



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

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

NAME

Set-AzSqlDatabaseAudit

SYNOPSIS

Changes the auditing settings for an Azure SQL Database.

SYNTAX

```
Set-AzSqlDatabaseAudit [-ResourceGroupName] <System.String> [-ServerName] <System.String> [-DatabaseName]
<System.String> [-AuditAction <System.String[]>]
                        [-AuditActionGroup {BATCH_STARTED_GROUP | BATCH_COMPLETED_GROUP |
APPLICATION_ROLE_CHANGE_PASSWORD_GROUP | BACKUP_RESTORE_GROUP |
DATABASE_LOGOUT_GROUP |
DATABASE_OBJECT_CHANGE_GROUP | DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP |
DATABASE_OBJECT_PERMISSION_CHANGE_GROUP | DATABASE_OPERATION_GROUP |
DATABASE_PERMISSION_CHANGE_GROUP | DATABASE_PRINCIPAL_CHANGE_GROUP |
DATABASE_PRINCIPAL_IMPERSONATION_GROUP | DATABASE_ROLE_MEMBER_CHANGE_GROUP |
FAILED_DATABASE_AUTHENTICATION_GROUP | SCHEMA_OBJECT_ACCESS_GROUP |
SCHEMA_OBJECT_CHANGE_GROUP | SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP |
SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP | SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP |
```

USER_CHANGE_PASSWORD_GROUP | LEDGER_OPERATION_GROUP | DBCC_GROUP |
 DATABASE_OWNERSHIP_CHANGE_GROUP | DATABASE_CHANGE_GROUP}} [-BlobStorageTargetState {Enabled | Disabled}] [-DefaultProfile
 <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>
 [-EventHubAuthorizationRuleResourceId <System.String>] [-EventHubName
 <System.String>] [-EventHubTargetState {Enabled | Disabled}] [-LogAnalyticsTargetState {Enabled | Disabled}]
 [-PassThru] [-PredicateExpression <System.String>]
 [-RetentionInDays <System.Nullable`1[System.UInt32]>] [-StorageAccountResourceId <System.String>]
 [-StorageKeyType {Primary | Secondary}] [-UseIdentity
 <System.String>] [-WorkspaceResourceId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

Set-AzSqlDatabaseAudit [-AuditAction <System.String[]>] [-AuditActionGroup {BATCH_STARTED_GROUP |
 BATCH_COMPLETED_GROUP | APPLICATION_ROLE_CHANGE_PASSWORD_GROUP |
 BACKUP_RESTORE_GROUP | DATABASE_LOGOUT_GROUP | DATABASE_OBJECT_CHANGE_GROUP |
 DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP | DATABASE_OBJECT_PERMISSION_CHANGE_GROUP |
 DATABASE_OPERATION_GROUP | DATABASE_PERMISSION_CHANGE_GROUP |
 DATABASE_PRINCIPAL_CHANGE_GROUP | DATABASE_PRINCIPAL_IMPERSONATION_GROUP |
 DATABASE_ROLE_MEMBER_CHANGE_GROUP | FAILED_DATABASE_AUTHENTICATION_GROUP |
 SCHEMA_OBJECT_ACCESS_GROUP | SCHEMA_OBJECT_CHANGE_GROUP |
 SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP | SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP |
 SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP | USER_CHANGE_PASSWORD_GROUP |
 LEDGER_OPERATION_GROUP | DBCC_GROUP | DATABASE_OWNERSHIP_CHANGE_GROUP |
 DATABASE_CHANGE_GROUP}}] [-BlobStorageTargetState {Enabled | Disabled}] -DatabaseObject
 <Microsoft.Azure.Commands.Sql.Database.Model.AzureSqlDatabaseModel> [-DefaultProfile
 <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>
 [-EventHubAuthorizationRuleResourceId <System.String>] [-EventHubName
 <System.String>] [-EventHubTargetState {Enabled | Disabled}] [-LogAnalyticsTargetState {Enabled | Disabled}]
 [-PassThru] [-PredicateExpression <System.String>]
 [-RetentionInDays <System.Nullable`1[System.UInt32]>] [-StorageAccountResourceId <System.String>]
 [-StorageKeyType {Primary | Secondary}] [-UseIdentity
 <System.String>] [-WorkspaceResourceId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Set-AzSqlDatabaseAudit cmdlet changes the auditing settings of an Azure SQL Database. To use the cmdlet, use the ResourceGroupName , ServerName , and DatabaseName

parameters to identify the database. When blob storage is a destination for audit logs, specify the StorageAccountResourceId parameter to determine the storage

account for the audit logs and the StorageKeyType parameter to define the storage keys. You can also define retention for the audit logs by setting the value of the

RetentionInDays parameter to define the period for the audit logs.

