Windows PowerShell Get-Help on Cmdlet 'New-AzKeyVaultCertificatePolicy'

PS:\>Get-HELP New-AzKeyVaultCertificatePolicy -Full

NAME

New-AzKeyVaultCertificatePolicy

SYNOPSIS

Creates an in-memory certificate policy object.

SYNTAX

New-AzKeyVaultCertificatePolicy [-IssuerName] <System.String> [-DnsName] <System.Collections.Generic.List`1[System.String]> [[-SubjectName] <System.String>] [-CertificateTransparency <System.Nullable`1[System.Boolean]>] [-CertificateType <System.String>] [-Curve {P-256 | P-384 | P-521 | P-256K | SECP256K1}] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Disabled] [-Ekus <System.Collections.Generic.List`1[System.String]>] [-EmailAtNumberOfDaysBeforeExpiry <System.Nullable`1[System.Int32]>] [-EmailAtPercentageLifetime <System.Nullable`1[System.Int32]>] [-KeyNotExportable] [-KeySize {2048 | 3072 | 4096 | 256 | 384 | 521}] [-KeyType {RSA | RSA-HSM | EC | EC-HSM}] [-KeyUsage {None | EncipherOnly | CrlSign | KeyCertSign | KeyAgreement | DataEncipherment | KeyEncipherment | NonRepudiation | DigitalSignature | DecipherOnly}]

[-RenewAtNumberOfDaysBeforeExpiry <System.Nullable`1[System.Int32]>] [-RenewAtPercentageLifetime <System.Nullable`1[System.Int32]>] [-ReuseKeyOnRenewal]

[-SecretContentType {application/x-pkcs12 | application/x-pem-file}] [-ValidityInMonths <System.Nullable`1[System.Int32]>] [-Confirm] [-WhatIf] [<CommonParameters>]

New-AzKeyVaultCertificatePolicy [-IssuerName] <System.String> [-SubjectName] <System.String> [-CertificateTransparency <System.Nullable`1[System.Boolean]>]

[-CertificateType <System.String>] [-Curve {P-256 | P-384 | P-521 | P-256K | SECP256K1}] [-DefaultProfile

<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Disabled] [-Ekus <System.Collections.Generic.List`1[System.String]>]

[-EmailAtNumberOfDaysBeforeExpiry <System.Nullable`1[System.Int32]>] [-EmailAtPercentageLifetime <System.Nullable`1[System.Int32]>] [-KeyNotExportable] [-KeySize

{2048 | 3072 | 4096 | 256 | 384 | 521}] [-KeyType {RSA | RSA-HSM | EC | EC-HSM}] [-KeyUsage {None | EncipherOnly | CrlSign | KeyCertSign | KeyAgreement |

DataEncipherment | KeyEncipherment | NonRepudiation | DigitalSignature | DecipherOnly}] [-RenewAtNumberOfDaysBeforeExpiry <System.Nullable`1[System.Int32]>]

[-RenewAtPercentageLifetime <System.Nullable`1[System.Int32]>] [-ReuseKeyOnRenewal] [-SecretContentType {application/x-pkcs12 | application/x-pem-file}]

[-ValidityInMonths <System.Nullable`1[System.Int32]>] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The New-AzKeyVaultCertificatePolicy cmdlet creates an in-memory certificate policy object for Azure Key Vault.

PARAMETERS

-CertificateTransparency <System.Nullable`1[System.Boolean]>

Indicates whether certificate transparency is enabled for this certificate/issuer; if not specified, the default is 'true'

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-CertificateType <System.String>

Specifies the type of certificate to the issuer.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Curve <System.String>

Specifies the elliptic curve name of the key of the certificate. The acceptable values for this parameter are: - P-256

- P-384

- P-521

- P-256K

- SECP256K1

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>

The credentials, account, tenant, and subscription used for communication with azure

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Disabled <System.Management.Automation.SwitchParameter>

Indicates that the certificate policy is disabled.

Required? false

Position? named

Default value False

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-DnsName <System.Collections.Generic.List`1[System.String]>

Specifies the DNS names in the certificate. Subject Alternative Names (SANs) can be specified as DNS names.

Required? true

Position? 1

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Ekus <System.Collections.Generic.List`1[System.String]>

Specifies the enhanced key usages (EKUs) in the certificate.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-EmailAtNumberOfDaysBeforeExpiry <System.Nullable`1[System.Int32]>

Specifies how many days before expiry the automatic notification process begins.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-EmailAtPercentageLifetime <System.Nullable`1[System.Int32]>

Specifies the percentage of the lifetime after which the automatic process for the notification begins.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-IssuerName <System.String>

Specifies the name of the issuer for the certificate.

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-KeyNotExportable <System.Management.Automation.SwitchParameter>

Indicates that the key is not exportable.

