

Ticket types for Cloud Security

Coro generates tickets for cloud applications when it identifies the following security incidents:

- **Abnormal admin activity**
- **Access permissions violation**
- **Malware in cloud drive**
- **Mass data deletion**
- **Mass data download**
- **Suspected bot attacks**
- **Suspected identity compromise**

Abnormal admin activity

Coro identified activity for an admin account of a connected cloud app where it originated from an unexpected IP address. Tickets are classified as *suggested for review* and are automatically closed after the review period of four weeks.

Action	Outcomes
Close ticket	<p>Close this ticket as considered remediated and take no further action.</p> <p>Note: When a device is removed from protection, all open tickets associated with the device are automatically closed.</p>
Suspend user from all cloud apps	<p>The user's access to their accounts on all protected cloud applications is temporarily suspended.</p> <p>Notifications "User's access to cloud app has been suspended" and "Users updated" are displayed.</p>
Suspend user from <cloud service>	<p>The user's access to their account on the designated cloud application is temporarily suspended.</p> <p>Notifications "User's access to cloud app has been suspended" and "Users updated" are displayed.</p>