Insecure warning in your browser? It might be OK...

After installing Syncplify Server! you will be able to manage it securely via web interface over HTTPS.

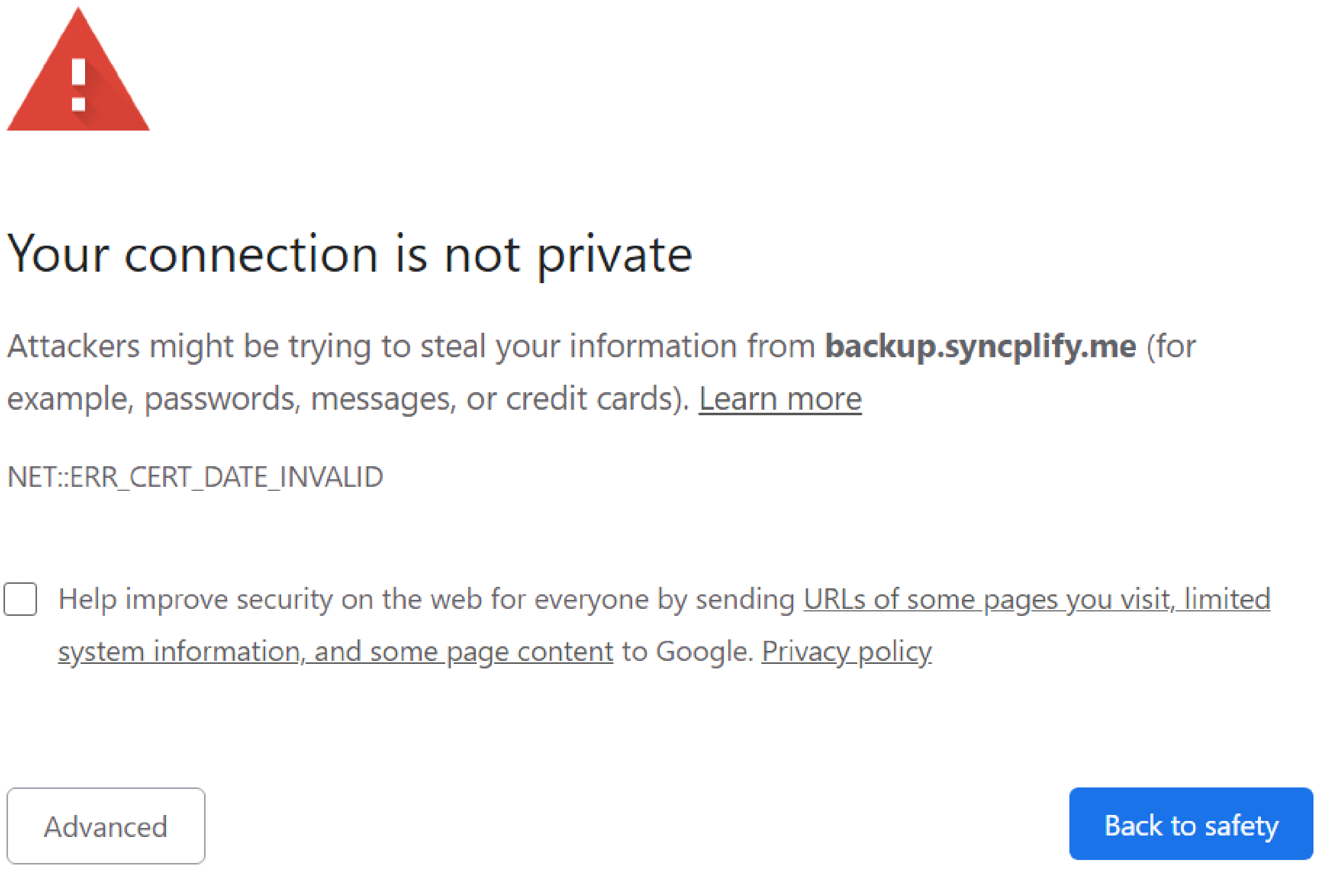
Now, a very common choice is to use a **self-signed certificate**, because it **saves money** and if you know what you’re doing it doesn’t compromise security. This is, in fact, the most common choice among our users (according to our surveys).

But **if you use a self-signed certificate, your browser will warn you** that your connection may not be private or secure. That’s because self-signed certificates are often used for man-in-the-middle (MitM) attacks. But this is not the case, of course, if you can verify that this particular self-signed certificate was created by you and for you.

