Nokia WiFi Beacon

WiFi Beacon 2

Beacon 2 Product Guide

3FE-49294-AAAA-TCZZA

Issue 1

December 2020

Nokia – Proprietary and Confidential
Use pursuant to applicable agreements

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.

Nokia is a registered trademark of Nokia Corporation. Other products and company names mentioned herein may be trademarks or tradenames of their respective owners.

The information presented is subject to change without notice. No responsibility is assumed for inaccuracies contained herein.

© 2020 Nokia.

Contains proprietary/trade secret information which is the property of Nokia and must not be made available to, or copied or used by anyone outside Nokia without its written authorization.

Not to be used or disclosed except in accordance with applicable agreements.

Contents

About this document **10**

1 What's new **15**
1.1 Overview **15**
1.2 What's new in BBD Release 20.04.00, Issue 1 ..... **15**

2 ANSI CPE safety guidelines **17**
2.1 Safety instructions **17**
2.2 Safety standards compliance **19**
2.3 Electrical safety guidelines **21**

3 ETSI CPE safety guidelines **23**
3.1 Safety instructions **23**
3.2 Safety standards compliance **24**
3.3 Electrical safety guidelines **26**

4 ETSI environmental and CRoHS guidelines **27**
4.1 Environmental labels **27**
4.2 Hazardous Substances Table (HST) **28**
4.3 Other environmental requirements **29**

5 Beacon 2 unit data sheet **31**
5.1 Overview **31**
5.2 Beacon 2 part numbers and identification **31**
5.3 Beacon 2 general description **32**
5.4 Beacon 2 software and installation feature support **35**
5.5 Beacon 2 interfaces and interface capacity **35**
5.6 Beacon 2 LEDs **37**
5.7 Beacon 2 detailed specifications **37**
5.8 Beacon 2 functional blocks **39**
5.9 Beacon 2 responsible party **39**
5.10 Beacon 2 special considerations **40**

6 Install a Beacon 2 ..... **43**
6.1 Overview **43**
6.2 Purpose **43**
6.3 General **43**
6.4 Prerequisites **43**

6.5 Recommended tools 43
6.6 Safety information 43
6.7 Procedure 44

7 Replace a Beacon 2 47
7.1 Overview 47
7.2 Purpose 47
7.3 General 47
7.4 Prerequisites 47
7.5 Recommended tools 47
7.6 Safety information 47
7.7 Procedure 48

8 Configure a Beacon 2 51
8.1 Overview 51
GUI configuration 53
8.2 Logging in to the web-based GUI of the Beacon 2 53
Viewing device information and connection status 56
8.3 Overview 56
8.4 Viewing device information 56
8.5 Viewing LAN status 57
8.6 Viewing WAN status 61
8.7 Viewing WAN Status IPv6 62
8.8 Viewing home networking information 64
Maintenance 67
8.9 Overview 67
8.10 Configuring the password 67
8.11 Managing the device 69
8.12 Restoring the configuration 70
8.13 Backing up the configuration 71
8.14 Upgrading firmware 71
8.15 Rebooting the device 72
8.16 Resetting to factory defaults 73
8.17 Diagnosing WAN connections 74
8.18 Viewing log files 76
Configuring Security 78
8.19 Overview 78
8.20 Configuring firewall 78

8.21 Configuring MAC filter 79
8.22 Configuring IP filter 81
8.23 Configuring DMZ and ALG 83
8.24 Configuring Access control 84
Configuring the network 87
8.25 Overview 87
8.26 Configuring LAN 87
8.27 Configuring LAN IPv6 89
8.28 Configuring WAN 91
8.29 Configuring WAN DHCP 93
8.30 Configuring Wireless (2.4GHz) 95
8.31 Configuring Wireless (5 GHz) 98
8.32 Configuring IP Routing 101
8.33 Configuring DNS 103
8.34 Configuring TR-069 104
8.35 Configuring Mesh 105
Configuring the application 108
8.36 Overview 108
8.37 Configuring port forwarding 108
8.38 Configuring port triggering 110
8.39 Configuring DDNS 111
8.40 Configuring NTP 113
8.41 Configuring UPNP 114
TroubleShooting 116
8.42 Overview 116
8.43 Troubleshooting 116

List of tables

Table 2-1 Safety labels....18
Table 3-1 Safety labels....24
Table 3-2 Safety labels....25
Table 5-1 Beacon 2 identification....31
Table 5-2 Beacon 2 power supply ordering information....32
Table 5-3 Beacon 2 function detail....34
Table 5-4 Beacon 2 interface connection capacity....35
Table 5-5 Beacon 2 physical connections....36
Table 5-6 Beacon 2 LED indications....37
Table 5-7 Beacon 2 physical specifications....37
Table 5-8 Beacon 2 dimension data specifications....38
Table 5-9 Beacon 2 power consumption specifications....38
Table 5-10 Beacon 2 environmental specifications....39
Table 5-11 Responsible party contact information....39
Table 8-1 Device Information parameters....57
Table 8-2 LAN Status parameters....60
Table 8-3 WAN Status parameters....62
Table 8-4 WAN Status IPv6 parameters....63
Table 8-5 Home Networking parameters....65
Table 8-6 Password parameters....68
Table 8-7 Device Management parameters....69
Table 8-8 Diagnostics parameters....75
Table 8-9 Log parameters....77
Table 8-10 Firewall parameters....79
Table 8-11 MAC filter parameters....80
Table 8-12 IP filter parameters....82
Table 8-13 ALG parameters....84
Table 8-14 DMZ parameters....84
Table 8-15 Access control parameters....85
Table 8-16 LAN parameters....88
Table 8-17 LAN parameters....90

Table 8-18 WAN parameters....92
Table 8-19 WAN DHCP parameters....94
Table 8-20 Wireless (2.4GHz) parameters....97
Table 8-21 Wireless (5GHz) parameters....99
Table 8-22 IP Routing parameters....102
Table 8-23 DNS parameters....103
Table 8-24 TR-069 network parameters....105
Table 8-25 Mesh parameters....106
Table 8-26 Port Forwarding parameters....109
Table 8-27 Port Triggering parameters....110
Table 8-28 DDNS parameters....112
Table 8-29 NTP parameters....113
Table 8-30 Troubleshooting parameters....117

List of figures

Figure 2-1 Sample safety label 19
Figure 3-1 Sample safety label 25
Figure 4-1 Products below MCV value label 27
Figure 4-2 Products above MCV value label 28
Figure 4-3 Recycling/take back/disposal of product symbol 29
Figure 5-1 Beacon 2 WiFi gateway/beacon 33
Figure 5-2 Beacon 2 physical connections 36
Figure 5-3 Single-residence WiFi CPE with Gigabit Ethernet 39
Figure 6-1 Beacon 2 connections 45
Figure 7-1 Beacon 2 connections 49
Figure 8-1 Beacon 2 web-based GUI dashboard 53
Figure 8-2 Web GUI Login page 54
Figure 8-3 Device Info page 57
Figure 8-4 LAN Wireless Info page 59
Figure 8-5 WAN Status page 61
Figure 8-6 WAN Status IPv6 page 63
Figure 8-7 Home Networking page 65
Figure 8-8 Password page 68
Figure 8-9 Device Management page 69
Figure 8-10 Backup and Restore page 70
Figure 8-11 Firmware Upgrade page 72
Figure 8-12 Reboot Device page 73
Figure 8-13 Factory Default page 74
Figure 8-14 Diagnostics page 75
Figure 8-15 Log page 76
Figure 8-16 Firewall page 78
Figure 8-17 MAC filter page 80
Figure 8-18 IP Filter page 82
Figure 8-19 ALG Config and DMZ Config page 83
Figure 8-20 Access control page 85
Figure 8-21 LAN page 88

Figure 8-22 LAN IPv6 page 90
Figure 8-23 WAN page 92
Figure 8-24 WAN DHCP page 94
Figure 8-25 Wireless (2.4 GHz) page 96
Figure 8-26 Wireless (5GHz) 99
Figure 8-27 IP Routing page 102
Figure 8-28 DNS page 103
Figure 8-29 TR-069 page 104
Figure 8-30 MESH page 106
Figure 8-31 Port Forwarding page 109
Figure 8-32 Port Triggering page 110
Figure 8-33 DDNS page 112
Figure 8-34 NTP page 113
Figure 8-35 UPNP page 114
Figure 8-36 Troubleshoot page 116

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 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 WiFi Beacon's 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, please 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, please 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

Select **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 list.

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/).

For ordering information, contact your Nokia sales representative.

How to comment

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

1 What's new

1.1 Overview

1.1.1 Purpose

1.1.2 Contents

1.1 Overview	15
1.2 What's new in BBD Release 20.04.00, Issue 1	15

1.2 What's new in BBD Release 20.04.00, Issue 1

The Product Guide is a new guide in BBD Release 20.04.00. In future releases, this chapter will provide tables of the feature and document changes applicable to this guide.

2 ANSI CPE safety guidelines

This chapter provides information about the mandatory regulations that govern the installation and operation of devices in the North American or ANSI market.

2.1 Safety instructions

This section describes the safety instructions that are provided in the CPE customer documentation and on the equipment.

2.1.1 Safety instruction boxes in customer documentation

The safety instruction boxes are provided in the CPE customer documentation. Observe the instructions to meet safety requirements.

The following is an example of the Danger box.

DANGER

Hazard

Possibility of personal injury.

The Danger box indicates that the described activity or situation may pose a threat to personal safety. It calls attention to a situation or procedure which, if not correctly performed or adhered to, may result in death or serious physical harm.

Do not proceed beyond a Danger box until the indicated conditions are fully understood and met.

The following is an example of the Warning box.

WARNING

Equipment Damage

Possibility of equipment damage.

Possibility of data loss.

The Warning box indicates that the described activity or situation may, or will, cause equipment damage, loss of data, or serious performance problems. It identifies a possible equipment-damaging situation or provides essential information to avoid the degradation of system operations or data.

Do not proceed beyond a warning until the indicated conditions are fully understood and met.

The following is an example of the Caution box.

CAUTION

Service Disruption

Possibility of service interruption.

Service interruption.

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

Do not proceed beyond a caution until the indicated conditions are fully understood and met.

The following is an example of the Note box.

Note: Information of special interest.

The Note box provides information that assists the personnel working with devices. It does not provide safety-related instructions.

2.1.2 Safety-related labels

The customer premises equipment is labeled with specific safety compliance information and instructions that are related to a variant of the CPE. Observe the instructions on the safety labels.

Table 2-1, “Safety labels” (p. 17) provides examples of the text in the various CPE safety labels.

Table 2-1 Safety labels

Label text	Description
ETL compliance	Communication service equipment US listed.
ESD warning	Caution: This assembly contains electrostatic sensitive device.
FCC standards compliance	Tested to comply with FCC standards for home or office use.

Figure 2-1, “Sample safety label” (p. 19) shows a sample safety label located on the bottom of the Beacon 2.

Figure 2-1 Sample safety label

2.2 Safety standards compliance

This section describes the CPE compliance with North American safety standards.

WARNING

Equipment Damage

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

2.2.1 EMC, EMI, and ESD standards compliance

The customer premises equipment complies with the following requirements:

- Federal Communications Commission (FCC) CFR 47, Part 15, Subpart B, Class A requirements for equipment

This equipment 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:

- Reorient 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 needed.
- Consult the dealer or an experienced radio/TV technician for help.

2.2.2 Energy-related products standby and off modes compliance

Hereby, Nokia declares that the Beacon 2 devices are in compliance with the essential requirements and other relevant provisions of Directive 2009/125/EC together with Commission Regulation (EC) No 1275/2008 and Commission Regulation (EC) No 801/2013.

The Beacon 2 devices qualify as high network availability (HiNA) equipment. Since the main purpose of Beacon 2 devices is to provide network functionality with HiNA 7 days/24 hours, the modes Off/Standby, Power Management, and Networked Standby are inappropriate.

For information about the type and number of network ports, see 5.5 “Beacon 2 interfaces and interface capacity” (p. 35) in Chapter 5, “Beacon 2 unit data sheet”.

For information about power consumption, see 5.7 “Beacon 2 detailed specifications” (p. 37) in Chapter 5, “Beacon 2 unit data sheet”.

2.2.3 FCC statement

This equipment 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:

- Reorient 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.

2.2.4 FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and consider removing the no-collocation statement.

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

1. this device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation.

Note: For product availability in the USA and Canada, only channels 1 to 11 can be operated. Selection of other channels is not possible.

This device is restricted for indoor use.

CAUTION

Service Disruption

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

2.2.5 Resistibility requirements compliance

The customer premises equipment complies with the requirements of ITU Recommendation K.21 for resistibility of telecommunication equipment installed in customer premises to overvoltage and overcurrents.

2.3 Electrical safety guidelines

This section provides the electrical safety guidelines for the customer premises equipment.

Beacon 2 devices are compliant with the following standards

- IEC-62368-1
- UL-62368-1

Note: The devices comply with the U.S. National Electrical Code. However, local electrical authorities have jurisdiction when there are differences between the local and U.S. standards.

2.3.1 Power supplies

The use of any non-Nokia approved power supplies or power adapters is not supported or endorsed by Nokia. Such use will void any warranty or support contract with Nokia. Such use greatly increases the danger of damage to equipment or property.

2.3.2 Cabling

The following are the guidelines regarding cables used for the customer premises equipment:

- Use only cables approved by the relevant national electrical code.

3 ETSI CPE safety guidelines

This chapter provides information about the mandatory regulations that govern the installation and operation of devices.

3.1 Safety instructions

This section describes the safety instructions that are provided in the CPE customer documentation and on the equipment.

3.1.1 Safety instruction boxes

The safety instruction boxes are provided in the CPE customer documentation. Observe the instructions to meet safety requirements.

The following is an example of the Danger box.

DANGER

Hazard

Possibility of personal injury.

The Danger box indicates that the described activity or situation may pose a threat to personal safety. It calls attention to a situation or procedure which, if not correctly performed or adhered to, may result in death or serious physical harm.

Do not proceed beyond a Danger box until the indicated conditions are fully understood and met.

The following is an example of the Warning box.

WARNING

Equipment Damage

Possibility of equipment damage.

Possibility of data loss.

The Warning box indicates that the described activity or situation may, or will, cause equipment damage, loss of data, or serious performance problems. It identifies a possible equipment-damaging situation or provides essential information to avoid the degradation of system operations or data.

Do not proceed beyond a warning until the indicated conditions are fully understood and met.

The following is an example of the Caution box.

CAUTION

Service Disruption

Possibility of service interruption.

Service interruption.

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

Do not proceed beyond a caution until the indicated conditions are fully understood and met.

The following is an example of the Note box.

Note: Information of special interest.

The Note box provides information that assists the personnel working with devices. It does not provide safety-related instructions.

3.1.2 Safety-related labels

The customer premises equipment is labeled with the specific safety instructions and compliance information that is related to a variant of the CPE. Observe the instructions on the safety labels.

Table 3-1, “Safety labels” (p. 23) provides sample safety labels on the customer premises equipment.

Table 3-1 Safety labels

Label text	Description
CE marking	Indicates compliance to the European Council Directives including EN 60950-1 and EN 62368-1 safety
ESD warning	Caution: This assembly contains an electrostatic sensitive device.

3.2 Safety standards compliance

This section describes the CPE compliance with the European safety standards.

3.2.1 EMC, EMI, and ESD compliance

The customer premises equipment complies with the following EMC, EMI, and ESD requirements:

- EN 300-386 V1.6.1: Electromagnetic Compatibility and Radio Spectrum Matters (ERM): Telecommunications Network Equipment; Electromagnetic Compatibility (EMC) requirements; Electrostatic Discharge (ESD) requirements
- EN 301489-1: Electromagnetic Compatibility and Radio Spectrum Matters (ERM): Telecommunications Network Equipment; Electromagnetic Compatibility (EMC) Standard for Radio Equipment and Servcies; part 1: Common Technical Requirements
- EN 301489-17: Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Electromagnetic Compatibility (EMC) Standard for Radio Equipment; Part 17: Specific Conditions for Broadband Data Transmission Systems.

- Radio Equipment Directive (RED) 2014/53/EU (applicable from 13 June 2016)
- EN 55032 (2015): Electromagnetic compatibility of multimedia equipment - Emission Requirements
- EN 55024 (2010): Information Technology Equipment, Immunity Characteristics, limits and methods of measurement
- Electromagnetic Compatibility (EMC) directive 2014/30/EU
- European Council Directive 2004/108/EC
- Low Voltage (LVD) directive 2014/35/EC

3.2.2 Equipment safety standard compliance

The customer premises equipment is labeled with specific safety compliance information and instructions that are related to a variant of the CPE. Observe the instructions on the safety labels.

Table 3-2, “Safety labels” (p. 24) provides examples of the text in the various CPE safety labels.

Table 3-2 Safety labels

Label text	Description
TUV compliance	Type 3R enclosure - Rainproof.
ESD warning	Caution: This assembly contains electrostatic sensitive device.
CDRH compliance	Complies with 21 CFR 1040.10 and 1040.11.
CE marking	There are various CE symbols for CE compliance.

Figure 3-1, “Sample safety label” (p. 25) shows a sample safety label located on the bottom of the Beacon 2.

Figure 3-1 Sample safety label

The customer premises equipment complies with the requirements of EN 60950-1 and EN 62368-1, Safety of Information Technology Equipment for use in a restricted location.

- ETS 300 019-2-1 Storage Class T1.2
- ETS 300 019-2-2 Transport Class T2.3
- ETS 300 019-2-3 Stationary Class T3.2

3.2.3 Environmental standard compliance

The customer premises equipment complies with the EN 300 019 European environmental standards.

3.2.4 CE RED RF Radiation Exposure Statement

This device complies with CE RED radiation exposure limits set forth for an uncontrolled environment. To comply with CE RED RF exposure compliance requirements, this grant is applicable only for mobile configurations. The antennas used for the transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

3.2.5 Resistibility requirements compliance

The customer premises equipment complies with the requirements of ITU Recommendation K.21 for resistibility of telecommunication equipment installed in customer premises to over voltage and overcurrents.

3.2.6 Acoustic noise emission standard compliance

The customer premises equipment complies with EN 300 753 acoustic noise emission limit and test methods.

3.3 Electrical safety guidelines

This section provides the electrical safety guidelines for the customer premises equipment.

Note: The devices comply with the U.S. National Electrical Code. However, local electrical authorities have jurisdiction when there are differences between the local and U.S. standards. The devices comply with BS EN 61140.

3.3.1 Power supplies

The use of any non-Nokia approved power supplies or power adapters is not supported or endorsed by Nokia. Such use will void any warranty or support contract with Nokia. Such use greatly increases the danger of damage to equipment or property.

3.3.2 Cabling

The following are the guidelines regarding cables used for the customer premises equipment:

- All cables must be approved by the relevant national electrical code.

4 ETSI environmental and CRoHS guidelines

This chapter provides information about the ETSI environmental China Restriction of Hazardous Substances (CRoHS) regulations that govern the installation and operation of devices. This chapter also includes environmental operation parameters of general interest.

4.1 Environmental labels

This section describes the environmental instructions that are provided with the customer documentation, equipment, and location where the equipment resides.

4.1.1 Overview

CRoHS is applicable to Electronic Information Products (EIP) manufactured or sold and imported in the territory of the mainland of the People's Republic of China. EIP refers to products and their accessories manufactured by using electronic information technology, including electronic communications products and such subcomponents as batteries and cables.

4.1.2 Environmental related labels

Environmental labels are located on appropriate equipment. The following are sample labels.

Products below Maximum Concentration Value (MCV) label

Figure 4-1, "Products below MCV value label" (p. 27) shows the label that indicates a product is below the maximum concentration value, as defined by standard SJ/T11363-2006 (Requirements for Concentration Limits for Certain Hazardous Substances in Electronic Information Products). Products with this label are recyclable. The label may be found in this documentation or on the product.

Figure 4-1 Products below MCV value label

18986

Products containing hazardous substances above Maximum Concentration Value (MCV) label

Figure 4-2, “Products above MCV value label” (p. 27) shows the label that indicates a product is above the maximum concentration value, as defined by standard SJ/T11363-2006 (Requirements for Concentration Limits for Certain Hazardous Substances in Electronic Information Products). The number contained inside the label indicates the Environment-Friendly User Period (EFUP) value. The label may be found in this documentation or on the product.

Figure 4-2 Products above MCV value label

18985

Together with major international telecommunications equipment companies, Nokia has determined it is appropriate to use an EFUP of 50 years for network infrastructure equipment and an EFUP of 20 years for handsets and accessories. These values are based on manufacturers' extensive practical experience of the design, manufacturing, maintenance, usage conditions, operating environments, and physical condition of infrastructure and handsets after years of service. The values reflect minimum values and refer to products operated according to the intended use conditions. See 4.2 “Hazardous Substances Table (HST)” (p. 28) for more information.

4.2 Hazardous Substances Table (HST)

This section describes the compliance of the OLT and CPE to the CRoHS standard when the product and subassemblies contain hazardous substances beyond the MCV value. This information is found in this user documentation where part numbers for the product and subassemblies are listed. It may be referenced in other OLT and CPE documentation.

In accordance with the People’s Republic of China Electronic Industry Standard Marking for the Control of Pollution Caused by Electronic Information Products (SJ/T11364-2006), customers may access the Nokia Hazardous Substance Table, in Chinese, from the following location:

- http://www.alcatel-sbell.com.cn/wwwroot/images/upload/private/1/media/ChinaRoHS.pdf

(http://www.alcatel-sbell.com.cn/wwwroot/images/upload/private/1/media/ChinaRoHS.pdf)

4.3 Other environmental requirements

Observe the following environmental requirements when handling the P-OLT or CPE

4.3.1 CPE environmental requirements

See the CPE technical specification documentation for more information about temperature ranges.

4.3.2 Transportation

According to EN 300-019-1-2 - Class 2.3, transportation of the equipment must be in packed, public transportation with no rain on packing allowed.

4.3.3 EU RoHS

European Union (EU) Directive 2011/65/EU, “Restriction of the use of certain Hazardous Substances” (RoHS), restricts the use of lead, mercury, cadmium, hexavalent chromium, and certain flame retardants in electrical and electronic equipment. Nokia products shipped to the EU comply with the EU RoHS Directive.

Nokia has implemented a material/substance content management process. The process is described in: Nokia process for ensuring RoHS Compliance (1AA002660031ASZZA). This ensures compliance with the European Union Directive 2011/65/EU on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment.

4.3.4 End-of-life collection and treatment

Electronic products bearing or referencing the symbol shown in Figure 4-3, “Recycling/take back/disposal of product symbol” (p. 29), 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.

Note: In the European Union, a solid bar under the symbol for a crossed-out wheeled bin indicates that the product was put on the market after 13 August 2005.

Figure 4-3 Recycling/take back/disposal of product symbol

About mark is used in compliance to European Union WEEE Directive (2012/19/EU).

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 Nokia products bearing the logo shown in Figure 4-3, “Recycling/take back/disposal of product symbol” (p. 29) at the end of their useful life, or products displaced by Nokia equipment offers. For information regarding take-back of equipment by Nokia, or for more information regarding the requirements for recycling/disposal of product, contact your Nokia account manager or Nokia take back support at sustainability.global@nokia.com.

5 Beacon 2 unit data sheet

5.1 Overview

5.1.1 Purpose

5.1.2 Contents

5.1 Overview	31
5.2 Beacon 2 part numbers and identification	31
5.3 Beacon 2 general description	32
5.4 Beacon 2 software and installation feature support	35
5.5 Beacon 2 interfaces and interface capacity	35
5.6 Beacon 2 LEDs	37
5.7 Beacon 2 detailed specifications	37
5.8 Beacon 2 functional blocks	39
5.9 Beacon 2 responsible party	39
5.10 Beacon 2 special considerations	40

5.2 Beacon 2 part numbers and identification

Table 5-1, “Beacon 2 identification” (p. 31) provides part numbers and identification information for the Beacon 2.

Table 5-1 Beacon 2 identification

Ordering part number	Provisioning number	Description	CLEC	CPR	ECI/ Bar code
3FE 49235 AA	3FE 49294 AA	Beacon2, AX1800, US Plug, US variant, 1 pack	—	—	—
3FE 49235 BA	3FE 49294 BA	Beacon2 AX1800, EU Plug, EU variant, 1 pack	—	—	—
3FE 49235 CA	3FE 49294 CA	Beacon2, AX1800, UK Plug, UK variant, 1 pack	—	—	—
3FE 49235 DA	3FE 49294 DA	Beacon2, AX1800, AU Plug, AU variant, 1 pack	—	—	—

Table 5-2, “Beacon 2 power supply ordering information” (p. 32) provides power supply ordering information for the Beacon 2.

