



Nokia WiFi Beacon

Beacon 4

Beacon 4 Product Guide

3TN-01772-AAAA-TCZZA
Issue 1
November 2025

Legal notice

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

This document includes Nokia proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of Nokia.

This document is intended for use by Nokia's customers ("You"/"Your") in connection with a product purchased or licensed from any company within Nokia Group of Companies. Use this document as agreed. You agree to notify Nokia of any errors you may find in this document; however, should you elect to use this document for any purpose(s) for which it is not intended, You understand and warrant that any determinations You may make or actions You may take will be based upon Your independent judgment and analysis of the content of this document.

Nokia reserves the right to make changes to this document without notice. At all times, the controlling version is the one available on Nokia's site.

No part of this document may be modified.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

Copyright and trademark: Nokia is a registered trademark of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective owners.

© 2025 Nokia.

Contents

About this document.....13

1 What's new.....19

1.1 Overview19

1.2 What's new in BBD Release 25.03a19

2 Beacon 4 unit data sheet.....21

2.1 Overview21

2.2 Beacon 4 part numbers and identification.....21

2.3 Beacon 4 general description23

2.4 Beacon 4 software and installation feature support28

2.5 Beacon 4 interfaces and interface capacity28

2.6 Beacon 4 LEDs30

2.7 Beacon 4 detailed specifications.....31

2.8 Beacon 4 functional blocks32

2.9 Beacon 4 responsible party33

2.10 Beacon 4 special considerations33

3 Install or replace a Beacon 4.....37

3.1 Overview37

3.2 Prerequisites37

3.3 Recommended tools37

3.4 Safety information37

3.5 Install a Beacon 438

3.6 Replace a Beacon 4.....39

3.7 Wall mount a Beacon 440

4 Configure Beacon 445

4.1 Overview45

GUI overview48

4.2 General configuration.....48

4.3 New password rules48

4.4 Logging in to the web-based GUI48

4.5 Beacon 4 WebGUI Menu49

4.6 Viewing overview information.....51

WAN Configuration	54
4.7 Overview	54
4.8 Configuring WAN Services	54
4.9 Viewing WAN Statistics	58
4.10 Configuring TR-069	60
4.11 Configuring TR-369	62
4.12 Configuring Static routing	63
4.13 Configuring QoS	64
LAN Configuration	68
4.14 Overview	68
4.15 Configuring DHCP IPv4	68
4.16 Configuring DHCP IPv6	70
4.17 Configuring DNS	72
4.18 Viewing LAN Statistics	75
WiFi Configuration	76
4.19 Overview	76
4.20 Configuring WiFi Network	76
4.21 Configuring Guest Network	79
4.22 Viewing Network Map, Adding WiFi Points, Renaming WiFi Points and Removing WiFi Points	81
4.23 Optimizing WiFi Network	85
4.24 Configuring Wireless 2.4 GHz	86
4.25 Configuring Wireless 5 GHz	87
4.26 Viewing WiFi Statistics	89
Devices	92
4.27 Overview	92
4.28 Viewing Device Information	92
Security Configuration	94
4.29 Overview	94
4.30 Configuring the Firewall	94
4.31 Configuring the MAC Filter	95
4.32 Configuring the IP Filter	97
4.33 Configuring Family Profiles	98
4.34 Configuring DMZ and ALG	105
4.35 Configuring Access Control	107
Advanced Settings	109
4.36 Overview	109
4.37 Configuring Port Forwarding	109

4.38	Configuring Port Triggering	110
4.39	Configuring DDNS	111
4.40	Configuring NTP	113
4.41	Configuring UPNP and DLNA	114
	Maintenance	115
4.42	Overview	115
4.43	Configuring the Password	115
4.44	Backing Up the Configuration	117
4.45	Restoring the Configuration	117
4.46	Upgrading Firmware	118
4.47	Diagnosing WAN Connections	119
4.48	Viewing Log Files	122
4.49	Viewing Container Management	123
4.50	Generating a delta configuration file	124
	Troubleshooting	126
4.51	Troubleshooting counters	126
4.52	Speed Test	127
5	Configure Beacon using a combined customized software package	131
5.1	Overview	131
5.2	Configuring Beacon using a Combined Customized Software Package	131
6	Environmental and Regulatory Compliance	133
6.1	Overview	133
6.2	For EU regulation market	133
6.3	For NAR regulation market	136



List of tables

Table 2-1	Beacon 4 identification	21
Table 2-2	Beacon 4 power supply ordering information	22
Table 2-3	Hardware parts required for Beacon 4 installations	22
Table 2-4	Beacon 4 function detail	24
Table 2-5	Support for TR-369 parameter categories	26
Table 2-6	Beacon 4 interface connection capacity	28
Table 2-7	Beacon 4 physical connections	29
Table 2-8	Beacon 4 LED indications	30
Table 2-9	Beacon 4 physical specifications	31
Table 2-10	Beacon 4 dimension data specifications	31
Table 2-11	Beacon 4 power consumption specifications	32
Table 2-12	Beacon 4 environmental specifications	32
Table 2-13	Responsible party contact information	33
Table 4-1	Beacon 4 WebGUI Menu	49
Table 4-2	<i>WAN services</i> parameters	56
Table 4-3	<i>WAN statistics</i> parameters	59
Table 4-4	<i>TR-069</i> parameters	61
Table 4-5	<i>TR-369</i> parameters	62
Table 4-6	<i>IP routing</i> parameters	64
Table 4-7	<i>QoS config</i> parameters	66
Table 4-8	<i>DHCP IPv4</i> parameters	69
Table 4-9	<i>Static DHCP</i> parameters	70
Table 4-10	<i>DHCP IPv6</i> parameters	71
Table 4-11	<i>DNS</i> parameters	74
Table 4-12	<i>LAN statistics</i> parameters	75
Table 4-13	<i>Add WiFi network</i> parameters	77
Table 4-14	<i>Guest network</i> parameters	80
Table 4-15	<i><Device></i> parameters	84
Table 4-16	<i>Wireless 2.4 GHz</i> parameters	87
Table 4-17	<i>Wireless 5 GHz</i> parameters	88
Table 4-18	<i>Neighboring AP</i> parameters	90

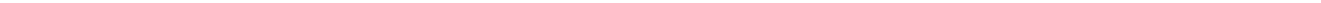
Table 4-19	<i>WLAN statistics</i> parameters.....	90
Table 4-20	<i>Firewall</i> parameters.....	95
Table 4-21	<i>MAC filter - Ethernet Interface</i> parameters	96
Table 4-22	<i>MAC filter - WiFi SSID</i> parameters	97
Table 4-23	<i>IP filter</i> parameters.....	98
Table 4-24	<i>ALG Configuration</i> parameters	106
Table 4-25	<i>DMZ Configuration</i> parameters.....	107
Table 4-26	<i>Access control</i> parameters.....	108
Table 4-27	<i>Trusted Network</i> parameters.....	108
Table 4-28	<i>Port forwarding</i> parameters.....	109
Table 4-29	<i>Port triggering</i> parameters.....	111
Table 4-30	<i>DDNS</i> parameters	112
Table 4-31	<i>NTP</i> parameters	113
Table 4-32	<i>Change password</i> parameters	116
Table 4-33	<i>Diagnostics</i> parameters	120
Table 4-34	<i>Log</i> parameters	122
Table 4-35	<i>Container management</i> parameters	123
Table 4-36	<i>Troubleshooting counters</i> parameters.....	127
Table 4-37	<i>Speed test</i> parameters.....	128
Table 6-1	Frequency bands and transmit power.....	135
Table 6-2	Applicable country codes	136

List of figures

Figure 2-1	Beacon 4 WiFi gateway/Beacon.....	23
Figure 2-2	Beacon 4 physical connections (back)	29
Figure 2-3	Beacon 4 bottom view	29
Figure 2-4	Beacon 4 LEDs.....	30
Figure 2-5	Single-residence WiFi CPE with Gigabit Ethernet.....	33
Figure 2-6	Sample safety label - CA	34
Figure 2-7	Sample safety label - EU/UK	34
Figure 2-8	Sample safety label - US	35
Figure 2-9	Sample safety label - AU	35
Figure 3-1	Beacon 4 wall mounting bracket.....	41
Figure 3-2	Beacon 4 in wall mount bracket.....	41
Figure 3-3	Fixing Beacon 4 on wall mount bracket.....	43
Figure 3-4	Beacon 4 to wall mount connection.....	44
Figure 4-1	Login page.....	48
Figure 4-2	Overview table in WAN services page.....	54
Figure 4-3	Create New Connection page	55
Figure 4-4	Create New Connection page - PPPoE Configuration	56
Figure 4-5	WAN Statistics page	59
Figure 4-6	WAN Statistics page info	59
Figure 4-7	TR-069 page.....	61
Figure 4-8	TR-369 page.....	62
Figure 4-9	IP routing page	63
Figure 4-10	QoS config page (L2 Criteria).....	65
Figure 4-11	QoS config page (L3 Criteria)	65
Figure 4-12	DHCP IPv4 page	69
Figure 4-13	DNS page (IPv4)	73
Figure 4-14	DNS page (IPv6)	74
Figure 4-15	LAN statistics page.....	75
Figure 4-16	WiFi network page.....	76
Figure 4-17	Add WiFi network page.....	77
Figure 4-18	WiFi network - example of SSID Configuration page	78

Figure 4-19	<i>Guest network page</i>	80
Figure 4-20	<i>Network map page</i>	81
Figure 4-21	<i><Device> page</i>	83
Figure 4-22	<i>Change the name of your WiFi point page</i>	84
Figure 4-23	<i>Advanced settings - 2.4 GHz tab</i>	86
Figure 4-24	<i>Advanced settings - 5 GHz tab</i>	88
Figure 4-25	<i>WiFi statistics page</i>	90
Figure 4-26	<i>Devices page</i>	92
Figure 4-27	<i>Device information page - L3 devices</i>	92
Figure 4-28	<i>Device Rename page</i>	93
Figure 4-29	<i>Firewall page</i>	94
Figure 4-30	<i>MAC filter page</i>	96
Figure 4-31	<i>IP filter page</i>	97
Figure 4-32	<i>Family profiles (Parental control) page</i>	99
Figure 4-33	<i>Add a profile page</i>	99
Figure 4-34	<i>Assign devices to family profile</i>	100
Figure 4-35	<i>Family profiles table</i>	100
Figure 4-36	<i>Family profile configuration page</i>	101
Figure 4-37	<i>DMZ and ALG page</i>	106
Figure 4-38	<i>Access control page</i>	107
Figure 4-39	<i>Port forwarding page</i>	109
Figure 4-40	<i>Port triggering page</i>	110
Figure 4-41	<i>DDNS page</i>	112
Figure 4-42	<i>NTP page</i>	113
Figure 4-43	<i>UPNP and DLNA page</i>	114
Figure 4-44	<i>Change password page</i>	116
Figure 4-45	<i>Backup and restore page</i>	117
Figure 4-46	<i>Backup and restore page</i>	118
Figure 4-47	<i>Firmware upgrade page</i>	118
Figure 4-48	<i>Example of upgrade status messages</i>	119
Figure 4-49	<i>Diagnostics page</i>	120
Figure 4-50	<i>Example of ping results</i>	121
Figure 4-51	<i>Example of traceroute results</i>	121

Figure 4-52	<i>Log page</i>	122
Figure 4-53	<i>Container management page</i>	123
Figure 4-54	<i>Delta CFG Tool page</i>	124
Figure 4-55	<i>Troubleshooting counters page</i>	126
Figure 4-56	<i>Speed test page</i>	128
Figure 6-1	<i>Recycling/take back/disposal of product symbol</i>	134



About this document

Purpose

This documentation set provides information about safety, features and functionality, ordering, hardware installation and maintenance, and software installation procedures for the current release.

Intended audience

This documentation set is intended for planners, administrators, operators, and maintenance personnel involved in installing, upgrading, or maintaining the Nokia WiFi Beacon.

The reader must be familiar with general telecommunications principles.

Safety information

For your safety, this document contains safety statements. Safety statements are given at points where risks of damage to personnel, equipment, and operation may exist. Failure to follow the directions in a safety statement may result in serious consequences.

Safety Information Examples



DANGER

Hazard

Danger indicates that the described activity or situation may result in serious personal injury or death; for example, high voltage or electric shock hazards.



WARNING

Equipment Damage

Warning indicates that the described activity or situation may, or will, cause equipment damage or serious performance problems.



CAUTION

Service Disruption

Caution indicates that the described activity or situation may, or will, cause service interruption.

Note: A note provides information that is, or may be, of special interest.

Acronyms and initialisms

The expansions and optional descriptions of most acronyms and initialisms appear in the glossary

Nokia quality processes

Nokia's WiFi Beacon manufacturing, testing, and inspecting practices are in compliance with TL 9000 requirements. These requirements are documented in the Fixed Networks Quality Manual 3FQ-30146-6000-QRZZA.

The quality practices adequately ensure that technical requirements and customer end-point requirements are met. The customer or its representatives may be allowed to perform on-site quality surveillance audits, as agreed upon during contract negotiations.

Documents

Documents are available using ALED or OLCS.

To download a ZIP file package of the customer documentation

- 1

Navigate to <http://customer.nokia.com/s/> and enter your user name and password. If you are a new user and require access to this service, contact your Nokia sales representative.
- 2

Select **Products**.
- 3

Type your product name in the **Find and select a product** field and click the search icon. Select a product.
- 4

Click **Downloads: ALED** to go to the Electronic Delivery: Downloads page.
- 5

Select **Documentation** from the list.
- 6

Select a release from the list.
- 7

Follow the on-screen directions to download the file.

END OF STEPS

To access individual documents

Individual PDFs of customer documents are also accessible through the Nokia Support Portal website.

-
- 1

Navigate to <http://customer.nokia.com/s/> and enter your user name and password. If you are a new user and require access to this service, contact your Nokia sales representative.
 - 2

Select **Products**.
 - 3

Type your product name in the **Find and select a product** field and click the search icon. Select a product.
 - 4

Click **Documentation: Doc Center** to go to the product page in the Doc Center.
 - 5

Select a release from the **Release** list and click **SEARCH**.
 - 6

Click on the PDF icon to open or Save the file.

END OF STEPS

Procedures with options or substeps

When there are options in a procedure, they are identified by letters. When there are required substeps in a procedure, they are identified by roman numerals.

Example of options in a procedure

At [Step 1](#), you can choose option a or b. At [Step 2](#), you must do what the step indicates.

- 1

This step offers two options. You must choose one of the following:
 - a. This is one option.
 - b. This is another option.
- 2

You must perform this step.

END OF STEPS

Example of required substeps in a procedure

At [Step 1](#), you must perform a series of substeps within a step. At [Step 2](#), you must do what the step indicates.

1

This step has a series of substeps that you must perform to complete the step. You must perform the following substeps:

- a. This is the first substep.
- b. This is the second substep.
- c. This is the third substep.

2

You must perform this step.

END OF STEPS

Multiple PDF document search

You can use Adobe Reader Release 6.0 and later to search multiple PDF files for a common term. Adobe Reader displays the results in a single display panel. The results are grouped by PDF file, and you can expand the entry for each file.

Note: The PDF files in which you search must be in the same folder.

To search multiple PDF files for a common term

1

Open Adobe Acrobat Reader.

2

Choose **Edit**→**Search** from the Acrobat Reader main menu. The Search PDF panel displays.

3

Enter the search criteria.

4

Select **All PDF Documents In**.

5

Select the folder in which to search using the drop-down menu.

6

Click **Search**.

Acrobat Reader displays the search results. You can expand the entries for each document by clicking on the + symbol.

END OF STEPS

Technical support

For details, refer to the [Nokia Support portal \(https://customer.nokia.com/support/s/\)](https://customer.nokia.com/support/s/).

For ordering information, contact your Nokia sales representative.

How to comment

Note to reviewers: The following "How to comment" text will appear in the final document when it is published. However, the feedback method described below is for use only on final documents. Please send your review comments to the author using the process you were given when you received this draft document.

To comment on this document, go to the [Online Comment Form \(https://documentation.nokia.com/comments/\)](https://documentation.nokia.com/comments/) or e-mail your comments to the [Comments Hotline \(mailto:comments@nokia.com\)](mailto:comments@nokia.com).



1 What's new

1.1 Overview

1.1.1 Purpose

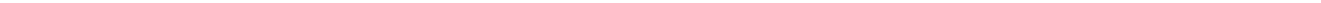
This chapter provides the details of features and other documentation changes updated in the product guide in each release.

1.1.2 Contents

1.1 Overview	19
1.2 What's new in BBD Release 25.03a	19

1.2 What's new in BBD Release 25.03a

The Product guide is a new guide in BBD Release 25.03a, issue 1. In future releases, this chapter will provide tables of the feature and document changes applicable to this guide.



2 Beacon 4 unit data sheet

2.1 Overview

2.1.1 Purpose

This chapter describes the Beacon 4 unit data sheet.

2.1.2 Contents

2.1 Overview	21
2.2 Beacon 4 part numbers and identification	21
2.3 Beacon 4 general description	23
2.4 Beacon 4 software and installation feature support	28
2.5 Beacon 4 interfaces and interface capacity	28
2.6 Beacon 4 LEDs	30
2.7 Beacon 4 detailed specifications	31
2.8 Beacon 4 functional blocks	32
2.9 Beacon 4 responsible party	33
2.10 Beacon 4 special considerations	33

2.2 Beacon 4 part numbers and identification

[Table 2-1, “Beacon 4 identification” \(p. 21\)](#) provides part numbers and identification information for Beacon 4.

Table 2-1 Beacon 4 identification

Ordering part number	Provisioning number	Description	CLEI Code	CPR	ECI/ Bar code
3TN01767AA	3TN01772AA	Beacon 4, US plug, 2.5G WAN, 2x1G LAN, WiFi 7 2+2	WDMFK10GRA	—	—
3TN01767AB	3TN01772AB	Beacon 4, CA/US plug, 2.5G WAN, 2x1G LAN, WiFi 7 2+2	WDMFL10GRA	—	—
3TN01767BA	3TN01772BA	Beacon 4, EU plug, 2.5G WAN, 2x1G LAN, WiFi 7 2+2	—	—	—
3TN01767CA	3TN01772CA	Beacon 4, UK plug, 2.5G WAN, 2x1G LAN, WiFi 7 2+2	—	—	—

Table 2-1 Beacon 4 identification (continued)

Ordering part number	Provisioning number	Description	CLEI Code	CPR	ECI/ Bar code
3TN01767DA	3TN01772DA	Beacon 4, AU plug, 2.5G WAN, 2x1G LAN, WiFi 7 2+2	—	—	—

Table 2-2, “Beacon 4 power supply ordering information” (p. 22) provides power supply ordering information for Beacon 4.

Table 2-2 Beacon 4 power supply ordering information

Ordering part number	Manufacturer	Applicable power supply model	Power information	Compliance detail	Notes
KIT: 3TN01767AA EMA: 3TN01772AA	Keli	KL-WA120150-H1/SW-WB330TEAW	12V 1.5A wall-mounted AC/DC power adapter with 2-pin US input plug	FCC/ETL ISED	—
	Moso	MS-V1500R120-018L0-US/SC980-U1			
KIT: 3TN01767AB EMA: 3TN01772AB	Keli	KL-WA120150-H1/SW-WB330TC6W	12V 1.5A wall-mounted AC/DC power adapter with 2-pin CA/US input plug	FCC/ETL ISED	—
	Moso	MS-V1500R120-018L0-US/SC980-U1			
KIT: 3TN01767BA EMA: 3TN01772BA	Keli	KL-AD3060VA/SW-WB330TEAW	12V 1.5A wall-mounted DC power adapter with 2-pin EU input plug	Europe, CE/CB certified	—
	Moso	MS-V1500R120-018L0-DE/SC980-V1			
KIT: 3TN01767CA EMA: 3TN01772CA	Keli	KL-AD3060VAB/SW-WB330BC	12V 1.5A wall-mounted AC/DC power adapter with 2-pin UK input plug	Europe, CE/CB certified	—
	Moso	MS-V1500R120-018L0-GB/SC980-B1			
KIT: 3TN01767DA EMA: 3TN01772DA	Keli	KL-WS120150-Q1/SW-WB463B	12V 1.5A wall-mounted AC/DC power adapter with 2-pin AU input plug	Australia, RSM/RCM	—
	Moso	MS-V1500R120-018L0-AU/SC980-S1			

Table 2-3, “Hardware parts required for Beacon 4 installations” (p. 22) lists the hardware parts required for mounting an Beacon 4.

Table 2-3 Hardware parts required for Beacon 4 installations

Part	Description
Beacon unit	The Beacon 4.
Wall mount bracket (Optional) (3TN02049AA)	The wall mount bracket is fastened to a wall. The Beacon 4 is seated in the wall mount bracket, with white color, 25 pcs per box.

Table 2-3 Hardware parts required for Beacon 4 installations (continued)

Part	Description
Mounting screws (Optional) (MCH000000293)	Two screws TA3.5x40 and anchors are required to mount the wall mount bracket. One screw M3.5X25 is required to fix the Beacon with the bracket together firmly when the Beacon is deployed on the wall.

2.3 Beacon 4 general description

WiFi is abundantly deployed in home networks. Users crave a seamless experience at home including effortlessly connecting their wireless devices to the network. Traditional WiFi networks require unique SSIDs for each of the access points or tedious set-up of WiFi extenders, which complicate the user experience. The Nokia WiFi network simplifies the user experience by providing a seamless mesh network with easy device onboarding and automated network optimization.

The overall Nokia WiFi solution is composed of one Nokia WiFi gateway (or Nokia WiFi Beacon) as root AP, one or more Nokia WiFi Beacons, the Nokia WiFi Care Portal for the operator's customer care team, and a mobile application for the end-user's self care.

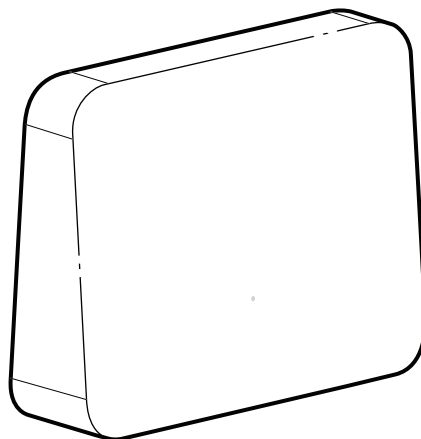
Note: The Nokia WiFi Care Portal can be accessed by the end user and the operator.

Beacon 4 can be deployed as either an Ethernet residential gateway or a WiFi Beacon in the Nokia WiFi solution. The residential gateway is the central point of the mesh network providing access to the broadband network (Internet) while the Beacon aids with extending the WiFi coverage to every corner of the home, providing seamless roaming to wireless connected devices.

The Beacon 4 has built-in concurrent dual-band Wi-Fi 802.11be networking with triple-play capability. Beacon 4 devices can be configured using the Nokia WiFi Mobile App, which can be downloaded on both iOS and Android devices.

