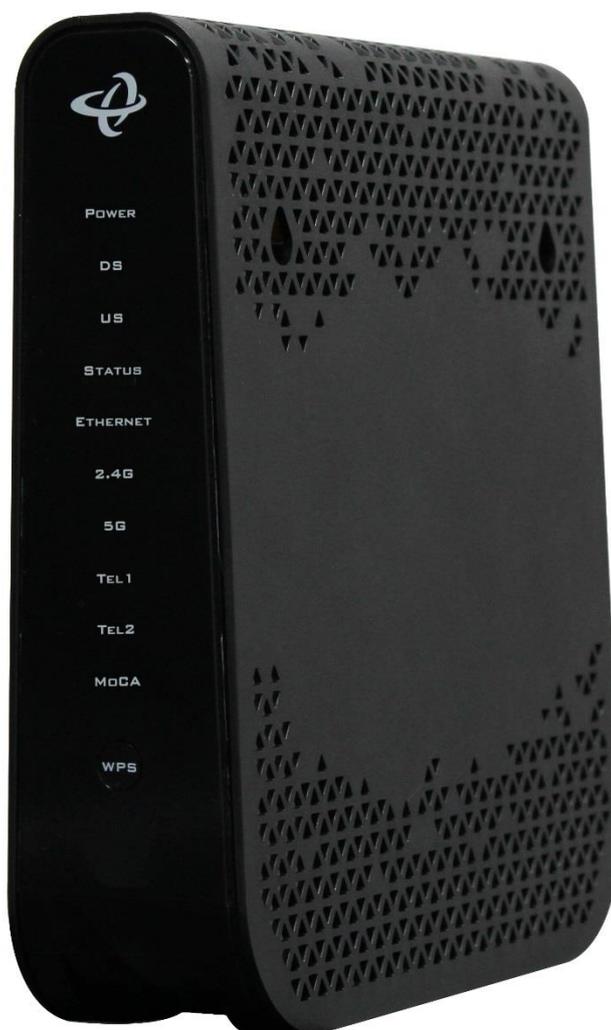


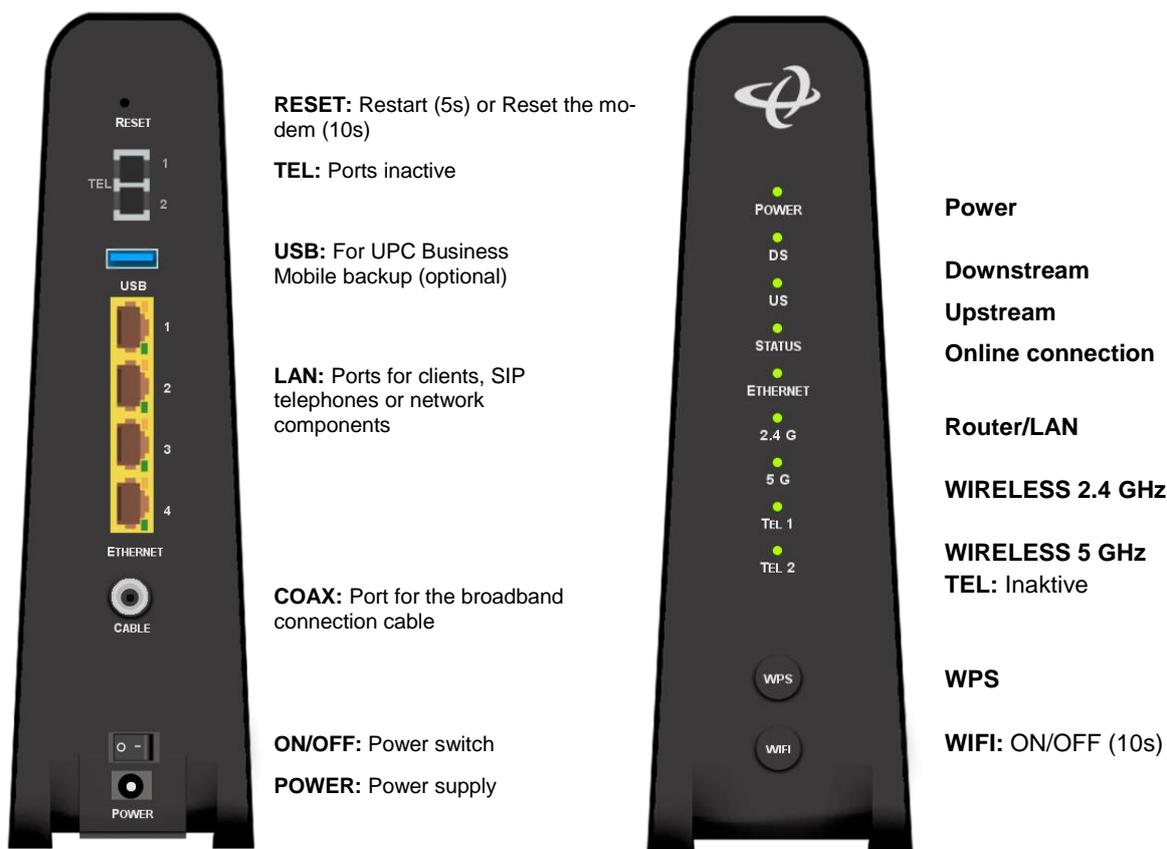
# UPC BUSINESS INTERNET DHCP CHITA MODEM



## Contents

<b>1</b>	<b>Ports and Displays .....</b>	<b>3</b>
1.1	LED Status.....	3
<b>2</b>	<b>Login: Modem .....</b>	<b>4</b>
<b>3</b>	<b>Status.....</b>	<b>4</b>
<b>4</b>	<b>Basic Settings.....</b>	<b>4</b>
4.1	LAN Setup .....	4
4.2	Gateway Function (Bridge).....	5
4.3	Port Forwarding .....	6
4.4	Port Triggering.....	7
4.5	DMZ.....	8
4.6	DNS .....	9
<b>5</b>	<b>WIRELESS .....</b>	<b>11</b>
5.1	Wifi Basic Settings.....	11
5.2	SSID Settings .....	12
5.3	WPS Connectivity.....	12
5.4	Guest Network .....	13
5.5	Access Control.....	14
5.6	ATF Air Time Fairness.....	15
<b>6</b>	<b>ADMIN .....</b>	<b>16</b>
6.1	Management.....	16
6.2	Diagnostics .....	16
6.3	Backup.....	17
6.4	Time Setting.....	17
6.5	Reset .....	17
<b>7</b>	<b>SECURITY.....</b>	<b>17</b>
7.1	Firewall .....	17
7.2	Port Blocking.....	18
7.3	Device Filter.....	21
7.4	Keyword Filter.....	23
7.1	DDNS.....	25

# 1 Ports and Displays



## 1.1 LED Status

LED	Status	Description
	Green – blinking	The modem is starting up. Searching for an upstream and downstream. (The process may take up to 30 minutes during the initial installation.)
	Blue – steady	The modem has located upstream and downstream channels.
	Green – blinking Green – steady	Establishing a connection to the internet. Connection to the internet has been made.
	Green – steady	There is a LAN connection.

