Windows PowerShell Get-Help on Cmdlet 'Add-AzKeyVaultKey'

PS:\>Get-HELP Add-AzKeyVaultKey -Full

NAME

Add-AzKeyVaultKey

SYNOPSIS

Creates a key in a key vault or imports a key into a key vault.

SYNTAX

Add-AzKeyVaultKey [-VaultName] <System.String> [-Name] <System.String> [-CurveName <System.String>] [-DefaultProfile

<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Destination {HSM | Software | HSM | Software} [-Disable] [-Expires

<System.Nullable`1[System.DateTime]>] [-Exportable] [-Immutable] [-KeyOps <System.String[]>] [-KeyType <System.String>] [-NotBefore

<System.Nullable`1[System.DateTime]>] [-ReleasePolicyPath <System.String>] [-Size <System.Nullable`1[System.Int32]>] [-Tag <System.Collections.Hashtable>]

[-UseDefaultCVMPolicy] [-Confirm] [-WhatIf] [<CommonParameters>]

Add-AzKeyVaultKey [-VaultName] <System.String> [-Name] <System.String> [-CurveName <System.String>] [-DefaultProfile

<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Destination {HSM | Software | HSM | Software}] [-Disable] [-Expires <System.Nullable`1[System.DateTime]>] [-KeyFilePassword <System.Security.SecureString>] -KeyFilePath <System.String> [-KeyOps <System.String[]>] [-KeyType <System.String>] [-NotBefore <System.Nullable`1[System.DateTime]>] [-Tag <System.Collections.Hashtable>] [-Confirm] [-WhatIf] [<CommonParameters>]

Add-AzKeyVaultKey [-Name] <System.String> [-CurveName <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Disable] [-Expires <System.Nullable`1[System.DateTime]>] [-Exportable] -HsmName <System.String> [-Immutable] [-KeyOps <System.String[]>] -KeyType <System.String> [-NotBefore <System.Nullable`1[System.DateTime]>] [-ReleasePolicyPath <System.String>] [-Size <System.Nullable`1[System.Int32]>] [-Tag <System.Collections.Hashtable>] [-UseDefaultCVMPolicy] [-Confirm] [-WhatIf] [<CommonParameters>]

Add-AzKeyVaultKey [-InputObject] <Microsoft.Azure.Commands.KeyVault.Models.PSKeyVault> [-Name] <System.String> [-CurveName <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Destination {HSM | Software | HSM | Software} [-Disable] [-Expires <System.Nullable`1[System.DateTime]>] [-Exportable] [-Immutable] [-KeyOps <System.String[]>] [-KeyType <System.String>] [-NotBefore <System.Nullable`1[System.DateTime]>] [-ReleasePolicyPath <System.String>] [-Size <System.Nullable`1[System.Int32]>] [-Tag <System.Collections.Hashtable>] [-UseDefaultCVMPolicy] [-Confirm] [-WhatIf] [<CommonParameters>]

Add-AzKeyVaultKey [-InputObject] <Microsoft.Azure.Commands.KeyVault.Models.PSKeyVault> [-Name] <System.String> [-CurveName <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Destination {HSM | Software | HSM | Software}] [-Disable] [-Expires <System.Nullable`1[System.DateTime]>] [-KeyFilePassword <System.Security.SecureString>] -KeyFilePath <System.String> [-KeyOps <System.String[]>] [-KeyType <System.String>] [-NotBefore <System.Nullable`1[System.DateTime]>] [-Tag <System.Collections.Hashtable>] [-Confirm] [-WhatIf] [<CommonParameters>]

Add-AzKeyVaultKey [-HsmObject] <Microsoft.Azure.Commands.KeyVault.Models.PSManagedHsm> [-Name] <System.String> [-CurveName <System.String>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Disable] [-Expires <System.Nullable`1[System.DateTime]>] [-Exportable]
[-Immutable] [-KeyOps <System.String[]>] -KeyType <System.String> [-NotBefore <System.Nullable`1[System.DateTime]>] [-ReleasePolicyPath <System.String>] [-Size
<System.Nullable`1[System.Int32]>] [-Tag <System.Collections.Hashtable>] [-UseDefaultCVMPolicy] [-Confirm] [-WhatIf] [<CommonParameters>]

