

Connectivity Monitoring Service

Service Description

Version 1.0 – 09/09/2026

Contents

1	Introduction	4
2	Business Outcome	5
3	What Does the Connectivity Monitoring Service Include?	6
3.1	Connectivity Monitoring Service Overview.....	6
3.1	Cost Plans	6
4	Service Components	7
4.1	Core Service Components	7
4.2	Proactive Monitoring	7
4.3	Incident Management – Connectivity.....	7
4.4	NG Managed Network Services.....	8
5	Service Levels.....	10
5.1	Fault Response Time	10
5.2	Service Level Exclusions	11
6	Prerequisites, Dependencies and Obligations	12
7	Appendix A: Definitions	13



Version Control

Current Version

Parameter	Value
Current Version	1.0
Release Date	09/09/2026
Author	Pat Rogers

Version History

Version	Date	Author	Description of Changes
1.0	09/07/2026	Pat Rodgers	Issue



1 Introduction

This Service Description describes Nasstar's Connectivity Monitoring Service. The Connectivity Monitoring Service is one of a suite of services within Nasstar's Digital Cloud adoption and enablement framework.

This Service Description assumes that all necessary pre-requisite work for solution design, solution delivery and/or other Professional Services will be completed prior to commencing Connectivity Monitoring Services. This Service Description does not apply to any other Services, including any work required on solution design, solution delivery or other Professional Services that may be required for implementation of Nasstar's Connectivity Monitoring Services or the connectivity itself.

Bespoke requirements for the Service or its configuration may be detailed in a Statement of Work or Service Agreement. The Statement of Work or Service Agreement will take priority over this Service Description in the event of any inconsistency between them.

In this Service Description, unless the context otherwise requires, defined terms will be given the meanings set out in Section 7 (Appendix A: Definitions) and all other terms will be interpreted in accordance with the other documents referred to or incorporated in the Contract.



2 Business Outcome

Nasstar's Connectivity Monitoring Service helps Customers maintain visibility of their WAN connectivity by providing 24x7 proactive monitoring of in-scope connectivity services and associated Customer Equipment. The Service is designed to identify service-impacting events, raise automated Incident Tickets, and support timely investigation of faults across Nasstar's connectivity services and permitted third-party connectivity services.

The Service enables Customers to benefit from continuous operational awareness across a mix of UK, international, public, private, mobile, broadband, ethernet, wireless, satellite or third-party connectivity by detecting faults, notifying the Customer, and managing applicable connectivity service Incidents through Nasstar's Service Desk.

The optional NG (Next Generation) Managed Network Services add a service management layer to help Customers govern the operational performance of their networking estate. Through Lite or Premium options, Customers can access structured service reviews, escalation support, contract management, risk register maintenance, performance review, incident and problem trend analysis, and continual service improvement activities aligned to their business priorities. The features of the NG Managed Network Services are out of scope of the Connectivity Monitoring Service and are only provided where NG Managed Network Services are expressly included in the Order Form / Contract.

Overall, the Connectivity Monitoring Service is designed to reduce operational blind spots, improve fault awareness, support faster incident triage, and provide Customers with a scalable monitoring and service management foundation for their UK and International connectivity services. It enables Customers to retain flexibility over their chosen connectivity and CE support models while benefiting from Nasstar's monitoring tools, Service Desk processes and expertise.



3 What Does the Connectivity Monitoring Service Include?

3.1 Connectivity Monitoring Service Overview

Nasstar's Connectivity Monitoring Service delivers 24x7 enterprise-class systems monitoring for connectivity services. Nasstar's Connectivity Monitoring Service requires access to the Customer Equipment (CE) used to terminate the connectivity service. Depending on the provisioned level of access and capabilities of the CE, Nasstar can monitor the status, health and performance of the Customer's connectivity at each of the Customer Sites covered by the Connectivity Monitoring Service.

The Connectivity Monitoring Service is designed for Customers who want an automated alerting service and incident management service for their connectivity services.

The Connectivity Monitoring Service proactively monitors the connectivity and CE status, and automatically identifies service impacting incidents

The Connectivity Monitoring Service includes optional NG (Next Generation) Managed Network Services with different Service Level options providing Customers with Customer Success Manager (CSM) resources who work closely with the Customer to align Nasstar resources with Customer business objectives and maximise Customer value realised from Nasstar's Connectivity Monitoring Service.

