

# 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 shows a 'Ticket Log' interface. At the top, there's a navigation bar with icons for settings, calendar, user profile, notifications, and a search bar. Below the navigation bar, the 'Ticket Log' section has tabs for 'Open', 'Closed', and 'All'. There are filters for 'Clear All', 'Cloud Security', 'Type', and 'During'. A search bar is also present. The main content area is divided into two columns. The left column shows a list of 10 tickets, with the first six visible. Each ticket entry includes a checkbox, a user icon, the title 'Suspected Identity Compromise', and a timestamp. The right column shows the details for a specific ticket (JGII-6786). The details are organized into sections: 'Users', 'When', 'Service', 'Key Details', and 'Event happened'. The 'Key Details' section lists IP addresses and countries. The 'Event happened' section shows the number of times the event occurred.

Users	Key Details
	<b>IP / Country</b>
	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)

When	Event happened
<b>From</b> Sep, 21 2023 , 5:54 PM	32 times
<b>To</b> Sep, 24 2023 , 8:42 PM	

Service
Microsoft 365

## 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