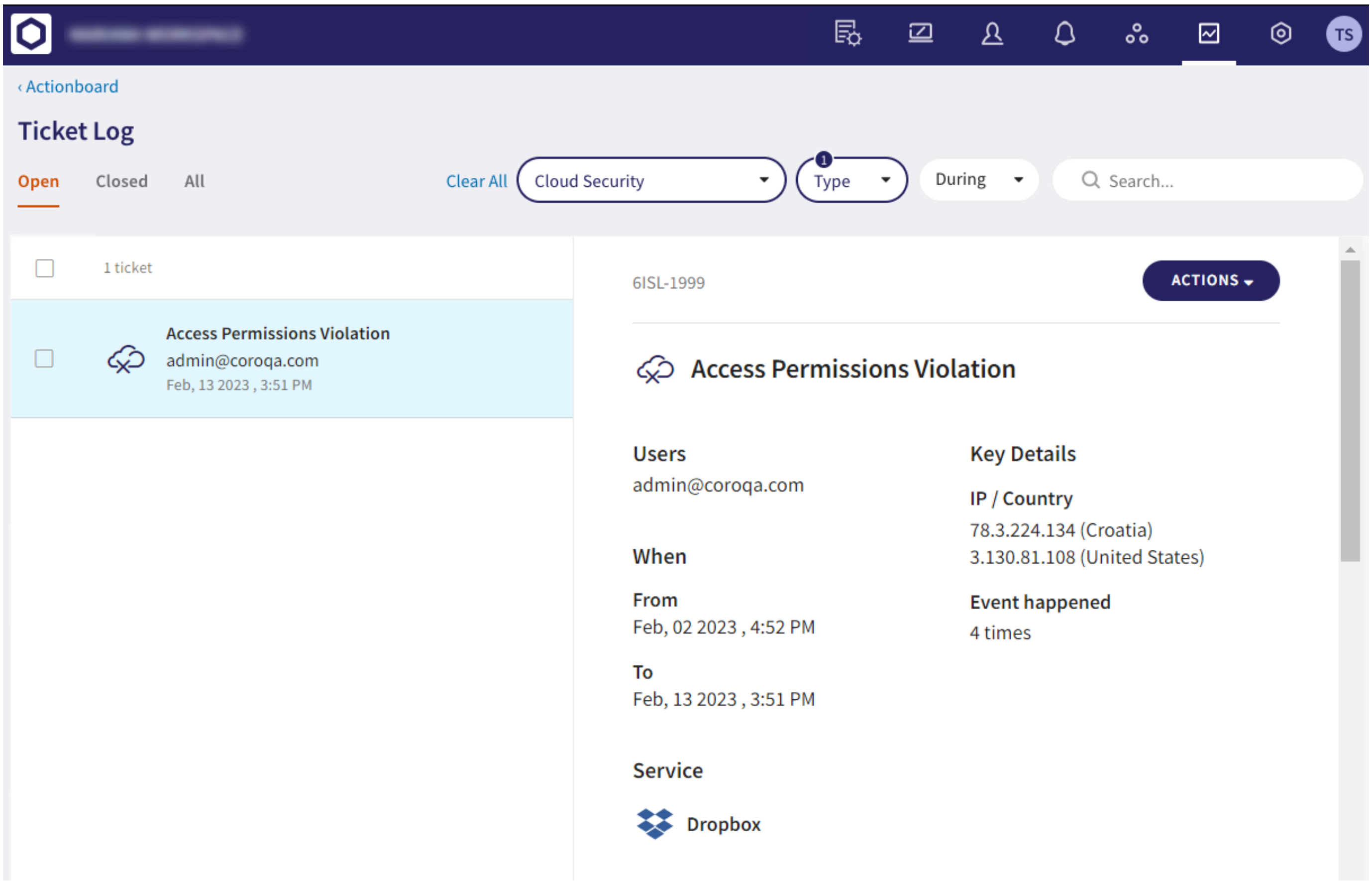
Access permissions violation

An **Access Permissions Violation** ticket displays details of a violation of specified access permissions for a cloud application. Tickets are raised only where the access attempt was successful, and are presented for admin user review.

The ticket includes the location of the user and identifies the specific service involved, such as Dropbox in this instance:



□ 1 ticket

□ Access Permissions Violation
admin@coroqa.com
Feb, 13 2023 , 3:51 PM

6ISL-1999

Access Permissions Violation

Users
admin@coroqa.com

When

From
Feb, 02 2023 , 4:52 PM

To
Feb, 13 2023 , 3:51 PM

Service
Dropbox

Key Details

IP / Country
78.3.224.134 (Croatia)
3.130.81.108 (United States)

Event happened
4 times

Admin users can specify access permissions for cloud applications through **Control Panel > Cloud Security**. For further information, see **Setting permissions for your cloud applications**.

Use the **Full Details** section to view the activities that triggered Coro to raise the ticket, with suspicious activities highlighted in red. In the example below, the user account has performed several activities (**Download** and **Login** on Dropbox) from different locations not permitted by the configured access permissions rules.