Table 5-2 Beacon 2 power supply ordering information

Ordering part number	Manufacturer	Applicable power supply model	Power information	Compliance detail	Notes
Kit: 1AF32499AAAA	Fu hua	UES18LU-120150SPA/ UE190819GWAD2RI	12V, 1.5A 18W AC/DC power adapter	ANSI municipality US, FCC/ETL	2-pin US input plug
	Ruide	RD1201500-C55-153MG/BS120150-UC6C-LL01	12V, 1.5A 18W AC/DC power adapter	ANSI municipality US, FCC/ETL	2-pin US input plug
Kit: 1AF32491EBAA	Fu hua	UES18LS-120150SPA/ UE190819GWAD4RI	12V, 1.5A 18W AC/DC power adapter	Europe, RCM certified	2-pin AU input plug
	Ruide	RD1201500-C55-81AG/ BK120150-FC6C-LL02	12V, 1.5A 18W AC/DC power adapter	Europe, RCM certified	2-pin AU input plug
Kit: 1AF32489AAAA	Fu hua	UES18LV-120150SPA/ UE190819GWAD1RI	12V, 1.5A 18W AC/DC power adapter	Europe, CE certified	2-pin EU input plug
Kit: 1AF32491EAAA	Ruide	RD1201500-C55-153OG/ BS120150-EC6C-LL01	12V, 1.5A 18W AC/DC power adapter	Europe, CE certified	2-pin EU input plug
Kit: 1AF32491AAAA	Fu hua	UES18LB-120150SPA/ UE190819GWAD3RI	12V, 1.5A 18W AC/DC power adapter	UK, CE certified	2-pin UK input plug
Kit: 1AF32491ECAA	Ruide	RD1201500-C55-153YG/ BS120150-YC6C-LL01	12V, 1.5A 18W AC/DC power adapter	UK, CE certified	2-pin UK input plug

5.3 Beacon 2 general description

Wi-Fi is abundantly deployed in home networks. Users crave a seamless experience at home including effortlessly connecting their wireless devices to the network. Traditional Wi-Fi networks require unique SSIDs for each of the access points or tedious set-up of Wi-Fi 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.

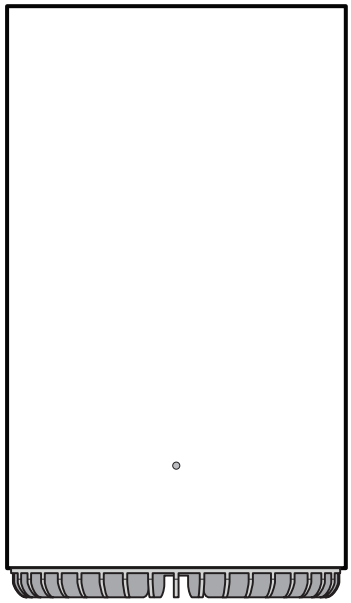
Note: The Nokia WiFi Care Portal can be accessed by the end user and the operator.

Beacon 2 devices can be deployed as either an Ethernet residential gateway or a Wi-Fi 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 Wi-Fi coverage to every corner of the home, providing seamless roaming to wireless connected devices.

The Beacon 2 has built-in concurrent dual-band Wi-Fi 802.11b/g/n/ax and 802.11n/ac/ax networking with triple-play capability. Beacon 2 devices can be configured using the Nokia WiFi mobile app, which can be downloaded to iOS and Android devices.

Figure 5-1, "Beacon 2 WiFi gateway/beacon" (p. 33) shows the Beacon 2.

Figure 5-1 Beacon 2 WiFi gateway/beacon



36526

The Beacon 2 provides the following functions and benefits.

- Automatically decide on wireless router mode or beacon mode (bridge mode) in a mesh network
- Dual-band concurrent IEEE 802.11b/g/n/ax 2x2 2.4 GHz and 802.11n/ac/ax 2x2 5 GHz
- One 10/100/1000Base-T WAN/LAN interface with RJ-45 connector and One 10/100/1000Base-T LAN interface with RJ-45 connector
- Nokia WiFi mesh middleware supports maximum three nodes in which one is root and the rest are extenders
- Embedded edge analytics optimize network performance in real-time

Benefits:

- PHY rate up to 574 Mb/s for 2.4 GHz and 1200 Mb/s for 5 GHz
- Self-healing, self-optimizing network
- Mesh topology and intelligent mesh routing
- Seamless roaming (IEEE 802.11k and 802.11v)
- Band steering, channel optimization
- High quality of service (QoS) video over Wi-Fi
- Ease of setup and user intuitive information

Table 5-3, “Beacon 2 function detail” (p. 34) lists additional function detail.

Table 5-3 Beacon 2 function detail

Function	Detail
Installation	Desk mounted
WLAN interfaces	• Supports 2x2 802.11b/g/n/ax 2.4 GHz wireless LAN (WLAN) interface • Supports 2x2 802.11n/ac/ax 5 GHz WLAN interface • Maximum effective isotropic radiated power (EIRP) on 2.4 GHz up to 500 mW and 5 GHz up to 1 W • 64-bit and 128-bit Wired Equivalent Privacy (WEP) support • Wi-Fi Protected Access (WPA) support including Pre-Shared Key (WPA-PSK), WPA2 and WPA3 personal. • Media access control (MAC) filters
Router mode	• IPv4 and IPv6 • 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 proxy/Multicast Listener Discovery (MLD) proxy • Supports TR-069/TR-111 • 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 supports maximum three nodes in which one is root and the rest are extenders
Beacon mode (Bridge mode)	• Supports IPv4 and IPv6 • Supports TR-069/TR-111 • Supports VPN pass-through for PPTP, L2TP and IPSec • IGMP v2/v3 snooping • Flexible video delivery options over Ethernet or wireless • Nokia WiFi mesh middleware supports maximum three nodes in which one is root and the rest are extenders
LED	Single multi-color LED for simple and intuitive status indication
Regulatory compliance	• UL 62368-1 • FCC Part 15 • CE

5.3.1 TR-069 object support for Wi-Fi parameters

The Beacon 2 supports the status retrieval and configuration of the following Wi-Fi 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. For more information, see 8.34 “Configuring TR-069” (p. 104).

5.3.2 Communication method to Nokia cloud management solution

The Beacon 2 communicates to the Nokia cloud management solution by TR-069 using an independent TR-069 session with the SaaS or 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.

5.3.3 TR-069 authentication using TLS and CA certificates

Beacon 2 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 2 can also authenticate the ACS using a pre-installed CA certificate.

5.4 Beacon 2 software and installation feature support

For information on installing or replacing the Beacon 2, see:

- Chapter 6, “Install a Beacon 2”
- Chapter 7, “Replace a Beacon 2”

5.5 Beacon 2 interfaces and interface capacity

Table 5-4, “Beacon 2 interface connection capacity” (p. 34) describes the supported interfaces and interface capacity for Beacon 2 devices.

Table 5-4 Beacon 2 interface connection capacity

Device type and model	Maximum capacity								
	POTS	10/100 BASE-T	10/100/1000 BASE-T	RF video (CATV)	MoCA	VDSL2	E1/T1	Local craft	GE uplink
Beacon 2	—	—	1	—	—	—	—	—	1

5.5.1 Beacon 2 connections and components

Figure 5-2, “Beacon 2 physical connections” (p. 36) shows the physical connections for Beacon 2.

Figure 5-2 Beacon 2 physical connections

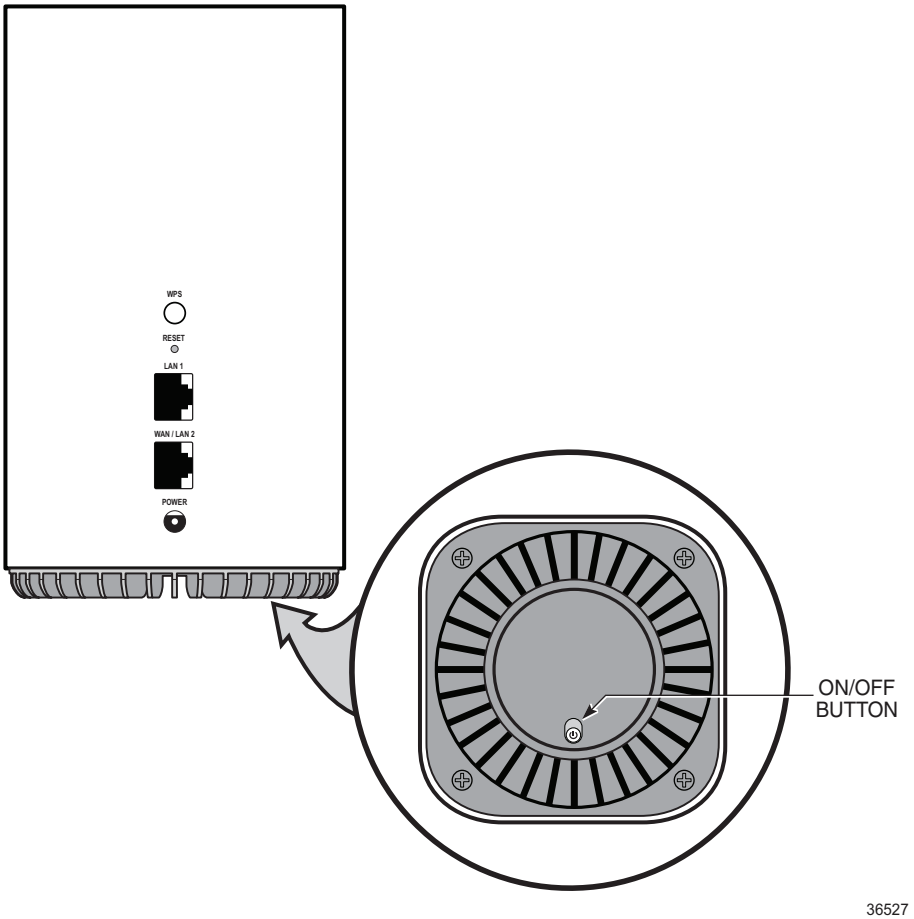


Table 5-5, “Beacon 2 physical connections” (p. 36) describes the physical connections for Beacon 2 devices.

Table 5-5 Beacon 2 physical connections

Connection	Description
WPS on/off 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 the Reset button for 10 seconds or more restores the Beacon to its factory defaults.
LAN	This connection is provided through Ethernet RJ-45 connectors. One 10/100/1000 Base-T Ethernet interface is supported. The Ethernet ports can support both data and in-band video services.
WAN port	This connection is provided through an RJ-45 Gigabit Ethernet interface.

Table 5-5 Beacon 2 physical connections (continued)

Connection	Description
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. Green illumination is “ON”. Red illumination is “OFF”.

5.6 Beacon 2 LEDs

The front of the Beacon 2 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 and the quality of its backhaul link.

Table 5-6, “Beacon 2 LED indications” (p. 37) provides LED descriptions for the Beacon 2.

Table 5-6 Beacon 2 LED indications

LED color	LED behavior	Router mode	Bridge 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.
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 not successful. A link to the next node is not operational.
	Fast pulsing	✓	✓	Factory reset
White	Solid	✓	✓	Power on

5.7 Beacon 2 detailed specifications

Table 5-7, “Beacon 2 physical specifications” (p. 37) lists the physical specifications for the Beacon 2.

Table 5-7 Beacon 2 physical specifications

Description	Specification
Length	96 mm (3.7 in.)
Width	96 mm (3.7 in.)

Table 5-7 Beacon 2 physical specifications (continued)

Description	Specification
Height	168 mm (6.6 in.)
Weight [within ± 0.5 lb (0.23 kg)]	452g (0.99 lb)

Table 5-8, “Beacon 2 dimension data specifications” (p. 38) lists the dimension data specifications for Beacon 2.

Table 5-8 Beacon 2 dimension data specifications

Dimension	Specification
Packet size supported	1518
number of IP addresses supported (or ranges)	In LAN network, the supported range is: • IPv4: 192.168.0.2 ~ 192.168.0.254 • IPv6: no limitation
number of supported Wi-Fi clients (per radio, per device, per mesh)	128 per radio, 128 per device
number of supported beacons /APs in a mesh	3 (including root AP)
number of supported WAN interfaces	8
number of supported VLANs	2-4094
number of LLIDs in the ONTs	-
number of priority queues, and overall buffer size	LAN port queques: 8; total buffer: 4MB WAN port queques: 8; total buffer: 4MB
number of multicast groups (DACL entries)	1024

Table 5-9, “Beacon 2 power consumption specifications” (p. 38) lists the power consumption specifications for the Beacon 2.

Table 5-9 Beacon 2 power consumption specifications

Maximum power (Not to exceed)	Condition	Minimum power	Condition
12.8 W	2 10/100/1000 Base-T Ethernet, Wi-Fi operational	4.89 W	interfaces/services not provisioned

Table 5-10, “Beacon 2 environmental specifications” (p. 39) lists the environmental specifications for Beacon 2.

Table 5-10 Beacon 2 environmental specifications

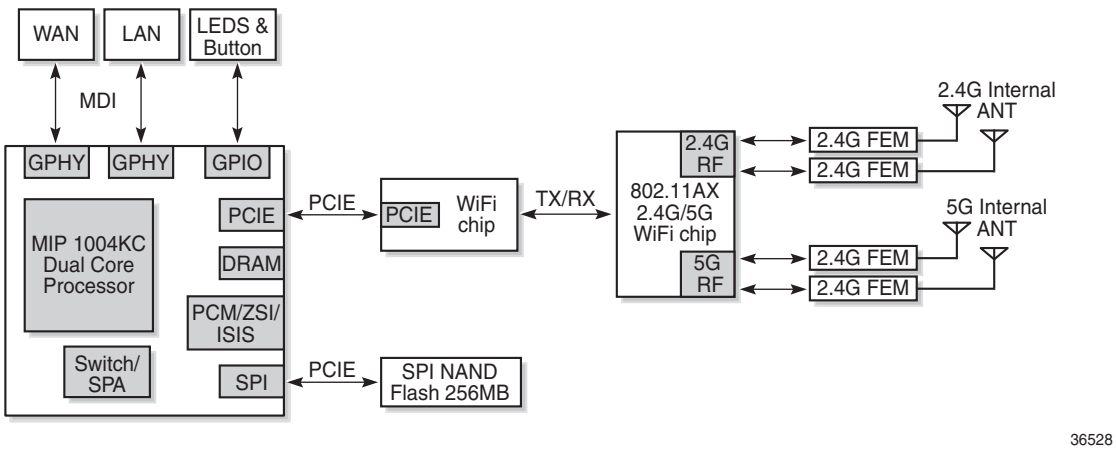
Mounting method	Temperature range and humidity	Altitude
On desk or shelf	Operating: -5°C to 45°C (23°F to 113°F) ambient temperature 95% relative humidity, non-condensing at 40°C	Contact your Nokia technical support representative for more information
	Storage: --20°C to 85°C (-4°F to 185°F)	

5.8 Beacon 2 functional blocks

Beacon 2 devices are single-residence units that support Wireless (Wi-Fi) service. Wi-Fi service on these devices is compliant with the IEEE 802.11 standard. In addition to the Wi-Fi service, these devices transmit Ethernet packets to two RJ-45 Ethernet ports.

Figure 5-3, “Single-residence WiFi CPE with Gigabit Ethernet” (p. 39) shows the functional blocks for the Beacon 2.

Figure 5-3 Single-residence WiFi CPE with Gigabit Ethernet



5.9 Beacon 2 responsible party

Table 5-11, “Responsible party contact information” (p. 39) lists the party in the US responsible for the Beacon.

Table 5-11 Responsible party contact information

Legal Company name	Nokia USA Inc.
Address	2301 SUGAR BUSH RD. STE 300, RALEIGH, NC 27612, USA
Phone, Fax	+1 866 582-3688

5.10 Beacon 2 special considerations

This section describes the special considerations for Beacon 2 devices.

5.10.1 Wi-Fi service

Beacon 2 devices feature Wi-Fi service as well as data services. Wi-Fi 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 Wi-Fi Alliance defines as the basis for Wi-Fi technology.

Wi-Fi standards and certifications

The Wi-Fi service on Beacon 2 devices supports the following IEEE standards and Wi-Fi Alliance certifications:

- ETL-Safety: UL 62368-1
- CB-Safety: EN 62368-1, EN60950-1
- FCC:
  - EMC CFR 47: part 15B (2017)
  - RF:2.4G: part 15C(2018), 5G/DFS: part 15E(2018)
  - MPE: Section 1.1310 of FCC 47 CFR part1
- CE-Safety: EN 60950-1/EN 62368-1, IEC 60950-1/IEC 62368-1, EN 60825-1, -2
  - EMC EN 300386 OTC (without WiFi)/EN 55024/EN 301489-1 (with WiFi)
  - RF: 2.4G: EN 300328, 5G/DFS: EN 301489
  - MPE: Section 1.1310 of FCC 47 CFR part1
- RCM/RCM-NZ
- Environmental: ETS 300 019-2-2 Transport Class T2.3, ETS 300 019-2-1 Storage Class T1.2, ETS 300 019-2-3 Stationary Class T3.1E/T3.2(no condense, no icing) -5-45C
- Resistibility: K.21
- Lightning, AC power port (US/UK/EU PSU): 6kV, port connected to internal cable (2.5Kv)
- ESD, 6kV/8kV
- WFA: Wi-Fi CERTIFIED™ a, b, g, n, ac, wi-fi6, WPA/WPA2/WPA3, WPS, WMM, easymesh
- Compliance with Energy Star Small Network Equipment (SNE) Specification Version 1
- Substance of Concern:
  - RoHS (2002/95/EC): Restriction of Hazardous Substances directive CROHS
  - REACH (EC 1907/2006): Registration, Evaluation, Authorisation and Restriction of Chemicals
  - WEEE (2012/19/EU): Waste Electrical and Electronic Equipment Directive

Wi-Fi GUI features

Beacon 2 devices have HTML-based Wi-Fi configuration GUIs.

In addition to the HTML-based GUI, the home user can download and use a mobile app for managing the Beacon. The Nokia WiFi app is available for iOS in the App Store, and for Android through Google Play.

5.10.2 Beacon 2 considerations and limitations

None

6 Install a Beacon 2

6.1 Overview

6.1.1 Purpose

6.1.2 Contents

6.1 Overview	43
6.2 Purpose	43
6.3 General	43
6.4 Prerequisites	43
6.5 Recommended tools	43
6.6 Safety information	43
6.7 Procedure	44

6.2 Purpose

This chapter provides the steps to install a Beacon 2.

6.3 General

The steps listed in this chapter describe installing and cabling for a Beacon 2.

6.4 Prerequisites

You need the following items before beginning the installation:

- One Ethernet cable (included with the device)
- AC power jack
- Access to the broadband network (Internet)

6.5 Recommended tools

You need the following tools for the installation:

- Paper clip

6.6 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.
- Indoor units must be installed with cables that are suitably rated and listed for indoor use.
- See the detailed specifications in the Chapter 5, “Beacon 2 unit data sheet” for the temperature ranges for these devices.

6.7 Procedure

Use this procedure to install a Beacon 2.

1

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

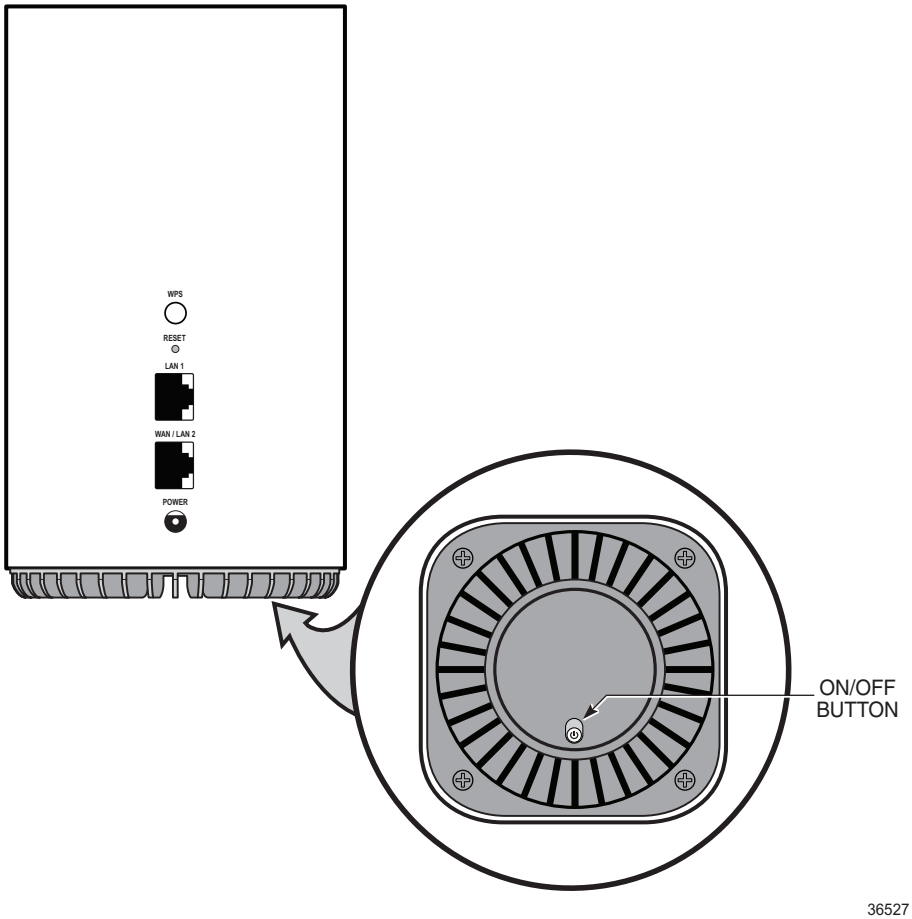
Note: The Beacon 2 cannot be stacked with another Beacon or with other equipment. The installation requirements are:

- 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 6-1, “Beacon 2 connections” (p. 45).

Figure 6-1 Beacon 2 connections



3

Connect the Ethernet cable to the RJ-45 port; see Figure 6-1, “Beacon 2 connections” (p. 45) for the location of the RJ-45 port.

4

Connect the WAN cable to the RJ-45 WAN port; see Figure 6-1, “Beacon 2 connections” (p. 45) for the location of the RJ-45 WAN port.

5

Connect the power cable to the power connector.

Note: Observe the following:

- 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, 1.5 A. The polarity of the power adapter plug must match the Beacon.

6

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

7

Verify the LED.

8

Onboard the Beacon 2 using the Nokia WiFi App.

9

If necessary, reset the Beacon 2.

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 6-1, “Beacon 2 connections” (p. 45).

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

7 Replace a Beacon 2

7.1 Overview

7.1.1 Purpose

7.1.2 Contents

7.1 Overview	47
7.2 Purpose	47
7.3 General	47
7.4 Prerequisites	47
7.5 Recommended tools	47
7.6 Safety information	47
7.7 Procedure	48

7.2 Purpose

This chapter provides the steps to replace a Beacon 2.

7.3 General

The steps listed in this chapter describe mounting and cabling for a Beacon 2.

7.4 Prerequisites

You need the following items before beginning the installation:

- One Ethernet cable (included with the device)
- AC power jack
- Access to the broadband network (Internet)

7.5 Recommended tools

You need the following tools for replacing the Beacon 2:

- Paper clip

7.6 Safety information

Read the following safety information before replacing 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.
- Indoor units must be installed with cables that are suitably rated and listed for indoor use.
- See the detailed specifications in the Chapter 5, “Beacon 2 unit data sheet” for the temperature ranges for these devices.

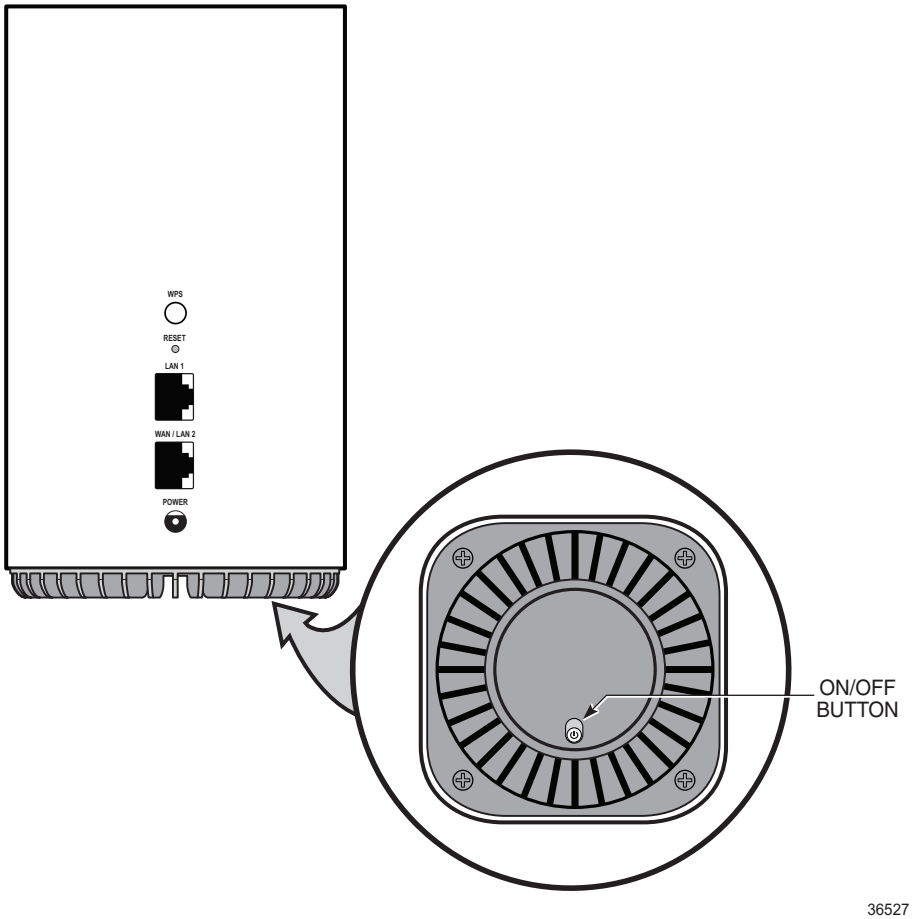
7.7 Procedure

Use this procedure to replace a Beacon 2.