The following figure shows the Beacon 4:

Figure 2-1 Beacon 4 WiFi gateway/Beacon



40398

The Beacon 4 provides the following functions and benefits:

- Dual-band WiFi7: concurrent IEEE802.11b/g/n/ax/be 2x2 2.4GHz and IEEE802.11a/n/ac/ax/be 2x2 5GHz
- Automatically decide on wireless router mode and Beacon mode in a mesh network
- One 2.5Gbase-T interface with RJ-45 connector for WAN and two 1Gbase-T interfaces with RJ-45 connectors for LAN
- Nokia intelligent EasyMesh
- Embedded edge analytics optimize network performance in real-time

Benefits:

- Latest Wi-Fi 7 technology that supports MLO operation allowing of up to 2 radio links to be assigned to a client enabling both higher speeds and lower latencies. An MLO link with 2.4 GHz + 5GHz can provide a maximum PHY rate of 3570 Mbps
- Additional features supported: Multiple RUs (MRU) per STA operation to avoid interference and increase efficiency, 40 MHz bandwidth in 2.4GHz radio, 160 MHz bandwidth in 5GHz radio, Higher efficiency with 4K QAM waveform
- PHY rate up to 688 Mb/s for 2.4 GHz and 2882 Mb/s for 5GHz
- Improves connection speeds throughout the home and provides WiFi where typically there would be none
- Client steering, channel optimization
- Real-time wireless spectrum scan and analysis
- High quality of service (QoS) video over WiFi
- Ease of setup and user intuitive information

The table below lists additional function detail:

Table 2-4 Beacon 4 function detail

Function	Detail
Installation	Desktop and wall mountable with optional wall mount bracket
Interfaces	• One RJ45 2.5 Gigabit Ethernet WAN port • Two RJ45 1 Gigabit Ethernet LAN ports • Supports 2x2 802.11b/g/n/ax/be 2.4 GHz wireless LAN (WLAN) interface • Supports 2x2 802.11a/n/ac/ax/be 5 GHz wireless LAN (WLAN) interface • Maximum Effective Isotropic Radiated Power (EIRP) on 2.4 GHz up to 100 mW and 5 GHz up to 200 mW • WPA support including WPA2 and WPA3 Personal encryption

Table 2-4 Beacon 4 function detail (continued)

Function	Detail
Router mode	• IPv4 and IPv6 The dual stack WAN (IPv4 and IPv6) can work in different IP address mode for DHCP mode (static/dynamic mode). • Point-to-Point Protocol over Ethernet (PPPoE) and IP over Ethernet (IPoE) • Network Address Translation (NAT), demilitarized zone (DMZ) and firewall • Dynamic Host Configuration Protocol (DHCP) and domain name system (DNS) proxy • Internet Group Management Protocol (IGMP) v2/v3 • Supports TR-069 with TR-181 datamodel. Supports USP/TR-369 • Supports virtual private network (VPN) pass- through for Point-to-Point Tunneling protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and IPSec • Port forwarding and DMZ/dynamic domain name system (DDNS) • Flexible video delivery options over Ethernet or wireless • Nokia WiFi mesh middleware
Beacon mode	• Supports IPv4/IPv6 UDP/TCP forwarding • Supports IPv4 for internal management • Supports TR-069 with TR-181 datamodel. • Supports USP/TR-369 • IGMP v2/v3 snooping • Flexible video delivery options over Ethernet or wireless • Nokia WiFi mesh middleware
Security	• Nokia Design for Security (DFSEC) compliant • Nokia Security Vulnerability Management (SVM) compliant • Immutable Hardware Root of Trust • Secure Boot • Secure Software Upgrading • Default Security Hardening • Anti-Brute Force Authentication Hardening • Cryptographic Sensitive Data Protection • (Provisionable) TLS/HTTPS-enabled OAM interfaces
LED	• Single multi-color LED for simple and intuitive status indication

Table 2-4 Beacon 4 function detail (continued)

Function	Detail
Regulatory compliance	• CB • CE • ETL • FCC • ISED • RCM • RSM

2.3.1 TR-069 object support for WiFi parameters

The Beacon 4 supports the status retrieval and configuration of the following WiFi parameters via TR-069:

- Channel
- SSID
- Password for WPA and WEP
- Tx power (transmission rate in dBm)

These are the same TR-069 object parameters that are supported in the GUI.

2.3.2 TR-369 parameter support

TR-369 parameter support has been introduced or enhanced for the parameter categories and functions listed in the following table:

For details about which parameters are supported, see your Nokia representative.

Table 2-5 Support for TR-369 parameter categories

Parameter category	Functionality
Diagnostics	Bulk data: collection, reports, HTTP, and encoding
	IP ping
	TR-143 Diagnostics
	Traceroute
	WiFi neighboring

Table 2-5 Support for TR-369 parameter categories (continued)

Parameter category	Functionality
End user functional features	Data model and vendor log
	IP interface configuration
	PPP interface
	WiFi: • Access Point configuration • Radio configuration • SSID configuration
Statistics and status monitoring	Device information, including processor and memory
	IP statistics Ethernet statistics Hosts
	WiFi radio statistics WiFi SSID statistics WiFi Access Point statistics WiFi Access Point Associated Device
Device Software Modules	TR157 software module life cycle management for third-party App dynamically installed to container.
Mesh middleware management	Data Element

2.3.3 Communication method to Nokia cloud management solution

The Beacon 4 communicates to the Nokia cloud management solution through MQTT and https.

The supported mechanism is specific to a customer deployment and the detailed description is available in the Customer Release Notes (CRN) of each release.

2.3.4 Software Module Managements

Beacon 4 supports Open Container Initiative (OCI) compliant software module life cycle management (LCM). The LCM uses Linux Containers (LXC), which is an operating system level virtualization technique, for running multiple isolated containers on the same host system. The life cycle of these containers is managed by TR-069 and TR-369 using the data-model parameters defined in TR-157 (which is merged with TR-181).

The Software Module Management data model objects are:

- Mange each software component via SoftwareModules.DeploymentUnit.
- Set software component execution environment via SoftwareModules.ExecEnv.
- Run software component and get the execution status via SoftwareModules.ExecutionUnit.

i Note: The available memory for third party applications needs a detailed study, considering the actual memory load of the current hardware, software, Beacon software evolution over

long time and the projected use by a third party application of the software. Therefore, Nokia suggests to review this case by case. Contact your Nokia support representative for more information.

2.3.5 TR-069 authentication using TLS and CA certificates

Beacon 4 devices support encrypted remote TR-069 management using TLS, as well as ACS authentication using SHA-256 pre-installed certificates.

If the ACS URL is set to the https://... format, by default, the connection will use TLS without authentication mode. The Beacon 4 can also authenticate the ACS using a pre-installed CA certificate.

2.4 Beacon 4 software and installation feature support

For information on installing or replacing the Beacon 4, see [Chapter 3, “Install or replace a Beacon 4”](#).

2.5 Beacon 4 interfaces and interface capacity

The table below describes the supported interfaces and interface capacity for Beacon 4 devices.

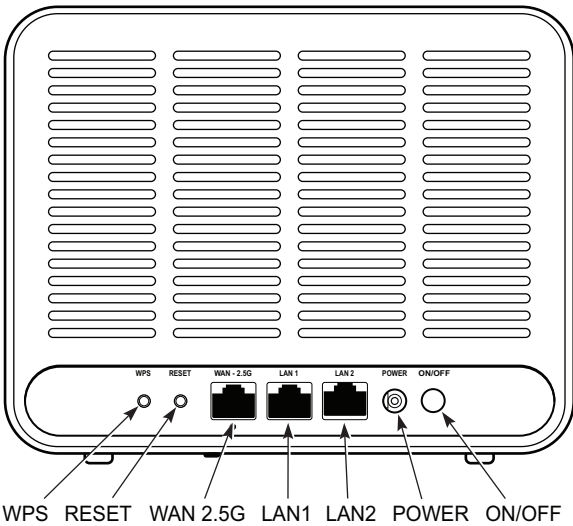
Table 2-6 Beacon 4 interface connection capacity

Device type and model	Maximum capacity		
	10GE LAN	1GE LAN	2.5GE WAN
Beacon 4	—	2	1

2.5.1 Beacon 4 connections and components

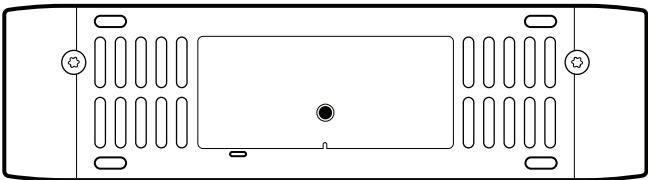
[Figure 2-2, “Beacon 4 physical connections \(back\)” \(p. 29\)](#) and [Figure 2-3, “Beacon 4 bottom view” \(p. 29\)](#) show the physical connections for Beacon 4.

Figure 2-2 Beacon 4 physical connections (back)



40399

Figure 2-3 Beacon 4 bottom view



40400

The table below describes the physical connections for Beacon 4 devices.

Table 2-7 Beacon 4 physical connections

Connection	Description
WPS button	This button is used to start the WiFi Protected Setup (WPS) for new WiFi devices.
Reset button	Pressing the reset button for less than 10 seconds reboots the Beacon. Pressing reset button for more than 10 seconds triggers normal factory reset, which retains the uploaded configuration files in the file system and can be restored whereas pressing the reset button 4 times consecutively within 2 seconds triggers a deep factory reset, which removes all previously uploaded configuration files from the device.
WAN port	This connection is provided through an 2.5GE interface.

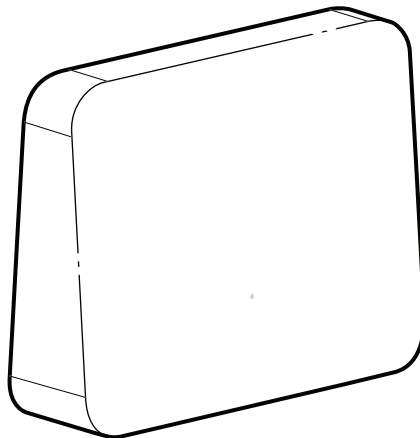
Table 2-7 Beacon 4 physical connections (continued)

Connection	Description
LAN 1/ LAN 2	This connection is provided through Ethernet RJ-45 connectors. Two 1Gbase-T interfaces with RJ45 connector are supported. The Ethernet ports can support both data and in-band video services on all two interfaces.
Power input	This connection is provided through the power connector. A power cable fitted with a barrel connector is used to make the connection.
On/Off button	This button powers the unit on or off.

2.6 Beacon 4 LEDs

The front of the Beacon 4 functions as a multi-color LED indicator. The LED color and pulse rate acts as a signal to the home user, which indicates the state of the Beacon 4 and the quality of its backhaul link.

Figure 2-4 Beacon 4 LEDs



40398

Table 2-8, “Beacon 4 LED indications” (p. 30) provides LED descriptions for the Beacon 4.

Table 2-8 Beacon 4 LED indications

LED color	LED behavior	Router mode	Extender mode	LED behavior description
Off	Off	✓	✓	Power off.
Blue-Green	Solid	✓		Good backhaul connection to the Internet.
	Solid		✓	Good backhaul connection. A link to the next node is available.

Table 2-8 Beacon 4 LED indications (continued)

LED color	LED behavior	Router mode	Extender mode	LED behavior description
Yellow	Solid		✓	Backhaul connection is successful but not optimal. A link to the next node is below standard.
	Slow pulsing	✓	✓	Configuration mode. The unit is waiting to be configured.
Red	Solid	✓		No connection to the Internet
	Solid		✓	Backhaul connection is successful but not optimal. A link to the next node is not operational.
	Fast pulsing	✓	✓	Factory reset.
White	Slow pulsing	✓	✓	WPS enabled.
	Solid	✓	✓	Powering on.
	3 sec quick pulse	✓	✓	WPS successful.
	Normal pulsing	✓	✓	Configuration mode to RGW/Extender mode.

2.7 Beacon 4 detailed specifications

The table below lists the physical specifications for the Beacon 4.

Table 2-9 Beacon 4 physical specifications

Description	Specification
Length	126 mm (4.96 in.)
Width	160 mm (6.29 in.)
Height	43.05 mm (1.69 in.)
Weight [within ± 0.5 lb (0.23 kg)]	285 g (0.62 lb)

Table 2-10, “Beacon 4 dimension data specifications” (p. 31) lists the dimension data specifications for Beacon 4.

Table 2-10 Beacon 4 dimension data specifications

Dimension	Specification
Packet size supported	1518
Number of IP addresses supported (or ranges)	In LAN network, the supported range is: • IPv4: 253 (support the IPv4 private network IP ranges) • IPv6: any allocated Global Unicast Addresses (GUA)
Number of supported WiFi clients (per radio, per device, per mesh)	120 per radio, 120 per device, 256 per mesh

Table 2-10 Beacon 4 dimension data specifications (continued)

Dimension	Specification
Number of supported beacons /APs in a mesh	4 (including root AP)
Number of supported WAN interfaces	8
Number of supported VLANs	2 to 4094
Number of LLIDs in the device	-
Number of priority queues, and overall buffer size	LAN port queues: 8; total buffer: 4MB WAN port queues: 8; total buffer: 4MB
Number of multicast groups (DACL entries)	256

Table 2-11, “Beacon 4 power consumption specifications” (p. 32) lists the power consumption specifications for the Beacon 4.

Table 2-11 Beacon 4 power consumption specifications

Maximum power (Not to exceed)	Condition	Minimum power	Condition
15 W	Ethernet ports and WiFi interfaces running at full load	7.2 W	WAN link active and connected to the Internet

Table 2-12, “Beacon 4 environmental specifications” (p. 32) lists the environmental specifications for Beacon 4.

Table 2-12 Beacon 4 environmental specifications

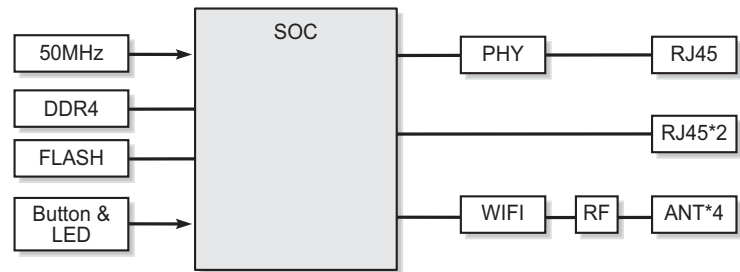
Mounting method	Temperature range and humidity	Altitude
On desk or shelf	Operating: -5°C to 45°C (23°F to 113°F) ambient temperature 95% relative humidity, non-condensing at 40°C	Contact your Nokia technical support representative for more information
	Storage: -20°C to 70°C (-68°F to 185°F)	

2.8 Beacon 4 functional blocks

Beacon 4 devices are single-residence units that support Wireless (WiFi) service. WiFi service on these devices is compliant with the IEEE 802.11 standard. In addition to the WiFi service, these devices transmit Ethernet packets to three RJ-45 Ethernet ports.

Figure 2-5, “Single-residence WiFi CPE with Gigabit Ethernet” (p. 33) shows the functional blocks for the Beacon 4.

Figure 2-5 Single-residence WiFi CPE with Gigabit Ethernet



40401

2.9 Beacon 4 responsible party

Table 2-13, “Responsible party contact information” (p. 33) lists the party in the US responsible for this device.

Table 2-13 Responsible party contact information

Legal Company name	Nokia Solutions and Networks OY	Nokia of America Corporation
Offices	Offices Nokia (https://www.nokia.com/contact-us/worldwide-offices/north-america/)	
Support	Support Nokia (https://www.nokia.com/support/)	
Other contacts	Contact us Nokia (https://www.nokia.com/contact-us/)	

2.10 Beacon 4 special considerations

This section describes the special considerations for Beacon 4 devices.

2.10.1 WiFi service

Beacon 4 devices feature WiFi service as well as data services. WiFi is a wireless networking technology that uses radio waves to provide wireless HSI and network connections. This device complies with the IEEE 802.11 standards, which the WiFi Alliance defines as the basis for WiFi technology.

WiFi standards and certifications

The WiFi service on Beacon 4 devices supports the following IEEE standards and Wi-Fi Alliance certifications (WFA132064):

- Compliant with IEEE 802.11 standards
- Certified for Wi-Fi 7
- Certified for WPA2 – Enterprise, Personal
- Certified for WPA3 – Enterprise, Personal
- Certified for Protected Management Frames

- Certified for Wi-Fi Agile Multiband, WMM®, Wi-Fi EasyMesh, Wi-Fi Protected Setup

Figure 2-6, “Sample safety label - CA” (p. 33) shows a sample safety label located on the bottom of the Beacon 4.

Figure 2-6 Sample safety label - CA



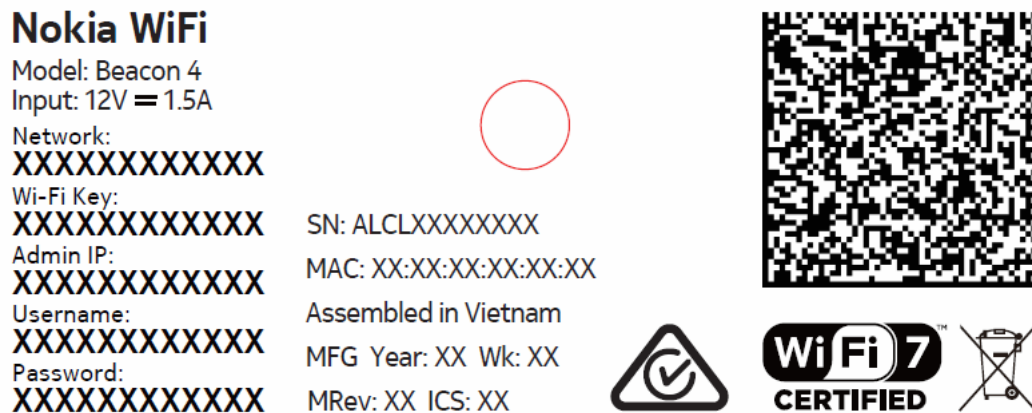
Figure 2-7 Sample safety label - EU/UK



Figure 2-8 Sample safety label - US



Figure 2-9 Sample safety label - AU



Nokia WiFi app configuration

The Nokia WiFi mobile app can be used to set up the Beacon 4 and manage the network.

It can be downloaded from the App Store for iOS <https://apps.apple.com/us/app/nokia-wifi/id1345278192> and the Google Play store for Android <https://play.google.com/store/apps/details?id=com.nokia.wifi>.

Information about the Nokia WiFi app can be found on the Nokia WiFi Help Center <https://wifi-helpcenter.nokia.com>

WiFi GUI features

Beacon 4 devices have HTML-based WiFi configuration GUIs.

2.10.2 Beacon 4 considerations and limitations

For details about the considerations and limitations, see the Customer Release Notes (CRN).

3 Install or replace a Beacon 4

3.1 Overview

3.1.1 Purpose

This chapter provides the steps to:

- Install a Beacon 4
- Replace a Beacon 4

3.1.2 Contents

3.1 Overview	37
3.2 Prerequisites	37
3.3 Recommended tools	37
3.4 Safety information	37
3.5 Install a Beacon 4	38
3.6 Replace a Beacon 4	39
3.7 Wall mount a Beacon 4	40

3.2 Prerequisites

Ensure that you have all required cables.

3.3 Recommended tools

You need the following tools:

- RJ-45 cable
- Paper clip

3.4 Safety information

Read the following safety information before installing the unit.

**DANGER****Hazard**

Hazardous electrical voltages and currents can cause serious physical harm or death. Always use insulated tools and follow proper safety precautions when connecting or disconnecting power circuits.

Make sure all sources of power are turned off and have no live voltages present on feed lines or terminals. Use a voltmeter to measure for voltage before proceeding.

Always contact the local utility company before connecting the enclosure to the utilities.

**CAUTION****Service Disruption**

Keep indoor devices out of direct sunlight. Prolonged exposure to direct sunlight can damage the unit.



Note: Observe the local and national laws and regulations that may be applicable to this installation.

Observe the following:

- The device should be installed in accordance with the applicable requirements of the NEC or CEC. Local authorities and practices take precedent when there is conflict between the local standard and the NEC or CEC.
- The device must be installed by qualified service personnel.
- indoor units must be installed with cables that are suitably rated and listed for indoor use.
- See the detailed specifications in the [Chapter 2, “Beacon 4 unit data sheet”](#) for the temperature ranges for these devices.

3.5 Install a Beacon 4

1

Place the unit on a flat surface, such as a desk or shelf.



Note: The Beacon 4 cannot be stacked with another or with other equipment. The installation requirements are:

- Allow a minimum 100 mm clearance above the top cover.
- Allow a minimum 50 mm clearance from the side vents.
- Do not place any heat source directly above the top cover or below the bottom cover.

2

Review the connection locations, as shown in [Figure 2-2, “Beacon 4 physical connections \(back\)”](#) (p. 29) and [Figure 2-3, “Beacon 4 bottom view”](#) (p. 29).

3

Connect the Ethernet cables to the RJ-45 ports and the WAN cable to the RJ-45 WAN port; see [Figure 2-2, “Beacon 4 physical connections \(back\)”](#) (p. 29) for the location of the RJ-45 ports and RJ-45 WAN port.

4

Connect the power cable to the power connector.



Note: Units must be powered by a Listed or CE approved and marked limited power source power supply with a minimum output rate of 12 V dc, 3 A. The polarity of the power adapter plug must match the Beacon 4.

5

Power up the unit by using the On/Off power switch.

6

Verify the LED status.

7

Activate and test the services.

8

If necessary, reset the Beacon 4.



Note: Resetting the device will return all settings to factory default values; any configuration customization will be lost.

a. Locate the **Reset** button as shown in [Figure 2-2, “Beacon 4 physical connections \(back\)”](#) (p. 29).

b. Insert the end of a straightened paper clip or other narrow object into the hole in the Reset button to reset the device.

END OF STEPS

3.6 Replace a Beacon 4

1

Power down the unit by using the On/Off power switch. See [Figure 2-3, “Beacon 4 bottom view”](#) (p. 29) for the connections on the Beacon 4.

2

Disconnect the WAN, Ethernet, and power cables from the Beacon 4; see [Figure 2-2, “Beacon 4 physical connections \(back\)”](#) (p. 29) for the connector locations on the Beacon 4.

3

Replace the Beacon 4 with the new device. The device can be placed on any flat surface, such as a desk or shelf.

4

Connect the Ethernet cables directly to the RJ-45 ports and the WAN cable directly to the RJ-45 port; see [Figure 2-2, “Beacon 4 physical connections \(back\)” \(p. 29\)](#) for the location of the RJ-45 ports and RJ-45 WAN port.

5

Connect the power cable to the power connector.



Note: Units must be powered by a Listed or CE approved and marked limited power source power supply with a minimum output rate of 12 V dc, 3 A. The polarity of the power adapter plug must match the Beacon 4.

6

Power up the unit by using the On/Off power switch.

7

Verify the LED status.

8

Activate and test the services.

9

If necessary, reset the Beacon 4.



Note: Resetting the device will return all settings to factory default values; any configuration customization will be lost.

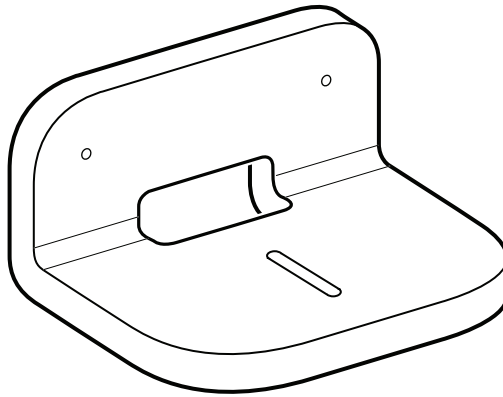
- a. Locate the Reset button on a Beacon 4 as shown in [Figure 2-2, “Beacon 4 physical connections \(back\)” \(p. 29\)](#).
- b. Insert the end of a straightened paper clip or other narrow object into the hole in the Reset button to reset the device.

