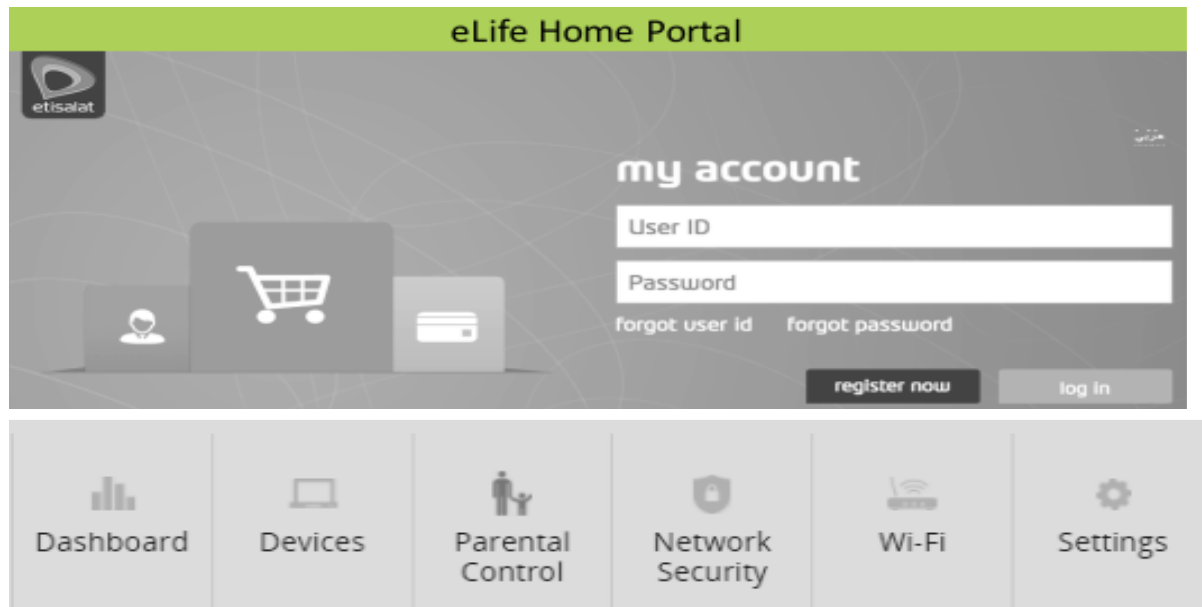


Etisalat (Emirates Telecommunications Corporation)
Head Office, P.O. Box 3838, Abu Dhabi, UAE
Visit us at: www.etisalat.ae



eLife Home Portal User Manual

Etisalat (Emirates Telecommunications Corporation)
Head Office, P.O. Box 3838, Abu Dhabi, UAE
Visit us at: www.etisalat.ae

COPYRIGHT NOTICE
Copyright© reserved by Etisalat
ALL RIGHTS RESERVED

The information contained herein is proprietary and confidential information for the use of Etisalat personnel only. No part of this material should be reproduced, published in any form by any means, electronic or mechanical including photocopy or any information storage or retrieval system nor should the materials be disclosed to third parties unless previously authorized in writing by Etisalat. Product names mentioned herein are for identification purposes only and may be Trademarks and/or Registered Trademarks of their respective companies.

Table of Contents

| | | |
|---|--|----|
| 1 | Introduction..... | 4 |
| | 1.1... <i>Scope and Purpose</i> | 4 |
| | 1.2... <i>eLife Home Portal overview</i> | 4 |
| | 1.3... <i>Eligibility</i> | 4 |
| 2 | Navigation..... | 4 |
| | 2.1... <i>eLife Home Portal login</i> | 4 |
| | 2.1.1 Customers that have been registered | 5 |
| | 2.1.2 Customers without Etisalat online account..... | 5 |
| | 2.2... <i>Dashboard</i> | 5 |
| 3 | Parental Control | 7 |
| | 3.1... <i>Create a new policy</i> | 7 |
| | 3.1.1 Content Filtering..... | 10 |
| | 3.1.2 Internet Access Time | 10 |
| | 3.2... <i>Policy Display</i> | 11 |
| 4 | Network Security | 12 |
| | 4.1... <i>Antivirus</i> | 13 |
| | 4.1.1 Activating/Deactivating Antivirus..... | 14 |
| | 4.2... <i>Firewall</i> | 15 |
| 5 | Managing other settings..... | 16 |
| | 5.1... <i>Managing WiFi networks</i> | 16 |
| | 5.2... <i>Managing Devices</i> | 17 |
| | 5.2.1 Modifying Devices | 19 |
| | 5.2.2 Pinning/Unpinning Devices..... | 20 |

1 Introduction

1.1 Scope and Purpose

This manual explains how to use eLife Home Portal to manage your broadband services from anywhere in the world.

1.2 eLife Home Portal overview

eLife Home Portal is a self service portal and initially the following value-added services will be available:

- Parental Control: restricting access to resources with gaming, social networks, communication, media streaming, peer-to-peer networks, and adult content. Parental control includes Scheduling—for a specified home device, subscriber can select week days and hours when the Internet is block
- Antivirus: subscriber can turn on antivirus scan for all traffic from his WiFi
- Cloud Powered firewall: Firewall—subscriber can block incoming traffic from the Internet to the certain IP addresses on his WiFi

The Self Service Portal is represented as a web-page, functionally divided into several tabs/pages with different content and controls.

1.3 Eligibility

Any eLife customer with D-link 850/ 850 or Technicolor Extreme router.

2 Navigation

2.1 eLife Home Portal login

Customer opens eLife Home Portal by simply clicking directly on <https://onlineservices.etisalat.ae>.

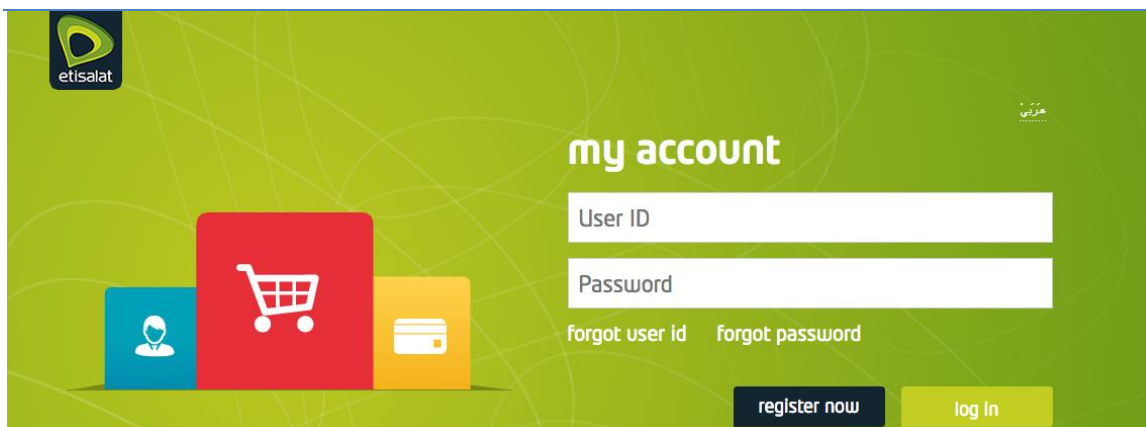


Fig. 1: eLife Home Portal login

2.1.1 Customers already registered on Etisalat online services

Already registered customer can login to eLife Home Portal using their existing account credentials.

2.1.2 Customers not registered on Etisalat online services

Customers that don't have online account need to go through the complete registration process when first setting up the service. The registered user ID and password that they chose during this process will be used for logging onto eLife Home Portal.


After logging in, customer lands on the Dashboard tab.

2.2 Dashboard

The Dashboard contains a summary of user home network current state:

- Wi-Fi Networks summary, both 2.4 GHz and 5 GHz modes.
- Traffic usage chart for outgoing and incoming traffic.
- Device list with device information (IP address, MAC address, device name, status).

Subscribers can change time period for traffic usage representation on the chart, and to manage devices.


