

Corporate Domain Glossary

Key terms for enterprise domain owners

The plain-language definitions of the terms you will need to know most: portfolio management, DNS and security, brand protection, dispute resolution, and dotBrand TLDs.

A

A record (and AAAA record): A DNS record that points a domain name to an IP address. A records hold IPv4 addresses; AAAA records hold IPv6 addresses. See also: CNAME, DNS.

ASCII (American Standard Code for Information Interchange): The basic character set of letters a–z, digits 0–9 and the hyphen that domain names were originally limited to. Names using other characters are IDNs, stored in DNS in an ASCII form that begins "xn--" (Punycode). See also: IDN.

Auth code (EPP code, transfer key): A unique password issued for a domain that authorizes its transfer to another registrar. Treat it as a credential: anyone holding it can start a transfer.

Auto-renew: A setting that renews a domain automatically before it expires. For corporate portfolios, it is the main safeguard against an accidental lapse.

B

Brand abuse: Any unauthorized use of a brand online: infringing domains, phishing sites, counterfeit stores, impersonating social accounts or misleading ads. See also: Brand protection.

Brand protection: The ongoing work of finding, prioritizing, and stopping brand abuse. For domains, it combines monitoring, defensive registrations, blocking, enforcement (UDRP, URS, takedowns) and recovery.

Brand Registry Group (BRG): A trade association representing companies that operate dotBrand TLDs, and their interests within ICANN.

C

CAA record (Certification Authority Authorization): A DNS record that names which certificate authorities may issue SSL/TLS certificates for a domain. It blocks unauthorized certificates being issued for your domains.

ccTLD (country-code top-level domain): A two-letter TLD tied to a country or territory, such as .uk, .de or .jp. Each ccTLD sets its own rules; many require a local presence and use their own dispute policy rather than the UDRP.

CNAME record (canonical name): A DNS record that makes one hostname an alias of another. Useful when many names should follow one target, but a CNAME left pointing at a retired service can be taken over. See also: Dangling DNS record.

Contention set: A group of new gTLD applications for identical or confusingly similar strings, where only one can be delegated.

Corporate registrar: A registrar built for enterprises rather than individuals. It offers portfolio management, security controls, consolidated billing, global TLD coverage, and dedicated account support.

Cybersquatting: Registering, holding or using a domain in bad faith to profit from someone else's trademark. See also: Typosquatting, UDRP.

D

Dangling DNS record: A DNS record that still points to a resource the company no longer controls, such as a deleted cloud app. Attackers can claim that resource and serve content on your subdomain (a subdomain takeover).

DDoS (distributed denial of service): An attack that floods a server or DNS service with traffic until it stops responding. Enterprise DNS hosting uses large, distributed networks to absorb these attacks.

Defensive registration: Registering a domain mainly to keep it out of others' hands, such as typos, key ccTLDs or brand terms in new gTLDs. Defensive names usually redirect to a primary site or stay inactive.

Delegation: The step where a TLD is added to the DNS root zone and starts working. For a new gTLD, it follows contract signing and pre-delegation testing.

DKIM (DomainKeys Identified Mail): An email authentication method that signs outgoing messages so receivers can confirm they came from your domain and were not altered. See also: DMARC, SPF.

DMARC (Domain-based Message Authentication, Reporting and Conformance): A DNS policy that tells receiving mail servers what to do with messages that fail SPF or DKIM checks and sends reports back. The policy is published as a TXT record, and a strict setting (quarantine or reject) is the main defense against email spoofing of your domains.

DNS (Domain Name System): The system that translates domain names into the IP addresses computers use. If DNS fails, websites, email and applications on the domain stop working.

DNS hosting: The service that answers DNS queries for your domains. Enterprise DNS hosting typically uses a global anycast network for speed, redundancy, and DDoS resilience.

DNS record: A single instruction in a domain's DNS that tells the internet how to handle one kind of request. Common types: A and AAAA (point a name to an IP address), CNAME (point a name to another name), MX (where email is delivered), TXT (text used for SPF, DKIM, DMARC and ownership checks), NS (which nameservers are authoritative) and CAA (which certificate authorities may issue certificates). Each type has its own entry in this glossary.

DNSSEC (DNS Security Extensions): A set of standards that add digital signatures to DNS so resolvers can confirm an answer really came from the domain's DNS and was not changed on the way. It protects against cache poisoning, which attackers use to send visitors to fake sites. DNSSEC works through a chain of trust from the root zone down: the zone is signed with a zone signing key (ZSK), that key is signed with a key signing key (KSK), and a matching DS record is published at the registry. Keys should be rotated on a schedule, which most enterprise DNS providers can manage for you.

