NEXUSGUARD

Nexusguard Support and Maintenance Guide

A comprehensive guide to direct, global Client support for Nexusguard products.

NEXUSGUARD

Table of Contents

NEXUSGUARD

Document Control

Title	Nexusguard Support and Maintenance Guide
Document Version	V1.0
Prepared by	Service Management Team

Copyright and Intellectual Property Rights

Use of this Information

The information in this document is provided “as is" and, to the fullest extent permissible under applicable law, Nexusguard Limited, disclaims all warranties, express or implied, including but not limited to, warranties of merchantability and fitness for a particular purpose. We do not warrant or make any representations regarding the use or obtainable results of the use of this information in terms of correctness, accuracy, reliability or otherwise. By using this information, you acknowledge your understanding of these terms and you agree to assume the entire risk and cost of any necessary configuration changes, testing, damages or remediation arising from such use.

Limitation of Liability

To the maximum extent possible under applicable law, Nexusguard Limited shall not be liable for any damages, including, but not limited to, special, indirect, incidental, punitive or consequential damage, that may result from the use or inability to use the information in this document, even if we or our authorized representative has be advices of the possibility of such damages.

About Nexusguard

Founded in 2008, Nexusguard is a leading cloud-based distributed denial of service (DDoS) security solution provider fighting malicious internet attacks.

Nexusguard ensures uninterrupted internet service, visibility, optimization and performance. Nexusguard is focused on developing and providing the best cybersecurity solution for every client across a range of industries with specific business and technical requirements.

Nexusguard also enables communication service providers to deliver DDoS protection solutions as a service. Nexusguard delivers on its promise to provide you with peace of mind by countering threats and ensuring maximum uptime.

For more information, please visit: www.nexusguard.com

Introducing the Nexusguard Service Management and Support Team

In Nexusguard, we value our clients above anything else. We are dedicated to provide our support to our customers through our Security Operations Center and Service Management Team. With this, we have established channels of communication that we provide so as to have our customer's Experience be gratified.

Nexusguard Security Operations Center is our frontline that is available 24x7x365, reachable through Live Chat, Email and Hotline. Our team of Network and Security Analysts and Specialists, will always be available to provide their utmost support to ensure the satisfaction of customers in terms of Client Experience.

Nexusguard Service Management Team is committed to hand hold our customers to achieve their success. Our Service Management Team serves as focal escalation points that could help tend to our customers' needs both technical and non-technical. We are dedicated to our customers ensuring that they would be given the utmost support that they deserve.

In Nexusguard, we are proud of how committed we are to guarantee our customers' Success. We value our relationship with our customers and hand hold each other in delivering top of the line DDoS Mitigation Services.

Help Center

Nexusguard Help Center was created in the collaboration of various teams within our organization, aimed to improve the level of support that we provide to all our clients. Nexusguard Help Center is a single support page that would be able to answer basic questions through our FAQ, chat with Nexusguard Support, maintenance announcements, ticket submissions and ticket tracking. Through this platform, we are supporting complete transparency to our clients as an assurance that we are on track to our commitment in providing the premium service tagged after our Company's Mission.