1

Power down the unit by using the on/off power switch. See Figure 7-1, “Beacon 2 connections” (p. 49) for the connections on the Beacon 2.

Figure 7-1 Beacon 2 connections



2

Disconnect the WAN, Ethernet, and power cables from the Beacon 2; see Figure 7-1, “Beacon 2 connections” (p. 49) for the connector locations on the Beacon 2.

3

Replace the Beacon 2 with the new device. The device can be placed on any flat surface, such as a desk or shelf.

4

Connect the Ethernet cable directly to the RJ-45 port; see Figure 7-1, “Beacon 2 connections” (p. 49) for the location of the RJ-45 port.

5

Connect the WAN cable directly to the RJ-45 port; see Figure 7-1, “Beacon 2 connections” (p. 49) for the location of the RJ-45 WAN port.

6

Connect the power cable to the power connector.

Note: Observe the following:

- Units must be powered by a Listed or CE approved and marked limited power source with a minimum output rate of 12 V dc, 1.5 A. The polarity of the power adapter plug must match the Beacon.

7

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

8

Verify the LED.

9

Onboard the Beacon 2 using the Nokia WiFi App.

10

If necessary, reset the Beacon 2.

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 2 as shown in Figure 7-1, “Beacon 2 connections” (p. 49).

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

8 Configure a Beacon 2

8.1 Overview

8.1.1 Purpose

This chapter describes the configuration procedures.

8.1.2 Contents

8.1 Overview	51
GUI configuration	53
8.2 Logging in to the web-based GUI of the Beacon 2	53
Viewing device information and connection status	56
8.3 Overview	56
8.4 Viewing device information	56
8.5 Viewing LAN status	57
8.6 Viewing WAN status	61
8.7 Viewing WAN Status IPv6	62
8.8 Viewing home networking information	64
Maintenance	67
8.9 Overview	67
8.10 Configuring the password	67
8.11 Managing the device	69
8.12 Restoring the configuration	70
8.13 Backing up the configuration	71
8.14 Upgrading firmware	71
8.15 Rebooting the device	72
8.16 Resetting to factory defaults	73
8.17 Diagnosing WAN connections	74
8.18 Viewing log files	76
Configuring Security	78
8.19 Overview	78

8.20 Configuring firewall	78
8.21 Configuring MAC filter	79
8.22 Configuring IP filter	81
8.23 Configuring DMZ and ALG	83
8.24 Configuring Access control	84
Configuring the network	87
8.25 Overview	87
8.26 Configuring LAN	87
8.27 Configuring LAN IPv6	89
8.28 Configuring WAN	91
8.29 Configuring WAN DHCP	93
8.30 Configuring Wireless (2.4GHz)	95
8.31 Configuring Wireless (5 GHz)	98
8.32 Configuring IP Routing	101
8.33 Configuring DNS	103
8.34 Configuring TR-069	104
8.35 Configuring Mesh	105
Configuring the application	108
8.36 Overview	108
8.37 Configuring port forwarding	108
8.38 Configuring port triggering	110
8.39 Configuring DDNS	111
8.40 Configuring NTP	113
8.41 Configuring UPNP	114
TroubleShooting	116
8.42 Overview	116
8.43 Troubleshooting	116

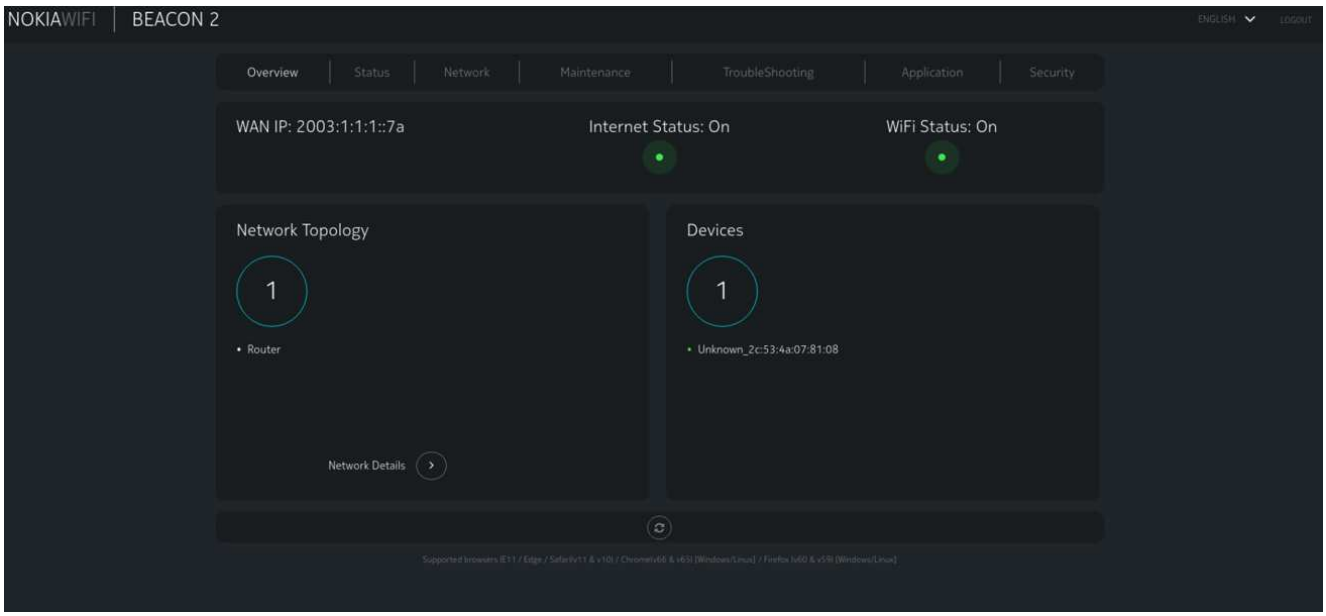
GUI configuration

Use the procedures below to use the web-based GUI for the Beacon 2.

The Beacon 2 is used as an Ethernet gateway to connect devices in the home to the Internet. The GUI provides a variety of features for the home network including routing and firewall capability. By using the GUI, users can configure the right network connectivity for all equipment in their home, including personal computers, set-top boxes, mobile phones, and other consumer electronics devices, to the Internet.

Figure 8-1, “Beacon 2 web-based GUI dashboard” (p. 53) shows the web-based GUI dashboard for the Beacon 2. Multilingual support is available when device names are displayed in the dashboard.

Figure 8-1 Beacon 2 web-based GUI dashboard



8.2 Logging in to the web-based GUI of the Beacon 2

1

Open a web browser and enter the IP address of the Beacon 2 in the address bar.

The default gateway IP address is http://192.168.18.1. You can connect to this IP address using your web browser after connecting your PC to one of Ethernet ports of the Beacon 2. The static IP address of your PC must be in the same 192.168.18.x subnet as the Beacon 2.

Note: When the Beacon 2 is in Bridge mode, there is no IP address to connect to the web-based GUI. In that case, use the following URL to log in:
http://www.webgui.nokiawifi.com (http://www.webgui.nokiawifi.com)

The Login page displays.

2

CAUTION

Service Disruption

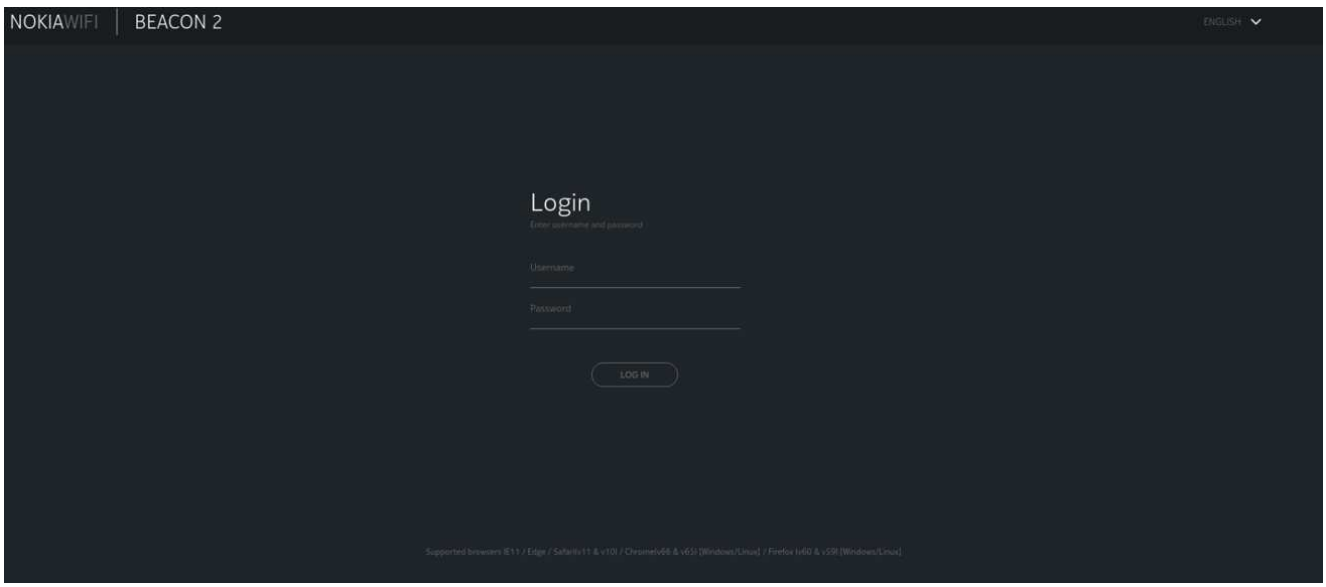
If you forget the current username and password, press the reset button for 10 seconds to reset the values to the default username and password at startup.

Pressing the **Reset** *button for less than 10 seconds reboots the device; pressing the* **Reset** *button for 10 seconds resets the device to the factory defaults.*

Enter your username and password in the Login page.

The default user name is admin. The default password is a random number, which is on the label. Refer Figure 2-1, “Sample safety label” (p. 19) for password details on the label.

Figure 8-2 Web GUI Login page



3

Click **LOG 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 2 password.
To increase password security, use a minimum of 10 characters, consisting of a mix of numbers and upper and lowercase letters.
A password must adhere to the following password rules:

- the password length must be from 8 to 24 characters.
- the first character must be a digital number or a letter.
- the password must contain at least two types of characters: numbers, letters, or special characters.
- the same character must not appear more than 8 times in a row.
- old password cannot be equal to new password.
- new password cannot be null.
- at least two character classes are required.
- the same character can not appear consecutively eight times.

End of steps

Viewing device information and connection status

8.3 Overview

8.3.1 Purpose

This chapter describes viewing the device information and connection status tasks performed from the web GUI of the Beacon 2.

8.3.2 Contents

8.3 Overview	56
8.4 Viewing device information	56
8.5 Viewing LAN status	57
8.6 Viewing WAN status	61
8.7 Viewing WAN Status IPv6	62
8.8 Viewing home networking information	64

8.4 Viewing device information

1

Select **Status** in the menu bar.

2

Click **Device Info** in the left pane. The Device Info page displays the following information about the device.

Figure 8-3 Device Info page

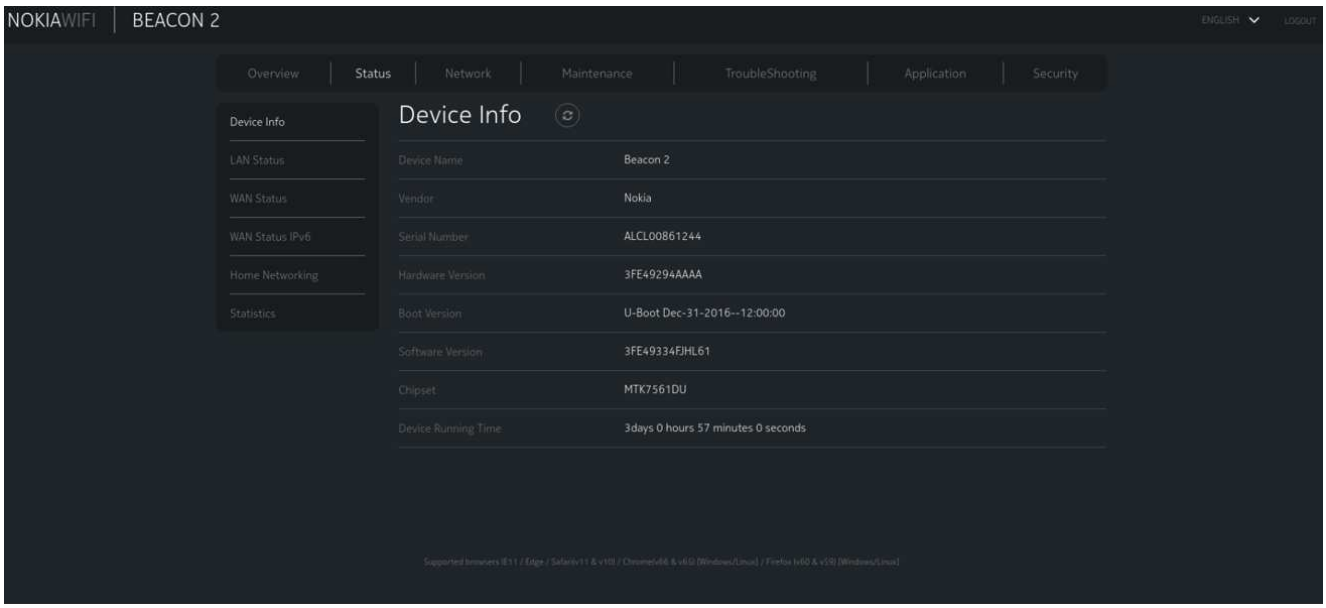


Table 8-1 Device Information parameters

Field	Description
Device Name	Name on the Beacon 2.
Vendor	Name of the vendor.
Serial Number	Serial number of the Beacon 2.
Hardware Version	Hardware version of the Beacon 2.
Boot Version	Boot version of the Beacon 2.
Software Version	Software version of the Beacon 2.
Chipset	Chipset of the Beacon 2.
Device Running Time	The duration device has run since the last reset in hours, minutes, and seconds.

You can click the **Refresh** icon to display up-to-date information.

END OF STEPS

8.5 Viewing LAN status

1

Click **Status** in the menu bar.

2

Click **LAN Status** in the left pane. The LAN Wireless Info page displays the following information.

Figure 8-4 LAN Wireless Info page

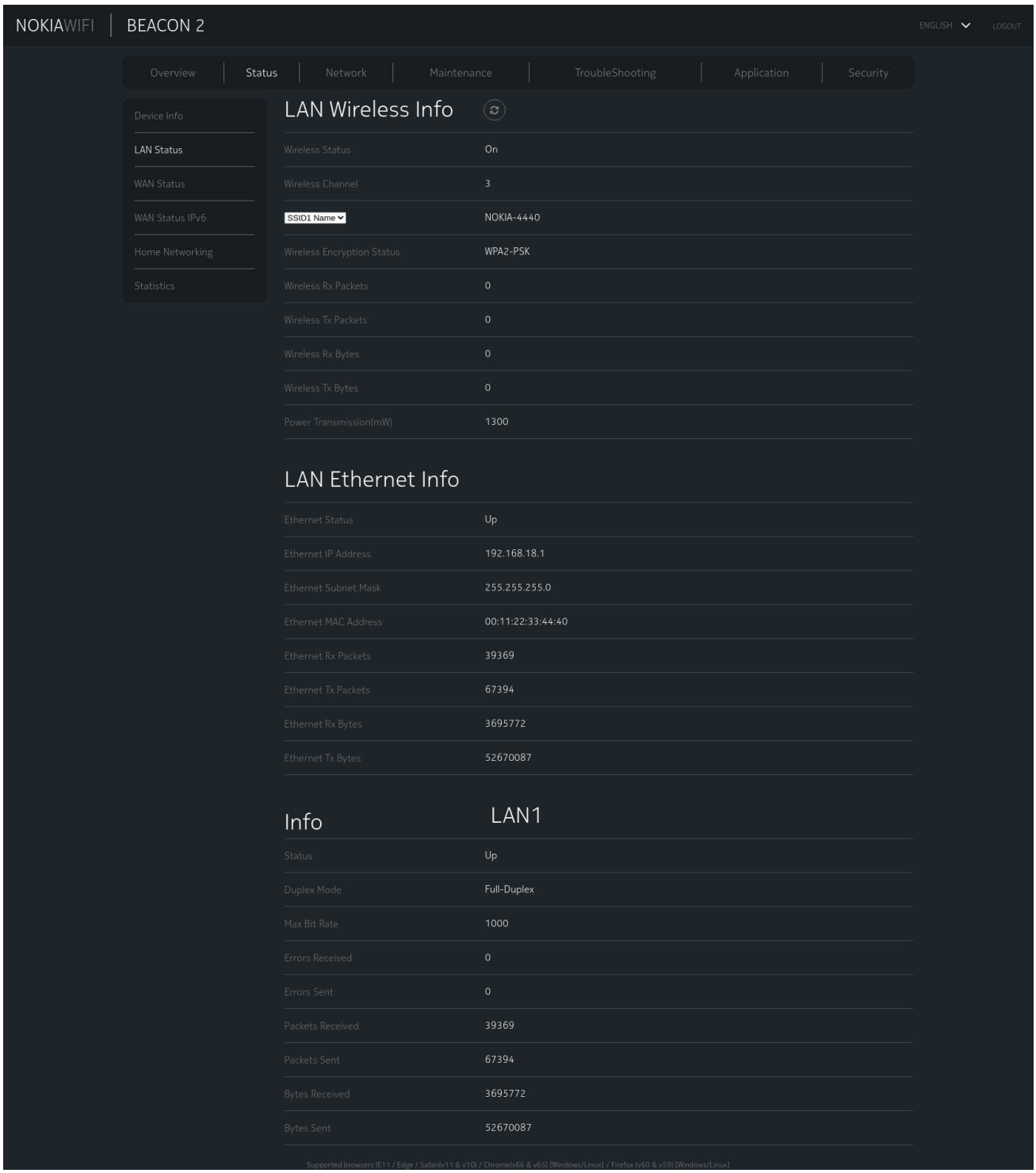


Table 8-2 LAN Status parameters

Field	Description
LAN Wireless Info	
Wireless Status	Indicates whether the wireless is on or off.
Wireless Channel	Indicates wireless channel number.
SSID Name	Name of each multilingual SSID.
Wireless Encryption Status	Encryption type used on the wireless connection. The encryption types are: • Wireless 2.4G- WPA/WPA2 Personal, WPA3 Personal, WEPEncryption, Open/none, WPA2/WPA3 Personal, WPA/WPA2 Enterprise • Wireless 5G low- WPA/WPA2 Enterprise,WPA2-AES,WPA2+WPA, WPA3+WPA2,Open/none • Wireless 5G high- WPA/WPA2 Enterprise,WPA2-AES,WPA2+WPA, WPA3+WPA2,Open/none
Wireless Encryption Status	Indicates wireless encryption status.
Wireless Rx Packets	Indicates wireless receiver packets.
Wirelss Tx Packets	Indicates wirless transmitter packets.
Wireless Rx Bytes	Power of the wireless transmission, in milliwatt (mW).
Wireless Tx Bytes	Power of the wireless transmission, in milliwatt (mW).
Power Transmission (mW)	Indicates power of the wireless transmission, in milliwatt (mW).
LAN Ethernet Info	
Ethernet Status	Indicates whether the Ethernet connection is on or off.
Ethernet IP Address	IP address of the Ethernet connection.
Ethernet Subnet Mask	Subnet mask of the Ethernet connection.
Ethernet MAC Address	MAC address of the Ethernet connection.
Ethernet Rx Packets	Indicates Ethernet receiver packets.
Ethernet Tx Packets	Indicates Ethernet transmitter packets.
Ethernet Rx Bytes	Power of the Ethernet transmission in bytes.
Ethernet Tx Bytes	Power of the Ethernet transmission in bytes.
Info	
Status	Displays the status of LAN1 and LAN2.
Duplex Mode	Displays the duplex mode of LAN1 and LAN2.
Max Bit Rate	Displays the maximum bit rate of LAN1 and LAN2.
Errors Received	Displays number of errors received.

Table 8-2 LAN Status parameters (continued)

Field	Description
Errors Sent	Displays number of errors sent.
Packets Received	Displays the packets received.
Packets Sent	Displays the packets sent.
Bytes Received	Displays the bytes received.
Bytes Sent	Displays the bytes sent.

You can click the **Refresh** icon to display up-to-date information.

END OF STEPS

8.6 Viewing WAN status

1

Click **Status** in the menu bar.

2

Click **WAN Status** in the left pane. The WAN Status page displays the following information.

Figure 8-5 WAN Status page

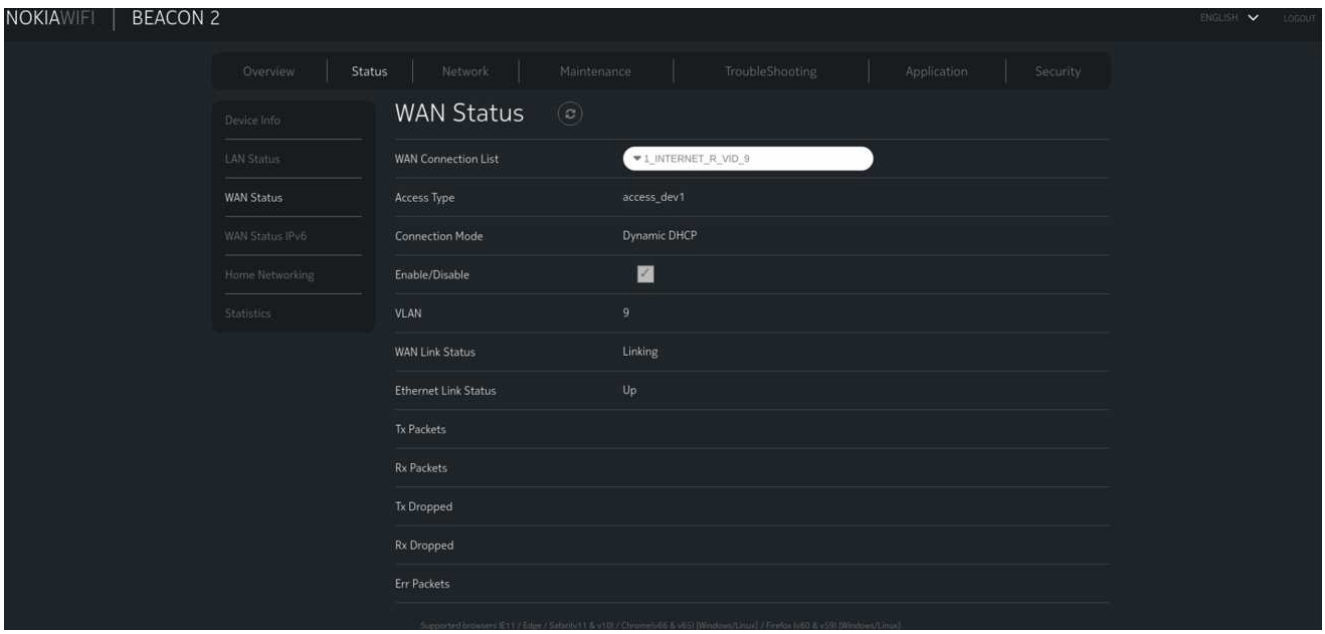


Table 8-3 WAN Status parameters

Field	Description
WAN connection list	Select the WAN connection for which to display the WAN status from the list.
Access Type	Displays the access type for the selected WAN connection.
Connection Mode	Connection mode of the WAN connection.
Enable/Disable	Displays if the WAN connection is enabled or disabled.
VLAN	Indicates the VLAN ID.
WAN Link Status	Indicates if the WAN link is up or down.
Ethernet Link Status	Indicates if the Ethernet link is up or down.
Tx Packets	Indicates transmitter packets.
Rx Packets	Indicates receiver packets.
Tx Dropped	Indicates transmitter packets dropped.
Rx Dropped	Indicated receiver packets dropped.
Err Packets	Indicates error packets.