## 2 Login: Modem

Internet Browser: 192.168.0.1  
 Username & Passwort from Modem

## 3 Status

**STATUS** GRUNDEINSTELLUNG WIRELESS ADMIN SICHERHEIT MOBIL

SYSTEM INFORMATION  
 DOCSIS-PROVISIONING  
 DOCSIS WAN  
 DOCSIS-EREIGNIS  
 WIRELESS  
 MTA

### STATUS

#### System information

HW-Version	1A
SW-Version	4.5.10.186-CD-E2-UPC
Seriennummer Schnittstelle	VBAP80043302
HFC MAC-Adresse	F8:1D:0F:2E:BE:80
Systemlaufzeit	Thu Jan 17, 2019, 12:55:48
System Up Time	00 Days,03 Hours,59 Minutes,24 Seconds
WAN IP	80.218.144.150/21
Private LAN IPv4 Subnet	192.168.0.1/24

## 4 Basic Settings

### 4.1 LAN Setup

The LAN setup section contains the IP address details that the gateway distributes to your local network or to the devices connected to your gateway.

**STATUS** **GRUNDEINSTELLUNG** WIRELESS ADMIN SICHERHEIT MOBIL

LAN-SETUP  
 GATEWAY-FUNKTION  
 PORT-WEITERLEITUNG  
 PORT-TRIGGERING  
 DMZ  
 DNS

### GRUNDEINSTELLUNGEN

#### LAN Settings

IP-Adresse:   
 Subnetzmaske:   
 DHCP-Status: **Aktiviert** Deaktiviert DHCP-Reservierung  
 Leasedauer:   
 Start IP-Adresse:   
 End IP-Adresse:

#### Connected Devices

Host-Name	IP-Adresse	MAC-Adresse	Type	Schnittstelle	Status
CHL000B726WZ1	192.168.0.10	EC:F4:BB:16:3B:7E	DHCP-IP	Ethernet	Active

**IP-Address:** The IP address is the LAN IP address of the gateway. Devices connected to your broadband service require DHCP IP addresses that belong to the same subnet as the private LAN IP address of your broadband service.

**Subnet mask:** This field defines the size of the LAN subnet used by the DHCP server of your services for private LAN addressing.

**Buttons for the activation/deactivation of LAN DHCP:** Use these buttons to activate/deactivate the DHCP server function for private LAN IP addresses. When the DHCP server is activated, LAN IP addresses and DNS information are assigned to the devices.

**DHCP reservation button:** Clicking this button opens a pop-up window in which IP addresses for specific devices can be permanently assigned.

**DHCP-Reservierung** ⊕

---

**Connected Devices**

Client Name	IP-Adresse	MAC-Adresse	Aktionen
CHL000B726WZ1	192.168.0.10	EC:F4:BB:16:3B:7E	<b>Hinzufügen</b>

---

**Manually Add Client**

Client Name	Reserved IP Address	MAC-Adresse	Aktionen
<input type="text" value="Client Name"/>	<input type="text" value="IP Address"/>	<input type="text" value="MAC Address"/>	<b>Hinzufügen</b>

---

**Reserved IP/MAC**

Client Name	Reserved IP Address	MAC-Adresse	Aktionen

Speichern
Schließen

**Lease time:** This is the IP lease time assigned by the LAN DHCP. The specification defines how long a certain IP address is reserved for a client. The client must report to the server again before then and apply for an "extension". If the client does not respond, the address will become free and can be re-assigned to another (or the same) client.

**DHCP Start IP** Displays the first available LAN IP address assigned by the LAN DHCP.

**DHCP End IP:** Displays the last available LAN IP address which is assigned by the LAN DHCP. The number of IP addresses between the DHCP start IP and the DHCP end IP determines the size of the DHCP IP address pool.

## 4.2 Gateway Function (Bridge)

Router mode is the standard mode. The Hitron router, firewall functions and wifi are available. Upon deactivation, the Hitron is set to the modem mode (bridge mode). This setting is necessary for the use of a personal router or firewall. Access to the modem interface is no longer possible in bridge mode. Resetting to the router mode is possible by resetting the modem.

STATUS **GRUNDEINSTELLUNG** WIRELESS ADMIN SICHERHEIT MOBIL

LAN-SETUP  
GATEWAY-FUNKTION  
PORT-WEITERLEITUNG  
PORT-TRIGGERING  
DMZ  
DNS

### GRUNDEINSTELLUNGEN

#### Capability

Router Function (disable for Modem Mode) Aktiviert Deaktiviert

UPnP IGD Aktiviert Deaktiviert

UPnP means Universal Plug and Play and refers to a standard by which a device in the LAN can automatically configure port forwarding in Hitron (and thus also affect the firewall!). Here you can define whether the Hitron allows UPnP or not.

### 4.3 Port Forwarding

Port forwarding is used to redirect incoming data traffic to the appropriate servers or specifically identified applications within your network.

STATUS **GRUNDEINSTELLUNG** WIRELESS ADMIN SICHERHEIT MOBIL

LAN-SETUP  
GATEWAY-FUNKTION  
**PORT-WEITERLEITUNG**  
PORT-TRIGGERING  
DMZ  
DNS

### GRUNDEINSTELLUNGEN

#### Port Forwarding Options

Port Forwarding Aktiviert Deaktiviert

Port Forwarding Rules

Nr.	Name	Public	Private	Protokoll	Local IP Address	Status
<span>Hinzufügen</span> <span>Bearbeiten</span> <span>Löschen</span>						
<span>Speichern</span> <span>Abbrechen</span> <span>Hilfe</span>						

Activated/deactivated: These buttons allow you to add/edit configurable details to the port forwarding table. Use the add/edit options to access a pop-up window where you can configure the rules for port forwarding in a table.

Add a rule for port forwarding service ↕

---

Port Forwarding Rule

Common Application	<input type="text" value="-SERVICES-"/>
Application Name	<input type="text" value="-SERVICES-"/>
Protokoll	<input type="text" value="TCP/UDP"/>
Public Port Range	<input type="text"/> ~ <input type="text"/>
Private Port Range	<input type="text"/> ~ <input type="text"/>
Local IP Address	<input type="text"/>

**Common Applications:** This function can be used to define rules that are specifically defined for common and well-known applications. The application can be made available via a drop-down menu. After selecting the application, the application name, protocol and public port range are automatically filled in.

**Protocol:** This field displays the internet protocol type which is used for the port forwarding rule. Examples of protocols are TCP, UDP, TCP/UDP, GRE and ESP.

**Public Port Range:** The public port range defines the ports that can be used to connect the LAN service you have created via port forwarding. The assignable ports are between 1 and 65535.

**Private Port Range** The private port range defines the port range on the device to which the rule routes traffic. The size of the private port range must match the size of the public port range and is automatically calculated for you.

