

GlobalSign Atlas API Credentials Generation and CertSecure Manager Requirements

Purpose

This document explains how to generate the API Credentials and mTLS certificate in GlobalSign Atlas and outlines the full set of requirements to integrate it with the CertSecure Manager Connector.

Section 1: Prerequisites for API Credentials Generation

1. Active GlobalSign Atlas Account

You must have a valid and accessible GlobalSign Atlas account with a valid certificate service and a valid identity, required to create API Credentials.

2. User Role with API Permissions

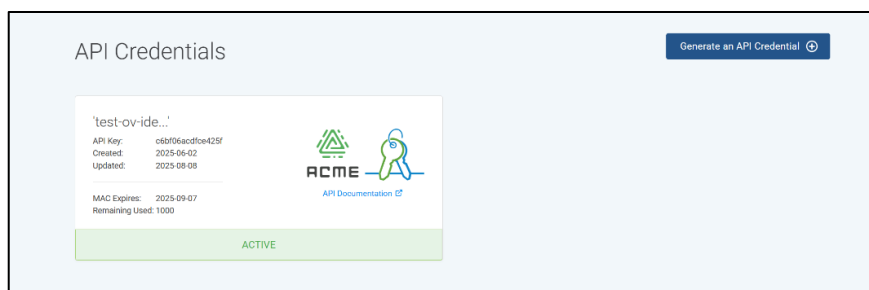
Recommended roles: Administrator or Manage Certificates and Manage Credentials.
Other roles may have limited API access.

Section 2: Steps for API Credentials Generation and mTLS Certificate Issuance via GlobalSign Atlas

1. Steps to Generate API Credentials

The following are the steps to create API Credentials for GlobalSign

1. Log in to [GMO GlobalSign Atlas](#)
2. In the left side panel, navigate to “Access Credentials > API Credentials”.
3. Click on the “Generate an API Credential” button.



4. Select “View and Copy” and click “Continue”.

Which method do you want to use?

View and Copy



View in browser, copy to clipboard.
Downloadable as a .csv file.

BACK

Encrypted File



Paste an RSA public key.
Download key and secret as .enc

CONTINUE

5. Select an active service and click continue.

Select Encryption Option **Link a Service** Link an Identity Familiar Name

Link to a Service

This API credential must be linked to an active service.

Test Certificates

50 Certificates
ID#: SRV-0002261
Key Type: RSA
Start Date: May 07, 2025



ACTIVE

BACK

API CREDENTIAL SUMMARY

ENCRYPTION SELECTED
No

SERVICE
ID#: SRV-0002261
Test Certificates - 50

FAMILIAR NAME

CONTINUE

6. Select a single valid identity and click continue.

Select Encryption Option Link a Service **Link an Identity** Familiar Name

Link to an Identity

This API credential must be linked to a single valid identity.

Only identity profiles applicable to your chosen service are shown here.

IDEN-04135

Profile: IDEN-04135_2025-05-07



Created May 07, 2025

Active

Request a new identity profile

NEW IDENTITY

BACK

API CREDENTIAL SUMMARY

ENCRYPTION SELECTED
No

SERVICE
ID#: SRV-0002261
Test Certificates - 50

FAMILIAR NAME

CONTINUE

7. Give the credentials a distinguishable name and click continue.

8. Download and save the API Credentials.

2. Steps to Generate a CSR for mTLS certificate

The following are the steps to create an mTLS certificate for the GlobalSign API Credentials.

1. Log in to CertSecure Manager
2. Navigate to “Enrollment > Generate CSR”
3. Fill in the certificate details for the mTLS certificate. Enter a password to encrypt the private key.

CertSecure Manager

Dashboard > [Generate CSR](#)

CertSecure Manager CS MTLS

Subject Alternative Names

DNS Names:

IP Addresses:

Enter DNS names as comma-separated values.

Enter IP Address as comma-separated values.

Email Address:

Organizational Information

Organization: Organization Unit:

City: State: Country Code:

Please provide country codes in ISO format, for example: US, CA.

Email ID:

Credential Information

Private Key Password: [Generate Password](#)

[Generate CSR](#)

- Click on the “Generate CSR” button and download the CSR and private key files.

CertSecure Manager CS MTLS.zip - ZIP archive, unpacked size 3,041 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
private_key.key	1,874	1,874	KEY File	8/8/2025 12:04 PM	2CDDFC7E
csr.pem	1,167	1,167	PEM File	8/8/2025 12:04 PM	665A8001

Note: We will be using this CSR to issue the GlobalSign mTLS certificate, and the private key file and the password will be required during the agent installation process.

- Next, Log in to [GMO GlobalSign Atlas](#)
- In the left side panel, navigate to “Access Credentials > mTLS Certificate”.
- Click on the “Generate a mTLS Certificate” button. Click on Continue under the “Directly via the API” option.

How do you plan to connect to the service?
How you connect affects your need for an mTLS certificate.

