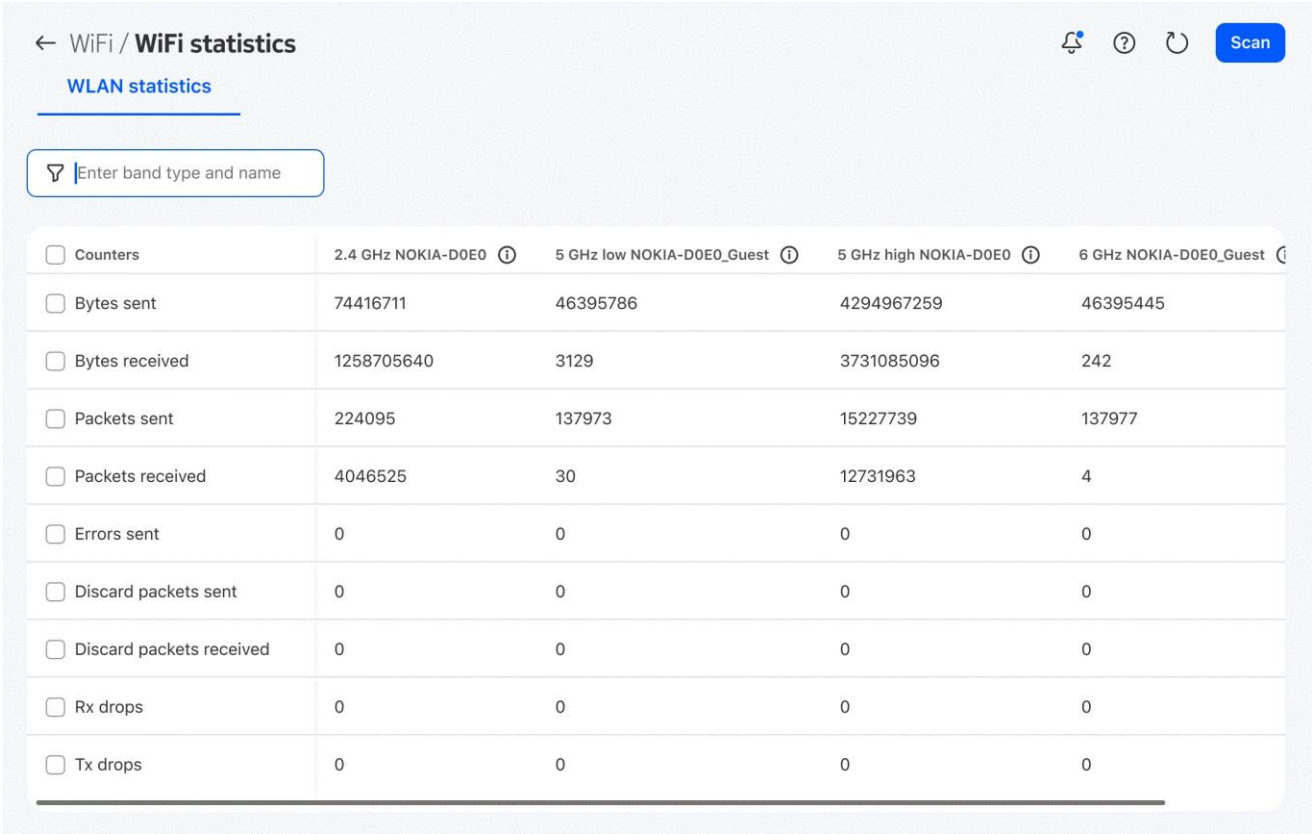


Figure 7-28 WiFi statistics page



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

END OF STEPS _____

Devices

7.26 Overview

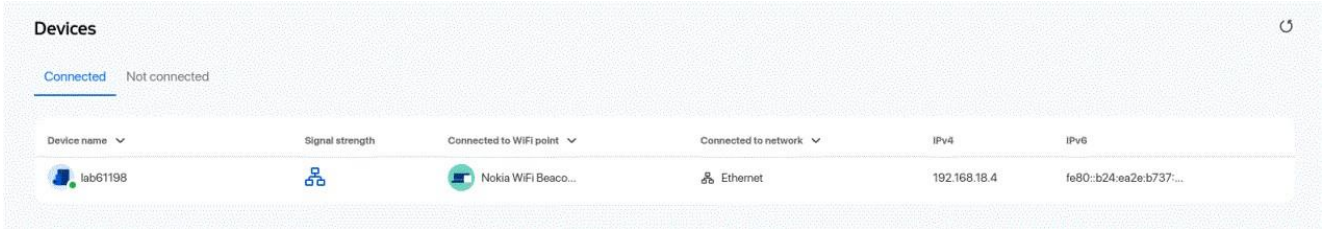
This section describes how to view device information from the **Device** menu.

