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
Online Subscription and Free Trial	Email and in-console support during the support hours in Section 3, with the response targets in Section 4, Table B	No availability commitment and no service credits
Order Form	Email and in-console support; Critical and High incidents 24×7; response and resolution targets in Section 4, Table A	Availability target in Section 4A, unless the Order Form states otherwise; no service credits

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.

For Order Form plans, Critical and High incidents may be raised at any time and are handled 24×7. Suspected security incidents may be reported to security@rezolve.ai at any time on every plan (Section 8.3).

4. Priority and response targets

Rezolve.ai assigns priority in consultation with the Customer, using the definitions below. Table A applies to Order Form plans; Table B applies to the Online Subscription and the Free Trial. Targets are measured from the time a case is logged. The KPI is the proportion of cases in a calendar month that meet the target. Business hours are the support hours stated in Section 3. An Order Form may set different support commitments.

Table A – Order Form plans

Priority	Definition	First response	Target resolution	Coverage	KPI
Critical	Rapport is unavailable for all Operators; or a confirmed compromise of Customer Data	2 hours	8 hours	24×7	95%
High	A core function (data collection, Device Actions, approvals, Agent updates) is materially impaired with no workaround; or a suspected risk to Customer Data	4 hours	24 hours	24×7	95%
Medium	A function is impaired but a workaround exists, or a non-core function is unavailable; no data exposure	8 hours	72 hours	Business hours	90%
Low	Questions, documentation issues and feature requests	1 business day	Best effort	Business hours	—

Table B – Online Subscription and Free Trial

Priority	Definition	First response	Coverage
Critical	As in Table A	4 business hours	Business hours; suspected security incidents are handled at any time under Section 8.3
High	As in Table A	1 business day	Business hours
Medium	As in Table A	2 business days	Business hours
Low	As in Table A	5 business days	Business hours

Resolution targets do not apply to Table B. For the Free Trial, the Table B targets are aims, not commitments, and Rezolve.ai may treat a Free Trial case at a lower priority than a paid case with the same definition.

4A. Availability

4A.1 For plans under an Order Form, Rezolve.ai will make the Rapport Console and the Rapport service available at least 99.8% of each calendar month, unless the Order Form states otherwise. Availability is calculated as (Actual Uptime ÷ Scheduled Uptime) × 100, where Scheduled Uptime is the minutes in the month less Excluded Downtime.

4A.2 Excluded Downtime means unavailability caused by: (a) planned maintenance notified under Section 8.2; (b) emergency maintenance to address a security vulnerability; (c) the Customer's devices, networks, configuration or third-party services, or events beyond Rezolve.ai's reasonable control; (d) the AI provider, for AI Features only, where Rapport's other functions remain available; or (e) the Agent on an individual device.

4A.3 Availability is measured by Rezolve.ai's monitoring and reported to the Customer on request. The availability commitment is a service target: no service credits or other financial remedy apply to a shortfall. If availability falls below the target in two consecutive months, Rezolve.ai will provide a root-cause analysis and remediation plan on request.

4A.4 No availability commitment applies to the Online Subscription, the Free Trial or any feature designated as preview, including the Linux Preview Agent.

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 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. For a Critical incident, the first notification is sent within the Critical first-response target.

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.

8.4 Critical and High incidents are followed by a root-cause analysis. Corrective and preventive actions are recorded and made available to affected Order Form Customers on request.

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. Rezolve.ai will notify affected Customers by email at least 30 days before changes that materially reduce support take effect. Changes do not reduce support commitments in an Order Form during its Subscription Term.