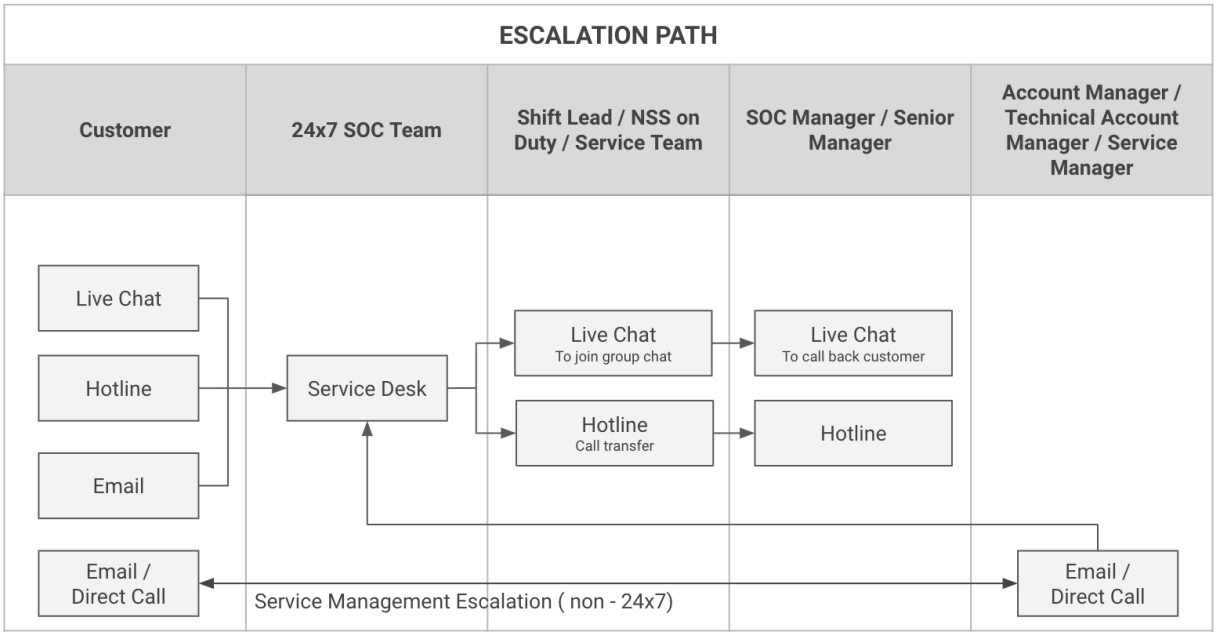
Accessibility

customers can access the Help Center by logging in via https://help.nexusguard.com. If the password reset link does not work for your browser, please click here to prompt the link for password reset. Please contact Nexusguard Support or your Service Manager if you have difficulty retrieving your password.

Key Features

1. Getting started
   - Introduction to Nexusguard customer portal.
2. Knowledge Base
   - A quick reference to basic information covering end to end technical know-how.
3. Announcements
   - A section to list out all upcoming events, feature updates, maintenance and etc.
4. Live Chat
   - Go straight to an instant chat with our support team any time you need assistance, 24 x7.
5. Ticket Submission and activities tracking
   - Send us your change request, report an incident or submit an inquiry directly without having to send via email, and start tracing the status of your tickets from the same location.
6. Nexusguard Blog
   - Check out Nexusguard news, and read up on the cybersecurity best practices and DDoS defense strategies.

General Escalation Procedures



NEXUSGUARD Help Center

For immediate access to:

- Best Practices
- FAQ
- Troubleshooting materials
- Live Chat
- Change request
- Ticket submission and tracking
- Announcements

Please refer here for login instructions.

Live Chat via Help Center

Log in to Help Center https://help.nexusguard.com to chat with our support representatives.
Client ID (4-6 digit number) will be required for user authentication.

support@nexusguard.com

+1-844-767-3368 | +852 3526 0626 (Dial “1” for support)

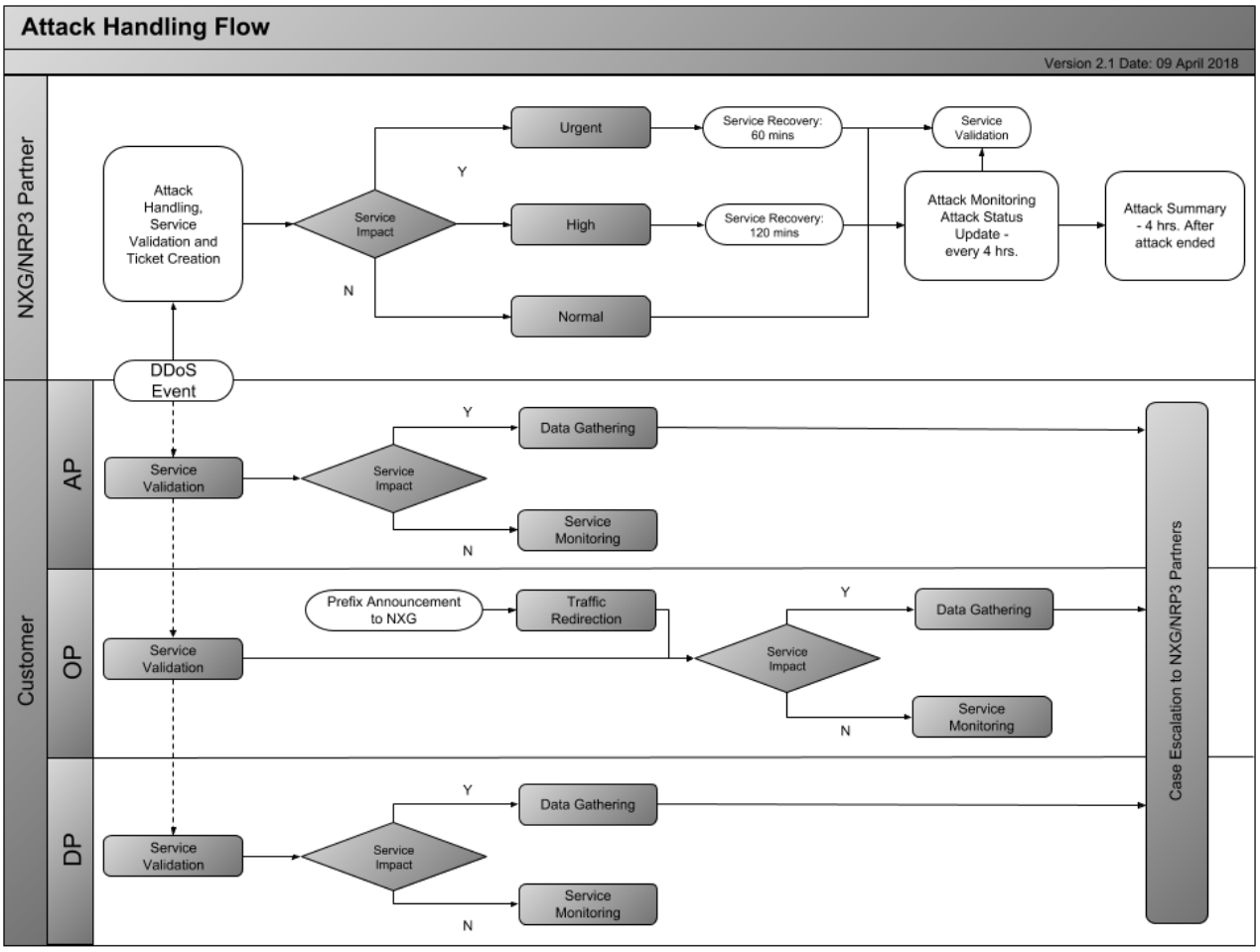
Event Management Guidelines - Cloud/Partner Services

