

Table 7-12 US Classifier - Classifier parameters (continued)

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

6

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

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

7

Select the **Classifier Rules** tab.

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

Figure 7-22 US Classifier - Classifier Rules page

WAN / US classifier

Policy

Classifier

Classifier Rules

Policy

Select option

Classifier

Select option

Interface

Select option

Source Mac

Destination MAC

Source IP

Destination IP

Source Port

Destination Port

IP protocol type

0-254

Save

Reset

Name	Interface	Source MAC	Source IP	Source Port	Destination MAC	Destination IP	Destination Port	IP Protocol	Policy	Classifier	Delete
1											Delete

8

Configure the following parameters:

Table 7-13 US Classifier - Classifier Rules parameters

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

9

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

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

END OF STEPS

LAN Configuration

7.18 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	7.19 "Configuring DHCP IPv4" (p. 124)
DHCP IPv6	7.20 "Configuring DHCP IPv6" (p. 126)
DNS	7.21 "Configuring DNS" (p. 128)
LAN statistics	7.22 "Viewing LAN Statistics" (p. 131)

7.19 Configuring DHCP IPv4

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

Figure 7-23 DHCP IPv4 page

LAN / DHCP IPv4

IPv4 address

192.168.1.254

Subnet mask

255.255.255.0

DHCP enable

DHCP start IP address

192.168.1.64

DHCP end IP address

192.168.1.253

DHCP lease time

1440

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

Primary DNS

Secondary DNS

Save

Static IPv4 address reservations

MAC address

IPv4 address

Add

© Nokia 2021-2024

[Recommended browsers](#)

2

Configure the following LAN parameters:

Table 7-14 DHCP IPv4 parameters

Field	Description
IPv4 address	Enter the IPv4 address of the ONT.
Subnet mask	Enter the subnet mask of the ONT.
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 7-15 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 _____

7.20 Configuring DHCP IPv6

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

LAN / DHCP IPv6

LAN prefix configuration

Prefix Config

Use WAN provided prefix

Interface

1_VOIP_TR069_INTERNET_R_VID_881

Received IPv6 prefix

2003:1118:93:ff08::/64

LAN prefix configuration for gateways

Enable prefix delegation

Prefix Config

Use WAN provided prefix

Interface

1_VOIP_TR069_INTERNET_R_VID_881

Child Prefix length

Select option

IPv6 address method

Address method

Stateful DHCPv6

Enable stateless and stateful DHCPv6 simultaneously

Advanced router advertisement configuration

© Nokia 2021-2024

Recommended browsers

Minimum interval for periodic RA messages

200

secs

August 2025
Issue 1

© 2025 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.
3TN-01672-AAAA-TCZZA

127

Review

2

Configure the following parameters:

Table 7-16 DHCP IPv6 parameters

Field	Description
LAN prefix configuration	
Prefix Config	Select a prefix configuration option from the list: • Use WAN provided prefix (prefix is obtained from the WAN) • Static (enables you to enter the prefix)
Interface	This field displays if you select the Use WAN provided prefix option from the Prefix Config list. Select a WAN connection interface from the list.
Received IPv6 prefix	This field displays the received IPv6 prefix. This field is displayed only when Prefix Config is set to Use WAN provided prefix .
Static IPv6 prefix	This field displays the static IPv6 prefix. This field is displayed only when Prefix Config is set to Static .
IPv6 address method	
Address method	Select a address method option from the list: • Stateless Address Autoconfig (SLAAC) • Stateful DHCPv6
Received additional options via DHCPv6	Select the toggle button to enable additional options via DHCPv6. This field is displayed only when Address method is set to Stateless Address Autoconfig (SLAAC) .
Advanced router advertisement configuration	
Maximum interval for periodic RA messages	Enter the maximum interval (in seconds) for periodic Router Advertisement messages. Allowed values: 4 to 1800 seconds.
Minimum interval for periodic RA messages	Enter the minimum interval (in seconds) for periodic Router Advertisement messages. Allowed values: 4 to 1800 seconds

3

Click **Save**.

END OF STEPS

7.21 Configuring DNS

7.21.1 IPv4 DNS configuration

1

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

Figure 7-24 DNS page (IPv4)

LAN / DNS

IPv4 IPv6

DNS Proxy ☒

Save

Domain Name

IPv4 address

Add

Origin Domain

New Domain

Add

Static DNS entries

Domain Name	IPv4 address	Delete
dsdevice.lan	192.168.1.254	Delete

2

Configure the following parameters:

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

The *DNS* table displays the configured domain names and the associated IPv4 address. Click **Delete** to delete the table entries.

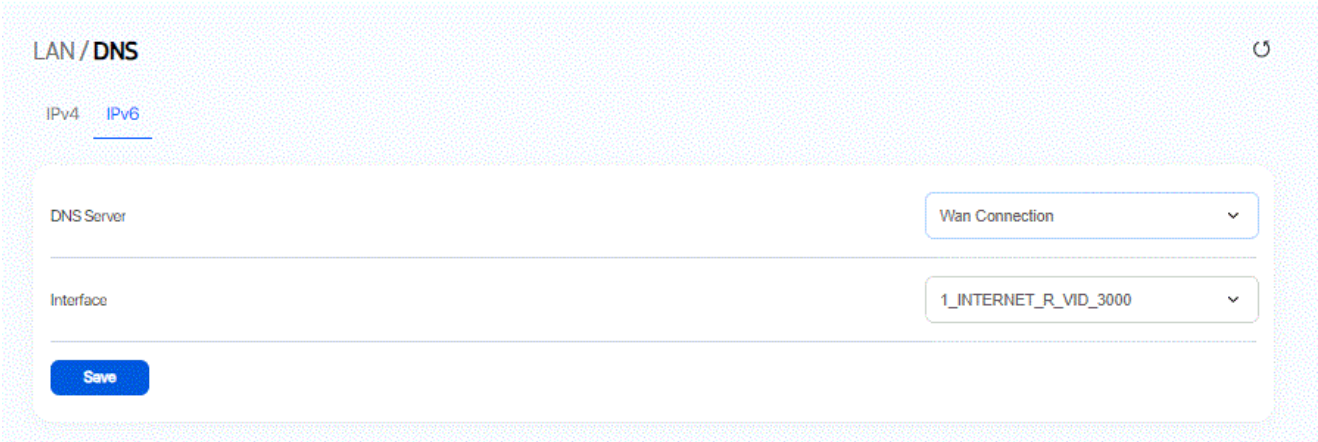
END OF STEPS

7.21.2 IPv6 DNS configuration

1

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

Figure 7-25 DNS page (IPv6)



2

Configure the following parameters

Table 7-17 DNS parameters

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

3

Click **Save**.

END OF STEPS

7.22 Viewing LAN Statistics

1

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

Figure 7-26 LAN statistics page

LAN / LAN statistics

LAN ethernet info

Ethernet status	Up
Ethernet IP address	192.168.1.254
Ethernet subnet mask	255.255.255.0
Ethernet MAC address	56-3d-71-19-71-51
Ethernet Rx packets	80447
Ethernet Tx packets	86597
Ethernet Rx bytes	10166670
Ethernet Tx bytes	27268183

Info	LAN 1	LAN 2	LAN 3	LAN 4
Status	Up	Down	Down	Up
Duplex mode	Full Duplex	Half Duplex	Half Duplex	Full Duplex
Max bit rate	1000	Auto	Auto	1000
Bytes sent	23344548	0	0	3935118
Bytes received	9964620	0	0	203094
Packets sent	71611	0	0	14999
Packets received	79912	0	0	543
Errors sent	0	0	0	0
Unicast packets received	67724	0	0	540
Discard packets sent	0	0	0	0
Discard packets received	2561	0	0	0
Multicast packets sent	5962	0	0	14663
Multicast packets received	11812	0	0	0
Broadcast packets sent	7	0	0	336
Broadcast packets received	376	0	0	3
CRC errors received	0	0	0	0

Table 7-18 LAN statistics parameters

Field	Description
LAN Ethernet info	Displays the Ethernet status IP address, subnet mask, MAC address, received and transmitted bytes and packets.
Info	Displays the information of each such as status, duplex mode, maximum bit rate, packets received and sent, CRC errors, and so on.

END OF STEPS

WiFi Configuration

7.23 Overview

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

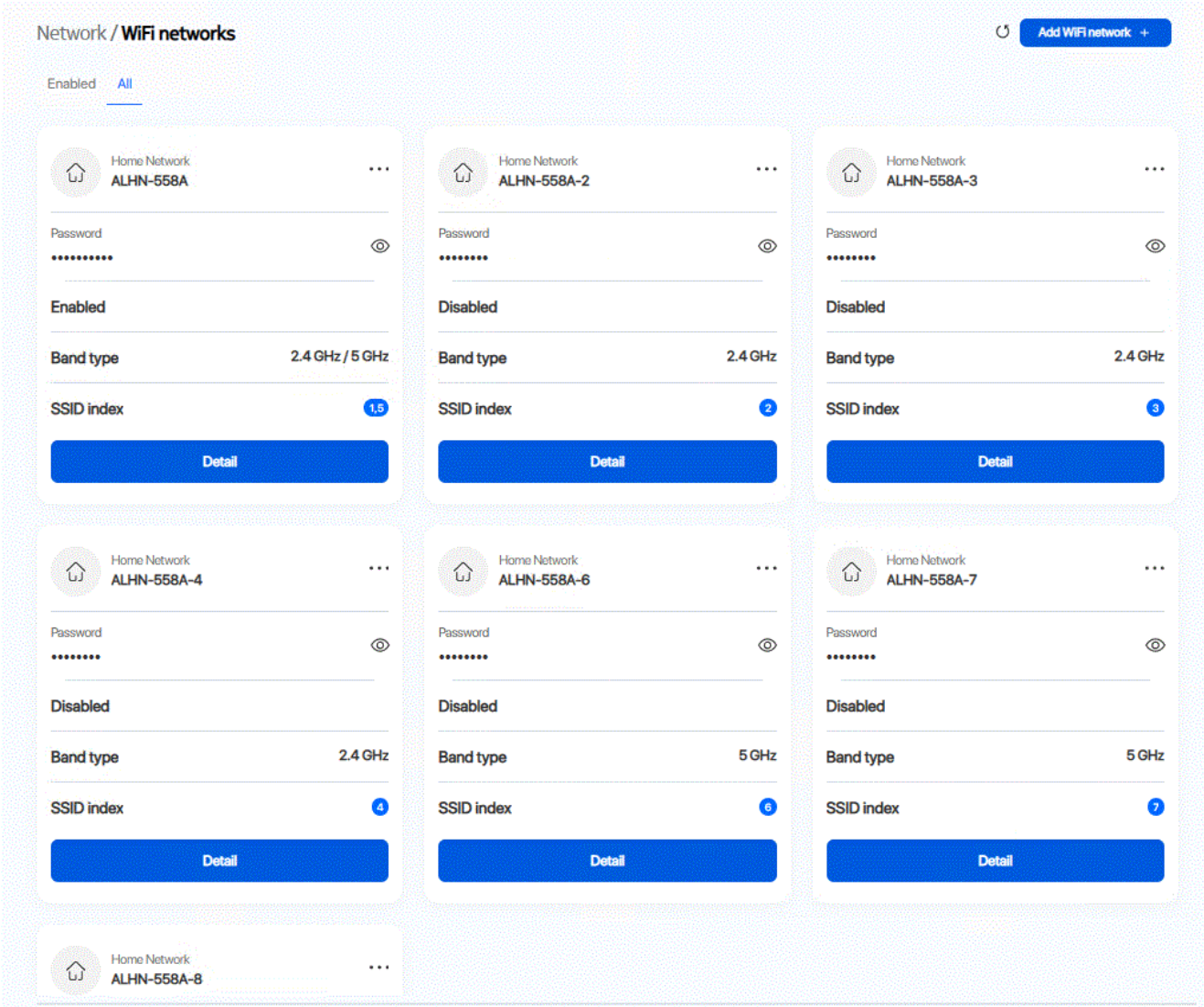
Sub-menu	Procedure
WiFi networks	7.24 "Configuring WiFi Network" (p. 133)
Network map	7.26 "Viewing Network Map, Adding WiFi Points, Renaming WiFi Points and Removing WiFi Points" (p. 139)
Advanced settings	7.28 "Configuring Wireless 2.4 GHz" (p. 143) 7.29 "Configuring Wireless 5 GHz" (p. 145)
Wireless schedule	7.30 "Configuring Wireless Schedules" (p. 147)
WiFi statistics	7.31 "Viewing WiFi Statistics" (p. 149)

7.24 Configuring WiFi Network

1

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

Figure 7-27 WiFi network page



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

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

Figure 7-28 Add WiFi network page

Add WiFi network

×

Please select a preferred network type from the options below.

