Pale Moon Commander User's guide

Table of contents:

Pale Moon Commander - General information

Introduction

Pale Moon Commander is a Mozilla Firefox compatible extension designed for the Pale Moon web browser. It is a configurator, meaning it will provide a user-friendly interface to advanced preferences that would otherwise require manual editing of parameters, which can be cumbersome and time-consuming to do.

How to access the add-on's settings

The add-on, when installed, adds a menu item "Advanced Options..." in two locations:

- In the Application Menu (Pale Moon/Firefox button) under Options -> Advanced Options...
- In the classic menu under Tools -> Advanced Options...

Clicking this menu item will open the preferences window that has been added by installing the add-on.

There be dragons here!

Using Pale Moon Commander to change advanced preferences is potentially dangerous and can leave your browser profile in a potentially unusable state. If you don't know what a setting is for, don't touch it. A number of the preferences made accessible through the add-on can prevent proper operation of the browser. Because all the add-on does is change preferences, you can, at all times, reset the preferences by starting Pale Moon with the SHIFT key depressed, and selecting "Reset preferences to Pale Moon defaults". Of course this will also reset any other modified preferences you may have.
Use of this add-on is at all times at your own risk. I do not give warranty or guarantees, and it is provided "as-is" although I've done my best to make sure it works as-intended.

Pale Moon Commander and Firefox

Pale Moon Commander is written first and foremost for Pale Moon, and a few features are available in the add-on that have no effect when used in Firefox, for example:

- Anything in the "padlock" tab of the Security category
- The setting "for domain-verified secure sites, display:" in the SSL tab of the Security category

Anything that is Pale Moon specific will be indicated in this User's Guide with **(Pale Moon only)**.

Structure of this document

This document is laid out in the same order, from left to right, of the preferences window of the add-on.

Category: Graphics

General

Use workarounds for specific driver bugs: The Mozilla code base has a number of workarounds implemented in the rendering engine for a few specific driver bugs that would severely break the browser if present. Selecting this option will enable these workarounds (default). Deselecting this could potentially increase performance, but can obviously be dangerous if your driver is buggy.
Initial paint delay: Wait this many ms before trying to render the web page for the first time. This delay prevents wasting processor time trying to render a page that does not have a sufficient amount of content downloaded yet to display anything. The default value of 150 ms is strongly recommended. Values less than 100 ms are not recommended, regardless of your connection speed.

Rendering

Enable Direct2D acceleration: Selecting this will use Direct2D accelerated rendering for page elements. This feature requires the use of DirectX 10 (Available on Windows Vista SP2 and later)
Force the use of Direct2D: Enforce the use of Direct2D even if your graphics driver has been blacklisted because of known issues. Enabling this is normally not recommended.
Layers acceleration enabled: Selecting this will use a hardware accelerated drawing method for page layers which can speed up page rendering significantly. You can switch this off if you run into strange graphical glitches in page rendering.
Layers acceleration forced: Enforce the use of hardware accelerated drawing of layers even if your graphics driver has been blacklisted because of known issues. Enabling this is normally not recommended.
Layers acceleration mode: Hardware accelerated drawing of layers is normally done using DirectX 10, which is the fastest and most complete acceleration method. If you run into issues because of poor DirectX 10 support in your drivers, you can select either DirectX 9 mode (works well on certain Intel embedded graphics) or the use of OpenGL (this has known issues on some configurations).

3D

Prefer OpenGL for WebGL: Normally, 3D hardware-accelerated rendering for WebGL is done using DirectX. Selecting this option tells the renderer to use OpenGL for 3D rendering instead of DirectX.
Force antialiasing on: This enforces the use of anti-aliasing for WebGL 3D graphics, even if it's normally switched off in your driver settings.
Level of antialiasing: This sets the level (strength) of antialiasing used. A higher value means smoother edges and less jagged looks at the expense of rendering speed.