END OF STEPS

3.7 Wall mount a Beacon 4

This section provides the steps to mount a Beacon 4.

Figure 3-1 Beacon 4 wall mounting bracket



40402

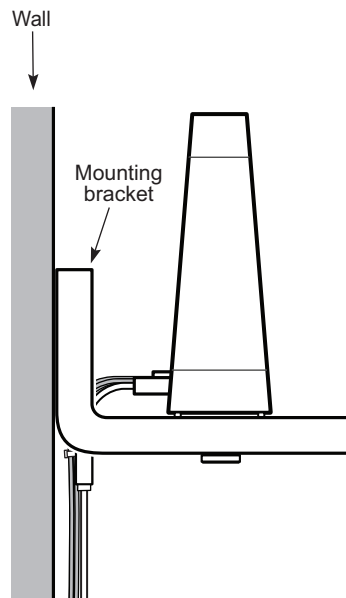
3.7.1 Procedure

Use this procedure to mount a Beacon 4 on a wall.

1

You can wall mount the Beacon 4 as shown in [Figure 3-2, “Beacon 4 in wall mount bracket” \(p. 41\)](#).

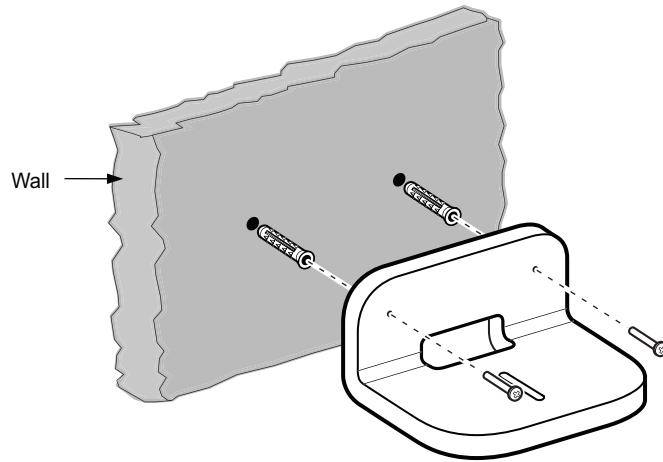
Figure 3-2 Beacon 4 in wall mount bracket



40405

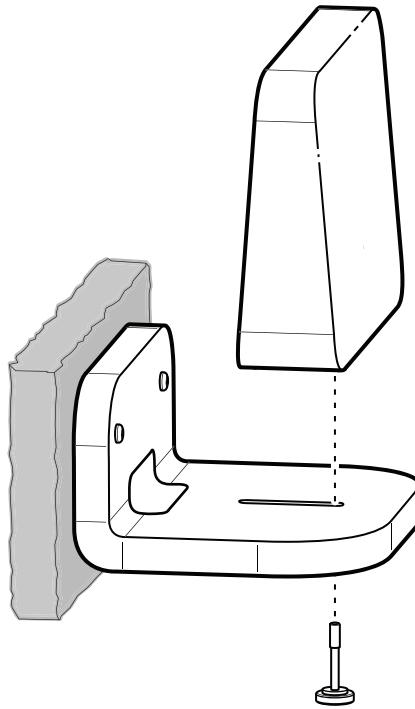
2

Mount the Beacon 4 on a wall using the wall mount bracket as shown in “Procedure” (p. 0).



40403

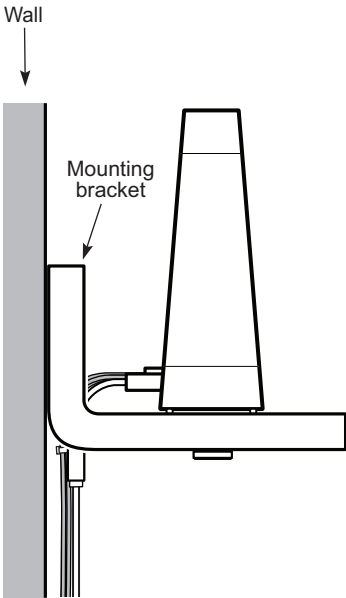
Figure 3-3 Fixing Beacon 4 on wall mount bracket



40404

- Determine the location of the two anchor holes for the wall mount bracket. The bracket can be used as a template for marking and drilling the holes.
It is recommended to use a level to ensure that the ONT unit is installed horizontally.
- Drill two holes into the wall and with the centers spaced 106.32 mm.
- Insert the two mounting screws and optional anchors into the holes.
- At this point, perform a test to ensure that the wall mount bracket fits securely over the screw heads. Mount the bracket flush to the wall so that it does not warp or twist.
- Install the Beacon 4 onto the wall mount bracket by placing the unit on the edge of the bracket and drill it in place with a screw from below to mount tightly. See [Figure 3-4, "Beacon 4 to wall mount connection" \(p. 44\)](#).

Figure 3-4 Beacon 4 to wall mount connection



40405

- f. Connect the power cord and other cables to the Beacon 4.

END OF STEPS

4 Configure Beacon 4

4.1 Overview

4.1.1 Purpose

This chapter describes the WebGUI configuration procedures.

4.1.2 Contents

4.1 Overview	45
GUI overview	48
4.2 General configuration	48
4.3 New password rules	48
4.4 Logging in to the web-based GUI	48
4.5 Beacon 4 WebGUI Menu	49
4.6 Viewing overview information	51
WAN Configuration	54
4.7 Overview	54
4.8 Configuring WAN Services	54
4.9 Viewing WAN Statistics	58
4.10 Configuring TR-069	60
4.11 Configuring TR-369	62
4.12 Configuring Static routing	63
4.13 Configuring QoS	64
LAN Configuration	68
4.14 Overview	68
4.15 Configuring DHCP IPv4	68
4.16 Configuring DHCP IPv6	70
4.17 Configuring DNS	72
4.18 Viewing LAN Statistics	75
WiFi Configuration	76
4.19 Overview	76

4.20 Configuring WiFi Network	76
4.21 Configuring Guest Network	79
4.22 Viewing Network Map, Adding WiFi Points, Renaming WiFi Points and Removing WiFi Points	81
4.23 Optimizing WiFi Network	85
4.24 Configuring Wireless 2.4 GHz	86
4.25 Configuring Wireless 5 GHz	87
4.26 Viewing WiFi Statistics	89
Devices	92
4.27 Overview	92
4.28 Viewing Device Information	92
Security Configuration	94
4.29 Overview	94
4.30 Configuring the Firewall	94
4.31 Configuring the MAC Filter	95
4.32 Configuring the IP Filter	97
4.33 Configuring Family Profiles	98
4.34 Configuring DMZ and ALG	105
4.35 Configuring Access Control	107
Advanced Settings	109
4.36 Overview	109
4.37 Configuring Port Forwarding	109
4.38 Configuring Port Triggering	110
4.39 Configuring DDNS	111
4.40 Configuring NTP	113
4.41 Configuring UPNP and DLNA	114
Maintenance	115
4.42 Overview	115
4.43 Configuring the Password	115
4.44 Backing Up the Configuration	117
4.45 Restoring the Configuration	117

4.46 Upgrading Firmware	118
4.47 Diagnosing WAN Connections	119
4.48 Viewing Log Files	122
4.49 Viewing Container Management	123
4.50 Generating a delta configuration file	124
Troubleshooting	126
4.51 Troubleshooting counters	126
4.52 Speed Test	127

GUI overview

This section provides an overview of the Beacon 4 WebGUI.

4.2 General configuration

For HTTP/HTTPS configuration procedures, refer to the **Nokia ONT Configuration, Management, and Troubleshooting Guide**.

4.3 New password rules

For security reasons, operators can mandate a change of password for the WiFi network and user accounts at the first login. Operators can also allow users to change passwords with or without password rules.

A pop-up message is displayed for users to change password for the WiFi network and user accounts at the first login.

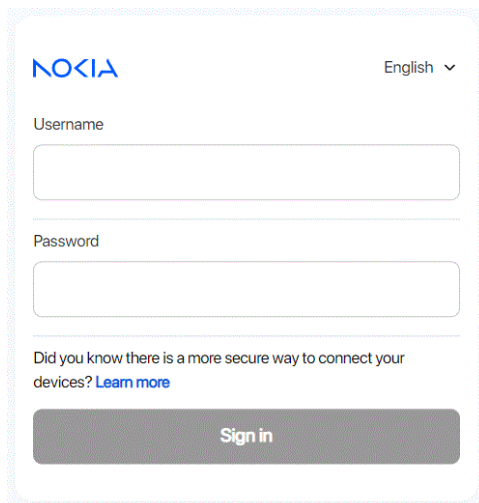
4.4 Logging in to the web-based GUI

1

Open a web browser and enter the IP address of the Beacon in the address bar.

The *Login* page displays.

Figure 4-1 Login page



The default gateway IP address must be same as the one printed on the device label. You can connect to this IP address using your web browser after connecting your PC to one of Ethernet ports of the Beacon or via WiFi connection. The static IP address of your PC must be in the

same default gateway subnet as the Beacon. You can also access the login page via "https://www.webgui.nokiawifi.com/" and " http://www.webgui.nokiawifi.com/".

2



CAUTION

Service Disruption

*If you forget the current username and password, press the **Reset** button for 10 seconds to reset the values to the default username and password provided at startup.*

*Pressing the **Reset** button for less than 10 seconds reboots the device.*

*Pressing the **Reset** button for more than 10 seconds performs a normal factory reset. Double-tick of the Reset button will trigger a Deep Factory reset.*

Enter your username and password in the *Login* page, as shown in [Figure 4-1, "Login page" \(p. 48\)](#).

The superadmin account is meant for the operator and the password is unique per device unless specified differently in customer specific pre configuration. Contact your Nokia representative to obtain the superadmin password for device.

The default end-user account name and the default password for this account are printed on the device label.

The superadmin user has access to all WebGUI features while the end-user account has only limited access to WebGUI features. This access for the end-user can be adapted with a WebGUI configuration file. Contact your Nokia representative to know the factory default settings of which WebGUI access is available to your end user or how to get a WebGUI configuration file.

3

Click **Sign in**. The *Overview* page displays.



Note: To help protect the security of your Internet connection, the application displays a pop-up reminder to change both the WiFi password and the Beacon password. To increase password security, use a minimum of 10 characters, consisting of a mix of numbers and upper and lower case letters.

END OF STEPS

4.5 Beacon 4 WebGUI Menu

The following table lists the main menu and sub-menu options in the Beacon 4 WebGUI:

Table 4-1 Beacon 4 WebGUI Menu

Main Menu	Sub-menu	Procedure Reference
Overview	-	4.6 "Viewing overview information" (p. 51)

Table 4-1 Beacon 4 WebGUI Menu (continued)

Main Menu	Sub-menu	Procedure Reference
WAN	WAN services	4.8 "Configuring WAN Services" (p. 54)
WAN	WAN statistics	4.9 "Viewing WAN Statistics" (p. 58)
WAN	TR-069	4.10 "Configuring TR-069" (p. 60)
WAN	TR-369	4.11 "Configuring TR-369" (p. 62)
WAN	Static routing	4.12 "Configuring Static routing" (p. 63)
WAN	Qos config	4.13 "Configuring QoS" (p. 64)
LAN	DHCP IPv4	4.15 "Configuring DHCP IPv4" (p. 68)
LAN	DHCP IPv6	4.16 "Configuring DHCP IPv6" (p. 70)
LAN	DNS	4.17 "Configuring DNS" (p. 72)
LAN	LAN statistics	4.18 "Viewing LAN Statistics" (p. 75)
WiFi	WiFi networks	4.20 "Configuring WiFi Network" (p. 76)
WiFi	Guest network	4.21 "Configuring Guest Network" (p. 79)
WiFi	Network map	4.22 "Viewing Network Map, Adding WiFi Points, Renaming WiFi Points and Removing WiFi Points" (p. 81)
WiFi	Optimizing WiFi Network	4.23 "Optimizing WiFi Network" (p. 85)
WiFi	Advanced settings	4.24 "Configuring Wireless 2.4 GHz" (p. 86)
WiFi	Advanced settings	4.25 "Configuring Wireless 5 GHz" (p. 87)
WiFi	WiFi statistics	4.26 "Viewing WiFi Statistics" (p. 89)
Devices	-	4.28 "Viewing Device Information" (p. 92)
Security	Firewall	4.30 "Configuring the Firewall" (p. 94)
Security	MAC filter	4.31 "Configuring the MAC Filter" (p. 95)
Security	IP filter	4.32 "Configuring the IP Filter" (p. 97)
Security	Family profiles	4.33 "Configuring Family Profiles" (p. 98)
Security	DMZ and ALG	4.34 "Configuring DMZ and ALG" (p. 105)
Security	Access control	4.35 "Configuring Access Control" (p. 107)
Advanced settings	Port forwarding	4.37 "Configuring Port Forwarding" (p. 109)
Advanced settings	Port triggering	4.38 "Configuring Port Triggering" (p. 110)
Advanced settings	DDNS	4.39 "Configuring DDNS" (p. 111)
Advanced settings	NTP	4.40 "Configuring NTP" (p. 113)
Advanced settings	UPNP and DLNA	4.41 "Configuring UPNP and DLNA" (p. 114)
Maintenance	Change password	4.43 "Configuring the Password" (p. 115)

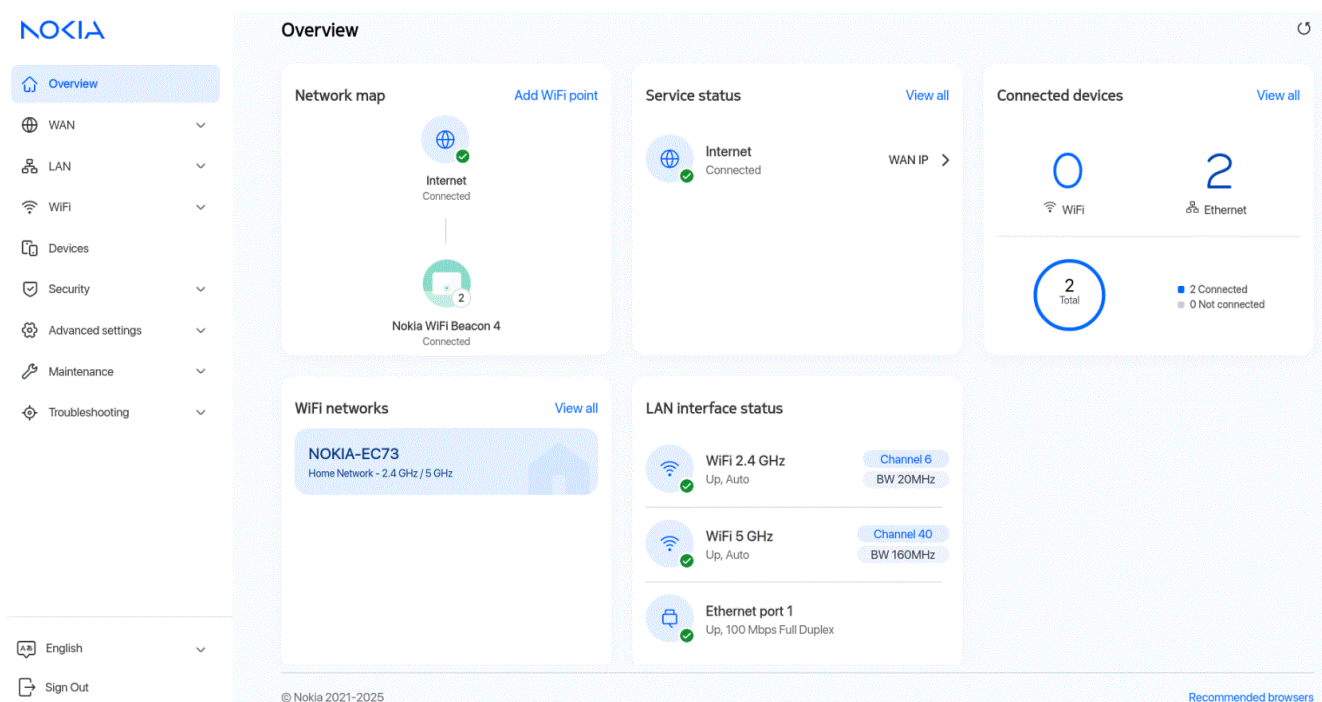
Table 4-1 Beacon 4 WebGUI Menu (continued)

Main Menu	Sub-menu	Procedure Reference
Maintenance	Backup and restore	4.44 "Backing Up the Configuration" (p. 117) 4.45 "Restoring the Configuration" (p. 117)
Maintenance	Firmware upgrade	4.46 "Upgrading Firmware" (p. 118)
Maintenance	Diagnostics	4.47 "Diagnosing WAN Connections" (p. 119)
Maintenance	Log	4.48 "Viewing Log Files" (p. 122)
Maintenance	Container management	4.49 "Viewing Container Management" (p. 123)
Maintenance	Delta configuration file	4.50 "Generating a delta configuration file" (p. 124)
Troubleshooting	Troubleshooting counters	4.51 "Troubleshooting counters" (p. 126)
Troubleshooting	Speed test	4.52 "Speed Test" (p. 127)

4.6 Viewing overview information

1

Click **Overview** from the left pane. The Overview page displays the following cards:



END OF STEPS

4.6.1 Network Map

Displays information about the status of the mesh network and connection to the internet. The status of the internet connection is defined by the presence of an IP address on the internet service. *Up* is indicated with green and *Down* is indicated with red.

Root device

Displays the mnemonic of the device. The colored indicator as well as the status under the name reflects the physical status of the WAN connection (4G/5G, PON port, WAN port). *Up* is Green, *Down* is Red.

Extender device

Displays the mnemonic of the device. The colored indicator as well as the status under the name reflects the physical status of the backhaul connection (Strong Signal = Green, Poor Signal = Amber, Not connected = red).

4.6.2 Radio Access

Displays the 4G, 5G or 6G signal connection status when a device is connected to an FWA receiver. Click the button to view the connection details.

4.6.3 Service Status

Displays the active status of the triple-play services.

Internet service

The internet service represents the presence of a WAN IP address for the routed network that has the internet attached to it. The card shows the WAN IP address (IPv4 and/or IPv6).

IPTV service

Shows the status of the IPTV service. If the IPTV flag is enabled on a routed service, the online or offline state is indicated by the presence of a WAN IP address for that routed service. If the IPTV is attached to a bridged service, the online or offline state is defined by the WAN uplink status.

4.6.4 WiFi Networks

Displays a network card per activated single or dual band WiFi network containing the bands supported, the name of the network and the type of network (bridge or routed).

4.6.5 Connected Clients

Displays the total number of online and offline clients connected to this device (single device or mesh system).

4.6.6 LAN Interface Status

Displays information about all the LAN ports of the device.

WiFi 2.4GHz

Shows the status of the 2.4GHz (Up/Down) network and the current band setting. This can either be auto which indicates Radio Resource Management is enabled or in the range 1-13 when manually configured.

WiFi 5GHz

Shows the status of the 5GHz network (Up/Down) and the current band setting. This can either be auto which indicates Radio Resource Management is enabled or is in the range 36-165 when manually configured.

Ethernet Port

Shows the status of the Ethernet ports (Up/Down), the sync rate (10Mbps, 100Mbps, 1Gbps, 2.5Gbps, 5Gbps, 10Gbps) and the duplex mode (Half duplex, Full duplex).

WAN Configuration

4.7 Overview

This section describes the WAN configuration procedures that can be performed from the following sub-menu options under the **WAN** menu:

Sub-menu	Procedure
WAN services	4.8 “Configuring WAN Services” (p. 54)
WAN statistics	4.9 “Viewing WAN Statistics” (p. 58)
TR-069	4.10 “Configuring TR-069” (p. 60)
TR-369	4.11 “Configuring TR-369” (p. 62)
IP routing	4.12 “Configuring Static routing” (p. 63)
Qos config	4.13 “Configuring QoS” (p. 64)

4.8 Configuring WAN Services

- 1
- Click **WAN**→**WAN services** in the left pane. The *WAN services* page displays the existing WAN connections in the *Overview* table. You can click on a connection to modify the connection configuration.
- The device supports dual-stack functionality on the WAN side, enabling it to use both IPv4 and IPv6 simultaneously. Typically, both addresses are assigned automatically through DHCP. However, the IPv4 address can also be configured manually (static), while IPv6 continues to be assigned automatically.

Figure 4-2 Overview table in WAN services page

WAN / WAN services

Overview

Service Name	Connection mode	Enable/Disable status	Service	IP address
1_TR069_INTERNET_OTHER_R_VID_0	Route	Enable	TR-069, Internet, IPTV	192.168.124.41

- 2
- Click **Add +** to create a WAN connection. The *Create New Connection* page displays.

Figure 4-3 Create New Connection page

← WAN / WAN services / 1_TR069_INTERNET_R_VID_3000

1 TR069_INTERNET_R_VID_3000

⌵

WAN connection list

1 TR069_INTERNET_R_VID_3000

Enabled

☒

Connection type

PPPoE

IP mode

IPv4&IPv6

NAT

☒

TR_OES

☒

Internet

☒

IPTV

☐

Enable VLAN

☒

VLAN ID

3000

VLAN PRI

0

WAN IP mode

PPPoE

Connection trigger

AlwaysOn

Username

abc

Password

Keep alive time

50

(0-60 seconds)

Keep alive retry

3

(0-10 times)

Echo value

150

MTU

1492

(0-1492)

Address method

AutoConfigured

Enable prefix delegation

☒

Prefix type

PrefixDelegation

Figure 4-4 Create New Connection page - PPPoE Configuration

← WAN / WAN services / 2_INTERNET_R_VID_980

↻

Delete

Save

WAN connection list

2_INTERNET_R_VID_980

Enabled

Connection type

PPPoE

IP mode

IPv4

NAT

TR-069

Internet

IPTV

Enable VLAN

3

Configure the following parameters:

Table 4-2 WAN services parameters

Field	Description
WAN connection list	Select a WAN connection from the list.
Enabled	Select the toggle button to enable the WAN connection.
Connection type	Select a connection type from the list: • IPoE • PPPoE
NAT	Select the toggle button to enable NAT. This option is applicable only if the connection mode is Route Mode .
TR-069	Select the toggle button to enable TR-069. This option is applicable only if the connection mode is Route Mode .
Internet	Select the toggle button to enable Internet. This option is applicable only if the connection mode is Route Mode .
IPTV	Select the toggle button to enable IPTV.