PARAMETERS

-AuditAction <System.String[]>

The set of audit actions.

The supported actions to audit are:

SELECT

UPDATE

INSERT

DELETE

EXECUTE

RECEIVE

REFERENCES

The general form for defining an action to be audited is: [action] ON [object] BY [principal] Note that [object] in the above format can refer to an object like a

table, view, or stored procedure, or an entire database or schema. For the latter cases, the forms DATABASE::[dbname] and SCHEMA::[schemaname] are used,

respectively. For example:

SELECT on dbo.myTable by public

SELECT on DATABASE::myDatabase by public

SELECT on SCHEMA::mySchema by public

For more information, see

<https://learn.microsoft.com/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions#database-level-audit-actions>.

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

-AuditActionGroup <Microsoft.Azure.Commands.Sql.Auditing.Model.AuditActionGroups[]>

The recommended set of action groups to use is the following combination - this will audit all the queries and stored procedures executed against the database, as well as successful and failed logins:

```
"BATCH_COMPLETED_GROUP",  
"SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP",  
"FAILED_DATABASE_AUTHENTICATION_GROUP"
```

This above combination is also the set that is configured by default. These groups cover all SQL statements and stored procedures executed against the database,

and should not be used in combination with other groups as this will result in duplicate audit logs. For more information, see

<https://learn.microsoft.com/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions#database-level-audit-action-groups>.

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

-BlobStorageTargetState <System.String>

Indicates whether blob storage is a destination for audit records.

Required?	false
-----------	-------

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

-DatabaseName <System.String>

SQL Database name.

Required? true
Position? 2
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-DatabaseObject <Microsoft.Azure.Commands.Sql.Database.Model.AzureSqlDatabaseModel>

The database object to manage its audit policy.

Required? true
Position? named
Default value None
Accept pipeline input? True (ByValue)
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

-EventHubAuthorizationRuleResourceId <System.String>

The resource Id for the event hub authorization rule

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

-EventHubName <System.String>

The name of the event hub. If none is specified when providing EventHubAuthorizationRuleResourceId, the default event hub will be selected.

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

-EventHubTargetState <System.String>

Indicates whether event hub is a destination for audit records.

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

-LogAnalyticsTargetState <System.String>

Indicates whether log analytics is a destination for audit records.

Required?	false
Position?	named
Default value	None

Accept pipeline input? False

Accept wildcard characters? false

-PassThru <System.Management.Automation.SwitchParameter>

Specifies whether to output the auditing policy at end of cmdlet execution

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-PredicateExpression <System.String>

The T-SQL predicate (WHERE clause) used to filter audit logs.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceGroupName <System.String>

The name of the resource group.

Required? true

Position? 0

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RetentionInDays <System.Nullable`1[System.UInt32]>

The number of retention days for the audit logs.

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

-ServerName <System.String>

SQL server name.

Required? true
Position? 1
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-StorageAccountResourceId <System.String>

The storage account resource id

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

-StorageKeyType <System.String>

Specifies which of the storage access keys to use.

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

-UseIdentity <System.String>

Indicates whether to use managed identity or not. It is required when you want to use managed identity while target storage is not behind firewall.

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

-WorkspaceResourceId <System.String>

The workspace ID (resource ID of a Log Analytics workspace) for a Log Analytics workspace to which you would like to send Audit Logs. Example:

/subscriptions/4b9e8510-67ab-4e9a-95a9-e2f1e570ea9c/resourceGroups/insights-integration/providers/Microsoft.Operation
allInsights/workspaces/viruela2

Required?	false
Position?	named
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

System.String

Microsoft.Azure.Commands.Sql.Database.Model.AzureSqlDatabaseModel

Microsoft.Azure.Commands.Sql.Auditing.Model.AuditActionGroups[]

System.String[]

System.Guid

Microsoft.Azure.Commands.Sql.Auditing.Model.DatabaseAuditModel

OUTPUTS

System.Boolean

NOTES

Example 1: Enable the blob storage auditing policy of an Azure SQL Database

```
Set-AzSqlDatabaseAudit -ResourceGroupName "ResourceGroup01" -ServerName "Server01" -DatabaseName  
"Database01" -BlobStorageTargetState Enabled  
-StorageAccountResourceId  
"/subscriptions/7fe3301d-31d3-4668-af5e-211a890ba6e3/resourceGroups/resourcegroup01/providers/Microsoft.Storage/sto  
rageAccounts/mystorage"
```

