

# 

# 

# Version Control

| # | Document Version | Date | Owner | Document Status | Comments |
| --- | --- | --- | --- | --- | --- |
| 1 | 3.2.0 | 03rd February 2024 | Crest Data Systems | Initial Solution |  |

# 

# Contents

[**Version Control 1**](#_30j0zll)

[**Contents**](#_46ptvxpgnbe8) **2**

[**Steps to Configure the Corelight Workbook (Dashboards)**](#_1t3h5sf) **3**

[**Steps to Install the Corelight Parsers**](#_ytzlng2dwlft) **7**

[**Steps to Update the Watchlist**](#_svx86gr9x4h8)  **8**

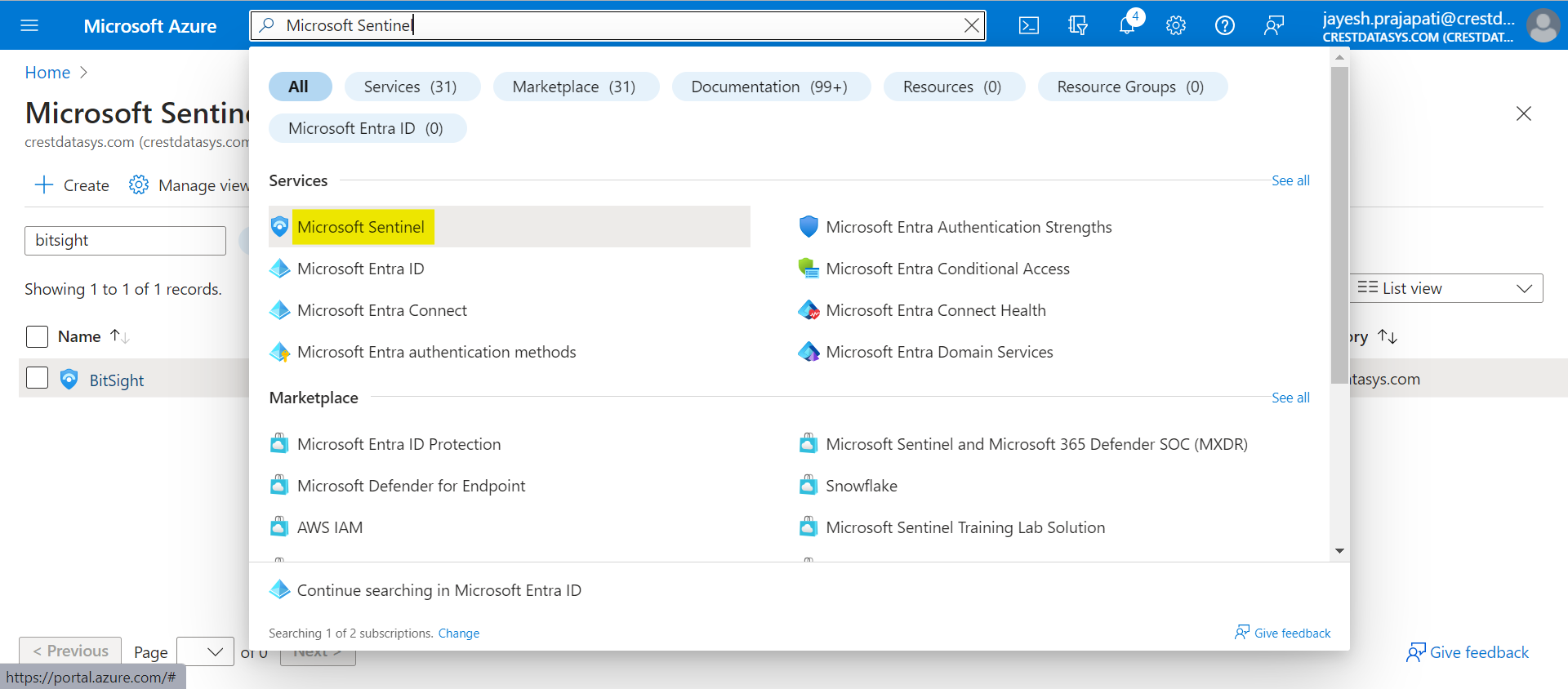
# 

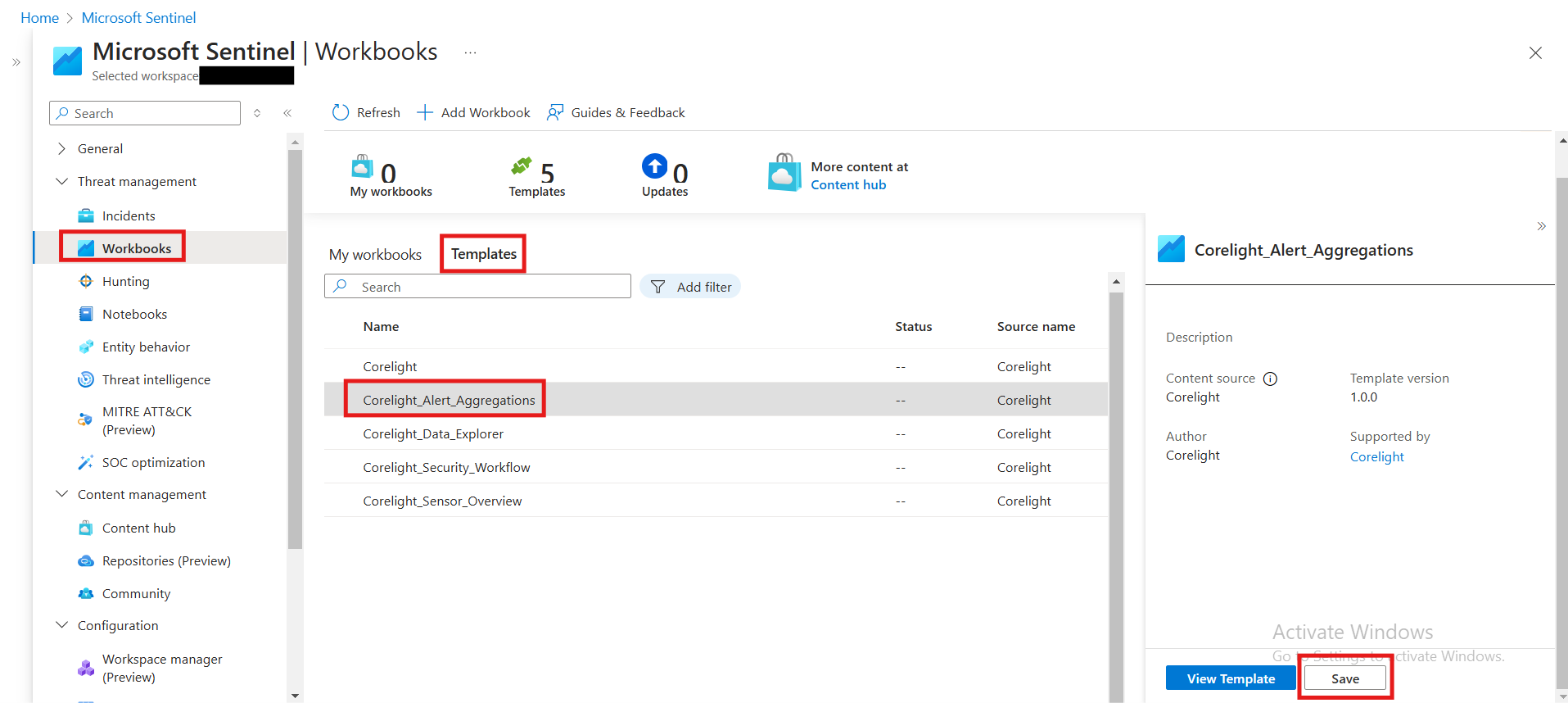
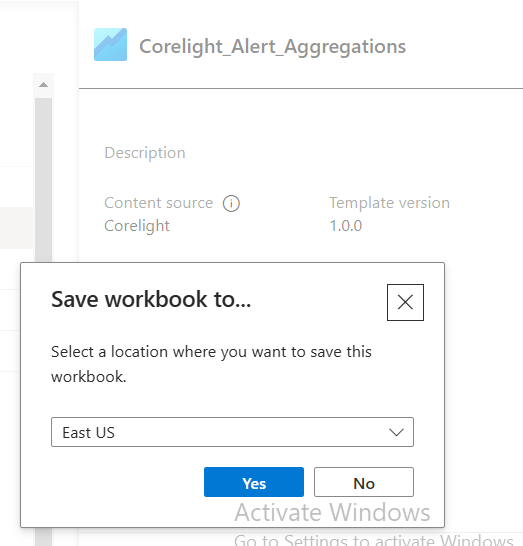
# Steps to Configure the Corelight Workbook (Dashboards)

