

Openprovider DNS: SOA record and expire value

You might have noticed that our nameserver configuration includes a Serial Number, Refresh, Retry, Expire, and Minimum TTL (Time To Live) value in the SOA record. Some of you have specifically inquired about the Expire value being set to 7 days (604800 seconds). This FAQ entry explains what the SOA record is and why we have chosen this particular value.

What is an SOA Record?

The Start of Authority (SOA) record is a crucial part of every DNS zone. It stores essential administrative information about the domain, including:

- Primary Nameserver: The main server responsible for the domain's DNS records.
- Responsible Authority's Email: An email address for the administrator of the domain.
- Serial Number: A version number that increments each time the DNS records for the domain are updated. This helps secondary nameservers detect changes.
- Refresh: How often secondary nameservers should query the primary nameserver to check for updates to the zone file.
- Retry: How often secondary nameservers should retry querying the primary nameserver if the initial refresh attempt fails.
- Expire: This is the value you're asking about. It specifies the maximum time a secondary nameserver can continue to respond to DNS queries for this zone if it cannot reach the primary nameserver. After this time expires, the secondary nameserver will stop serving the zone, preventing potentially outdated information from being propagated.
- Minimum TTL (Time To Live): The default TTL for all records in the zone. This specifies how long resolvers (like your ISP's DNS servers) should cache DNS information before querying the nameservers again.

Why is our Expire value set to 7 days (604800 seconds)?

Our Expire value is intentionally set to 7 days (604800 seconds) for the following key reasons:

- Ensuring Data Consistency: A shorter expire time ensures that secondary nameservers will stop serving potentially outdated information relatively quickly if they lose contact

with the primary nameserver for an extended period. This minimizes the risk of inconsistencies in DNS resolution for your domain.

- **Balancing Resilience and Freshness:** While a very short expire time might seem ideal for immediate data consistency, it could put unnecessary strain on the secondary nameservers and the network if the primary server experiences temporary issues. A 7-day window provides a reasonable balance between ensuring data freshness and allowing sufficient time for any connectivity issues to be resolved without interrupting DNS service.
- **Industry Best Practices:** While specific expire values can vary, a setting within the range of a few days to a couple of weeks is generally considered a good practice for maintaining reliable DNS infrastructure. Our 7-day setting falls within this well-established range.
- **Our Robust Infrastructure:** We have a highly reliable and redundant DNS infrastructure in place with multiple secondary nameservers. This significantly reduces the likelihood of all secondary servers losing contact with the primary server for an extended period exceeding 7 days.

What does this mean for you?

In most normal operating conditions, you will not experience any impact from this 7 day expire value. Our monitoring systems and infrastructure are designed to ensure continuous and reliable DNS service. The 7 day value is a safety mechanism to prevent the propagation of stale DNS data in the unlikely event of a prolonged outage affecting the primary nameserver and its ability to communicate with the secondaries.

In summary, our 7 day (604800 seconds) expire value in the SOA record is a deliberate choice that prioritizes data consistency and reliability within a robust and well-maintained DNS infrastructure.

Revision #2

Created 2026-08-07 14:48:57 UTC by Sarath

Updated 2026-08-07 15:58:32 UTC by Sarath