

MAIN.8.2. EPP and RDAP Status Values

TLDTR implements EPP and RDAP status values in strict accordance with RFC 8056, which defines the exact mapping between EPP status values and their corresponding RDAP JSON status values.

To actively mitigate abusive registrations and protect Internet users, the TLDTR platform utilizes specific EPP and RDAP status values as enforcement mechanisms. This operational strategy is governed by comprehensive policies aligned with ICANN's Registry Agreement, specifically Specification 11 for proactive threat mitigation and Specification 6 for robust DNS security controls. Furthermore, TLDTR's status-based interventions are supported by ISO 27001 standards for strict incident management and are carefully balanced with GDPR and global privacy regulations to ensure user rights are fully protected during investigations.

EPP status values are used internally by the registry system and communicated through EPP to registrars. In RDAP responses, these values are explicitly translated and represented using the corresponding lowercase RDAP status values as defined in the IANA RDAP JSON Values registry.

To ensure exact alignment, the complete set of applied mappings from EPP to RDAP statuses is as follows:

EPP Status → RDAP Status

- `addPeriod` → `add period`
- `autoRenewPeriod` → `auto renew period`
- `clientDeleteProhibited` → `client delete prohibited`
- `clientHold` → `client hold`
- `clientRenewProhibited` → `client renew prohibited`
- `clientTransferProhibited` → `client transfer prohibited`
- `clientUpdateProhibited` → `client update prohibited`
- `inactive` → `inactive`
- `linked` → `associated`
- `ok` → `active`
- `pendingCreate` → `pending create`
- `pendingDelete` → `pending delete`
- `pendingRenew` → `pending renew`
- `pendingRestore` → `pending restore`
- `pendingTransfer` → `pending transfer`
- `pendingUpdate` → `pending update`
- `redemptionPeriod` → `redemption period`
- `renewPeriod` → `renew period`
- `serverDeleteProhibited` → `server delete prohibited`

- `serverHold` → `server hold`
- `serverRenewProhibited` → `server renew prohibited`
- `serverTransferProhibited` → `server transfer prohibited`
- `serverUpdateProhibited` → `server update prohibited`
- `transferPeriod` → `transfer period`

RDAP responses exclusively expose these exact, space-separated RDAP status strings in the status array (e.g., "`client hold`"), rather than exposing the original camelCase EPP status identifiers (e.g., "`clientHold`").

Additional context related to abuse handling or operational restrictions may be conveyed through RDAP remarks, events, or notices, while maintaining strict compliance with RFC 8056 and the IANA RDAP JSON Values registry.

This approach ensures full interoperability with RDAP clients and alignment with ICANN RDAP requirements.

TLDTTR's Approach to Minimising Abusive Registrations

To actively mitigate abusive domain registrations, TLDTR will enforce the following core policies and processes:

- **Domain Name Monitoring and Early Detection:** To catch threats early, TLDTR proactively monitors domain registrations for potentially abusive behavior. This includes identifying suspicious patterns such as bulk registrations, the use of malicious keywords, and unusual registrar activity. Furthermore, TLDTR utilizes AI-powered, human-in-the-loop systems to rapidly detect and respond to the most recent emerging threats.
- **Thorough Investigation:** Streamlined processes for abuse reporting and analysis. TLDTR utilizes automated triage tools alongside dedicated abuse desks to ensure all reports are processed immediately.
- **Decisive Action:** Rapid abuse response and remediation protocols. Once abuse is verified, we immediately apply restrictive EPP status codes (such as `serverHold`) to neutralize the threat. This swift intervention minimizes the active lifespan of malicious domains and protects end-users.
- **Strategic Partnerships:** Ongoing collaboration with law enforcement and industry stakeholders. TLDTR will actively share threat intelligence and coordinate global takedown efforts with cybersecurity organizations. This unified approach ensures compliance with legal frameworks while strengthening the broader internet infrastructure.
- **Technical Safeguards:** Advanced DNS abuse prevention utilizing DNSSEC and rate limiting. DNSSEC protects the integrity of DNS queries by preventing spoofing and cache-poisoning attacks. Additionally, strict rate limiting curbs automated bot activity and helps mitigate the severity of DDoS attacks.

EPP Status Values for Abusive Registrations

When a domain is under investigation for abusive behaviour (e.g., phishing, malware, or spam), the following EPP status codes may be applied to restrict its operation:

- **serverHold:** Disables DNS resolution.
- **serverTransferProhibited:** Freezes registrar transfers during investigations.
- **serverDeleteProhibited:** Prevents deletion to preserve data for law enforcement.
- **serverRenewProhibited:** Blocks the domain from being renewed.
- **serverUpdateProhibited:** Prevents any configuration updates to the domain.

RDAP Status Values for Abusive Registrations

In accordance with strict RFC 8056 mappings, the corresponding RDAP JSON status values for domains under abuse investigation are:

- **server hold:** Disables DNS resolution due to confirmed abuse.
- **server delete prohibited:** Prevents deletion to preserve data for law enforcement
- **server transfer prohibited:** Freezes registrar transfers during investigations.
- **server renew prohibited:** Registry blocked renewal due to enforcement actions
- **server update prohibited:** Prevents any configuration updates to the domain.