NOKIA

Nokia WiFi Beacon

Beacon G6 Product Guide

3FE-49949-AAAA-TCZZA

Issue 1

June 2022

Legal notice

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

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

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

No part of this document may be modified.

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

Contents

Use subject to agreed restrictions on disclosure and use.

List of tables

List of figures

Use subject to agreed restrictions on disclosure and use.

Use subject to agreed restrictions on disclosure and use.

About this document

Purpose

This documentation set provides information about safety, features and functionality, ordering, hardware installation and maintenance, and software installation procedures of this device 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 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’sWiFi Beacon manufacturing, testing, and inspecting practices are in compliance with TL 9000 requirements. These requirements are documented in the Fixed Networks Quality Manual 3FQ-30146-6000-QRZZA.

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

Documents

Documents are available using ALED or OLCS.

To download a ZIP file package of the customer documentation

1

Navigate to http://customer.nokia.com/s/ and enter your user name and password. If you are a new user and require access to this service, 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

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

3

Enter the search criteria.

4

Select **All PDF Documents In**.

5

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

6

Click **Search**.

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

END OF STEPS

Technical support

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

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 theComments Hotline (mailto:comments@nokia.com).

1 What's new

1.1 Overview

1.1.1 Purpose

This section provides tables of the feature and document changes applicable to this guide.

1.1.2 Contents

1.2 What's new in BBD Release 22.02

The Product guide is a new guide in BBD Release 22.02, issue 1. In future releases, this section will provide tables of the feature and document changes applicable to this guide.

2 ETSI CPE safety guidelines

2.1 Overview

2.1.1 Purpose

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

2.1.2 Contents

2.2 Safety instructions

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

2.2.1 Safety instructions

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

The following is an example of the Danger instruction.

DANGER

Hazard

Possibility of personal injury.

The Danger instruction 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 a Warning instruction.

WARNING

Equipment Damage

Possibility of equipment damage.

Possibility of data loss.

The Warning instruction 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 instruction.

CAUTION

Service Disruption

Possibility of service interruption.

Service interruption.

The Caution instruction 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 instruction.

Note: Information of special interest.

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

2.2.2 Safety-related labels

The WiFi Beacon is labeled with the specific safety instructions and compliance information that is related to a variant of the WiFi Beacon. Observe the instructions on the safety labels.

Table 2-1, “Safety labels” (p. 22) provides sample safety labels.

Table 2-1 Safety labels

Label text	Description
CE marking	Indicates compliance to the European Council Directives including EN60950-1 safety
ESD warning	Caution: This assembly contains an electrostatic sensitive device.

2.3 Safety standards compliance

This section describes the WiFi Beacon compliance with the European safety standards.

2.3.1 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

2.3.2 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.

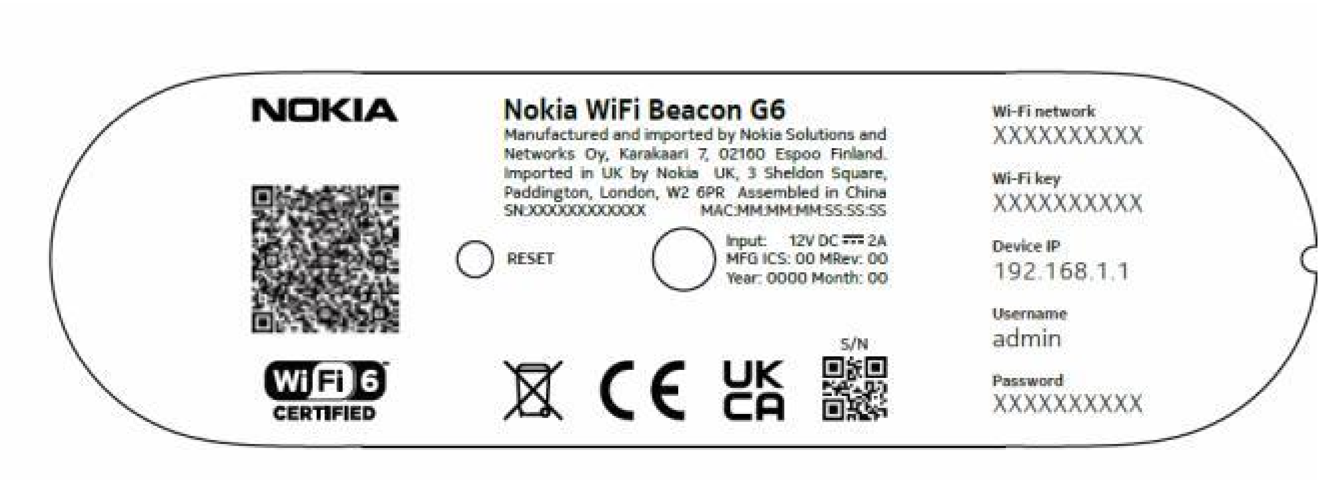
Table 2-2, “Safety labels” (p. 23) provides examples of the text in the various CPE safety labels.

Table 2-2 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.
UKCA marking	There is UKCA symbol for UKCA compliance.

Figure 2-1, “Sample safety labels” (p. 24) shows a sample safety label located on the bottom of the Beacon G6.

Figure 2-1 Sample safety labels



The customer premises equipment complies with the requirements of EN 60950-1, 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

2.3.3 Environmental standard compliance

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

2.3.4 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.

2.3.5 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.

2.3.6 Acoustic noise emission standard compliance

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

2.4 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.

2.4.1 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.

2.4.2 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.

3 ETSI environmental and CRoHS guidelines

3.1 Overview

3.1.1 Purpose

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.

3.1.2 Contents

3.2 Environmental labels

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

3.2.1 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.

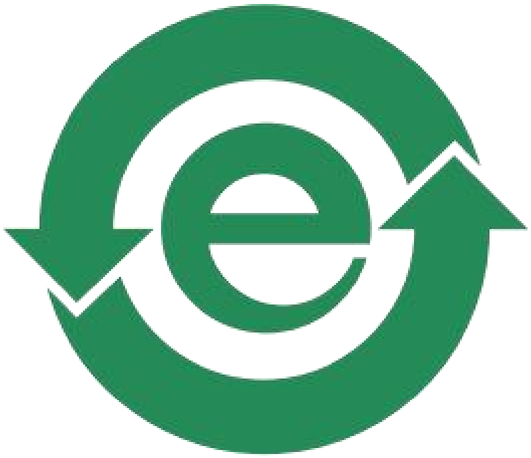
3.2.2 Environmental labels

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

Products below Maximum Concentration Value (MCV) label

Figure 3-1, “Products below MCV value label” (p. 28) 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 3-1 Products below MCV value label

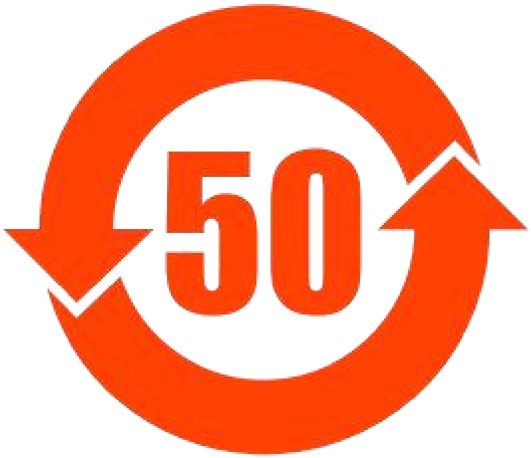


18986

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

The following figure 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 3-2 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 3.3 "Hazardous Substances Table (HST)" (p. 28)for more information.

3.3 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.nokia-sbell.com/wwwroot/images/upload/private/1/media/ChinaRoHS.pdf

3.4 Other environmental requirements

Observe the following environmental requirements when handling the WiFi Beacon.

3.4.1 WiFi Beacon environmental requirements

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

3.4.2 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.

3.4.3 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.

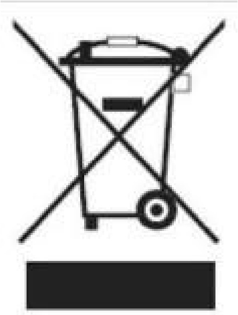
Nokia has implemented a material/substance content management process. The process is described in: Nokia process for ensuring RoHS Compliance (1AA002660031ASZZA). This ensures compliance with the European Union Directive 2011/65/EU on the Restriction of the Use of Certain Hazardous Substances in Electrical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

3.4.4 End-of-life collection and treatment

Electronic products bearing or referencing the symbol shown in following figure, 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 3-3 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 the figure 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.

4 ANSI CPE safety guidelines

4.1 Overview

4.1.1 Purpose

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

4.1.2 Contents

4.2 Safety instructions

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

4.2.1 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.

4.2.2 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.

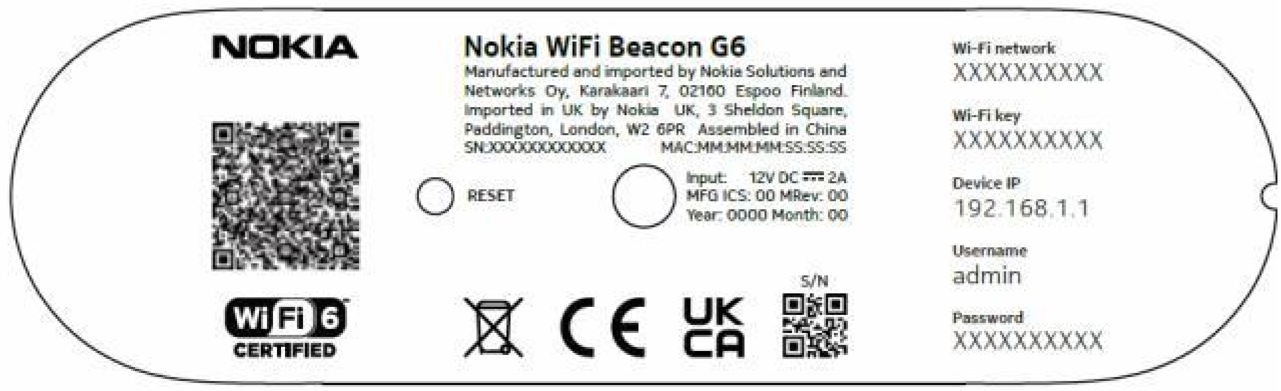
The following table provides examples of the text in the various CPE safety labels.

Table 4-1 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 4-1, “Sample safety label” (p. 33) shows a sample safety label located on the bottom of the Beacon G6.

Figure 4-1 Sample safety label



4.3 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.

4.3.1 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 B 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.

4.3.2 Energy-related products standby and off modes compliance

Hereby, Nokia declares that the Beacon G6 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 G6 devices qualify as high network availability (HiNA) equipment. Since the main purpose of Beacon G6 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 in chapter Chapter 5, “Beacon G6 unit data sheet”

For information about power consumption, see 5.7 “Beacon G6 detailed specifications” (p. 46)

4.3.3 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.

4.3.4 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.

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.

4.3.5 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.

4.4 Electrical safety guidelines

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

Beacon G6 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.

4.4.1 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.

4.4.2 Cabling

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

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

5 Beacon G6 unit data sheet

5.1 Overview

5.1.1 Purpose

5.1.2 Contents

5.2 Beacon G6 part numbers and identification

Table 5-1, “Identification of Beacon G6 ” (p. 37) provides part numbers and identification information for the Beacon G6 .

Table 5-1 Identification of Beacon G6

Ordering kit part number	Provisioning number	Description	CLEI Code	CPR	ECI/ Bar code
3FE 49882 AA	3FE 49949 AA	Beacon G6 US plug, 2.5G WAN,1x2.5G + 2x1 G LAN, 4x4 + 4x4 11ax Includes a wall mounted 12V AC/DC power adapter with 2-pin US input plug	—	—	—
3FE 49882 BA	3FE 49949 BA	Beacon G6 EU plug, 2.5G WAN,1x2.5G + 2x1 G LAN, 4x4 + 4x4 11ax Includes a wall mounted 12V AC/DC power adapter with 2-pin EU input plug	—	—	—

Table 5-1 Identification of Beacon G6 (continued)

Ordering kit part number	Provisioning number	Description	CLEI Code	CPR	ECI/ Bar code
3FE 49882 CA	3FE 49949 CA	Beacon G6 UK plug, 2.5G WAN,1x2.5G + 2x1 G LAN, 4x4 + 4x4 11ax Includes a wall mounted 12V AC/DC power adapter with 3-pin UK input plug	—	—	—
3FE 49882 DA	3FE 49546 DA	Beacon G6 AU plug, 2.5G WAN,1x2.5G + 2x1 G LAN, 4x4 + 4x4 11ax Includes a wall mounted 12V AC/DC power adapter with 2-pin AU input plug	—	—	—

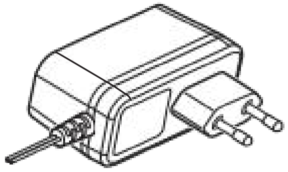
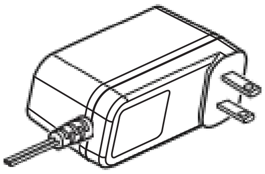
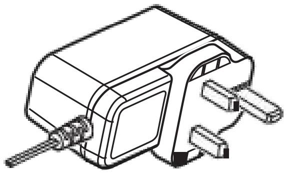
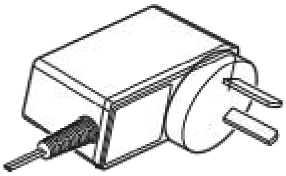
Table 5-2, “Beacon G6 power supply ordering information” (p. 38) provides the power supply information for the Beacon G6 . For more information on power supplies, see the **Nokia ONT Power Supply and UPS Guide**.

Table 5-2 Beacon G6 power supply ordering information

Part numbers	Power information (Model No./Manufacture Part Number)	Power information	Customer category or country compliance tested for	Notes
Kit: 3FE 49882 AA EMA: 3FE 49949 AA	FUHUA:UES36WU-120300SPA/ UE191205GWZF2RI HONOR: ADS-40FKJ-12N 12036EPCU / 1081FKJ12V3AEPCU	12V wall mounted AC/DC power adapter with 2-pin US input plug	ANSI municipality US, Canada UL/ETL IEC62368-1 and FCC/CB certified	2-pin US input plug
Kit: 3FE 49882 BA EMA: 3FE 49949 BA	FUHUA: UES36WV-120300SPA / UE191205GWZF1RI HONOR:ADS-40FKJ-12N 12036EPG / 1081FKJ12V3AEPG	12V wall mounted AC/DC power adapter with 2-pin EU input plug	Europe CE/CB certified	2-pin EU input plug
Kit: 3FE 49882 CA EMA:3FE 49949 CA	FUHUA:UES36WB-120300SPA / UE191205GWZF3RI HONOR:ADS-40FKJ-12N 12036EPB / 1081FKJ12V3AEPB	12V wall mounted AC/DC power adapter with 3-pin UK input plug	UK certified	3-pin UK input plug
Kit: 3FE 49882 DA EMA: 3FE 49546 DA	ADS-36FKJ-12N 12036EPSA-H / 1081FKJ12V3AEPSA	12V/ wall mounted AC/DC power adapter with AU input plug	Australia certified	-

The following table describes the various plug types used in the devices.

Table 5-3 Plug types

Plug type	Icon
2-pin EU plug	
2-pin US plug	
3-pin UK plug	
2-pin AU plug	

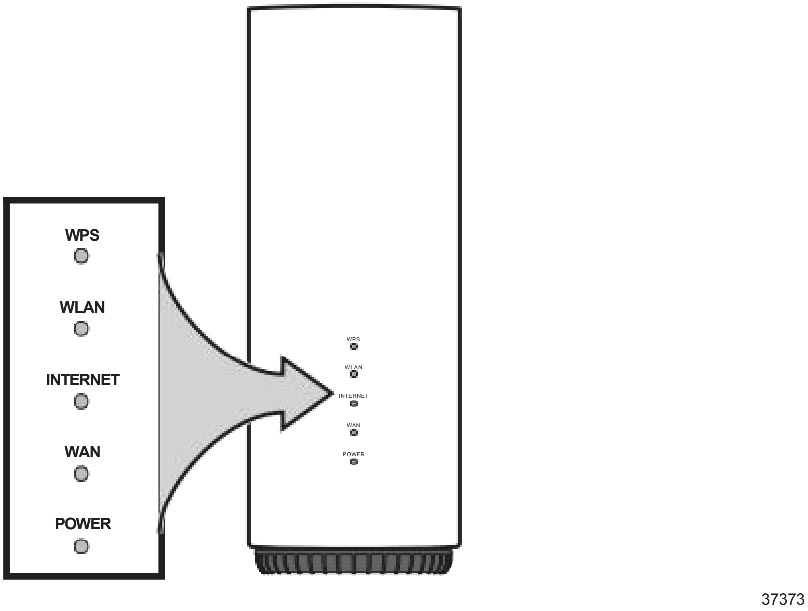
5.3 Beacon G6 general description

These devices provide the subscriber interface for the network by terminating the PON interface and converting it to user interfaces that directly connect to subscriber devices.

The Beacon G6 has built-in Wi-Fi 802.11 b/g/n/ac/ax networking with triple play capability and can provide triple play services with voice, video and data.

The Beacon G6 can be placed on a flat surface, such as a desk or shelf.

Figure 5-1 Beacon G6



This device provides the following functions:

- Dual-band concurrent 4x4 802.11b/g/n/ac/ax 2.4 GHz and 4x4 802.11ac/ax MU-MIMO 5 GHz
- Supports 802.11b/g/n/ac/ax 4x4 Wireless 2.4 GHz MIMO; Channel bandwidth 20, 40 MHz, auto
- Supports 802.11ac/ax 4x4 Wireless 5 GHz Mu-MIMO; Channel bandwidth 20, 40, 80, 160 MHz, auto
- One 2.5G/1G/100M/10M -Base-T standard RJ-45 WAN port
- One 2.5G/1G/100M/10M -Base-T standard RJ-45 LAN port
- Two 1G/100M/10M -Base-T standard RJ-45 LAN ports
- All RJ-45 ports support auto-negotiation and MDI/MDIX
- 512 MB NAND Flash with bad block management, 1 GB DDR3 RAM
- WLAN on/off push button
- WPS on/off push button
- Reset button
- Video and high speed Internet access
- Built-in layer 2 switch; Line Rate L2 traffic
- IP video distribution
- 4 inner antennas for 2.4G, 4 inner antennas for 5G
- WPA2, WPA-PSK/TKP
- WPA2, WPA2-PSK/AES

- WPA3, WPA3-SAE
- VLAN tagging/detagging and marking/remarking of IEEE 802.1p per Ethernet port.
- Support for multiple WI-Fi networks (private and public instances); contact your Nokia representative for further details.
- Conductive power (US Version): 800 mW/29 dBm (2.4 GHz); 900 mW/29.5 dBm (5 GHz)
- Maximum Effective Isotropic Radiated Power (EIRP) (US Version): 1600 mW/32 dBm (2.4 GHz); 2000 mW/33dBm (5 GHz)
- Maximum EIRP (EU Version): 100 mW/20 dBm (2.4 GHz); 1000 mW/30dBm (5 GHz)
- Maximum EIRP (AU Version): 2000 mW/33 dBm (2.4 GHz); 2000 mW/33dBm (5 GHz)
- Bridged mode (VLAN-binding mode) or routed mode per LAN port
- Ethernet-based Point-to-Point (PPPoE)
- DHCP client/server
- DNS server/client
- DDNS
- Port forwarding
- Network Address Translation (NAT)
- Network Address Port Translation (NAPT)
- UPnP IGD2.0 support
- ALG
- IGMP snooping and proxy (v2/v3)
- Traffic classification and QoS capability
- Configurable through WebGUI, TR-069, TR-369 and the Nokia WiFi mobile application
- Performance monitoring and alarm reporting
- Remote software image downloading and activation
- IP/MAC/URL filter
- Multi-level firewall and ACL

5.3.1 TR-069 parameter support

The Beacon G6 supports the following TR-069 features:

- Host object
- Port forwarding
- Object support for WiFi parameters
- Statistics and troubleshooting
- Diagnostic parameters

Host object support

The Beacon G6 provides host object support for: InternetGatewayDeviceLANDevice.Hosts.Host.

Port forwarding support

The Beacon G6 supports the port forwarding of objects via TR-069:

- Application Name
- WAN Port
- LAN Port
- Internal Client
- Protocol
- Enable Mapping
- WAN Connection List

These are the same port forwarding parameters supported in the GUI.

Object support for WiFi parameters

The Beacon G6 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 percentage of maximum transmit power)
- WPS

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

Statistics and troubleshooting support

The Beacon G6 supports TR-069 statistics and troubleshooting for LAN, WAN, and WiFi.

5.3.2 TR69 authentication using TLS and CA certificates

Beacon G6 supports TLS, as well as ACS authentication using SHA-256 pre-installed certificates.

If the URL is set to the https://... format, by default, the connection will use TLS without authentication mode. The Beacon G6 can also authenticate the ACS using a pre-installed CA certificate.

These devices support TLSv1.3 for TR069. The Beacon G6 supports download certification from ACS.

5.3.3 TR-111 support

The Beacon G6 supports TR-111, which extends the WAN Management Protocol defined in TR-069 to enhance the ability to remotely manage LAN devices.

The device-gateway association enables an ACS to identify the associated gateway through which a device is connected.

A connect request via the NAT gateway enables an ACS to initiate a TR-069 session with a device that is operating behind a NAT gateway.

5.3.4 TR-157 support

The Beacon G6 can support LXC container for third party software components on this devices with minimal 512 M memory. These software components are managed by ACS with the parameters defined in TR-157.

The TR-157 objects are:

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

Note: The device reserves and limits to 64 MB RAM and 32 MB flash in total for all of the third party applications. The maximum CPU load created or provided to the third party application is limited to approximately 30%. Underlying non-priority processes may still use the remaining memory on a temporary basis.

Nokia can assist to review specific applications, taking into account the actual memory load of the current hardware, current and projected software evolution over time, and the projected use by a third party application of the software.

5.4 Beacon G6 software and installation feature support

For information on installing or replacing the Beacon G6 see Chapter 6, “Install or replace a Beacon G6”

5.5 Beacon G6 interfaces and interface capacity

Table 5-4, “Beacon G6 indoor interface connection capacity” (p. 43) describes the supported interfaces and interface capacity for Beacon G6 .

Table 5-4 Beacon G6 indoor interface connection capacity

Beacon type and model	Maximum capacity										
	POTS	2.5G/1G/ 100M BASE-T	100/ 10 BASE-T	1000/ 100/ 10 BASE-T	RF video (CATV)	MoCA	USB	VDSL2	E1/T1	Local craft	XG-SPON SC/APC
Beacon G6 [1]	—	1 x WAN, 1xLAN	—	2 x LAN	—	—	—	—	—	—	—

Notes:

1. The Beacon G6 provide Wi-Fi service that is enabled and disabled using a Wi-Fi on/off switch.

5.5.1 Beacon G6 connections and components

The following figure shows the physical connections for Beacon G6 .

Figure 5-2 Beacon G6 connections and components

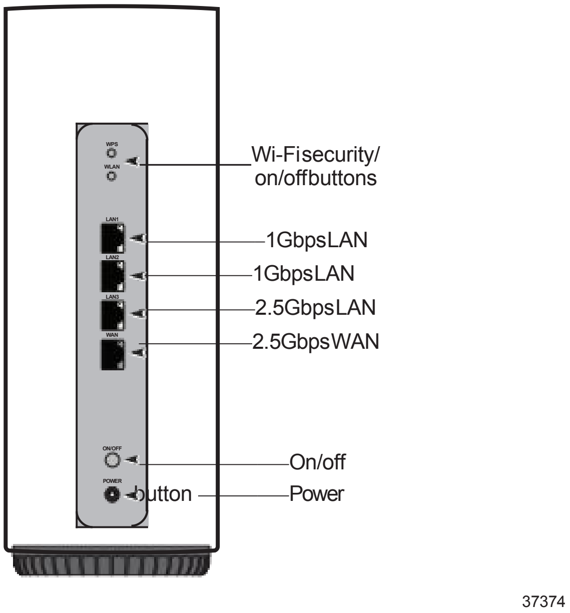


Table 5-5, " Beacon G6 physical connections" (p. 44) describes the physical connections for Beacon G6 .

Table 5-5 Beacon G6 physical connections

Connection [1]	Print Letters	Description
Ethernet ports	LAN1 to LAN3 and WAN	This connection is provided through Ethernet RJ-45 connectors. The connections support the following: • LAN1 and LAN2 are 1000/100/10 Base-T • LAN3 is 2.5G/1G/100M Base-T • WAN is 2.5G/1G/100M Base-T
Power input	POWER	This connection is provided through the power connector. A power cable fitted with a barrel connector is used to make the connection.
Reset button See Figure 6-2, "Beacon G6 reset button at the bottom of the device" (p. 55)	RESET	Pressing the Reset button for less than 10 seconds reboots the Beacon G6; pressing the Reset button for 10 seconds resets the Beacon G6 to the factory defaults.
WLAN button	WLAN	Wi-Fi service is compliant with IEEE 802.11 standards. If the WiFi signal is disabled, extender Wi-Fi points that use wireless mesh backhauling will looses their backhaul connection and goes into an error state until the W-Fi service on the Beacon G6 is restored.
WPS button	WPS	The Wi-Fi Protected Setup (WPS) button enables and disables the WPS.

Table 5-5 Beacon G6 physical connections (continued)

Connection [1]	Print Letters	Description
On/Off button	ON/OFF	This button turns the Beacon G6 on or off.

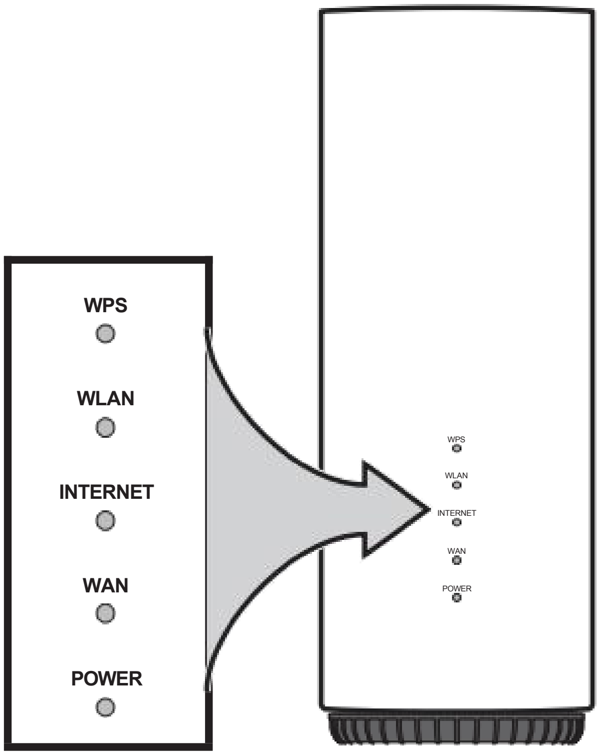
Notes:

1. The primary path for the earth ground for these devices is provided by the 12V Return signal in the power connector.

5.6 Beacon G6 LEDs

Figure 5-3, “Beacon G6 indoor LEDs” (p. 45)shows the Beacon G6 indoor LEDs.

Figure 5-3 Beacon G6 indoor LEDs



37373

Table 5-6, “Beacon G6 indoor LED descriptions” (p. 46) provides LED descriptions for Beacon G6 .

Table 5-6 Beacon G6 indoor LED descriptions

Indicator	LED color and behavior	LED behavior description
Power	Solid green	Power on.
	Blinking green	Software update
	Red solid	Light failed on startup (for example corrupt flash), or self test failed on startup, or self test failed during regular operation.
WAN	Off	No WAN ethernet cable connected. No physical uplink.
	Solid Green	WAN has a physical uplink and is synced at 2.5Gbps or 1Gbps
	Solid Orange	WAN has a physical uplink and is synced at 100 or 10M
INTERNET	Green solid	HSI WAN is connected the device has an IP address assigned from IPCP, DHCP, or static.
	Green Flashing	PPPoE or DHCP connection is in progress.
	Off	HSI WAN is not connected, the reasons could be either of the following: • there is no physical interface connection • the device is in bridge mode without an assigned IP address • the session has been dropped for reasons other than idle time-out.
WPS	Green Solid	WiFi protected setup link is up (negotiation and auto-configuration successful)
	Green Flashing	WiFi protected setup link activity (negotiation and auto-configuration ongoing)
	Red Solid	WiFi protected setup processing exception or multiple peers using WPS simultaneously
	Off	WiFi protected setup link down or no link connected (negotiation has not started or has failed)
WLAN	Green solid	WiFi enabled for at least one radio frequency (RF)
	Blinking	WiFi data traffic passing
	Off(dark)	WLAN is down
WAN/LAN/ RJ45 (Executed on the RJ45 connectors)	Green Solid	LAN link active
	Off	LAN link is OFF or has LOS (line of signal) transmission issue.

5.7 Beacon G6 detailed specifications

The following table lists the physical specifications for Beacon G6 .

Table 5-7 Beacon G6 indoor physical specifications

Description	Specification
Depth	6.29 in. (160 mm)
Width	3.34 in. (85 mm)
Height (including antenna)	8.85 in. (225 mm)

Table 5-7 Beacon G6 indoor physical specifications (continued)

Description	Specification
Weight	2.55 lbs (1.16kg)

Table 5-8, "Beacon G6 indoor power consumption specifications" (p. 47) lists the power consumption specifications for Beacon G6.

Table 5-8 Beacon G6 indoor power consumption specifications

Mnemonic	Maximum power (Not to exceed)	Condition	Minimum power	Condition
Beacon G6	24.3 W	2 1000/100/10 Base-T Ethernet, 2 x 2.5G/1000 M /100/10 BASE-T Ethernet,WI-Fi operational	9.6W	Wi-Fi active, other interface / service not provisioned

Table 5-9, "Beacon G6 environmental specifications" (p. 47) lists the environmental specifications for Beacon G6 indoor .

Table 5-9 Beacon G6 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: -25°C to 70°C (4°F to 185°F)	

Table 5-10, "Beacon G6 dimension data specifications" (p. 47) lists the dimension data specifications for Beacon G6

Table 5-10 Beacon G6 dimension data specifications

Dimension	Specification
Packet size supported	Less than 2000 jumbo frames Max MTU of IP diagram -1500
Number of IP addresses supported (or ranges)	In LAN network, the supported range is: • IPv4: 192.168.1.2 - 192.168.1.254 (default) • IPv6: no limitation
Number of supported Wi-Fi clients (per radio, per device, per mesh)	• 128 clients per radio • 128 clients per device • 256 clients per mesh supported
Number of supported beacons /APs in a mesh	6 (including the device)

Table 5-10 Beacon G6 dimension data specifications (continued)

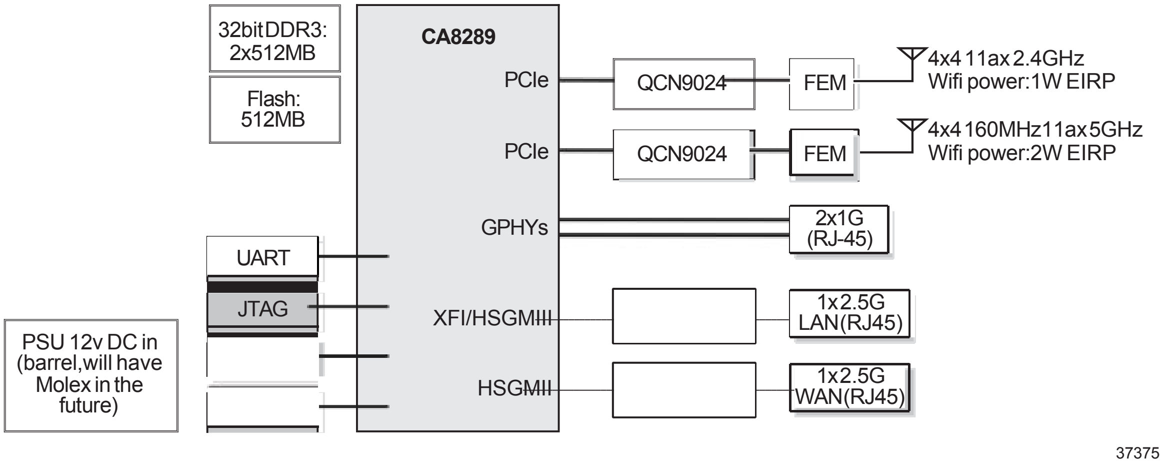
Dimension	Specification
Number of supported WAN services	Supports 6 WAN services: WAN - Router: • Connection Type: IPoE • Service: INTERNET • WAN IP Mode: DHCP
Number of supported VLANs	Supports 6 VLANs. Supports only untagged packets in upstream.
Number of priority queues, and overall buffer size	64 priority queues. Max 16MB for WAN and 4MB for LAN
Number of multicast groups (DACL entries)	64

5.8 Beacon G6 functional blocks

Beacon G6 s are single-residence devices that support a 2.5Gbps WAN port and a 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 three RJ-45 Ethernet ports.

Figure 5-4, “Beacon G6 functional block” (p. 48) shows the functional blocks for Beacon G6 indoor .

Figure 5-4 Beacon G6 functional block



5.9 Standards and compliance

This section lists the standards and compliances.

5.9.1 Beacon G6 standards/compliance

These devices are compliant with the following standards:

- CE marking for European standards for health, safety, and environmental protection
- EN 300-328 v1.9.1 wide band data transmission standards for 2.4GHz bands
- FCC, ETL, WFA, RoHS, WEEE, REACH
- IEEE 802.1p for traffic prioritization
- IEEE 802.1q for VLANs
- IEEE 802.3 (2012)
- IEEE 802.11b/g/n/ac/ax for WIFI

5.9.2 Responsible party

The following lists the party in the US responsible for this device.

Table 5-11 Responsible party contact information

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

5.9.3 Energy-related products standby and off modes compliance

Hereby, Nokia declares that the Beacon G6 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.

These devices qualify as equipment with high network availability (HiNA) functionality. Since the main purpose of Beacon G6 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 G6 interfaces and interface capacity” (p. 43) in this section.

For information about power consumption, see 5.7 “Beacon G6 detailed specifications” (p. 46) in this section.

5.9.4 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.

5.9.5 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.

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.

5.10 Beacon G6 special considerations

This section describes the special considerations for Beacon G6 devices.

5.10.1 WiFi service

Beacon G6 devices feature WiFi service as well as data services. WiFi is a wireless networking technology that uses radio waves to provide wireless HSI and network connections. This device complies with the IEEE 802.11 standards, which the WiFi Alliance defines as the basis for WiFi technology.

