IPFS Deprecated Support for TLS 1.0 and 1.1

Transport Layer Security (TLS) is a critical cryptographic protocol that provides authentication and data encryption between different endpoints (for example, between your desktop and the application server) and secures HTTPS. To best safeguard this Web traffic, it is important to use current and more secure versions of the TLS protocol. The legacy TLS 1.0 and 1.1 versions account for a very small percentage of Web traffic today. TLS 1.2 was published to address weaknesses in TLS 1.0 and 1.1 and has seen wide adoption since then. To ensure compliance with industry standards, IPFS will disable support for TLS 1.0 and TLS 1.1 on March 6, 2021.

What does this mean?

In short, TLS is the way your internet browser communicates and connects with IPFS and the rest of the web. As the web has evolved, the threats posed by hackers and other bad actors has evolved too, and new security protocols are required to keep pace.

That's why TLS 1.0 and 1.1 are now being phased out, and TLS 1.2 and 1.3 is used instead. Both TLS 1.0 and 1.1 contain security vulnerabilities that could potentially allow third parties to "see" the information being exchanged between your browser and IPFS, including sensitive business details.

How this affects your business

As of March 6, 2021, the IPFS.com site will become inaccessible on any browser that still relies on TLS 1.0 or TLS 1.1; users of those browsers will see a blank screen or an error message when attempting to access the site. As these updated standards are adopted across the web, you will encounter similar difficulties with other websites as well.

How you can prepare

These outdated security protocols are primarily used by older browser models, and our research shows that only a small percentage of users will be affected. Modern browsers already support TLS 1.2, so it's likely you won't notice any difference at all.

To guard against any disruption in service, however, we recommend you confirm your browser's compatibility before March 6, 2021.

1055 Broadway, 11th Floor | Kansas City, MO 64105 | p. 816.627.0530

Browser Support

For the best software experience, we recommend using the latest version of Firefox, Chrome, Safari, or Edge.

The following table lists the version and date by which common internet browsers supported TLS 1.2.

Browser	Supported version and date
Chrome	Version 30 (August 2013)
Edge	Version 12 (July 2015)
Firefox	Version 27 (February 2014)
Internet Explorer	Version 11 (October 2013)
Safari	Version 7 (October 2013)

Source: https://caniuse.com/#feat=tls1-2.

To ensure access to IPFS.com after March 6, 2021, confirm your browser supports TLS 1.2 and 1.3 by clicking this link.

If your browser supports TLS 1.2 and 1.3, you will see the message, "Your user agent has good protocol support."

If your browser does not support TLS 1.2 and 1.3, you will need to upgrade your browser to the latest version.

If you try to connect to IPFS using an incompatible browser, you will likely see one of the following messages:

- ERR_SSL_VERSION_OR_CIPHER_MISMATCH
- SSL_ERROR_UNSUPPORTED_VERSION
- Cannot connect securely to this page

If you have additional questions regarding this upgrade, please contact your local branch office.