**Local IP address:** This field displays the device to which data traffic is forwarded.

#### 4.4 Port Triggering

You can activate dynamic port forwarding for certain services/uses with port triggering. The modem monitors the outgoing data traffic on the ports specified in the trigger range. When activity is detected on these ports, the IP address of the device sending the data is stored and the incoming data traffic on the ports in the destination area is forwarded to this IP address on your network. The destination port area is opened so that the traffic released by the Internet can pass through the router's firewall during the time-out period.

Activated/deactivated: These buttons allow you to add/edit configurable details to the port triggering table.

**Port Triggering Add/Edit** ✚

---

**Port Triggering Rule**

Application Name	<input type="text"/>
Trigger Port Range	<input type="text"/> ~ <input type="text"/>
Target Port Range	<input type="text"/> ~ <input type="text"/>
Protokoll	Both <input type="button" value="v"/>
AllowAll	ON <input type="button" value="v"/>
Timeout (ms)	<input type="text"/>

**APPLICATION NAME:** This field is used to identify the port triggering rules.

**TRIGGER PORT RANGE:** This field displays the outbound port range with which this rule opens the destination port range for incoming traffic sessions.

**TARGET PORT RANGE:** This field displays the port to which incoming data traffic is forwarded on the local client PC.

**PROTOCOL:** This field displays the protocol used for this rule.

**TIMEOUT:** This field displays the value of the effective time for triggered and forwarded ports.

## 4.5 DMZ

DMZ (Demilitarized Zone) allows a selected device to bypass firewall functions and allows unrestricted access from the Internet. If a local client cannot properly run an Internet application behind a NAT firewall, that client can be set up with unrestricted bidirectional Internet access by setting the client up as a DMZ host.

Enabled/Disabled: This field can only be edited if "DMZ" is enabled.

- LAN-SETUP
- GATEWAY-FUNKTION
- PORT-WEITERLEITUNG
- PORT-TRIGGERING
- DMZ**
- DNS

## GRUNDEINSTELLUNGEN

### DMZ Settings

DMZ Aktiviert Deaktiviert

DMZ-Host  Connected Devices

Speichern
Abbrechen
Hilfe

**“CONNECTED DEVICES” BUTTON:** This button displays a pop-up window with the title "Connection Information". The connected devices in your network are shown in this window. Users can select the IP address of the connected devices in order to enter them in the "DMZ Host" field.

### Connected Devices

Host-Name	IP-Adresse	MAC-Adresse	Type	Schnittstelle	Status
CHL000B726WZ1	192.168.0.10	EC:F4:BB:16:3B:7E	DHCP-IP	Ethernet	Active

Schließen

Alternatively, you can manually enter an IP address, which must be located in the private LAN subnet of your network.

## 4.6 DNS

DNS (Domain Name System) is used to translate naming conventions for websites into numeric IP addresses. DNS information can be derived from the DNS server and provided directly to the end user device.

STATUS **GRUNDEINSTELLUNG** WIRELESS ADMIN SICHERHEIT MOBIL

LAN-SETUP  
GATEWAY-FUNKTION  
PORT-WEITERLEITUNG  
PORT-TRIGGERING  
DMZ  
**DNS**

### GRUNDEINSTELLUNGEN

#### LAN DNS Settings

LAN DNS Obtain  Automatisch  Manuell

LAN DNS Proxy  Aktiviert  Deaktiviert

Domain Suffix

Proxy Hostname1

Proxy Hostname2

**LAN DNS OBTAIN:** When the "Auto" button is selected and the LAN DNS Proxy is disabled, the DNS server address used by the router is automatically given. When the "Manual" button is selected, the DNS server addresses used by the router can be entered manually.

**LAN DNS PROXY:** When "enabled" is selected, your router acts as a DNS proxy server. This setting provides the router's private LAN IP address as the DNS server for the devices on the network. When "disabled" is selected, the router does not act as a DNS proxy server, and the addresses retrieved by the router are provided to devices on the network on the LAN DHCP.

**DOMAIN SUFFIX:** This field defines the domain name of the service. Devices in the network are provided on the LAN-DHCP. If the proxy host names are not defined, they are given a default domain suffix for accessing the Internet. A domain suffix consists of a sub-domain name and a top-level domain name separated by dots (e.g. myoffice.com).

**PROXY HOSTNAME1:** This field should contain the setting "Domain Suffix". End users can use this setting together with the domain suffix to form a fully qualified domain name (FQDN) to access the router's GUI for administration. For example, if this field is called "host1" and the domain suffix is "my-office.com", the FQDN for local web access is http://host1.myoffice.com.

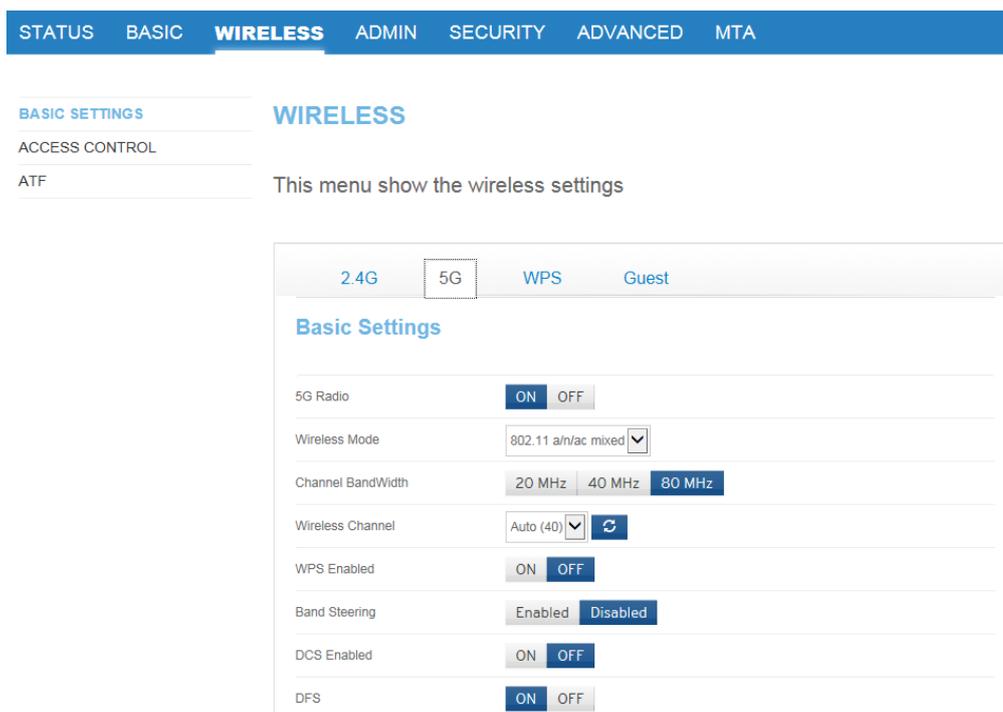
**PROXY HOSTNAME2:** This field should contain the setting "Domain Suffix". End users can use this setting together with the domain suffix to form a fully qualified domain name (FQDN) to access the router's GUI for administration. For example, if this field is called "host2" and the domain suffix is "my-office.com", the FQDN for local web access is http://host2.myoffice.com.