The table below summarises the Service Components included in the Connectivity Monitoring Service:

Service Components	Unit of Sale	Service Options
Proactive Monitoring	Per CE Device / connectivity interface	Included*
Incident Management – Connectivity	Per connectivity interface (underlay and / or overlay)	Included
NG Managed Network Services	Per Connectivity Monitoring Services estate	Optional**

*The provision of the Connectivity Monitoring Service is subject to the technical capability of the CE Devices, the presence of sufficient connectivity from Nasstar's management network and the level of access to the CE Devices that terminate the connectivity service.

** An NG (Next Generation) Managed Network Service must be purchased for the size of the connectivity services estate. This Service will only be provided if expressly included within the scope of contracted Services.

3.1 Cost Plans

The Connectivity Monitoring Service and optional extra Service Components included in this Service Description are billed as a one-off charge and thereafter a monthly recurring charge, in advance, throughout the Term of the Contract.



4 Service Components

4.1 Core Service Components

The Core Service Components detailed in this section describe the foundational service operations management activities delivered by Nasstar as part of Connectivity Monitoring Service.

1. Escalate major incidents for further investigation with Customer and connectivity service provider where applicable and as appropriate.
2. Participate in major incident investigations with connectivity service provider as appropriate.

The table below outlines the core Service Operations Management components:

Service Component	Description
Core Service Components	Below is an overview of the activities provided as a core service component when subscribing to a Nasstar Connectivity Monitoring Service: Incident Management – Management of incidents for in-scope service components through to resolution. Problem Management - proactively manage the lifecycle of problems with the goal of preventing future incidents and minimising the impact of incidents that cannot be prevented.*

More details of the Service components are detailed below.

* Problem management is restricted by the level of access the Customer provides Nasstar to the Customer Equipment.

4.2 Proactive Monitoring

Service Component	Description
Proactive Monitoring	The Proactive Monitoring Service Component provides 24x7 monitoring for Customer connectivity services and automatically identifies connectivity service faults and CE access faults. Nasstar's proactive monitoring tool continuously collects reachability and uptime status information about the connectivity service and CE devices that are covered by the Connectivity Monitoring Service. Identified Faults that breach the Time to Alarm time period will result in the proactive monitoring tool raising an alarm into Nasstar's Service Desk to automatically generate an Incident, which is logged and assigned to a Nasstar Service Desk engineer as an Incident Ticket for further investigation as part of the Incident Management Service Components. Incidents where the same Fault is no longer detected for the Time to Clear time period will result in the proactive monitoring tools raising an auto resolution trigger into Nasstar's Service Desk to automatically change the Incident Ticket to resolved.

4.3 Incident Management – Connectivity

Service Component	Description
Incident Management – Connectivity	The Incident Management Service Component provides Incident support for the Nasstar connectivity services or third-party connectivity services



This Service Component provides Incident support on Incidents logged with Nasstar's Service Desk through Nasstar's proactive monitoring tool or by a Customer notification.

Incidents qualified as Faults with the connectivity are managed through to resolution in accordance with the relevant connectivity service SLAs or escalated to third party providers in respect of Faults affecting the relevant third-party connectivity services.

Incidents qualified as Faults with the CE Devices by Nasstar in collaboration with the Customer and their onsite teams will be handed over to the Customer to manage the incident through to resolution with their hardware maintenance and support provider.

The Customer or Customer's hardware maintenance and support provider is responsible for the resolution of defective hardware or software, including connecting the device to the network, and ensuring the CE Device is provisioned with the same technical capability, configuration, software level and connectivity access level for Nasstar's management network to that of the defective CE Device.

The number of Incidents raised in respect of the Connectivity Monitoring Service will not be limited but will be reviewed on a regular basis and recommendations made from time to time.

All Incidents raised by a Customer notification must be logged by a Customer authorised named user registered with the Nasstar Service Desk.

4.4 NG Managed Network Services

The Next Generation (NG) Managed Network Services are available as one of the two (2) options: – Lite or Premium. The two service options are detailed below:

	Lite	Premium
Service Management:		
Quarterly Customer Success Manager (CSM)	x	
Monthly Customer Success Manager (CSM)		x
Management of Customer contact record, notification, and subscriptions.	x	x
Management of commercial and contract updates.	x	x
User access for portals	x	x
Establish and Maintain the Risk Register	x	x
Operational queries, escalation, and advisory services.	x	x
Document any approved process changes in the service design.	x	x
Operational Reviews:	Quarterly	Monthly
Escalation matrix review	x	x
Service performance review	x	x
Incident, Change and Request volumes and analysis.	x	x
Summary of Problem Management, Major Incidents, and Root Cause Analysis.	x	x
Drive Continual Service Improvement (CSI)	x	x