To get rid of this annoying message, you basically have 2 options:

1. Spend some money to buy a trusted X.509 (SSL/TLS) certificate from a Certification Authority like DigiCert, Comodo, Thawte, and the like. It goes without saying that this is the recommended choice, as it takes advantage of the inherent trust chain provided by the Certification Authority.
2. Verify and accept the self-signed certificate you have just created and add it to the trusted keychain of your browser. In this case, you are advised to always verify the certificate’s fingerprint to make sure it’s really the one you created yourself, and that you’re not a victim of a Man-in-the-Middle (MitM) attack.

If you have chosen option #2, here’s how you do it in Chrome:



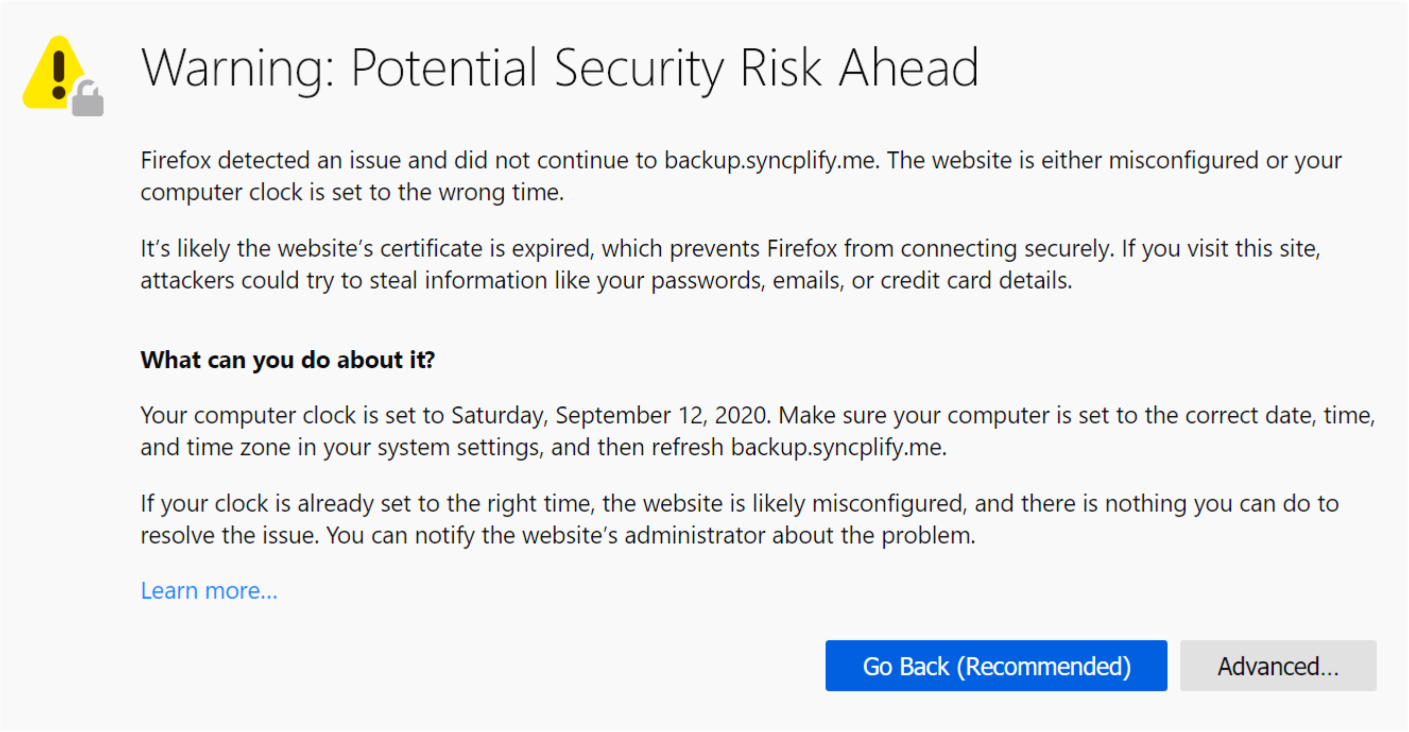
Your connection is not private

Attackers might be trying to steal your information from **backup.syncplify.me** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_DATE_INVALID

□ Help improve security on the web for everyone by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

This is how you do it in Firefox:



Warning: Potential Security Risk Ahead

Firefox detected an issue and did not continue to backup.syncplify.me. The website is either misconfigured or your computer clock is set to the wrong time.