The hostname settings can only be used when the LAN DNS proxy setting is set to "enabled". If it is disabled, end users cannot define it and must use IP addresses to access the GUI.

## 5 WIRELESS

### 5.1 Wifi Basic Settings

Wifi is activated in the standard configuration. The login information is on the back of the modem. Use the on/off buttons to activate or deactivate the wireless network, or push the WIFI Button on the Modem Front.



**2.4G- and 5G tabs:** Change the tabs to select the frequency band which you would like to configure.

**Radio:** ON/OFF switch

**Wireless Mode:** Choose the standard your device supports. The default setting is "802.11b/g/n mixed" for the 2.4 GHz band and "802.11n/ac mixed" for the 5 GHz band.

**Channel Bandwidth:** The 2.4 GHz frequency supports 20 MHz and 20/40 MHz. 20/40 MHz is the default setting. The 5 GHz frequency supports 20 MHz, 40 MHz and 80 MHz. 80 MHz is the default setting.

**Wireless Channel:** Choose the wireless channel you want your device to use. When set to "Auto", your service scans the surroundings and selects the optimum available wireless channel. This setting is set to "Auto" by default. In the 5 GHz band, it can take up to ten minutes (depending on the channel) after selecting manually before the wireless network becomes visible.

**WPS Enabled:** general WPS ON/OFF switch

**Band Steering:** Band steering automatically connects your devices to the best available WiFi frequency – 2.4 GHz and 5 GHz – and ask you to choose between them when connecting a device to your network. When enabled you don't need to choose which frequency will best support your device – the modem does it automatically.

**DCS Enable:** Enable/disable DCS (Dynamic Channel Selection) support.

Dynamic Channel Selection is a feature that monitor noise levels on the channel and makes the gateway change to a clean channel automatically.

**DFS (DYNAMIC FREQUENCY SELECTION):** This function is only available for the 5 GHz band and is used to avoid interference. Use the On/Off buttons to enable or disable this setting. If DFS is switched off, the transmission power is reduced and the number of available channels is greatly reduced.

## 5.2 SSID Settings

### SSID Settings

**5G Primary SSID**

Network Name (SSID)

Enable 5G Network  ON  OFF

Broadcast SSID  ON  OFF

WMM(QoS)  ON  OFF

Security Mode

Auth Mode

Password

**Network Name (SSID):** Enter your SSID name here.

**Enable 2.4G Network:** Use the On/Off buttons to enable/disable the wifi network. If both 2.4G and 5G networks are disabled, the wifi is completely switched off.

**Broadcast SSID:** Use the On/Off buttons to make the transmission of a specific SSID visible/invisible. By selecting "Off" this SSID is not visible to other devices.

**WMM (QoS):** Wi-Fi Multimedia (WMM) is a wireless Quality of Service (QoS) feature that improves the quality of audio, video and voice applications by prioritizing wireless data traffic. The setup section contains the IP information that is distributed by the gateway to your local area network.

**Security Mode:** In the displayed table, you can select the type of wireless security you want to use. WIRELESS SECURITY MODE: The drop-down menu allows users to choose between "NONE", "WEP" and "WPA Personal". If NO-NE is selected, no security mechanism is applied, and any wireless client can connect to this AP. If you select «WEP» or «WPA-Personal», the corresponding table is displayed for further settings.

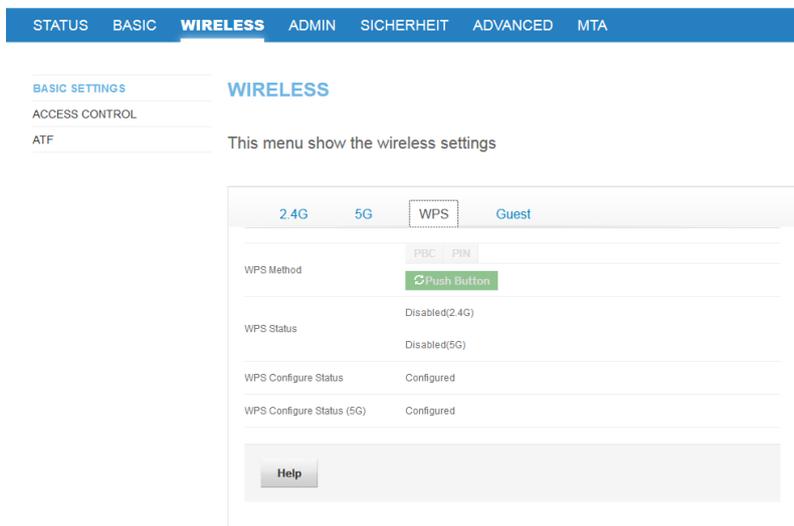
**Authentication:** Users can choose WPA-PSK (WPA Pre-Shared Key), WPA2-PSK or Auto (compatible with WPA-PSK and WPA2-PSK client).

**Password:** This is the password used by WPA / WPA2 encryption. The default password can be overwritten.

## 5.3 WPS Connectivity

For the WPS operation, the PBC (push-button Configuration) function will start using the WPS button (on the Modem Front or virtually). If it's pressed, the device would begin the WPS negotiation process with another wireless client which run PBC mode also.

If the PIN button is pressed, the device would pop-up a dialog box for users to fill in a 8-character PIN code for WPS negotiation. At the same time, the wireless client must use the same PIN code for WPS negotiation.



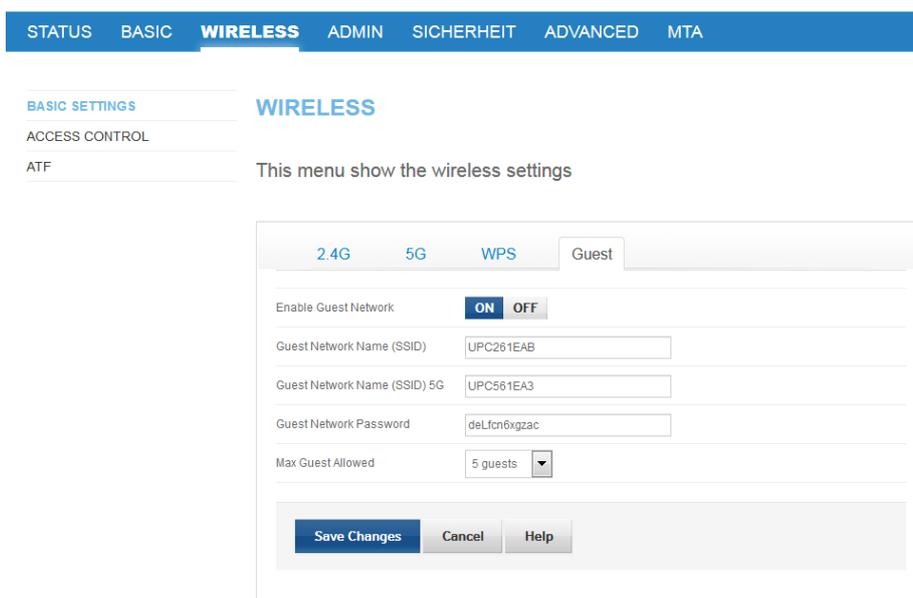
The screenshot shows the 'WIRELESS' settings page. On the left, there are tabs for 'BASIC SETTINGS', 'ACCESS CONTROL', and 'ATF'. The main content area is titled 'WIRELESS' and includes a sub-header 'This menu show the wireless settings'. Below this, there are tabs for '2.4G', '5G', 'WPS', and 'Guest'. The 'WPS' tab is active, showing a 'WPS Method' section with 'PBC' and 'PIN' options, where 'Push Button' is selected. Below this, 'WPS Status' is shown as 'Disabled(2.4G)' and 'Disabled(5G)'. 'WPS Configure Status' is 'Configured' for both bands. A 'Help' button is located at the bottom of the configuration area.

