How to enable / disable TLS 1.3 in Windows 10

For TLS to work, it must be enabled on both the client and the server. For Windows server users, TLS 1.3 is enabled by default in IIS / HTTP.SYS.

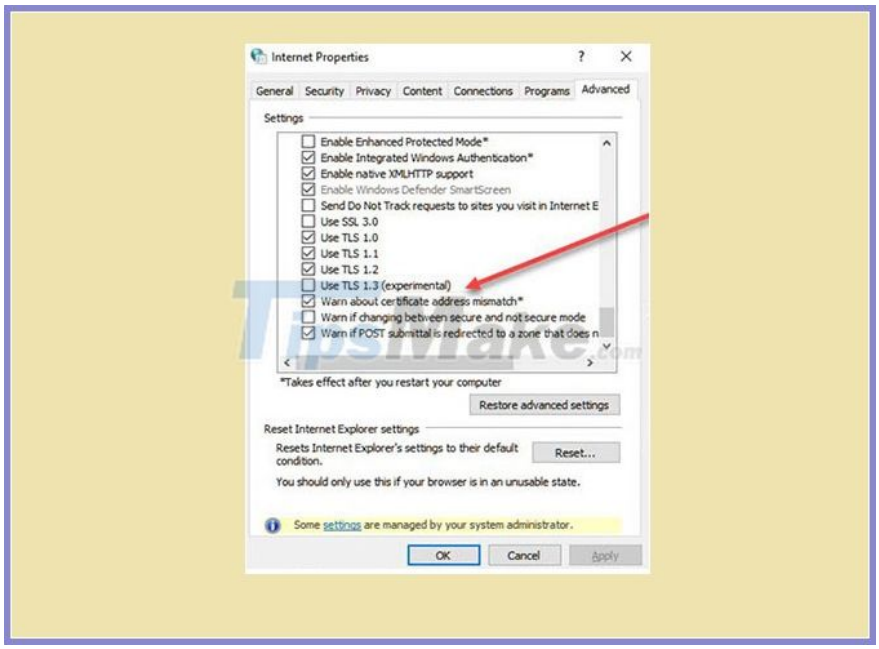
TLS or Transport Layer Security is a security protocol designed with two goals in mind - maintaining privacy and keeping data secure on the Internet. So when an email is sent from a computer to a server, the web browser loads a web page or does VoIP, TLS can encrypt them. If you know what SSL is, then TLS is an evolution of this protocol. It is interesting to note: HTTPS is an implementation of TLS over the HTTP protocol.

How to enable / disable TLS 1.3 in Windows 10

For TLS to work, it must be enabled on both the client and the server. For Windows server users, TLS 1.3 is enabled by default in IIS / HTTP.SYS. In Windows 10, starting with Insider Preview Build 20170, users can enable TLS on Microsoft Edge Legacy, in Microsoft Edge (Chromium), Chrome and Firefox.

After enabling the setting, you should restart your browser for TLS 1.3 to take effect. Please note that this feature is still rolling out to all browsers and may show up in your browser a bit late.

1. Enable TLS on Microsoft Edge Legacy



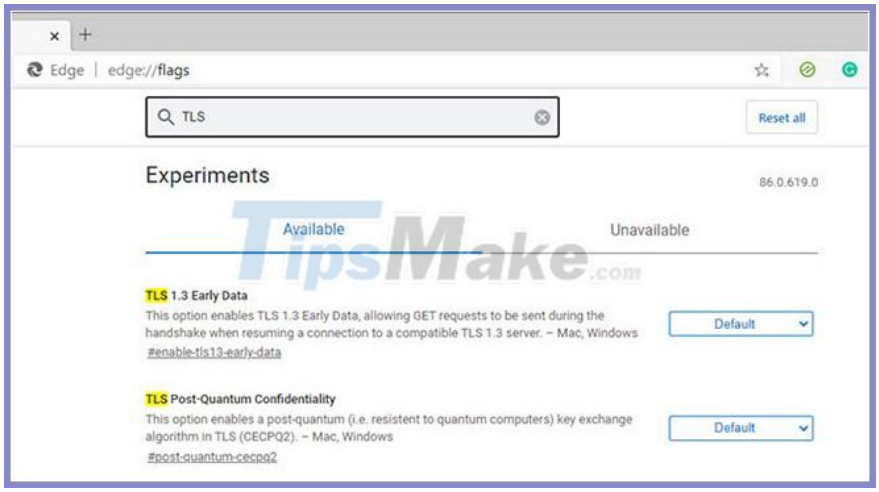
Step 1. Type **inetcpl.cpl** into **Run** (**Win + R**) and press **Enter** key **.**

Step 2. The **Internet Properties** window will open. Let's move on to the **Advanced** section **.**

Step 3. In the security section, check the box **TLS 1.3.**

Step 4. Restart the browser.

