# **Condition: User account is disabled. The account has been disabled by an administrator**

**Condition**

**Description:**

* Azure Active Directory (Azure AD) tracks user activity and sign-in metrics and creates audit log data that help you understand how your users access and use Azure AD services.
* The sign-ins activity data helps you determine who performed the tasks reported by audit log data. The sign-ins activity data helps you answer questions like:
* What is the sign in pattern of a user?
* How many users have signed in during the last week?
* What's the status of these sign-ins?

**Impact:** If user account is disabled, then user is unable to sign-in and perform his activity. Delay in performing task may impact client’s business.

**Criticality:** Critical

**Frequency:** 15 Minutes

**Trigger Details**

**Trigger Condition:** Trigger condition will be the “50057” errorCode in the azure AD sign-in logs

**Method to capture trigger point:**

* Microsoft Graph API can be used to capture azure active directory sign in logs.
* REST API URI is as mentioned below:

<https://graph.microsoft.com/v1.0/auditLogs/signIns>

* Reference link:

https://docs.microsoft.com/en-us/graph/api/resources/azure-ad-auditlog-overview?view=graph-rest-1.0

<https://docs.microsoft.com/en-us/graph/api/resources/signin?view=graph-rest-1.0>

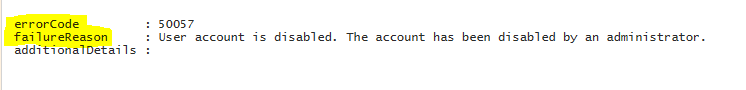
https://docs.microsoft.com/en-in/azure/active-directory/reports-monitoring/howto-configure-prerequisites-for-reporting-api

* Alert will be triggered ifvalues of sub property “**errorCode**” of property “**status**” is “**50057**”.

**Sample Output from API:**



Status property has following 3 subproperties:



**Alert Details**

**Alert Category:** Azure Active Directory

**Details required along with Alert:**

1. User Principal Name (Principal name of the user that initiated the sign-in – userPrincipalName)
2. Error Code (errorCode)
3. Error Message (failureReason)
4. Event Creation Time (The time sign-in was initiated - createDateTime)