Table 4-2 WAN services parameters (continued)

Field	Description
Enable VLAN	Select the toggle button to enable VLAN. This option is applicable only if the connection mode is Route Mode .
VLAN ID	Enter the VLAN ID. Allowed values: 2 to 4094 In the bridge mode, this option is applicable only if the VLAN mode is Tunnel .
VLAN PRI	Enter the VLAN PRI. VLAN priority allows to assign a priority to outbound packets containing the specified VLAN ID. Allowed values: 0 to 7 In the bridge mode, this option is applicable only if the VLAN mode is Tunnel or Transparent .
WAN IP mode	Select an IP mode from the list: • DHCP • PPPoE This option is visible only if you select PPPoE as the connection type. • Static
Manual DNS	If the selected IP mode is IPv4 and the WAN IP mode is DHCP , enter the Domain Name Server (DNS) to be configured manually.
IPv4 Address	If the selected IP mode is IPv4 or IPv4&IPv6 and the WAN IP mode is Static , enter the static IPv4 address.
Netmask	If the selected IP mode is IPv4 or IPv4&IPv6 and the WAN IP mode is Static , enter the netmask.
Gateway	If the selected IP mode is IPv4 or IPv4&IPv6 and the WAN IP mode is Static , enter the gateway IP address.
Pri DNS	If the selected IP mode is IPv4 or IPv4&IPv6 and the WAN IP mode is Static , enter the primary Domain Name Server (DNS).
Sec DNS	If the selected IP mode is IPv4 or IPv4&IPv6 and the WAN IP mode is Static , enter the secondary Domain Name Server (DNS).
Ter DNS	If the selected IP mode is IPv4 or IPv4&IPv6 and the WAN IP mode is Static , enter the tertiary Domain Name Server (DNS).
Connection trigger	Select the connection trigger type from the list. The default option is Always On . This option is applicable only if the WAN IP mode is PPPoE.
Username	Enter the username to log in to the configuration server. This option is applicable only if the WAN IP mode is PPPoE .
Password	Enter the password to log in to the configuration server. Allowed values are limited to numbers, letters and special characters ! # + , - . / : = @ _ . This option is applicable only if the WAN IP mode is PPPoE .
Keep alive time	The PPPoE connection type triggers one heartbeat each, at the configured time interval to keep the session online. Allowed values: 5 to 60 seconds. This option is applicable only if the WAN IP mode is PPPoE .

Table 4-2 WAN services parameters (continued)

Field	Description
Keep alive retry	Configure the number of retries to check the Keep Alive status of the PPPoE session after time-out. Allowed values: 1 to 10. This option is applicable only if the WAN IP mode is PPPoE .
Echo value	Indicates the number of times the device sends messages to the server to check if the IP address is available or not. This option is applicable only if the WAN IP mode is PPPoE .
Address method	If the selected IP mode is IPv6 or IPv4&IPv6 , select the address method from the list: • AutoConfigured • DHCPv6 • DHCPv6_PD • DHCPv6_NA • Static
Enable prefix delegation	If the selected address method is AutoConfigured , select the toggle button to enable inclusion of the Identity Association (IA) for Prefix Delegation option in Solicit messages.
Prefix type	Displays mechanism through which the prefix was assigned or most recently updated.
IP Address (v6)	If the selected address method is Static , enter the IPv6 address.
Gateway (v6)	If the selected address method is Static , enter the gateway IPv6 address.
IPv6 address prefix	If the selected address method is Static , enter the IPv6 address prefix.
Pri DNS (v6)	If the selected address method is Static , enter the primary DNS IP address.
Sec DNS (v6)	If the selected address method is Static , enter the secondary DNS IP address.
DHCP option 50 persistent	Select the toggle button to enable DHCP Option 50 persistent.
Enable DHCP option 60	Select the toggle button to enable DHCP Option 60 (vendor class identifier).
Enable DHCP option 61	Select the toggle button to enable DHCP Option 61 (client identifier).
Enable DHCP option 77	Select the toggle button to enable DHCP Option 77 (user class information).
Enable DHCP option 90	Select the toggle button to enable DHCP Option 90 (authentication information).

4

Click **Save**. The connection is listed in the *Overview* table of the *WAN services* page.

END OF STEPS

4.9 Viewing WAN Statistics

1

Click **WAN**→**WAN statistics** in the left pane. The *WAN Statistics* page displays the following information for WAN ports.

Figure 4-5 WAN Statistics page

WAN / WAN statistics				
Overview				
Service Name	Connection mode	Enable/Disable status	Service	IP address
1_INTERNET_R_VID_980	Route	Enable	Internet	192.168.125.19
2_TR069_R_VID_1001	Route	Enable	TR-069	192.168.91.194
3_INTERNET_R_VID_1002	Route	Enable	Internet	192.168.92.101

2

Click on the service name to display the WAN statistics details page.

Figure 4-6 WAN Statistics page info

← WAN / WAN statistics / 1_TR069_INTERNET_OTHER_R_VID_0	
WAN port status	
Ethernet link status	Up
Sync speed	1000
Duplex mode	Full Duplex
Service	
WAN connection list	1_TR069_INTERNET_OTHER_R_VID_0
Enabled	
Service details	
Access type	access_dev1
Connection mode	Dynamic DHCP
VLAN	0
WAN link status	Linking
MAC address	48:41:7b:67:06:f1
WAN link status(v6)	Linking
Service statistics	
Counters	1_TR069_INTERNET_OTHER_R_VID_0
Bytes sent	18448
Bytes received	11186
Packets sent	147

Table 4-3 WAN statistics parameters

Field	Description
WAN port status	
Ethernet link status	Displays the Ethernet link status whether it is Up or Down.

Table 4-3 WAN statistics parameters (continued)

Field	Description
Sync speed	Displays the current synchronization speed of the WAN port, typically measured in Mbits per second (Mbps). It indicates the maximum data transfer rate that device can achieve between device WAN port to the next hop device in the network.
Duplex mode	Displays whether the WAN port is operating in full-duplex or half-duplex mode. Full-duplex: Allows simultaneous data transmission in both directions. Half-duplex: Allows data transmission in only one direction at a time.
Service	
WAN connection list	Select a WAN connection from the list.
Enabled	Displays whether WAN connection is either enabled or disabled.
Service details	
Access type	Displays the access type.
VLAN	Displays the VLAN mode based on WAN connection mode.
Primary DNS	Displays the primary DNS address.
Secondary DNS	Displays the secondary DNS address.
Ethernet link status	Displays the Ethernet status link whether it is Up or Down.
Pri DNS(v6)	Displays the primary DNS address. This option is available when the IP mode is IPv4 & IPv6 or IPv6 .
Service statistics	
Counters	Displays the counters details.
Bytes sent/received	Displays the bytes sent and received.
Packets sent/received	Displays the packets sent and received.
Errors sent/received	Displays the errors sent and received.
Unicast packets sent/received	Displays the unicast packets sent and received.
Discard packets sent/received	Displays the discard packets sent and received.
Broadcast packets sent/received	Displays the broadcast packets sent and received.
Unknown proto packets received	Displays the proto packets received.
Rx/Tx drops	Displays the Rx/Tx dropped packets.
Rx/Tx errors	Displays the Rx/Tx error packets.

END OF STEPS

4.10 Configuring TR-069

1

Click **WAN**→**TR-069** in the left pane. The *TR-069* page displays.

Figure 4-7 TR-069 page

WAN / TR-069

Save

Enable

Periodic inform enable

Periodic inform interval(s)

3600

URL

http://135.249.60.21:7003/cwmpWeb/C

Username

admin

Password

.....

Connection request username

itms

Connection request password

.....

2

Configure the following parameters:

Table 4-4 TR-069 parameters

Field	Description
Enable	Select the toggle button to enable CWMP function.
Periodic inform enable	Select the toggle button to enable periodic inform updates.
Periodic inform interval(s)	Enter the time between periodic inform updates, in seconds.
URL	Enter the URL of the auto-configuration server. Note: When you enter a HTTP URL, a security warning is displayed that a HTTPS URL is recommended. Click OK to continue.
Username	Enter the Username used to authenticate the CPE when making a connection to the ACS.
Password	Enter the Password used to authenticate the CPE when making a connection to the ACS.
Connect request username	Enter the Username used to authenticate an ACS making a Connection Request to the CPE.
Connect request password	Enter the Password used to authenticate an ACS making a Connection Request to the CPE.

3

Click **Save**.

END OF STEPS

4.11 Configuring TR-369

Note: The TR-369 configuration option is available only if the TR-181 data model is active.

1

Click **WAN**→**TR-369** in the left pane. The *TR-369* page displays.

Figure 4-8 TR-369 page

WAN / TR-369 Save

Enable TR369/USP

Controller endpoint ID

MTP protocol MQTT

Transport Select option

Broker address

Broker Port 1883

Username

Password

2

Configure the following parameters:

Table 4-5 TR-369 parameters

Field	Description
Enable TR369/USP	Select the toggle button to enable TR-369/USP and click Save .
Controller endpoint ID	Enter the controller endpoint ID.
MTP Protocol	Select the MTP protocol from the list (currently only MQTT is supported).

Table 4-5 TR-369 parameters (continued)

Field	Description
Transport	Select the transport option from the list: • TCP/IP • TLS Note: If you attempt to change the configuration from TLS to TCP/IP, a security warning is displayed that this option poses security risks. Click OK to continue.
Broker address	Enter the broker IP address.
Broker port	Enter the broker port number.
Username	Enter the username to authenticate with MQTT broker.
Password	Enter the password to authenticate with MQTT broker.

3 _____
Click **Save**.

END OF STEPS _____

4.12 Configuring Static routing

1 _____
Click **WAN**→**Static routing** in the left pane. The *IP routing* page displays.

Figure 4-9 IP routing page

WAN / Static routing

IP routing

Enable IP routing

Destination IP address

Destination netmask

Gateway

IPv4 interface

Forwarding policy ⓘ

Add

0.0.0.0

1_TR069_INTERNET_OTHER_R_VID_0

Select option

2

Configure the following parameters:

Table 4-6 IP routing parameters

Field	Description
Enable IP routing	Select the toggle button to enable IP routing.
Destination IP address	Enter the destination IP address.
Destination netmask	Enter the destination netmask.
Gateway	Enter the gateway IP address.
IPv4 interface	Select an IPv4 interface from the list.
Forwarding policy	Select a forwarding policy from the list.

3

Click **Add**. The IP route is added to the *IP routing table*.

END OF STEPS

4.13 Configuring QoS

1

Click **WAN→QoS config** in the left pane. The *QoS config* page displays.

Figure 4-10 QoS config page (L2 Criteria)

WAN / QoS config

Type

L2 Criteria

Classification criteria

Source Mac

Ex. AA:BB:CC:DD:EE:FF

Enable source MAC mask

Source MAC mask

Exclude

Interface

Select option

Classification row

DSCP remark

Range 0-63

802.1p Remark

Range 0-7

Figure 4-11 QoS config page (L3 Criteria)

WAN / QoS config

Type

L3 Criteria

Classification criteria

Protocol

None

Exclude

Applications

Customer Setting

Source IP

Exclude

Source IP Mask

Dest IP

Exclude

Dest IP Mask

Source Port

Exclude

Source Port Max

Destination Port

Exclude

Dest Port Max

802.1p

Interface

Select Option

2

Configure the following parameters:

Table 4-7 QoS config parameters

Field	Description
Type	Select a QoS service layer type from the list: • L2 Criteria • L3 Criteria
Classification criteria (L2)	
Source MAC	Enter the source MAC address.
Enable source MAC mask	Select the toggle button to enable the source MAC mask. This button is disabled by default.
Source MAC mask	Enter the source MAC mask address. The syntax is for example: FF:FF:FF:00:00:00 which must be a continuous bit mask pattern on this device. This field is visible only if the Enable source MAC mask button is enabled.
Interface	Select an interface from the list.
Classification criteria (L3)	
Protocol	Select a protocol from the list.
Application	Select an application from the list or select Custom Settings and enter an application name.
Source IP	Enter the source IP address.
Source IP mask	Enter the source IP address netmask.
Destination IP	Enter the destination IP address.
Destination IP mask	Enter the destination IP address netmask.
Source port	Enter the source port number.
Source port max	Enter the values for the source port max (highest port number).
Destination port	Enter the destination port number.
Destination port max	Enter the values for the destination port max (highest port number).
802.1p	Indicates whether 802.1p is enabled.
Interface	Select an interface from the list.
Classification row	
DSCP remark	Enter the value for the DSCP remark (applicable only for L3 criteria). Allowed values: 0 to 63
802.1p Remark	Enter the value for the 802.1p remark. Allowed values: 0 to 7
Forwarding policy	Enter the number for the forwarding policy. Allowed values: 1 to 7

3

Click **Add** to add a QoS policy.

END OF STEPS

LAN Configuration

4.14 Overview

This section describes the LAN configuration procedures that can be performed from the following sub-menu options under the **LAN** menu:

Sub-menu	Procedure
DHCP IPv4	4.15 "Configuring DHCP IPv4" (p. 68)
DHCP IPv6	4.16 "Configuring DHCP IPv6" (p. 70)
DNS	4.17 "Configuring DNS" (p. 72)
LAN statistics	4.18 "Viewing LAN Statistics" (p. 75)

4.15 Configuring DHCP IPv4

- 1
- Click **LAN**→**DHCP IPv4** in the left pane. The *DHCP IPv4* page displays.

Figure 4-12 DHCP IPv4 page

LAN / DHCP IPv4

IPv4 address

192.168.18.1

Subnet mask

255.255.255.0

DHCP enable

DHCP start IP address

192.168.18.2

DHCP end IP address

192.168.18.253

DHCP lease time

1440

(5~129600 mins, or 0 means 1 day)mins.

Primary DNS

Secondary DNS

Save

Static IPv4 address reservations

MAC address

IPv4 address

Add

2

Configure the following LAN parameters:

Table 4-8 DHCP IPv4 parameters

Field	Description
IPv4 address	Enter the IPv4 address of the Beacon.
Subnet mask	Enter the subnet mask of the Beacon.
DHCP enable	Select the toggle button to enable DHCP. If this toggle button is not enabled, the DHCP functionality cannot be used. you need not configure DHCP start IP address, DHCP end IP address and DHCP lease time if this toggle button is not enabled.

Table 4-8 DHCP IPv4 parameters (continued)

Field	Description
DHCP start IP address	Enter the starting range of the DHCP IP address.
DHCP end IP address	Enter the ending range of the DHCP IP address.
DHCP lease time	Enter the DHCP lease time (in minutes). Allowed values: 5 to 129600 minutes or 0 for 1 day
Primary DNS	Enter the primary DNS IP address.
Secondary DNS	Enter the secondary DNS IP address.

- 3 Click **Save**.
- 4 Configure the Static DHCP parameters.

Table 4-9 Static DHCP parameters

Field	Description
MAC address	Enter the hexadecimal MAC address to associate with the LAN.
IPv4 address	Enter the IPv4 address to associate with the bound MAC address.

- 5 Click **Add**. Repeat steps 4 and 5 for all MAC addresses to be bound.

END OF STEPS

4.16 Configuring DHCP IPv6

- 1 Click **LAN→DHCP IPv6** in the left pane. The *DHCP IPv6* page displays.

LAN / DHCP IPv6 Save

LAN prefix configuration

Prefix Config

Static

Static IPv6 prefix

2003:10:10:e13::/64

IPv6 address method

Address method

Stateless Address Autoconfig (SLAAC)

Stateful DHCPv6

Stateless Address Autoconfig (SLAAC) ✓

Receive additional options via DHCPv6

Advanced router advertisement configuration

Maximum interval for periodic RA messages

600

secs

Minimum interval for periodic RA messages

200

secs

2

Configure the following parameters:

Table 4-10 DHCP IPv6 parameters

Field	Description
LAN prefix configuration	
Prefix Config	Select a prefix configuration option from the list: • Use WAN provided prefix (prefix is obtained from the WAN) • Static (enables you to enter the prefix)
Interface	This field displays if you select the Use WAN provided prefix option from the Prefix Config list. Select a WAN connection interface from the list.
Received IPv6 prefix	This field displays the received IPv6 prefix. This field is displayed only when Prefix Config is set to Use WAN provided prefix .
Static IPv6 prefix	This field displays the static IPv6 prefix. This field is displayed only when Prefix Config is set to Static .
IPv6 address method	
Address method	Select a address method option from the list: • Stateless Address Autoconfig (SLAAC) • Stateful DHCPv6

Table 4-10 DHCP IPv6 parameters (continued)

Field	Description
Enable stateless and stateful DHCPv6 simultaneously	Select the toggle button to enable stateless or stateful DHCPv6 simultaneously. This parameter is visible only if the Address method is Stateful DHCPv6 .
DHCP Start IP Address	Enter the starting range of the DHCP IP address. This parameter is visible only if the address method is Stateful DHCPv6 .
DHCP End IP Address	Enter the ending range of the DHCP IP address. This parameter is visible only if the address method is Stateful DHCPv6 .
Received additional options via DHCPv6	Select the toggle button to enable additional options via DHCPv6. This field is displayed only when Address method is set to Stateless Address Autoconfig (SLAAC) .
Advanced router advertisement configuration	
Maximum interval for periodic RA messages	Enter the maximum interval (in seconds) for periodic Router Advertisement messages. Allowed values: 4 to 1800 seconds.
Minimum interval for periodic RA messages	Enter the minimum interval (in seconds) for periodic Router Advertisement messages. Allowed values: 4 to 1800 seconds

3

Click **Save**.

END OF STEPS

4.17 Configuring DNS

4.17.1 IPv4 DNS configuration

1

Click **LAN→DNS→IPv4** in the left pane. The *DNS* page displays.

Figure 4-13 DNS page (IPv4)

LAN / DNS

IPv4

IPv6

DNS Proxy

Save

Domain Name

IPv4 address

Add

Origin Domain

New Domain

Add

Static DNS entries

Domain Name	IPv4 address	Delete
www.webgui.nokia.com	192.168.18.1	Delete

2

Configure the following parameters:

- a. Select the **DNS proxy** toggle button to enable the DNS proxy and click **Save**.
- b. Configure the following:
 - 1. Enter the domain name in the Domain Name field.
 - 2. Enter the domain IP address in the IPv4 Address field.
 - 3. Click **Add**.
- c. Configure the following:
 - 1. Enter the origin domain name in the Origin Domain field.
 - 2. Enter the new domain name in the New Domain field.

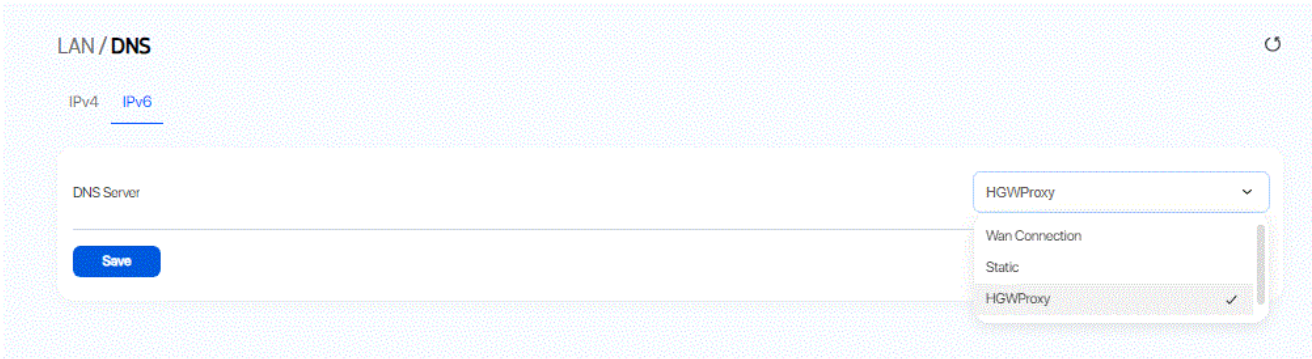
3. Click **Add** to associate an origin domain with a new domain.
- The *DNS* table displays the configured domain names and the associated IPv4 address. Click **Delete** to delete the table entries.

END OF STEPS

4.17.2 IPv6 DNS configuration

- 1
- Click **LAN**→**DNS**→**IPv6** in the left pane. The *DNS* page displays.

Figure 4-14 DNS page (IPv6)



- 2
- Configure the following parameters

Table 4-11 DNS parameters

Field	Description
DNS Server	Select DNS server option from the list: • Wan Connection (Server address is obtained from the WAN.) • Static (enables you to enter the address.) • HGWProxy (The Home Gateway acts as DNS Proxy).
Preferred DNS	Enter the preferred IPv6 address. This parameter is visible only if the DNS Server is Static .
Alternate DNS	Enter the Alternate IPv6 address. This parameter is visible only if the DNS Server is Static .
Interface	This field is displayed if you select the Wan Connection option from the DNS Server list.

3

Click **Save**.

END OF STEPS

4.18 Viewing LAN Statistics

1

Click **LAN**→**LAN statistics** in the left pane. The *LAN statistics* page displays the following information.

Figure 4-15 LAN statistics page

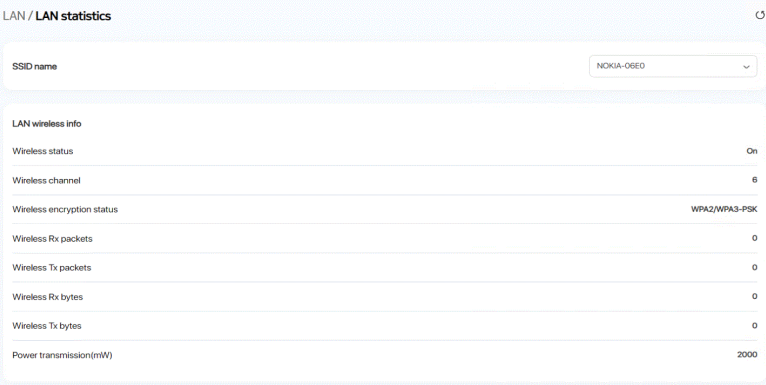


Table 4-12 LAN statistics parameters

Field	Description
SSID name	Select an SSID from the list.
LAN Wireless info	Displays the wireless status, wireless channel, encryption status, received and transmitted bytes and packets and power transmission in mW.
LAN Ethernet info	Displays the Ethernet status IP address, subnet mask, MAC address, received and transmitted bytes and packets.
Info	Displays the information of each such as status, duplex mode, maximum bit rate, packets received and sent, CRC errors, and so on.

END OF STEPS

WiFi Configuration

4.19 Overview

This section describes the WiFi configuration procedures that can be performed from the following sub-menu options under the **WiFi** menu:

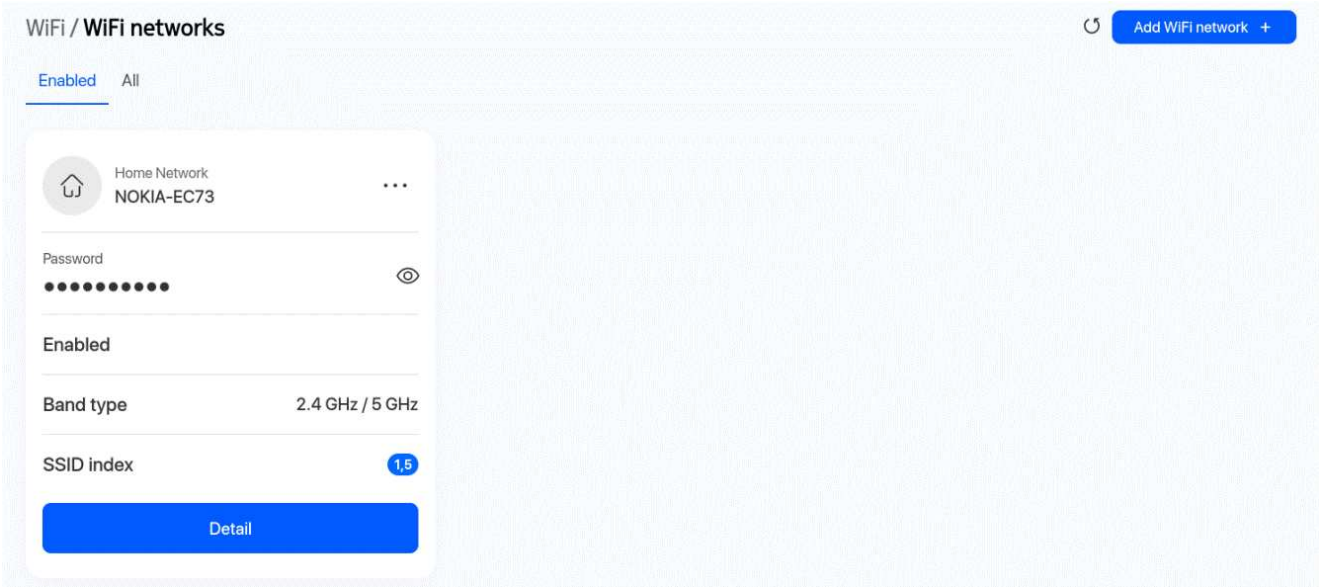
Sub-menu	Procedure
WiFi networks	4.20 "Configuring WiFi Network" (p. 76)
Guest network	4.21 "Configuring Guest Network" (p. 79)
Network map	4.22 "Viewing Network Map, Adding WiFi Points, Renaming WiFi Points and Removing WiFi Points" (p. 81)
Optimizing WiFi Network	4.23 "Optimizing WiFi Network" (p. 85)
Advanced settings	4.24 "Configuring Wireless 2.4 GHz" (p. 86)
Advanced settings	4.25 "Configuring Wireless 5 GHz" (p. 87)
WiFi statistics	4.26 "Viewing WiFi Statistics" (p. 89)

4.20 Configuring WiFi Network

1

Click **WiFi**→**WiFi network** in the left pane. The *WiFi network* page displays the existing WiFi networks. You can click **Detail** on a network to view the network details.