Multi Band

Recommended — Band steering will intelligently move your devices from the 2.4GHz and 5GHz network based on usage, speed, coverage and distance.

☒

2.4 GHz

☐

5 GHz

☐

Next

3

Configure the following parameters:

Table 7-19 Add WiFi network parameters

Field	Description
Multiband	Select this option to configure a multiband wireless network. This option is recommended your devices on 2.4 GHz bands 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.

4

Click **Next**.

5

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

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



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

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

Figure 7-29 WiFi network - example of SSID Configuration page

← WiFi / WiFi networks / Camera

SSID configuration

SSID name

Camera

Enable WiFi network

☒

Band type

2.4 GHz / 5 GHz

SSID index

1,5

Broadcast the WiFi network

☒

Guest mode

Disabled

Port Mode

Route

Isolation

☐

Total max users

64

Encryption mode

WPA3-Personal-Transition

Password

••••••••••••••••

Enable WPS

☐

Domain grouping

☐

Save

- 8
- Configure the following parameters:

Field	Description
SSID name	Displays the SSID name.
Band type	Displays the band type.
SSID index	Displays the SSID index.

Field	Description
Broadcast the WiFi network	Select the toggle button to enable broadcasting of the WiFi network.
Enable WPS	Select the toggle button to enable WPS. Note: When you select Enable, a security warning is displayed. Click OK to continue.
WPS Mode	Select the required WPS mode from the list: • PBC • STA PIN • AP PIN Select a WPS mode from the list: PBC (Push Button Connect) or STA PIN (Personal Identification Number) or AP PIN (Access Point Personal Identification Number). If the WPS mode is AP PIN, Click Get PIN Number . A PIN Code Number is generated. Then, the end user must click WPS Connect and enter the generated PIN Code Number into the station, so that the station can connect to the selected SSID. If the WPS mode is STA PIN, the PIN Code Number will be generated by the station. Then, the end user must enter this PIN Code Number into the PIN Code Number field and click WPS Connect , so that the station can connect to the selected SSID.
Domain Grouping	Select the toggle button to enable domain grouping.

Notes:

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

9

Click **Save**.

END OF STEPS

7.25 Configuring the WiFi Password

A password must adhere to the following password rules:

- The password must consist of uppercase letters, lowercase letters, numbers, and the following special characters ! # + , - . / : = @ _
- The password length must be from 8 to 63 characters.
- The first character must be a number or a letter.
- The password must contain all three types of characters: numbers, letters, or special characters.
- The same character must not appear more than 8 times in a row.
- The password cannot be a dictionary password (for example:12345678).

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

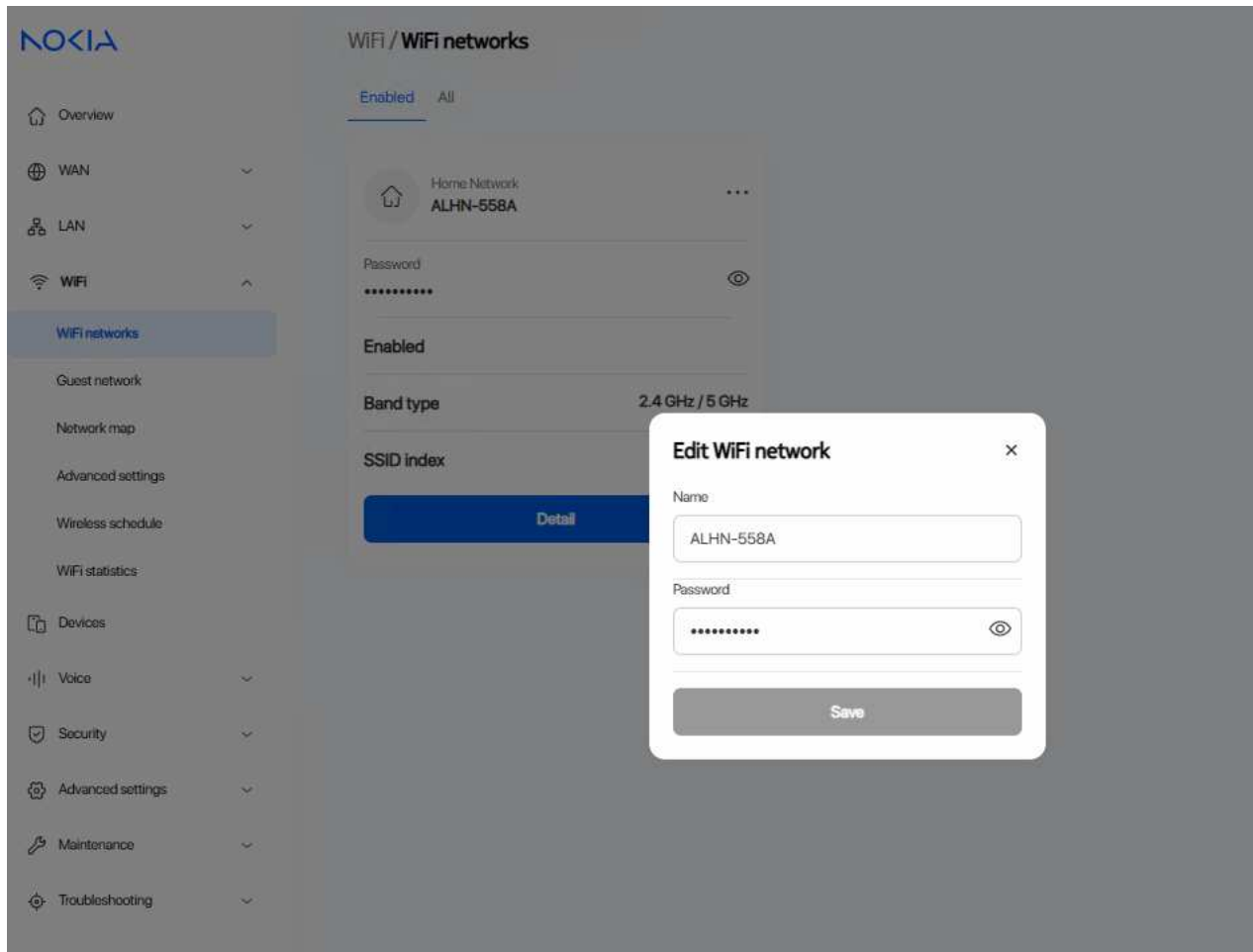
When the password does not meet the password rules, the application displays a message to indicate which password rule has not been followed, for example:

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

1

Click **WiFi** → **Wi-Fi networks** → **3 dots to edit** → **Change password** in the left pane. The *Edit Wi-Fi network* page displays.

Figure 7-30 Edit Wi-Fi network page



2 _____
Enter the new password.

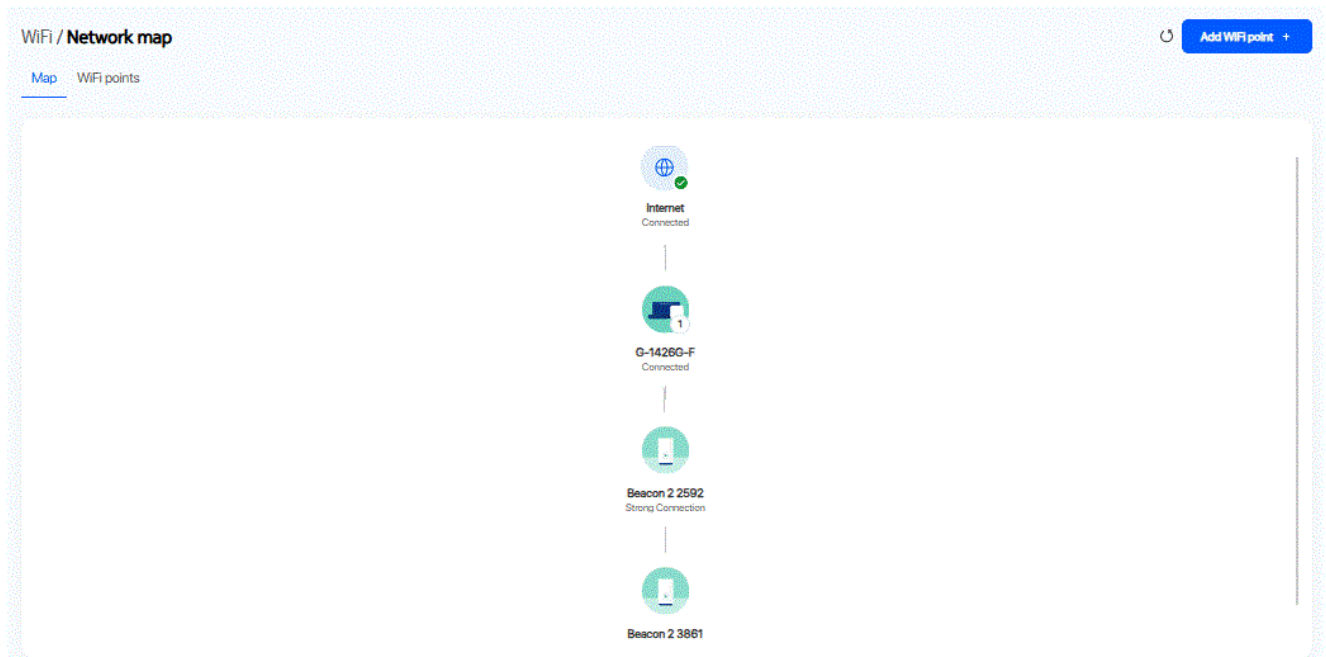
3 _____
Click **Save**.

END OF STEPS _____

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

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

Figure 7-31 Network map page



2 _____
Perform the following steps to add a WiFi point:
a. Click **Add WiFi point** at the top right corner of the *Device Info* page. A message displays

that it is recommended to use the Nokia WiFi mobile app to add a WiFi point.