Dashboard
Devices
Parental Control
Network Security
Wi-Fi
Settings
Tasks ▾

Wi-Fi Networks

Wi-Fi access 2.4 GHz

Wi-Fi access 2.4 GHz

 Modify

Wi-Fi access 5 GHz

Wi-Fi access 5 GHz

 Modify

Utilization of the Internet Channel

Last 24 hours
Last week
Last month

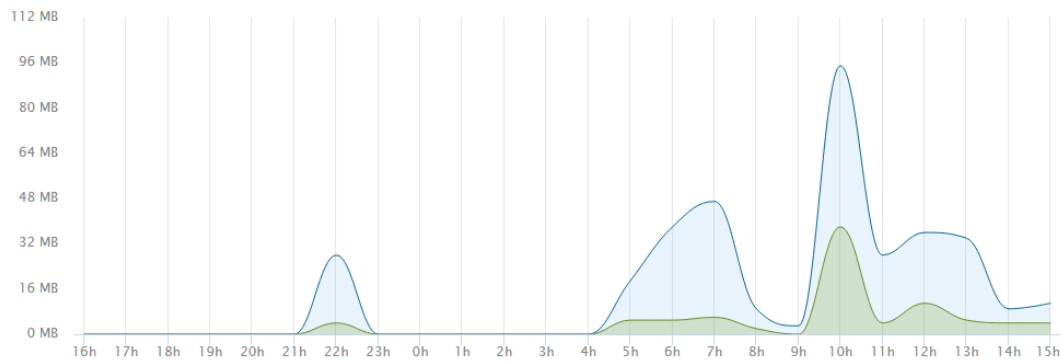


Fig. 2: eLife Home Portal Dashboard

3 Parental Control

From the dashboard, customer selects the Parental Control tab in order to create new policies, view/change existing policies and delete policies.

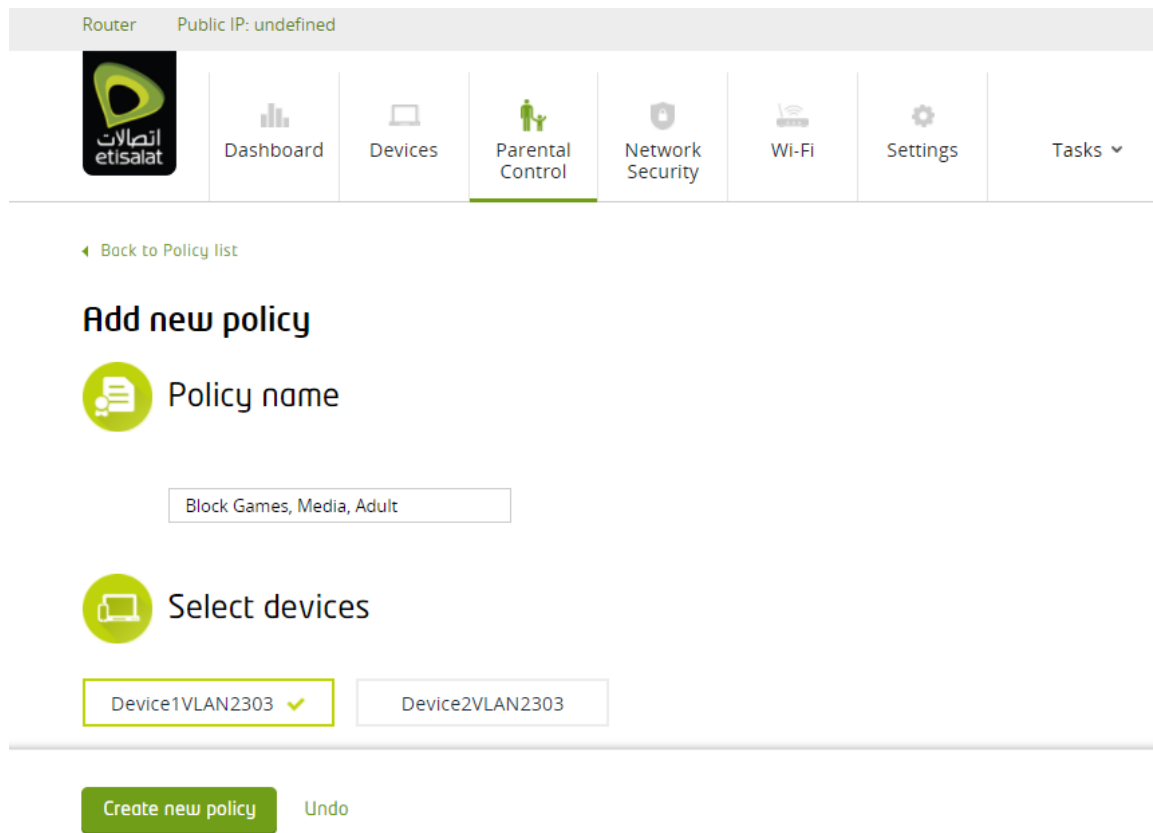


Fig. 3: Parental Control Tab

3.1 Create a new policy

To create a new policy, the subscriber should perform the following steps:

- Open the Parental Control tab.
- Click Add New Policy.
- Specify the name of the new policy (must be unique).
- Select devices to include into the new policy.
- Select the types of content to block—games, social networks, communications, peer-to-peer networks, media streaming, adult content (see 3.1.1 Content Filtering)
- Turn on or off the time scheduling feature (See 3.1.2 Internet Access Time)

- Set up days and hours for time scheduling feature
- Click Create New Policy.

The same algorithm is applied to modify existing policy. At least one device must be assigned to a policy. A device can be assigned only to one policy.

Router Public IP: 37.245.64.2

الاتصالات
etisalat

Dashboard Devices **Parental Control** Network Security Wi-Fi Settings

← Back to Policy list

Add new policy

Policy name

Name

Select devices

Intel Corporate KMM LCFC(HeFei) Electronic...

SAMSUNG ELECTRO-M... WS-3428 WS-6876-1

Options

Content Filtering
Filters allow you to block access to unwanted web sites, content and applications in the Internet.

Games

Block on-line games and game resources e.g. Steam, BattleNet, Origin, etc.

Block

Social networks

Block social networking sites e.g. Twitter, Facebook, LinkedIn, Pinterest, Insta...

Block

Communication

Block text messaging audio and video calls e.g. Skype, WhatsApp, Viber, etc.

Block

Media streaming

Block video and sound streaming services e.g. Netflix, Apple TV, Amazon Video, etc.

Block

Peer-to-peer networks

Block peer-to-peer file sharing e.g. BitTorrent, eDonkey, Pirate Bay, etc.

Block

18+ Adult content

Block access to adult resources e.g. PornHub, XVideos, RedTube, etc.

Block

Internet Access Time
Time Scheduling allows you to set weekdays and hours when device will have access to the Internet.

| Day | 0:00 | 2:00 | 6:00 | 8:00 | 10:00 | 12:00 | 14:00 | 16:00 | 18:00 | 20:00 | 22:00 |
|-----------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|
| Sunday | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked |
| Monday | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked |
| Tuesday | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked |
| Wednesday | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked |
| Thursday | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked | Blocked |

Internet Access Time

Time Scheduling allows you to set weekdays and hours when device will have access to the Internet.

0:00 2:00 6:00 8:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00

Sunday
Monday
Tuesday
Wednesday
Thursday

Create new policy Undo

Fig. 4: Creating Policy

3.1.1 Content Filtering

This feature allows customers to block access to unwanted websites, content and applications on the internet. It can be used when creating or modifying existing policies.