You can click the **Refresh** icon to display up-to-date information.

END OF STEPS

8.7 Viewing WAN Status IPv6

1

Click **Status** in the menu bar.

2

Click **WAN Status IPv6** in the left pane. The WAN Status page displays the following information.

Figure 8-6 WAN Status IPv6 page

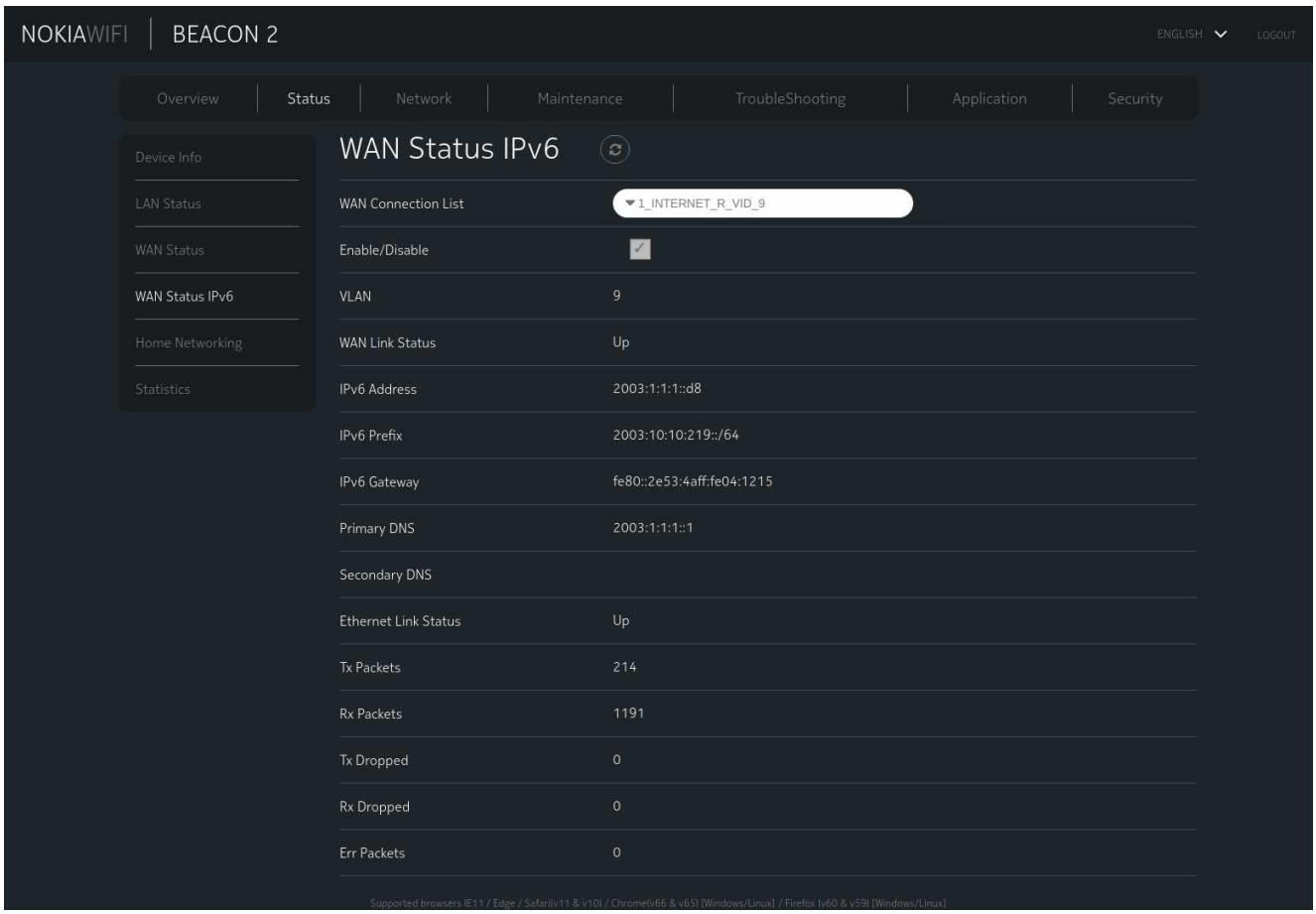


Table 8-4 WAN Status IPv6 parameters

Field	Description
WAN connection list	Select the WAN connection for which to display the WAN status from the list.
Enable/Disable	Displays if the WAN connection is enabled or disabled.
VLAN	Indicates the VLAN ID.
WAN Link Status	Indicates if the WAN link is up or down.
IPv6 Address	Indicated IPv6 address.
IPv6 Prefix	Indicates IPv6 prefix address.
IPv6 Gateway	Indicates IPv6 gateway address.
Primary DNS	Indicates primary Domain Name Server address.

Table 8-4 WAN Status IPv6 parameters (continued)

Field	Description
Secondary DNS	Indicates secondary Domain Name Server address.
Ethernet Link Status	Indicates if the Ethernet link is up or down.
Tx Packets	Indicates transmitter packets.
Rx Packets	Indicates receiver packets.
Tx Dropped	Indicates transmitter packets dropped.
Rx Dropped	Indicates receiver packets dropped.
Err Packets	Indicates error packets.

You can click the **Refresh** icon to display up-to-date information.

End of steps

8.8 Viewing home networking information

1

Click **Status** in the menu bar.

2

Click **Home Networking** in the left pane. The Home Networking page displays the following information.

Figure 8-7 Home Networking page

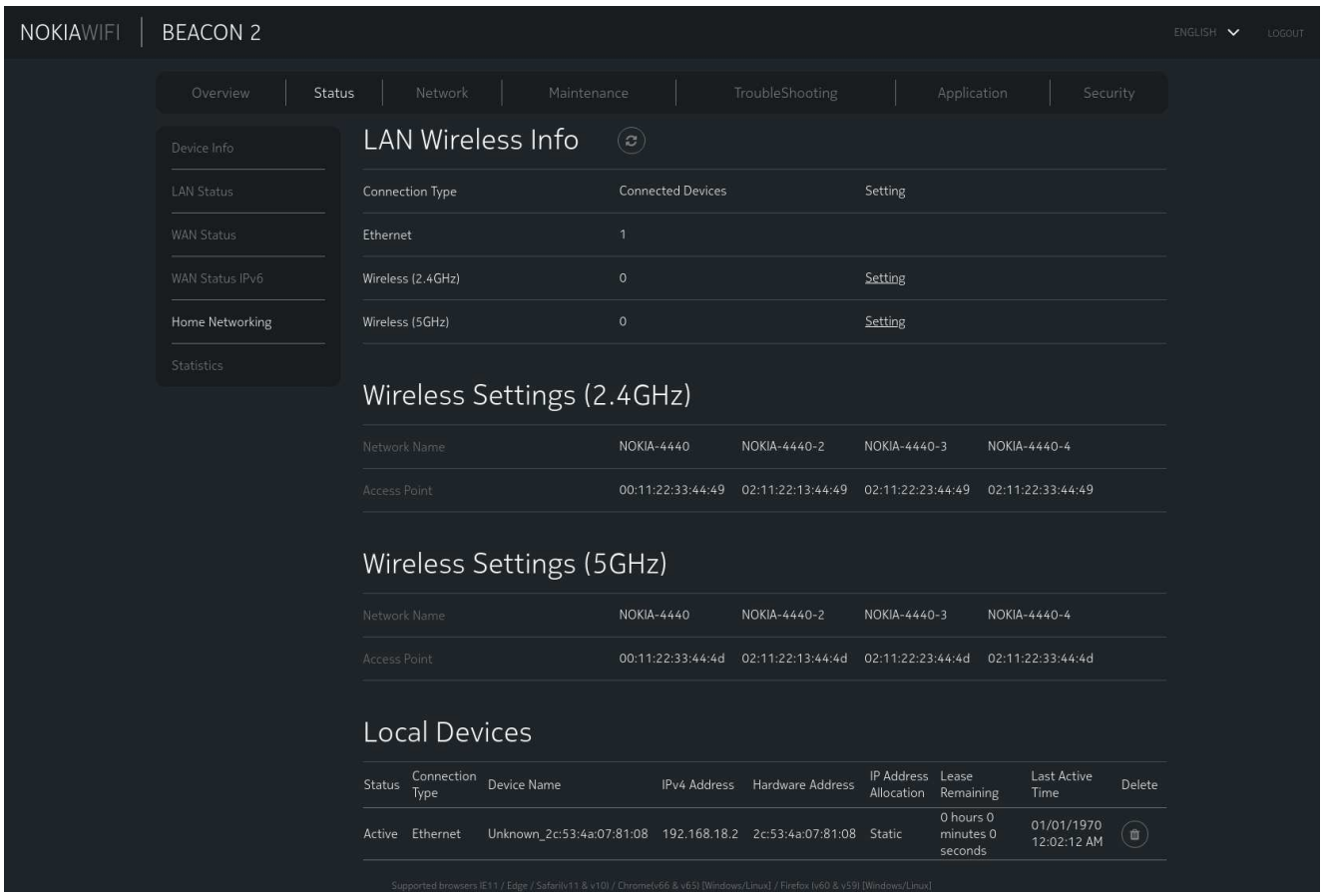


Table 8-5 Home Networking parameters

Field	Description
LAN Wireless Info	
Connection Type	The connection types are IPoe and PPPoe.
Ethernet	Displays the number of a Ethernet connections.
Wireless (2.4GHz)	Displays the number of Wireless (2.4GHz) connections.
Wireless (5GHz)	Displays the number of Wireless (5GHz) connections.
Settings	Provides a link to view the settings of the connection.
Wireless Settings (2.4GHz and 5GHz)	
Network Name	Name of the wireless network access point.
Access Point	Hexadecimal address of the wireless access point.

Table 8-5 Home Networking parameters (continued)

Field	Description
Local Devices	
Table entry	Each entry indicates the status (active or inactive), connection type, device name, IP address, hardware address, and IP address allocation, lease remaining, and last active time of each connected local device.

Click the **Delete** icon to delete a local device.

End of steps

Maintenance

8.9 Overview

8.9.1 Purpose

This chapter describes the maintenance tasks supported by Beacon 2.

8.9.2 Contents

8.9 Overview	67
8.10 Configuring the password	67
8.11 Managing the device	69
8.12 Restoring the configuration	70
8.13 Backing up the configuration	71
8.14 Upgrading firmware	71
8.15 Rebooting the device	72
8.16 Resetting to factory defaults	73
8.17 Diagnosing WAN connections	74
8.18 Viewing log files	76

8.10 Configuring the password

A password must adhere to the following password rules:

- the password may consist of uppercase letters, lowercase letters, digital numbers, and the following special characters **! # + , - / @ _ : =]**
- the password length must be from 8 to 24 characters
- the first character must be a digital number or a letter
- the password must contain at least two types of characters: numbers, letters, or special characters
- the same character must not appear more than 8 times in a row

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:

- the password is too short.
- the password is too long.
- the first character cannot be a special character.
- there are not enough character classes.

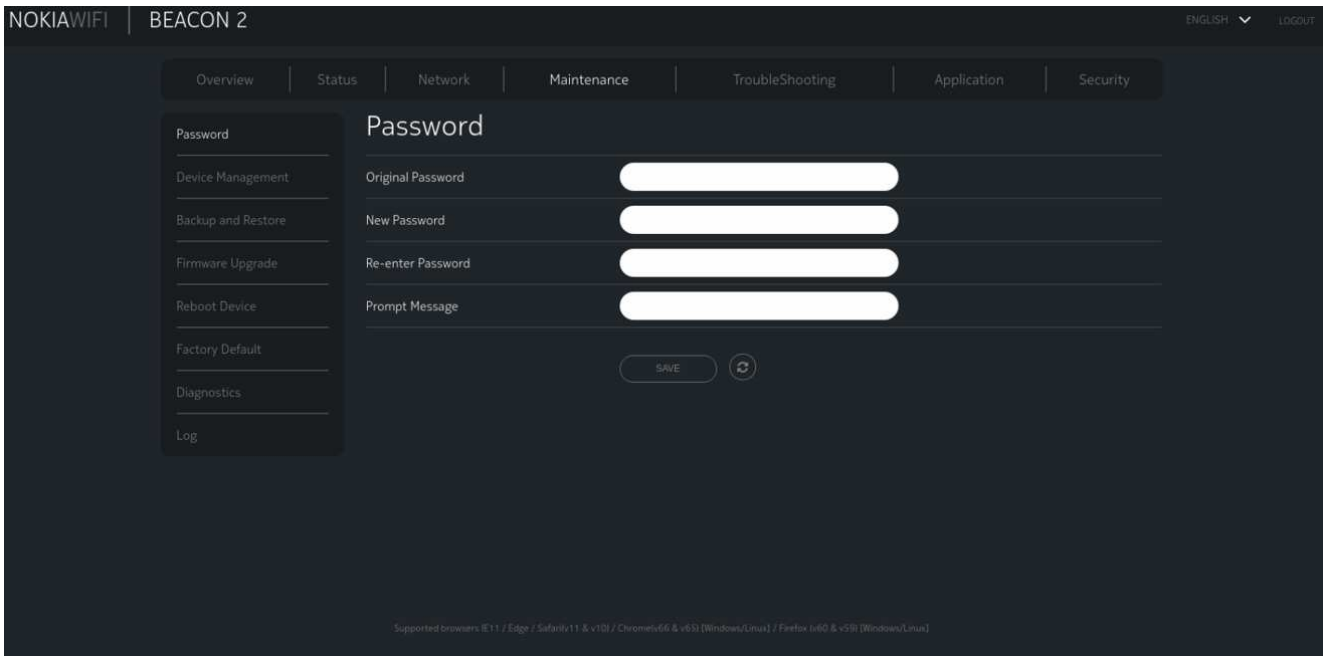
1

Click **Maintenance** in the menu bar.

2

Click **Password** in the left pane. The Password page displays.

Figure 8-8 Password page



3

Configure the following parameters:

Table 8-6 Password parameters

Field	Description
Original Password	Enter the current password.
New Password	Enter the new password (must adhere to the password rules).
Re enter Password	Re-enter the password. The new password must match entered above.
Prompt Message	Enter the password prompt message.

4

Click **SAVE**.

You can click the **Refresh** icon to update displayed information.

END OF STEPS

8.11 Managing the device

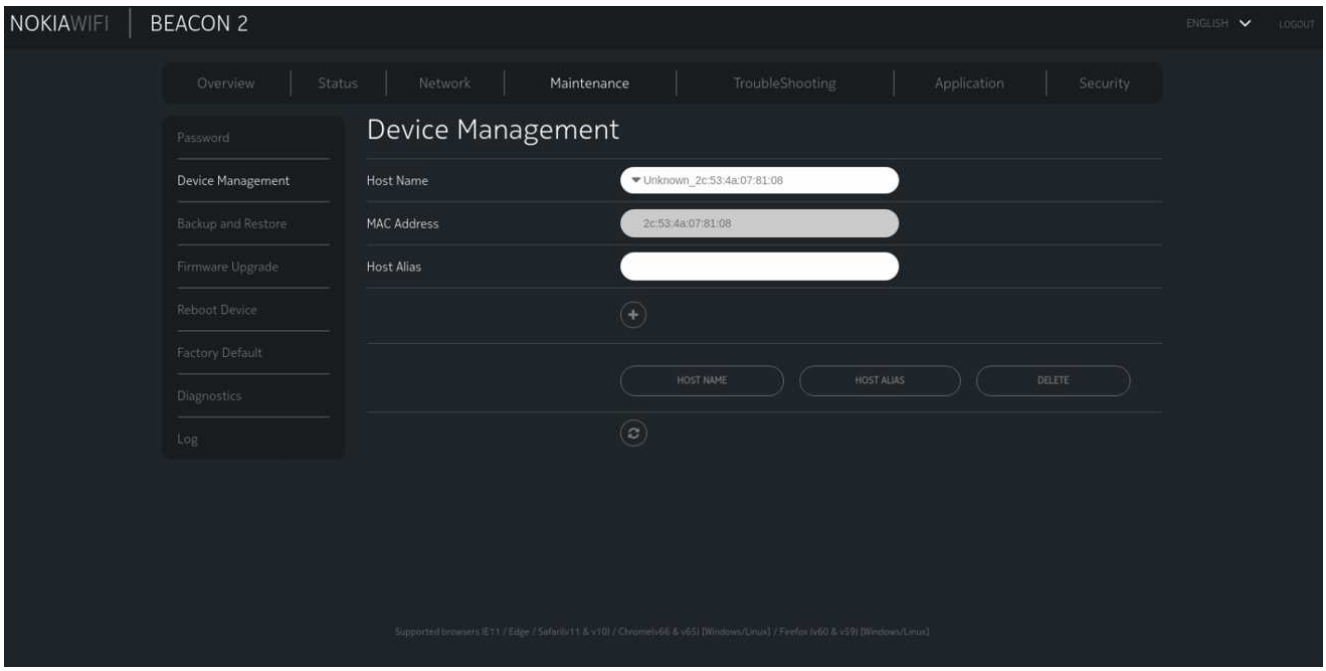
1

Click **Maintenance** in the menu bar.

2

Click **Device Management** in the left pane. The Device Management page displays.

Figure 8-9 Device Management page



3

Configure the following parameters:

Table 8-7 Device Management parameters

Field	Description
Host Name	Select a host from the list. Three multilingual host names can be listed.
MAC Address	Displays the MAC address.

Table 8-7 Device Management parameters (continued)

Field	Description
Host Alias	Enter an alias for the selected host. Three multilingual aliases can be listed.

4

Click the **Add** icon to add a host. The host is added to the table.

You can:

- Click **DELETE** to delete a particular Host Name and Host Alias.
- Click the **Refresh** icon to update displayed information.

END OF STEPS

8.12 Restoring the configuration

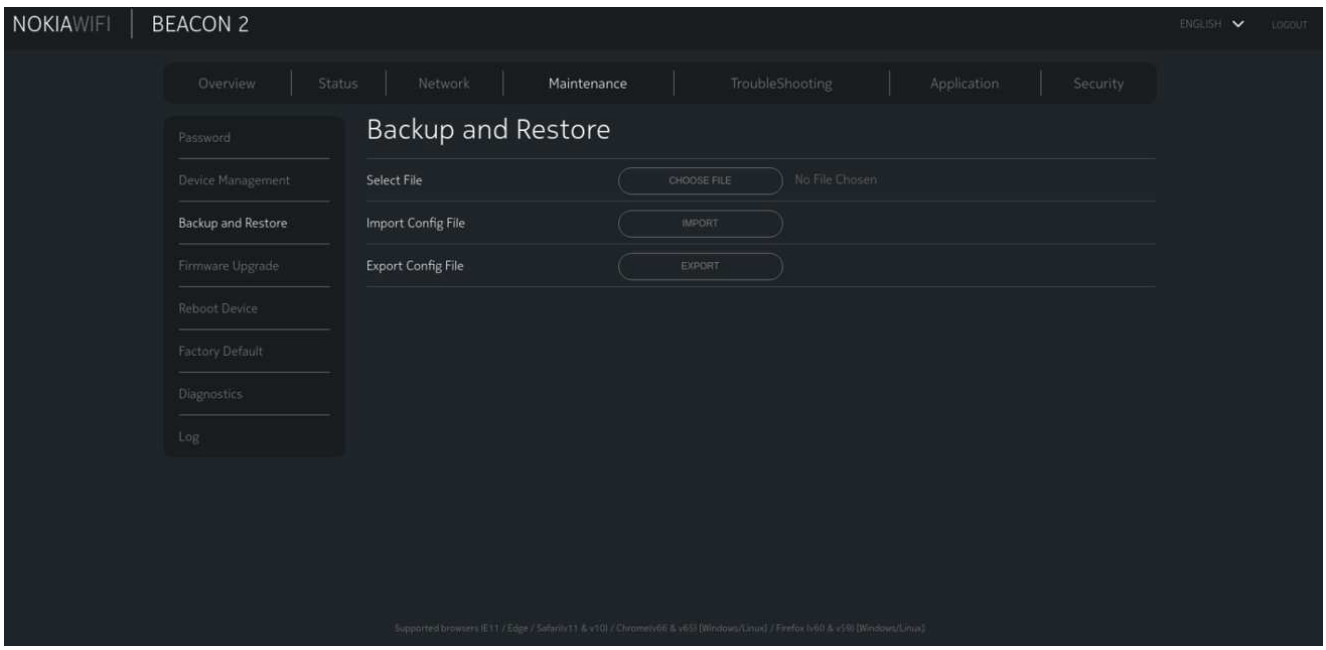
1

Click **Maintenance** in the menu bar.

2

Click **Backup and Restore** in the left pane. The Backup and Restore page displays.

Figure 8-10 Backup and Restore page



3

Click **CHOOSE FILE** and select the previously backed-up configuration file.

4

Click **IMPORT** to import the previously backed-up configuration file.

Result: The *Done upload* message displays next to the **IMPORT** button and reboot is triggered.

END OF STEPS

8.13 Backing up the configuration

1

Click **Maintenance** in the menu bar.

2

Click **Backup and Restore** in the left pane. The Backup and Restore page displays. See figure Figure 8-10, “Backup and Restore page” (p. 70).

3

Click **CHOOSE FILE** and select the previously backed-up configuration file that you want to restore.

4

Click **EXPORT** to export the previously backed-up configuration file.

When you export a file, there is a prompt to save the file in local PC with default filename as *config.cfg*.

END OF STEPS

8.14 Upgrading firmware

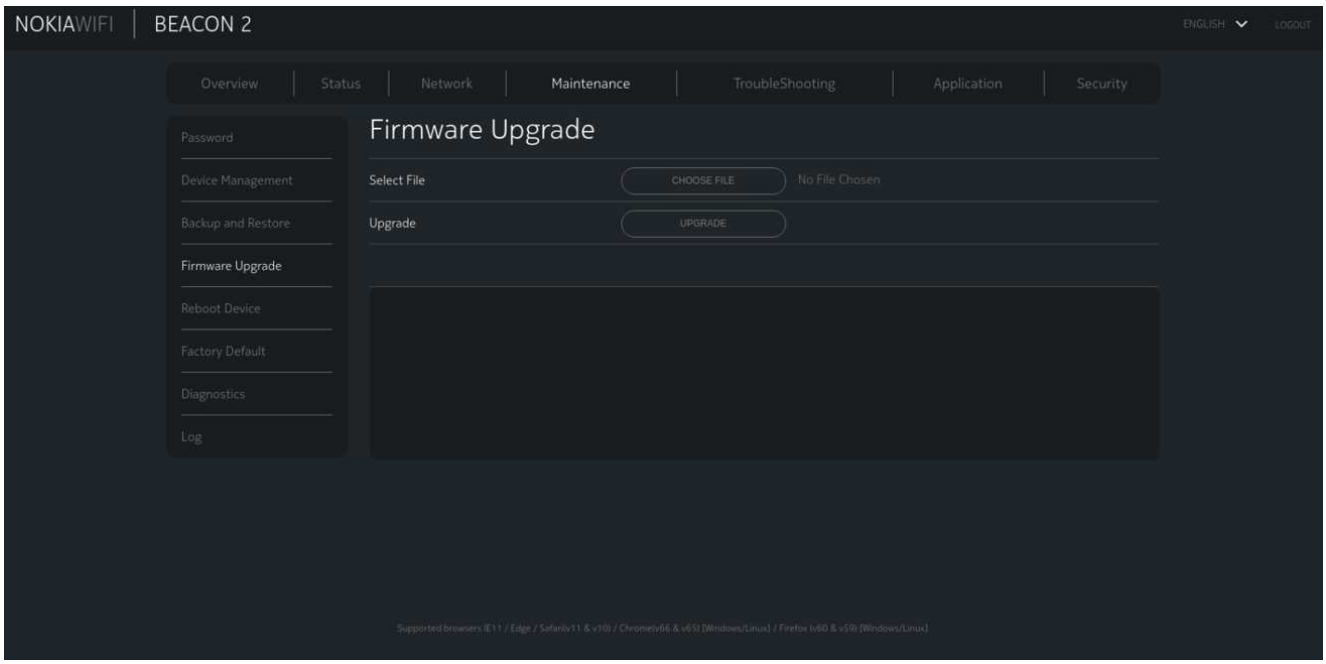
1

Click **Maintenance** in the menu bar.

2

Click **Firmware Upgrade** in the left pane. The Firmware Upgrade page displays.

Figure 8-11 Firmware Upgrade page



3

Click **CHOOSE FILE** to select the file for firmware upgrade.

4

Click **UPGRADE** to upgrade the firmware.