It's likely the website's certificate is expired, which prevents Firefox from connecting securely. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

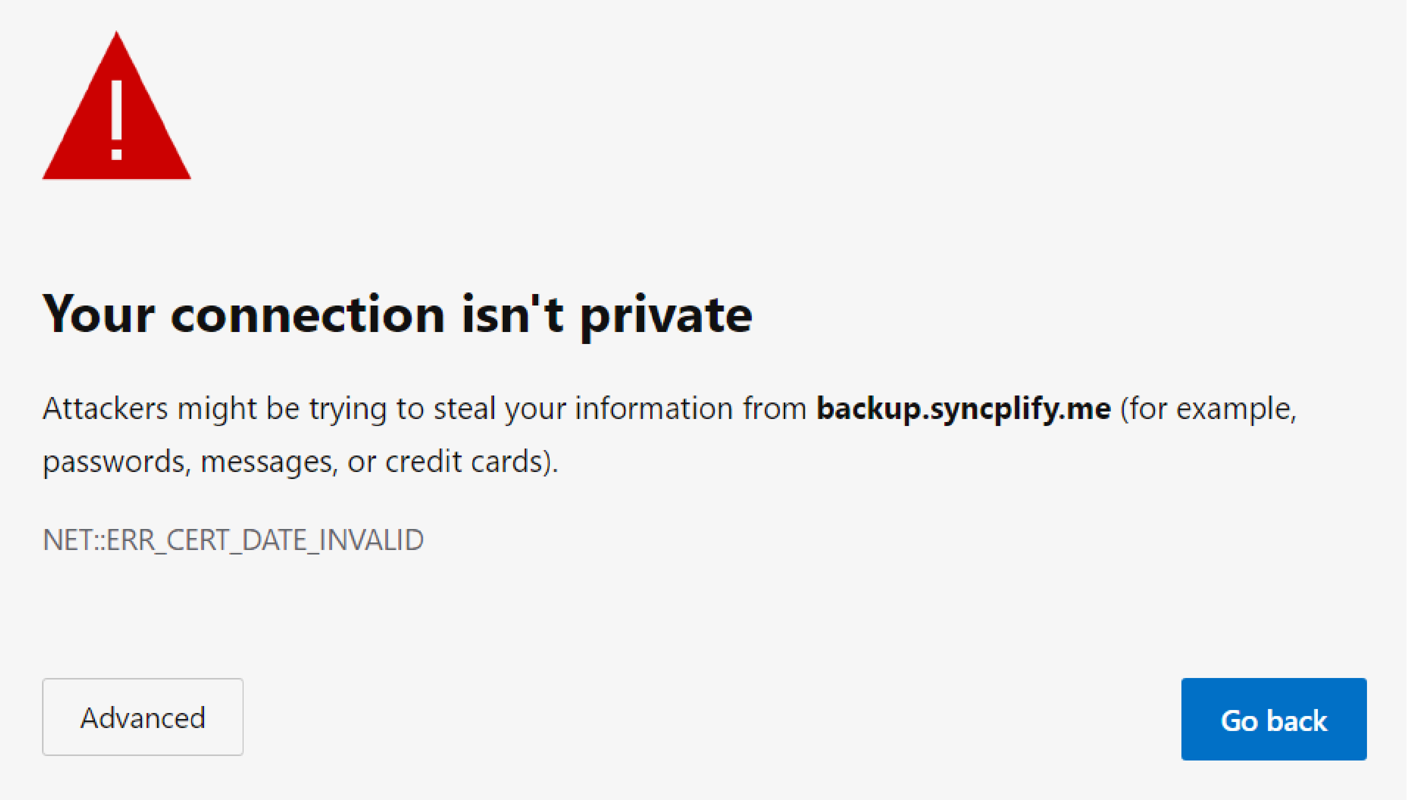
What can you do about it?

Your computer clock is set to Saturday, September 12, 2020. Make sure your computer is set to the correct date, time, and time zone in your system settings, and then refresh backup.syncplify.me.

If your clock is already set to the right time, the website is likely misconfigured, and there is nothing you can do to resolve the issue. You can notify the website's administrator about the problem.

Learn more...

And this is how you do it in the new Chrome-based Microsoft Edge (the old Edge is very similar though):



Your connection isn't private

Attackers might be trying to steal your information from **backup.syncplify.me** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_DATE_INVALID

> If you're using a self-signed certificate (or if you're accessing the management UI via its IP address instead of host name) it's totally normal for this to happen, and you can safely go ahead and skip the browser warning. Once you do that, you will be able to securely access Syncplify.me Server!'s a web management interface.

We purposely don't show any screenshot taken with Internet Explorer, as its JavaScript support (depending on the browser version) is generally too buggy, and we do not support its use in conjunction with our software.

Revision #3
Created 7 February 2023 00:37:27 by DevTeam
Updated 7 February 2023 22:52:04 by DevTeam