Fonts

Use GDI table loading for DirectWrite: Turns on software GDI rendering engine for compatibility with older graphics cards. Switching this off lets the graphics processor also render GDI fonts.
Enable graphite font rendering: Enables the use of graphite font rendering for special accents on non-western fonts true to the intended looks of those accents (a form of advanced hinting). See http://scripts.sil.org/cms/scripts/page.php?site_id=projects&item_id=graphite_fontdemo
Always use ClearType for content: This applies ClearType font rendering to all fonts on a web page, which may improve legibility.
Use ClearType for downloadable fonts: Apply ClearType font rendering to custom fonts that have been downloaded on-the-fly through CSS.
ClearType rendering mode: This selects one of the different available rendering modes for ClearType rendering of fonts. Each mode has different effects for font rendering and edge smoothing of fonts. Automatic is recommended to automatically adjust the rendering mode based on font face and font size (see also below). Be careful with the "aliased" setting, as it may make your fonts instantly invisible which will make it difficult to restore a sane setting.
ClearType level: This is the level (strength) of ClearType effect applied to ClearType rendered fonts. -1 means using the default level. Other values are 0 (none) to 100 (full).
ClearType contrast: Adds enhanced contrast between the text and surrounding background. -1 means using the default level (50). Possible other values are 0 to 1000.
ClearType gamma: gamma correction applied to ClearType rendered font edges (luminance curve). -1 means using the default level and is recommended. Possible other (sane) values are between 1000 and 2200 (= factor 1.0 - 2.2)
Subpixel rendering: this sets the type of subpixel rendering to apply for font edges. Automatic is recommended, with other values being Flat (greyscale), RGB (for RGB ordered LCD matrices) or BGR (for BGR ordered LCD matrices - uncommon). What works best of the manual selections is very much hardware dependent.
Render with GDI Classic up to font size: This selects the font size (in pt) up to which GDI classic font rendering is used, which looks better for small size fonts and keeps them more legible. The default of 17 pt is recommended for most screens.

Colors

General

Don't use accessibility theme page colors (Pale Moon only): Enabling this setting tells the browser to not apply accessibility theme colors (like high contrast themes) used for visually impaired people to page content. By default, these accessibility themes will also apply to web pages, converting layout and colors to the same accessible theme. In some cases, this is undesirable, e.g. when it destroys page layout of websites that aren't designed to be converted this way,

and checking this option will make the browser render page content in a normal way, while still applying the accessibility theme to the user interface and controls.

Color Management System (CMS)

Mozilla applications have an integrated color management system (CMS) that allows you to display images visually "as-intended" if they were designed for media other than a computer screen and have an embedded color profile (ICC profile). The options on this tab allow you to enable/disable this system and to specify how to render the colors.
Important: If you make any changes to the settings in this tab, you need to completely shut down and restart the browser for the changes to come into effect.
Enable ICC version 4 profiles: This enables the parsing and use of ICC version 4 profiles, in addition to version 2. As a result, more images will display "as-intended" and on occasion more accurately correct the colors than if version 2 profiles are used. Keeping this enabled (default) is strongly recommended, because version 4 profiles are commonplace these days.
CMS Mode: This allows you to choose when to apply color correction to images. You can either switch the CMS Off entirely, force the color conversion on all images (not recommended), or use the CMS only for images which have embedded ICC profiles.
Rendering intent (color conversion): Determines what color conversion to use. Perceptual is the default, which tries to match the colors as close to perceptually accurate as possible. The other color conversion modes have specific uses which go beyond the scope of this document. If you are interested in knowing more about color conversion and ICC profiles, check out the International Color Consortium website at www.color.org.

Category: Network

Domain Names

Automatically try to fix incomplete addresses: If you are typing an incomplete address in the address bar, the browser can attempt to automatically fix this for you by adding a prefix and/or suffix to what you typed to try and make a complete host name. Selecting this option (on by default) attempts this automatic fixing, deselecting turns it off.
Prefix and Suffix: the specific fixups to apply to try and complete a hostname. e.g. **www.** prefix and **.com** suffix will, when you type "*example*" in the address bar, try "*example.com*" and "*www.example.com*" as fixups.
Enable IPv6 lookups: Perform name lookups for using the IP version 6 protocol. If you don't use an IPv6 router or internet connection, you can disable this, which will give you a small performance win.
Prefetch DNS lookups: Enabling this will perform DNS lookups on addresses found in web pages. The idea behind this is to speed up browsing by having all name lookups done before you even click a link, but in practice this causes a lot of extra and unnecessary traffic that can hang up routers. Name lookups are usually very fast so this is not needed.
Cached DNS entries: Remember this many name-to-IP lookups.
Cached DNS expiration: Remember name-to-IP lookups for this many seconds. (default 3600 seconds = 1 hour)

