GlobalSign & Microsoft Azure Key Vault Integration Guide

Secure Key Management for cloud apps

GLOBALSIGN INTEGRATION GUIDE

INTRODUCTION

This document will walk you through the process of issuing a SSL certificate from your GlobalSign Managed SSL account into an Azure Key Vault. If you do not currently have a GlobalSign account, please contact us here.

Requirements

You will need to have Azure PowerShell Version 2.2.0 or greater which is available for download here.

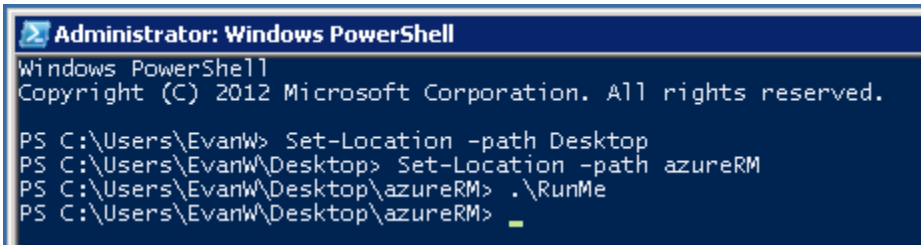
https://github.com/Azure/azure-powershell/releases

Steps

Run GlobalSign Key Vault folder via PowerShell

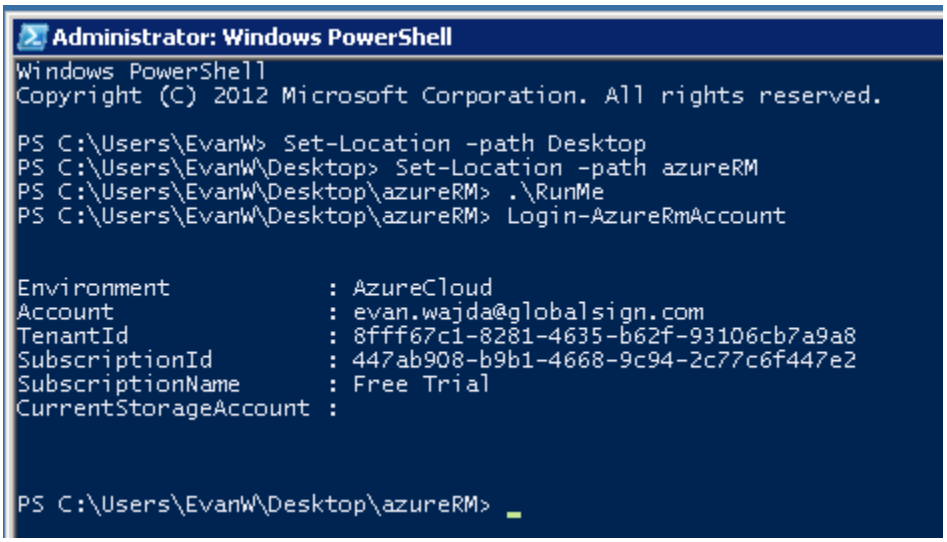
Unzip attached folder (GlobalSign.KeyVault) and run the RunMe.ps1 from the attached folder

(1-RunMe_PowerShell_1)