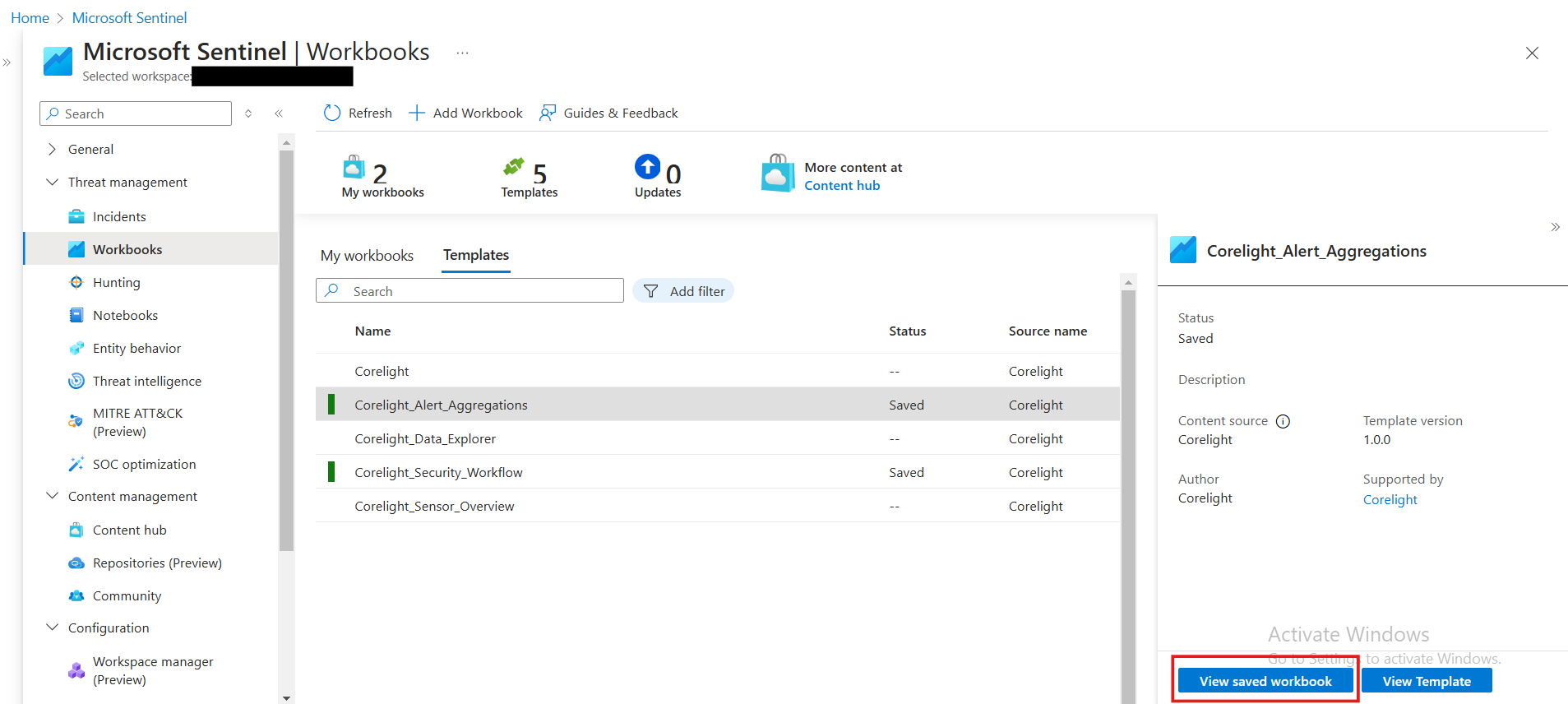
Workbooks in Microsoft Sentinel provide a flexible canvas for data analysis and the creation of rich visual reports within the Microsoft Azure portal. Corelight Sentinel offers a convenient workbook to analyze various events and logs provided by Corelight

1. There is a workbook provided in Corelight MS Sentinel.
   1. Corelight Workbook.