7.27 Viewing Device Information

1

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

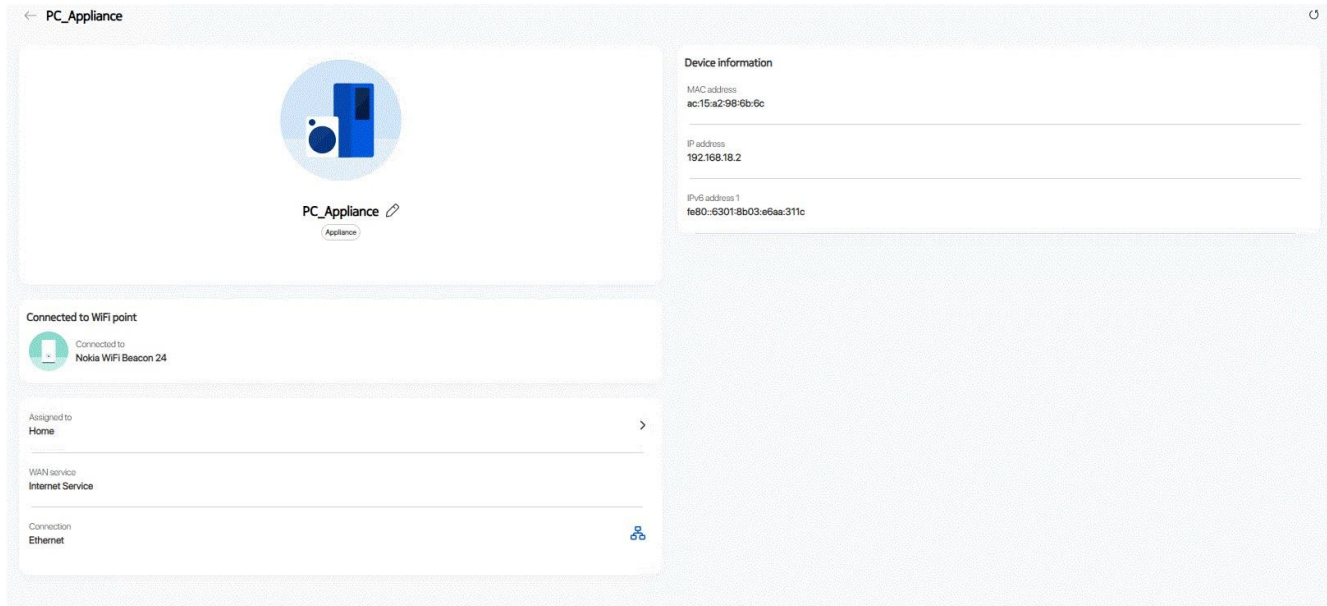
Figure 7-29 *Devices* page



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 7-30 Device information page - L3 devices



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

Perform the following steps to rename the client device:

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

Figure 7-31 Device Rename page

Edit

×

Name

61-30-PC

Category

Other

Appliance

Audio

Camera

Game console

Health

Save

END OF STEPS

Security Configuration

7.28 Overview

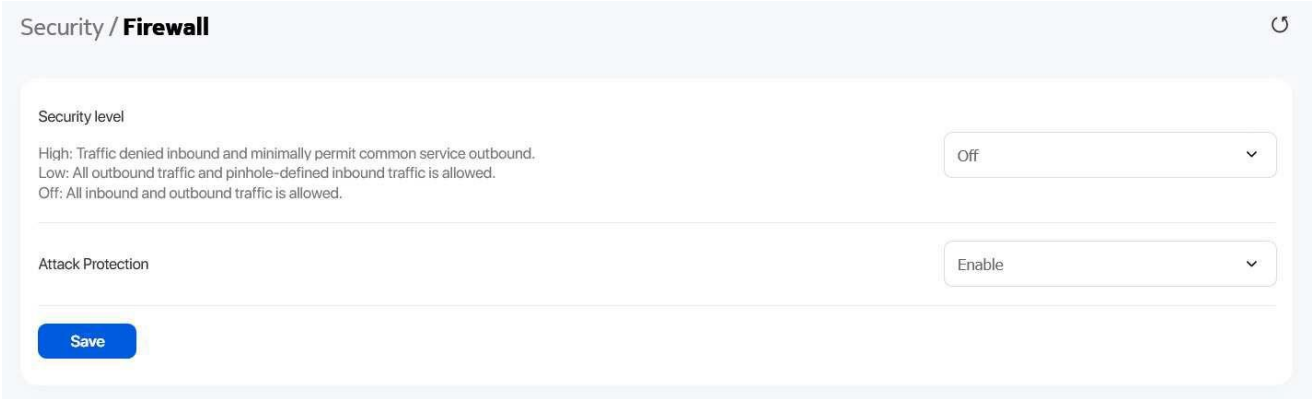
This section describes the security configuration procedures that can be performed from the following sub-menu options under the **Security** menu:

Sub-menu	Procedure
Firewall	7.29 “Configuring the Firewall” (p. 119)
MAC filter	7.30 “Configuring the MAC Filter” (p. 120)
IP filter	7.31 “Configuring the IP Filter” (p. 122)
Family profiles	7.32 “Configuring Family Profiles” (p. 123)
DMZ and ALG	7.33 “Configuring DMZ and ALG” (p. 134)
Access control	7.34 “Configuring Access Control” (p. 135)

7.29 Configuring the Firewall

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

Figure 7-32 Firewall page



- 2
- Configure the following parameters.