Governance of Nasstar ITIL processes on behalf of the Customer.	x	x
Customer CSAT – NPS.	x	x
Review Customer strategic objectives and plan key initiatives to support goals		x



5 Service Levels

5.1 Fault Response Time

5.1.1 Nasstar's Obligations

The Fault Response Time target for the services that make up the Connectivity Monitoring Service (calculated from time of registration of monitoring alert) are shown in the table below:

Priority	Definition	Response Time
P1	System/Site/Service is completely unavailable. Critical business impact	30 minutes
(critical)	P1 can only be declared if the Customer has purchased an Ethernet Service	24 x 7
P2	System/Site/Service severely degraded for all Users. Workaround is possible or solution can run on back-up	1 hour
(high)	Broadband / Mobile Data / Services are completely unavailable	24 x 7
P3	System/Site/Service is degraded*	2 Operating Hours
(medium)	A group of users are experiencing a degradation of service but are still able to work. Business critical work is not seriously impacted*	

*By default, a degradation of service is not registered as a Fault by Nasstar's Monitoring tool, it must be registered by a Customer notification logged by a Customer authorised named user registered with the Nasstar Service Desk.

Information Requests: General queries, advice and guidance related to the System/Site/Service from an authorised users carries an 8 Operating Hours response time.

Fault Resolution Times in respect to the connectivity are detailed in the relevant connectivity service Service Description

Fault Response Time in respect of the Connectivity Monitoring Service are not contractual obligations and do not carry any service credits if the times are not met.



5.2 Service Level Exclusions

Nasstar will not be liable or responsible for any failure to meet any Response Time targets where such failure is caused by or due to or in respect of any of the following:

- Planned Maintenance
- Emergency Maintenance
- Unsupported Hardware or Unsupported Software
- Unpatched CE
- denial of Service attack(s)
- Software bugs, unless such bugs are as a result of Nasstar's' default or negligence
- where the Contract otherwise states that Nasstar is not liable or responsible

Nasstar shall not be in breach of contract or otherwise liable to the Customer for any loss or damage (including to data, systems or programs) arising as a result of any CE or hardware or software becoming Unsupported Hardware or Unsupported Software or being classified as Unpatched CE.



6 Prerequisites, Dependencies and Obligations

The following additional pre-requisites are expected from the Customer to ensure a successful Service initiation and Service delivery:

- Each Customer Site covered by the Connectivity Monitoring Service must be connected to Nasstar's management network via a private network underlay / overlay.
- Each Customer Site covered by the Connectivity Monitoring Service must be connected to the internet and/or a private network underlay / overlay through Nasstar's connectivity services or third-party connectivity services.
- Nasstar's connectivity services are purchased separately to the Connectivity Monitoring Service and are subject to separate terms.
- Nasstar must have a written letter of authorisation, from the customer and their third-party connectivity service provider, to raise a Fault with the third-party connectivity service provider on the Customer's behalf, Otherwise the Customer will raise the Fault with the third-party connectivity service provider
- Each Customer Site must have a CE device where the monitored connectivity terminates, with an IP address, and Nasstar must have appropriate unrestricted access to its network interface so Nasstar's proactive monitoring tools can monitor the connectivity
- Appoint a single point of contact (for example, project manager) who will be the liaison between Nasstar and the Customer's project teams for the Service initiation and the continued Connectivity Monitoring Service
- Provide experienced resources to deliver the Customer's service initiation project responsibilities in a timely manner, including assistance with progressing the project, including but not limited to approving project docs, program plans, and acceptance testing plans.
- Provide Nasstar with such access to data, information systems, and facilities relevant to this engagement as may be reasonably necessary to enable it to implement the Service initiation and deliver the continued Connectivity Monitoring Service.
- Perform configuration changes on existing network components that are not managed by Nasstar and are necessary to interface with Nasstar's Monitoring tools, for example, VPN appliances, routers, firewalls, switches. Changes including but not limited to allowing required management and analytical flows between the CEs and Nasstar management tools.
- Customer provides administrative remote access to all Sites as required.
- Nasstar may charge additional fees or recover third-party costs, plus administrative overheads, where Nasstar's or Nasstar's third party fault resolution engineers are called out due for faults which Nasstar or Nasstar's third party connectivity service provider is not responsible.
- Internal communication to the Customer business personnel regarding works impacting operations.
- The Customer and Customer's third-party service providers who interact with Nasstar's Service Desk for all global sites must speak fluent English.



