

GlobalSign Integration Guide

GlobalSign Managed SSL (MSSL) and
Azure KeyVault



Introduction

This technical integration guide describes how to integrate the Microsoft Azure KeyVault platform with GlobalSign's Managed SSL (MSSL) service to provision SSL certificate to be accessed and utilized through the Microsoft Azure cloud platform.

GlobalSign Managed SSL (MSSL)

A Complete Enterprise SSL Solution. Managed SSL is a SaaS solution to reduce the effort, cost and time associated with managing enterprise SSL Certificates. The Managed SSL platform was designed around enterprise-specific security requirements and gives access to all types of SSL Certificates. It supports the enterprise's needs to host public websites as well as for non-public and internal servers. GlobalSign offers unique features and functionality that make it easy to manage your certificates no matter how large or distributed your organization.

A robust platform that allows Instant issuance of all types of SSL Certificates on-demand, including Organization Validated (OV), Extended Validation (EV), Wildcard, and Multi-domain, with options to add Subject Alternative Names (SANs).

For more information on MSSL, see <https://www.globalsign.com/en/ssl/managed-ssl/>

Microsoft Azure Key Vault

Secure key management is essential to protect data in the cloud. Use Azure Key Vault to encrypt keys and small secrets like passwords that use keys stored in hardware security modules (HSMs). For more assurance, import or generate keys in HSMs, and Microsoft processes your keys in FIPS 140-2 Level 2 validated HSMs (hardware and firmware). With Key Vault, Microsoft doesn't see or extract your keys.

Provision new vaults and keys in minutes and centrally manage keys, secrets, and policies. You keep control over your keys—simply grant permission for your own and partner applications to use them as needed. Applications never have direct access to keys. Developers manage keys used for Dev/Test and seamlessly migrate to production the keys that are managed by security operations. Simplify and automate tasks related to SSL/TLS certificates—Key Vault enables you to enroll and automatically renew certificates from supported public Certificate Authorities.

For more information on Azure KeyVault, see <https://azure.microsoft.com/en-us/services/key-vault/>

GlobalSign Contact Information

GlobalSign Americas Tel: 1-877-775-4562 www.globalsign.com sales-us@globalsign.com	GlobalSign EU Tel: +32 16 891900 www.globalsign.eu sales@globalsign.com	GlobalSign UK Tel: +44 1622 766766 www.globalsign.co.uk sales@globalsign.com
GlobalSign FR Tel: +33 1 82 88 01 24 www.globalsign.fr ventes@globalsign.com	GlobalSign DE Tel: +49 30 8878 9310 www.globalsign.de verkauf@globalsign.com	GlobalSign NL Tel: +31 20 8908021 www.globalsign.nl verkoop@globalsign.com

Once logged into the Azure portal, if you do not have a Key Vault setup yet or would like to create a new one click on the “New” tab on the left hand side menu and choose “Key Vault” icon. (Note: If it does not auto populate you can use the search bar and it will pop up).

The screenshot shows the Microsoft Azure portal interface for Key Vault. The left-hand navigation menu includes options like Dashboard, All resources, Resource groups, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The 'New' button is highlighted with a red arrow. The main content area features a header for 'Key Vault' and three main sections: 'Enhance data protection and compliance', 'All of the control, none of the work', and 'Boost performance and achieve global scale'. Below these sections are social media icons and a preview of the Key Vault 'Keys' page. At the bottom, a blue 'Create' button is highlighted with a red arrow.

Create key vault ✕

* Name
Vault-Name ✓

* Subscription
Pay-As-You-Go Dev/Test ▾

* Resource Group
 Create new Use existing
My-Vault ✓

* Location
North Central US ▾

Pricing tier
Standard >

Access policies
1 principal selected >

Pin to dashboard

Create Automation options

Now you will want to Name your key vault. Once named choose your subscription preferences, resource group (new or existing), location, pricing tier and the vaults access policies. Once complete, click the “Create” button.

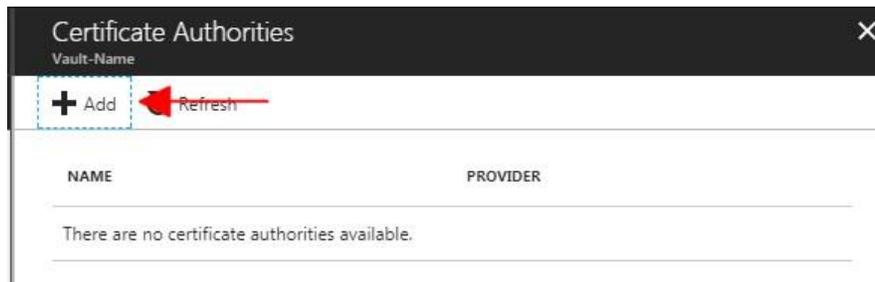
Your vault will now be created and you will be taken to an overview of its configuration.