Add-AzKeyVaultKey [-ResourceId] <System.String> [-Name] <System.String> [-CurveName <System.String>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Destination {HSM | Software | HSM | Software} [-Disable] [-Expires
<System.Nullable`1[System.DateTime]>] [-Exportable] [-Immutable] [-KeyOps <System.String[]>] [-KeyType <System.String>] [-NotBefore
<System.Nullable`1[System.DateTime]>] [-ReleasePolicyPath <System.String>] [-Size <System.Nullable`1[System.Int32]>] [-Tag <System.Collections.Hashtable>]
[-UseDefaultCVMPolicy] [-Confirm] [-WhatIf] [<CommonParameters>]

Add-AzKeyVaultKey [-ResourceId] <System.String> [-Name] <System.String> [-CurveName <System.String>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Destination {HSM | Software | HSM | Software}] [-Disable] [-Expires
<System.Nullable`1[System.DateTime]>] [-KeyFilePassword <System.Security.SecureString>] -KeyFilePath <System.String> [-KeyOps <System.String[]>] [-KeyType
<System.String>] [-NotBefore <System.Nullable`1[System.DateTime]>] [-Tag <System.Collections.Hashtable>] [-Confirm] [-WhatIf] [<CommonParameters>]

Add-AzKeyVaultKey [-Name] <System.String> [-CurveName <System.String>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Disable] [-Expires <System.Nullable`1[System.DateTime]>] [-Exportable]
-HsmResourceId <System.String> [-Immutable] [-KeyOps <System.String[]>] -KeyType <System.String> [-NotBefore

<System.Nullable`1[System.DateTime]>] [-ReleasePolicyPath

<System.String>] [-Size <System.Nullable`1[System.Int32]>] [-Tag <System.Collections.Hashtable>] [-UseDefaultCVMPolicy] [-Confirm] [-WhatIf] [<CommonParameters>]

Add-AzKeyVaultKey [-Name] <System.String> [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Disable]

[-Expires <System.Nullable`1[System.DateTime]>] -HsmName <System.String> [-KeyFilePassword <System.Security.SecureString>] -KeyFilePath <System.String> [-KeyOps

<System.String[]>] [-NotBefore <System.Nullable`1[System.DateTime]>] [-Tag <System.Collections.Hashtable>] [-Confirm] [-WhatIf] [<CommonParameters>]

Add-AzKeyVaultKey [-HsmObject] <Microsoft.Azure.Commands.KeyVault.Models.PSManagedHsm> [-Name] <System.String> [-DefaultProfile

<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Disable] [-Expires <System.Nullable`1[System.DateTime]>]

[-KeyFilePassword <System.Security.SecureString>] -KeyFilePath <System.String> [-KeyOps <System.String[]>] [-NotBefore <System.Nullable`1[System.DateTime]>] [-Tag

<System.Collections.Hashtable>] [-Confirm] [-WhatIf] [<CommonParameters>]

Add-AzKeyVaultKey [-Name] <System.String> [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Disable]

[-Expires <System.Nullable`1[System.DateTime]>] -HsmResourceId <System.String> [-KeyFilePassword <System.Security.SecureString>] -KeyFilePath <System.String> [-KeyOps

<System.String[]>] [-NotBefore <System.Nullable`1[System.DateTime]>] [-Tag <System.Collections.Hashtable>] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Add-AzKeyVaultKey cmdlet creates a key in a key vault in Azure Key Vault, or imports a key into a key vault. Use this cmdlet to add keys by using any of the

following methods: - Create a key in a hardware security module (HSM) in the Key Vault service.

- Create a key in software in the Key Vault service.

- Import a key from your own hardware security module (HSM) to HSMs in the Key Vault service.

- Import a key from a .pfx file on your computer.

- Import a key from a .pfx file on your computer to hardware security modules (HSMs) in the Key Vault service.