To install this workbook, start by navigating to the Microsoft Sentinel homepage:



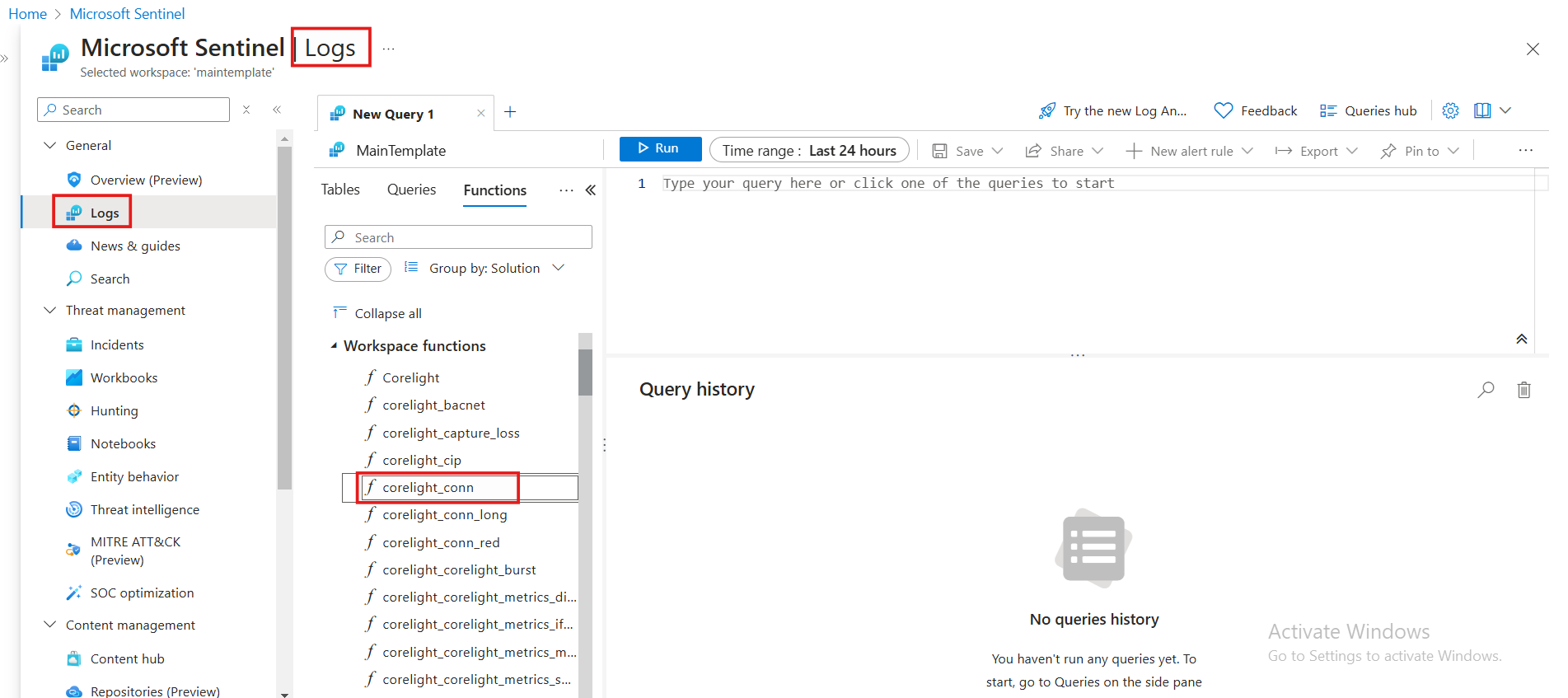
1. Now go to Microsoft Sentinel Workspace in which you have installed the template, go to Workbooks, search for the Corelight, click on installed workbook and Click on **save**.  
   ****
2. Select the location of your Microsoft Sentinel Workspace and click on **Yes**.  
   