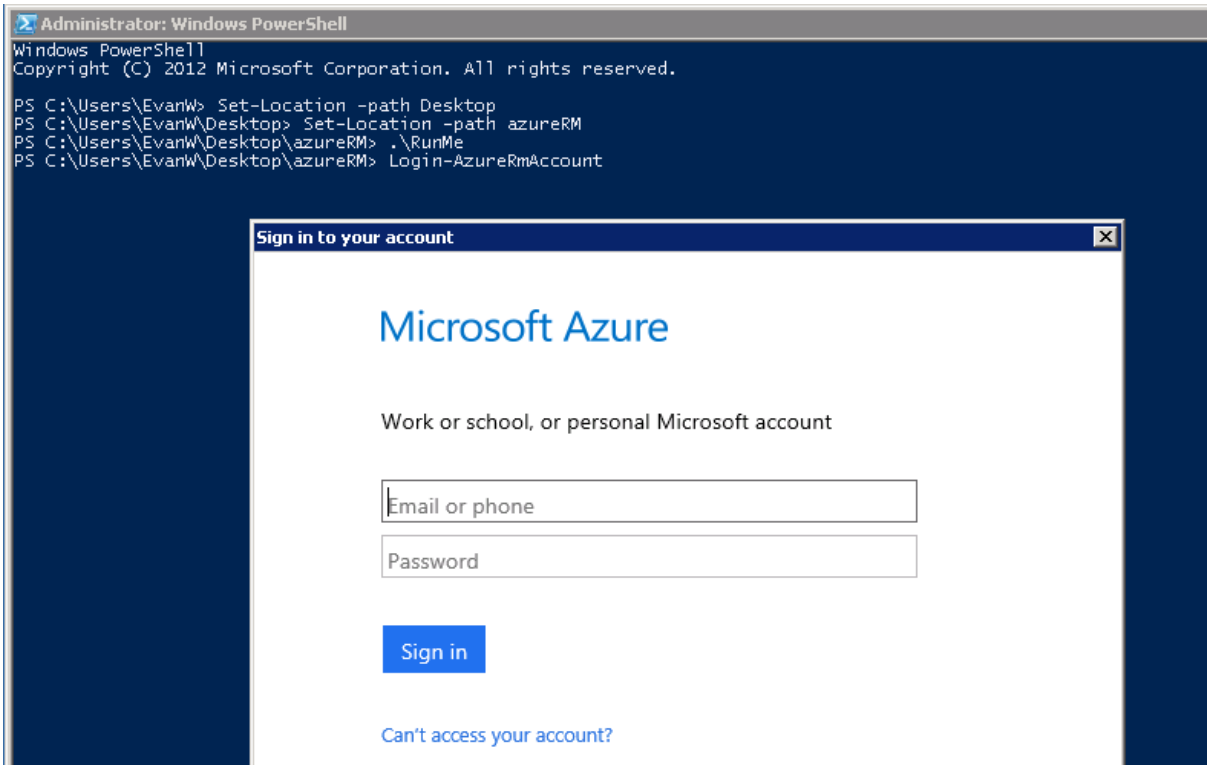
Login-AzureRmAccount

(2-RunMe & Azure_Log_In_PowerShell)



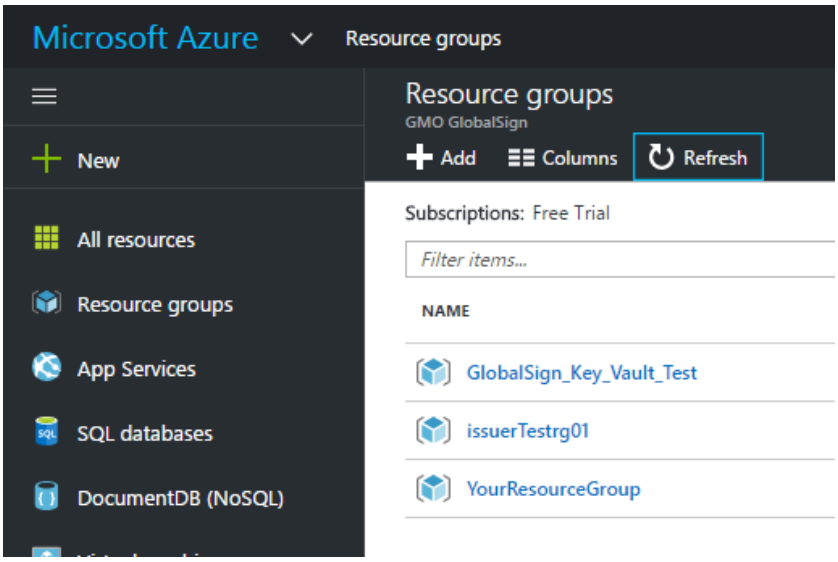
You will then be prompted for you Microsoft Azure Account credentials. I you don't have an Azure account you will need to create one here https://azure.microsoft.com/en-us/

(3-Azure_Log_In_PoweShell_2)



You will now need to set reference group. If you have a resource group already created you would like to use, you want to reference that now or create a new reference group. You can access and add additional reference groups in the Azure portal.

