Enabling TLS 1.2 in Major Browsers

Table of Contents

If you get an error message/ are not able to access Fannie Mae site due to your computer's security settings, please follow the instructions to update your internet browser.

Updating Microsoft Internet Explorer

✦ Microsoft Internet Explorer Version 7: TLS 1.2 support added; disabled by default
✦ Microsoft Internet Explorer Version 11: TLS 1.2 enabled by default
✦ Microsoft Edge: TLS 1.2 enabled by default on all versions
✦ If you are using an Internet Explorer version prior to IE V.7, you must update your internet browser.
✦ If you are using a Windows Operating System prior to Windows 7, you will need to update your OS before you are able to update Internet Explorer to a version which supports TLS 1.2. You can update your Windows OS **here**.
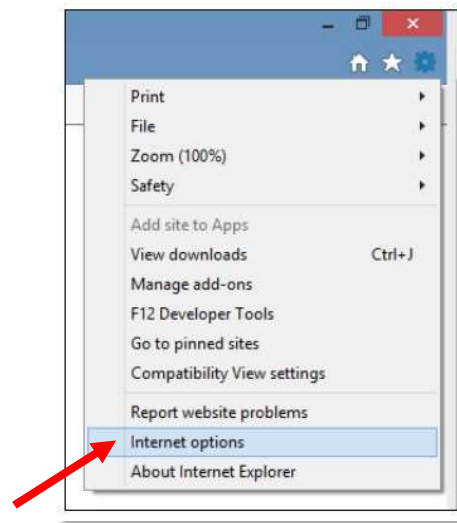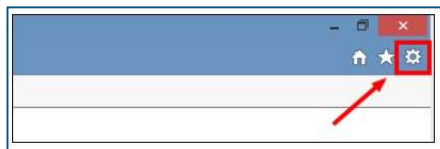
Microsoft updates Internet Explorer using its Windows update feature. As long as you are regularly installing the latest Windows updates from Microsoft, you should have the latest version of Internet Explorer.

If you do not have Windows automatic updates enabled in Windows 8 and earlier versions, you need to update Internet Explorer on your computer manually by following these steps:

1. Open the Control Panel
2. Click on and open the **Windows Update** utility.
3. In the left navigation pane, click the **Check for updates** link.
4. You can choose to install all available updates or select the updates you want to install.

Enabling or Disabling TLS Protocols in Internet Explorer

✦ If you are using IE v.7-10, to enable TLS 1.2:
✦ Click on the gear in the upper right corner of the browser ❼ Internet Options ❼ Advanced.
✦ Scroll down to the SSL and TLS protocol and enable TLSv1.2.
✦ Select   **Apply** and **OK**.
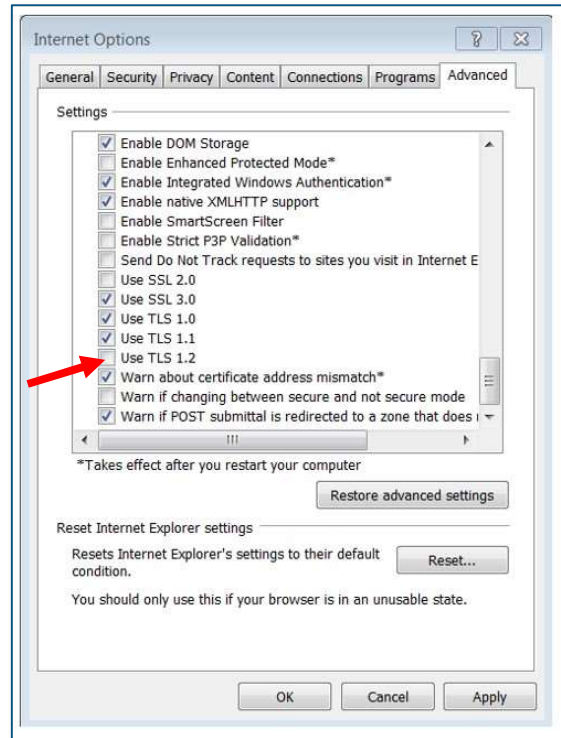
Updating Mozilla Firefox

- ✦ Mozilla Firefox Version 24 : TLS 1.2 support added; Disabled by default
- ✦ Mozilla Firefox Version 27: TLS 1.2 enabled by default
- ✦ If you are using a Firefox version prior to V.24, you must update your internet browser
- ✦ If you are using a Windows Operating System prior to Windows 7, you will need to update your OS before you are able to update Mozilla Firefox to a version which supports TLS 1.2. You can update your Windows OS **here**.

