



Windows PowerShell Get-Help on Cmdlet 'Update-AzSqlInstanceDatabaseVulnerabilityAssessmentSetting'

PS:\>Get-HELP Update-AzSqlInstanceDatabaseVulnerabilityAssessmentSetting -Full

NAME

Update-AzSqlInstanceDatabaseVulnerabilityAssessmentSetting

SYNOPSIS

Updates the vulnerability assessment settings of a managed database.

SYNTAX

```
Update-AzSqlInstanceDatabaseVulnerabilityAssessmentSetting [-ResourceGroupName] <System.String>
[-InstanceName] <System.String> [-DatabaseName] <System.String>
-BlobStorageSasUri <System.Uri> [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-EmailAdmins
<System.Boolean>] [-NotificationEmail <System.String[]>] [-RecurringScansInterval {None | Weekly}] [-Confirm] [-WhatIf]
[<CommonParameters>]
```

```
Update-AzSqlInstanceDatabaseVulnerabilityAssessmentSetting [-ResourceGroupName] <System.String>
[-InstanceName] <System.String> [-DatabaseName] <System.String>
[-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>]
[-EmailAdmins <System.Boolean>] -InputObject
<Microsoft.Azure.Commands.Sql.VulnerabilityAssessment.Model.VulnerabilityAssessmentSetting>
```

```

[-NotificationEmail <System.String[]>] [-RecurringScansInterval
{None | Weekly}] [-Confirm] [-WhatIf] [<CommonParameters>]

Update-AzSqlInstanceDatabaseVulnerabilityAssessmentSetting [-ResourceGroupName] <System.String>
[-InstanceName] <System.String> [-DatabaseName] <System.String>
[-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>]
[-EmailAdmins <System.Boolean>] [-NotificationEmail
<System.String[]>] [-RecurringScansInterval {None | Weekly}] [-ScanResultsContainerName <System.String>]
[-StorageAccountName <System.String>] [-Confirm] [-WhatIf]
[<CommonParameters>]

```

DESCRIPTION

The `Update-AzSqlInstanceDatabaseVulnerabilityAssessmentSetting` cmdlet updates the vulnerability assessment settings of an Azure SQL Managed Database. Note that you need to run `Enable-AzSqlInstanceAdvancedDataSecurity` cmdlet as a prerequisite for using this cmdlet.

PARAMETERS

`-BlobStorageSasUri <System.Uri>`

A SAS URI to a storage container that will hold the scan results.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

`-DatabaseName <System.String>`

SQL Managed Database name.

Required? true

Position? 2

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

-EmailAdmins <System.Boolean>

A value indicating whether to email service and co-administrators on recurring scan completion.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-InputObject <Microsoft.Azure.Commands.Sql.VulnerabilityAssessment.Model.VulnerabilityAssessmentSettingsModel>

The Vulnerability Assessment settings object to set

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-InstanceName <System.String>

SQL Managed Instance name.

Required? true
Position? 1
Default value None
Accept pipeline input? True (ByPropertyName)
Accept wildcard characters? false

-NotificationEmail <System.String[]>

A list of mail addresses to send on recurring scan completion.

Required? false
Position? named
Default value None
Accept pipeline input? True (ByPropertyName)
Accept wildcard characters? false

-RecurringScansInterval <Microsoft.Azure.Commands.Sql.VulnerabilityAssessment.Model.RecurringScansInterval>

The recurring scans interval.

Required? false
Position? named
Default value None
Accept pipeline input? True (ByPropertyName)
Accept wildcard characters? false

-ResourceGroupName <System.String>

The name of the resource group.

Required? true
Position? 0
Default value None
Accept pipeline input? True (ByPropertyName)
Accept wildcard characters? false

-ScanResultsContainerName <System.String>

The name of the storage container that will hold the scan results.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-StorageAccountName <System.String>

The name of the storage account that will hold the scan results.

