GlobalSign ACME Configuration Guide

May 2025

Table of Contents

Change Log

Version	Change
January 2022	First publication, featuring information about the GlobalSign ACME DV service and how it integrates with GlobalSign's PKI Platform Atlas. This version included a few FAQs
February 2022	• Added a technical addendum with information on how to do domain validation via DNS CNAME records, and how to use Certbot with NGINX. • Added more FAQs
July 2022	• Moved the FAQ to a dedicated Support website • Minor copy updates
March 2023	Added information about GlobalSign's new ACME OV service
December 2023	• Added information about new functionality that enables a user to change the email address associated with their ACME client account • Added information about new functionality that enables a user to deactivate their ACME client account
February 2024	• Added information about the hash algorithm that is used by our service for issuing certificates • Added an ACME Directory Objects section to the Technical Addendum
May 2024	• Added information on the implementation of the ACME Key Change endpoint according to RFC 8555 • Updated the subdomain verification process to incorporate a new backend logic change that bypasses subdomain verification if the parent domain already has a valid, active domain claim against it.
May 2025	• Annual review of material for accuracy and readability improvements • Removed Technical Addendum section and reorganized content into other areas.

Overview

ACME (Automated Certificate Management Environment) is a protocol defined in RFC 8555 that is designed to automate the issuance, provisioning, and renewal of digital certificates. ACME allows users to conduct certificate management actions using a set of JavaScript Object Notation (JSON) messages carried over HTTPS. Certificate issuance via ACME resembles that of a traditional certificate authority, in which a user creates an account, requests a certificate, and demonstrates control over the domain(s) covered by the requested certificate.

With GlobalSign's ACME service, customers set up an account on the GlobalSign Atlas platform and validate their organization information. Through External Account Binding (EAB), your ACME client is linked to your Atlas account. With EAB established, ACME can be used to automatically request and issue both publicly and privately trusted digital certificates from Atlas.

Getting Started

Set up GlobalSign Atlas Account

1. Create an account on the GlobalSign Atlas portal. Refer to our support article about creating an account for more information.
2. If you are using a service that issues OV or EV certificates, create an identity profile in the Atlas portal. This information will populate the subjectDN details in your certificates. Refer to our support article about creating an identity profile for more information. DV services automatically create an identity profile.
3. Generate your API credentials and obtain the MAC key (also known as HMAC) so that you can establish external account binding (EAB) with your ACME client.
    a. Refer to our support article for generating API credentials for more information.
    b. To generate the MAC key, go to the API Credentials page in Atlas and click **Request an ACME MAC** on the credential card. A pop-up window will display with your MAC key. Please note that this key is not stored by GlobalSign and this will be your only opportunity to save it for future use. Refer to the GlobalSign MAC Key section for more information.

Choose an ACME Client

Select an ACME client that will best fit your environment and ACME implementation needs. The instructions in this guide are written with the Certbot client in mind. No matter what client you use, make sure you have the latest version installed on your endpoint.

Establish External Account Binding

Register your ACME client with your GlobalSign Atlas account. You will need the following information:

- Atlas API key (aka Key ID)
- Atlas MAC Key
- GlobalSign ACME server URL: https://emea.acme.atlas.globalsign.com/directory

Certificate Management

Leveraging the automation provided by ACME, GlobalSign allows ACME clients to request and renew publicly and privately trusted digital certificates from Atlas. Coupled with the Atlas portal, users have visibility of their issued certificates in a GUI platform to centrally manage those certificates and credentials. You can also take advantage of non-ACME domain challenges in the Atlas portal for environments that cannot yet fully adopt ACME workflows.

Please note that we rotate our TLS ICAs every quarter. Your ACME client will use the provided ICA(s) when configuring your web server. Please refer to this support article for more information.

Domain Validation and Certificate Issuance

HTTP Validation

With the HTTP domain validation method (http-01), the GlobalSign ACME server issues the ACME client a token, which the client then places in a file on your webserver. The client then tells the GlobalSign ACME server to check for the file and validate the token. The following code sample demonstrates how to register Certbot with your GlobalSign Atlas account and request a certificate using the HTTP validation method.

```
certbot certonly --webroot -w <PATH TO SERVER ROOT FOLDER> -d <YOUR
DOMAIN> --agree-tos --eab-kid <YOUR-API-KEY> --eab-hmac-key <YOUR MAC KEY>
-m <YOUR EMAIL ADDRESS> --server
https://emea.acme.atlas.globalsign.com/directory --key-type rsa
```

If your ACME client is already registered with your Atlas account, you can run a similar script as demonstrated above but remove the `--agree-tos`, `--eab-kid`, `--eab-hmac-key`, and `-m` flags.

Please keep the following notes in mind:

- Certbot uses the HTTP domain validation method by default
- Certbot submits CSRs with the ECC key type by default. The above code samples specify the RSA key type; if you wish to request a certificate with an ECC key type,

remove the `--key-type rsa` flag.
- According to the CA/Browser Forum baseline requirements, you cannot use the HTTP validation method to validate a wildcard SAN, you must instead use the DNS validation method.

DNS Validation

With the DNS validation method (dns-01), the GlobalSign ACME server issues the ACME client a token, which the client then puts into a DNS TXT record under the specified domain name. The client then tells the GlobalSign ACME server to query the DNS system for the TXT record.

For Certbot, a variety of DNS plugins are available for specific DNS providers. For more information and installation and configuration steps, please refer to the Certbot documentation.

EMAIL Validation

GlobalSign supports the email domain validation method through the Atlas portal and APIs, which can be used to validate domains for endpoints that cannot rely on ACME automation workflows. Domains validated in this way can be used to issue certificates through an ACME client.

