

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

Identity protection recommendations are used to monitor identity activities in a subscription. They're designed so that the customer can take proactive measures before the incident takes place or reactive measure to stop an attack attempt.

The configuration of the Data Connector is done solely by enabling the Connector with the Connect button. The events coming in from this Data Connector will be stored as part of the SecurityAlert table. Not every single event may be turned into an alert from the Identity Protection end. This depends upon the configuration of the alerts from the Identity Protection Portal. Under Notify – Users at risk detected alerts – the customer may choose under “Alert on user risk level at or above” from alerting at high, medium, or low. The default is set to high. So, if the customer does not see in Sentinel alerts some of the events from Identity Protection, it may be that this setting is filtering such events and not converting these into alerts that will be sent over the Data Connector. In which case they may want to modify this setting to generate alerts for lower severity events.

Identity Protection | Risk detections
🔍 ...

<>
 Learn more
 Download
 Refresh
 Columns
 Got feedback?

Diagnose and solve problems

Protect

- User risk policy
- Sign-in risk policy
- MFA registration policy

Report

- Risky users
- Risky sign-ins
- Risk detections**

Auto refresh : Off Detection time : Last 1 month Show dates as : Local Detection type : None Selected Risk state : 5 selected Risk level : Low, Medium, High


+ Add filters

Detection time ↑↓	User ↑↓	IP address ↑↓	Location	Detection type ↑↓	Risk state ↑↓	Risk level ↑↓	Request ID ↑↓
12/27/2021, 3:27:04 PM	naser mohammad	46.32.125.138	'Amman, 'Amman, JO	Impossible travel	Dismissed	Medium	2833946e-f0fc-4532-84... ***
12/20/2021, 5:03:53 PM	naser mohammad	20.56.20.154	Amsterdam, Noord-Holl...	Atypical travel	Dismissed	Medium	9dcf607a-8d01-4d71-b... ***
12/20/2021, 3:49:33 PM	naser mohammad	20.56.20.154	Amsterdam, Noord-Holl...	Unfamiliar sign-in prope...	Remediated	High	498ec1a0-a427-4cbc-ba... ***

In the Sentinel Log Analytics Workspace, you can see the same value under VendorOriginalId field:

TimeGenerated [UTC]	DisplayName	AlertName	AlertSeverity	Description
ProviderName	IPC			
VendorName	Microsoft			
VendorOriginalId	e2c4c04389ba41028e21fb74ca36774e690abd7cb9de345b868c442c2587d935			
SystemAlertId	cf33dbaf-8212-949a-3b9f-e433bea75b55			
AlertType	ImpossibleTravel			

Azure Active Directory Identity Protection Incidents

Incidents ingested from Identity Protection can be ingested in an initially closed state. This can be confirmed by examining the following code: https://msazure.visualstudio.com/One/_git/ASI-Cases?path=%2Fsrc%2FCasesIngestorService%2FCaseCreation%2FCaseCreationLogic.cs&a=contents&version=GBdev_elp 

```
public const string ResolvedAtSourceCommentText = "Resolved at source";
public const string DismissedAtSourceCommentText = "Dismissed at source";

.....

if (alert.Status == AlertStatus.Resolved)
{
    SetCaseStatusToClosedWithReasonAndAddComment(newCase, alertDataModel, ResolvedAtSourceCommentT
}
if (alert.Status == AlertStatus.Dismissed)
{
    SetCaseStatusToClosedWithReasonAndAddComment(newCase, alertDataModel, DismissedAtSourceComment
}

.....

private void SetCaseStatusToClosedWithReasonAndAddComment(Case @case, AlertDataModel alertDataModel, string co
{
    // Set case status to closed and closure reason to benign positive
    @case.Status = CaseStatus.Closed;
    @case.CloseReason = CaseCloseReason.BenignPositive;

    //Add a closing comment explaining the closure reason
    @case.ClosedReasonText = comment;
}
```