1. After successful completion, you will be able to see the “View saved workbook” button to see the configured workbook.  
   

# Steps to Install the Corelight Parser

The **workbook** uses a parser based on a Kusto Function to normalize fields. For Corelight, it’s required to install and save all the parsers. Without a parser, the workbook won’t be able to access the ingested data.

1. Once you install the Corelight solution, all the parsers are automatically installed to their correct location, so there is no need to install them separately.  
   Note: Marked one parser - corelight\_conn for the reference

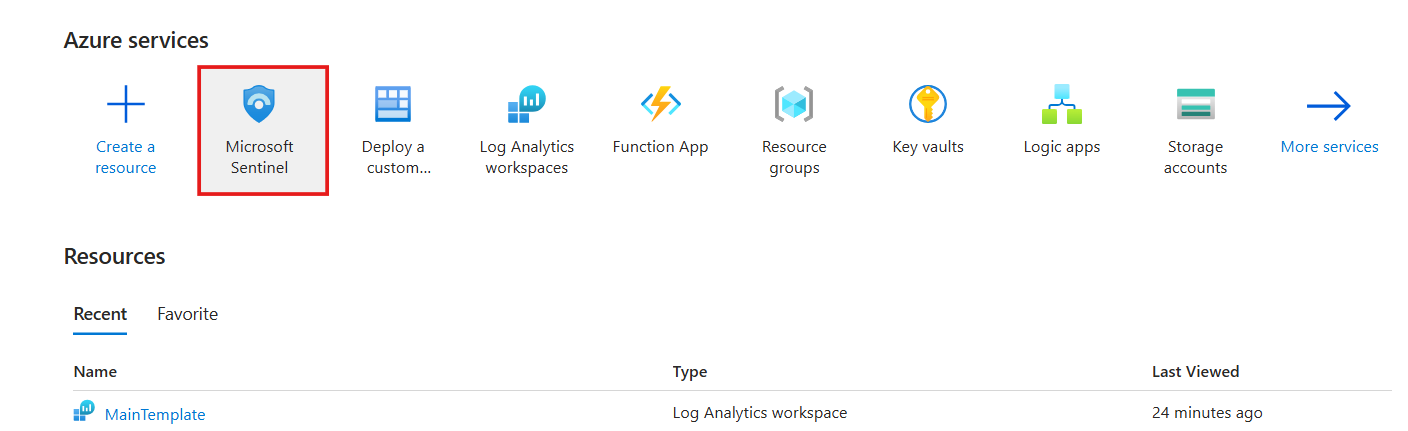


# 

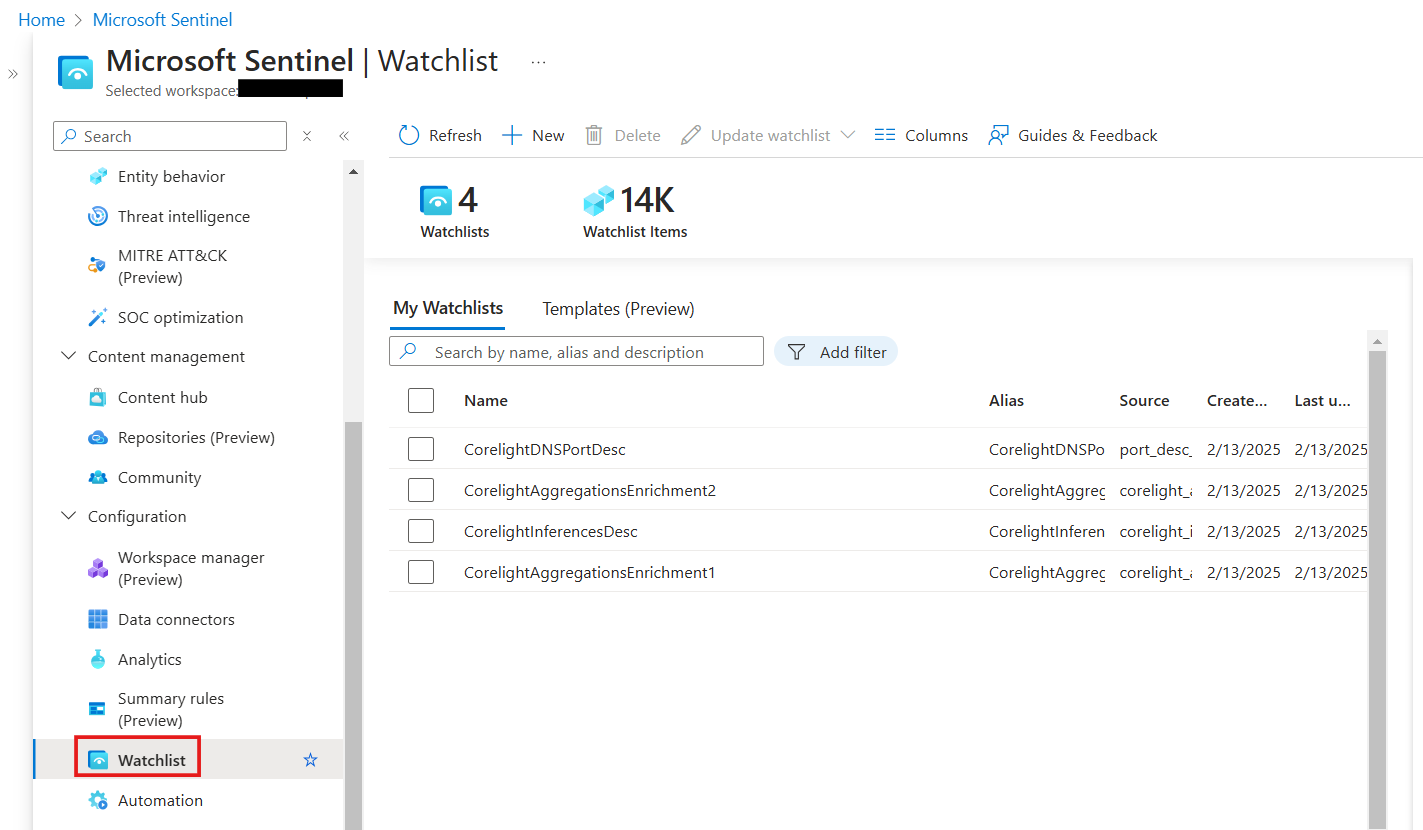
# Steps to update Watchlist

* The Watchlist in Microsoft Sentinel is used to efficiently manage and correlate data from external sources like Corelight, which provides high-fidelity network telemetry and security analytics.
* To efficiently analyze and correlate network telemetry from Corelight within Microsoft Sentinel, you can import structured CSV data into a watchlist. A watchlist enables you to store and reference external data sources.
* Once you install the Corelight solution, the temporary watchlists are automatically installed to their correct location, so there is only need to update csv files.
* Follow the mentioned steps:
  + This workbook requires you to import two CSV files into specific Watchlists:
    - corelight\_aggregations\_enrichment\_1.csv -> CorelightAggregationsEnrichment1 Watchlist
    - corelight\_aggregations\_enrichment\_2.csv -> CorelightAggregationsEnrichment2 Watchlist