Via Our Technology Partners

Connecting to your service via technology partner integrations doesn't require an mTLS certificate. To learn more about partner integrations, [contact your local sales team](#).

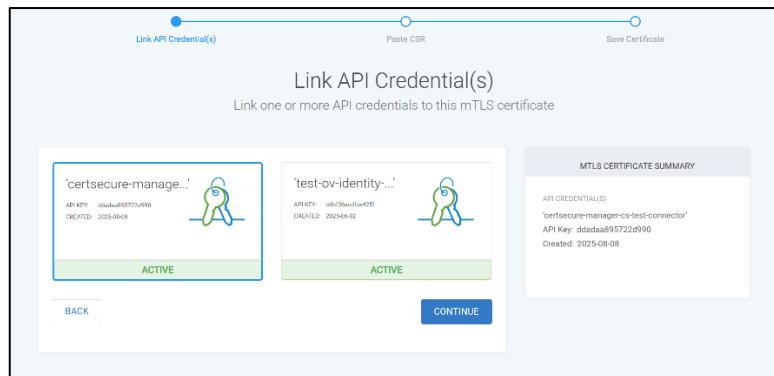
[OK, RETURN TO DASHBOARD](#)

Directly via the API

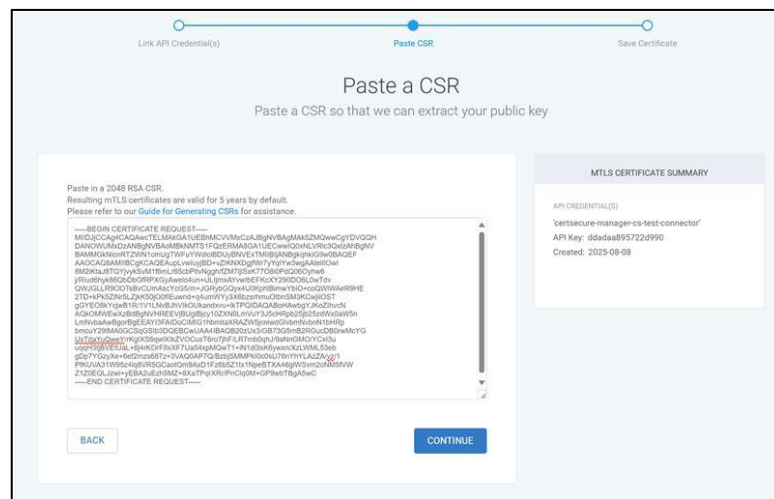
Connecting via the API requires an mTLS certificate for secure access.

[CONTINUE](#)

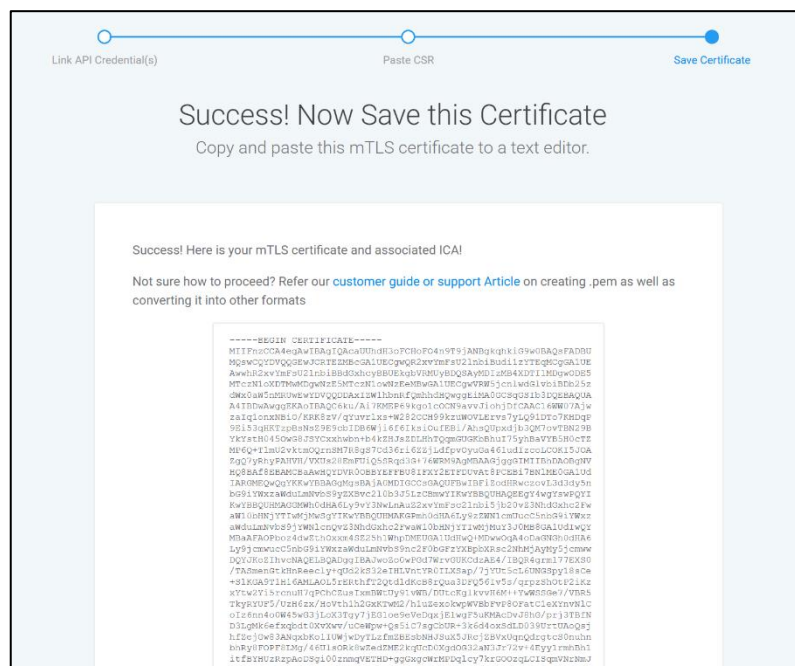
8. Select the API Credential that we created in the previous step and click continue.



9. Paste the CSR that we have generated from CertSecure Manager earlier and click on “continue”.



10. Download and save the mTLS Certificate.



Section 2: Additional Requirements for CertSecure Manager Connector Integration

1. CertSecure Manager Connector Configuration

Once the API credentials and mTLS certificate are generated:

- The CLM Connector must be configured with the API credentials.
- Ensure the connector machine has access to the GlobalSign API endpoint (using the mTLS certificate)

<https://emea.api.hvca.globalsign.com:8443/v2>