PARABLU

Technical Support & SLA Agreement

Technical Support

Support is a break/fix mechanism. This means, once the backup tenant (in the case of a hosted setup) is set up, or an installation (in the case of an on-premise installation) is completed, if a technical issue arises out of misconfiguration, configuration changes, or bugs – Parablu's tech support team can be contacted to help fix these problems. In addition to this, Parablu also provides software version upgrades, hotfixes, patches and feature enhancements via our technical support team.

Troubleshooting of third-party elements involved in functioning of Parablu's software (e.g.: Network infrastructure, hardware failure, security certificates, browser or OS errors) are considered "Out of Scope". However, Parablu's technical support team will assist on a best-effort basis. If the trouble-shooting reaches a point where Parablu support engineers do not have the required expertise to arrive at a resolution, our engineers may request customers to contact the thirdparty vendor for assistance. The decision of this will be at the sole discretion of Parablu Support.

In the case of an on-premise setup, regular monitoring of infrastructure such as health of server(s), the network, the disk sub-systems, etc. are the customer's responsibility. During such monitoring, should any technical issues or questions relating to Parablu's software arise, Parablu Support can be contacted via a support ticket for specific assistance.

Additional services like re-installation, re-onboarding, re-configuration of the setup, additional con- sole configuration, migration between domains, migrating to / from on-premise to a hosted model, can be purchased at an additional cost by contacting your Sales account manager. The costs will vary based on the complexity of services and will be communicated to you for sign-off before we begin such work.

Incident Management

Parablu support can be contacted 24x7 via support@parablu.com. Paying customers also receive credentials to login to our support portal at https://www.support.parablu.com to gain access to our incident tracking system, our latest documentation, and knowledgebase. Support incidents are classified based on priority and are worked on by the Parablu support team in that order.

In case of multiple concurrent support requests, each having the same priority, the priority proce-dure to handle these requests will be determined in consultation with the customer's IT team managing Parablu's services. Parablu can work with the customer nominated SPoC or designated employee to arrive at an acceptable resolution plan.

Ticket Classification

Ticket Priority	Description
Normal	Problem resulting in no interruption to normal operations – No business impact
Medium	Problem resulting in minimum interruptions to normal operations – No business impact
High	Problem causes interruptions to normal procedure. It doesn't prevent the operation of a production system or there could be a minor degradation in performance.
Urgent	Problem results in serious interruptions to a Production System (single BluKrypt/ParaCloud) but overall system still works, although with serious impact in performance.
Critical	Problem results in extremely serious interruptions to multiple production system and has already affected the entire user community.

1.1 Ticket Response and Resolution Time

Ticket Priority	Initial Response Time (In hours)	Response Update Frequency (In hours)
Normal	24	168 (In weekly)
Medium	12	48
High	8	24
Urgent	4	8
Critical	2	4

Response time is the time interval taken by the Parablu support team or the concerned team to respond back to the ticket.

Where possible, the Parablu Support team will try to provide a resolution or quick work around. But in cases, where a software update is required, the time and plan will be mutually agreed between the customer SPoC and Parablu's support team.

Response Update frequency is the frequency in which Parablu support team will update the customer's SPoC (or designated employee) about the status of the issue.

1.2 Support Scope

- First level Support (L1) will be provided by the customer's internal Helpdesk.
- Level 2/3/4 Support will be provided by the Parablu technical support team.

Support Levels

L1 Support

The L1 support team are the first point of contact with actual end users. They handle all informative and how-to types of questions from end users. They perform the initial level of trouble shooting to identify the problem and ensure that it is a product problem and not related with infrastructure / user rights.

In case of a product bug, the Helpdesk team will escalate the issue to Parablu's support team via an email to support@parablu.com, or via the https://support.parablu.com portal. In all cases the ticket should be accompanied by relevant logs and a description of steps followed until then to troubleshoot.

L2 Support

Parablu's L2 support team will respond back to the customer on the intial support request within the specified time frame. They will work with the customer's support desk to decide whether the issue in the working of the product or if it is related to infrastructure or configuration. They may request additional logs or in some cases, remote access to a particular endpoint system for further troubleshooting.

L3 Support

The L3 Support team are Subject Matter Experts in their area of work and will assist the L2 Support team for solving complex or new issues. They are responsible in reviewing the Support Ticket with L2 team, assessing the time already spent by on the issue raised and prioritizing the ticket so that time is managed optimally.