Table 7-19 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. 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

7.30 Configuring the MAC Filter

1

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

Figure 7-33 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

Wi-Fi 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 7-20 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 7-21 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 _____

7.31 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 7-34 IP filter page

← Security / IP filter / **Add IPv4 filter** ↻ Save

Enable IP filter 🔴

Mode

Drop for upstream ▼

Source

Drop for upstream ✓
Drop for downstream
Accept for upstream
Accept for downstream

Local IP address

Local subnet mask

Destination IP address

Destination subnet mask

Protocol

ALL ▼

3

Configure the following parameters:

Table 7-22 IP filter parameters

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

4

Click **Save**.

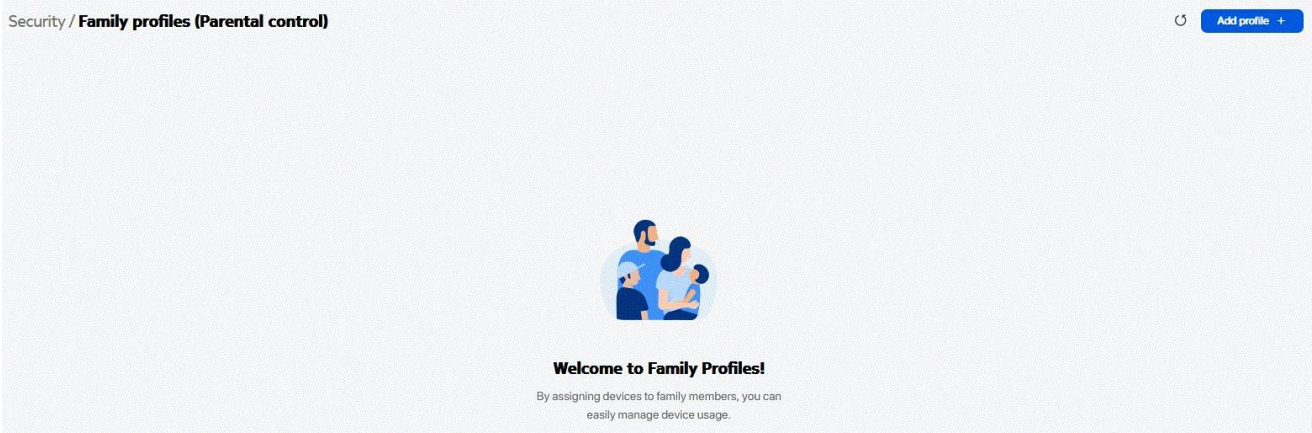
END OF STEPS

7.32 Configuring Family Profiles

1

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

Figure 7-35 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 7-36 Add a profile page

