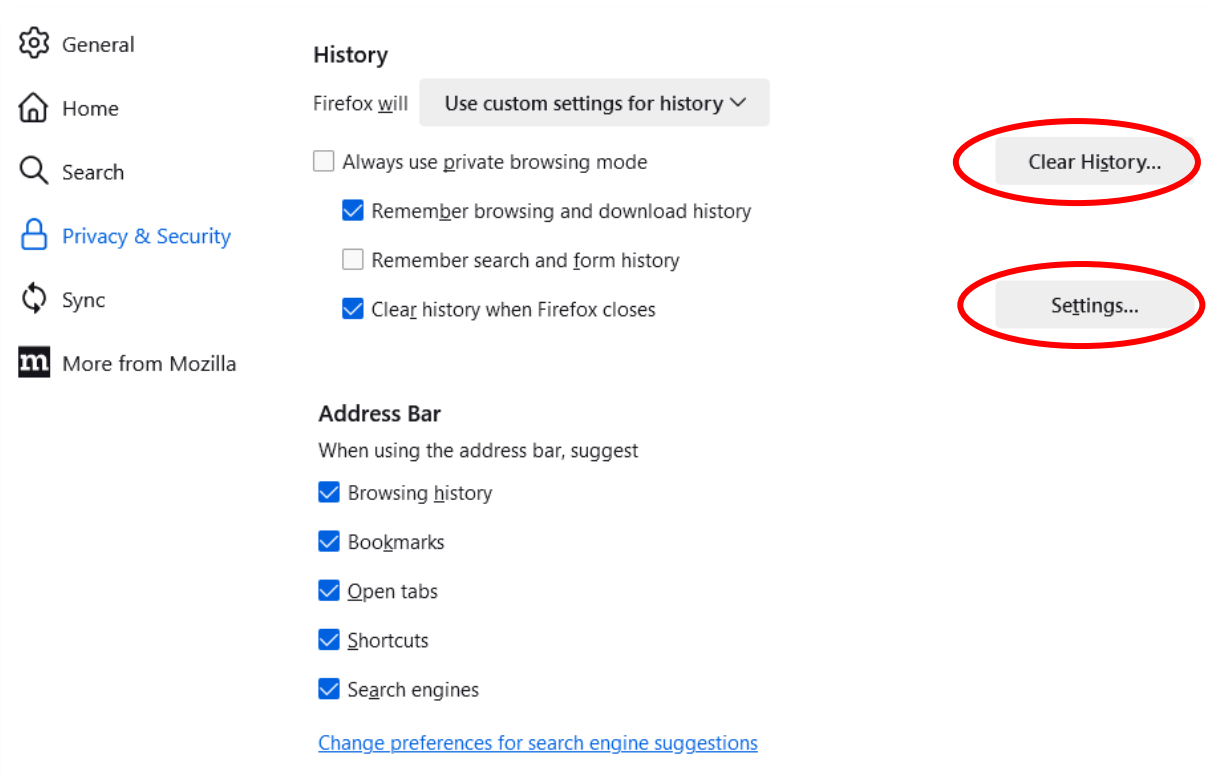
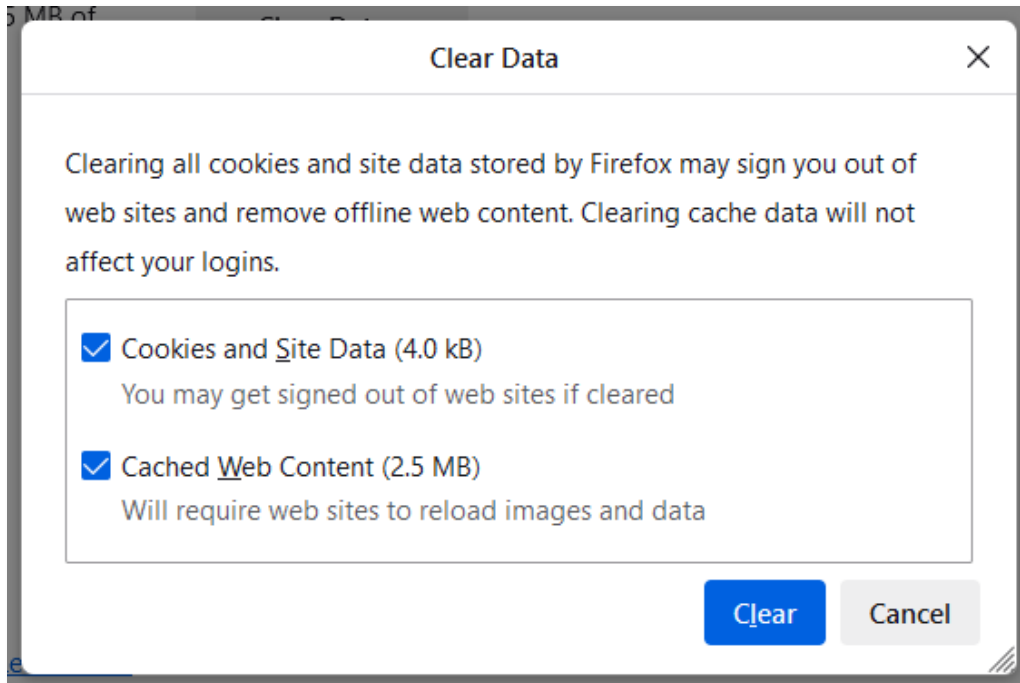
A little bit further down you can adjust the settings for **Cookies and Site Data**, so for example **Clear Data**.