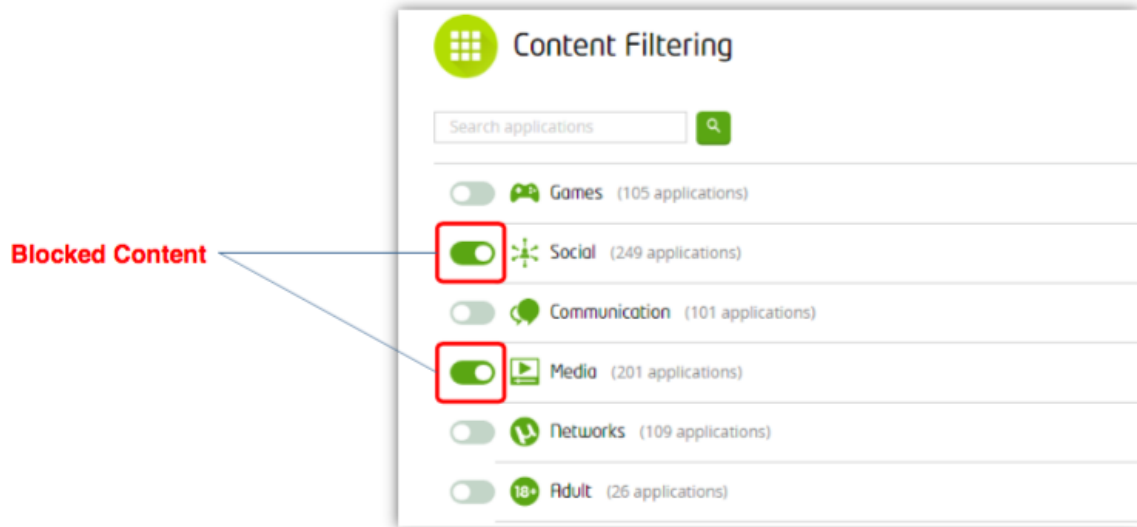


Fig. 5: Block Content

3.1.2 Internet Access Time

This feature allows users to set weekdays and hours when device will have access to the internet.

- Customer navigates to Parental Control tab.
- Existing policy for a device currently being online is selected to be modified.
- Customer activates Internet Access Time and set current time to be blocked.
- Customer updates policy.
- No devices related to this policy are able to navigate through the Internet.

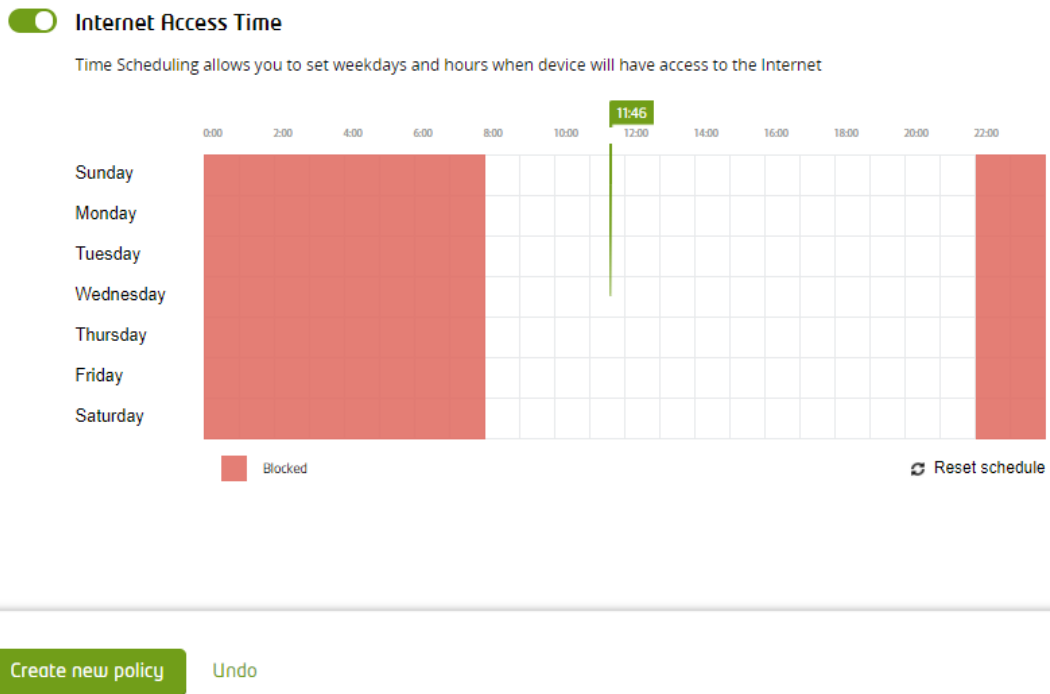
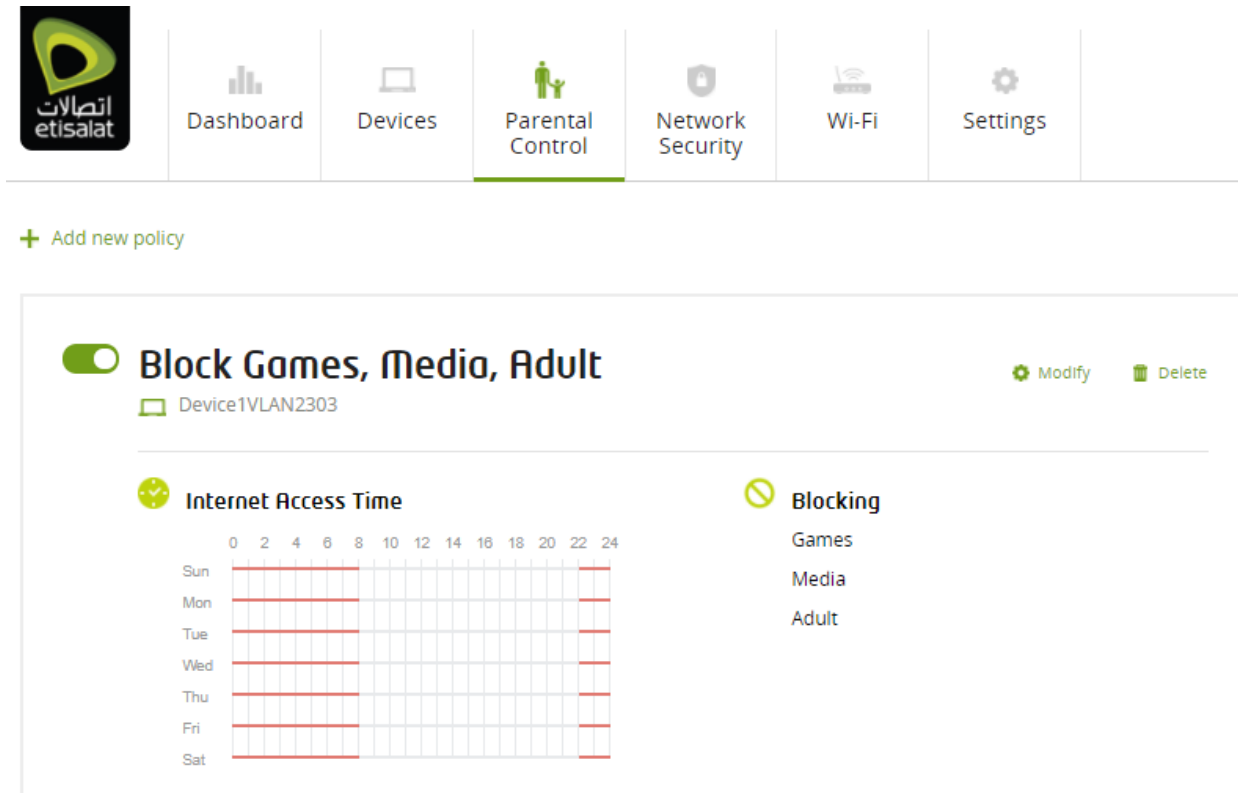


Fig. 6: Block Access Time

3.2 Policy Display

The following details are displayed for each policy:

- Policy Name
- List of devices assigned to the policy
- List of blocked content categories
- Scheduling properties



The screenshot displays the Etisalat parental control dashboard. At the top, there is a navigation menu with icons for Dashboard, Devices, Parental Control (highlighted), Network Security, Wi-Fi, and Settings. Below the menu is a '+ Add new policy' button. The main content area shows a policy titled 'Block Games, Media, Adult' for device 'Device1VLAN2303'. The policy is active, indicated by a green toggle switch. To the right of the title are 'Modify' and 'Delete' buttons. Below the title, there are two sections: 'Internet Access Time' and 'Blocking'. The 'Internet Access Time' section shows a grid with days of the week (Sun to Sat) on the y-axis and hours (0 to 24) on the x-axis. Red lines indicate blocked access times. The 'Blocking' section has a 'Blocking' toggle switch and lists 'Games', 'Media', and 'Adult' as blocked categories.

Fig. 7: Policy Display

4 Network Security

Network Security tab provides control to 2 value added services:

- Antivirus
- Firewall rules.