HTTP

Use fast IPv6 to IPv4 fallback: If you have support for the IPv6 protocol on your network, it will be attempted first to make a connection. If the connection using that protocol fails or takes too long, IPv4 connections will be used instead. This option makes sure there are minimal delays for trying IPv6 before using IPv4.
HTTP connection timeout: After this much time has passed, it is assumed that the web server is not responding, and the browser gives up trying to connect.
HTTP connection retry after xxx ms: If a connection is not yet established after this many milliseconds, a second connection attempt is made in parallel.
HTTP persistent connection timeout: Persistent HTTP connections (so-called "keep-alive" connections) will close after they have been idle for this many seconds. The default of 115 seconds is a recommended maximum, because IIS servers don't properly handle a timeout like this server-side and the IIS timeout is 120 seconds - you want to make sure to close the connection on the browser side before that happens.
Total maximum HTTP connections: Open no more than this many concurrent HTTP connections. Setting this number too high will saturate most wireless and residential routers. The default of 48 is highly recommended.
Maximum HTTP connections per server/proxy: Open no more than this many concurrent, persistent HTTP connections to a single web server or proxy server.
Enable HTTP protocol diagnostics: Enable this for detailed debugging information about the HTTP protocol. Not recommended as it will cause a severe

loss of performance, but may in some cases be useful if there are connectivity problems.

Pipelining

Enable pipelining: Pipelining is a way of transporting multiple files over a single persistent HTTP connection without waiting for the previous transfer to finish before the next item is requested. This can increase page load speed and efficiency, especially over slow networks. This option enables the use of pipelining for HTTP requests.
Enable pipelining over SSL: This option enables the use of pipelining when a secure connection is established to a server (https://)
Enable pipelining over proxy connections: This option enables pipelining when using a web proxy. By default this option is disabled because there are a number of commonly used pieces of web proxy server software that are broken in this respect and which will cause severe issues (pages not loading or not completing, etc.)
Use aggressive pipelining: This option tells the browser to use pipelining of requests whenever possible. The more lax method (option off) doesn't use pipelining for all requests and opens more concurrent connections.
Maximum number of requests in the pipeline: The maximum number of outstanding requests for page elements for each pipelined connection (request sent without waiting for receipt of the element).
Maximum optimistic pipelining requests: The maximum number of requests that are put in the pipeline which could have been sent over a separate connection instead.
Maximum size of elements to pipeline: The maximum size (in Bytes) of elements to request pipelined. If an element is larger than this, a separate connection will be made to the server to request the element.
Pipelining read time-out before requesting it non-pipelined: Wait at most this many milliseconds for an element to be served through a pipeline before considering it lost and re-requesting it over a separate connection.
Reschedule slow pipelining requests to another pipeline: If an element takes too long (see next option) to receive through a pipeline (e.g. because a larger/slower element is "ahead of it in the line") then the request for the same element will be made in another pipeline so it doesn't get hung up.
Time before rescheduling requests to another pipeline: This is the time to wait in milliseconds after a request is made before it is moved to a different pipeline (see previous option).

Miscellaneous

Enable the SPDY protocol: Enables the use of Google's SPDY protocol over SSL if the server supports it.
Disable HSTS (HTTP Strict Transport Security) (Pale Moon only): This disables the use of HSTS, which is a server-enforced policy for client connections. This is a trade-off between privacy (HSTS off) and security (HSTS on enforcing SSL usage on specific websites).

Number of network layer buffers and **size of network layer buffers**: This determines the amount and size of buffers used for network data transfer. Default size is 32 KB per buffer, and up to 24 buffers of that size. Defaults are very strongly recommended but can be changed for non-standard environments where this is needed.

Category: Performance

Javascript

Browser Chrome

These options affect the Browser's "chrome", i.e. the user interface and Javascript parts of the browser and add-on functionality.
Enable Baseline JIT compiler for UI scripts: Enable the use of the JIT (Just-In-Time) compiler for chrome elements to speed up code execution for often-used ("hot") scripts in the user interface.

Page Content

These options affect Javascript in web pages.
Enable Baseline JIT compiler for web pages: Enable the use of the baseline (reference) JIT compiler for page scripts to speed up code execution for often-used ("hot") scripts.
Enable IonMonkey: Enable the use of the main and modern JIT compiler for page scripts.
Enable OdinMonkey: Enable specific JIT optimizations for the asm.js library to achieve near-native code speed for javaScript.

Other Options

Completely disable JavaScript: This is a "master kill switch" for the use of JavaScript in web pages. WARNING: This will cripple your browsing experience and will make many websites dysfunctional. Note that disabling JavaScript completely this way for security reasons is also not recommended and will not mitigate much (if any) malicious content.
Enable JavaScript type inference: This is a whole-program, hybrid static and dynamic analysis that attempts to find the set of possible types for stack slots, arguments, and local variables. It is strongly recommended to keep this enabled because it greatly speeds up JavaScript execution.

