Windows PowerShell Get-Help on Cmdlet 'Import-AzKeyVaultSecurityDomain'

PS:\>Get-HELP Import-AzKeyVaultSecurityDomain -Full

NAME

Import-AzKeyVaultSecurityDomain

SYNOPSIS

Imports previously exported security domain data to a managed HSM.

SYNTAX

Import-AzKeyVaultSecurityDomain [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -DownloadExchangeKey [-Force] -Name <System.String> -OutFile <System.String> [-PassThru] [-SubscriptionId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

Import-AzKeyVaultSecurityDomain [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -ExchangeKeyPath <System.String> [-Force] -Keys <Microsoft.Azure.Commands.KeyVault.SecurityDomain.Models.KeyPath[]> -OutFile <System.String> [-PassThru] -RestoreBlob -SecurityDomainPath <System.String> [-SubscriptionId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

Import-AzKeyVaultSecurityDomain [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -ImportRestoredBlob -Name <System.String> [-PassThru] -SecurityDomainPath <System.String> [-SubscriptionId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

Import-AzKeyVaultSecurityDomain [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -InputObject <Microsoft.Azure.Commands.KeyVault.Models.PSKeyVaultIdentityItem> -Keys <Microsoft.Azure.Commands.KeyVault.SecurityDomain.Models.KeyPath[]> [-PassThru] -SecurityDomainPath <System.String> [-SubscriptionId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

Import-AzKeyVaultSecurityDomain [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Keys <Microsoft.Azure.Commands.KeyVault.SecurityDomain.Models.KeyPath[]> -Name <System.String> [-PassThru] -SecurityDomainPath <System.String> [-SubscriptionId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

This cmdlet imports previously exported security domain data to a managed HSM.

PARAMETERS

-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

-DownloadExchangeKey <System.Management.Automation.SwitchParameter>

When specified, an exchange key will be downloaded to specified path.

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-ExchangeKeyPath <System.String>

Local path of exchange key used to encrypt the security domain data. Generated by running Import-AzKeyVaultSecurityDomain with -DownloadExchangeKey.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Force <System.Management.Automation.SwitchParameter>

Specify whether to overwrite existing file.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-ImportRestoredBlob <System.Management.Automation.SwitchParameter>

When specified, SecurityDomainPath should be encrypted security domain data generated by Restore-AzKeyVaultSecurityDomainBlob.

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

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

Object representing a managed HSM.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-Keys <Microsoft.Azure.Commands.KeyVault.SecurityDomain.Models.KeyPath[]>

Information about the keys that are used to decrypt the security domain data. See examples for how it is constructed.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <System.String>

Name of the managed HSM.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-OutFile <System.String>

Local file path to store the security domain encrypted with the exchange key.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PassThru <System.Management.Automation.SwitchParameter>

When specified, a boolean will be returned when cmdlet succeeds.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-RestoreBlob <System.Management.Automation.SwitchParameter>

When specified, the security domain data will be decrypted and encrypted using generated ExchangeKey locally.

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-SecurityDomainPath <System.String>

Specify the path to the encrypted security domain data.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SubscriptionId <System.String>

The ID of the subscription. By default, cmdlets are executed in the subscription that is set in the current context. If the user specifies another subscription,

the current cmdlet is executed in the subscription specified by the user. Overriding subscriptions only take effect during the lifecycle of the current cmdlet. It

does not change the subscription in the context, and does not affect subsequent cmdlets.

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

Microsoft.Azure.Commands.KeyVault.Models.PSKeyVaultIdentityItem

OUTPUTS

System.Boolean

NOTES

---------- Example 1: Import Security domain ----------

$keys = @{PublicKey = "sd1.cer"; PrivateKey = "sd1.key"}, @{PublicKey = "sd2.cer"; PrivateKey = "sd2.key"}, @{PublicKey = "sd3.cer"; PrivateKey = "sd3.key"}

Import-AzKeyVaultSecurityDomain -Name testmhsm -Keys $keys -SecurityDomainPath sd.ps.json

First, the keys need be provided to decrypt the security domain data. Then, The Import-AzKeyVaultSecurityDomain command restores previous backed up security domain

data to a managed HSM using these keys.

----- Example 2: Import Security domain by separate steps -----

```
$exchangeKeyOutputPath = "ExchangeKey.cer"
$SecurityDomainRestoredBlob = "HsmRestoreBlob.json"
    $keys = @{PublicKey = "sd1.cer"; PrivateKey = "sd1.key"}, @{PublicKey = "sd2.cer"; PrivateKey = "sd2.key"}, @{PublicKey = "sd3.cer"; PrivateKey = "sd3.key"}
Import-AzKeyVaultSecurityDomain -Name testmhsm -OutFile $exchangeKeyOutputPath -DownloadExchangeKey
Import-AzKeyVaultSecurityDomain -Keys $keys -ExchangeKeyPath  $exchangeKeyPath -SecurityDomainPath sd.ps.json -OutFile sd_restored.ps.json -RestoreBlob
        Import-AzKeyVaultSecurityDomain -Name testmhsm -SecurityDomainPath $SecurityDomainRestoredBlob -ImportRestoredBlob
```

First, an exchange key should be downloaded by adding `-DownloadExchangeKey`. Then, the security domain data should be decrypted locally using key pairs and encrypted

using generated exchange key by adding `-RestoreBlob`. Finally, the restored security domain data can be imported to a managed HSM using `-ImportRestoredBlob`.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.keyvault/import-azkeyvaultsecuritydomain