At Nexusguard, we are committed to providing our Anti-DDoS Solution. At an instance of an event, may it be an attack or incident, Nexusguard has defined a set of Standard Operating Procedures to ensure customer's services are running smoothly.

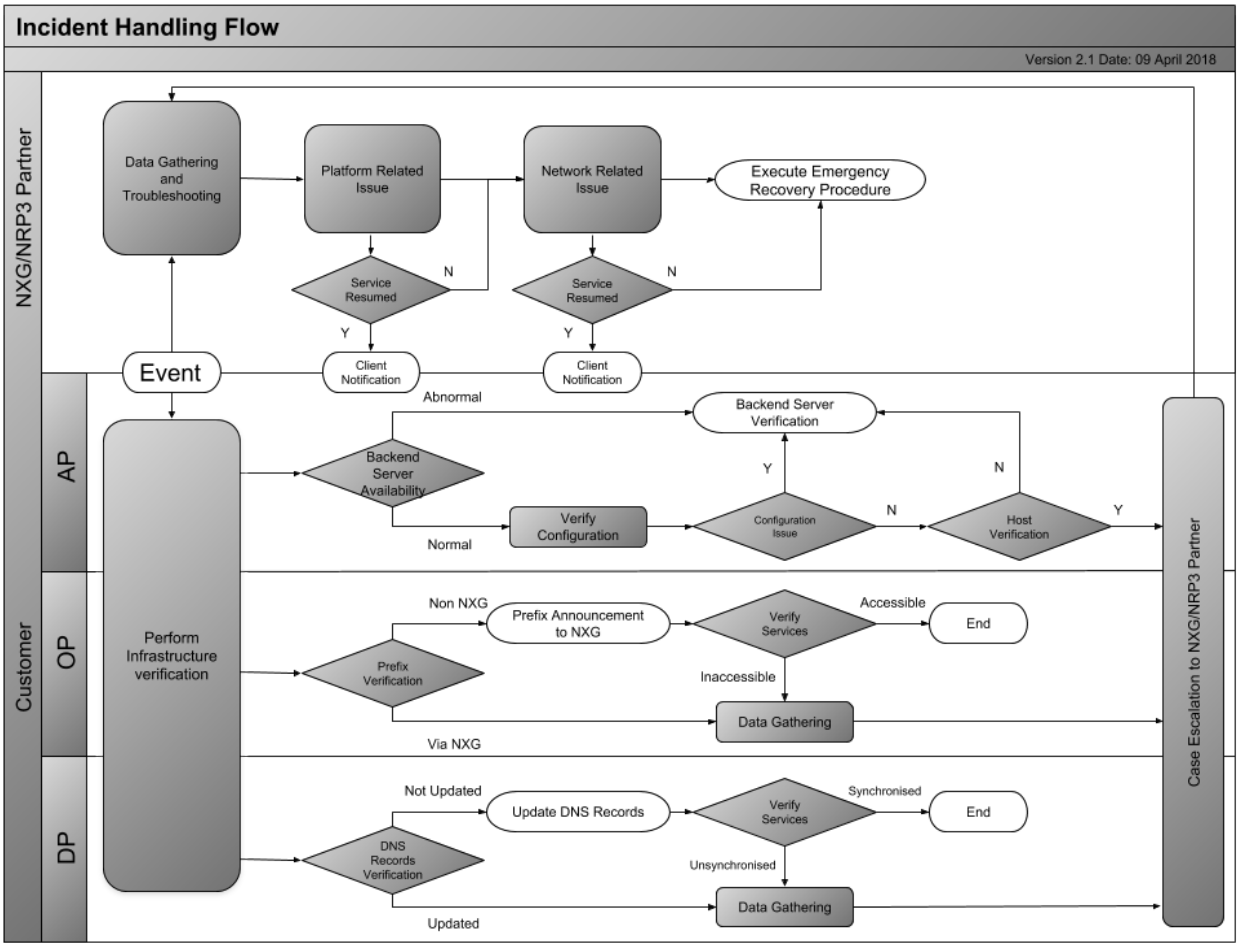
At the instance that our Support Team is able to monitor an event, an email notification will be used to inform our customers upon verification of an event alert. This notification will be able to create a ticket number informing the respective contacts, and will also be used to update the current status of the event. Further communication or follow-up to either our Service or Support Team will be required, the ticket number would be needed for immediate tracking of updates and/or follow-up actions.