Router Public IP: 37.245.64.2

Antivirus

Antivirus examines files being downloaded from the Internet for threats such as a virus or other malware. If Antivirus finds a threat it blocks the file even before it reaches your home network. It also blocks access to the web sites which are known to have links to malicious software.

Firewall rules

Ip v4 Ip v6

+ Add Firewall Rule

Port Forwarding Remote IP Address Prefix Length Remote Peer Port

apache 1

In order to filter incoming traffic to your device from Internet, the configuration needs to be applied first in Port Mapping section at Settings Page

Apply Rule Undo Rule

Figure 8: Network Security Tab

On the Network Security tab, subscribers can:

- Switch antivirus on and off
- Create new firewall rules
- Edited existing firewall rules
- Delete firewall rules

4.1 Antivirus

Antivirus examines files being downloaded from the internet for threats such as a virus or other malware. If antivirus finds a threat it blocks the file even before it reaches user's home network. It also blocks access to the web sites which are known to have links to malicious software.

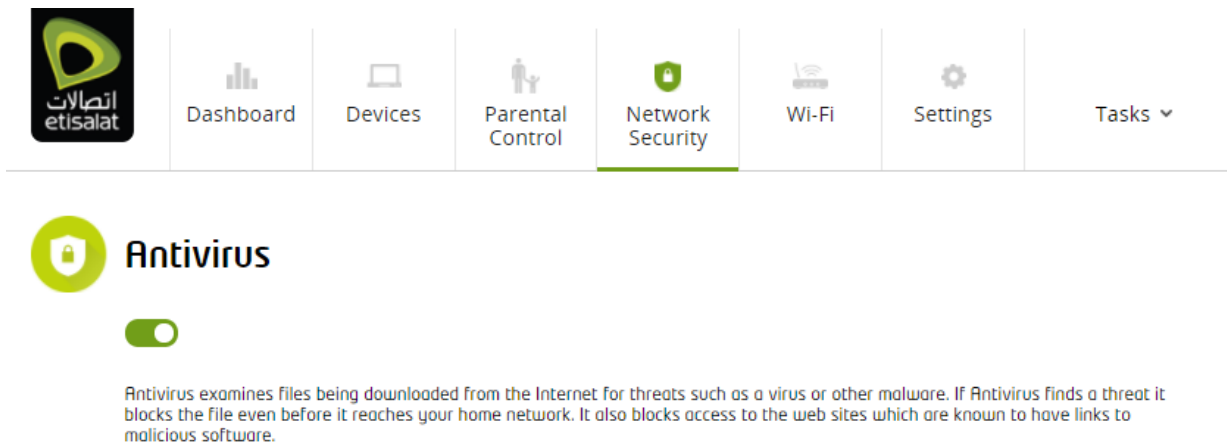


Fig. 9: Network Security/Antivirus

4.1.1 Activating/Deactivating Antivirus

To activate Antivirus instantly, subscriber should perform the following steps:

- Open the Network Security tab.
- Flick the antivirus switch to the On position.

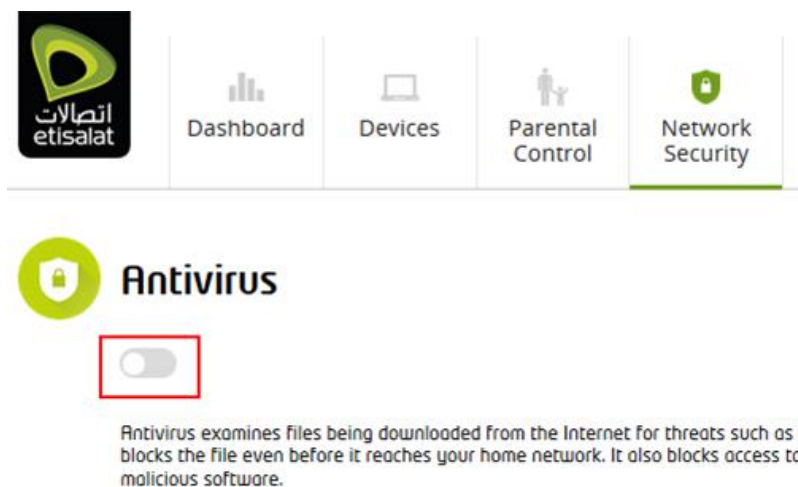


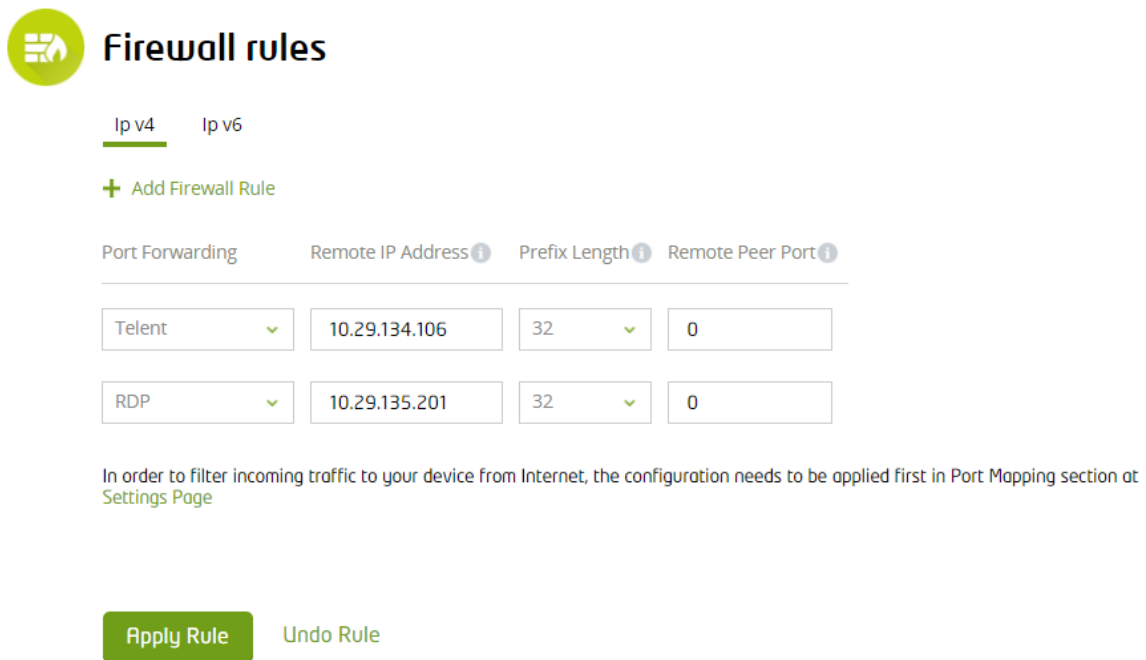
Fig. 10: Antivirus switch

4.2 Firewall

Firewall Rule enables subscribers to allow access to internal resources from particular external IP address(es).

To set up a firewall rule:

- Navigate to Network Security tab.
- Click Add Firewall Rule.
- Select existing Port Forwarding.
- Specify Remote IP Address, Prefix Length, and Remote Peer Port.
- Click Apply Rule.



Firewall rules

Ip v4 Ip v6

+ Add Firewall Rule

| Port Forwarding | Remote IP Address ⓘ | Prefix Length ⓘ | Remote Peer Port ⓘ |
|-----------------|---------------------|-----------------|--------------------|
| Telnet | 10.29.134.106 | 32 | 0 |
| RDP | 10.29.135.201 | 32 | 0 |

In order to filter incoming traffic to your device from Internet, the configuration needs to be applied first in Port Mapping section at Settings Page

Apply Rule Undo Rule

Fig. 11: Firewall rules

5 Managing other settings

5.1 Managing WiFi networks

Subscribers can manage Wi-Fi networks on the **Wi-Fi** tab. The SSP provides functionality to manage up to 4 Wi-Fi networks: 2 Main Wi-Fi networks for 2.4 GHz band and for 5 GHz band, and 2 Guest Wi-Fi networks for 2.4 GHz band and for 5 GHz band. For each of the Wi-Fi networks, the following parameters can be set:

- Enable or disable the Network.
- Set up SSID (Wi-Fi name).
- Set up WPA2-PSK key for the Network.

Note: Guest Wi-Fi can be enabled only if main Wi-Fi is activated for the same band.