WiFi standards and certifications

The WiFi service on Beacon G6 devices supports the following IEEE standards and WiFi Alliance certifications :

- Compliant with IEEE 802.11 standards

- Certified for Wi-Fi6
- Certified for IEEE 802.11b,g,n,ac
- Certified for WPA™ – Enterprise, Personal
- Certified for WPA2™ – Enterprise, Personal
- Certified for WPA3™ – Enterprise, Personal (Aug 2019)
- Certified for Protected Management Frames
- Certified for Wi-Fi Agile Multiband™,WMM®, WMM®-Power Save, Wi-Fi Protected Setup™
- Certified for Easymesh R2

Nokia WiFi app configuration

The Nokia WiFi mobile app can be used to set up the Beacon G6 and manage the network.

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

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

WiFi GUI features

Beacon G6 devices have HTML-based WiFi configuration GUIs.

5.10.2 Beacon G6 considerations and limitations

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

6 Install or replace a Beacon G6

6.1 Overview

6.1.1 Purpose

This chapter provides the steps to:

- Install a Beacon G6
- Replace a Beacon G6

6.1.2 Contents

6.2 Prerequisites

Ensure that you have all required cables.

6.3 Recommended tools

You need the following tools:

- RJ-45 cable
- Paper clip

6.4 Safety information

Read the following safety information before installing the unit.

DANGER

Hazard

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

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

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

CAUTION

Service Disruption

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

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

Observe the following:

- The device should be installed in accordance with the applicable requirements of the NEC or CEC. Local authorities and practices take precedent when there is conflict between the local standard and the NEC or CEC.
- The device must be installed by qualified service personnel.
- Indoor units must be installed with cables that are suitably rated and listed for indoor use.
- See the detailed specifications in the Chapter 5, "Beacon G6 unit data sheet"for the temperature ranges for these devices.

6.5 Install a Beacon G6

1

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

Note: The Beacon G6 cannot be stacked with another or with other equipment. The installation requirements are:

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

2

Review the connection locations, as shown in Figure 6-1, "Beacon G6 connections" (p. 55).

Figure 6-1 Beacon G6 connections

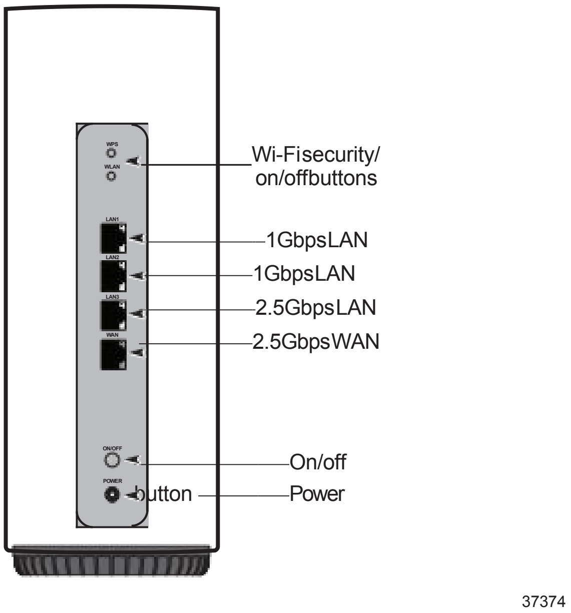
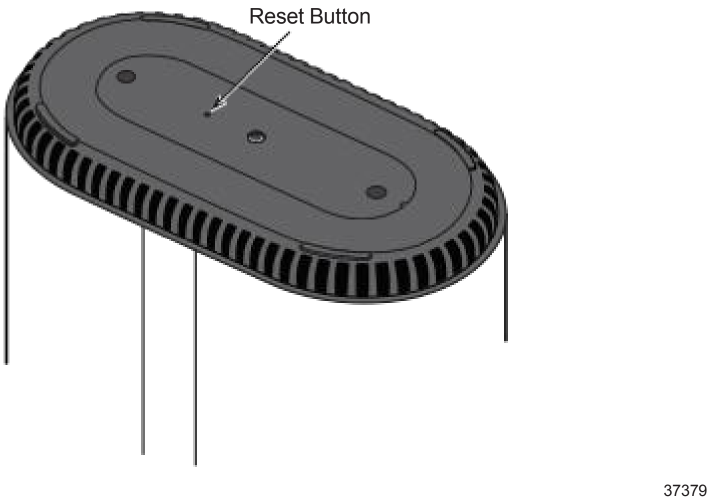


Figure 6-2 Beacon G6 reset button at the bottom of the device



3

Connect the Ethernet cables to the RJ-45 ports; see Figure 6-1, “Beacon G6 connections” (p. 55)for the location of the RJ-45 ports.

4

Connect the WAN cable to the RJ-45 WAN port; see Figure 6-1, “Beacon G6 connections” (p. 55)for the location of the RJ-45 WAN port.

5

Connect the power cable to the power connector.

ℹ **Note:** Units must be powered by a Listed or CE approved and marked limited power source power supply with a minimum output rate of 12 V dc, 2 A. The polarity of the power adapter plug must match the Beacon G6.

6

Power up the unit by using the On/Off power switch. The POWER LED indicator should be solid green in color.

7

Verify the LEDs and voltage status. The Table 5-6, “Beacon G6 indoor LED descriptions” (p. 46) indicates the behavior of the LEDs.

8

Activate and test the services.

9

If the Beacon G6 is in a failure state or is not providing the services that are expected, perform a factory reset.

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

a. Locate the **Reset** button as shown in Figure 6-1, “Beacon G6 connections” (p. 55).

b. Insert the end of a straightened paper clip or other narrow object into the hole and keep the reset button pushed for 10s until the Power LED blinks red.

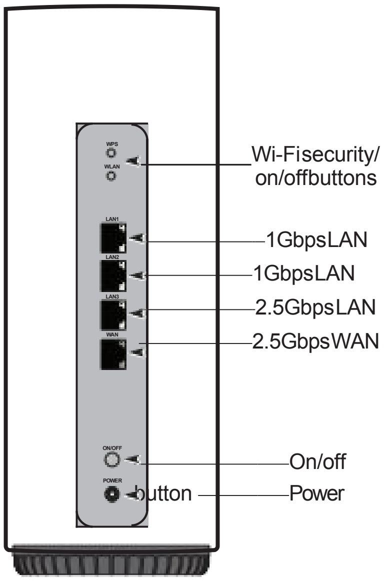
c. Your device will reboot with the factory default settings.

END OF STEPS

6.6 Replace a Beacon G6

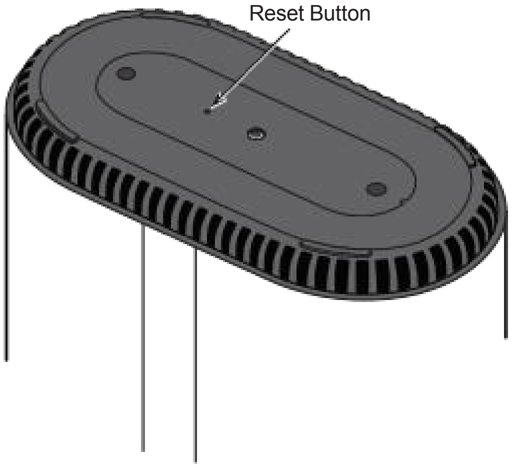
1

Power down the unit by using the on/off power switch. See for the connections on the Beacon G6.



37374

Figure 6-3 Beacon G6 connections



37379

Figure 6-4 Beacon G6 reset button at the bottom of the device

2

Disconnect the WAN, LAN, and power cables from the Beacon G6; see Figure 6-3, “ Beacon G6 connections” (p. 57)for the connector locations on the Beacon G6.

3

Replace the Beacon G6 with the new device. The device can be placed on any flat surface, such as a desk or shelf.

4

Connect the LAN cables directly to the RJ-45 ports; see Figure 6-3, “ Beacon G6 connections” (p. 57)for the location of the RJ-45 ports.

5

Connect the WAN cable directly to the LAN RJ-45 port; see Figure 6-3, “ Beacon G6 connections” (p. 57)for the location of the RJ-45 WAN port.

6

Connect the power cable to the power connector.

Note: Units must be powered by a Listed or CE approved and marked limited power source power supply with a minimum output rate of 12 V dc, 2 A. The polarity of the power adapter plug must match the Beacon G6.

7

Power up the unit by using the On/Off power button. The POWER LED indicator should be solid green in color.

8

Verify the LEDs and voltage status.The Table 5-6, “Beacon G6 indoor LED descriptions” (p. 46)indicates the behavior of the LEDs.

9

Activate and test the services.

10

If the Beacon G6 is in a failure state or is not providing the services that are expected, perform a factory reset.

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

a. Locate the Reset button on a Beacon G6 as shown in Figure 6-3, “ Beacon G6 connections” (p. 57).

b. Insert the end of a straightened paper clip or other narrow object into the hole and keep the reset button pushed for 10s until the Power LED blinks red.

c. Your device will reboot with the factory default settings.

END OF STEPS

7 Configure a Beacon G6

7.1 Overview

7.1.1 Purpose

This chapter describes the WebGUI configuration procedures.

7.1.2 Contents

GUI overview

7.2 Overview

7.2.1 Purpose

This section provides an overview of the Beacon G6 WebGUI.

7.2.2 Contents

7.3 General configuration

Refer to the configuration information provided with your OLT for the software configuration procedure for a Beacon G6.

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

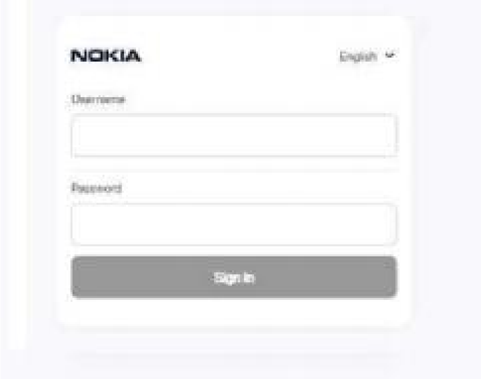
7.4 Logging in to the web-based GUI

1

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

The *Login* page displays.

Figure 7-1 *Login* page



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

2

CAUTION

Service Disruption

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

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

Pressing the **Reset** *button for 10 seconds resets the device to the factory defaults, except for the LOID and SLID.*

Pressing the **Reset** *button for 10 seconds resets the device to the factory defaults.*

Enter your username and password in the *Login* page, as shown in Figure 7-1, "Login page" (p. 62).

The superadmin account is meant for the operator and is unique per device. Contact your Nokia representative to obtain the superadmin password for device.

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

3

Click **Sign in**. The Device Information page displays.

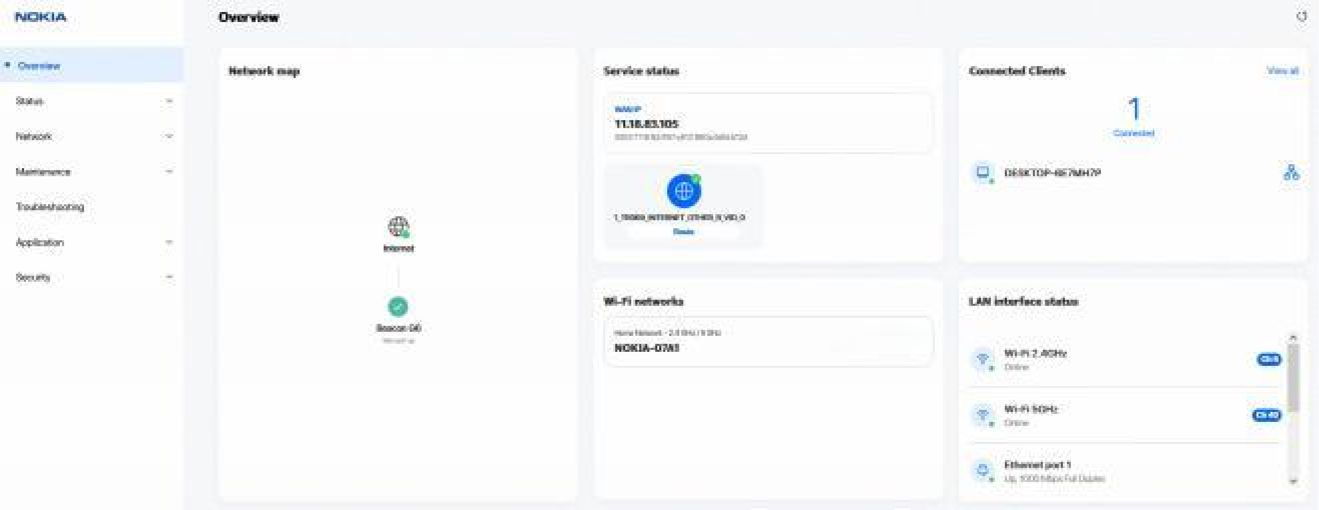
Note: To help protect the security of your Internet connection, the application displays a pop-up reminder to change both the Wi-Fi password and the Beacon password.
To increase password security, use a minimum of 10 characters, consisting of a mix of numbers and upper and lower case letters.

END OF STEPS

7.5 Viewing overview information

1

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



Overview

Network map

Service status

WAN IP
11.18.83.105

1_TR069_INTERNET_OTHER_R_VID_0

Connected Clients

1
Connected

DESKTOP-6E7MH7P

Wi-Fi networks

Home Network - 2.4 GHz / 5 GHz
NOKIA-07A1

LAN interface status

Wi-Fi 2.4GHz
Online

Wi-Fi 5GHz
Online

Ethernet port 1
Up, 1000 Mbps Full Duplex

END OF STEPS

7.5.1 Network Map

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

Root device

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

Extender device

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

7.5.2 Service Status

Displays the active status of the triple-play services.

Internet service

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

IPTV service

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

7.5.3 Wi-Fi Networks

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

7.5.4 Connected Clients

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

7.5.5 LAN Interface Status

Displays information about all the LAN ports of the device.

Wi-Fi 2.4GHz

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

Wi-Fi 5GHz

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

Ethernet Ports

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

Viewing device information and status

7.6 Overview

7.6.1 Purpose

This section describes procedures to view device information and status on the Beacon G6.

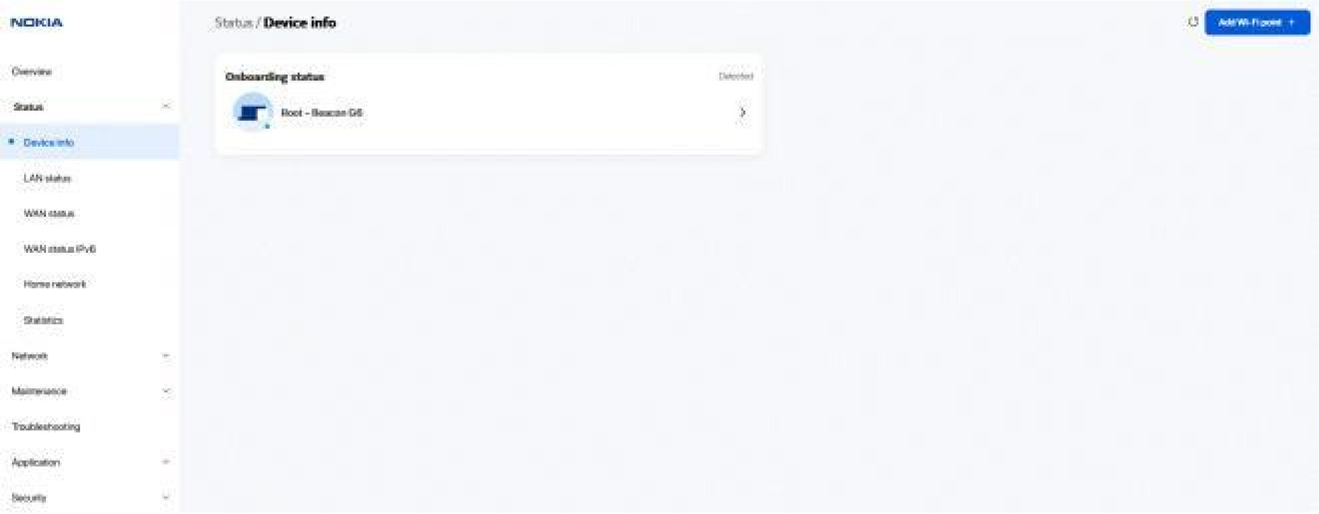
7.6.2 Contents

7.7 Viewing device information and adding Wi-Fi points

1

Click **Status**→ **Device Info** in the left pane. The Device Information page displays the onboarding status of the Wi-Fi points added to the network.

Figure 7-2 Device info page

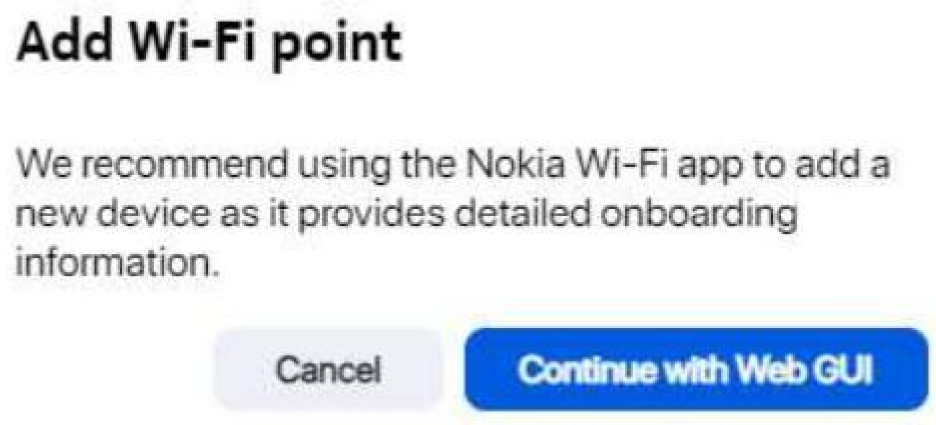


2

Perform the following steps to add a Wi-Fi point:

a. Click **Add Wi-Fi point** at the top right corner of the *Device Info* page. A message displays that it is recommended to use the Nokia Wi-Fi mobile app to add a Wi-Fi point.

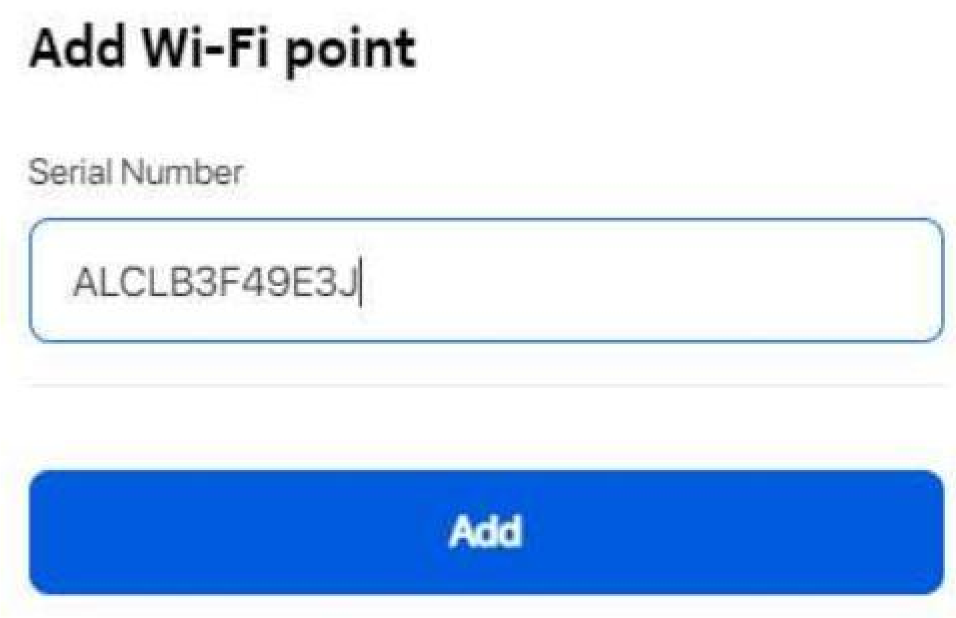
b. To add a Wi-Fi point using the WebGUI, click **Continue with WebGUI**.



Add Wi-Fi point

We recommend using the Nokia Wi-Fi app to add a new device as it provides detailed onboarding information.

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



Add Wi-Fi point

Serial Number

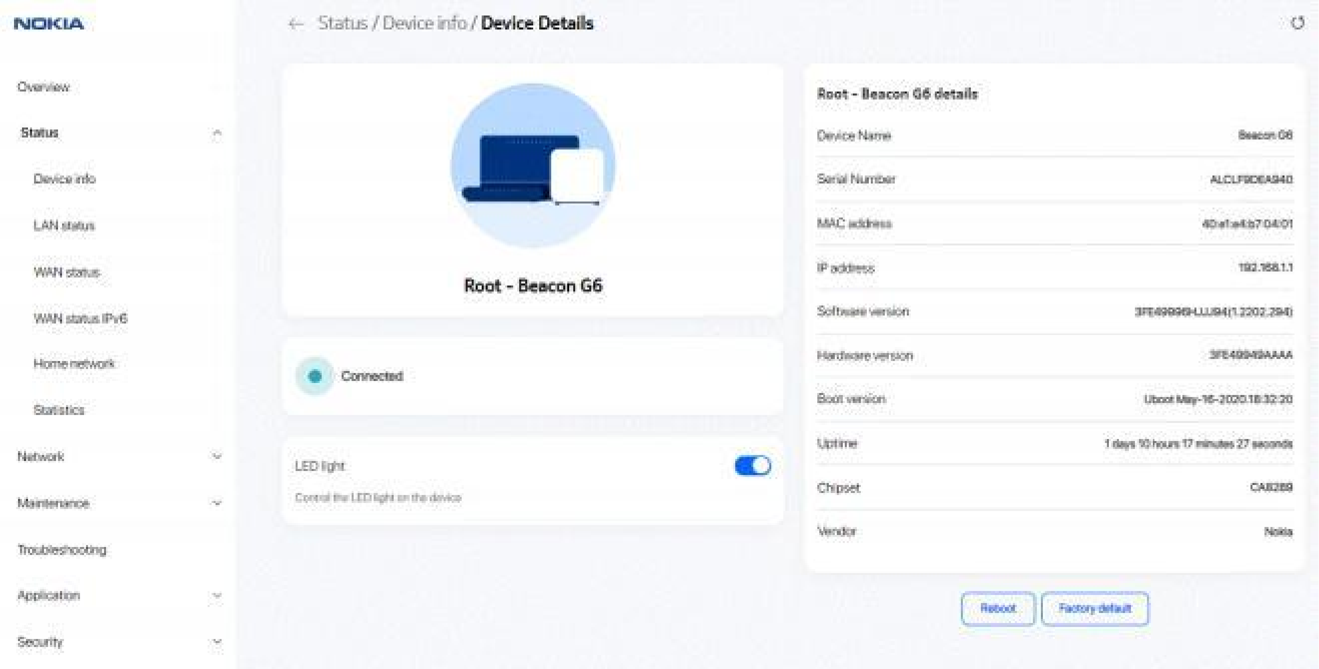
ALCLB3F49E3J

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

3

Click the arrow next to a Wi-Fi point to view the device details. The *Device Info* page displays the details of the selected device in the network, including connection status.

Figure 7-3 Device info - Device Details page



Root - Beacon G6 details

Device Name Beacon G6
Serial Number ALCLF9D6A940
MAC address 40:e1:e4:b7:04:01
IP address 192.168.1.1
Software version 3FE49996HLLU94(1.2202.294)
Hardware version 3FE49949AAAA
Boot version Uboot May-16-2020.18:32:20
Uptime 1 days 10 hours 17 minutes 27 seconds
Chipset CA8289
Vendor Nokia

Table 7-1 Device Info parameters

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

4

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

5

Perform any of the following, as applicable:

- **Reboot the device:**
  1. Click **Reboot**. A message displays asking if you want reboot the device.
  2. Click **OK** to reboot the Beacon. The device reboots and displays the login page.
- **Reset the device to factory default settings:**
  1. Click **Factory default**. A message displays asking if you want to reset the system configuration to the factory default settings.
  2. Click **OK** to reset the Beacon to the factory default settings.

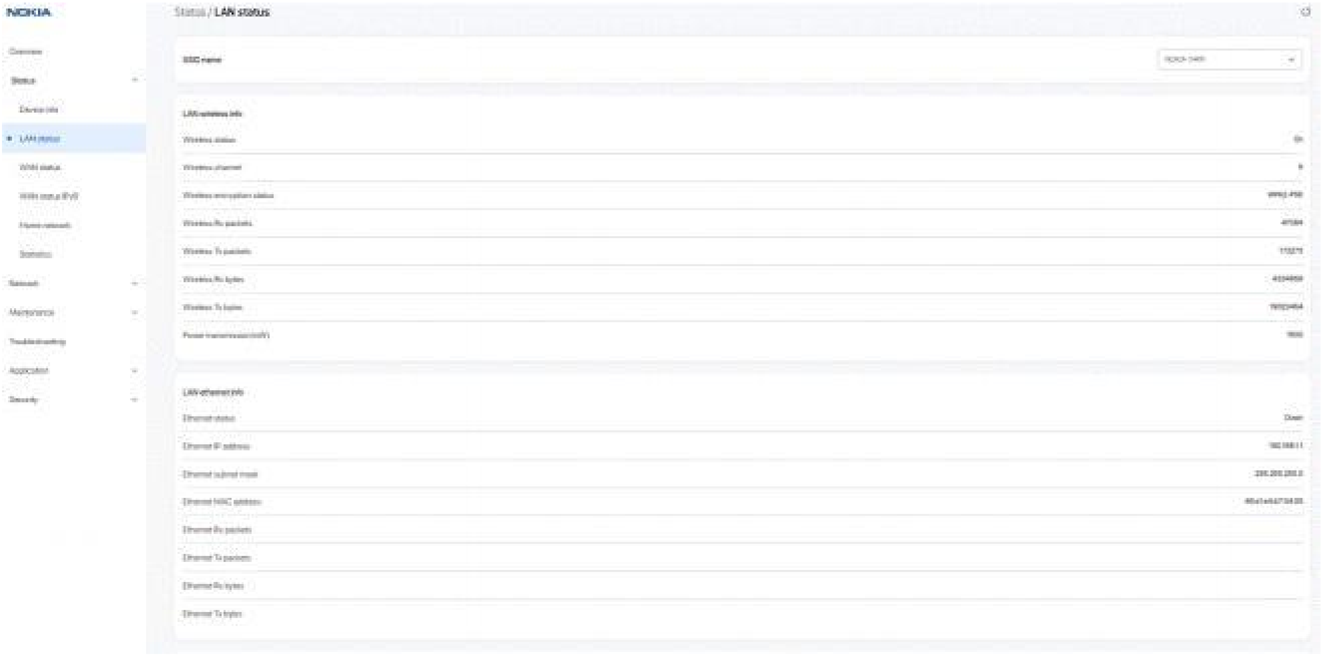
END OF STEPS

7.8 Viewing LAN status

1

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

Figure 7-4 LAN status page



Status / LAN status

SSID name [illegible]

LAN wireless info

Wireless status On
Wireless channel 6
Wireless encryption status WPA2-PSK
Wireless Rx packets [illegible]
Wireless Tx packets [illegible]
Wireless Rx bytes [illegible]
Wireless Tx bytes [illegible]
Power transmission (mW) [illegible]

LAN ethernet info

Ethernet status Down
Ethernet IP address 192.168.1.1
Ethernet subnet mask 255.255.255.0
Ethernet MAC address [illegible]
Ethernet Rx packets
Ethernet Tx packets
Ethernet Rx bytes
Ethernet Tx bytes

Table 7-2 LAN status parameters

Field	Description
SSID name	Select an SSID from the list.
LAN wireless info	
Wireless status	Indicates whether the wireless is on or off.
Wireless channel	Wireless channel number.
Wireless encryption status	Encryption type used on the wireless connection.
Wireless Rx packets	Number of packets received on the wireless connection.
Wireless Tx packets	Number of packets transmitted on the wireless connection.
Wireless Rx bytes	Number of bytes received on the wireless connection.
Wireless Tx bytes	Number of bytes transmitted on the wireless connection.
Power transmission (mW)	Power of the wireless transmission, in 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	Number of packets received on the Ethernet connection.
Ethernet Tx packets	Number of packets transmitted on the Ethernet connection.
Ethernet Rx bytes	Number of bytes received on the Ethernet connection.
Ethernet Tx bytes	Number of bytes transmitted on the Ethernet connection.
Info	
Status	Displays the status of the LAN.
Duplex Mode	Displays the duplex mode of the LAN.
Max bit rate	Displays the maximum bit rate of the LAN.
Errors received	Displays errors received in bytes.
Errors sent	Displays errors transmitted in bytes.
Packets received	Displays the received packets.
Packets sent	Displays the transmitted packets.
Bytes received	Displays the received bytes.
Bytes sent	Displays the transmitted bytes.

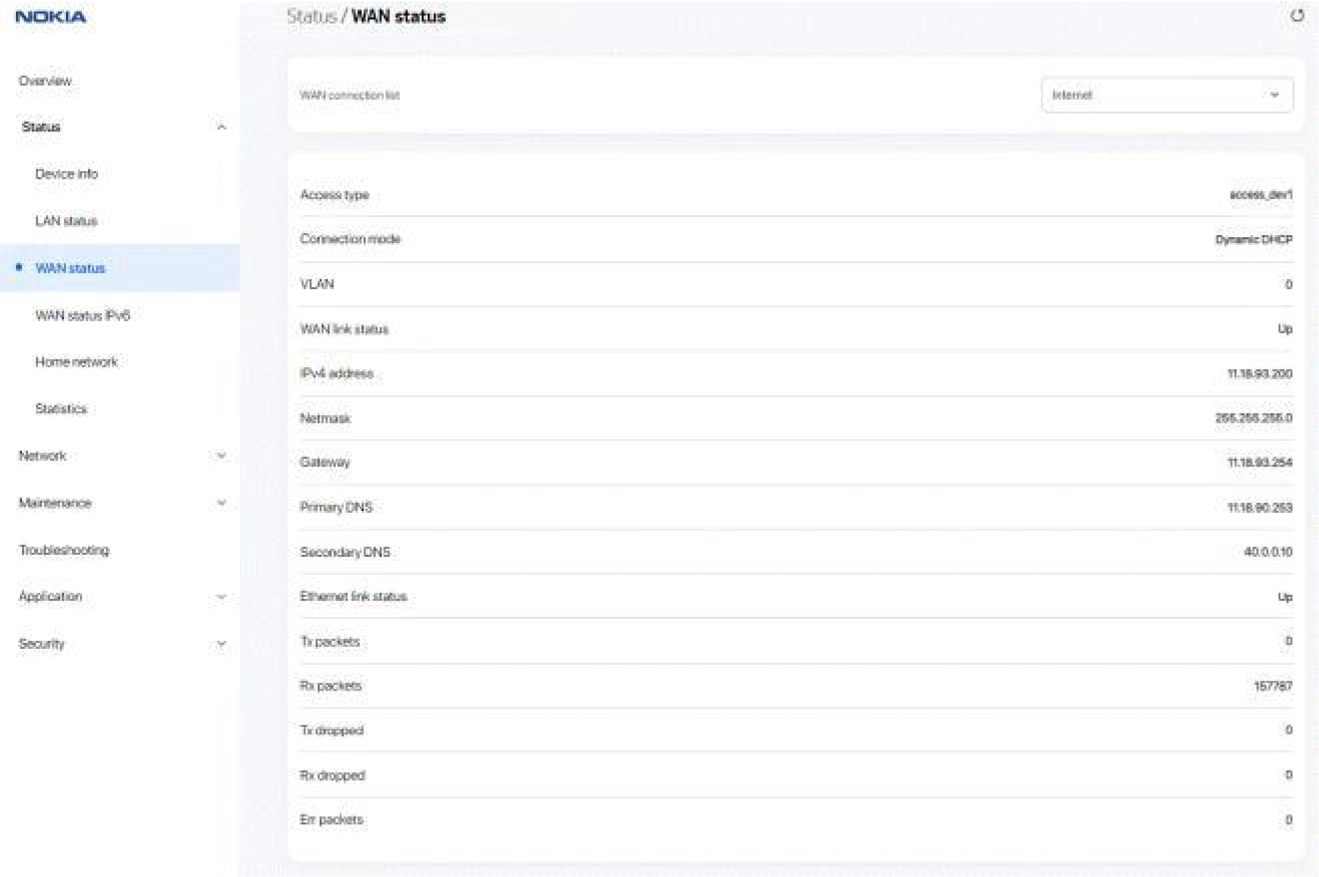
END OF STEPS

7.9 Viewing WAN status

1

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

Figure 7-5 *WAN Status* page



WAN connection list	Internet
Access type	access_dev1
Connection mode	Dynamic DHCP
VLAN	0
WAN link status	Up
IPv4 address	11.18.93.200
Netmask	255.255.255.0
Gateway	11.18.93.254
Primary DNS	11.18.90.253
Secondary DNS	40.0.0.10
Ethernet link status	Up
Tx packets	0
Rx packets	157787
Tx dropped	0
Rx dropped	0
Err packets	0

Table 7-3 *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	Displays the connection mode of the WAN connection
VLAN	Displays the VLAN ID.

Table 7-3 WAN Status parameters (continued)

Field	Description
WAN link status	Displays whether the WAN link is connected or disconnected.
IPv4 address	Displays the IP address.
Netmask	Displays the netmask address.
Gateway	Displays the gateway address.
Primary DNS	Enter the primary domain name server address.
Secondary DNS	Enter the secondary domain name server address.
Ethernet link status	Displays whether the Ethernet link is up or down.
Tx packets	Displays the number of packets transmitted.
Rx packets	Displays the number of packets received.
Tx dropped	Displays the number of transmitted packets dropped.
Rx dropped	Displays the number of received packets dropped.
Err packets	Displays the number of error packets.

