

Suspected identity compromise

Suspected Identity Compromise tickets report instances of potential user account breaches and abnormal admin activity, focusing on actions that pose a significant threat to customer data.

These tickets present key details of the event, including the access point location and descriptions of the specific activities deemed suspicious:

The screenshot displays a 'Ticket Log' interface. At the top, there's a navigation bar with icons for settings, calendar, user, notifications, and a search bar. Below the navigation bar, the 'Ticket Log' section is active, showing a list of tickets. The tickets are filtered by 'Open' status and 'Cloud Security' type. The list shows six tickets, all titled 'Suspected Identity Compromise', with timestamps ranging from Sep, 23 2023 to Sep, 25 2023. The third ticket is highlighted. To the right of the list, a detailed view of the selected ticket (JGII-6786) is shown. It includes a 'Suspected Identity Compromise' title, a 'Users' section, a 'When' section with 'From' and 'To' dates, a 'Service' section showing 'Microsoft 365', and a 'Key Details' section with 'IP / Country' information and 'Event happened' count.

Open	Closed	All	Clear All	Cloud Security	Type	During	Search...
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							

JGII-6786 **Suspected Identity Compromise**

Users

When

From
Sep, 21 2023 , 5:54 PM

To
Sep, 24 2023 , 8:42 PM

Service
Microsoft 365

Key Details

IP / Country
94.206.201.16 (United Arab Emirates)
94.206.125.54 (United Arab Emirates)
94.202.39.214 (United Arab Emirates)
5.30.23.160 (United Arab Emirates)

Event happened
32 times

Note

Suspected Identity Compromise tickets are classified as suggested for review, and are automatically closed after a review period of two weeks.

The **Full Details** section provides references to normative actions taken in close proximity to suspected activities. The suspected activities use a red indicator, while the presumably normative activities use a green indicator. In the example