END OF STEPS

8.15 Rebooting the device

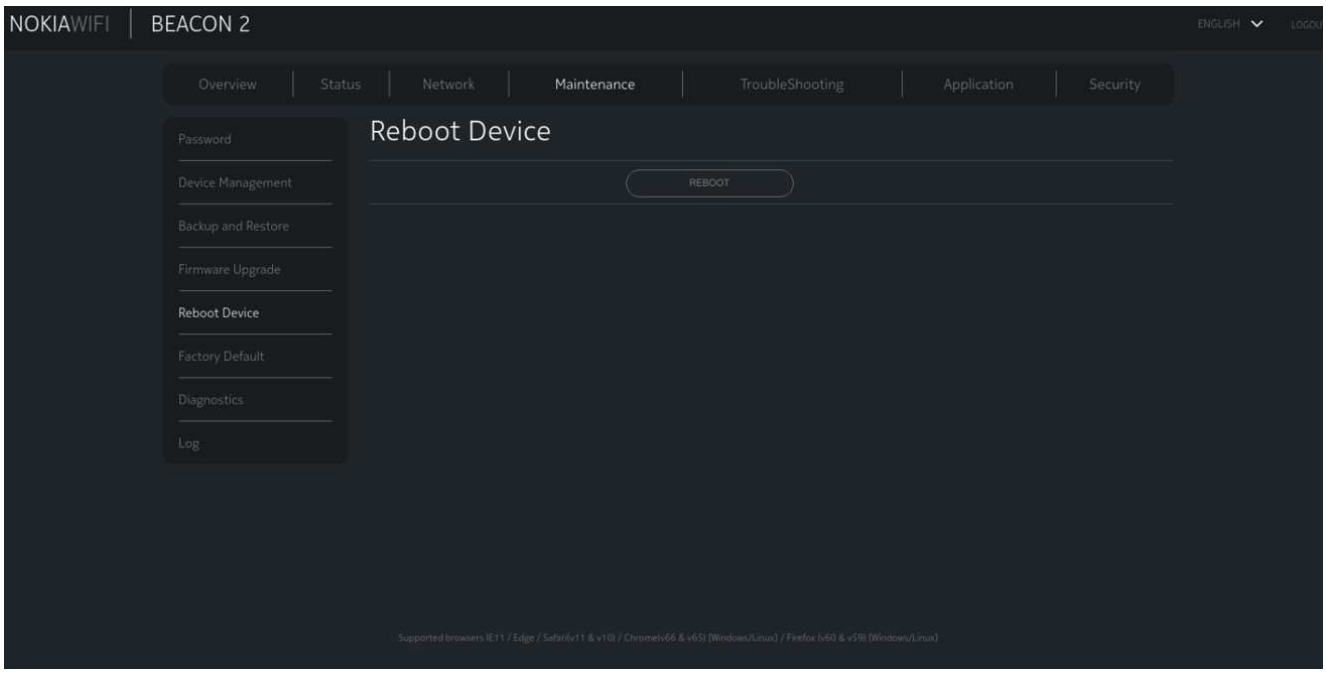
1

Click **Maintenance** in the menu bar.

2

Click **Reboot Device** in the left pane. The Reboot Device page displays.

Figure 8-12 Reboot Device page



3

Click **REBOOT** to reboot the device.

END OF STEPS

8.16 Resetting to factory defaults

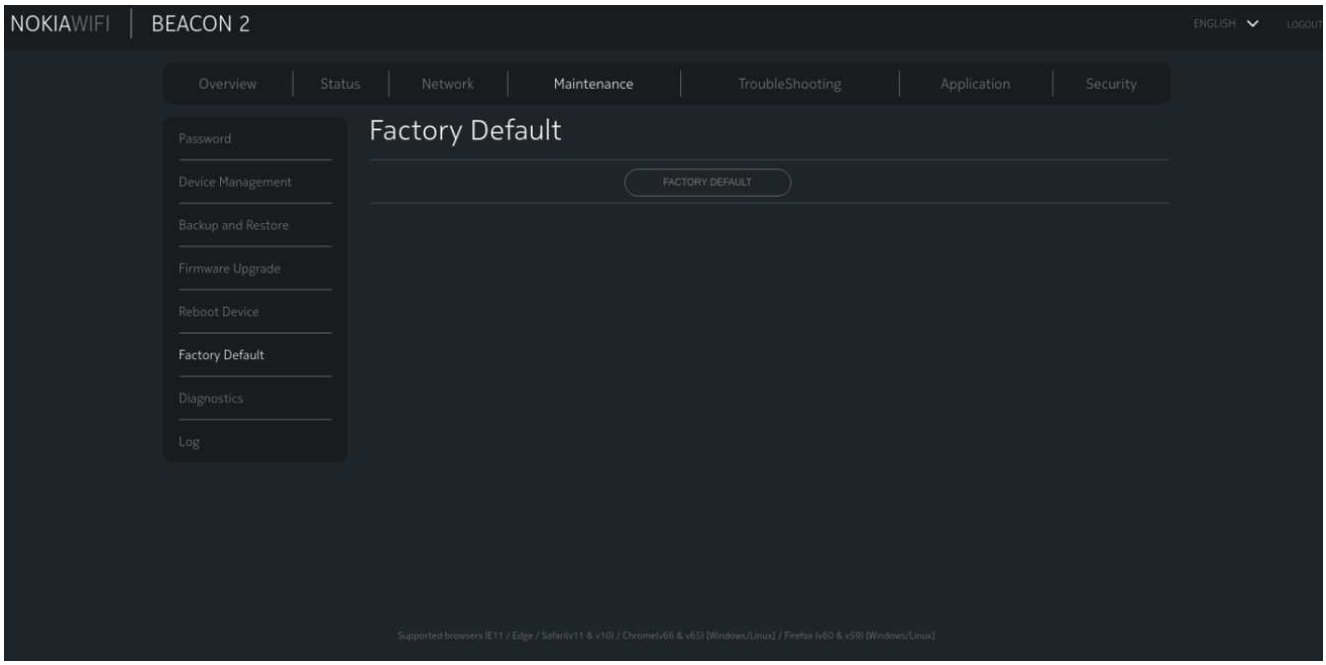
1

Click **Maintenance** in the menu bar.

2

Click **Factory Default** in the left pane. The Factory Default page displays.

Figure 8-13 Factory Default page



3

Click **FACTORY DEFAULT** to reset the configuration to factory default settings.

END OF STEPS

8.17 Diagnosing WAN connections

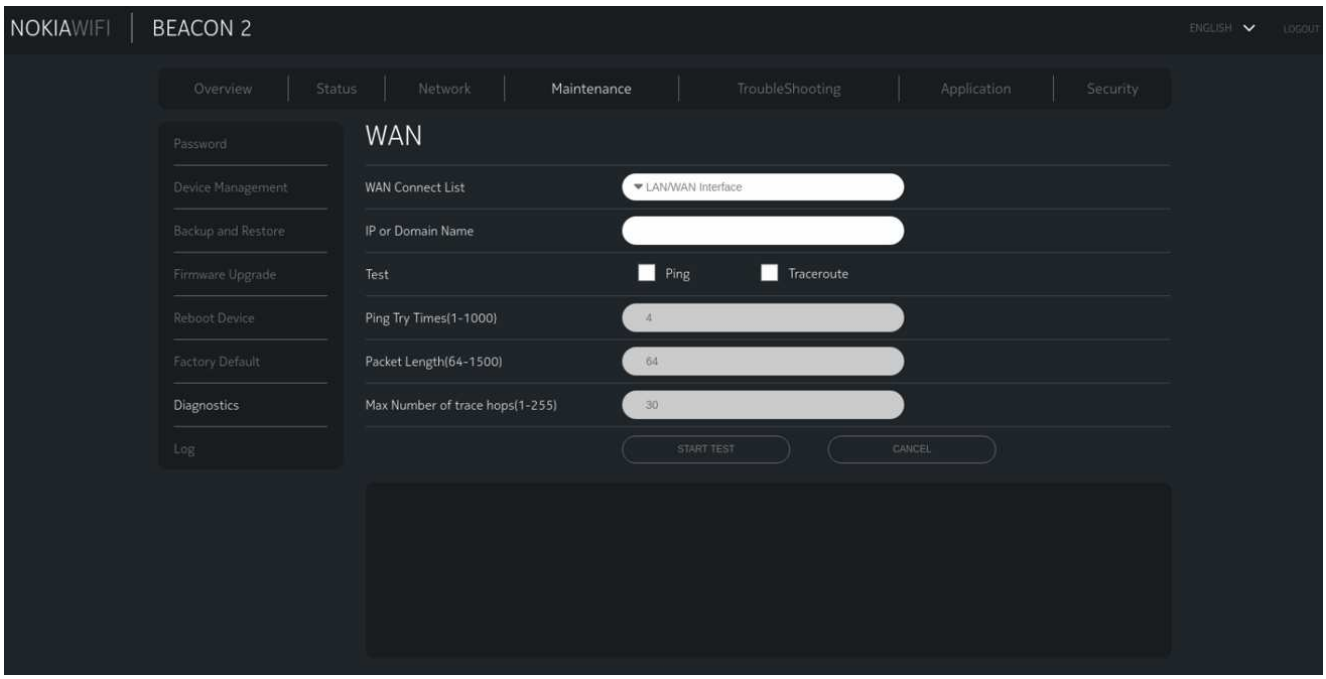
1

Click **Maintenance** in the menu bar.

2

Click **Diagnostics** in the left pane. The Diagnostics page displays.

Figure 8-14 Diagnostics page



3

Configure the following parameters.

Table 8-8 Diagnostics parameters

Field	Description
WAN Connection List	Choose a WAN connection to diagnose from the drop-down menu.
IP or Domain Name	Enter the IP address or domain name.
Test	Select the test type: ping, traceroute, or both.
Ping Try Times (1 ~ 1000)	Enter the number of ping attempts to perform (1 - 1000); the default is 4.
Packet Length (64 ~ 1500)	Enter a ping packet length (64-1024); the default is 64.
Max no of trace hops (1 ~ 255)	Enter the maximum number of trace hops (1-255); the default is 30.

4

Click **Start Test**. Results will be displayed at the bottom of the window.

Click **Cancel** to cancel the test.

END OF STEPS

8.18 Viewing log files

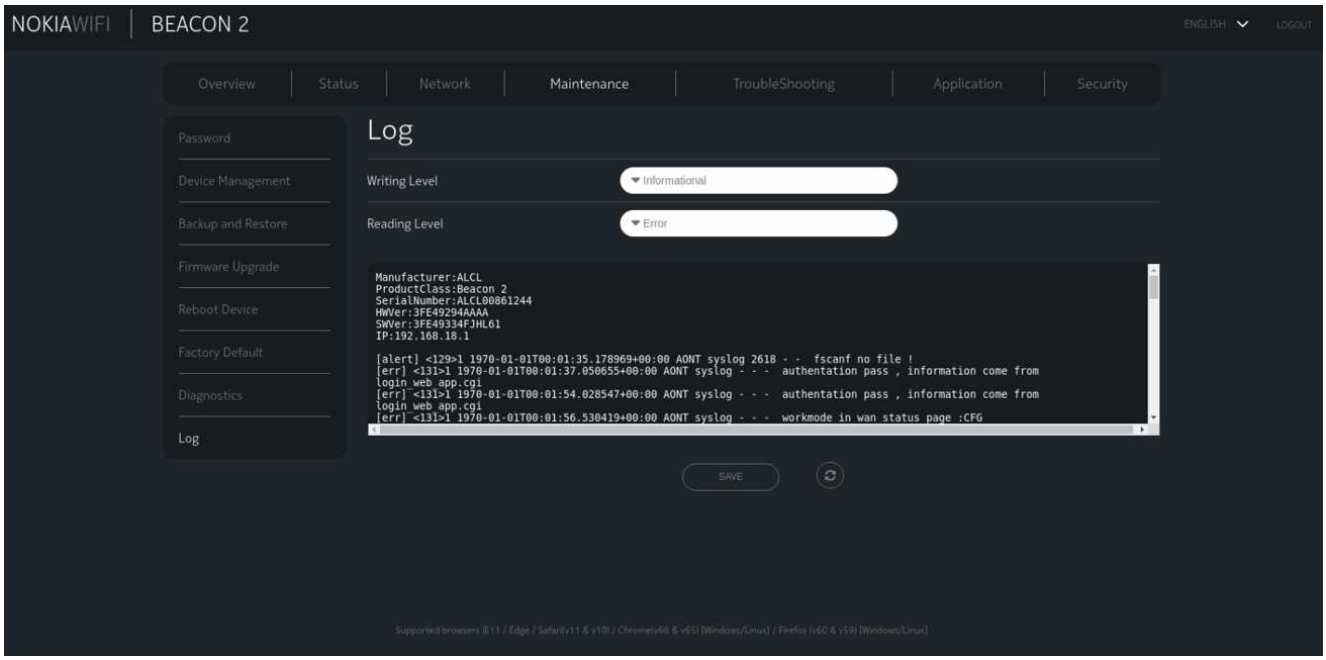
1

Click **Maintenance** in the menu bar.

2

Click **Log** from the left pane. The Log page displays.

Figure 8-15 Log page



3

Configure the following parameters:

Table 8-9 Log parameters

Field	Description
Writing Level	Choose a write level from the drop-down menu to determine which types of events are recorded in the log file: • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debug
Reading Level	Choose a read level from the drop-down menu to determine which types of events are recorded in the log file: • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debug

The log file is displayed at the bottom of the window.

4

Click **Save** to save the log file.

You can click the **Refresh** icon to update displayed information.

END OF STEPS

Configuring Security

8.19 Overview

8.19.1 Purpose

The Beacon 2 supports security configuration tasks using the WEB based GUI.

8.19.2 Contents

8.19 Overview	78
8.20 Configuring firewall	78
8.21 Configuring MAC filter	79
8.22 Configuring IP filter	81
8.23 Configuring DMZ and ALG	83
8.24 Configuring Access control	84

8.20 Configuring firewall

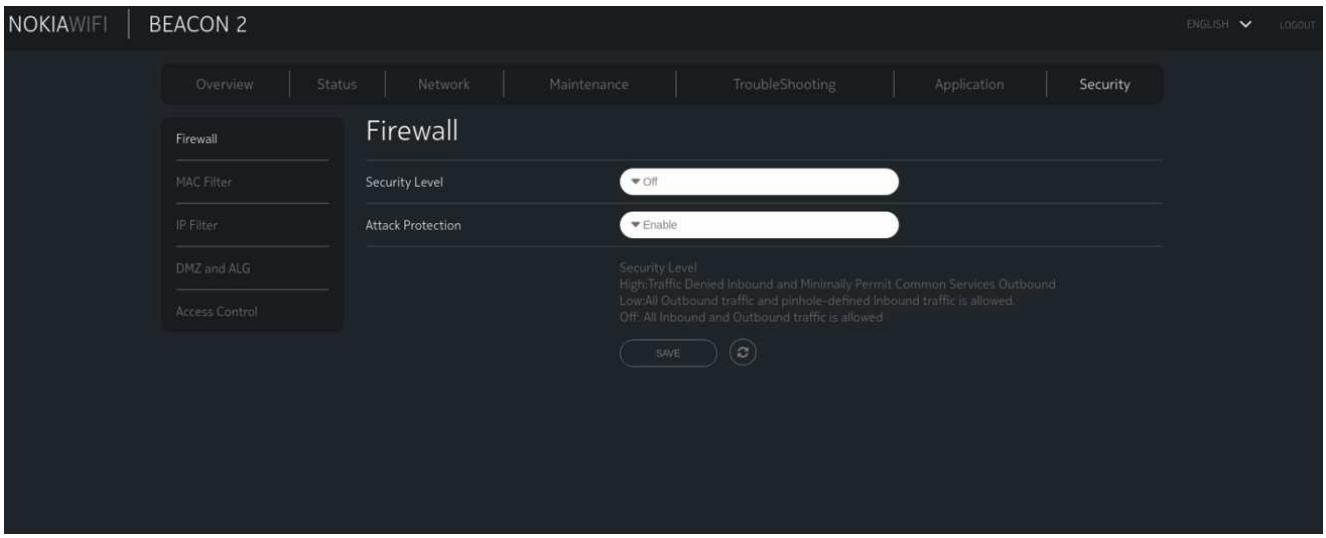
1

Click **Security** in the menu bar.

2

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

Figure 8-16 Firewall page



3

Configure the following parameters:

Table 8-10 Firewall parameters

Field	Description
Security Level	Select the security level from the list: • **Off**: No firewall security is in effect. • **Low**: 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, TR-069, and VoIP. 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. • **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.
Attack Protection (Protection against DoS or DDoS attacks)	Select an option to enable or disable attack protection from the list. The default is **Disable**.

4

Click **SAVE**.

You can click the **Refresh** icon to update displayed information.

END OF STEPS

8.21 Configuring MAC filter

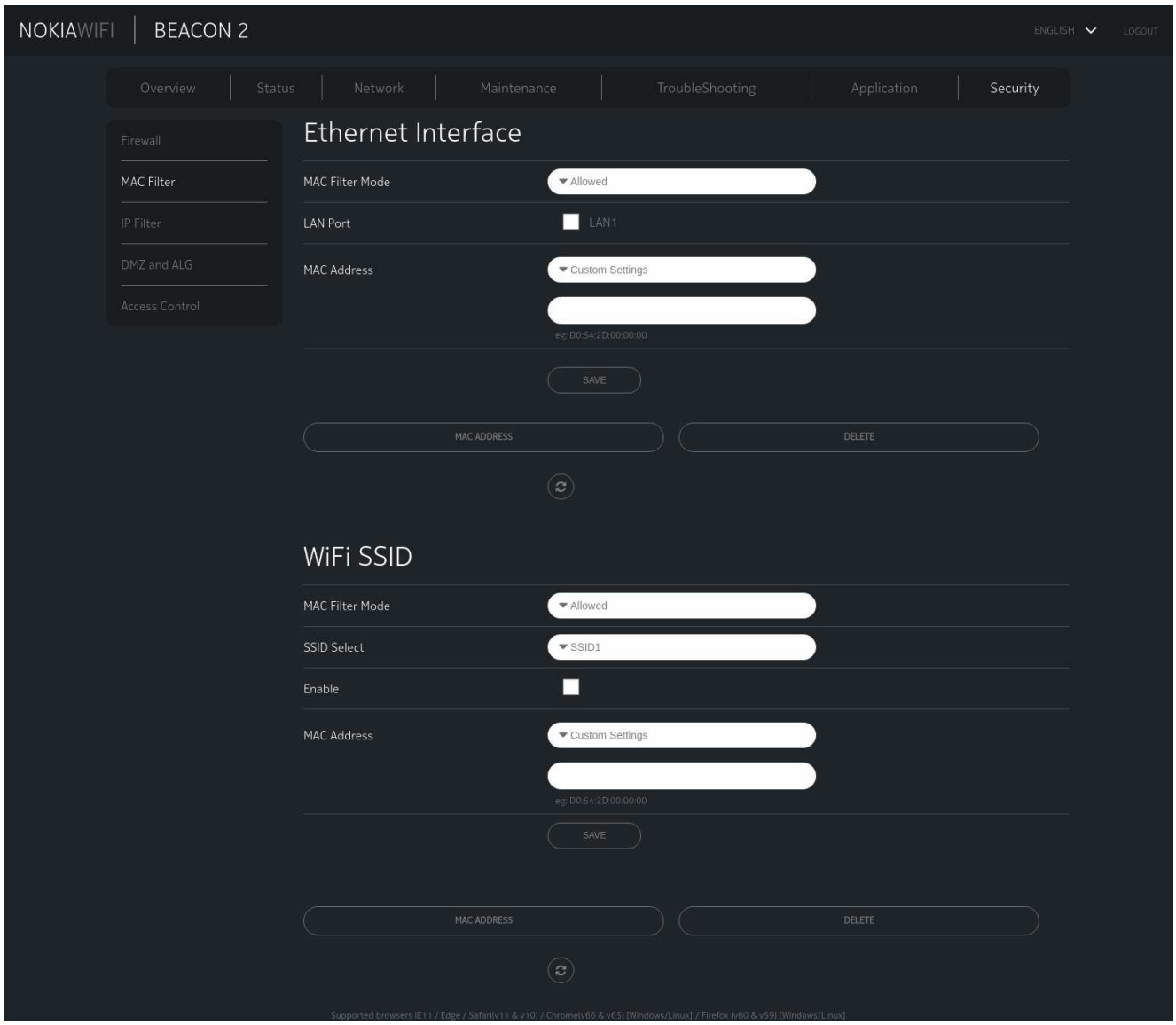
1

Click **Security** in the menu bar.

2

Click **MAC Filter** from the left pane. The MAC Filter page displays.

Figure 8-17 MAC filter page



3

Configure the following parameters.

Table 8-11 MAC filter parameters

Field	Description
Ethernet Interface	

Table 8-11 MAC filter parameters (continued)

Field	Description
Mac Filter Mode	Choose the MAC filter mode from this drop-down menu: Blocked or Allowed.
LAN Port	Select the desired LAN ports.
Mac Address	Select a MAC address from the drop-down menu or enter the address in the text field.
WiFi SSID	
Mac Filter Mode	Choose the MAC filter mode from this drop-down menu: Blocked or Allowed.
SSID select	Select the desired SSID.
Enable	Select this checkbox to enable the WiFi SSID.
Mac Address	Select a MAC address from the drop-down menu or enter the address in the text field.

4

Click **Save**.

You can also use this panel to **Delete** a MAC address.

You can click the **Refresh** icon to update displayed information.

END OF STEPS

8.22 Configuring IP filter

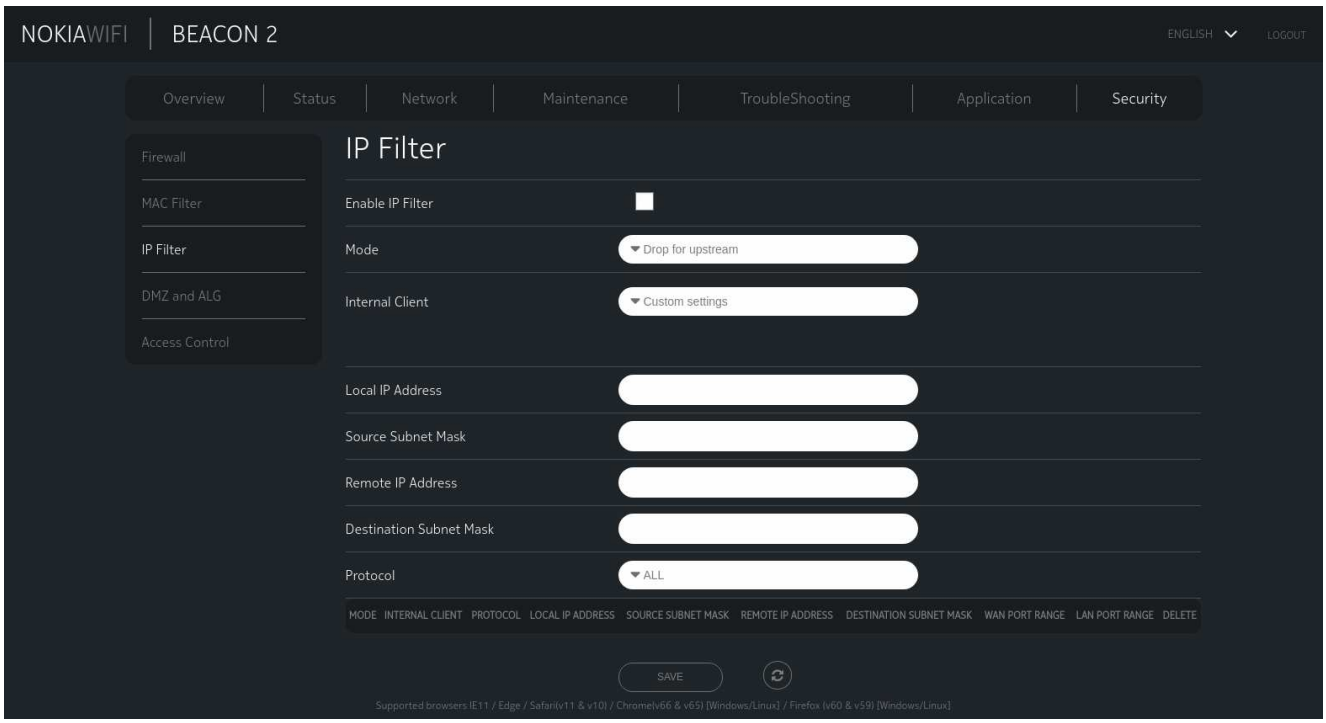
1

Click **Security** in the menu bar.

2

Click **IP Filter** from the left pane. The IP Filter page displays.

Figure 8-18 IP Filter page



3

Configure the following parameters.

Table 8-12 IP filter parameters

Field	Description
Enable IP Filter	Select this checkbox to enable an IP filter.
Mode	Choose an IP filter mode from the drop-down menu: • Drop for upstream • Drop for downstream. • Accept for upstream/downstream.
Internal Client	Choose an internal client from the drop-down menu: • Customer setting - uses the IP address input below. • IP - uses the connecting devices' IP to the ONT.
Local IP Address	Local IP address.
Source Subnet Mask	Source subnet mask.
Remote IP Address	Remote IP address.