Garbage collection

Garbage collection (GC) is a form of programmatic maintenance to clear and reclaim memory that is no longer in use by scripts, e.g. when a script temporarily uses a number of variables but is done with them.
Perform GC on memory pressure: This option tells the browser to perform a GC run immediately if it's running low on free scripting memory.
Perform GC per compartment: This options tells the browser to use individual maintenance runs for different compartments (e.g. tabs)
Enable explicit GC for compartments: This option tells the browser to honor explicit requests for a GC run on a compartment (i.e. explicitly triggered by a running script)

Use dynamic GC memory heap and **Use dynamic GC memory slices**: This allows for the browser to dynamically allocate memory for the storage of JavaScript data and GC on it. It is strongly recommended to leave these options enabled.
Enable incremental GC: To prevent pauses in the browser during the GC maintenance runs, a method has been implemented to cut these GC runs up into small chunks that are processed each time slice (see next option). This is called Incremental Garbage Collection. Enabling this option will enable the use of this method to reduce noticeable pauses in the browser while doing GC.
Time slice used for incremental GC: This is the time interval with which an incremental GC chunk is processed. You would want to keep this number low to prevent a drop in frame rate, but not too low to prevent unnecessary overhead for the chunk dispatcher (especially important on slower machines). The default of 20 ms in Pale Moon has been based on trials with general use on a wide range of systems and is an optimal compromise.

Cache

Enable Disk Cache: Enables the use of disk space to cache previously requested items on web pages.
Automatically size the Disk Cache: automatically determines the maximum size on the disk to use for caching based on available free disk space.
Disk Cache capacity if not automatically sized: Lets you configure the maximum size of the disk cache manually, for when the previous option is not used. Remember that this is an upper limit, and the cache will use "up to" this amount of disk space to cache items. The maximum is 1GB.
Maximum element size in Disk Cache: Individual files in the disk cache can not be larger than this size. This prevents the disk cache from discarding cached items to make room for very large files that are normally not desirable to cache (downloads, large media files, etc.)
Cache compression: Determines if, and to what extent, items in the cache should be compressed to more efficiently use disk space. No compression means files are stored as-is. Low, Medium (the default) and High compression are a tradeoff: Low is minimal compression but very fast, Medium is a balanced setting between CPU usage/speed and disk space saved, and High applies maximum compression which uses more processing power but less disk space. Changing this setting will immediately empty your disk cache.
Enable Memory Cache: Enables the use of memory to cache previously requested items on web pages. Note that this cache works differently than the disk cache and is not a replacement for it. The memory cache will only be used for certain page elements.
Memory Cache capacity: How much memory to reserve for caching items in memory. Keep in mind that the memory cache is conservative by nature, so manually selecting a large capacity here will not necessarily speed up your browsing, but just increase the amount of memory the browser uses.
Maximum element size in Memory Cache: Similar to element size in the Disk Cache explained above.

Compare cached pages to pages on the network: Determines when the browser compares items in the disk/memory cache to items on the network. The default is "when expired".
Possible settings are:

- **When expired**: The browser will re-check if the item on the network has changed if the expiration date/time has passed for the item. **This is strongly recommended**.
- **Once per session**: The browser checks once per browsing session (complete browser shutdown/restart) if the item has changed, and will serve files from the cache after this initial check, regardless.
- **Always**: Always compares a cached item against the copy on the network, even if it's not expired yet. This uses more bandwidth and will be slower, but you will always have the latest version of pages.
- **Never**: Always serves cached items when they are available. This uses less bandwidth and may be faster, but the websites you are seeing may not be the latest versions and have stale content.

Sessions

These settings relate to the browser's "session store" (a saved state of your browsing session).
Remember this many session pages: This is the total amount of pages the browser will remember for use with the back/forward navigation buttons across all tabs.
Number of fully rendered pages to keep in RAM: This is the number of web pages the browser will keep stored as fully parsed and rendered pages in working memory to make back/forward navigation instant without needing to re-parse the page. A higher setting will make the browser use more memory (this can be significant) and considering normal browsing behavior, the default setting is strongly recommended for efficient browsing.
Save your session to disk every xx seconds: You browsing session (open windows, tabs, session page history) will be saved to disk in your browser profile at regular intervals. Pale Moon by default saves this state once every minute, but you may make this interval shorter or longer if you wish. If you use a very large number of open tabs in the browser, then increasing this value may prevent the browser from becoming hung up on disk I/O from saving the session.
Restore exact window positions (Pale Moon only): When enabled, the browser will always restore the browser windows (e.g. when your start up page setting is to restore windows and tabs from last time) to their exact saved positions. By default, Pale Moon will check if windows are positioned outside of your desktop space (either partially or completely) and will adjust the location/size of these windows to always fit on your screen. Exact positioning will allow these windows to be partially or completely off-screen and may, in some situations, cause an inaccessible window (e.g. if it was on a second monitor no longer connected/active).
Automatically resume your session if crashed: This will restore your session if a browser crash occurred, regardless of your default startup setting.

