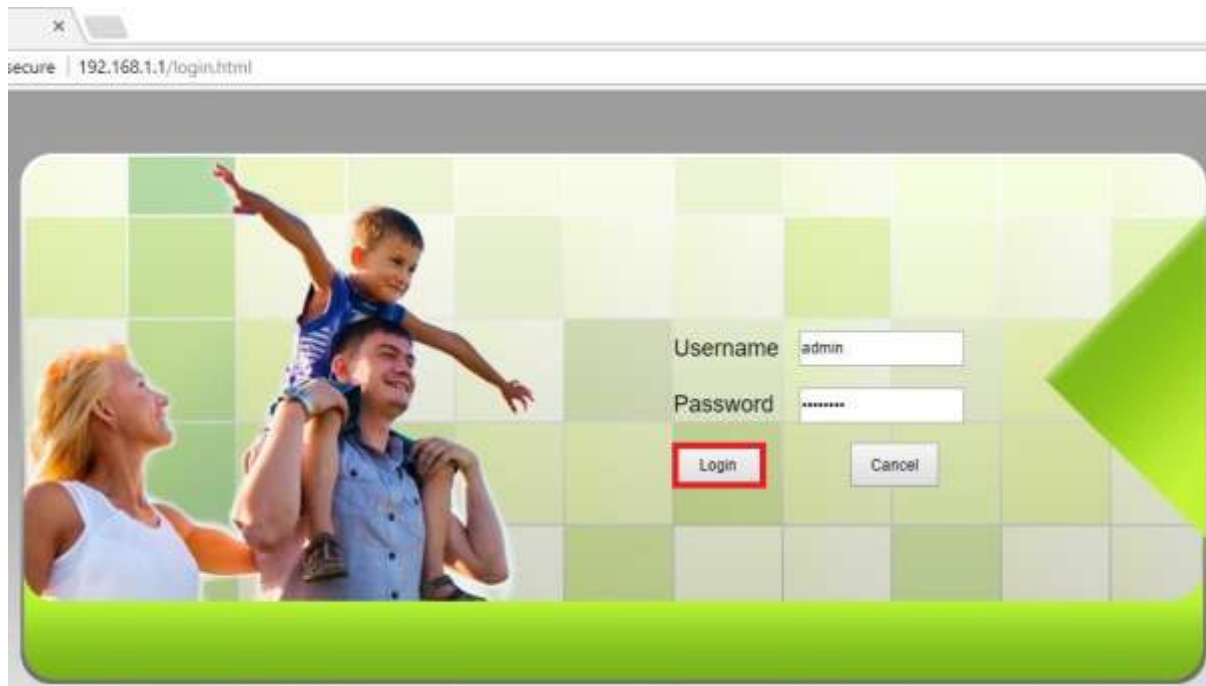


Block MAC address for FiberHome AN5506-04-CG

1. Open a browser e.g. Chrome and type **192.168.1.1** then press **Enter**

- Username = **admin**
- Password = **password**
- Press **Login**



2. It'll lead to **Status page**

secure | 192.168.1.1/login.html Logout

[Status](#) [Network](#) [Security](#) [Application](#) [Management](#)

Device Information Status » Device Information » Device Information

On this page, you can query device information.

Device Information	
Software Version	RP2601
Hardware Version	WKE2.134.285C3G
Device Model	AN5506-04-CG
Device Description	GPON
ONU State	O1(STATE_INIT)
ONU Regist State	INIT
LOID	fiberhome
CPU Usage	0.00%
Memory Usage	37.35%
Web Server port	80
CATV Enable	Enable
CATV Recived Power	-40.00dBm
CATV RF Power	-4.01dBmV

3. Go to Security > Firewall > MAC Filtering

- **MAC Filtering Enable** : choose **Enable**
- **MAC Filtering Blacklist /Whitelist** :
 - To **Block** choose **Black List**
 - To **Allow** choose **White List**
- Press **Apply**
- **MAC Address** : enter MAC Address of device to block as per the correct Format (ex. 00:24:21:19:BD:E4)
- **Start Time** : start time to block that MAC Address
- **End Time** : end time to block that MAC Address
- **Enable** : choose **Enable**
- Then press **Apply**

192.168.1.1/login.html

Logout

Status Network **Security** Application Management

Firewall Security » Firewall » MAC Filtering

If the firewall is enabled, the rules take effect, then the MAC Addresses matching the filter rules will be banned.

MAC Filtering Enable Enable Disable *
 MAC Filtering Blacklist/Whitelist White List Black List *

Add Delete Delete All

ID	MAC Address	Time	Enable

MAC Address 00:24:21:19:BD:E4 (You can input alphanumeric and ";", such as 00:24:21:19:BD:E4)
 Start Time 0 : 0 (Hour:Min, 24)
 End Time 24 : 0 (Hour:Min, 24)
 Enable Enable ▾

Apply Cancel

4. When finished at MAC Address Filtering Table, it will show information

atus Network **Security** Application Management

Security » Firewall » MAC Filtering

If the firewall is enabled, the rules take effect, then the MAC Addresses matching the filter rules will be banned.

MAC Filtering Enable Enable Disable *

MAC Filtering Blacklist/Whitelist White List Black List *

Apply Cancel

Add Delete Delete All

MAC Address Filtering Table			
ID	MAC Address	Time	Enable
1	00:24:21:19:bd:e4	0:0-24:0	Enable <input type="checkbox"/>

MAC Address (You can input alphanumeric and ':', such as 00:24:21:19:BD:E4)

Start Time : (Hour:Min, 24)

End Time : (Hour:Min, 24)

Enable ▼

Apply Cancel