

# PARENTAL CONTROL SETUP GUIDE

NF20MESH FAQs



## Parental Control Setup Guide

The Parental Control feature allows you to take advanced measures to ensure the computers connected to the LAN are used only when and how you decide.

Make sure to activate the Internet Time server synchronization, so that the scheduled times match your local time.

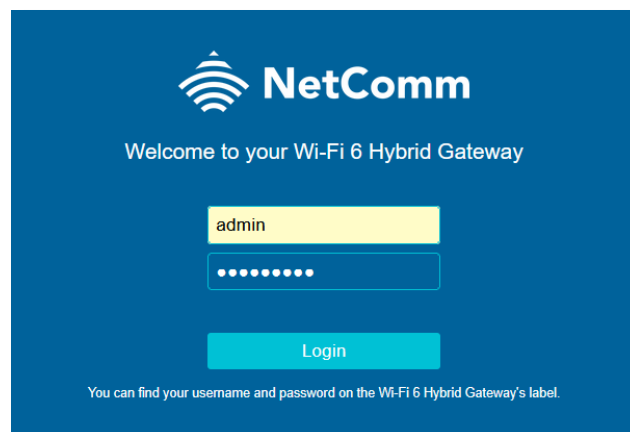
### Prerequisite: Internet Time server synchronization

1. Open a web browser (such as Internet Explorer, Google Chrome or Firefox), type following address into the address bar and press enter.

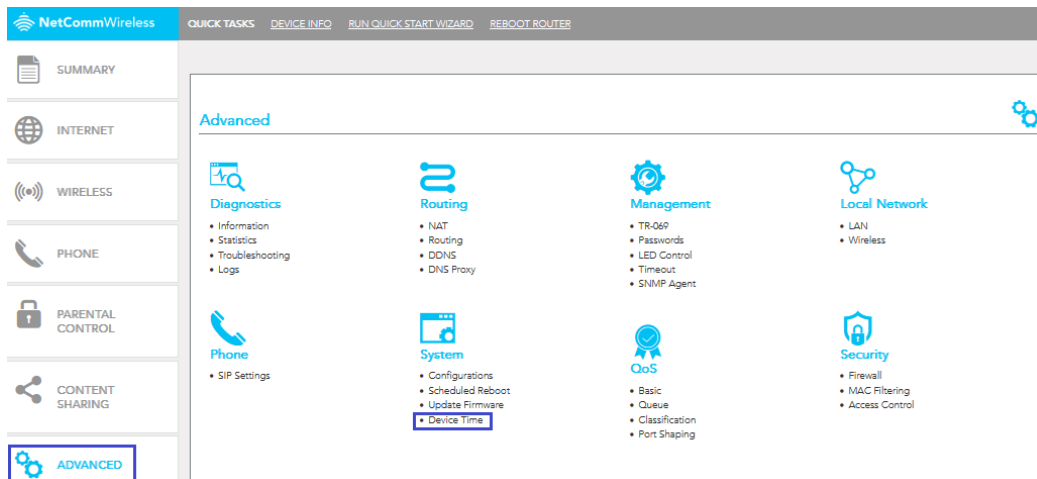
<http://192.168.20.1>

Type “**admin**” in the Username and password printed on the back of the modem in the Password field and click the **Login** button.

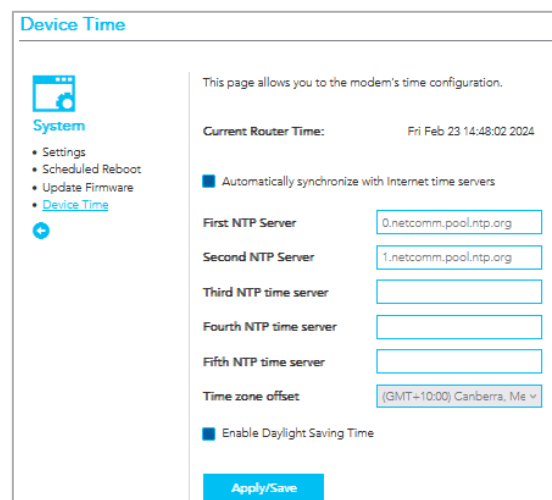
NOTE – Some Internet Service Providers use custom password. If login fails, contact your Internet Service Provider. Use your own password if it is changed.



2. Select the **ADVANCED** menu, then select the **Device Time** page.



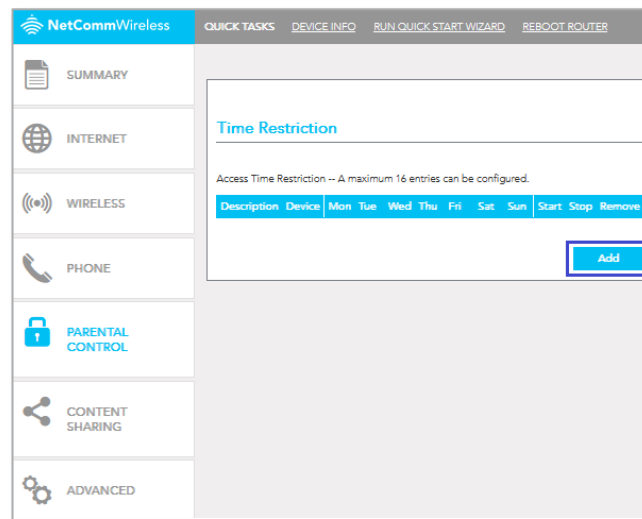
3. By default, NetComm NTP servers are configured as **First** and **Second NTP time server**.
4. Check and change “**Time zone offset**” and ☒ **Enable Daylight Saving Time**, if required.
5. Click Apply/Save.