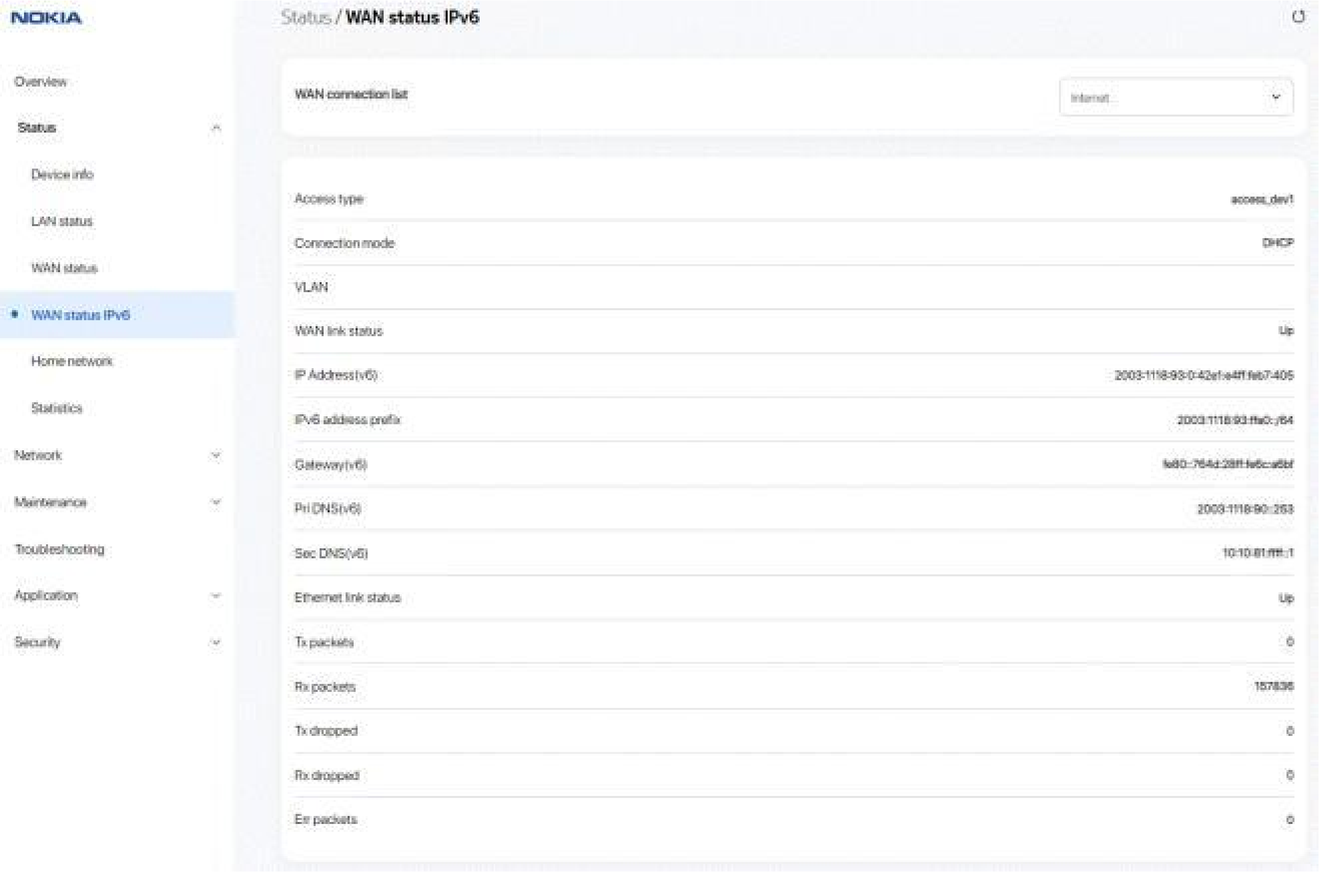
END OF STEPS

7.10 Viewing WAN IPv6 status

1

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

Figure 7-6 WAN status IPv6 page



Status / **WAN status IPv6**

WAN connection list: Internet...

Access type: access_dev1
Connection mode: DHCP
VLAN
WAN link status: Up
IP Address(v6): 2003:1118:93:0:42ef:e4ff:feb7:405
IPv6 address prefix: 2003:1118:93:ffa0::/64
Gateway(v6): fe80::764d:28ff:fe6c:a6bf
Pri DNS(v6): 2003:1118:90::253
Sec DNS(v6): 10:10:81:fff::1
Ethernet link status: Up
Tx packets: 0
Rx packets: 157836
Tx dropped: 0
Rx dropped: 0
Err packets: 0

Table 7-4 WAN status IPv6 parameters

Field	Description
WAN connection list	Select a WAN connection from the list. The details related to the connection are displayed.
Access type	Indicates the access type.
Connection mode	Indicates the mode of connection.
VLAN	Indicates the VLAN ID.
WAN link status	Indicates whether the WAN link is up or down.
IP Address (v6)	Indicates the IPv6 address that identifies the device and its location.
IPv6 address prefix	Indicates the IPv6 address prefix.
Gateway (v6)	Indicates the IPv6 gateway address.
Primary DNS (v6)	Indicates the Primary Domain Name Server.

Table 7-4 WAN status IPv6 parameters (continued)

Field	Description
Ethernet link status	Indicates whether the Ethernet link is up or down.
Tx packets	Indicates the number of packets transmitted on the WAN connection.
Rx packets	Indicates the number of packets received on the WAN connection.
Tx dropped	Indicates the number of transmitted packets dropped on the WAN connection.
Rx dropped	Indicates the number of received packets dropped on the WAN connection.
Err packets	Indicates the number of error packets on the WAN connection.

END OF STEPS

7.11 Viewing STA information

1

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

Figure 7-7 STA information page

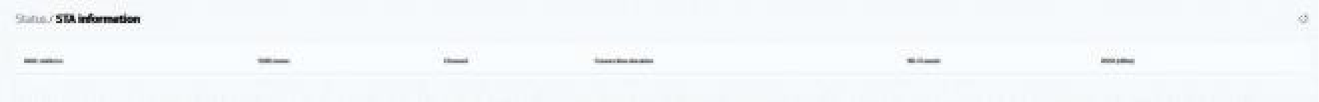


Table 7-5 STA information parameters

Field	Description
MAC address	Indicates the MAC address of the Ethernet connection.
SSID name	Indicates the name of each SSID.
Channel	Indicates the channel number.
Connection duration	Indicates the connection duration.
Wi-Fi mode	Indicates the Wi-Fi mode.
RSSI (dBm)	Indicates the received signal strength.

END OF STEPS

7.12 Viewing Neighboring Access Points

1

Click **Status→ Neighboring AP** in the left pane. The *Neighboring AP* page displays the following information.

Figure 7-8 Neighboring AP page

Table 7-6 Neighboring AP parameters

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

2

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

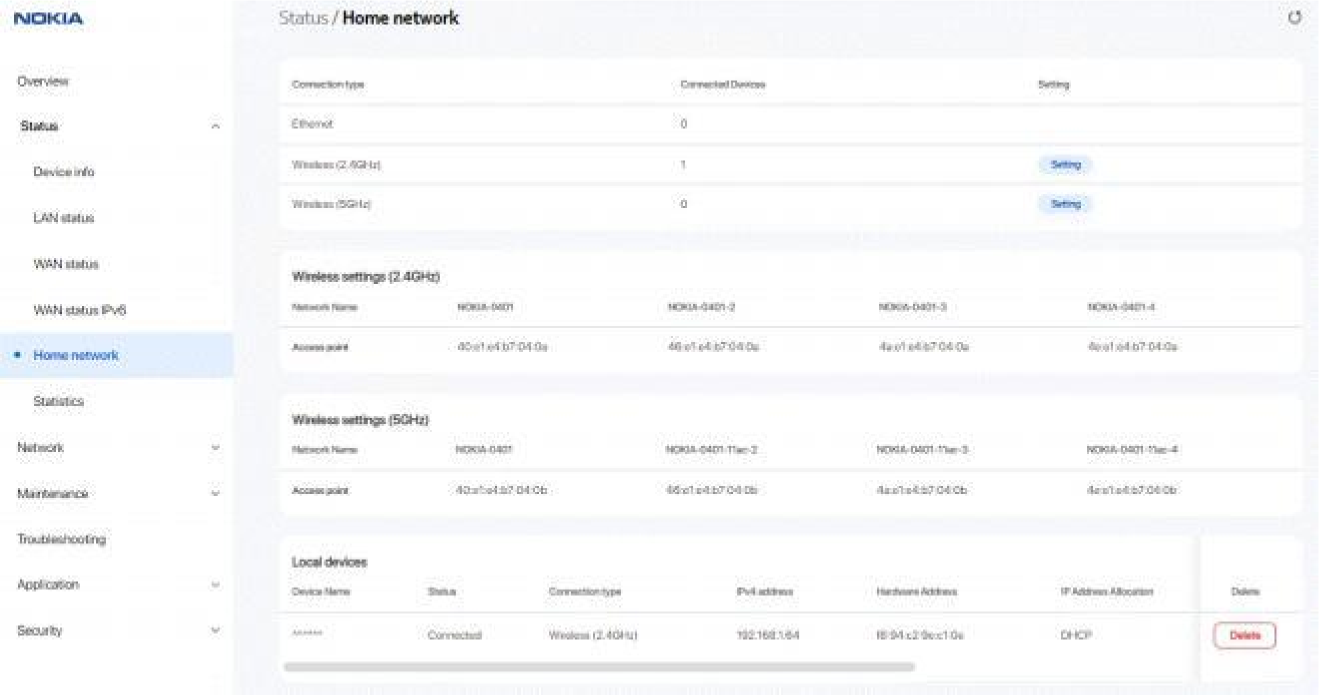
END OF STEPS

7.13 Viewing home network

1

Click **Status→ Home network** in the left pane. The *Home network* page displays the following information.

Figure 7-9   Home network page



Status / **Home network**

Connection type	Connected Devices	Setting
Ethernet	0	
Wireless (2.4GHz)	1	Setting
Wireless (5GHz)	0	Setting

Wireless settings (2.4GHz)

Network Name	NOKIA-0401	NOKIA-0401-2	NOKIA-0401-3	NOKIA-0401-4
Access point	40:c1:e4:b7:04:0a	46:c1:e4:b7:04:0a	4a:c1:e4:b7:04:0a	4e:c1:e4:b7:04:0a

Wireless settings (5GHz)

Network Name	NOKIA-0401	NOKIA-0401-11ac-2	NOKIA-0401-11ac-3	NOKIA-0401-11ac-4
Access point	40:c1:e4:b7:04:0b	46:c1:e4:b7:04:0b	4a:c1:e4:b7:04:0b	4e:c1:e4:b7:04:0b

Local devices

Device Name	Status	Connection type	IPv4 address	Hardware Address	IP Address Allocation	Delete
******	Connected	Wireless (2.4GHz)	192.168.1.64	f8:94:c2:9e:c1:0a	DHCP	Delete

Table 7-7   Home network parameters

Field	Description
Connection Type and Connected Devices	
Ethernet	Displays the number of Ethernet connections and their settings.
Wireless	Displays the number of wireless connections and their settings (2.4GHz and 5GHz).
Wireless settings (2.4GHz and 5GHz)	
Network Name	Name of the wireless network.
Access point	Hexadecimal address of the wireless access point.
Local devices A table indicating the status (active or inactive), connection type, device name, IP address, hardware address, IP address allocation, lease remaining, and last active time of each connected local device.	

END OF STEPS

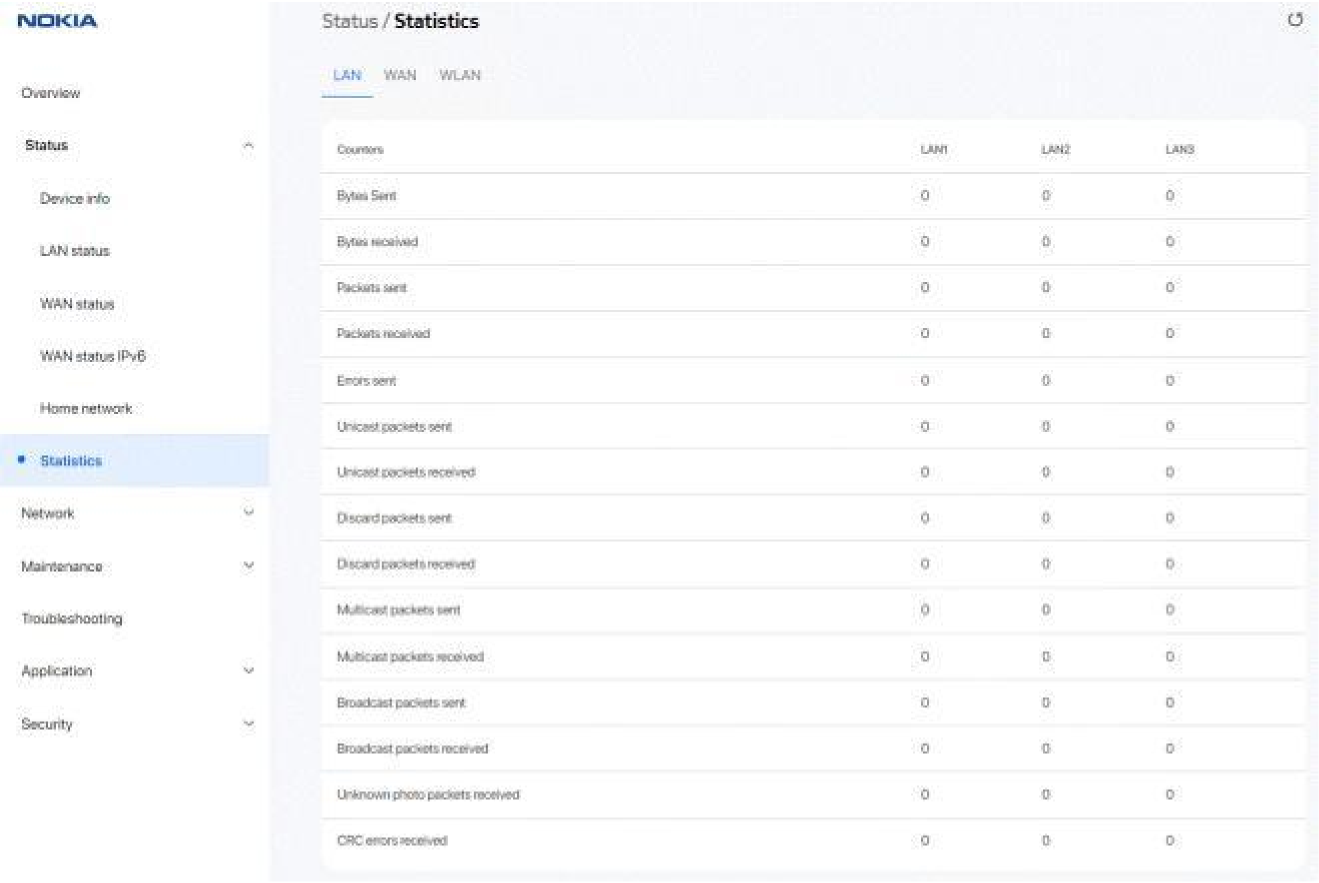
7.14 Viewing statistics

1

Click **Status→Statistics** in the left pane. The Statistics page displays the following information. Statistics are available for LAN ports, WAN ports, and WLAN ports.

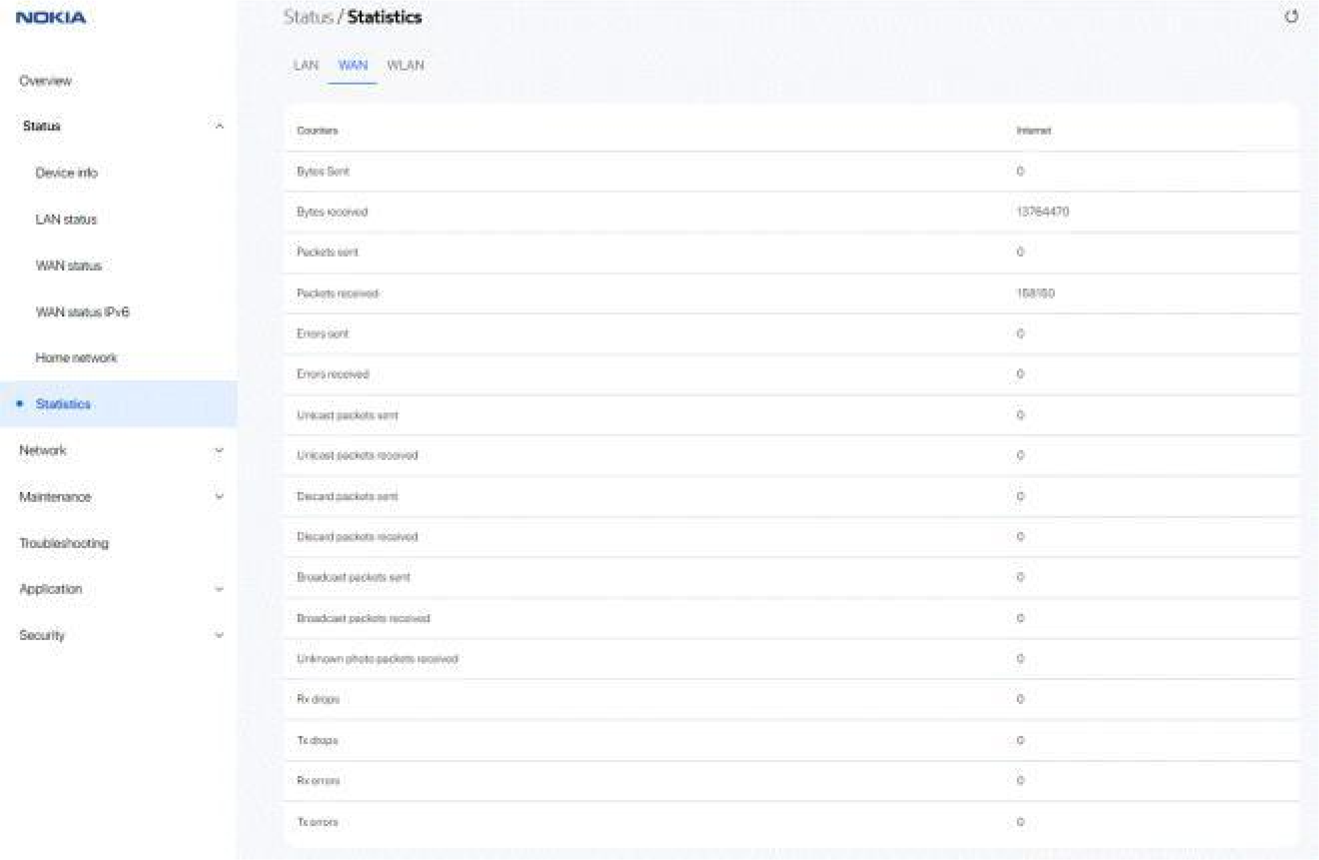
Select the **LAN** tab, **WAN** tab or **WLAN** tab to view the respective ports.

Figure 7-10 LAN Statistics page



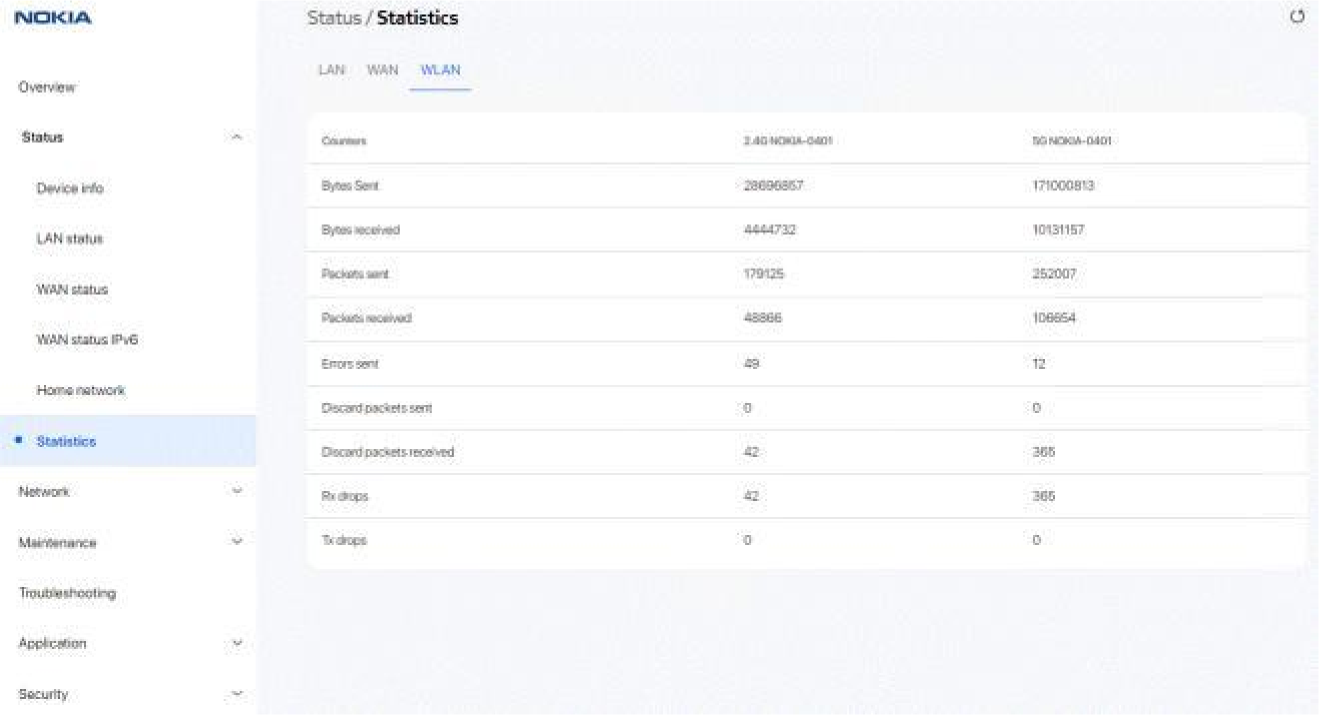
Counters	LAN1	LAN2	LAN3
Bytes Sent	0	0	0
Bytes received	0	0	0
Packets sent	0	0	0
Packets received	0	0	0
Errors sent	0	0	0
Unicast packets sent	0	0	0
Unicast packets received	0	0	0
Discard packets sent	0	0	0
Discard packets received	0	0	0
Multicast packets sent	0	0	0
Multicast packets received	0	0	0
Broadcast packets sent	0	0	0
Broadcast packets received	0	0	0
Unknown photo packets received	0	0	0
CRC errors received	0	0	0

Figure 7-11 WAN Statistics page



Counters	Internet
Bytes Sent	0
Bytes received	13764470
Packets sent	0
Packets received	158160
Errors sent	0
Errors received	0
Unicast packets sent	0
Unicast packets received	0
Discard packets sent	0
Discard packets received	0
Broadcast packets sent	0
Broadcast packets received	0
Unknown photo packets received	0
Rx drops	0
Tx drops	0
Rx errors	0
Tx errors	0

Figure 7-12 *WLAN Statistics* page



Counters	2.4G NOKIA-0401	5G NOKIA-0401
Bytes Sent	28696857	171000813
Bytes received	4444732	10131157
Packets sent	179125	252007
Packets received	48866	106654
Errors sent	49	12
Discard packets sent	0	0
Discard packets received	42	365
Rx drops	42	365
Tx drops	0	0

END OF STEPS

Network configuration

7.15 Overview

7.15.1 Purpose

This section describes the network configuration procedures supported by the Beacon G6 WebGUI.

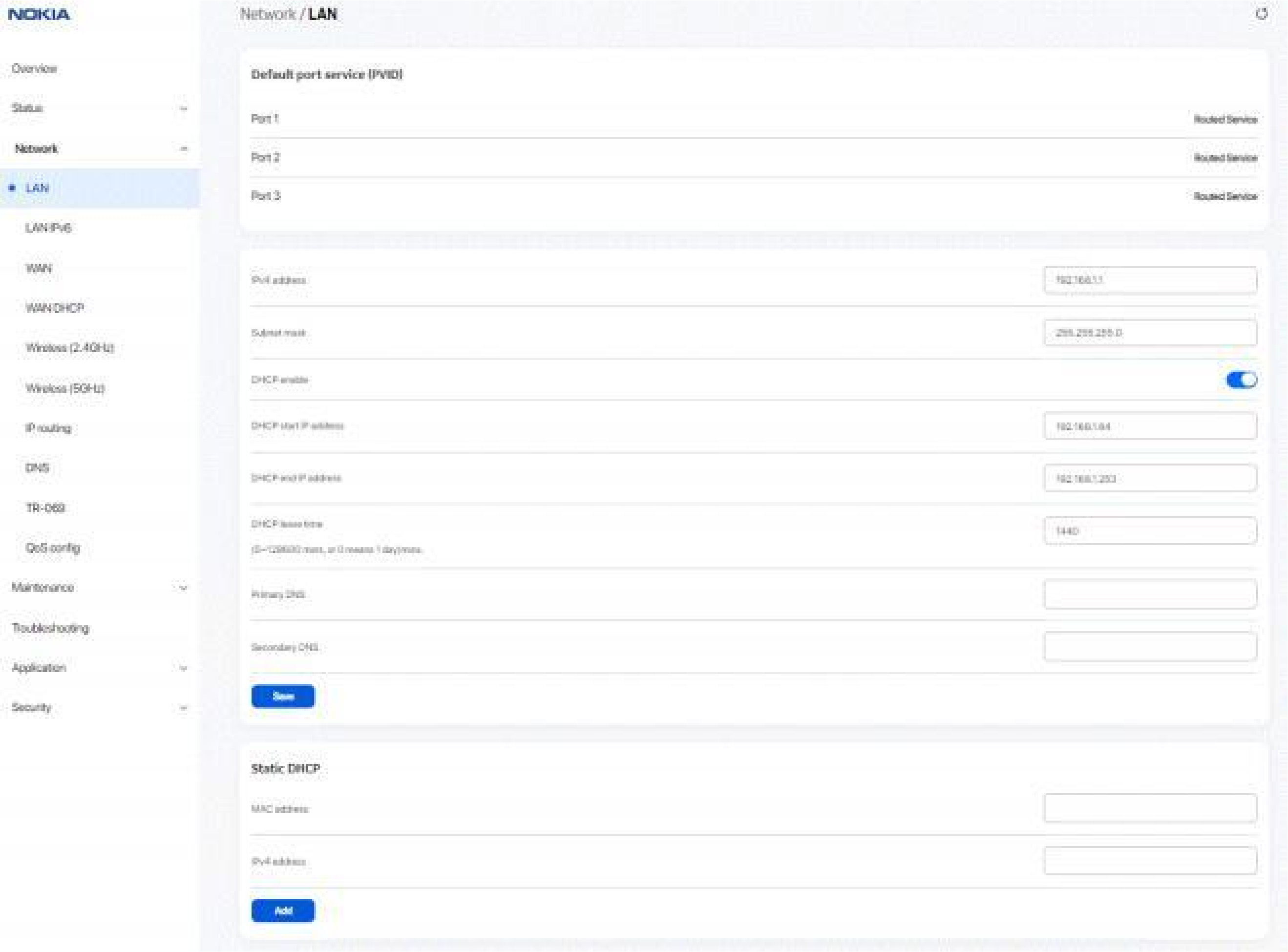
7.15.2 Contents

7.16 Configuring LAN

1

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

Figure 7-13 *LAN* page



Default port service (PVID)

Port 1: Routed Service
Port 2: Routed Service
Port 3: Routed Service

IPv4 address: 192.168.1.1
Subnet mask: 255.255.255.0
DHCP enable: on
DHCP start IP address: 192.168.1.64
DHCP end IP address: 192.168.1.253
DHCP lease time: 1440
(0~129600 mins, or 0 means 1 day)mins.
Primary DNS:
Secondary DNS:

Static DHCP

MAC address:
IPv4 address:

2

Configure the following LAN parameters:

Table 7-8 *LAN* parameters

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

Table 7-8 *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). Allowed values: 5 to 129600 minutes or 0 for 1 day
Primary DNS	Enter the primary DNS IP address.
Secondary DNS	Enter the secondary DNS IP address.

3

Click **Save**.

4

Configure the Static DHCP parameters.

Table 7-9 *Static DHCP* parameters

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

5

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

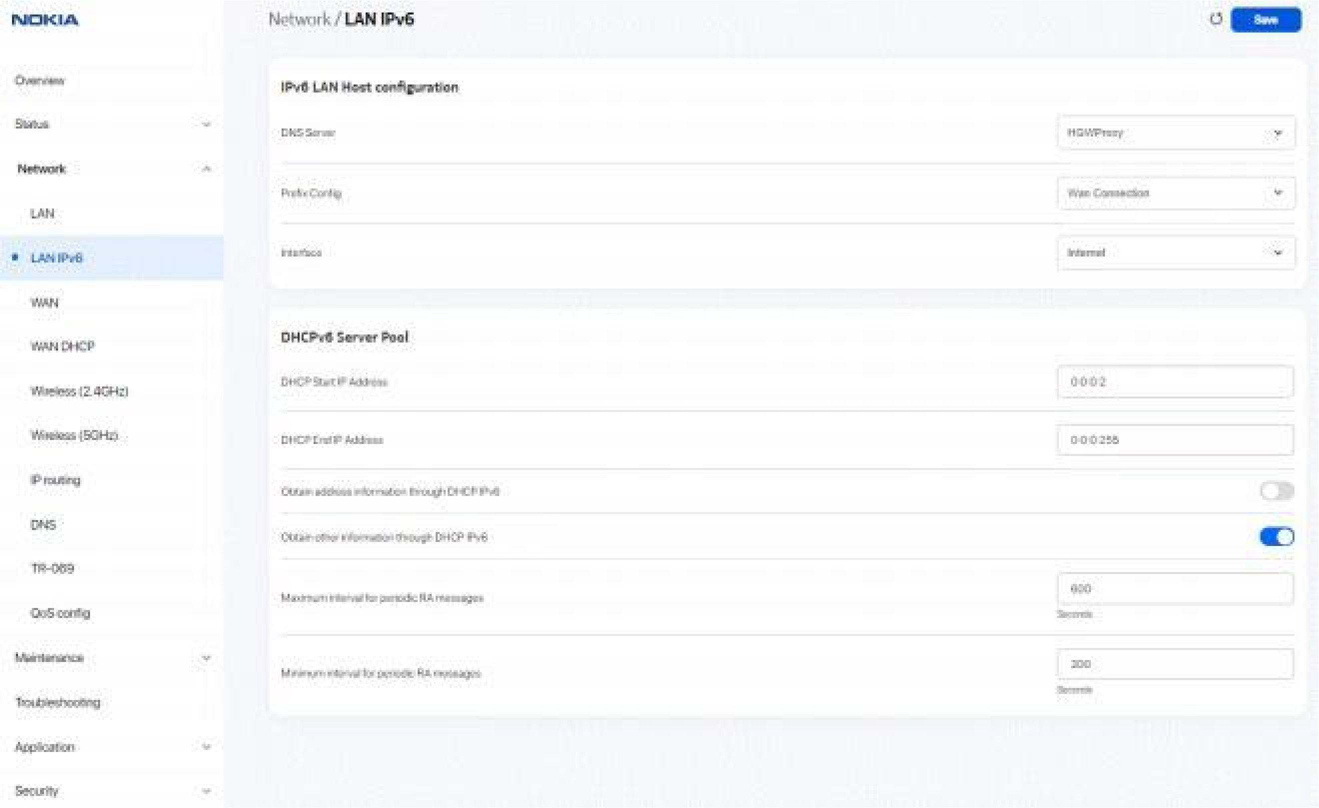
END OF STEPS

7.17 Configuring LAN IPv6

1

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

Figure 7-14 *LAN IPv6* page



Network / **LAN IPv6**

IPv6 LAN Host configuration

DNS Server: HGWProxy

Prefix Config: Wan Connection

Interface: Internet

DHCPv6 Server Pool

DHCP Start IP Address: 0:0:0:2

DHCP End IP Address: 0:0:0:255

Obtain address information through DHCP IPv6: ○

Obtain other information through DHCP IPv6: ●

Maximum interval for periodic RA messages: 600 Seconds

Minimum interval for periodic RA messages: 200 Seconds

2

Configure the following parameters:

Table 7-10 *LAN IPv6* parameters

Field	Description
IPv6 LAN Host Configuration	
DNS Server	Select a DNS server from the list.
Prefix Config	Select a prefix configuration option from the list: • **WAN Connection** (prefix is obtained from the WAN), or • **Static** (enables you to enter the prefix)
Interface	This field displays if you select the **WAN Connection** option from the Prefix Config list. Select a WAN connection interface from the list.
DHCPv6 Server Pool	
DHCP Start IP Address	Enter the starting range of the DHCP IP address.

Table 7-10 LAN IPv6 parameters (continued)

Field	Description
DHCP End IP Address	Enter the ending range of the DHCP IP address.
Obtain address information through DCHP IPv6	Select the toggle button to enable address information retrieval through DHCP.
Obtain other information through DHCP IPv6	Select the toggle button to enable retrieval of other information through DHCP.
Maximum interval for periodic RA messages	Enter the maximum interval (in seconds) for periodic Router Advertisement messages. Allowed values: 4 to 1800 seconds
Minimum interval for periodic RA messages	Enter the minimum interval (in seconds) for periodic Router Advertisement messages. Allowed values: 4 to 1800 seconds

3

Click **Save**.

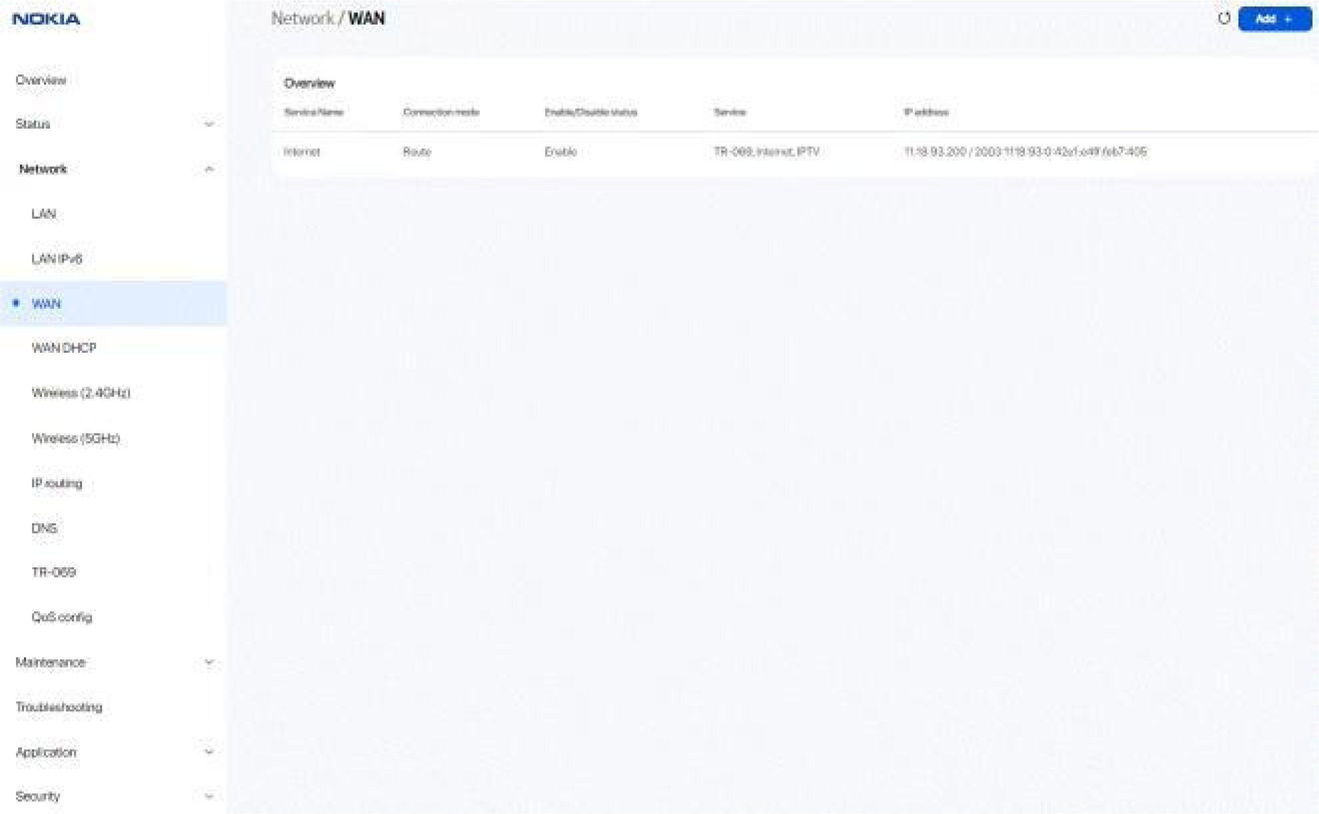
END OF STEPS

7.18 Configuring WAN

1

Click **Network→WAN** in the left pane. The *WAN* page displays the existing WAN connections in the *Overview* table. You can click on a connection to modify the connection configuration.