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

Add WiFi point



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

Cancel

Continue with Web GUI

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

Add WiFi point



Serial number

ALCLB3F49E3J

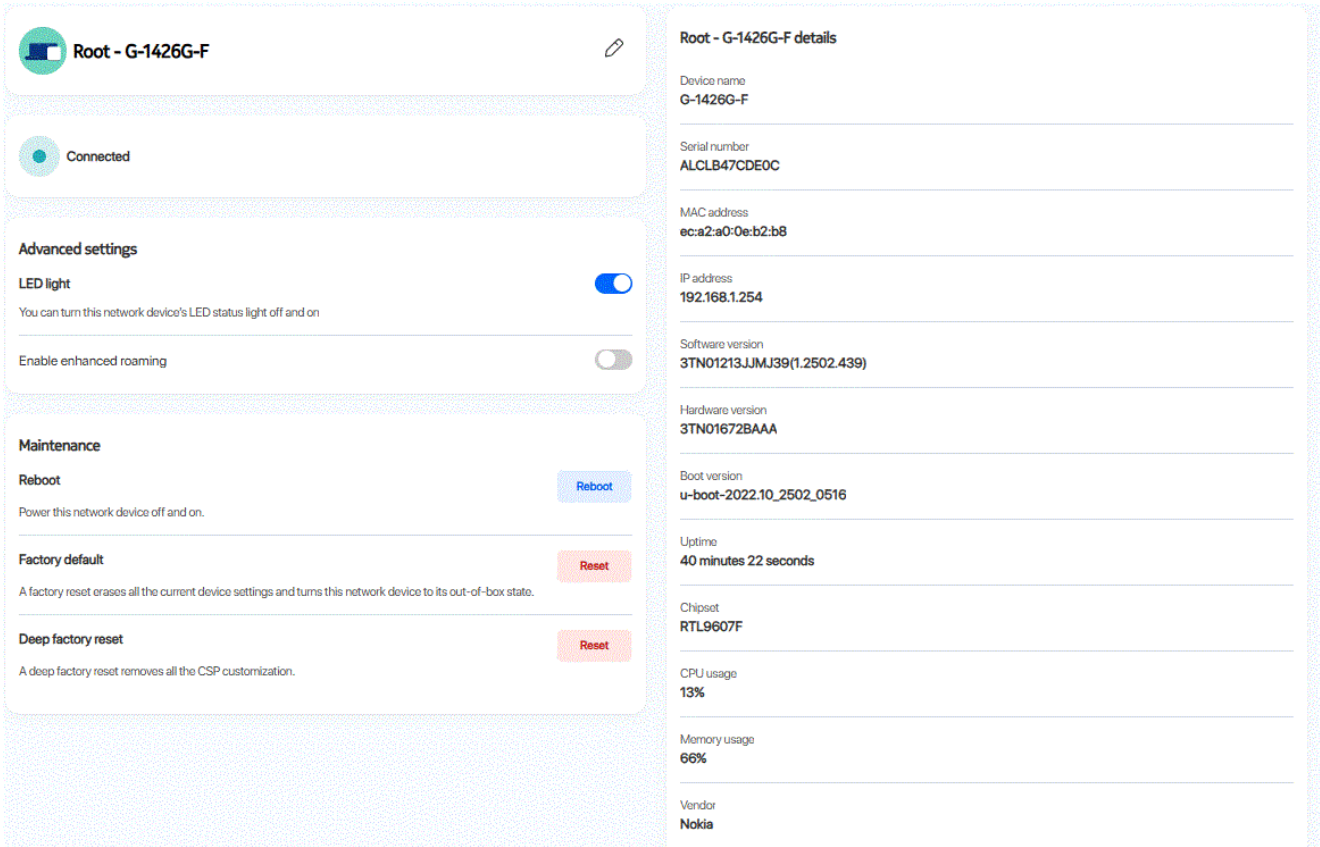
Add

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

3

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

Figure 7-32 <Device> page



4

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

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

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

Figure 7-33 Change the name of your WiFi point page

Change the name of your WiFi point

Pick a name or create your own.

Custom

Custom name

G-1426G-D

Maximum length is 17 characters.

Save

Table 7-20 <Device> parameters

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

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

6 _____
Perform any of the following, as applicable:

- **Reboot the device:**
 1. Click **Reboot**. A message displays asking if you want reboot the device.

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

END OF STEPS

7.27 Optimizing WiFi Network

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

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

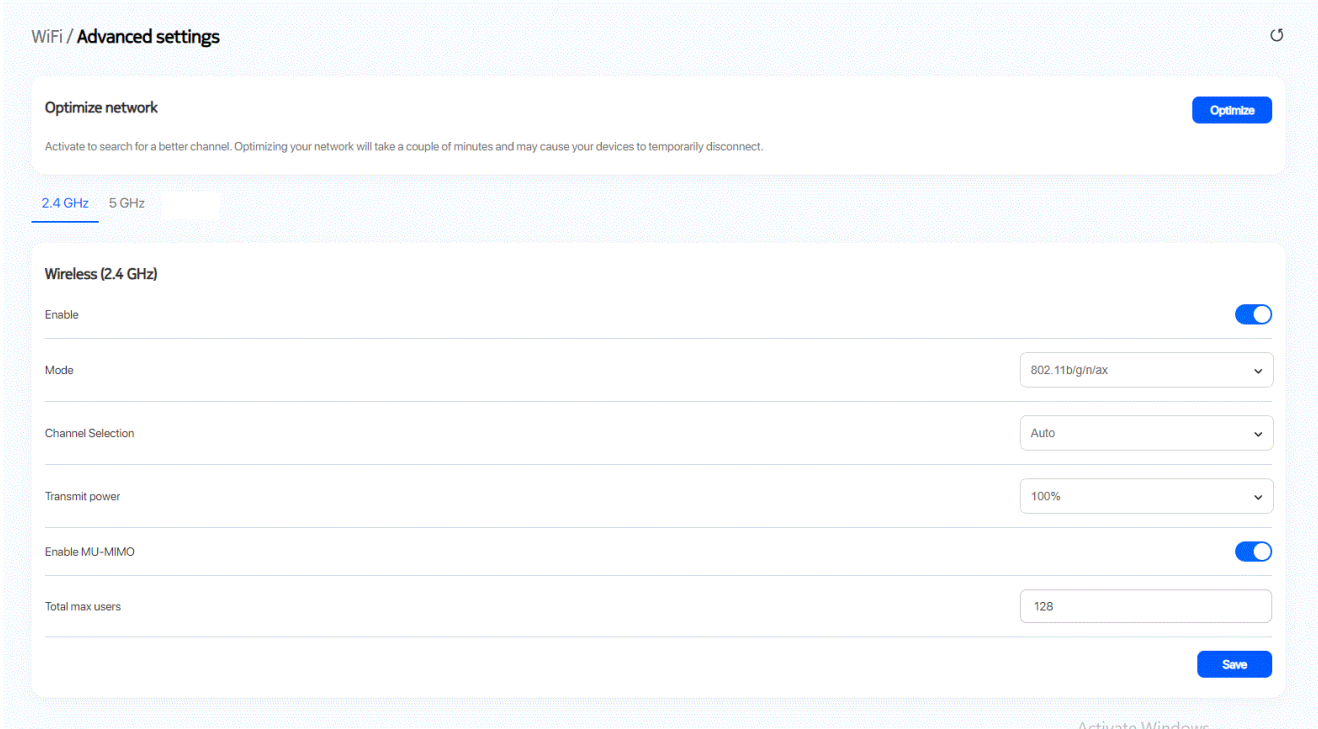
In some cases, the system could possibly run on a more suitable channel, but it does not change the channel to avoid interrupting ongoing client traffic.

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

7.28 Configuring Wireless 2.4 GHz

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

Figure 7-34 Advanced settings - 2.4 GHz tab



3 Configure the following parameters:

Table 7-21 Wireless 2.4 GHz parameters

Field	Description
Enable	Select the toggle button to enable Wireless (2.4 GHz).
Channel Selection	Select a channel from the list: • Auto • Manual Note: When changing from automatic to manual channel management, depending on the channel, channel bandwidth, and region, it can take several minutes for the changes to take into effect and for the wireless network to be functional again. Also, after a reboot, this same delay is observed. It is recommended to set this value to "Auto".
Channel bandwidth	Select the bandwidth range from the list: • 20 MHz • 40 MHz This parameter is visible only if the Channel Selection is Manual .

Table 7-21 Wireless 2.4 GHz parameters (continued)

Field	Description
Channel	Select a channel from the list . This parameter is visible only if the Channel Selection is Manual .
Transmit power	Select a percentage for the transmitting power from the list: • 25% • 50% • 100%
Enable MU-MIMO	Select the toggle button to enable or disable MU-MIMO.

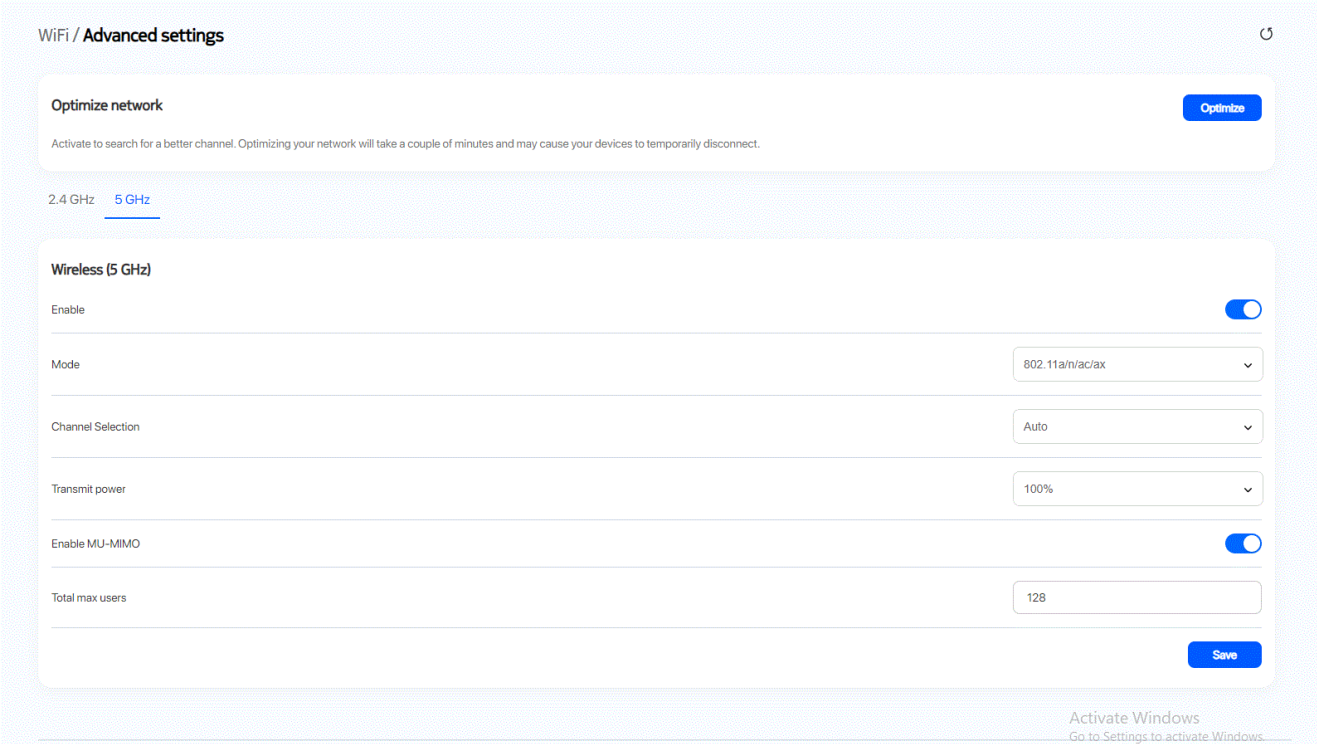
4 _____
Click **Save**.

END OF STEPS _____
For optimizing WiFi network, see [7.27 “Optimizing WiFi Network” \(p. 143\)](#).

7.29 Configuring Wireless 5 GHz

- 1 _____
Click **WiFi→Advanced settings** in the left pane. The *Advanced settings* page displays.
- 2 _____
Select the **5 GHz** tab to configure the wireless 5 GHz parameters.

Figure 7-35 Advanced settings - 5 GHz tab



3

Configure the following parameters:

Table 7-22 Wireless 5 GHz parameters

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

Table 7-22 Wireless 5 GHz parameters (continued)

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

4

Click **Save**.

END OF STEPS

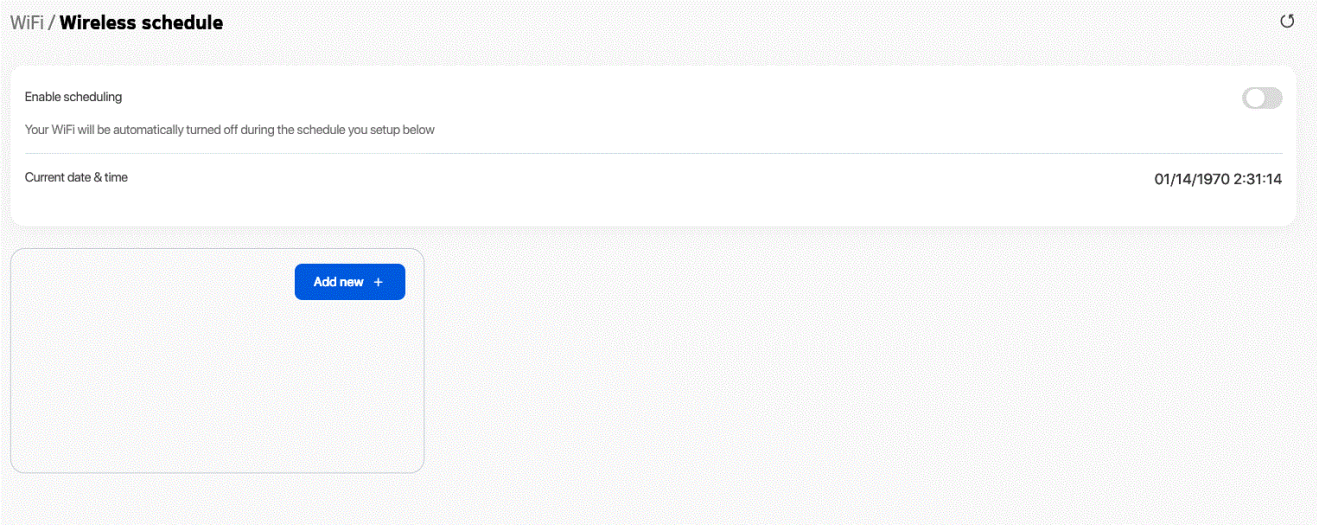
For optimizing the WiFi network, see [7.27 “Optimizing WiFi Network” \(p. 143\)](#).