**WPS PBC:** Push Button Configuration.

**WPS Client PIN:** Enter the PIN generated from your client device.

## 5.4 Guest Network

Guest access allows visitors to connect to the Internet without accessing other computers or personal information. You can connect to your guest network, go online and surf the Internet. The guest LAN is a separate network.



The screenshot shows the 'WIRELESS' settings page with the 'Guest' tab selected. The 'Enable Guest Network' toggle is turned 'ON'. Below this, there are input fields for 'Guest Network Name (SSID)' with the value 'UPC261EAB', 'Guest Network Name (SSID) 5G' with the value 'UPC561EA3', and 'Guest Network Password' with the value 'deLfcn6xgzac'. The 'Max Guest Allowed' dropdown is set to '5 guests'. At the bottom, there are 'Save Changes', 'Cancel', and 'Help' buttons.

## 5.5 Access Control

In this section, you can specify which users and devices can access specific SSIDs.

STATUS
BASIC
WIRELESS
ADMIN
SICHERHEIT
ADVANCED
MTA

BASIC SETTINGS

ACCESS CONTROL

ATF

### WIRELESS

This menu show the wireless settings

#### Wireless Client Filter

You can block/allow the wireless access for specified devices here

Connected Devices
Refresh

Host Name	IP Address	MAC Address	Type	Interface	Status	Action
Galaxy-S9	192.168.0.77	6C:C7:EC:2E:E4:D3Static		WIFI-5G	Active	Manage
	null					

Managed Wireless Clients

Block Rules
Allow All
Allow Listed
Block Listed

Host Name	MAC Address	Action

Save Changes
Add Managed Device
Help

The "**Block Listed**" button allows certain devices to access the gateway. You can access the devices on this list via "**Allow Listed**". "**Allow All**" allows gateway access to all devices connected to the gateway.

Devices can be added to the rule table in two different ways:

The first method is to use the device's "**Manage**" button in the "**Connected Devices**" table. As soon as this button has been pressed, a pop-up window will appear with the following fields to be configured:

MAC address: This field is filled with the MAC addresses from the "**Connected Devices**" table.

#### Manage Device ✕

Host-Name

MAC-Adresse

Device Managed 
 JA
  NEIN

Übernehmen
Schließen

The second method is to click the "Add Managed Device" button. A pop-up window opens showing no information in the Host Name field and a predefined MAC address with "00: 00: 00: 00: 00: 00". End

users must enter the settings in these two fields manually. The other fields in this pop-up window can be configured in the same way as the first method above.

**Manage Device** ↕

---

Host-Name

---

MAC-Adresse

---

Device Managed  JA  NEIN

---

Press "Apply" to confirm or "Close" to ignore.

Users must return to the "Access Control" page and click "Save Changes" to activate the changes.

## 5.6 ATF Air Time Fairness

Air Time Fairness (ATF) focuses primarily on planning fairness for the transmission of access point (AP) traffic and the efficient use of wifi bandwidth. The algorithm does not deal with the transmission of frames from other clients.

STATUS
BASIC
WIRELESS
ADMIN
SICHERHEIT
ADVANCED
MTA

BASIC SETTINGS

ACCESS CONTROL

ATF

### WIRELESS

This menu show the wireless settings

2.4G

5G

#### Air Time Fairness

ATF Enable  Enabled  Disabled

---

ATF Policy  Restrict  Fair

---

SSID-based Airtime Allocation

---

**ATM algorithm type:** This parameter is used to disable the ATM algorithm or configure the type of ATM algorithm that must be used to apply Air Time Fairness. This parameter **must** have the following values: Disable, Global Fairness or Weighted Fairness.

**ATF Policy** controls two different scheduling algorithms that are mutually exclusive: restrict queuing and fair queuing. Restrict queuing follows a strict send time allocation as configured by the user and does not attempt to use unused bandwidth. The "fair queue" algorithm, on the other hand, guarantees configured transmission time in overloaded environments and also uses unused bandwidth.

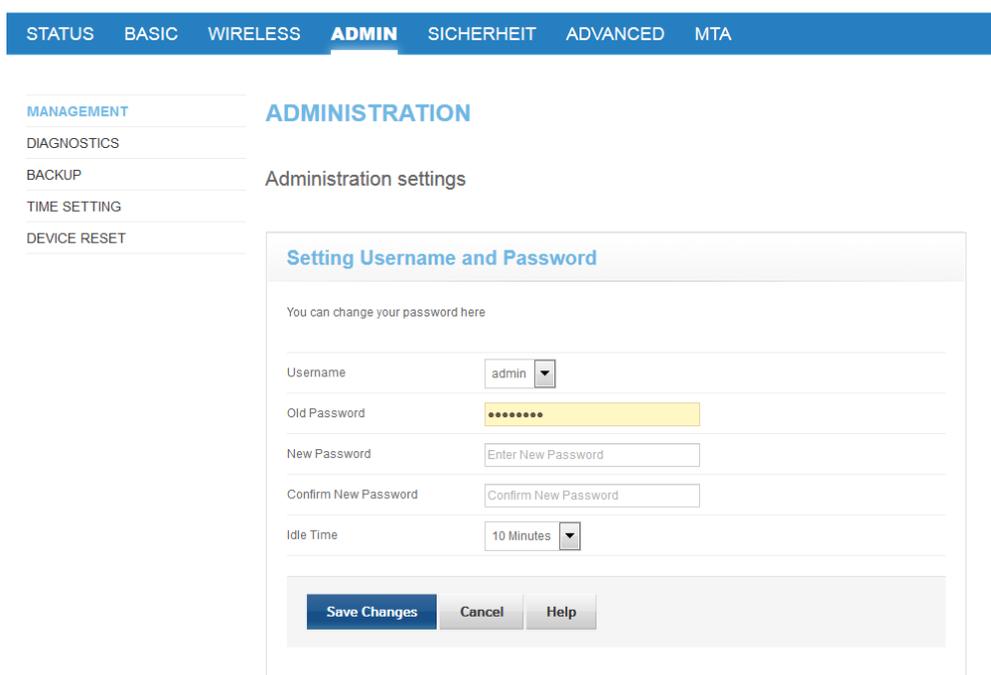
**SSID-based air time allocation:** This parameter configures the weighting for each SSID. The ATM weighting of an SSID must be a value between 5 and 100. When you press the "Delete" button, the Air Time percentage of this SSID becomes -1. This means that the Air Time percentage of this SSID is deleted. If you want to set a transmission time for an SSID, you must first press the Set button. If the SSID status is disabled, the transmission time of the SSID you specified is invalid.