Table 8-12 IP filter parameters (continued)

Field	Description
Destination Subnet Mask	Destination subnet Mask.
Protocol	Choose an application protocol or all from the drop-down menu.

4

Click **Save**.

You can click the **Refresh** icon to update displayed information.

You can click **Delete** to delete a Mode, Internal Client, Protocol, Local IP Address, Local Subnet Mask, Remote IP Address, Remote Subnet Mask, Destination Subnet Mask, WAN Port Range and LAN Port Range.

End of steps

8.23 Configuring DMZ and ALG

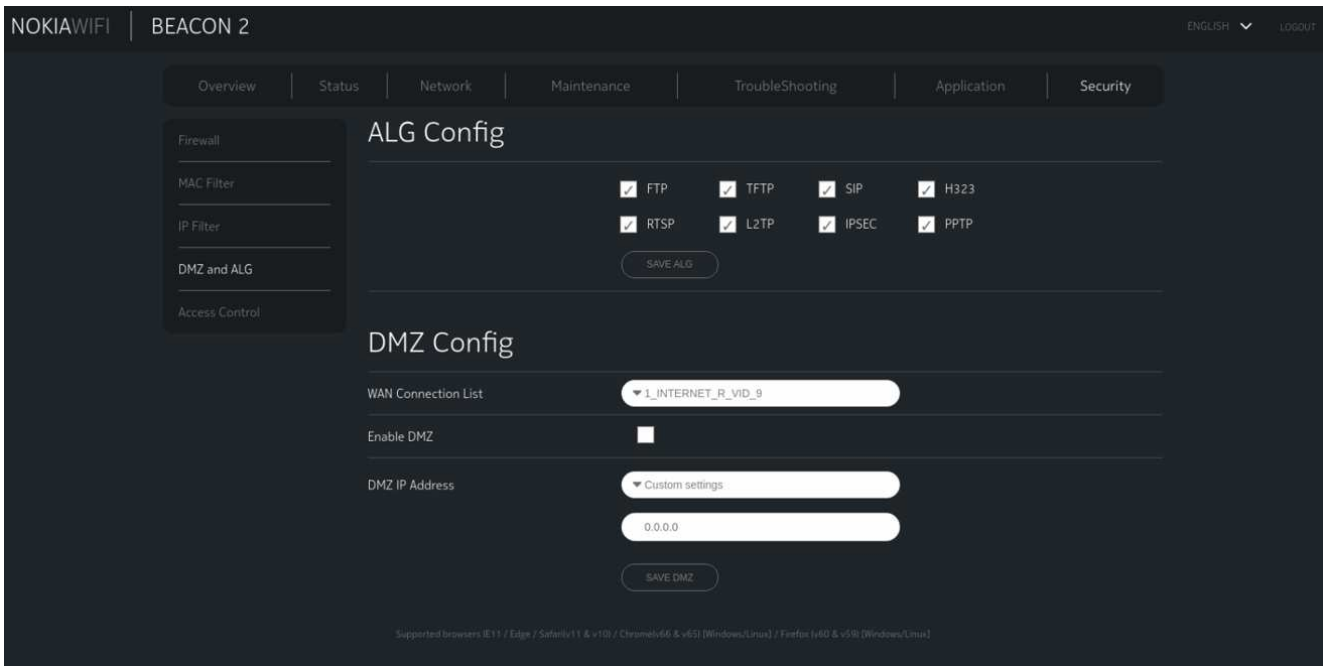
1

Click **Security** in the menu bar.

2

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

Figure 8-19 ALG Config and DMZ Config page



3

Configure the following parameters:

Table 8-13 ALG parameters

Field	Description
ALG Config	Select the checkboxes to enable the protocols to be supported: • FTP • TFTP • SIP • H323 • RTSP • L2TP • IPSEC • PPTP

4

Click **SAVE ALG**.

5

Configure the following parameters:

Table 8-14 DMZ parameters

Field	Description
WAN Connection List	Select a WAN connection from the list.
Enable DMZ	Select this checkbox to enable DMZ on the selected 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.

6

Click **SAVE DMZ**.

END OF STEPS

8.24 Configuring Access control

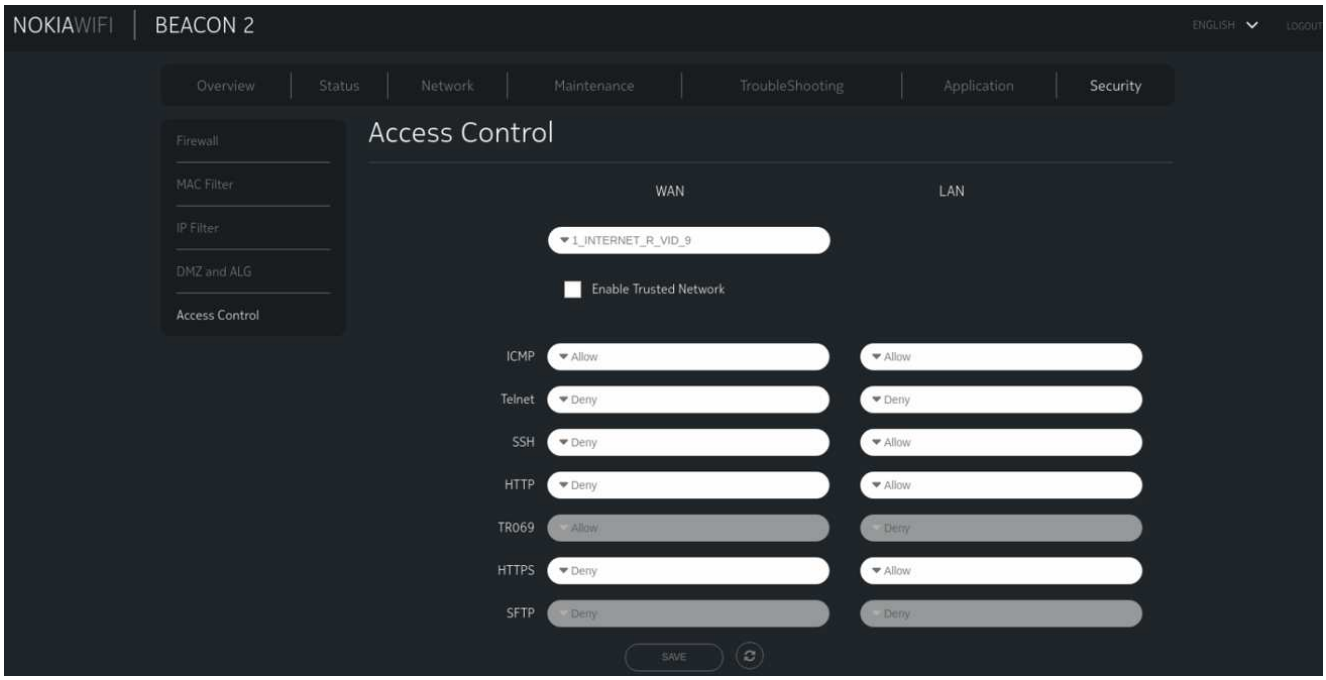
1

Click **Security** in the menu bar.

2

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

Figure 8-20 Access control page



3

Configure the following parameters:

Table 8-15 Access control parameters

Field	Description
Enable Trusted Network	Select this checkbox to choose the trusted network.
ICMP, Telnet, SSH, HTTP, TR069, HTTPS, SFTP	Select an access control level for each protocol: WAN side: Allow, Deny, or Trusted Network Only. LAN side: Allow or Deny.
Trusted Network	
Source IP Start	Enter a start IP address for the new subnet trusted network.
Source IP End	Enter an end IP address for the new subnet trusted network.

4

Click **Save**.

You can click the **Refresh** icon to update displayed information.

End of steps

Configuring the network

8.25 Overview

8.25.1 Purpose

This chapter describes the network configuration tasks supported by the Beacon 2.

8.25.2 Contents

8.25 Overview	87
8.26 Configuring LAN	87
8.27 Configuring LAN IPv6	89
8.28 Configuring WAN	91
8.29 Configuring WAN DHCP	93
8.30 Configuring Wireless (2.4GHz)	95
8.31 Configuring Wireless (5 GHz)	98
8.32 Configuring IP Routing	101
8.33 Configuring DNS	103
8.34 Configuring TR-069	104
8.35 Configuring Mesh	105

8.26 Configuring LAN

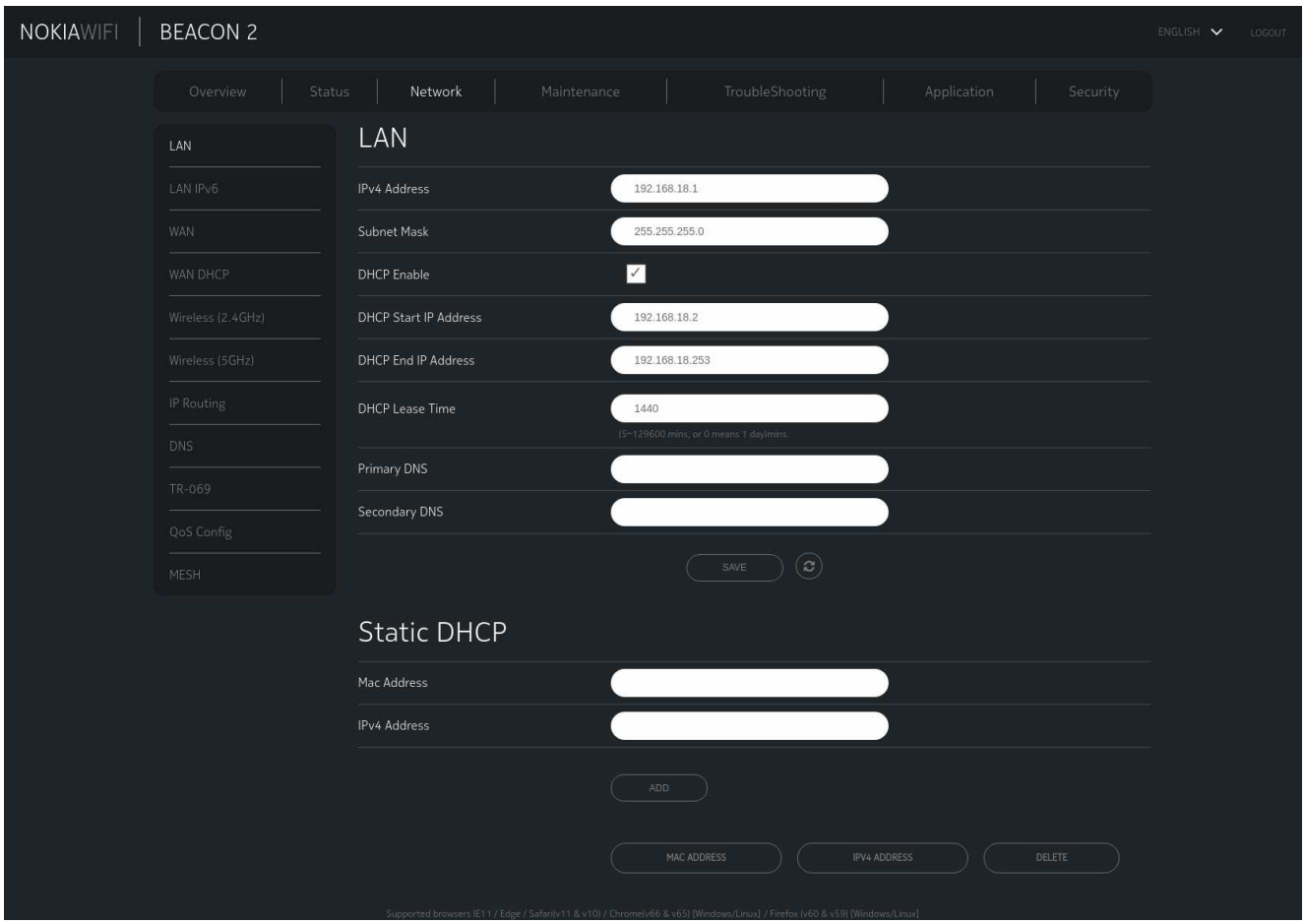
1

Click **Network** in the menu bar.

2

Click **LAN** in the left pane. The LAN page displays.

Figure 8-21 LAN page



3

Configure the following LAN parameters:

Table 8-16 LAN parameters

Field	Description
LAN	
IPv4 Address	Enter IP address of the device.
Subnet Mask	Enter the subnet mask of the device.
DHCP Enable	Select this checkbox to enable DHCP. if this checkbox is not enabled, the DHCP functionality cannot be used. There is no need to enter the DHCP IP Address, DHCP End IP Address and DHCP Lease Time if this checkbox is not enabled.

Table 8-16 LAN 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).
Primary DNS	Enter the primary domain name server address.
Secondary DNS	Enter the secondary domain name server address.
Static DHCP	
MAC Address	MAC address for the static DHCP.
IPv4 Address	IPv4 address for the static DHCP.

4

Click **ADD**.

You can click **DELETE** to delete the LAN configuration.

END OF STEPS

8.27 Configuring LAN IPv6

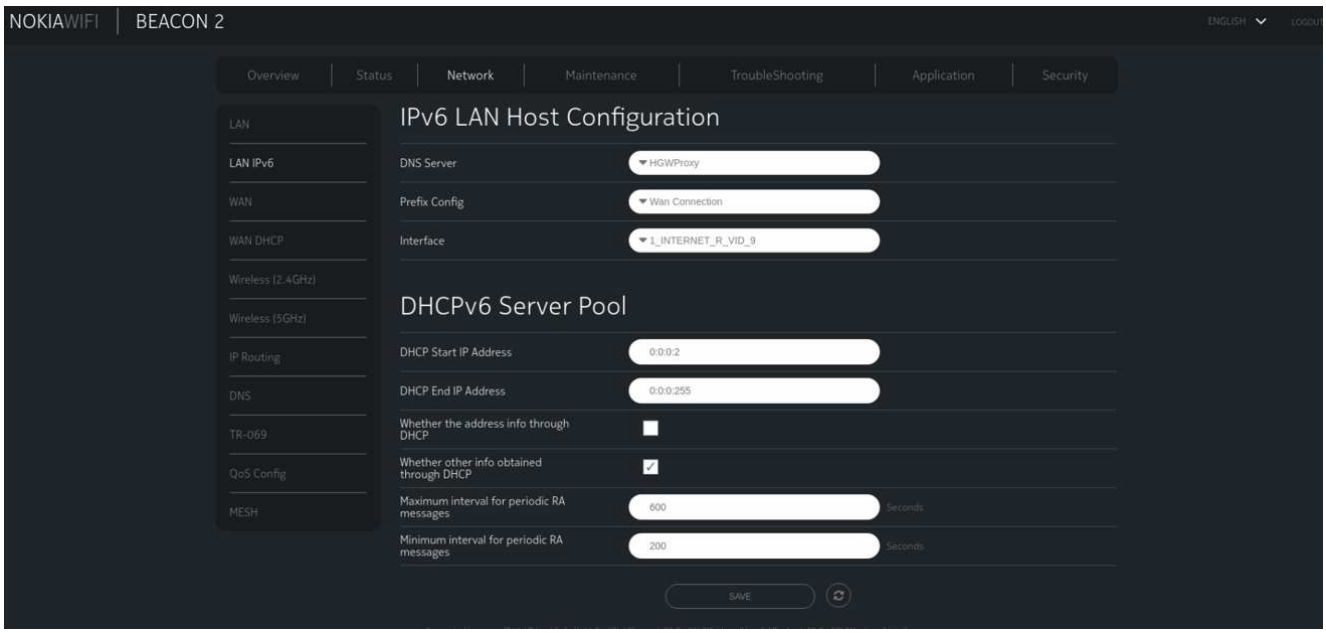
1

Click **Network** in the menu bar.

2

Click **LAN IPv6** in the left pane. The LAN IPv6 page displays.

Figure 8-22 LAN IPv6 page



3

Configure the following LAN parameters:

Table 8-17 LAN parameters

Field	Description
IPv6 LAN Host Configuration	
DNS Server	Enter IP address of the device.
Prefix Config	Enter the subnet mask of the device.
Interface	Select this checkbox to enable DHCP. if this checkbox is not enabled, the DHCP functionality cannot be used. There is no need to enter the DHCP IP Address, DHCP End IP Address and DHCP Lease Time if this checkbox is not enabled.
DHCPv6Server Pool	
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.
Whether the address info through DHCP	Select this checkbox if address information is obtained.
Whether the other info obtained through DHCP	Select this checkbox if other information is obtained through DHCP.

Table 8-17 LAN parameters (continued)

Field	Description
Maximum interval for periodic RA messages	Enter the primary domain name server address.
Minimum interval for periodic RA messages	Enter the secondary domain name server address.

4

Click **SAVE**.

You can click the **Refresh** icon to update displayed information.

End of steps

8.28 Configuring WAN

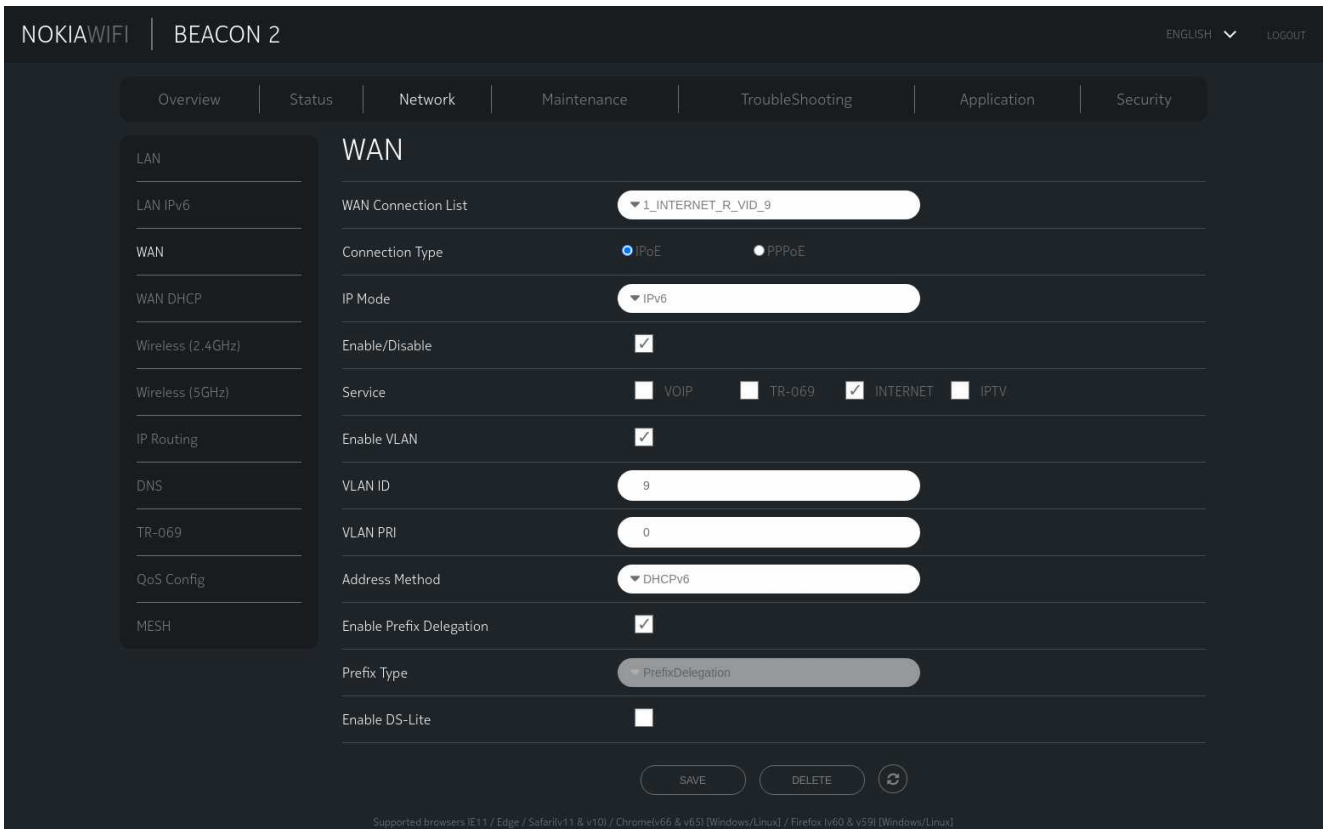
1

Click **Network** in the menu bar.

2

Click **WAN** in the left pane. The WAN page displays.

Figure 8-23 WAN page



3

Configure the following parameters.

Table 8-18 WAN parameters

Field	Description
WAN Connection List	Select WAN connection from the list to set the connection parameters.
Connection Type	Select a connection type: • **IPoE** • **PPPoE**
IP Mode	Select this checkbox for required IP mode.
Enable/Disable	Select this checkbox to enable the WAN connection.
Service	Select the checkboxes to enable service types for this connection.
Enable VLAN	Select this checkbox to enable VLAN.

Table 8-18 WAN parameters (continued)

Field	Description
VLAN ID	Enter the VLAN ID The allowed range is 2 to 4094.
WAN IP Mode	Indicates whether the IP mode is IPoe or PPPoe.
VLAN PRI	Enter the VLAN PRI. VLAN priority allows to assign a priority to outbound packets containing the specified VLAN-ID. The range is 0 to 7.
Address Method	Select this checkbox for required address method.
Enable Prefix Delegation	Select this checkbox to enable prefix delegation.
Prefix Type	Select this checkbox for required prefix type.
Enable DS-Lite	Select this checkbox to enable DS-Lite.

4

Click **SAVE** to save the WAN configuration.

You can:

- Click **DELETE** to delete the WAN configuration.
- You can click the **Refresh** icon to update displayed information.

END OF STEPS

8.29 Configuring WAN DHCP

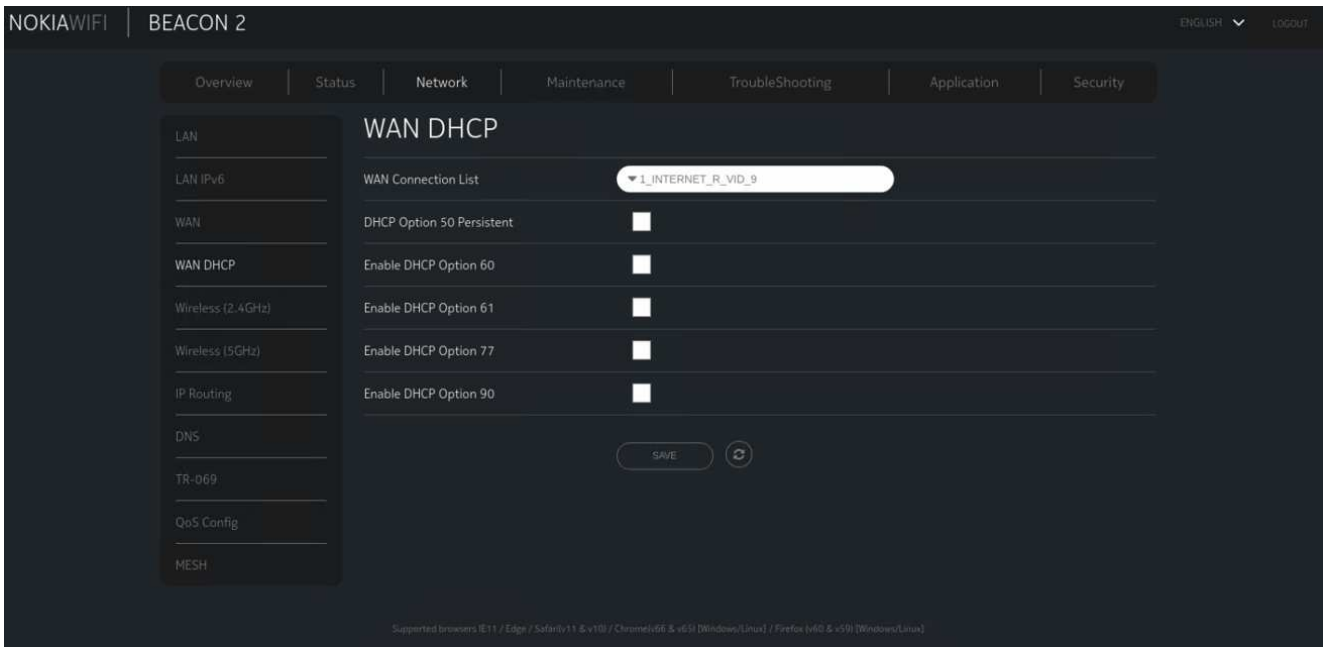
1

Click **Network** in the menu bar.

2

Click **WAN DHCP** in the left pane. The WAN DHCP page displays.