For any of these operations, you can provide key attributes or accept default settings. If you create or import a key that has the same name as an existing key in

your key vault, the original key is updated with the values that you specify for the new key. You can access the previous values by using the version-specific URI for

that version of the key. To learn about key versions and the URI structure, see About Keys and Secrets (http://go.microsoft.com/fwlink/?linkid=518560)in the Key Vault

REST API documentation. Note: To import a key from your own hardware security module, you must first generate a BYOK package (a file with a .byok file name extension)

by using the Azure Key Vault BYOK toolset. For more information, see How to Generate and Transfer HSM-Protected Keys for Azure Key Vault

(http://go.microsoft.com/fwlink/?LinkId=522252). As a best practice, back up your key after it is created or updated, by using the Backup-AzKeyVaultKey cmdlet. There

is no undelete functionality, so if you accidentally delete your key or delete it and then change your mind, the key is not recoverable unless you have a backup of it

that you can restore.

PARAMETERS

-CurveName <System.String>

Specifies the curve name of elliptic curve cryptography, this value is valid when KeyType is EC.

Required? false

Position? named

Default value None

Accept pipeline input? False

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

-Destination <System.String>

Specifies whether to add the key as a software-protected key or an HSM-protected key in the Key Vault service. Valid values are: HSM and Software. Note: To use

HSM as your destination, you must have a key vault that supports HSMs. For more information about the service tiers and capabilities for Azure Key Vault, see the

Azure Key Vault Pricing website (http://go.microsoft.com/fwlink/?linkid=512521). This parameter is required when you create a new key. If you import a key by

using the KeyFilePath parameter, this parameter is optional: - If you do not specify this parameter, and this cmdlet imports a key that has .byok file name

extension, it imports that key as an HSM-protected key. The cmdlet cannot import that key as software-protected key. - If you do not specify this parameter, and

this cmdlet imports a key that has a .pfx file name extension, it imports the key as a software-protected key.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Disable <System.Management.Automation.SwitchParameter>

Indicates that the key you are adding is set to an initial state of disabled. Any attempt to use the key will fail. Use this parameter if you are preloading keys

that you intend to enable later.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Expires <System.Nullable`1[System.DateTime]>

Specifies the expiration time of the key in UTC, as a DateTime object, for the key that this cmdlet adds. If not specified, key will not expire. To obtain a

DateTime object, use the Get-Date cmdlet. For more information, type `Get-Help Get-Date`. Please notice that expirys is ignored for Key Exchange Key used in BYOK

process.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Exportable <System.Management.Automation.SwitchParameter>

Indicates if the private key can be exported.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-HsmName <System.String>

HSM name. Cmdlet constructs the FQDN of a managed HSM based on the name and currently selected environment.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-HsmObject <Microsoft.Azure.Commands.KeyVault.Models.PSManagedHsm>

HSM object.

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-HsmResourceId <System.String>

Resource ID of the HSM.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Immutable <System.Management.Automation.SwitchParameter>

Sets the release policy as immutable state. Once marked immutable, this flag cannot be reset and the policy cannot be changed under any circumstances.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-InputObject <Microsoft.Azure.Commands.KeyVault.Models.PSKeyVault>

Vault object.

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-KeyFilePassword <System.Security.SecureString>

Specifies a password for the imported file as a SecureString object. To obtain a SecureString object, use the ConvertTo-SecureString cmdlet. For more information,

type `Get-Help ConvertTo-SecureString`. You must specify this password to import a file with a .pfx file name extension.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-KeyFilePath <System.String>

Specifies the path of a local file that contains key material that this cmdlet imports. The valid file name extensions are .byok and .pfx. - If the file is a

.byok file, the key is automatically protected by HSMs after the import and you cannot override this default. - If the file is a .pfx file, the key is

automatically protected by software after the import. To override this default, set the Destination parameter to HSM so that the key is HSM-protected. When you

specify this parameter, the Destination parameter is optional.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-KeyOps <System.String[]>

Specifies an array of operations that can be performed by using the key that this cmdlet adds. If you do not specify this parameter, all operations can be

performed. The acceptable values for this parameter are a comma-separated list of key operations as defined by the JSON Web Key (JWK) specification

(http://go.microsoft.com/fwlink/?LinkID=613300): - encrypt

- decrypt

- wrapKey

- unwrapKey

- sign

- verify

- import (for KEK only, see example 7)

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-KeyType <System.String>

Specifies the key type of this key. When importing BYOK keys, it defaults to 'RSA'.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <System.String>

Specifies the name of the key to add to the key vault. This cmdlet constructs the fully qualified domain name (FQDN) of a key based on the name that this

parameter specifies, the name of the key vault, and your current environment. The name must be a string of 1 through 63 characters in length that contains only

0-9, a-z, A-Z, and - (the dash symbol).