**Allocation of transmission time per station:** This mechanism will primarily be used to ensure that STAs are allocated sufficient bandwidth to perform their respective tasks (video streaming, etc.). This parameter is used to define the weightings for the individual STAs. The transmission time of STAs connected to an SSID **must not** exceed 100%.

## 6 ADMIN

### 6.1 Management

Users can use this section to change their password to access the GUI. The settings for the username and the GUI Idle Timeout can only be changed by the user.



The screenshot shows the 'ADMIN' tab selected in the top navigation bar. On the left, a sidebar menu lists 'MANAGEMENT', 'DIAGNOSTICS', 'BACKUP', 'TIME SETTING', and 'DEVICE RESET'. The main content area is titled 'ADMINISTRATION' and 'Administration settings'. A form titled 'Setting Username and Password' is displayed, containing the following fields:

- Username: A dropdown menu with 'admin' selected.
- Old Password: A text input field with masked characters (dots).
- New Password: A text input field with the placeholder 'Enter New Password'.
- Confirm New Password: A text input field with the placeholder 'Confirm New Password'.
- Idle Time: A dropdown menu with '10 Minutes' selected.

At the bottom of the form, there are three buttons: 'Save Changes' (highlighted in blue), 'Cancel', and 'Help'.

### 6.2 Diagnostics

Ping or Traceroute for a connection check.

STATUS BASIC WIRELESS **ADMIN** SICHERHEIT ADVANCED MTA

MANAGEMENT  
**DIAGNOSTICS**  
BACKUP  
TIME SETTING  
DEVICE RESET

## ADMINISTRATION

### Administration settings

#### Diagnostics

You can diagnose your network with ping and traceroute here.

Destination (IP or domain)

Result

Ping \*8.8.8.8\*: 56 data bytes

4 packets transmitted, 4 packet(s) received, 0 packet(s) loss

round-trip min/avg/max = 8/10/12 ms

====Complete=====

### 6.3 Backup

Here the configurations of the Hitron modem can be stored locally. With the restore option, the saved state can be restored at any time.

### 6.4 Time Setting

On this page, users can choose between two time setting protocols, ToD and SNTP.

For each time setting log, users can select the time zone they are in.

The ToD protocol is selected by default based on the DOCSIS provisioning settings.

This page also contains the Daylight Saving Time function. When this feature is enabled, the service follows the Daylight Saving Time rule defined for each time zone so that users can adjust the time.

### 6.5 Reset

Restart the modem or reset to factory settings

## 7 SECURITY

### 7.1 Firewall

Users can define the firewall security level which is needed for their service. There are three pre-defined firewall levels. Maximum, standard and minimum. Users can define their own firewall rules with the user-defined setting.

FIREWALL

PORT BLOCKING

DEVICE FILTER

KEYWORD FILTER

## SECURITY

Firewall and parental control settings

IPv4
IPv6

### Firewall Settings

Allow user define firewall level by using the firewall controls listed below.  
Keep the default Minimum Security (Low) settings if you are unfamiliar with configuring firewall settings.

Firewall Level
Maximum
Typical
Minimum
Custom

**Minimum Security (Low):** Allow (LAN-to-WAN):All

No application or traffic is blocked.

**Blocked:**  
IDS enabled  
IDENT (port 113)

Ping From WAN
Allow
Deny

Save Changes
Cancel
Help

**MAXIMUM SECURITY:** From LAN to WAN, all applications including voice applications (e.g. GTalk, Skype) and P2P applications are blocked. This setting enables Internet surfing, e-mail services, VPN services, DNS services and iTunes services.

**TYPICAL SECURITY:** From LAN to WAN, P2P applications and ping to the gateway are blocked, but all traffic is allowed.

**MINIMUM SECURITY** No application or traffic is blocked from LAN to WAN. This is the standard configuration.

**USER-DEFINED SECURITY:** Frequently-used applications can be blocked by clicking the "Reject" button. All other services can be activated by default. To block a specific port, you can use the "Service Filter" option.

## 7.2 Port Blocking

Port Blocking is used to block certain outbound traffic that is directed from a computer on the internal network to a specific destination port or port range. In the list of trusted PCs, a PC entered in the list is excluded from the filtering defined in the service filter table.

- FIREWALL
- PORT BLOCKING**
- DEVICE FILTER
- KEYWORD FILTER

## SECURITY

Firewall and parental control settings

### Port Blocking

Service filtering is used to block certain outbound traffic which is destined to specific target port or port range from specific device in the internal network.

---

**Managed Services**

Filter Enabled:  Enabled  Disabled

Application Name	Protocol	Port Range	Managed Weekdays	Managed Time	Status	Manage	Action
<input type="button" value="Add Managed Service"/>							

---

**Trusted PC List**

Application Name	IP Address	Status	Manage	Action
<input type="button" value="Add Trusted Device"/> <input type="button" value="Save Changes"/> <input type="button" value="Help"/>				

This is how you configure the service filter rules:

Service filtering is used to block certain outbound traffic that is directed from a computer on the internal network to a specific destination port or port range. If the filter rule is enabled, users can press the "Add Managed Service" button to add a service filter rule. A pop-up window is displayed to work below the settings.

### Manage Service ✚

---

Application Name:

Protokoll:  ▼

Port-Range:  ~

Rule Status:  Aktiviert  Deaktiviert

Manage All Day:  JA  NEIN

---

Application name: The rule is specified in this field.

**Protocol:** Users can select the protocol (TCP, USP or TCP/UDP) for the filter rule.

**Port Range:** With this setting users can set-up the port range, which allows the setting from 1 to 65535.

**Rule Status:** In this field the specific rule is activated/deactivated.

**Manage All Day** This field will be used to control the time plan for how the rule is used. If you select the "YES" button, more control panels will be available for schedule management.

The additional setting used for planning, including the weekday setting and the start/end time setting.

**Managed Weekdays** If "Manage All Day" is set to "YES", this field will be shown. Users can select the days this rule should be used on. Saturdays and Sundays are included in the weekdays.

**Manage Time** This field is used to set the start time and the end time of the rule.

After you have set the above setting, click the "Apply" button to apply the setting to the Service Filter table, or press "Close" to ignore the setting. If you want to delete the rule, simply select the "Deactivated" button for the "Rule Status" field.

After returning to the Service Filter page, users still need to click "Save Changes" to make the setting effective.

How to configure a list of trusted PCs:

Users can click the "Add Trusted Device" button to add devices to the list. When you click the "Add Trusted Device" button, a pop-up window appears where users can make the settings as described below.



