M365 Defender incident integration Data Connector

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

Contents

TSG Microsoft 365 Defender-Sentinel Bi-directional incident integration

Mandatory information to collect when investigating an issue:

- Issue description as detailed as possible
- Azure Tenant ID
- Azure Workspace ID
- Sentinel / /M365 Defender Incident ID(s)
- Screenshots
- Timeframe
- Errors & stack trace if available

Known issues & limitations

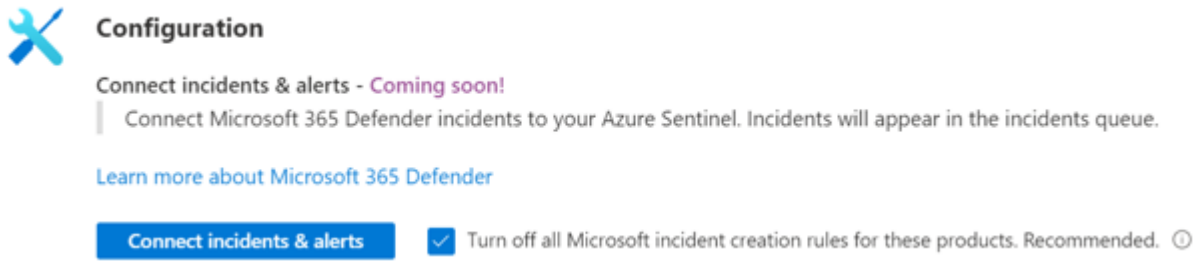
- Sentinel incidents can contain max 150 alerts, M365 Defender incidents support more alerts.
- M365 Defender incidents may take up to 10 minutes to appear in Sentinel.
- An incident can contain 0 alerts! In this case the incident will contain a tag of "Redirected".
- Disconnecting the following connectors is disabled while M365 defender connector is connected: Microsoft Defender for Endpoint Microsoft Defender for Identity Microsoft Defender for Office 365 Microsoft Cloud App Security
- In order to disconnect these connectors, you must first disconnect M365 defender connector.

Documentation to send to customers:

[Microsoft 365 Defender integration with Azure Sentinel]
[Connect data from Microsoft 365 Defender to Azure Sentinel]

Duplicated Incidents

This may be caused due to incident creation rule + incident integration both enabled. While Connecting the connector we have a checkbox offering the user to disables his alert rules but this isn't enforced.



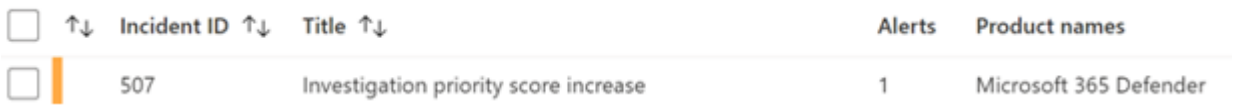
This appears in the documentation: [Microsoft 365 Defender integration with Azure Sentinel]

Issues related to M365 Defender internal providers should be forwarded to M365 Defender provider.

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alert Evidence

M365 Defender incident doesn't sync after changing an incident

- Did you try to choose the incident in Sentinel after refresh?
- Are you sure this incident is from the incident integration and not from an incident creation rule? Validate the "Product name" of the incident in the incidents page is "Microsoft 365 Defender".



- How did you change the incident (via Sentinel portal or via MTP portal)? Could you please try different direction?
- Did you receive some error during the change?
- Could you please reproduce again the issue on most updated incidents and send screenshots and time frame?

Notes: Bi-directional sync between Sentinel and Microsoft 365 Defender incidents on **status, owner, and closing reason**. The synchronization will take place in both portals immediately after the change to the incident is applied, with no delay. A refresh might be required to see the latest changes.

M365 Defender incident doesn't appear in Sentinel

- Do you see the Incident in MTP portal?
- Can you find the incident in Sentinel in LA query?
- Please re-check that you are searching data in correct LA Workspace and with correct time interval?
- Was this incident created before the incident integration (MTP connector) was connected?
- Do you see other incidents from Product name = "Microsoft 365 Defender" or is this the only one missing?

M365 Defender incidents retention

M365 Defender incidents have a retention period (default is 6 months), these incidents will continue to appear in Sentinel but the link to M365 Defender portal will redirect to the home page and not the incident page. Notice this can occur to incidents that are 6 months old.

Backend KQL queries for debugging

Multiple workspaces with incident creation enabled

The connector might be enabled in multiple workspaces, this query helps understand where by looking at the incident creation events.

```
// creation of a new case searching by alert ID
let ProviderName ="Microsoft 365 Defender";
// you need at least one of these 2 parameters
let AlertIds="6cd106ea-45e9-1a98-1134-bdac6ec923e5";
let ProviderIncidentUrl=""; //example "https://security.microsoft.com/incidents/10?tid=22447fe8-34aa-4d5c-925f
// optionals parameters
let workspaceId="";
let CaseNumber=""; // Sentinel incident number
let ProviderIncidentId="";
let SentinelIncidentName=""; // Sentinel IncidentName
database("SecurityInsightsProd").ServiceFabricOperations
| project env_time,operationName,resultType,customData
// adjust the time range as needed
| where env_time > ago(2d) and operationName == "Sentinel.CasesManagement.Cases.CasesManager.IngestNewCase"
| where customData.ProviderIncidentId has ProviderIncidentId and customData.ProviderIncidentUrl has ProviderIn
customData.workspaceId has workspaceId and customData.CaseNumber has CaseNumber and customData.AlertIds has Al
| sort by env_time desc
```

Update events for existing Sentinel incidents

```
// update of an existing case searching by alert ID
let ProviderName ="Microsoft 365 Defender";
// you need at least one of these 2 parameters
let AlertIds="6cd106ea-45e9-1a98-1134-bdac6ec923e5";
let ProviderIncidentUrl=""; //example "https://security.microsoft.com/incidents/10?tid=22447fe8-34aa-4d5c-925f
// optionals parameters
let workspaceId="";
let CaseNumber=""; // Sentinel incident number
let ProviderIncidentId="";
let SentinelIncidentName=""; // Sentinel IncidentName
database("SecurityInsightsProd").ServiceFabricOperations
| project env_time,operationName,resultType,customData
// adjust the time range as needed
| where env_time > ago(2d) and operationName == "Sentinel.CasesManagement.Cases.CasesManager.UpdateExistingCas
| where customData.ProviderIncidentId has ProviderIncidentId and customData.ProviderIncidentUrl has ProviderIn
customData.workspaceId has workspaceId and customData.CaseNumber has CaseNumber and customData.AlertIds has Al
| sort by env_time desc
```