Mozilla Firefox should automatically download updates and prompt you when they are available to install. To verify that your version of Firefox is the latest or update it manually, follow these steps:

1. Open the Mozilla Firefox browser.
2. Click the **Open menu** button in the upper-right corner of the screen.
3. In the menu that appears, click the **Help** option at the bottom.
4. Select **About Firefox**.
5. The window that appears will automatically check for updates and show you the current version of Firefox. If an update is available, you can click the **Restart to update Firefox** button to install the update.

Enabling or Disabling TLS Protocols in Firefox

✦ If using Firefox Versions 24-26:

✦ Type about:config in the url space in the browser ❼ Accept the risk to change the settings

✦ Search for "security.tls" in the search bar

✦ Double-click on "security.tls.version.min."

   ✦ Change the value to "2" and click Ok

Updating Google Chrome

- ✦ Google Chrome Version 30 : TLS 1.2 support added
- ✦ If you are using a Chrome version prior to V.30, you must update your internet browser
- ✦ If you are using a Windows Operating System prior to Windows 7, you will need to update your OS before you are able to update Google Chrome to a version which supports TLS 1.2. You can update your Windows OS **here**.
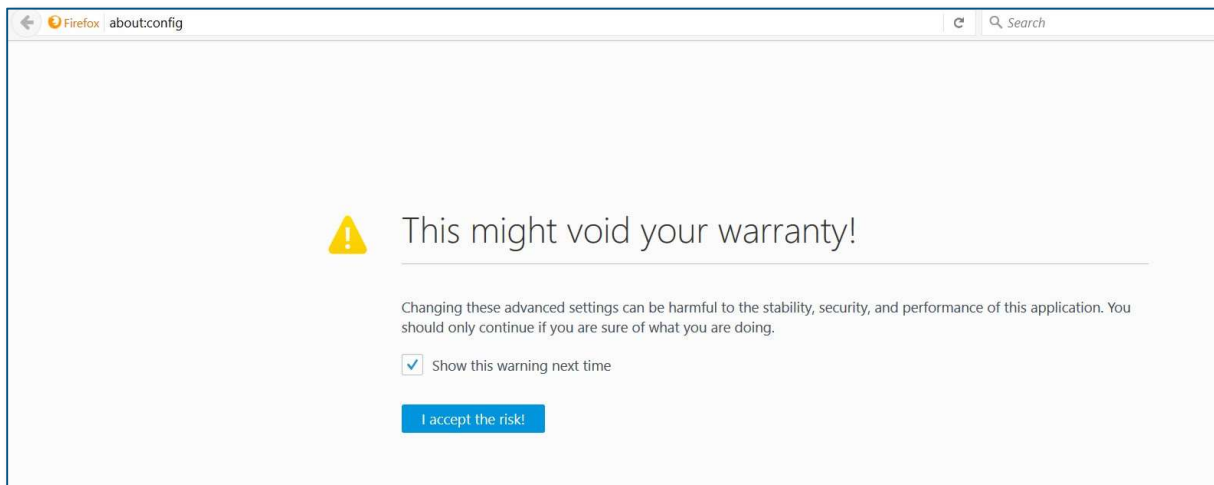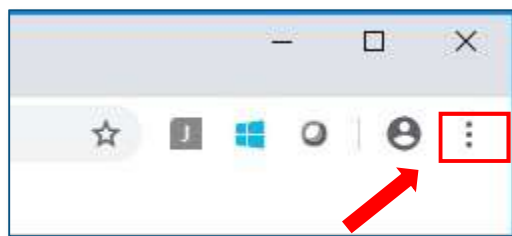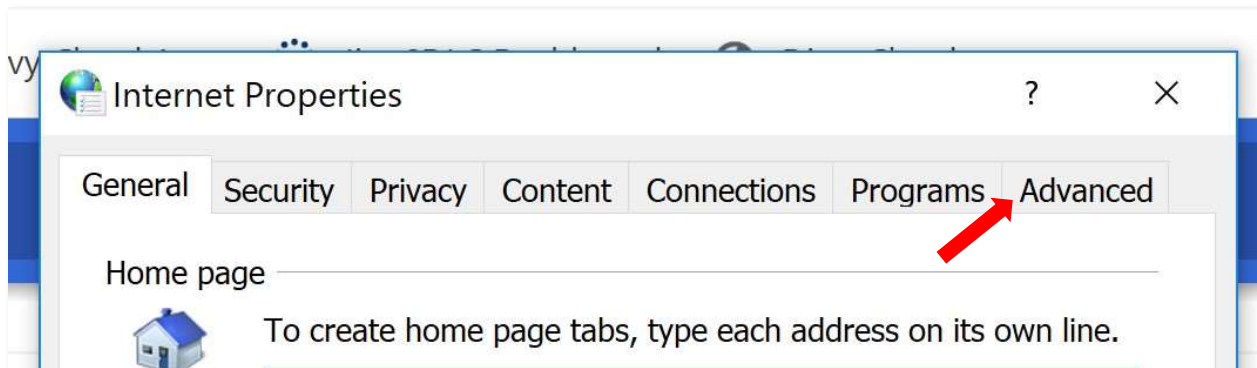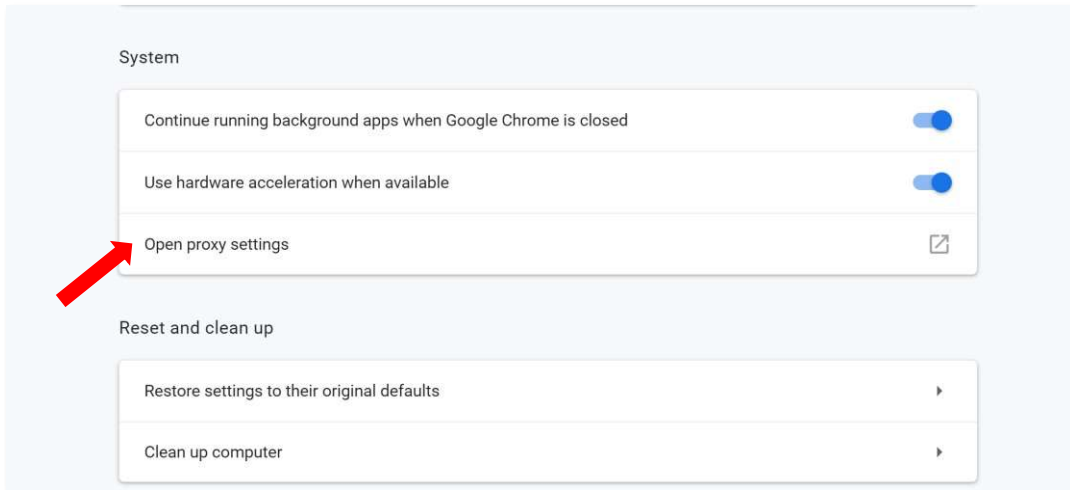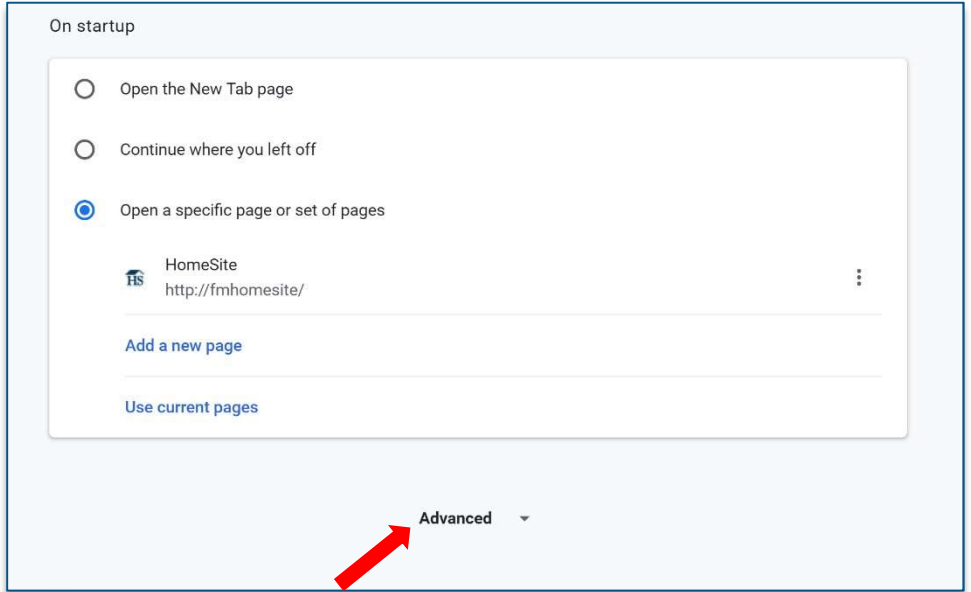
Google Chrome will update automatically as new iterations are released to the public. To verify that your version of Chrome is the latest or update it manually, follow these steps:

1. Open the Google Chrome browser.
2. Click the **Customize and control Google Chrome** button ⋮ in the upper-right corner of the screen.
3. From the drop-down menu that appears, select **Help**, then select **About Google Chrome**.
4. The window that appears will automatically check for updates and show you the current version of Chrome. If an update is available, Chrome will be updated automatically. After Chrome is updated, click the **RELAUNCH** option to restart Chrome and complete the update.