**Manage Trusted Device**

Host-Name

MAC-Adresse

Rule Status

**Host Name** The host name of the added device is given in this field.

**MAC address** This field contains the trusted PC's MAC address.

**Rule Status:** Users can activate/deactivate this rule using the "Activated"/"Deactivated" buttons.

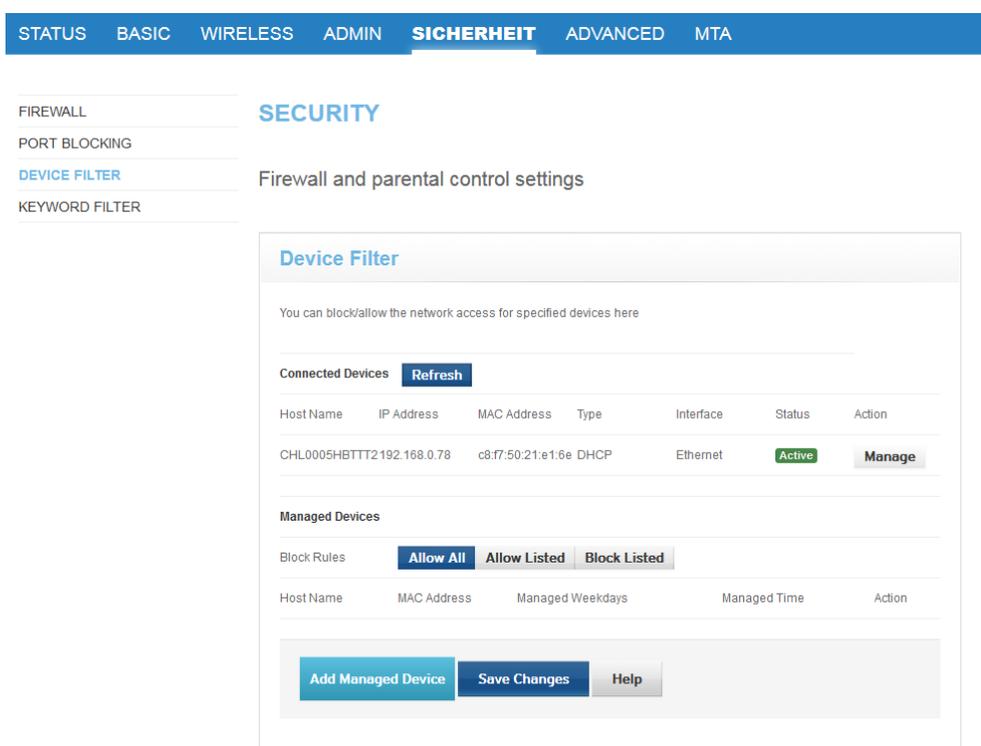
After you have set the above setting, click the “Apply” button to add the setting to the list of trusted PCs, or press “Close” to ignore the setting.

After returning to the service filter page, users still need to click "Save Changes" to activate the settings.

“Delete” button Deletes an existing rule from the list of trusted PCs.

### 7.3 Device Filter

The "Device filter" setting allows you to specify on which computers access to the Internet and your network may be blocked. Also, the setting can control blocking/allowing based on the schedule, which is defined by the rule.



The screenshot shows the 'SECURITY' section of the router's web interface, specifically the 'Device Filter' configuration page. The page title is 'Device Filter' and it includes a sub-header 'You can block/allow the network access for specified devices here'. There are two main sections: 'Connected Devices' and 'Managed Devices'. The 'Connected Devices' section has a 'Refresh' button and a table with columns: Host Name, IP Address, MAC Address, Type, Interface, Status, and Action. One device is listed: CHL0005HBT2 192.168.0.78 with MAC c8:f7:50:21:e1:6e, Type DHCP, Interface Ethernet, and Status Active. The 'Managed Devices' section has 'Block Rules' with buttons for 'Allow All', 'Allow Listed', and 'Block Listed'. Below this is a table with columns: Host Name, MAC Address, Managed Weekdays, Managed Time, and Action. At the bottom, there are buttons for 'Add Managed Device', 'Save Changes', and 'Help'.

How to configure the device filter setting:

You can use the device filter to create a list of computers that are denied connection to the gateway via the LAN switch ports. All of the computers in the list cannot connect to your gateway if you click the “**Block Listed**” button and the access time meets the schedule set by the rule. Any computer specified in the list can connect to your gateway if you click the “**Allow Listed**” button and the access time meets the schedule set by the rule. After pressing the "**Allow All**" button, all computers, regardless of the settings in the rules table, can connect to the Gateway.

There are two different methods for inserting the PC into the rule table.

The first is to press the "Manage" button of the learned PC in the "Connected Devices" table. After you click the Manage button, a pop-up window appears with the following field:

**Manage Device** ↕

---

Host-Name

---

MAC-Adresse

---

Device Managed

---

Manage All Day

---

**MAC address** This field is filled with the learned MAC addresses from the connected devices table.

**Manage Device** If you press the "YES" button here, the line "Manage all day" is created. If the "NO" button is pressed and the "Apply" button is also pressed, the rule in the device filter table is deleted.

**Manage All Day** The default setting is "YES". This means that the rule is applied seven days a week and 24 hours a day. If you press the "NO" button, the "Managed Weekdays" and "Time" lines are displayed and the user can set the schedule for the rule.

**Manage Device** ↕

---

Host-Name

---

MAC-Adresse

---

Device Managed

---

Manage All Day

---

Managed Weekdays

---

Managed Time From  :  To  :

---

**Managed Weekdays** Users can press any combination of the seven keys (Sunday to Saturday).

**Manage Time** Users can select the hours and minutes of the day for the schedule of the rule.

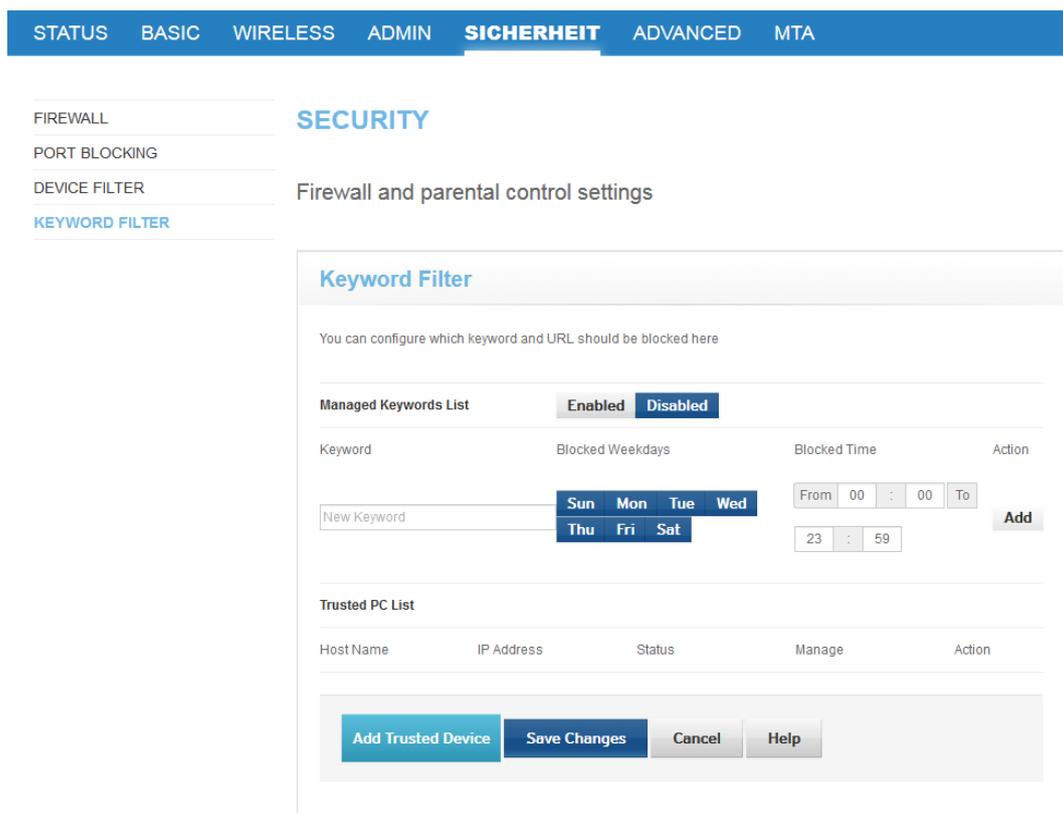
The second method is to click the "**Add Managed Device**" button. A pop-up window that allows you to add manually.