(4-Azure_UI_Resource_Groups)



Or in PowerShell.

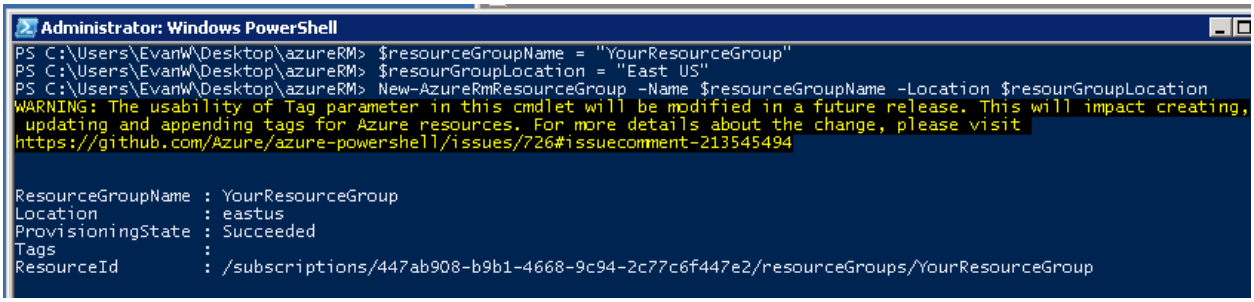
$resourceGroupName = "YourResourceGroup"

$resourceGroupLocation = "Your Location"

New-AzureRmResourceGroup -Name $resourceGroupName -Location $resourceGroupLocation

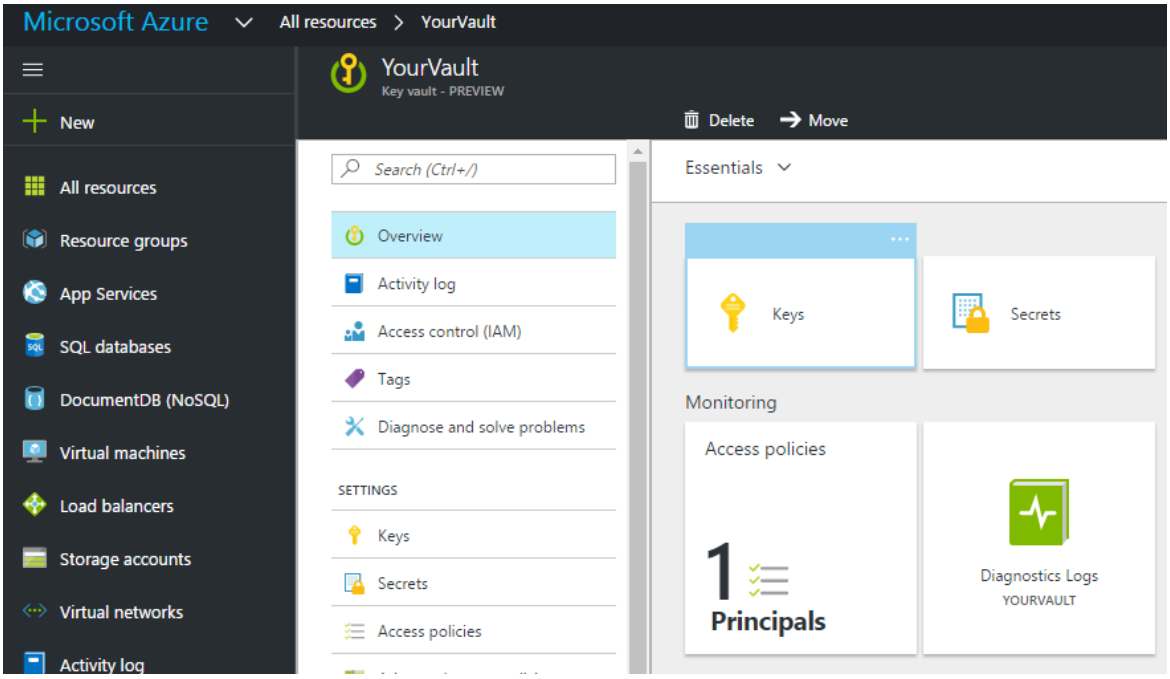
Note: A list of locations are available in your Azure Portal.