Add a profile

×

Name

eg. Alex

Cancel

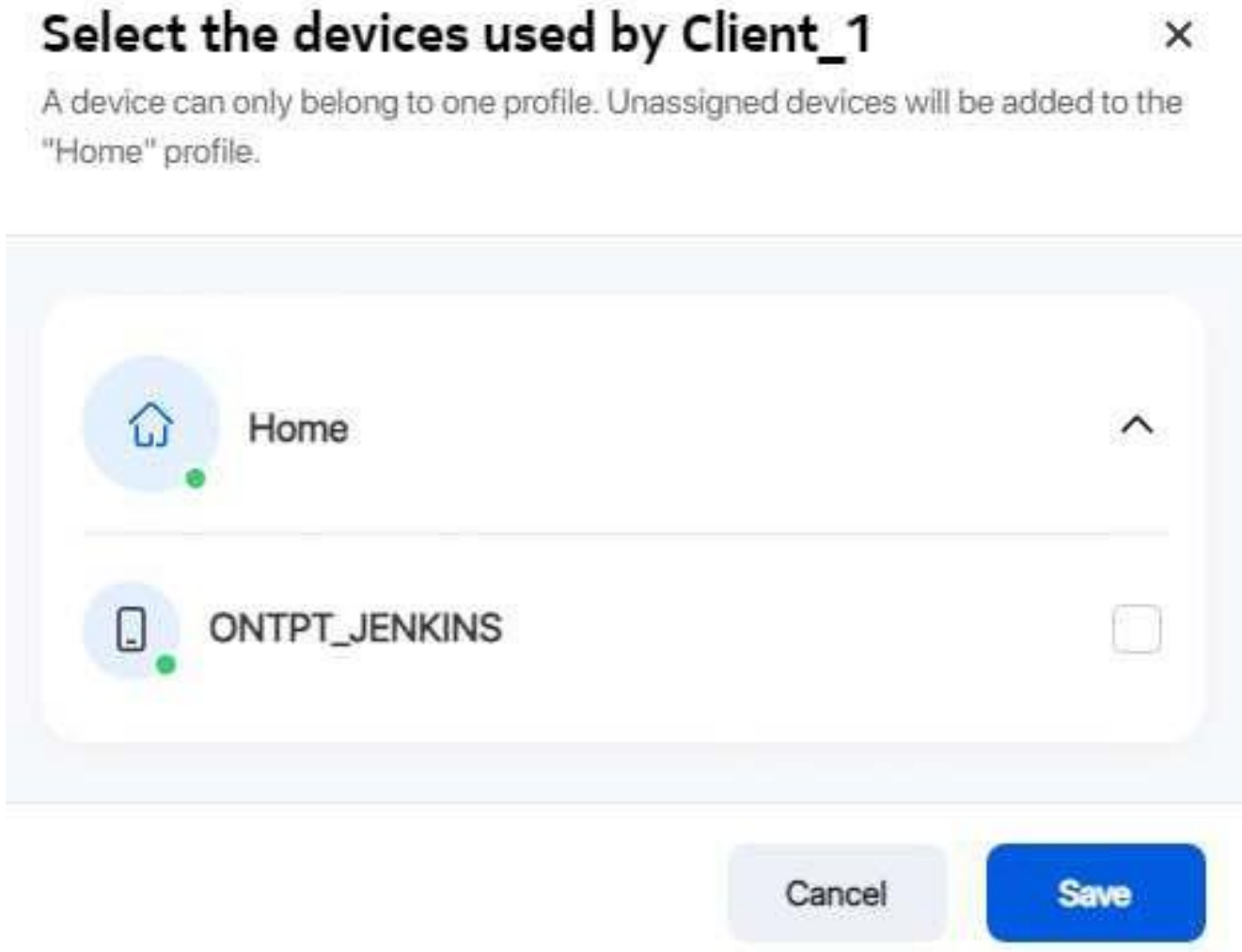
Add

4

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

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

Figure 7-37 Assign devices to family profile



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

Figure 7-38 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 7-39 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:

- 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.



Device	Icon	Selection
Home		☒
ONTPT_JENKINS		☐

Cancel Save

- 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:

- 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

Start time

:

End time

:

Days of the week

M

TU

W

TH

F

SA

SU

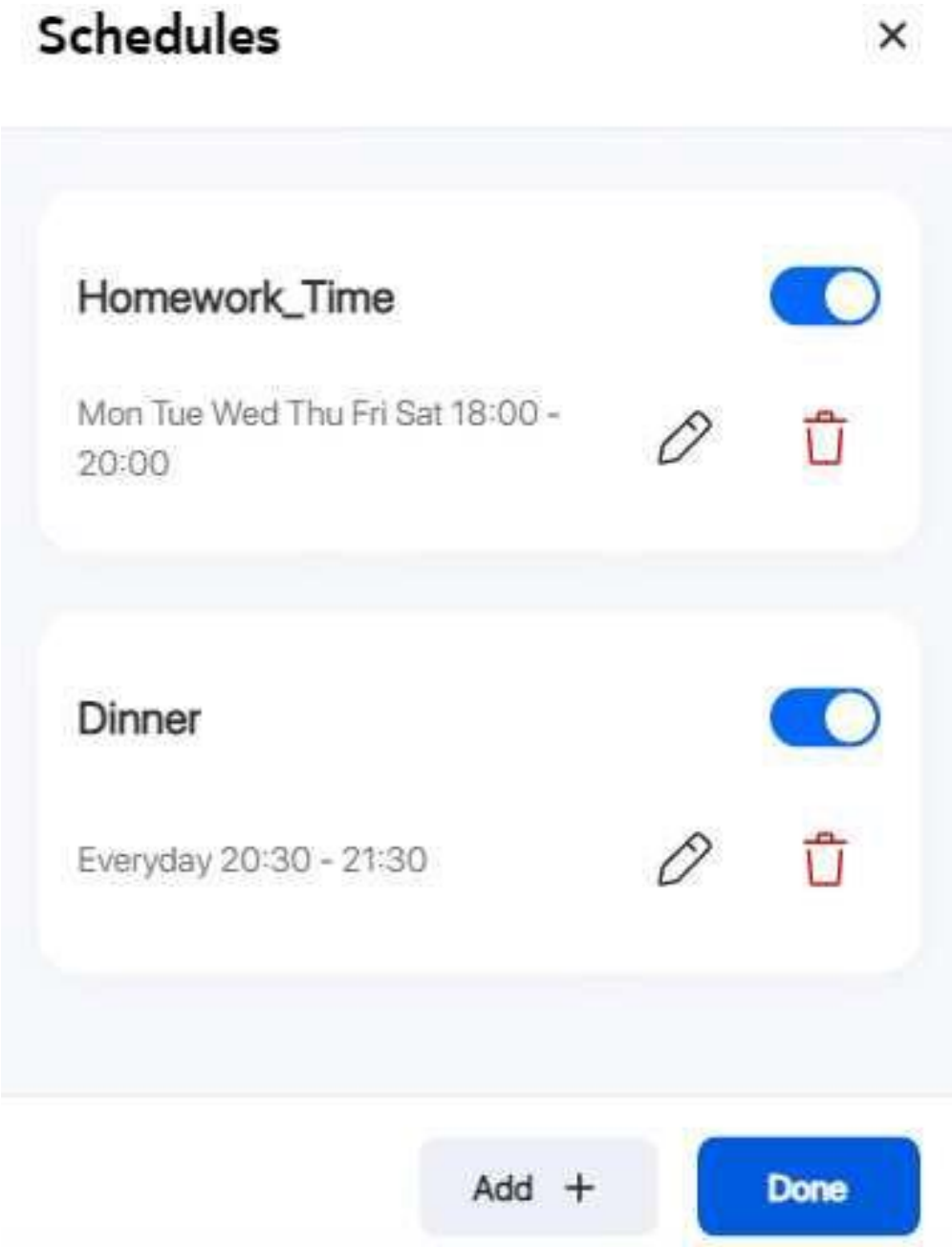
Cancel

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 +**.