Figure 4-16 WiFi network page

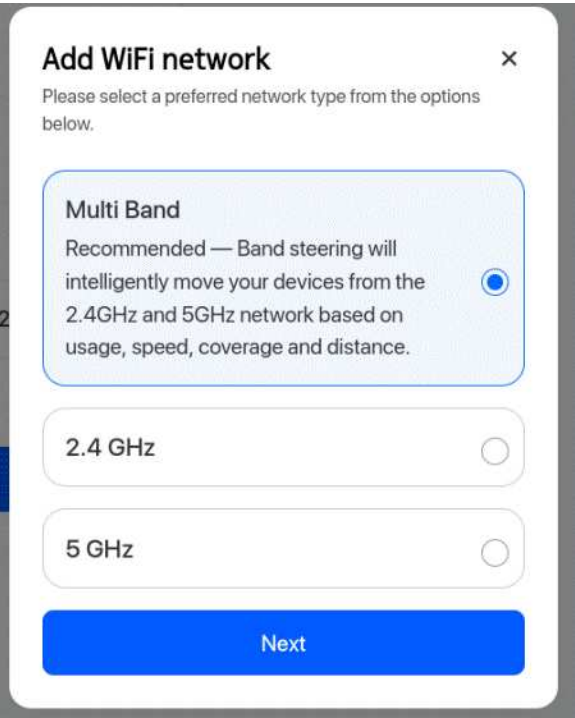


2

Click **Add WiFi network +** to create a WiFi network. The *Add WiFi network* page displays.

 **Note:** The **Add WiFi point** option is displayed only when the mesh feature is enabled.

Figure 4-17 Add WiFi network page



3

Configure the following parameters:

Table 4-13 Add WiFi network parameters

Field	Description
Multiband	Select this option to configure a multiband wireless network on all supported bands. This option is recommended. Your devices will roam to a different wireless band based on usage, speed, coverage and distance. The wireless encryption of this network is WPA3-Personal Transition.
2.4 GHz	Select this option to configure a 2.4 GHz wireless network. This might be needed if some older devices have issues connecting to a band-steering network. The wireless encryption of this new network is WPA2-Personal.

Table 4-13 Add WiFi network parameters (continued)

Field	Description
5 GHz	Select this option to configure a 5 GHz wireless network. This might be needed if some older devices have issues connecting to a band-steering network. The wireless encryption of this new network is WPA2-Personal.

4 Click **Next**.

5 Enter the name of your network in the Name field and click **Save**.

6 Enter the password for the network in the Password field and click **Save**.
The WiFi network is created and is displayed as a card in the **Enabled** tab of the *WiFi networks* page.

 **Note:** You can click the ellipsis icon on the card of your WiFi network and select **Edit** to edit and save the network name and password.

7 Click **Detail** to view and edit the SSID configuration for your network.

Figure 4-18 WiFi network - example of SSID Configuration page

← Network / WiFi networks / NOKIA-06E0

SSID configuration

SSID name

NOKIA-06E0

Enable WiFi network

☒

Band type

2.4 GHz / 5 GHz / 6 GHz

SSID index

1,5,9

Broadcast the WiFi network

☒

Save

SSID configuration Multi-link operation (MLO)

Multi-Link Operation (MLO) in WiFi 7 allows devices to concurrently transmit and receive data across different frequency bands and channels.

Enabled

☐

8

Configure the following parameters:

Field	Description
SSID name	Displays the SSID name.
Enable WiFi network	Select the toggle button to enable WiFi network.
Band type	Displays the band type.
SSID index	Displays the SSID index.
Broadcast the WiFi network	Select the toggle button to enable broadcasting of the WiFi network.
Guest Mode	Indicates whether guest mode is enabled or disabled. When a particular SSID is enabled with Guest Mode, LAN devices connected to the SSID can only connect to the Internet. Such devices cannot see or communicate with other LAN devices.
Port Mode	Select the required port from the list.
Total MAX users	Enter the maximum number of users.
Encryption Mode	Select an encryption mode from the list: • None • WPA2-Personal • WPA3-Personal • WPA3-Personal-Transition
Enable WPS	Select the toggle button to enable WPS. Note: When you select Enable, a security warning is displayed. Click OK to continue.

Notes:

1. The EasyMesh standard does not support synchronizing WPA3-only mode to the other nodes that participate in the mesh. For this reason, the WPA3 (only) mode should not be used on devices that participate in an EasyMesh mesh. Instead, WPA2/WPA3 mode should be used, as is also mentioned in the EasyMesh standard.

9

Click **Save**.

END OF STEPS

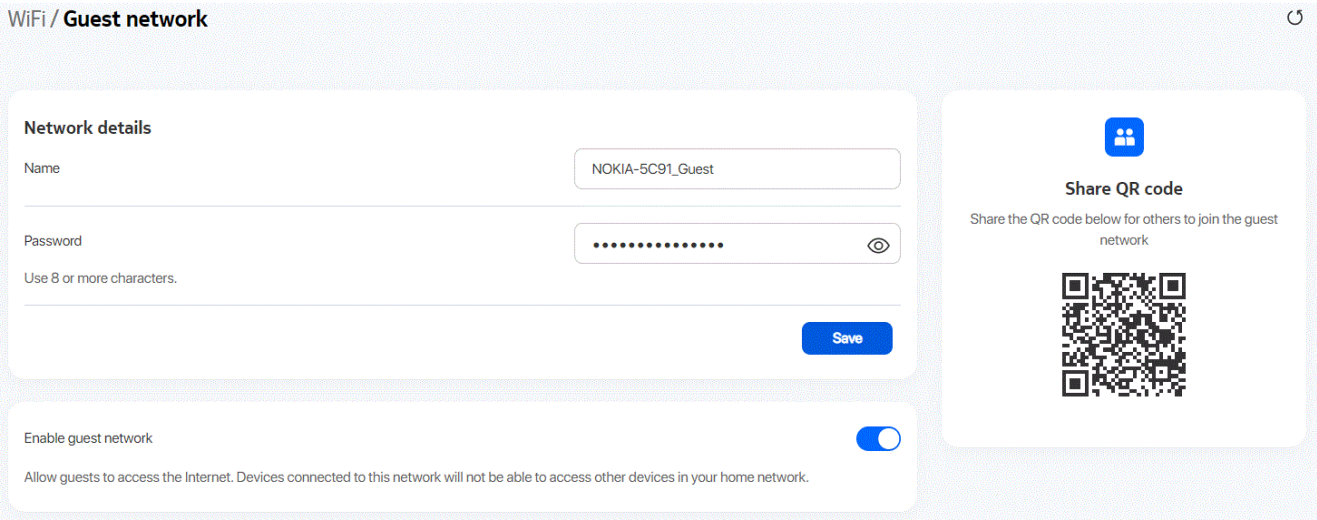
4.21 Configuring Guest Network



Note: Guest WiFi function is not supported.

- 1
- Click **WiFi**→**Guest network** in the left pane. The *Guest network* page displays the network details.

Figure 4-19 Guest network page



- 2
- Configure the following parameters:

Table 4-14 Guest network parameters

Field	Description
Name	Enter the name for guest network.
Password	Enter a password for guest network. Click Save .
Enable guest network	Select this toggle button to enable guest WiFi. Enabling the Guest SSID creates a multiband network (2.4GHz and 5GHz). Atleast one 2.4GHz and one 5GHz SSID index must be available to enable Guest network. After enabling the Guest Network a new WiFi card can be seen in WiFi networks page and Overview page with Guest SSID details.

- 3
- Share the QR code for others to join the guest network.

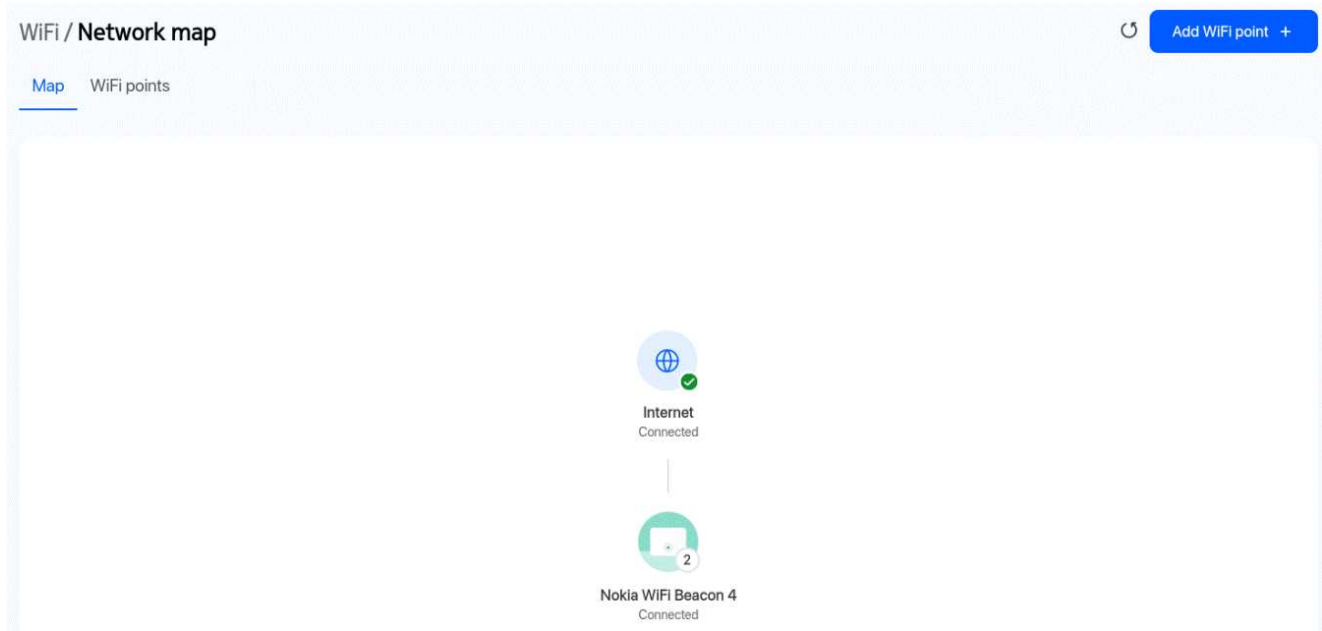
END OF STEPS

4.22 Viewing Network Map, Adding WiFi Points, Renaming WiFi Points and Removing WiFi Points

1

Click **WiFi**→**Network map** in the left pane. The *Network map* page displays the WiFi points added to the network.

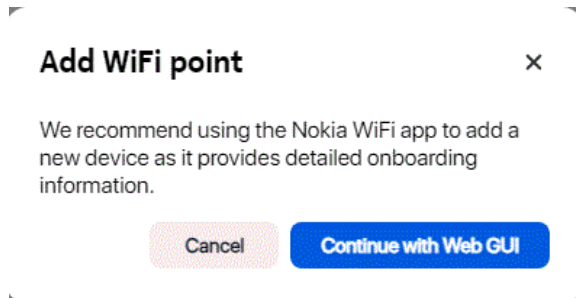
Figure 4-20 Network map page



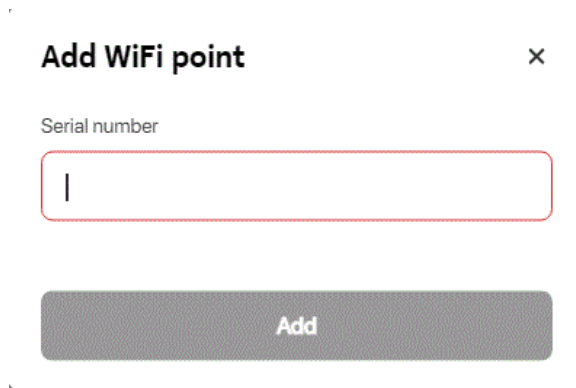
2

Perform the following steps to add a WiFi point:

- a. Click **Add WiFi point** at the top right corner of the *Device Info* page. A message displays that it is recommended to use the Nokia WiFi mobile app to add a WiFi point.
- b. To add a WiFi point using the WebGUI, click **Continue with WebGUI**.



- c. In the *Add WiFi point* page, enter the serial number and click **Add**.

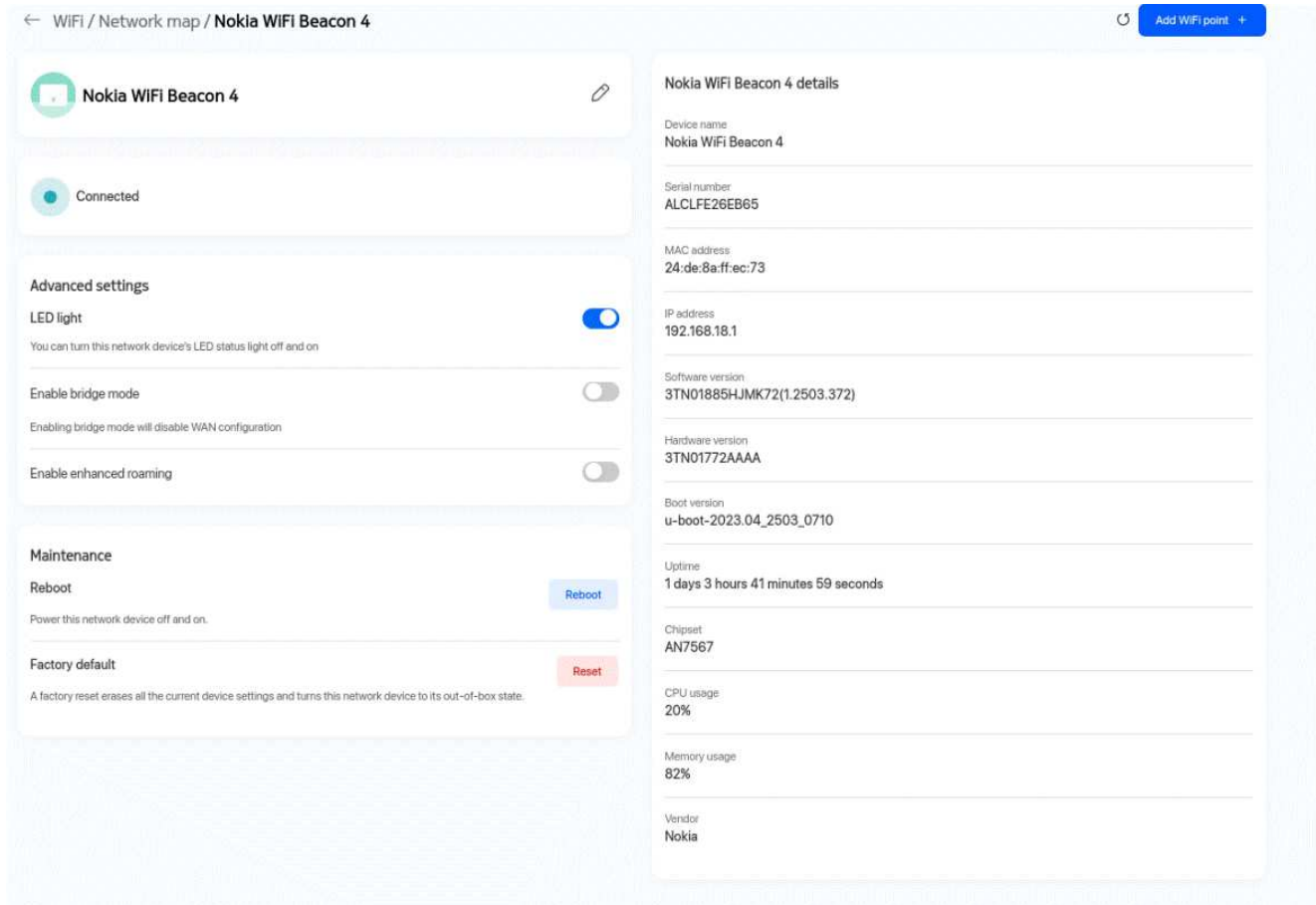


The WiFi point is displayed in the *Detected* or *Not detected* list of the *Onboarding Status* panel in the *Device Info* page.

3

Click on a WiFi point to view the device details. The *<Device>* page displays the details of the selected device in the network, including connection status.

Figure 4-21 <Device> page



4

The WiFi point name can be edited by clicking the edit icon .

Perform the following steps to change the name of your WiFi point:

- To edit the name of the WiFi point, click the Edit icon . The **Change the name of your WiFi point** page displays.
- On the page **Change the name of your WiFi point**, click the drop-down menu to select a name for the WiFi point, or enter a **Custom name** to create your own customized name.
- Click **Save**.

Figure 4-22 Change the name of your WiFi point page

Change the name of your WiFi point ×

Pick a name or create your own.

Custom

▼

Custom name

G6_E

Maximum length is 17 characters.

Save

Table 4-15 <Device> parameters

Field	Description
Device name	Name on the device
Serial number	Serial number of the device
MAC address	MAC address of the device
IP address	IP address of the device
Software version	Software version of the device (displays only for a root device)
Hardware version	Hardware version of the device (displays only for a root device)
Boot version	Boot version of the device (displays only for a root device)
Uptime	Amount of time the device has run since last reset in hours, minutes, and seconds (displays only for a root device)
Chipset	Chipset of the device (displays only for a root device)
Vendor	Name of the vendor (displays only for a root device)
Onboarding status	Onboarding status of the device in the WiFi network (displays only for an extender device)
Backhaul status	Backhaul status of the device (displays only for an extender device)
Location nickname	Name of the location of the device (displays only for an extender device)

- 5
- Click **LED Light** to enable the LED light on the device.

6

Perform any of the following, as applicable:

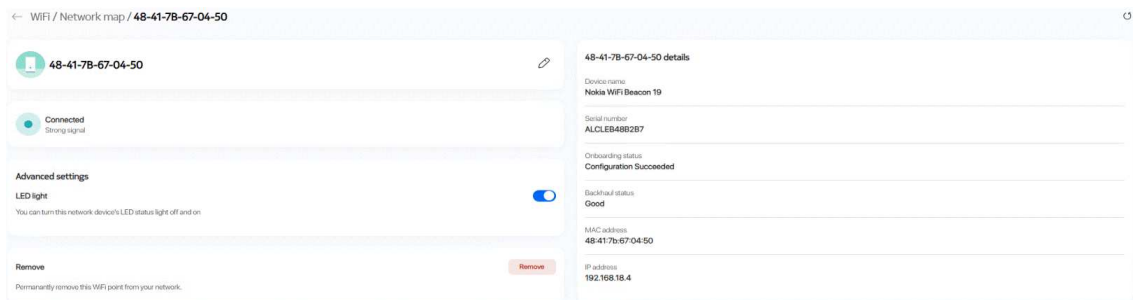
- **Reboot the device:**
 1. Click **Reboot**. A message displays asking if you want reboot the device.
 2. Click **OK** to reboot the Beacon. The device reboots and displays the login page.
- **Reset the device to factory default settings:**
 1. Click **Factory default**. A message displays asking if you want to reset the system configuration to the factory default settings.
 2. Click **OK** to reset the Beacon to the factory default settings.
- **Reset the device to deep factory default settings:**
 1. Click **Deep factory reset**. A message displays asking if you want to reset the system configuration to the factory default settings.
 2. Click **OK** to reset the ONT so that all the downloaded configuration files such as Web customization, delta-config, certification file and so on will be removed.

END OF STEPS

4.22.1 Remove WiFi points

To remove WiFi points, perform the following:

1. Click any extender device and the following *Network map* page is displayed.



The device name can be renamed by clicking the edit icon .

2. Ensure to power off the extender and wait for a few minutes to get the extender in offline status and click **Remove** to permanently remove the WiFi point from your network.

When the extender is in powered on state, a message is displayed to power off the extender and then remove it permanently.

The WiFi point is removed from your network. If you want to use the WiFi point on a different network, factory reset it first.

4.23 Optimizing WiFi Network

In the **WiFi**→**Advanced settings**, the **Run channel optimization** button can be clicked by the user to initiate an immediate network assessment. If a more suitable channel is available, the system initiates a channel switch.

With Channel Selection set to **Auto**, to minimize frequent disconnections of client devices, the radio resource management (RRM) algorithms are designed to change the wireless channel only when internal thresholds are reached or because of regulatory reasons.