Required? true

Position? 1

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-NotBefore <System.Nullable`1[System.DateTime]>

Specifies the time, as a DateTime object, before which the key cannot be used. This parameter uses UTC. To obtain a DateTime object, use the Get-Date cmdlet. If

you do not specify this parameter, the key can be used immediately.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ReleasePolicyPath <System.String>

A path to a file containing JSON policy definition. The policy rules under which a key can be exported.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceId <System.String>

Vault Resource Id.

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

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

RSA key size, in bits. If not specified, the service will provide a safe default.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Tag <System.Collections.Hashtable>

Key-value pairs in the form of a hash table. For example: @{key0="value0";key1=$null;key2="value2"}

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-UseDefaultCVMPolicy <System.Management.Automation.SwitchParameter>

Specifies to use default policy under which the key can be exported for CVM disk encryption.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-VaultName <System.String>

Specifies the name of the key vault to which this cmdlet adds the key. This cmdlet constructs the FQDN of a key vault based on the name that this parameter

specifies and your current environment.

Required? true

Position? 0

Default value None

Accept pipeline input? False

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

Microsoft.Azure.Commands.KeyVault.Models.PSKeyVault

Microsoft.Azure.Commands.KeyVault.Models.PSManagedHsm

System.String

OUTPUTS

Microsoft.Azure.Commands.KeyVault.Models.PSKeyVaultKey

NOTES

---------- Example 1: Create a key ----------

Add-AzKeyVaultKey -VaultName 'contoso' -Name 'ITSoftware' -Destination 'Software'

Vault/HSM Name : contoso

Name : ITSoftware

Key Type : RSA

Key Size : 2048

Curve Name :

Version : 67da57e9cadf48a2ad8d366b115843ab

Id : https://contoso.vault.azure.net:443/keys/ITSoftware/67da57e9cadf48a2ad8d366b115843ab

Enabled : True

Expires :

Not Before :

Created : 5/21/2018 11:10:58 PM

Updated : 5/21/2018 11:10:58 PM

Purge Disabled : False

Tags :

This command creates a software-protected key named ITSoftware in the key vault named Contoso.

---------- Example 2: Create an EC key ----------

Add-AzKeyVaultKey -VaultName test-kv -Name test-key -Destination Software -KeyType EC

Vault/HSM Name : test-kv

Name : test-key

Key Type : EC

Key Size :

Curve Name : P-256

Version : 4da74af2b4fd47d6b1aa0b05c9a2ed13

Id : https://test-kv.vault.azure.net:443/keys/test-key/4da74af2b4fd47d6b1aa0b05c9a2ed13

Enabled : True

Expires :

Not Before :

Created : 8/24/2021 6:38:34 AM

Updated : 8/24/2021 6:38:34 AM

Recovery Level : Recoverable+Purgeable

Tags :

This command creates a software-protected EC key named test-key in the key vault named test-kv. Its curve name is P-256 by default.

---------- Example 3: Create an HSM-protected key ----------

Add-AzKeyVaultKey -VaultName 'contoso' -Name 'ITHsm' -Destination 'HSM'

Vault Name : contoso

Name : ITHsm

Version : 67da57e9cadf48a2ad8d366b115843ab

Id : https://contoso.vault.azure.net:443/keys/ITSoftware/67da57e9cadf48a2ad8d366b115843ab

Enabled : True

Expires :

Not Before :

Created : 5/21/2018 11:10:58 PM

Updated : 5/21/2018 11:10:58 PM

Purge Disabled : False

Tags :

This command creates an HSM-protected key in the key vault named Contoso.