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
- Microsoft.Azure.Commands.Sql.VulnerabilityAssessment.Model.VulnerabilityAssessmentSettingsModel
- System.Uri
- Microsoft.Azure.Commands.Sql.VulnerabilityAssessment.Model.RecurringScansInterval
- System.Boolean
- System.String[]

OUTPUTS

NOTES

Example 1: Update Vulnerability Assessment settings with storage account name

```
Update-AzSqlInstanceDatabaseVulnerabilityAssessmentSetting `
  -ResourceGroupName "ResourceGroup01" `
  -InstanceName "ManagedInstance01" `
  -DatabaseName "Database01" `
  -StorageAccountName "mystorage" `
  -ScanResultsContainerName "vulnerability-assessment" `
  -RecurringScansInterval Weekly `
  -EmailAdmins $true `
  -NotificationEmail @"("mail1@mail.com" , "mail2@mail.com")
```

```
ResourceGroupName : ResourceGroup01
InstanceName      : ManagedInstance01
DatabaseName      : Database01
StorageAccountName : mystorage
ScanResultsContainerName : vulnerability-assessment
RecurringScansInterval : Weekly
EmailAdmins       : True
NotificationEmail  : {mail1@mail.com , mail2@mail.com}
```

Example 2: Update Vulnerability Assessment settings with blob storage SAS URI

Update-AzSqlInstanceDatabaseVulnerabilityAssessmentSetting `

```
-ResourceGroupName "ResourceGroup01" `
-InstanceName "ManagedInstance01" `
-DatabaseName "Database01" `
-BlobStorageSasUri "https://mystorage.blob.core.windows.net/vulnerability-assessment?st=XXXXXX" `
-RecurringScansInterval Weekly `
-EmailAdmins $true `
-NotificationEmail @"("mail1@mail.com" , "mail2@mail.com")
```

ResourceGroupName : ResourceGroup01

InstanceName : ManagedInstance01

DatabaseName : Database01

StorageAccountName : mystorage

ScanResultsContainerName : vulnerability-assessment

RecurringScansInterval : Weekly

EmailAdmins : True

NotificationEmail : {mail1@mail.com , mail2@mail.com}

Example 3: Update the Vulnerability Assessment settings from ManagedDatabaseVulnerabilityAssessmentSettingsModel
instance definition

Update-AzSqlInstanceDatabaseVulnerabilityAssessmentSetting `

```
-ResourceGroupName "ResourceGroup01" `
-InstanceName "ManagedInstance01" `
-DatabaseName "Database01" `
-StorageAccountName "mystorage" `
-ScanResultsContainerName "vulnerability-assessment" `
-RecurringScansInterval Weekly `
-EmailAdmins $true `
```

-NotificationEmail @"(\"mail1@mail.com\" , \"mail2@mail.com\")

Get-AzSqlInstanceDatabaseVulnerabilityAssessmentSetting `

-ResourceGroupName "ResourceGroup01" `

-InstanceName "ManagedInstance01" `

-DatabaseName "Database01"

| Update-AzSqlInstanceDatabaseVulnerabilityAssessmentSetting `

-ResourceGroupName "ResourceGroup02" `

-InstanceName "ManagedInstance02" `

-DatabaseName "Database02"

ResourceGroupName : ResourceGroup02

InstanceName : ManagedInstance02

DatabaseName : Database02

StorageAccountName : mystorage

ScanResultsContainerName : vulnerability-assessment

RecurringScansInterval : Weekly

EmailAdmins : True

NotificationEmail : {mail1@mail.com , mail2@mail.com}

This command updated the Vulnerability Assessment settings on Database02 from the settings on Database01

Example 4: Update the Vulnerability Assessment settings on all the databases under a managed instance

Get-AzSqlInstanceDatabase -ResourceGroupName "ResourceGroup01" `

-InstanceName \$"ManagedInstance01" `

| Where-Object {\$_.Name -ne "master"} `

| Update-AzSqlInstanceDatabaseVulnerabilityAssessmentSetting `

-StorageAccountName "mystorage" `

-ScanResultsContainerName "vulnerability-assessment" `

-RecurringScansInterval Weekly `

-EmailAdmins \$true `

-NotificationEmail @"mail1@mail.com" , "mail2@mail.com")

ResourceGroupName : ResourceGroup01
InstanceName : ManagedInstance01
DatabaseName : Database01
StorageAccountName : mystorage
ScanResultsContainerName : vulnerability-assessment
RecurringScansInterval : Weekly
EmailAdmins : True
NotificationEmail : {mail1@mail.com , mail2@mail.com}

ResourceGroupName : ResourceGroup01
InstanceName : ManagedInstance01
DatabaseName : Database02
StorageAccountName : mystorage
ScanResultsContainerName : vulnerability-assessment
RecurringScansInterval : Weekly
EmailAdmins : True
NotificationEmail : {mail1@mail.com , mail2@mail.com}

This command updates all Vulnerability Assessment settings on all the databases under ManagedInstance01

RELATED LINKS

Online

Version:

<https://learn.microsoft.com/powershell/module/az.sql/update-azsqlinstancedatabasevulnerabilityassessmentsetting>