L4 Support

The L4 Support team are engineers and developers of the product. If a problem has been clearly diagnosed to be an issue with the product's working, which requires a patch or a software update, they will work on those as identified by L3 team.

Cloud services

Parablu's fully hosted "Backup as a Service" (BaaS) doesn't require any on-premise infrastructure to be set up in the form of compute or storage. Only the BluVault backup agent will need to be distrib- uted to all the user endpoints. This can be accomplished using SCCM, InTune, AD GPO or any other suitable mass deployment mechanism.

The customer's backup administrators will exercise complete control over their backup operations using the web-based management console they get access to. More administrators can be added as well as delegated administrators with limited rights (for example to manage specific locations or departments). Users can be provisioned/de-provisioned using Parablu's Azure Active Directory connector – or can be managed using Parablu's native namespace.

Administrators can create policies which define all aspects of backup behavior and assign users to these policies. Even very large numbers of users spread out over multiple geographies can easily be managed with a handful of policies.

Parablu's hosted services span the globe and can provide multiple points of presence. Users, no matter which part of the world they work in, will by default, back up to the closest Backup tenant detected by the endpoint agent.

Parablu's software is hosted in data centers which are ISO 27001 and ISO 90001 certified, with SLAs of 99.9% data availability.

Upon expiration or termination of the subscription, at the customer's written request made within Fifteen (15) days after expiration, Parablu will provide the customer with temporary and limited access to the data restore functionality for a period of Thirty (30) days, solely for the customer to retrieve data (but not any other purpose). After such Thirty (30) day period, Parablu will have no obligation to maintain or provide access to such data retrieval and shall thereafter, unless legally prohibited, delete all customer data in its possession or control.

Performance Measurement

Parablu's management console is designed to equip Administrators with all the information they need to execute successfully on their backup strategy. Backup History reports, Overview reports, Backup summaries – and several tools are available for an Administrator to easily track data protection perfomance.

Reports can be run on demand, downloaded as PDF/xls, or even scheduled to be run at frequent intervals and automatically emailed to Administrators.

End-user email reporting can also be enabled – to allow end-users a transparent view as to how their backups are performing on a weekly basis.

A good way to get a high-level view of backup performance across the customer's entire backup tenant would be for the customer's backup administrators to pull (or have emailed to themselves) a Data Protection Scorecard report every day. It gives a view for how many endpoints are configured, how many are actively in contact with the BaaS cloud, and how many are actively being protected. If these #s are getting lower than a threshold (such as 90%) it is important to drill down and take action.

For a drill down, the Backup Overview Report is very handy. This gives backup administrators a comprehensive view of each user, their devices, and detailed backup status for each with dates, sizes, and times taken.

It is important to note that backup and restore performance can be highly variable depending on a number of factors – and needs to be monitored frequently. A number of these reasons are usually unrelated
to the software, but could be infrastructure or user related.

A few reasons backups may stop working are:

1. A new device may have been provisioned to a given user, but without the backup agent installed. The old device is off and not actively being backed up.
2. Changes in networking rules – such as firewall whitelists, client proxies, Windows firewall etc. may be preventing the backup agent from connecting to the BaaS in the cloud.
3. Security software on the endpoint – Anti-virus, Anti-malware, DLP, EDR, etc. may be interfering with the backup agent's working.
4. The end-user may be frequently stopping or pausing the backup. Or they may have uninstalled the software.
5. Backup policies may have been changed to disallow certain folders are file types – via exclusions or filters.
6. Backup schedules may have been modified to become less frequent.

A few reasons backups and restores might be performing slower than desired:

1. Poor or very slow network links connecting the endpoint to the internet.
2. An excessively high network throttle setting (i.e. a very low Mbps or Kbps value) set in the backup policy.
3. A poor Wi-Fi connection that frequently stops and starts.
4. Slowness in the Microsoft 365 tenant (in the case of M365 backups or backups using One- Drive as a backup target).

The Parablu Tech Support team is of course always available, and can help the customer narrow down and identify root cause if necessary.

Periodic restore drills are recommended to confirm correct working. Parablu's technical support team will be standing by to support in case the customer faces any issues during such restore drills.

The following are the best ways to reach Parablu's technical support team:

1. https://support.parablu.com – login with your credentials and open a ticket
2. Email support@parablu.com – with a clear description of the problem you're facing along with screenshots if possible.
3. Failing the above methods, the customer may use the escalation matrix supplied to them by the Parablu support team at the time they were onboarded.