To further equip our Support Team in resolving events, it is vital that our customers closely work with us for immediate resolution of issues. We highly recommend that cooperation between both parties would be established on such instances.

Here are some scenarios for further reference:



Notes	
	Service Impact: - Urgent - total service outage - High - service degrade (site is accessible but having functionality problems, intermittent accessibility, service disconnections, etc.) - Normal - No service impact encountered **OP Prefix Announcement** (as agreed between Client and NXG): - Client is to ensure that prefixes are properly announced via NXG or own IP Transit. - Coordination is highly encouraged to avoid possible Routing Issues or BGP/Route Dampening **Case Escalation to NXG - Data Gathering:** 1. Source/Impacted IP Address 2. Impacted Domain/Service including service port (eg. 80/443) 3. TCP Traceroutes and/or MTR Results 4. Test Results (eg. Nslookup, Dig, Host File Verification, browser access, etc.) 5. Error Messages **Reminder:** 1. Standard cool-down period is set to 48 hrs. (Normal mitigation and routing configurations will be reverted) 2. Possible increase of latency may be encountered due to mitigation techniques applied during a DDoS Event.



Notes	
	OP Prefix Announcement (as agreed between Client and NXG): - Client is to ensure that prefixes are properly announced via NXG or own IP Transit. - Coordination is highly encouraged to avoid possible Routing Issues or BGP/Route Dampening **Case Escalation to NXG - Data Gathering:** 1. Source/Impacted IP Address 2. Impacted Domain/Service including service port (eg. 80/443) 3. TCP Traceroutes and/or MTR Results 4. Test Results (eg. Nslookup, Dig, Host File Verification, browser access, etc.) 5. Error Messages

Operations Remote Troubleshooting

Nexusguard is committed to work the extra mile to make sure that the highest quality of service is provided to all our customers. With this in line, our Operations can remotely access end-users desktop or notebook using our Remote Troubleshooting Tool.

Tools are readily downloadable to be installed, after which the username and password is to be forwarded to our Support Team for remote access and troubleshooting.

Note: Disclaimer is provided for reference. Full intention is for troubleshooting purposes only, no data or any personal information will be seized during the duration of the Remote Access.

Remote Support Tool Download Links:
http://nexusguard.com/quicksupport_mac.zip
http://nexusguard.com/quicksupport_windows.exe

Route and Mitigation Handling

As part of the housekeeping and maintenance of our Support Team, we do a periodic clean-up of configurations that were placed during an event of an attack.

Cool Down Duration is defined as the time duration after an attack event has been concluded. After the cool down timer has expired configuration on both mitigation and prefix announcement will be adjusted back to peace time status.

Mitigation Revert Time - Applied countermeasures will be removed to loosen the policies and avoid any false positive blocking by our platform. The configuration will then be documented for future reference.

Route Revert Time - Any changes on the prefix announcement during the event of the attack will be reverted back to the peace time announcement to ensure optimal service availability.