The screenshot shows the 'Overview' page of an Azure Key Vault. The left-hand navigation pane includes sections for 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', and 'Diagnose and solve problems'. Below these are 'SETTINGS' such as 'Keys', 'Secrets', 'Certificates', 'Access policies', 'Properties', 'Locks', and 'Automation script'. The main content area displays resource information: Resource group (My-Vault), Location (North Central US), Subscription (Pay-As-You-Go Dev/Test), and Subscription ID (4398c475-a895-4f64-bd4e-6d720324a575). It also shows the DNS Name (https://vault-name.vault.azure.net/) and Sku (Standard). A 'Monitoring' section allows selecting a time range (1 hour, 6 hours, 12 hours, 1 day, 7 days, 30 days) and shows a graph for 'Total requests (Vault-Name)' with a y-axis from 30 to 100.

Next you will want to create a GlobalSign Certificate Authority for the vault to access. From the left side menu choose "Certificates". A menu will open and on the upper right hand side choose "Certificate Authorities".

The screenshot shows the 'Certificates' page within the Azure Key Vault. The left-hand navigation pane has 'Certificates' highlighted with a red arrow. The main content area features a toolbar with '+ Add', 'Refresh', 'Certificate Cont...', and 'Certificate Authorities' (the last one has a red arrow pointing to it). Below the toolbar is a table with columns 'NAME' and 'THUMBPRINT'. The table is currently empty, displaying the message 'There are no certificates available.'

Under the Certificate Authorities menu select “Add”.



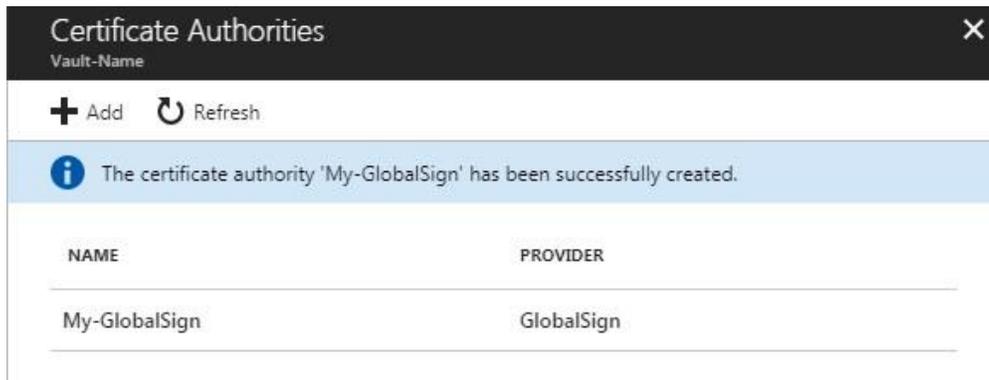
Once you name your certificate authority accordingly, you will want to click on the “Provider” tab and from the drop down menu select “GlobalSign”. The menu will then populate fields for you to enter your GlobalSign account information.

The screenshot shows a form titled "Create a certificate authority" with a close button (X) in the top right corner. The form contains several input fields, each with a green checkmark indicating it is valid:

