W

WHOIS and RDAP: How to Look Up Domain Registration Data

RDAP is now the definitive source for gTLD registration data. Learn how it differs from legacy WHOIS, how to read results, and how to avoid false conclusions.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

WHOIS is the familiar name for looking up domain-registration records. **RDAP** (Registration Data Access Protocol) is the newer, structured protocol designed to replace the legacy text-based WHOIS service. Since **January 28, 2025**, RDAP has been the definitive source for registration information for generic top-level domains (gTLDs), according to ICANN.

People still say “WHOIS lookup,” and some WHOIS services remain for particular country-code domains, IP addresses, or legacy systems. For a modern `.com`, `.org`, or other gTLD investigation, start with RDAP.

WHOIS vs. RDAP

- **WHOIS** returns loosely formatted text, uses inconsistent labels, and has limited support for secure access and internationalized data.
- **RDAP** returns standardized JSON over HTTPS, supports authoritative service discovery, clearer status information, internationalization, and differentiated access to nonpublic data.
- **ICANN Lookup** provides a human-readable interface and a raw RDAP response for supported domain names.

RDAP does not make all registrant details public. Privacy laws, contractual rules, privacy/proxy services, and registrar policies often result in redacted contact fields.

How to look up a domain safely

1. Enter the exact registered domain—not a full page path—into ICANN Lookup or another tool that follows authoritative RDAP discovery.
2. Confirm the result names the domain you intended. Watch for lookalike characters, extra subdomains, and punycode.
3. Record the registrar, creation and expiration dates, last update, domain statuses, nameservers, and DNSSEC information.
4. Open the raw RDAP response when a field is missing or the display simplifies it. Follow the registrar's abuse contact for a credible abuse report.
5. For an IP address, use the relevant Regional Internet Registry's RDAP service. Domain registration and IP allocation are different records.

How to read common RDAP and WHOIS fields

- **Registrar:** the company sponsoring the domain registration. It is not necessarily the website host or owner.
- **Creation date:** when the current registry record was created. It does not prove when a brand, company, or website began.

- **Expiration date:** the registry expiration date, which may differ from the registrant's billing or renewal status.
- **Updated date:** a registry change occurred. It does not tell you which field changed.
- **Domain status:** Extensible Provisioning Protocol (EPP) codes such as `clientTransferProhibited`, `redemptionPeriod`, or `pendingDelete`. A transfer lock is common and not evidence of abuse.
- **Nameservers:** servers authoritative for DNS. Shared providers can host many unrelated customers.
- **DNSSEC:** whether the delegation uses DNSSEC. It protects DNS integrity; it does not certify that site content is honest or safe.
- **Registrant contact:** may be redacted or represented by a privacy/proxy service. Redaction is normal and not a scam signal by itself.

What a domain lookup cannot prove

A WHOIS or RDAP record cannot by itself prove who controls a website, whether a shop will deliver, whether a download is safe, or whether a message is genuine. Old domains can be compromised or sold, and new domains can belong to legitimate projects. Privacy protection is common for both honest and malicious registrants.

Use registration data as one part of an investigation. Compare it with the exact URL, DNS records, certificate transparency, website history, independent business records, payment method, reputation, and observed behavior. Do not turn a single signal such as “recently registered” into a definitive verdict.

Reporting abuse and requesting nonpublic data

Use the registrar or registry abuse contact listed in RDAP and include the domain, URLs, timestamps, evidence, and the type of harm. A hosting provider may be a separate organization and may also need a report.

Nonpublic registration data is not available simply because someone is curious about a domain. Parties with a legitimate legal basis may use registrar disclosure procedures or ICANN's Registration Data Request Service where applicable. Requirements and outcomes vary, and access is not guaranteed.

WHOIS and RDAP FAQ

Is WHOIS gone?

For gTLD registration data, RDAP became definitive in 2025, but the word WHOIS and some legacy services remain in other contexts.

Why is the owner hidden?

Public output may be redacted for privacy or represented by a proxy. That is expected and does not automatically indicate abuse.

Can a lookup tell me whether a domain is malicious?

No. It supplies registration clues, not a safety verdict.

ICANN explains the transition in its RDAP launch and WHOIS sunset update and its Lookup FAQ.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com