7.30 Configuring Wireless Schedules

1

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

Figure 7-36 Wireless schedule page



- 2
Select the **Enable Scheduling** toggle button to turn off the wireless signal for the configured period.
- i

Note: The ONT stores the settings of the current wireless signal and restores with the same settings when WiFi is enabled or disabled until the programmed wireless signal rule is triggered. The stored value is restored if the active wireless signal schedule rule is deleted.
- 3
Click **Add new +** to add a scheduling rule.
- 4
Enter a start time and end time for the period during which you want to turn off the wireless signal.
- 5
Select **Everyday** or **Individual Days** from the list.
- 6
If you select **Individual Days**, select the checkboxes for the desired days.
The Recurrence Pattern shows the rules created to date.

7

If required, click **Add new +** to add more rules.

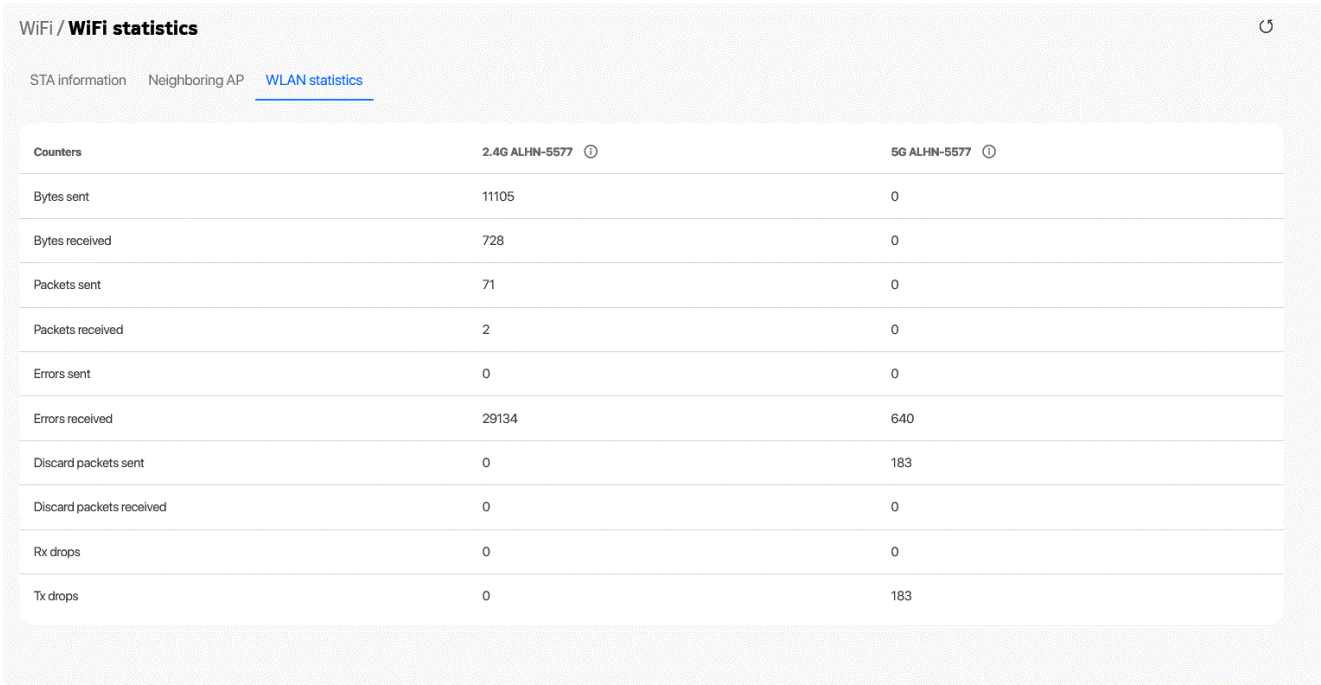
END OF STEPS

7.31 Viewing WiFi Statistics

1

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

Figure 7-37 WiFi statistics page



2

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

Table 7-23 WLAN statistics parameters

Field	Description
Bytes sent	Displays the bytes sent.
Bytes received	Displays the bytes received.
Packets sent	Displays the packets sent.

Table 7-23 WLAN statistics parameters (continued)

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

END OF STEPS

Devices

7.32 Overview

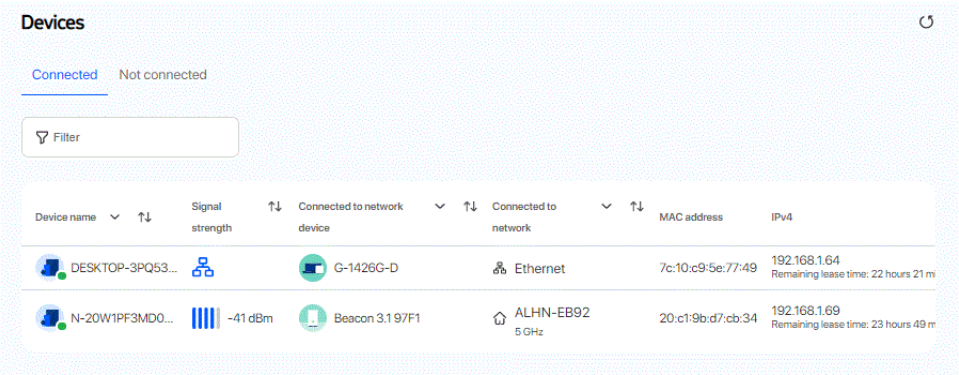
This section describes how to view device information from the **Device** menu.

7.33 Viewing Device Information

1

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

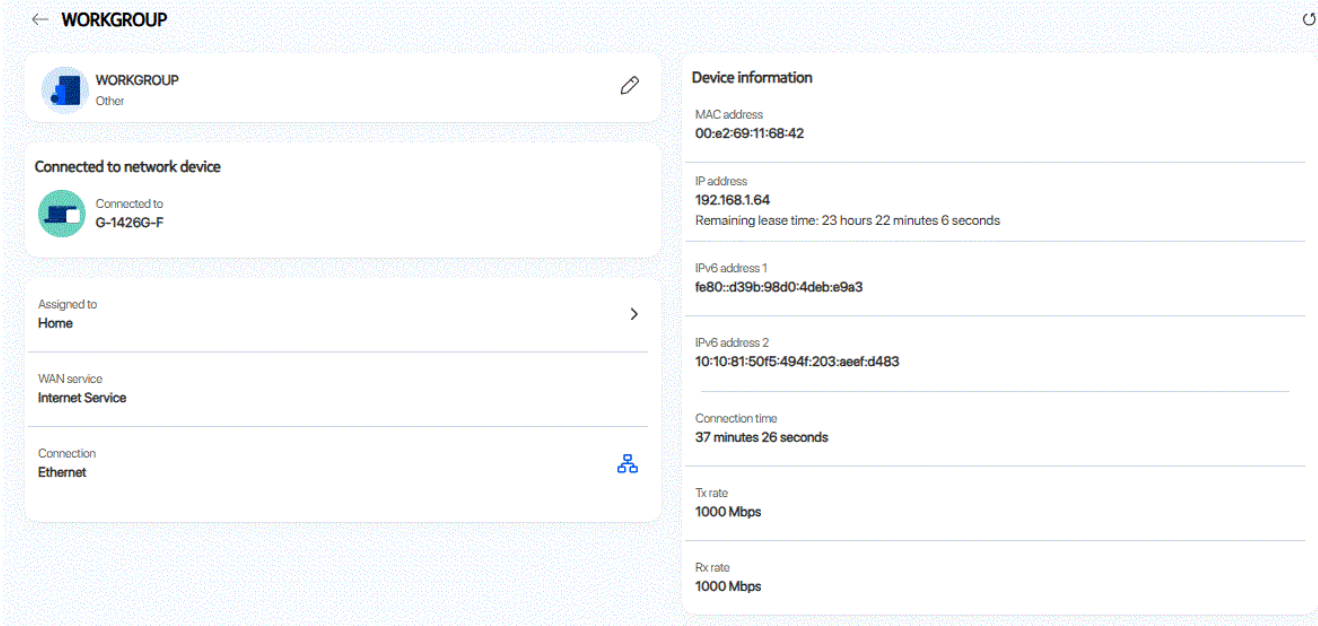
Figure 7-38 *Devices* page



2

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

Figure 7-39 Device information page - L3 devices



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

Perform the following steps to rename the client device:

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

Figure 7-40 Device Rename page

Edit

×

Name

61-30-PC

Category

Other

^

Appliance

Audio

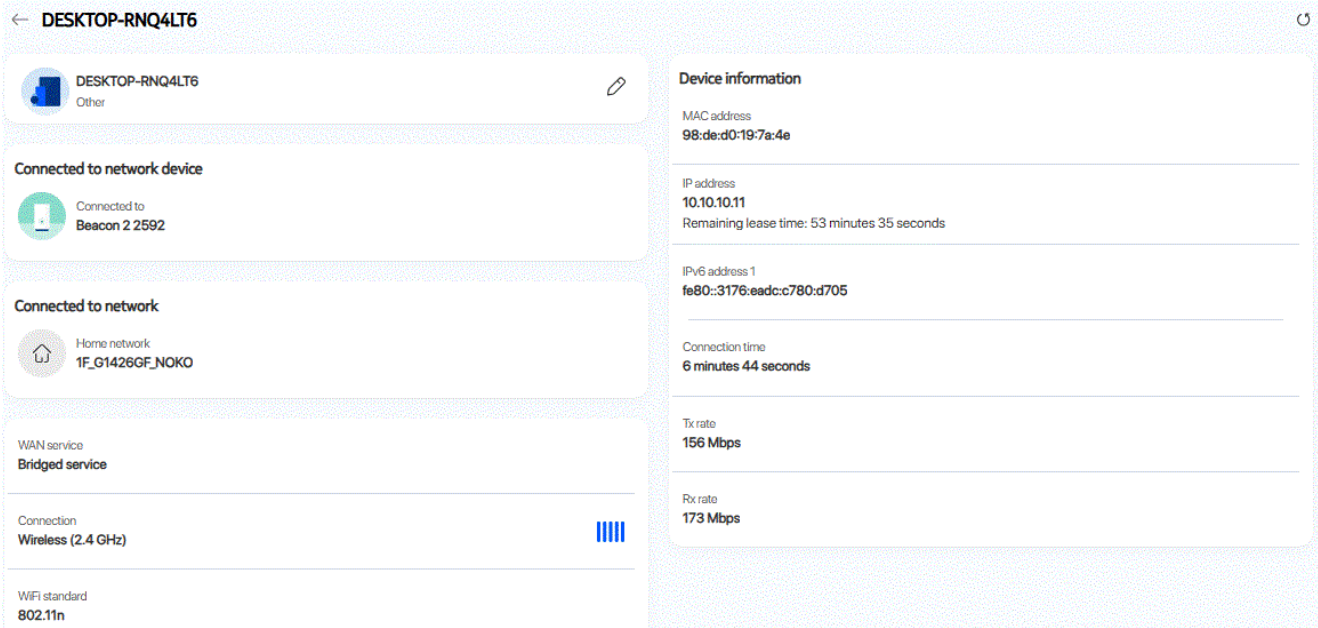
Camera

Game console

Health

Save

Figure 7-41 Device information page - L2 devices



END OF STEPS

Voice Configuration

7.34 Overview

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

Sub-menu	Procedure
Voice setting	7.35 "Configuring Voice Settings" (p. 155)
Voice status	7.36 "Viewing Voice Status" (p. 157)

7.35 Configuring Voice Settings

- 1
- Click **Voice**→**Voice Setting** in the left pane. The *Voice Setting* page displays.