Domain acquisition: Buying a domain already registered by someone else, often through a broker who negotiates anonymously, so the buyer's identity does not inflate the price.

Domain benchmarking: Comparing a company's domain portfolio with those of peers or competitors on size, TLD coverage, security settings and spend. It shows where a portfolio is over- or under-invested relative to its industry. See also: Gap analysis.

Domain blocking: A registry service that prevents registration of a brand term (and sometimes variants) across many TLDs for a single fee, without registering each name. See also: DPML, GlobalBlock.

Domain hijacking: Taking control of a domain without authorization, usually through compromised registrar credentials, social engineering or a fraudulent transfer. Registry Lock and MFA are the main defenses.

Domain monitoring (domain watch): Ongoing scanning of new registrations, DNS changes and web content for domains that match or resemble your brands. It feeds brand protection and enforcement decisions.

Domain name: A human-readable address, such as gcd.com, that maps to internet resources through DNS. It is made of labels separated by dots: the TLD on the right, then the second-level domain, then any subdomains.

AT A GLANCE

Parts of a domain

A domain reads right to left, from most general to most specific.

shop.example.com

Subdomain

Optional prefix you create
in your own DNS

Second-level domain (SLD)

The name you register
usually your brand

Top-level domain (TLD)

The extension, run by a registry

Domain name council (domain governance council): A cross-functional group, often drawn from legal and IP, IT and security, marketing and procurement, that meets on a regular schedule to set and oversee domain name policy for the whole company. The goal is to open communication between business units, agree on shared policies and strategy, get teams using the same core processes, keep portfolio reporting and governance in one place, and run the domain lifecycle from registration to retirement efficiently.

Domain portfolio: All the domains a company owns, across brands, regions and TLDs. Corporate portfolios often run to thousands of names.

Domain portfolio optimization (rationalization): Reviewing a portfolio to keep, consolidate, redirect or drop names based on use, risk and cost. The goal is the right balance of domains at the right spend.

dotBrand (.brand, brand TLD, branded TLD): A top-level domain that matches a brand and is operated by the brand owner for its own use, such as .godaddy, .bmw or .google. Only the owner and its affiliates can register names in it. Also written .BRAND, dot brand or brand gTLD. See also: New gTLD Program.

DPML (Domains Protected Marks List): A blocking service from Identity Digital (formerly Donuts) that blocks a trademarked term from registration across the large group of TLDs it operates, for a fixed term. Higher tiers extend the block to variants of the mark. Eligibility rules and covered TLDs change, so check the current list. See also: Domain blocking, TMCH.

E

EPP status codes: Standard codes showing a domain's state at the registry and registrar, such as clientTransferProhibited, serverUpdateProhibited or pendingDelete. They are visible in RDAP lookups and show at a glance whether a domain is locked.

Expiration date: The date a registration ends unless renewed. Missed renewals are one of the most common causes of corporate website and email outages. See also: Auto-renew.

G

Gap analysis: A review comparing a company's brands and key terms against the TLDs and markets that matter to it, showing where registrations are missing or unnecessary.

GDPR (General Data Protection Regulation): The EU data protection law. Since 2018 it has led registrars and registries to hide most personal registrant data from public lookups. See also: RDAP, WHOIS.

General Availability (GA): The launch phase when anyone can register names in a TLD, first come, first served. It follows Sunrise and any other early-access periods.

GlobalBlock: A cross-registry blocking service that blocks a brand term, and optionally its confusing variants and homographs, across participating TLDs from many registries in a single order. See also: Domain blocking, DPML.

gTLD (generic top-level domain): A TLD not tied to a country, such as .com, .org, .shop or a dotBrand. gTLDs operate under contracts with ICANN.

H

Homograph attack: Using look-alike characters, often from other scripts, to create a domain that appears identical to a real one (for example, a Cyrillic "a" in place of a Latin "a"). See also: IDN, Lookalike domain.

Hostname: The full name of one specific machine or service within a domain, such as www.example.com or mail.example.com. The bare domain (example.com, sometimes called the apex or naked domain) commonly redirects to the www hostname, or the other way around.

I

IANA (Internet Assigned Numbers Authority): The function, operated under ICANN, that manages the DNS root zone, IP address allocation and protocol parameters.