Example 2: Disable the blob storage auditing policy of an Azure SQL Database

```
Set-AzSqlDatabaseAudit -ResourceGroupName "ResourceGroup01" -ServerName "Server01" -DatabaseName  
"Database01" -BlobStorageTargetState Disabled
```

Example 3: Enable the blob storage auditing policy of an Azure SQL Database with filtering using a T-SQL predicate

```
Set-AzSqlDatabaseAudit -ResourceGroupName "ResourceGroup01" -ServerName "Server01" -DatabaseName  
"Database01" -PredicateExpression "schema_name <> 'sys'"  
-BlobStorageTargetState Enabled -StorageAccountResourceId  
"/subscriptions/7fe3301d-31d3-4668-af5e-211a890ba6e3/resourceGroups/resourcegroup01/providers/Microsoft.Storage/sto  
rageAccounts/mystorage"
```

Example 4: Remove the filtering from the auditing policy of an Azure SQL Database

```
Set-AzSqlDatabaseAudit -ResourceGroupName "ResourceGroup01" -ServerName "Server01" -DatabaseName  
"Database01" -PredicateExpression ""
```

Example 5: Enable the event hub auditing policy of an Azure SQL Database

```
Set-AzSqlDatabaseAudit -ResourceGroupName "ResourceGroup01" -ServerName "Server01" -DatabaseName  
"Database01" -EventHubTargetState Enabled -EventHubName  
"EventHubName" -EventHubAuthorizationRuleResourceId "EventHubAuthorizationRuleResourceId"
```

Example 6: Disable the event hub auditing policy of an Azure SQL Database

```
Set-AzSqlDatabaseAudit -ResourceGroupName "ResourceGroup01" -ServerName "Server01" -DatabaseName
```

"Database01" -EventHubTargetState Disabled

Example 7: Enable the log analytics auditing policy of an Azure SQL Database

```
Set-AzSqlDatabaseAudit -ResourceGroupName "ResourceGroup01" -ServerName "Server01" -DatabaseName  
"Database01" -LogAnalyticsTargetState Enabled -WorkspaceResourceId
```

```
"/subscriptions/4b9e8510-67ab-4e9a-95a9-e2f1e570ea9c/resourceGroups/insights-integration/providers/Microsoft.Operation  
nalInsights/workspaces/viruela2"
```

Example 8: Disable the log analytics auditing policy of an Azure SQL Database

```
Set-AzSqlDatabaseAudit -ResourceGroupName "ResourceGroup01" -ServerName "Server01" -DatabaseName  
"Database01" -LogAnalyticsTargetState Disabled
```

Example 9: Disable, through pipeline, the log analytics auditing policy of an Azure SQL Database

```
Get-AzSqlDatabase -ResourceGroupName "ResourceGroup01" -ServerName "Server01" -DatabaseName "Database01"  
| Set-AzSqlDatabaseAudit -LogAnalyticsTargetState Disabled
```

Example 10: Disable sending audit records of an Azure SQL Database to blob storage, and enable sending them to log

analytics.

```
Set-AzSqlDatabaseAudit -ResourceGroupName "ResourceGroup01" -ServerName "Server01" -DatabaseName  
"Database01" -LogAnalyticsTargetState Enabled -WorkspaceResourceId  
"/subscriptions/4b9e8510-67ab-4e9a-95a9-e2f1e570ea9c/resourceGroups/insights-integration/providers/Microsoft.OperationInsights/workspaces/viruela2"  
-BlobStorageTargetState Disabled
```

Example 11: Enable sending audit records of an Azure SQL Database to blob storage, event hub and log analytics.

```
Set-AzSqlDatabaseAudit -ResourceGroupName "ResourceGroup01" -ServerName "Server01" -DatabaseName  
"Database01" -BlobStorageTargetState Enabled  
-StorageAccountResourceId  
"/subscriptions/7fe3301d-31d3-4668-af5e-211a890ba6e3/resourceGroups/resourcegroup01/providers/Microsoft.Storage/storageAccounts/mystorage"  
-EventHubTargetState Enabled -EventHubName "EventHubName" -EventHubAuthorizationRuleResourceId  
"EventHubAuthorizationRuleResourceId" -LogAnalyticsTargetState Enabled  
-WorkspaceResourceId  
"/subscriptions/4b9e8510-67ab-4e9a-95a9-e2f1e570ea9c/resourceGroups/insights-integration/providers/Microsoft.OperationInsights/workspaces/viruela2"
```

RELATED LINKS

Online Version: <https://learn.microsoft.com/powershell/module/az.sql/Set-AzSqlDatabaseAudit>