Figure 7-42 Voice Setting page

Voice / **Voice Setting**

Outbound Proxy

Outbound Proxy Port

5060

Proxy Server

Proxy Server Port

5060

Registrar Server

Registrar Server Port

5060

User Agent Domain

User Agent Port

5060

Digit Map

*XX|#[XX|*X#|XXXXXXXXX|(88885010)E|0901XXXXXXXXXX| 09001XXXXXXXXXX|0900X.T|09020|090[3-8][0-3]|0903[4-9]|0904[6-9]|090[5-8][4-9]|09090|0902[1-9]XXXXXXXXXX|0909[1-9]XX.T|XX.T

DTMF Mode

RFC2833

FAXT38

True

POTS line

Line1

Enable

Directory Number

Auth User Name

Auth Password

URI

Save

2

Configure the following parameters:

Table 7-24 Voice Setting parameters

Field	Description
Outbound Proxy	Enter the outbound proxy details.
Outbound Proxy Port	Enter the outbound proxy port.
Proxy Server	Enter the proxy server details.
Proxy Server Port	Enter the proxy server port.
Registrar Server	Enter the registrar server details.
Registrar Server Port	Enter the registrar server port.
User Agent Domain	Enter the user agent domain details.
User Agent Port	Enter the user agent port.
Digit Map	Enter the digit map value.
DTMF Mode	Select a DTMF mode from the list.
FAXT38	Select True or False from the list.
POTS Line	Select a POTS line from the list.
Enable	Select the toggle button to enable.
Directory Number	Enter the directory number.
Auth User Name	Enter the authentication username.
Auth Password	Enter the authentication password.
URI	Enter the URI.

3

Click **Save**.

END OF STEPS

7.36 Viewing Voice Status

1

Click **Voice**→**Voice status** in the left pane. The *Voice status* page displays the following information:

Figure 7-43 Voice status page

Voice / **Voice status**

POTS 1 registration status

POTS 1 line state

Disabled

Softswitch line 1

Telephone line 1 phone number

Line 1 registration error code

Line 1 registration error reason

User agent IP

Table 7-25 Voice status parameters

Field	Description
POTS 1 registration status	Indicates if POTS 1 is registered or not. If POTS 1 is registered, the status displays as Registered. The status is empty if no voice service is provisioned.
POTS 1 line state	Indicates the line in POTS 1. The default is Disabled.
Softswitch line 1	Proxy IP address; blank if the line is not registered.
Telephone line 1 phone number	Phone number configured for a telephone line 1.
Line 1 registration error code	SIP standard error code for the registration status; for example, 401, 403, 503. This field is blank if the registration is OK.
Line 1 registration error reason	SIP standard error reason for the register status. This field is blank if the registration is OK.
User agent IP	IP address of the user agent.

END OF STEPS

Security Configuration

7.37 Overview

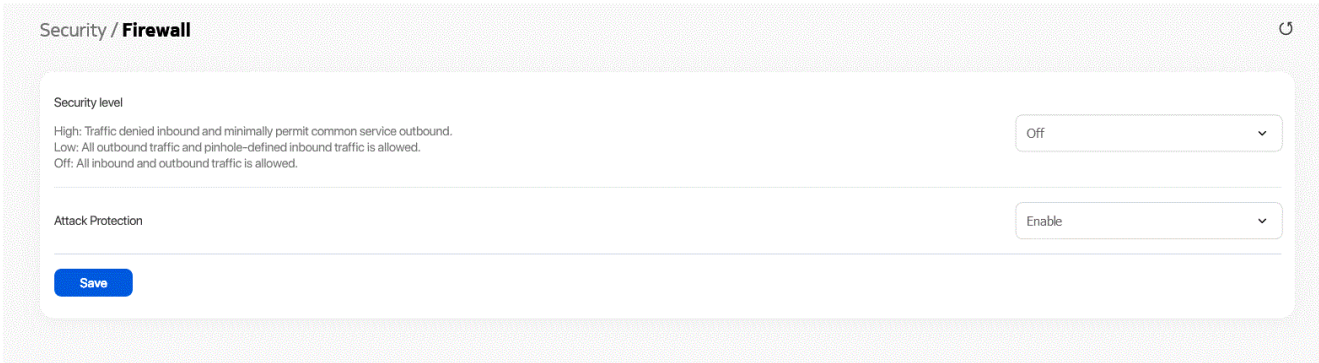
This section describes the security configuration procedures that can be performed from the following sub-menu options under the **Security** menu:

Sub-menu	Procedure
Firewall	7.38 "Configuring the Firewall" (p. 159)
MAC filter	7.39 "Configuring the MAC Filter" (p. 160)
IP filter	7.40 "Configuring the IP Filter" (p. 162)
URL filter	7.41 "Configuring the URL Filter" (p. 164)
Family profiles	7.42 "Configuring Family Profiles" (p. 166)
DMZ and ALG	7.43 "Configuring DMZ and ALG" (p. 172)
Access control	7.44 "Configuring Access Control" (p. 174)

7.38 Configuring the Firewall

- 1
- Click **Security**→**Firewall** in the left pane. The *Firewall* page displays.

Figure 7-44 Firewall page



- 2
- Configure the following parameters.

Table 7-26 Firewall parameters

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

3

Click **Save**.

END OF STEPS

7.39 Configuring the MAC Filter

1

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

Figure 7-45 MAC filter page

Security / **MAC filter**

Ethernet interface

MAC filter mode

Allowed

LAN port

LAN 1

LAN 2

LAN 3

LAN 4

MAC address

Custom Settings

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

Save

WiFi SSID

MAC filter mode

Allowed

SSID select

SSID 1

Enabled

MAC address

Custom Settings

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

Save

2

Configure the following parameters:

Table 7-27 MAC filter - Ethernet Interface parameters

Field	Description
Ethernet Interface	
MAC Filter mode	Select the MAC filter mode from the list: - Blocked - Allowed

Review

August 2025
Issue 1

© 2025 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.
3TN-01672-AAAA-TCZZA

161

Table 7-27 MAC filter - Ethernet Interface parameters (continued)

Field	Description
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 7-28 MAC filter - WiFi SSID parameters

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

5 _____
Click **Save**.

END OF STEPS _____

7.40 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 7-46 IP filter page

← Security / IP filter / Add IPv6 filter

Save

Enable IP filter

Mode

Drop for upstream

Source

Custom Settings

Source IP address

Source prefix

Destination IP address

Destination prefix

Protocol

ALL

3

Configure the following parameters:

Table 7-29 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 • Accept for upstream • Accept 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 ONT
Add IPv4 filter parameters	
Local IP address	Enter the local IP address.
Local subnet mask	Enter the local subnet mask.

Table 7-29 IP filter parameters (continued)

Field	Description
Destination IP address	Enter the destination IP address.
Destination subnet mask	Enter the destination 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 _____

7.41 Configuring the URL Filter

 **Note:** You can add up to 100 URL filters.

1 _____

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

Figure 7-47 URL filter page

Security / URL filter

URL filter

Please select the type of filter and then configure the URL. Support upto 100 URL filters.

Enable URL filter

URL filter type

Block

URL address

Port number

The default port number is 80

Add filter +

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

2 Configure the following parameters:

Table 7-30 URL filter parameters

Field	Description
Enable URL filter	Select the toggle button to enable the URL filter.
URL filter type	Select a URL filter type from the list: - Block - Allow
URL address	Enter the URL address.
Port number	Enter the port number. Default value: 80

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

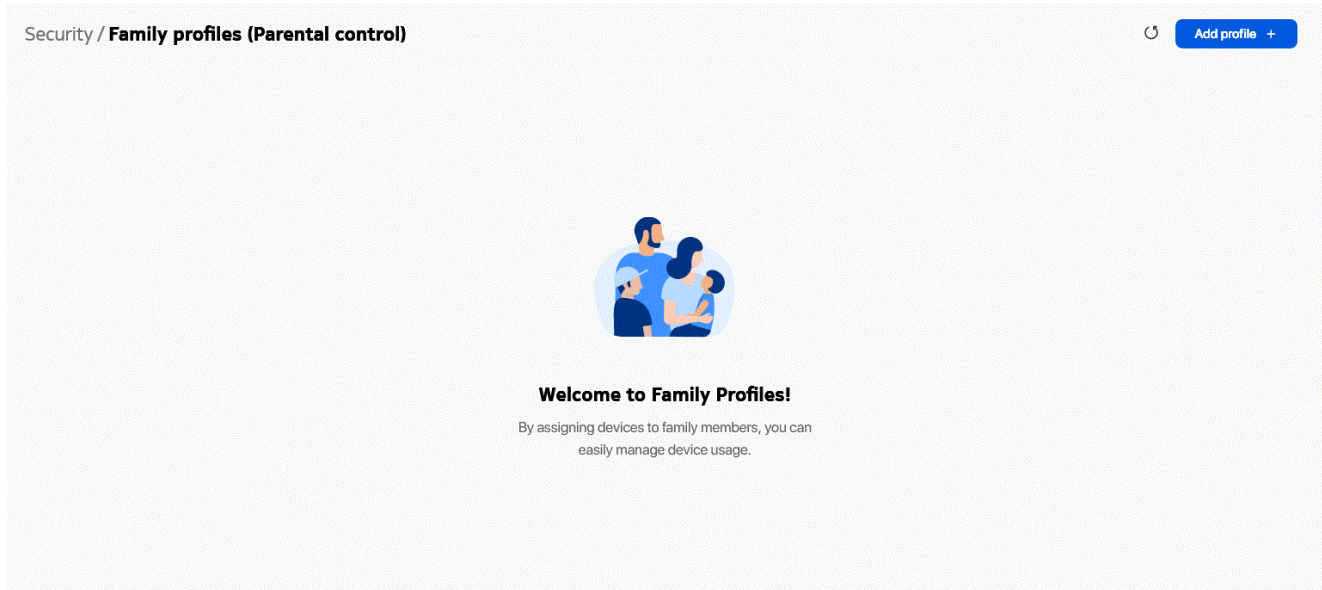
END OF STEPS

7.42 Configuring Family Profiles

1

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

Figure 7-48 Family profiles (Parental control) page



2

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

3

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

Figure 7-49 Add a profile page

Add a profile

×

Name

eg. Alex

Cancel

Add

4

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

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

Figure 7-50 Assign devices to family profile

Select the devices used by this profile

×

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

T

test

DESKTOP-R6N34A7

Cancel

Save

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

August 2025
Issue 1

© 2025 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.
3TN-01672-AAAA-TCZZA

167

Review

Figure 7-51 Family profiles table

Security / Family profiles (Parental control) ↻ Add profile +

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

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

Figure 7-52 Family profile configuration page

Security / Family profiles (Parental control) ↻

 test
Enabled

Assigned Devices
1 Device ✎

Internet Access
Enabled for this profile 🔴

Schedules
None ✎

Bedtime
None ✎

Website blocking
Disabled ✎

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

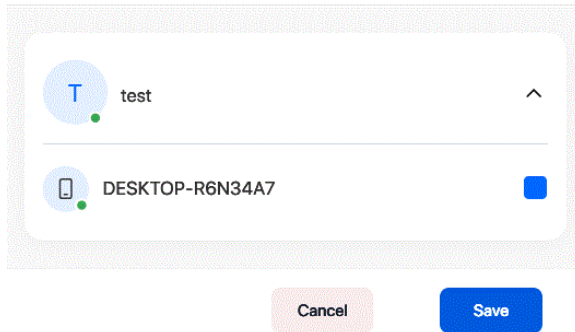
Assign more devices

7

Assign more devices to the profile, if required:

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

Select the devices used by this profile ×
A device can only belong to one profile. Unassigned devices will be added to the "Home" profile.



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

Configure and enable schedules

8

Configure schedules for the profile:

- 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.
- Click **Create Schedule**.
- In the *Add a schedule* page, configure the following:

Add a schedule

×

Name

e.g. Dinner, Chores, Homework

Start time

14

:

12

End time

15

:

12

Days of the week

M

TU

W

TH

F

SA

SU

Cancel

Save

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

Add +

Done

Configure and enable bedtime

10

Configure bedtime for the profile:

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

Add a bedtime ×

Bedtime

:

Wake Up

:

Days of the week

☐ M ☐ TU ☐ W ☐ TH ☐ F ☐ SA ☐ SU

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

Configure website blocking

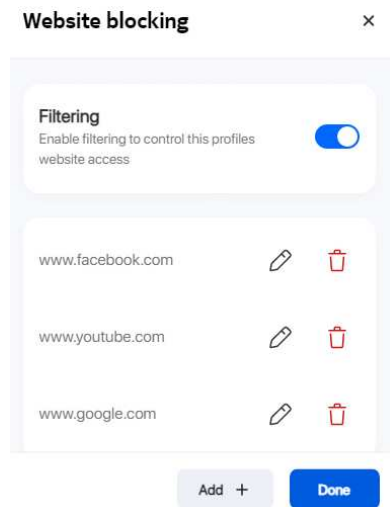
11

Configure website blocking for the profile:

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

b. Click **Continue**.