Only restore tabs when clicked: If enabled, the contents of tabs will only be loaded if you activate the tab in question. Disabling this setting will make the browser restore tab contents automatically (see next option).
Restore this many tabs at a time (Pale Moon only): When restoring tabs automatically, the browser will restore/load the contents of tabs this many tabs at a time. A setting of 1 (the minimum) causes the browser to only restore the next tab if the previous one is completely done loading, one at a time. The default of 3 is recommended, but if your network and computer is fast enough, you can increase this to a maximum of 10.
Only restore pinned tabs when clicked: If enabled, the contents of pined tabs will not be loaded until you activate the pinned tab. Normally, pinned tabs are always loaded because they are intended to be used for "web application" type webpages that you always want to keep loaded/refreshed.
Maximum number of tabs/windows to undo close: This allows you to set how many recently closed tabs and windows the browser will remember for you to recall instantly.

Category: User Interface

General

Automatically complete addresses: enables the URL text in the address bar to be automatically completed from history when typing.
Also use previously typed addresses: automatic completion of text in the address bar also includes text that has previously been typed, in addition to looking up matches in history and bookmarks.
Enable domain highlighting: this highlights the top domain of the address URLs visited by dimming the rest of the address. This is useful for quickly seeing the top domain you are currently visiting, but may potentially make the rest of the address hard to read.
Enable protocol trimming: removes the protocol prefix from the displayed address in the address bar (e.g. http:// or ftp:///). Disabled by default in Pale Moon since it is considered essential information.
Display the feed indicator in the address bar (Pale Moon only): This will enable the web feed indicator in the address bar when the website visited offers web feeds.
Use custom error pages: enable this to display user-friendly error pages instead of raw errors when there is a problem browsing to a page.
Background color for stand-alone images (Pale Moon only): The background color to use for stand-along images (also called top-level images), e.g. when opening a .jpg image directly in the browser. This determines the background color for the displayed image, including the color for any transparent parts of an image. The default value is #2E3B41 in Hex, but you can use named colors as well, e.g. "maroon" or "black".
Hide UI placeholder text when focusing input: Some UI elements have so-called placeholder text. E.g.: the name of the search engine in the search box, or the generic text in the address bar when it's empty. If this option is checked, the placeholder will be hidden the moment the box gets focus; if unchecked, the text stays in place until you start typing something.
New tab URL: This allows you to enter a custom URL to be loaded for new tabs.

Tabs

Animate tabs: Animate the moving, scrolling, opening and closing of tabs.
Draw tabs in the title bar: Allows tabs to be drawn in the title bar of the window (e.g. next to the Pale Moon application button).
When I open a bookmark in a new tab, switch to it immediately: If enabled, then if you open a bookmark in a new tab, e.g. by Ctrl+clicking or clicking with the mouse wheel on a bookmark/-toolbar entry, the new tab will immediately get focus. If disabled, the bookmark will be loaded in a new tab but will load in the background (the active tab retains focus).
Allow prompts to switch tab focus (Pale Moon only): If enabled (default), this will automatically select and bring the tab to the front that has a (JavaScript) prompt pop up like an alert box. Disabling this will not change focus and leave

the currently selected tab active, but with the risk of you not knowing that a background tab needs your attention.
Show tab close button: Controls when and where the close button (X) for tabs is shown:

- **On the active tab only**: Only shows a close button on the tab that currently has focus
- **On all tabs if wide enough**: Shows a close button on all tabs as long as the tabs are wide enough (default)
- **Don't show close buttons**: Doesn't show close buttons on tabs at all. You will have to close tabs with the right-click menu or by using the keyboard shortcut.
- **On the end of the tab strip**: Shows a single close button on the far end of the tab strip, like in the first versions of Firefox.