Figure 8-24 WAN DHCP page



3

Configure the following parameters:

Table 8-19 WAN DHCP parameters

Field	Description
WAN Connection List	Select a WAN connection from the list.
DHCP Option 50 persistent	Select this checkbox to enable DHCP Option 50.
Enable DHCP Option 60	Select this checkbox to enable DHCP Option 60 (vendor class identifier).
Enable DHCP Option 61	Select this checkbox to enable DHCP Option 61.
Enable DHCP Option 77	Select this checkbox to enable DHCP Option 77.
Enable DHCP Option 90	Select this checkbox to enable DHCP Option 90.

4

Click **SAVE**.

You can click the **Refresh** icon to update displayed information.

END OF STEPS

8.30 Configuring Wireless (2.4GHz)

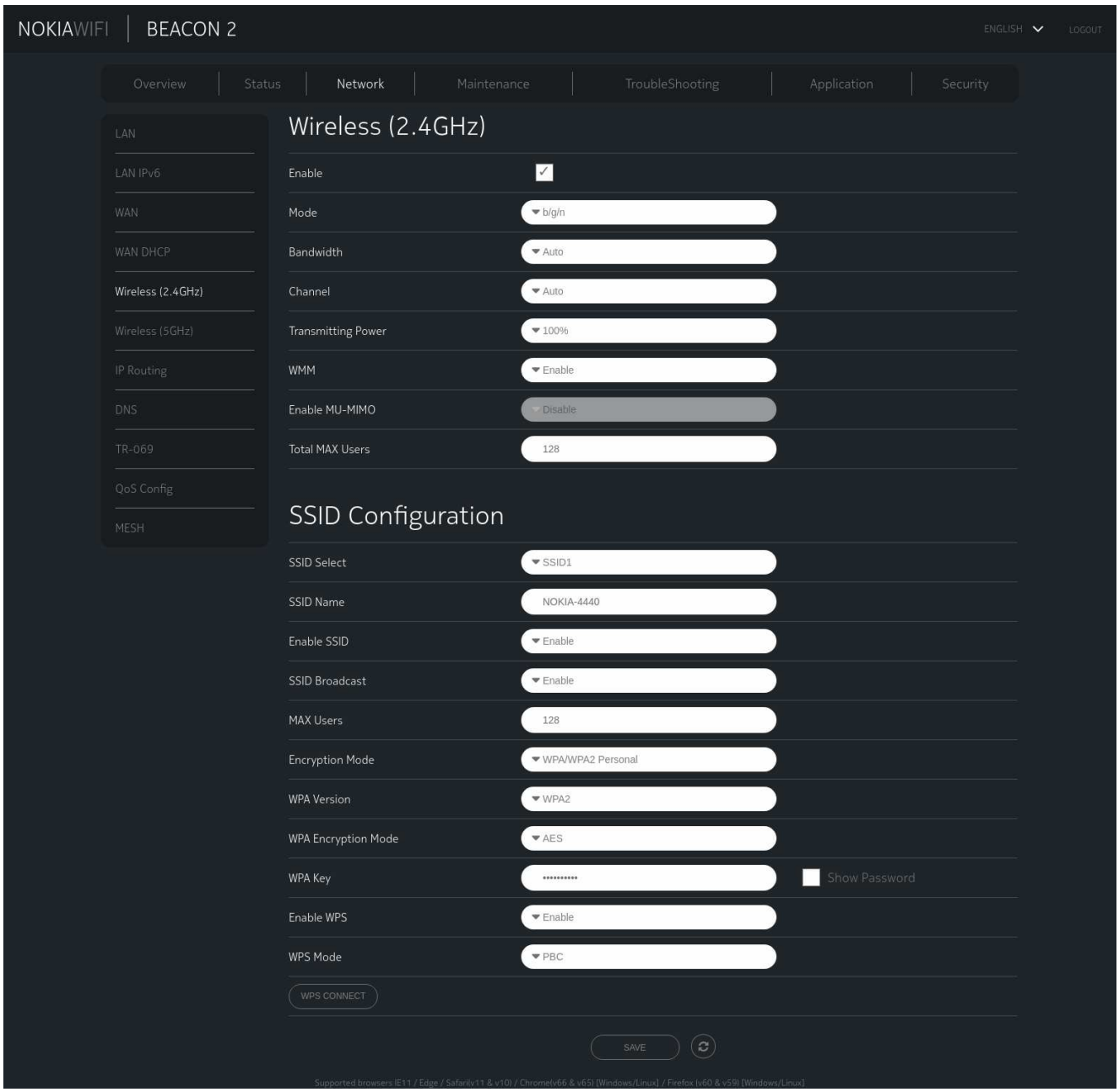
1

Click **Network** in the menu bar.

2

Click **Wireless (2.4 GHz)** in the left pane. The Wireless (2.4 GHz) page displays.

Figure 8-25 Wireless (2.4 GHz) page



3

Configure the following parameters:

Table 8-20 Wireless (2.4GHz) parameters

Field	Description
Wireless (2.4GHz)	
Enable	Select this checkbox to enable Wi-Fi.
Mode	Select a Wi-Fi mode from the list: • **auto (b/g/n/ax)** • **b** • **g** • **b/g** • **n/g** • **ax/g**
Bandwidth	Select **20 MHz** or **40 MHz** from the list.
Channel	Select a channel from the list or select Auto to auto-assign.
Transmitting Power	Select the percentage transmitting power from the list.
WMM	Select this checkbox to enable or disable wireless multimedia.
Enable MU-MMC	Select this checkbox to enable or disable MU-MMC. 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.
Total MAX Users	Enter the maximum numbers of users.
SSID Configuration	
SSID Select	Select the SSID from the list. When SSID 2, 3, 4, 6, 7, or 8 is selected, the Guest Mode option is available. When an 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.
SSID Name	Enter the SSID name.
Enable SSID	Select an option to enable or disable SSID from this list.
SSID Broadcast	Select an option to enable or disable SSID broadcast from this list.
MAX Users	Enter the maximum number of MAX users. This field refers to the maximum number of WiFi connections that are allowed. The maximum users allowed are 128.
Encryption Mode	Select an encryption mode from the list: • **WPA/WPA2 Personal** • **WPA/WPA2 Enterprise** • **WPA3 Personal** • **WEPEncryption** • **Open/none** • **WPA2/WPA3 Personal**

Table 8-20 Wireless (2.4GHz) parameters (continued)

Field	Description
WPA Version	Select a WPA version from the list: • **WPA1** • **WPA2** • **WPA1/WPA2**
WPA Encryption Mode	Select a WPA encryption mode from the list: • **TKIP** • **AES** • **TKIP/AES**
WPA Key	Enter the WPA key.
Enable WPS	Enable or disable WPS from this list
WPS Mode	Select a WPS mode from the list: • **PBC** (Push Button Connect) • **PIN AP** (Personal Identification Number) generated by the AP (Access Point) • **PIN STA** (Personal Identification Number) generated by the Wi-Fi client (STA)

4

If you have enabled and configured WPS, click **WPS CONNECT**.

Result: The *WPS success* message displays near the **WPS CONNECT** button.

5

Click **SAVE**.

You can click the **Refresh** icon to update displayed information.

END OF STEPS

8.31 Configuring Wireless (5 GHz)

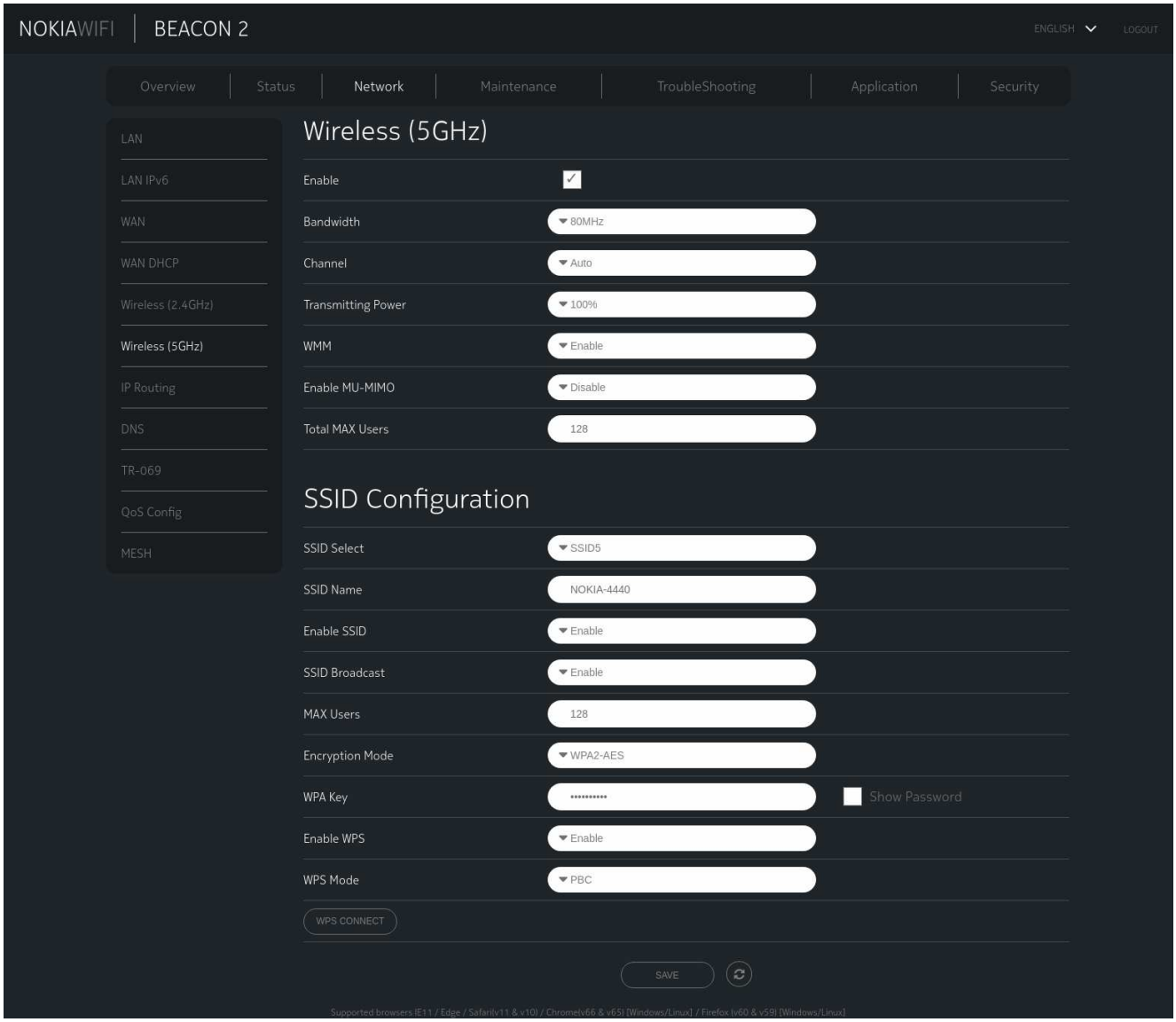
1

Click **Network** in the menu bar.

2

Click **Wireless (5 GHz)** in the left pane. The Wireless (5GHz) page displays.

Figure 8-26 Wireless (5GHz)



3

Configure the following parameters:

Table 8-21 Wireless (5GHz) parameters

Field	Description
Wireless (5GHz)	

Table 8-21 Wireless (5GHz) parameters (continued)

Field	Description
Enable	Select this checkbox to enable WiFi.
Bandwidth	Select from: • **20 MHz** • **40 MHz** • **80 MHz**
Channel	Select a channel from the list or select **Auto** to have the channel automatically assigned.
Transmitting Power	Select a percentage for the transmitting power from the list: • Low (20%) • Medium (40%) • High (60%) • Maximum (100%)
WMM	Select this checkbox to enable or disable wireless multimedia.
Total MAX Users	Enter the total number of MAX users. The maximum users allowed is 128.
Enable MU-MMO	Select **Enable** or **Disable** from the list. 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.
SSID Configuration	
SSID Select	Select the SSID from the list. When SSID 2, 3, 4, 6, 7, or 8 is selected, the Guest Mode option is available. 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.
SSID Name	Change the name of the selected SSID.
Enable SSID	Select **Enable** or **Disable** from this list.
SSID Broadcast	Select **Enable** or **Disable** from this list.
Users MAX	Enter the maximum number of MAX users.
Encryption Mode	Select an encryption mode from the list: • **OPEN** • **WPA/WPA2 Personal** • **WPA/WPA2 Enterprise** [1 2]
WPA Key	Enter the WPA key.
Enable WPS	Select Enable or disable WPS from this list.
WPS Mode	Select the required WPS mode.

Notes:

1. When Encryption Mode is set to “WPA/WPA2 Enterprise”, the following options are no longer available: WPA encryption mode, WPA key, Enable WPS, WPS mode.

2. When Encryption Mode is set to “WPA/WPA2 Enterprise”, the following options become available: Primary RADIUS server, port and password; Secondary RADIUS server, port, and password; RADIUS accounting port.

4

If you have enabled and configured WPS, click **WPS CONNECT**.

Result: The *WPS success* message displays near the **WPS CONNECT** button.

5

Click **SAVE**.

You can click the **Refresh** icon to update displayed information.

END OF STEPS

8.32 Configuring IP Routing

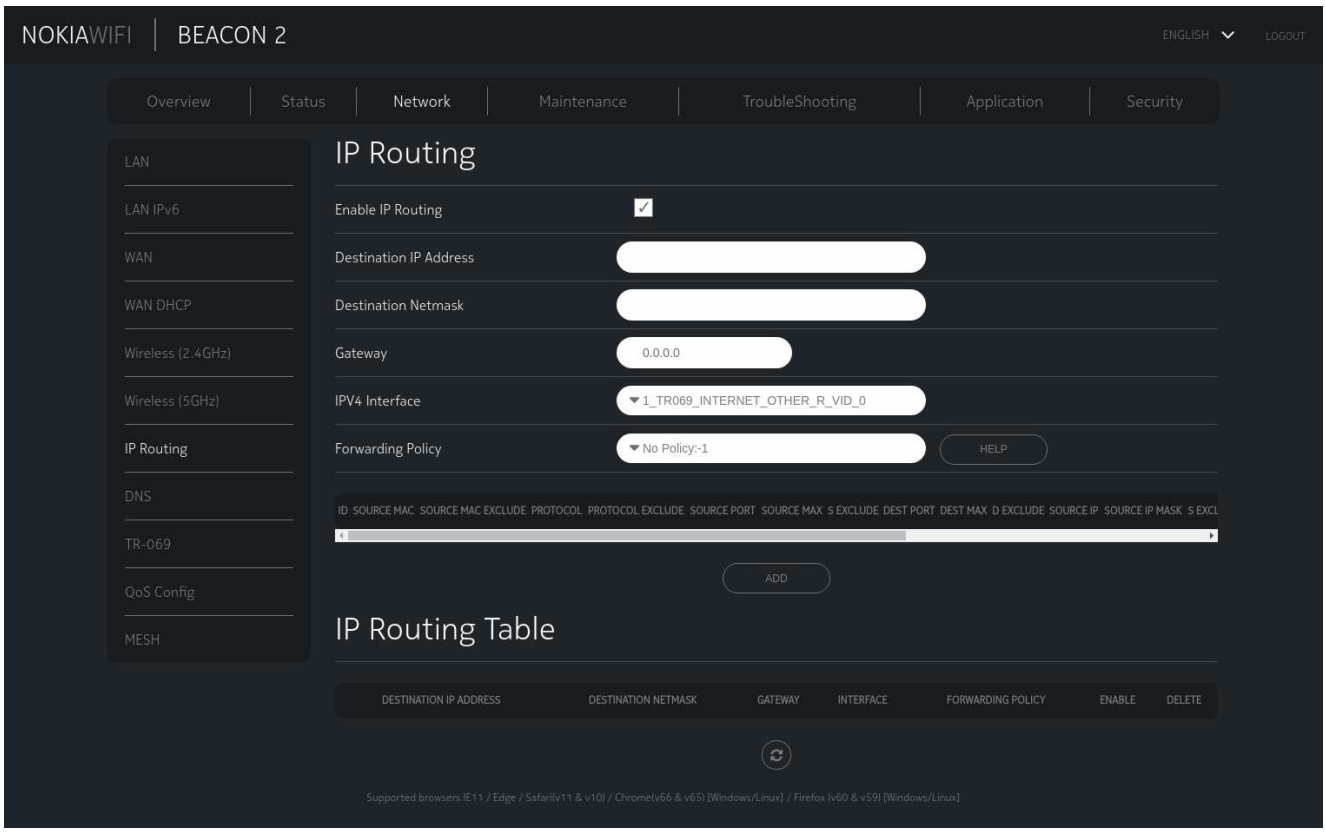
1

Click **Network** in the menu bar.

2

Click **IP Routing** in the left pane. The IP Routing page displays.

Figure 8-27 IP Routing page



3

Configure the following parameters:

Table 8-22 IP Routing parameters

Field	Description
Enable Routing	Select this checkbox to enable static routing.
Destination IP Address	Enter the destination IP address.
Destination Netmask	Enter the destination network mask.
Gateway	Enter the gateway address.
IPv4 Interface	Select a WAN connection previously created in the WAN page from the list.

4

Click **ADD**.

You can click the **Delete** icon in the IP Routing Table to delete routing information.

You can click the **Refresh** icon to update displayed information.

End of steps

8.33 Configuring DNS

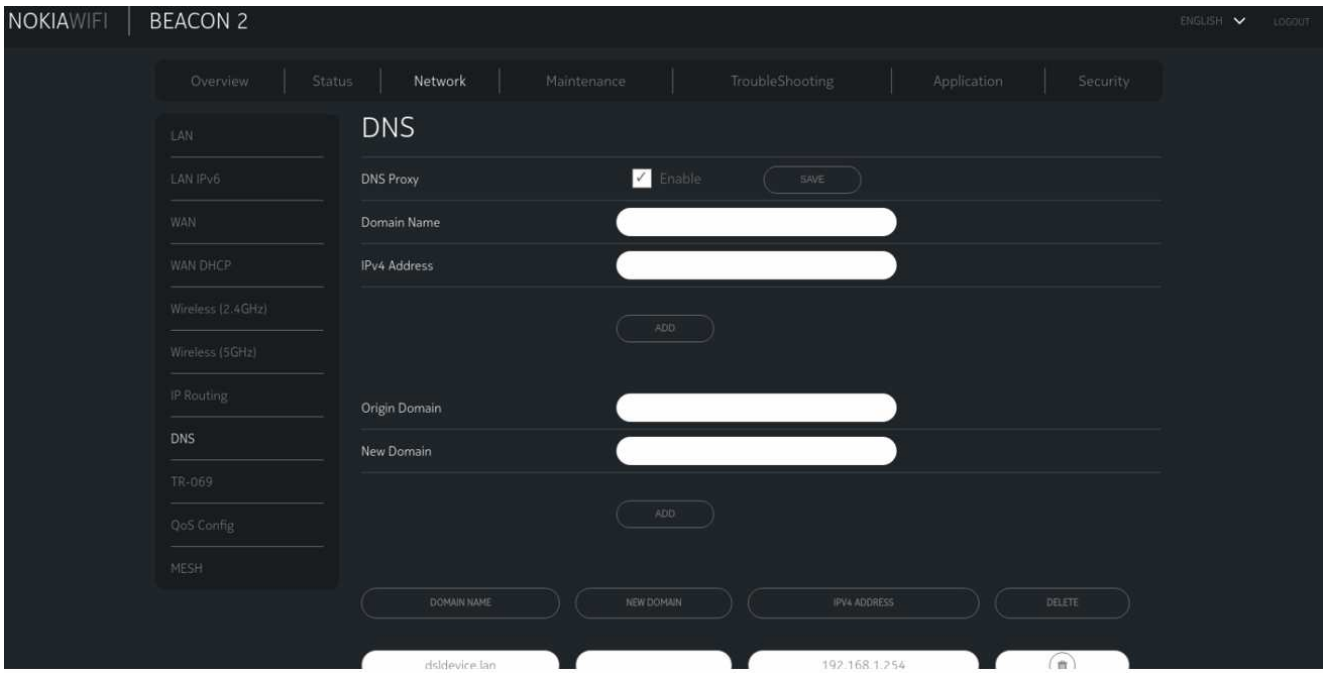
1

Click **Network** in the menu bar.

2

Click **DNS** in the left pane. The DNS page displays.

Figure 8-28 DNS page



3

Configure the following parameters:

Table 8-23 DNS parameters

Field	Description
DNS Proxy	Select this checkbox to enable DNS proxy. Click **SAVE** to save the proxy.

Table 8-23 DNS parameters (continued)

Field	Description
Domain Name IPv4 Address	Enter the domain name and domain IP address and click **ADD**.
Origin Domain New Domain	Enter the origin domain name and new domain name and click **ADD**.

4

Click **ADD** to add the particular DNS.

You can click the **Delete** icon to delete a particular domain.

END OF STEPS

8.34 Configuring TR-069

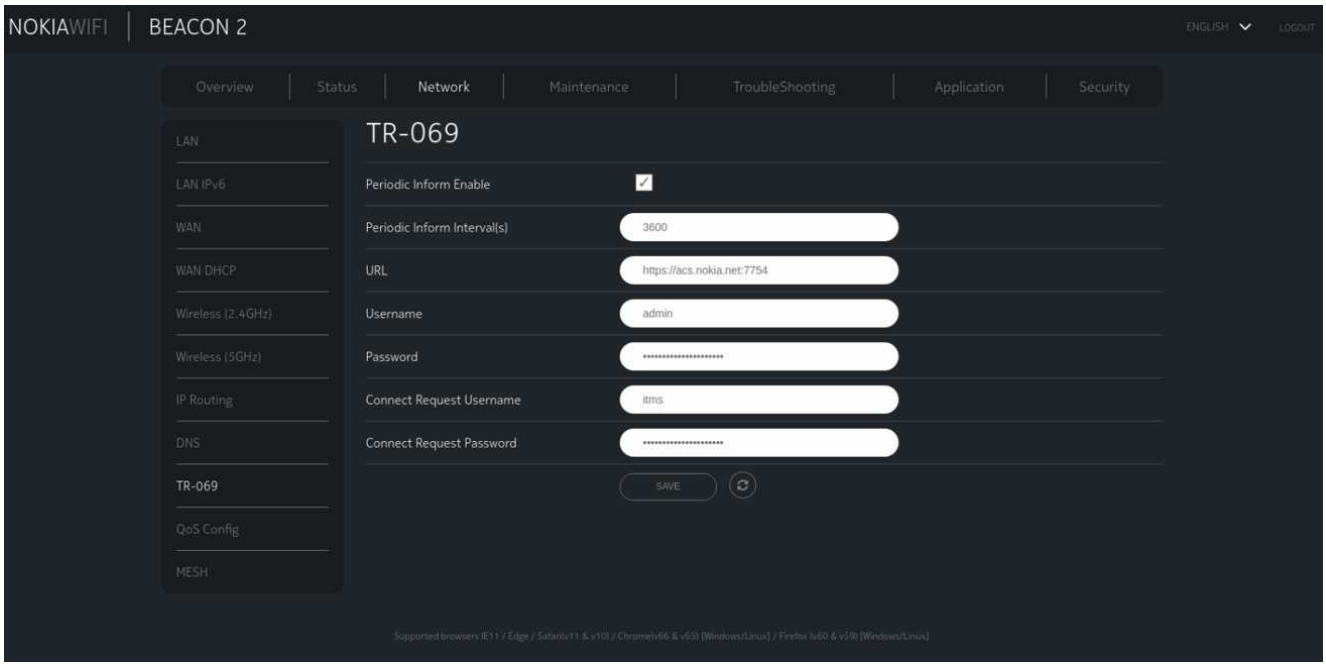
1

Click **Network** in the menu bar.

2

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

Figure 8-29 TR-069 page



3

Configure the following parameters:

Table 8-24 TR-069 network parameters

Field	Description
Periodic Inform Enable	Select this checkbox 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.
Username	Enter the username used to log in to the Beacon 2.
Password	Enter the password used to log in to the Beacon 2.
Connect Request Username	Enter the username used to log in to the auto-configuration server.
Connect Request Password	Enter the password used to log in to the auto-configuration server.

4

Click **SAVE**.

You can click the **Refresh** icon to update displayed information.

