# Search, Archive, and Restoration Preview

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

---

Product feedback channel for CSS input defined:

Please send feedback to bnick and juliango via email

Bug tracking access provided: Work item tracking is in ADO. Here is a link to the Search backlog: FEATURE 12539994 Search – Backlog. I believe you should already have access.

Real-time collaboration (dev and support) established: Here are the following contacts for the teams channel for search: Igal Shapira Igal.Shapira@microsoft.com; Snow Kang snowkang@microsoft.com; Dorian Latchague dlatchague@microsoft.com; Mohamed Rouatbi mohamedr@microsoft.com; Julian Gonzalez juliango@microsoft.com; Ben Nick bnick@microsoft.com

Product PM provides the correct escalation path from CSS to dev team (starting at Public Preview). here is our teams ICM channel contact info - Sentinel US / Hunters

## TSG

### Resolve Microsoft Sentinel Search and Restore issues

**Microsoft Sentinel Search Page – Creating a Search**

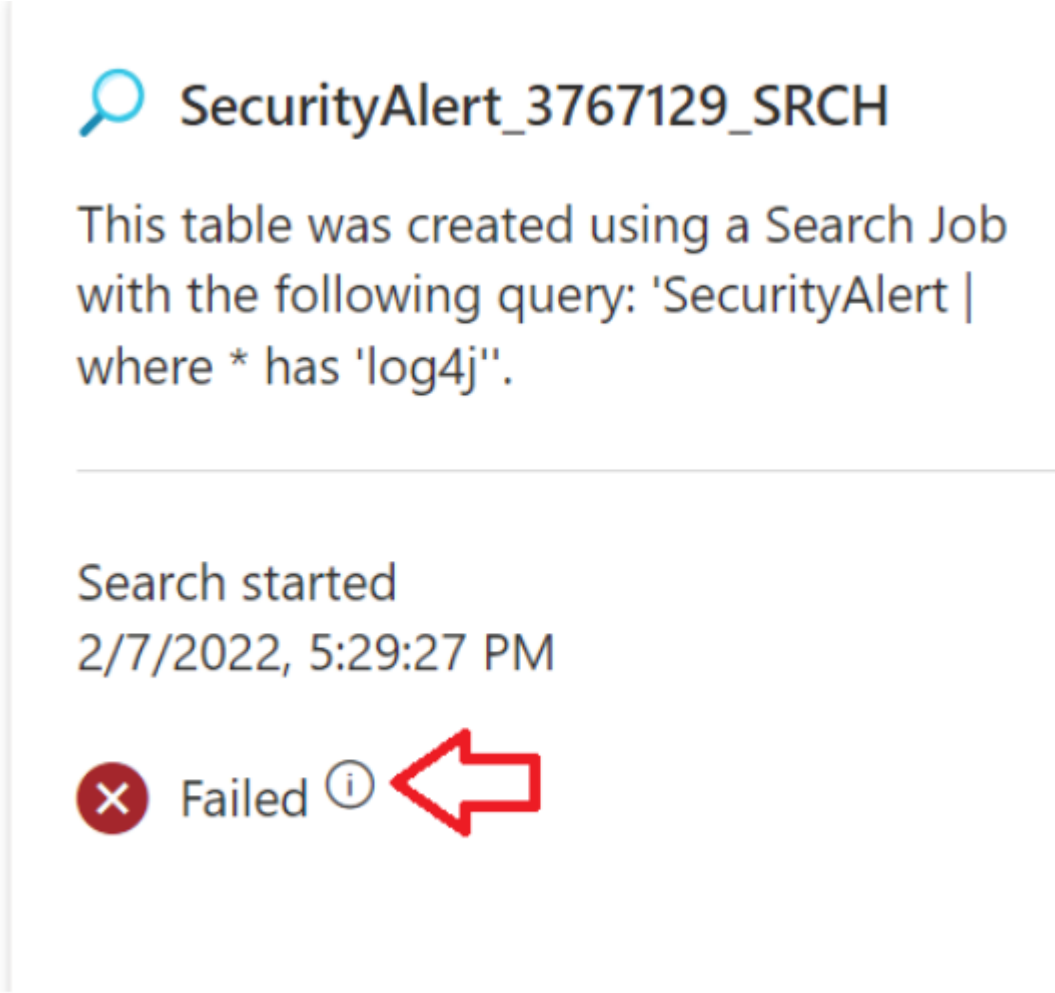
Before starting a search job, ensure you have one of the required roles: Microsoft Sentinel Contributor, Azure Monitor Contributor, or Microsoft Sentinel reader.