Figure 7-15 *Overview* table in *WAN* page



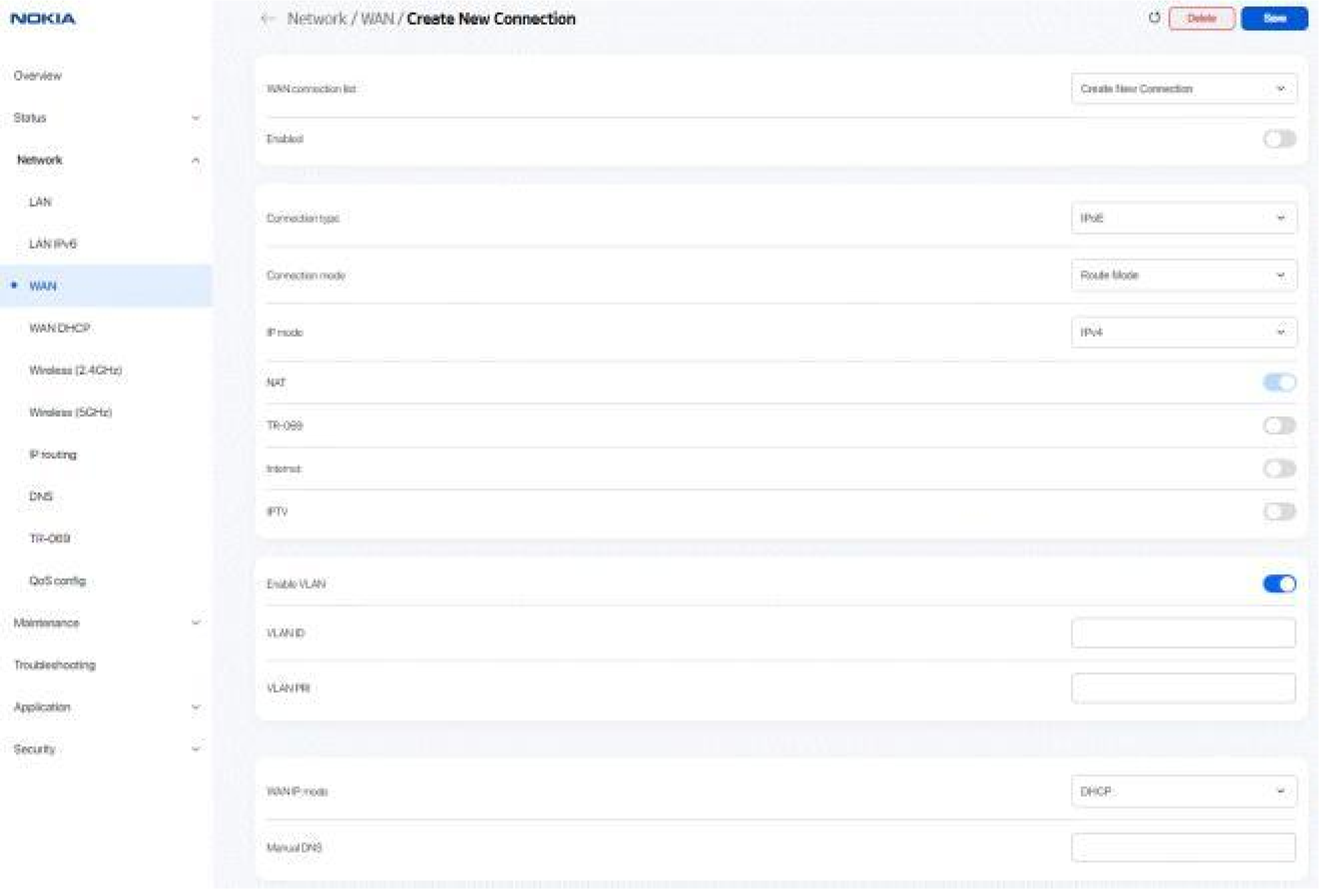
Overview

Service Name	Connection mode	Enable/Disable status	Service	IP address
Internet	Route	Enable	TR-069, Internet, IPTV	11.18.93.200 / 2003:1118:93:0:42a1:e4ff:feb7:405

2

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

Figure 7-16 *Create New Connection* page



Network / WAN / **Create New Connection**

WAN connection list: Create New Connection
Enabled: ○
Connection type: IPoE
Connection mode: Route Mode
IP mode: IPv4
NAT: ●
TR-069: ○
Internet: ○
IPTV: ○
Enable VLAN: ●
VLAN ID:
VLAN PRI:
WAN IP mode: DHCP
Manual DNS:

3

Configure the following parameters:

Table 7-11 *WAN* parameters

Field	Description
WAN connection list	Select a WAN connection from the list.
Enabled	Select the toggle button to enable the WAN connection.
Connection type	Select a connection type from the list: • **IPoE** • **PPPoE**

Table 7-11 *WAN* parameters (continued)

Field	Description
Connection mode	Select the connection mode of the WAN connection from the list: • **Route Mode** • **Bridge Mode**
IP mode	This field is applicable only if the connection mode is **Route Mode**. Select an IP mode from the list: • **IPv4** • **IPv4 & IPv6** • **IPv6** When the IP mode **IPv4 & IPv6** or **IPv6** is selected, you need to configure **Address method**, **Enabled prefix delegation** and **Prefix type**.
NAT	Select the toggle button to enable NAT. This option is applicable only if the connection mode is **Route Mode**.
TR-069	Select the toggle button to enable TR-069. This option is applicable only if the connection mode is **Route Mode**.
VOIP	Select the toggle button to enable VoIP. This option is applicable only if the connection type is **IPoE** and the connection mode is **Route Mode**.
Internet	Select the toggle button to enable Internet. This option is applicable only if the connection mode is **Route Mode**.
IPTV	Select the toggle button to enable IPTV.
Enable VLAN	Select the toggle button to enable VLAN. This option is applicable only if the connection mode is **Route Mode**.
VLAN mode	Select a VLAN mode from the list: • **VLAN binding** • **Tunnel** • **Transparent** This option is applicable only if the connection mode is **Bridge Mode**.
VLAN ID	Enter the VLAN ID. Allowed values: 2 to 4094 In the bridge mode, this option is applicable only if the VLAN mode is **Tunnel** or **VLAN binding**.
VLAN PRI	Enter the VLAN PRI. VLAN priority allows to assign a priority to outbound packets containing the specified VLAN ID. Allowed values: 0 to 7 In the bridge mode, this option is applicable only if the VLAN mode is **VLAN binding**.
LAN port binding	Select the toggle button next to the LAN to enable it. Select the toggle button next to the PVID to enable it. This option is not applicable if the VLAN mode is **Tunnel** or **Transparent**.

Table 7-11 *WAN* parameters (continued)

Field	Description
SSID port binding	Select the toggle button next to the SSID to enable it. Select the toggle button next to the PVID to enable it. This option is not applicable if the VLAN mode is **Tunnel** or **Transparent**.
WAN IP mode	Select an IP mode from the list: • **DHCP** • **PPPoE** • **Static**
Manual DNS	If the selected IP mode is **IPv4** and the WAN IP mode is **DHCP**, enter the Domain Name Server (DNS) to be configured manually.
IPv4 Address	If the selected IP mode is **IPv4** or **IPv4&IPv6** and the WAN IP mode is **Static**, enter the static IPv4 address.
Netmask	If the selected IP mode is **IPv4** or **IPv4&IPv6** and the WAN IP mode is **Static**, enter the netmask.
Gateway	If the selected IP mode is **IPv4** or **IPv4&IPv6** and the WAN IP mode is **Static**, enter the gateway IP address.
Pri DNS	If the selected IP mode is **IPv4** or **IPv4&IPv6** and the WAN IP mode is **Static**, enter the primary Domain Name Server (DNS).
Sec DNS	If the selected IP mode is **IPv4** or **IPv4&IPv6** and the WAN IP mode is **Static**, enter the secondary Domain Name Server (DNS).
Ter DNS	If the selected IP mode is **IPv4** or **IPv4&IPv6** and the WAN IP mode is **Static**, enter the tertiary Domain Name Server (DNS).
Connection trigger	Select the connection trigger type from the list. The default option is **Always On**.
Username	Enter the username to log in to the configuration server. This option is applicable only if the WAN IP mode is **PPPoE**.
Password	Enter the password to log in to the configuration server. Allowed values are limited to numbers, letters and special characters ! # + , - . / : = @ _. This option is applicable only if the WAN IP mode is **PPPoE**.
Keep alive time	The PPPoE connection type triggers one heartbeat each, at the configured time interval to keep the session online. Allowed values: 5 to 60 seconds This option is applicable only if the WAN IP mode is **PPPoE**.
Keep alive retry	Configure the number of retries to check the Keep Alive status of the PPPoE session after time-out. Allowed values: 1 to 10. This option is applicable only if the WAN IP mode is **PPPoE**.
Echo value	Indicates the number of times the device sends messages to the server to check if the IP address is available or not. This option is applicable only if the WAN IP mode is **PPPoE**.

Table 7-11 *WAN* parameters (continued)

Field	Description
Address method	If the selected IP mode is **IPv4** or **IPv4&IPv6**, select the address method from the list: • **AutoConfigured** • **DHCPv6** • **DHCPv6_PD** • **DHCPv6_NA** • **Static**
Enable prefix delegation	If the selected address method is **AutoConfigured**, select the toggle button to enable inclusion of the Identity Association (IA) for Prefix Delegation option in Solicit messages.
Prefix type	Displays mechanism through which the prefix was assigned or most recently updated.
IP Address (v6)	If the selected address method is **Static**, enter the IPv6 address.
Gateway (v6)	If the selected address method is **Static**, enter the gateway IPv6 address.
IPv6 address prefix	If the selected address method is **Static**, enter the IPv6 address prefix.
Pri DNS (v6)	If the selected address method is **Static**, enter the primary DNS IP address.
Sec DNS (v6)	If the selected address method is **Static**, enter the secondary DNS IP address.

4

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

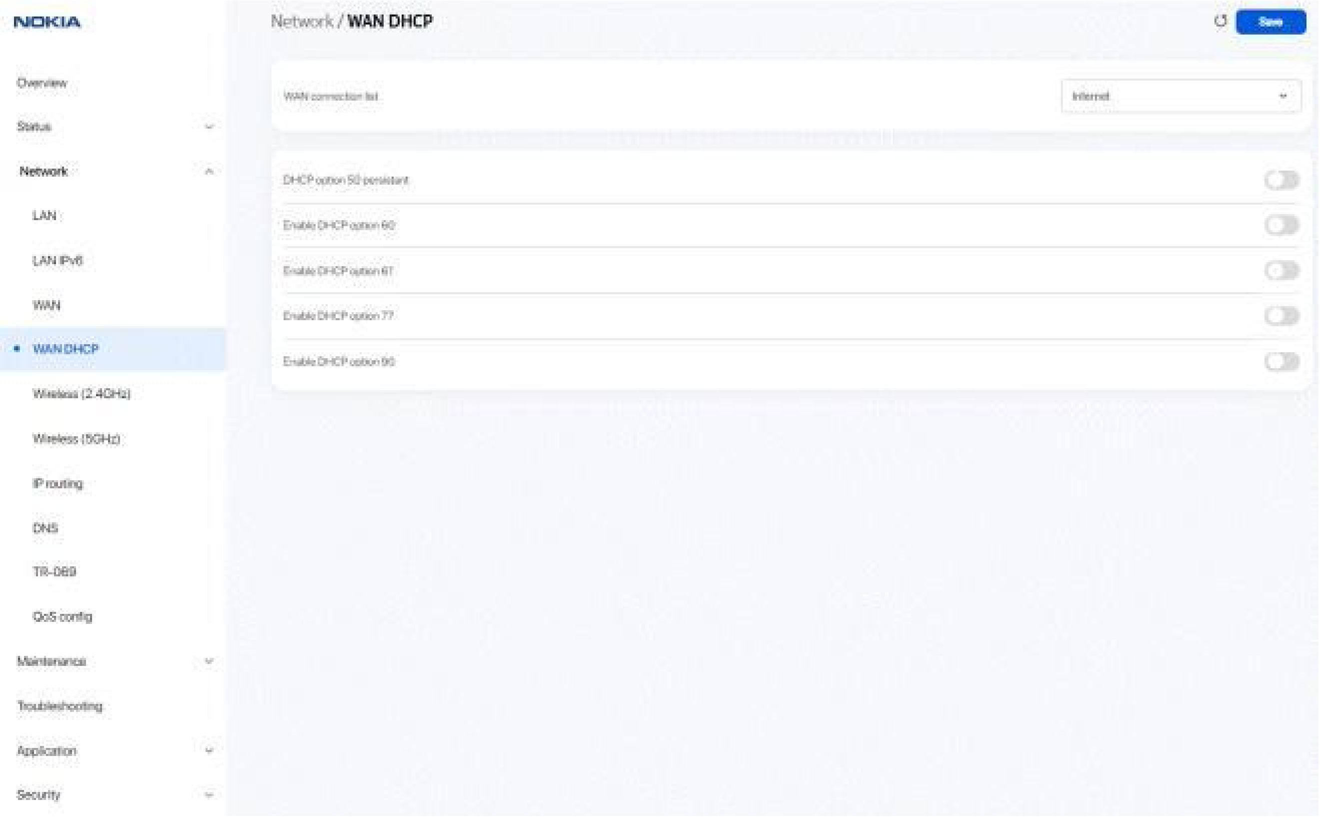
END OF STEPS

7.19 Configuring WAN DHCP

1

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

Figure 7-17 *WAN DHCP* page



WAN connection list: Internet

DHCP option 50 persistent

Enable DHCP option 60

Enable DHCP option 61

Enable DHCP option 77

Enable DHCP option 90

2

Configure the following parameters:

Table 7-12 *WAN DHCP* parameters

Field	Description
WAN connection list	Select a WAN connection from the list.
DHCP option 50 persistent	Select the toggle button to enable DHCP Option 50 persistent.
Enable DHCP option 60	Select the toggle button to enable DHCP Option 60 (vendor class identifier).
Enable DHCP option 61	Select the toggle button to enable DHCP Option 61 (client identifier).
Enable DHCP option 77	Select the toggle button to enable DHCP Option 77 (user class information).
Enable DHCP option 90	Select the toggle button to enable DHCP Option 90 (authentication information).

3

Click **Save**.

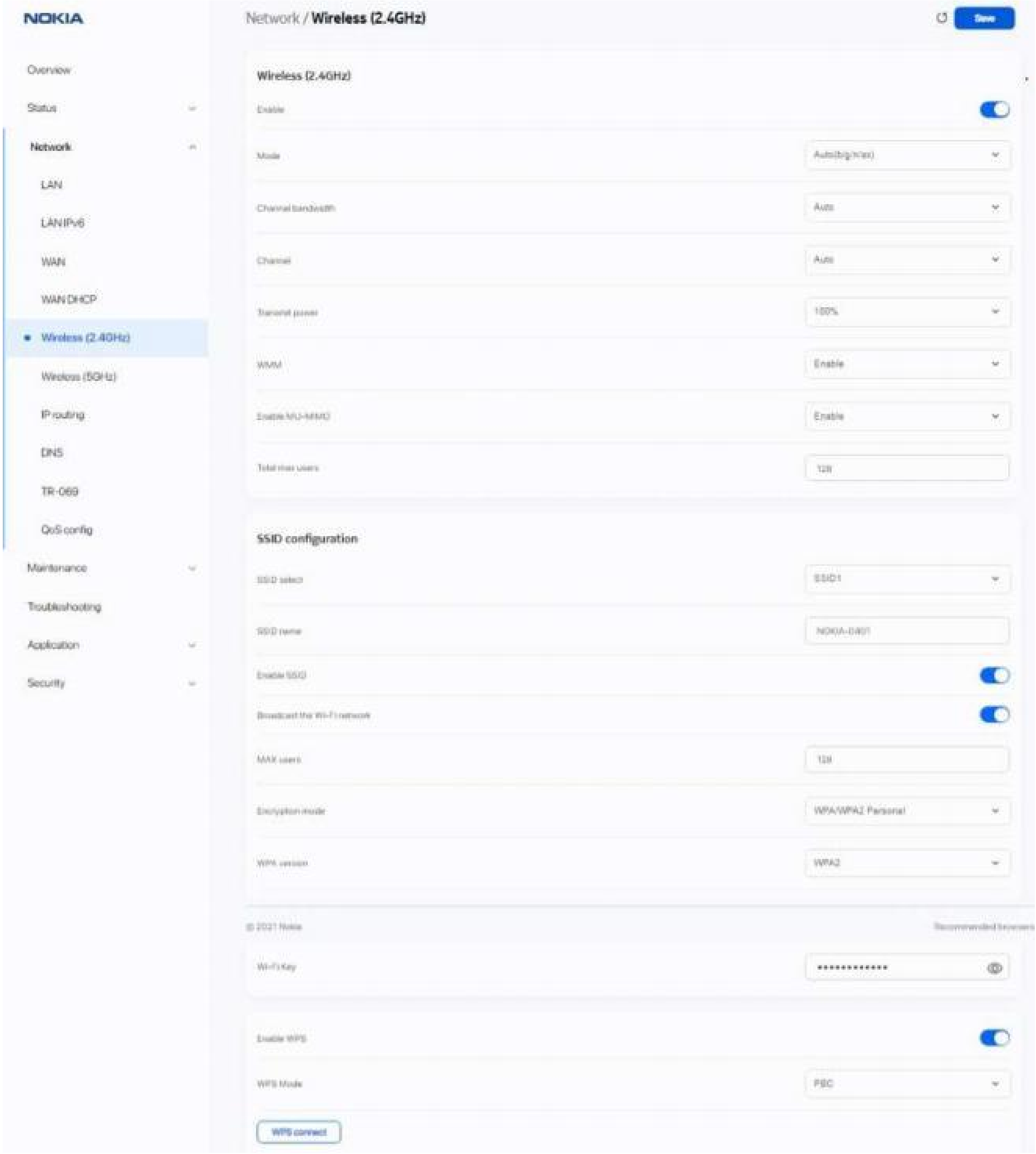
END OF STEPS

7.20 Configuring wireless 2.4 GHz

1

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

Figure 7-18 Wireless (2.4GHz) page



Network / **Wireless (2.4GHz)**

Wireless (2.4GHz)

Enable	●
Mode	Auto(b/g/n/ax)
Channel bandwidth	Auto
Channel	Auto
Transmit power	100%
WMM	Enable
Enable MU-MIMO	Enable
Total max users	128

SSID configuration

SSID select	SSID1
SSID name	NOKIA-D401
Enable SSID	●
Broadcast the Wi-Fi network	●
MAX users	128
Encryption mode	WPA/WPA2 Personal
WPA version	WPA2

© 2021 Nokia

Wi-Fi Key	•••••••••••••
Enable WPS	●
WPS Mode	PBC

2

Configure the following parameters:

Table 7-13 *Wireless (2.4GHz)* parameters

Field	Description
Enable	Select the toggle button to enable Wireless (2.4 GHz).
Mode	Select a wireless mode from the list: • **Auto (b/g/n/ac/ax)** • **Auto (b/g/n/ax)** • **b/g/n** • **b** • **g** • **n** • **b/g** • **g/n** • **n/g** • **ax/g**
Bandwidth	Select the bandwidth range from the list: • **Auto** (auto-assigns the bandwidth range) • **20 MHz** • **40 MHz** • **20/40 MHz**
Channel	Select a channel from the list or select **Auto** to auto-assign the channel.
Transmitting Power	Select a percentage for the transmitting power from the list: • **25%** • **50%** • **75%** • **100%**
WMM	Select an option from the list to enable or disable wireless multimedia: • **Enable** • **Disable**
Enable MU-MIMO	Select an option from the list to enable or disable MU-MIMO: • **Enable** • **Disable**
Total max users	Enter the maximum number of users.
SSID Configuration	
SSID select	Select an SSID from the list.

Table 7-13 Wireless (2.4GHz) parameters (continued)

Field	Description
SSID name	Enter the SSID name.
Enable SSID	Select the toggle button to enable SSID.
SSID broadcast	Select the toggle button to enable SSID broadcast.
MAX users	Enter the maximum number of users.
Encryption Mode	Select an encryption mode from the list: • **WPA/WPA2 Personal** • **WPA3 Personal** • **WPA2/WPA3 Personal** • **WPA/WPA2 Enterprise** • **WEP** • **OPEN**
WPA version	Select a WPA version from the list: • **WPA2** • **WPA/WPA2**
WPA Encryption Mode	Select a WPA encryption mode from the list: • **TKIP** • **AES** • **TKIP/AES**
Wi-Fi Key	Enter the Wi-Fi key.
Enable WPS	Select the toggle button to enable WPS .
Domain Grouping	Select the toggle button to enable domain grouping.

3

If you have enabled and configured WPS, click **WPS connect**. The *WPS success* message displays.

4

Click **Save**.

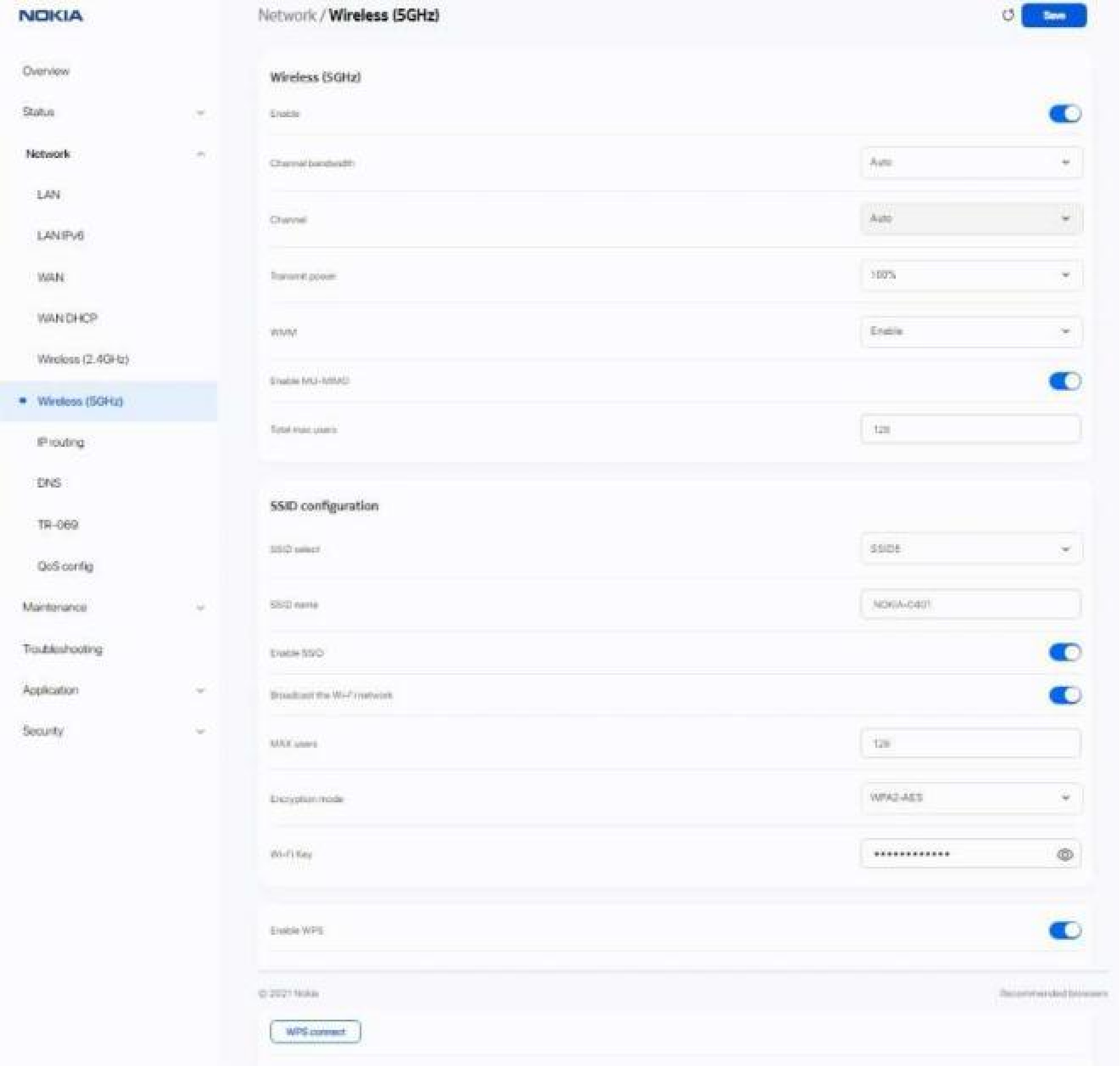
END OF STEPS

7.21 Configuring wireless 5GHz

1

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

Figure 7-19 Wireless (5GHz) page



Wireless (5GHz)

Enable	●
Channel bandwidth	Auto
Channel	Auto
Transmit power	100%
WMM	Enable
Enable MU-MIMO	●
Total max users	128

SSID configuration

SSID select	SSID5
SSID name	NOKIA-C401
Enable SSID	●
Broadcast the Wi-Fi network	●
MAX users	128
Encryption mode	WPA2-AES
Wi-Fi Key	*************
Enable WPS	●

2

Configure the following parameters:

Table 7-14 Wireless (5GHz) parameters

Field	Description
Enable	Select this toggle button to enable WiFi.
Bandwidth	Select the bandwidth range from the list: • **20 MHz** • **40 MHz** • **80 MHz** • **Auto**
Channel	Select a channel from the list or select **Auto** to auto-assign the channel.
Transmitting power	Select a percentage for the transmitting power from the list: • **25%** • **50%** • **75%** • **100%**
WMM	Select **Enable** or **Disable** from the list to enable or disable WiFi multimedia.
Enable MU-MIMO	Select the toggle button to enable MU-MMO. 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 total number of MAX users. The maximum users allowed is 128.
DFS Re-entry	Click to enable or disable DFS Re-entry.
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	Enter the SSID name.
Enable SSID	Select **Enable** or **Disable** from this list.
SSID Broadcast	Select **Enable** or **Disable** SSID broadcast from this list.
Port Mode	Select a port mode from the list. The default value is Route.
Isolation	Select the toggle button to enable Isolation.
MAX Users	Enter the number of MAX users.

Table 7-14 Wireless (5GHz) parameters (continued)

Field	Description
Encryption Mode	Select an encryption mode from the list: • **None** • **OPEN** • **WPA/WPA2 Enterprise** • **WPA2-AES** • **WPA2+WPA** • **WPA3** • **WPA3+WPA2** • **WPA3-AES** • **WPA2+WPA3-AES** • **WPA** • **WPA2-Enterprise**
WPA Key	Enter the WPA key.
Enable WPS	Select the toggle button to enable WPS.
WPS Mode	Select the required WPS mode from the list: • **PBC** • **STA PIN** • **AP PIN**
Domain Grouping	Select the toggle button to enable domain grouping.

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.

3

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

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

4

Click **Save**.

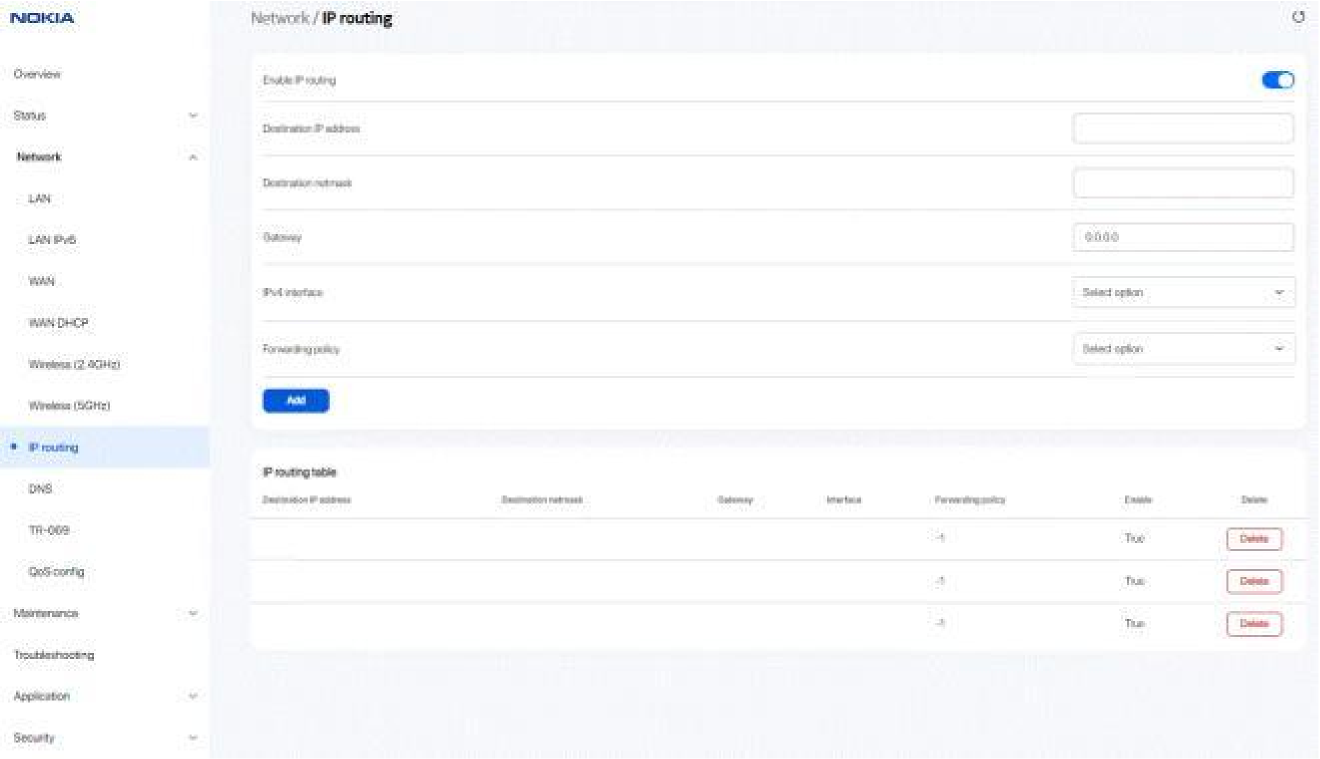
END OF STEPS

7.22 Configuring IP routing

1

Click **Network→ IP routing** in the left pane. The *IP routing* page displays.

Figure 7-20 *IP routing* page



Enable IP routing	●
Destination IP address	
Destination netmask	
Gateway	0.0.0.0
IPv4 interface	Select option
Forwarding policy	Select option

IP routing table

Destination IP address	Destination netmask	Gateway	Interface	Forwarding policy	Enable	Delete
				-1	True	Delete
				-1	True	Delete
				-1	True	Delete

2

Configure the following parameters:

Table 7-15 *IP routing* parameters

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

Table 7-15 *IP routing* parameters (continued)

Field	Description
Forwarding policy	Select a forwarding policy from the list:

3

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

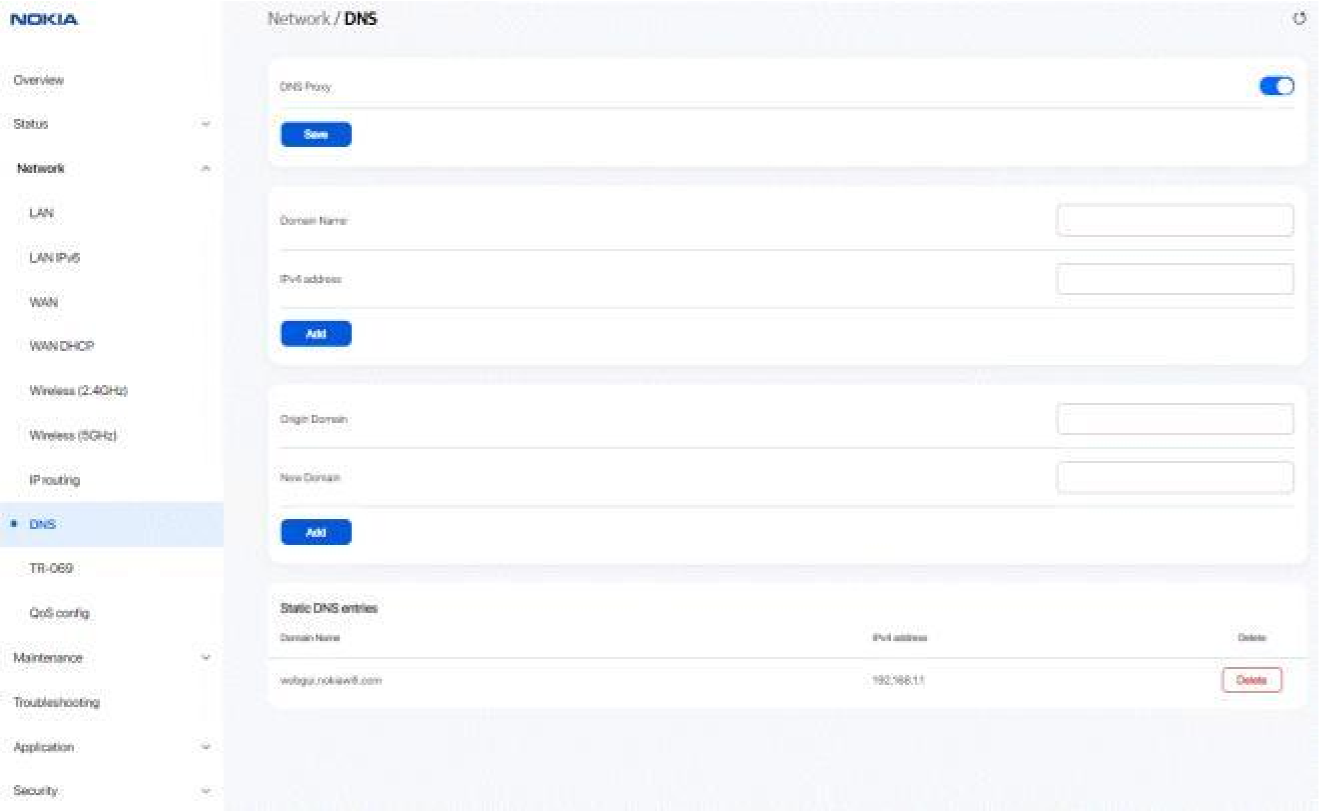
END OF STEPS

7.23 Configuring DNS

1

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

Figure 7-21 *DNS* page



Static DNS entries

Domain Name	IPv4 address	Delete
webgui.nokiawifi.com	192.168.1.1	Delete

2

Configure the following parameters:

a. Select the **DNS proxy** toggle button to enable the DNS proxy and click **Save**.

b. Configure the following:

1. Enter the domain name in the Domain Name field
2. Enter the domain IP address in the IPv4 address field.
3. Click **Add**.

c. Configure the following:

1. Enter the origin domain name in the Origin Domain field
2. Enter the new domain name in the New Domain field.
3. Click **Add** to associate an origin domain with a new domain.