------- Example 4: Create a key with non-default values -------

$KeyOperations = 'decrypt', 'verify'

$Expires = (Get-Date).AddYears(2).ToUniversalTime()

$NotBefore = (Get-Date).ToUniversalTime()

$Tags = @{'Severity' = 'high'; 'Accounting' = ''true''}

Add-AzKeyVaultKey -VaultName 'contoso' -Name 'ITHsmNonDefault' -Destination 'HSM' -Expires $Expires -NotBefore $NotBefore -KeyOps $KeyOperations -Disable -Tag $Tags

Vault/HSM Name : contoso

Name : ITHsmNonDefault

Key Type : RSA

Key Size : 2048

Version : 929bfc14db84439b823ffd1bedadaf5f

Id : https://contoso.vault.azure.net:443/keys/ITHsmNonDefault/929bfc14db84439b823ffd1bedadaf5f

Enabled : False

Expires : 5/21/2020 11:12:43 PM

Not Before : 5/21/2018 11:12:50 PM

Created : 5/21/2018 11:13:17 PM

Updated : 5/21/2018 11:13:17 PM

Purge Disabled : False

Tags : Name Value

Severity high

Accounting true

The first command stores the values decrypt and verify in the $KeyOperations variable. The second command creates a DateTime object, defined in UTC, by using the

Get-Date cmdlet. That object specifies a time two years in the future. The command stores that date in the $Expires variable. For more information, type `Get-Help

Get-Date`. The third command creates a DateTime object by using the Get-Date cmdlet. That object specifies current UTC time. The command stores that date in the

$NotBefore variable. The final command creates a key named ITHsmNonDefault that is an HSM-protected key. The command specifies values for allowed key operations

stored $KeyOperations. The command specifies times for the Expires and NotBefore parameters created in the previous commands, and tags for high severity and IT. The

new key is disabled. You can enable it by using the Set-AzKeyVaultKey cmdlet.

---------- Example 5: Import an HSM-protected key ----------

Add-AzKeyVaultKey -VaultName 'contoso' -Name 'ITByok' -KeyFilePath 'C:\Contoso\ITByok.byok' -Destination 'HSM'

Vault Name : contoso

Name : ITByok

Version : 67da57e9cadf48a2ad8d366b115843ab

Id : https://contoso.vault.azure.net:443/keys/ITByok/67da57e9cadf48a2ad8d366b115843ab

Enabled : True

Expires :

Not Before :

Created : 5/21/2018 11:10:58 PM

Updated : 5/21/2018 11:10:58 PM

Purge Disabled : False

Tags :

This command imports the key named ITByok from the location that the KeyFilePath parameter specifies. The imported key is an HSM-protected key. To import a key from

your own hardware security module, you must first generate a BYOK package (a file with a .byok file name extension) by using the Azure Key Vault BYOK toolset. For

more information, see How to Generate and Transfer HSM-Protected Keys for Azure Key Vault (http://go.microsoft.com/fwlink/?LinkId=522252).

---------- Example 6: Import a software-protected key ----------

$Password = ConvertTo-SecureString -String 'Password' -AsPlainText -Force

Add-AzKeyVaultKey -VaultName 'contoso' -Name 'ITPfx' -KeyFilePath 'C:\Contoso\ITPfx.pfx' -KeyFilePassword $Password

Vault Name : contoso

Name : ITPfx

Version : 67da57e9cadf48a2ad8d366b115843ab

Id : https://contoso.vault.azure.net:443/keys/ITPfx/67da57e9cadf48a2ad8d366b115843ab

Enabled : True

Expires :

Not Before :

Created : 5/21/2018 11:10:58 PM

Updated : 5/21/2018 11:10:58 PM

Purge Disabled : False

Tags :

The first command converts a string into a secure string by using the ConvertTo-SecureString cmdlet, and then stores that string in the $Password variable. For more

information, type `Get-Help ConvertTo-SecureString`. The second command creates a software password in the Contoso key vault. The command specifies the location for

the key and the password stored in $Password.

-------- Example 7: Import a key and assign attributes --------

```
$Password = ConvertTo-SecureString -String 'password' -AsPlainText -Force
$Expires = (Get-Date).AddYears(2).ToUniversalTime()
$Tags = @{ 'Severity' = 'high'; 'Accounting' = "true" }
Add-AzKeyVaultKey -VaultName 'contoso' -Name 'ITPfxToHSM' -Destination 'HSM' -KeyFilePath 'C:\Contoso\ITPfx.pfx' -KeyFilePassword $Password -Expires $Expires -Tag
$Tags
```

Vault Name : contoso

Name : ITPfxToHSM

Version : 929bfc14db84439b823ffd1bedadaf5f

Id : https://contoso.vault.azure.net:443/keys/ITPfxToHSM/929bfc14db84439b823ffd1bedadaf5f