Search jobs are created using Azure Monitor Search Jobs. Before you start a Search job, be aware of the following limitations.

- Optimized to query one table at a time.
- Search date range is up to one year.
- Supports long running searches up to a 24-hour time-out.
- Results are limited to one million records in the record set.
- Concurrent execution is limited to five search jobs per workspace.
- Limited to 100 search results tables per workspace.
- Limited to 100 search job executions per day per workspace.

To learn more, see Search job limitations in the Azure Monitor documentation:

If you encounter a failure when creating a search job, hover your mouse over the info button next to the failure notification to get details.



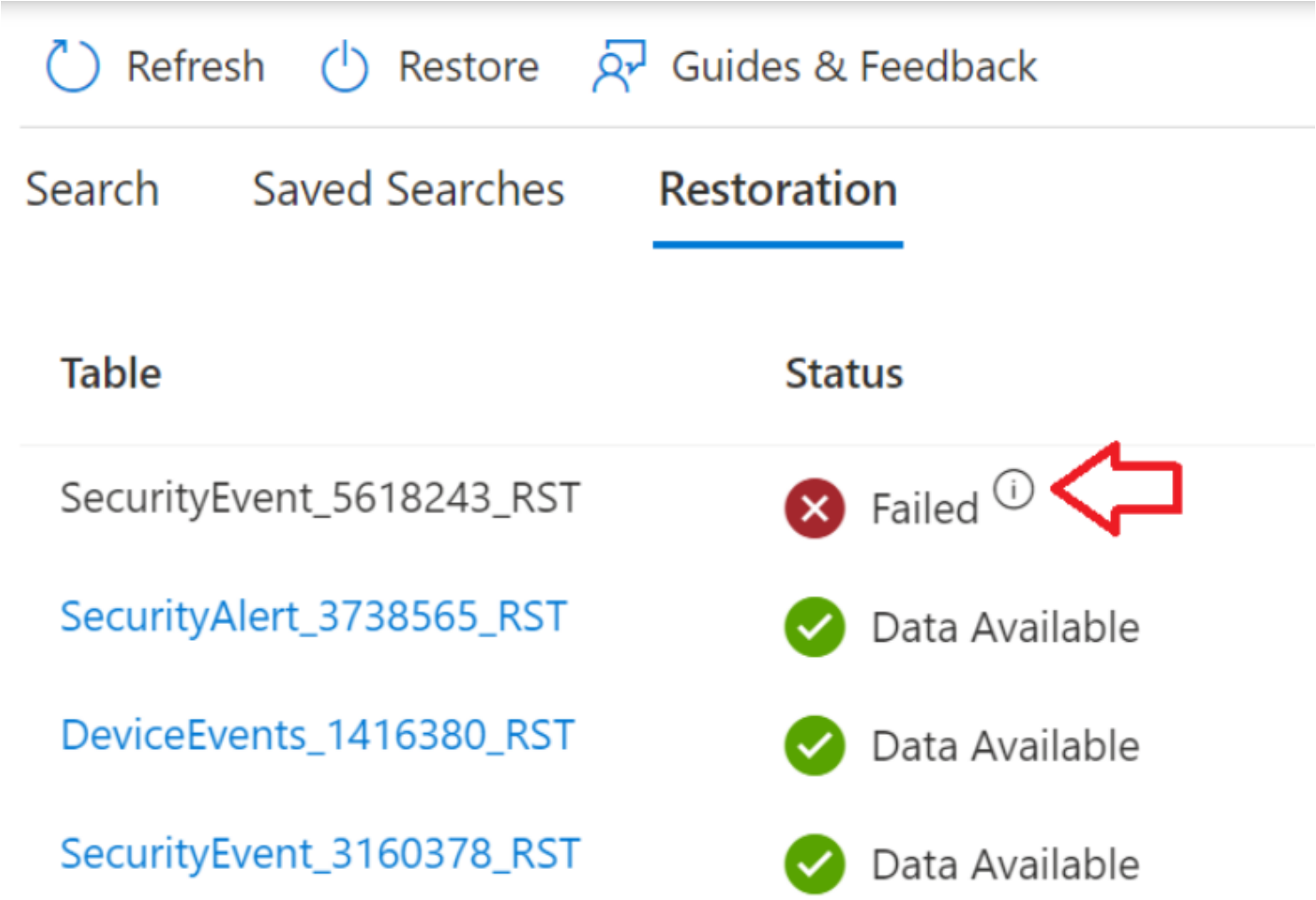

Note that the status dialog for the failed searches is removed when you refresh the Search page or if you visit a different page and return to the Search page. To recreate the failed status dialog resubmit the failing search job.
If you are not seeing the expected results in a search results table in the Logs table over a given timeframe, make sure you are using _OriginalTimeGenerated column to see the TimeGenerated value from the original source table. See Search job table Schema in Azure Monitor Documentation for more details.
Pricing details for using the restore feature is here: link TBD

**Microsoft Sentinel Search Page – Restoring an Archived or Basic log table**

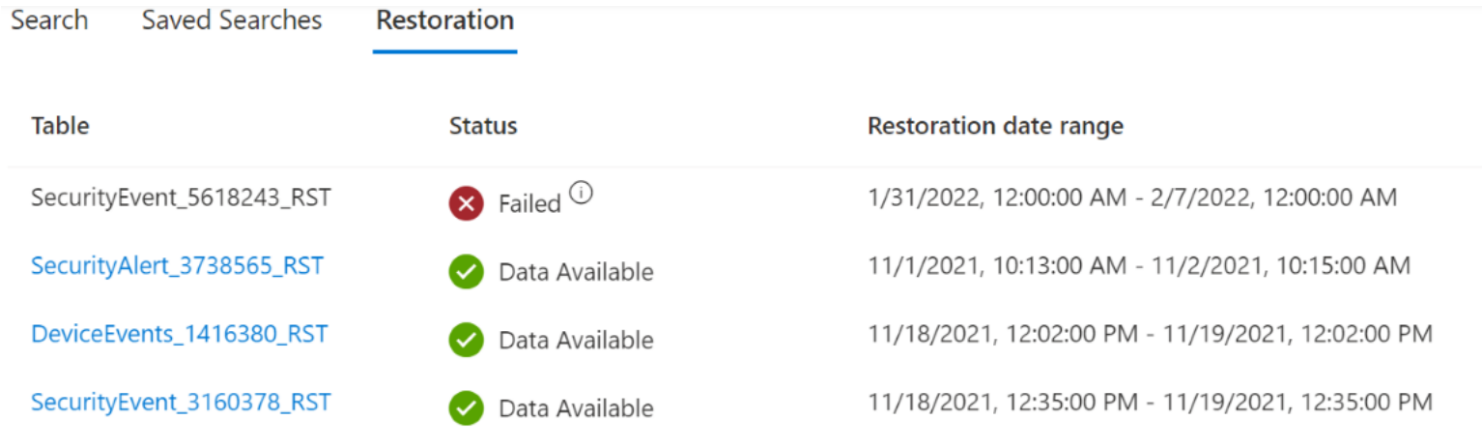
