Cloudflare DNS Integration Guide

CertSecure Manager uses Cloudflare as a DNS provider to complete ACME DNS-01 domain validation for automated certificate issuance and renewal.

Prerequisites

- An active Cloudflare account with the target zone(s) already hosted on Cloudflare - the domain's nameservers must point to Cloudflare.
- Permission in Cloudflare to create API tokens with DNS edit rights for those zones.
- Administrative access to CertSecure Manager, including Utilities → ACME → Domain.
- Outbound HTTPS (443) connectivity from the CertSecure Manager server to api.cloudflare.com.
- An ACME profile configured for the intended CA (e.g. Let's Encrypt, Google Public CA).

Step 1: Create a Cloudflare API Credential

- Log in to the Cloudflare dashboard → My Profile → API Tokens → Create Token.
- Grant the token DNS edit rights for the target zone: Permissions → Zone → DNS → Edit, scoped to the specific zone(s).
- Create the token and copy it (Cloudflare shows the token value only once).

Note: The token must be able to create and delete TXT records for the DNS-01 challenge.

Step 2: Add the Domain in CertSecure Manager

- Go to: Utilities → ACME → Domain.
- Click + Add Domain and fill in:
  - Domain: the FQDN managed in Cloudflare (e.g. example.com)
  - Provider: Cloudflare
  - API Token: the Cloudflare credential from Step 1
- Click Save.

Step 3: Validate DNS Ownership

- Use the Validate action on the domain entry to trigger a DNS-01 check - CertSecure creates and removes a TXT record via the Cloudflare API.
- When successful, the Validation column shows Valid. Domains must be Valid before certificate issuance.

Step 4: Use in ACME Issuance

- The validated Cloudflare-managed domain can now be selected by ACME profiles (Let's Encrypt, Google Public CA) for automated DNS-01 issuance and renewal.