

SUPPORT AND SERVICE LEVEL AGREEMENT (SLA)

Last Updated: August 1, 2026

1. DEFINITIONS

“Request” (Claim): A service outage, performance issue, or technical support request submitted by the Customer to node101.

“Downtime”: The total duration during which the RPC (Remote Procedure Call) or Indexing services provided by node101 are unavailable. A service is considered to be experiencing downtime when it fails at all monitoring locations.

“Scheduled Downtime”: Downtime planned in advance due to infrastructure, security, or system updates. Scheduled downtime shall be communicated to customers by email at least seven days in advance.

“Emergency Downtime”: Downtime required due to unexpected circumstances requiring urgent intervention. Emergency downtime may occur no more than once per calendar month and shall not exceed four hours.

“Network Issue”: A situation in which node101’s monitoring checks from multiple regions fail to receive a response from only one location. Such situations are deemed to result from regional network routing or Customer-side connectivity issues and are not counted as downtime.

“RPO (Recovery Point Objective)”: The maximum acceptable period of data loss. In the event of an unexpected incident, data up to this point in time must be preserved. The target is four hours for RPC services and one hour for Indexing services.

“RTO (Recovery Time Objective)”: The maximum period within which the system must be fully restored following a failure or outage. The target is four hours for RPC services and two hours for Indexing services.

“SEV1–SEV4 Incidents”: The classification of incidents according to their impact on the service.



SEV	Description	Impact Level
SEV1	All RPC access has stopped or no response is received	Critical
SEV2	Access issues or high latency on certain endpoints	High
SEV3	Partial errors or slowdown	Medium
SEV4	Information request or minor error report	Low

“Service Credit”: A discount granted to the Customer if availability falls below the specified level. The service credit rate for node101 is fixed at 10%. The credit is not a cash refund and shall instead be applied as a discount on the next invoice or as an extension of the service period.

“Uptime”: The ratio of the period during which a service is active and accessible to the total period being measured.

2. SERVICE AND SERVICE LEVEL COMMITMENT

The Customer has the right, and where required by law or security obligations, the duty, to compare the performance and availability of the services provided by node101 with data obtained from other third-party providers offering similar services.

Such comparisons may only be conducted by the Customer for its own operational assessments, performance analyses, and security protocols.

The Customer may not publicly disclose data obtained from such comparisons or use such data for commercial, promotional, or competitive purposes without node101’s prior written consent.



2.1. Uptime Guarantee

node101 commits to **99.70%** quarterly availability for all network types, including mainnet and testnet. This permits a maximum of 394.2 minutes, or 6.57 hours, of downtime during a three-month period of approximately 131,400 minutes.

If availability falls below this target, the Customer shall be entitled to a Service Credit equal to 10% of the total amount paid for the relevant service. The Customer may request to use this entitlement during the following quarterly period. Any entitlement not used during the following quarterly period shall expire.

2.2. Measurement Method

node101 monitors its RPC and Indexing services every 30 seconds from Europe, Türkiye, North America, and APAC.

Monitoring is conducted through node101's proprietary Cloudflare-based monitoring infrastructure. Responses received from three or more regions are considered "active."

The system is marked as experiencing downtime when simultaneous failures occur in all regions.

2.3. Scheduled and Emergency Maintenance

- Scheduled Maintenance: Announced at least seven days in advance and shall not exceed four hours.
- Emergency Maintenance: Performed when deemed necessary. The Customer shall be informed by email and Telegram.
- Maintenance Window: Saturdays and Sundays between 06:00 and 10:00 UTC.

Scheduled maintenance is excluded from uptime calculations. Any period exceeding the scheduled duration shall be treated as downtime.



3. SUPPORT SERVICES

3.1. Support Channels

node101 provides its customers with 24/7 technical support through the following channels:

- Email: support@node101.io
- Microsoft Teams, Slack, Google Chat, or Telegram: A dedicated group established for the relevant counterparty

Support channels may only be used by persons authorized by the Customer.