Don't show close button if tab width is less than: If the previous setting is set to "On all tabs if wide enough", then this setting controls what is considered "wide enough" to display the close buttons on non-active tabs, in pixels.
Use graphical tab switching with Ctrl-Tab: Uses a graphical "quick switch" panel when pressing Ctrl+Tab (showing a limited number of tabs) or Ctrl+Shift+Tab (showing all tabs with search). If you disable this, Ctrl+Tab will immediately page forward through the open tabs and Ctrl+Shift+Tab will page backward through the open tabs.
Prioritize recently used tabs for Ctrl-Tab: This will prioritize display of tabs in the Ctrl-Tab pane that have recently been used, making switching between actively used tabs quicker by allowing you to jump between tabs that are far apart.
Use graphical pane when listing all tabs (Pale Moon only): Uses a graphical panel with search to display all tabs. Disabling this will switch the "all tabs" button to a drop-down menu of tabs.

Task Bar

Jump List features (application control from the task bar button with a right-click) are available on Windows 7 or later only.
Enable jump lists: Enable the use of jump lists for the browser taskbar buttons.
Show frequently used sites in jump list: Lists the most frequently used web pages in the jump list.
Show recently visited sites in jump list: Lists the web pages you most recently visited in the jump list.
Show browser tasks in jump list: Lists common browser tasks in the jump list (open new tab, open new window, etc.).
Limit the number of jump list items to: Tells the browser not to display more than this number of items in the jump list for recently/frequently visited sites.

Full Screen

Auto-hide the Navigation and Tab toolbars in full screen mode:
Automatically hides the toolbars when switching the browser to full screen mode, allowing page content to fill the entire screen. Moving the pointer to the edge of the screen will call up the toolbars.

Animate the hiding of toolbars: Animates (slides) the toolbars off the screen when in full screen mode. Possible values are:

- **Never**: Never animates the hiding of toolbars, they are always instantly hidden/shown.
- **First time only**: Only animated the hiding animation of the toolbars the first time after switching to full screen, to indicate the toolbars are there. Subsequent mouse-overs and mouse-outs will have the toolbars shown/hidden instantly.
- **Always**: Always animates the showing and hiding of the toolbars in full screen mode.

HTML5 Full Screen relates to the options for HTML5 web pages/web applications to request and use full screen mode.
Enable full screen mode for HTML5 applications: Allow HTML5 applications to switch the browser to full screen mode.
Require per-site approval for full screen: Requires that the user approves the use of full screen mode by an HTML5 application on a site-by-site basis. You will be asked for site approval when an application switches the browser to full screen.
Exit full screen when the application deactivates: If focus is shifted from the HTML5 application to something else, or when the application finishes for a limited-run application, the browser will automatically leave full screen mode.
Lock the pointer to the full screen window: This will lock the pointer to the full screen window and full screen running application, useful for e.g. games.
Only allow user interaction to switch to full screen: Does not allow scripted events to switch the browser to full screen mode (e.g. by just surfing to a page) and requires some form of user interaction to initiate full-screen mode.

Category: Security

General

Enable Javascript JIT hardening: Enables additional security measures to make the JIT JavaScript compiler more resilient to potential "JIT spraying" attacks.
Allow JavaScript to: This controls whether page scripts are allowed to do certain things or not. The specific choices are:

- **Change image source attributes**: Enable this to allow scripts to change the content of images loaded in a page.
- **Raise or lower windows**: Enable this to allow scripts to bring windows to the front or send them to the back.
- **Move or resize windows**: Quite self-explanatory; allows scripts to change the dimensions and location of the browser window(s).
- **Close windows**: Enable this to allow scripts to close browsing windows/tabs. Commonly used for popup windows on pages.
- **Manipulate the clipboard**: Enable this to allow scripts to manipulate clipboard data: add or remove data when you copy or paste, prevent copying of text, determine which text a user has selected, etc. etc.
- **Disable or change the right-click menu**: Some websites will want to use the right-click menu to add additional options specific to the website (extra functionality or removal of irrelevant or unwanted functions). This setting controls whether websites are allowed to change this menu for the page visited or not.

Use strict origin policy for file://: Applies the "strict origin policy", a security measure to prevent cross-domain exploits, to files opened locally in the browser. It is strongly recommended to leave this enabled because it would potentially make your browser vulnerable and expose your local file system to a malicious website by using a local file on your computer. Disabling this setting allows developers to use local files for testing code more easily.
Require a click to enable plug-ins (Click-to-Play): Enables the option to "Always ask" if a plugin should be allowed or not on a site-by-site basis. If disabled, control of plugins can only be done globally (either enabled or disabled everywhere).