Required? false

Position? named

Default value False

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-KeySize <System.Int32>

Specifies the key size of the certificate. The acceptable values for this parameter are: - 2048

- 3072

- 4096

- 256

- 384

- 521

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-KeyType <System.String>

Specifies the key type of the key that backs the certificate. The acceptable values for this parameter are: - RSA

- RSA-HSM

- EC

- EC-HSM

Required? false

Position? named

Default value RSA

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-KeyUsage <System.Collections.Generic.List`1[System.Security.Cryptography.X509Certificates.X509KeyUsageFlags]>

Specifies the key usages in the certificate.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-RenewAtNumberOfDaysBeforeExpiry <System.Nullable`1[System.Int32]>

Specifies the number of days before expiry after which the automatic process for certificate renewal begins.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-RenewAtPercentageLifetime <System.Nullable`1[System.Int32]>

Specifies the percentage of the lifetime after which the automatic process for certificate renewal begins.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ReuseKeyOnRenewal <System.Management.Automation.SwitchParameter>

Indicates that the certificate reuse the key during renewal.

Required? false

Position? named

Default value False

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-SecretContentType <System.String>

Specifies the content type of the new key vault secret. The acceptable values for this parameter are: - application/x-pkcs12

- application/x-pem-file

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-SubjectName <System.String>

Specifies the subject name of the certificate.

> [!NOTE] > If you must use a comma (,) or a period (.) within a property in the `SubjectName` parameter, > you must enclose the property field in quotation

marks. For example, you may use O="Contoso, Ltd." in the Organization Name field.

Required? true

Position? 1

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ValidityInMonths <System.Nullable`1[System.Int32]>

Specifies the number of months the certificate is valid.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Confirm <System.Management.Automation.SwitchParameter>

Prompts you for confirmation before running the cmdlet.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-WhatIf <System.Management.Automation.SwitchParameter>

Shows what would happen if the cmdlet runs. The cmdlet is not run.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug,

ErrorAction, ErrorVariable, WarningAction, WarningVariable,

OutBuffer, PipelineVariable, and OutVariable. For more information, see

about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

INPUTS

System.String

System.Collections.Generic.List`1[[System.String, System.Private.CoreLib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=7cec85d7bea7798e]]

System.Nullable`1[[System.Int32, System.Private.CoreLib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=7cec85d7bea7798e]]

System.Management.Automation.SwitchParameter

System.Collections.Generic.List`1[[System.Security.Cryptography.X509Certificates.X509KeyUsageFlags, System.Security.Cryptography.X509Certificates, Version=4.2.1.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a]]

OUTPUTS

Microsoft.Azure.Commands.KeyVault.Models.PSKeyVaultCertificatePolicy

NOTES

---------- Example 1: Create a certificate policy ----------

New-AzKeyVaultCertificatePolicy -SecretContentType "application/x-pkcs12" -SubjectName "CN=contoso.com" -IssuerName "Self" -ValidityInMonths 6 -ReuseKeyOnRenewal

SecretContentType : application/x-pkcs12

Kty :

KeySize : 2048

Curve :

Exportable :

ReuseKeyOnRenewal : True

SubjectName : CN=contoso.com

DnsNames :

KeyUsage :

Ekus :

ValidityInMonths : 6

IssuerName : Self

CertificateType :

RenewAtNumberOfDaysBeforeExpiry :

RenewAtPercentageLifetime :

EmailAtNumberOfDaysBeforeExpiry :

EmailAtPercentageLifetime :

CertificateTransparency :

Enabled : True

Created :

Updated :

This command creates a certificate policy that is valid for six months and reuses the key to renew the certificate.

---------- Example 2 ----------

New-AzKeyVaultCertificatePolicy -IssuerName 'Self' -KeyType RSA -RenewAtNumberOfDaysBeforeExpiry <Int32> -SecretContentType application/x-pkcs12 -SubjectName

'CN=contoso.com' -ValidityInMonths 6

Example 3: Create a Subject Alternate Name (or SAN) certificate

```
New-AzKeyVaultCertificatePolicy -SecretContentType "application/x-pkcs12" -SubjectName "CN=contoso.com"
-DnsName
"contoso.com","support.contoso.com","docs.contoso.com" -IssuerName "Self"

SecretContentType             : application/x-pkcs12
Kty                           : RSA
KeySize                       : 2048
Curve                         :
Exportable                    :
ReuseKeyOnRenewal             : False
SubjectName                   : CN=contoso.com
DnsNames                      : {contoso.com, support.contoso.com, docs.contoso.com}
KeyUsage                      :
Ekus                          :
ValidityInMonths              :
IssuerName                    : Self
CertificateType               :
RenewAtNumberOfDaysBeforeExpiry :
RenewAtPercentageLifetime     :
EmailAtNumberOfDaysBeforeExpiry :
EmailAtPercentageLifetime     :
CertificateTransparency       :
Enabled                       : True
Created                       :
Updated                       :
```

This example creates a SAN certificate with 3 DNS names.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.keyvault/new-azkeyvaultcertificatepolicy

Get-AzKeyVaultCertificatePolicy

Set-AzKeyVaultCertificatePolicy