END OF STEPS

8.35 Configuring Mesh

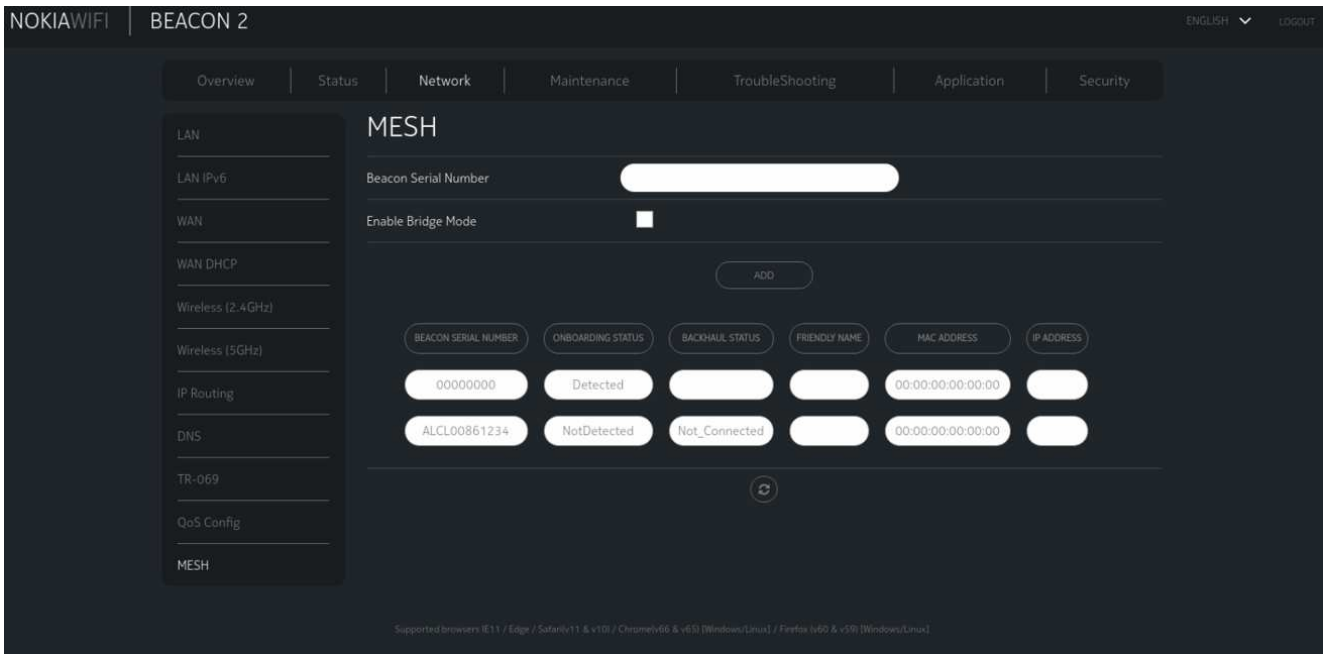
1

Click **Network** in the menu bar.

2

Click **MESH** in the left pane. The MESH page displays.

Figure 8-30 MESH page



3

Configure the following parameters:

Table 8-25 Mesh parameters

Field	Description
Beacon Serial Number	Enter the serial number of the Beacon 2 that appears on the hardware kit.
Enable Bridge Mode	Select this checkbox to enable bridge more.
Onboarding Status	Indicates whether or not the Beacon 2 associated with the serial number is onboarded to the mesh.
Backhaul Status	Indicates the status of the backhaul connection.
Friendly Name	Indicates a name determined by the user for the Beacon 2 associated with the serial number.
MAC Address	Indicates the MAC address.
IP Address	Indicates the IP address.

4

Click **ADD**.

You can click the **Refresh** icon to update displayed information.

End of steps

Configuring the application

8.36 Overview

8.36.1 Purpose

This chapter describes the application configuration tasks supported by Beacon 2.

8.36.2 Contents

8.36 Overview	108
8.37 Configuring port forwarding	108
8.38 Configuring port triggering	110
8.39 Configuring DDNS	111
8.40 Configuring NTP	113
8.41 Configuring UPNP	114

8.37 Configuring port forwarding

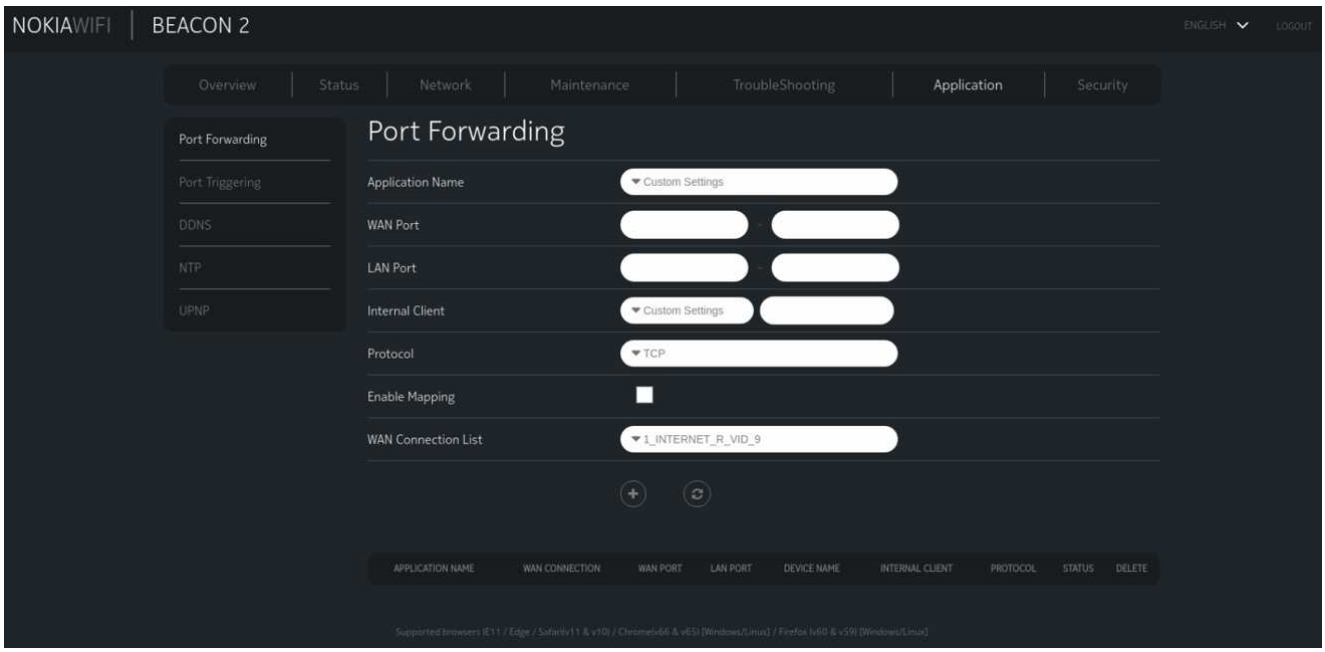
1

Click **Application** in the menu bar.

2

Click **Port Forwarding** in the left pane. The Port Forwarding page displays.

Figure 8-31 Port Forwarding page



3

Configure the following parameters:

Table 8-26 Port Forwarding parameters

Field	Description
Application Name	Select an application name from the list.
WAN Port	Enter the WAN port range. The maximum range is 32.
LAN Port	Enter the LAN port range. The maximum range is 32.
Internal Client	Select a connected device from the list and enter the associated IP address.
Protocol	Select the port forwarding protocol from the list: • **TCP** • **UDP** • **TCP/UDP**
Enable Mapping	Select this checkbox to enable mapping.
WAN Connection List	Select a WAN connection from the list. Only active devices are shown on this list.

4

Click the **Add** icon to add port forwarding information to the table.

You can click the **Delete** icon corresponding to a row in the table to delete a configuration.

You can click the **Refresh** icon to update displayed information.

END OF STEPS

8.38 Configuring port triggering

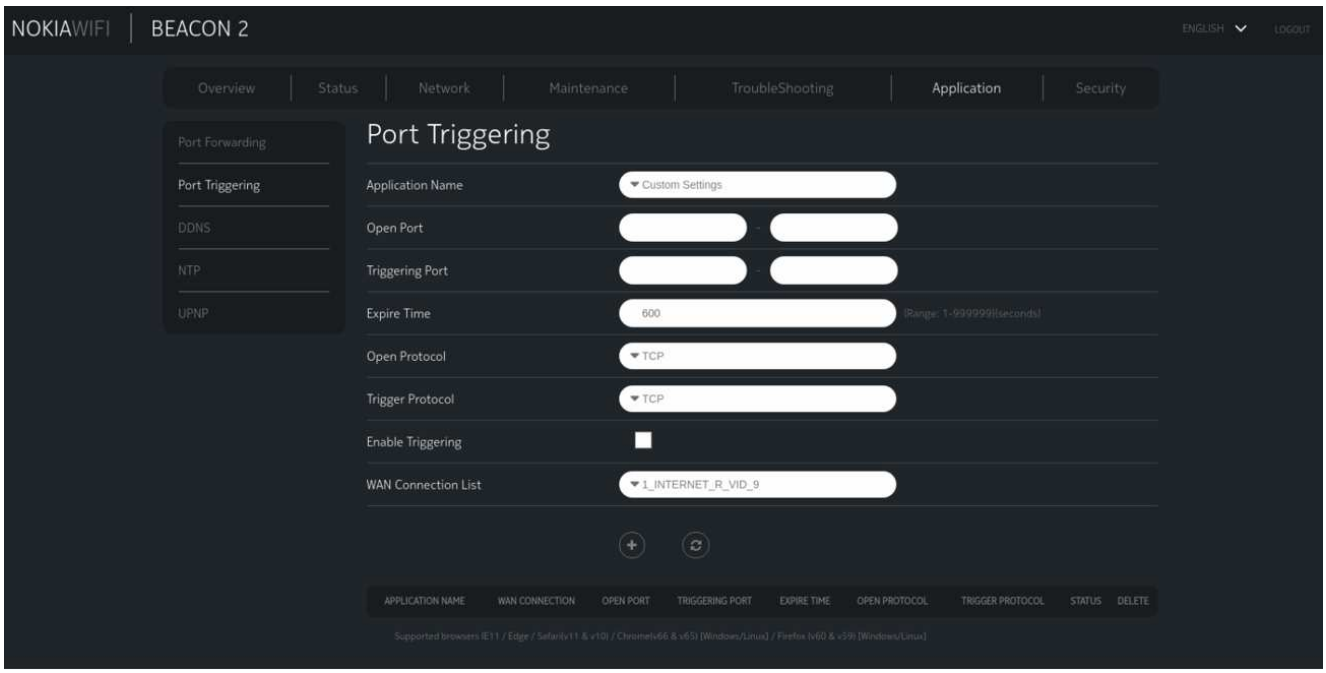
1

Click **Application** in the menu bar.

2

Click **Port Triggering** in the left pane. The Port Triggering page displays.

Figure 8-32 Port Triggering page



3

Configure the following parameters:

Table 8-27 Port Triggering parameters

Field	Description
Application Name	Select an application name from the list.

Table 8-27 Port Triggering parameters (continued)

Field	Description
Open Port	Enter the open port range.
Triggering Port	Enter the triggering port range.
Expire Time	Enter the expiration time in 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**
Enable Triggering	Select this checkbox to enable port triggering.
WAN Connection List	Select a WAN connection from the list. Only active devices are shown on this list.

4

Click the **Add** icon to add port forwarding information to the table.

You can click the **Delete** icon corresponding to a row in the table to delete a configuration.

You can click the **Refresh** icon to update displayed information.

END OF STEPS

8.39 Configuring DDNS

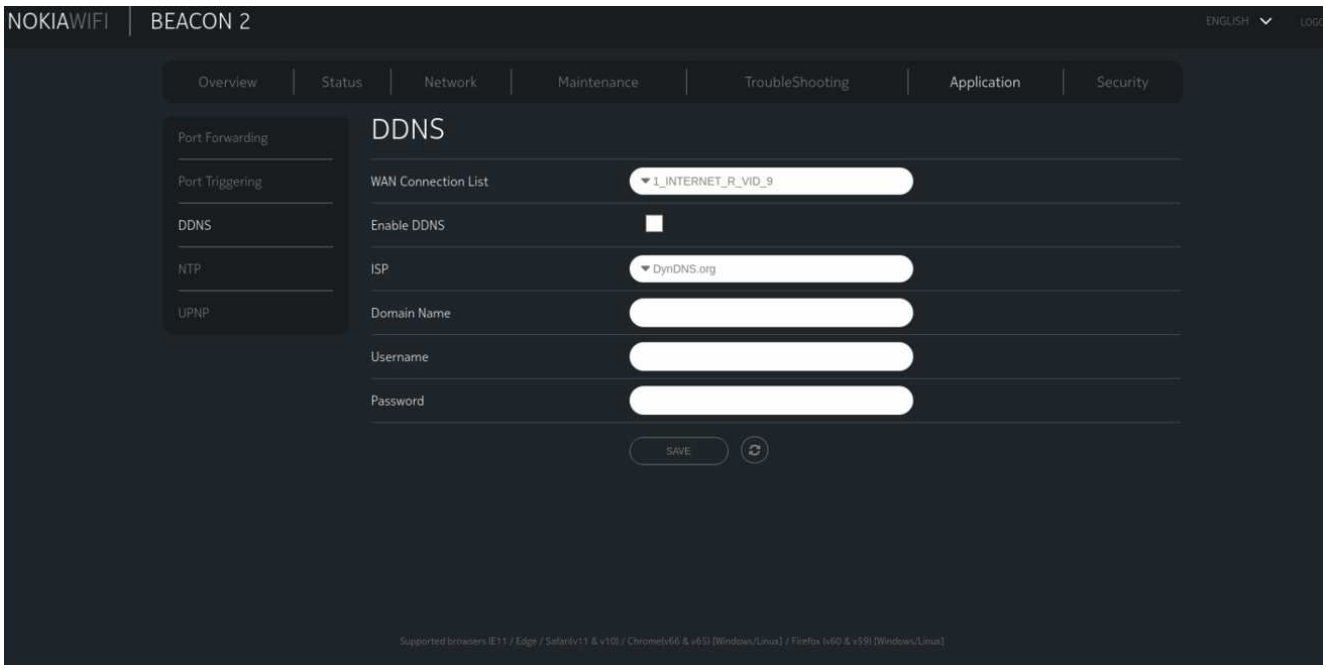
1

Click **Application** in the menu bar.

2

Click **DDNS** in the left pane. The DDNS page displays.

Figure 8-33 DDNS page



3

Configure the following parameters:

Table 8-28 DDNS parameters

Field	Description
WAN Connection List	Select a WAN connection from the list.
Enable DDNS	Select this checkbox to enable DDNS on the selected WAN connection. If this checkbox is not enabled, the DNS request will not be sent out from Beacon.
ISP	Select an ISP from the list.
Domain Name	Enter the domain name of the DDNS server.
Username	Enter the username of the DDNS server.
Password	Enter the password of the DDNS server.

4

Click **SAVE**.

You can click the **Refresh** icon to update displayed information.

END OF STEPS

8.40 Configuring NTP

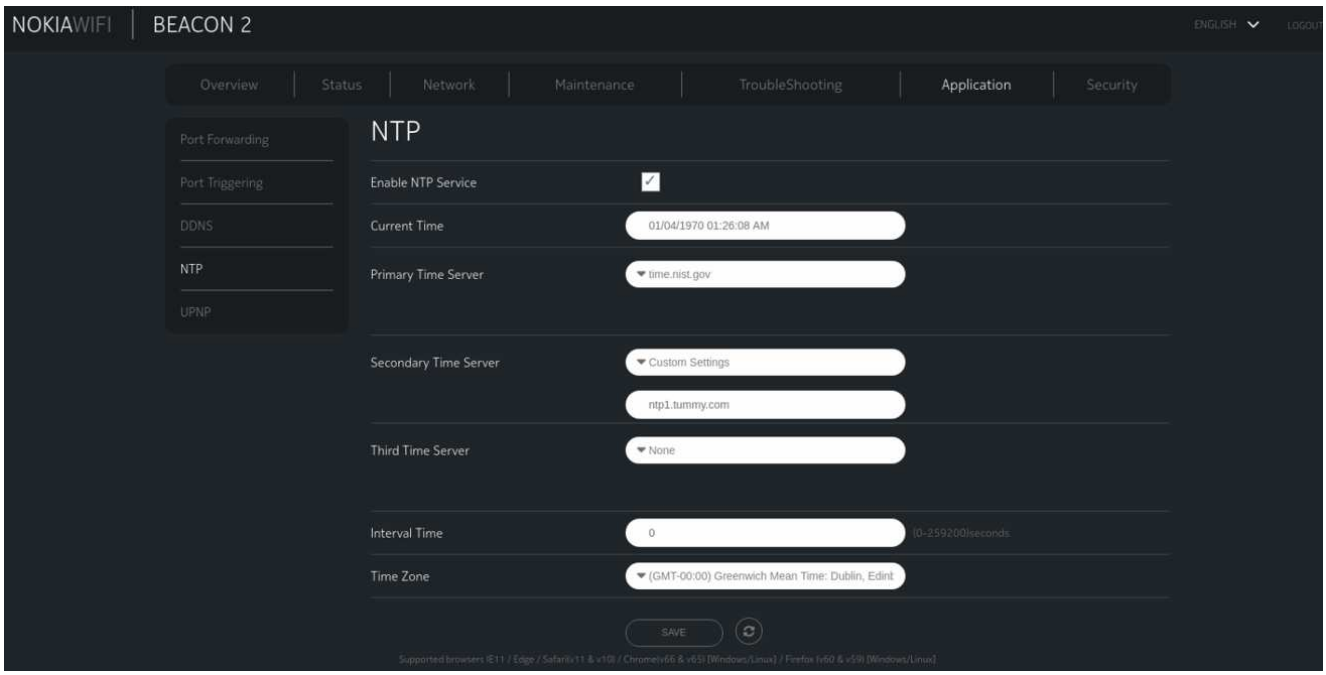
1

Click **Application** in the menu bar.

2

Click **NTP** in the left pane. The NTP page displays.

Figure 8-34 NTP page



3

Configure the following parameters:

Table 8-29 NTP parameters

Field	Description
Enable NTP Service	Select the Enable NTP Service checkbox.
Current Time	Displays the current time and date of the service.
Primary Time Server	Displays the primary server URL.
Secondary Time Server	Displays the secondary server URL.
Third Time Server	Displays the third server URL.

Table 8-29 NTP parameters (continued)

Field	Description
Interval Time	Enter the password of the DDNS server.
Time Zone	Indicates the current time zone of the server.

4

Click **SAVE**.

You can click the **Refresh** icon to update displayed information.

END OF STEPS

8.41 Configuring UPNP

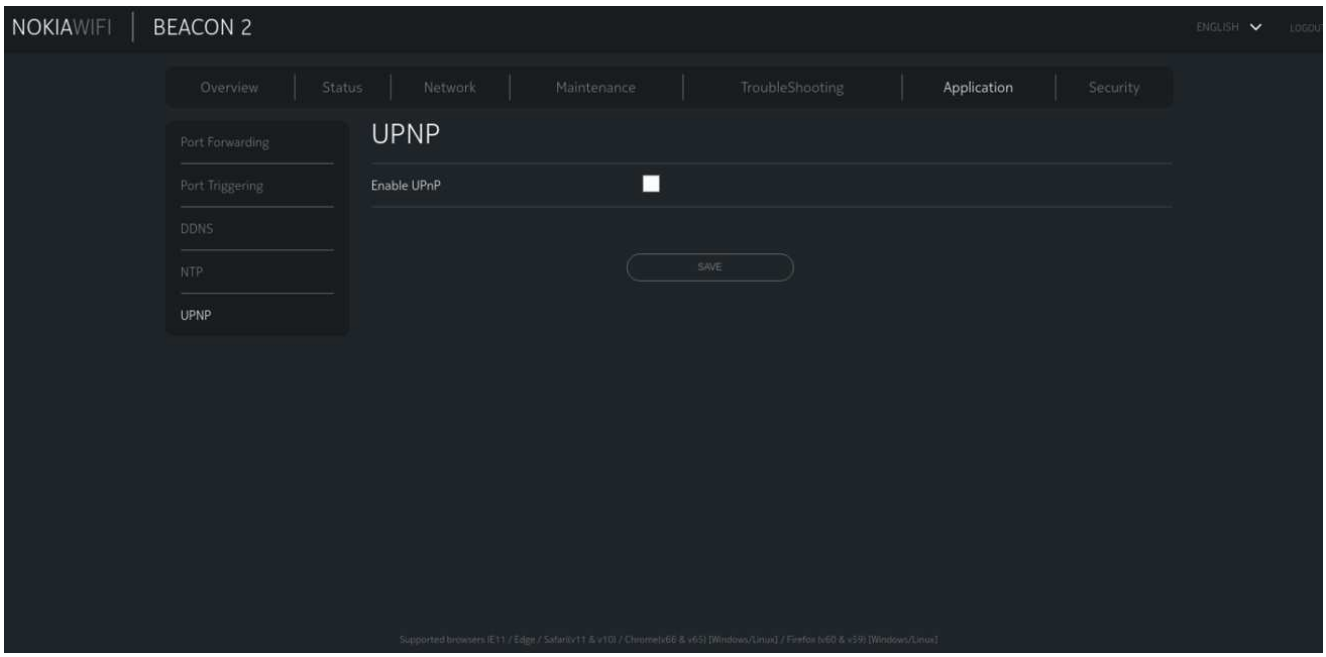
1

Click **Application** in the menu bar.

2

Click **UPNP** in the left pane. The UPNP page displays.

Figure 8-35 UPNP page



3

Select the **Enable UPnP** checkbox to enable UPnP.

If this checkbox is not enabled, the UPNP and DLNA process will not start.

4

Click **SAVE**.

End of steps

TroubleShooting

8.42 Overview

8.42.1 Purpose

This section describes the troubleshooting task that is performed by WEB based GUI.

8.42.2 Contents

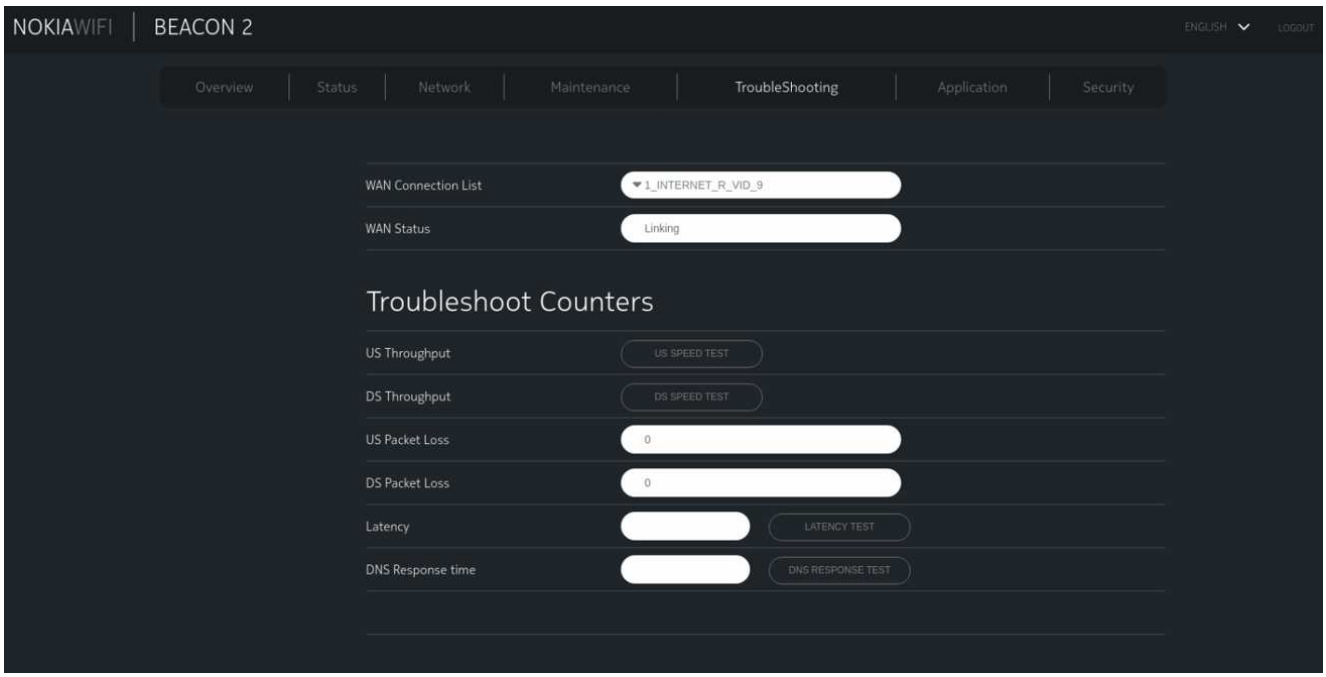
8.42 Overview	116
8.43 Troubleshooting	116

8.43 Troubleshooting

1

Click **Troubleshooting** from the menu bar. The Troubleshoot page displays.

Figure 8-36 Troubleshoot page



2

Configure the following parameters.

Table 8-30 Troubleshooting parameters

Field	Description
WAN Connection List	Select the required connection list from the drop-down menu.
WAN Status	Displays Whether the WAN status is active
US Throughput	This test is used to determine the upstream throughput/speed Click US Speed Test to specify the time for the upstream test The default is weekly, performed at idle to a public server
DS Throughput	This test is used to determine the downstream throughput/speed Click DS Speed Test to specify the time for the downstream test The default is weekly, performed at idle to a public server
US Packet Loss	The number of upstream packages lost
DS Packet Loss	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 The default is weekly, performed at idle to a public server
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 The default is weekly, performed at idle to a public server

END OF STEPS