(5-Create_Resorce_Group_PowerShell)



If you have a vault already created you would like to use, you want to reference that now or create a new vault. You can access and add additional vaults in the Azure portal.

(6-Create_Vault_Azure_UI)



Or in PowerShell.

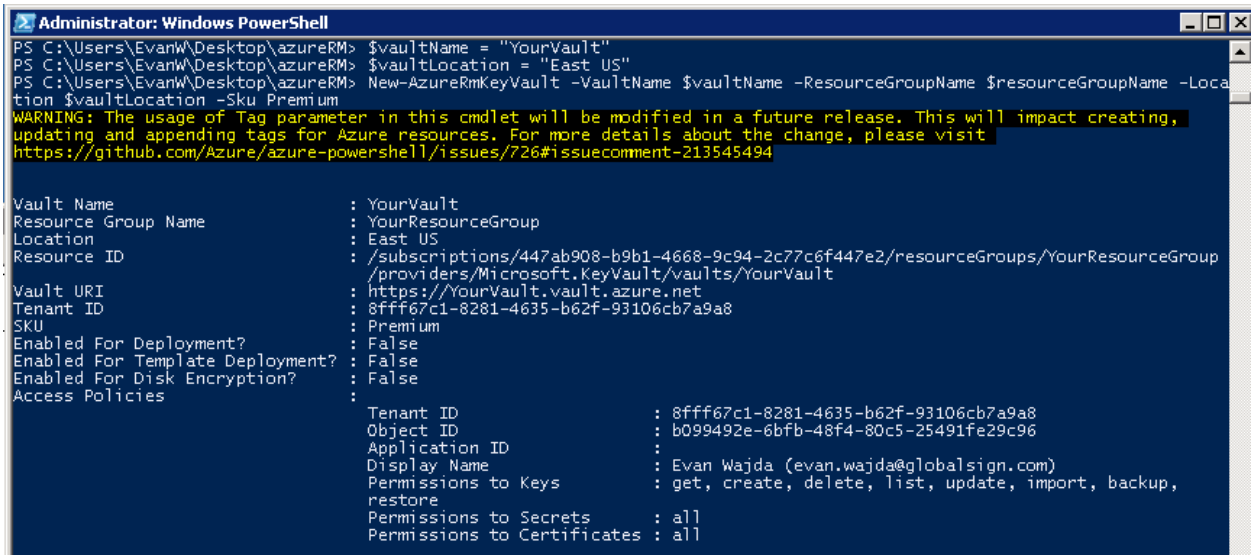
$vaultName = "YourVaultNameHere"

$vaultLocation = "Your Location"

New-AzureRmKeyVault -VaultName $vaultName -ResourceGroupName $resourceGroupName -Location $vaultLocation -Sku Premium

Note: A list of locations are available in your Azure Portal.

(7-Create_Vault_PS)



You will now want to create an Administrator for the issuer. This will assign a point of contact for the issued certificate.

$firstName = "KeyVault"

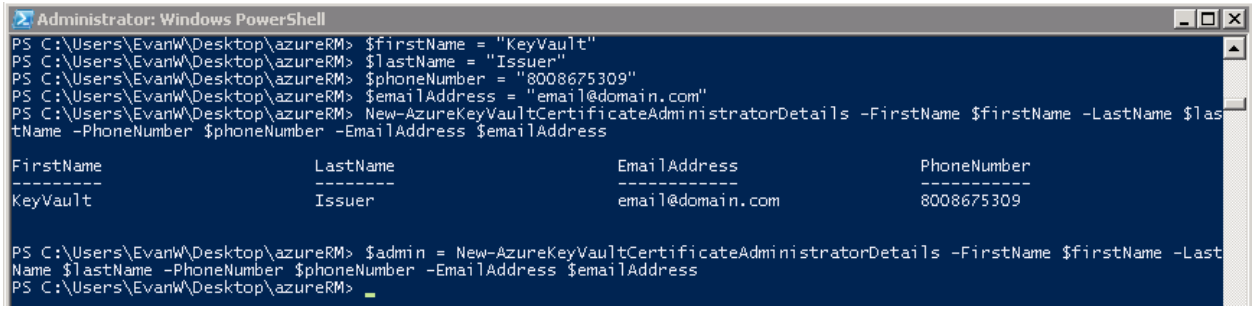
$lastName = "Issuer"