Enabling or Disabling TLS Protocols in Chrome

- ✦ If using Chrome Version 30 or newer.
- ✦ Chrome should connect with the highest protocol accepted from the server
  - ✦ If TLS 1.2 is not already enabled:
- ✦ Click the Internet Options button on top far right of browser page
- ✦ Scroll down and click Settings
- ✦ Scroll to bottom of page then click "Advanced"
- ✦ Scroll down to "System" and click "Open proxy settings"
- ✦ Click "Advanced" (top, far right) on tab of pop up options screen ✦ Scroll down to "Security" and click "Use TLS 1.2" box

On startup

○ Open the New Tab page

○ Continue where you left off

● Open a specific page or set of pages

HS   HomeSite
http://fmhomesite/   ⋮

Add a new page

Use current pages

Advanced ▾

New tab   Ctrl+T
New window   Ctrl+N
New incognito window   Ctrl+Shift+N

History ▸
Downloads   Ctrl+J
Bookmarks ▸

Zoom   −   100%   +   ⛶

Print...   Ctrl+P
Cast...
Find...   Ctrl+F
More tools ▸

Edit   Cut   Copy   Paste

Settings
Help ▸
Exit

⊞ Managed by your organization

System

Continue running background apps when Google Chrome is closed   ⬤

Use hardware acceleration when available   ⬤

Open proxy settings   ⧉

Reset and clean up

Restore settings to their original defaults ▸

Clean up computer ▸

🌐 Internet Properties   ?   ✕

General   Security   Privacy   Content   Connections   Programs   Advanced

Home page

To create home page tabs, type each address on its own line.

Updating Apple Safari

If you have Apple updates turned on, Safari should stay up-to-date automatically. To verify that your version of Safari is the latest or update manually, follow these steps:

- ✦ Open the **Apple menu** and choose **App Store**.
- ✦ In the top of the window that appears, click the **Updates button** in the toolbar.
- ✦ Find Safari and click **Update** (or **Update all** to do every app).

Enabling or Disabling TLS Protocols in Apple Safari

- ✦ There are no options for enabling SSL/TLS protocols. If you are using Safari version 7 or greater, TLS 1.1 and TLS 1.2 are automatically enabled.
- ✦ If you are using a Safari version older than V.7, you must update your browser.
- ✦ If you are using an Operating System prior to OS X 10.9, you will need to update your OS before you are able to update Safari to a version which supports TLS 1.2. You can update your mac OS **here**.

Appendix - TLS 1.2 Browser Support Table

*If using a Windows platform, you must have the Windows 7 Operating system installed at minimum for compatibility with any browser which supports TLS 1.2. You can update to a compatible Windows OS **here***

Browser	OS Platforms	Browser Version	TLS 1.2
Google Chrome	Windows (7+) OS X (10.10+) Linux Android (4.1+) iOS (9.0+) Chrome OS		
		1-29	Not supported
		30-75	Supported
Mozilla Firefox	Windows (7+) OS X (10.9+) Linux Android (4.1+) iOS (9.0+)		
		1-23	Not supported
		24-26	Supported (Disabled by default)
		27-67	Supported
Microsoft Internet Explorer	Windows 3.1, 95, 98, NT, 2000[n 21][n 22], XP, Server 2003, Vista Mac OS 7.1, 8, X, Solaris, HP-UX		
		1.x-9	Not supported
	Server 2008	7,8,9	Supported (Disabled by default)
	Windows 7, Server 2008 R2	8,9,10	Supported (Disabled by default)
		11	Supported
	Windows 8, Server 2012	10	Supported (Disabled by default)
	Windows 8.1, Server 2012/ R2, Windows 10	11	Supported
Microsoft Edge	Windows 10 V.1507 - Windows 10 V.1903, Server V.1709 - Server V.1903, Server 2016 V.1607 - Server 2019 V.1809	IE 11	Supported
Apple Safari	OS X 10.2 - OS X 10.8	1-6	Not supported
	OSX 10.9 - OS X 10.11, macOS 10.12 - macOS 10.15	7-13	Supported