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

21

:

00

Wake Up

06

:

00

Days of the week

M

TU

W

TH

F

SA

SU

Cancel

Save

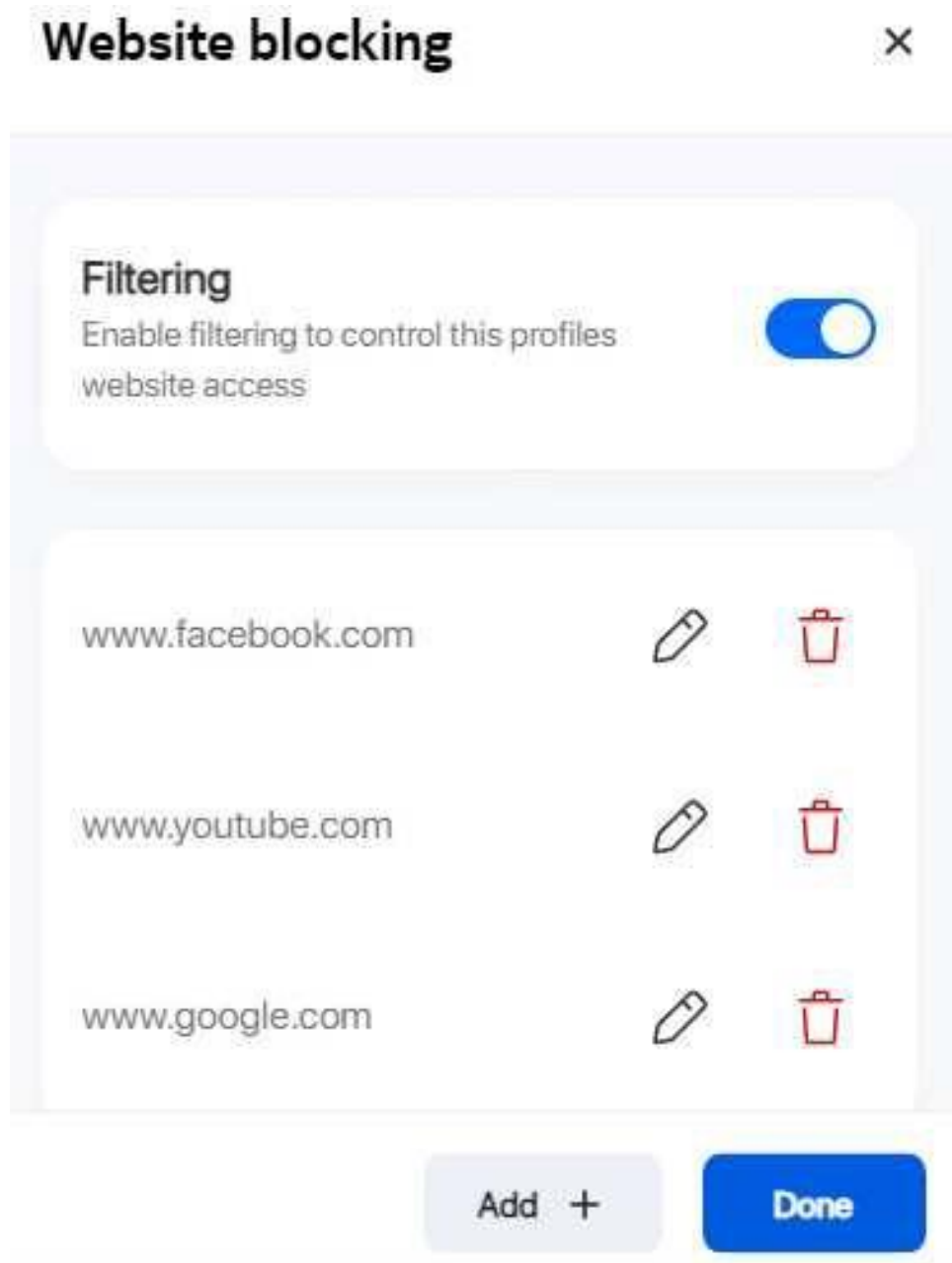
1. Select the Bedtime, Wake Up time, and select the days of the week on which the bedtime will be in effect.
2. Click **Save**. The bedtime is created and listed in the *Bedtime* page.
- d. In the *Bedtime* page, select the toggle button to enable the bedtime and click **Done**.

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:



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**.