$phoneNumber = "8008675309"

$emailAddress = "youremail@domain.com"

$admin = New-AzureKeyVaultCertificateAdministratorDetails -FirstName $firstName -LastName $lastName -PhoneNumber $phoneNumber -EmailAddress $emailAddress

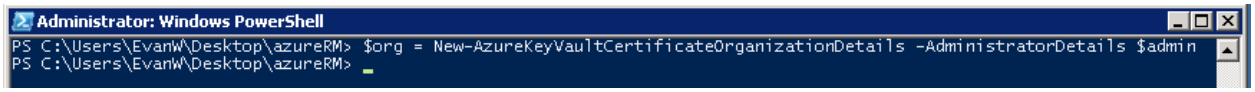
(8-Admin_User)



You will now want to create an Organization for the issuer.

$org = New-AzureKeyVaultCertificateOrganizationDetails -AdministratorDetails $admin

(9-Create_Organization)



Next, you will want to create an issuer. The “apiKey” is your GlobalSign password and the “accountId” is your GlobalSign User ID assigned when creating your GlobalSign account.

$apiKey = "YourGlobalSignUserPassword"

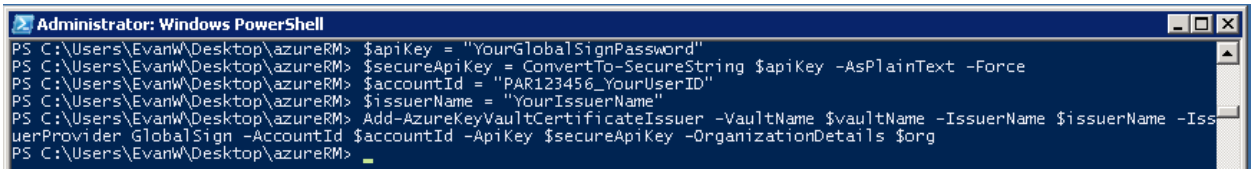
$secureApiKey = ConvertTo-SecureString $apiKey -AsPlainText -Force

$accountId = "PAR123456_YourUserID"

$issuerName = "YourIssuerName"

Add-AzureKeyVaultCertificateIssuer -VaultName $vaultName -IssuerName $issuerName -IssuerProvider GlobalSign -AccountId $accountId -ApiKey $secureApiKey -OrganizationDetails $org

(10-Create_Issuer)

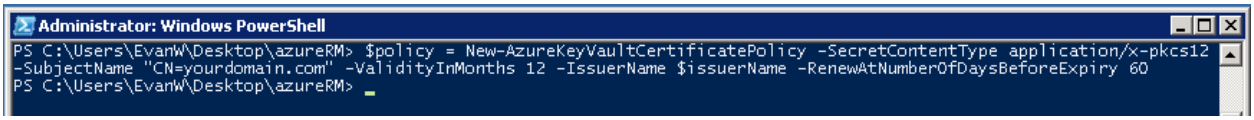


Then you will want to create a certificate policy. This is where you set the common name (from you pre-vetted GlobalSign domains) to be issued. You will also specify the validity period (in months) and how many day before expiry you would like the certificate to be renewed.

