

# The browser will stop using TLS 1.0 and TLS 1.1 in 2020

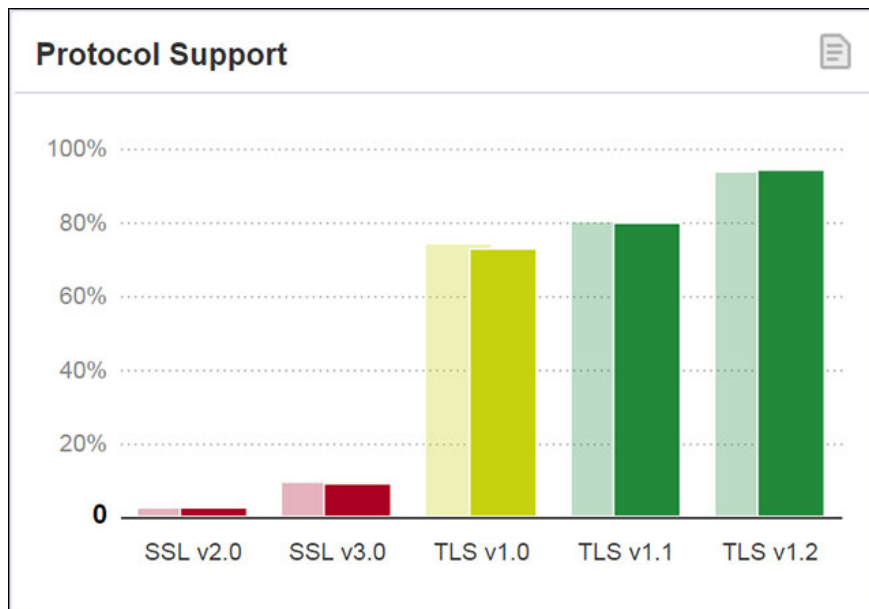
Microsoft, Google, Apple and Mozilla jointly announced that they will stop using TLS 1.0 and TLS 1.1 security communication protocols from 2020.

Microsoft, Google, Apple and Mozilla jointly announced that they will stop using TLS 1.0 and TLS 1.1 security communication protocols from 2020.

TLS (Transport Layer Security) is the protocol used to encrypt the connection between the browser and the website the user visits. This protocol creates an encrypted channel for data to be sent and received to encrypted websites and unreachable third parties. While it is important for all activities, it is especially important when you provide information such as passwords, accounts .

Over the past 20 years, browsers have been supporting TLS 1.0, then TLS 1.1 successors, but less and less have used this protocol and moved to TLS 1.2 and 1.3 standards. The new standard is not only better security but also supports new network protocols like https / 2 and speed up web browsing.

More than 94% of pages surveyed by Qualys SSL Labs currently support TLS 2.1 so the over 20-year-old protocol has been 'retired' and replaced with a new, safer protocol.



*94% of websites in the survey used TLS 1.2*

Chrome, Safari, Edge or Firefox statistics also show that most users no longer use this protocol.

1. Google says only 0.5% of https connections on Chrome use TLS 1.0 or TLS 1.1.
2. Apple said that less than 0.36% https connection on Safari uses TLS 1.0 or TLS 1.1.
3. Microsoft says only 0.72% of secure Edge connections use TLS 1.0 or TLS 1.1.
4. Firefox has the highest number of connections using TLS 1.0 or TLS 1.1, up to 1.2% but still a very small number.

Each company has its own plan to stop using this protocol.

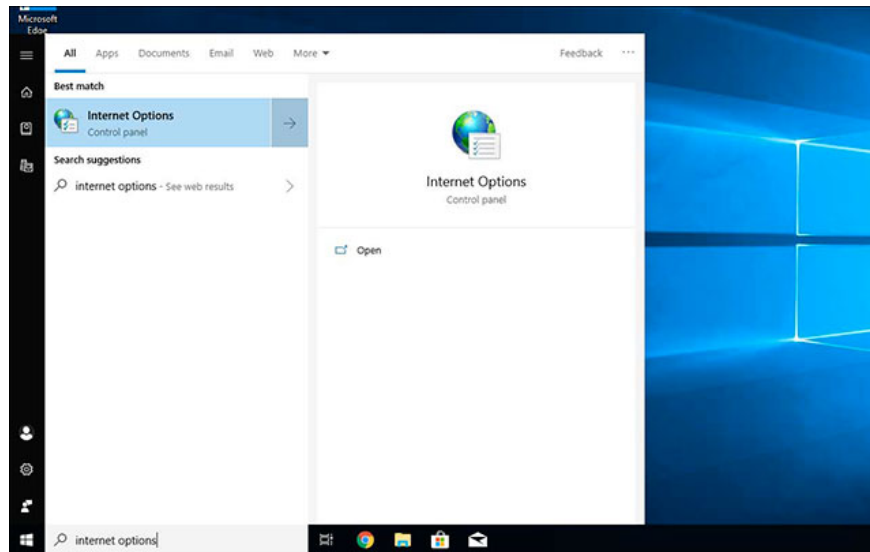
1. Google will release TLS 1.0 and TLS 1.1 stop notifications on Chrome 72, from Chrome 81 will completely abandon this protocol.
2. Mozilla stopped supporting TLS 1.0 and TLS 1.1 on Firefox from 3/2020. Users of Beta, Developer and Nightly will see these changes sooner.
3. Microsoft will stop supporting TLS 1.0 and 1.1 on Edge and Internet Explorer in the first half of 2020.
4. Apple stopped supporting these protocols on iOS and macOS from 3/2020.

