How long should my SSO tokens live?

Domain, access and SEO

Short: 300 seconds (5 minutes) is a good default, and it's what the **Token TTL** setting recommends.

A token only has to live long enough to reach HelpCenter.io. Your Login URL redirects the reader straight to /sso/jwt, so a few minutes leaves plenty of room, and once the reader is signed in the token isn't needed again.

- **Sign-in keys work once.** The key HelpCenter.io sends to your Login URL is good for one sign-in, so a longer token life gives readers nothing extra. It only widens the window in which a leaked token could be used.
- **Token TTL caps widget tokens only.** The widget rejects tokens older than your Token TTL (30 to 86,400 seconds), even if their exp is later. For sign-in through your Login URL or an iframe, exp is the only limit, so keep it short on your side.
- **The widget gets fresh tokens on its own.** It asks your onAuthExpired function for a new one when it needs it, so short tokens don't bother your readers.
- **The token's life isn't the sign-in's life.** Once a reader is signed in to your help center, **Reader sign-in lasts** decides how long they stay signed in: from 1 hour to 30 days, 24 hours by default. See Sign readers in with your own login (JWT SSO).
- **Clocks matter.** exp is required, and HelpCenter.io allows 30 seconds of difference on iat and exp. Keep your server's clock in sync, for example with NTP.

The full rules are in JWT claims and validation rules on the developer portal.

Related articles

- Sign readers in with your own login (JWT SSO)
- Sign readers into the widget with a JWT on the developer portal