The *Static DNS entries* table displays the configured domain names and the associated IPv4 address.

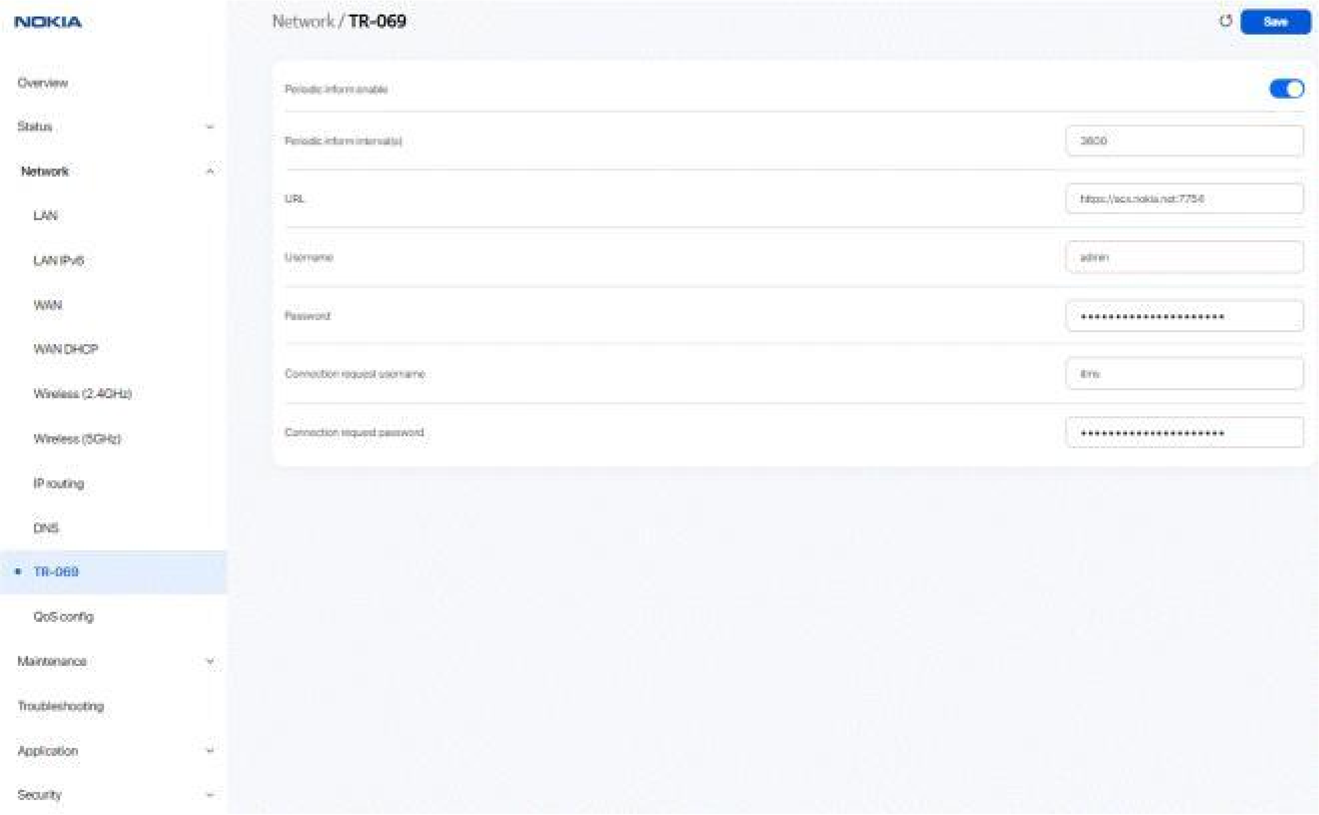
END OF STEPS

7.24 Configuring TR-069

1

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

Figure 7-22 *TR-069* page



Network / **TR-069**

Periodic inform enable

Periodic inform interval(s) 3600

URL https://acs.nokia.net:7754

Username admin

Password ••••••••••••••••••••••

Connection request username itms

Connection request password ••••••••••••••••••••••

2

Configure the following parameters:

Table 7-16 *TR-069* parameters

Field	Description
Periodic inform enable	Select the toggle button to enable periodic inform updates.
Periodic inform interval(s)	Enter the time between periodic inform updates, in seconds.
URL	Enter the URL of the auto-configuration server.
Username	Enter the username to log in to the Beacon.
Password	Enter the password to log in to the Beacon.
Connect request username	Enter the username to log in to the auto-configuration server.
Connect request password	Enter the password to log in to the auto-configuration server.

3

Click **Save**.

END OF STEPS

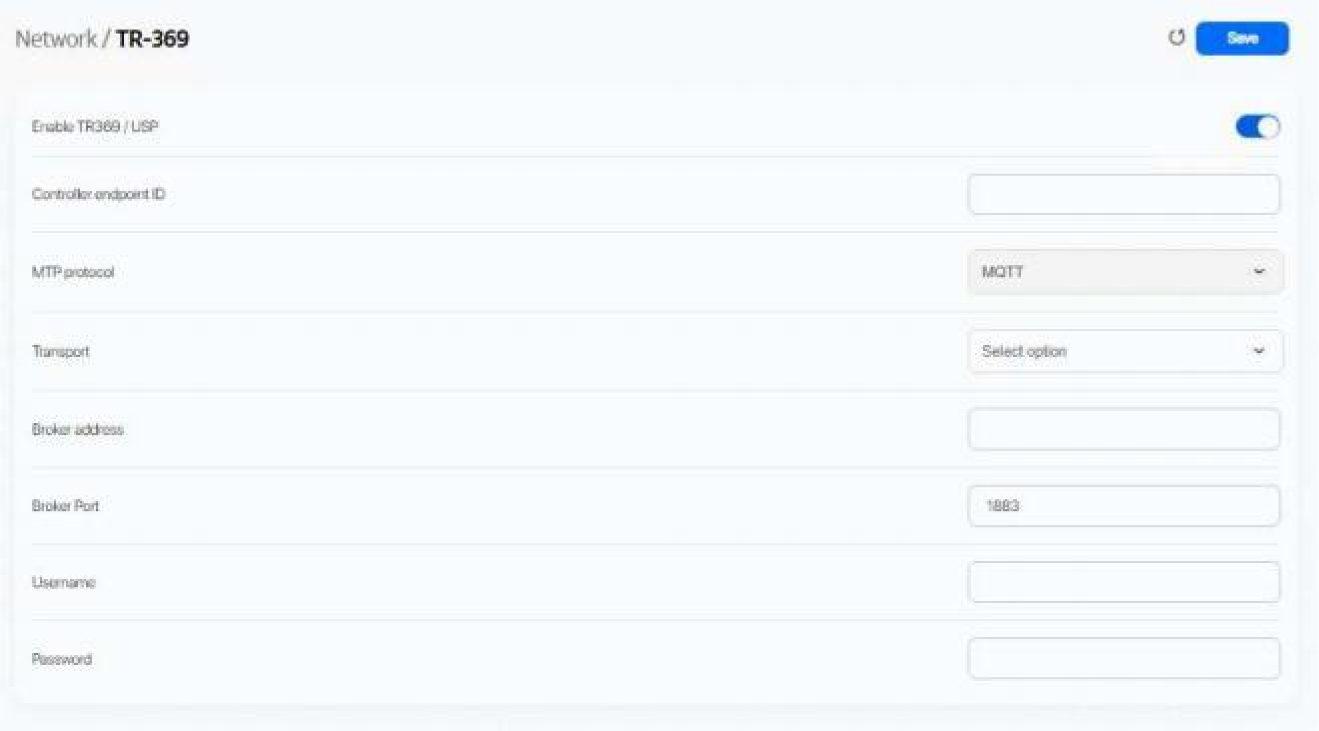
7.25 Configuring TR-369

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

1

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

Figure 7-23 *TR-369* page



Enable TR369 / USP
Controller endpoint ID
MTP protocol: MQTT
Transport: Select option
Broker address
Broker Port: 1883
Username
Password

2

Configure the following parameters:

Table 7-17 *TR-369* parameters

Field	Description
Enable TR369/USP	Select the toggle button to enable TR-369/USP and click **Save**.

Table 7-17 *TR-369* parameters (continued)

Field	Description
Controller endpoint ID	Enter the controller endpoint ID.
MTP Protocol	Select the MTP protocol from the list (currently only **MQTT** is supported).
Transport	Select the transport option from the list: • **TCP/IP** • **TLS**
Broker address	Enter the broker IP address.
Broker port	Enter the broker port number.
Username	Enter the username to authenticate with MQTT broker.
Password	Enter the password to authenticate with MQTT broker.

3

Click **Save**.

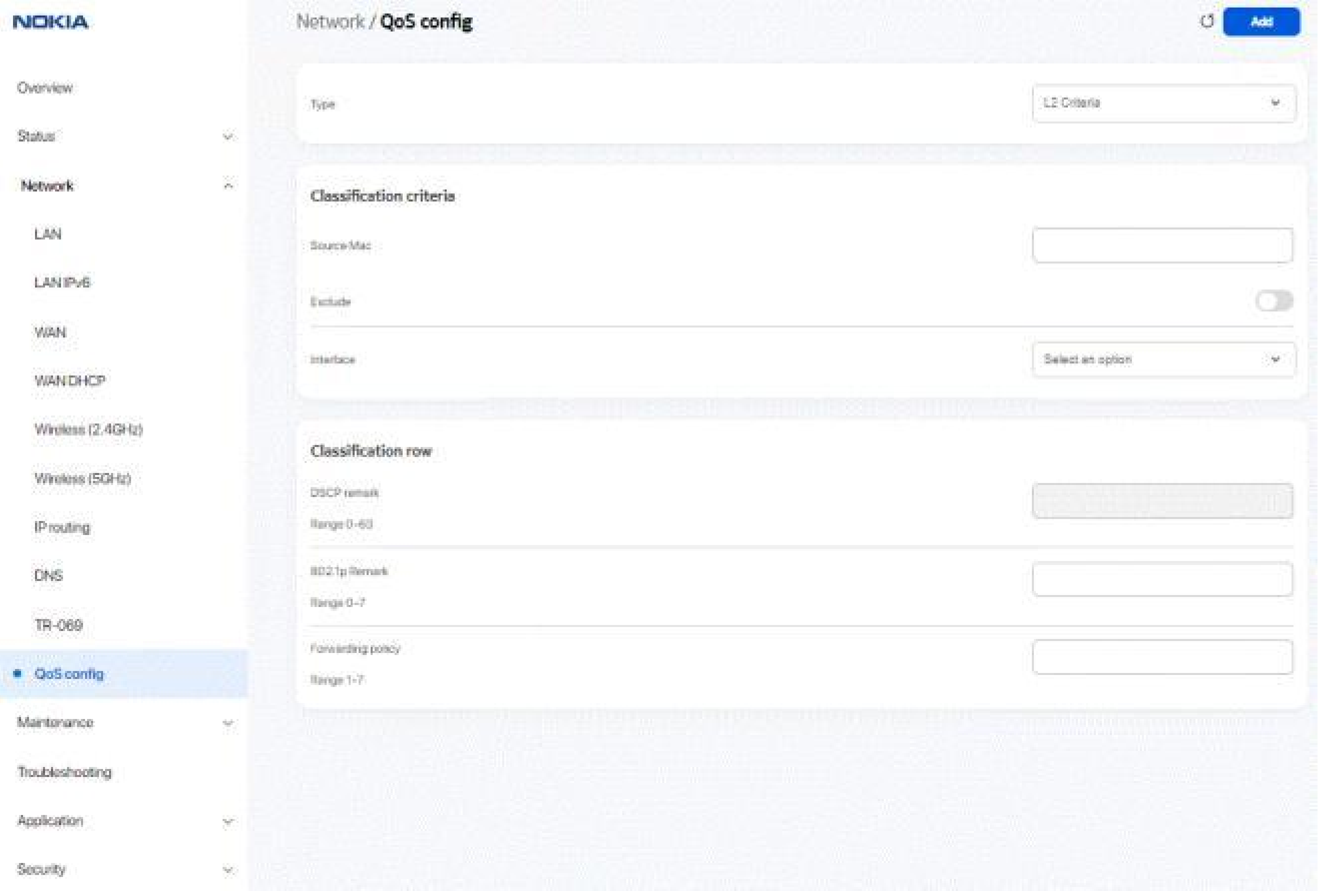
END OF STEPS

7.26 Configuring QoS

1

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

Figure 7-24 *QoS config* page (L2 Criteria)



Network / **QoS config**

Type: L2 Criteria

Classification criteria

Source Mac

Exclude

Interface: Select an option

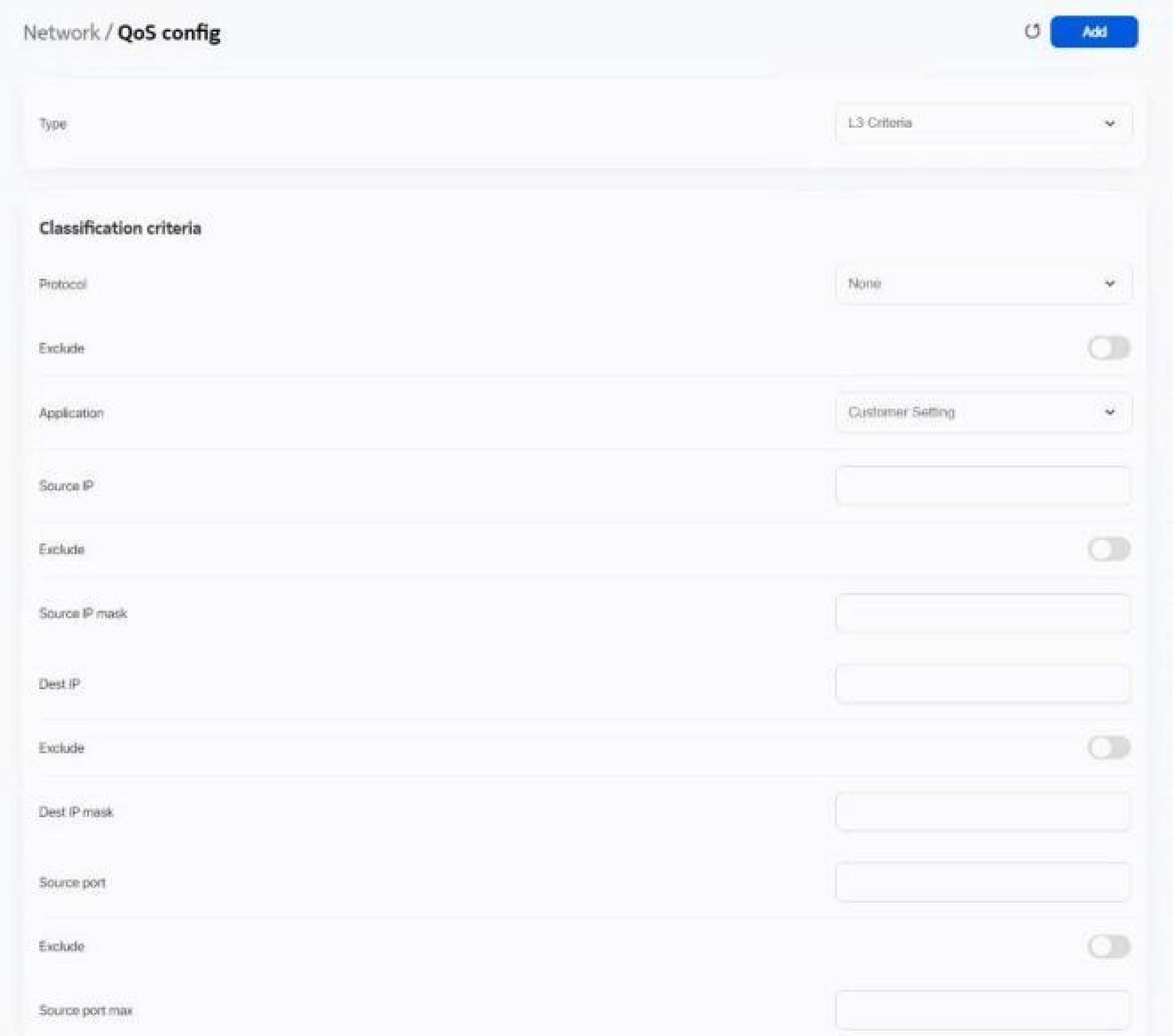
Classification row

DSCP remark
Range 0-63

802.1p Remark
Range 0–7

Forwarding policy
Range 1-7

Figure 7-25 *QoS config* page (L3 Criteria)



Network / **QoS config**

Type: L3 Criteria

Classification criteria

Protocol: None

Exclude

Application: Customer Setting

Source IP

Exclude

Source IP mask

Dest IP

Exclude

Dest IP mask

Source port

Exclude

Source port max

2

Configure the following parameters:

Table 7-18 *QoS config* parameters

Field	Description
Type	Select a QoS service layer type from the list: • **L2 Criteria** • **L3 Criteria**
Classification criteria (L2)	
Source MAC	Enter the source MAC address.
Exclude	Select the toggle button to exclude the source MAC address.
Interface	Select an interface from the list.
Classification criteria (L3)	
Protocol	Select a protocol from the list.
Exclude	Select the toggle button to exclude the protocol.
Application	Select an application from the list or select **Custom Settings** and enter an application name.
Source IP	Enter the source IP address.
Exclude	Select the toggle button to exclude the source IP address.
Source IP mask	Enter the source IP address netmask.
Destination IP	Enter the destination IP address.
Exclude	Select the toggle button to exclude the destination IP address.
Destination IP mask	Enter the destination IP address netmask.
Source port	Enter the source port number.
Exclude	Select the toggle button to exclude the source port.
Source port max	Enter the values for the source port max (highest port number)
Destination port	Enter the destination port number.
Exclude	Select the toggle button to exclude the destination port.
Destination port max	Enter the values for the destination port max (highest port number)
Classification row	
DSCP remark	Enter the value for the DSCP remark (applicable only for L3 criteria). Allowed values: 0 to 63
802.1p Remark	Enter the value for the 802.1p remark. Allowed values: 0 to 7
Forwarding policy	Enter the number for the forwarding policy. Allowed values: 1 to 7

3

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

END OF STEPS

7.27 Configuring Upstream (US) Classifier

The US Classifier feature is used to create policies, classifiers, and classifier rules for upstream traffic handling. This feature is available to admin users (super users) only.

A policy defines an action to be performed on a set of LAN or WAN packets. A policy can be created at any time and then subsequently assigned to one or more classifiers.

A classifier is used to select key fields for which the classifier rules will be written. A classifier can be created at any time and then subsequently assigned to one or more classifier rules.

A classifier rule is used to assign actions to a group of packets based on a set of parameters. A classification rule must be created against a pre-defined classifier.

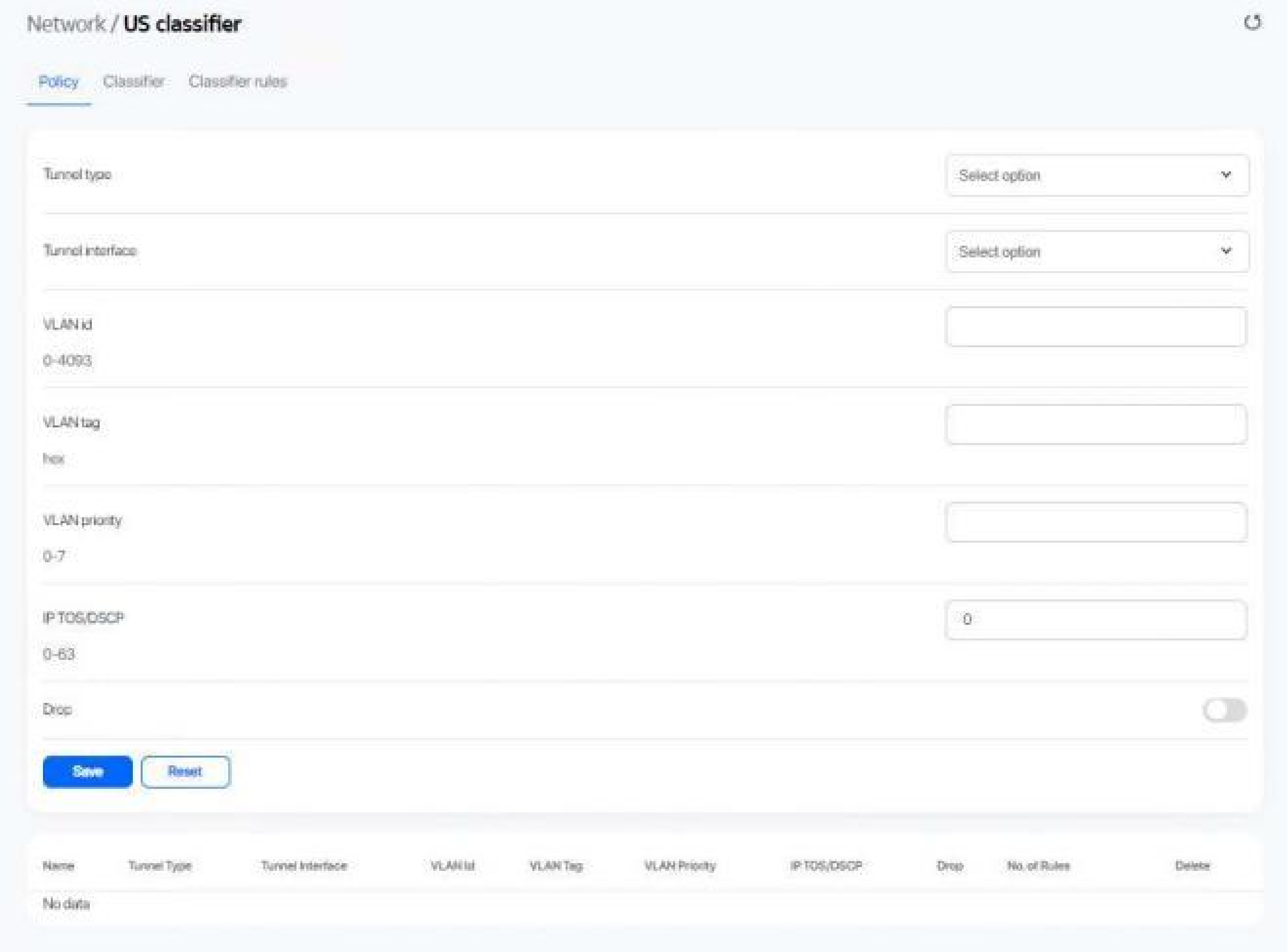
Up to 16 policies can be created, with up to 8 classifiers and 32 classifier rules.

1

Click **Network→ US Classifier** in the left pane and select the **Policy** tab.

All classifier policies are displayed in the policy table in the page.

Figure 7-26 US Classifier - Policy page



Network / **US classifier**

Policy Classifier Classifier rules

Tunnel type: Select option

Tunnel interface: Select option

VLAN id
0-4093

VLAN tag
hex

VLAN priority
0-7

IP TOS/DSCP: 0
0-63

Drop

Save Reset

Name	Tunnel Type	Tunnel Interface	VLAN Id	VLAN Tag	VLAN Priority	IP TOS/DSCP	Drop	No. of Rules	Delete
No data									

2

Configure the following parameters:

Table 7-19 US Classifier - Policy parameters

Field	Description
Tunnel Type	The tunnel type is set to GRE and cannot be modified.
Tunnel Interface	Select a tunnel interface from the list: • **No Tunnel** • **GRE Tunnel** • **LAN traffic**

Table 7-19 US Classifier - Policy parameters (continued)

Field	Description
VLAN ID	Enter a VLAN ID. Allowed values: 0 to 4093
VLAN Tag	This field is not configurable. The VLAN tag is set to 8100 (hexadecimal). Determines the VLAN tag used inside the GRE tunnel.
VLAN Priority	Enter a VLAN priority level. A lower number indicates a higher priority. Allowed values: 0 to 7
IP TOS/DSCP	This field is not configurable. All tunnel packets are generated with a default DSCP value (usually 0). Allowed values: 0 to 63
Drop	Select the toggle button to enable dropping of the packets.

3

Click **Save**. The policy is added to the policies table.

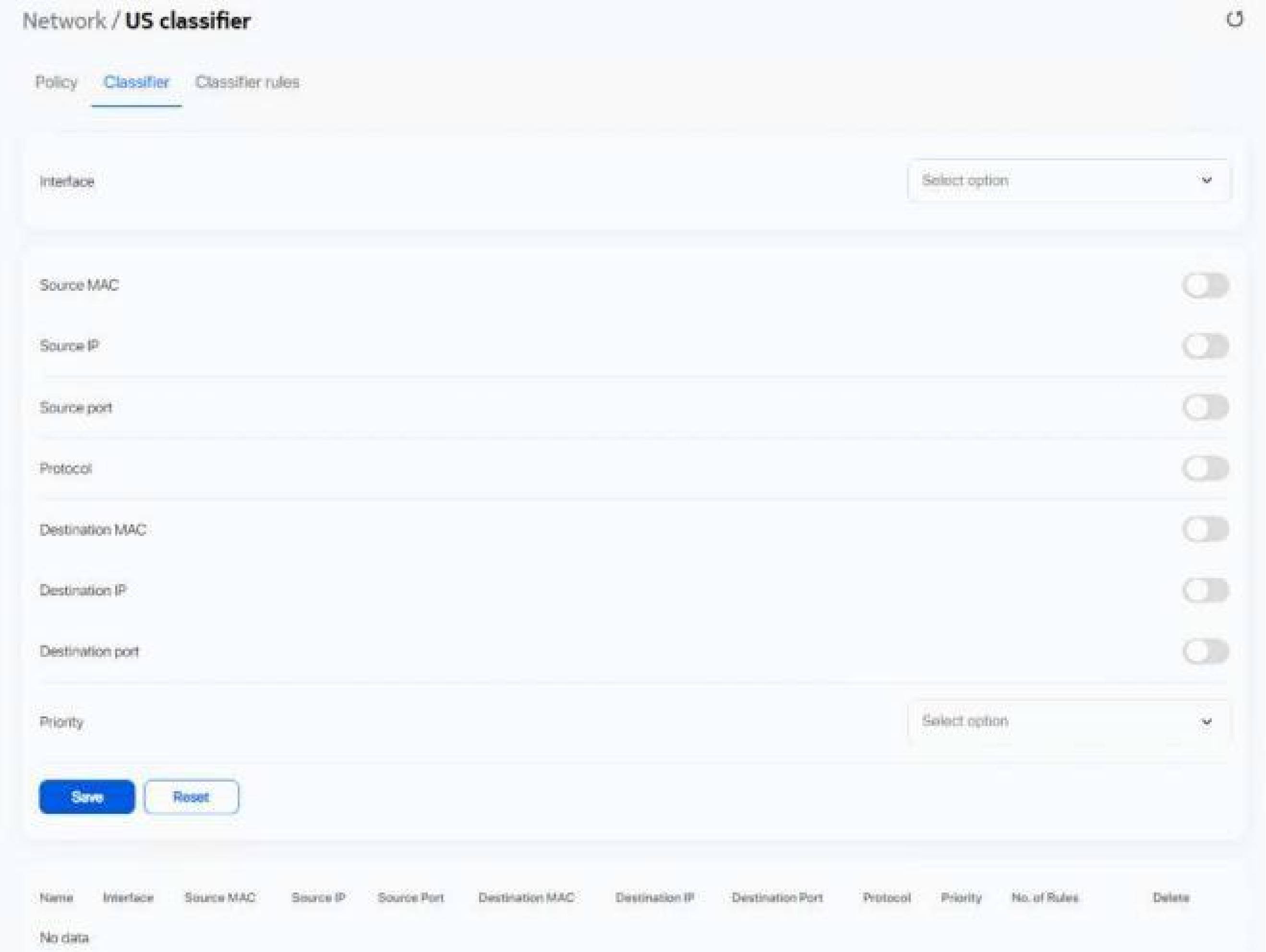
To delete a policy, click **Delete** next to the policy entry in the table. A policy can only be deleted if it is not associated with any classifier rules.

4

Select the **Classifier** tab.

All classifiers are displayed in the classifier table in the page.

Figure 7-27 US Classifier - Classifier page



Network / **US classifier**

Interface: Select option

Source MAC

Source IP

Source port

Protocol

Destination MAC

Destination IP

Destination port

Priority: Select option

Name	Interface	Source MAC	Source IP	Source Port	Destination MAC	Destination IP	Destination Port	Protocol	Priority	No. of Rules	Delete
No data											

5

Configure the following parameters:

Table 7-20 US Classifier - Classifier parameters

Field	Description
Interface	Select an interface from the list; for example, None, LAN, 2.4G SSID, or 5G SSID. The option **None** indicates that all interfaces are selected.
Source MAC	Select the toggle button to enter a source MAC address.
Source IP	Select the toggle button to enter a source IP address.
Source Port	Select the toggle button to enter a source port.

Table 7-20 US Classifier - Classifier parameters (continued)

Field	Description
Protocol	Select the toggle button to enter a protocol.
Destination MAC	Select the toggle button to enter a destination MAC address.
Destination IP	Select the toggle button to enter a destination IP address.
Destination Port	Select the toggle button to enter a destination port.
Priority	Select a priority level from 1 to 8. The lower the number, the higher the priority. Only one classifier can be created with the same priority.

6

Click **Save**. The US classifier is listed in the classifiers table.

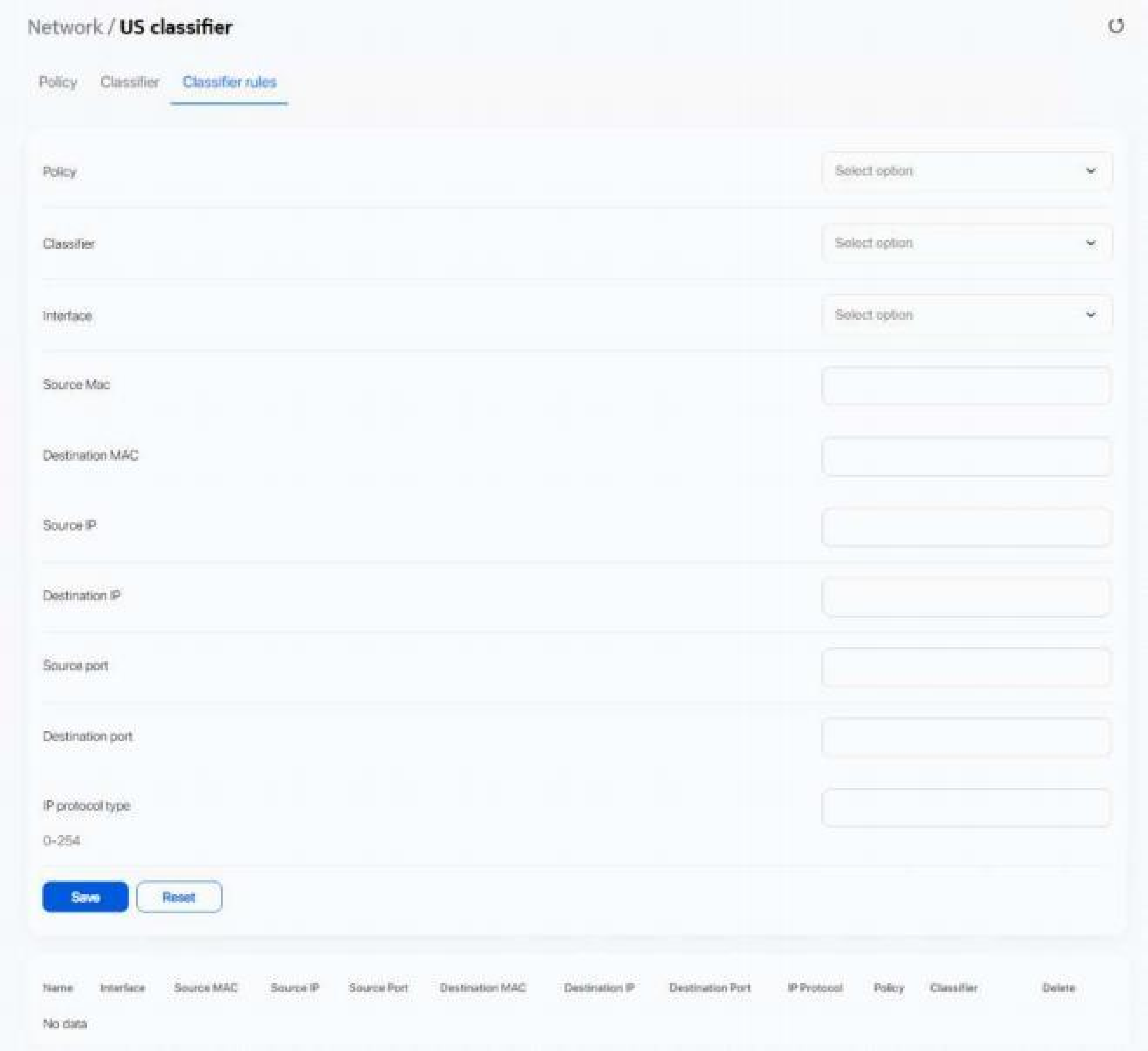
To delete a classifier, click **Delete** next to the classifier entry in the table. A classifier can only be deleted if it is not associated with any classifier rules.

7

Select the **Classifier Rules** tab.

All classifier rules are displayed in the classifier rules table in the page.

Figure 7-28 *US Classifier - Classifier Rules* page



Policy	Select option
Classifier	Select option
Interface	Select option
Source Mac	
Destination MAC	
Source IP	
Destination IP	
Source port	
Destination port	
IP protocol type 0-254	

Name	Interface	Source MAC	Source IP	Source Port	Destination MAC	Destination IP	Destination Port	IP Protocol	Policy	Classifier	Delete
No data											

8

Configure the following parameters:

Table 7-21 US Classifier - Classifier Rules parameters

Field	Description
Policy	Select a policy from the list.
Classifier	Select a classifier from the list.
Interface	Select an interface from the list; for example, None, LAN, 2.4G SSID, 5G SSID.
Source MAC	Enter a source MAC address.
Destination MAC	Enter a destination MAC address.
Source IP	Enter a source IP address.
Destination IP	Enter a destination IP address.
Source Port	Enter a source port.
Destination Port	Enter a destination port.
IP Protocol Type	Enter a value between 0 and 254.