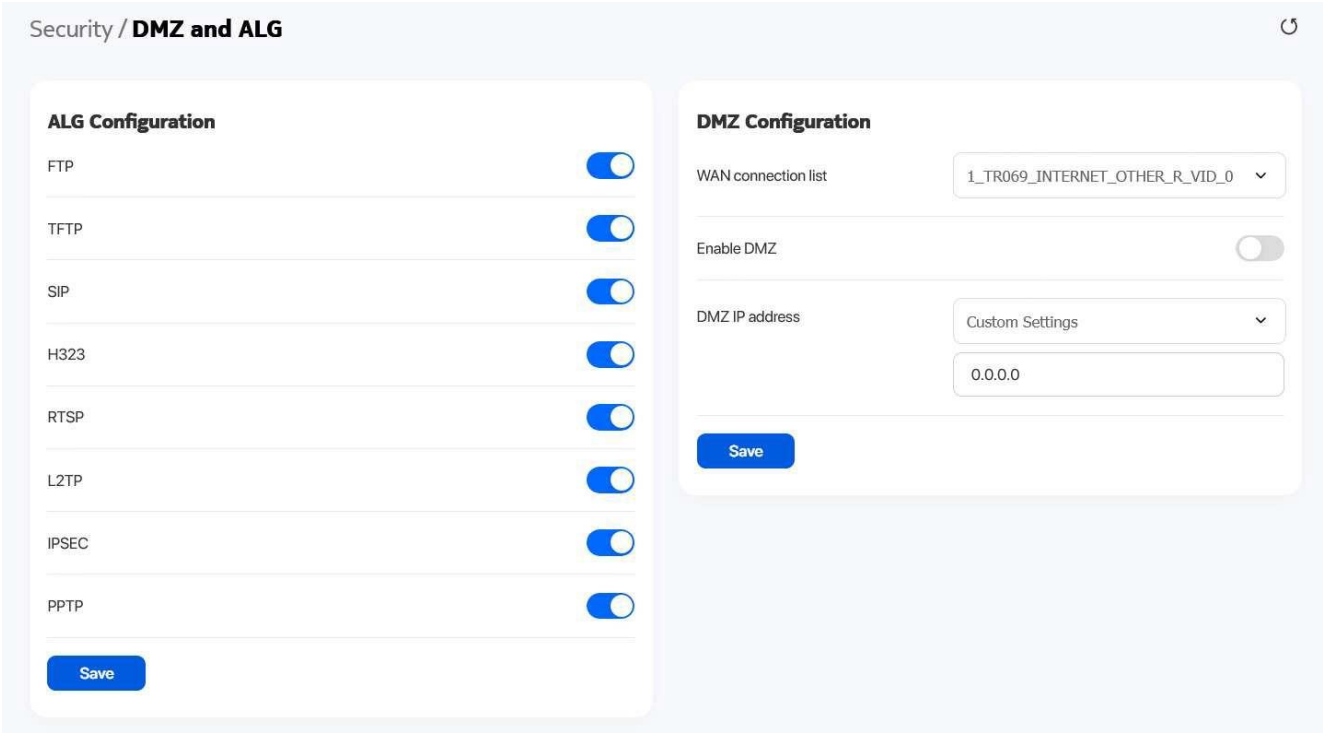
4. Click **Add +** to add more website URLs to be blocked or click **Done**.

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 7-40 DMZ and ALG page



- 2
- Configure the following parameters:

Table 7-23 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

3

Click **Save**.

4

Configure the following parameters:

Table 7-24 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 7-41 Access control page

Security / Access control

WAN connection list

1_TR069_INTERNET_OTHER_R_VID_0

Enable trusted network

WAN

ICMP

Allow

Telnet

Deny

SSH

Deny

HTTP

Deny

TR-069

Allow

HTTPS

Deny

SFTP

Deny

LAN

ICMP

Allow

Telnet

Deny

SSH

Allow

HTTP

Allow

TR-069

Deny

HTTPS

Allow

SFTP

Deny

Save

Trusted network

Source IP start

Source IP end

Add +

2

Configure the following parameters:

Draft

136

© 2024 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

3TN-00789-AAAA-TCZZA

September 2024
Issue 1

Table 7-25 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 7-26 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. 138)
Port triggering	7.37 “Configuring Port Triggering” (p. 139)
DDNS	7.38 “Configuring DDNS” (p. 140)
NTP	7.39 “Configuring NTP” (p. 142)

7.36 Configuring Port Forwarding

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

Figure 7-42 Port forwarding page

Advanced settings / **Port forwarding** ↺ Save

WAN port

-

LAN port

-

Internal client

Custom Settings▼

Protocol

TCP ▼

WAN connection list

1_INTERNET_OTHER_R_VID_400 ▼

- 2
- Configure the following parameters:

Table 7-27 Port forwarding parameters

Field	Description
WAN port	Enter the WAN port range.

Table 7-27 Port forwarding parameters (continued)

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

3

Click **Save**.

END OF STEPS

7.37 Configuring Port Triggering

1

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

Figure 7-43 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

1_INTERNET_OTHER_R_VID_400

▼

2

Configure the following parameters:

Table 7-28 Port triggering parameters

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

3

Click **Save**.