2. Enable TLS in Microsoft Edge (Chromium)



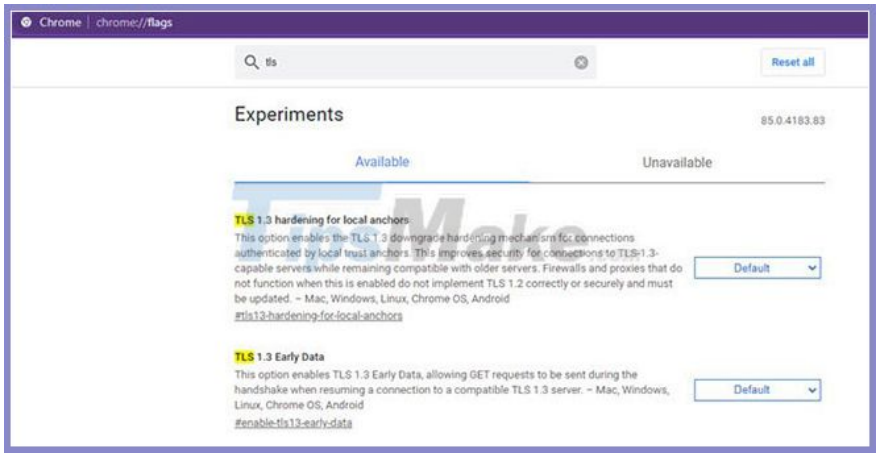
This version of Edge is built on Chromium Engine, does not use the Windows TLS stack. You will have to configure them independently using the **edge: // flags** dialog box **.**

On a new tab in Edge, type **edge: // flags.**

Search for **TLS 1.3** and turn on the setting

Keep in mind that it's still in beta (first rolled out with Windows 10 Insider and will be expanded).

3. Enable TLS 1.3 in the Chrome browser



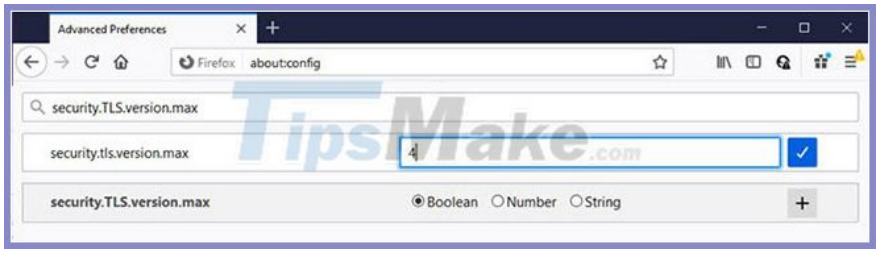
Since Chrome and Edge both use Chromium Engine, you can enable or change the settings in a similar way with Chrome Flags.

Type **chrome: // flags** in a new tab on Edge and press the **Enter** key **.**

Search for **TLS 1.3** and turn on the setting.

You will notice that the setting is enabled by default for Chrome. The same thing will happen to all browsers in the near future.

4. Enable TLS 1.3 in Firefox

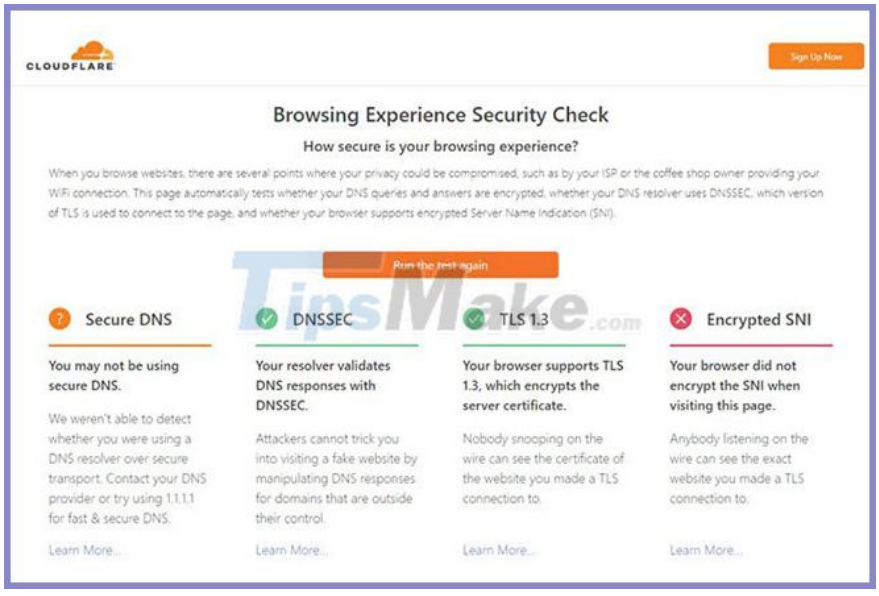


1. Launch Firefox and type **about: config** , then hit the **Enter** key in a new tab.
2. The configuration area with the search box opens.
3. Find the flag **security.tls.version.max** and double click to edit the value.
4. Change the value from **3** to **4** .
5. Restart Firefox browser.

Hopefully the tutorial is easy to follow and if you're going to use TLS, you can enable it in Windows, as well as all supported browsers. If you want to disable TLS, change the value to 3.

Check if TLS 1.3 is enabled properly

You can use Cloudflare's Browsing Experience Security Check to see if TLS 1.3 is enabled by default.



Once on the page, press the **Check My Browser** button and it will show details like Secure DNS, DNSSEC, TLS 1.3 and Encrypted SNI.

You finished reading the article "**How to enable / disable TLS 1.3 in Windows 10**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
