Rapport Support Policy

Technical support for Rapport

This Support Policy describes the technical support Actionable Science, Inc. ("Rezolve.ai") provides for Rapport. It forms part of the Rapport Product Terms. Capitalised terms have the meanings given in those terms.

1. Scope

1.1 Support covers the Rapport Console, the Agent on Supported Platforms (Schedule B of the Rapport Product Terms), the AI Features, Customer Integrations provided by Rezolve.ai, and the Documentation.

1.2 Support does not cover: the Customer's devices, operating systems, networks or third-party software; scripts written by the Customer; issues caused by changes to Rapport's safeguards contrary to the Documentation or by unsupported Agent versions; or consulting and implementation services, which are available under an Order Form.

2. Plans

Plan	Support	Service levels
Free plan (beta)	Email support on a best effort basis, with indicative response targets under section 4	None; no service credits
Paid plans	As set out in the Order Form	As set out in the Order Form

3. Contacting support

Purpose	Channel
Technical issues and questions	support@rezolve.ai
Suspected security incident or vulnerability	security@rezolve.ai (Vulnerability Disclosure Policy)
Privacy requests and data-subject requests	privacy@rezolve.ai
Data export or account closure	support@rezolve.ai, from an Administrator account

Support hours: Monday to Friday, 9:00 am to 5:00 pm US Pacific Time, excluding US federal holidays.

4. Priority and response targets

Priority	Definition	Target first response (beta)
P1 – Critical	Rapport is unavailable for all Operators; or a suspected security incident affecting the Customer's tenant or Agents	4 business hours
P2 – High	A core function (data collection, Device Actions, approvals, Agent updates) is materially impaired with no workaround	1 business day
P3 – Normal	A function is impaired but a workaround exists, or a non-core function is unavailable	2 business days
P4 – Low	Questions, documentation issues and feature requests	5 business days

Rezolve.ai assigns priority in consultation with the Customer. Targets apply to first response, not resolution. Beta response targets are indicative and are not guaranteed. Business hours are the support hours stated in Section 3. Applicable commitments for paid plans are set out in the Order Form.

5. Customer responsibilities

- Designate Administrators to raise and manage support cases.
- Provide the tenant name, affected devices or features, time of occurrence, error messages, Agent version and steps to reproduce.
- Keep Agents on a supported release and devices on a Supported Platform.
- Never send passwords, Enrollment Tokens or API keys to support. Rezolve.ai staff will never ask for them.

6. Support access to the Customer's tenant

6.1 Rezolve.ai support personnel, including personnel of its affiliate Actionable Science Labs Private Limited in India, may access the Customer's tenant only as needed to resolve a support case or to operate and secure Rapport. **Access is limited to the specific support case, is made remotely and is logged.** Such access and Processing are subject to the Data Processing Addendum and the applicable Sub-processor List.

6.2 Access is granted on a least-privilege basis, is logged and is reviewed. Support personnel do not initiate Device Actions on Enrolled Devices without the Customer's written instruction.

7. Agent and platform support

7.1 Rezolve.ai supports the current Agent release and the immediately preceding release. Customers should adopt new releases through the release settings in the Rapport Console.

7.2 When an operating system version reaches the end of vendor security support, it ceases to be a Supported Platform. Rezolve.ai will give at least 30 days' notice before ending support for an operating system version that remains vendor-supported.

7.3 The Linux Preview Agent is supported on a best-effort basis.

8. Incidents and maintenance

8.1 Rezolve.ai will notify Administrators by email of incidents materially affecting Rapport availability or security, and will provide updates until resolution.

8.2 Planned maintenance that may interrupt Rapport will be notified in advance where practicable.

8.3 Customers should report suspected security incidents to security@rezolve.ai. Security incident reports received outside normal support hours will be escalated to designated incident-response personnel for assessment and appropriate action. Such reports are handled separately from routine support requests and are not subject to the response targets in Section 4. Personal Data Breach notifications remain governed by the Data Processing Addendum.

9. Data export and account closure

9.1 Operators can export reports in CSV format at any time.

9.2 On request from an Administrator, Rezolve.ai will assist with export and, on account closure, deletion of the Customer's Rapport data, completing each within 30 days of the request, as set out in Clause 13.8 of the Data Processing Addendum or upon termination. The applicable deadlines, export arrangements and deletion exceptions are governed by that clause.

10. Changes

Rezolve.ai may update this policy. Changes that materially reduce support for paid plans apply from the Customer's next renewal. Rezolve.ai will notify affected Customers by email at least 30 days before changes that materially reduce support take effect.