9

Click **Save**. The rule is added to the classifier rules table.

To delete a classifier rule, click **Delete** next to the classifier rule entry in the table.

END OF STEPS

Maintenance

7.28 Overview

7.28.1 Purpose

This section describes the maintenance tasks supported by the Beacon G6 WebGUI.

7.28.2 Contents

7.29 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”.

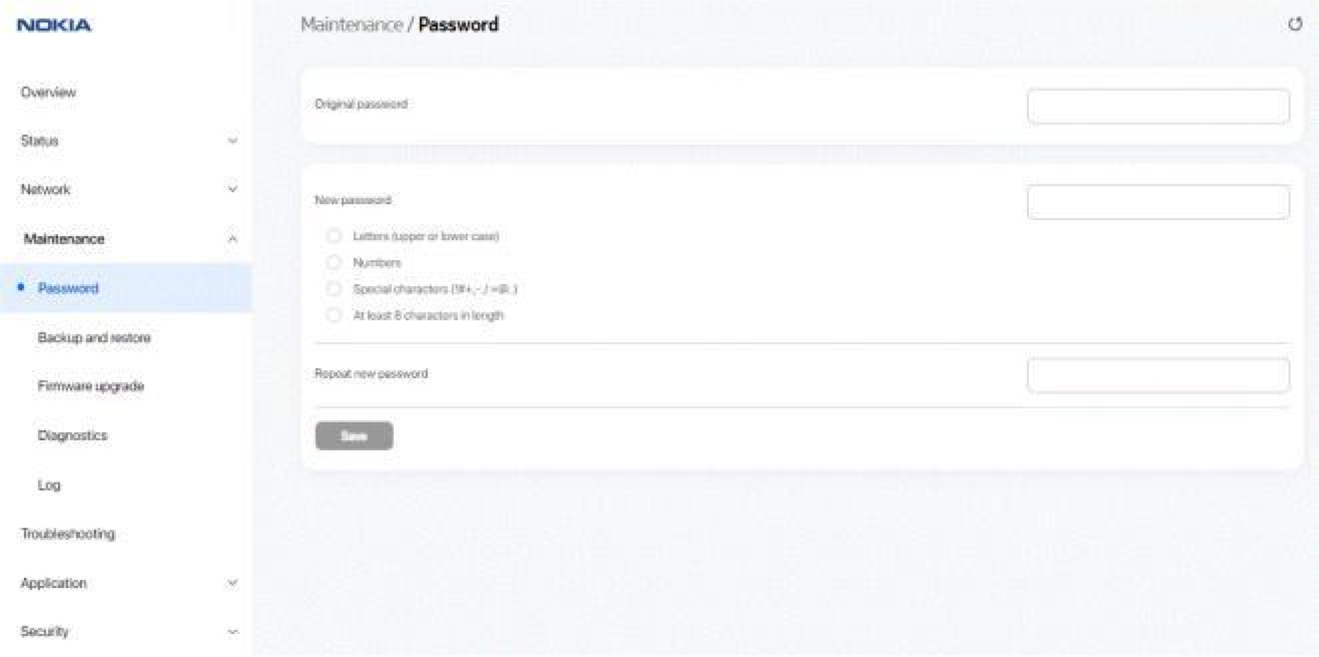
When the password does not meet the password rules, the application displays a message to indicate which password rule has not been followed, for example:

- 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→ Password** in the left pane. The *Password* page displays.

Figure 7-29 *Password* page



2

Configure the following parameters:

Table 7-22 *Password* parameters

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

3

Click **Save**.

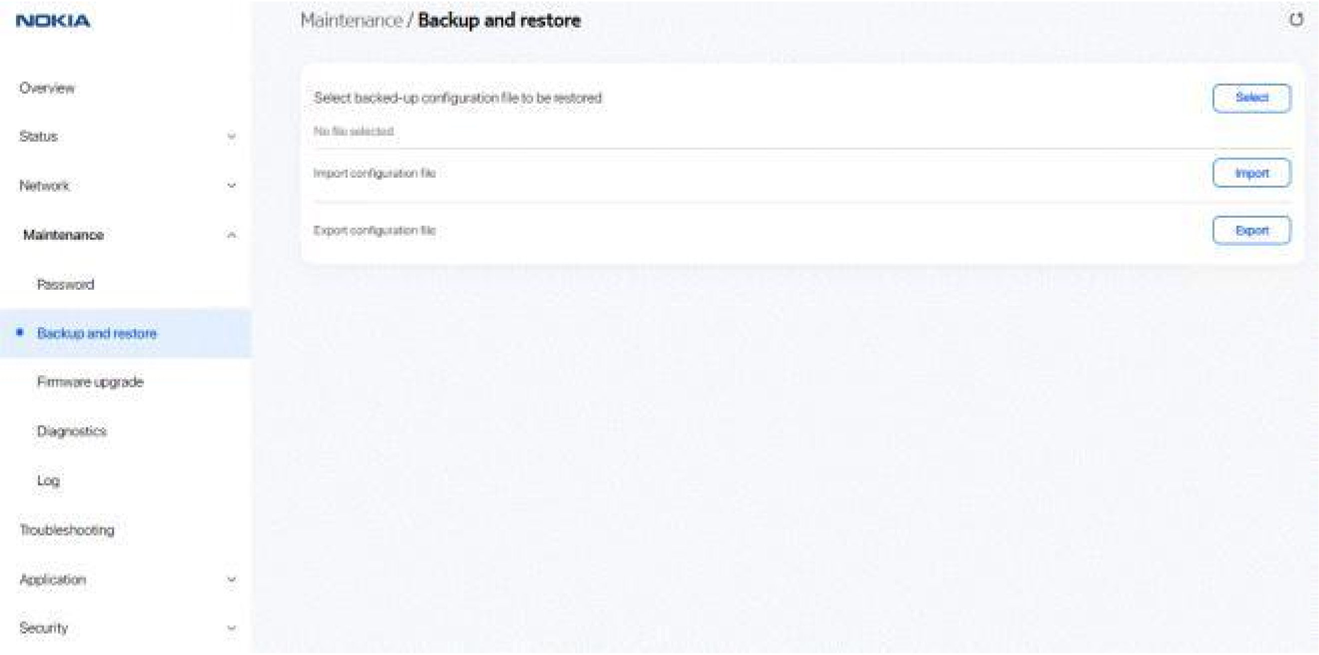
END OF STEPS

7.30 Backing up the configuration

1

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

Figure 7-30 Backup and restore page



Select backed-up configuration file to be restored

No file selected

Import configuration file

Export configuration file

2

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

END OF STEPS

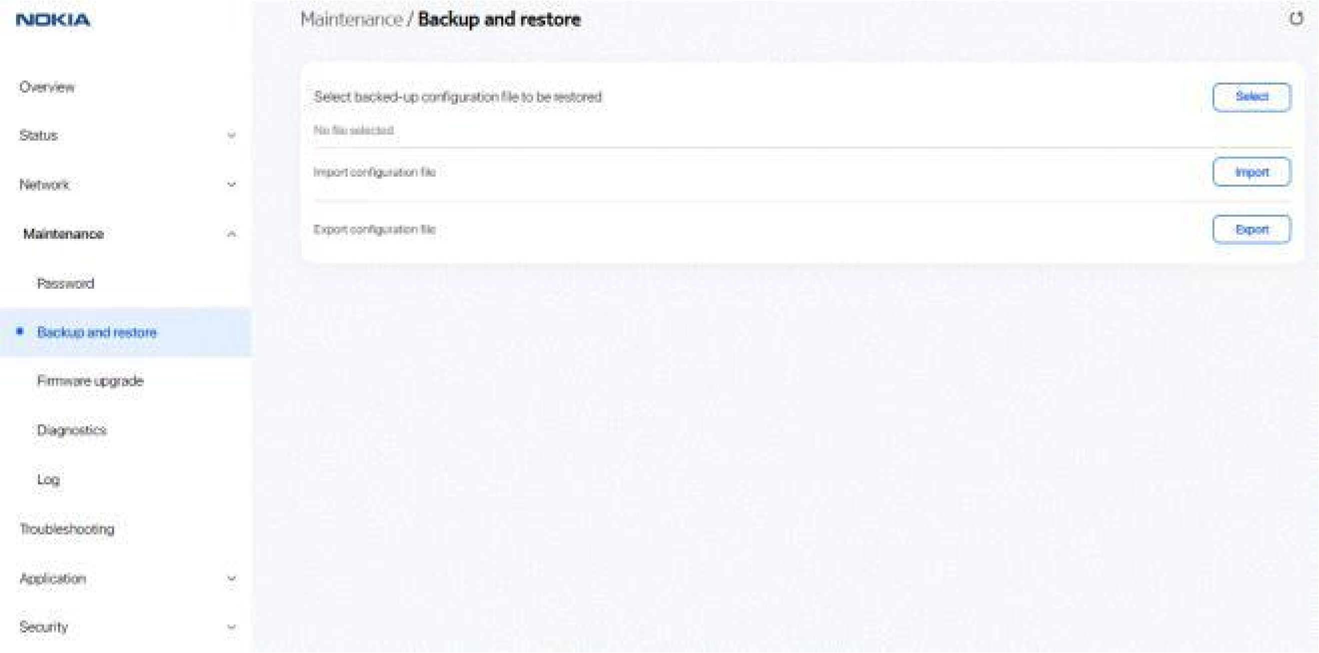
7.31 Restoring the configuration

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

1

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

Figure 7-31 Backup and restore page



Maintenance / **Backup and restore**

Select backed-up configuration file to be restored

No file selected

Import configuration file

Export configuration file

2

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

3

Click **Import** to import the configuration file and restore the Beacon to the backed-up configuration.

A confirmation message displays after successful restore and the Beacon reboots.

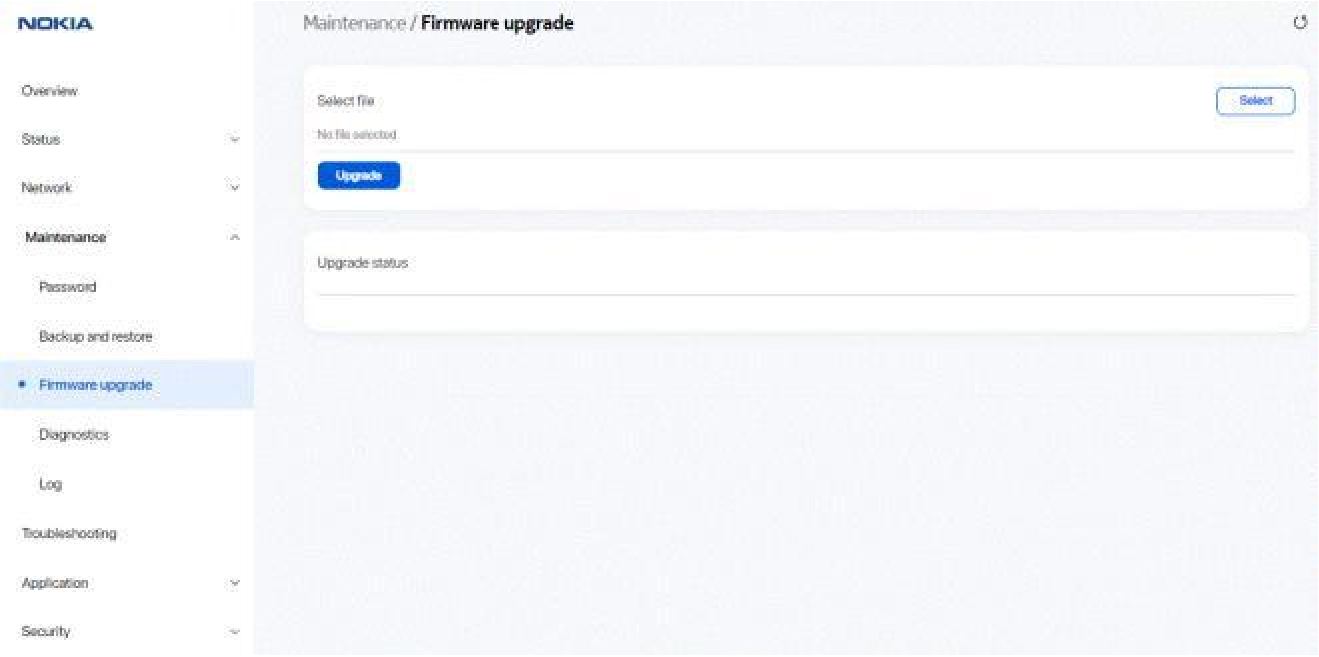
END OF STEPS

7.32 Upgrading firmware

1

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

Figure 7-32 *Firmware upgrade* page



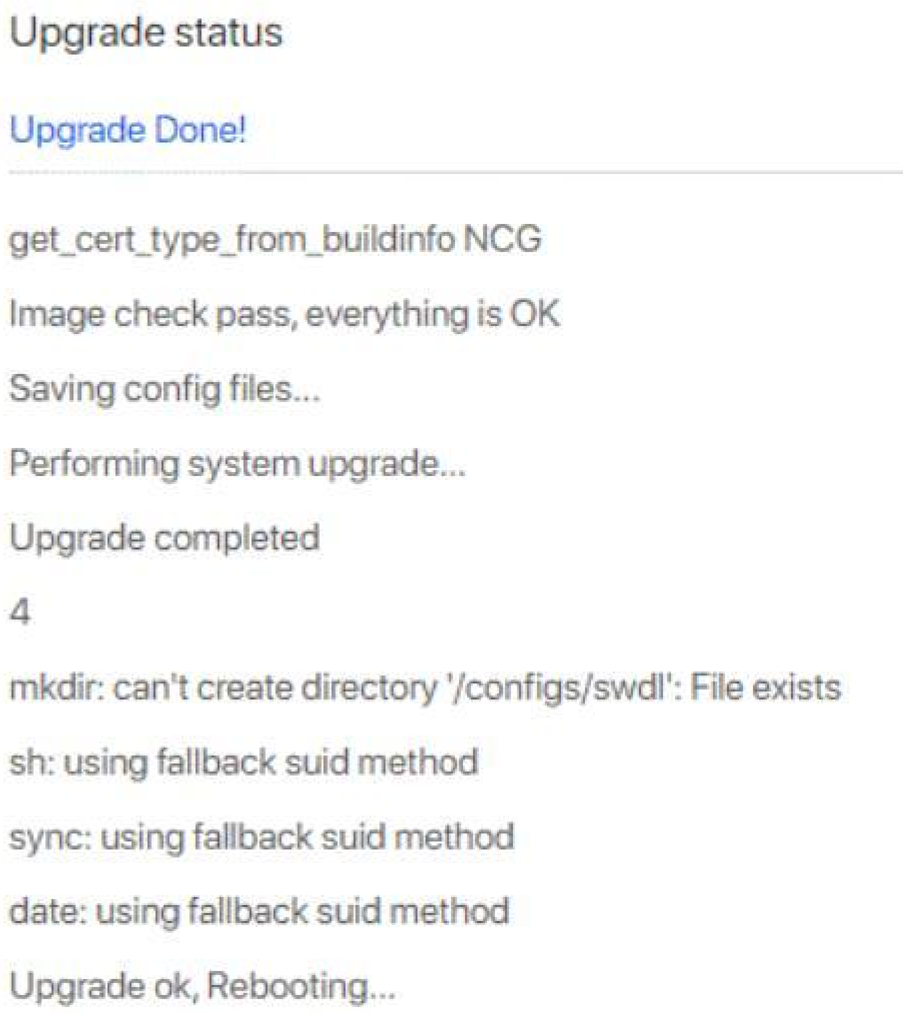
2

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

3

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

Figure 7-33 Example of upgrade status messages



Upgrade status

Upgrade Done!

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

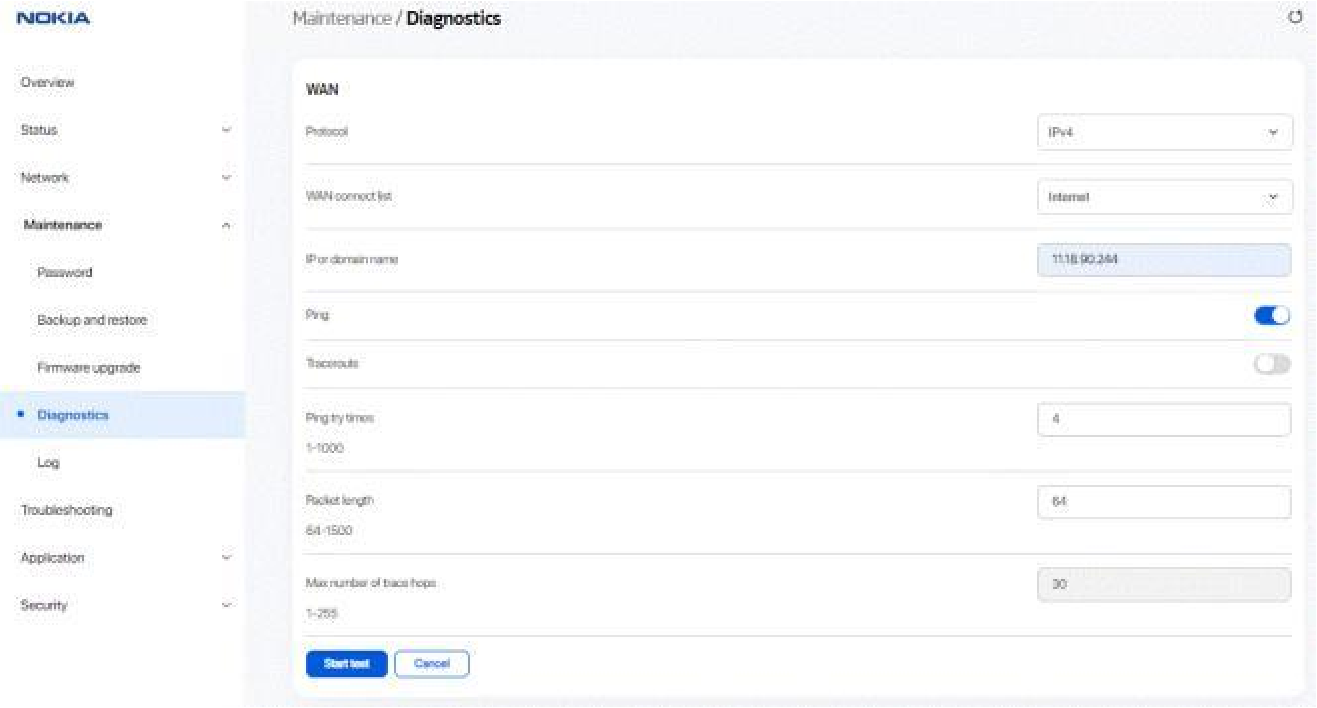
END OF STEPS

7.33 Diagnosing WAN connections

1

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

Figure 7-34   Diagnostics page



Maintenance / **Diagnostics**

WAN

Protocol: IPv4

WAN connect list: Internet

IP or domain name: 11.18.90.244

Ping: on

Traceroute: off

Ping try times (1-1000): 4

Packet length (64-1500): 64

Max number of trace hops (1-255): 30

2

Configure the following parameters.

Table 7-23   Diagnostics parameters

Field	Description
Protocol	Select a protocol from the list: • **IPv4** • **IPv6**
WAN connection list	Select a WAN connection to diagnose from the list.
IP or domain name	Enter the IP address or domain name.
Ping	Select this toggle button to enable ping.
Traceroute	Select this toggle button to enable traceroute.
Ping try times	Enter the number of ping attempts. This field is enabled only if you select the **Ping** toggle button. Allowed values: 1 to 1000 Default value: 4

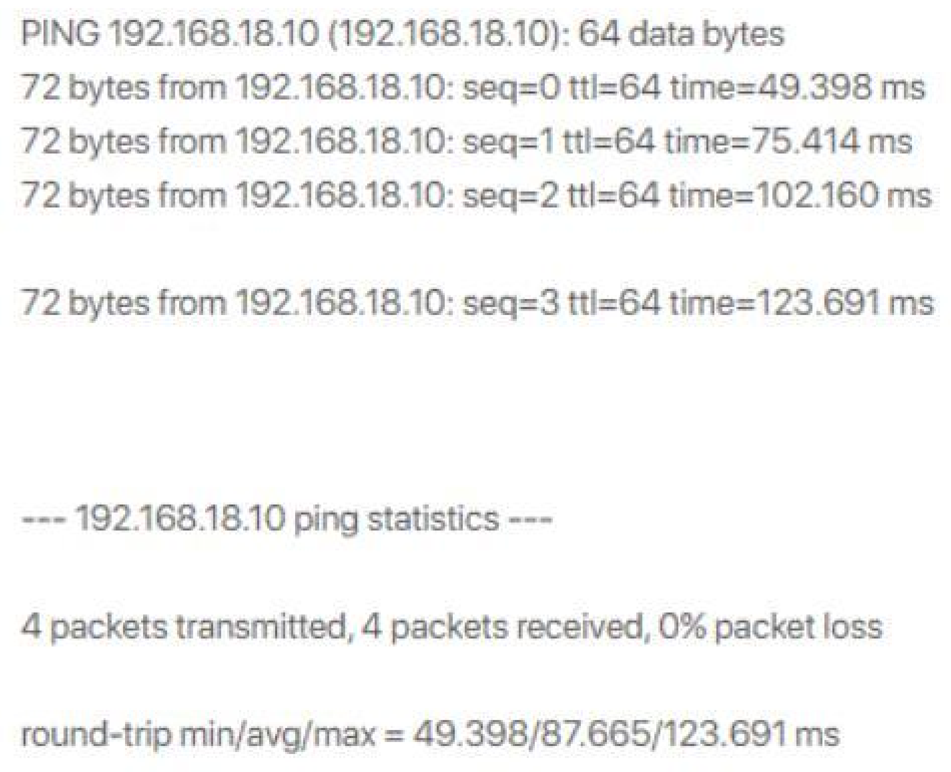
Table 7-23 *Diagnostics* parameters (continued)

Field	Description
Packet length	Enter a packet length. Allowed values: 64 to 1500 Default value: 64
Max number of trace hops	Enter the maximum number of trace hops. This field is enabled only if you select the **Traceroute** toggle button. Allowed values: 1 to 255 Default value: 30

3

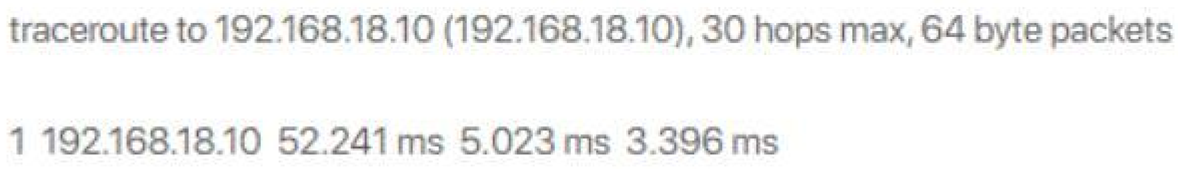
Click **Start test** to start the test. Results are displayed at the bottom of the page.

Figure 7-35 Example of ping results



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

72 bytes from 192.168.18.10: seq=3 ttl=64 time=123.691 ms



--- 192.168.18.10 ping statistics ---

4 packets transmitted, 4 packets received, 0% packet loss

round-trip min/avg/max = 49.398/87.665/123.691 ms
```

Figure 7-36 Example of traceroute results



```
traceroute to 192.168.18.10 (192.168.18.10), 30 hops max, 64 byte packets

1 192.168.18.10  52.241 ms  5.023 ms  3.396 ms
```

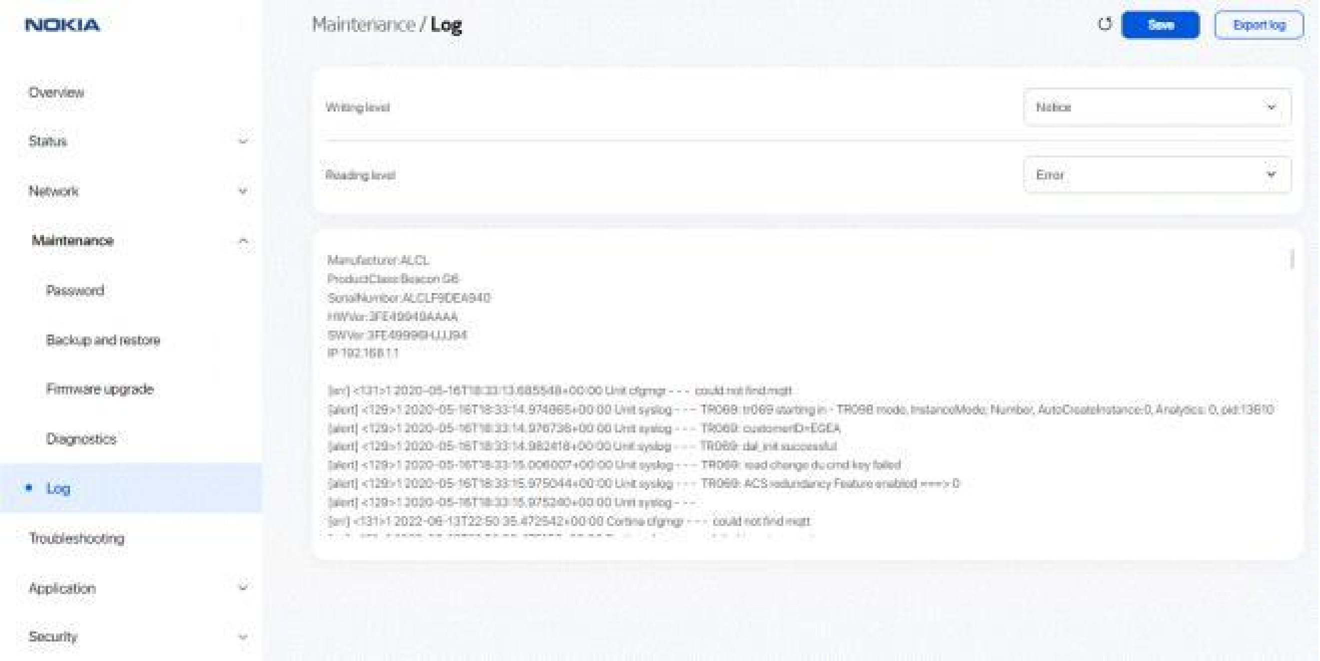
End of steps

7.34 Viewing log files

1

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

Figure 7-37 *Log* page



Writing level: Notice

Reading level: Error

```
Manufacturer:ALCL
ProductClass:Beacon G6
SerialNumber:ALCLF9DE4940
HWVer:3FE49949AAAA
SWVer:3FE49998HJJJ94
IP:192.168.1.1