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



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

END OF STEPS

7.43 Configuring DMZ and ALG

1

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

Figure 7-53 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_VOIP_R_VID_881

Enable DMZ

DMZ IP address

Custom Settings

0.0.0.0

Save

2

Configure the following parameters:

Table 7-31 ALG Configuration parameters

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

3

Click **Save**.

4

Configure the following parameters:

Table 7-32 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

7.44 Configuring Access Control

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



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

1

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

Figure 7-54 Access control page

Security / Access control

WAN connection list

1_VOIP_TR069_INTERNET_R_VID_881

Enable trusted network

Protocol

Caution: Disabling both HTTP and HTTPS on LAN may lock you out from accessing the web GUI and mobile application. Ensure at least one protocol is enabled to maintain access. HTTPS is recommended for secure communication.

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

Save

Trusted network

Source IP start

© 2021 Nokia

Recommended browsers

Add +

2

Configure the following parameters:

Table 7-33 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 Note: If you allow SSH/Telnet/HTTP/HTTPS on WAN, a security warning is displayed. Click OK to continue.
LAN	The following protocols are supported: ICMP, Telnet, SSH, HTTP, TR-069, HTTPS, SFTP. Select an access control level for each protocol: LAN side: Allow or Deny Notes: - If you allow Telnet or HTTP on LAN, a security warning is displayed. Click OK to continue. - If you Deny HTTP and HTTPS on LAN at same time, the following warning message is displayed, 'Disabling both HTTP and HTTPS on LAN may lock you out from accessing the web GUI and mobile application. Atleast one of them should be enabled.' Click OK to continue.

3

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

4

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

Table 7-34 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

7.45 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	7.46 "Configuring Port Forwarding" (p. 177)
Port triggering	7.47 "Configuring Port Triggering" (p. 178)
DDNS	7.48 "Configuring DDNS" (p. 179)
NTP	7.49 "Configuring NTP" (p. 180)
USB	7.50 "Configuring USB" (p. 182)
UPNP and DLNA	7.51 "Configuring UPNP and DLNA" (p. 183)

7.46 Configuring Port Forwarding

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

Figure 7-55 Port forwarding page

Advanced settings / **Port forwarding**

Save

WAN port

 -

LAN port

 -

Internal client

Custom Settings

Protocol

TCP

WAN connection list

2_INTERNET_R_VID_2101

- 2
- Configure the following parameters:

Table 7-35 Port forwarding parameters

Field	Description
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

7.47 Configuring Port Triggering

1

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

Figure 7-56 Port triggering page

Advanced settings / **Port triggering**

Save

Open port

 -

Triggering port

 -

Expiration time

Range: 1-999999 secs

600

Open protocol

TCP

Trigger protocol

TCP

WAN connection list

2_INTERNET_R_VID_2101

2

Configure the following parameters:

Table 7-36 Port triggering parameters

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

3

Click **Save**.

END OF STEPS

7.48 Configuring DDNS

1

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

Figure 7-57 DDNS page

Advanced settings / **DDNS**

WAN connection list

1_TR069_INTERNET_VOIP_R_VID_881

Enable DDNS

ISP

DynDNS.org

Domain Name

Username

Password

Save

2

Configure the following parameters:

Table 7-37 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

7.49 Configuring NTP

1

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

Figure 7-58 NTP page

Advanced settings / **NTP**

Enable NTP service

01/14/1970 03:08:55 AM

Current date & time

Primary Time Server

Secondary Time Server

Third time server

Interval time

0,15-259200 secs

Time zone

Custom Settings

None

None

0

(GMT-00:00) Casablanca, Monrovia

Save

2

Configure the following parameters:

Table 7-38 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

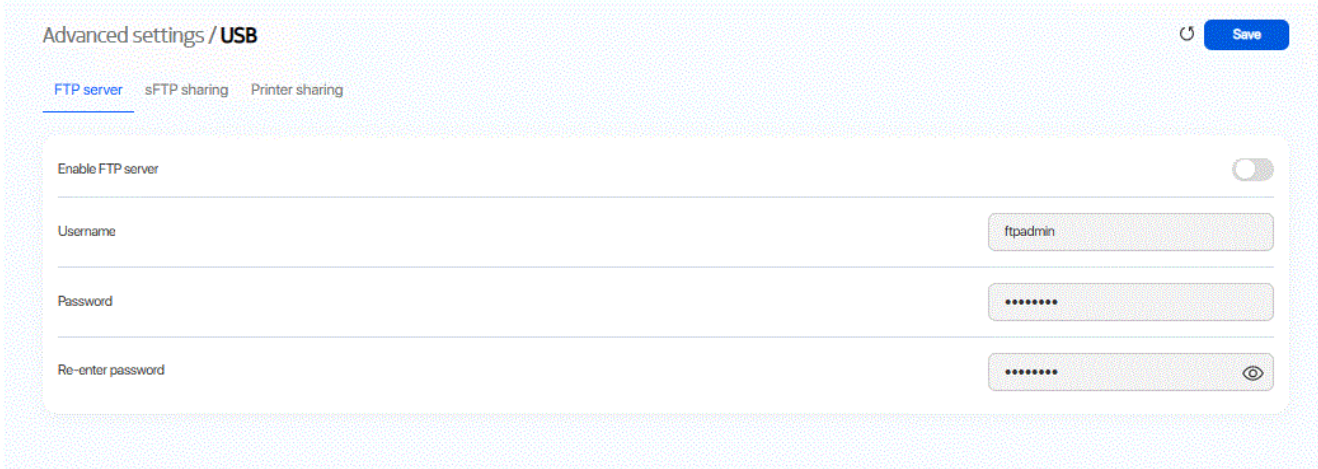
7.50 Configuring USB

You can connect USB storage devices and USB printers to the USB ports of the device. The USB menu enables you to configure FTP and SFTP for your USB storage devices.

The USB connected devices are shown in a table at the bottom of the *USB* page.

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

Figure 7-59 USB page



- 2
- Configure the following parameters:

Table 7-39 USB parameters

Field	Description
FTP server parameters	
Enable FTP server	Select the toggle button to enable an FTP server. By default, FTP server is disabled.
Username	Enter the username of the FTP server.
Password	Enter the password of the FTP server.
Re-enter password	Re-enter the password of the FTP server.
sFTP sharing parameters	
Enable SFTP Server	Select the toggle button to enable an SFTP server. By default, SFTP server is disabled.
Enable SFTP for Remote Access	Select the toggle button to enable SFTP for remote access. By default, SFTP is disabled.

Table 7-39 USB parameters (continued)

Field	Description
Username	Enter the username of the SFTP server.
Password	Enter the password of the SFTP server.
Re-enter password	Re-enter the password of the SFTP server.
Printer sharing parameters	
Enable printer sharing	Select the toggle button to enable printer sharing. By default, printer sharing is disabled.
Username	Enter the username of the printer.
Password	Enter the password of the printer.
Re-enter password	Re-enter the password of the printer.

3

Click **Save**.

A table displays the following information for each server or printer that is connected to the device through a USB port:

- Host Number: For example, Printer1, Printer2
- Device Name: Name or identifier of the device
- Format: Storage format (applies only to a USB storage device)
- Total space (applies only to a USB storage device)
- Free space (applies only to a USB storage device)

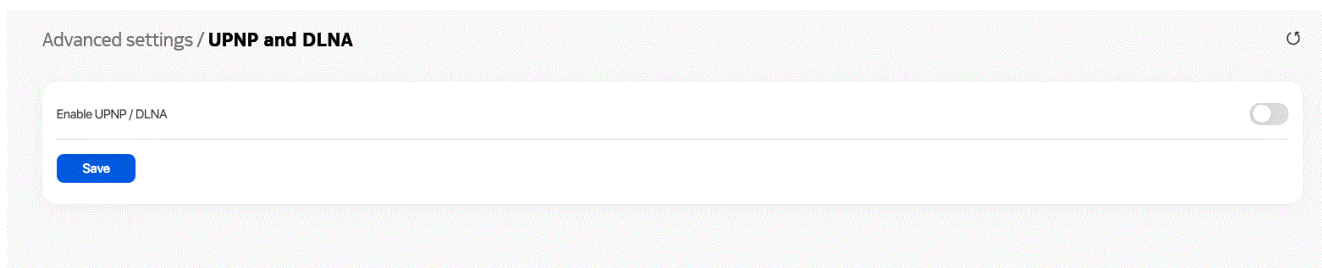
END OF STEPS

7.51 Configuring UPNP and DLNA

1

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

Figure 7-60 UPNP and DLNA page



2

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

3

Click **Save**.

END OF STEPS

Maintenance

7.52 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	7.53 "Configuring the Password" (p. 185)
Backup and restore	7.54 "Backing Up the Configuration" (p. 187) 7.55 "Restoring the Configuration" (p. 187)
Firmware upgrade	7.56 "Upgrading Firmware" (p. 189)
LOID config	7.57 "Configuring LOID" (p. 190)
SLID configuration	7.58 "Configuring SLID" (p. 191)
Diagnostics	7.59 "Diagnosing WAN Connections" (p. 192)
Log	7.60 "Viewing Log Files" (p. 197)
Delta CFG tool	7.61 "Generating a delta configuration file" (p. 198)

7.53 Configuring the Password

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

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

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

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

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

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

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

- Password should be at most 24 characters
- The same character cannot appear consecutively 8 times

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

Figure 7-61 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 7-40 Change password parameters

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

3 Click **Save**.

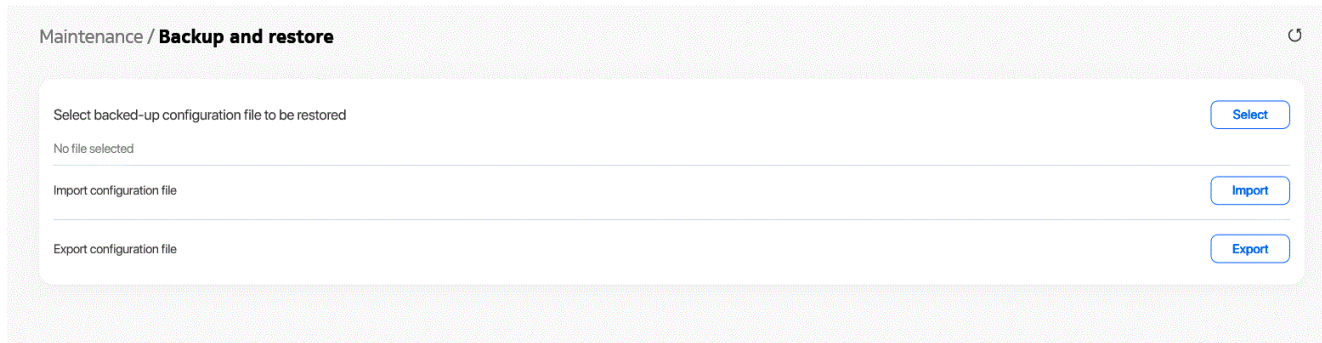
END OF STEPS

7.54 Backing Up the Configuration

1

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

Figure 7-62 Backup and restore page



2

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

END OF STEPS

7.55 Restoring the Configuration

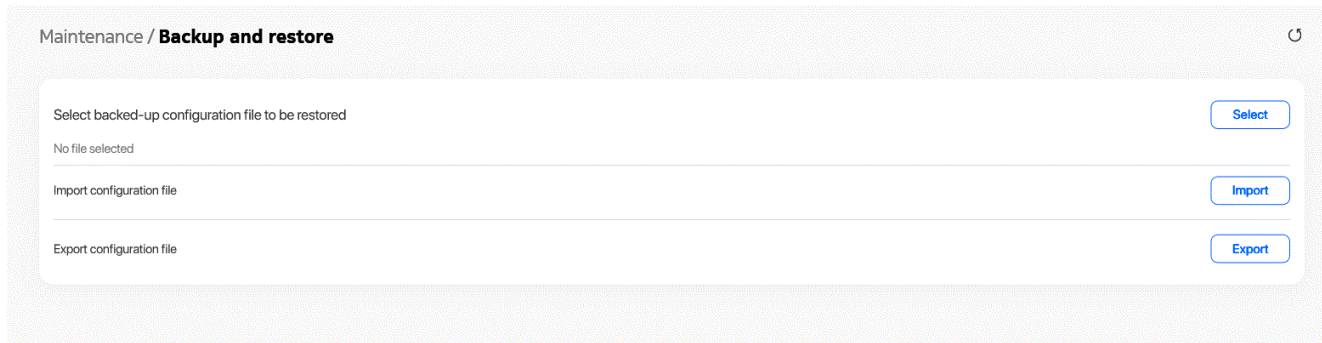


Note: Ensure that you have a previously backed-up configuration file.