END OF STEPS

7.38 Configuring DDNS

1

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

Figure 7-44 DDNS page

Advanced settings / **DDNS**

WAN connection list

1_TR069_INTERNET_OTHER_R_VID_0

Enable DDNS

ISP

DynDNS.org

Domain Name

Username

Password

Save

2

Configure the following parameters:

Table 7-29 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 7-45 NTP page

Advanced settings / **NTP**

Enable NTP service

☒

Current date & time

07/19/2022 12:33:04 PM

Primary Time Server

time.nist.gov

Secondary Time Server

Custom Settings

ntp1.tummy.com

Third time server

None

Interval time

0

0,15-259200 secs

Time zone

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

Save

- 2
- Configure the following parameters:

Table 7-30 NTP parameters

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

Table 7-30 NTP parameters (continued)

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

3

Click **Save**.

END OF STEPS

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. 144)
Backup and restore	7.42 "Backing Up the Configuration" (p. 146) 7.43 "Restoring the Configuration" (p. 146)
Firmware upgrade	7.44 "Upgrading Firmware" (p. 148)
Diagnostics	7.45 "Diagnosing WAN Connections" (p. 149)
Log	7.46 "Viewing Log Files" (p. 153)

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 7-46 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 7-31 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**.

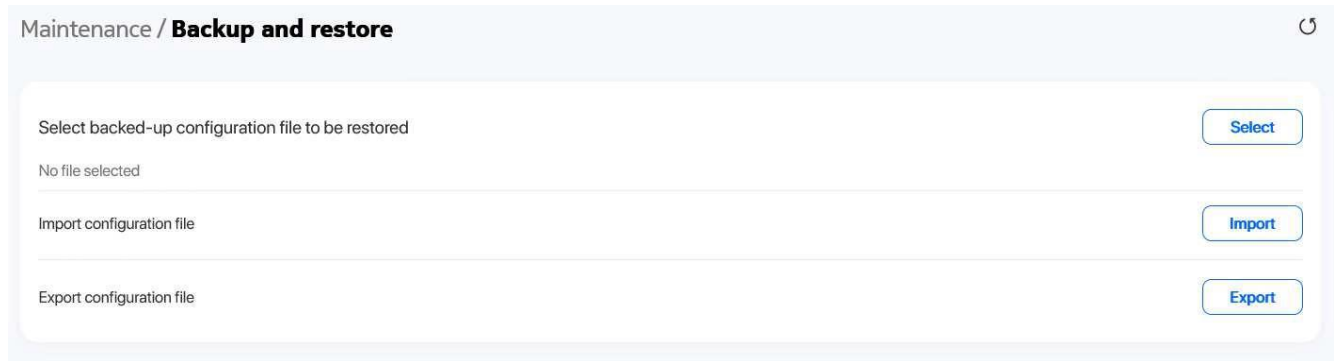
END OF STEPS

7.42 Backing Up the Configuration

1

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

Figure 7-47 Backup and restore page



2

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

END OF STEPS

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 7-48 Backup and restore page

The screenshot shows a web interface titled "Maintenance / Backup and restore". It contains three sections: "Select backed-up configuration file to be restored" with a "Select" button, "Import configuration file" with an "Import" button, and "Export configuration file" with an "Export" button. The "Select" button is highlighted with a yellow border.

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

- 3 Click **Import** to import the configuration file created in [7.42 “Backing Up the Configuration” \(p. 146\)](#) and restore the Beacon to the backed-up configuration.
 - a. If the configuration file is from the same Beacon variant with a different serial number, you will be prompted to enter the serial number of the original device.

Figure 7-49 Backup and restore: Serial number

The screenshot shows a modal dialog box titled "Serial number" with a close button (X). It contains a label "Serial number" above a text input field. Below the input field is a blue button labeled "Import".

- 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 Beacon variant, OPID, or different release prior to Release 2402.
- A confirmation message displays after successful restore and the Beacon reboots.

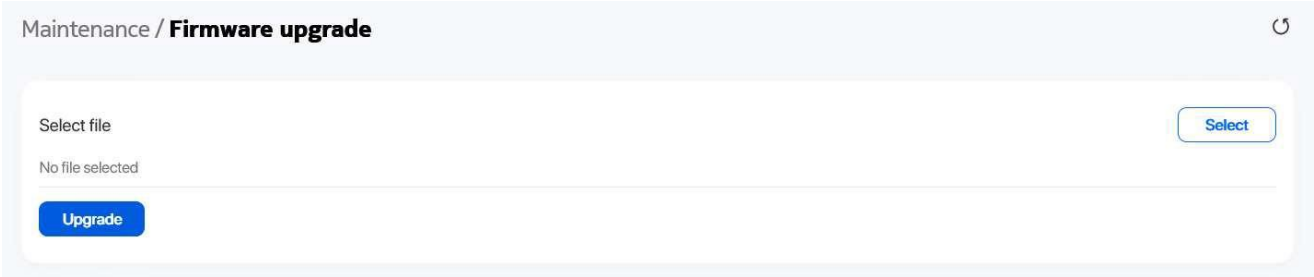
END OF STEPS

7.44 Upgrading Firmware

1 _____

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

Figure 7-50 *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 7-51 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 Diagnosing WAN Connections

1

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

Figure 7-52 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 7-32 Diagnostics parameters