[err] <131>1 2020-05-16T18:33:13.685548+00:00 Unit cfgmgr - - - could not find mqtt
[alert] <129>1 2020-05-16T18:33:14.974865+00:00 Unit syslog - - - TR069: tr069 starting in - TR098 mode, InstanceMode: Number, AutoCreateInstance:0, Analytics: 0, pid:13610
[alert] <129>1 2020-05-16T18:33:14.976736+00:00 Unit syslog - - - TR069: customerID=EGEA
[alert] <129>1 2020-05-16T18:33:14.982418+00:00 Unit syslog - - - TR069: dal_init successful
[alert] <129>1 2020-05-16T18:33:15.006007+00:00 Unit syslog - - - TR069: read change du cmd key failed
[alert] <129>1 2020-05-16T18:33:15.975044+00:00 Unit syslog - - - TR069: ACS redundancy Feature enabled ====> 0
[alert] <129>1 2020-05-16T18:33:15.975240+00:00 Unit syslog - - -
[err] <131>1 2022-06-13T22:50:35.472542+00:00 Cortina cfgmgr - - - could not find mqtt
```

2

Configure the following parameters:

Table 7-24 *Log* parameters

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

3

Click **Save**. The log file is displayed at the bottom of the page.

4

Click **Export log** to download the log file to your PC. The filename of the log is *onu_info.log*.

END OF STEPS

Troubleshooting

7.35 Overview

7.35.1 Purpose

This section describes the troubleshooting procedures supported by the Beacon G6 WebGUI.

7.35.2 Contents

7.36 Troubleshooting

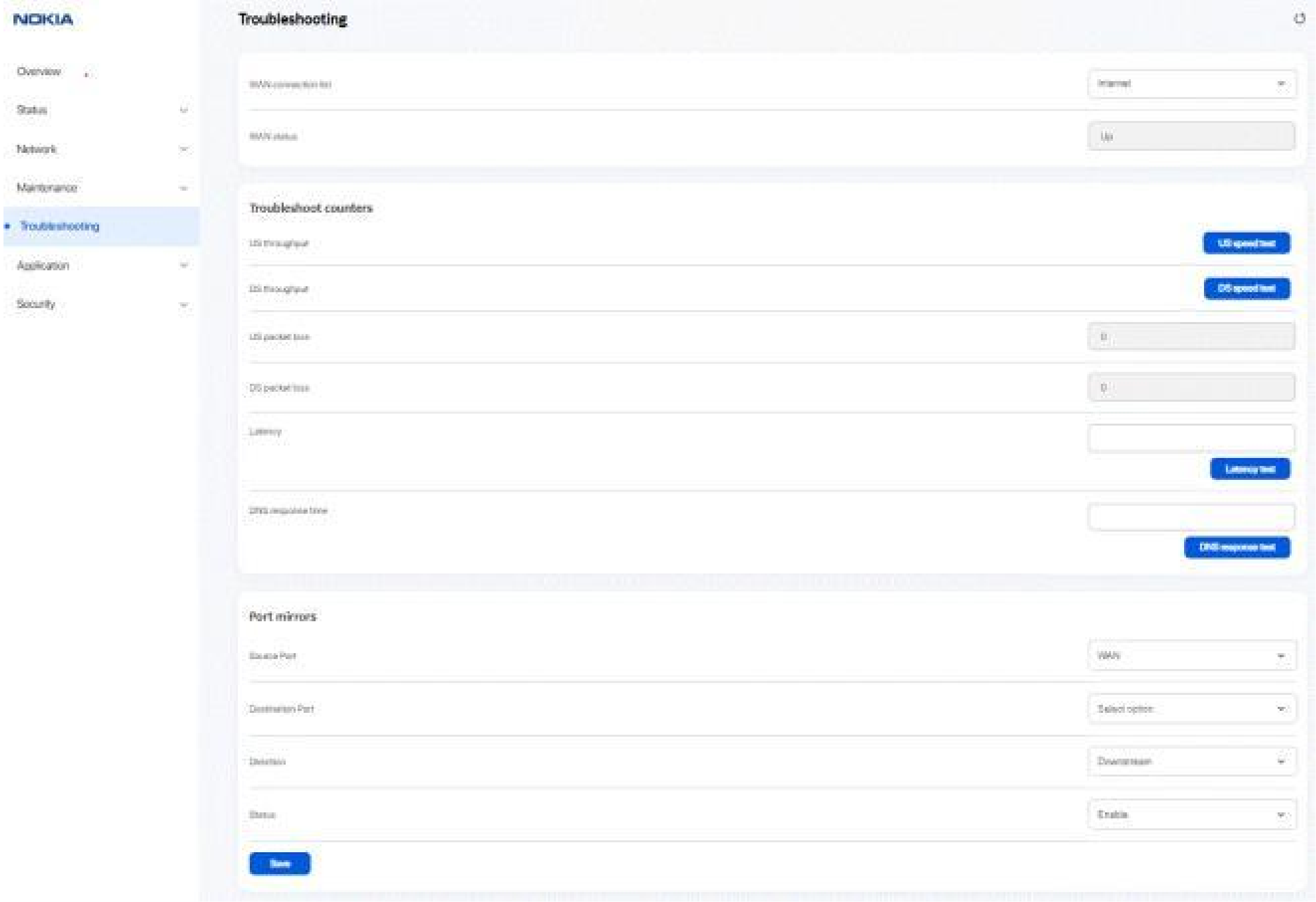
The Troubleshooting feature enables service providers and end users to monitor the performance of their broadband connection.

Tests are run to retrieve upstream and downstream throughput, latency, and DNS response time. The Troubleshooting page also displays upstream and downstream packet loss and Internet status.

1

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

Figure 7-38 *Troubleshooting* page



Troubleshooting

WAN connection list: Internet

WAN status: Up

Troubleshoot counters

US throughput

DS throughput

US packet loss: 0

DS packet loss: 0

Latency

DNS response time

Port mirrors

Source Port: WAN

Destination Port: Select option

Direction: Downstream

Status: Enable

2

Configure the following parameters:

Table 7-25 *Troubleshooting* parameters

Field	Description
WAN Connection List	Select a WAN connection from the list.
WAN Status	Displays the WAN status: • Up • Down
Troubleshoot counters	
US throughput	This test is used to determine the upstream throughput/speed. Click **US speed test** to specify the time for the upstream test.

Table 7-25 *Troubleshooting* parameters (continued)

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

3

Click **Save.**

END OF STEPS

Application configuration

7.37 Overview

7.37.1 Purpose

This section describes the application configuration tasks supported by the Beacon G6 WebGUI.

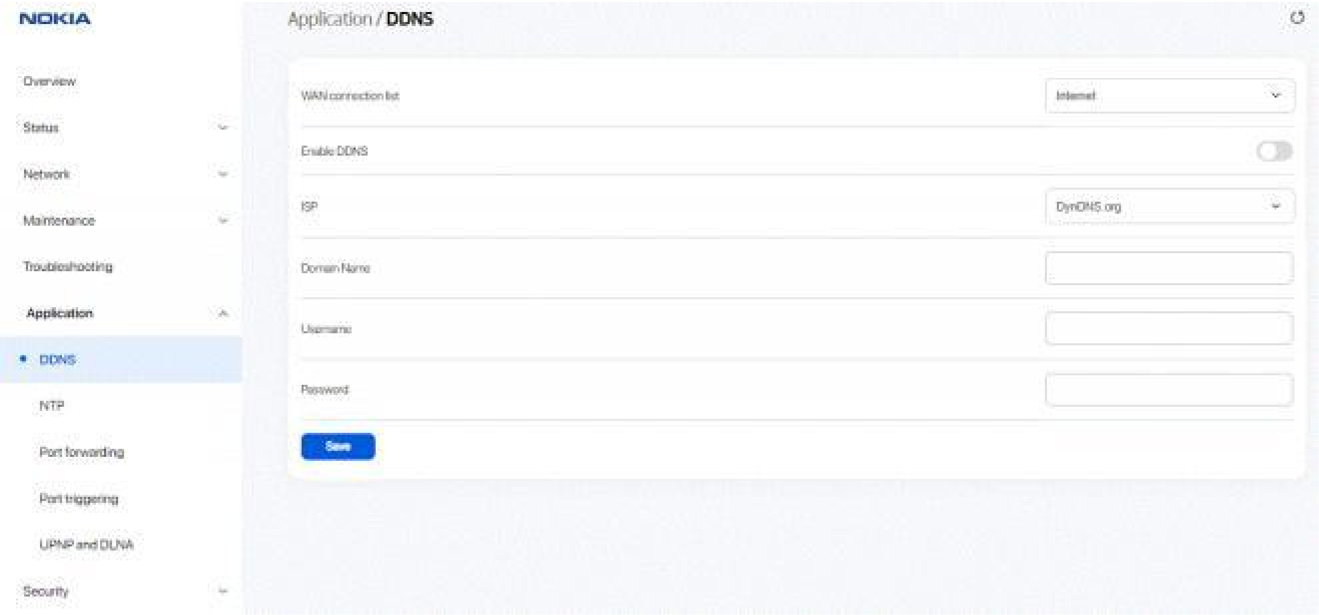
7.37.2 Contents

7.38 Configuring DDNS

1

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

Figure 7-39 *DDNS* page



Application / **DDNS**

WAN connection list: Internet

Enable DDNS

ISP: DynDNS.org

Domain Name

Username

Password

2

Configure the following parameters:

Table 7-26 DDNS parameters

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

3

Click **Save.**

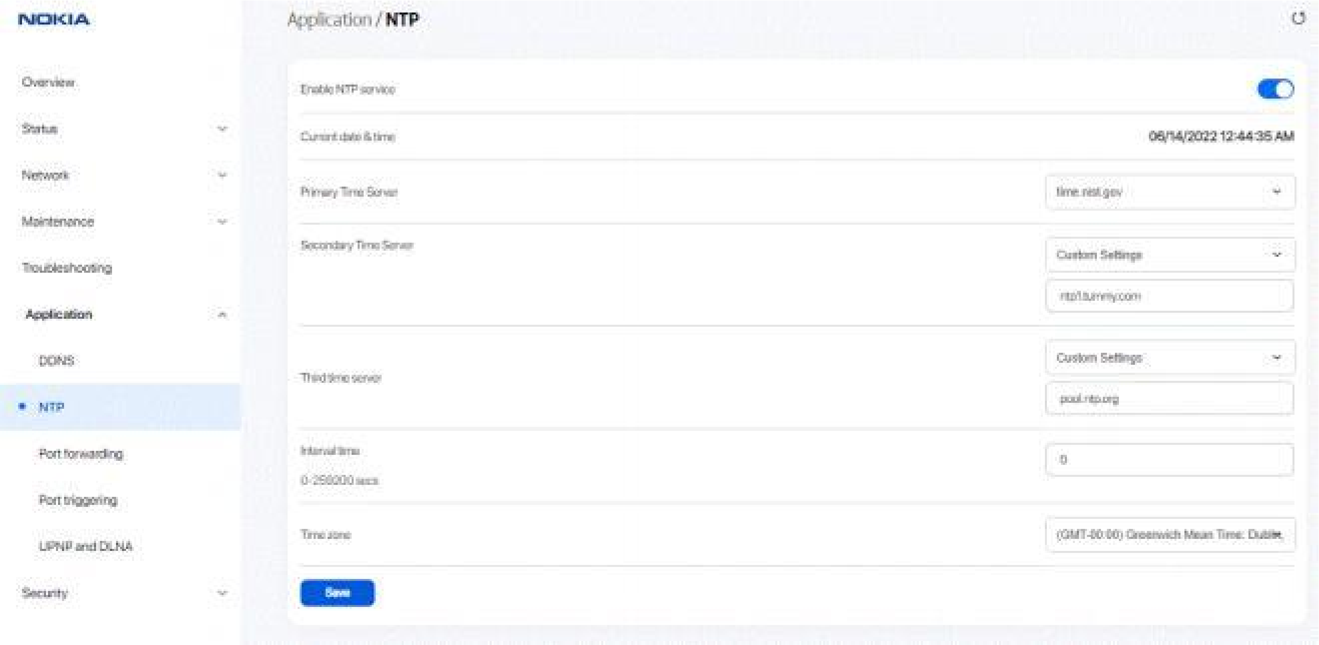
END OF STEPS

7.39 Configuring NTP

1

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

Figure 7-40 *NTP* page



Enable NTP service

Current date & time 06/14/2022 12:44:35 AM

Primary Time Server: time.nist.gov

Secondary Time Server: Custom Settings, ntp1.tummy.com

Third time server: Custom Settings, pool.ntp.org

Interval time 0-259200 secs: 0

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

2

Configure the following parameters:

Table 7-27 *NTP* parameters

Field	Description
Enable NTP Service	Select the toggle button to enable the NTP service.
Current date & time	Displays the current local date and time.
Primary Time Server Secondary Time Server Third Time Server	Select a time server from the list or select **Custom Settings** and enter the IP address of the time server. You can select **None** if you do not want configure a secondary or tertiary server.
Interval time	Enter the interval at which to get the time from the time server, in seconds. Allowed values: 0 to 259200 seconds
Time zone	Select the local time zone from the list.

3

Click **Save**.

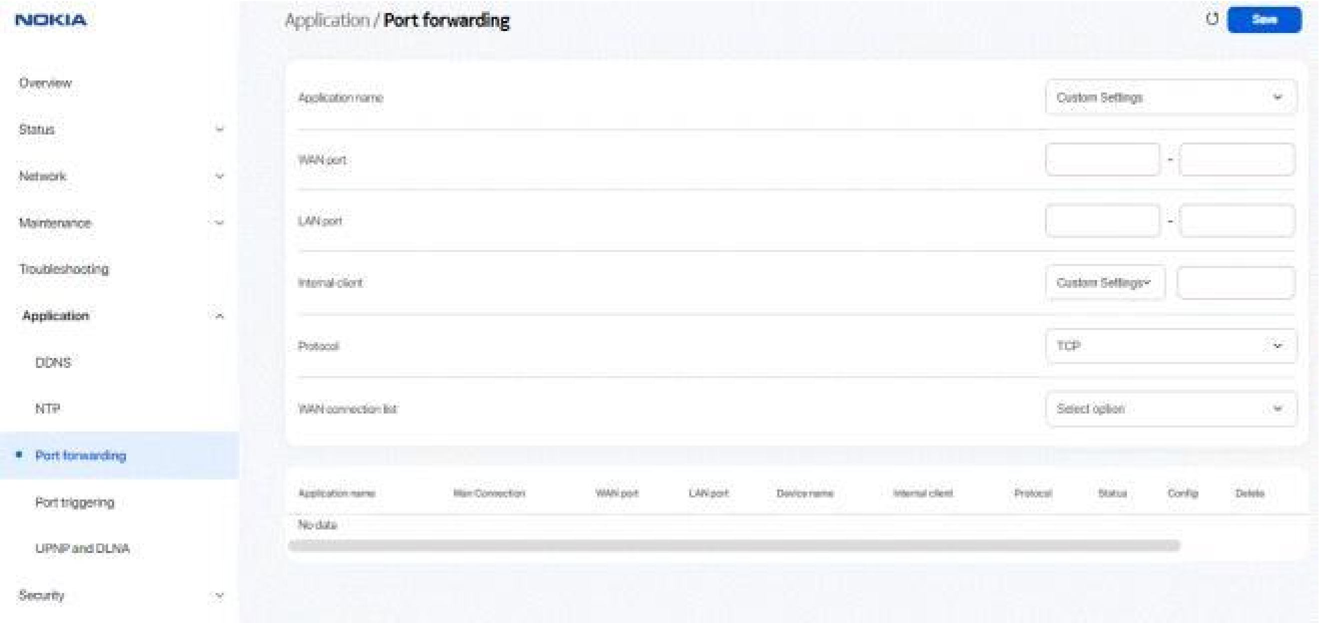
END OF STEPS

7.40 Configuring port forwarding

1

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

Figure 7-41 Port forwarding page



Application name: Custom Settings

WAN port: -

LAN port: -

Internal client: Custom Settings

Protocol: TCP

WAN connection list: Select option

Application name	Wan Connection	WAN port	LAN port	Device name	Internal client	Protocol	Status	Config	Delete
No data									

2

Configure the following parameters:

Table 7-28 Port forwarding parameters

Field	Description
Application Name	Select an application name from the list. The default is **Custom Settings**.
WAN port	Enter the WAN port range.
LAN port	Enter the LAN port range.
Internal client	Select a connected device from the list and enter the associated IP address. The default is **Custom Settings**.

Table 7-28 Port forwarding parameters (continued)

Field	Description
Protocol	Select the port forwarding protocol from the list: • **TCP** • **UDP** • **TCP/UDP**
WAN connection list	Select a WAN connection from the list. Only active devices are displayed in the list.

3

Click **Save**.

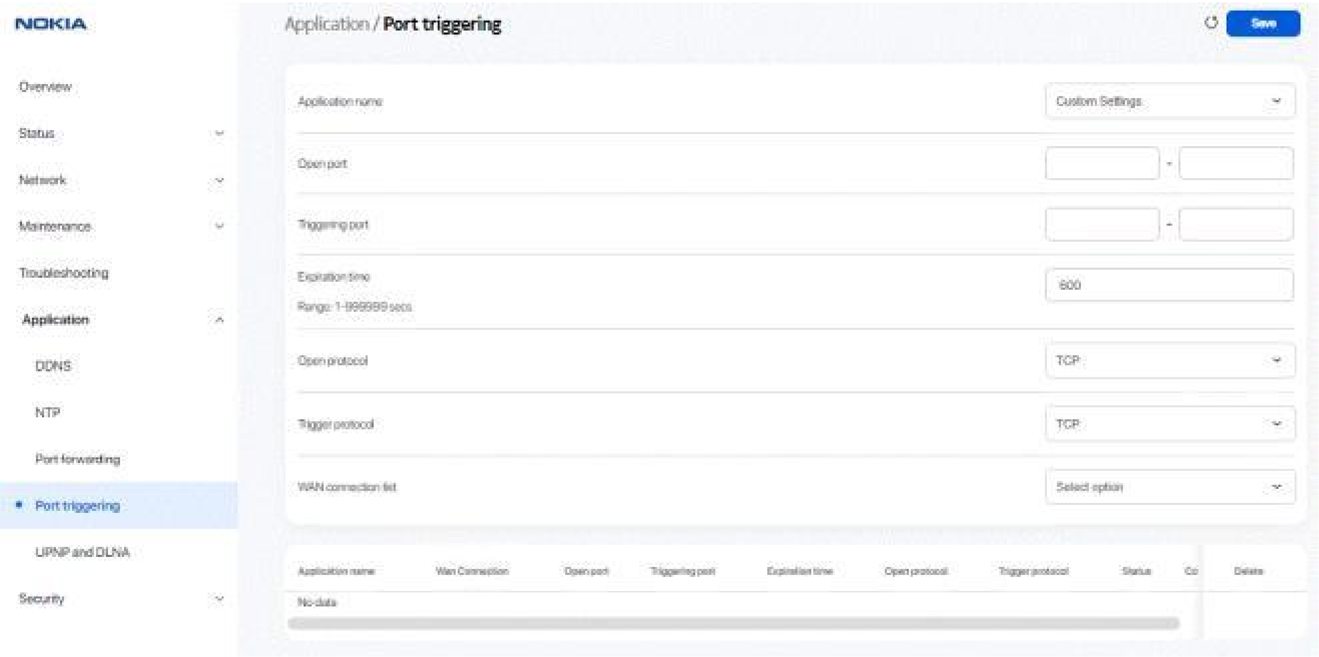
END OF STEPS

7.41 Configuring port triggering

1

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

Figure 7-42 Port triggering page



Application / Port triggering

Application name: Custom Settings

Open port: -

Triggering port: -

Expiration time: 600

Range: 1-999999 secs

Open protocol: TCP

Trigger protocol: TCP

WAN connection list: Select option

Application name	Wan Connection	Open port	Triggering port	Expiration time	Open protocol	Trigger protocol	Status	Co	Delete
No data									

2

Configure the following parameters:

Table 7-29 Port triggering parameters

Field	Description
Application name	Select an application name from the list. The default is **Custom settings**.
Open port	Enter the open port range.
Triggering port	Enter the triggering port range.
Expire time	Enter the expiration time in seconds. Allowed range: 1 to 999999 seconds
Open protocol	Select the open port protocol from the list: • **TCP** • **UDP** • **TCP/UDP**
Trigger protocol	Select the triggering port protocol from the list: • **TCP** • **UDP** • **TCP/UDP**
WAN connection list	Select a WAN connection from the list. Only active devices are displayed in the list.

3

Click **Save.**

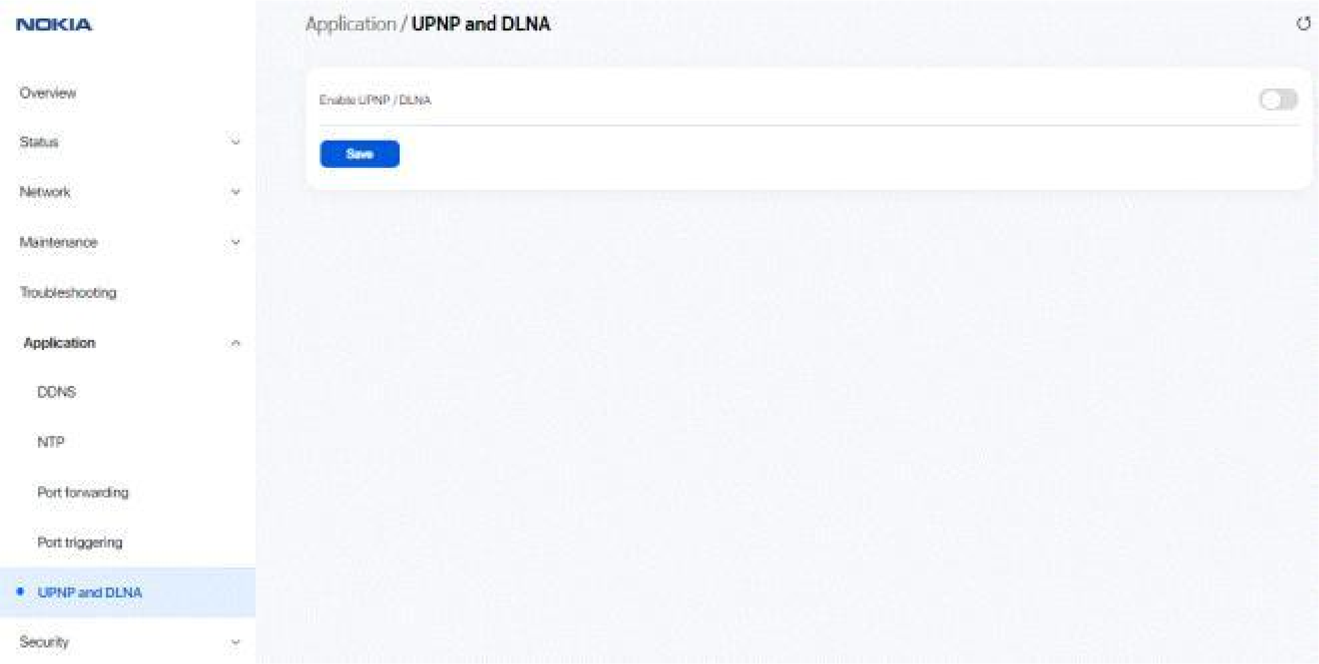
END OF STEPS

7.42 Configuring UPNP and DLNA

1

Click **Application→ UPNP and DLNA** from the left pane. The *UPNP and DLNA* page displays.

Figure 7-43 *UPNP and DLNA* page



Enable UPNP / DLNA

2

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

3

Click **Save**.

END OF STEPS

Security configuration

7.43 Overview

7.43.1 Purpose

This section describes the security configuration tasks supported by the Beacon G6 WebGUI

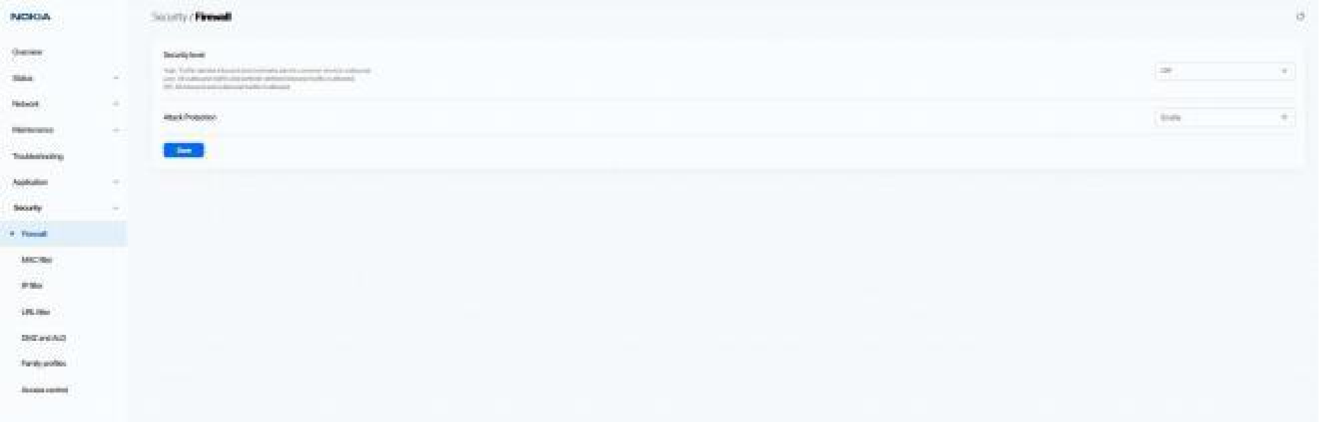
7.43.2 Contents

7.44 Configuring the firewall

1

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

Figure 7-44 *Firewall* page



2

Configure the following parameters.

Table 7-30 Firewall parameters

Field	Description
Security level	Select the security level from the list: • **High**: Pre-routing and application services are not supported. UDP Port 8000 can be used to access the services. For example, FTP can use 8021 and Telnet can use 8023. Regular UDP cannot be used. RG access is permitted via the LAN side but not via the WAN side. • **Low**: All outbound traffic and pinhole-defined inbound traffic is allowed. Pre-routing is supported: port forwarding, DMZ, host application, and host drop. Also supported are application services: DDNS, DHCP, DNS, H248, IGMP, NTP client, SSH, Telnet, TFTP, 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. • **Off**: All inbound and outbound traffic is allowed. No firewall security is in effect.
Attack Protection	Select **Enable** or **Disable** from the list to enable or disable protection against DoS or DDoS attacks. Default value: **Enable**.

3

Click **Save**.

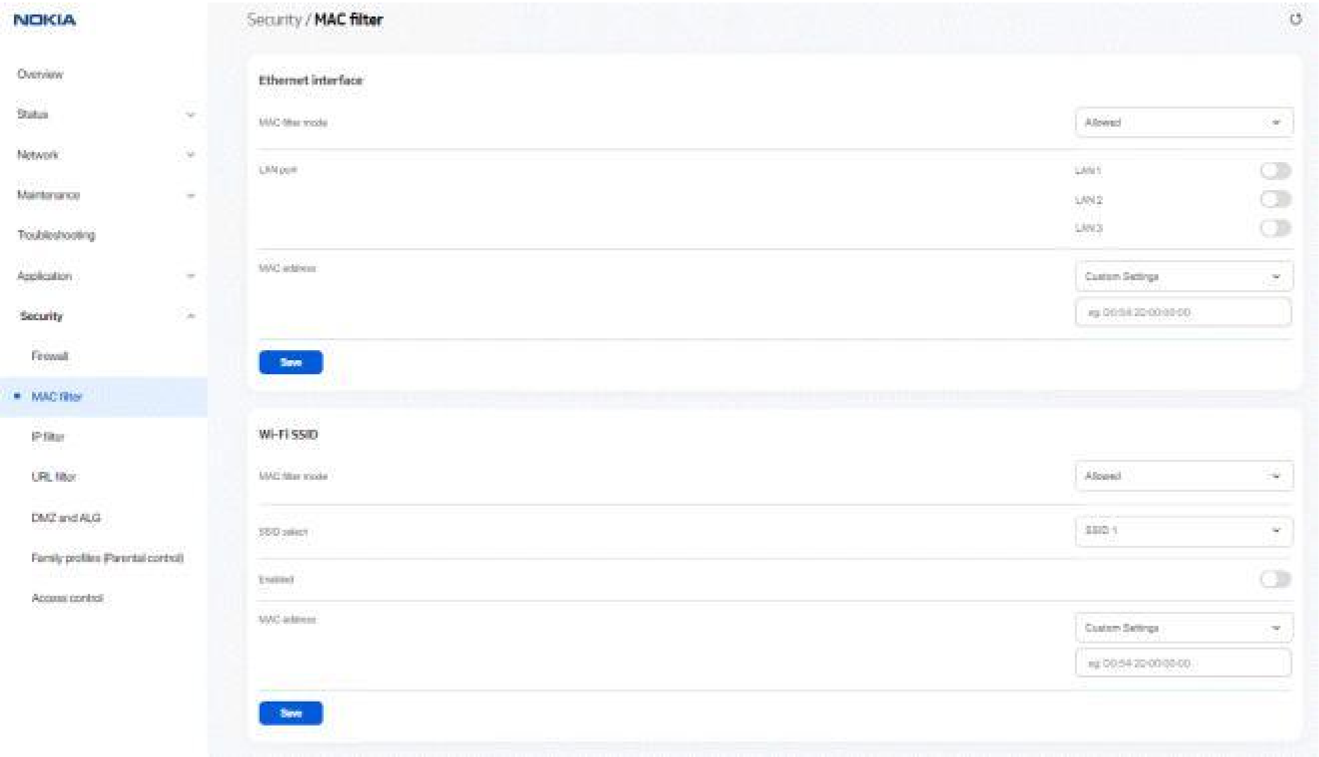
END OF STEPS

7.45 Configuring the MAC filter

1

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

Figure 7-45 MAC filter page



Security / **MAC filter**

Ethernet interface

MAC filter mode: Allowed

LAN port: LAN 1, LAN 2, LAN 3

MAC address: Custom Settings; eg: 00:54:20:00:00:00

Wi-Fi SSID

MAC filter mode: Allowed