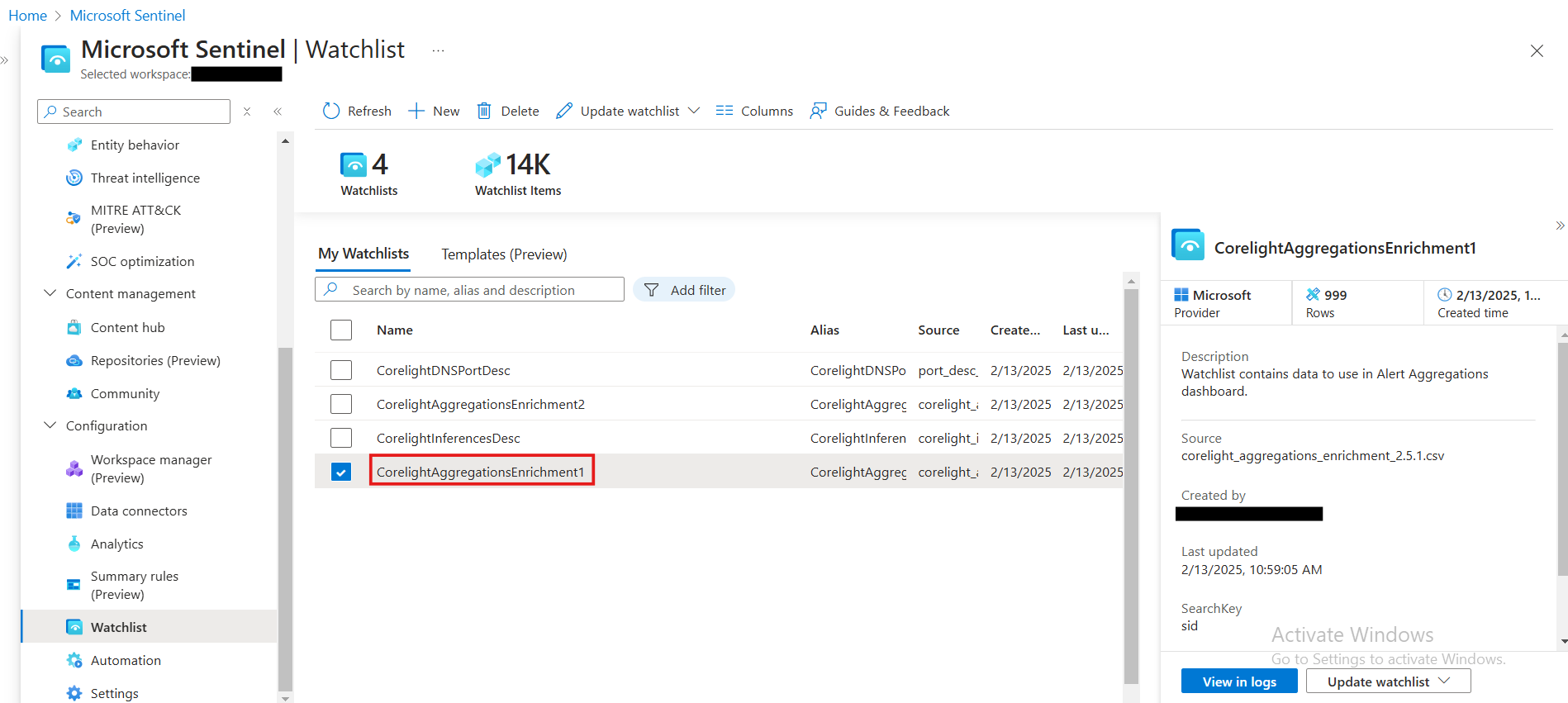
1. Navigate to the Microsoft Sentinel



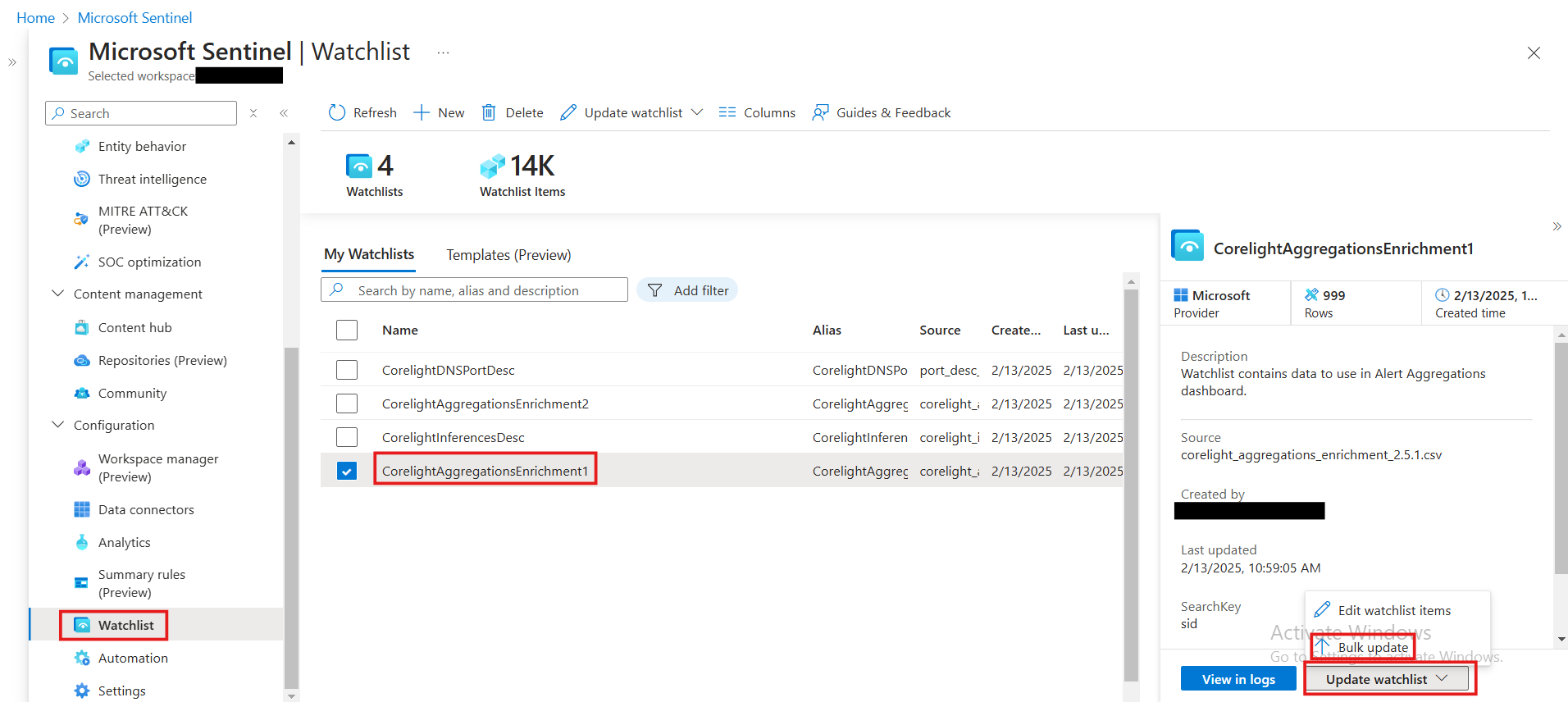
1. Search your workspace and access the Watchlists section