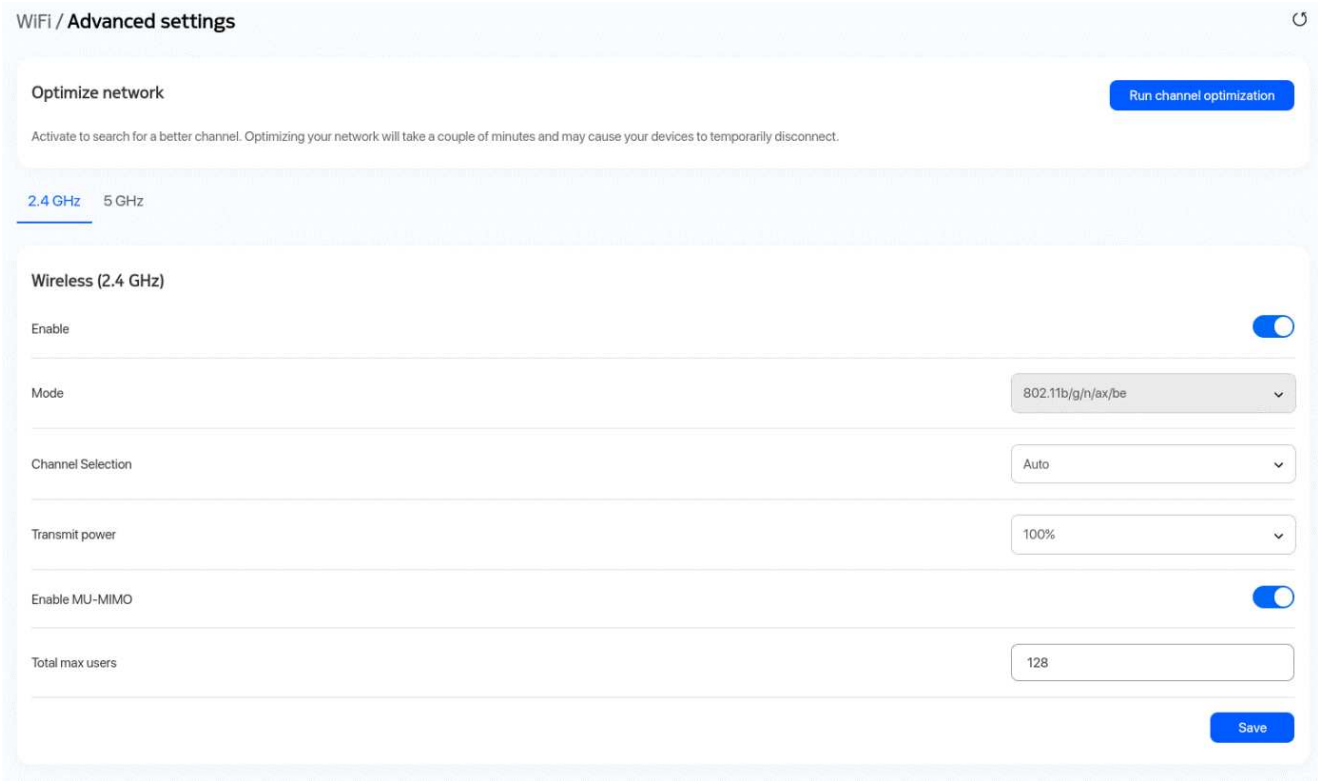
In some cases, the system could possibly run on a more suitable channel, but it does not change the channel to avoid interrupting ongoing client traffic.

Note that this action may cause a brief downtime of the wireless network during the channel transition.

4.24 Configuring Wireless 2.4 GHz

- 1 _____
Click **WiFi→Advanced settings** in the left pane. The *Advanced settings* page displays.
- 2 _____
Select the **2.4 GHz** tab to configure the wireless 2.4 GHz parameters.

Figure 4-23 Advanced settings - 2.4 GHz tab



3

Configure the following parameters:

Table 4-16 Wireless 2.4 GHz parameters

Field	Description
Enable	Select the toggle button to enable Wireless (2.4 GHz).
Mode	The wireless mode 802.11b/g/n/ax/be is selected by default.
Channel Selection	Select a channel from the list: • Auto • Manual Note: When changing from automatic to manual channel management, depending on the channel, channel bandwidth, and region, it can take several minutes for the changes to take into effect and for the wireless network to be functional again. Also, after a reboot, this same delay is observed. It is recommended to set this value to "Auto".
Channel bandwidth	Select the bandwidth range from the list: • 20 MHz • 40 MHz This parameter is visible only if the Channel Selection is Manual .
Channel	Select a channel from the list or select Auto to auto-assign the channel. This parameter is visible only if the Channel Selection is Manual .
Transmit power	Select a percentage for the transmitting power from the list: • 25% • 50% • 75% • 100%
Enable MU-MIMO	Select the toggle button to enable or disable MU-MIMO.

4

Click **Save**.

END OF STEPS

For optimizing WiFi network, see [4.23 "Optimizing WiFi Network" \(p. 85\)](#).

4.25 Configuring Wireless 5 GHz

1

Click **WiFi→Advanced settings** in the left pane. The *Advanced settings* page displays.

2

Select the **5 GHz** tab to configure the wireless 5 GHz parameters.

Figure 4-24 Advanced settings - 5 GHz tab

WiFi / Advanced settings

Optimize network

Run channel optimization

Activate to search for a better channel. Optimizing your network will take a couple of minutes and may cause your devices to temporarily disconnect.

2.4 GHz

5 GHz

Wireless (5 GHz)

Enable

Mode

802.11a/n/ac/ax/be

Channel Selection

Auto

Transmit power

100%

Enable MU-MIMO

Total max users

128

Save

3

Configure the following parameters:

Table 4-17 Wireless 5 GHz parameters

Field	Description
Enable	Select this toggle button to enable WiFi.
Mode	The wireless mode 802.11 a/n/ac/ax/be is selected by default.
Channel Selection	Select a channel from the list: • Auto • Manual Note: When changing from automatic to manual channel management, depending on the channel, channel bandwidth, and region, it can take several minutes for the changes to take into effect and for the wireless network to be functional again. Also, after a reboot, this same delay is observed. It is recommended to set this value to "Auto".

Table 4-17 Wireless 5 GHz parameters (continued)

Field	Description
Channel bandwidth	Select the bandwidth range from the list: • 20 MHz • 40 MHz • 80 MHz • 160 MHz This parameter is visible only if the Channel Selection is Manual .
Channel	Select a channel from the list or select Auto to auto-assign the channel. This parameter is visible only if the Channel Selection is Manual .
Transmit power	Select a percentage for the transmitting power from the list: • 25% • 50% • 75% • 100%
Enable MU-MIMO	Select the toggle button to enable MU-MIMO. This can be enabled when multiple users are trying to access the wireless network. When this parameter is enabled, multiple users can access router functions without the congestion.

4

Click **Save**.

END OF STEPS

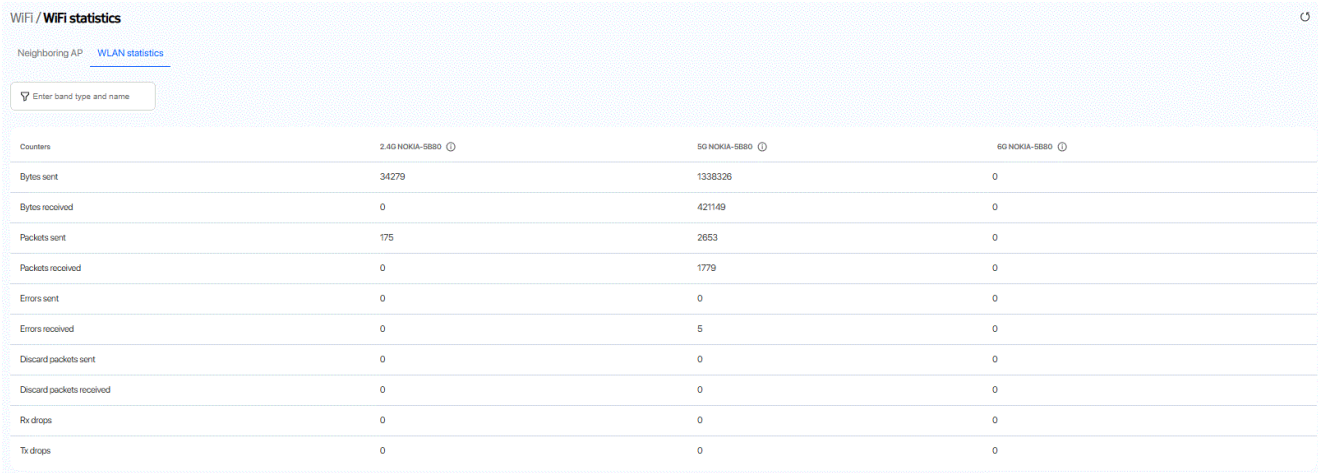
For optimizing the WiFi network, see [4.23 “Optimizing WiFi Network” \(p. 85\)](#).

4.26 Viewing WiFi Statistics

1

Click **WiFi**→**WiFi statistics** in the left pane. The *WiFi statistics* page displays.

Figure 4-25 WiFi statistics page



2

Select the **Neighboring AP** tab to display Neighboring AP parameters.

Table 4-18 Neighboring AP parameters

Field	Description
Index	Name of the index.
SSID name	Name of each SSID.
MAC address	MAC address of the Ethernet connection.
Channel	Channel number.
RSSI (dBm)	Received signal strength in dBm.
Authentication mode	Authentication mode.
WiFi mode	Indicates the WiFi mode
Network type	Indicates the network type

Click **Scan** to scan for neighboring access points.

3

Select the **WLAN statistics** tab to display WLAN statistics.

Table 4-19 WLAN statistics parameters

Field	Description
Bytes sent	Displays the bytes sent.

Table 4-19 WLAN statistics parameters (continued)

Field	Description
Bytes received	Displays the bytes received.
Packets sent	Displays the packets sent.
Packets received	Displays the packets received.
Errors sent	Displays the errors sent.
Errors received	Displays the errors received.
Discard packets sent	Displays the discard packets sent.
Discard packets received	Displays the broadcast packets received.
Rx drops	Displays the Rx dropped packets.
Tx drops	Displays the Tx dropped packets.

END OF STEPS

Devices

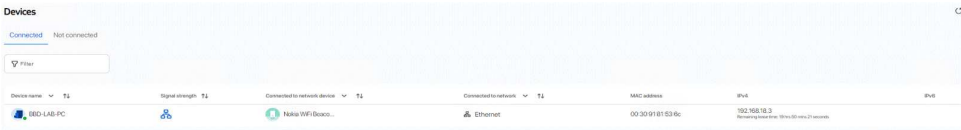
4.27 Overview

This section describes how to view device information from the **Device** menu.

4.28 Viewing Device Information

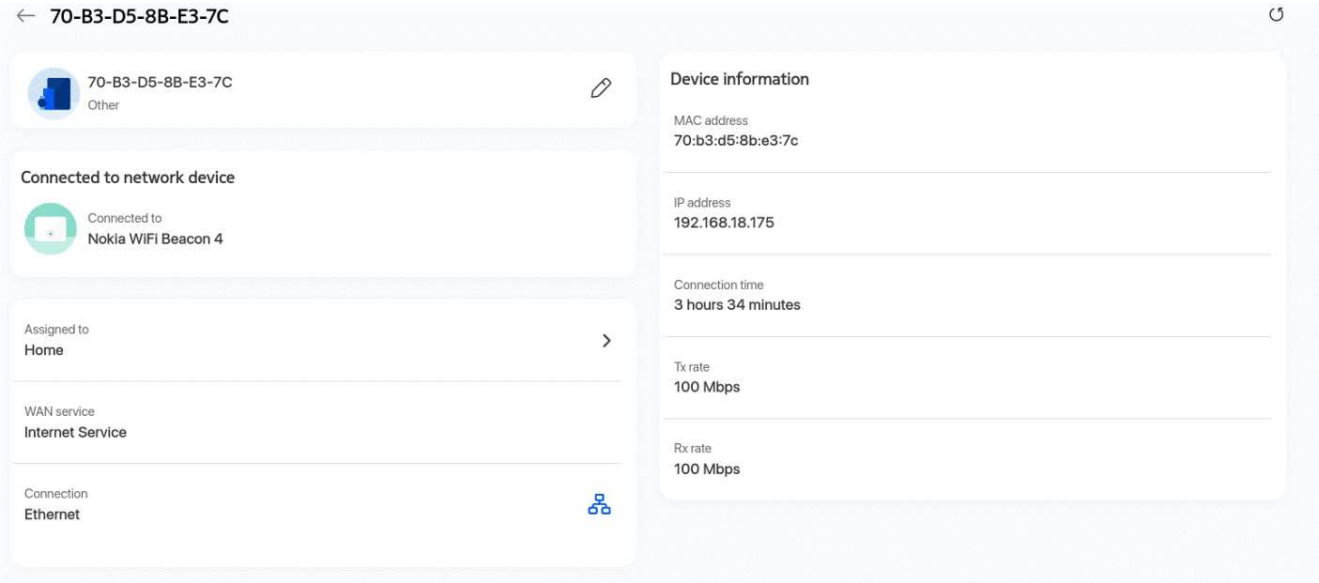
- 1
- Click **Devices** in the left pane. The *Devices* page displays the devices.

Figure 4-26 Devices page



- 2
- The Devices page lists the devices. Click on a Device to view the respective device Info page. The *Device Info* page displays the details of the selected device in a network.

Figure 4-27 Device information page - L3 devices

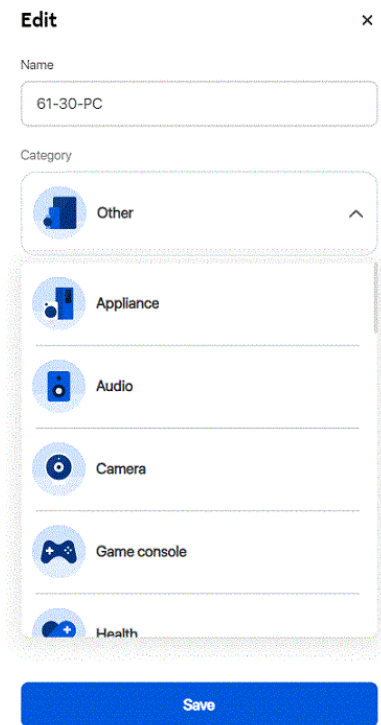


The device name can be renamed by clicking the edit icon .

Perform the following steps to rename the client device:

- To rename the client device, click the Edit icon . The **Edit** page displays.
- On the **Edit** page, enter the name to create your own customized name or select a category listed in the drop-down menu.
- Click **Save**.

Figure 4-28 Device Rename page



Edit x

Name

61-30-PC

Category

Other ^

Appliance

Audio

Camera

Game console

Health

Save

END OF STEPS

Security Configuration

4.29 Overview

This section describes the security configuration procedures that can be performed from the following sub-menu options under the **Security** menu:

Sub-menu	Procedure
Firewall	4.30 "Configuring the Firewall" (p. 94)
MAC filter	4.31 "Configuring the MAC Filter" (p. 95)
IP filter	4.32 "Configuring the IP Filter" (p. 97)
Family profiles	4.33 "Configuring Family Profiles" (p. 98)
DMZ and ALG	4.34 "Configuring DMZ and ALG" (p. 105)
Access control	4.35 "Configuring Access Control" (p. 107)

4.30 Configuring the Firewall

1 _____

Click **Security**→**Firewall** in the left pane. The *Firewall* page displays.

Figure 4-29 Firewall page

Security / Firewall

Security level

High: Traffic denied inbound and minimally permit common service outbound.
Low: All outbound traffic and pinhole-defined inbound traffic is allowed.
Off: All inbound and outbound traffic is allowed.

Off

Attack Protection

Enable

Save

2 _____

Configure the following parameters.

Table 4-20 Firewall parameters

Field	Description
Security level	Select the security level from the list: • High: Pre-routing and application services are not supported. UDP Port 8000 can be used to access the services. For example, FTP can use 8021 and Telnet can use 8023. Regular UDP cannot be used. RG access is permitted via the LAN side but not via the WAN side. • Low: All outbound traffic and pinhole-defined inbound traffic is allowed. Pre-routing is supported: port forwarding, DMZ, host application, and host drop. Also supported are application services: DDNS, DHCP, DNS, H248, IGMP, NTP client, SSH, Telnet, TFTP, and TR-069,. The following types of ICMP messages are permitted: echo request and reply, destination unreachable, and TTL exceeded. Other types of ICMP messages are blocked. DNS proxy is supported from LAN to WAN but not from WAN to LAN. • Off: All inbound and outbound traffic is allowed. No firewall security is in effect.
Attack Protection	Select Enable or Disable from the list to enable or disable protection against DoS or DDoS attacks. Default value: Enable. Note: If you select Disable, a security warning is displayed that this option poses security risks. Click OK to continue.

3

Click **Save**.

END OF STEPS

4.31 Configuring the MAC Filter

1

Click **Security**→**MAC filter** in the left pane. The *MAC filter* page displays.

Figure 4-30 MAC filter page

Security / MAC filter

Ethernet

WiFi

SSID

SSID 1

Filter mode

Allowed

Enabled

Save

SSID

SSID 1

MAC address

Custom Settings

eg: D0:54:2D:00:00:00

Add

2

Configure the following parameters:

Table 4-21 MAC filter - Ethernet Interface parameters

Field	Description
Ethernet	
Filter mode	Select the MAC filter mode from the list: • Blocked • Allowed
LAN port	Select the toggle button to enable any of the LAN ports.
MAC address	Select a MAC address from the list or enter the MAC address in the text field.

3

Click **Save**.

4

Configure the following parameters:

Table 4-22 MAC filter - WiFi SSID parameters

Field	Description
WiFi	
Filter mode	Select the MAC filter mode from the list: • Blocked • Allowed
SSID	Select the SSID from the list.
Enabled	Select the toggle button to enable the MAC filter.
MAC address	Select a MAC address from the list or enter the MAC address in the text field.

5 _____
Click **Save**.

END OF STEPS _____

4.32 Configuring the IP Filter

1 _____
Click **Security**→**IP filter** in the left pane.

2 _____
Click **Add Filter** to add a IPv4 or IPv6 filter. The *Add IP filter* page displays.

Figure 4-31 IP filter page

← Security / IP filter / Add IPv4 filter ↺ Save

Enable IP filter 🔴

Mode

Drop for upstream ▼

Drop for upstream ✓

Drop for downstream

Accept for upstream

Accept for downstream

Source

Local IP address

Local subnet mask

Destination IP address

Destination subnet mask

Protocol

ALL ▼

3

Configure the following parameters:

Table 4-23 IP filter parameters

Field	Description
Add IPv4 filter or Add IPv6 filter parameters	
Enable IP filter	Select the toggle button to enable an IP filter.
Mode	Select an IP filter mode from the list: • Drop for upstream • Drop for downstream
Source	Select an internal client from the list: • Custom Settings: uses the IP address input below • IP: uses the connecting devices' IP to the Beacon
Add IPv4 filter parameters	
Local IP address	Enter the local IP address.
Local subnet mask	Enter the local subnet mask.
Remote IP address	Enter the remote IP address.
Remote subnet mask	Enter the remote subnet mask.
Protocol	Select an application protocol or select ALL from the list.
Add IPv6 filter parameters	
Source IP address	Enter the source IP address.
Source Prefix	Enter the source prefix.
Destination IP address	Enter the destination IP address.
Destination prefix	Enter the destination prefix.
Protocol	Select an application protocol or select ALL from the list.

4

Click **Save**.

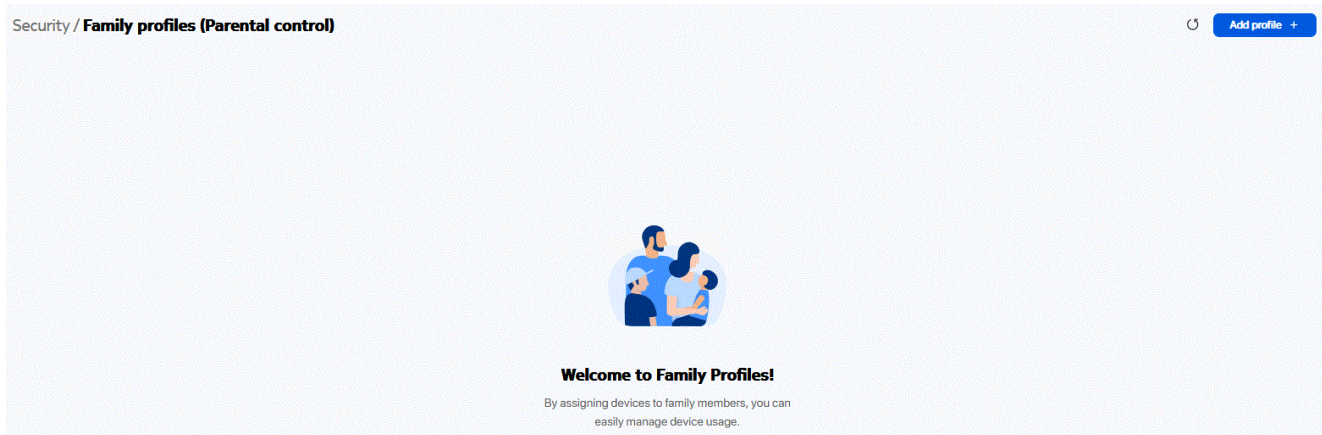
END OF STEPS

4.33 Configuring Family Profiles

1

Click **Security**→**Family profiles (Parental control)** from the left pane. The *Family profiles (Parental control)* page displays.

Figure 4-32 Family profiles (Parental control) page



- 2 _____
- Click **Add profile +** to add a profile with parental controls.

- 3 _____
- In the *Add a profile* page, enter a name for the profile and click **Add**.

Figure 4-33 Add a profile page

Add a profile ×

Name

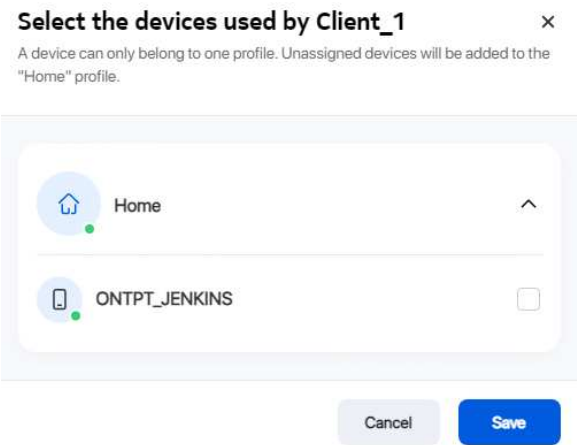
eg. Alex

Cancel Add

- 4 _____
- In the *Select the devices used by <profile>* page, select the check box next to the device name and click **Save** to assign the device to the profile.

i **Note:** A device can be assigned to only one profile. Unassigned devices are added to the *Home* profile.

Figure 4-34 Assign devices to family profile



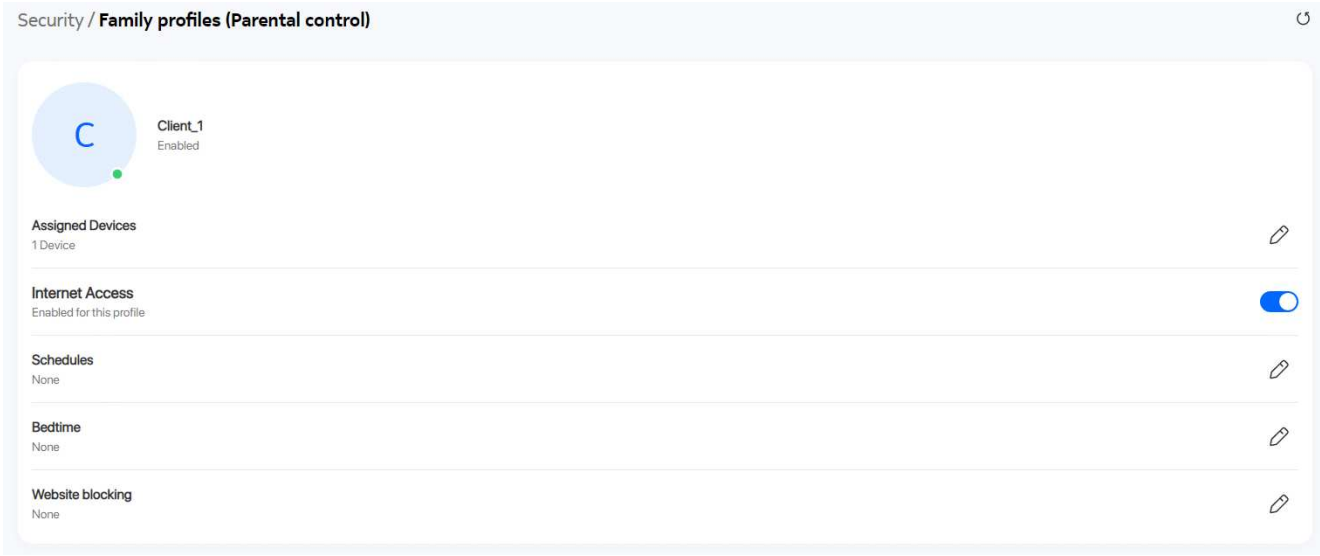
The new profile name is listed in the table in the *Family profiles (Parental control)* page.

