Recast

Event Collectors

Last Modified on 04.16.26

> The Access Manager license is required for this feature.

A Security Information and Event Management (SIEM) solution aggregates, consolidates and sorts your data, identify threats, verifies data compliance and quickly responds to potential threats that would otherwise disrupt the business operations of your company.

The event collector functionality lets you send out events information to the Splunk and Microsoft Sentinel external SIEM systems.

Event collectors list

The first row in the event collector list represents the database overview, with all the information that is collected according to your configurations. No changes can be made to it.

Selecting multiple rows from the table

- To select multiple adjacent rows, click on the first row, then hold down the Shift key and click on the last row in the range; all rows between will be selected.
- To select multiple non-adjacent rows, hold down the Ctrl key (or "Command" on Mac) and click on each row you want to select individually.
- To select multiple adjacent rows using the mouse only, click and hold the left mouse button on the first row, then drag the cursor up or down across the rows to highlight the desired ones.
- Selecting rows using only the keyboard is not possible.

Table toolbar

To create a new event collector, click on the **Create** button; to view the details of an event collector or edit it, double-click its entry or select the event collector and click the **Edit** button.

Views gives you control on how the table is displayed.
The default view contains all your event collectors in alphabetic ascending order, and the following columns: **Name**, **Type** and **Enabled**.
You can create your own personalized view of the table, by filtering the event collectors or adding/deleting columns and clicking **Save as** in the drop-down menu of **Views**.

Detailed view of an event collector

See below the description of each screen in the detailed view of an event collector, and what actions you can perform in each of them.

Overview screen

The overview screen provides basic information of the collector that is currently opened.

Settings screen

Recast

Microsoft Azure Sentinel

Type – The type of the Azure environment, an Azure public cloud or a custom one for a region that has their own Azure environment.
Workspace ID – The ID of your Microsoft Log Analytics workspace.
Key – The primary key associated with your Microsoft Log Analytics workspace.
URI – The address of the Microsoft Azure Sentinel server.

For more information, see Microsoft Sentinel documentation.

How to configure Microsoft Azure Sentinel

1. You need to create a Microsoft Log Analytics workspace to get a subscription and resource group.

2. In your new Log Analytics workspace go to Settings > Agent and copy the workspace id and primary key into Application Workspace.

Splunk

URI – The address of the Splunk server. Note that you must append the HTTP port number you can find in your Splunk instance > Edit global settings.
Access token – The authentication token that grants access to a Splunk platform instance. You can find in your Splunk instance > Settings > Data input > HTTP event collectors
Client certificate – The certificate must be first uploaded to Application Workspace.

How to configure Splunk

You need to insert the URI and Access token from Splunk into Application Workspace. See Splunk documentation on how to set up and use HTTP Event Collector in Splunk Web.

Event tags screen

The event tags you create are sent to Splunk where you can use them to further filter events.

Filter screen

Filter Application Workspace events that you want to add to the SIEM system(s):

- User login
- User logoff
- Distribute package
- Install package
- Launch package
- Uninstall package
- Repair package

Enable on which entities you want to track changes through auditing:

- Create – Create a new entity
- Update – Update an existing entity
- Delete – Delete an existing entity
- Add – Add a reference between entities
- Remove – Remove a reference between entities
- Action – Execute something on the server, for example export a certificate

For the PowerShell cmdlets, see Event Collector.

Recast

Auditing screen

View a comprehensive log of changes to this event collector, displaying the identity behind each modification.
This screen is available only if the auditing is enabled in the Database Event Collector. For more information, see Auditing.