1

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

Figure 7-63 Backup and restore page



2

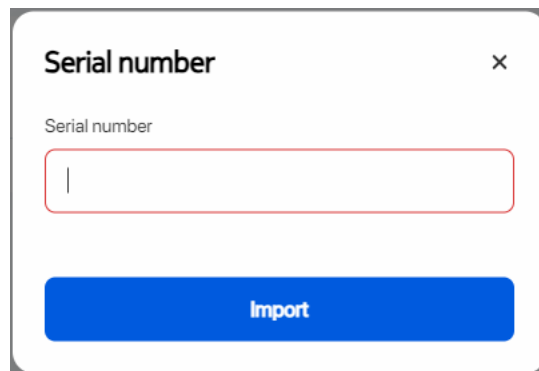
Click **Select** and select the previously backed-up configuration file.

3

Click **Import** to import the configuration file created in [7.54 “Backing Up the Configuration” \(p. 187\)](#) and restore the ONT to the backed-up configuration.

- a. If the configuration file is from the same ONT variant with a different serial number, you will be prompted to enter the serial number of the original device.

Figure 7-64 Backup and restore: Serial number



- b. If you enter an invalid serial number, the back up fails and an error message is displayed.
- c. The backup cannot be restored for the configuration files from a different ONT variant, OPID, or different release prior to Release 2402.

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

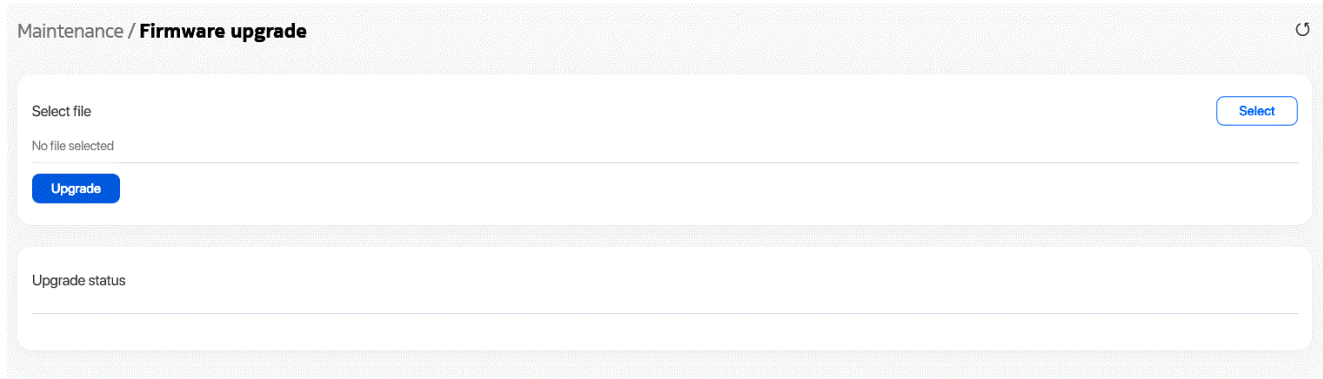
END OF STEPS

7.56 Upgrading Firmware

1

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

Figure 7-65 Firmware upgrade page



2

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

3

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

Figure 7-66 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

7.57 Configuring LOID

- 1
- Click **Maintenance**→**LOID config** in the left pane. The *LOID config* page displays.

Figure 7-67 LOID config page

Maintenance / **LOID config**

LOID authentication

Please enter the LOID (length < 25 characters) and password (length < 13 characters). If the password is null, leave the password field blank

LOID

Password

Save

- 2
- Configure the following parameters:

Table 7-41 LOID config parameters

Field	Description
LOID authentication	
LOID	Enter the LOID. Maximum number of characters: 24
Password	Enter the password. If the password is null, leave this field blank. Maximum number of characters: 12

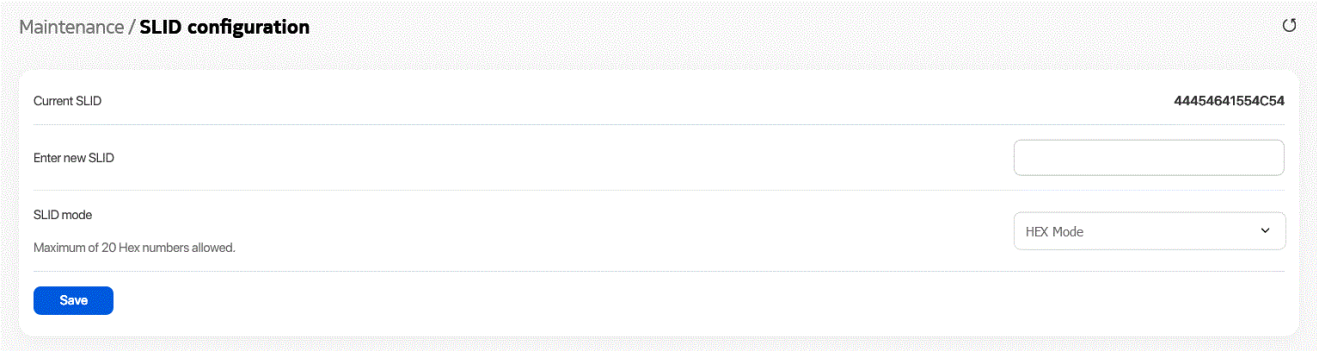
- 3
- Click **Save**.

END OF STEPS

7.58 Configuring SLID

- 1
- Click **Maintenance**→**SLID configuration** in the left pane. The *SLID configuration* page displays.

Figure 7-68 SLID configuration page



- 2
- Configure the following parameters:

Table 7-42 SLID configuration parameters

Field	Description
Current SLID	Displays the current SLID.
Enter new SLID	Enter the new SLID.
SLID mode	Select a SLID mode from the list. The default is HEX Mode. • ASCII Mode • HEX Mode In ASCII Mode, the allowed characters are 0-9, a-z and the maximum number of characters is 10. Special character is not allowed. In HEX Mode, the allowed characters are 0-9, a-f, A-F and the maximum number of characters is 20. Special character is not allowed.

3

Click **Save**.

END OF STEPS

7.59 Diagnosing WAN Connections

1

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

Figure 7-69 Diagnostics page

Maintenance / **Diagnostics**

WAN

Protocol

IPv4

WAN connect list

LAN/WAN Interface

IP or domain name

Ping

Traceroute

Ping try times

4

1-1000

Packet length

64

64-1500

Max number of trace hops

30

1-255

Start test

Cancel

2

Configure the following parameters.

Table 7-43 Diagnostics parameters

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

Table 7-43 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 7-70 Example of ping results

Maintenance / **Diagnostics**

WAN

Protocol

IPv4

WAN connect list

1_VOIP_TR069_INTERNET_R_VID_1102

IP or domain name

11.18.92.254

Ping

Traceroute

Ping try times

4

1-1000

Packet length

64

64-1500

Max number of trace hops

30

1-255

Start test

Cancel

Please wait! Ping is in progress...

PING 11.18.92.254 (11.18.92.254) from 11.18.92.115: 64 data bytes

72 bytes from 11.18.92.254: seq=0 ttl=64 time=1.117 ms

72 bytes from 11.18.92.254: seq=1 ttl=64 time=1.092 ms

72 bytes from 11.18.92.254: seq=2 ttl=64 time=1.039 ms

72 bytes from 11.18.92.254: seq=3 ttl=64 time=1.069 ms

11.18.92.254 ping statistics ---

Maintenance / **Diagnostics**

WAN

ProtocolIPv4

WAN connect list1_VOIP_TR069_INTERNET_R_VID_1102

IP or domain name11.18.92.254

Ping

Traceroute

Ping try times4

Packet length64

Max number of trace hops30

Start test

Cancel

tracert to 11.18.92.254 (11.18.92.254) from 11.18.92.115, 30 hops max, 64 byte packets

1 11.18.92.254 0.910 ms 0.551 ms 0.601 ms

tracert job completed!!

© 2021 Nokia

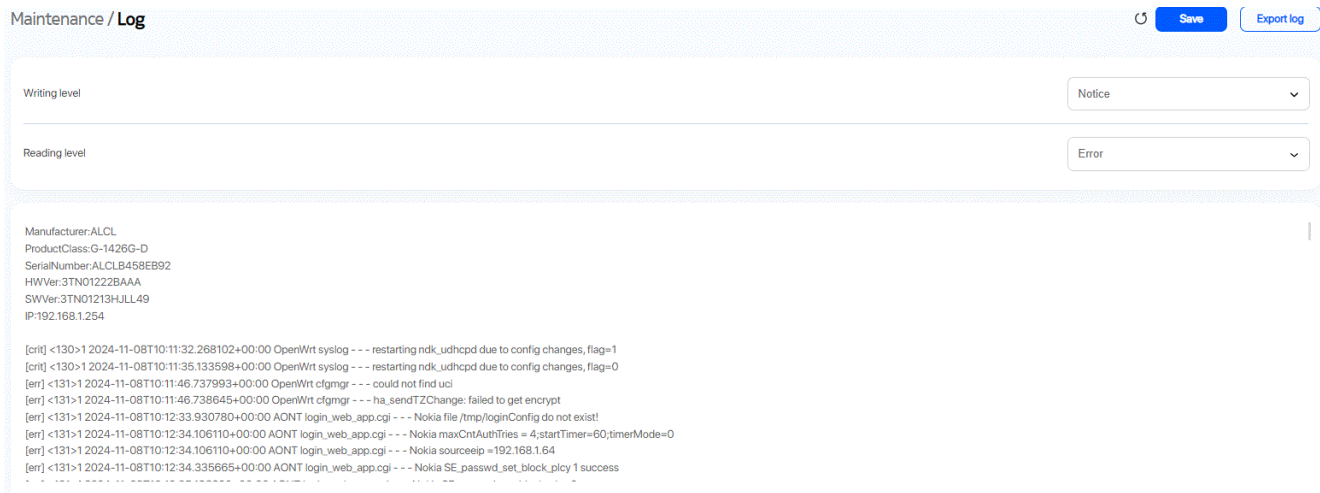
Recommended browser

END OF STEPS

7.60 Viewing Log Files

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

Figure 7-72 Log page



- 2
- Configure the following parameters:

Table 7-44 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

Table 7-44 Log parameters (continued)

Field	Description
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

7.61 Generating a delta configuration file

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

1

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

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

Figure 7-73 Delta CFG Tool page

Maintenance / **Delta CFG tool**

Please double confirm if you are trying to modify the parameters in Delta CFG below, such as the WIFI SSID name or password. These are usually controlled by the end user, so changing these parameters may impact their usage.

Merge Delta CFG file

This will include the content of the Delta CFG file you select to the new one.
Pay attention to the dynamic objects when using this option.

No file selected **Select file** **Start recording**

Export Delta CFG file **Export**

2

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

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

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

3

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

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

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

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

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



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

END OF STEPS

Troubleshooting

7.62 Troubleshooting counters

The Troubleshooting counters feature enables service providers and end users to monitor the performance of their broadband connection for about 10 seconds from the time the test is triggered.

