Recast

# Event Collector

Last Modified on 2026-11-02

## Get-LiquitEventCollector

This command displays a list of all event collectors known within the Application Workspace or you can just select one in particular.

### Syntax

```
Get-LiquitEventCollector
   [-LiquitContext <LiquitContext>]
   [<CommonParameters>]

Get-LiquitEventCollector
   [-ID] <guid[]>
   [-LiquitContext <LiquitContext>]
   [<CommonParameters>]

 Get-LiquitEventCollector
   [-EntityRef] <EntityRef[]>
   [-LiquitContext <LiquitContext>]
   [<CommonParameters>]

Get-LiquitEventCollector
   [-Type] <string[]>
   [-LiquitContext <LiquitContext>]
   [<CommonParameters>]

Get-LiquitEventCollector
   [-Search] <string>
   [-LiquitContext <LiquitContext>]
   [<CommonParameters>]

Get-LiquitEventCollector
   [-Name] <string>
   [-LiquitContext <LiquitContext>]
   [<CommonParameters>]
```

### Parameters

| Name | Value | Description | Required | Default value |
|---|---|---|---|---|
| Type | `{microsoftsentinel\|splunk}` | The type of the collector for SIEM. | Yes | |

| Name | Value | Description | Required | Default value |
|---|---|---|---|---|
| Search | `<string>` | This parameter serves a similar purpose to the search box found in the event collectors table from the Application Workspace UI. It enables users to search multiple columns within the table, such as Name and Type. When a search term is provided, the parameter filters records by matching values in these indexed columns. However, it's important to note that not all columns in the table are indexed, meaning that searches for values in these non-indexed columns will not return results. Non-indexed columns include for example the ID and columns containing checkboxes. | | |
| Name | `<string>` | Searches on the event collector name itself. | | |
| LiquitContext | `<LiquitContext>` | Determines the selected zone. | No | Default |

---

## New-LiquitEventCollector

This command creates a new event collector.

### Syntax

For Microsoft Azure Sentinel:

```
New-LiquitEventCollector
   [-Type microsoftsentinel]
   [-Name] <string>
   [-Enabled] <boolean>
   [-WorkspaceId] <string>
   [-Key] <string>
   [-Description <string>]
   [-Filters {UserLogin | DistributePackage | LaunchPackage | InstallPackage | UninstallPackage | UserLogoff | RepairPackage | InstallDeployment | RestCreate| RestUpdate | RestDelete | RestAdd | RestRemove | RestAction} ]
   [-LiquitContext <LiquitContext>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

For Splunk:

```
New-LiquitEventCollector
   [-Type splunk]
   [-Name] <string>
   [-Enabled] <boolean>
   [-AccessToken] <string>
   [-Uri] <string>
   [-Description <string>]
   [-Filters {UserLogin | DistributePackage | LaunchPackage | InstallPackage | UninstallPackage | UserLogoff | RepairPackage | InstallDeployment | RestCreate| RestUpdate | RestDelete | RestAdd | RestRemove | RestAction} ]
   [-ClientCertificate <Certificate>]
   [-LiquitContext <LiquitContext>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

## Examples

The following script creates a new Application Workspace Event Collector named "PS-Test-Splunk" that sends selected auditing and user activity events to a specified Splunk endpoint using an access token for authentication:

```
New-LiquitEventCollector -Type "Splunk" -Name "PS-Test-Splunk" -Uri "https://splunk.recastsoftware.com:9997/services/collector/event" -AccessToken "asdjhgdasjkasdjlkasd" -AuditingFilters @("RestCreate","RestUpdate","RestDelete","RestAdd","RestRemove","RestAction") -Filters @("UserLogin","UserLogoff","DistributePackage","InstallPackage","LaunchPackage","UninstallPackage","RepairPackage")
```