Entered parameters are validated by the following rules:

- **SSID** must contain only letters (A-z), numbers (0-9), dashes (-), underscores (_), apostrophes ('), periods (.), spaces (), and commas (,).
- **SSID** must be a minimum of 1 character and a maximum of 32 characters.
- **WPA2-PSK key** must be a minimum of 8 characters and a maximum of 63 characters.
- **WPA2-PSK key** must contain only letters (A-z) and numbers (0-9).

Figure 1 Wi-Fi management view



Wi-Fi

Wi-Fi access 2.4 GHz

Wi-Fi Name (SSID)

WPA2-PSK Key

Wi-Fi access 5 GHz

Wi-Fi Name (SSID)

WPA2-PSK Key

Guest Wi-Fi access 2.4 GHz

Wi-Fi Name (SSID)

WPA2-PSK Key

Guest Wi-Fi access 5 GHz

Wi-Fi Name (SSID)

WPA2-PSK Key

5.2 Managing Devices

The Devices tab displays subscriber's devices with the following details:

- Device name
- IP address
- MAC address
- Vendor
- Is device associated with policy
- Is device online
- Is device pinned
- MAC address

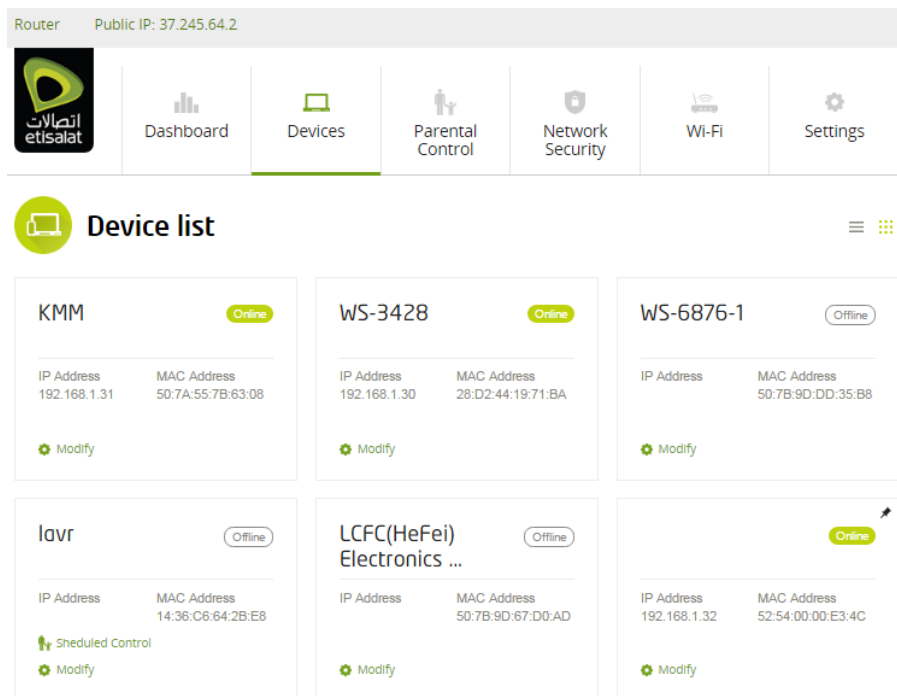


Fig. 13 Devices Tab. Icon Representation

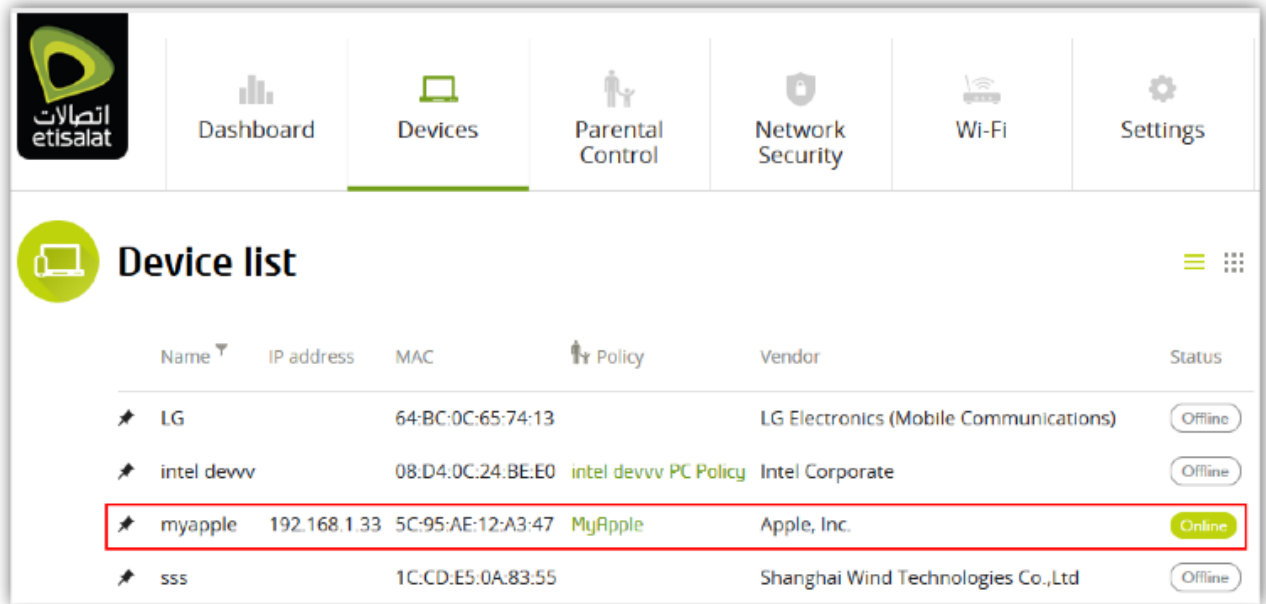


Fig. 14 Devices List

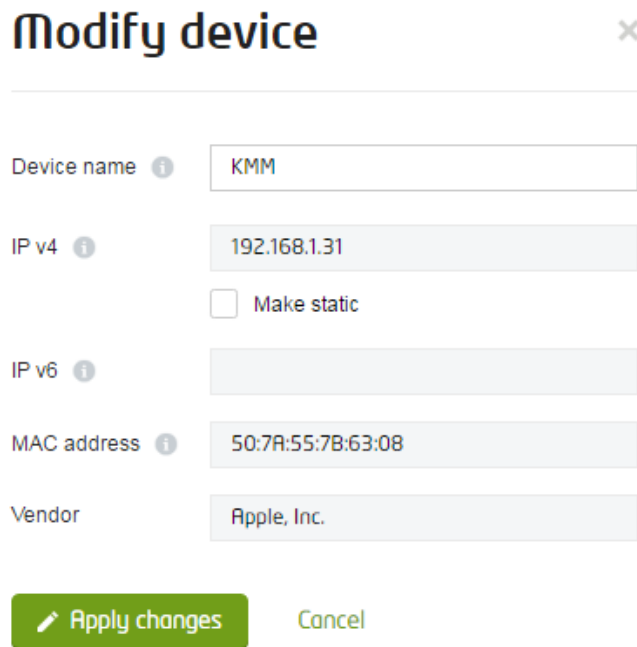
5.2.1 Modifying Devices

Subscribers can change the following parameters of devices:

- Device name
- IPv4–value within range (only for static devices)
- Make static

To modify a device:

- Open the Devices tab.
- Click Modify next to the necessary device.
- Update the parameters of the device.
- Click Apply Changes.