Before restoring a table, ensure you have one of the required roles: Microsoft Sentinel Contributor, Azure Monitor Contributor, or Microsoft Sentinel reader.
Archived data is restored using Azure Monitor Restore <link TBD>. This has the following limitations:

- Minimum of 2 days of log data to restore.
- Data to restore must be older than 14 days.
- Upperlimit of 60TB per single restore.
- Up to 4 restores per workspace per week.
- Up to 2 restore processes in a workspace can be concurrently running.
- One active restore at a time per table.

If you encounter a failure when restoring a table, hover your mouse over the info button next to the failure notification to get details.




If the restore job failed because data from the target table is already restored. You need to delete the corresponding "<SourceTableName>_<RandomNumber>_RST" table using the delete action. Then you can submit a new restore job.




Pricing details for using the restore feature is here: link TBD

## General notes for CSS

This functionality is in Preview and supported in Public Clouds only.

Failures displayed in the Sentinel UX are sourced from Azure Monitor Search Job and Restore Job APIs. Diagnosing these issues is best done by Azure Monitor Support.  To transfer the support ticket, you will need to provide the WorkspaceID or WorkspaceName, and table name (<SourceTableName>_<RandomNumber>_SRCH or <SourceTableName>_<RandomNumber>_RST), if applicable.

Restored data not displayed in normalized table (E.g., imDNS, imAuthentication).