$policy = New-AzureKeyVaultCertificatePolicy -SecretContentType application/x-pkcs12 -SubjectName "CN=healthytest.xyz" -ValidityInMonths 12 -IssuerName $issuerName -RenewAtNumberOfDaysBeforeExpiry 60

CN=’s Common Name (FQDN) of certificate

(11-Create_Policy)



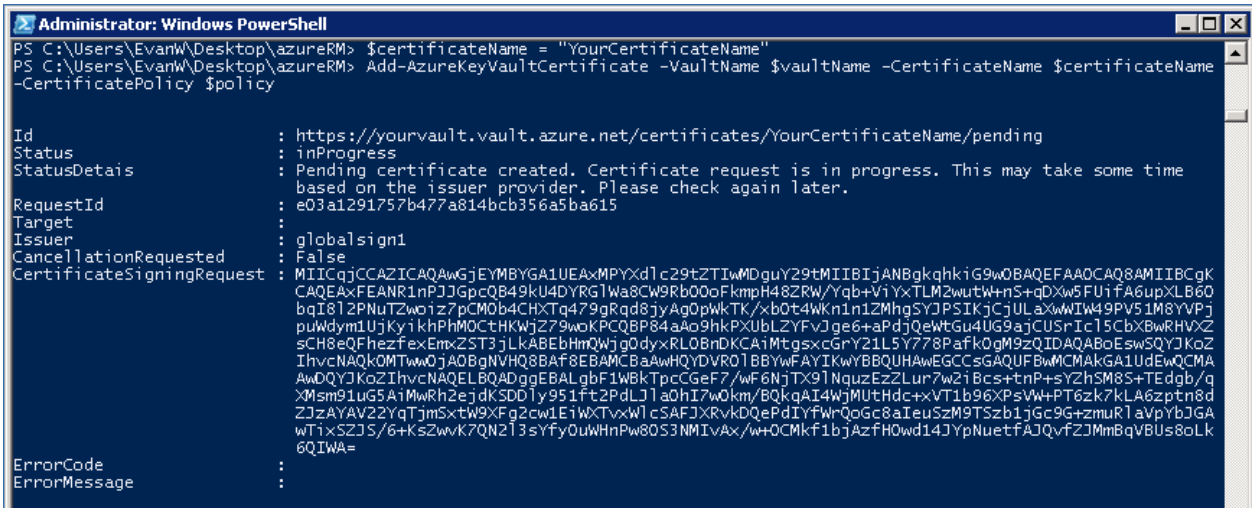
Next you will request for certificate enrollment. If successful, you will get a “Status” of inProgress as well as a confirmation under “StatusDetails” that the Pending certificate is being created and the request is in process as well as the CSR.

$certificateName = "globalsignTrial01"

Add-AzureKeyVaultCertificate -VaultName $vaultName -CertificateName $certificateName -CertificatePolicy $policy

Note: If you receive an Error, please send the Error Message along with your account information to support@globalsign.com. Please reference “Azure Key Vault Error” in the subject.

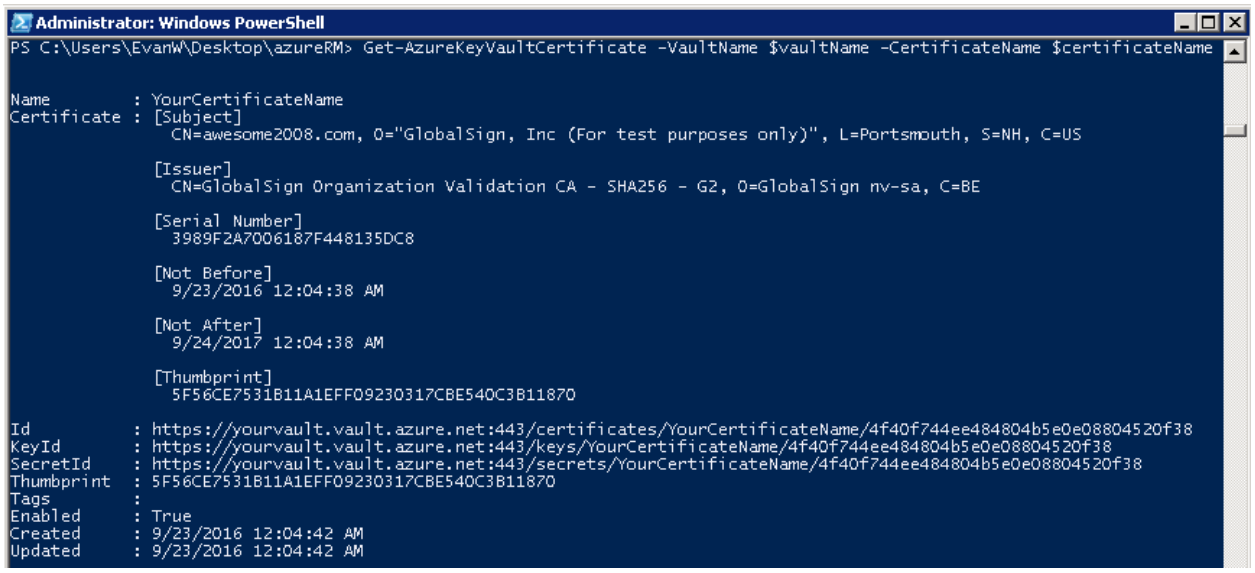
(12-Request-Certificate)