3.2. Incident Priorities and Response Times

SEV Level	Example	Initial Response Time	Resolution Approach
SEV1	All RPC access has stopped and/or malfunctions have occurred in the Indexing service	Less than 2 hours	Emergency intervention; the on-call system is activated
SEV2	RPC remains active	Less than 5 hours	Critical priority; rapid deployment
SEV3	Partial errors or slowdown	Less than 10 hours	Resolution within the normal workflow
SEV4	Information request or minor error report	Less than 24 hours	Scheduled resolution

For SEV1 and SEV2 incidents, node101 notifies its DevOps team through an automated PagerDuty on-call system.

PagerDuty is a system that sends emergency notifications to authorized persons by SMS, email, and automated phone call in critical incidents.

A root cause analysis (RCA) shall be prepared and delivered to the Customer within 48 hours following each critical incident.

4. SECURITY AND ACCESS CONTROL

node101's infrastructure is designed in accordance with Zero Trust principles. Zero Trust is a security model under which no system or user is considered secure by default, and every access request is subject to identity and contextual verification.

The node101 DevOps team performs management and maintenance operations through a private vLAN (Virtual Local Area Network), isolated using Zero Trust technology and accessible only by the team.

This structure completely blocks access from the outside world and permits access only to authorized engineers.

Additionally:

- Authentication: Token-based access is provided by default. At the Customer's request, mTLS (mutual TLS) or an IP-based access allowlist may be implemented.
 - Data Encryption: All data traffic is encrypted using the TLS 1.3 standard.
 - Access Logs: All access records are retained for at least 90 days.
 - Personnel Security: All node101 engineers use multi-factor authentication (MFA) for system access.
 - DDoS Protection: All RPC endpoints are protected by rate-limiting and traffic-filtering systems that detect high-volume requests. These systems ensure service continuity by preventing malicious Distributed Denial of Service traffic.
 - Load Balancer: Traffic is routed to nodes located in different regions. This mechanism automatically redirects traffic to other healthy nodes if one server fails.
-



5. BACKUP AND DISASTER RECOVERY

- node101 services are regularly backed up.
 - RPO/RTO targets:
 - RPC: RPO 4 hours / RTO 4 hours
 - Indexing: RPO 1 hour / RTO 2 hours
 - Backups are stored in geographically separate data centers.
 - Data integrity for critical components is verified through checksum and log audits.
-

6. MONITORING AND REPORTING

node101 monitors all of its services through Prometheus-based metrics collection and Grafana-based monitoring infrastructure.

Customers are provided with an authenticated Grafana dashboard accessible only by them. RPC response times, node versions, and uptime data can be monitored in real time through this dashboard.

Dashboard access is an as-is service restricted to node101's technical team and the relevant Customer.

At the Customer's request, a report may be prepared for a specific period. node101 does not publish regular performance reports; system data is shared in real time through the dashboard.

7. CLAIMING SERVICE CREDITS

The Customer may request a Service Credit by applying by email to support@node101.io within 30 days following the end of the relevant quarterly period.



Service Credits:

- Are fixed at 10%;
 - Are not cash refunds;
 - Are applied during the next invoicing period;
 - Become invalid upon termination of the agreement.
-

8. EXCLUDED CIRCUMSTANCES

The following circumstances are excluded from availability calculations:

1. Infrastructure or configuration errors on the Customer's side;
 2. Third-party service outages outside node101's control;
 3. Scheduled maintenance periods;
 4. Legal restrictions, cyberattacks, or natural disasters;
 5. Customer internet connection or local network issues;
-

9. LIMITATION OF LIABILITY

- node101 shall not be liable for indirect damages, data loss, or loss of revenue.
- This SLA constitutes the sole and exclusive remedy for service outages.
- node101's total liability shall not exceed the service fees paid during the relevant contractual period.