### Check if you are affected

For Windows users, you can check to see if stopping support for these protocols affects you by disabling them. In the Windows Internet Options section, disable TLS 1.0 and 1.1 to see if it affects pages or access.

### Steps to disable TLS 1.0 and 1.1 on Windows

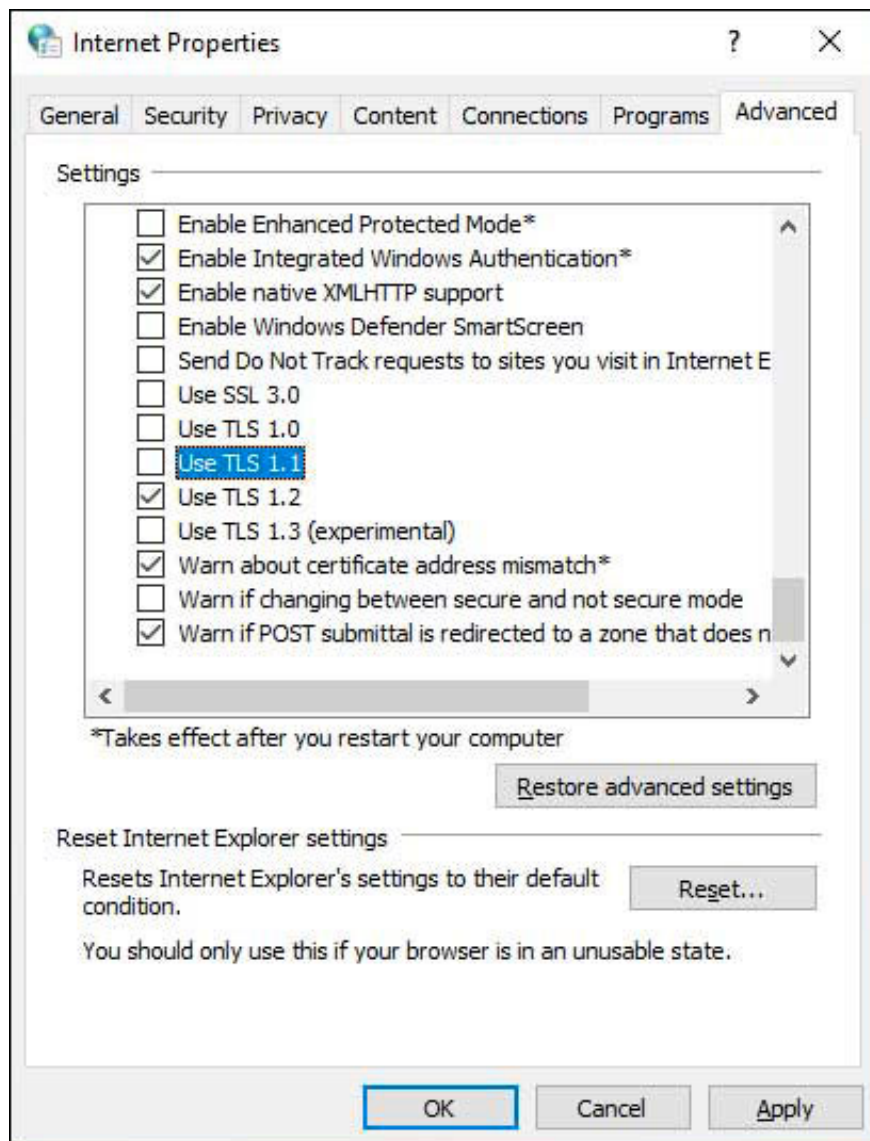
**Step 1 - Open Start Menu, type Internet Options and select Internet Options Control Panel.**



*Open Internet Options*

**Step 2 - Open Internet Properties and select the Advanced tab .**

**Step 3 - scroll down and find Use TLS 1.0 and Use TLS 1.1 in Security. Then uncheck these 2 items.**



*Uncheck to use TLS 1.0 and 1.1 protocols*

**Step 4** - Click **Apply** and click **OK** to save the changes.

Now you can browse the web as usual to see if this change has any effect.

See more:

1. Officially released TLS 1.3, promising a faster, safer Internet world
2. 7 reasons your website needs an SSL certificate
3. Knowledge of TCP / IP network protocols

You finished reading the article "**The browser will stop using TLS 1.0 and TLS 1.1 in 2020**" 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.