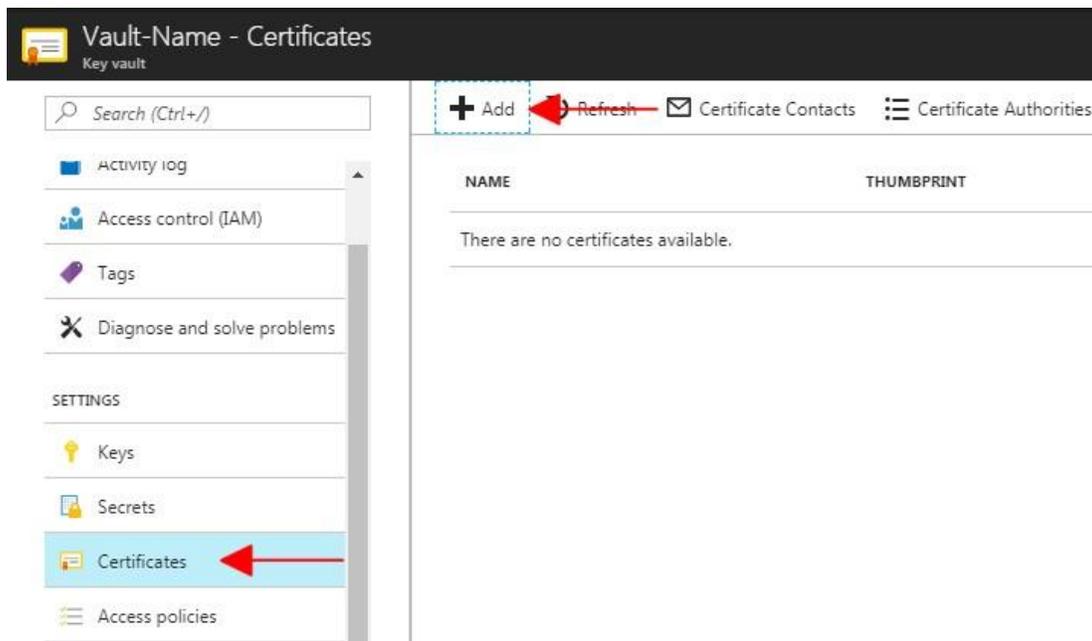
- Name: My-GlobalSign
- Provider: GlobalSign (highlighted in yellow)
- Account ID: PAR123456_UserID
- Account Password: [Redacted]
- First Name of Administrator: Global
- Last Name of Administrator: Sign
- E-mail of Administrator: admin@globalsign.com
- Phone Number of Administrator: 603-123-4567

At the bottom of the form, there is a checkbox labeled "Pin to dashboard" which is unchecked. Below the checkbox is a blue "Create" button with a red arrow pointing left towards it.

You should then get notification that the certificate authority has been successfully created.



Next step is to add a new certificate to the vault. To do this, click on the "Certificates" tab on the left hand side menu and then click "Add".



Here you will want to choose “Generate” as the method of certificate generation and then specify a certificate name. (Note: This is a friendly name that it will be referred to with in the vault, it is not the common name of the actual certificate.)

You will then want to select “Certificate issued by an integrated CA” from the “Type of Certificate Authority (CA)” drop down menu.

Then click the “Certificate Authority (CA) *Not Configured*” tab.

Create a certificate [X]

Method of Certificate Creation
Generate [v]

* Certificate Name
GlobalSign-Certificate [v]

Type of Certificate Authority (CA)
Certificate issued by an integrated CA [v]

* Certificate Authority (CA)
Not configured [v] ←

Next you will want to select the GlobalSign Certificate Authority that you created. This will take you back to the Create a certificate form.

Certificate Authorities [X]
Vault-Name

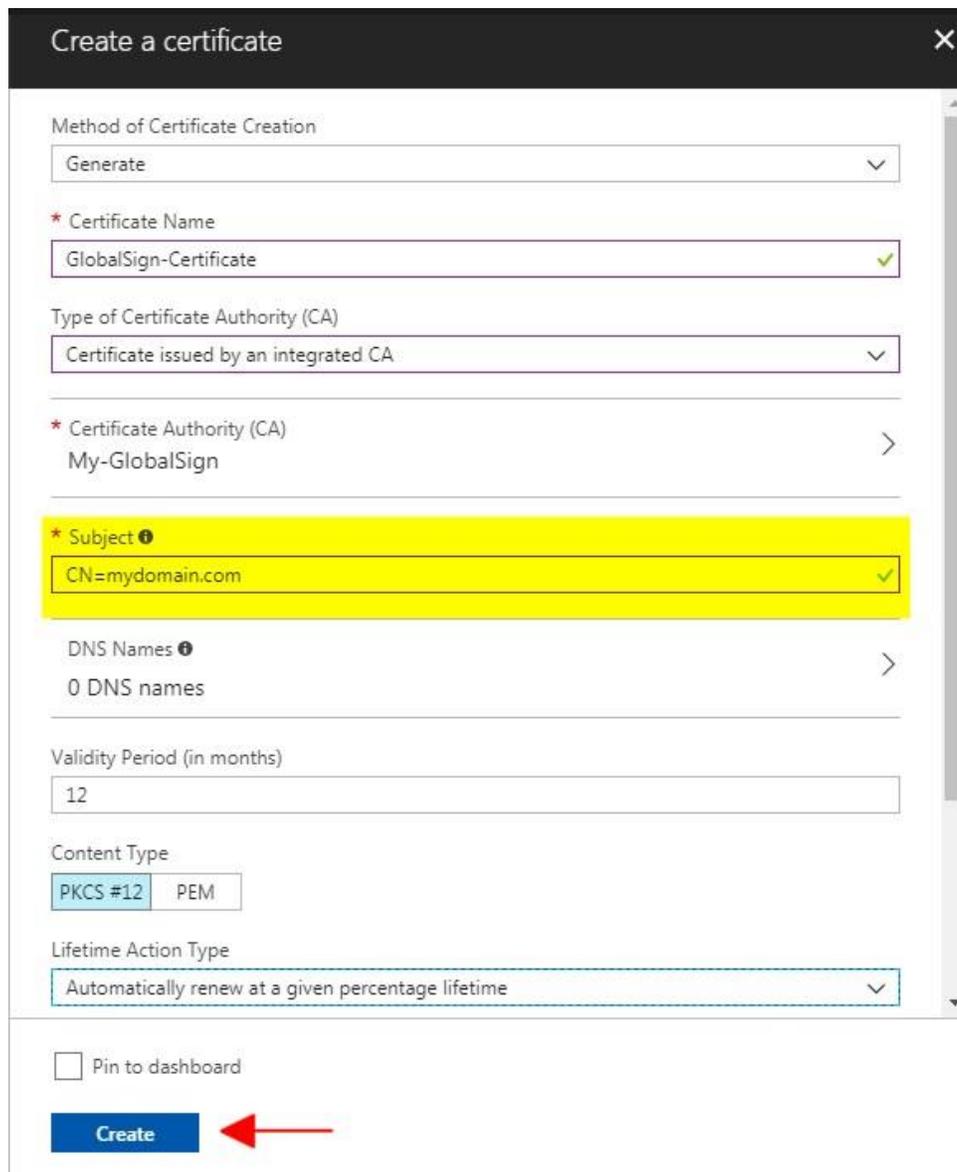
+ Add [Refresh]