SSID select: SSID 1

Enabled

MAC address: Custom Settings; eg: 00:54:20:00:00:00

2

Configure the following parameters:

Table 7-31 MAC filter - Ethernet Interface parameters

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

3

Click **Save**.

4

Configure the following parameters:

Table 7-32 MAC filter - WiFi SSID parameters

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

5

Click **Save**.

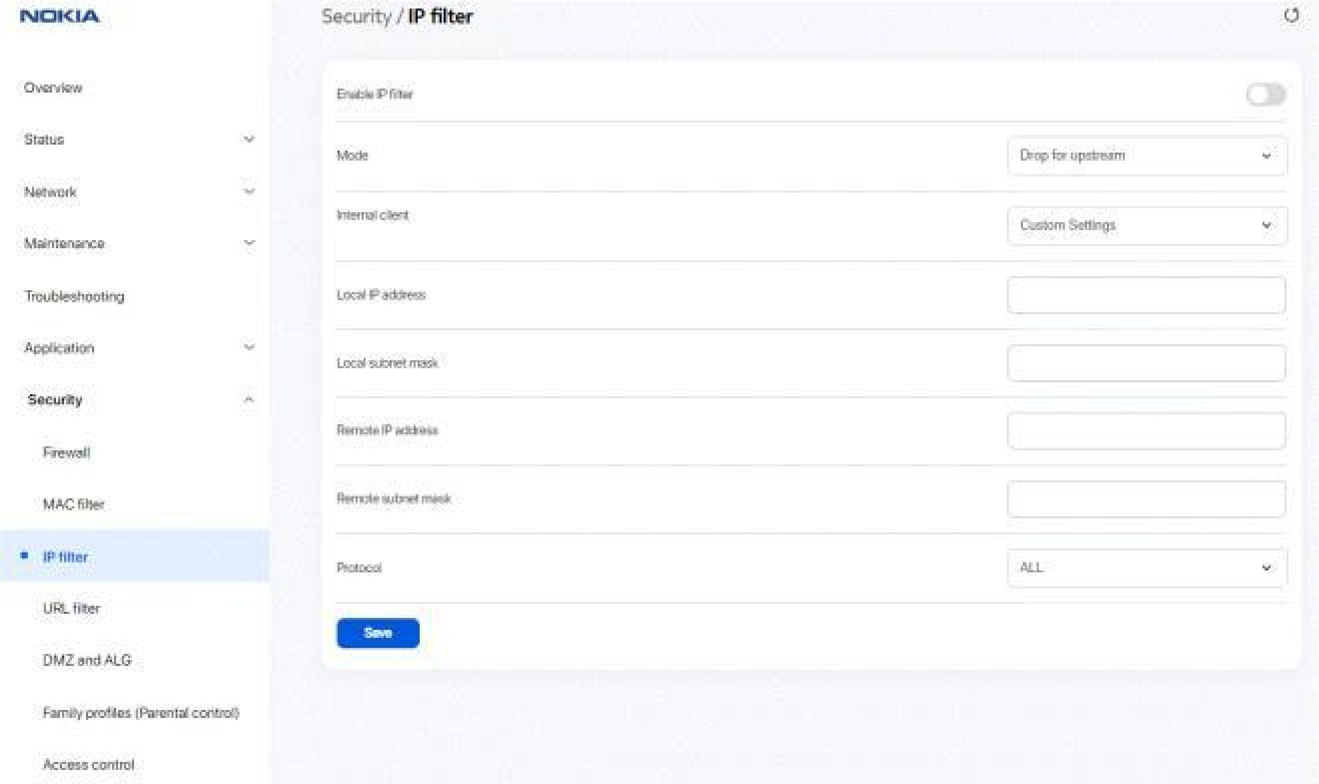
END OF STEPS

7.46 Configuring the IP filter

1

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

Figure 7-46 *IP filter* page



Security / **IP filter**

Enable IP filter	○
Mode	Drop for upstream
Internal client	Custom Settings
Local IP address	
Local subnet mask	
Remote IP address	
Remote subnet mask	
Protocol	ALL

2

Configure the following parameters:

Table 7-33 *IP filter* parameters

Field	Description
Enable IP filter	Select the toggle button to enable an IP filter.
Mode	Select an IP filter mode from the list: • **Drop for upstream** • **Drop for downstream**
Internal client	Select an internal client from the list: • **Custom Settings**: uses the IP address input below • **IP**: uses the connecting devices' IP to the Beacon
Local IP address	Enter the local IP address.
Local subnet mask	Enter the local subnet mask.
Remote IP address	Enter the remote IP address.

Table 7-33 *IP filter* parameters (continued)

Field	Description
Remote subnet mask	Enter the remote subnet mask.
Protocol	Select an application protocol or select **ALL** from the list.

3

Click **Save**.

END OF STEPS

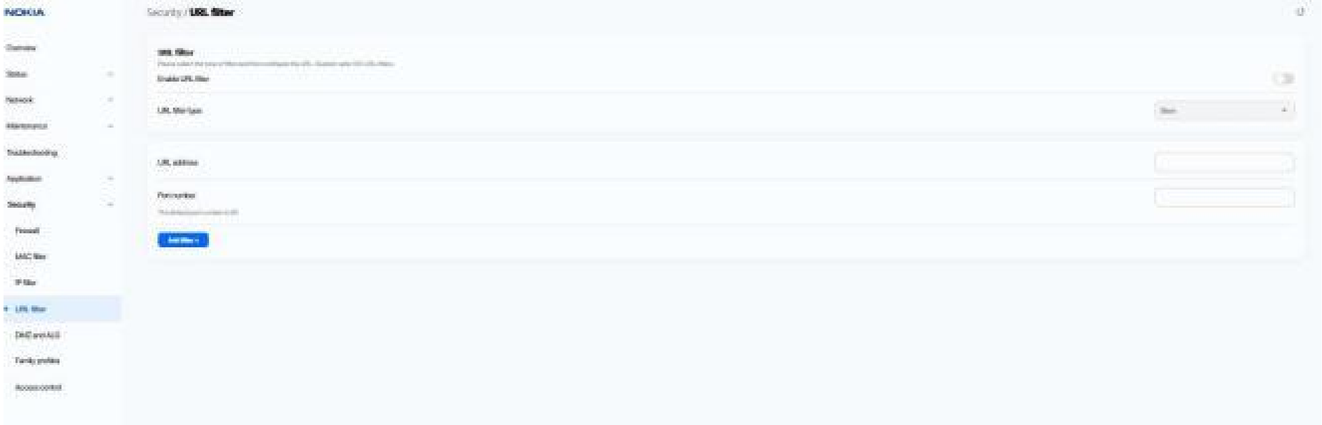
7.47 Configuring the URL filter

Note: You can add up to 100 URL filters.

1

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

Figure 7-47 *URL filter* page



Note: You cannot use URL filtering for HTTPS. The URL is encrypted when using HTTPS.

2

Configure the following parameters:

Table 7-34 *URL filter* parameters

Field	Description
Enable URL filter	Select the toggle button to enable the URL filter.

Table 7-34 *URL filter* parameters (continued)

Field	Description
URL filter type	Select a URL filter type from the list: • **Block** • **Allow**
URL address	Enter the URL address.
Port number	Enter the port number. Default value: 80 Allowed values: <>

3

Click **Add filter+** to add the URL filter.

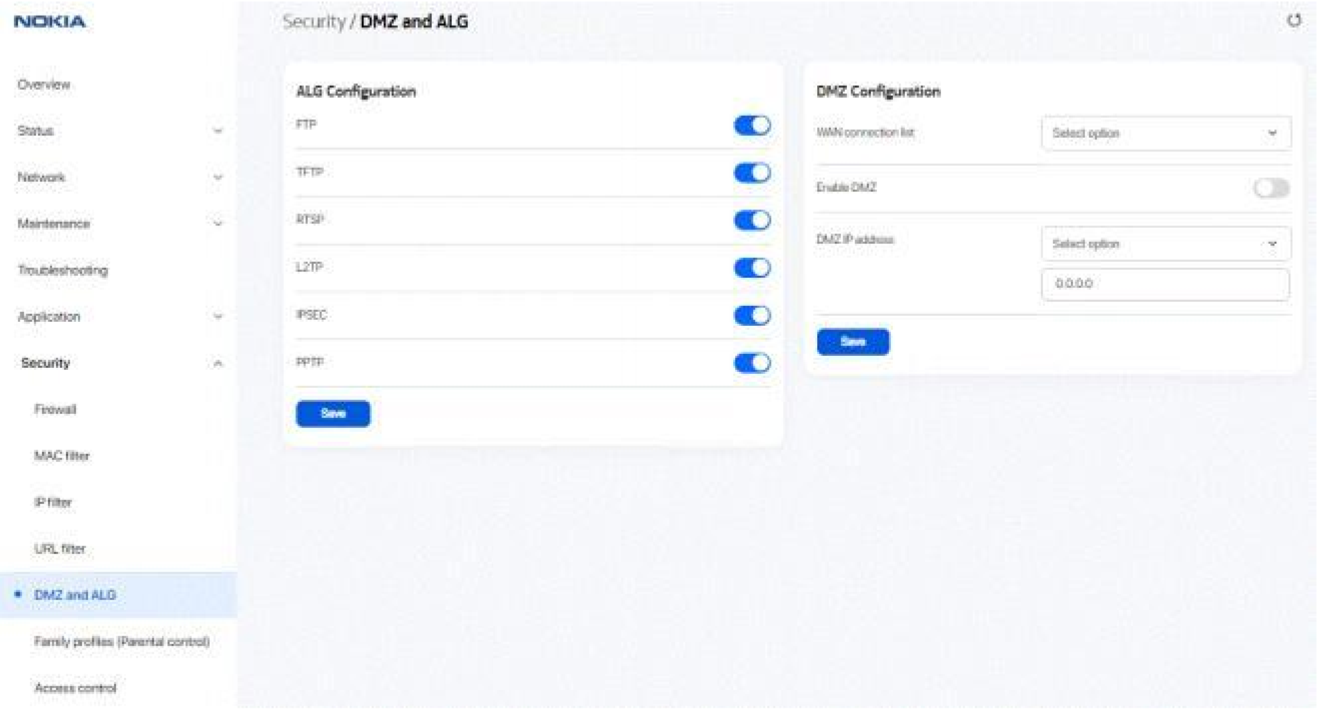
END OF STEPS

7.48 Configuring DMZ and ALG

1

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

Figure 7-48 *DMZ and ALG* page



2

Configure the following parameters:

Table 7-35 ALG Configuration parameters

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

3

Click **Save** .

4

Configure the following parameters:

Table 7-36 DMZ Configuration parameters

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

5

Click **Save**.

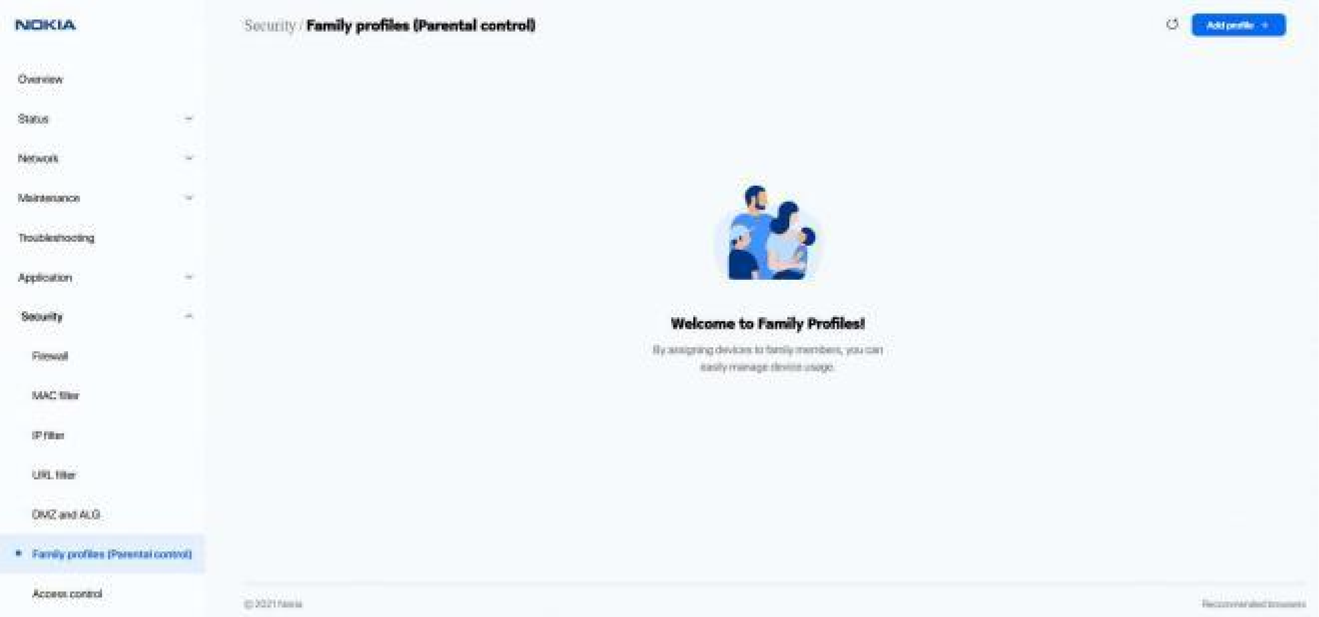
END OF STEPS

7.49 Configuring family profiles

1

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

Figure 7-49   Family profiles (Parental control) page



Welcome to Family Profiles!

By assigning devices to family members, you can easily manage device usage.

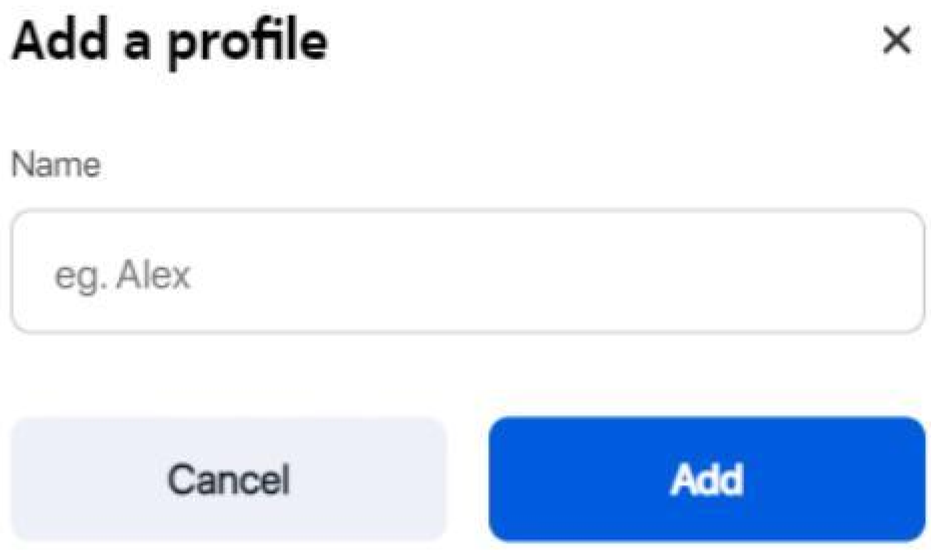
2

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

3

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

Figure 7-50 Add a profile page



Add a profile

Name

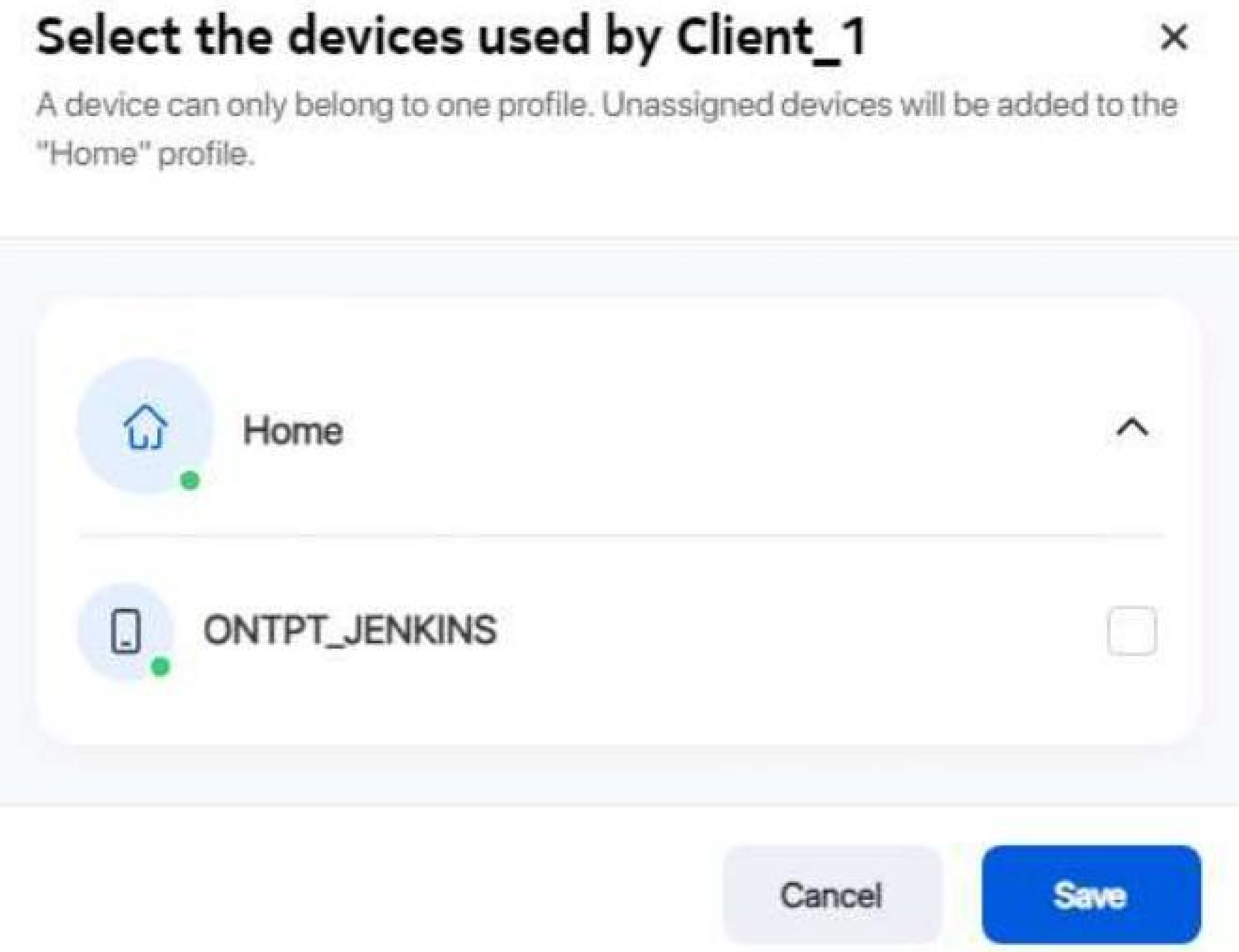
eg. Alex

4

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

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

Figure 7-51 Assign devices to family profile

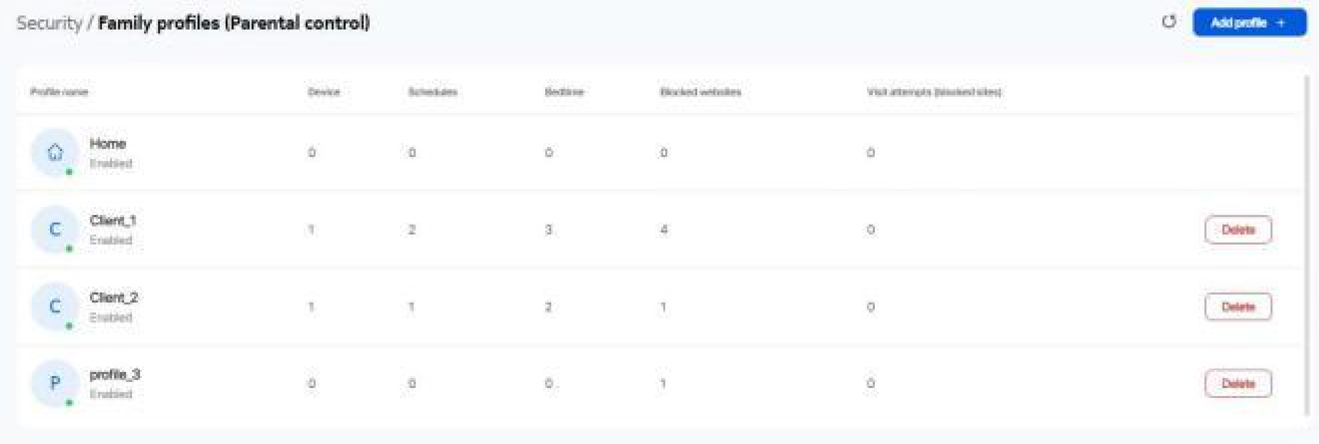


Select the devices used by Client_1

A device can only belong to one profile. Unassigned devices will be added to the "Home" profile.

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

Figure 7-52 Family profiles table



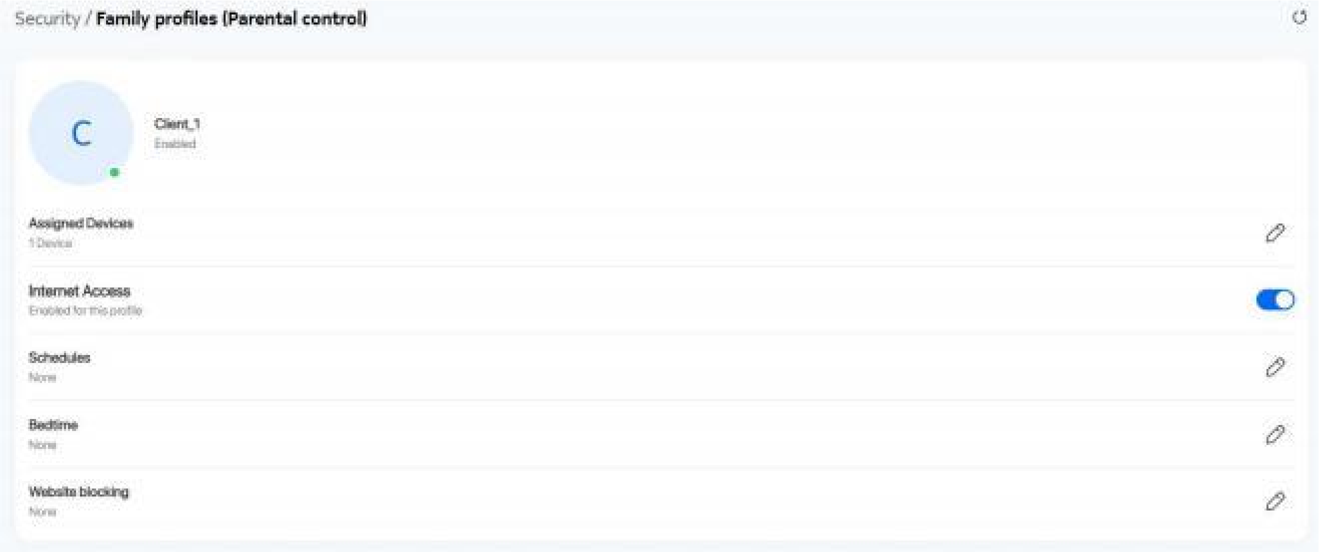
Security / **Family profiles (Parental control)**

Profile name	Device	Schedules	Bedtime	Blocked websites	Visit attempts (blocked sites)	
Home Enabled	0	0	0	0	0	
Client_1 Enabled	1	2	3	4	0	Delete
Client_2 Enabled	1	1	2	1	0	Delete
profile_3 Enabled	0	0	0	1	0	Delete

5

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

Figure 7-53 Family profile configuration page



Security / **Family profiles (Parental control)**

Client_1
Enabled

Assigned Devices
1 Device

Internet Access
Enabled for this profile

Schedules
None

Bedtime
None

Website blocking
None

6

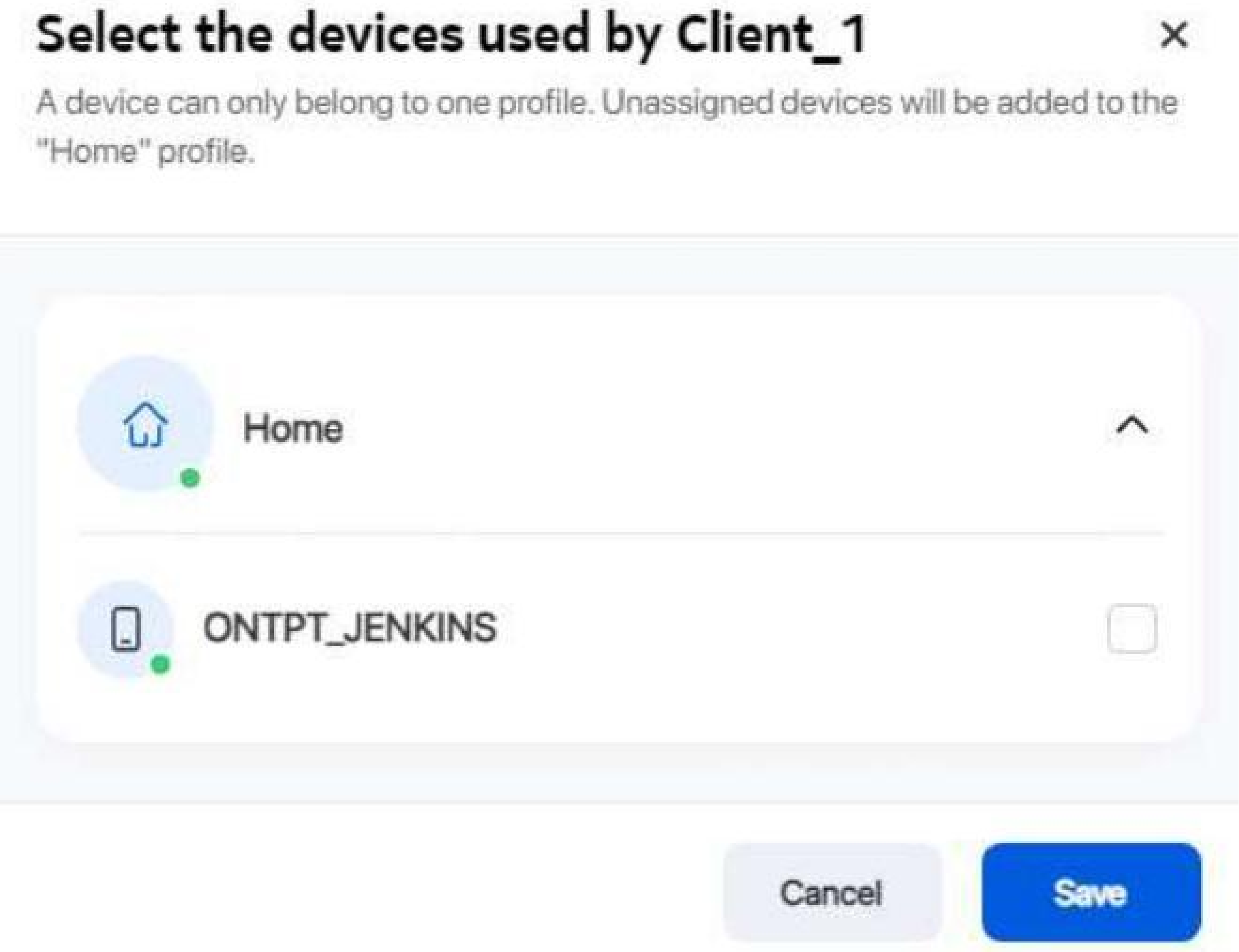
Select the **Internet Access** toggle button to enable internet access.

Assign more devices

7

Assign more devices to the profile, if required:

a. In the profile page, click the edit icon ✎ next to **Assigned Devices** to assign devices to the profile. The *Select the devices used by <profile>* page displays.



Select the devices used by Client_1

A device can only belong to one profile. Unassigned devices will be added to the "Home" profile.

b. Select the check box next to the device to assign to the profile.

c. Click **Save**.

Configure and enable schedules

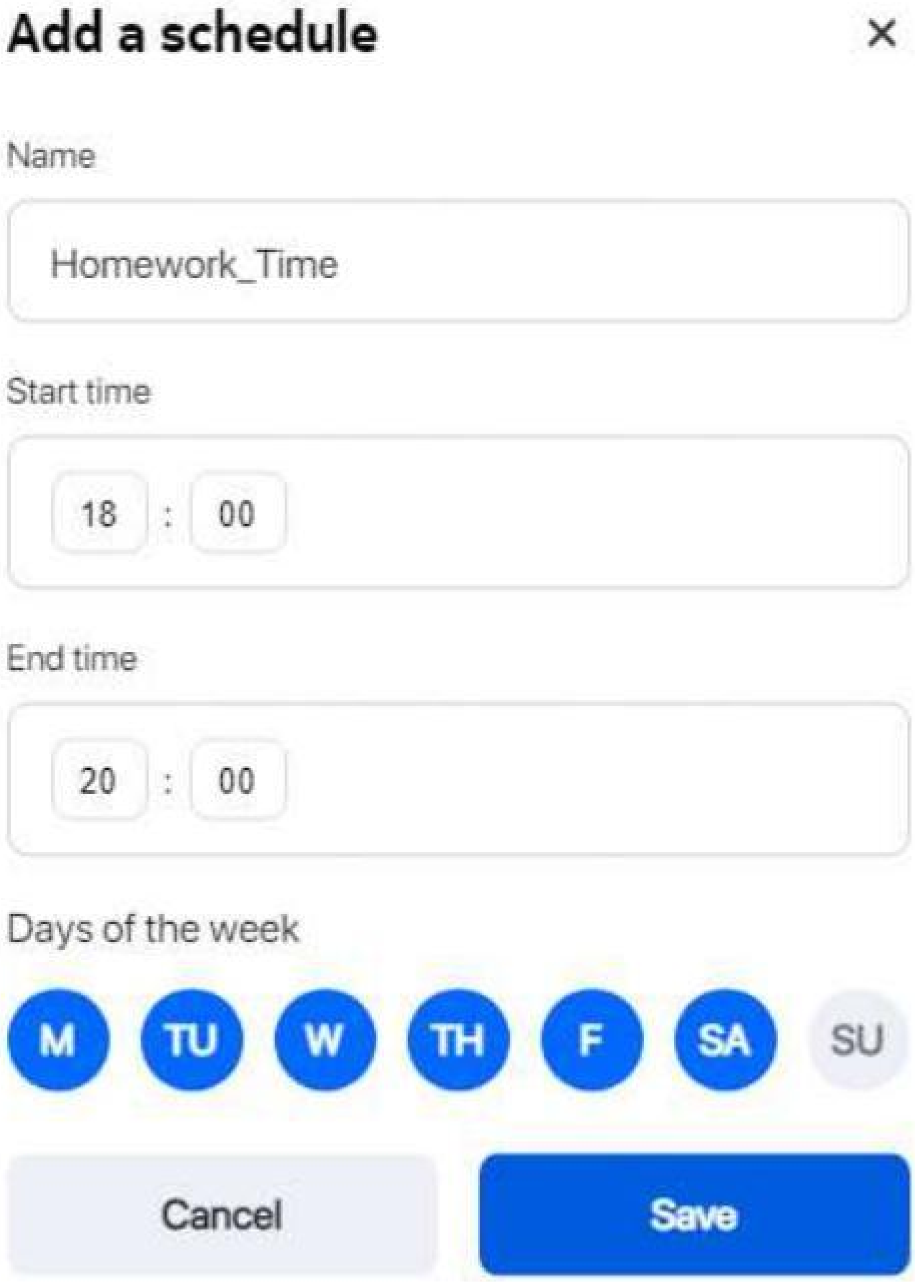
8

Configure schedules for the profile:

a. In the profile page, click the edit icon ✎ next to **Schedules** to create one or more schedules for the profile to set specific days and time slots when the Internet should be turned off.

b. Click **Create Schedule.**

c. In the *Add a schedule* page, configure the following:



Add a schedule

Name

Homework_Time

Start time

18 : 00

End time

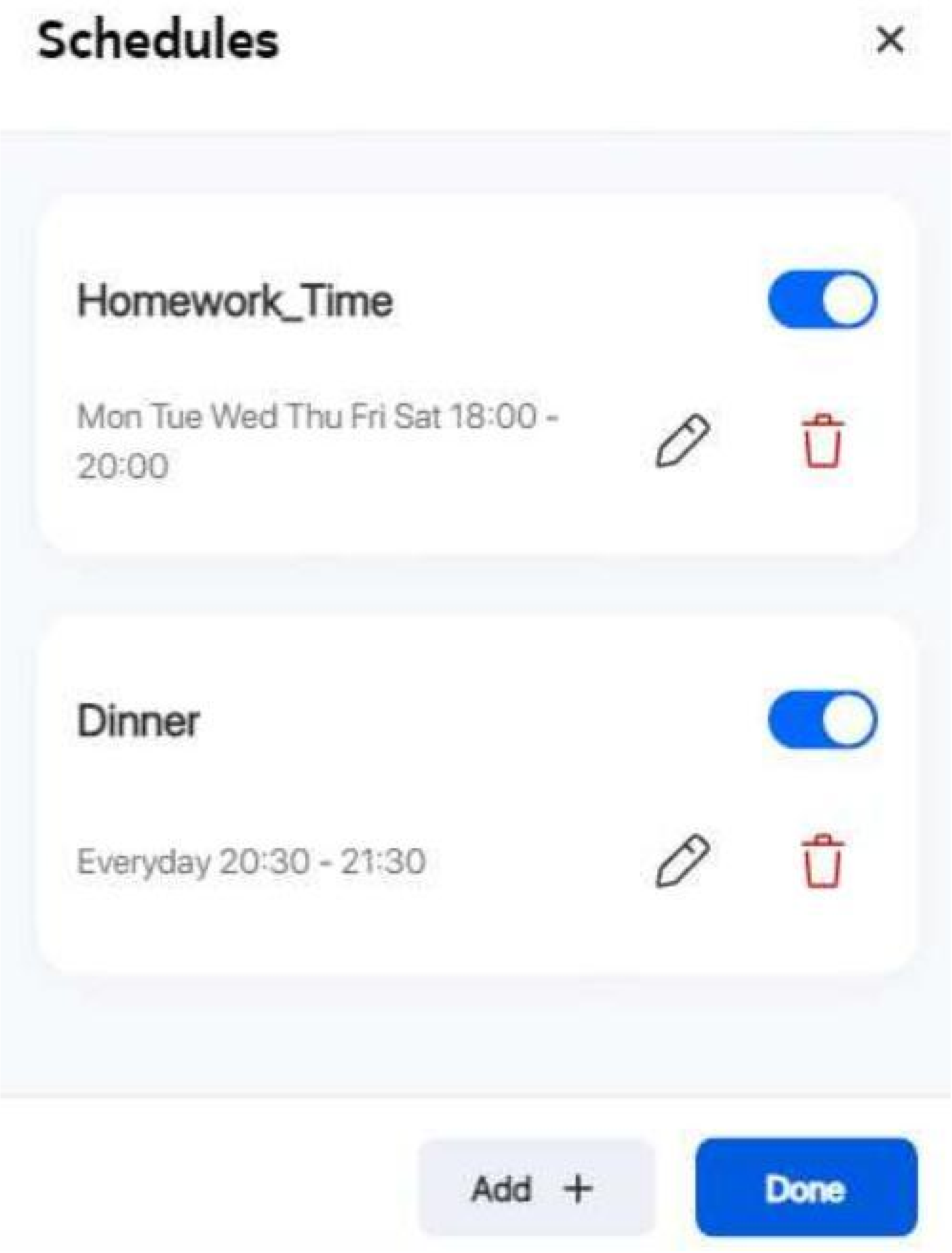
20 : 00

Days of the week

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

9

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



Schedules

Homework_Time

Mon Tue Wed Thu Fri Sat 18:00 - 20:00

Dinner

Everyday 20:30 - 21:30

Configure and enable bedtime

10

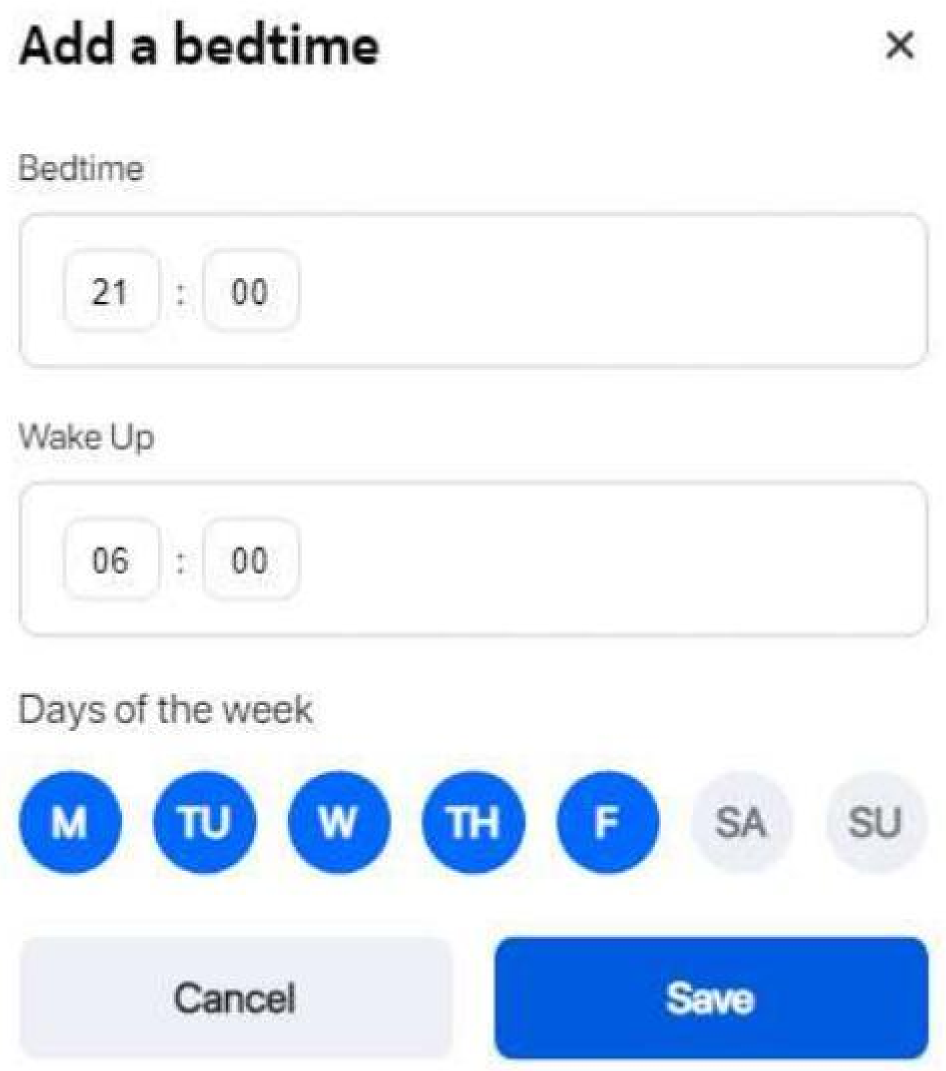
Configure bedtime for the profile:

a. In the profile page, click the edit icon 🖉 next to **Bedtime** to configure bedtime for the profile to automatically pause internet access at this time.

Only one bedtime can be assigned per day.

b. Click **Create Bedtime**.

c. In the *Add a bedtime* page, configure the following:



Add a bedtime

Bedtime: 21 : 00

Wake Up: 06 : 00

Days of the week: M, TU, W, TH, F selected; SA, SU not selected

1. Select the Bedtime, Wake Up time, and select the days of the week on which the bedtime will be in effect.
2. Click **Save**. The bedtime is created and listed in the *Bedtime* page.

d. In the *Bedtime* page, select the toggle button to enable the bedtime and click **Done**.

Configure website blocking

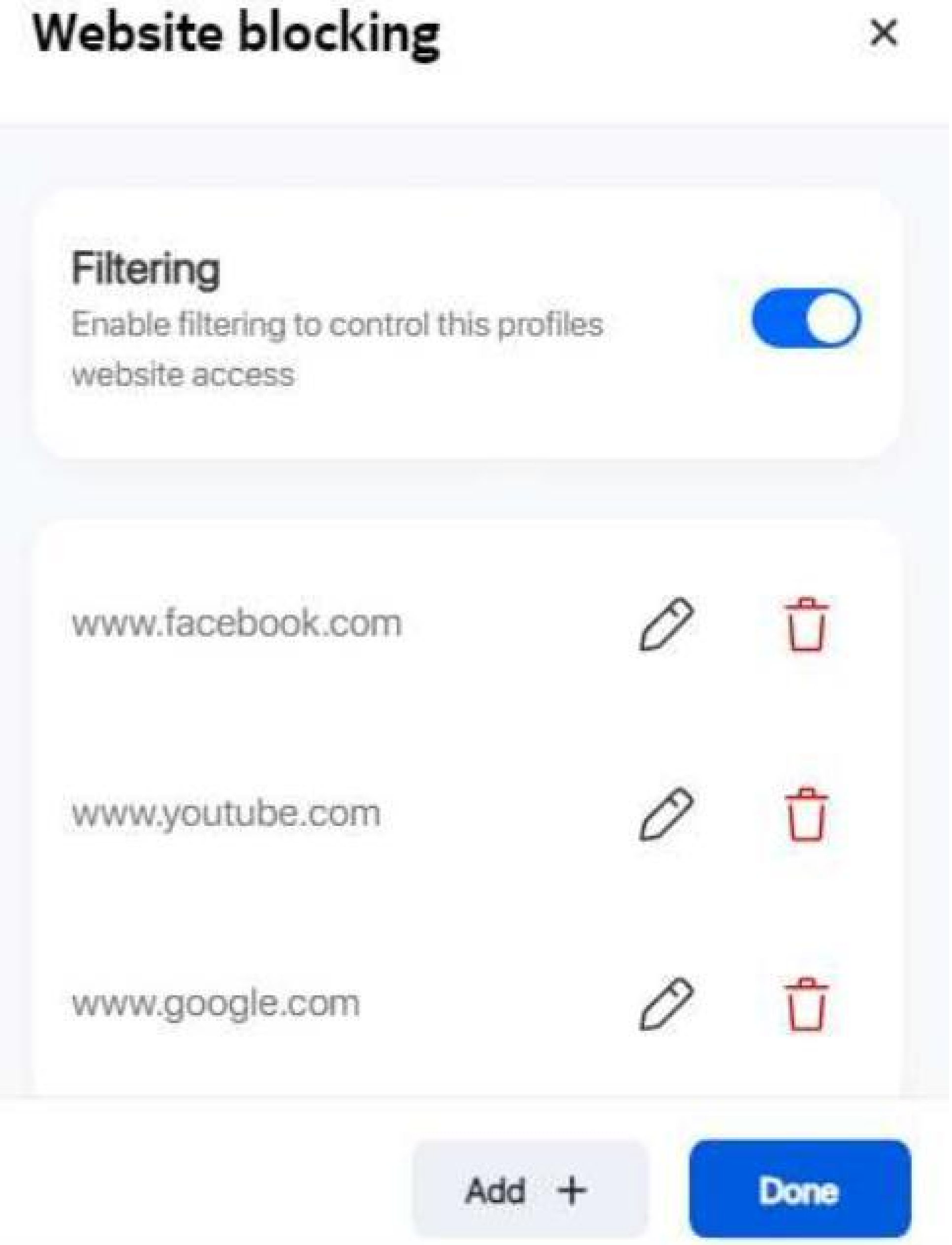
11

Configure website blocking for the profile:

a. In the profile page, click the edit icon ✎ next to **Website blocking** to control websites and services that devices assigned to the profile can access.

b. Click **Continue**

c. In the *Website blocking* page, perform the following:



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

4. Click **Add +** to add more website URLs to be blocked or click **Done**.

END OF STEPS

7.50 Configuring access control

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

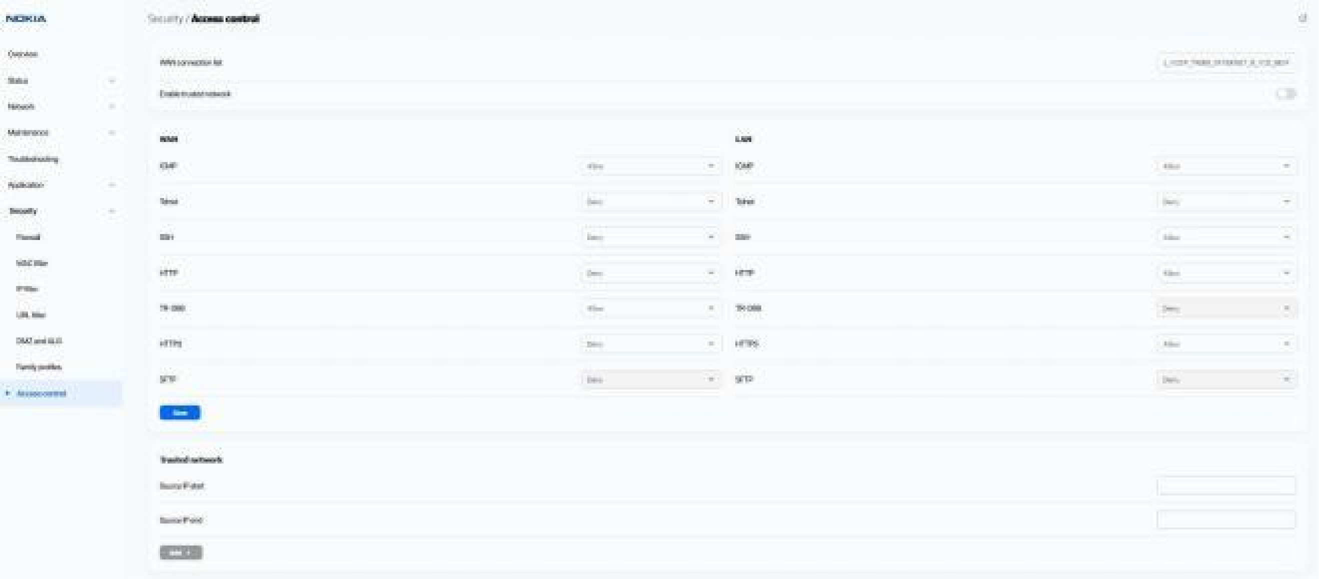
Note: ACL takes precedence over the firewall policy.

The trusted network will be shared for all WAN connections; it is not applied individually to a WAN connection.

1

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

Figure 7-54 Access control page



WAN connection list: [illegible]
Enable trusted network

WAN
ICMP: Allow
Telnet: Deny
SSH: Deny
HTTP: Deny
TR-069: Allow
HTTPS: Deny
SFTP: Deny

LAN
ICMP: Allow
Telnet: Deny
SSH: Allow
HTTP: Allow
TR-069: Deny
HTTPS: Allow
SFTP: Deny

Trusted network
Source IP start
Source IP end

2

Configure the following parameters:

Table 7-37 Access control parameters

Field	Description
WAN connection list	Select a WAN connection from the list.
Enable trusted network	Select the toggle button to enable a trusted network.

Table 7-37 Access control parameters (continued)

Field	Description
WAN	The following protocols are supported: ICMP, Telnet, SSH, HTTP, TR-069, HTTPS, SFTP. Select an access control level for each protocol: **Allow**, **Deny**, or **Trusted Network Only** LAN side: **Allow** or **Deny**
LAN	The following protocols are supported: ICMP, Telnet, SSH, HTTP, TR-069, HTTPS, SFTP. Select an access control level for each protocol: LAN side: **Allow** or **Deny**

3

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

4

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

Table 7-38 Trusted Network parameters

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

5

Click **Add +**.

END OF STEPS