

ClockSkew

SAML, like most security protocols, relies on correct time synchronization between servers to work properly. Clients are generally not required to be well-configured, but servers **MUST** be synchronized to within a few minutes of each other. In particular, an SP must be within a few minutes of the IdP or various errors can result, and the browser user will see an error message mentioning clock skew or expiration of some sort.

The exact tolerance is set by the `clockSkew` attribute in the root element of the [ShibbolethXml](#) file. It is set in seconds and defaults to a 3 minute window on either side.

Errors resulting cannot be fixed except by adjusting one or both parties' clock. Usually one party is correct and the other is not, but it is impossible to know which without looking at a correct time source.

Proper Shibboleth installation **REQUIRES** a good time source using NTP or some other time protocol. Most operating systems can be configured to synchronize against a correct time source.

If you're running Windows, this article might be helpful: <http://support.microsoft.com/kb/816042>