Figure 4-35 Family profiles table

Security / Family profiles (Parental control)						Refresh	Add profile +
Profile name	Device	Schedules	Bedtime	Blocked websites	Visit attempts (blocked sites)		
Home Enabled	0	0	0	0	0		
Client_1 Enabled	1	2	3	4	0	Delete	
Client_2 Enabled	1	1	2	1	0	Delete	
profile_3 Enabled	0	0	0	1	0	Delete	

- 5
- Click a profile to configure parental control for the profile. A page displays the profile parameters.

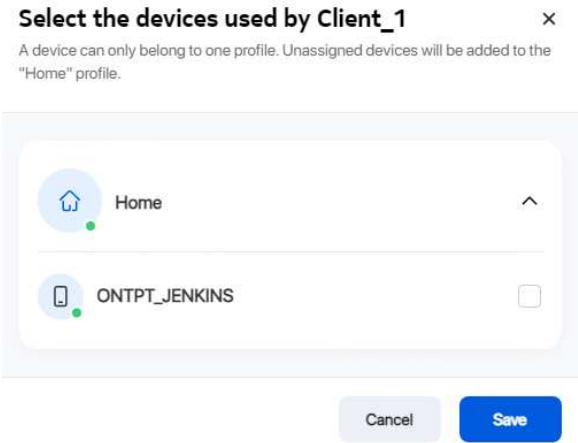
Figure 4-36 Family profile configuration page



- 6 _____
- Select the **Internet Access** toggle button to enable internet access.

Assign more devices

- 7 _____
- Assign more devices to the profile, if required:
- In the profile page, click the edit icon  next to **Assigned Devices** to assign devices to the profile. The *Select the devices used by <profile>* page displays.



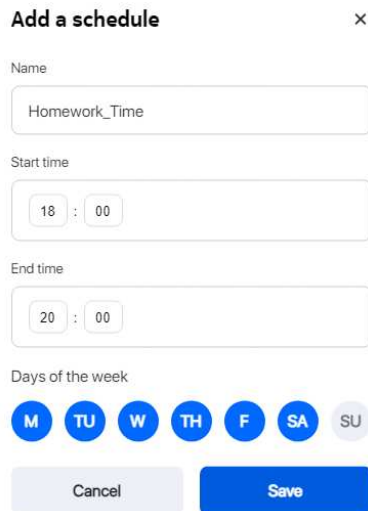
- b. Select the check box next to the device to assign to the profile.
- c. Click **Save**.

Configure and enable schedules

8

Configure schedules for the profile:

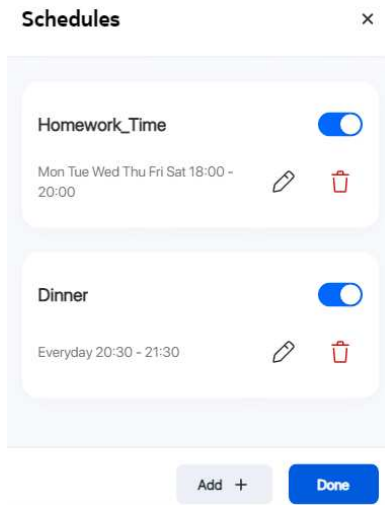
- a. In the profile page, click the edit icon  next to **Schedules** to create one or more schedules for the profile to set specific days and time slots when the Internet should be turned off.
- b. Click **Create Schedule**.
- c. In the *Add a schedule* page, configure the following:



1. Enter the name of the schedule in the Name field.
2. Select the start time, end time, and select the days of the week on which the schedule will be in effect.
3. Click **Save**. The schedule is created and listed in the Schedules page.

9

In the *Schedules* page, select the toggle button to enable the schedule and click **Done**. To add more schedules, you can click **Add +**.

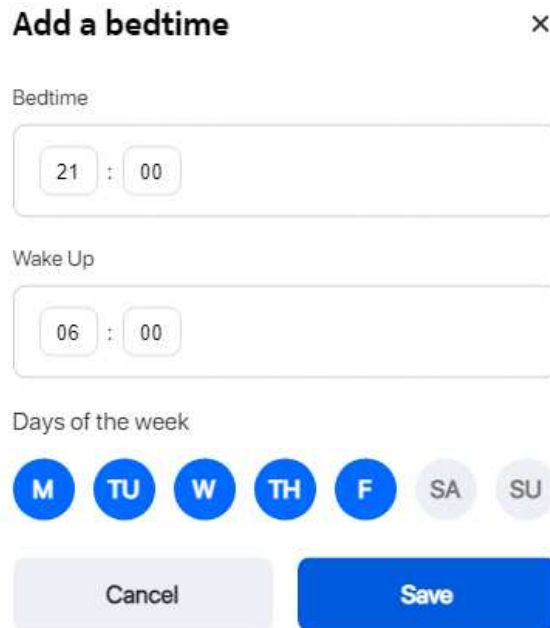


Configure and enable bedtime

10

Configure bedtime for the profile:

- In the profile page, click the edit icon  next to **Bedtime** to configure bedtime for the profile to automatically pause internet access at this time.
Only one bedtime can be assigned per day.
- Click **Create Bedtime**.
- In the *Add a bedtime* page, configure the following:



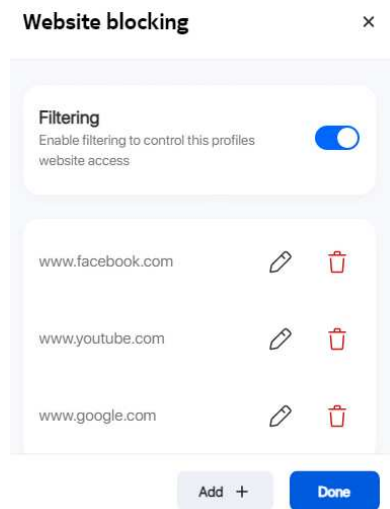
1. Select the Bedtime, Wake Up time, and select the days of the week on which the bedtime will be in effect.
2. Click **Save**. The bedtime is created and listed in the *Bedtime* page.
- d. In the *Bedtime* page, select the toggle button to enable the bedtime and click **Done**.

Configure website blocking

11

Configure website blocking for the profile:

- a. In the profile page, click the edit icon  next to **Website blocking** to control websites and services that devices assigned to the profile can access.
- b. Click **Continue**.
- c. In the *Website blocking* page, perform the following:



1. Select the toggle button next to **Filtering** to enable filtering to control the profile's website access.
2. Click **Add +** to add a website URL to be blocked.
3. Enter the URL in the Website URL field and click **Save**.
4. Click **Add +** to add more website URLs to be blocked or click **Done**.

END OF STEPS

4.34 Configuring DMZ and ALG

1

Click **Security**→**DMZ and ALG** in the left pane. The *DMZ and ALG* page displays.

Figure 4-37 DMZ and ALG page

Security / **DMZ and ALG**

ALG Configuration

FTP

TFTP

SIP

H323

RTSP

L2TP

IPSEC

PPTP

Save

DMZ Configuration

WAN connection list

1_TR069_INTERNET_OTHER_R_VID_0

Enable DMZ

DMZ IP address

Custom Settings

0.0.0.0

Save

2

Configure the following parameters:

Table 4-24 ALG Configuration parameters

Field	Description
ALG Configuration	Select the toggle button next to the protocol name to enable the protocols to be supported by ALG: • FTP • TFTP • SIP • H323 • RTSP • L2TP • PPTP • IPSEC

3

Click **Save**.

4

Configure the following parameters:

Table 4-25 DMZ Configuration parameters

Field	Description
WAN connection list	Select a WAN connection from the list.
Enable DMZ	Select the toggle button to enable DMZ on the WAN connection.
DMZ IP address	Select Custom Settings and enter the DMZ IP address or select the IP address of a connected device from the list.

5

Click **Save**.

END OF STEPS

4.35 Configuring Access Control

This procedure describes how to configure the access control level (ACL).

Note: ACL takes precedence over the firewall policy.
The trusted network will be shared for all WAN connections; it is not applied individually to a WAN connection.

1

Click **Security**→**Access control** in the left pane. The *Access control* page displays.

Figure 4-38 Access control page

2

Configure the following parameters:

Table 4-26 Access control parameters

Field	Description
WAN connection list	Select a WAN connection from the list.
Enable trusted network	Select the toggle button to enable a trusted network.
WAN	The following protocols are supported: ICMP, Telnet, SSH, HTTP, TR-069, HTTPS. Select an access control level for each protocol: Allow, Deny, or Trusted Network Only LAN side: Allow or Deny Note: If you allow SSH/Telnet/HTTP/HTTPS on WAN, a security warning is displayed. Click OK to continue.
LAN	The following protocols are supported: ICMP, Telnet, SSH, HTTP, TR-069, HTTPS. Select an access control level for each protocol: LAN side: Allow or Deny Notes: • If you allow Telnet or HTTP on LAN, a security warning is displayed. Click OK to continue. • If you Deny HTTP and HTTPS on LAN at same time, the following warning message is displayed, 'Disabling both HTTP and HTTPS on LAN may lock you out from accessing the web GUI and mobile application. Atleast one of them should be enabled.' Click OK to continue.

3

Click **Save** to save the ACL configuration.

4

If the **Enable trusted network** option is enabled, add one or more subnet trusted networks. You can add up to 32 trusted networks.

Table 4-27 Trusted Network parameters

Field	Description
Source IP start	Enter a start IP address range for the new subnet trusted network.
Source IP end	Enter an end IP address range for the new subnet trusted network.

5

Click **Add +**.

END OF STEPS

Advanced Settings

4.36 Overview

This section describes the advanced settings that can be performed from the following sub-menu options under the **Advanced settings** menu:

Sub-menu	Procedure
Port forwarding	4.37 “Configuring Port Forwarding” (p. 109)
Port triggering	4.38 “Configuring Port Triggering” (p. 110)
DDNS	4.39 “Configuring DDNS” (p. 111)
NTP	4.40 “Configuring NTP” (p. 113)

4.37 Configuring Port Forwarding

1

Click **Advanced settings**→**Port forwarding** in the left pane. The *Port forwarding* page displays.

Figure 4-39 Port forwarding page

Advanced settings / Port forwarding Save

WAN port

-

LAN port

-

Internal client

Custom Settings

Protocol

TCP

WAN connection list

1_INTERNET_OTHER_R_VID_400

2

Configure the following parameters:

Table 4-28 Port forwarding parameters

Field	Description
WAN port	Enter the WAN port range.

Table 4-28 Port forwarding parameters (continued)

Field	Description
LAN port	Enter the LAN port range.
Internal client	Select a connected device from the list and enter the associated IP address. The default is Custom Settings .
Protocol	Select the port forwarding protocol from the list: • TCP • UDP • TCP/UDP
WAN connection list	Select a WAN connection from the list. Only active devices are displayed in the list.

3

Click **Save**.

END OF STEPS

4.38 Configuring Port Triggering

1

Click **Advanced settings**→**Port triggering** in the left pane. The *Port triggering* page displays.

Figure 4-40 Port triggering page

Advanced settings / Port triggering

Open port

-

Triggering port

-

Expiration time

Range: 1-999999 secs

600

Open protocol

TCP

Trigger protocol

TCP

WAN connection list

1_INTERNET_OTHER_R_VID_400

Save

2

Configure the following parameters:

Table 4-29 Port triggering parameters

Field	Description
Open port	Enter the open port range.
Triggering port	Enter the triggering port range.
Expire time	Enter the expiration time in seconds. Allowed range: 1 to 999999 seconds
Open protocol	Select the open port protocol from the list: • TCP • UDP • TCP/UDP
Trigger protocol	Select the triggering port protocol from the list: • TCP • UDP • TCP/UDP
WAN connection list	Select a WAN connection from the list. Only active devices are displayed in the list.

3

Click **Save**.

END OF STEPS

4.39 Configuring DDNS

1

Click **Advanced settings**→**DDNS** in the left pane. The *DDNS* page displays.

Figure 4-41 DDNS page

Advanced settings / **DDNS**

WAN connection list

1_TR069_INTERNET_OTHER_R_VID_0

Enable DDNS

ISP

DynDNS.org

Domain Name

Username

Password

Save

2

Configure the following parameters:

Table 4-30 DDNS parameters

Field	Description
WAN connection list	Select a WAN connection from the list.
Enable DDNS	Select the toggle button to enable DDNS on the WAN connection.
ISP	Select an ISP from the list.
Domain Name	Enter the domain name of the DDNS server.
Username	Enter the username.
Password	Enter the password.

3

Click **Save**.

END OF STEPS

4.40 Configuring NTP

- 1
- Click **Advanced settings**→**NTP** in the left pane. The *NTP* page displays.

Figure 4-42 NTP page

Advanced settings / **NTP**

Enable NTP service

☒

Current date & time

07/19/2022 12:33:04 PM

Primary Time Server

time.nist.gov

Secondary Time Server

Custom Settings

ntp1.tummy.com

Third time server

None

Interval time

0

0,15-259200 secs

Time zone

(GMT-00:00) Greenwich Mean Time: Dublin

Save

- 2
- Configure the following parameters:

Table 4-31 NTP parameters

Field	Description
Enable NTP service	Select the toggle button to enable the NTP service.
Current date & time	Displays the current local date and time.
Primary Time Server Secondary Time Server Third Time Server	Select a time server from the list or select Custom Settings and enter the IP address of the time server. You can select None if you do not want configure a secondary or tertiary time server.

Table 4-31 NTP parameters (continued)

Field	Description
Interval time	Enter the interval at which to get the time from the time server, in seconds. Allowed values: 0 to 259200 seconds.
Time zone	Select the local time zone from the list.

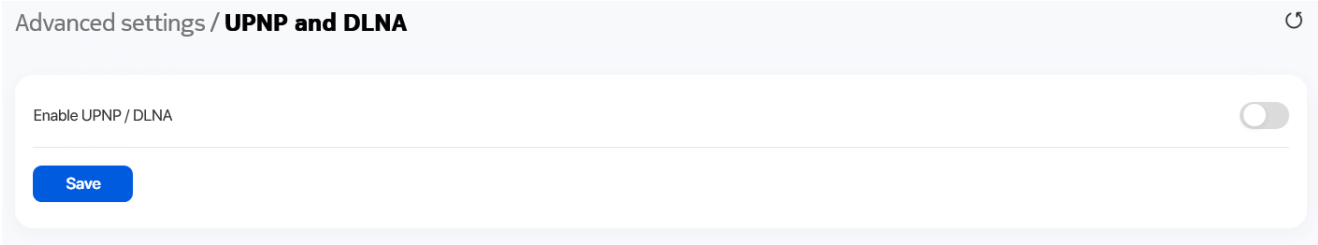
- 3
- Click **Save**.

END OF STEPS

4.41 Configuring UPNP and DLNA

- 1
- Click **Advanced settings**→**UPNP and DLNA** from the left pane. The *UPNP and DLNA* page displays.

Figure 4-43 UPNP and DLNA page



- 2
- Select the **Enable UPNP/DLNA** toggle button to enable UPNP/DLNA. If this toggle button is not enabled, the UPNP and DLNA process will not start.
- 3
- Click **Save**.

END OF STEPS

Maintenance

4.42 Overview

This section describes the maintenance procedures that can be performed from the following sub-menu options under the **Maintenance** menu:

Sub-menu	Procedure
Change password	4.43 "Configuring the Password" (p. 115)
Backup and restore	4.44 "Backing Up the Configuration" (p. 117) 4.45 "Restoring the Configuration" (p. 117)
Firmware upgrade	4.46 "Upgrading Firmware" (p. 118)
Diagnostics	4.47 "Diagnosing WAN Connections" (p. 119)
Log	4.48 "Viewing Log Files" (p. 122)

4.43 Configuring the Password

Operators can allow users to set passwords with or without password rules.

The password rules are different based on each operator's configuration.

Password rule configuration can be any or all of these as well as additional added rules. The following password rules can be applied:

- First character cannot be special one.
- Password can only contain numbers, letters and special character !#+, -./:=@_
- Password should be at most 63 characters.
- At least two character classes are required.
- Password should be at least 8 characters.
- The same character can not appear consecutively 8 times.

When the password meets the password rules, the application displays the message "Your password has been changed successfully".

When the password does not meet the password rules, the application displays a message to indicate which password rule has not been followed, for example:

- First character cannot be special one
- Password can only contain numbers, letters and special character !#+, -./:=@
- The password should use at least one uppercase letter, one lowercase letter, one number, and one special character
- Password should be at least 8 characters
- Password should be at most 24 characters
- The same character cannot appear consecutively 8 times

1 Click **Maintenance**→**Change password** in the left pane. The *Change password* page displays.

Figure 4-44 Change password page

Maintenance / **Change password**

Original password

New password

☐ At least 1 number

☐ At least 1 lower case letter

☐ At least 1 upper case letter

☐ At least 8 characters

☐ At least 1 special character (only !#+,-./:;=@_)

☐ No consecutive 8 identical characters

☐ The first character must not be special

☐ No more than 24 characters

Repeat new password

Password hint

For better security, avoid using your password or any part of it in the password hint.

Save

2 Configure the following parameters:

Table 4-32 Change password parameters

Field	Description
Original password	Enter the current password.
New password	Enter the new password as per the password rules.
Repeat new password	Re-enter the new password (must match the password entered above).
Password hint	Enter the password hint message.

3 Click **Save**.

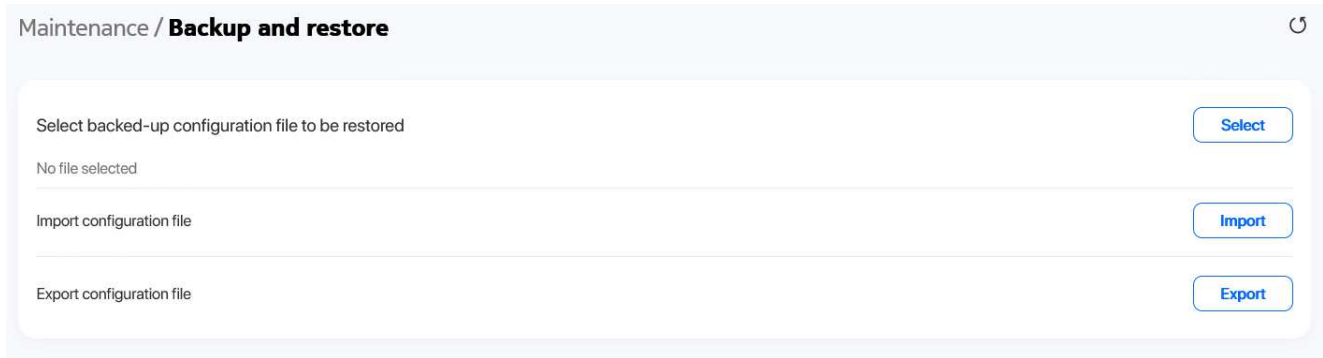
END OF STEPS

4.44 Backing Up the Configuration

1

Click **Maintenance**→**Backup and restore** in the left pane. The *Backup and restore* page displays.

Figure 4-45 Backup and restore page



2

Click **Export** to export the current Beacon configuration to your PC. The configuration filename is *config.cfg*.

END OF STEPS

4.45 Restoring the Configuration

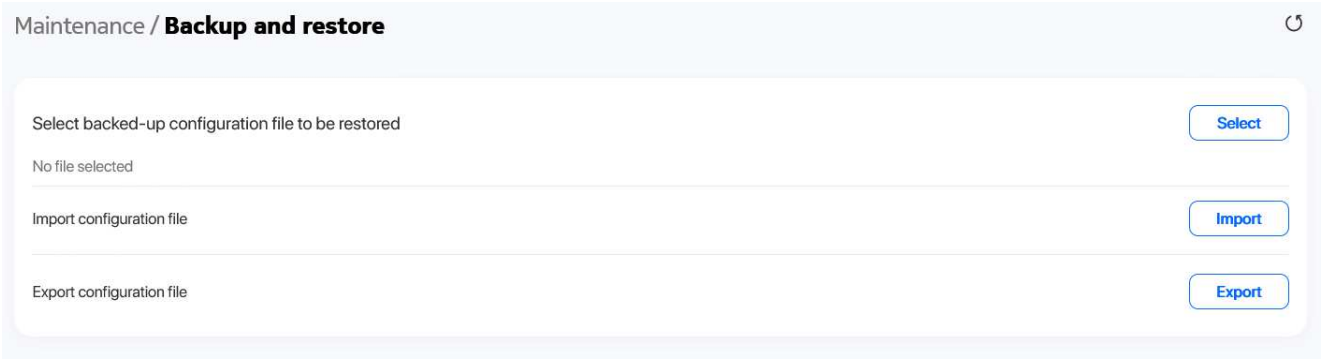


Note: Ensure that you have a previously backed-up configuration file.

1

Click **Maintenance**→**Backup and restore** in the left pane. The *Backup and restore* page displays.

Figure 4-46 Backup and restore page



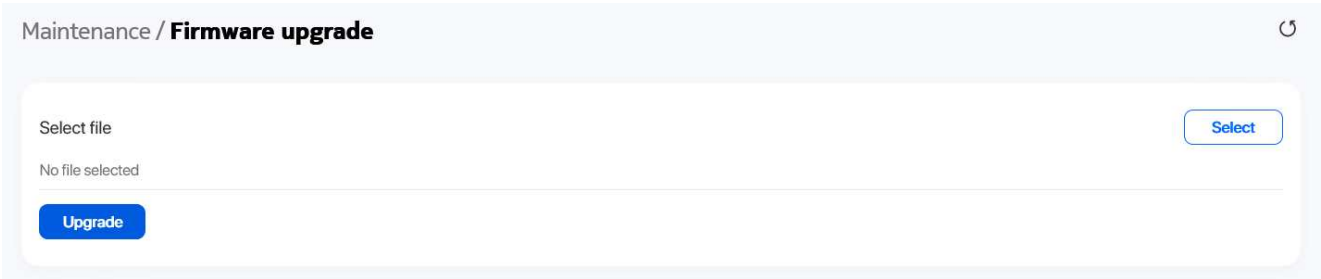
- 2
- Click **Select** and select the previously backed-up configuration file.
- 3
- Click **Import** to import the configuration file created in [4.44 “Backing Up the Configuration” \(p. 117\)](#) and restore the Beacon to the backed-up configuration.
A confirmation message displays after successful restore and the Beacon reboots.

END OF STEPS

4.46 Upgrading Firmware

- 1
- Click **Maintenance**→**Firmware upgrade** in the left pane. The *Firmware upgrade* page displays.

Figure 4-47 Firmware upgrade page



2 Click **Select** and select the file for firmware upgrade.

3 Click **Upgrade** to upgrade the firmware. The status displays in the *Upgrade status* panel. The device reboots after firmware upgrade and displays the login page.

