



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

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

NAME

Set-AzSqlInstanceTransparentDataEncryptionProtector

SYNOPSIS

Sets the Transparent Data Encryption (TDE) protector for a SQL managed instance.

SYNTAX

```

Set-AzSqlInstanceTransparentDataEncryptionProtector [-Instance]
<Microsoft.Azure.Commands.Sql.ManagedInstance.Model.AzureSqlManagedInstanceModel> [-Type]
{AzureKeyVault | ServiceManaged} [[-KeyId] <System.String>] [-AutoRotationEnabled
<System.Nullable`1[System.Boolean]>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Force] [-Confirm]
[-WhatIf] [<CommonParameters>]

Set-AzSqlInstanceTransparentDataEncryptionProtector [-ResourceGroupName] <System.String> [-InstanceName]
<System.String> [-Type] {AzureKeyVault | ServiceManaged}
[[ -KeyId] <System.String>] [-AutoRotationEnabled <System.Nullable`1[System.Boolean]>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Force] [-Confirm]
[-WhatIf] [<CommonParameters>]

```

```
Set-AzSqlInstanceTransparentDataEncryptionProtector [-InstanceResourceId] <System.String> [-Type] {AzureKeyVault |
ServiceManaged} [[-KeyId] <System.String>]
                        [-AutoRotationEnabled <System.Nullable`1[System.Boolean]>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>]
[-Force] [-Confirm] [-WhatIf] [<CommonParameters>]
```

DESCRIPTION

The Set-AzSqlInstanceTransparentDataEncryptionProtector cmdlet sets the TDE protector for a SQL managed instance. Changing the TDE protector type will rotate the protector.

PARAMETERS

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

The key auto rotation opt-in status.

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

-Force <System.Management.Automation.SwitchParameter>

Skip confirmation message for performing the action

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Instance <Microsoft.Azure.Commands.Sql.ManagedInstance.Model.AzureSqlManagedInstanceModel>

The instance input object

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-InstanceName <System.String>

The instance name

Required? true

Position? 1

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-InstanceResourceId <System.String>

The instance resource id

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-KeyId <System.String>

The Azure Key Vault KeyId.

Required? false

Position? 2

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceGroupName <System.String>

The Resource Group Name

Required? true

Position? 0

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Type <Microsoft.Azure.Commands.Sql.TransparentDataEncryption.Model.EncryptionProtectorType>

The Azure Sql Database Transparent Data Encryption Protector type.

Required? true

Position? 1

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

INPUTS

Microsoft.Azure.Commands.Sql.ManagedInstance.Model.AzureSqlManagedInstanceModel
System.String

OUTPUTS

Microsoft.Azure.Commands.Sql.TransparentDataEncryption.Model.AzureRmSqlManagedInstanceTransparentDataEncryptionProtectorModel

NOTES

Example 1: Set the Transparent Data Encryption (TDE) protector type to ServiceManaged

```
Set-AzSqlInstanceTransparentDataEncryptionProtector -ResourceGroupName 'ContosoResourceGroup' -InstanceName  
'ContosoManagedInstanceName' -Type ServiceManaged
```

```
ResourceGroupName      : ContosoResourceGroup  
ManagedInstanceName   : ContosoManagedInstanceName  
Type                   : ServiceManaged  
ManagedInstanceKeyVaultKeyName : ServiceManaged  
KeyId                  :
```

This command updates a managed instance's TDE protector type to Service Managed.

Example 2: Set the Transparent Data Encryption protector type to Azure Key Vault

```
Set-AzSqlInstanceTransparentDataEncryptionProtector -ResourceGroupName 'ContosoResourceGroup' -InstanceName  
'ContosoManagedInstanceName' -Type AzureKeyVault -KeyId  
'https://contoso.vault.azure.net/keys/contosokey/01234567890123456789012345678901'
```

```
ResourceGroupName      : ContosoResourceGroup  
ManagedInstanceName   : ContosoManagedInstanceName  
Type                   : AzureKeyVault  
ManagedInstanceKeyVaultKeyName : contoso_contosokey_01234567890123456789012345678901  
KeyId                  : https://contoso.vault.azure.net/keys/contosokey/01234567890123456789012345678901
```

This command updates the specified managed instance to use the Managed instance Key Vault Key with Id

'https://contoso.vault.azure.net/keys/contosokey/01234567890123456789012345678901' as the TDE protector

Example 3: Set the Transparent Data Encryption protector type to Azure Key Vault using managed instance object

```
$managedInstance = Get-AzSqlInstance -Name 'ContosoManagedInstanceName' -ResourceGroupName  
'ContosoResourceGroup'
```

```
Set-AzSqlInstanceTransparentDataEncryptionProtector -Instance $managedInstance -Type AzureKeyVault -KeyId  
'https://contoso.vault.azure.net/keys/contosokey/01234567890123456789012345678901'
```

ResourceGroupName : ContosoResourceGroup

ManagedInstanceName : ContosoManagedInstanceName

Type : AzureKeyVault

ManagedInstanceKeyVaultKeyName : contoso_contosokey_01234567890123456789012345678901

KeyId : https://contoso.vault.azure.net/keys/contosokey/01234567890123456789012345678901

This command updates the specified managed instance to use the Managed instance Key Vault Key with Id
'https://contoso.vault.azure.net/keys/contosokey/01234567890123456789012345678901' as the TDE protector.

Example 4: Set the Transparent Data Encryption protector type to Azure Key Vault using resource id

```
$managedInstance = Get-AzSqlInstance -Name 'ContosoManagedInstanceName' -ResourceGroupName  
'ContosoResourceGroup'
```

```
Set-AzSqlInstanceTransparentDataEncryptionProtector -InstanceResourceid $managedInstance.Resourceid -Type  
AzureKeyVault -KeyId
```

```
'https://contoso.vault.azure.net/keys/contosokey/01234567890123456789012345678901'
```

ResourceGroupName : ContosoResourceGroup

ManagedInstanceName : ContosoManagedInstanceName

Type : AzureKeyVault

ManagedInstanceKeyVaultKeyName : contoso_contosokey_01234567890123456789012345678901

KeyId : https://contoso.vault.azure.net/keys/contosokey/01234567890123456789012345678901

This command updates the specified managed instance to use the Managed instance Key Vault Key with Id 'https://contoso.vault.azure.net/keys/contosokey/01234567890123456789012345678901' as the TDE protector.

Example 5: Set the Transparent Data Encryption protector type to Azure Key Vault using piping

```
$managedInstance = Get-AzSqlInstance -Name 'ContosoManagedInstanceName' -ResourceGroupName 'ContosoResourceGroup'
```

```
$managedInstance | Set-AzSqlInstanceTransparentDataEncryptionProtector -Type AzureKeyVault -KeyId 'https://contoso.vault.azure.net/keys/contosokey/01234567890123456789012345678901'
```

ResourceGroupName : ContosoResourceGroup

ManagedInstanceName : ContosoManagedInstanceName

Type : AzureKeyVault

ManagedInstanceKeyVaultKeyName : contoso_contosokey_01234567890123456789012345678901

KeyId : https://contoso.vault.azure.net/keys/contosokey/01234567890123456789012345678901

This command updates the specified managed instance to use the Managed instance Key Vault Key with Id 'https://contoso.vault.azure.net/keys/contosokey/01234567890123456789012345678901' as the TDE protector.

RELATED LINKS

Online

Version:

<https://learn.microsoft.com/powershell/module/Az.sql/Set-AzSqlInstanceTransparentDataEncryptionProtector>