Nexusguard Service	Mitigation Revert Time	Route Revert Time
Clean Pipe & Origin Protection	4 hours (every 4, 8, 12 am/pm GMT+8)	4 hours (every 4, 8, 12 am/pm GMT+8)
Application Protection	4 hours (every 4, 8, 12 am/pm GMT+8)	24 hours (every 6 am GMT+8)

Post-Incident Report (IR)

An Incident Report (IR) will be available within 3 working days upon request for an incident that causes impact to Client's service.

The incident report will consist of the following information:

- **Incident ticket number:** Nexusguard ticket that is created as reference for the Incident.
- **Affected service(s):** Nexusguard subscribed services.
- **Type of impact:** Impact definition based on symptoms as reported or monitored.
- **Incident occur date, time, duration:** Incident information as reported or monitored.
- **Reporting channel:** Defined as either phone call, chat or email as a reporting medium to Nexusguard.
- **Incident classification:** Case type as concluded by Nexusguard.
- **Incident summary:** A description of the event as it was handled and resolved by Nexusguard.
- **Action taken:** A summary of how the incident was resolved by Nexusguard.
- **Current service status:** Service status after the resolution of the incident.
- **Root cause analysis:** An in depth analysis on what caused the issue.
- **Preventive and corrective actions:** Follow-up actions that would need to be taken by either Nexusguard or client.
- **Sequence of event:** Timeline of the incident from start to end.

Event Management Guidelines - Nexusguard Platform, Software and Hardware Products

Warranty, support & maintenance for your Hardware

The product you have purchased from Nexusguard may include Hardware supplied by one of our third party original equipment manufacturer partners, including any warranty, support and maintenance services that would have been itemized in your purchase agreement.

For warranty, technical assistance, support and maintenance, Return Material Authorization (RMA), please refer to the respective OEM documentation and policies indicated in your purchase agreement.

Platform & Software Maintenance

Nexusguard is a leading Cloud and Hybrid based DDoS Mitigation Provider, platform stability and availability is crucial to continuously safeguard our clients and customers.

Nexusguard conducts periodic maintenance and upgrades to enhance our platform reliability. This ensures that Nexusguard is equipped with the most up-to-date technology and protection in this fast-paced environment.

With our microservices architecture, we grouped our releases into Major and Minor. Major Release would pertain to core components and engine upgrades which may potentially lead to service degradation and will be given a defined maintenance window. Minor releases are the non-core components of our platform which will be carried out continuously within a predefined maintenance window. Notifications are done as illustrated below:

Maintenance Type	Notification	Maintenance Window
Minor Release	3 days prior	16:30-20:00 HKT GMT+8
Major Release	2 weeks prior	03:00-12:00 HKT GMT+8

Nexusguard complies with the international standards for Service Providers, all changes undergo a thorough review by our Change Advisory Board. Risk Assessments are done and to be approved by major stakeholders within the group. This ensures that there will be minimal to null impact will be experienced by our clients and customers.

Severity Classifications

In Nexusguard, we value our commitment to our customers. We have defined a high level Service Level Agreement to our customers to ensure maximum service availability. A reference below is provided to clarify the various definitions of ticket priority and resolution time.

Incident Severity *	Definition
Urgent Severity (Priority 1)	The presence of an Urgent Severity Error implies that services cannot be substantially used, or have a major negative impact on the total system operation, system functionality, or system reliability with regard to customer's system or service availability with regard to customer's service.
High Severity (Priority 2)	The presence of a High Severity Error seriously affects the functionality of the services but can be circumvented so that the services can be used, or implies that a function in the Services cannot be used although other functions remain unaffected, or implies that the Services as a whole function but a certain function are somewhat give incorrect results or do not conform to the standards in the Documentation.
Normal Severity (Priority 3)	A Low Severity Error has no significant effect on the functionality of the Platform Services.

In line with our commitment is our Service Availability, using our cloud platform, our customer's are able to maximise the global capacity of Nexusguard. With this, we have defined our platform availability as follows:

Platform Availability	99.99%
Service Availability *	99.95%
Incident Handling - Acknowledgement	15 minutes
Urgent Severity Case - Service Recovery *	60 minutes
High Severity Case - Service Recovery *	120 minutes
Normal Severity Case - Service Completion *	240 minutes
Attack Handling - **Notification** - **Mitigation Fine Tuning**	 15 minutes 15 minutes

*** NOTE: Not applicable for Origin Protection InfraProtect Service.**

Contact us at
support@nexusguard.com
for any queries.

Follow us on Twitter
@Nexusguard

Join us on Facebook
www.facebook.com/NXG.PR

Follow our LinkedIn Page
www.linkedin.com/company/nexusguard