NAME	PROVIDER
My-GlobalSign	GlobalSign

The final requirement is the “Subject” field. This is where you will enter the common name for the certificate you are requesting (Format: CN=commonname.com).

There are additional fields which are optional:

- DNS Names – Where add additional Subject Alternative Names (SANs)
- Validity Period – To select how long the certificate is valid for in month designation
- Content Type
 - PKCS#12 – private public key pair
 - PEM – public key
- Lifetime Action Type – Set certificate renewals or renewal reminders
- Advanced Policy Configuration – Add additional EKUs and set advanced key features



Create a certificate [X]

Method of Certificate Creation
Generate [v]

* Certificate Name
GlobalSign-Certificate [v]

Type of Certificate Authority (CA)
Certificate issued by an integrated CA [v]

* Certificate Authority (CA)
My-GlobalSign [>]

* Subject ⓘ
CN=mydomain.com [v]

DNS Names ⓘ
0 DNS names [>]

Validity Period (in months)
12

Content Type
PKCS #12 | PEM

Lifetime Action Type
Automatically renew at a given percentage lifetime [v]

Pin to dashboard

Create ←

A pop up in the right corner will confirm the certificate is being created. You can also click on the blue information bar to monitor the generation process.

The screenshot shows a notification bar at the top with a blue information icon and the text: "The creation of certificate 'GlobalSign' is currently pending. Click here to monitor its progress. →". Below this is a table with columns for NAME, THUMBPRINT, and STATUS. The table is currently empty, displaying "There are no certificates available." A pop-up notification in the top right corner shows a green checkmark and the text: "Creating the certificate 'GlobalSign'. 10:12 AM" and "The certificate 'GlobalSign' has been successfully created."

Status completed confirms that the certificate has been issued and stored in the vault.

The screenshot shows a window titled "GlobalSign Certificate Operation". It has a menu bar with "Refresh", "Download CSR", "Merge Signed Request", "Request Cancellation", and "Delete". The main content area shows a green checkmark and the word "Completed". Below this, the "Request ID" is displayed as "5b9720486fb447f59d94196510a35b7e" and the "CA Name" is "My-GlobalSign".

Under the menu bar, go to "Certificates" to see your list of issued Certificates. You are now able to utilize the certificate through the Azure platform.

The screenshot shows the "Vault-Name - Certificates" page. On the left is a navigation sidebar with "Certificates" selected. The main area has a menu bar with "Add", "Refresh", "Certificate Contacts", and "Certificate Authorities". Below is a table with columns for NAME, THUMBPRINT, STATUS, and EXPIRATION DATE. The table contains two entries:

NAME	THUMBPRINT	STATUS	EXPIRATION DATE
GlobalSign	373EED7DC4694571F2726BAEC041...	✓ Enabled	1/26/2019
GlobalSign-SSL	C90E36E6E5DF464B3E900596DE943E...	✓ Enabled	1/26/2019