Modify device ✕

Device name ⓘ

IP v4 ⓘ
 Make static

IP v6 ⓘ

MAC address ⓘ

Vendor

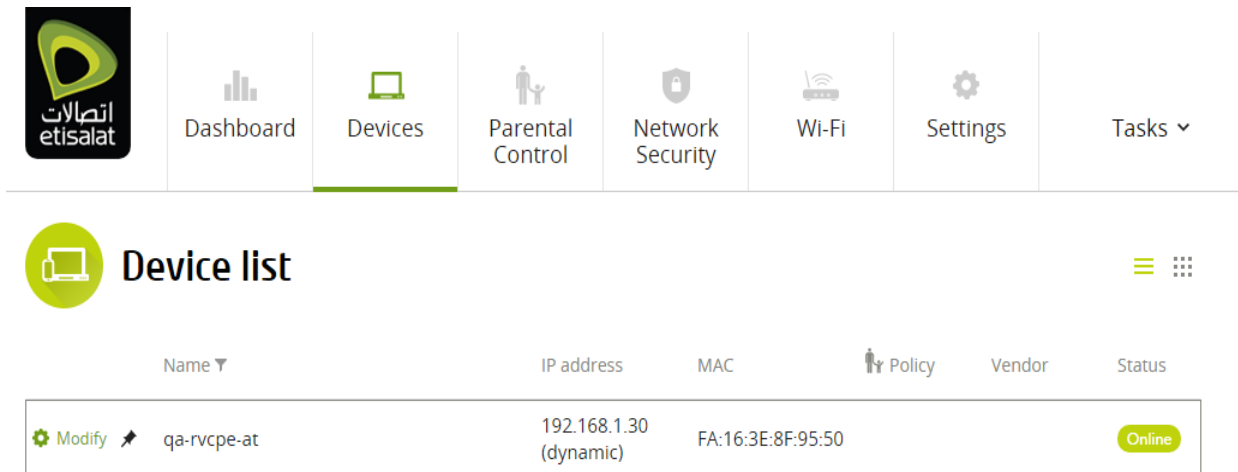
Fig 15: Modifying devices

5.2.2 Pinning/Unpinning Devices

By default, the SSP provides managing devices only in the Online status. To allow changes to offline devices, the user should pin it.

To pin a device:

- Open the Devices tab.
- Click Pin near the device in Offline status.
- After that, a subscriber can rename the device, change device IP, and assign a police to the device.



The screenshot shows the Etisalat network management interface. At the top, there is a navigation menu with the following items: Dashboard, Devices (highlighted), Parental Control, Network Security, Wi-Fi, Settings, and Tasks. Below the menu is the 'Device list' section, which includes a table with the following columns: Name, IP address, MAC, Policy, Vendor, and Status. A single device is listed in the table:

| Name | IP address | MAC | Policy | Vendor | Status |
|------------|---------------------------|-------------------|--------|--------|--------|
| qa-rcpe-at | 192.168.1.30 (dynamic) | FA:16:3E:8F:95:50 | | | Online |

Fig. 16: Pin/Unpin devices

5.3 Usage Monitoring

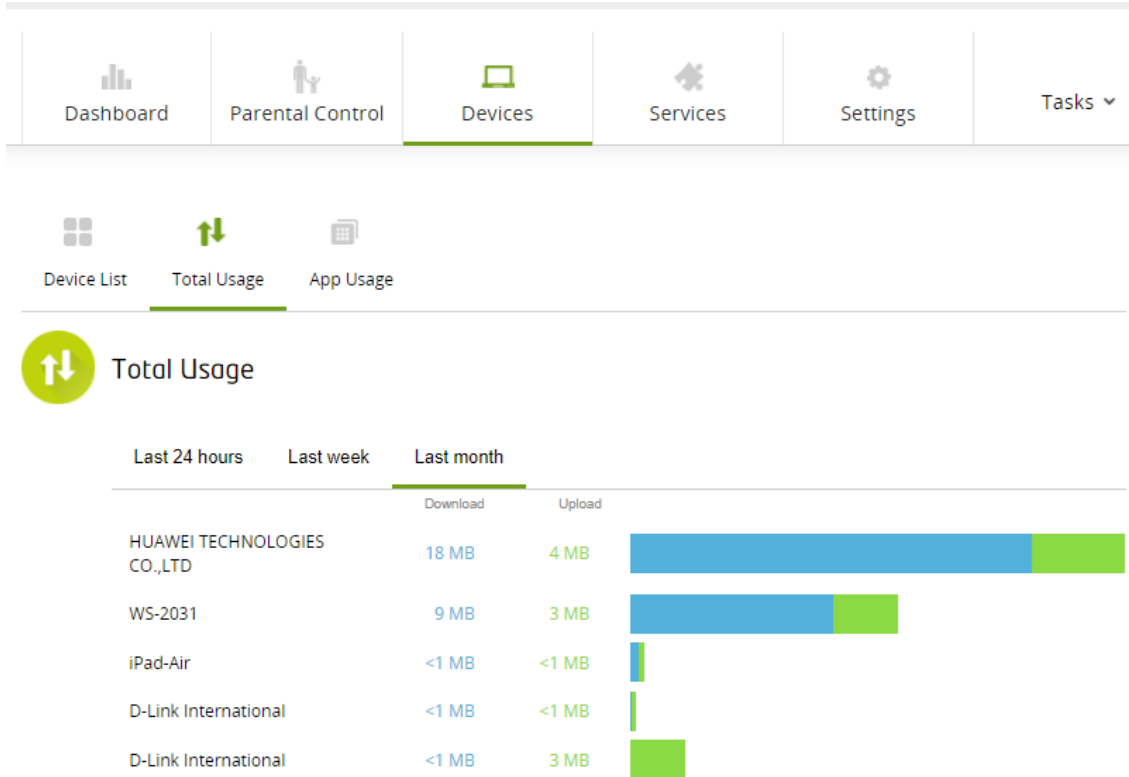
The **Total Usage** page displays traffic consumption statistics by device for a selected period. Both download and upload statistics are displayed in Megabytes. By default, 24h time period is selected. Subscribers are able to choose one of the following time periods for statistics:

- Last 24 hours
- Last week
- Last month

The devices table sorts by amount of consumed traffic and begins from the device with the biggest consumption.

The **Total Usage** page also displays a graphical representation of statistics using a bar chart:

Figure 2 Total usage view



5.4 App Usage

The **App Usage** page displays a report of traffic consumption per application for selected devices. Devices can be selected by enabling Track App Usage on the **Device List** page or **Modify Device** page.

The top 10 applications with the highest traffic consumption are displayed. All traffic from applications that were not covered in the top 10 are displayed as "OTHERS." If traffic was not recognized (for example, encrypted traffic), it will be marked as "UNKNOWN."

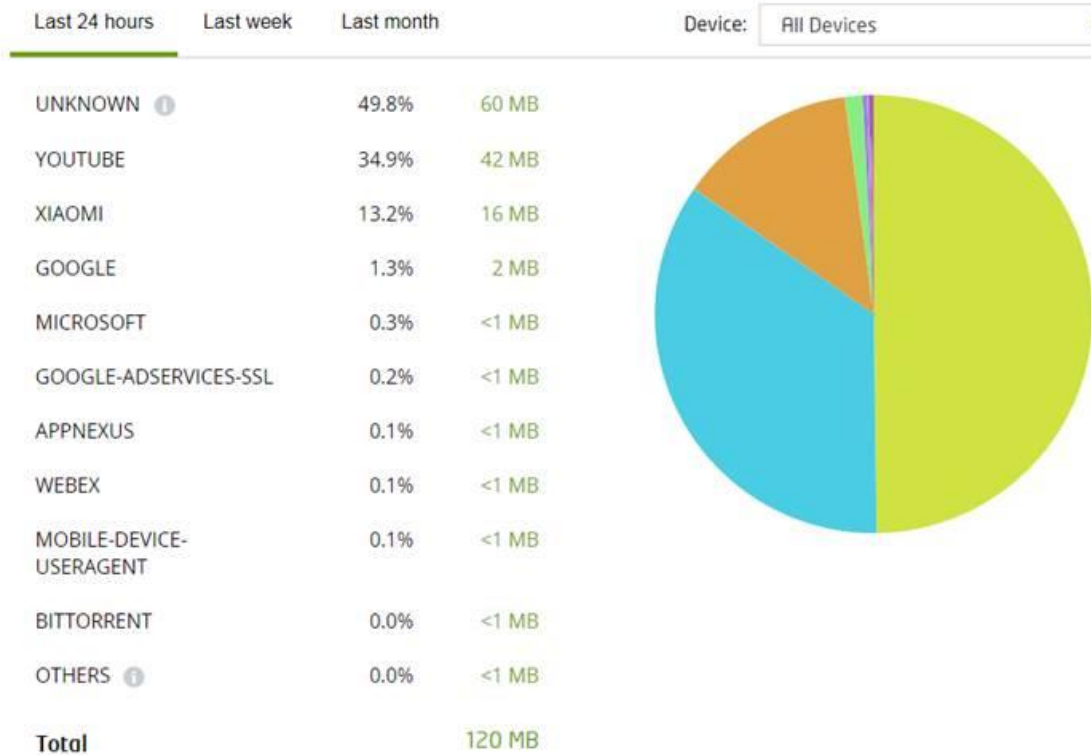
By default, the 24h time period is selected. Subscribers are able to choose one of following time periods for statistics:

- Last 24 hours
- Last week
- Last month

By default, the **App Usage** page displays reports for all selected devices. Subscribers are able to choose a particular device from the drop-down list.