ICANN (Internet Corporation for Assigned Names and Numbers): The nonprofit that coordinates the global DNS, contracts with gTLD registries and registrars, and sets gTLD policy through its multistakeholder community.

IDN (internationalized domain name): A domain that uses characters beyond a-z, 0-9 and the hyphen, such as accented letters or non-Latin scripts (Arabic, Chinese, Cyrillic). Brands may need IDN versions for key markets.

IP address: The numeric address of a device or server on the internet. DNS maps domain names to IP addresses. See also: A Record

L

Local presence (trustee service): A service that meets a ccTLD's requirement for an in-country registrant or contact, so a company can register there without a local office.

Lookalike domain: A domain built to resemble a real brand domain through typos, swapped characters, added words or a different TLD. Lookalikes are a common tool for phishing and fraud.

M

MFA (multi-factor authentication): Requiring two or more proofs of identity to sign in, such as a password plus an authenticator app or hardware key. It should be mandatory on every account that can change your domains or DNS.

MX record (mail exchanger): A DNS record that tells other servers where to deliver email for a domain.

N

Nameserver (NS record): A server that holds and answers DNS records for a domain. NS records at the registry tell the internet which nameservers are authoritative for that domain.

New gTLD: Any generic TLD added through ICANN's New gTLD Program, as opposed to the older extensions such as .com, .net and .org. More than 1,200 arrived from the 2012 round, including open TLDs like .shop and .app and dotBrands like .godaddy; more will follow from the 2026 Round.

New gTLD Program: ICANN's program for adding new generic TLDs through application rounds. The first round opened in 2012. The 2026 Round (also called the Next Round) accepted applications from 30 April to 12 August 2026. See also: dotBrand.

P

Parked domain: A registered domain with no active website, often showing a placeholder or ads. Unused corporate names are usually better redirected to a primary site.

Phishing: Using a fake website or email, often on a lookalike domain, to trick people into giving up credentials, payment details or data.

Premium domain: A name the registry or a reseller prices above the standard fee because of its perceived value, such as short or common-word domains.

Privacy/proxy service: A service that keeps a registrant's details out of public lookups. Corporate domains are usually registered openly in the company's name; privacy on a lookalike domain is common in abuse cases.

R

RDAP (Registration Data Access Protocol): The structured, secure successor to WHOIS for looking up domain registration data. It replaced WHOIS as the authoritative source for gTLD data in January 2025.

Redirect (domain forwarding): Sending visitors from one domain to another, such as from defensive or legacy names to a primary site. HTTPS redirects need a valid certificate on each forwarded domain.

AT A GLANCE**Who does what with your domain**

Three parties touch every domain. Knowing which is which tells you who to call.

Registrant

Your company

Owns the domain and decides how it is used

**Registrar**

e.g., GCD

Registers and manages domains on your behalf

**Registry**

e.g., Verisign for .com

Runs the master database for one TLD

Registrant: The person or organization that holds the registration for a domain, recorded as its legal owner. For corporate portfolios, this should be the company or a designated holding entity, never an individual employee.

Registrar: A company accredited by ICANN (and by ccTLD registries) to register domains for customers and pass that data to registries.

Registrar Accreditation Agreement (RAA): ICANN's contract with each accredited registrar, setting its obligations to registrants.

Registrar lock (domain lock): A set of statuses applied at the registrar that block changes to a domain until they are lifted through the registrar's verification process. The three common ones are clientDeleteProhibited (blocks deletion), clientTransferProhibited (blocks transfer to another registrar) and clientUpdateProhibited (blocks changes to contacts and nameservers). Support varies by TLD. For stronger protection, see Registry Lock. See also: EPP status codes.

Registry: The authoritative database of all domains in a TLD. The registry operator runs it and publishes the zone file that makes those domains work.

Registry Agreement: The contract between ICANN and a gTLD registry operator. dotBrand operators sign the same base agreement, with an added specification that reserves registrations for the brand owner and its affiliates.

Registry Lock: A security service set at the registry, one level above the registrar, that freezes a domain's nameservers and registrar. It guards against hijacking, automation mistakes, and a compromised registrar account. To make a change, the registrar asks the registry to unlock the domain, and the registry confirms the request out of band with named contacts (often by phone) before anything moves. It is the strongest protection for business-critical domains.

Registry Operator: The organization that runs a TLD: it sets registration policy, keeps the registry database, and publishes the zone file. For gTLDs it is the party contracted with ICANN, including a company running its own dotBrand. Older usage sometimes calls it a NIC (network information center).

