

---

## Article

[Katherine Reid](#) · Nov 27, 2017 1m read

## Upgrading TLS configurations

Caché will not change the cryptographic settings in an existing TLS configuration when you upgrade. This means that unless you've updated them yourself, you're still using the values from the very first version you started using SSL in.

If you've upgraded since creating your TLS configurations, take a moment to look at the enabled protocols and ciphersuites to make sure you've enabled all the versions you want, and disabled the old versions you don't want. You can find existing TLS configurations in the management portal under System Administration -> Security -> SSL/TLS configurations.

The default ciphersuite string has changed to include new options and is now: ALL:!aNULL:!eNULL:!EXP:!SSLv2 If you're still using the old default (TLSv1:SSLv3:!ADH:!LOW:!EXP:@STRENGTH) you may want to change to the new string, as the old one does not include new ciphersuites which some sites require.

More and more sites are moving to requiring TLS v1.2, which may not be enabled if you upgraded from a version before it was available.

[#SSL](#) [#Tips & Tricks](#) [#Cache](#)

---

Source URL: <https://community.intersystems.com/post/upgrading-tls-configurations>