## Time Restriction

This Parental Control function allows you to restrict internet access from a Local Area Network (LAN) connected on selected days and at certain times.

1. Navigate to **PARENTAL CONTROL**, under Time restriction, click on **Add** button to set schedule time.



2. Enter Description (write any description for your reference), select **Device** under the drop-down menu or select Manual Input and manually input MAC address of the device that you want to restrict. Then select Blocking time and select days and click **Apply/Save** button.

### Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Wi-Fi Hub. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

**Description:**

**Device:**

**Blocking Time:**  :  -  :

| Mon                      | Tue                      | Wed                      | Thu                      | Fri                      | Sat                                 | Sun                                 |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

**Apply/Save** **Close**

| Time Restriction                                                   |            |     |     |     |     |     |     |     |             |
|--------------------------------------------------------------------|------------|-----|-----|-----|-----|-----|-----|-----|-------------|
| Access Time Restriction -- A maximum 16 entries can be configured. |            |     |     |     |     |     |     |     |             |
| Description                                                        | Device     | Mon | Tue | Wed | Thu | Fri | Sat | Sun | Start Stop  |
| WeekendRestriction                                                 | NTCLT01745 | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | 00:00 23:00 |

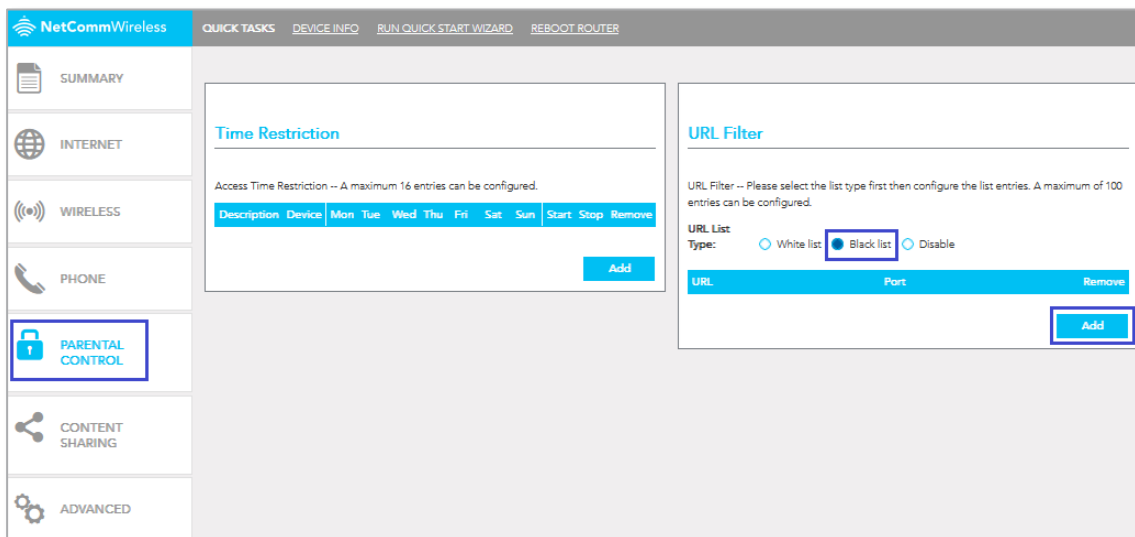
## Site Restrictions Block lists

With the URL Site Restrictions Block lists, you can add certain websites or URLs to a safe or blocked list. This will provide you added security to ensure any website you deem unsuitable will not be able to be seen by anyone who is accessing the Internet via the **NF20MESH**.

1. Navigate to **PARENTAL CONTROL**, under URL Filter select URL List Type as Blacklist, click on **Add** button to filter the URL.

**Whitelist:** If using a whitelist, users will only be able to access URLs which are on the list. All other URLs will be blocked.

**Blacklist:** If using a blacklist, then users will not be able to access the URLs on the list.



2. In the URL address field, enter the URL address of the address that should be filtered. In the Port Number field, enter the port that should be filtered. To filter HTTP traffic, enter port 80. To filter HTTPS traffic, enter port 443. If you are unsure, you should add both ports by adding a second URL filter. Click Apply/Save button.

### URL Filter Add

Enter the URL address and port number then click "Apply/Save" to add the entry to the URL filter.

URL Address:

Port Number:

### URL Filter Add

Enter the URL address and port number then click "Apply/Save" to add the entry to the URL filter.

URL Address:

Port Number: