Nokia WiFi Beacon

Beacon 10

Beacon 10 Product Guide

3TN-00200-AAAA-TCZZA
Issue 1
June 2023

Legal notice

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

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

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

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

No part of this document may be modified.

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

Contents

About this document....13

1 What's new....19
1.1 Overview....19
1.2 What's new in BBD Release 23.02....19

2 ANSI CPE safety guidelines....21
2.1 Overview....21
2.2 Safety instructions....21
2.3 Safety standards compliance....23
2.4 Electrical safety guidelines....26

3 ETSI CPE safety guidelines....27
3.1 Overview....27
3.2 Safety instructions....27
3.3 Safety standards compliance....28
3.4 Electrical safety guidelines....30

4 ETSI environmental and CRoHS guidelines....31
4.1 Overview....31
4.2 Environmental labels....31
4.3 Hazardous Substances Table (HST)....33
4.4 Other environmental requirements....33

5 Beacon 10 unit data sheet....35
5.1 Overview....35
5.2 Beacon 10 part numbers and identification....35
5.3 Beacon 10 general description....36
5.4 Beacon 10 software and installation feature support....39
5.5 Beacon 10 interfaces and interface capacity....39
5.6 Beacon 10 LEDs....41
5.7 Beacon 10 detailed specifications....42
5.8 Beacon 10 functional blocks....43
5.9 Beacon 10 responsible party....44
5.10 Beacon 10 special considerations....45

6 Install or replace a Beacon 10 47
6.1 Overview 47
6.2 Prerequisites 47
6.3 Recommended tools 47
6.4 Safety information 47
6.5 Install a Beacon 10....48
6.6 Replace a Beacon 10....50
6.7 Wall mount an Beacon 10 52

7 Configure Beacon 10 57
7.1 Overview 57
GUI overview 60
7.2 General configuration....60
7.3 Logging in to the web-based GUI....60
7.4 Beacon 10 WebGUI Menu 61
7.5 Viewing overview information....62
WAN Configuration 65
7.6 Overview 65
7.7 Configuring WAN Services....65
7.8 Viewing WAN Statistics 68
7.9 Configuring TR-069....71
7.10 Configuring TR-369....73
7.11 Configuring IP Routing 74
7.12 Configuring QoS....75
LAN Configuration 78
7.13 Overview 78
7.14 Configuring DHCP IPv4....78
7.15 Configuring DHCP IPv6....80
7.16 Configuring DNS 82
7.17 Viewing LAN Statistics 84
Wi-Fi Configuration....87
7.18 Overview 87
7.19 Configuring Wi-Fi Network 87
7.20 Configuring Guest Network 92
7.21 Viewing Network Map, Adding Wi-Fi Points and Removing Wi-Fi Points....94
7.22 Configuring Wireless 2.4 GHz....98
7.23 Configuring Wireless 5GHz....99

7.24 Configuring Wireless 6GHz 101
7.25 Viewing Wi-Fi Statistics 102
Devices 104
7.26 Overview 104
7.27 Viewing Device Information 104
Security Configuration 106
7.28 Overview 106
7.29 Configuring the Firewall 106
7.30 Configuring the MAC Filter 107
7.31 Configuring the IP Filter 109
7.32 Configuring Family Profiles 111
7.33 Configuring DMZ and ALG 122
7.34 Configuring Access Control 123
Advanced Settings 126
7.35 Overview 126
7.36 Configuring Port Forwarding 126
7.37 Configuring Port Triggering 127
7.38 Configuring DDNS 129
7.39 Configuring NTP 130
Maintenance 133
7.40 Overview 133
7.41 Configuring the Password 133
7.42 Backing Up the Configuration 135
7.43 Restoring the Configuration 135
7.44 Upgrading Firmware 136
7.45 Managing the Device 138
7.46 Diagnosing WAN Connections 138
7.47 Viewing Log Files 141
7.48 Viewing Container Management 142
Troubleshooting 144
7.49 Troubleshooting 144

List of tables

Table 2-1 Safety labels....22

Table 3-1 Safety labels....28

Table 3-2 Safety labels....29

Table 5-1 Beacon 10 identification....35

Table 5-2 Beacon 10 power supply ordering information....36

Table 5-3 Beacon 10 function detail....38

Table 5-4 Beacon 10 interface connection capacity....40

Table 5-5 Beacon 10 physical connections....40

Table 5-6 Beacon 10 LED indications....42

Table 5-7 Beacon 10 physical specifications....43

Table 5-8 Beacon 10 power consumption specifications....43

Table 5-9 Beacon 10 environmental specifications....43

Table 5-10 Responsible party contact information....44

Table 7-1 Beacon 10 WebGUI Menu....61

Table 7-2 *WAN services* parameters....66

Table 7-3 *WAN services* parameters....71

Table 7-4 *TR-069* parameters....72

Table 7-5 *TR-369* parameters....73

Table 7-6 *IP routing* parameters....74

Table 7-7 *QoS config* parameters....76

Table 7-8 *DHCP IPv4* parameters....79

Table 7-9 *Static DHCP* parameters....80

Table 7-10 *DHCP IPv6* parameters....81

Table 7-11 *LAN statistics* parameters....86

Table 7-12 *Add Wi-Fi network* parameters....89

Table 7-13 *Guest network* parameters....93

Table 7-14 *<Device>* parameters....96

Table 7-15 *Wireless 2.4 GHz* parameters....99

Table 7-16 Wireless 5 GHz....100

Table 7-17 Wireless 6 GHz....102

Table 7-18 *Firewall* parameters....107

Table 7-19 *MAC filter - Ethernet Interface* parameters 108
Table 7-20 *MAC filter - Wi-Fi SSID* parameters 109
Table 7-21 *IP filter* parameters 110
Table 7-22 *ALG Configuration* parameters 123
Table 7-23 *DMZ Configuration* parameters....123
Table 7-24 *Access control* parameters....125
Table 7-25 *Trusted Network* parameters....125
Table 7-26 *Port forwarding* parameters....127
Table 7-27 *Port triggering* parameters 128
Table 7-28 *DDNS* parameters....130
Table 7-29 *NTP* parameters....131
Table 7-30 *Change password* parameters....134
Table 7-31 *Device management* parameters....138
Table 7-32 *Diagnostics* parameters 139
Table 7-33 *Log* parameters....142
Table 7-34 *Container management* parameters 143
Table 7-35 *Troubleshooting* parameters 144

List of figures

Figure 2-1 Sample safety label 23
Figure 4-1 Products below MCV value label 32
Figure 4-2 Products above MCV value label 32
Figure 4-3 Recycling/take back/disposal of product symbol 34
Figure 5-1 Beacon 10 WiFi gateway/beacon 37
Figure 5-2 Beacon 10 physical connections 40
Figure 5-3 Beacon 10 LEDs....41
Figure 5-4 Single-residence WiFi CPE with Gigabit Ethernet....44
Figure 6-1 Beacon 10 connections 49
Figure 6-2 Beacon 10 connections 50
Figure 6-3 Beacon 10 wall mounting bracket....52
Figure 6-4 Beacon 10 in wall mount bracket....53
Figure 6-5 Beacon 10 wall mount bracket 53
Figure 6-6 Beacon 10 to wall mount connection....54
Figure 7-1 *Login* page....60
Figure 7-2 *Overview* table in *WAN services* page....65
Figure 7-3 *Create New Connection* page 66
Figure 7-4 *WAN Statistics* page....69
Figure 7-5 *WAN Statistics* page info 70
Figure 7-6 *TR-069* page....72
Figure 7-7 *TR-369* page....73
Figure 7-8 *IP routing* page 74
Figure 7-9 *QoS config* page (L2 Criteria)....75
Figure 7-10 *QoS config* page (L3 Criteria)....76
Figure 7-11 *DHCP IPv4* page....79
Figure 7-12 *DHCP IPv6* page 81
Figure 7-13 *DNS* page 83
Figure 7-14 *LAN statistics* page....85
Figure 7-15 *Wi-Fi network* page....87
Figure 7-16 *Add Wi-Fi network* page 88
Figure 7-17 *Wi-Fi network - SSID Configuration (2.4 GHz band)* page 90

Figure 7-18 *Wi-Fi network - SSID Configuration (5 GHz band)* page 90
Figure 7-19 *Wi-Fi network - SSID Configuration (6 GHz band)* page 91
Figure 7-20 *Guest network* page 93
Figure 7-21 *Network map* page 94
Figure 7-22 *<Device>* page 96
Figure 7-23 *Advanced settings - 2.4 GHz* tab 98
Figure 7-24 *Wireless 5 GHz* page 100
Figure 7-25 *Wireless 6 GHz* page 101
Figure 7-26 *Wi-Fi statistics* page 103
Figure 7-27 *Devices* page 104
Figure 7-28 *<Device>* page 105
Figure 7-29 *Firewall* page 106
Figure 7-30 *MAC filter* page 108
Figure 7-31 *IP filter* page 110
Figure 7-32 *Family profiles (Parental control)* page 111
Figure 7-33 *Add a profile* page 112
Figure 7-34 Assign devices to family profile 113
Figure 7-35 Family profiles table 114
Figure 7-36 Family profile configuration page 114
Figure 7-37 *DMZ and ALG* page 122
Figure 7-38 *Access control* page 124
Figure 7-39 *Port forwarding* page 126
Figure 7-40 *Port triggering* page 128
Figure 7-41 *DDNS* page 129
Figure 7-42 *NTP* page 131
Figure 7-43 *Change password* page 134
Figure 7-44 *Backup and restore* page 135
Figure 7-45 *Backup and restore* page 136
Figure 7-46 *Firmware upgrade* page 136
Figure 7-47 Example of upgrade status messages 137
Figure 7-48 *Device management* page 138
Figure 7-49 *Diagnostics* page 139
Figure 7-50 Example of ping results 140

Figure 7-51 Example of traceroute results 141

Figure 7-52 *Log* page 141

Figure 7-53 *Container management* page 143

Figure 7-54 *Troubleshooting* page 144

About this document

Purpose

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

Intended audience

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

The reader must be familiar with general telecommunications principles.

Safety information

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

Safety Information Examples

DANGER

Hazard

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

WARNING

Equipment Damage

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

CAUTION

Service Disruption

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

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

Acronyms and initialisms

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

Nokia quality processes

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

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

Documents

Documents are available using ALED or OLCS.

To download a ZIP file package of the customer documentation

1

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

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

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

1 What’s new

1.1 Overview

1.1.1 Purpose

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

1.1.2 Contents

1.1 Overview	19
1.2 What’s new in BBD Release 23.02	19

1.2 What’s new in BBD Release 23.02

The product guide is a new guide in BBD Release 23.02. In future releases, this section will provide tables of the feature and document changes applicable to this guide.

2 ANSI 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 in the North American or ANSI market.

2.1.2 Contents

2.1 Overview	21
2.2 Safety instructions	21
2.3 Safety standards compliance	23
2.4 Electrical safety guidelines	26

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 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.

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

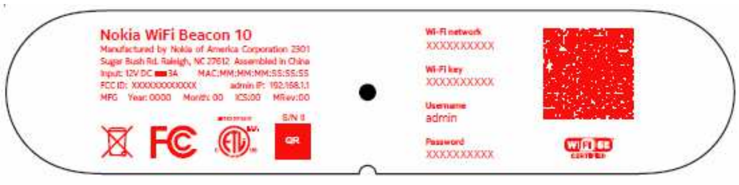
Table 2-1, "Safety labels" (p. 22) provides examples of the text in the various CPE safety labels.

Table 2-1 Safety labels

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

Figure 2-1, "Sample safety label" (p. 23) shows a sample safety label located on the bottom of the Beacon 10.

Figure 2-1 Sample safety label


Nokia WiFi Beacon 10
Manufactured by Nokia of America Corporation 2301
Sugar Bush Rd. Raleigh, NC 27612 Assembled in China
Input: 12V DC 3A MAC:MM:MM:MM:SS:SS:SS
FCC ID: XXXXXXXXXXXX admin IP: 192.168.1.1
MFG Year: 0000 Month: 00 ICS:00 MRev:00
S/N
QR
Wi-Fi network
XXXXXXXXXX
Wi-Fi key
XXXXXXXXXX
Username
admin
Password
XXXXXXXXXX

2.3 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.

2.3.1 FCC/ ISED warning

This section describes the FCC warning.

WARNING

Equipment Damage

Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s licence- exempt RSS(s). Operation is subject to the following two conditions:

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

ISED warning

L’émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d’Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L’exploitation est autorisée aux deux conditions suivantes :

1. L’appareil ne doit pas produire de brouillage;
2. L’appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d’en compromettre le fonctionnement.

The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Les dispositifs fonctionnan+D9t dans la bande de 5150 à 5250 MHz sont réservés uniquement pour une utilisation à l’intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

1. Operation shall be limited to indoor use only.
2. Operation on oil platforms, automobiles, trains, maritime vessels and aircraft shall be prohibited except for on large aircraft flying above 3,048 m (10,000 ft).

1. leur utilisation doit être limitée à l’intérieur seulement;
2. leur utilisation à bord de plateformes de forage pétrolier, d’automobiles, de trains, de navires maritimes et d’aéronefs doit être interdite, sauf à bord d’un gros aéronef volant à plus de 3 048 m (10 000 pi) d’altitude.

This equipment complies with Innovation, Science and Economic Development Canada RF exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated to ensure a minimum of 23cm spacing to any person at all times.

Cet équipement est conforme aux limites d'exposition RF d'Innovation, Science et Développement économique Canada établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé de manière à assurer un espacement d'au moins 23cm avec toute personne en tout temps.

2.3.2 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.

2.3.3 Energy-related products standby and off modes compliance

Hereby, Nokia declares that the Beacon 10 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 10 devices qualify as high network availability (HiNA) equipment. Since the main purpose of Beacon 10 devices is to provide network functionality with HiNA 7 days/24 hours, the modes Off/Standby, Power Management, and Networked Standby are inappropriate.

For information about the type and number of network ports, see 5.5 “Beacon 10 interfaces and interface capacity” (p. 39) in Chapter 5, “Beacon 10 unit data sheet”.

For information about power consumption, see 5.7 “Beacon 10 detailed specifications” (p. 42) in Chapter 5, “Beacon 10 unit data sheet”.

2.3.4 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.

2.3.5 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.

2.3.6 Resistibility requirements compliance

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

2.4 Electrical safety guidelines

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

Beacon 10 devices are compliant with the following standards

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

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

2.4.1 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:

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

3 ETSI CPE safety guidelines

3.1 Overview

3.1.1 Purpose

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

3.1.2 Contents

3.1 Overview	27
3.2 Safety instructions	27
3.3 Safety standards compliance	28
3.4 Electrical safety guidelines	30

3.2 Safety instructions

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

3.2.1 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.

3.2.2 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 3-1, “Safety labels” (p. 28) provides sample safety labels.

Table 3-1 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.

3.3 Safety standards compliance

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

3.3.1 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

3.3.2 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 3-2, “Safety labels” (p. 29) provides examples of the text in the various CPE safety labels.

Table 3-2 Safety labels

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

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

3.3.3 Environmental standard compliance

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

3.3.4 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.

3.3.5 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.

3.3.6 Acoustic noise emission standard compliance

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

3.4 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.

3.4.1 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.

3.4.2 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.

4 ETSI environmental and CRoHS guidelines

4.1 Overview

4.1.1 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.

4.1.2 Contents

4.1 Overview	31
4.2 Environmental labels	31
4.3 Hazardous Substances Table (HST)	33
4.4 Other environmental requirements	33

4.2 Environmental labels

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

4.2.1 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.

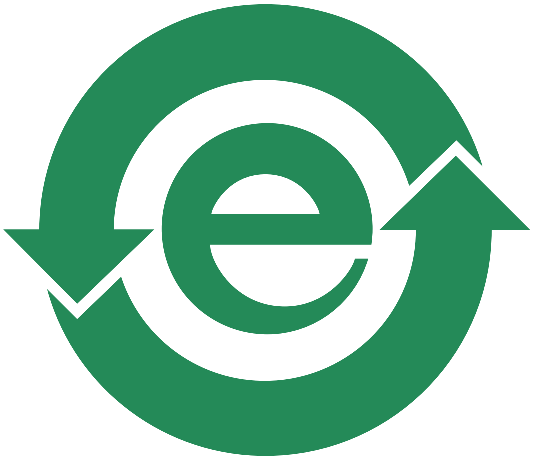
4.2.2 Environmental labels

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

Products below Maximum Concentration Value (MCV) label

Figure 4-1, “Products below MCV value label” (p. 32) shows the label that indicates a product is below the maximum concentration value, as defined by standard SJ/T11363-2006 (Requirements for Concentration Limits for Certain Hazardous Substances in Electronic Information Products). Products with this label are recyclable. The label may be found in this documentation or on the product.

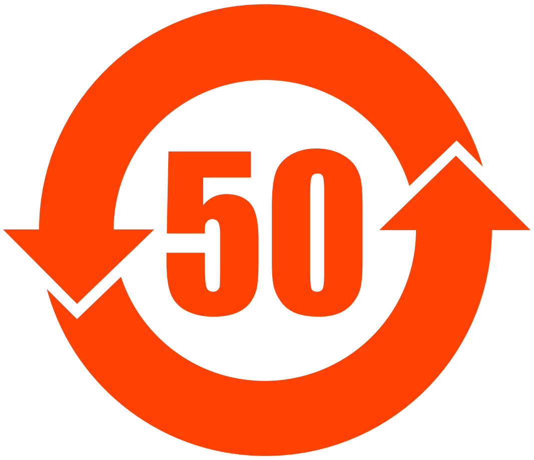
Figure 4-1 Products below MCV value label



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

Figure 4-2, “Products above MCV value label” (p. 32) shows the label that indicates a product is above the maximum concentration value, as defined by standard SJ/T11363-2006 (Requirements for Concentration Limits for Certain Hazardous Substances in Electronic Information Products). The number contained inside the label indicates the Environment-Friendly User Period (EFUP) value. The label may be found in this documentation or on the product.

Figure 4-2 Products above MCV value label



Together with major international telecommunications equipment companies, Nokia has determined it is appropriate to use an EFUP of 50 years for network infrastructure equipment and an EFUP of 20 years for handsets and accessories. These values are based on manufacturers' extensive practical experience of the design, manufacturing, maintenance, usage conditions, operating environments, and physical condition of infrastructure and handsets after years of service. The values reflect minimum values and refer to products operated according to the intended use conditions. See 4.3 “Hazardous Substances Table (HST)” (p. 32) for more information.

4.3 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

4.4 Other environmental requirements

Observe the following environmental requirements when handling the WiFi Beacon.

4.4.1 WiFi Beacon environmental requirements

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

4.4.2 Storage

According to ETS 300-019-1-1 - Class 1.1, storage of CPE equipment must be in Class 1.1, weather-protected, temperature-controlled locations.

4.4.3 Transportation

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

4.4.4 EU RoHS

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

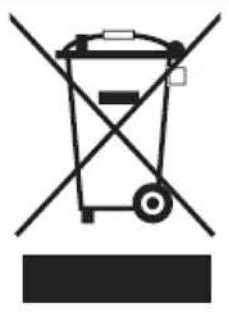
Nokia has implemented a material/substance content management process. The process is described in: Nokia process for ensuring RoHS Compliance (1AA002660031ASZZA). This ensures compliance with the European Union Directive 2011/65/EU on the Restriction of the Use of Certain Hazardous Substances in Electrical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

4.4.5 End-of-life collection and treatment

Electronic products bearing or referencing the symbol shown in Figure 4-3, “Recycling/take back/disposal of product symbol” (p. 33), when put on the market within the European Union (EU), shall be collected and treated at the end of their useful life, in compliance with applicable EU and local legislation. They shall not be disposed of as part of unsorted municipal waste. Due to materials that may be contained in the product, such as heavy metals or batteries, the environment and human health may be negatively impacted as a result of inappropriate disposal.

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

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



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

There can be different requirements for collection and treatment in different member states of the European Union.

In compliance with legal requirements and contractual agreements, where applicable, Nokia will offer to provide for the collection and treatment of Nokia products bearing the logo shown in Figure 4-3, “Recycling/take back/disposal of product symbol” (p. 34) at the end of their useful life, or products displaced by Nokia equipment offers. For information regarding take-back of equipment by Nokia, or for more information regarding the requirements for recycling/disposal of product, contact your Nokia account manager or Nokia take back support at sustainability.global@nokia.com.

5 Beacon 10 unit data sheet

5.1 Overview

5.1.1 Purpose

This chapter describes the Beacon 10 unit data sheet.

5.1.2 Contents

5.1 Overview	35
5.2 Beacon 10 part numbers and identification	35
5.3 Beacon 10 general description	36
5.4 Beacon 10 software and installation feature support	39
5.5 Beacon 10 interfaces and interface capacity	39
5.6 Beacon 10 LEDs	41
5.7 Beacon 10 detailed specifications	42
5.8 Beacon 10 functional blocks	43
5.9 Beacon 10 responsible party	44
5.10 Beacon 10 special considerations	45

5.2 Beacon 10 part numbers and identification

Table 5-1, “Beacon 10 identification” (p. 35) provides part numbers and identification information for the Beacon 10.

Table 5-1 Beacon 10 identification

Ordering part number	Provisioning number	Description	CLEC	CPR	ECI/ Bar code
3TN 00195 AA	3TN 00200 AA	Beacon 10, US plug, 10G WAN, 1x2.5G+2x1G LAN, 2x2+4x4+4x4 11ax Wi-Fi6E	BVMLW10FRA	—	—

Table 5-2, “Beacon 10 power supply ordering information” (p. 36) provides power supply ordering information for the Beacon 10.

Table 5-2 Beacon 10 power supply ordering information

Ordering part number	Manufacturer	Applicable power supply model	Power information	Compliance detail	Notes
Kit: 3TN 00195 AA EMA: 3TN 00200 AA	Honor	ADS-40FKJ-12N 12036EPCU/ 9040108111201202R (3FE49227NCAA)	12V 2.5A 30W AC/DC power adapter	ANSI municipality US, FCC/ETL	2-pin US input plug
	Keli	KL-WA120300-A1/SW-WB042N (3FE49227ANAA)	12V 3A 36W AC/DC power adapter		

5.3 Beacon 10 general description

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

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

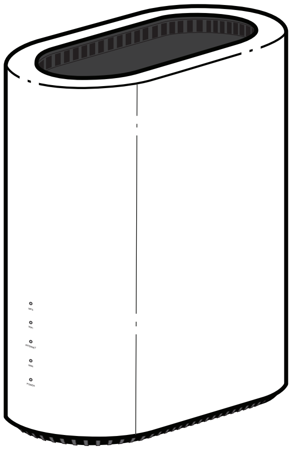
Note: The Nokia WiFi Care Portal can be accessed by the end user and the operator.

Beacon 10 can be deployed as either an Ethernet residential gateway or a WiFi beacon in the Nokia WiFi solution. The residential gateway is the central point of the mesh network providing access to the broadband network (Internet) while the beacon aids with extending the WiFi coverage to every corner of the home, providing seamless roaming to wireless connected devices.

The Beacon 10 has built-in concurrent triband WiFi 802.11a/b/g/n/ac/ax networking with triple-play capability. Beacon 10 devices can be configured using the Nokia WiFi Mobile App, which can be downloaded on both iOS and Android devices.

The following figure shows the Beacon 10.

Figure 5-1 Beacon 10 WiFi gateway/beacon



The Beacon 10 provides the following functions and benefits.

- Tri-band Wifi6: concurrent IEEE 802.11b/g/n/ax 2x2 2.4 GHz, 802.11 a/n/ac/ax 2x2 5.2 GHz, and 802.11 a/n/ac/ax 4x4 5.8 GHz
- Automatically decide on wireless router mode and beacon mode in a mesh network
- Three 1000/100/10Base-T interface with RJ-45 connectors
- Nokia intelligent Easy Mesh
- Embedded edge analytics optimize network performance in real-time

Benefits:

- OFDMA and MU-MIMO are multiuser technologies that enable simultaneous bidirectional communication between an access point (AP) and end users. While MU-MIMO increases capacity and efficiency in high-bandwidth applications like mission-critical voice calls and video streaming, OFDMA is ideal for low-bandwidth, small-packet applications such as IoT sensors
- PHY rate up to 574 Mb/s for 2.4 GHz, 1200 M b/s for low 5 GHz, and 2400 Mb/s for High 5 GHz
- Improves connection speeds throughout the home and provides Wi-Fi where typically there would be none
- Better mesh performance by using dedicate 4x4 5G radio for Wi-Fi backhaul seamless roaming (IEEE 802.11k and 802.11v)
- Client steering, channel optimization
- Real-time wireless spectrum scan and analysis
- High quality of service (QoS) video over Wi-Fi
- Ease of setup and user intuitive information

The table below lists additional function detail:

Table 5-3 Beacon 10 function detail

Function	Detail
Installation	Desk mounted
Interfaces	• Three RJ45 Gigabit Ethernet LAN ports; one can be used as Ethernet backhaul link • Supports 2+4+4 802.11a/b/g/n/ac/ax 2.4 GHz wireless LAN (WLAN) interface • Supports 2+4+4 802.11a/b/g/n/ac/ax 5.2 GHz wireless LAN (WLAN) interface • Supports 2+4+4 802.11a/b/g/n/ac/ax 5.8 GHz wireless LAN (WLAN) interface • Maximum effective isotropic radiated power (EIRP) on 2.4 GHz up to 1000 mW, 5.2 GHz (5G low band) up to 1000 mw, and 5.8 GHz (5G high band) up to 2 W • WPA support including WPA2 and WPA3 Personal encryption • Nokia Design for Security (DFSEC) requirement compliant • 64-bit and 128-bit Wired Equivalent Privacy (WEP) support
Router mode	• IPv4 and IPv6 • Point-to-Point Protocol over Ethernet (PPPoE) and IP over Ethernet (IPoE) • Network Address Translation (NAT), demilitarized zone (DMZ) and firewall • Dynamic Host Configuration Protocol (DHCP) and domain name system (DNS) proxy • Internet Group Management Protocol (IGMP) v2/v3 • LXC container and TR157 Software module management • Supports TR-069 • Supports virtual private network (VPN) pass- through for Point-to-Point Tunneling protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and IPSec • Port forwarding and DMZ/dynamic domain name system (DDNS) • Flexible video delivery options over Ethernet or wireless • Nokia WiFi mesh middleware
Beacon mode	• Supports IPv4 • Supports TR-069/XMPP • Supports VPN pass-through for PPTP, L2TP and IPSec • IGMP v2/v3 snooping • Flexible video delivery options over Ethernet or wireless • Nokia WiFi mesh middleware
LED	• LEDs for simple and intuitive status indication
Regulatory compliance	• ETL • FCC Part 15 • CB

5.3.1 TR-069 object support for WiFi parameters

The Beacon 10 supports the status retrieval and configuration of the following WiFi parameters via TR-069:

- Channel

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

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

5.3.2 Communication method to Nokia cloud management solution

The Beacon 10 communicates to the Nokia cloud management solution through MQTT and https.

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

5.3.3 TR-157 Software Module Managements

Beacon 10 can support LXC container for third party software components. Life cycle of 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.
- Set software component execution environment via SoftwareModules.ExecEnv.
- Run software component and get the execution status via SoftwareModules.ExecutionUnit.

Note: The available memory for third party applications needs a detailed study, considering the actual memory load of the current hardware, software, Beacon software evolution over long time and the projected use by a third party application of the software. Therefore, Nokia suggests to review this case by case. Please contact your Nokia support representative for more information.

5.3.4 TR-069 authentication using TLS and CA certificates

Beacon 10 devices support encrypted remote TR-069 management using TLS, as well as ACS authentication using SHA-256 pre-installed certificates.

If the ACS URL is set to the https://... format, by default, the connection will use TLS without authentication mode. The Beacon 10 can also authenticate the ACS using a pre-installed CA certificate.

5.4 Beacon 10 software and installation feature support

For information on installing or replacing the Beacon 10, see Chapter 6, “Install or replace a Beacon 10”.

5.5 Beacon 10 interfaces and interface capacity

The table below describes the supported interfaces and interface capacity for Beacon 10 devices.

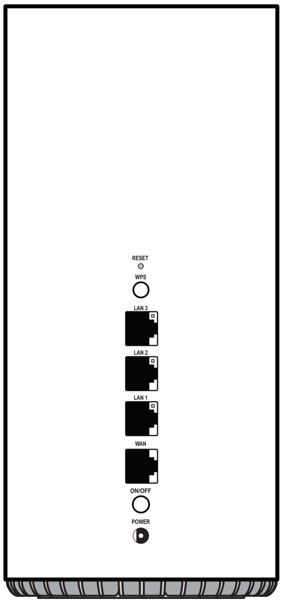
Table 5-4 Beacon 10 interface connection capacity

Device type and model	Maximum capacity								
	POTS	100/ 10 BASE-T	1000/ 100/10 BASE-T	RF video (CATV)	10GE WAN	2.5GE LAN	1GE LAN	Local craft	USB3. 1(gen1)
Beacon 10	—	—	3	—	1	1	2	—	—

5.5.1 Beacon 10 connections and components

Figure 5-2, "Beacon 10 physical connections" (p. 40) shows the physical connections for Beacon 10.

Figure 5-2 Beacon 10 physical connections



38359

The table below describes the physical connections for Beacon 10 devices.

Table 5-5 Beacon 10 physical connections

Connection	Description
On/Off button	This button powers the unit on or off.
LAN 1/LAN 2/LAN 3	This connection is provided through Ethernet RJ-45 connectors. Up to three 1000/100/10 Base-T Ethernet interfaces are supported. The Ethernet ports can support both data and in-band video services on all three interfaces.
WAN port	This connection is provided through an RJ-45 Gigabit Ethernet interface.

Table 5-5 Beacon 10 physical connections (continued)

Connection	Description
WPS ON/Off button	This button is used to start the WiFi Protected Setup (WPS) for new WiFi devices.
Reset button	Pressing the Reset button for less than 10 seconds reboots the Beacon; pressing the Reset button for 10 seconds or more restores the Beacon to its factory defaults.
Power input	This connection is provided through the power connector. A power cable fitted with a barrel connector is used to make the connection.

5.6 Beacon 10 LEDs

The circular top of the Beacon 10 functions as a multi-color LED indicator. The LED color and pulse rate acts as a signal to the home user, which indicates the state of the Beacon 10 and the quality of its backhaul link.

Figure 5-3 Beacon 10 LEDs

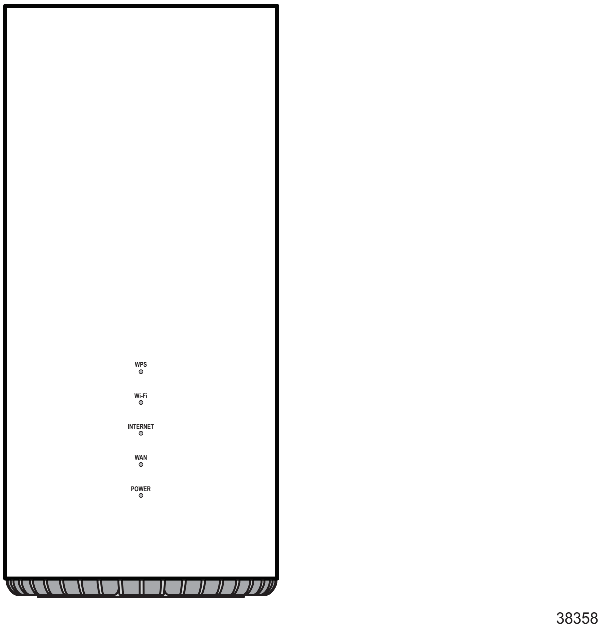


Table 5-6, “Beacon 10 LED indications” (p. 42) provides LED descriptions for the Beacon 10.

Table 5-6 Beacon 10 LED indications

LED	LED Color	LED behavior description
POWER	Off	No power
	Solid green	Power on out of mains supply, no battery alarms
	Blinking green	SW update
	Solid red	Failure at startup
WAN	Off	No WAN Ethernet cable connected. No physical uplink
	Solid green	WAN has a physical uplink and is synced at 10Gbps, 5Gbps, 2.5Gbps or 1Gbps
	Solid amber	WAN has a physical uplink and is synced at 100Mbps
INTERNET	Solid green	HSI WAN is connected: the device has an IP address assigned from IPCP, DHCP, PPPoE or static
	Solid Amber	Weak backhaul connection (for extender mode)
	Amber flashing	In CFG mode
	Solid Red	No backhaul connection (for extender mode)
	Green Flashing	PPPoE or DHCP connection is in progress
	Off (dark)	HSI WAN is not connected: a) there is no physical interface connection; b) the device is in bridged mode without an assigned IP address; the session has been dropped for reasons other than idle timeout
WPS	Solid green	WiFi protected setup link is up (negotiation and auto-configuration successful)
	Green Flashing	WiFi protected setup link activity (negotiation and auto-configuration ongoing)
	Solid red	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)
Wi-Fi	Solid green	WiFi enabled for at least 1 RF
	Off (dark)	WLAN is down
WAN/LAN RJ-45 connectors	Solid green	LAN link active
	Green Flashing	LAN traffic
	Off	LAN link is off or LOS

5.7 Beacon 10 detailed specifications

The table below lists the physical specifications for the Beacon 10.

Table 5-7 Beacon 10 physical specifications

Description	Specification
Length	188 mm (7.40 in.)
Width	101 mm (3.90 in.)
Height	220 mm (8.66 in.)
Weight [within ± 0.5 lb (0.23 kg)]	1570g (3.4 lb)

Table 5-8, “Beacon 10 power consumption specifications” (p. 43) lists the power consumption specifications for the Beacon 10.

Table 5-8 Beacon 10 power consumption specifications

Maximum power (Not to exceed)	Condition	Minimum power	Condition
36W	3 1000/100/10 Base-T Ethernet, WiFi operational	6.63W	Interfaces/services not provisioned

Table 5-9, “Beacon 10 environmental specifications” (p. 43) lists the environmental specifications for Beacon 10.

Table 5-9 Beacon 10 environmental specifications

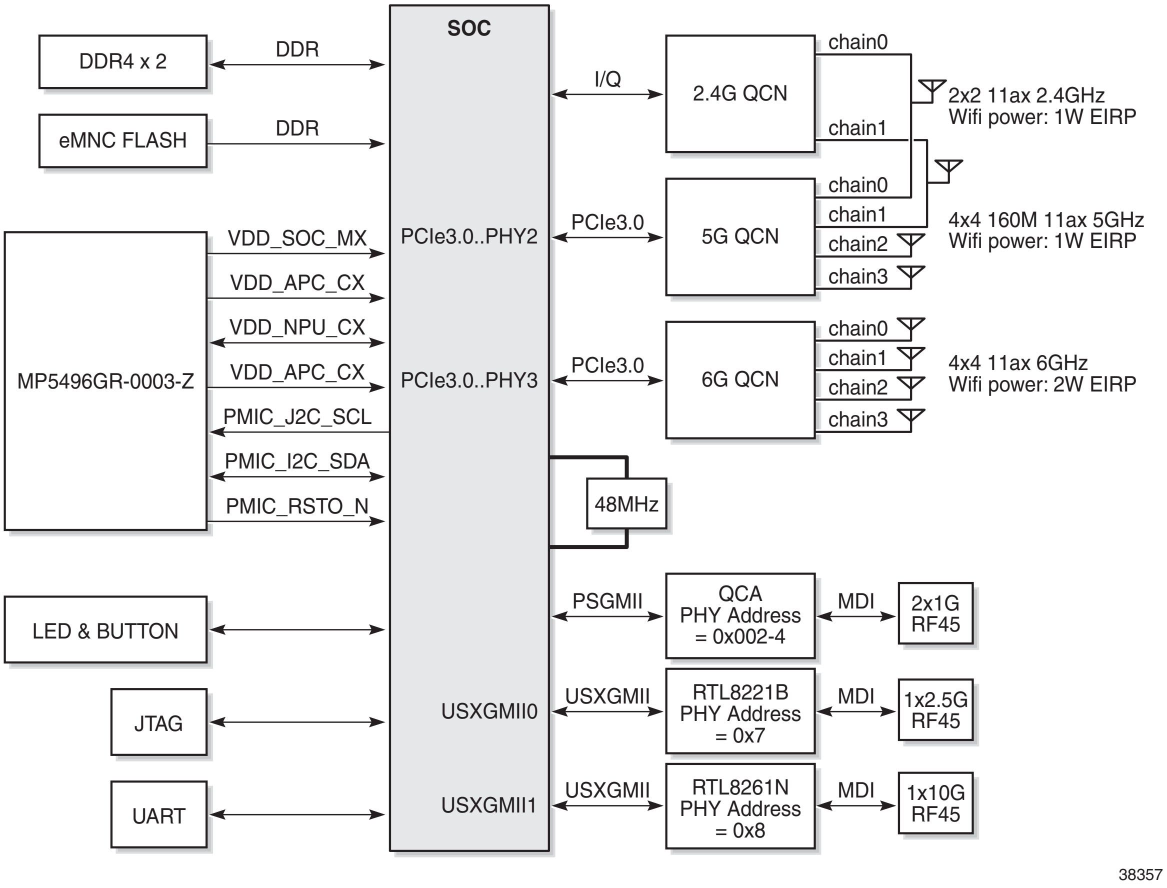
Mounting method	Temperature range and humidity	Altitude
On desk or shelf	Operating: -5°C to 45°C (23°F to 113°F) ambient temperature 95% relative humidity, non-condensing at 40°C	Contact your Nokia technical support representative for more information
	Storage: --25°C to 70°C (-4°F to 185°F)	

5.8 Beacon 10 functional blocks

Beacon 10 devices are single-residence units that support Wireless (WiFi) service. WiFi service on these devices is compliant with the IEEE 802.11 standard. In addition to the WiFi service, these devices transmit Ethernet packets to three RJ-45 Ethernet ports.

Figure 5-4, “Single-residence WiFi CPE with Gigabit Ethernet” (p. 44) shows the functional blocks for the Beacon 10.

Figure 5-4 Single-residence WiFi CPE with Gigabit Ethernet



5.9 Beacon 10 responsible party

Table 5-10, “Responsible party contact information” (p. 44) lists the party in the US responsible for this device.

Table 5-10 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/)	

5.10 Beacon 10 special considerations

This section describes the special considerations for Beacon 10 devices.

5.10.1 WiFi service

Beacon 10 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 10 devices supports the following IEEE standards and WiFi Alliance certifications (WFA100049 for 2x2, WFA100571 for 4x4):

- 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™
- Compliant for Easymesh R2

Nokia WiFi app configuration

The Nokia WiFi mobile app can be used to set up the Beacon 10 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 10 devices have HTML-based WiFi configuration GUIs.

5.10.2 Beacon 10 considerations and limitations

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

6 Install or replace a Beacon 10

6.1 Overview

6.1.1 Purpose

This chapter provides the steps to:

- Install a Beacon 10
- Replace a Beacon 10

6.1.2 Contents

6.1 Overview	47
6.2 Prerequisites	47
6.3 Recommended tools	47
6.4 Safety information	47
6.5 Install a Beacon 10	48
6.6 Replace a Beacon 10	50
6.7 Wall mount an Beacon 10	52

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.
- Iindoor units must be installed with cables that are suitably rated and listed for indoor use.
- See the detailed specifications in the Chapter 5, “Beacon 10 unit data sheet” for the temperature ranges for these devices.

6.5 Install a Beacon 10

1

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

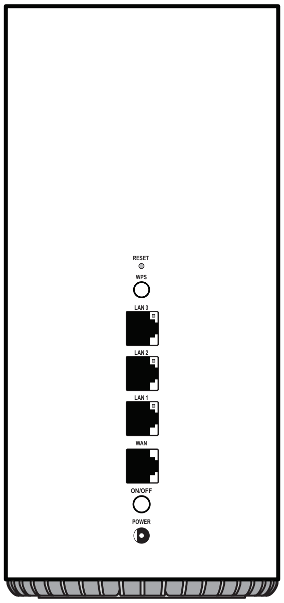
Note: The Beacon 10 cannot be stacked with another or with other equipment. The installation requirements are:

- 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 10 connections” (p. 49).

Figure 6-1 Beacon 10 connections



38359

3

Connect the Ethernet cables to the RJ-45 ports; see Figure 6-1, “Beacon 10 connections” (p. 49) for the location of the RJ-45 ports.

4

Connect the WAN cable to the RJ-45 WAN port; see Figure 6-1, “Beacon 10 connections” (p. 49) for the location of the RJ-45 WAN port.

5

Connect the power cable to the power connector.

Note: Units must be powered by a Listed or CE approved and marked limited power source power supply with a minimum output rate of 12 V dc, 2 A. The polarity of the power adapter plug must match the Beacon 10.

6

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

7

Verify the LEDs and voltage status.

8

Activate and test the services.

9

If necessary, reset the Beacon 10.

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

a. Locate the **Reset** button as shown in Figure 6-1, “Beacon 10 connections” (p. 49).

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

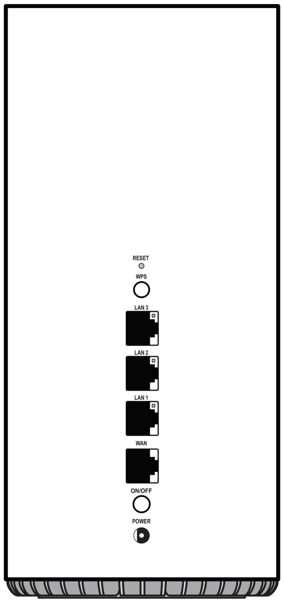
END OF STEPS

6.6 Replace a Beacon 10

1

Power down the unit by using the on/off power switch. See Figure 6-2, “Beacon 10 connections” (p. 49) for the connections on the Beacon 10.

Figure 6-2 Beacon 10 connections



38359

2

Disconnect the WAN, Ethernet, and power cables from the Beacon 10; see Figure 6-2, “Beacon 10 connections” (p. 50) for the connector locations on the Beacon 10.

3

Replace the Beacon 10 with the new device. The device can be placed on any flat surface, such as a desk or shelf.

4

Connect the Ethernet cables directly to the RJ-45 ports; see Figure 6-2, “Beacon 10 connections” (p. 50) for the location of the RJ-45 ports.

5

Connect the WAN cable directly to the RJ-45 port; see Figure 6-2, “Beacon 10 connections” (p. 50) for the location of the RJ-45 WAN port.

6

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 10.

7

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

8

Verify the LEDs and voltage status.

9

Activate and test the services.

10

If necessary, reset the Beacon 10.

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

a. Locate the Reset button on a Beacon 10 as shown in Figure 6-2, “Beacon 10 connections” (p. 50).

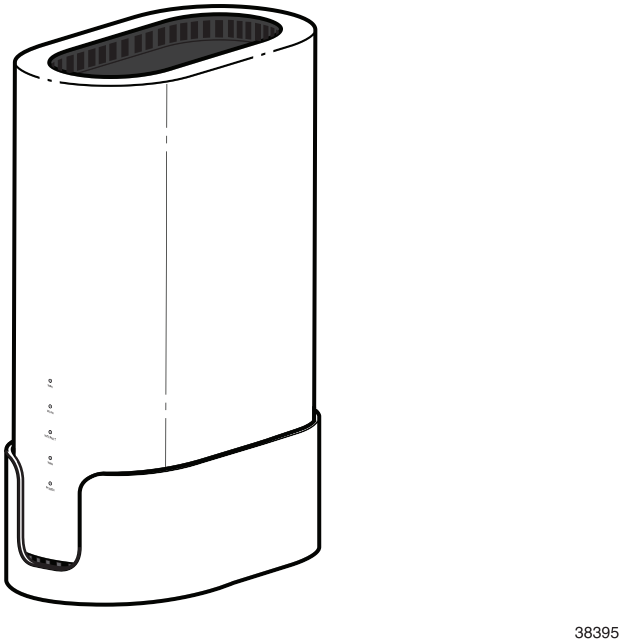
b. Insert the end of a straightened paper clip or other narrow object into the hole in the Reset button to reset the device.

End of steps

6.7 Wall mount an Beacon 10

This section provides the steps to mount an Beacon 10.

Figure 6-3 Beacon 10 wall mounting bracket



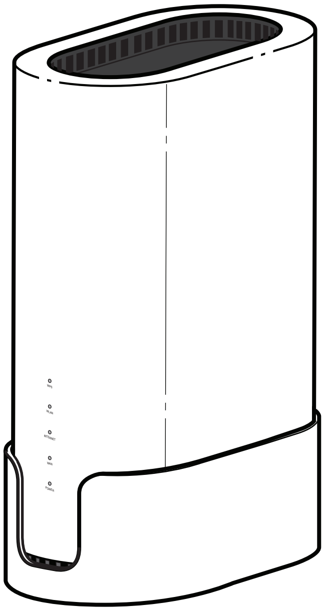
6.7.1 Procedure

Use this procedure to mount an Beacon 10 on a wall.

1

You can wall mount the Beacon 10 as shown in Figure 6-4, “Beacon 10 in wall mount bracket” (p. 53).

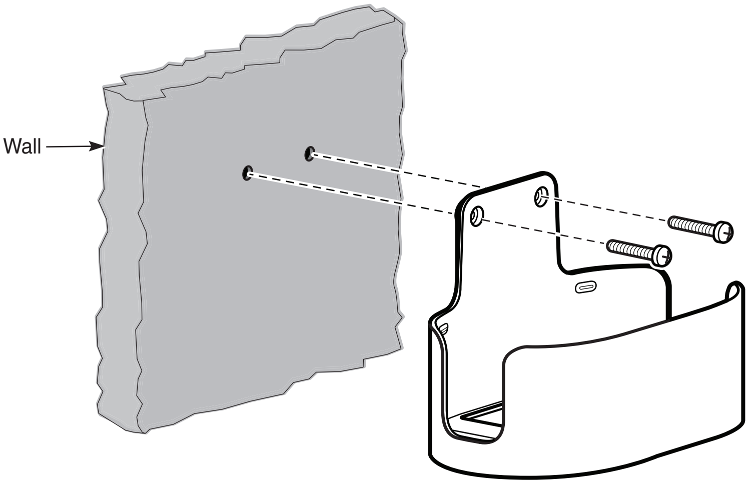
Figure 6-4 Beacon 10 in wall mount bracket



2

Mount the Beacon 10 on a wall using the wall mount bracket as shown in Figure 6-5, “Beacon 10 wall mount bracket” (p. 53).

Figure 6-5 Beacon 10 wall mount bracket



a. Determine the location of the two anchor holes for the wall mount bracket. The bracket can be used as a template for marking and drilling the holes.

   It is recommended to use a level to ensure that the ONT unit is installed horizontally.

b. Drill two holes into the wall and with the centers spaced 65 mm.

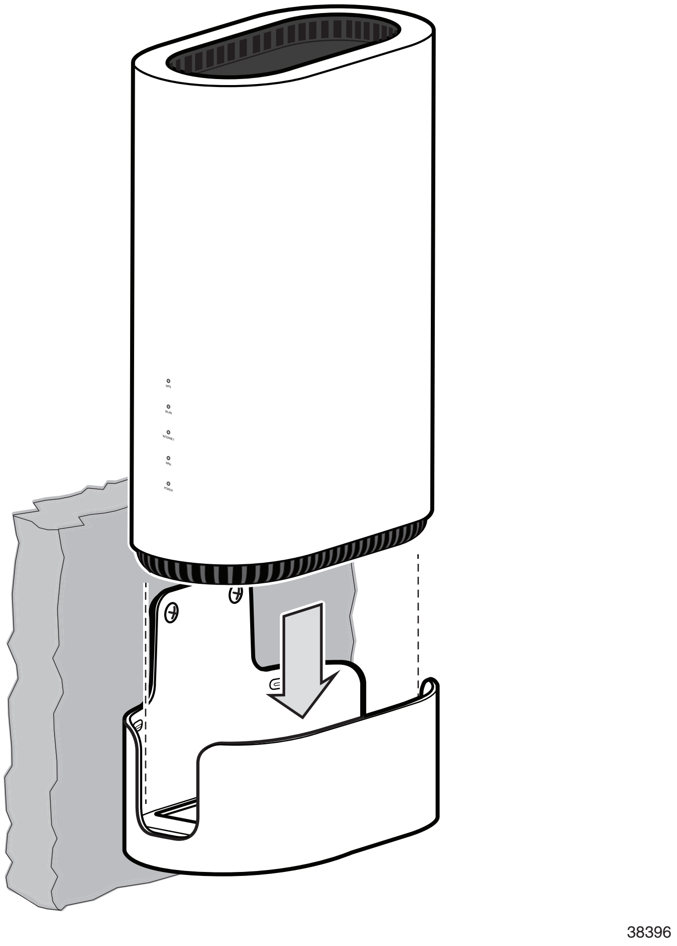
c. Insert the two mounting screws and optional anchors into the holes.

d. At this point, perform a test to ensure that the wall mount bracket fits securely over the screw heads. Mount the bracket flush to the wall so that it does not warp or twist.

e. Remove the wall mount bracket from the wall.

f. Install the Beacon 10 into the wall mount bracket by lifting the unit above the bracket and sliding it downward onto the bottom ledge of the bracket. See Figure 6-6, “Beacon 10 to wall mount connection” (p. 53).

Figure 6-6 Beacon 10 to wall mount connection



g. Connect the power cord and other cables to the Beacon 10.

END OF STEPS

7 Configure Beacon 10

7.1 Overview

7.1.1 Purpose

This chapter describes the WebGUI configuration procedures.

7.1.2 Contents

7.1 Overview	57
GUI overview	60
7.2 General configuration	60
7.3 Logging in to the web-based GUI	60
7.4 Beacon 10 WebGUI Menu	61
7.5 Viewing overview information	62
WAN Configuration	65
7.6 Overview	65
7.7 Configuring WAN Services	65
7.8 Viewing WAN Statistics	68
7.9 Configuring TR-069	71
7.10 Configuring TR-369	73
7.11 Configuring IP Routing	74
7.12 Configuring QoS	75
LAN Configuration	78
7.13 Overview	78
7.14 Configuring DHCP IPv4	78
7.15 Configuring DHCP IPv6	80
7.16 Configuring DNS	82
7.17 Viewing LAN Statistics	84
Wi-Fi Configuration	87
7.18 Overview	87
7.19 Configuring Wi-Fi Network	87

7.20 Configuring Guest Network 92
7.21 Viewing Network Map, Adding Wi-Fi Points and Removing Wi-Fi Points 94
7.22 Configuring Wireless 2.4 GHz 98
7.23 Configuring Wireless 5GHz 99
7.24 Configuring Wireless 6GHz 101
7.25 Viewing Wi-Fi Statistics 102
Devices 104
7.26 Overview 104
7.27 Viewing Device Information 104
Security Configuration 106
7.28 Overview 106
7.29 Configuring the Firewall 106
7.30 Configuring the MAC Filter 107
7.31 Configuring the IP Filter 109
7.32 Configuring Family Profiles 111
7.33 Configuring DMZ and ALG 122
7.34 Configuring Access Control 123
Advanced Settings 126
7.35 Overview 126
7.36 Configuring Port Forwarding 126
7.37 Configuring Port Triggering 127
7.38 Configuring DDNS 129
7.39 Configuring NTP 130
Maintenance 133
7.40 Overview 133
7.41 Configuring the Password 133
7.42 Backing Up the Configuration 135
7.43 Restoring the Configuration 135
7.44 Upgrading Firmware 136
7.45 Managing the Device 138
7.46 Diagnosing WAN Connections 138

7.47 Viewing Log Files	141
7.48 Viewing Container Management	142
Troubleshooting	144
7.49 Troubleshooting	144

GUI overview

This section provides an overview of the Beacon 10 WebGUI.

7.2 General configuration

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

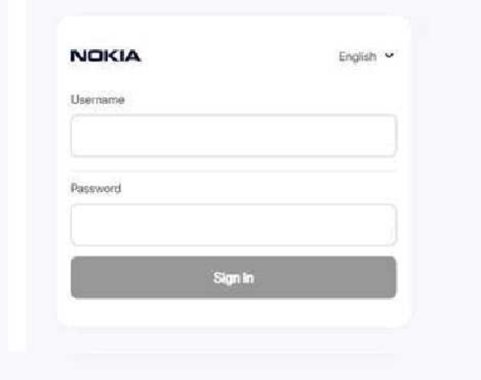
7.3 Logging in to the web-based GUI

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.*

Enter your username and password in the *Login* page, as shown in Figure 7-1, “Login page” (p. 60).

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

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

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

3

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

Note: To help protect the security of your Internet connection, the application displays a pop-up reminder to change both the 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

7.4 Beacon 10 WebGUI Menu

The following table lists the main menu and sub-menu options in the Beacon 10 WebGUI:

Table 7-1 Beacon 10 WebGUI Menu

Main Menu	Sub-menu	Procedure Reference
Overview	-	7.5 “Viewing overview information” (p. 62)
WAN	**WAN services**	7.7 “Configuring WAN Services” (p. 65)
WAN	**WAN statistics**	7.8 “Viewing WAN Statistics” (p. 68)
WAN	**TR-069**	7.9 “Configuring TR-069” (p. 71)
WAN	**TR-369**	7.10 “Configuring TR-369” (p. 73)
WAN	**IP routing**	7.11 “Configuring IP Routing” (p. 74)
WAN	**Qos config**	7.12 “Configuring QoS” (p. 75)
LAN	**DHCP IPv4**	7.14 “Configuring DHCP IPv4” (p. 78)
LAN	**DHCP IPv6**	7.15 “Configuring DHCP IPv6” (p. 80)
LAN	**DNS**	7.16 “Configuring DNS” (p. 82)
LAN	**LAN statistics**	7.17 “Viewing LAN Statistics” (p. 84)
Wi-Fi	**Wi-Fi networks**	7.19 “Configuring Wi-Fi Network” (p. 87)

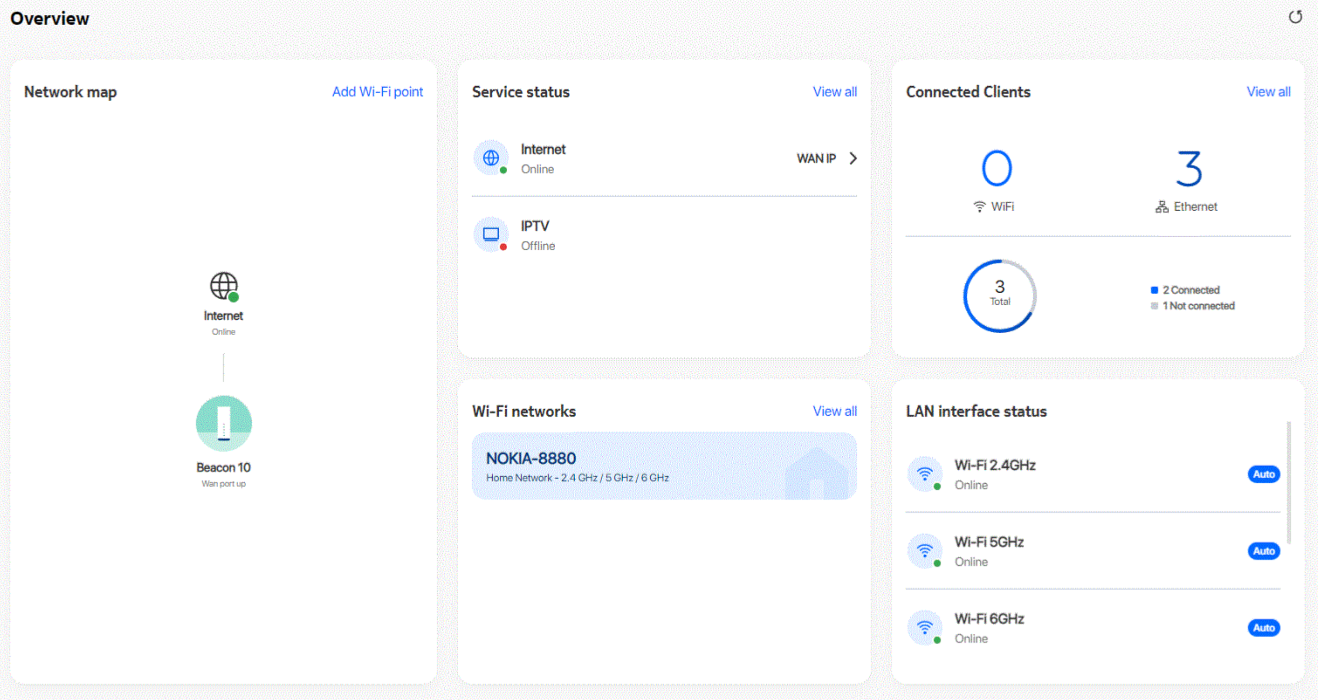
Table 7-1 Beacon 10 WebGUI Menu (continued)

Main Menu	Sub-menu	Procedure Reference
Wi-Fi	**Guest network**	7.20 “Configuring Guest Network” (p. 92)
Wi-Fi	**Network map**	7.21 “Viewing Network Map, Adding Wi-Fi Points and Removing Wi-Fi Points” (p. 94)
Wi-Fi	**Advanced settings**	7.22 “Configuring Wireless 2.4 GHz” (p. 98)
Wi-Fi	**Wi-Fi statistics**	7.25 “Viewing Wi-Fi Statistics” (p. 102)
Devices	-	7.27 “Viewing Device Information” (p. 104)
Security	**Firewall**	7.29 “Configuring the Firewall” (p. 106)
Security	**MAC filter**	7.30 “Configuring the MAC Filter” (p. 107)
Security	**IP filter**	7.31 “Configuring the IP Filter” (p. 109)
Security	**Family profiles**	7.32 “Configuring Family Profiles” (p. 111)
Security	**DMZ and ALG**	7.33 “Configuring DMZ and ALG” (p. 122)
Security	**Access control**	7.34 “Configuring Access Control” (p. 123)
Advanced settings	**Port forwarding**	7.36 “Configuring Port Forwarding” (p. 126)
Advanced settings	**Port triggering**	7.37 “Configuring Port Triggering” (p. 127)
Advanced settings	**DDNS**	7.38 “Configuring DDNS” (p. 129)
Advanced settings	**NTP**	7.39 “Configuring NTP” (p. 130)
Maintenance	**Change password**	7.41 “Configuring the Password” (p. 133)
Maintenance	**Backup and restore**	7.42 “Backing Up the Configuration” (p. 135) 7.43 “Restoring the Configuration” (p. 135)
Maintenance	**Firmware upgrade**	7.44 “Upgrading Firmware” (p. 136)
Maintenance	**Device management**	7.45 “Managing the Device” (p. 138)
Maintenance	**Diagnostics**	7.46 “Diagnosing WAN Connections” (p. 138)
Maintenance	**Log**	7.47 “Viewing Log Files” (p. 141)
Troubleshooting	-	7.49 “Troubleshooting” (p. 144)

7.5 Viewing overview information

1

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



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 Radio Access

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

7.5.3 Service Status

Displays the active status of the triple-play services.

Internet service

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

IPTV service

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

7.5.4 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).

7.5.5 Connected Clients

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

7.5.6 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 low

Shows the status of the 5GHz low network (Up/Down) and the current band setting. This can either be auto which indicates Radio Resource Management is enabled or is in the range 36-64 when manually configured.

Wi-Fi 6GHz

Shows the status of the 6GHz high network (Up/Down) and the current band setting. This can either be auto which indicates Radio Resource Management is enabled or is in the range of 100-165 when manually configured.

Ethernet Port

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

WAN Configuration

7.6 Overview

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

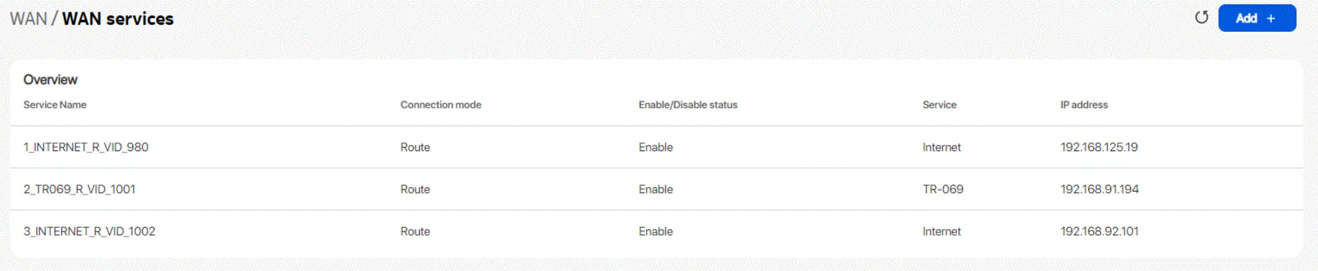
Sub-menu	Procedure
WAN services	7.7 “Configuring WAN Services” (p. 65)
WAN statistics	7.8 “Viewing WAN Statistics” (p. 68)
TR-069	7.9 “Configuring TR-069” (p. 71)
TR-369	7.10 “Configuring TR-369” (p. 73)
IP routing	7.11 “Configuring IP Routing” (p. 74)
Qos config	7.12 “Configuring QoS” (p. 75)

7.7 Configuring WAN Services

1

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

Figure 7-2 *Overview* table in *WAN services* page



WAN / **WAN services**

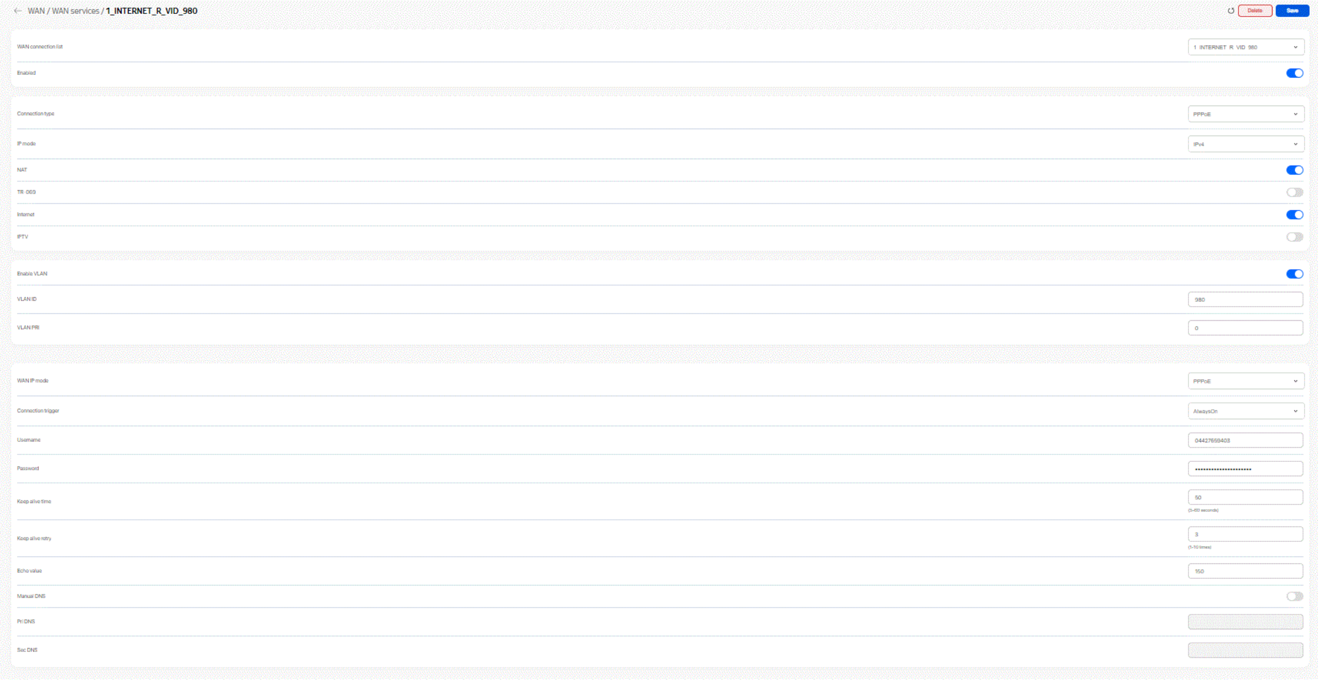
Overview

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

2

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

Figure 7-3 *Create New Connection* page



WAN connection list: 1 INTERNET R VID 980

Enabled: ●

Connection type: PPPoE

IP mode: IPv4

NAT: ●

TR-069: ○

Internet: ●

IPTV: ○

Enable VLAN: ●

VLAN ID: 980

VLAN PRI: 0

WAN IP mode: PPPoE

Connection trigger: AlwaysOn

Username: 04427659403

Password: ••••••••••••••••••••••

Keep alive time: 50 (5-60 seconds)

Keep alive retry: 3 (1-10 times)

Echo value: 150

Manual DNS: ○

Pri DNS:

Sec DNS:

3

Configure the following parameters:

Table 7-2 *WAN services* parameters

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

Table 7-2 WAN services parameters (continued)

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

Table 7-2 WAN services parameters (continued)

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

4

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

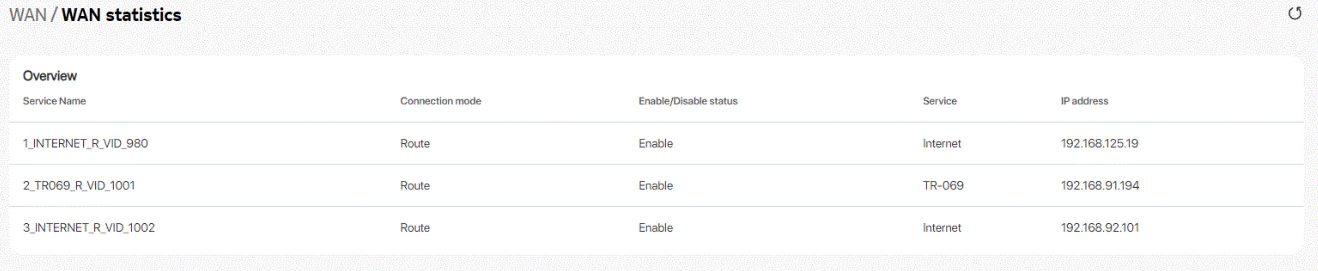
END OF STEPS

7.8 Viewing WAN Statistics

1

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

Figure 7-4 *WAN Statistics* page



WAN / **WAN statistics**

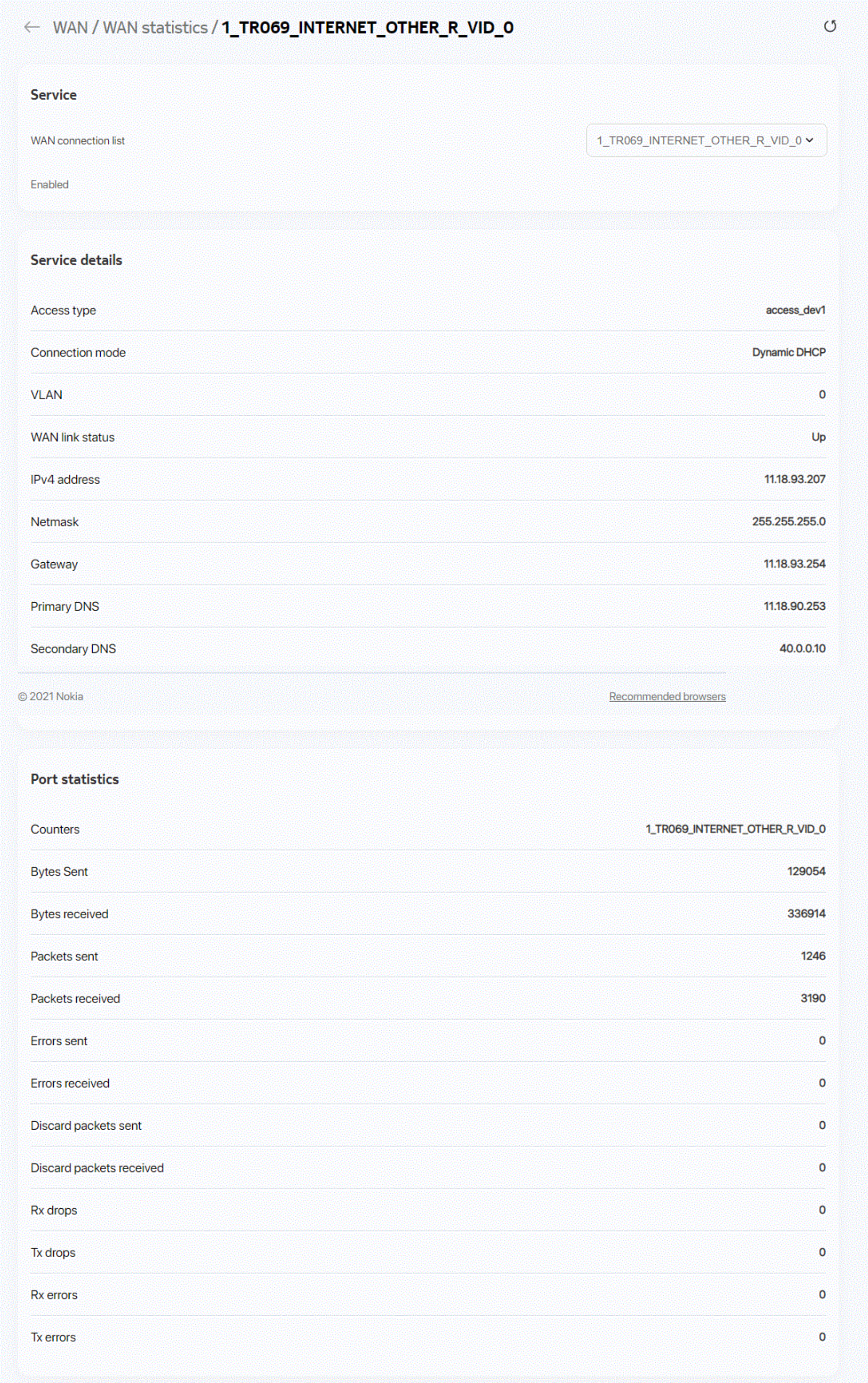
Overview

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

2

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

Figure 7-5 *WAN Statistics* page info



WAN / WAN statistics / **1_TR069_INTERNET_OTHER_R_VID_0**

Service

WAN connection list	1_TR069_INTERNET_OTHER_R_VID_0
Enabled	

Service details

Access type	access_dev1
Connection mode	Dynamic DHCP
VLAN	0
WAN link status	Up
IPv4 address	11.18.93.207
Netmask	255.255.255.0
Gateway	11.18.93.254
Primary DNS	11.18.90.253
Secondary DNS	40.0.0.10

© 2021 Nokia

Recommended browsers

Port statistics

Counters	1_TR069_INTERNET_OTHER_R_VID_0
Bytes Sent	129054
Bytes received	336914
Packets sent	1246
Packets received	3190
Errors sent	0
Errors received	0
Discard packets sent	0
Discard packets received	0
Rx drops	0
Tx drops	0
Rx errors	0
Tx errors	0

Table 7-3 WAN services parameters

Field	Description
WAN connection list	Select a WAN connection from the list.
Enabled	Displays whether WAN connection is either enabled or disabled.
Service details	
Access type	Displays the access type.
Primary DNS	Displays the primary DNS address.
Secondary DNS	Displays the secondary DNS address.
Ethernet link status	Displays the Ethernet status link whether it is Up or Down.
Pri DNS(v6)	Displays the primary DNS address. This option is available when the IP mode is **IPv4 & IPv6** or **IPv6**.
Port statistics	
Counters	Displays the counters details.
Bytes sent/received	Displays the bytes sent and received.
Packets sent/received	Displays the packets sent and received.
Errors sent/received	Displays the errors sent and received.
Unicast packets sent/received	Displays the unicast packets sent and received.
Discard packets sent/received	Displays the discard packets sent and received.
Broadcast packets sent/received	Displays the broadcast packets sent and received.
Unknown proto packets received	Displays the proto packets received.
Rx/Tx drops	Displays the Rx/Tx dropped packets.
Rx/Tx errors	Displays the Rx/Tx error packets.

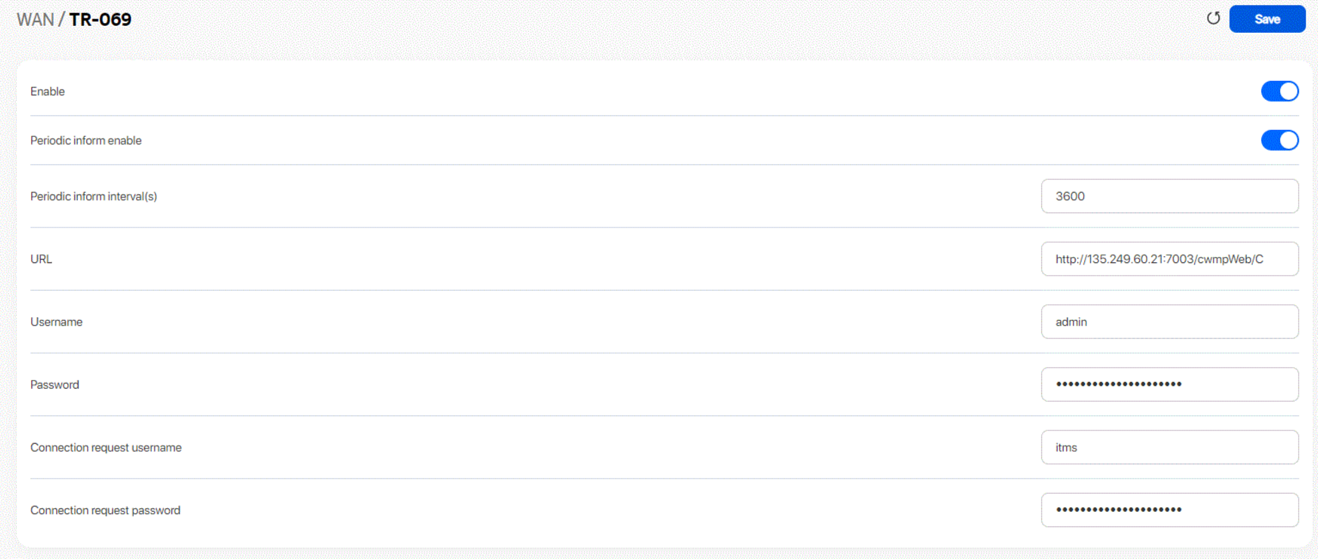
END OF STEPS

7.9 Configuring TR-069

1

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

Figure 7-6 *TR-069* page



WAN / **TR-069**

Enable	●
Periodic inform enable	●
Periodic inform interval(s)	3600
URL	http://135.249.60.21:7003/cwmpWeb/C
Username	admin
Password	••••••••••••••••••••
Connection request username	itms
Connection request password	••••••••••••••••••••

2

Configure the following parameters:

Table 7-4 *TR-069* parameters

Field	Description
Enable	Select the toggle button to enable CWMP function.
Periodic inform enable	Select the toggle button to enable periodic inform updates.
Periodic inform interval(s)	Enter the time between periodic inform updates, in seconds.
URL	Enter the URL of the auto-configuration server.
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

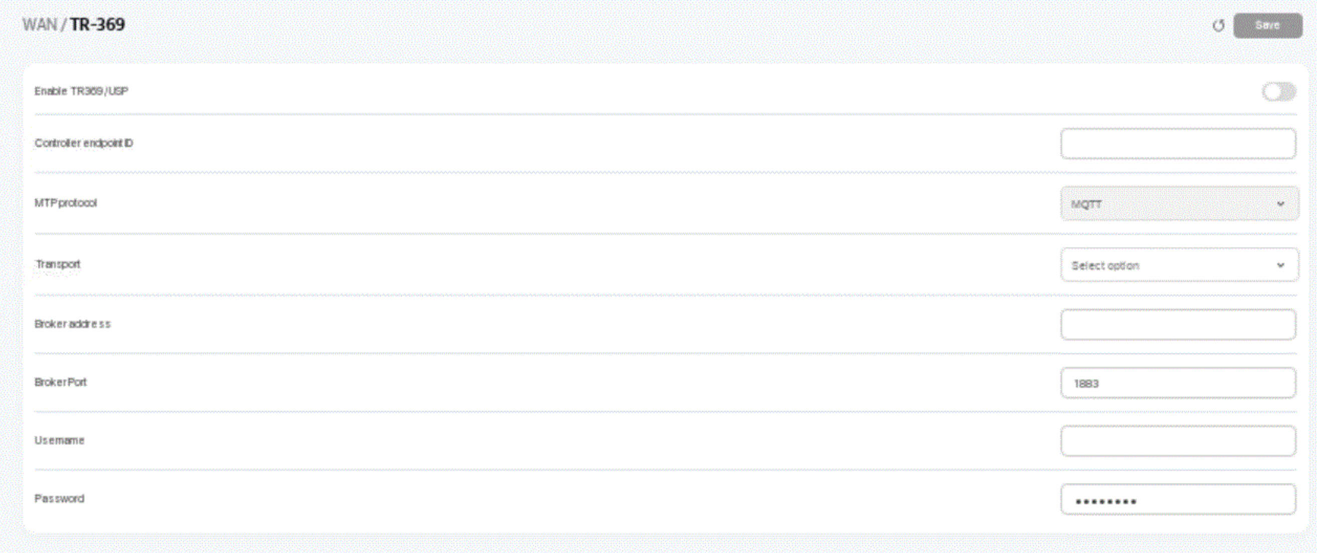
7.10 Configuring TR-369

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

1

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

Figure 7-7 *TR-369* page



WAN / **TR-369**

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 7-5 *TR-369* parameters

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

Table 7-5 *TR-369* parameters (continued)

Field	Description
Password	Enter the password to authenticate with MQTT broker.

3

Click **Save**.

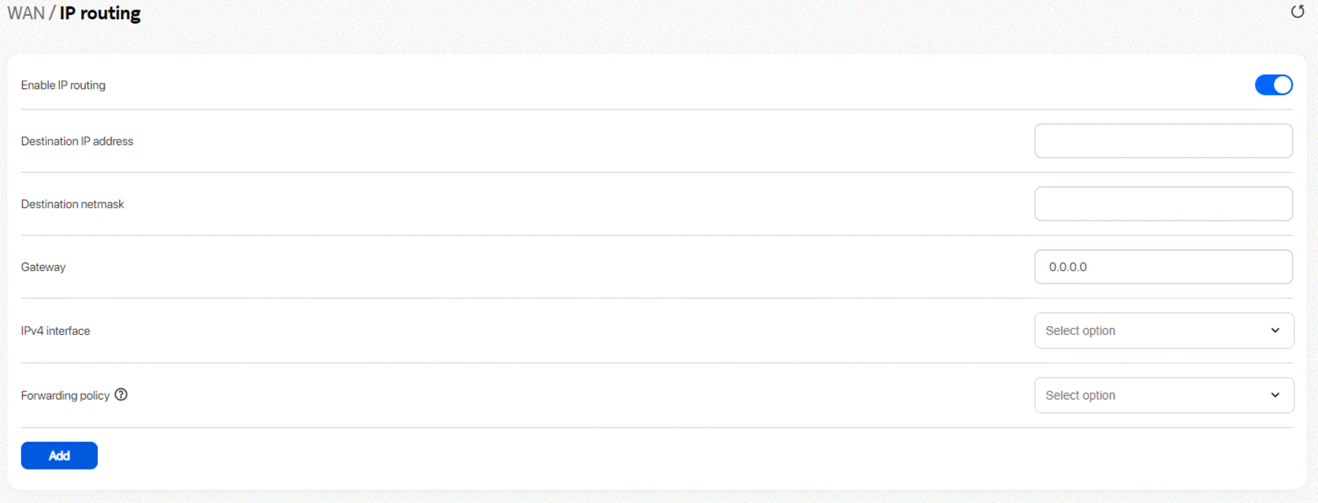
End of steps

7.11 Configuring IP Routing

1

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

Figure 7-8 *IP routing* page



WAN / **IP routing**

Enable IP routing: on

Destination IP address:

Destination netmask:

Gateway: 0.0.0.0

IPv4 interface: Select option

Forwarding policy: Select option

2

Configure the following parameters:

Table 7-6 *IP routing* parameters

Field	Description
Enable IP routing	Select the toggle button to enable IP routing.
Destination IP address	Enter the destination IP address.
Destination netmask	Enter the destination netmask.

Table 7-6 *IP routing* parameters (continued)

Field	Description
Gateway	Enter the gateway IP address.
IPv4 interface	Select an IPv4 interface from the list.
Forwarding policy	Select a forwarding policy from the list.

3

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

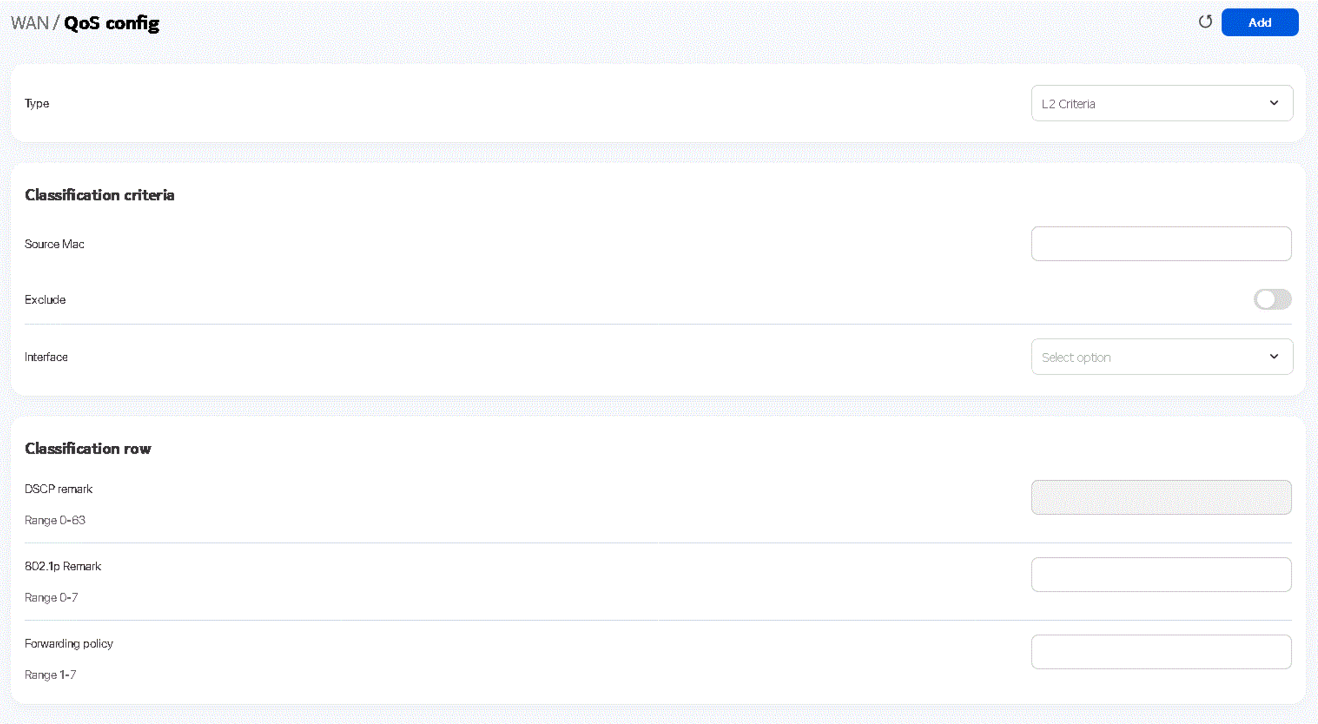
END OF STEPS

7.12 Configuring QoS

1

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

Figure 7-9 *QoS config* page (L2 Criteria)



WAN / **QoS config**

Type: L2 Criteria

Classification criteria

Source Mac

Exclude

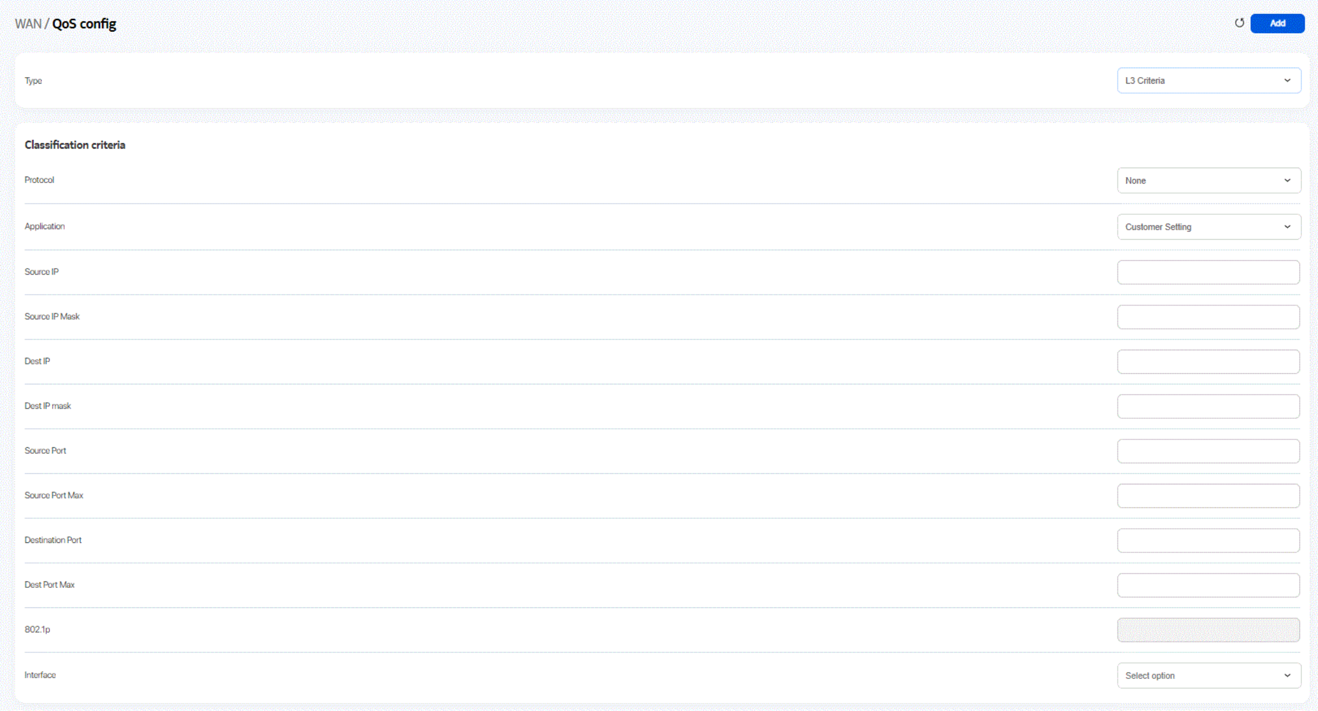
Interface: Select option

Classification row

DSCP remark
Range 0-63

802.1p Remark
Range 0-7

Forwarding policy
Range 1-7



Type: L3 Criteria

Classification criteria

Protocol: None

Application: Customer Setting

Source IP

Source IP Mask

Dest IP

Dest IP mask

Source Port

Source Port Max

Destination Port

Dest Port Max

802.1p

Interface: Select option

Figure 7-10 *QoS config* page (L3 Criteria)

2

Configure the following parameters:

Table 7-7 *QoS config* parameters

Field	Description
Type	Select a QoS service layer type from the list: • **L2 Criteria** • **L3 Criteria**
Classification criteria (L2)	
Source MAC	Enter the source MAC address.
Interface	Select an interface from the list.
Classification criteria (L3)	
Protocol	Select a protocol from the list.
Application	Select an application from the list or select **Custom Settings** and enter an application name.
Source IP	Enter the source IP address.
Source IP mask	Enter the source IP address netmask.

Table 7-7 *QoS config* parameters (continued)

Field	Description
Destination IP	Enter the destination IP address.
Destination IP mask	Enter the destination IP address netmask.
Source port	Enter the source port number.
Source port max	Enter the values for the source port max (highest port number)
Destination port	Enter the destination port number.
Destination port max	Enter the values for the destination port max (highest port number)
Classification row	
DSCP remark	Enter the value for the DSCP remark (applicable only for L3 criteria). Allowed values: 0 to 63
802.1p Remark	Enter the value for the 802.1p remark. Allowed values: 0 to 7
Forwarding policy	Enter the number for the forwarding policy. Allowed values: 1 to 7

3

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

END OF STEPS

LAN Configuration

7.13 Overview

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

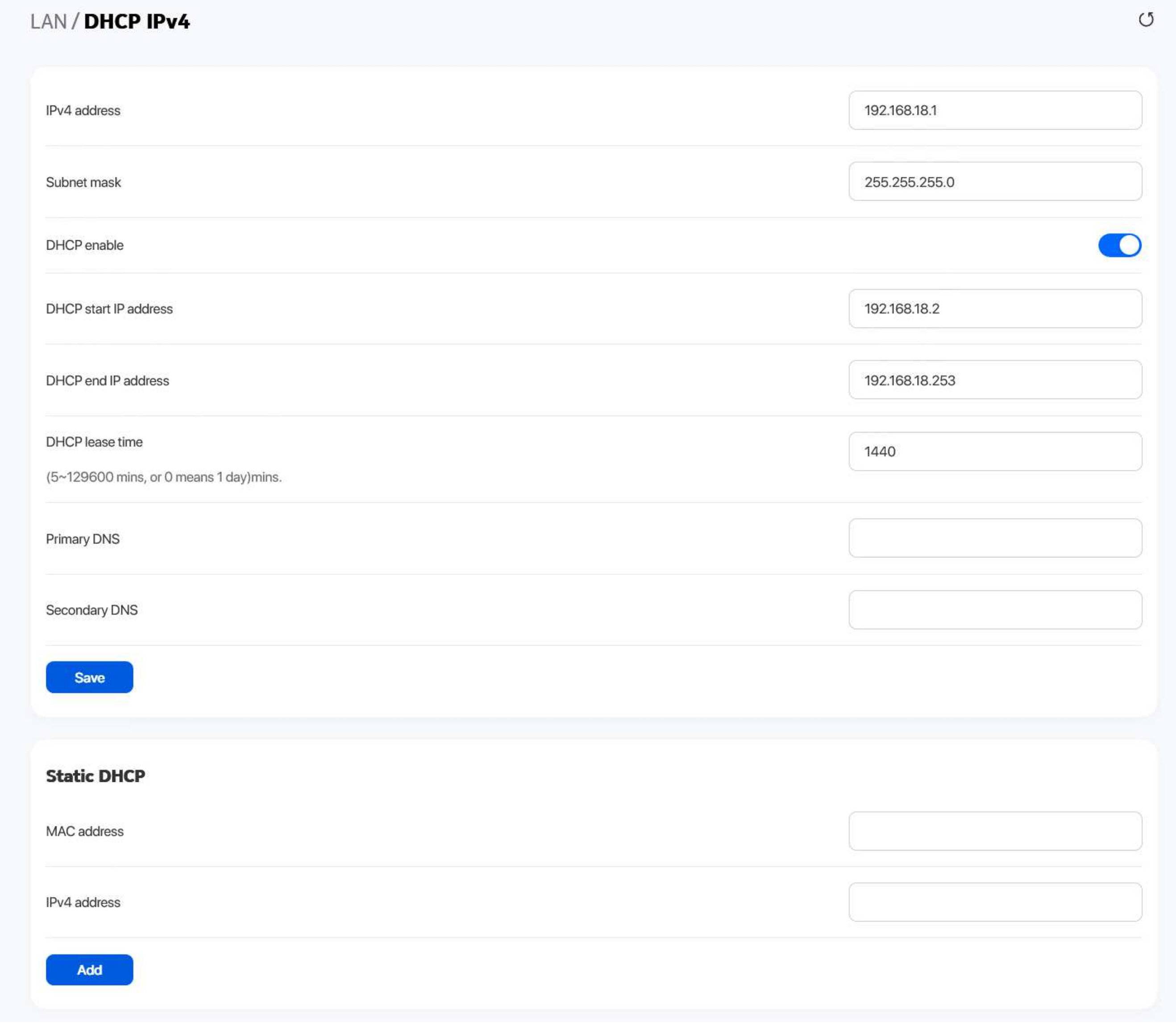
Sub-menu	Procedure
DHCP IPv4	7.14 “Configuring DHCP IPv4” (p. 78)
DHCP IPv6	7.15 “Configuring DHCP IPv6” (p. 80)
DNS	7.16 “Configuring DNS” (p. 82)
LAN statistics	7.17 “Viewing LAN Statistics” (p. 84)

7.14 Configuring DHCP IPv4

1

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

Figure 7-11 *DHCP IPv4* page



LAN / **DHCP IPv4**

IPv4 address: 192.168.18.1

Subnet mask: 255.255.255.0

DHCP enable: ●

DHCP start IP address: 192.168.18.2

DHCP end IP address: 192.168.18.253

DHCP lease time (5~129600 mins, or 0 means 1 day)mins.: 1440

Primary DNS:

Secondary DNS:

Save

Static DHCP

MAC address:

IPv4 address:

Add

2

Configure the following LAN parameters:

Table 7-8 *DHCP IPv4* parameters

Field	Description
IPv4 address	Enter the IPv4 address of the Beacon.

Table 7-8 DHCP IPv4 parameters (continued)

Field	Description
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.
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.

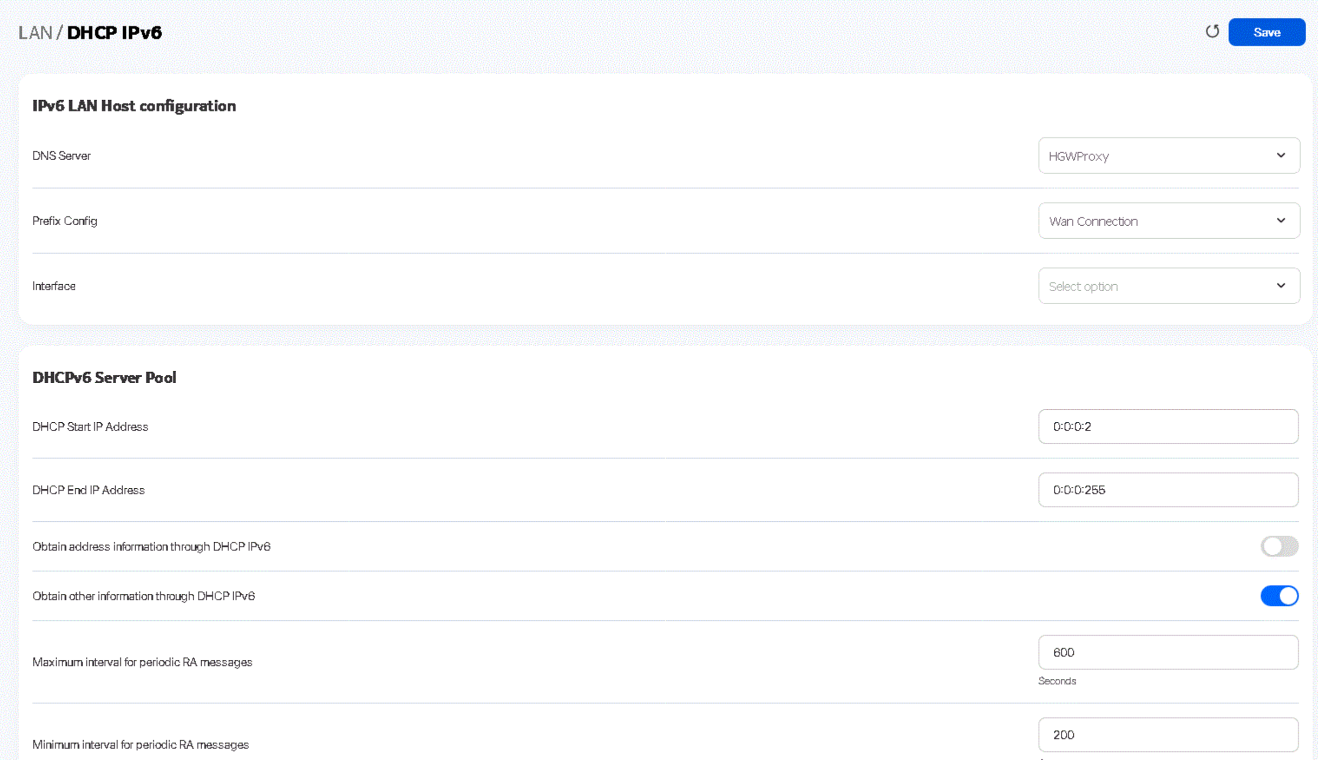
End of steps

7.15 Configuring DHCP IPv6

1

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

Figure 7-12 DHCP IPv6 page



LAN / **DHCP IPv6**

IPv6 LAN Host configuration

DNS Server: HGWProxy

Prefix Config: Wan Connection

Interface: Select option

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: ○ off

Obtain other information through DHCP IPv6: ● on

Maximum interval for periodic RA messages: 600 Seconds

Minimum interval for periodic RA messages: 200

2

Configure the following parameters:

Table 7-10 DHCP 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.
DHCP End IP Address	Enter the ending range of the DHCP IP address.

Table 7-10 DHCP IPv6 parameters (continued)

Field	Description
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**.

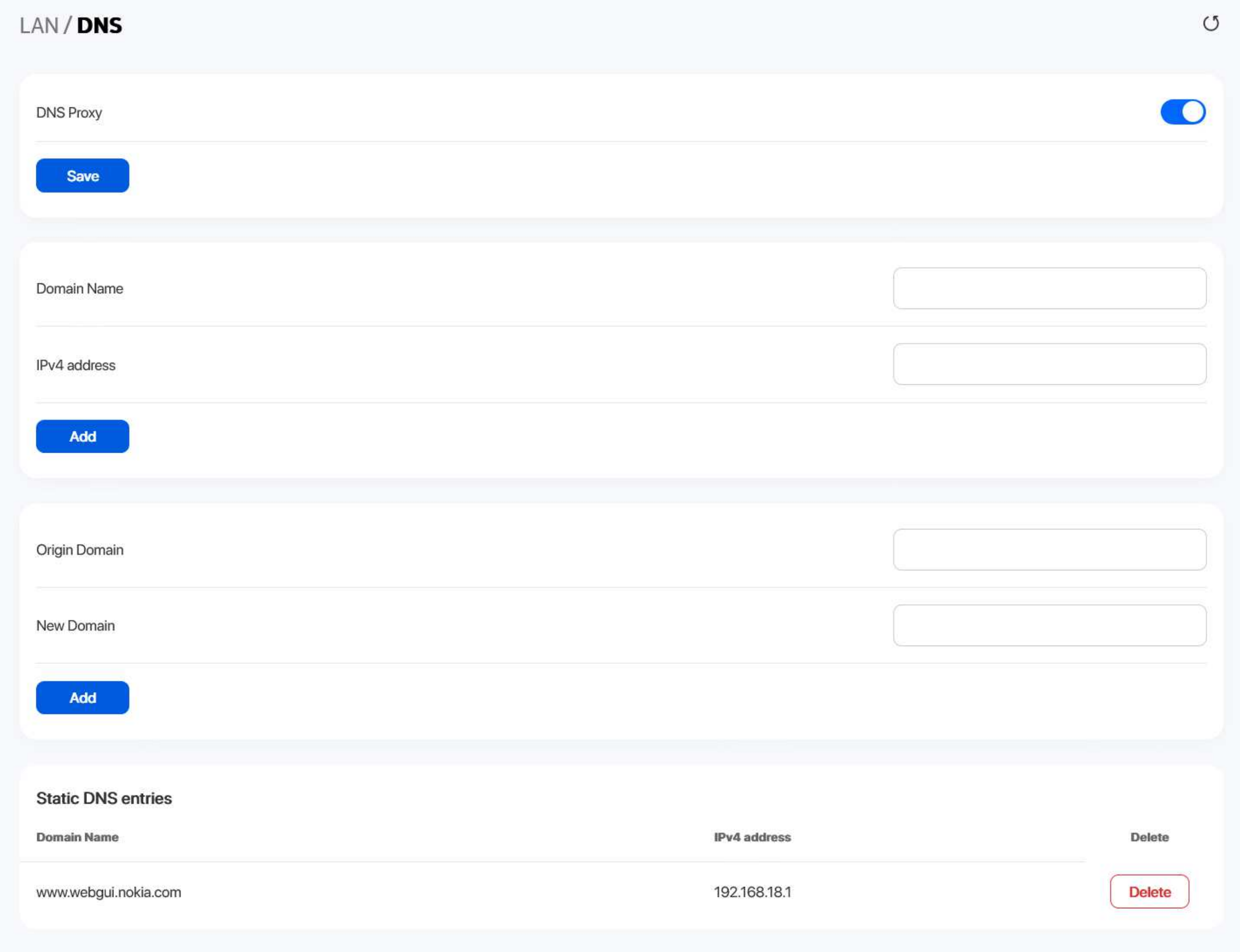
END OF STEPS

7.16 Configuring DNS

1

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

Figure 7-13 DNS page



Static DNS entries

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

2

Configure the following parameters:

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

b. Configure the following:

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

c. Configure the following:

1. Enter the origin domain name in the Origin Domain field

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

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

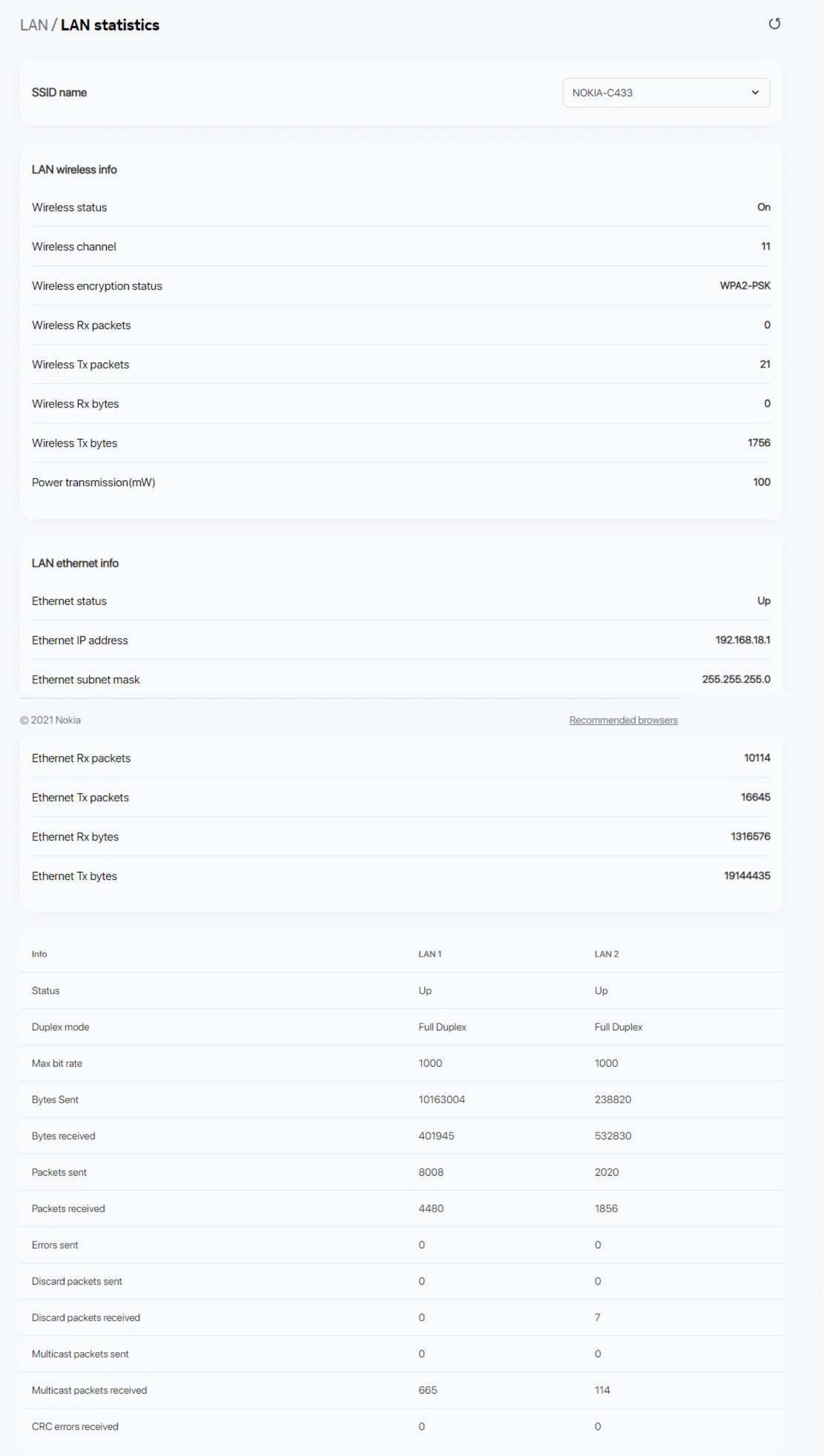
END OF STEPS

7.17 Viewing LAN Statistics

1

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

Figure 7-14 *LAN statistics* page



LAN / **LAN statistics**

SSID name	NOKIA-C433

LAN wireless info

Wireless status	On
Wireless channel	11
Wireless encryption status	WPA2-PSK
Wireless Rx packets	0
Wireless Tx packets	21
Wireless Rx bytes	0
Wireless Tx bytes	1756
Power transmission(mW)	100

LAN ethernet info

Ethernet status	Up
Ethernet IP address	192.168.18.1
Ethernet subnet mask	255.255.255.0

© 2021 Nokia Recommended browsers

Ethernet Rx packets	10114
Ethernet Tx packets	16645
Ethernet Rx bytes	1316576
Ethernet Tx bytes	19144435

Info	LAN 1	LAN 2
Status	Up	Up
Duplex mode	Full Duplex	Full Duplex
Max bit rate	1000	1000
Bytes Sent	10163004	238820
Bytes received	401945	532830
Packets sent	8008	2020
Packets received	4480	1856
Errors sent	0	0
Discard packets sent	0	0
Discard packets received	0	7
Multicast packets sent	0	0
Multicast packets received	665	114
CRC errors received	0	0

Table 7-11 *LAN statistics* parameters

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

END OF STEPS

Wi-Fi Configuration

7.18 Overview

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

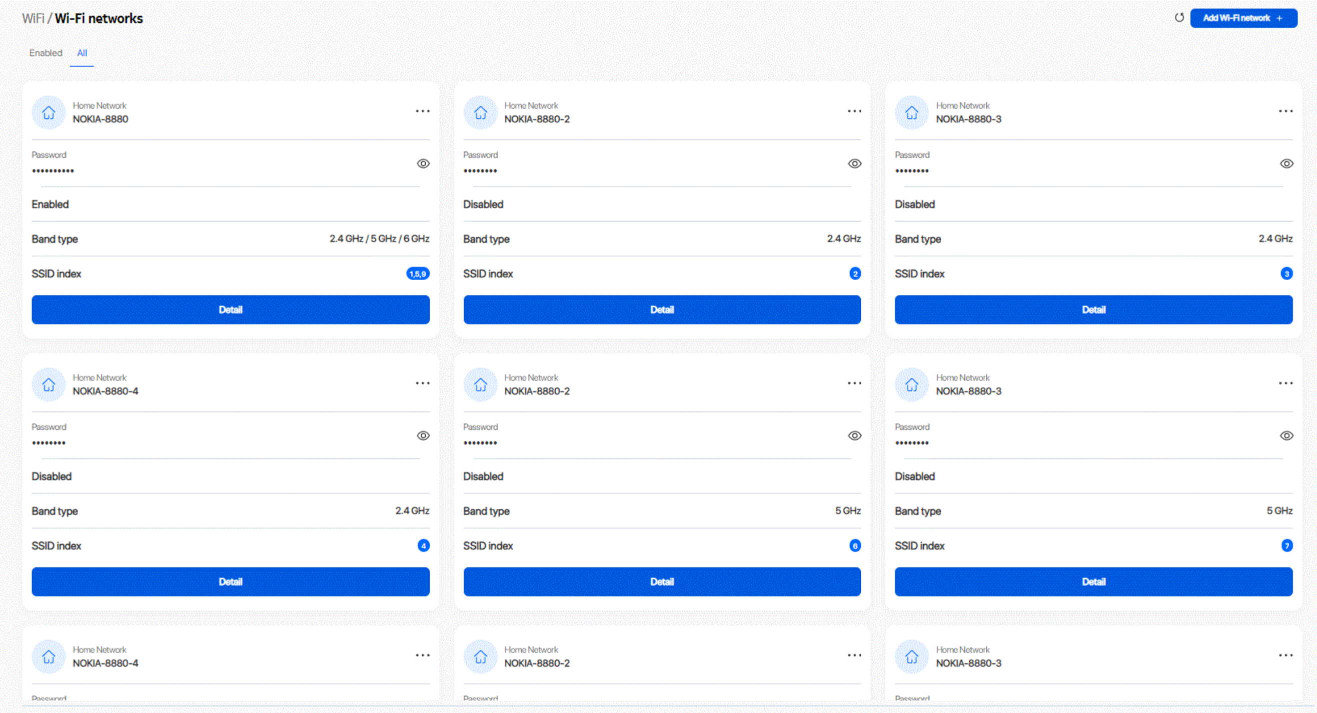
Sub-menu	Procedure
Wi-Fi networks	7.19 “Configuring Wi-Fi Network” (p. 87)
Guest network	7.20 “Configuring Guest Network” (p. 92)
Network map	7.21 “Viewing Network Map, Adding Wi-Fi Points and Removing Wi-Fi Points” (p. 94)
Advanced settings	7.22 “Configuring Wireless 2.4 GHz” (p. 98)
Wi-Fi statistics	7.25 “Viewing Wi-Fi Statistics” (p. 102)

7.19 Configuring Wi-Fi Network

1

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

Figure 7-15 Wi-Fi network page



WiFi / **Wi-Fi networks**

Home Network
NOKIA-8880
Password ••••••••••
Enabled
Band type 2.4 GHz / 5 GHz / 6 GHz
SSID index 1,5,9
Detail

Home Network
NOKIA-8880-2
Password ••••••••
Disabled
Band type 2.4 GHz
SSID index 2
Detail

Home Network
NOKIA-8880-3
Password ••••••••
Disabled
Band type 2.4 GHz
SSID index 3
Detail

Home Network
NOKIA-8880-4
Password ••••••••
Disabled
Band type 2.4 GHz
SSID index 4
Detail

Home Network
NOKIA-8880-2
Password ••••••••
Disabled
Band type 5 GHz
SSID index 6
Detail

Home Network
NOKIA-8880-3
Password ••••••••
Disabled
Band type 5 GHz
SSID index 7
Detail

Home Network
NOKIA-8880-4
Password

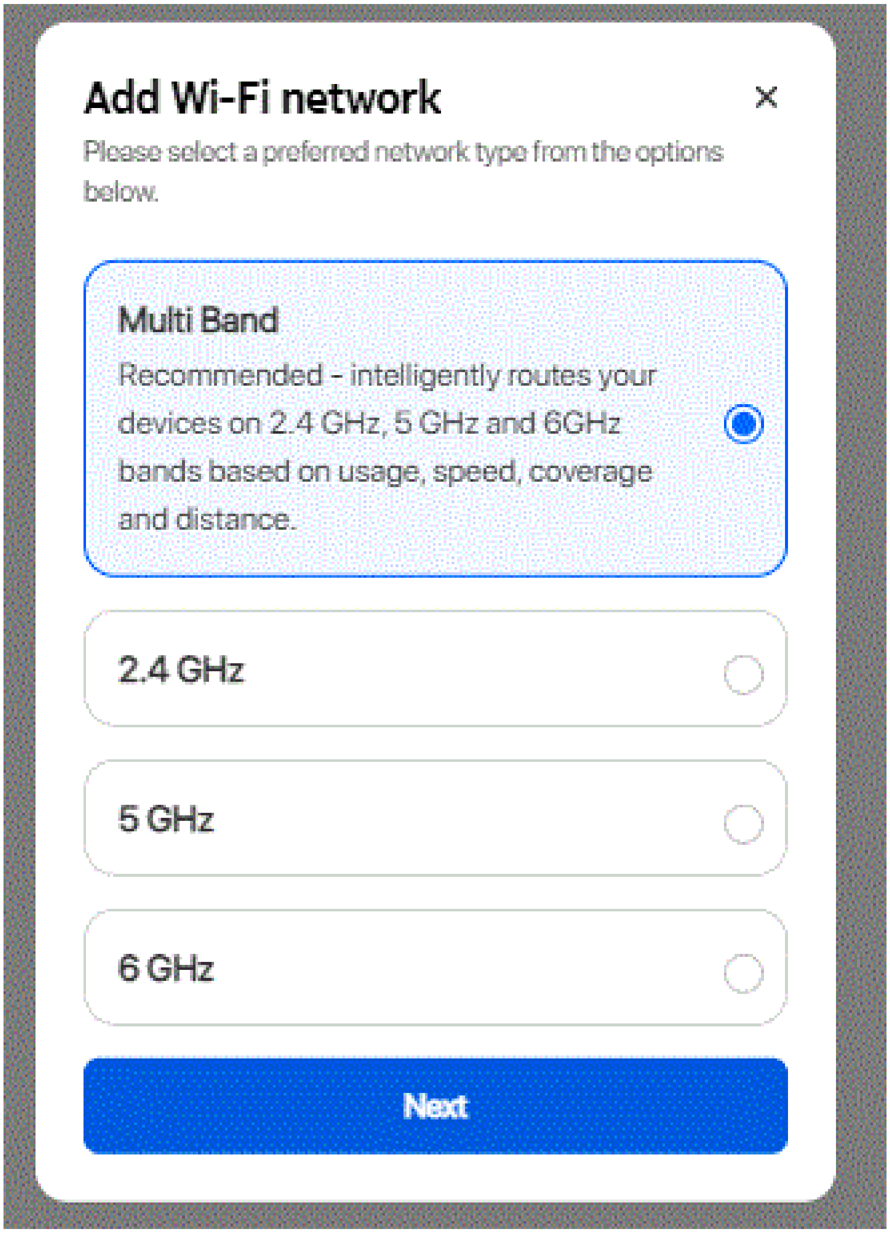
Home Network
NOKIA-8880-2
Password

Home Network
NOKIA-8880-3
Password

2

Click **Add Wi-Fi network +** to create a Wi-Fi network. The *Add Wi-Fi network* page displays.

Figure 7-16 Add Wi-Fi network page



Add Wi-Fi network

Please select a preferred network type from the options below.

● Multi Band
Recommended - intelligently routes your devices on 2.4 GHz, 5 GHz and 6GHz bands based on usage, speed, coverage and distance.

○ 2.4 GHz

○ 5 GHz

○ 6 GHz

3

Configure the following parameters:

Table 7-12 Add Wi-Fi network parameters

Field	Description
Multiband	Select this option to configure a multiband wireless network. This option is recommended your devices on 2.4 GHz or 5 GHzbands based on usage, speed, coverage and distance.
2.4 GHz	Select this option to configure a 2.4 GHz wireless network.
5 GHz	Select this option to configure a 5 GHz wireless network.
6 GHz	Select this option to configure a 6 GHz wireless network.

4

Click **Next**.

5

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

6

Enter the password for the network in the Password field and click **Save**.

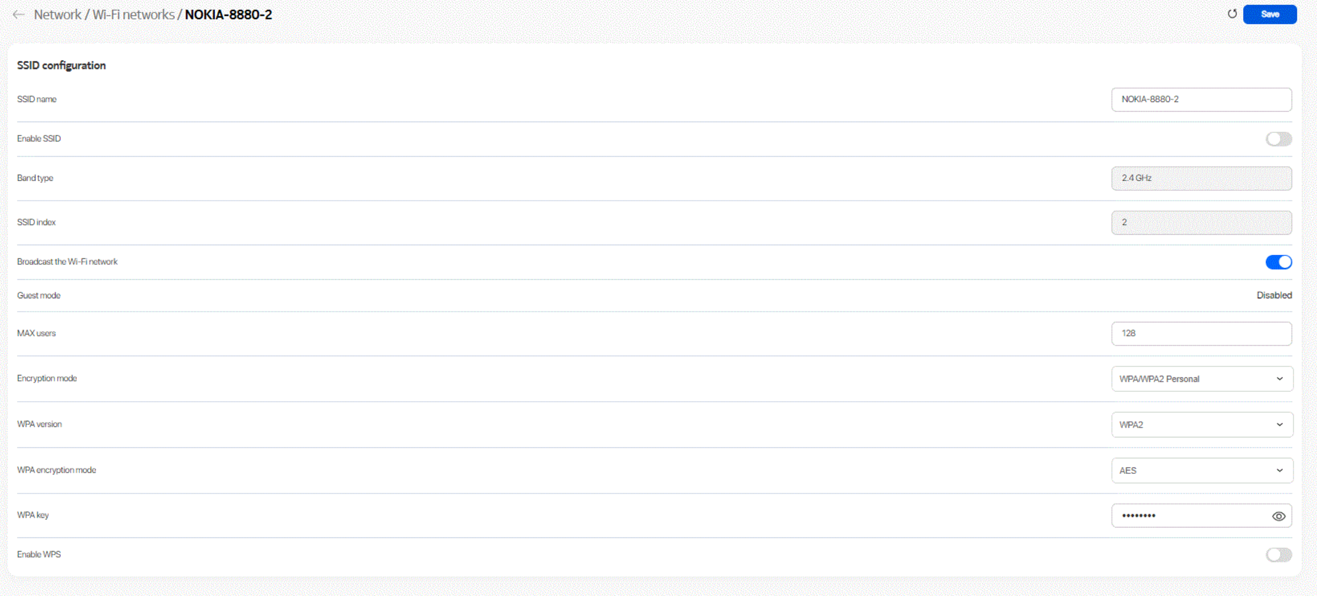
The Wi-Fi network is created and is displayed as a card in the **Enabled** tab of the *Wi-Fi networks* page.

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

7

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

Figure 7-17 Wi-Fi network - SSID Configuration (2.4 GHz band) page

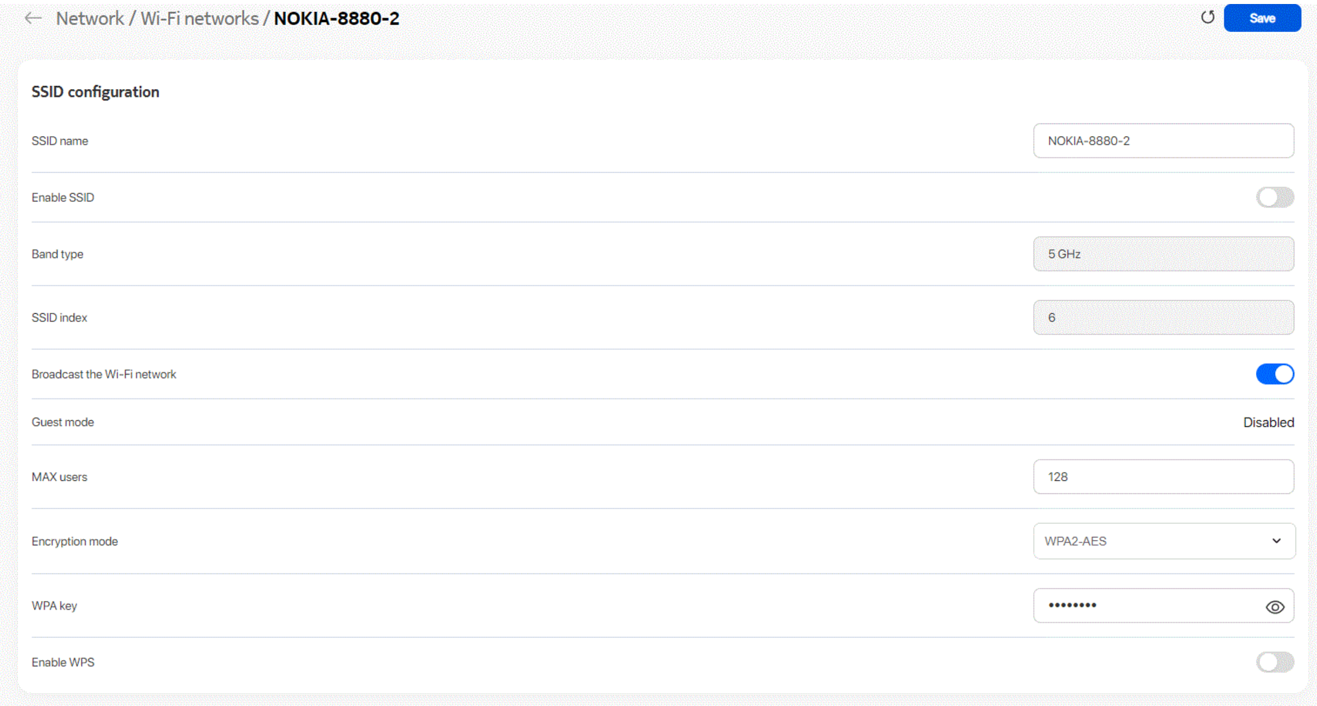


Network / Wi-Fi networks / **NOKIA-8880-2** Save

SSID configuration

SSID name	NOKIA-8880-2
Enable SSID	○
Band type	2.4 GHz
SSID index	2
Broadcast the Wi-Fi network	●
Guest mode	Disabled
MAX users	128
Encryption mode	WPA/WPA2 Personal
WPA version	WPA2
WPA encryption mode	AES
WPA key	••••••••
Enable WPS	○

Figure 7-18 Wi-Fi network - SSID Configuration (5 GHz band) page

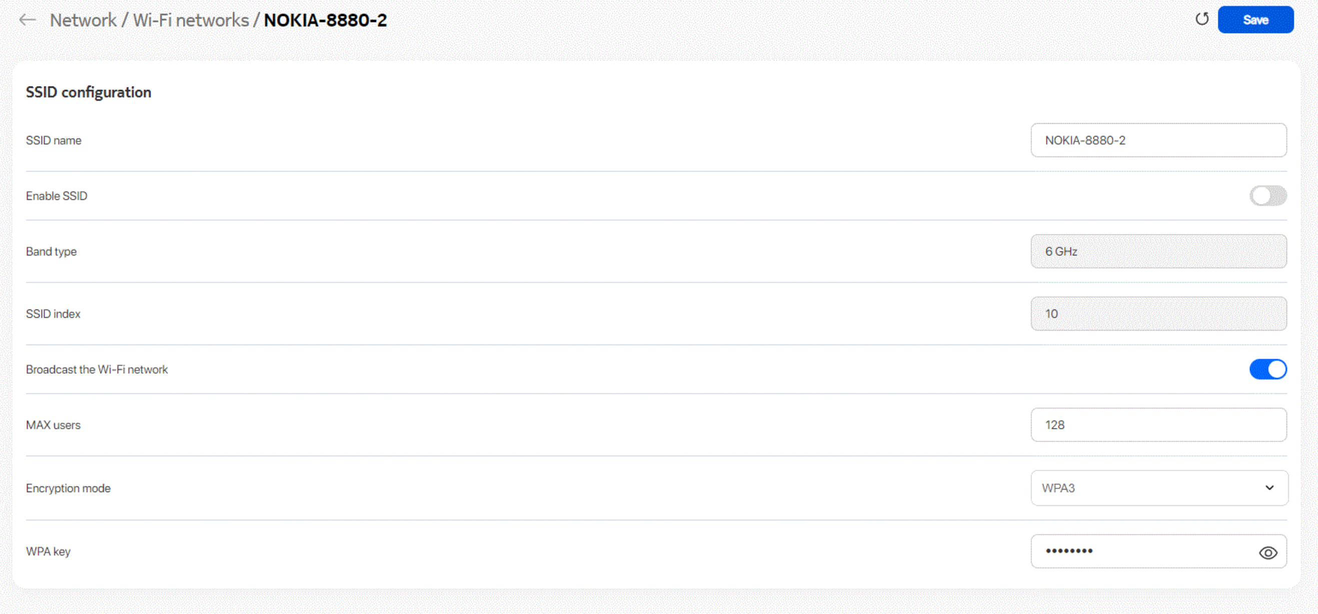


Network / Wi-Fi networks / **NOKIA-8880-2** Save

SSID configuration

SSID name	NOKIA-8880-2
Enable SSID	○
Band type	5 GHz
SSID index	6
Broadcast the Wi-Fi network	●
Guest mode	Disabled
MAX users	128
Encryption mode	WPA2-AES
WPA key	••••••••
Enable WPS	○

Figure 7-19 Wi-Fi network - SSID Configuration (6 GHz band) page



Network / Wi-Fi networks / **NOKIA-8880-2**

SSID configuration

SSID name: NOKIA-8880-2

Enable SSID: off

Band type: 6 GHz

SSID index: 10

Broadcast the Wi-Fi network: on

MAX users: 128

Encryption mode: WPA3

WPA key: ••••••••

8

Configure the following parameters:

Field	Description
SSID name	Displays the SSID name.
Enable SSID	Select the toggle button to enable SSID.
Band type	Displays the band type.
SSID index	Displays the SSID index.
Broadcast the Wi-Fi network	Select the toggle button to enable broadcasting of the Wi-Fi network.
Guest Mode	Indicates whether guest mode is enabled or disabled. When a particular SSID is enabled with Guest Mode, LAN devices connected to the SSID can only connect to the Internet. Such devices cannot see or communicate with other LAN devices.
MAX users	Enter the maximum number of users.

Field	Description
Encryption Mode	In case of 2.4 GHz band type, select an encryption mode from the list: • **WPA/WPA2 Personal** • **WPA3 Personal** • **WPA2/WPA3 Personal** • **WPA/WPA2 Enterprise** • **Open** In case of 5 GHz band type, select an encryption mode from the list: • **WPA2-AES** • **WPA2+WPA** • **WPA3-AES** • **WPA2+WPA3-AES** • **WPA/WPA2 Enterprise** • **NONE-OPEN**
WPA version	Select a WPA version from the list: • **WPA2** • **WPA/WPA2** This parameter is visible only if the band type is 2.4 GHz.
WPA Encryption Mode	Select a WPA encryption mode from the list: • **AES** • **TKIP/AES** This parameter is visible only if the band type is 2.4 GHz.
WPA Key	Enter the WPA key.
Enable WPS	Select the toggle button to enable WPS .

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; RADIUS accounting port.

9

Click **Save**.

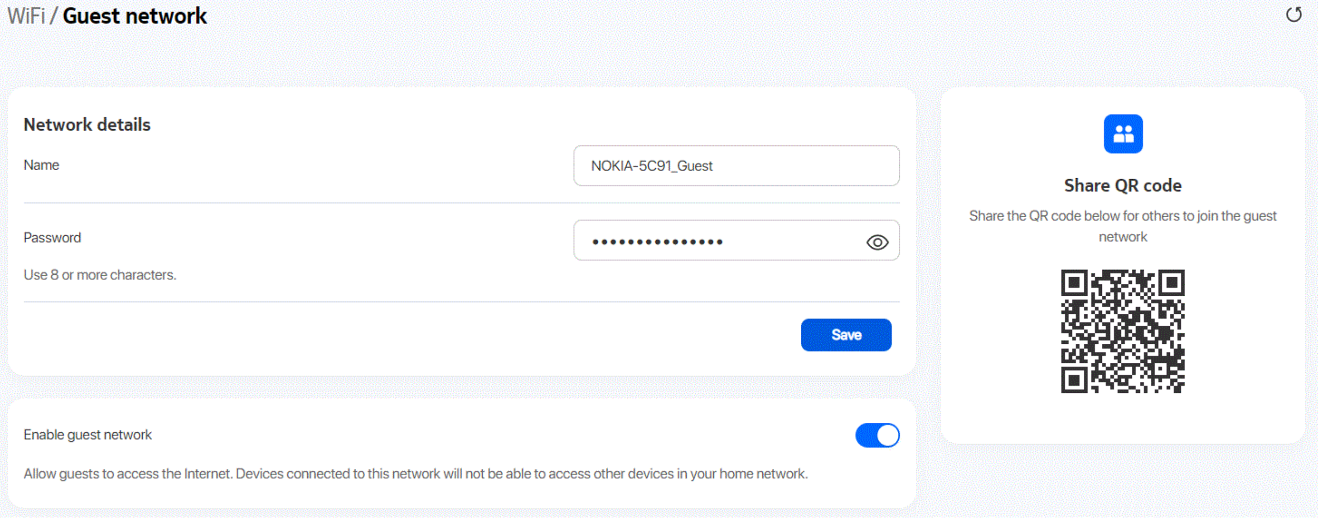
End of steps

7.20 Configuring Guest Network

1

Click **Wi-Fi→Guest network** in the left pane. The *Guest network* page displays the network details.

Figure 7-20 *Guest network* page



WiFi / **Guest network**

Network details

Name: NOKIA-5C91_Guest

Password: ••••••••••••••••

Use 8 or more characters.

Enable guest network

Allow guests to access the Internet. Devices connected to this network will not be able to access other devices in your home network.

Share QR code

Share the QR code below for others to join the guest network

2

Configure the following parameters:

Table 7-13 *Guest network* parameters

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

3

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

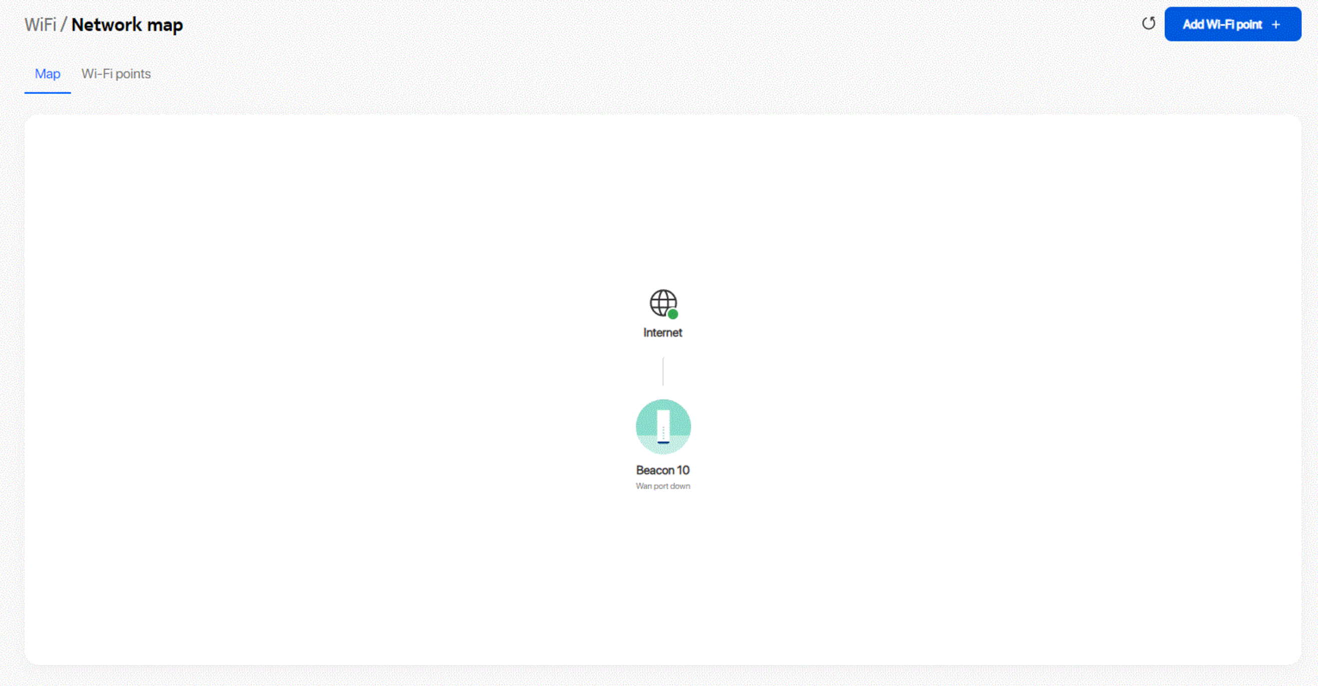
END OF STEPS

7.21 Viewing Network Map, Adding Wi-Fi Points and Removing Wi-Fi Points

1

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

Figure 7-21 *Network map* page

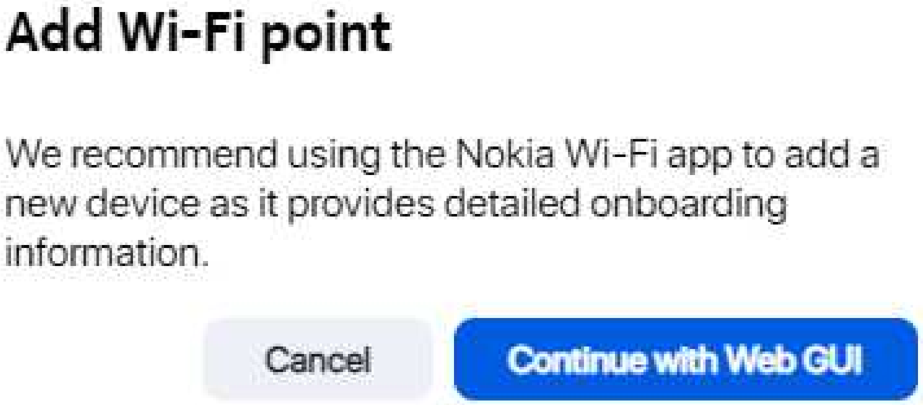


2

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.

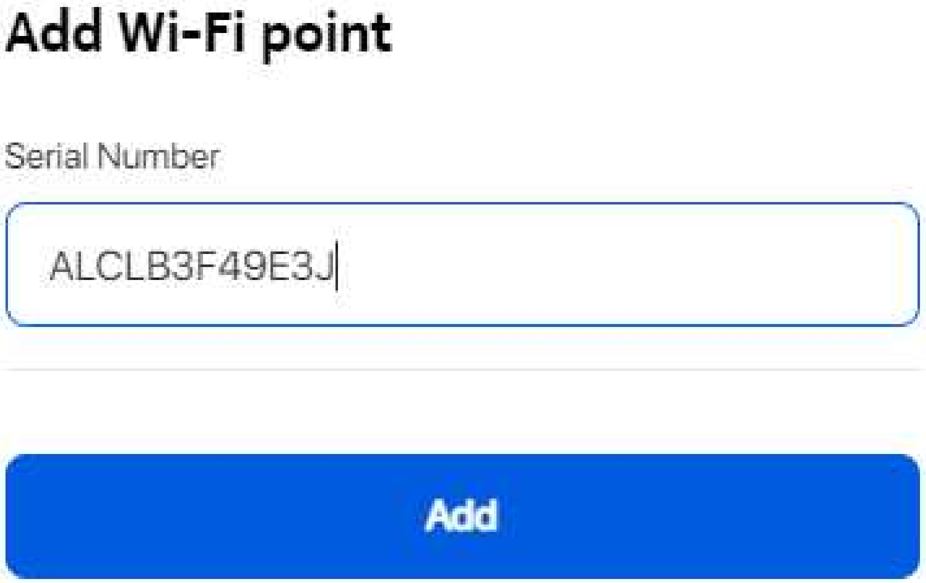
b. To add a Wi-Fi point using the WebGUI, click **Continue with WebGUI**.



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

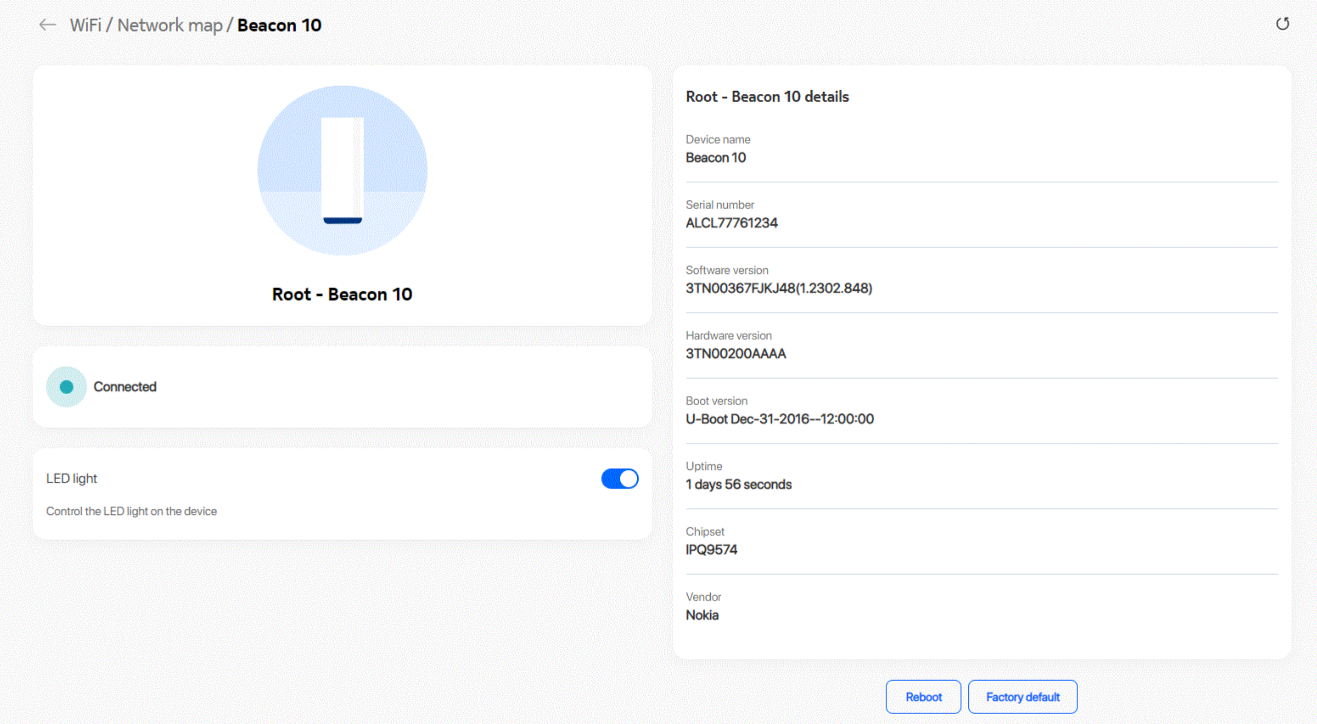
Serial Number: ALCLB3F49E3J

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

Figure 7-22 <*Device*> page



Root - Beacon 10

Connected

LED light

Control the LED light on the device

Root - Beacon 10 details

Device name
Beacon 10

Serial number
ALCL77761234

Software version
3TN00367FJKJ48(1.2302.848)

Hardware version
3TN00200AAAA

Boot version
U-Boot Dec-31-2016--12:00:00

Uptime
1 days 56 seconds

Chipset
IPQ9574

Vendor
Nokia

Table 7-14 <*Device*> parameters

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

Table 7-14 *<Device>* parameters (continued)

Field	Description
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:

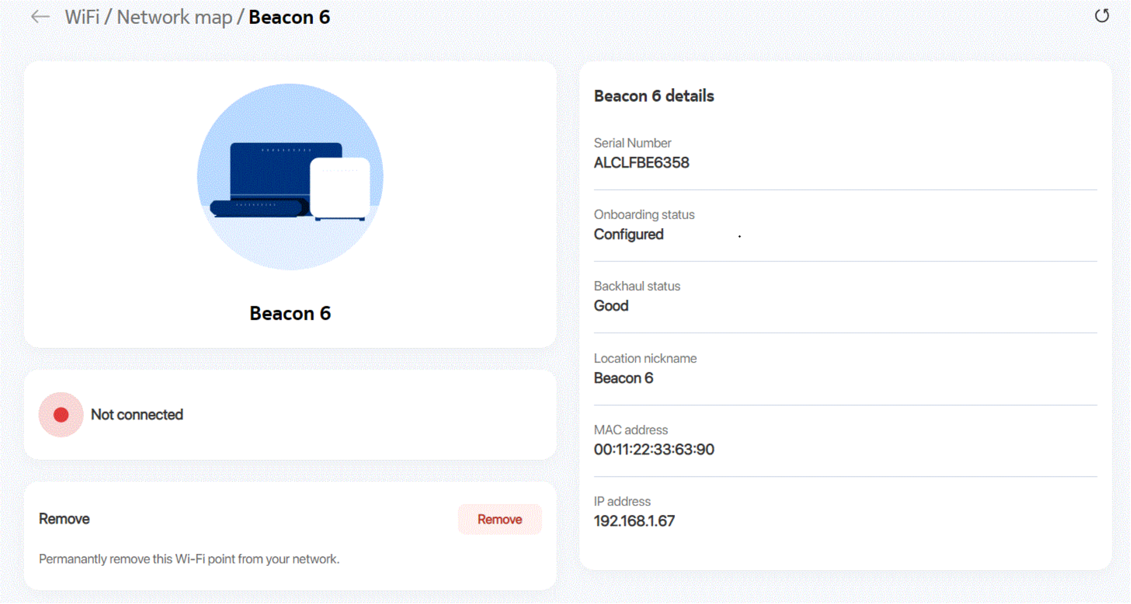
- **Reboot the device:**
  1. Click **Reboot**. A message displays asking if you want reboot the device.
  2. Click **OK** to reboot the Beacon. The device reboots and displays the login page.
- **Reset the device to factory default settings:**
  1. Click **Factory default**. A message displays asking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

7.21.1 Remove Wi-Fi points

To remove Wi-Fi points, perform the following:

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



Not connected

Remove

Permanantly remove this Wi-Fi point from your network.

Beacon 6 details

Serial Number
ALCLFBE6358

Onboarding status
Configured

Backhaul status
Good

Location nickname
Beacon 6

MAC address
00:11:22:33:63:90

IP address
192.168.1.67

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

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

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

7.22 Configuring Wireless 2.4 GHz

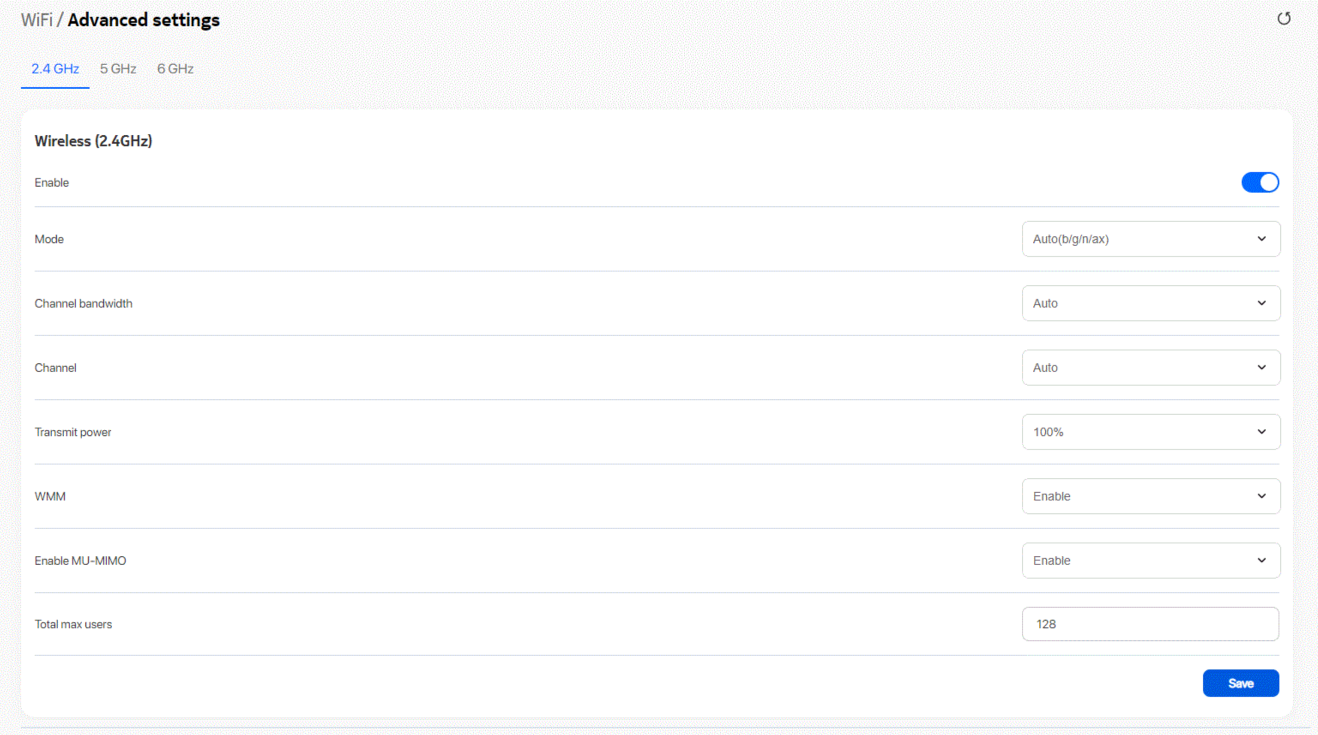
1

Click **Wi-Fi→Advanced settings** in the left pane. The *Advanced settings* page displays.

2

Select the **2.4 GHz** tab to configure the wireless 2.4 GHz parameters.

Figure 7-23 Advanced settings - 2.4 GHz tab



Wireless (2.4GHz)

Enable: On

Mode: Auto(b/g/n/ax)

Channel bandwidth: Auto

Channel: Auto

Transmit power: 100%

WMM: Enable

Enable MU-MIMO: Enable

Total max users: 128

3

Configure the following parameters:

Table 7-15 Wireless 2.4 GHz 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/ax)** • **b/g/n** • **b** • **g** • **n** • **b/g** • **g/n** • **n/ax**
Channel bandwidth	Select the bandwidth range from the list: • **Auto** (auto-assigns the bandwidth range) • **20 MHz** • **40 MHz**
Channel	Select a channel from the list or select **Auto** to auto-assign the channel.
Transmit power	Select a percentage for the transmitting power from the list: • **12%** • **25%** • **50%** • **100%**
WMM	Select an option from the list to enable or disable wireless multimedia: • **Enable** • **Disable**
Total max users	Enter the maximum number of users.

4

Click **Save**.

END OF STEPS

7.23 Configuring Wireless 5GHz

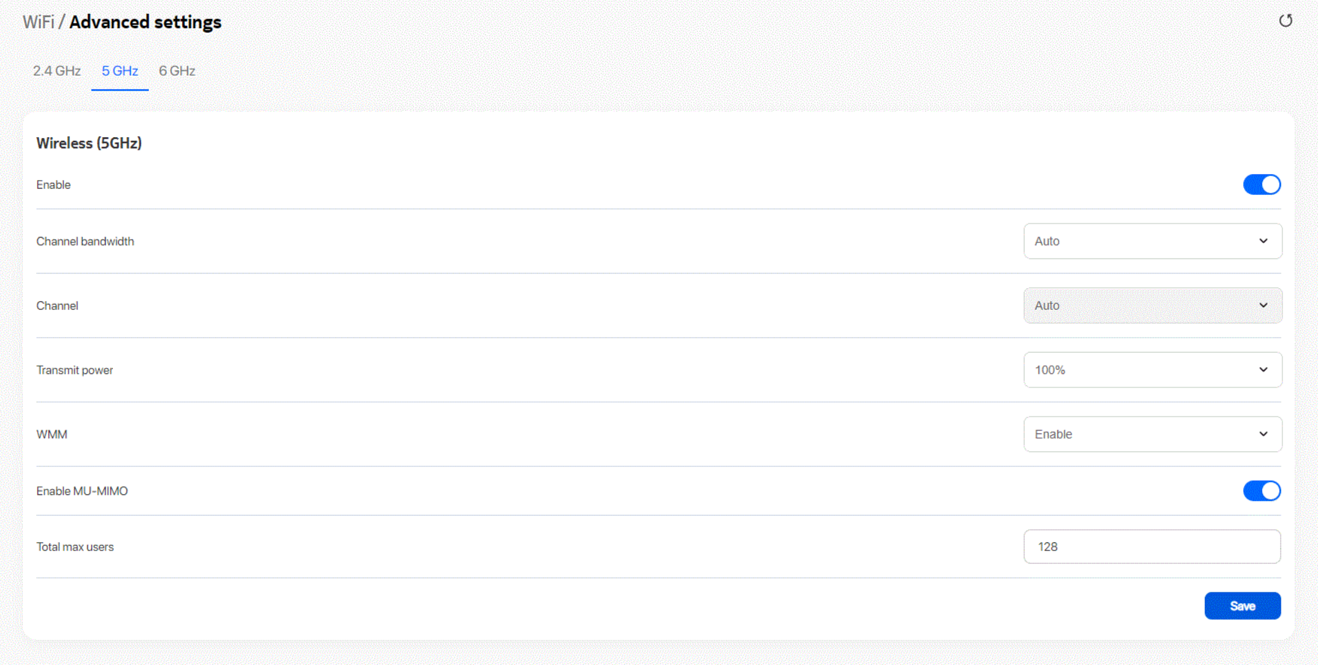
1

Click **Wi-Fi→Advanced settings** in the left pane. The *Advanced settings* page displays.

2

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

Figure 7-24 *Wireless 5 GHz* page



Wireless (5GHz)

Enable: on

Channel bandwidth: Auto

Channel: Auto

Transmit power: 100%

WMM: Enable

Enable MU-MIMO: on

Total max users: 128

3

Configure the following parameters:

Table 7-16 Wireless 5 GHz

Field	Description
Enable	Select this toggle button to enable WiFi.
Channel bandwidth	Select an option 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.
Transmit power	Select a percentage for the transmitting power from the list: • **12%** • **25%** • **50%** • **100%**
WMM	Select **Enable** or **Disable** from the list to enable or disable WiFi multimedia.

Table 7-16 Wireless 5 GHz (continued)

Field	Description
Enable MU-MMO	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.

4

Click **Save**.

END OF STEPS

7.24 Configuring Wireless 6GHz

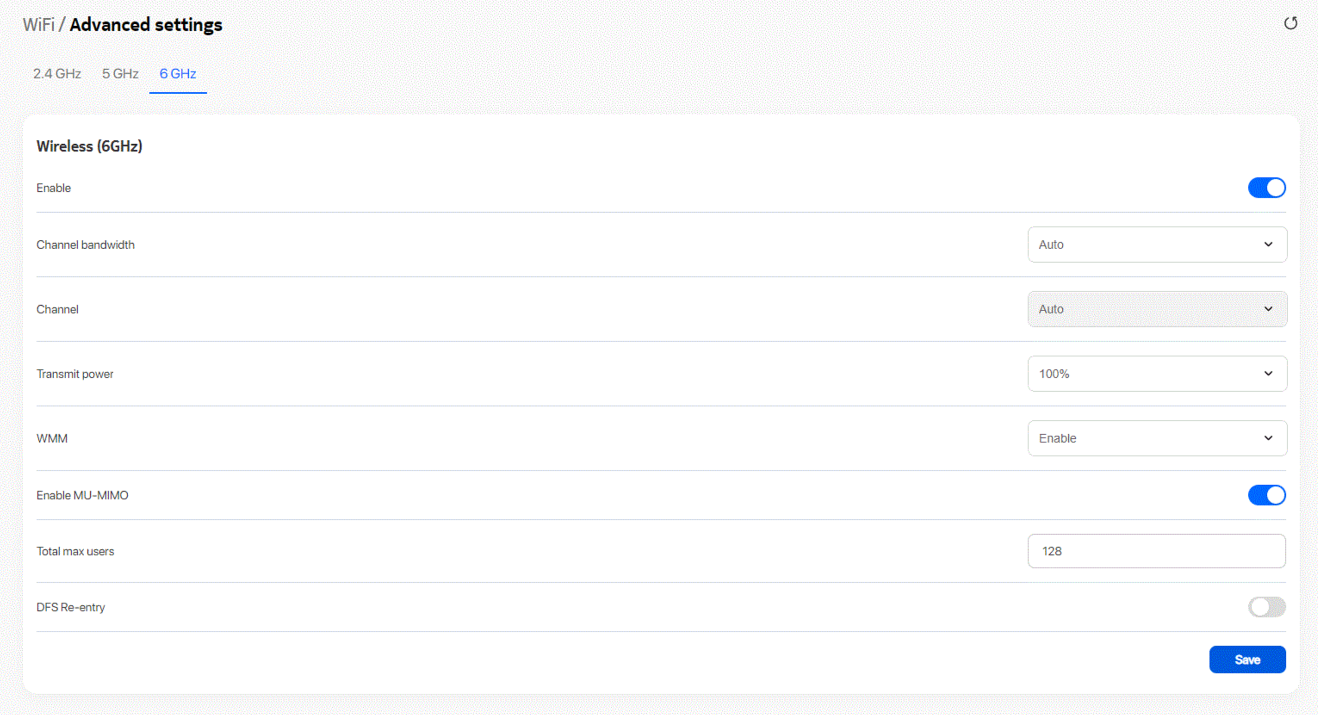
1

Click **Wi-Fi→Advanced settings** in the left pane. The *Advanced settings* page displays.

2

Select the 6 GHz tab to configure the wireless 6 GHz parameters

Figure 7-25 *Wireless 6 GHz* page



Wireless (6GHz)

Enable	● On
Channel bandwidth	Auto
Channel	Auto
Transmit power	100%
WMM	Enable
Enable MU-MIMO	● On
Total max users	128
DFS Re-entry	○ Off

3

Configure the following parameters:

Table 7-17 Wireless 6 GHz

Field	Description
Enable	Select this toggle button to enable WiFi.
Channel bandwidth	Select an option 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.
Transmit power	Select a percentage for the transmitting power from the list: • **12%** • **25%** • **50%** • **100%**
WMM	Select **Enable** or **Disable** from the list to enable or disable WiFi multimedia.
Enable MU-MMO	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	Select the toggle button to enable DFS re entry.

4

Click **Save**.

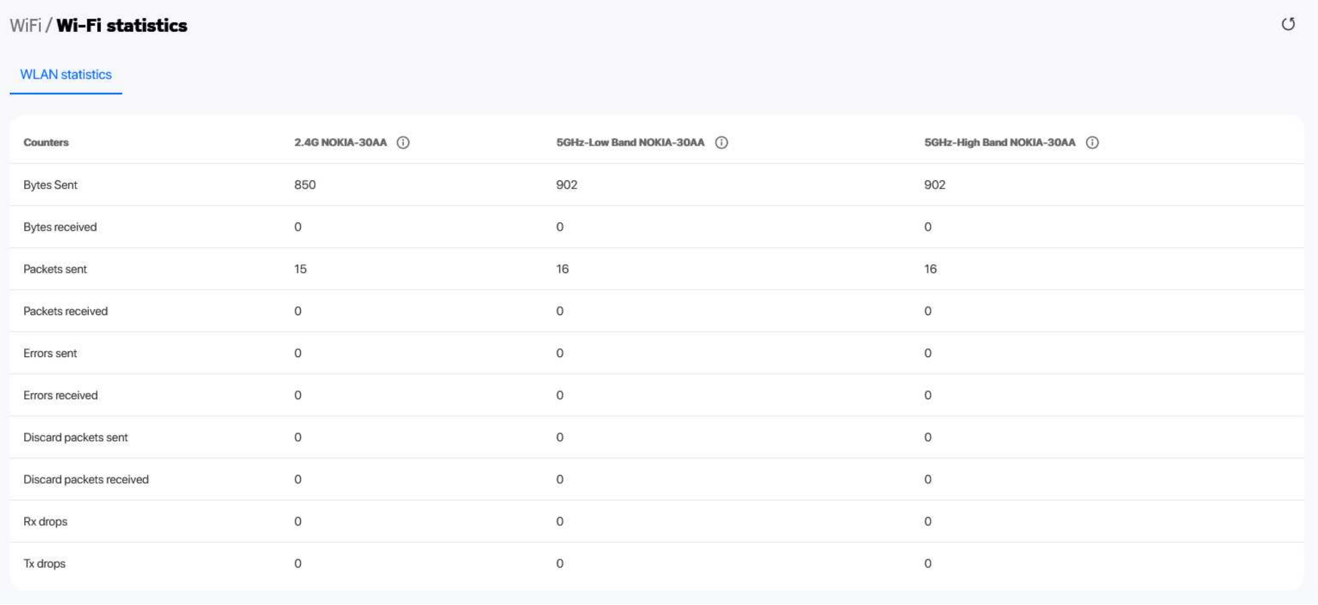
END OF STEPS

7.25 Viewing Wi-Fi Statistics

1

Click **Wi-Fi→Wi-Fi statistics** in the left pane. The *Wi-Fi statistics* page displays.

Figure 7-26 Wi-Fi statistics page



WiFi / **Wi-Fi statistics**

WLAN statistics

Counters	2.4G NOKIA-30AA ⓘ	5GHz-Low Band NOKIA-30AA ⓘ	5GHz-High Band NOKIA-30AA ⓘ
Bytes Sent	850	902	902
Bytes received	0	0	0
Packets sent	15	16	16
Packets received	0	0	0
Errors sent	0	0	0
Errors received	0	0	0
Discard packets sent	0	0	0
Discard packets received	0	0	0
Rx drops	0	0	0
Tx drops	0	0	0

2

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

END OF STEPS

Devices

7.26 Overview

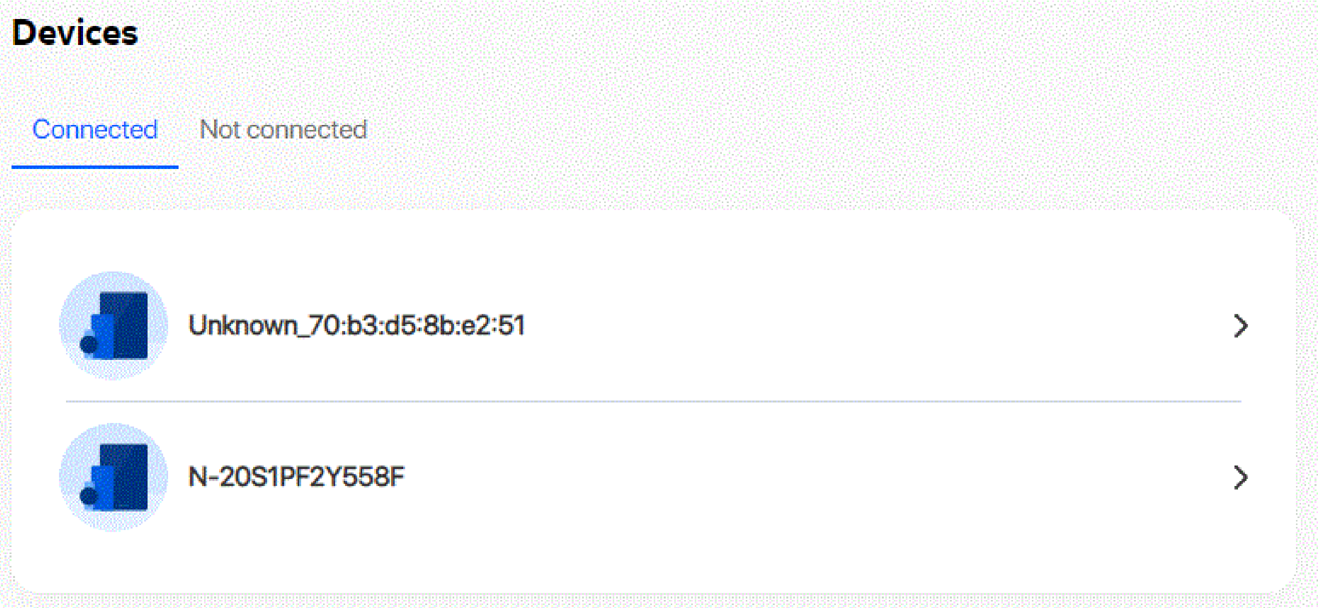
This section describes how to view device information from the **Device** menu.

7.27 Viewing Device Information

1

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

Figure 7-27 *Devices* page



Devices

Connected Not connected

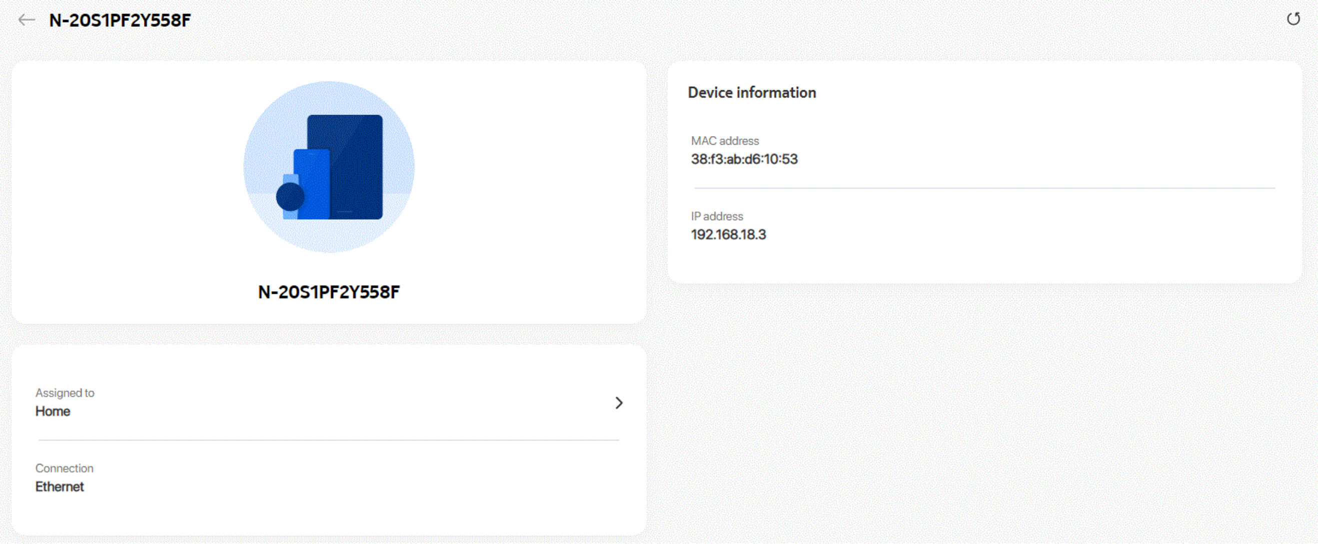
Unknown_70:b3:d5:8b:e2:51

N-20S1PF2Y558F

2

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

Figure 7-28 *<Device>* page



N-20S1PF2Y558F

N-20S1PF2Y558F

Device information

MAC address
38:f3:ab:d6:10:53

IP address
192.168.18.3

Assigned to
Home

Connection
Ethernet

END OF STEPS

Security Configuration

7.28 Overview

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

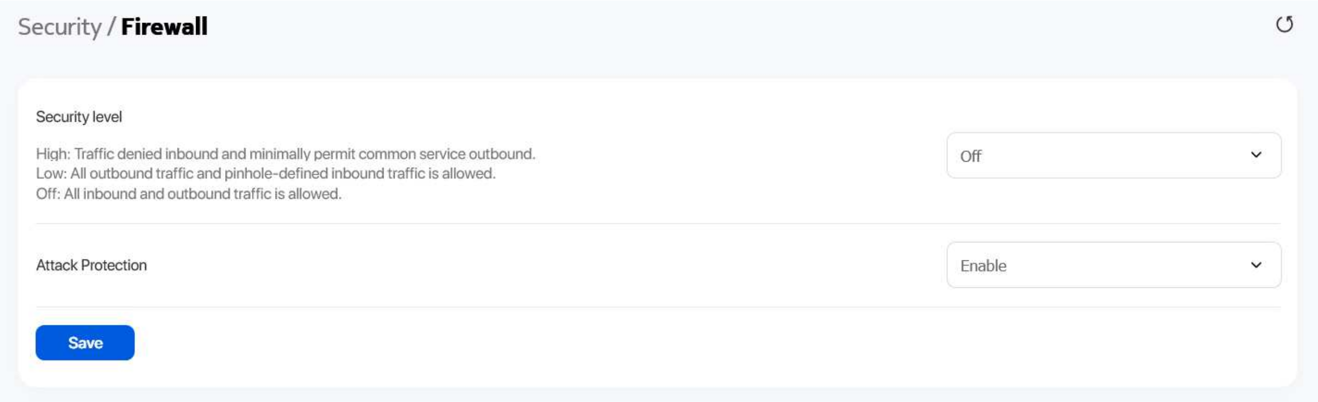
Sub-menu	Procedure
Firewall	7.29 “Configuring the Firewall” (p. 106)
MAC filter	7.30 “Configuring the MAC Filter” (p. 107)
IP filter	7.31 “Configuring the IP Filter” (p. 109)
Family profiles	7.32 “Configuring Family Profiles” (p. 111)
DMZ and ALG	7.33 “Configuring DMZ and ALG” (p. 122)
Access control	7.34 “Configuring Access Control” (p. 123)

7.29 Configuring the Firewall

1

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

Figure 7-29 *Firewall* page



Security / **Firewall**

Security level

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

Off

Attack Protection

Enable

2

Configure the following parameters.

Table 7-18 *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**.

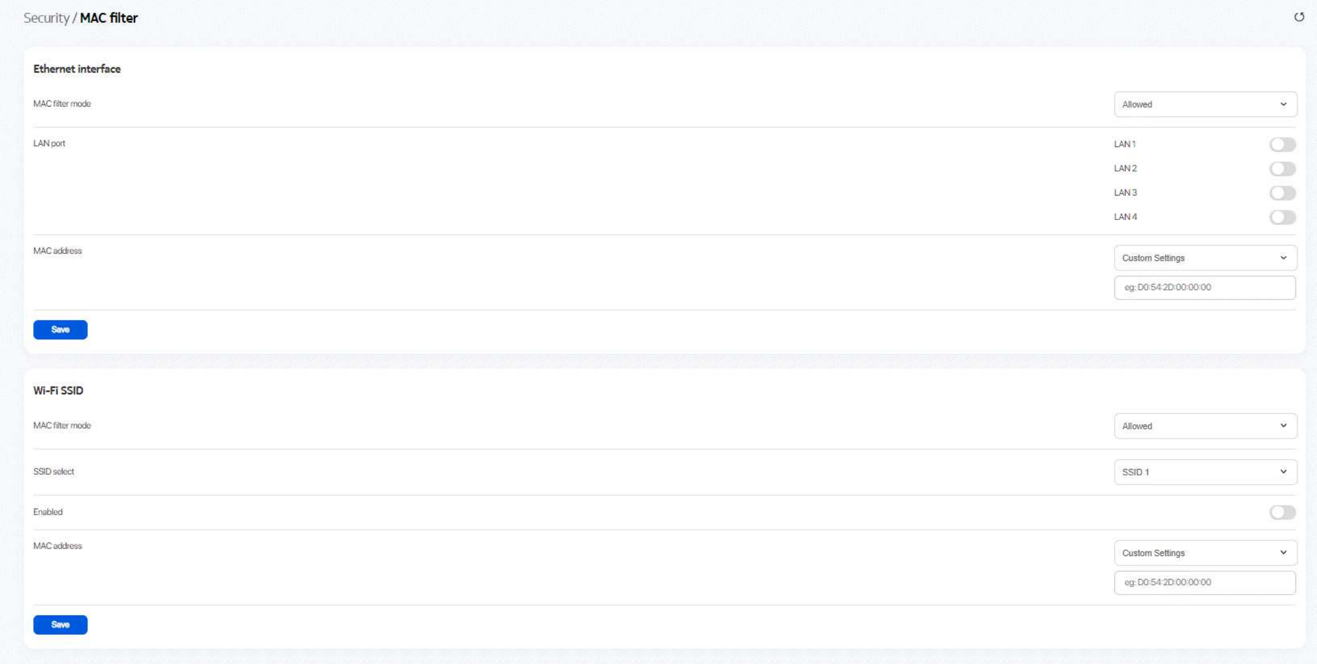
END OF STEPS

7.30 Configuring the MAC Filter

1

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

Figure 7-30 *MAC filter* page



Security / **MAC filter**

Ethernet interface

MAC filter mode: Allowed

LAN port: LAN 1, LAN 2, LAN 3, LAN 4

MAC address: Custom Settings

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

Wi-Fi SSID

MAC filter mode: Allowed

SSID select: SSID 1

Enabled

MAC address: Custom Settings

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

2

Configure the following parameters:

Table 7-19 *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 7-20 MAC filter - Wi-Fi SSID parameters

Field	Description
Wi-Fi 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

7.31 Configuring the IP Filter

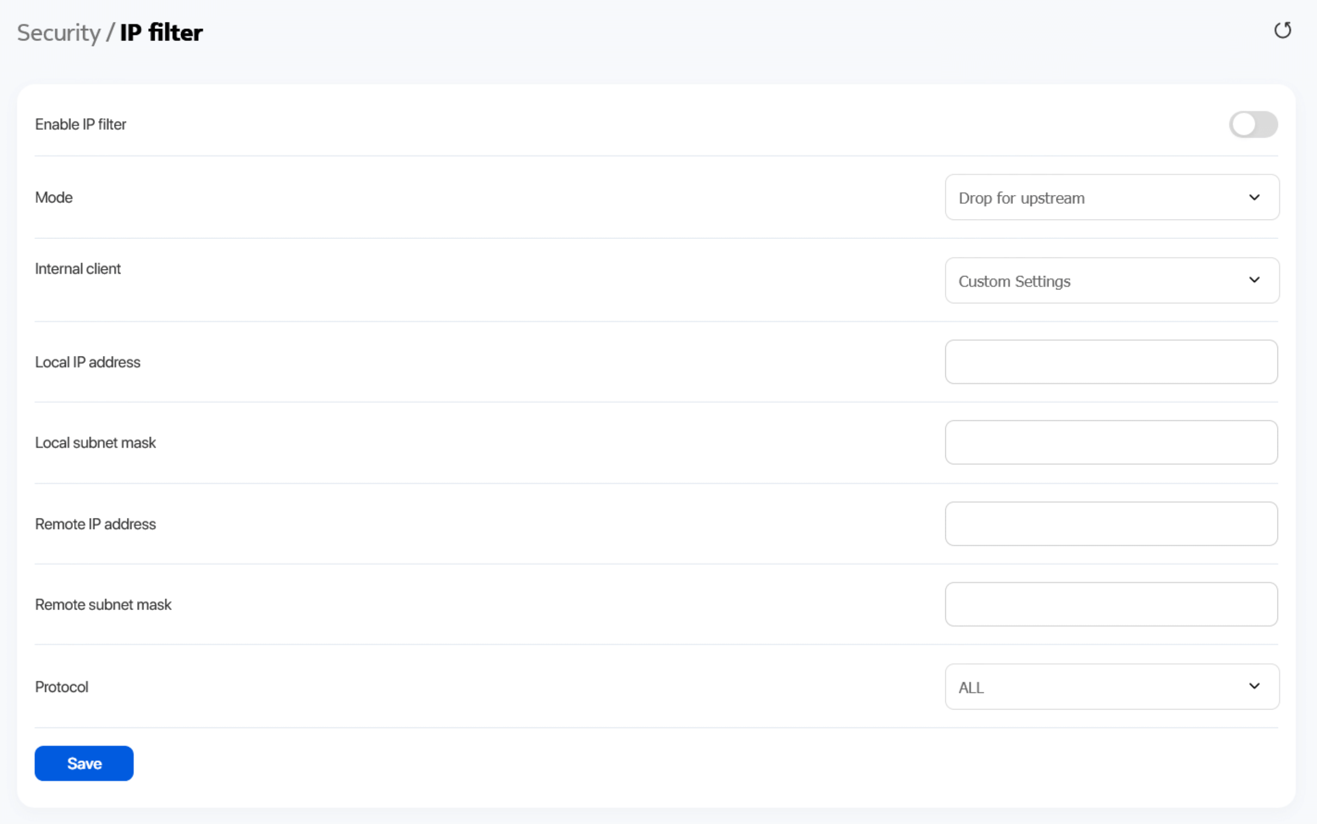
1

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

2

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

Figure 7-31 *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

3

Configure the following parameters:

Table 7-21 *IP filter* parameters

Field	Description
Add IPv4 filter or **Add IPv6 filter** parameters	
Enable IP filter	Select the toggle button to enable an IP filter.
Mode	Select an IP filter mode from the list: • **Drop for upstream** • **Drop for downstream**
Source	Select an internal client from the list: • **Custom Settings**: uses the IP address input below • **IP**: uses the connecting devices' IP to the Beacon
Add IPv4 filter parameters	

Table 7-21 *IP filter* parameters (continued)

Field	Description
Local IP address	Enter the local IP address.
Local subnet mask	Enter the local subnet mask.
Remote IP address	Enter the remote IP address.
Remote subnet mask	Enter the remote subnet mask.
Protocol	Select an application protocol or select **ALL** from the list.
Add IPv6 filter parameters	
Source IP address	Enter the source IP address.
Source Prefix	Enter the source prefix.
Destination IP address	Enter the destination IP address.
Destination prefix	Enter the destination prefix.
Protocol	Select an application protocol or select **ALL** from the list.

4

Click **Save**.

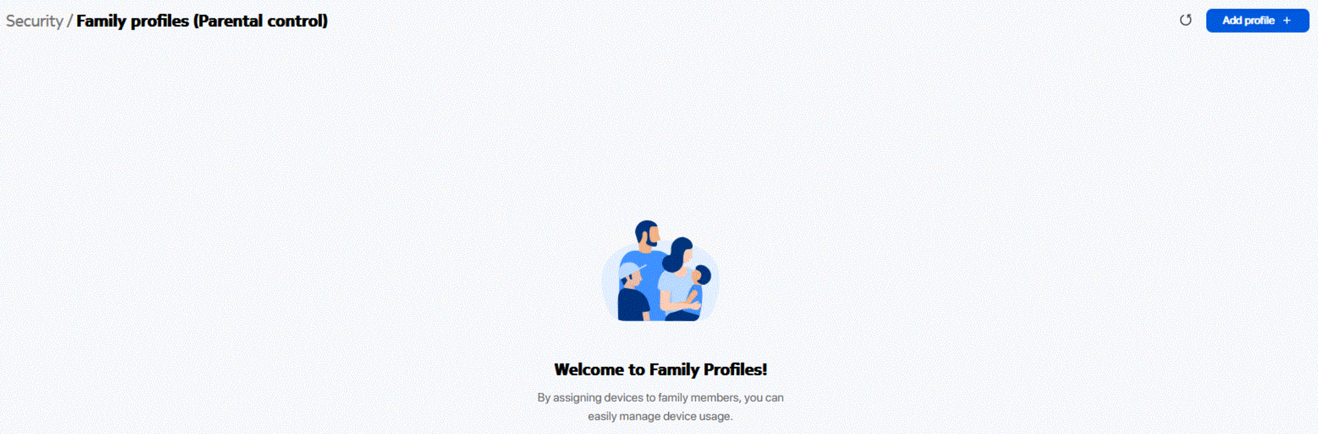
END OF STEPS

7.32 Configuring Family Profiles

1

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

Figure 7-32 *Family profiles (Parental control)* page



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

Welcome to Family Profiles!

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

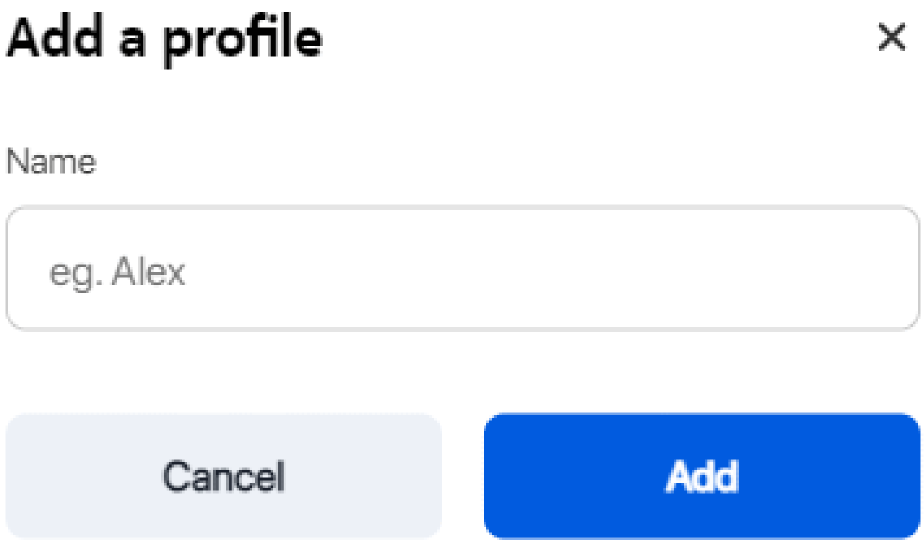
2

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 7-33 Add a profile page

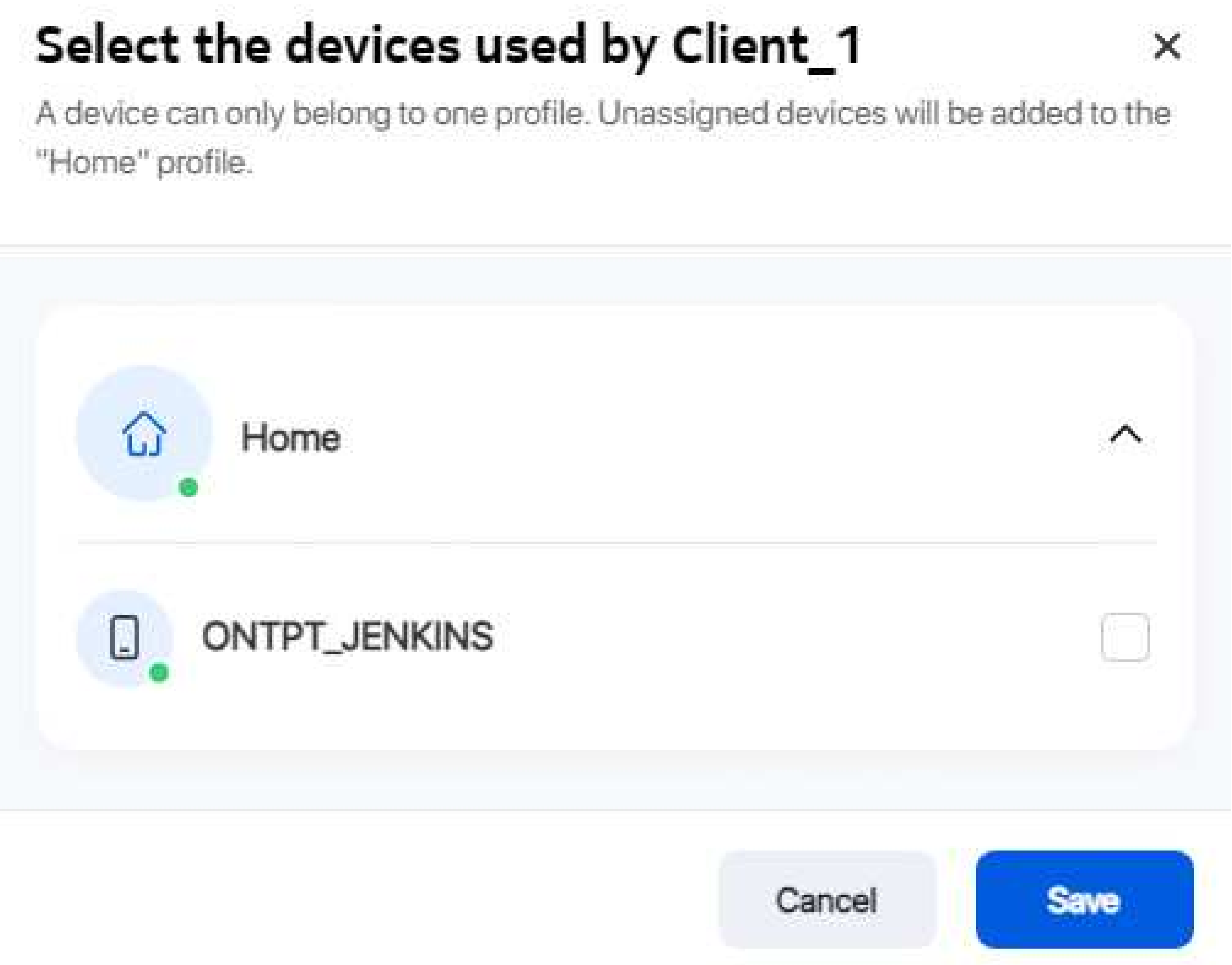


4

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 7-34 Assign devices to family profile

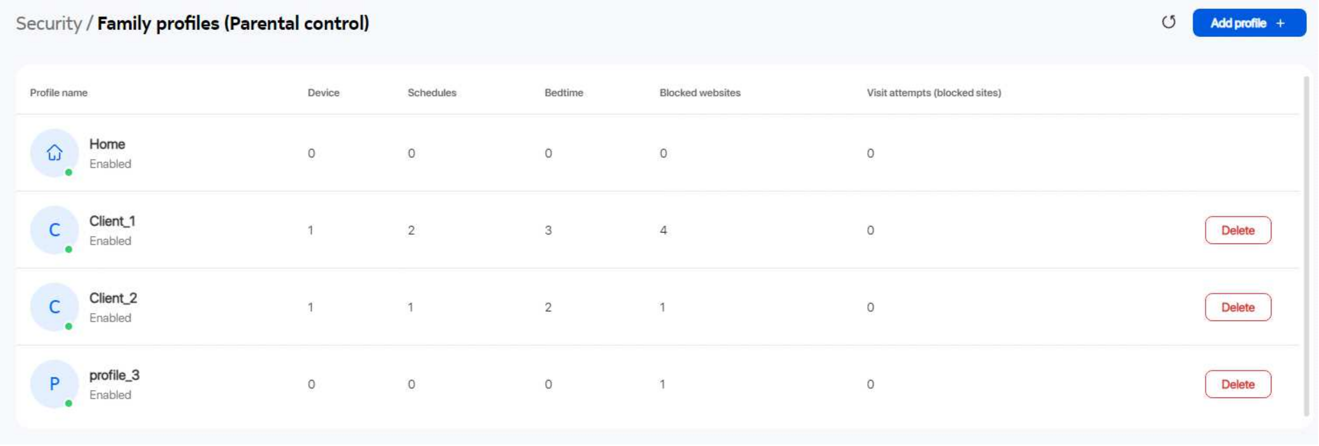


Select the devices used by Client_1

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 7-35 Family profiles table



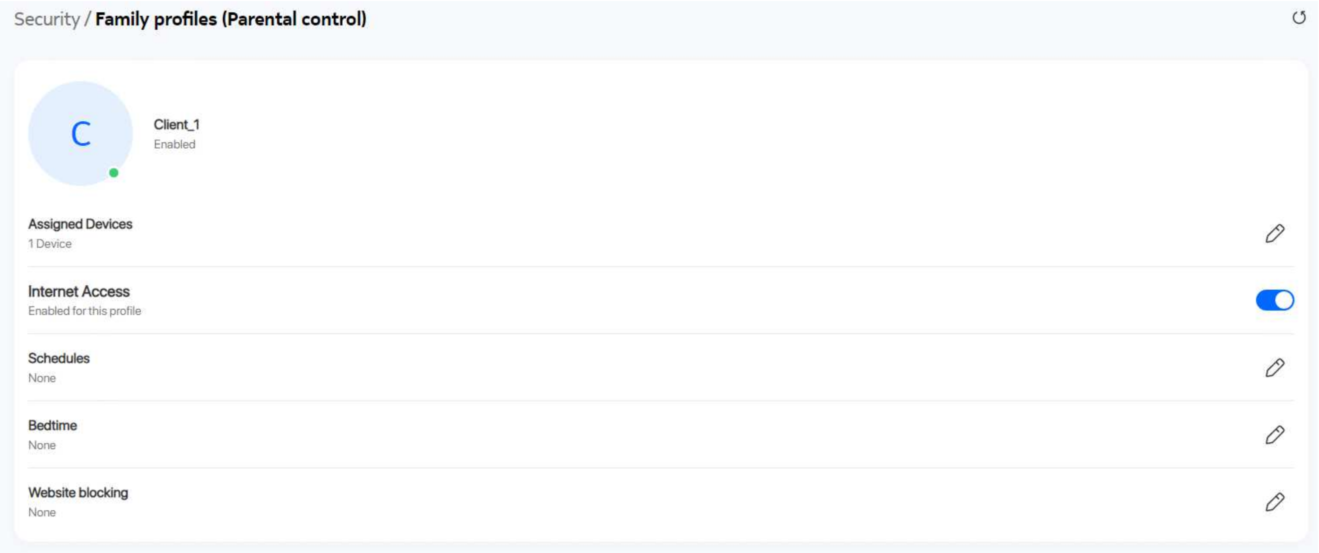
Security / **Family profiles (Parental control)**

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 7-36 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

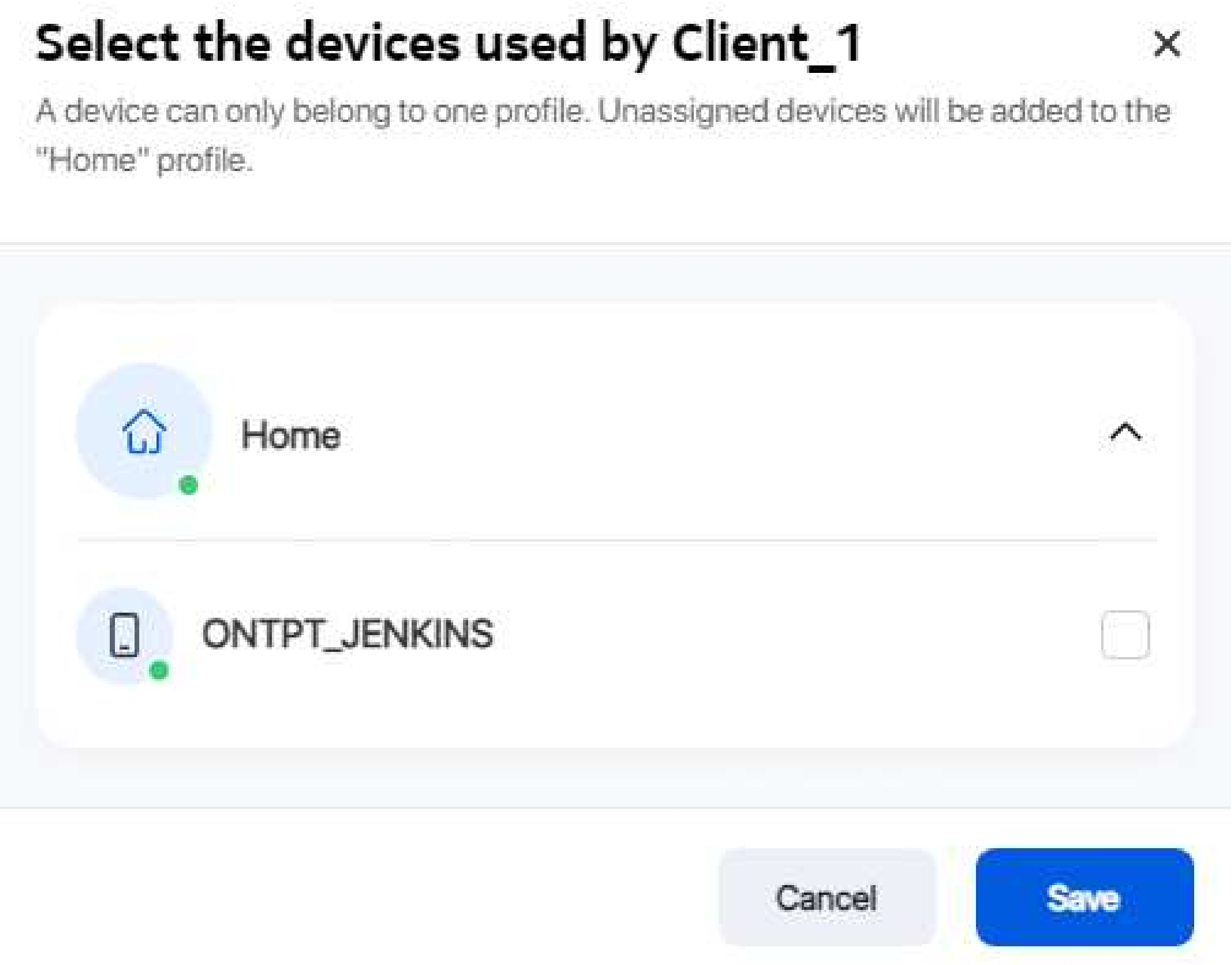
Select the **Internet Access** toggle button to enable internet access.

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

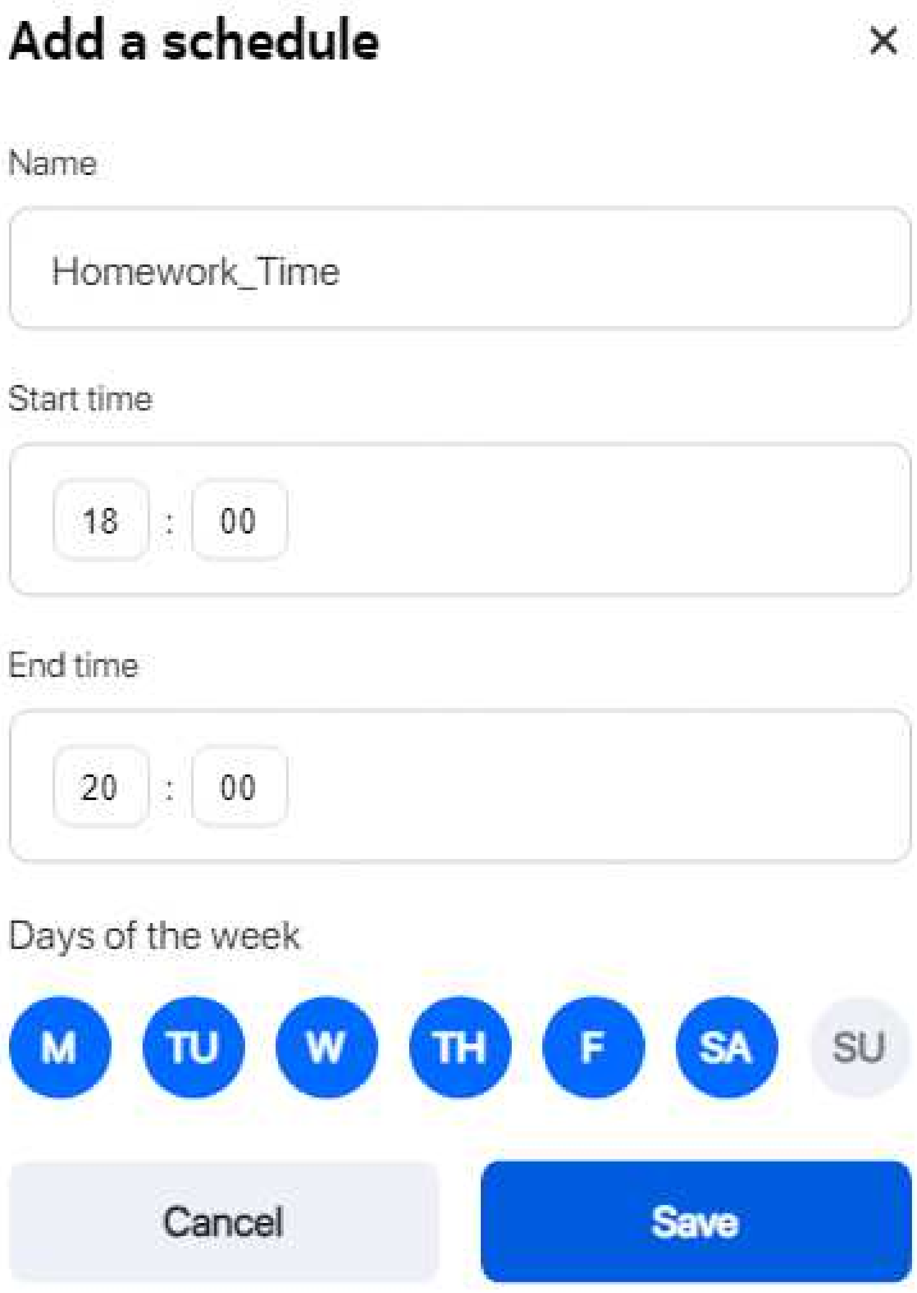
8

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

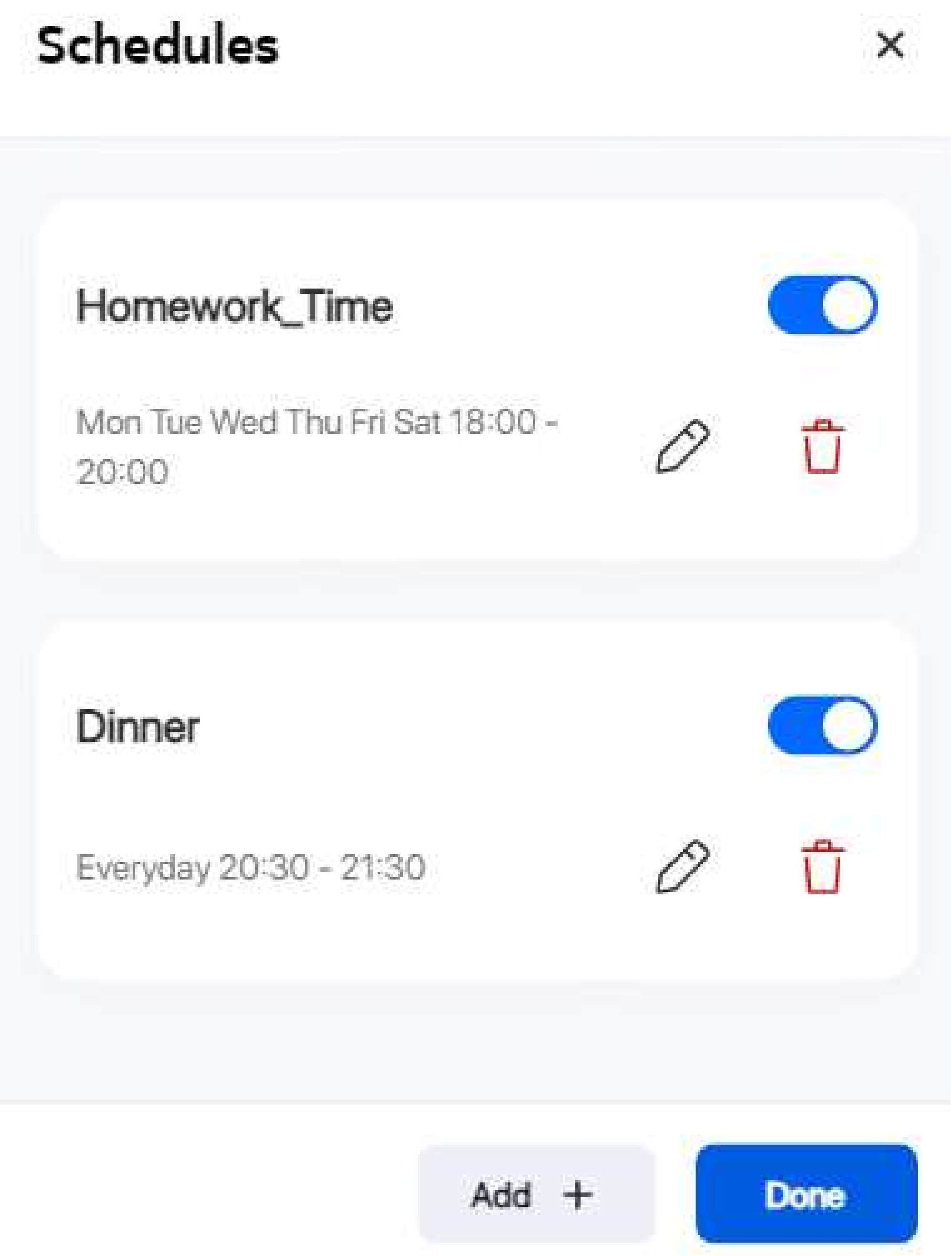
20 : 00

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

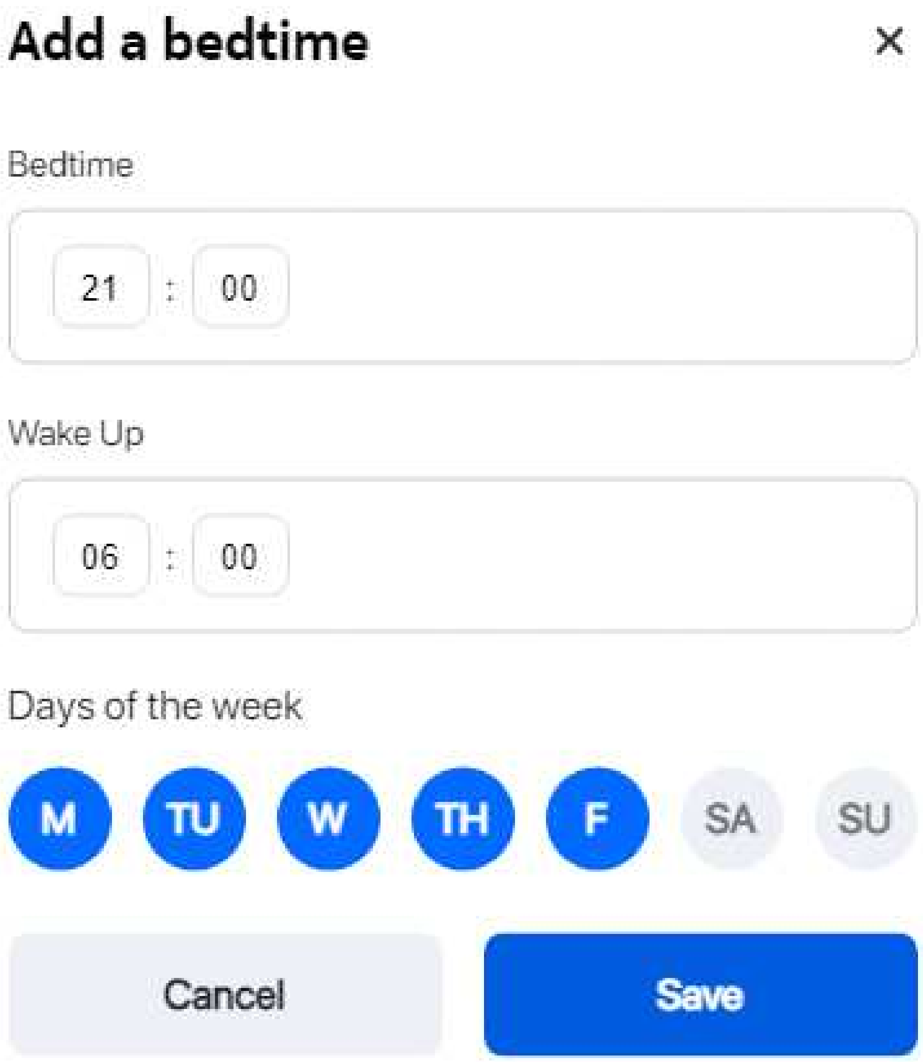
Configure bedtime for the profile:

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 SA SU

Cancel Save

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

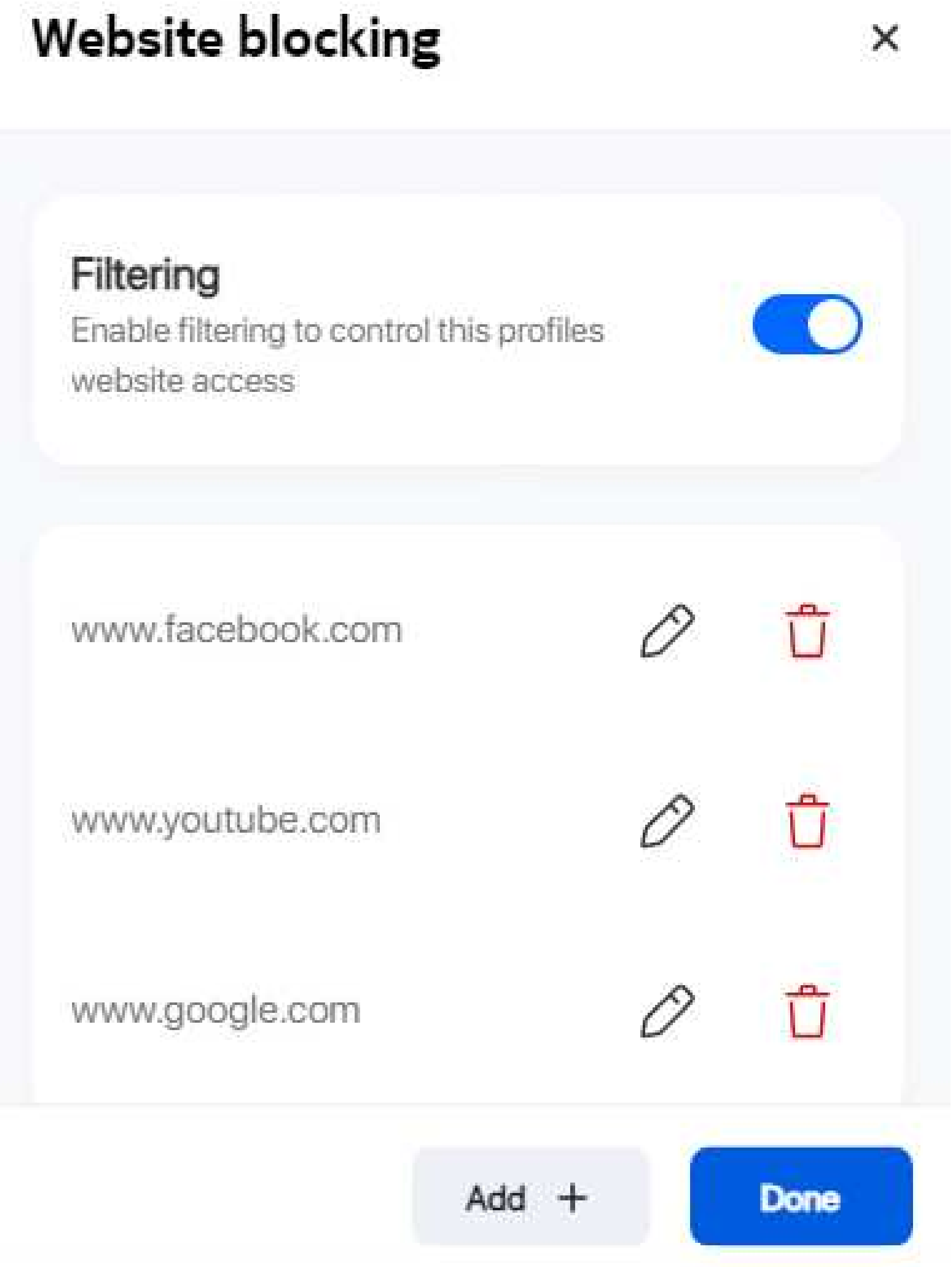
11

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:



Website blocking

Filtering
Enable filtering to control this profiles website access

www.facebook.com

www.youtube.com

www.google.com

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**.

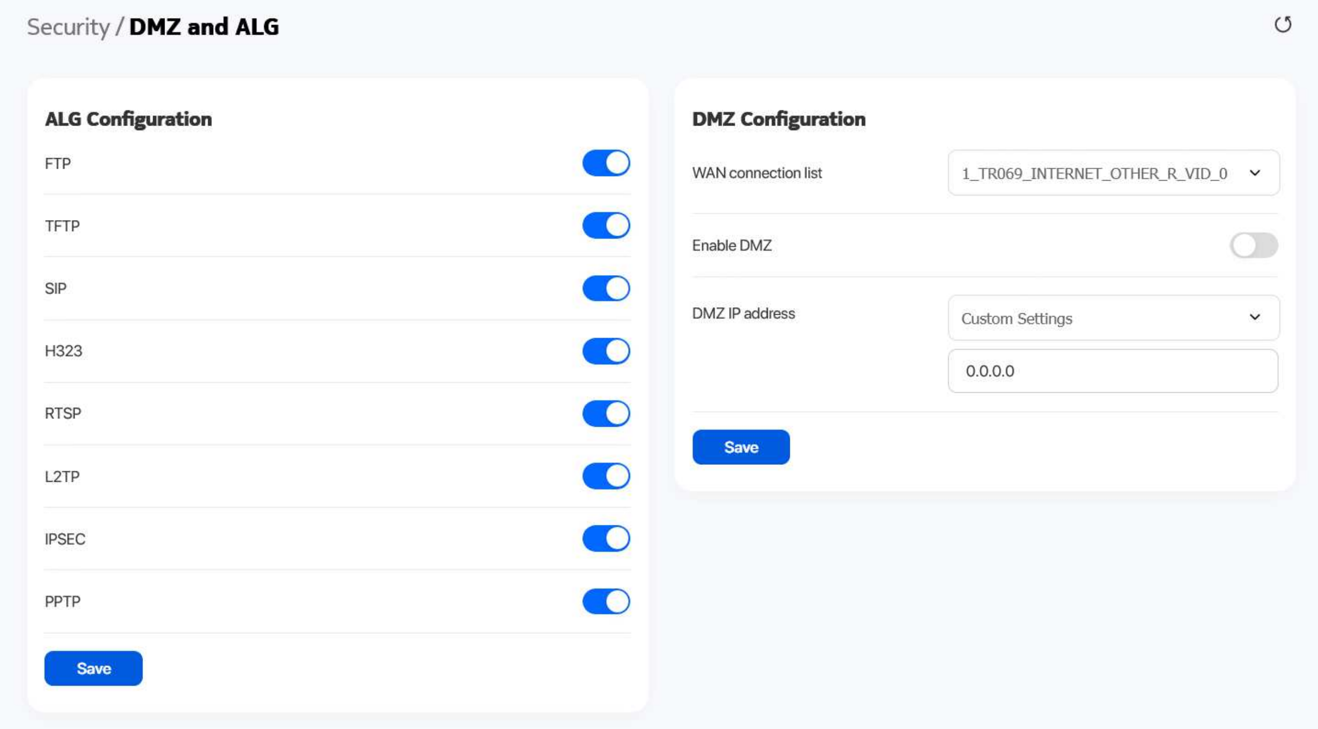
End of steps

7.33 Configuring DMZ and ALG

1

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

Figure 7-37 *DMZ and ALG* page



Security / **DMZ and ALG**

ALG Configuration

FTP
TFTP
SIP
H323
RTSP
L2TP
IPSEC
PPTP

Save

DMZ Configuration

WAN connection list 1_TR069_INTERNET_OTHER_R_VID_0

Enable DMZ

DMZ IP address Custom Settings
0.0.0.0

Save

2

Configure the following parameters:

Table 7-22 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 7-23 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

7.34 Configuring Access Control

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

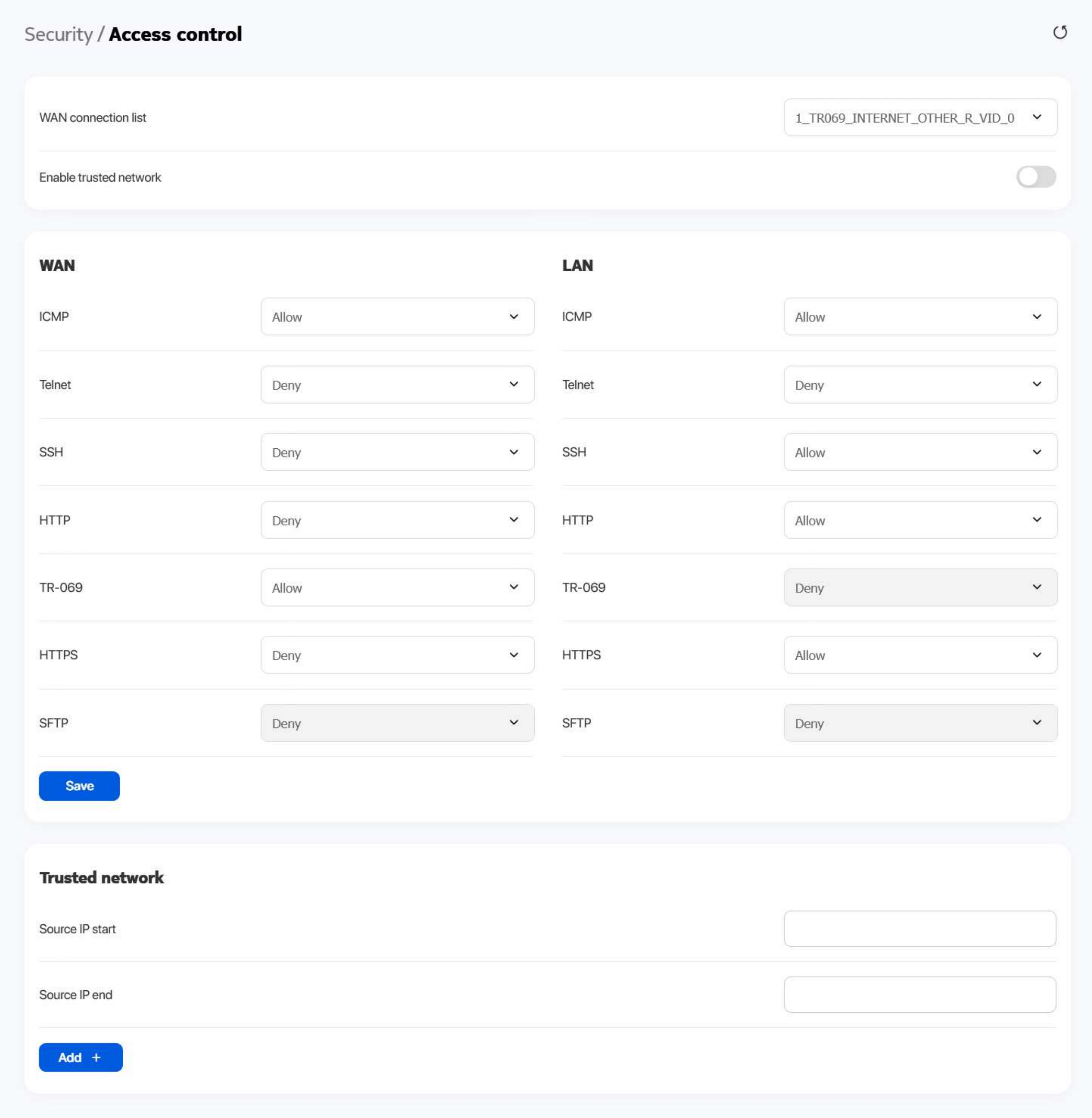
Note: ACL takes precedence over the firewall policy.

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 7-38 *Access control* page



Security / **Access control**

WAN connection list: 1_TR069_INTERNET_OTHER_R_VID_0

Enable trusted network

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

Trusted network

Source IP start

Source IP end

2

Configure the following parameters:

Table 7-24 *Access control* parameters

Field	Description
WAN connection list	Select a WAN connection from the list.
Enable trusted network	Select the toggle button to enable a trusted network.
WAN	The following protocols are supported: ICMP, Telnet, SSH, HTTP, TR-069, HTTPS, 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 7-25 *Trusted Network* parameters

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

5

Click **Add +**.

END OF STEPS

Advanced Settings

7.35 Overview

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

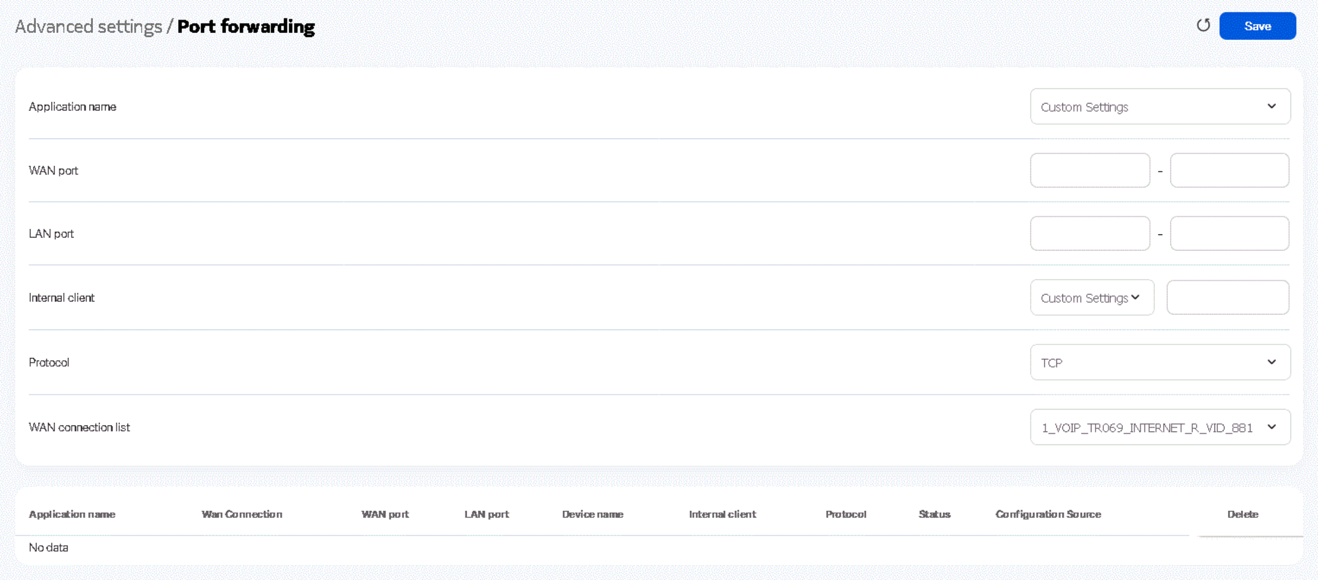
Sub-menu	Procedure
Port forwarding	7.36 “Configuring Port Forwarding” (p. 126)
Port triggering	7.37 “Configuring Port Triggering” (p. 127)
DDNS	7.38 “Configuring DDNS” (p. 129)
NTP	7.39 “Configuring NTP” (p. 130)

7.36 Configuring Port Forwarding

1

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

Figure 7-39 *Port forwarding* page



Application name: Custom Settings

WAN port: -

LAN port: -

Internal client: Custom Settings

Protocol: TCP

WAN connection list: 1_VOIP_TR069_INTERNET_R_VID_881

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

2

Configure the following parameters:

Table 7-26 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**.
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**.

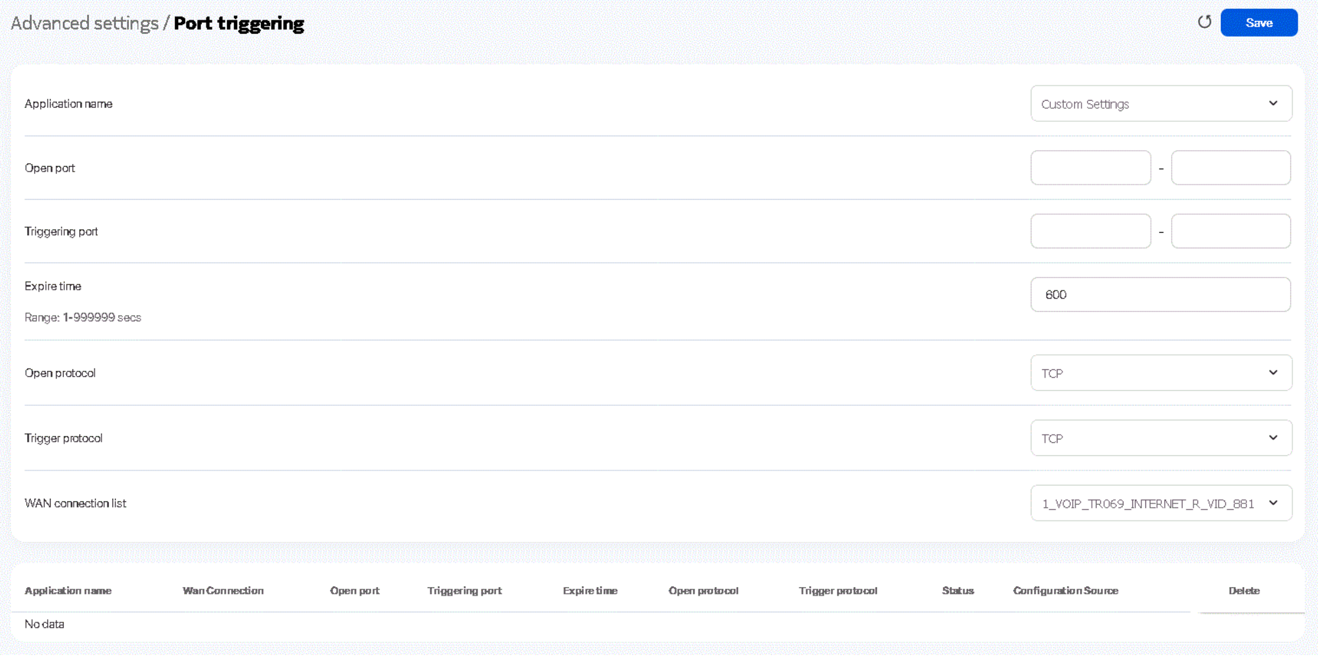
END OF STEPS

7.37 Configuring Port Triggering

1

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

Figure 7-40 *Port triggering* page



Advanced settings / **Port triggering**

Application name: Custom Settings

Open port: -

Triggering port: -

Expire time: 600
Range: 1-999999 secs

Open protocol: TCP

Trigger protocol: TCP

WAN connection list: 1_VOIP_TR069_INTERNET_R_VID_881

Application name	Wan Connection	Open port	Triggering port	Expire time	Open protocol	Trigger protocol	Status	Configuration Source	Delete
No data									

2

Configure the following parameters:

Table 7-27 *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**

Table 7-27 Port triggering parameters (continued)

Field	Description
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**.

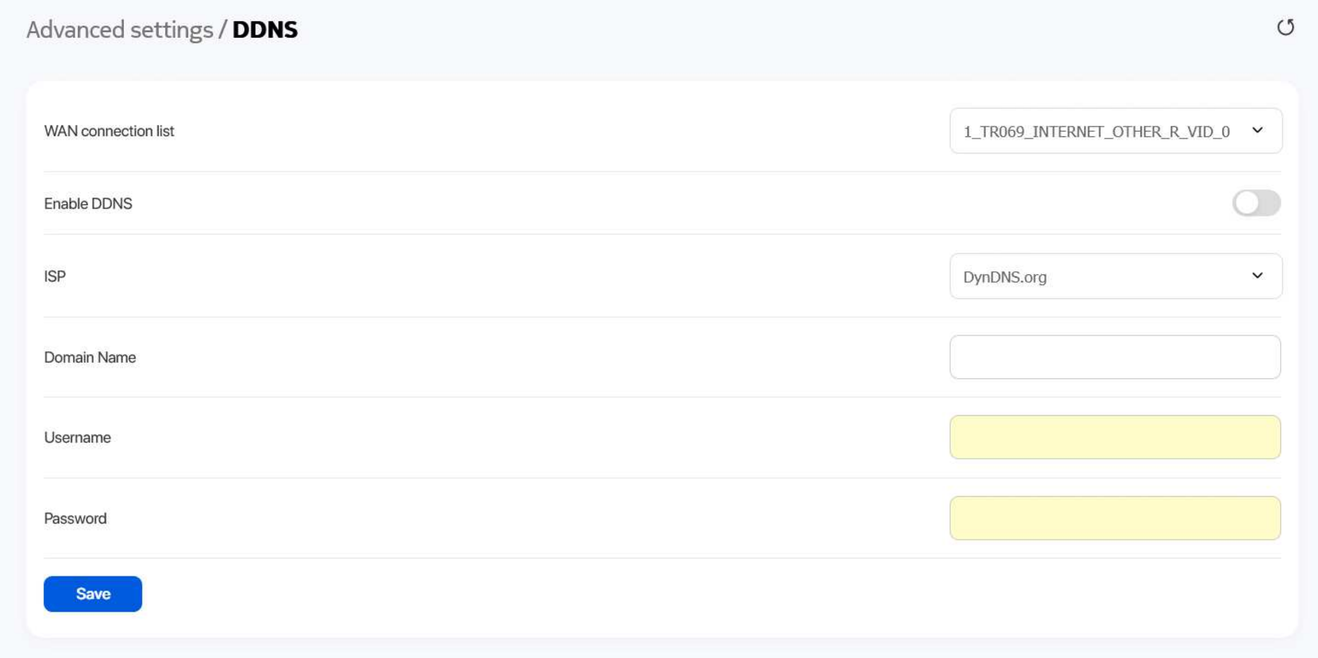
End of steps

7.38 Configuring DDNS

1

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

Figure 7-41 DDNS page



Advanced settings / **DDNS**

WAN connection list: 1_TR069_INTERNET_OTHER_R_VID_0

Enable DDNS: off

ISP: DynDNS.org

Domain Name:

Username:

Password:

2

Configure the following parameters:

Table 7-28 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**.

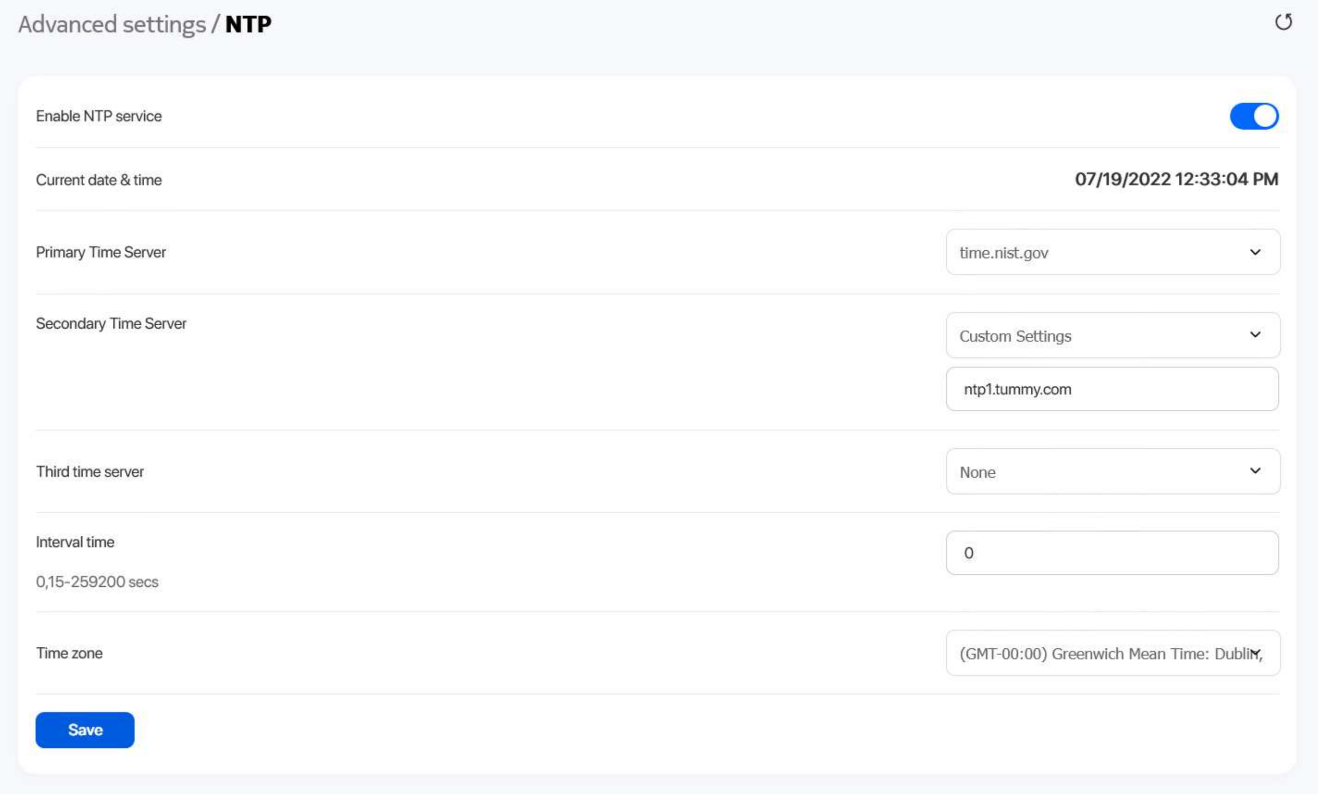
END OF STEPS

7.39 Configuring NTP

1

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

Figure 7-42 *NTP* page



Advanced settings / **NTP**

Enable NTP service: on

Current date & time: 07/19/2022 12:33:04 PM

Primary Time Server: time.nist.gov

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

Third time server: None

Interval time (0,15-259200 secs): 0

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

2

Configure the following parameters:

Table 7-29 *NTP* parameters

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

Maintenance

7.40 Overview

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

Sub-menu	Procedure
Change password	7.41 “Configuring the Password” (p. 133)
Backup and restore	7.42 “Backing Up the Configuration” (p. 135) 7.43 “Restoring the Configuration” (p. 135)
Firmware upgrade	7.44 “Upgrading Firmware” (p. 136)
Device management	7.45 “Managing the Device” (p. 138)
Diagnostics	7.46 “Diagnosing WAN Connections” (p. 138)
Log	7.47 “Viewing Log Files” (p. 141)

7.41 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”.

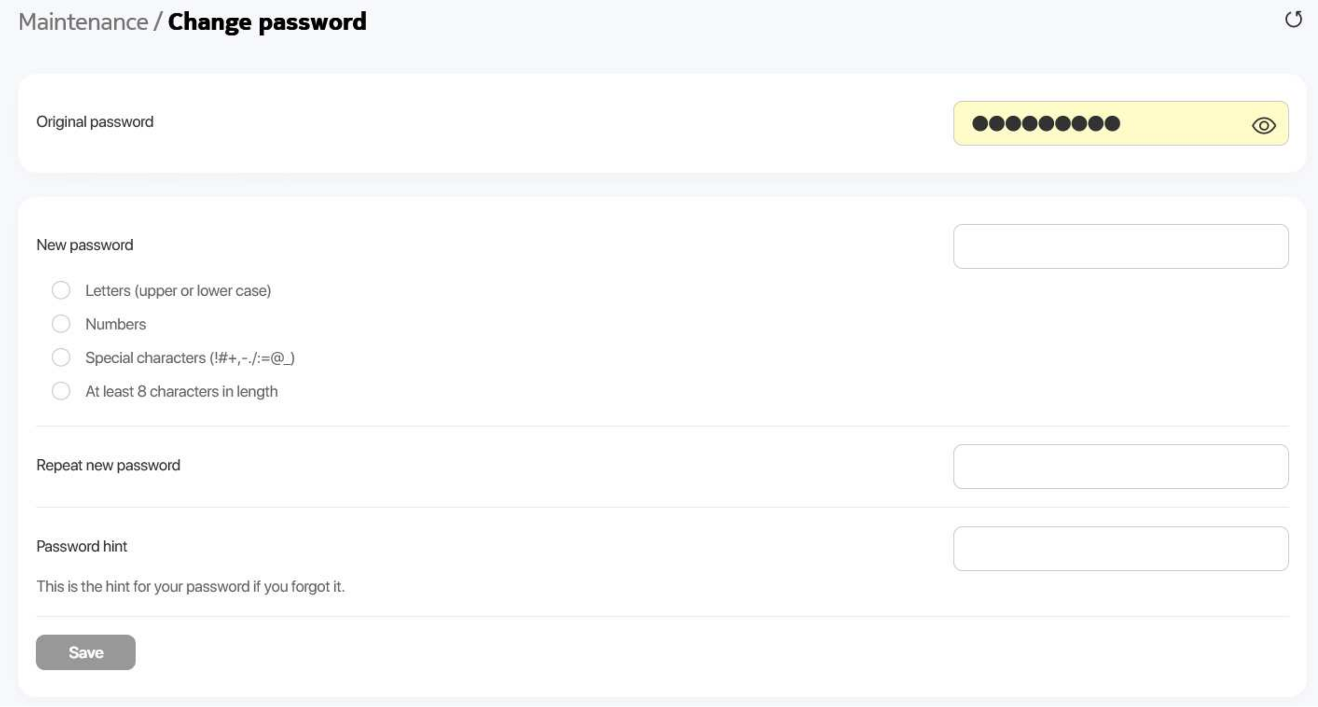
When the password does not meet the password rules, the application displays a message to indicate which password rule has not been followed, for example:

- 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→Change password** in the left pane. The *Change password* page displays.

Figure 7-43 *Change password* page



Maintenance / **Change password**

Original password ●●●●●●●●●

New password

○ Letters (upper or lower case)
○ Numbers
○ Special characters (!#+,-./:=@_)
○ At least 8 characters in length

Repeat new password

Password hint

This is the hint for your password if you forgot it.

Save

2

Configure the following parameters:

Table 7-30 *Change password* parameters

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

3

Click **Save**.

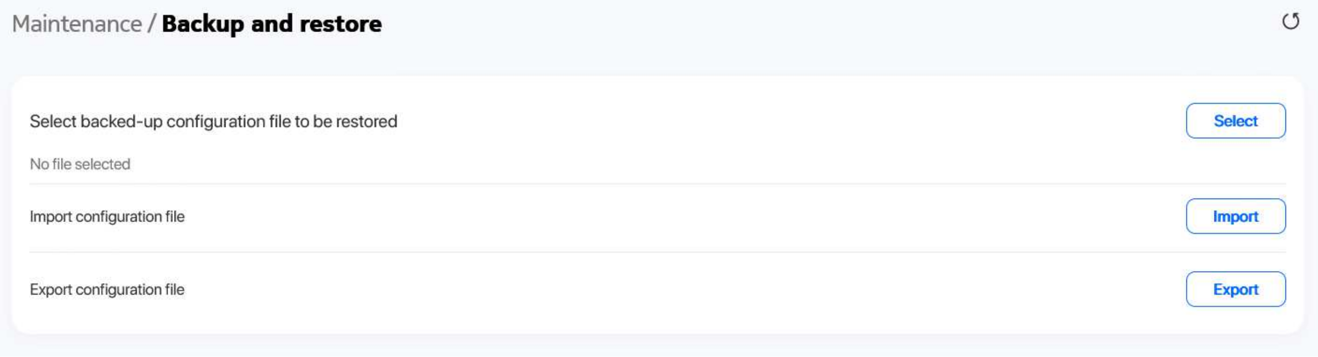
END OF STEPS

7.42 Backing Up the Configuration

1

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

Figure 7-44 *Backup and restore* page



Maintenance / **Backup and restore**

Select backed-up configuration file to be restored — Select

No file selected

Import configuration file — Import

Export configuration file — Export

2

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

END OF STEPS

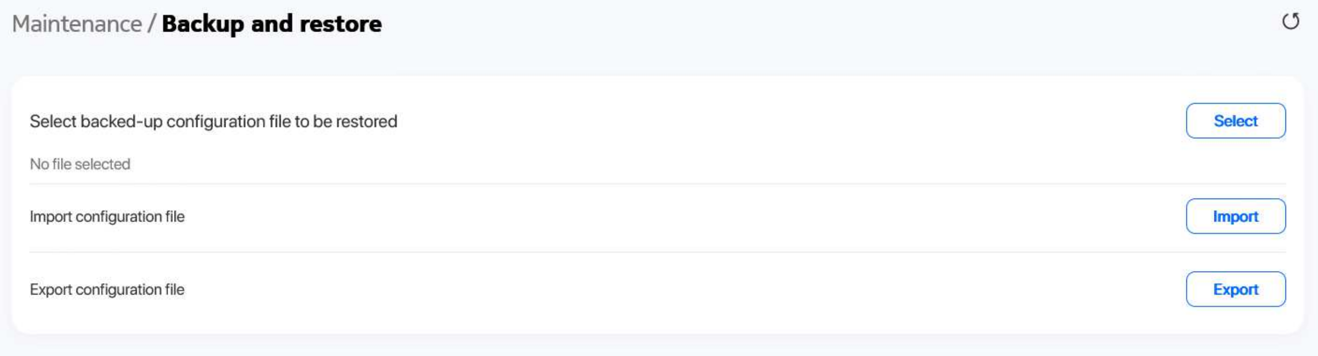
7.43 Restoring the Configuration

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 7-45 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.

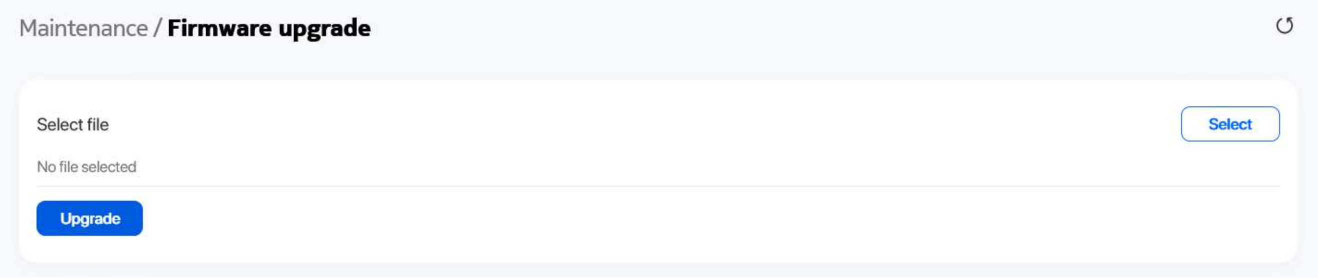
END OF STEPS

7.44 Upgrading Firmware

1

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

Figure 7-46 Firmware upgrade page



Maintenance / **Firmware upgrade**

Select file

No file selected

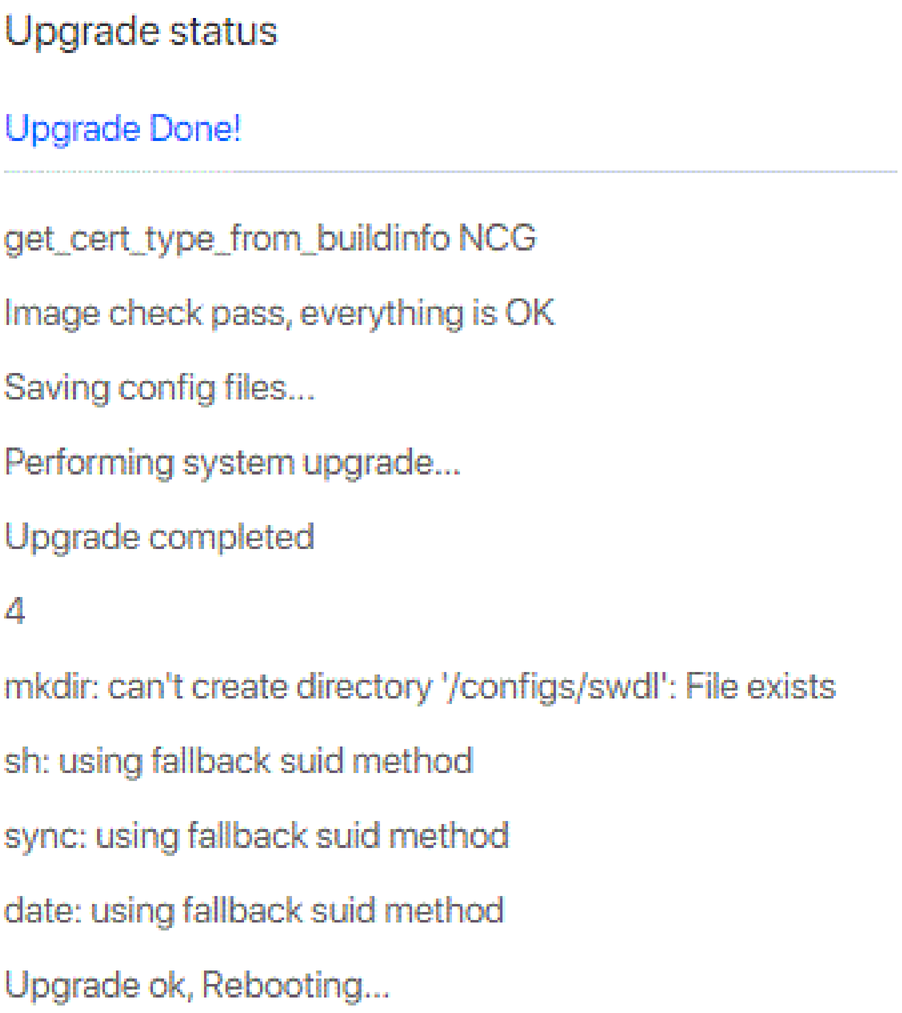
2

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 7-47 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...
```

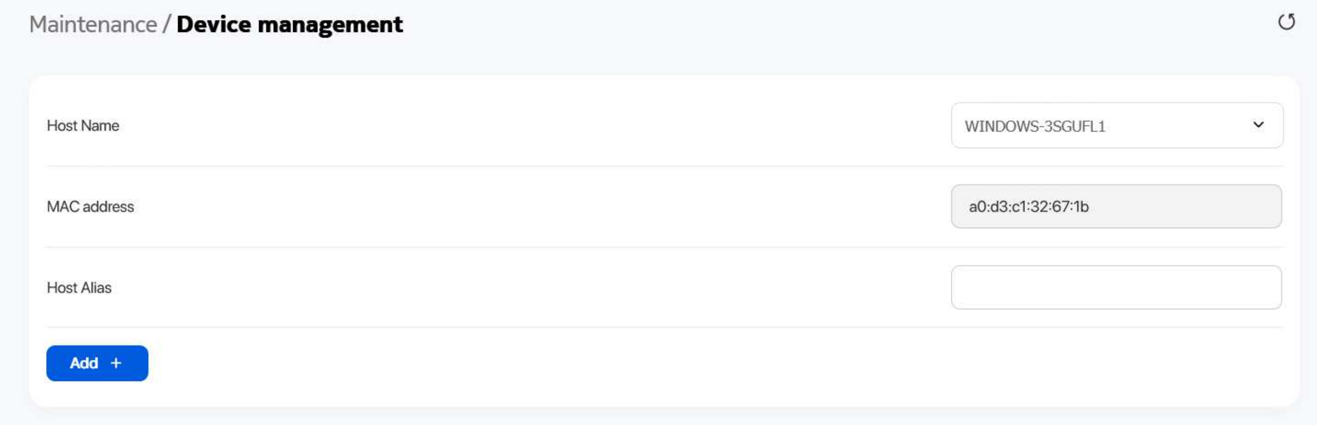
END OF STEPS

7.45 Managing the Device

1

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

Figure 7-48 *Device management* page



Maintenance / **Device management**

Host Name: WINDOWS-3SGUFL1

MAC address: a0:d3:c1:32:67:1b

Host Alias:

2

Configure the following parameters:

Table 7-31 *Device management* parameters

Field	Description
Host Name	Select a host name from the list. Three multilingual host names can be listed.
MAC address	Indicates the MAC address.
Host Alias	Enter an alias for the selected host. Three multilingual aliases can be listed.

3

Click **Add +** to add the host. The host is added to the *Device* table.

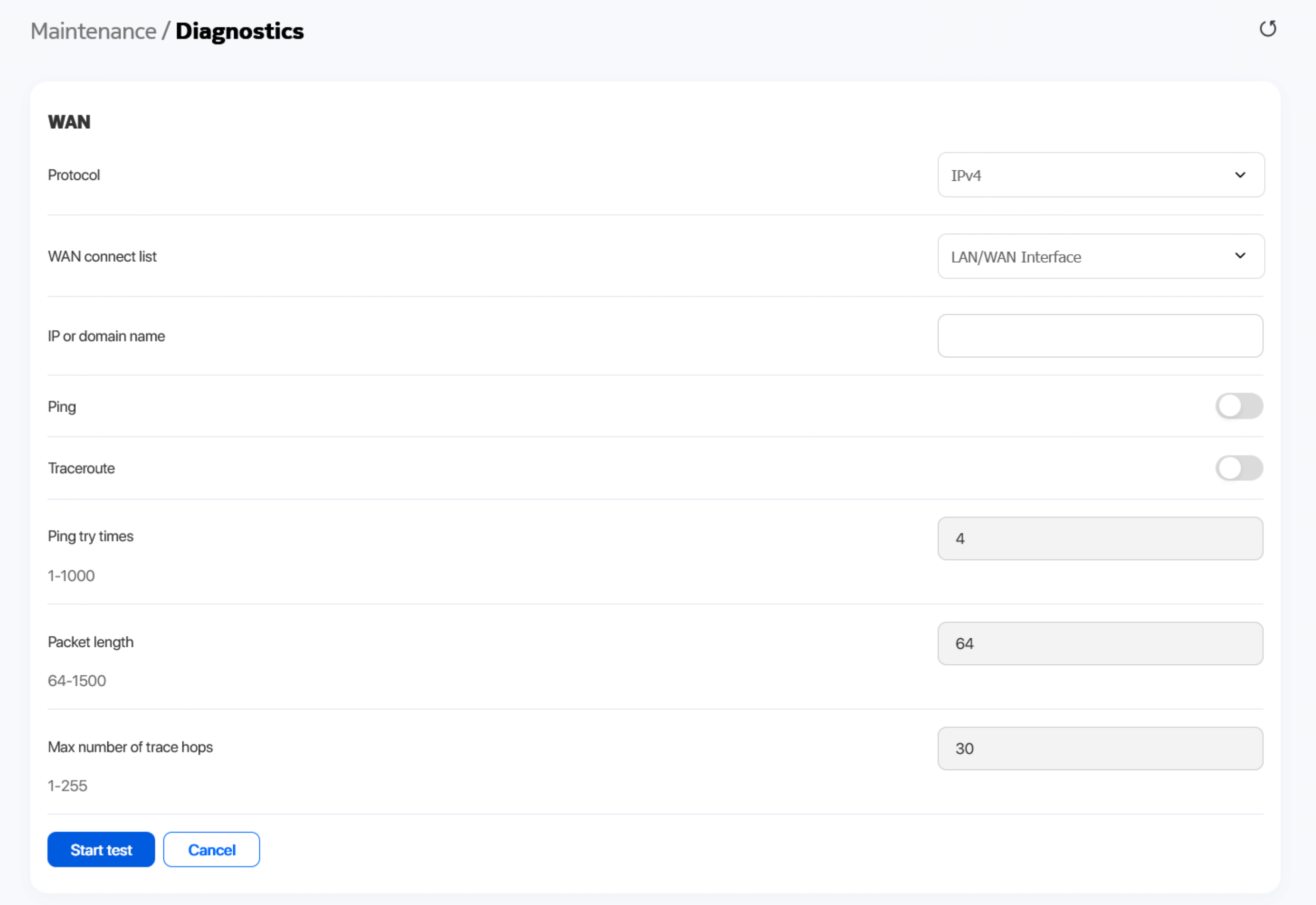
End of steps

7.46 Diagnosing WAN Connections

1

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

Figure 7-49 *Diagnostics* page



Maintenance / **Diagnostics**

WAN

Protocol: IPv4

WAN connect list: LAN/WAN Interface

IP or domain name:

Ping: ○

Traceroute: ○

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 7-32 *Diagnostics* parameters

Field	Description
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.

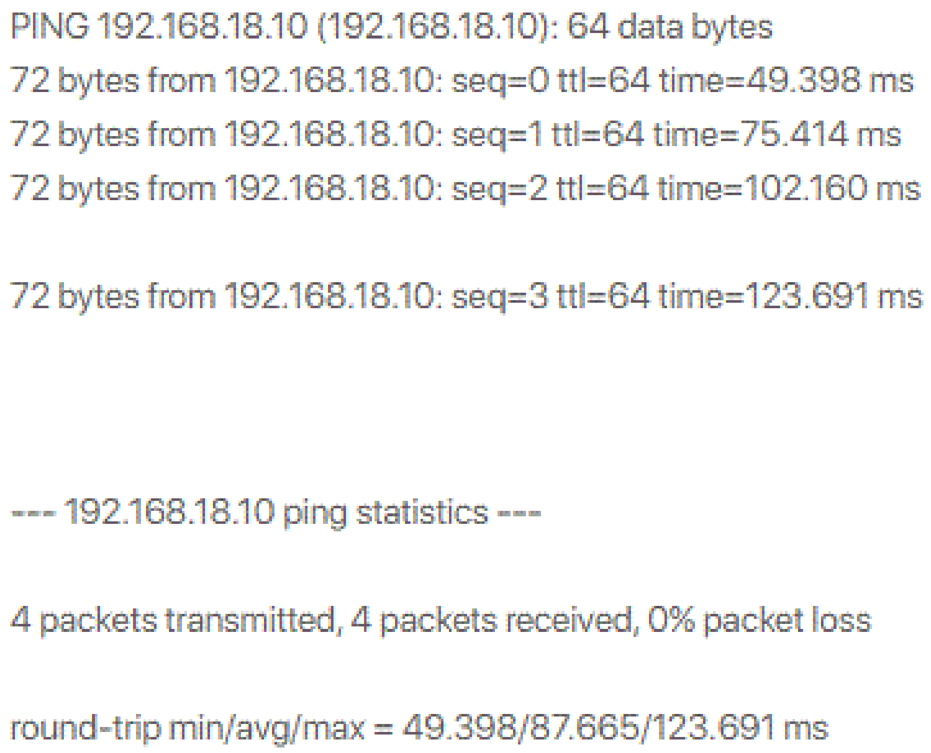
Table 7-32 *Diagnostics* parameters (continued)

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

3

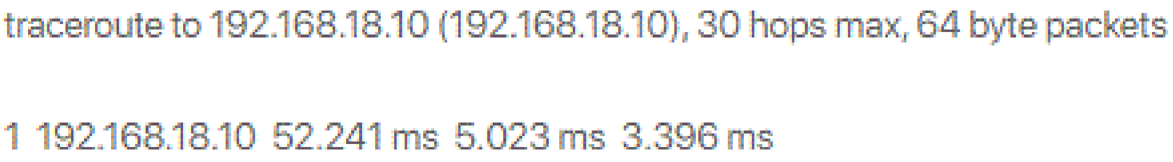
Click **Start test** to start the test. Results are displayed at the bottom of the page.

Figure 7-50 Example of ping results



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

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



--- 192.168.18.10 ping statistics ---

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

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

Figure 7-51 Example of traceroute results



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

1  192.168.18.10  52.241 ms  5.023 ms  3.396 ms
```

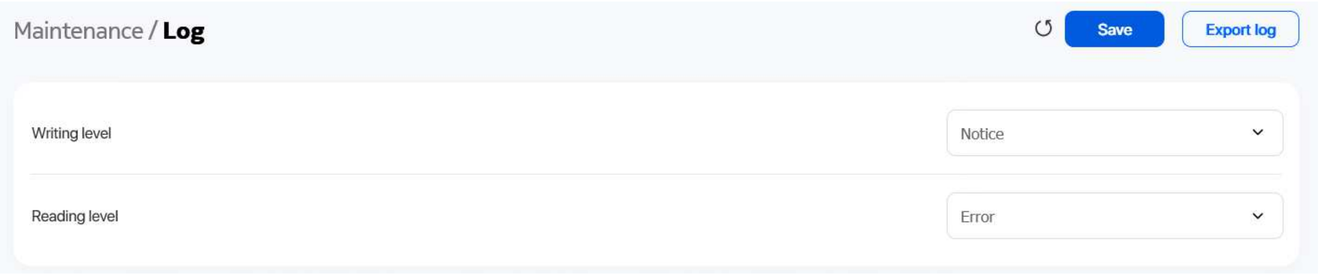
End of steps

7.47 Viewing Log Files

1

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

Figure 7-52 *Log* page



Writing level: Notice

Reading level: Error

2

Configure the following parameters:

Table 7-33 *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*.

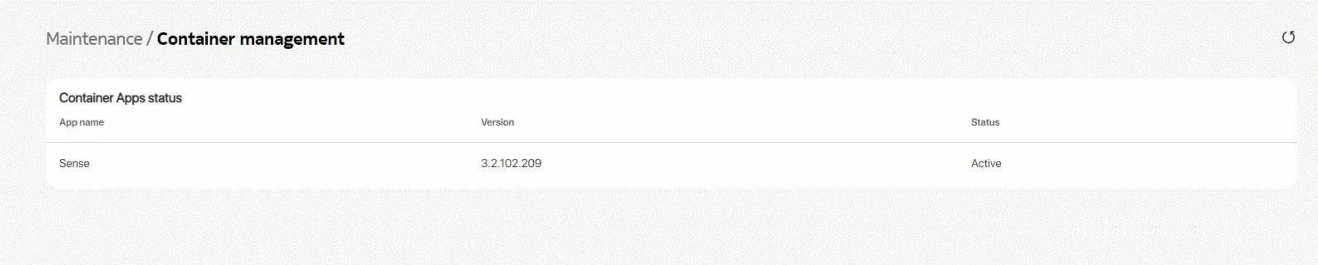
END OF STEPS

7.48 Viewing Container Management

1

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

Figure 7-53 Container management page



Maintenance / **Container management**

Container Apps status

App name	Version	Status
Sense	3.2.102.209	Active

2

Configure the following parameters:

Table 7-34 Container management parameters

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

END OF STEPS

Troubleshooting

7.49 Troubleshooting

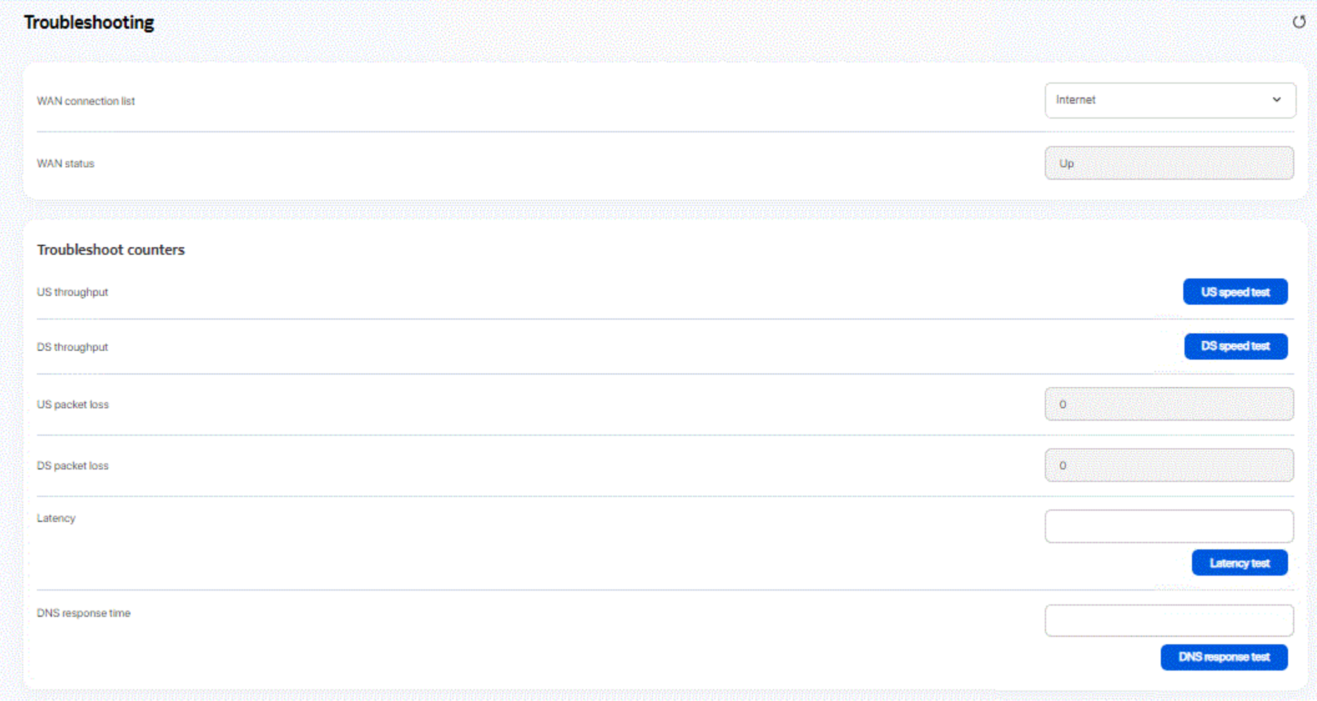
The Troubleshooting feature enables service providers and end users to monitor the performance of their broadband connection.

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 7-54 *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

2

Configure the following parameters:

Table 7-35 *Troubleshooting* parameters

Field	Description
WAN Connection List	Select a WAN connection from the list.

Table 7-35 *Troubleshooting* parameters (continued)

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

3

Click **Save**.

End of steps