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

1

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

Figure 7-74 Troubleshooting counters page

Troubleshooting / Troubleshooting counters

WAN connection list

1_TR069_INTERNET_VOIP_R_VID_881

WAN status

Down

Troubleshoot counters

US throughput snapshot

Take snapshot

DS throughput snapshot

Take snapshot

US packet loss

0

DS packet loss

0

Latency

Latency test

DNS response time

DNS response test

Port mirrors

Source Port

WAN

Destination Port

LAN1

Direction

Downstream

Status

Enable

Save

2

Configure the following parameters:

Table 7-45 Troubleshooting counters parameters

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

3

Click **Save**.

END OF STEPS

7.63 Speed Test

1

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

Figure 7-75 Speed test page

Results

Upload speed

-

Download speed

-

Latency

0

Start test

Table 7-46 Speed test parameters

Field	Description
TR-143 server settings	
Upload test server URL	Enter the Upload test server URL.
Number of upload connections	Enter the Number of upload connections.
Download test server URL	Enter the Download test server URL.
Number of download connections	Enter the Number of download connections.
Host	Enter Host.
Test mode	Select a Test mode: • Time based • File based
Upload file size	Displays the file size in MB. This parameter is visible only if the Test mode is File Based .
Duration	Displays the time duration is sec. This parameter is visible only if the Test mode is Time Based .
Results	
Upload speed	Displays the upload speed.
Download speed	Displays the download speed.
Latency	Displays the latency.

2

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

3

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

END OF STEPS

8 ONT configuration file over OMCI

8.1 Overview

8.1.1 Purpose

8.1.2 Contents

8.1 Overview	205
8.2 Purpose	205
8.3 Supported configuration file types	205
8.4 ONT configuration file over OMCI	208

8.2 Purpose

This procedure describes how to use configuration files over OMCI to configure ONTs. Some advantages include:

- Flexibility to change the ONT default behavior by downloading configuration file
- Flexibility to update a deployed ONT by downloading updated parameters
- Ability to securely download any configuration file to an ONT
- Ability to avoid using embedded configuration files in ONT software

 **Note:** This feature is supported for use with the 7360 ISAM FX and the 7342 ISAM FTTU.

8.3 Supported configuration file types

Table 8-1, “Supported configuration files” (p. 206) describes the configuration file types that are supported from Nokia ONT R05.02.00 and later.

Table 8-1 Supported configuration files

File Index	Description	Details	Supported ONTs/DPU
PRE	ONT pre-configuration file	The XML-based PRECONFIG file controls the working mechanics of the ONT for various services. The default behavior of different ONTs may vary based on the factory settings. The pre-configuration file includes the factory default value for the residential gateway. Note: The pre-configuration file does not work with SFU ONTs; therefore, this feature applies only to Residential Gateway ONTs. The pre-configuration file can be used as is, but Nokia provides its customers with the flexibility to customize the pre-configuration file. This pre-configuration file enables operators to change the default behavior by downloading a customized pre-configuration based on customer inputs. This PRE XML file includes a custom OPERID. The Nokia defined index for the PRECONFIG file is: "PRE"	All Nokia GPON and 10 GPON ONT.
CFG	ONT configuration delta file	The XML-based CFG file updates the configurable parameters (the PRE settings) in the existing PRE file of a deployed ONT, where required. This configuration file enables operators to change the deployed behavior by downloading customized updates in the CFG file. This file is used only to modify the parameters in the PRE file; it is not used for service provisioning. No OPERID is required, because the update is based on the OPERID used for the PRE file. The Nokia defined index for the PRECONFIG DELTA file is: "CFG"	All Nokia GPON and 10GPON ONT.
XML	Voice XML file	The Voice XML file provides an alternate method for securely downloading voice parameters from the OLT, rather than using FTP (OMCIv1/OMCIv2) or HTTPS (TR-069). Downloading this file makes the applicable changes in the voice parameters. This file enables operators to change the voice behavior by downloading the updated voice XML file. Nokia recommends using this procedure, rather than embedded voice XML files. The Nokia defined index for the Voice XML file is: "XML"	All Nokia GPON and 10 GPON ONT.

Table 8-1 Supported configuration files (continued)

File Index	Description	Details	Supported ONTs/DPU
GFT	G.fast-related configuration file	This text-based json script file controls the default behavior of the G.Fast ONT. This file includes the provisioning parameters of the G.fast transports layer; it does not include VLAN or QoS provisioning. While the ONT functions well with the default values; they can optionally be customized. While default values can work in VDSL mode, a download file is required for the device to function as a G.fast ONT. The Nokia defined index for the G.fast file is: "GFT"	Nokia G.fast.

8.3.1 Filename conventions

Nokia provides the raw configuration files, which must be saved by the operator in a TAR file to be uploaded. TAR file names must be unique.

The filenames of the raw configuration files may not adhere to the naming conventions outlined below. In this case, the files must be renamed to adhere to the naming conventions before the operator generates the TAR file. Filenames are not case-sensitive.

ABCXXXVER

where

ABC is the file index type (PRE, CFG, XML, GFT)

XXXX is the operator ID

For PRE and CFG, a valid operator ID is required

For XML and GFT, any characters may be used

VER is the file version (from 001 to 999)

i **Note:** You cannot update the configuration using two files with the same name.

8.3.2 Download configuration file

The following table provides the supported download options for ONT pre-configuration file and configuration file.

Table 8-2 Download configuration files

ONT type	Legacy method download		Zero management download	
	PRE file	CFG file	PRE file	CFG file
Broadlight(eg.I240WA-3FE54869AFGA80)	—	✓	—	✓
Broadcom(eg.G240WB-3FE56773BFGA07)	—	✓	✓	✓

Table 8-2 Download configuration files (continued)

ONT type	Legacy method download		Zero management download	
	PRE file	CFG file	PRE file	CFG file
MTK(eg.G240WF)	—	✓	✓	✓

8.4 ONT configuration file over OMCI



WARNING

Equipment Damage

Executing the following procedure will trigger the ONT to reboot, which will impact ongoing services.

Use this procedures to configure ONTs using configuration files via legacy method and OMCI.

8.4.1 Configuring an ONT using a configuration file via legacy method

1

Upload the ABCXXXXXVER TAR file to the /ONT/ directory in the OLT.
A maximum of 250 files can be kept in the OLT file system.

2

Using OLT commands, download the TAR file to the ONT.

For OLT commands, refer to the *7360 ISAM FX CLI Command Guide for 100_320Gbps FD NT and FX NT*, or the **7342 ISAM FTTU Operation and Maintenance Using TL1 and CLI**.

Please note:

- **pri-cfgfile-pland/dnload** or **sec-cfgfile-pland/dnload** can be 1 to 14 characters.
- **pri-cfgfile-pland** and **pri-cfgfile-dnload** should be the same name.

Examples



Note: X can be 1 or 2 unless specified:

- If **pland-cfgfileX= Disabled** and **dnload-cfgfileX= Disabled**,
no file is downloaded to the ONT.
- If **pland-cfgfileX=FILENAME1** and **dnload-cfgfileX= Disabled**,
FILENAME1 is downloaded and FILENAME1 is made active. An ONT reboot is required.
- If **pland-cfgfileX=Disabled** and **dnload-cfgfileX= FILENAME2**,
FILENAME2 is downloaded and FILENAME2 is made passive. An ONT reboot is not required.
- If **pland-cfgfileX=FILENAME3** and **dnload-cfgfileX= FILENAME4**, the OLT reports an error because the filenames are not the same.

- e. Configure equipment interface **pland-cfgfile1=XMLXXXXXX1** and **dnload-cfgfile1 XMLXXXXXX1**

Configure equipment interface **pland-cfgfile2=XMLXXXXXX2** and **dnload-cfgfile2 XMLXXXXXX2**

Although the OLT permits the above two steps without reporting an error, Nokia does not recommend executing them, because the ONT may exhibit unexpected behavior.

- f. If **pland-cfgfileX=Auto** and **dnload-cfgfileX= Auto**

The OLT will download the XML file from "sw-ctrl-list" (**configure equipment ont sw-ctrl**)

END OF STEPS

The ONT will distribute the configuration files to the different services based on the active indication from the OLT and on the Nokia defined index.

The ONT automatically reboots to apply the configuration files. After the ONT reboots and reports the active version, the OLT completes the file download procedure.

Operators must check the committed file from the OLT to verify whether the corresponding file has been applied. If an error occurs, contact Nokia for support.

8.4.2 Configuring an ONT using a configuration file via OMCI

1

Generate the TAR file to be uploaded to the OLT.

Using the raw configuration file(s) provided by Nokia, generate the TAR file as follows:

- a. On a Linux platform, rename the raw configuration file to adhere to the naming convention, as described in section [8.3 "Supported configuration file types" \(p. 205\)](#).
- b. Tar the **ABCXXXXXVER** raw configuration file:

```
tar -cf ABCXXXXXVER.tar ABCXXXXXVER
```

Where

ABCXXXXXVER

Is the name of the file created in step i.

This creates two files: **ABCXXXXXVER** and **ABCXXXXXVER.tar**.

- c. Rename **ABCXXXXXVER** to **ABCXXXXXVER.org**
- d. Remove the ".tar" extension from **ABCXXXXXVER.tar** file.

2

Upload the ABCXXXXXVER TAR file to the /ONT/ directory in the OLT.

A maximum of 250 files can be kept in the OLT file system.

3

Using OLT commands, download the TAR file to the ONT.

For OLT commands, refer to the *7360 ISAM FX CLI Command Guide for 100_320Gbps FD NT*

and FX NT, or the **7342 ISAM FTTU Operation and Maintenance Using TL1 and CLI**.

Please note:

- **pri-cfgfile-pland/dnload** or **sec-cfgfile-pland/dnload** can be 1 to 14 characters.
- **pri-cfgfile-pland** and **pri-cfgfile-dnload** should be the same name.

Examples

 **Note:** Note: X can be 1 or 2 unless specified:

- If **pland-cfgfileX= Disabled** and **dnload-cfgfileX= Disabled**
no file is downloaded to the ONT.
- If **pland-cfgfileX=FILENAME1** and **dnload-cfgfileX= Disabled**
FILENAME1 is downloaded and FILENAME1 is made active. An ONT reboot is required.
- If **pland-cfgfileX=Disabled** and **dnload-cfgfileX= FILENAME2**
FILENAME2 is downloaded and FILENAME2 is made passive. An ONT reboot is not required.
- If **pland-cfgfileX=FILENAME3** and **dnload-cfgfileX= FILENAME4**, the OLT reports an error because the filenames are not the same.
- Configure equipment interface **pland-cfgfile1=XMLXXXXXX1** and **dnload-cfgfile1 XMLXXXXXX1**
Configure equipment interface **pland-cfgfile2=XMLXXXXXX2** and **dnload-cfgfile2 XMLXXXXXX2**
Although the OLT permits the above two steps without reporting an error, Nokia does not recommend executing them, because the ONT may exhibit unexpected behavior.
- If **pland-cfgfileX=Auto** and **dnload-cfgfileX= Auto**
The OLT will download the XML file from "sw-ctrl-list" (**configure equipment ont sw-ctrl**)

END OF STEPS

The ONT will distribute the configuration files to the different services based on the active indication from the OLT and on the Nokia defined index.

The ONT automatically reboots to apply the configuration files. After the ONT reboots and reports the active version, the OLT completes the file download procedure.

Operators must check the committed file from the OLT to verify whether the corresponding file has been applied. If an error occurs, contact Nokia for support.

8.4.3 Configuring ONT using a Combined Customized Software Package

ONT supports a combined customized software package which includes a new software-version and one or more configuration files (Config, Delta Config, Voice XML and WebGUI config), allowing to download and install it as a single package into the ONT. This is specially useful in deployment scenarios with third party OLTs, which do not support Nokia configuration files download via OMCI.

 **Note:**

1. If the ONT exist on your OLT system, and before configuring the ONT using customized firmware the **pri-cfgfile-pland** and **pri-cfgfile-dnload** files must be disabled.
2. The pre-config, delta config, voice xml and/or WebGUI configuration files as well as the required firmware version file must be shared with Nokia representatives in order to create the customized combined firmware.
3. Nokia will generate the combined customized firmware file and share with the operator.

1

The customer must upload the customized firmware file to the OLT.

2

Using OLT commands, the combined customized firmware file is downloaded.

3

The ONT automatically reboots to apply the configuration files. After the ONT reboots and reports the active version, the OLT completes the file download procedure.

END OF STEPS