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

Table 7-32 Diagnostics parameters (continued)

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

3

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

Figure 7-53 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 7-54 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

7.46 Viewing Log Files

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

Figure 7-55 Log page

Maintenance / **Log**

 Save Export log

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

7.47 Viewing Container Management

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

Figure 7-56 Container management page



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

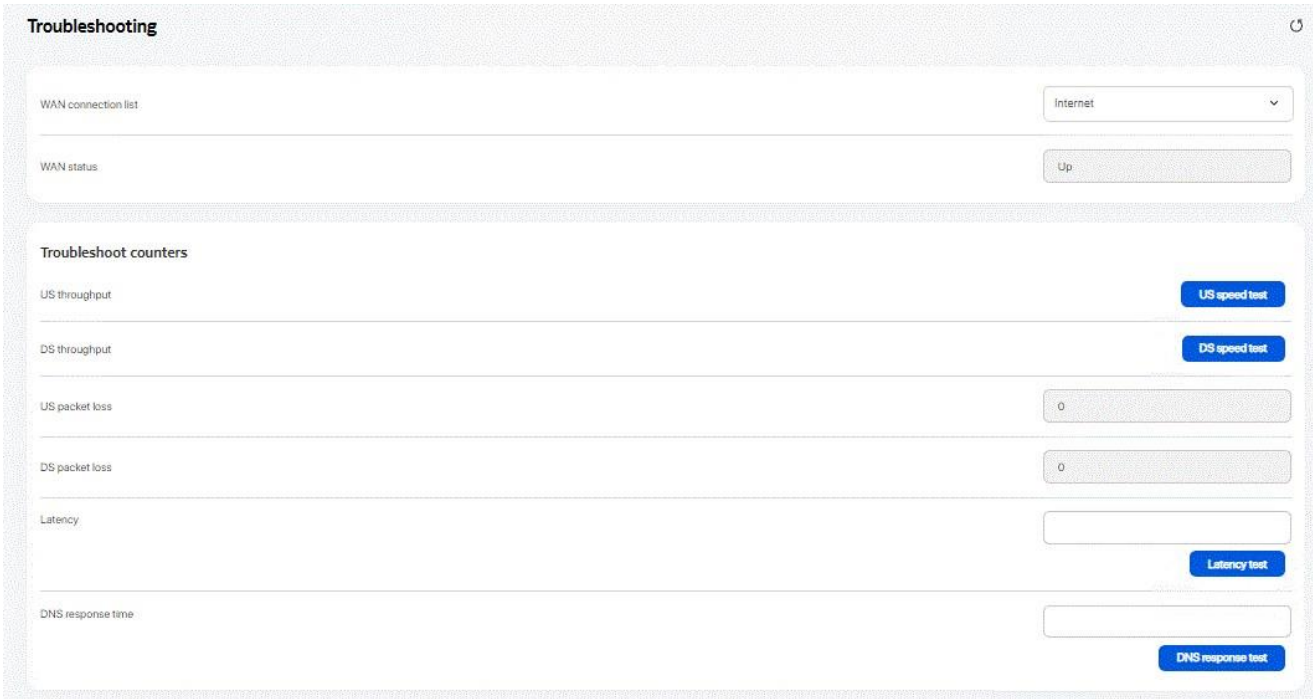
Troubleshooting

7.48 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 7-57 Troubleshooting counters page



- 2
- Configure the following parameters:

Table 7-35 Troubleshooting counters parameters

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

3

Click **Save**.

END OF STEPS

7.49 Viewing Speed Test

1

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

Figure 7-58 Speed test page

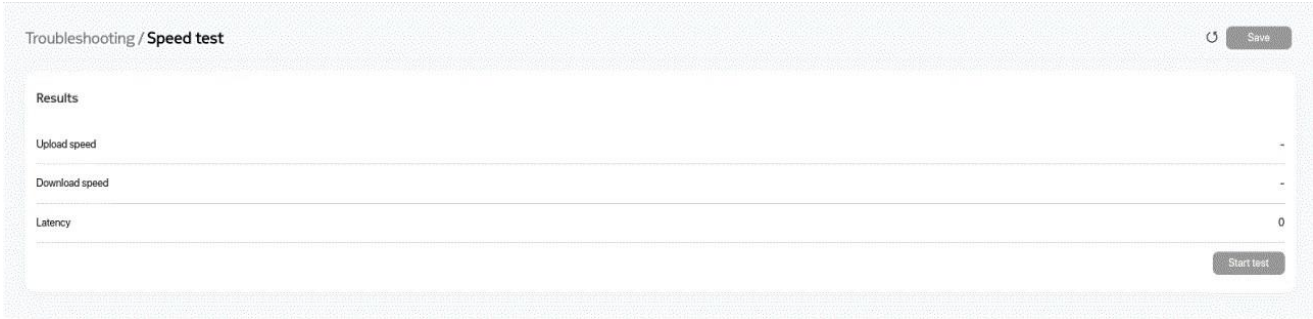


Table 7-36 Speed test parameters

Field	Description
Upload speed	Displays the upload speed.
Download speed	Displays the download speed.
Latency	Displays the latency.

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

END OF STEPS