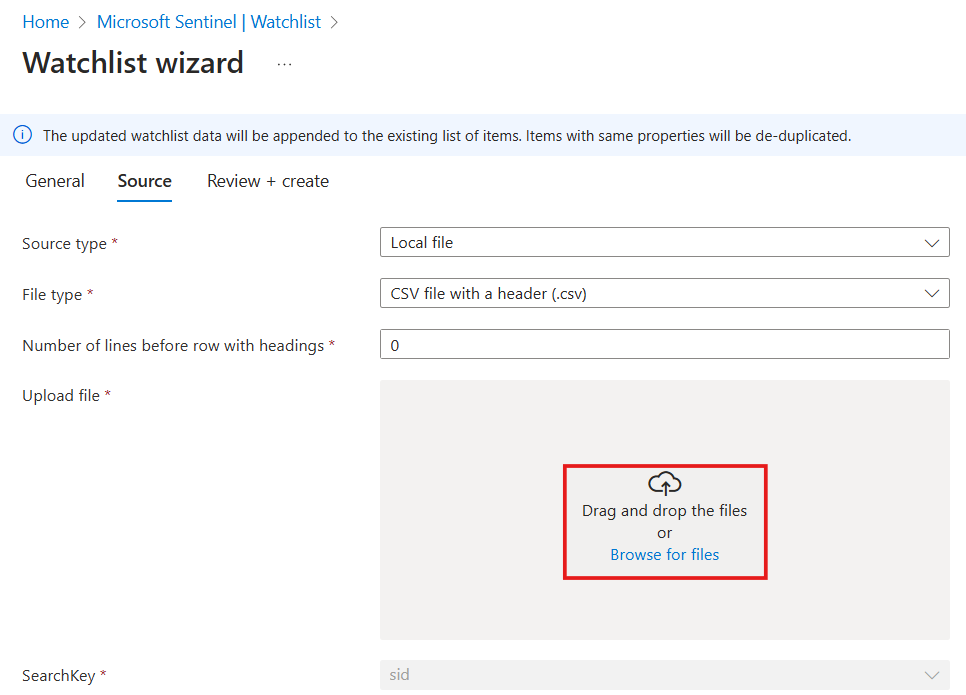
1. Select the appropriate watchlist (**CorelightAggregationsEnrichment1** or **CorelightAggregationsEnrichment2**)