Enabled : True

Expires : 5/21/2020 11:12:43 PM

Not Before :

Created : 5/21/2018 11:13:17 PM

Updated : 5/21/2018 11:13:17 PM

Purge Disabled : False

Tags : Name Value

Severity high

Accounting true

The first command converts a string into a secure string by using the ConvertTo-SecureString cmdlet, and then stores that string in the $Password variable. The second

command creates a DateTime object by using the Get-Date cmdlet, and then stores that object in the $Expires variable. The third command creates the $tags variable to

set tags for high severity and IT. The final command imports a key as an HSM key from the specified location. The command specifies the expiration time stored in

$Expires and password stored in $Password, and applies the tags stored in $tags.

Example 8: Generate a Key Exchange Key (KEK) for "bring your own key" (BYOK) feature

$key = Add-AzKeyVaultKey -VaultName $vaultName -Name $keyName -Destination HSM -Size 2048 -KeyOps "import"

Generates a key (referred to as a Key Exchange Key (KEK)). The KEK must be an RSA-HSM key that has only the import key operation. Only Key Vault Premium SKU supports

RSA-HSM keys. For more details please refer to https://learn.microsoft.com/azure/key-vault/keys/hsm-protected-keys

-------- Example 9: Create a secure key in managed hsm --------

```
<# release_policy_template.json
{
  "anyOf": [
    {
      "allOf": [
        {
          "claim": "<claim name>",
```

```
            "equals": "<value to match>"
          }
        ],
        "authority": "<issuer>"
      }
    ],
    "version": "1.0.0"
  }
  #>
```

Add-AzKeyVaultKey -HsmName testmhsm -Name test-key -KeyType RSA -Exportable -ReleasePolicyPath release_policy.json

```
  Vault/HSM Name : testmhsm
  Name           : test-key
  Key Type       : RSA
  Key Size       : 2048
  Curve Name     :
  Version        : ed6b026bf0a605042006635713d33ef6
  Id             : https://testmhsm.managedhsm.azure.net:443/keys/test-key/ed6b026bf0a605042006635713d33ef6
  Enabled        : True
  Expires        :
  Not Before     :
  Created        : 6/2/2022 7:14:37 AM
  Updated        : 6/2/2022 7:14:37 AM
  Recovery Level : Recoverable+Purgeable
  Release Policy :
                   Content Type   : application/json; charset=utf-8
                   Policy Content : {"anyOf":[{"allOf":[{"claim":"x-ms-sgx-is-debuggable","equals":"true"}],"authority":"htt
                   ps://sharedeus.eus.attest.azure.net/"}],"version":"1.0.0"}
                   Immutable      : False


  Tags           :
```

Create a secure key in managed hsm named testmhsm. Its name is test-key and type is RSA.

- Example 10: Add a key for a Confidential VM to a key vault. -

New-AzKeyVault -Name $keyVaultName -Location $location -ResourceGroupName $resourceGroupName -Sku Premium -EnablePurgeProtection -EnabledForDiskEncryption;
$cvmAgent = Get-AzADServicePrincipal -ApplicationId 'bf7b6499-ff71-4aa2-97a4-f372087be7f0';
Set-AzKeyVaultAccessPolicy -VaultName $keyVaultName -ResourceGroupName $resourceGroupName -ObjectId $cvmAgent.id -PermissionsToKeys get,release;

$keySize = 3072;
Add-AzKeyVaultKey -VaultName $keyVaultName -Name $keyName -Size $keySize -KeyOps wrapKey,unwrapKey -KeyType RSA -Destination HSM -Exportable -UseDefaultCVMPolicy;

Vault/HSM Name : <Vault Name>
Name : <Key Name>
Key Type : RSA
Key Size : 3072
Curve Name :
Version : <Version>
Id : <Id>
Enabled : True
Expires :
Not Before :
Created : 9/9/2022 8:36:00 PM
Updated : 9/9/2022 8:36:00 PM
Recovery Level : Recoverable
Release Policy :
Content Type : application/json; charset=utf-8
Policy Content : <Policy Content>
Immutable : False

Tags :

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.keyvault/add-azkeyvaultkey

Backup-AzKeyVaultKey

Get-AzKeyVaultKey

Remove-AzKeyVaultKey