7 Appendix A: Definitions

In this Service Description, unless the context otherwise requires, these terms will be given the following meanings:

‘Contract’: a contract for the supply of Services between Nasstar and the Customer, whether in the form of a statement of work, service agreement, standalone order form, or other ordering document.

‘Customer Equipment (CE)’: any equipment at the Customer Site owned by the Customer or a third-party other than Nasstar or Nasstar’s third-party providers, which allows the Customer to obtain and/or receive the Services.

‘Customer Success Manager’: the Customer Success Manager (CSM) is the Customer’s primary interface for service delivery. The CSM governs and orchestrates service delivery activities within Nasstar to ensure contracted services are continually reviewed, improved, and delivered.

‘Customer Site’: the Customer’s premises at which Customer Equipment is located in relation to which the Network Monitoring Service is provided as specified in the Order / Contract.

‘Emergency Maintenance’: emergency maintenance required including all necessary equipment maintenance or network upgrades, where Nasstar is not able to provide the standard notice period for planned maintenance.

‘Fault’: any event or incident affecting connectivity covered by the Connectivity Monitoring Service.

‘Fault Response Time’: the period of time within which Nasstar will commence the applicable connectivity service Fault resolution process or notify the relevant third-party connectivity service provider of a Fault.

‘Incident’: A record of an unplanned interruption to a service or a reduction in service quality.

‘Incident Ticket’: The record which is raised in Nasstar’s Service Desk systems in relation to an impact to the connectivity services within scope of the Connectivity Monitoring Service. A unique ticket ID is automatically assigned.

IP Broadband (FTTP) Services’: a Service which uses a DSL fibre to the Customer Site connected to the relevant network to provide connectivity from the Customer Site to the internet or private WAN

‘Broadband (MPF Data Only) Services’: a Service which uses a copper line (Metallic Path Facility) connected to the relevant network to provide connectivity from the Customer Site to the internet or private WAN.

‘Broadband (SOGEA) Services’: a Service which uses a DSL fibre to the local street cabinet to the Customer Site and copper tail into the Customer Site to provide connectivity from the Customer Site to the internet or private WAN.

‘Broadband Services’: the IP Broadband (FTTP) Services, IP Broadband (MPF Data Only) Services and IP Broadband (SOGEA) Services as applicable.

‘Ethernet Service’: a Service which uses a leased line to provide connectivity from the Site to the internet or private WAN.

‘Mobile Data Services’: the WAN ICC Access Services which use mobile connectivity to enable the Customer to connect to the internet or private WAN.

‘Network Operator’: any telecommunications operator used by Nasstar or a third-party provider to deliver connectivity services to the Customer, as applicable, to and from a Customer Site.

‘Operating Hours’: the standard Nasstar Service Desk hours of 08:00 – 18:00 Monday-Friday, excluding bank and public holidays in England & Wales, unless otherwise specified in a Contract.

‘Planned Maintenance’: a period of time during which Nasstar or an affiliate, agent or third-party subcontractor is performing planned activities or planned maintenance which may impact the Service and this has been communicated in advance to the Customer.

‘Service Level’: an agreed level of service or target applicable to the Service as stated in this Service Description.

‘Services’: any services to be provided by Nasstar pursuant to the Contract, as selected and set out in the Contract (including any additional services as Nasstar may agree to provide in accordance with the



Contract), and as described in the relevant Service Descriptions and the other provisions of the Contract.

'Software': all application computer software and other computer programs comprised in the Customer Equipment and/or provided as part of the Service.

'Time to Alarm': The Time to Alarm is the amount of time in minutes for the proactive monitoring tool to raise an alarm after a qualifying fault is detected.

'Time to Clear': The Time to Clear is the amount of time in minutes from when a fault is no longer detected by the proactive monitoring tool and an auto resolution alarm is raised into Nasstar's Service Desk.

'WAN': a Wide Area Network being a network that connects multiple smaller networks, such as local area networks (LANs), across a large geographical area. A WAN can be a private network or a public network i.e. the internet.

'Unpatched CE': Customer Equipment that has been excluded from Nasstar's recommended software patch or upgrade scheduled timeslot.

'Unsupported Hardware': hardware which is not supported by the relevant manufacturer or in respect of which a hardware maintenance contract is not in place.

'Unsupported Software': software that is not supported by the relevant licensor or in respect of which a software maintenance contract is not in place.