The **App Usage** page also displays a graphical representation of the report using a pie chart:

Figure 3 Application usage view



5.5 Setting Up Firewall Rules

Firewall Rules enable subscribers to allow access to the existing port forwardings from particular external IP address(es).

To set up IPv4 firewall rules, the subscriber should perform the following steps:

1. Navigate to the **Network Security** page.
2. Select **Ip v4** (opens by default).
3. Click **Add Firewall Rule**.
4. Select one of the available values from the **Port Forwarding** drop-down menu.
5. Specify **Remote IP Address**, **Prefix Length** if you need to grant access to a pool of IP addresses, and **Remote Peer Port** if you want to specify the very port of the external device. Note that the "0" value provides access for all ports of the device within the specified pool of IP addresses.
6. Click **Apply Rule**.

Figure 4 Firewall Rules



Firewall rules

Ip v4 Ip v6

+ Add Firewall Rule

| Port Forwarding | Remote IP Address | Prefix Length | Remote Peer Port |
|-----------------|-------------------|---------------|------------------|
| 123test | 122.3.22.22 | 30 | 0 |

It's an online world and teenagers and children have unprecedented access to it. For a parent, the limit the time they spend online - all that chatting, gaming, social networking, shopping, and watch you protect them from potentially harmful and inappropriate material? [Settings Page](#)

Apply Rule Undo Rule

To set up IPv6 firewall rules, the subscriber should perform the following steps:

1. Navigate to the **Network Security** page.
2. Select **Ip v6**.
3. Click **Add Firewall Rule**.
4. Select one of the available values from the **Port Forwarding** drop-down menu
5. Specify **Filter Name, Internal IP and Internal Port, Protocol, Remote IP Address, Prefix Length** if you need to grant access to a pool of IP addresses, and **Remote Peer Port** if you want to specify the very port of the external device. Note that the "0" value provides access for all ports of the device within the specified pool of IP addresses.
6. Click **Apply Rule**.

Figure 5 Firewall rules



Firewall rules

Ip v4 Ip v6

+ Add Firewall Rule

| Filter Name | Internal IP | Internal Port | Protocol | Remote IP Address | Prefix Length | Remote Peer Port |
|-------------|------------------|---------------|----------|-------------------|---------------|------------------|
| DNS | 2001:8f8:0:6e::0 | 53 | TCP | 64:ff9b::96 | 1 | 53 |

Apply Rule Undo Rule

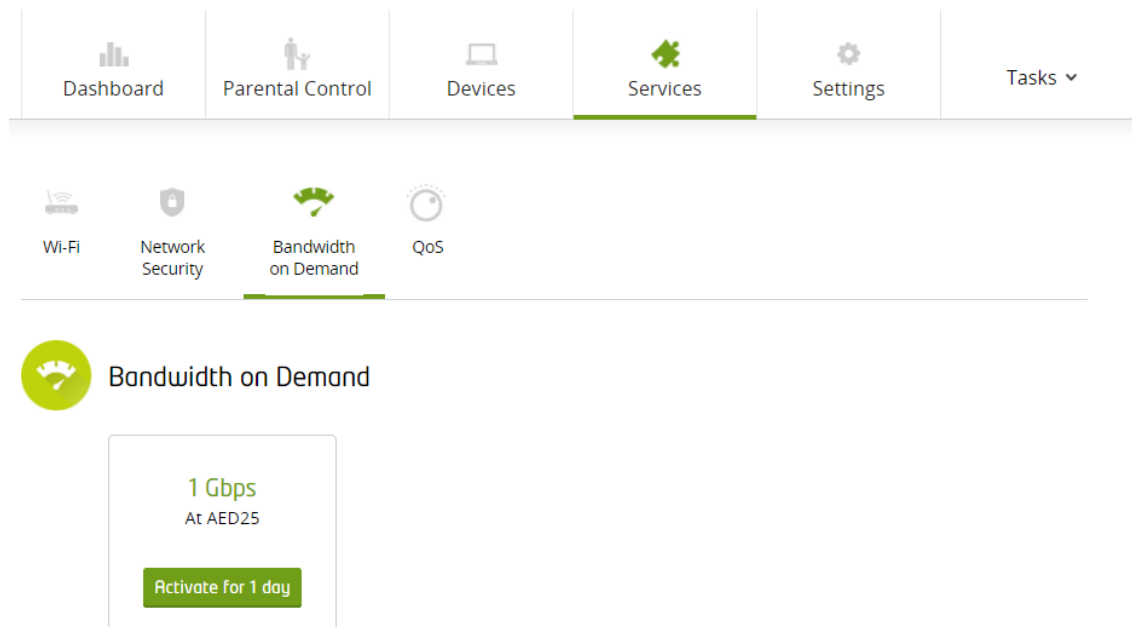
5.6 Bandwidth on Demand

To activate Bandwidth on Demand, the subscriber should perform the following steps:

1. Open the **Bandwidth on Demand** page on the **Service** tab.
2. Choose one of proposed Rate Plans and click **Activate for 1 day**.

Note: Proposed Rate Plan List depends on the current subscriber's tariff and eligibility check.

Figure 6 Bandwidth on demand view



5.7 Quality of Service (QoS)

To configure Quality of Service, the subscriber should perform the following steps:

1. Open the Services → QoS page.
2. Activate QoS using the toggle.
3. Select devices to include in the service.
4. Choose Application Group and Priority for the Group.
5. Create up to 20 rules by clicking the "**Add New**" button.
6. Click **Apply settings**.

The priority with which the application's traffic will be treated on network can be set from the Priority drop-down menu. The following priorities are available:

- Very High priority
- High priority
- Medium priority

- Low priority

Very High grants priority over all other traffic, Low grants lowest priority over all other traffic.

Note: At least one device should be selected for activation the service.

Figure 7 Quality of Service configuration view

Wi-Fi Network Security Bandwidth on Demand QoS

Quality of Service

QoS is inactive

Select Devices

WS-2031 iPad-Air ✓

QoS Settings

Application Group Priority Add New

No QoS classification rules, yet

Apply Settings Undo

6 Advanced Settings

The **Settings** tab gives access to settings for:

- Information (opens by default)
- DHCP v4
- DHCP v6
- Port Forwarding
- Dynamic DNS

Figure 8 Dynamic DNS configuration view

| IPv4 Configuration | | IPv6 Configuration | |
|-----------------------|------------------------------|-----------------------|----------------------|
| Gateway | 192.168.2.2 | DHCP IP Range | ::60 - ::fe |
| Subnet Mask | 255.255.255.0 | DNS Primary Address | 2001:4860:4860::8888 |
| DNS Primary Address | 8.8.8.8 | DNS Secondary Address | |
| DNS Secondary Address | | | |
| DHCP IP Range | 192.168.2.30 - 192.168.2.100 | | |
| Ports Mapped | 1 | | |
| Firewall rules | 1 | | |

6.1 Information Page

The **Information** section is read-only. Users can quickly review the summary of home network settings.

Figure 9 Information view

| IPv4 Configuration | | IPv6 Configuration | |
|-----------------------|------------------------------|-----------------------|----------------------|
| Gateway | 192.168.2.2 | DHCP IP Range | ::60 - ::fe |
| Subnet Mask | 255.255.255.0 | DNS Primary Address | 2001:4860:4860::8888 |
| DNS Primary Address | 8.8.8.8 | DNS Secondary Address | |
| DNS Secondary Address | | | |
| DHCP IP Range | 192.168.2.30 - 192.168.2.100 | | |
| Ports Mapped | 1 | | |
| Firewall rules | 1 | | |

6.2 DHCP v4


The **DHCP v4** section enables subscribers to modify IPv4 network configuration.