Now you will want to confirm the certificate has been issued

Get-AzureKeyVaultCertificate -VaultName $vaultName -CertificateName $certificateName

(13-Certificate_Creation_Confirmation)



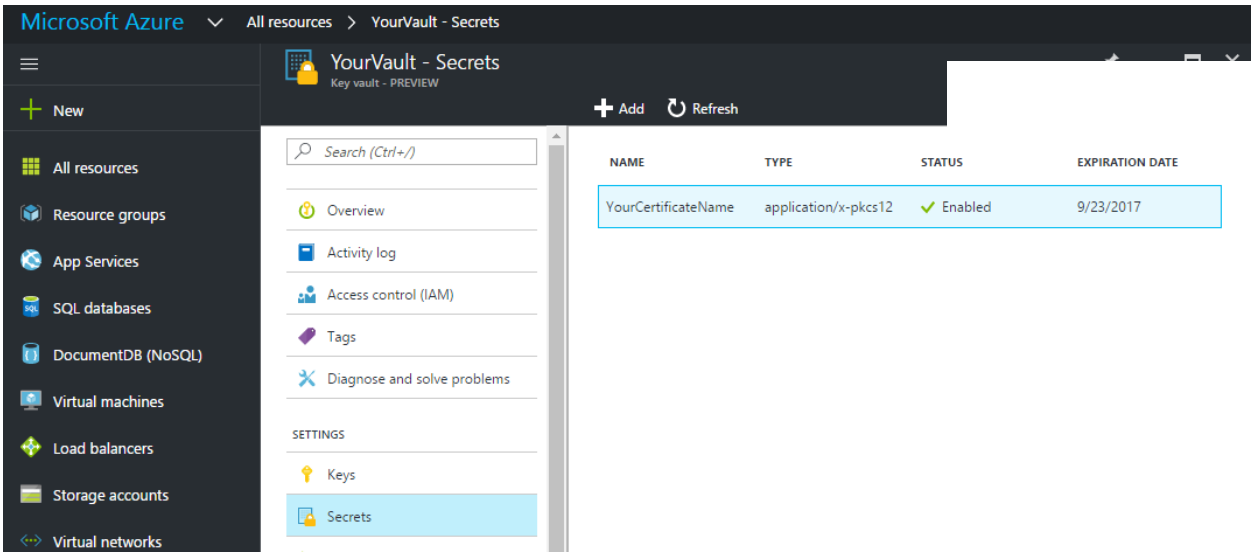
Note: If the certificate is still pending issuance you can check the status enrollment by using the script below.

Get-AzureKeyVaultCertificateOperation -VaultName $vaultName -CertificateName $certificateName

(14-Certificate_Status)

Certificate issued in Azure Portal

(15-Certificate_Azure_UI)



ABOUT GLOBALSIGN

GlobalSign is a leading provider of trusted identity and security solutions enabling businesses, large enterprises, cloud service providers and IoT innovators around the world to secure online communications, manage millions of verified digital identities and automate authentication and encryption. Its high-scale PKI and Identity and Access Management (IAM) solutions support the billions of services, devices, people and things comprising the Internet of Everything (IoE).

US: +1 877 775 4562
UK: +144 1622 766766
EU: +32 16 89 19 00
sales@globalsign.com

For additional information, please visit www.globalsign.com