Registry Service Provider (RSP): The technical provider that runs a registry's systems: database, DNS and registration interfaces. Most dotBrand owners outsource this role. ICANN evaluates RSPs before the 2026 Round's applications can rely on them.

S

Second-level domain: The label directly to the left of the TLD, such as "gcd" in gcd.com. It is the part a company registers.

SPF (Sender Policy Framework): A TXT record listing the servers allowed to send email for a domain, so receiving servers can flag mail from anywhere else. The record's ending shows how strict it is: "-all" says reject everything not listed, "~all" says treat it as suspicious. Domains that never send email should publish "v=spf1 -all". See also: DKIM, DMARC.

Sponsored TLD (sTLD): A gTLD run for a specific community or industry, where a sponsoring organization sets who may register. Examples include .aero, .museum, .travel and .jobs.

SSL/TLS certificate: A digital certificate that proves a website's identity and encrypts traffic to it, shown as HTTPS in the browser. Certificates expire and must be renewed, so they belong in the same inventory as the domains they cover.

String: The characters that make up a TLD or domain label. In the New gTLD Program, the "applied-for string" is the proposed TLD, such as .brand.

String similarity (string confusion): The test of whether a proposed TLD is so similar to an existing or applied-for one that users would confuse them. Confusingly similar applications are placed in a contention set or rejected.

Subdomain: A name to the left of the registered domain, such as shop.example.com. A company creates subdomains in its own DNS without registering anything new.

Sunrise: A launch phase of at least 30 days, before a new TLD opens to the public, when trademark owners recorded in the TMCH can register matching names first.

T

TLD (top-level domain): The last label of a domain name, such as .com, .uk or .bank. TLDs are either generic (gTLD) or country-code (ccTLD).

AT A GLANCE

Types of top-level domain

The extension after the last dot sets who can register and which rules apply.

.com

gTLD
(generic)

Not tied to a country;
usually open to anyone

.uk

ccTLD

(country code)

Two letters; each
country sets its rules

.aero

sTLD

(sponsored)

Limited to one
community or industry

.brand

Brand TLD

(dotBrand)

Owned and used only by
the brand itself

TMCH (Trademark Clearinghouse): A central database of verified trademarks used across new gTLDs. A recorded mark gives access to Sunrise registrations, Trademark Claims notices and many blocking services.

Transfer (registrar transfer): Moving a domain's management from one registrar to another, usually with an auth code. Consolidating a portfolio at one corporate registrar involves many transfers. See also: Transfer lock.

Transfer lock: A period, set by ICANN policy or the registrar, during which a domain cannot move to another registrar, for example after a new registration or a change of registrant. It is a fraud safeguard; check the current policy before planning a migration.

TXT record: A DNS record holding text, used for SPF, DMARC and DKIM, and to prove domain ownership to services such as email providers and certificate authorities.

Typosquatting: Registering misspellings of a brand or its domain (for example, g0daddy.com or godadddy.com) to catch mistyped traffic, often for phishing, ads or malware. See also: Cybersquatting, Lookalike domain.

U

UDRP (Uniform Domain-Name Dispute-Resolution Policy): ICANN's administrative process for transferring or cancelling a gTLD domain registered in bad faith. The complainant must show the domain is identical or confusingly similar to its mark, the registrant has no legitimate interest in it, and it was registered and used in bad faith. Cases are decided by providers such as WIPO. It covers all gTLDs and the ccTLDs that have chosen to adopt it.

URS (Uniform Rapid Suspension): ICANN's expedited process for suspending a domain involved in a clear-cut case of trademark infringement. It has a higher burden of proof than the UDRP and does not transfer or cancel the domain; it suspends the domain for the remainder of its registration period.

V

Vanity URL (promotional URL): A short, memorable domain used in advertising or print that redirects to where the content actually lives, such as a campaign name sending visitors to a page on the main corporate site. See also: Redirect.

W

Web hosting: The service that runs a website or application on servers. In domain terms, the hosting domain is where content actually lives, as opposed to vanity or defensive domains that redirect to it.

WHOIS: The original protocol and service for looking up who registered a domain. For gTLDs it has been replaced by RDAP, and most personal data is now hidden after GDPR. The term is still widely used for any registration-data lookup.

WIPO (World Intellectual Property Organization): The UN agency for intellectual property. Its Arbitration and Mediation Center is the largest UDRP provider and handles disputes for many ccTLDs.

Z

Zone file: The file of DNS records for a domain or TLD. A TLD's zone file lists every active domain in it, which makes it a key data source for domain monitoring.