- **Default Gateway** and **Subnet Mask** are set automatically.
- **Host Address** shows the range used for allocating IP in the internal network.
- **Primary** and **Secondary DNS** are used to translate word-based address URLs to numerical IP addresses.


Subscribers must follow these rules:


- **Host Address Range** - Start and End IPv4 addresses must have the format XXX.XXX.XXX.XXX. The initial IP address in a range must be less than the end IP address
- **Primary DNS** must have the format XXX.XXX.XXX.XXX.
- **Secondary DNS** must have the format XXX.XXX.XXX.XXX.


Figure 10 DHCP configuration



Information


DHCP v4


DHCP v6


Port Forwarding


Dynamic DNS



DHCP v4 Configuration

| | |
|---|--|
| Default Gateway ⓘ | <input type="text" value="192.168.2.2"/> |
| Subnet Mask ⓘ | <input type="text" value="255.255.255.0"/> |
| Host Address Range* ⓘ | <input type="text" value="192.168.2.30"/> — <input type="text" value="192.168.2.100"/> |
| Primary DNS* ⓘ | <input type="text" value="8.8.8.8"/> |
| Secondary DNS ⓘ | <input type="text" value="8.8.4.4"/> |

Apply Settings

Undo

6.3 DHCP v6

The **DHCP v6** section displays current v6 configuration in read-only mode.

[Figure 11 DHCP configuration](#)

Information DHCP v4 **DHCP v6** Port Forwarding Dynamic DNS

DHCP v6 Configuration

Start IP Address ⓘ ::60

End IP Address ⓘ ::fe

Primary DNS ⓘ 2001:4860:4860::8888

Secondary DNS ⓘ

Apply Settings Undo

6.4 Port Forwarding

Port forwarding settings disclose the external IP of the router to external requests from the Web. If a user wants to view their home security camera remotely, or if a home LAN has a server with data to be shared, e.g. music or gaming server, the **Port Forwarding** section enables:

- Switching **UPnP** "ON" or "OFF"
- Specifying **DMZ Host**
- Operating **Port Forwarding** rules

UPnP (Universal Plug & Play) is a set of network protocols for automatic configuration services enabling data sharing within the network.

DMZ Host directs all external requests to the LAN device, whose IP address the user specifies. Consider using proper safety software and settings on that device if you have any private data on it.

Port Forwarding makes particular internal IP available from an external network:

- **Global Port** – External communication port. Can be empty. The possible values are between 1-65535. External requests must know and have this port specified if a user sets it.
- **Private IP** – IP address from your LAN subnet 192.168.2.0/24. The address of LAN device disclosed for external requests.

- **Private Port** – Internal communication port. The possible values are between 1-65535. The port of the LAN device that responds when external requests knock on the **Global Port**.
- **Protocol** – Traffic protocol, TCP or UDP. Depends on the application on the LAN device.

6.4.1 Creating Port Forwarding

Port Forwarding is a useful feature whenever you want to share your local resources externally. It can have many uses, including gaming servers, music servers, remote desktops, and others. This example considers how to configure Port Forwarding for accessing a home security camera.

The first step of the configuration will be to navigate to the list of your home LAN devices on the **Devices** tab of SSP. Among other information, you need to copy the value of the **IP Address** parameter field and make sure that the Make Static check box is selected. Once this is done, navigate to the **Settings** tab, and follow these instructions:

1. In the **Port Forwarding** edit box, specify the proper name. It is better to use a name associated with the shared resource.
2. In the **Global Port** edit box, specify the external communication port.
3. In the **Private IP** edit box, paste the previously copied IP of the shared LAN device.
4. In the **Private Port** edit box, specify the port of the LAN device that will be open for external requests.
5. From the **Protocol** drop-down list box, select the TCP or UDP value according to the shared application. If you do not know the value for sure, we recommend you search for the information in the application's settings.
6. Click **Apply Settings**.

Once Port Forwarding is specified, you need to decide whether you want to share the device with all external requests, with some selected IP, or with an IP range. In this example, we assume that you will need to protect the home security camera from random viewers. To ensure this protection, you need to add a Firewall Rule for the created Port Forwarding. For information on Firewall Rules, see [Setting Up Firewall Rules](#).

Another good example of sharing your LAN devices can be a gaming server. If you have a separate server for any online game you can specify its Private IP in the **DMZ Host** edit box and it will become available for any Internet user. If you do so, please consider protecting ports that are not affiliated with the provides service and use proper safety software to protect the data from attacks.

6.5 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with DNS services. This way, you can access your device (such as your webcam or internal server) using a

domain name (for instance yourname.noip.me, where yourname is a name of your choice) that will never change, instead of using an IP address that changes each time you reconnect. At the moment, 2 service providers are supported:

- Dynect.net
- Noip.com

To **connect** to Dynamic DNS service providers, the subscriber should perform the following steps:

1. Before using the Dynamic DNS service, visit the Dynamic DNS service provider's website, and register a user account and a domain name.
2. In the Self-Service portal, navigate to the Dynamic DNS page (Settings → Dynamic DNS).
3. Choose Dynamic DNS Service Provider.
4. Enter Customer Name (DYNECT case only), User Name, and Password.
5. Click the **Connect** button.
6. When the connection establishes, the status will change to "Active," and the Customer Name field will be only in Read Only mode.

Figure 12 Dynamic DNS configuration view

The screenshot displays the 'Dynamic DNS configuration' page. At the top, a navigation bar includes icons for Information, DHCP v4, DHCP v6, Port Forwarding, and Dynamic DNS. The 'Dynamic DNS' section is highlighted with a green underline. Below this, a globe icon is followed by the title 'Dynamic DNS configuration'. There are two tabs: 'Dynect.net' (selected) and 'Noip.com'. Under 'Account settings', there is a form with three input fields: 'Customer Name', 'Account', and a password field (masked with dots). To the right of the password field is an 'Inactive' status indicator and a 'Connect' button. Below the form is the 'Active DynDns records' section, which has a table with a 'Host Name' column and an 'Add New' button. The table is currently empty, and a message 'You don't have any records at this time' is displayed below it. At the bottom of the page, there are 'Apply Settings' and 'Undo' buttons.

To **create** a Dynamic DNS record, the subscriber should perform the following steps:

1. Connect to Dynamic DNS Service Provider.

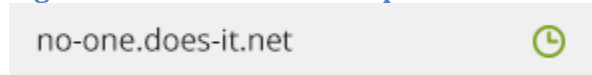
2. Fill in Host Name.Zone in the appropriate field (for instance, yourname.noip.me).
3. Click the **Add New** button. A new DynDNS record displays below the green icon.
4. Click the **Apply Changes** button.

To **delete** a Dynamic DNS record, the subscriber should perform the following steps:

1. Connect to Dynamic DNS Service Provider;
2. Hover the cursor over the DynDNS record. The record is highlighted, and has a **Delete** button on the left of the record.
3. Click the **Delete** button near the DynDNS record. The DynDNS record marks as strikethrough with the red icon.
4. Click the **Apply Changes** button.

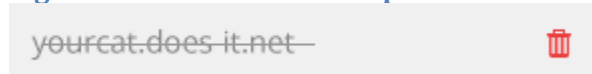
Record to be created:

Figure 13 Notification example



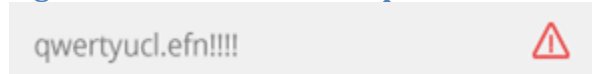
Record to be deleted:

Figure 14 Notification example



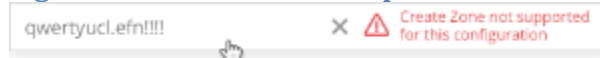
Record with creating/deleting error:

Figure 15 Notification example



Record with creating/deleting error hover:

Figure 16 Notification example



To **update** a password for connection to Dynamic DNS provider, the subscriber should perform the following steps:

1. Before using the Dynamic DNS service, visit the Dynamic DNS service provider's website, and register a user account and a domain name.
2. On the Dynamic DNS page in the Self-Service Portal, click the **Update** button. The button will be available instead of "Connect."
3. Enter the old account password and the new password in their respective fields.
4. Click **Update Password** button

Note: Password updating on all systems can take up to 15-20 minutes, so the subscriber may see credential errors during this time.