The following script sets up an Application Workspace Event Collector named "PS-Test-MicrosoftSentinel" that sends selected auditing and activity events to a Microsoft Sentinel workspace in the Azure public cloud, using a workspace ID and key for authentication.

```
New-LiquitEventCollector -Type MicrosoftSentinel -Name "PS-Test-MicrosoftSentinel" -LocationType 'Azure public cloud' -WorkspaceId "d7a6bca9-45cf-4136-afd0-89fbb6981b30" -Key "jVxR8DtFCDBgNDQIv0Lo//InzufMzTMgM0CirEMaHAdFHn9X8LuKmuf59G0TK2uCGI8VrelAakD1iya+uW7ptQ==" -AuditingFilters @("RestCreate","RestUpdate","RestDelete","RestAdd","RestRemove","RestAction") -Filters @("UserLogin","UserLogoff","DistributePackage","InstallPackage","LaunchPackage","UninstallPackage","RepairPackage")
```

## Parameters

| Name | Value | Description | Required | Default value |
|---|---|---|---|---|
| Type | `{microsoftsentinel\|splunk}` | The type of the collector for SIEM. | Yes | |
| Name | `<string>` | Provide a name for the collector. | Yes | |
| Enabled | `<boolean>` | Determines whether or not the collector is enabled. | Yes | |
| WorkspaceId | `<string>` | The ID of your Microsoft Log Analytics workspace. | Yes | |
| AccessToken | `<string>` | The authentication token that grants access to a Splunk platform instance. | Yes | |

| Name | Value | Description | Required | Default value |
|---|---|---|---|---|
| URI | `<string>` | The address of the Splunk server. | Yes | |
| Key | `<string>` | The primary key associated with your Microsoft Log Analytics workspace. | Yes | |
| Description | `<string>` | The description of the collector. | No | |
| Filters | `UserLogin \| DistributePackage \| LaunchPackage \| InstallPackage \| UninstallPackage \| UserLogoff \|RepairPackage \| InstallDeployment \| RestCreate \| RestUpdate \| RestDelete \| RestAdd \| RestRemove \| RestAction` | The types of events you want to send to the SIEM. | No | |
| LiquitContext | `<LiquitContext>` | Determines the selected zone. | No | Default |

## Set-LiquitEventCollector

```
Set-LiquitEventCollector
   [-EventCollector] <EventCollector[]>
   [-AccessToken <string>]
   [-ClientCertificate <Certificate>]
   [-Description <string>]
   [-Enabled <bool>]
   [-Filters {UserLogin | DistributePackage | LaunchPackage | InstallPackage | UninstallPackage | UserLogoff | RepairPackage | InstallDeployment | RestCreate| RestUpdate | RestDelete | RestAdd | RestRemove | RestAction} ]
   [-AuditingFilters {RestCreate | RestUpdate | RestDelete | RestAdd | RestRemove | RestAction}]
   [-EventTags <hashtable>]
   [-Name <string>]
   [-Key <string>]
   [-Uri <string>]
   [-WorkspaceId <string>]
   [-LiquitContext <LiquitContext>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

### Parameters

| Name | Value | Description | Required | Default value |
|---|---|---|---|---|
| EventCollector | `<EventCollector[]>` | The type of the collector for SIEM. | Yes | |
| Filters | `UserLogin \| DistributePackage \| LaunchPackage \| InstallPackage \| UninstallPackage \| UserLogoff \|RepairPackage \| InstallDeployment \| RestCreate \| RestUpdate \| RestDelete \| RestAdd \| RestRemove \| RestAction` | The types of events you want to send to the SIEM. | No | |

| Name | Value | Description | Required | Default value |
|---|---|---|---|---|
| AuditingFilters | `RestCreate \| RestUpdate \| RestDelete \| RestAdd \| RestRemove \| RestAction` | The type of entities you want to audit. For more information, see Auditing. | No | |
| LiquitContext | `<LiquitContext>` | Determines the selected zone. | No | Default |

### See also

Event Collectors

## Remove-LiquitEventCollector

This command removes an event collector.

```
Remove-LiquitEventCollector
   [-EventCollector] <EventCollector[]>
   [-LiquitContext <LiquitContext>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

### Parameters

| Name | Value | Description | Required | Default value |
|---|---|---|---|---|
| EventCollector | `<EventCollector[]>` | The type of the collector for SIEM. | Yes | |
| LiquitContext | `<LiquitContext>` | Determines the selected zone. | No | Default |