Padlock (Pale Moon only)

Show the padlock: Display the padlock on secure sites.
Where to show the padlock: Controls where to display the padlock in the browser. Possible values are:

- **In the identity panel, right side**: Shows the padlock icon in the identity panel (in front of the URL) on the right side of the panel (to the right of domain names or vendor names). This is the default setting.

- **In the identity panel, left side**: Shows the padlock icon in the identity panel (in front of the URL) on the left side of the panel (right next to the web site's icon).
- **At the end of the address bar**: On the right of the address bar, next to the bookmark star.
- **In the status bar**: At the bottom of the browser window in the browser's status bar, like old versions of Firefox and a number of other browsers.
- **In the tabs bar, right side**: Displays the padlock on the strip with tabs on the far right side.
- **Classic (the other 5 choices)**: These are the same locations as above, but using the "classic" style padlock.

Address bar effect for secure sites: Determines the effect to use on the address bar to further improve visibility of the status of secure sites.

- **No visual effect**: Do not shade the address bar
- **Secure sites only**: Only shade verified secure sites (domain-verified and EV)
- **Secure sites and mixed-mode**: Shade both secure sites and sites that are partially encrypted
- **All states**: Apply address bar shading for all https states, including broken security states

DOM

Scripts on websites can change or hide certain user elements to provide custom functionality or to prevent unnecessary controls in pop-up windows. These options control what scripts on pages are allowed to do in that respect.

When a popup window is opened, allow the script to: These checkboxes allow you to control what scripts are allowed to do when opening a pop-up window. For security reasons (to prevent spoofing), removing the address bar and removing the status bar are not allowed by default. This way you can always verify that the pop-up is on the intended domain and allows you to check where any potential links in the popup will take you.

SSL

For domain-verified secure sites, display (Pale Moon only): If you visit domain-verified secure sites (blue padlock), Pale Moon allows you to control what to show in the identity panel for the site:

- **No text**: Just displays the padlock.
- **Top domain only**: Displays the top domain name of the site you are visiting (e.g. google.com).
- **The entire host name**: Displays the full name of the host system you are connected to (e.g. accounts.google.com).

Lowest/Highest supported protocol: Allows you to force a lowest/highest supported HTTPS protocol. Although SSL3.0 is still available as an option it should only be used in emergencies, since it is no longer a secure protocol and has been obsoleted.

Mixed content sites are web pages that have elements that are retrieved from sites over an encrypted connection (https) as well as elements retrieved from sites over a regular connection (http). This is usually unsafe because there is no indication which elements are received encrypted and which are not encrypted (and originate from a non-secure site). This state can potentially be abused, as non-secure scripts can snoop on the content received securely. The browser has a few features to help mitigate this snooping. Both of these options may cause issues if you are using a restored session with cached items/pages, because cached items are not considered secure.
Block non-SSL scripts: this will block scripts and other active content that has been received non-encrypted. This is the most common way that mixed-content sites can be abused.
Block non-SSL display items: this will block visual items (images, etc.) that have been received non-encrypted. Selecting this in addition to the previous option makes you more secure as it prevents maliciously configured websites from serving active content disguised as images, but will also prevent the display of externally linked images on secure sites, e.g. when viewing an e-mail with an image attached/embedded that is on a non-encrypted file host (e.g. common photo sharing sites) while on a secure webmail server, the image will be blocked.

SSL hardening further improves the security of SSL connections, but this is usually not required unless you are using the browser for corporate, internal or specifically set up high-security sites and this may possibly break normal browsing to secure sites on the Internet.
Require safe SSL negotiation: If set to true, Pale Moon will reject all connection attempts to servers that are still using the old SSL/TLS protocol. Setting this to true will break all secure sites that do not support enhanced SSL/TLS versions.
Treat unsafe SSL negotiation as broken: A visual feedback option: if old protocols are used for the initial negotiation of encrypted connections, Pale Moon will treat the website as having "broken" SSL. The connection is still established and encrypted but will display as having broken encryption. This is not recommended for normal use and should only be used by people understanding the potential issue with old protocols and the information outlined on the Security:Renegotiation Wiki page.

Enable false starts for SSL handshakes: Allows for slightly faster negotiation of encrypted connections, but is potentially vulnerable to attacks.
Enable OCSP-stapling: Allows web servers to attach signed and time-constricted OCSP responses to certificates so a separate OCSP request to the CA server is no longer needed.
Allow expired stapled OCSP responses (unsafe) (Pale Moon only): Enabling this option will make the browser accept connections even if the OCSP responses stapled to offered server certificated have exceeded their lifetime. This can potentially be abused so is considered unsafe, but is offered as a workaround for certain server implementations that have OCSP-stapling bugs and that will sometimes attach a response even if it's already expired.

