ACME Protocol Integration Guide

CertSecure Manager includes a built-in ACMEv2 (RFC 8555) server, letting standard ACME clients - certbot, win-acme, acme.sh, and others - enroll and renew certificates directly against CertSecure using CSR-based enrollment, with every issued certificate tracked alongside the rest of your certificate inventory.

Prerequisites

- CertSecure Manager is installed and reachable over HTTPS at the host you will use as the ACME directory URL.
- An Issuing CA is connected to CertSecure Manager and its certificates are in sync.
- A certificate template is available on that CA for the certificates this profile will issue.
- Your CertSecure user account has permission to open Utilities → ACME and create ACME profiles.
- An ACME client (certbot, win-acme, acme.sh, or similar) that supports External Account Binding (EAB) is installed on the target host.
- The domain or host being enrolled is resolvable and reachable from wherever challenge validation is performed - HTTP-01 requires inbound reachability, DNS-01 requires access to the DNS zone.
- Network access is permitted from the ACME client to CertSecure over HTTPS (port 443).
- A valid email address to associate with the ACME account for expiry and renewal notices.

Step 1: Connect the Issuing CA

- Ensure the Issuing CA you want ACME clients to enroll against is connected to CertSecure Manager and that all certificates are in sync.

Step 2: Open the ACME Utility

- Go to: Utilities → ACME.

Step 3: Start ACME Enrollment

- Click New ACME Profile in the top right.

Step 4: Configure the ACME Profile

- Email: the address to associate with this ACME account (used for expiry/renewal notices).

Note: CertSecure generates the profile and returns its EAB credentials - kid and hmac - one time only, shown directly on this screen. Copy both immediately; they cannot be retrieved again after you leave this screen (only the profile's email and expiry status remain visible afterward).

Step 5: Bind the Profile to a CA and Template

- Certificate Authority: choose the CA connected in Step 1.
- Template: the certificate template to issue against for this profile.

Every certificate requested through this ACME profile will be issued from this CA/template pair.

Step 6: Configure Your ACME Client

Point your ACME client at CertSecure's directory URL and supply the EAB credentials from Step 4:

- Directory URL: https://<certsecure-host>/v2/acme
- EAB kid: the kid value from Step 4.

- EAB HMAC key: the hmac value from Step 4.

Most clients accept these as flags, e.g.:

```
certbot --server https://<certsecure-host>/v2/acme \
  --eab-kid <kid> --eab-hmac-key <hmac>
```

Step 7: Enroll and Renew

Once the client registers its account with the EAB credentials, it generates its own key pair and CSR locally, completes an HTTP-01 or DNS-01 challenge, and submits the CSR to CertSecure for signing - standard ACME behavior. The issued certificate appears in Inventory under the CA/template chosen in Step 5, and renewals follow the same flow automatically.

Note: EAB credentials are informationally flagged as expired after 90 days on the profiles list, but are not currently enforced at enrollment time - rotate them periodically as a best practice regardless.

Note: For HTTP-01 or DNS-01 challenges to succeed, the domain/host being enrolled must be reachable (or its DNS records resolvable) from wherever challenge validation is performed, or enrollment will fail at the authorization step.