Figure 4-48 Example of upgrade status messages

```
Upgrade status
Upgrade Done!
-----
get_cert_type_from_buildinfo NCG
Image check pass, everything is OK
Saving config files...
Performing system upgrade...
Upgrade completed
4
mkdir: can't create directory '/configs/swdl': File exists
sh: using fallback suid method
sync: using fallback suid method
date: using fallback suid method
Upgrade ok, Rebooting...
```

END OF STEPS

4.47 Diagnosing WAN Connections

1 Click **Maintenance**→**Diagnostics** in the left pane. The *Diagnostics* page displays.

Figure 4-49 Diagnostics page

Maintenance / **Diagnostics**

WAN

Protocol

IPv4

WAN connect list

LAN/WAN Interface

IP or domain name

Ping

Traceroute

Ping try times

4

1-1000

Packet length

64

64-1500

Max number of trace hops

30

1-255

Start test

Cancel

2

Configure the following parameters.

Table 4-33 Diagnostics parameters

Field	Description
Protocol	Select a protocol from the list: • IPv4 • IPv6
WAN connect list	Select a WAN connection to diagnose from the list.
IP or domain name	Enter the IP address or domain name.
Ping	Select this toggle button to enable ping.

Table 4-33 Diagnostics parameters (continued)

Field	Description
Traceroute	Select this toggle button to enable traceroute.
Ping try times	Enter the number of ping attempts. This field is enabled only if you select the Ping toggle button. Allowed values: 1 to 1000 Default value: 4
Packet length	Enter a packet length. Allowed values: 64 to 1500 Default value: 64
Max number of trace hops	Enter the maximum number of trace hops. This field is enabled only if you select the Traceroute toggle button. Allowed values: 1 to 255 Default value: 30

3

Click **Start test** to start the test. Results are displayed at the bottom of the page.

Figure 4-50 Example of ping results

```
PING 192.168.18.10 (192.168.18.10): 64 data bytes
72 bytes from 192.168.18.10: seq=0 ttl=64 time=49.398 ms
72 bytes from 192.168.18.10: seq=1 ttl=64 time=75.414 ms
72 bytes from 192.168.18.10: seq=2 ttl=64 time=102.160 ms
72 bytes from 192.168.18.10: seq=3 ttl=64 time=123.691 ms

--- 192.168.18.10 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 49.398/87.665/123.691 ms
```

Figure 4-51 Example of traceroute results

```
traceroute to 192.168.18.10 (192.168.18.10), 30 hops max, 64 byte packets
1 192.168.18.10 52.241 ms 5.023 ms 3.396 ms
```

END OF STEPS

4.48 Viewing Log Files

1 Click **Maintenance**→**Log** in the left pane. The *Log* page displays.

Figure 4-52 Log page

Maintenance / **Log**

 **Save** Export log

Writing level

Notice

Reading level

Error

2 Configure the following parameters:

Table 4-34 Log parameters

Field	Description
Writing level	Select a writing level from the list to determine the event types recorded in the log file: - Emergency - Alert - Critical - Error - Warning - Notice - Informational - Debug
Reading level	Select a reading level from the list to determine the event types displayed in the log file: - Emergency - Alert - Critical - Error - Warning - Notice - Informational - Debug

- 3
- Click **Save**. The log file is displayed at the bottom of the page.
- 4
- Click **Export log** to download the log file to your PC. The filename of the log is *onu_info.log*.

END OF STEPS

4.49 Viewing Container Management

- 1
- Click **Maintenance**→**Container management** in the left pane. The *Container management* page displays.

Figure 4-53 Container management page



- 2
- Configure the following parameters:

Table 4-35 Container management parameters

Field	Description
App name	Indicates the name of the application.
Version	Indicates the version of the application.
Status	Displays the status of the application: • Active • Idle

END OF STEPS

4.50 Generating a delta configuration file

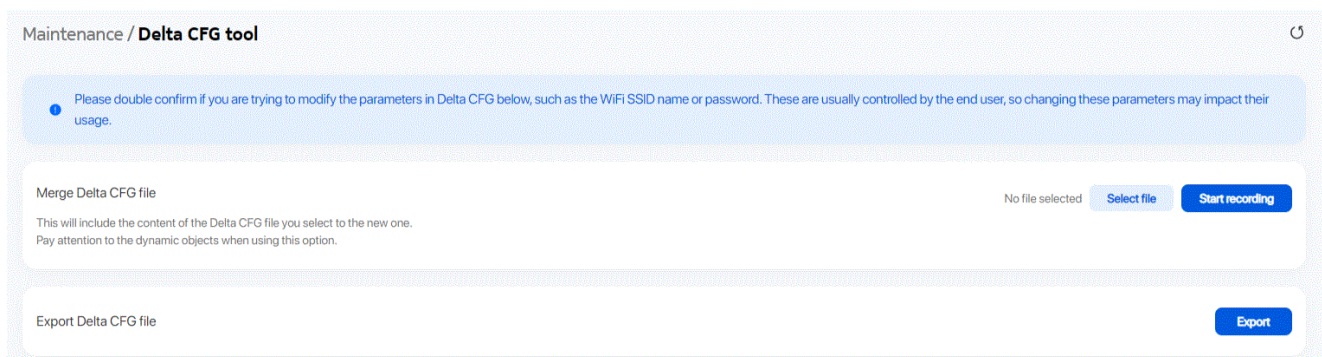
The delta CFG tool is used to generate a delta CFG file which records the parameter changes on the WebGUI. The tool also allows to merge the generated delta configuration file with a previously existing delta config file.

1

Click **Maintenance**→**Delta CFG tool** from the left pane. The Delta CFG tool page displays.

- To generate a delta CFG file without merging with a previous CFG file, go to [Step 2](#).
- To merge delta CFG file, go to [Step 3](#).

Figure 4-54 Delta CFG Tool page



2

Generating a delta CFG file without merging with a previous delta CFG file

- Click **Start recording**.
- Perform the required configuration such as adding/deleting WAN connection, changing WAN connection VLAN ID, changing ACS URL and so on. If reboot is needed after modifying a parameter, for example, changing LAN port mode from route to bridge, wait until the Beacon is rebooted and continue with the configuration.
- Click **Stop recording** to stop recording.
- Click **Export** to download the delta CFG file to the local computer. The delta CFG file is in plain text format with the filename *delta_config_result file*. If required, rename the file and convert the file to .tar format before downloading it to the Beacon.



Note: For merging the downloaded delta config, the previously downloaded delta file must be renamed by adding “CFG” at the start of the filename and .cfg extension to be added to the delta config file (CFG_*.cfg) to upload the file successfully in Delta CFG tool page.

3

Generating a delta CFG file and merging the file with a previously generated file

This option allows a user to select a delta CFG file from the local computer which will be merged with the recorded commands. The generated delta CFG file will include the content of the selected delta CFG file and the new modifications.

- a. Click **Select file** and select an existing delta CFG file from the local computer to merge with the recorded commands.



Note: Choose the delta CFG file before clicking **Start recording**. The delta CFG file chosen needs to be in plain text format and not in the .tar format.

- b. Click **Start recording**.
- c. Perform the required configuration such as adding/deleting WAN connection, changing WAN connection VLAN ID, changing ACS URL and so on. If reboot is needed after modifying a parameter, for example, changing LAN port mode from route to bridge, wait until the Beacon is rebooted and continue with the configuration.
- d. Click **Stop recoding** to stop recording.
- e. Click **Export** to download the delta CFG file to the local computer. The delta CFG file is in plain text format with the filename *delta_config_result file*. If required, rename the file and convert the file to .tar format before downloading it to the Beacon.



Note: For merging the downloaded delta config, the previously downloaded delta file must be renamed by adding "CFG" at the start of the filename and .cfg extension to be added to the delta config file (CFG_*.cfg) to upload the file successfully in Delta CFG tool page.

END OF STEPS

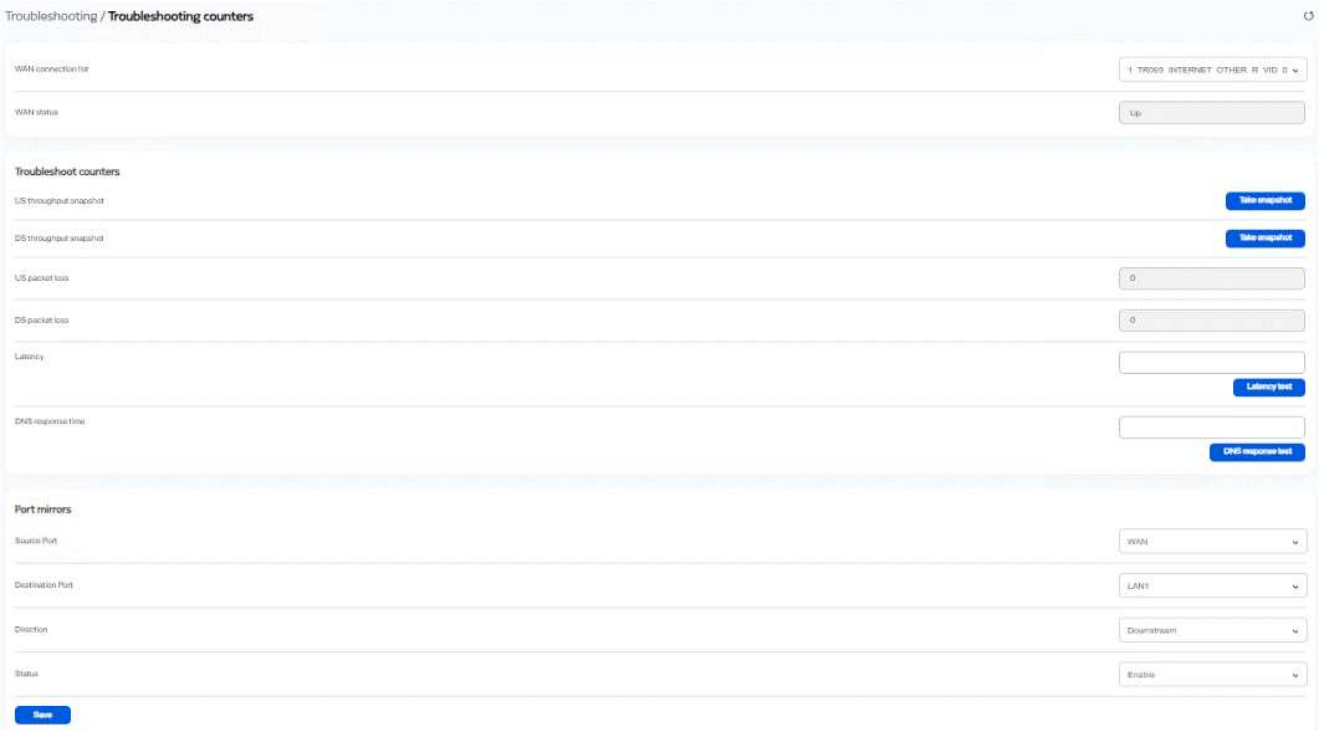
Troubleshooting

4.51 Troubleshooting counters

The Troubleshooting counters feature enables service providers and end users to monitor the performance of their broadband connection for about 10 seconds from the time the test is triggered. Tests are run to retrieve upstream and downstream throughput, latency, and DNS response time. The Troubleshooting counters page also displays upstream and downstream packet loss and Internet status.

- 1
- Click **Troubleshooting**→**Troubleshooting counters** in the left pane. The *Troubleshooting counters* page displays.

Figure 4-55 Troubleshooting counters page



- 2
- Configure the following parameters:

Table 4-36 Troubleshooting counters parameters

Field	Description
WAN Connection List	Select a WAN connection from the list.
WAN Status	Displays the WAN status: • Up • Down
Troubleshoot counters	
US throughput	This test is used to determine the upstream throughput/speed. Click US speed test to specify the time for the upstream test.
DS throughput	This test is used to determine the downstream throughput/speed. Click DS speed test to specify the time for the downstream test.
US packet loss	Displays the number of upstream packages lost.
DS packet loss	Displays the number of downstream packages lost.
Latency	This test is used to determine the lowest round-trip time in milliseconds by pinging the target server multiple times. Click Latency test to specify the time for the test.
DNS response time	This test is used to determine the lowest round-trip time in milliseconds by sending a request to the target DNS server. Click DNS response test to specify the time for the test.
Port mirrors	
Source port	Select a source port for port mirroring from the list.
Destination port	Select a destination port for port mirroring from the list.
Direction	Select a direction from the list: • Upstream • Downstream
Status	Select a port mirroring status from the list: • Enable

3

Click **Save**.

END OF STEPS

4.52 Speed Test

1

Click **Troubleshooting**→**Speed test** in the left pane. The *Speed test* page displays.

Figure 4-56 Speed test page

Troubleshooting / Speed test

TR-143 server settings

Upload test server URL

URL Ex.http://upload.server.com/test

Number of upload connections

10

Download test server URL

URL Ex.http://download.server.com/download.fil

Number of download connections

10

Host

IP address Ex.192.168.50.32

Test mode

File based

Upload file size

File size in MB Ex.1000

Results

Upload speed

-

Download speed

-

Latency

0

Start test

Table 4-37 Speed test parameters

Field	Description
TR-143 server settings	
Upload test server URL	Enter the Upload test server URL.
Number of upload connections	Enter the Number of upload connections.
Download test server URL	Enter the Download test server URL.
Number of download connections	Enter the Number of download connections.
Host	Enter Host.

Table 4-37 Speed test parameters (continued)

Field	Description
Test mode	Select a Test mode: • Time based • File based
Upload file size	Displays the file size in MB. This parameter is visible only if the Test mode is File Based .
Duration	Displays the time duration is sec. This parameter is visible only if the Test mode is Time Based .
Results	
Upload speed	Displays the upload speed.
Download speed	Displays the download speed.
Latency	Displays the latency.

2

Click **Save** to save the TR-143 settings.

3

Click **Start test** to start the speed test.

END OF STEPS

5 Configure Beacon using a combined customized software package

5.1 Overview

5.1.1 Purpose

This procedure describes how to configure the Beacon using a combined customized software package.

5.1.2 Contents

5.1 Overview	131
5.2 Configuring Beacon using a Combined Customized Software Package	131

5.2 Configuring Beacon using a Combined Customized Software Package

The Beacon runs a firmware and when it is successfully upgraded, the operator can upgrade a customized combined firmware to update the special configuration files such as **pre-cfg**, **delta config** and **webGUI config** files.



Note:

1. The **pre-cfg**, **delta config**, **webGUI config** and the required firmware version files must be shared with Nokia and contact Nokia representatives.
2. Nokia will generate the combined customized firmware file and share with the operator.

1

The customer must upload the combined customized firmware file to the ACS or Nokia Corteca Home Controller.

2

Using the device management interface, upload and activate the combined customized firmware files to the device.

The combined customized firmware file can also be uploaded and activated through the webGUI or via the Nokia Corteca OTA service.

3

The Beacon automatically reboots to apply the configuration files. The Beacon becomes online and reports its new firmware.

4

The operators must check the committed file from the ACS or Nokia Corteca Home Controller to verify whether the corresponding file has been applied. If an error occurs, contact Nokia for support.

END OF STEPS

6 Environmental and Regulatory Compliance

6.1 Overview

6.1.1 Purpose

This chapter provides information about the environmental and regulatory compliance.

6.1.2 Contents

6.1 Overview	133
6.2 For EU regulation market	133
6.3 For NAR regulation market	136

6.2 For EU regulation market

The Products are manufactured by Nokia Solutions and Networks Oy and imported by Nokia Solutions and Networks Oy, Karakaari 7,02610 Espoo, Finland.

Nokia is a registered trademark of Nokia Corporation.

Nokia Solutions and Networks Oy declares that the device is in compliance with Radio Equipment Directive 2014/53/EU(for device with WiFi); Low Voltage Directive 2014/35/EU(for device without WiFi); EMC Directive 2014/30/EU(for device without WiFi); RoHS Directive 2011/65/EU; Eco-design Directive 2009/125/EC and EAA - Directive 2019/882/EU.

6.2.1 RoHS (Restriction of Hazardous Substances Directive)

Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (European Union (EU) Directive 2011/65/EU and as amended).

Nokia Solutions and Networks Oy declares that the device is in compliance with the EU RoHS Directive.

6.2.2 WEEE (End of Life Collection and Treatment)

In the European Union, the below label indicates that this device should not be disposed of with household waste. It should be deposited in an appropriate facility to enable recovery and recycling.

Figure 6-1 Recycling/take back/disposal of product symbol



The device is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. Electronic products bearing or referencing the WEEE mark shown above, when put on the market within the European Union (EU), shall be collected and treated at the end of their useful life, in compliance with applicable EU and local legislation. They shall not be disposed of as part of unsorted municipal waste.

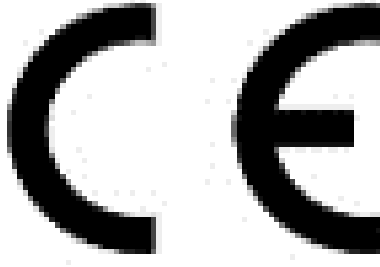
Due to materials that may be contained in the Product, such as heavy metals or batteries, the environment and human health may be negatively impacted as a result of inappropriate disposal.

At the end of their life, the Products are subject to the applicable local legislations that implement the European Directive 2012/19/EU on WEEE. There can be different requirements for collection and treatment in different member states of the European Union.

In compliance with legal requirements and contractual agreements, where applicable, Nokia will offer to provide for the collection and treatment of Products bearing the logo above at the end of their useful life, or Products displaced by Nokia equipment offers. The equipment can be disposed at electronic waste collection points or to stores that sell electronics.

For more information regarding the requirements for recycling/disposal of the Product you may contact Nokia or your service provider.

6.2.3 Simplified EU Declaration of Conformity



Hereby, Nokia Solutions and Networks Oy declares that the device is in compliance with:

- Radio Equipment Directive 2014/53/EU; (for device with WiFi)
- Low Voltage Directive 2014/35/EU; (for device without WiFi)
- EMC Directive 2014/30/EU; (for device without WiFi)
- RoHS Directive 2011/65/EU
- Eco-design Directive 2009/125/EC
- Directive European Accessibility Act - 2019/882/EU

In accordance with Article 10.8(a) and 10.8(b) of the RED, the below table provides information on the frequency bands used and the maximum radio frequency transmit power of the Products with WiFi.

Table 6-1 Frequency bands and transmit power

Radio Frequency Maximum	Transmit Power
2400 – 2483.5 MHz	100mW EIRP
5150 – 5350 MHz	200mW EIRP
5470 – 5725 MHz	1000mW EIRP

The full text of the EU declaration of conformity is available at Declaration of conformity | Nokia.com.

6.2.4 Specific precautions for EMC Warning

The device is compliant with Class B of EN 55032. In a residential environment this equipment may cause radio interference. The Products are tested to the requirements of EN 55032 (Emissions) and EN 55035 (immunity).

There are no specific precautions which must be taken in order to comply with the requirements of Directive 2014/30/EU Essential Requirements in Section 1 of Annex I. In addition, the Products are further tested to ensure spurious emissions are within the specified limits, as well as meeting the requirements for adaptivity, which mitigates against problems caused by co-location with other

wireless products. The Products are not subject to the requirements in Section 2 of Annex I of Directive 2014/30/EU for fixed installations.

6.2.5 Restriction used in European for devices with WiFi

The device with WiFi could be used with a separation distance of 20 cm to the human body.

The device with WiFi is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range, see [Table 6-2, “Applicable country codes” \(p. 135\)](#) regarding indoor use in the 5150 to 5350 MHz frequency range for applicable country codes.

Table 6-2 Applicable country codes

AT	BE	BG	HR	NO
CY	CZ	DK	EE	IS
FI	FR	DE	EL	LI
HU	IE	IT	LV	CH
LT	LU	MT	NL	TR
PL	PT	RO	SK	
SI	ES	SE	UK (NI)	

6.3 For NAR regulation market

6.3.1 ETL Listing



The device has been tested by Intertek, which is the NRTL (National Recognized Testing Laboratory) lab in USA and also the ATO (Accredited Testing Organization) in Canada, the device is in compliance with the following national standards across the US and Canada.

- UL 62368-1:2019 Ed3, Audio/Video, Information And Communication Technology Equipment - Part 1: Safety Requirements
- CSA C22.2#62368-1:2019 Ed3, Audio/Video, Information And Communication Technology Equipment - Part 1: Safety Requirements

6.3.2 FCC EMC Compliance

The device is in compliance with FCC regulation.

The device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

6.3.3 FCC Restriction for devices with WiFi

Operation shall be limited to indoor use only.

The Product and its antenna(s) must not be co-located or operated in conjunction with any other antenna or transmitter.

No Unauthorized Modifications: Do not make any changes or modifications to the Product without the prior express written approval of Nokia. Any changes or modifications made without express written approval could void the user's authority to operate the device.

The Product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure: The device complies with FCC radiation exposure limits set forth for an uncontrolled environment. The Product should be installed and operated with minimum distance of 24 cm (depend on test result) between the radiator and your body.

6.3.4 ISED EMC compliance

The device complies with the Canadian ICES-003 Class B specifications. CAN ICES-3(B)/ NMB-3 (B).

This device complies with Innovation, Science and Economic Development Canada's license exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause

interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil exempt de licence est conforme aux CNR d'Innovation, Science et Développement économique Canada. Son utilisation est sujette aux deux conditions suivantes: (1) Cet appareil ne doit pas produire d'interférences; et (2) Cet appareil doit accepter tout type d'interférences, notamment les interférences pouvant provoquer une utilisation non désirée de l'appareil.

The device complies with Innovation, Science and Economic Development Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

6.3.5 ISED Restriction for devices with WiFi

Innovation, Science and Economic Development Canada license-exempt Radio Standards Specification (RSS) statement

- To satisfy ISED RF exposure requirements, a separation distance of 29 cm or more should be maintained between the antenna of this device and the person during the device operation. To ensure compliance, operations at closer than this distance is not recommended.
- The device for operation in the band 5150-5250 MHz is only for indoor use and to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the E.I.R.P. limit.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the E.I.R.P. limits as appropriate.
- Where applicable, antenna type(s), antenna models, and worst-case tilt angle(s) necessary to remain compliant with the E.I.R.P. elevation mask requirement set forth in section 6.2.2.3 (RSS-247) shall be clearly indicated.
- The operation shall be limited to indoor use only.

Déclaration de conformité au Cahier des charges sur les normes radioélectriques (CNR) d'Innovation, Sciences et Développement économique Canada applicables aux appareils exempts de licence

- Pour répondre aux normes d'exposition aux RF d'ISDE, une distance de séparation de 29 cm (depend on test result) ou plus doit être maintenue entre l'antenne de cet appareil et toute personne pendant son fonctionnement. Pour garantir la conformité, toute utilisation à une distance inférieure est déconseillée.
- Cet appareil désigné pour la bande 5150-5250 MHz est réservé à une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.
- Pour les appareils dotés d'une ou plusieurs antennes amovibles et situés dans les bandes 5250-5350 MHz et 5470-5725 MHz, le gain d'antenne maximal autorisé pour les appareils doit être conforme à la limite de PIRE.

-
- Pour les appareils dotés d'une ou plusieurs antennes amovibles et situés dans la bande 5725-5850 MHz, le gain d'antenne maximal autorisé doit être conforme à la limite de PIRE.
 - Si nécessaire, le(s) type(s) d'antenne, les modèles d'antenne et le(s) pire(s) angle(s) d'inclinaison nécessaire(s) pour rester conforme à l'exigence de PIRE applicable au masque d'élévation, énoncée à la section 6.2.2.3 (CNR-247), doivent être clairement indiqués.
 - L'opération doit être limitée à l'usage d'intérieur seulement.

