



Windows PowerShell Get-Help on Cmdlet 'Set-AzRecoveryServicesVaultProperty'

PS:\>Get-HELP Set-AzRecoveryServicesVaultProperty -Full

NAME

Set-AzRecoveryServicesVaultProperty

SYNOPSIS

Updates properties of a Vault.

SYNTAX

```

Set-AzRecoveryServicesVaultProperty [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>]
[-DisableHybridBackupSecurityFeature <System.Nullable`1[System.Boolean]>] [-SoftDeleteFeatureState {Enable |
Disable | AlwaysON}] [-Token <System.String>] [-VaultId
<System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

```

```

Set-AzRecoveryServicesVaultProperty [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -EncryptionKeyId
<System.String> [-InfrastructureEncryption] [-KeyVaultSubscriptionId <System.String>] [-UserAssignedIdentity
<System.String>] [-UseSystemAssignedIdentity
<System.Boolean>] [-VaultId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

```

DESCRIPTION

The Set-AzRecoveryServicesVaultProperty cmdlet updates properties of a Recovery services vault. This cmdlet can be used to Enable/Disable/AlwaysON soft delete or set

CMK encryption for a vault with two different parameter sets. SoftDeleteFeatureState property of a vault can be disabled only if there are no registered containers in

the vault. InfrastructureEncryption can only be set the first time a user updates the CMK vault.

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

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

Optional flag (\$true/\$false) to disable/enable security setting for hybrid backups against accidental deletes and add additional layer of authentication for

critical operations. Provide \$false to enable the security.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-EncryptionKeyId <System.String>

KeyId of the encryption key to be used for CMK.

Required? true
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-InfrastructureEncryption <System.Management.Automation.SwitchParameter>

Enables infrastructure encryption on this vault. Infrastructure encryption must be enabled when configuring encryption.

Required? false
Position? named
Default value False
Accept pipeline input? False
Accept wildcard characters? false

-KeyVaultSubscriptionId <System.String>

Subscription Id of the Key Vault.

Required? false
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-SoftDeleteFeatureState <System.String>

SoftDeleteFeatureState of the Recovery Services Vault. Allowed values are Disable, Enable, AlwaysON.

Required? false
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-Token <System.String>

Auxiliary access token for authenticating critical operation to resource guard subscription

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-UserAssignedIdentity <System.String>

ARM Id of UserAssigned Identity to be used for CMK encryption. Provide this parameter if UseSystemAssignedIdentity is \$false.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-UseSystemAssignedIdentity <System.Boolean>

Boolean flag to indicate if SystemAssigned Identity will be used for CMK encryption. Accepted Vaules: \$true, \$false

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-VaultId <System.String>

ARM ID of the Recovery Services Vault.

Required? false

Position? named

Default value None
Accept pipeline input? True (ByValue)
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.

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

INPUTS

System.String

OUTPUTS

Microsoft.Azure.Management.RecoveryServices.Backup.Models.BackupResourceVaultConfigResource

NOTES

----- Example 1: Update SoftDeleteFeatureState of a vault -----

```
$vault = Get-AzRecoveryServicesVault -ResourceGroupName "rgName" -Name "vaultName"
```

```
$props = Set-AzRecoveryServicesVaultProperty -VaultId $vault.Id -SoftDeleteFeatureState Enable
```

The first command gets a Vault object and then stores it in the \$vault variable. The second command Updates the SoftDeleteFeatureState property of the vault to

"Enabled" state. Allowed values for SoftDeleteFeatureState are Disable, Enable, AlwaysON.

Example 2: Update CMK encryption of a vault to use SystemAssigned MSIIdentity

```
$vault = Get-AzRecoveryServicesVault -ResourceGroupName "rgName" -Name "vaultName"
```

```
$keyVault = Get-AzKeyVault -VaultName "keyVaultName" -ResourceGroupName "RGName"
```

```
$key = Get-AzKeyVaultKey -VaultName "keyVaultName" -Name "keyName"
```

```
Set-AzRecoveryServicesVaultProperty -EncryptionKeyId $key.ID -InfrastructureEncryption -VaultId $vault.ID  
-UseSystemAssignedIdentity $true
```

First cmdlet gets the RSVault to update encryption properties. Second cmdlet gets the azure key vault. Third cmdlet gets the key from the key vault. Fourth cmdlet

updates the customer managed encryption key within the RSVault to be accessed via SystemAssigned identity. Use -InfrastructureEncryption param to enable infrastructure encryption for the first time update.

Example 3: Update CMK encryption of a vault to use userAssigned MSIIdentity

```
$vault = Get-AzRecoveryServicesVault -ResourceGroupName "rgName" -Name "vaultName"
$keyVault = Get-AzKeyVault -VaultName "keyVaultName" -ResourceGroupName "RGName"
$key = Get-AzKeyVaultKey -VaultName "keyVaultName" -Name "keyName"
Set-AzRecoveryServicesVaultProperty -EncryptionKeyId $key.ID -VaultId $vault.ID -UseSystemAssignedIdentity $false
-UserAssignedIdentity
$vault.Identity.UserAssignedIdentities.Keys[0]
```

First cmdlet gets the RSVault to update encryption properties. Second cmdlet gets the azure key vault. Third cmdlet gets the key from the key vault. Fourth cmdlet updates the customer managed encryption key within the RSVault to be accessed via UserAssigned identity.

--- Example 4: Update HybridBackupSecurityFeature of a vault ---

```
$vault = Get-AzRecoveryServicesVault -ResourceGroupName "rgName" -Name "vaultName"
$prop = Set-AzRecoveryServicesVaultProperty -VaultId $vault.Id -DisableHybridBackupSecurityFeature $false
```

The first command gets a Vault object and then stores it in the \$vault variable. The second command disables the HybridBackupSecurityFeature of the vault, set \$true to enable it again.

RELATED LINKS

Online Version: <https://learn.microsoft.com/powershell/module/az.recoveryservices/set-azrecoveryservicesvaultproperty>

Get-AzRecoveryServicesVault