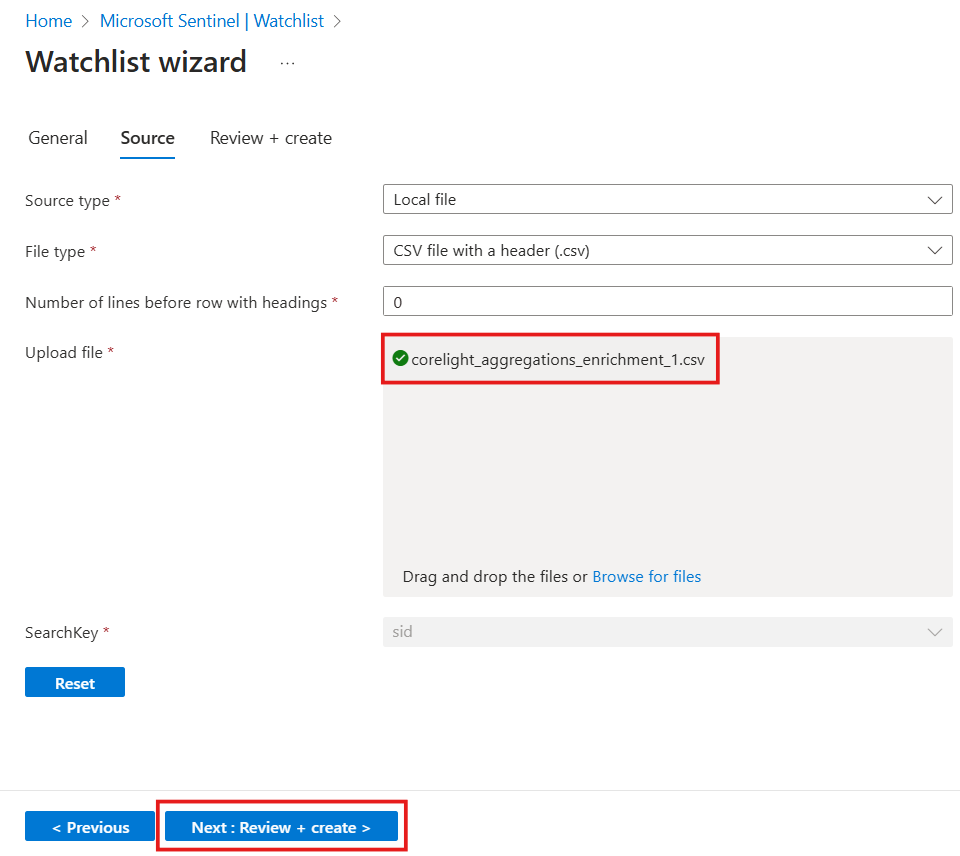
1. Choose **Update watchlis**t -> **Bulk update**



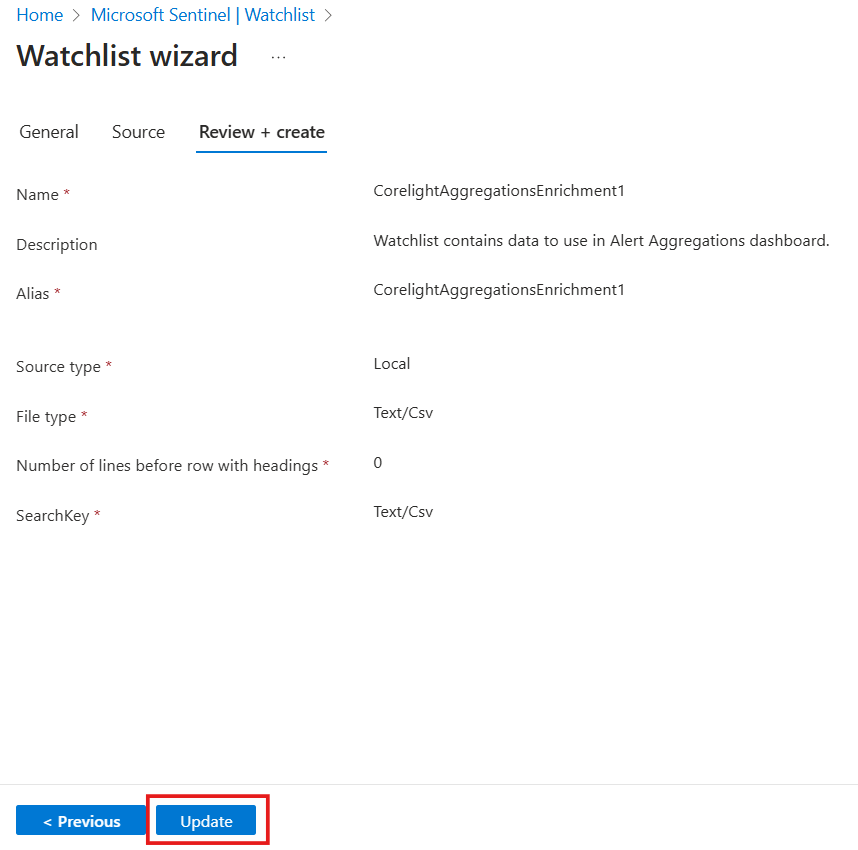
1. Upload the corresponding CSV file



1. Proceed through **Next: Review + create**



1. Finalize by clicking **Update**



# 

# Limitations

Workbook

| **Visualization/ Parameter** | **Limits** |
| --- | --- |
| Grid | Grids can display 10,000 rows at max. Any further items are ignored, and a warning appears. |
| Charts | Charts are limited to 100 series.  Charts are limited to 10,000 data points. Charts are limited to 50 segments. |
| Maps | Maps are limited to displaying 100 points. Any further items are ignored, and a warning appears. |
| Drop down (Filters) | Drop-down-based parameters are limited to 1,000 items. Any items returned by a query after that are ignored. |
| Drill down | In Time chart, it is feasible but will not get exported time accurately |

Watchlist

* A **maximum of 10,000 records** can be stored per watchlist.
* The **file size limit** for a CSV upload is **3.8 MB**.