

Google Public CA Integration Guide

This guide describes adding Google Public CA in CertSecure Manager. Google Public CA is a publicly trusted, ACME-based Certification Authority (like Let's Encrypt). No software installation is required on a separate host.

Note: Google Public CA uses External Account Binding (EAB) – an HMAC key and Key ID (KID) – issued by Google Cloud for your project. These must be generated in the Google Cloud Console (or with gcloud) before adding the entry in CertSecure Manager. If Google Public CA appears greyed/unconfigured on your tenant, it becomes selectable once the corresponding entitlement is enabled.

Prerequisites

- CertSecure Manager frontend and backend are fully operational.
- Your account has permission to manage Certification Authorities / ACME URLs.
- A Google Cloud project with the Public Certificate Authority API enabled.
- External Account Binding (EAB) credentials for that project – an HMAC key and Key ID (KID) – generated via the Google Cloud Console or the gcloud CLI.
- A valid email address to register the ACME account with Google.
- The domain(s) you plan to issue certificates for, and API credentials for your DNS provider (e.g. Cloudflare, Route 53, Google Cloud DNS).
- Outbound HTTPS (443) connectivity from the CertSecure Manager backend to dv.acme-v02.api.pki.goog.

Connection Reference

Item	Requirement / Value
Name	Friendly label for this ACME URL entry
URL	https://dv.acme-v02.api.pki.goog/directory – Google Public CA's ACME directory endpoint
Google Public CA	Checkbox that marks this entry as a Google Public CA endpoint and enables the EAB fields below
HMAC	External Account Binding HMAC key from Google Cloud
KID	External Account Binding Key ID (KID) from Google Cloud
Email	Contact email used to register the ACME account

Configuration Steps

Step 1: Generate External Account Binding (EAB) Credentials in Google Cloud

- Make sure that you have the Public CA External Account Key Creator (roles/publicca.externalAccountKeyCreator) IAM role. To grant this role, run:

```
gcloud projects add-iam-policy-binding PROJECT_ID \  
  --member=user:USER \  
  --role=roles/publicca.externalAccountKeyCreator
```

- Replace PROJECT_ID with the ID of your Google Cloud project, and USER with the unique identifier of the user to whom you want to assign the IAM role.
- In the Google Cloud Console, enable the Public Certificate Authority API for the project you want to issue certificates from:

```
gcloud services enable publicca.googleapis.com
```

- Create an External Account Key for that project (Cloud Console, or the gcloud CLI):

```
gcloud publicca external-account-keys create
```

- Record the returned HMAC key and Key ID (KID) immediately – Google only displays the HMAC value once.

Step 2: Add the Google Public CA Entry in CertSecure Manager

- Go to Administration > Certificate Authorities and click the Google tile (or go to Utilities > ACME > URL).
- Click Add URL.
- Enter: Name and URL (<https://dv.acme-v02.api.pki.goog/directory>).
- Check Google Public CA.
- Enter: HMAC, KID, and Email.
- Click Save.

Step 3: Verify Registration

- CertSecure Manager registers an ACME account with Google Public CA using the EAB credentials and email you supplied. On success, the entry appears in the ACME URL list and GooglePublicCA becomes selectable as a CA during enrollment.
- If registration fails, re-check that the HMAC and KID belong to the same Google Cloud project where the Public CA API is enabled, and confirm the email address is valid.

Step 4: Add and Validate a Domain

- Certificates can only be issued for domains registered in CertSecure Manager's domain registry. Go to Utilities > ACME > Domain and click Add Domain.
- Enter the Domain (fully-qualified) and select a DNS Provider (Cloudflare, Route 53, and others are supported).
- Click Save. CertSecure Manager validates the domain before it becomes available for enrollment.
- Repeat for every domain or sub-domain you plan to request certificates for.

Step 5: Enroll / Renew / Revoke

- **Issue:** Enrollment > Generate Certificate → select GooglePublicCA as the CA, choose the registered Domain and enter the Sub Domain Name → Submit.
- **Renew / Revoke:** performed from Inventory, the same as any other CA.

Troubleshooting

Symptom	Likely Cause	Fix
CA type greyed out	Entitlement/feature flag not enabled	Confirm license for Google Public CA
ACME account registration failed when saving the URL	Invalid or mismatched HMAC/KID, or the Public CA API is not enabled	Regenerate the EAB key pair in Google Cloud and re-enter both

Symptom	Likely Cause	Fix
	on that project	values together
Domain validation failed	DNS provider credentials are incorrect, or the DNS record has not propagated yet	Re-check the DNS provider credentials; allow time for propagation and retry
Enrollment fails – domain not found/validated	The domain was not added and validated under Utilities > ACME > Domain before enrolling	Add and validate the domain first (Step 4), then retry enrollment
Certificate request stuck in pending	The ACME challenge has not yet been resolved by Google	Confirm the DNS TXT record is publicly visible, then retry
TLS error contacting Google	Corporate proxy or firewall intercepting TLS to pki.goog	Allow outbound HTTPS 443 from the CertSecure Manager backend to dv.acme-v02.api.pki.goog without TLS interception