To validate a domain via email using the Atlas APIs, refer to our Atlas API documentation.

To use the Atlas portal:

1. Login to the Atlas portal and navigate to **Certificates > Domains** on the left navigation.
2. Click **+ New Domain**, choose the identity profile associated with your TLS service, enter your desired domain, and then click **Save and continue**.
3. You can proceed to verify the domain now or later. If you want to do so now, click **Verify domain**. On the modal window choose the Email validation method and follow the on-screen prompts to complete validation.

Domain Reuse Period

Domain claims validated through the GlobalSign ACME service can be reused for 398 days before they need to be revalidated.

Domain Validation for Subdomains

GlobalSign's ACME server is configured so that if you have successfully verified control of a parent domain, you may request certificates for subdomains of that parent domain without having to validate the subdomains as well. For example, if you have successfully validated example.com, then if you submit a certificate request for shop.example.com, GlobalSign will automatically bypass the domain verification step since the parent domain has already been verified. In accordance with the CA/Browser Forum baseline requirements, this logic has been implemented for the DNS and EMAIL validation methods only.

CSR Signature Algorithm

GlobalSign will only accept CSRs signed with a minimum SHA-256 signature algorithm. If you encounter an error when requesting a certificate that seems to indicate a problem with the signature algorithm, you may need to modify the ACME client config files to specify using a SHA-256 signature algorithm or generate your own CSR and instruct the client to use that instead.

Revoke a Certificate

The following code sample demonstrates how to revoke a certificate using Certbot. When revoking a certificate, you can specify the reason for the revocation by using the reason flag.

```
certbot revoke --cert-name <YOUR DOMAIN> --reason unspecified
```

Renew a Certificate

It is expected that ACME clients will automatically renew certificates prior to expiration. At a certain amount of time in advance of expiration, the ACME client will send a new certificate request to the ACME server and follow the same process to validate the domain (if necessary) and issue the certificate as was done for the original certificate order. If you manually issue a certificate, automatic renewals may not be configured by default; it is best to refer to the documentation associated with your ACME client.

Account Management

Update Your Contact Email

The following code sample demonstrates how to change the email address associated with your ACME client's account. This will ensure the GlobalSign ACME server has the most up-to-date information to contact the client for issues related to the account. This action will not affect any other aspects of the account.

```
certbot update_account --email <UPDATED EMAIL ADDRESS>
```

Deactivate Your Account

The following code sample demonstrates how to deactivate your ACME client account. You may wish to do this when the account key is compromised or has been decommissioned. A deactivated account can no longer request certificates or access resources related to the account, such as orders or authorizations. Any pending operations authorized by the account's key will be cancelled (e.g., certificate orders). Certificates issued by the account will not be revoked.

There is no way to reactivate a deactivated account, you must create a new one and do EAB again.

```
certbot unregister
```

Account Key Rollover

The GlobalSign ACME server supports requests for account key rollovers. If you want to change the public key that is associated with your ACME client account, to recover from a key compromise or proactively mitigate the impact of an unnoticed key compromise, you may do so with the GlobalSign ACME `https://emea.acme.atlas.globalsign.com/key-change` endpoint. The request sent to the server needs to contain signatures by both the old and new account keys. The new key signature covers the account URL and the old key, signifying a request by the new key holder to take over the account from the old key holder. The old key signature covers this request and its signature and indicates the old key holder's assent to the rollover request.

No other changes are made to your account when you perform this action. You will not need to perform EAB or other authentication actions afterward. This change will not impact any pending certificate orders or authorizations. This action may be preferred over deactivating your account.

Not all ACME clients support this action natively (such as Certbot). You will have to research if your ACME client supports this feature.

About GlobalSign ACME Service

GlobalSign MAC Key

The MAC key is a shared secret between the ACME client and the GlobalSign ACME server, which permits users to bind an ACME client public key to an Atlas account (more precisely, to an API credential within the customer Atlas account). This action is called External Account Binding. The MAC key is only used for this purpose; it is not required for other ACME client requests.

When you generate a MAC key through the Atlas poral, copy and paste it somewhere secure. This will be your only opportunity to do this, as we do not store the key and you will not be able to view your MAC key again in the Atlas portal.

To reduce the risk of MAC key compromise or abuse, each MAC key can be used for a maximum of 30 days or up to 1000 times. The validity and remaining uses are available on the API credential card in the Atlas portal. In the event that the MAC key is inadvertently disclosed or compromised, or it expires or has been used the maximum number of times, you can generate a new MAC key in the Atlas portal. This will overwrite the original MAC key, but any ACME clients that used the original MAC key will continue to make requests as normal. If the original MAC key is compromised, you may want to consider redoing External Account Binding with any ACME clients that have used that MAC key with a new one.

If you need to disable an affected client, you will need to get a new API and MAC key, re-bind the ACME client with the new credentials, and then revoke the original credentials in the Atlas portal.

GlobalSign ACME Directory Objects

GlobalSign supports the following directory URLs and account management functions according to the ACME RFC.

Field	Description
newNonce	Request a new nonce
newOrder	Request a new (certificate) order
newAuthz	Request a new authorization
newAccount	Request a new account
onlyReturnExisting	A client can look up an account URL based on an account key
contact	A client can modify the contact details of an existing account
externalAccountBinding	An ACME account securely binds itself to a CA account for dedicated certificate management
deactivated	Deactivate an ACME account
revokeCert	Revoke a certificate
keyChange	Change the public key that is associated with an account