Ciphers 1 and 2

These two tabs allow you to select which encryption methods (ciphers) the browser uses to negotiate a secure connection to websites. It is recommended to leave all of the listed ciphers enabled as disabling them (even if some are deprecated for use) may break secure websites.

Privacy

Do not cache pages received over secure connections: This prevents any page received over an encrypted connection from being permanently cached.
Always accept session cookies: Always accept cookies that will expire when the browser session is closed. This can help web pages to function if you are using a strict cookie retention policy.
Clear 3rd party cookies when closing the browser: Clear cookies that are set by third parties when you close your browser. By default, if you accept third party cookies, they will be retained until their set expiration time (by default). This setting allows you to treat all third party cookies differently and have them removed when the browser closes.
Enable browser location awareness: Enable geolocation functionality in the browser. You will still be asked for confirmation to share your location if a website requests geolocation. Disabling this makes any request for your location automatically fail.

Referers: The HTTP referer (originally a misspelling of referrer) is an HTTP header field that identifies the address of the webpage (i.e. the URI or IRI) that linked to the resource being requested. By checking the referrer, the new webpage can see where the request originated.
Send referer headers: Determines when referer headers are sent to the server along with the request: Never, when clicking links, or when clicking links and requesting images (default). Any setting but the default may cause issues on some sites (see below).
Spoof referer to target URL: this will send a referer header equal to the target website to the server, masking the actual origin of the request.
Trim referers: This allows you to select how much information from the originating location to include in the referer header.
Cross-origin referer policy: This allows you to restrict referer headers being sent for cross-origin requests, only sending either if the base domain or the exact host matches, and not sending otherwise.

Note that restricting referers, although a privacy benefit, may have sites or servers refusing service to you for good and understandable reasons like preventing bandwidth theft and deep linking.

Category: Other

Tools

This section allows you to enable/disable specific modules included in the browser. ***Pale Moon includes these developer tools as-is and any support for them will have to be directed to the Mozilla developers of these tools directly****.*
Any changes to the tools listed here being enabled or disabled requires that you completely exit the browser and restart it.
Developer tools: The different web developer tools that are part of the underlying Firefox code can be individually enabled or disabled. Not all combinations make sense, and if enabled may increase resource use by the browser.
Enable built-in PDF viewer: Enables the built-in, JavaScript based PDF document viewer. This viewer is disabled by default because it is very limited in its functionality and will not display a large number of PDF documents correctly or as-intended. Use of the built-in PDF viewer may also subject you to security vulnerabilities through malicious PDF documents and is always at your own risk. It is strongly recommended you use this feature for emergencies only, when you don't have access to a full PDF reader but still need to quickly open a PDF document.

Reset

If the browser has become misconfigured in such a way that it causes problems, one click on the reset button here will clear all preferences, and restore all factory defaults of the browser. Be aware of the following before you use this feature:

- You will lose all user-set preferences, including preferences set that are not apart of this add-on. If you have set other options to non-defaults (e.g. showing previous windows and tabs when the browser starts), these will be reset as well and you will have to reconfigure those options.
- You will lose any configuration you have done in add-ons. Extension preferences will be reset to their supplied factory defaults as well.

Other

Make this many bookmark backups: Pale Moon will make backups of your bookmarks whenever you close a session. This setting controls how many backups of the bookmarks library should be retained by the browser before the oldest one is removed to make room for a new one.
Export a bookmark backup as HTML upon shutdown: Enable this to also export your bookmarks as an html file when you close the browser. Regular backups are made in .json format which is less readable and less compatible for third party software than html would be.
Enable HTML5 local storage: Enables the use of HTML5 "local storage" by the browser. This is a space-limited storage area that can be used by websites to

save settings and other data in your browser profile with more flexibility than cookies offer.
Default limit for the amount of data stored per domain: HTML5 storage is space-limited. This setting controls up to how much data a single top domain is allowed to store on your system. Default setting is 5MB.

Miscellaneous

Support

For support, please visit the pale Moon forum: http://forum.palemoon.org/

Contacting the author/developer

The author (Moonchild) can also best be reached through the forum, although if needed e-mail is an option. moonchild [at] palemoon [dot] org

Licensing

The extension is released as **Copyrighted Freeware with disclosed source**. Note that the extension is **not** an open-source product and is **not** subject to GPL, MPL or other common licenses. The source may only be used for educational purposes and may not be copied verbatim to other software.
See: http://www.palemoon.org/freeware-license.shtml