The screenshot shows the Firefox Settings interface. On the left is a navigation menu with icons for General, Home, Search, Privacy & Security (highlighted in blue), Sync, and More from Mozilla. The main content area is titled 'Privacy & Security' and contains several sections:

- General:** 'Send web sites a "Do Not Track" signal that you don't want to be tracked' with a 'Learn more' link. Radio buttons for 'Always' and 'Only when Firefox is set to block known trackers' (selected).
- Cookies and Site Data:** 'Your stored cookies, site data, and cache are currently using 2.5 MB of disk space. Learn more'. A 'Clear Data...' button is circled in red. Other buttons include 'Manage Data...', 'Manage Exceptions...', and 'Delete cookies and site data when Firefox is closed' (checked).
- Logins and Passwords:** 'Ask to save logins and passwords for web sites' (checked). Other options include 'Autofill logins and passwords', 'Suggest and generate strong passwords' (checked), 'Enable Firefox Relay in your Firefox password manager' (with 'Learn more' link), 'Show alerts about passwords for breached web sites' (checked, with 'Learn more' link), 'Use a Primary Password' (with 'Learn more' link and 'Formerly known as Master Password'), and 'Allow Windows single sign-on for Microsoft, work, and school accounts' (with 'Learn more' link and 'Manage accounts in your device settings').



Or manage the data at all. Which data should be cleared or also specify what should be cleared when you close Firefox.





Likewise, you can set how to deal with access data and passwords.

And what should happen to the history.

You can clear the history in between, or even set how to deal with the history when Firefox is closed.

Clear Recent History

Time range to clear: Last hour

History

- Browsing & download history
- Cookies
- Active logins
- Cache
- Form & search history

Data

- Site settings
- Offline web site data

Clear Now Cancel

Settings for Clearing History

When closed, Firefox should automatically clear all

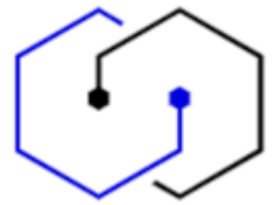
History

- Browsing & download history
- Cookies
- Active logins
- Cache
- Form & search history

Data

- Site settings
- Offline web site data

OK Cancel



In addition, you can make settings for **Permissions**, for example, whether a website may access your **Location** or your **Camera**.

The screenshot shows the Firefox Settings application. On the left is a sidebar with menu items: General, Home, Search, Privacy & Security, Sync, and More from Mozilla. The main content area is titled 'Permissions' (circled in red) and lists several permissions: Location, Camera, Microphone, Notifications, Autoplay, and Virtual Reality. Each permission has a 'Settings...' button to its right. Below these are two checked options: 'Block pop-up windows' and 'Warn you when web sites try to install add-ons', each with an 'Exceptions...' button. A section titled 'Firefox Data Collection and Use' follows, containing a paragraph of text and four unchecked checkboxes with 'Learn more' links: 'Allow Firefox to send technical and interaction data to Mozilla', 'Allow Firefox to make personalised extension recommendations', 'Allow Firefox to install and run studies', and 'Allow Firefox to send backlogged crash reports on your behalf'. At the bottom left, a partially visible 'Extensions & Themes' option is shown.



And there are even more advanced settings for security. The default settings are quite useful.

Security

Deceptive Content and Dangerous Software Protection

- Block dangerous and deceptive content [Learn more](#)
- Block dangerous downloads
- Warn you about unwanted and uncommon software

Certificates

- Query OCSP responder servers to confirm the current validity of certificates

[View Certificates...](#)

[Security Devices...](#)

HTTPS-Only Mode

HTTPS provides a secure, encrypted connection between Firefox and the web sites you visit. Most web sites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS.

[Learn more](#)

- Enable HTTPS-Only Mode in all windows
- Enable HTTPS-Only Mode in private windows only
- Don't enable HTTPS-Only Mode

[Manage Exceptions...](#)

DNS over HTTPS

Domain Name System (DNS) over HTTPS sends your request for a domain name through an encrypted connection, creating a secure DNS and making it harder for others to see which web site you're about to access.

[Learn more](#)