After you have specified the above setting, press the "**Apply**" button to apply the setting to the device filter table, or press "**Close**" to ignore the setting. If you want to delete the rule, simply select the "NO" button for the "Device managed" field.

After returning to the device filter page, users must click "Save Changes" for the settings to take place.

## 7.4 Keyword Filter

Users can configure which keyword should be locked when it is used in the URL. At the same time, users can set up a schedule to be used with the rule. If users want some computers to be excluded from keyword locking, this can be configured in the list of trusted PCs.



The screenshot shows the 'SECURITY' configuration page with the 'KEYWORD FILTER' tab selected. The page title is 'Keyword Filter' and it includes a sub-header 'Firewall and parental control settings'. The main content area contains a 'Managed Keywords List' section with an 'Enabled' button selected. Below this is a table for adding keywords with columns for 'Keyword', 'Blocked Weekdays', 'Blocked Time', and 'Action'. The 'Blocked Weekdays' section shows a calendar grid with 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', and 'Sat' buttons. The 'Blocked Time' section has a 'From' field set to '00:00' and a 'To' field set to '23:59'. An 'Add' button is present next to the time fields. Below the keyword list is a 'Trusted PC List' section with columns for 'Host Name', 'IP Address', 'Status', 'Manage', and 'Action'. At the bottom of the page, there are four buttons: 'Add Trusted Device', 'Save Changes', 'Cancel', and 'Help'.

This is how you configure the keyword filter:

If you want to specify one or more keywords, you must first click on the **"Enabled"** button. Then enter the keyword you want to block and select the time. Finally, click on the **"Add"** button. Users can repeat this procedure to add the keyword individually.

How to configure a list of trusted PCs:

Users can click the **"Add Trusted Device"** button to add devices to the list. When you click the **"Add Trusted Device"** button, a pop-up window appears where users can make the settings as described below.

**Manage Trusted Device** 

---

Host-Name

---

MAC-Adresse

---

Rule Status

---

**Hostname** This field specifies the hostname of the computer.

**MAC addresses** This field must be filled with the computer's MAC address which is excluded from keyword filter.

**Rule Status:** Users can activate/deactivate this rule using the "Activated"/"Deactivated" buttons.

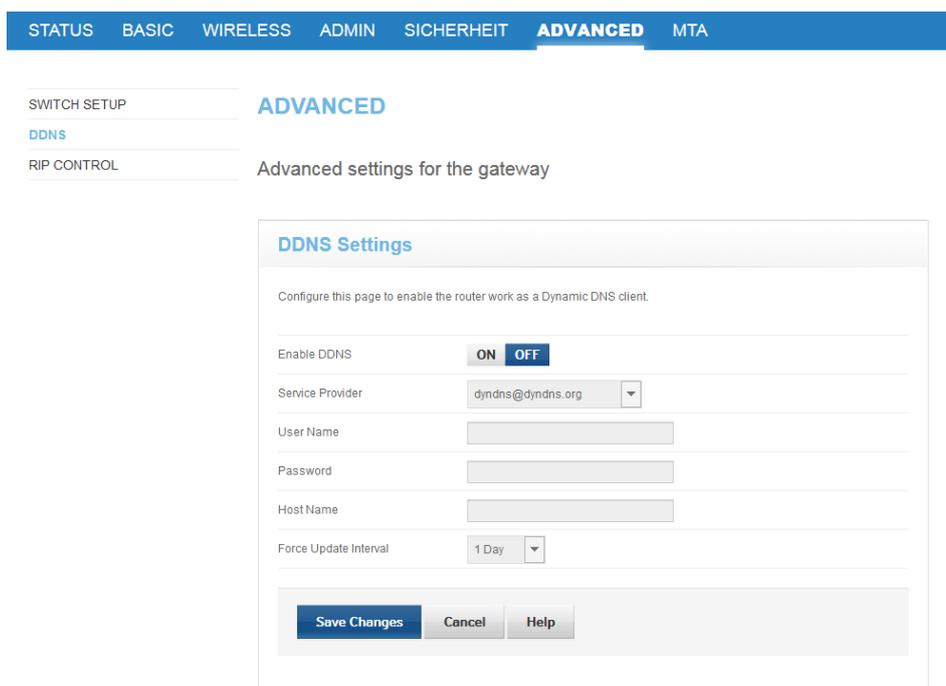
After you have made the above setting, click the "Apply" button to add the setting to the list of trusted PCs, or press "Close" to ignore the setting.

After returning to the keyword filter page, users still need to click "Save Changes" to activate the setting.

"Delete" button: Deletes an existing rule from the list of trusted PCs.

## 7.1 DDNS

Dynamic DNS or DDNS is a technique for dynamically updating domains in the Domain Name System (DNS). The purpose is that a computer (e.g. a PC or a router) automatically and quickly changes the associated domain entry after changing its IP address.



The screenshot shows a web interface for configuring DDNS. At the top, there is a navigation bar with tabs: STATUS, BASIC, WIRELESS, ADMIN, SICHERHEIT, **ADVANCED**, and MTA. Below the navigation bar, there is a sidebar with links: SWITCH SETUP, **DDNS**, and RIP CONTROL. The main content area is titled "ADVANCED" and "Advanced settings for the gateway". The "DDNS Settings" section is highlighted. It contains the following fields:

- Enable DDNS: A toggle switch currently set to "OFF".
- Service Provider: A drop-down menu currently showing "dyndns.dyndns.org".
- User Name: A text input field.
- Password: A text input field.
- Host Name: A text input field.
- Force Update Interval: A drop-down menu currently showing "1 Day".

At the bottom of the form, there are three buttons: "Save Changes", "Cancel", and "Help".

**DDNS** Use the on/off button to activate/deactivate the DDNS service. When the DDNS service is disabled, the remaining fields are not available for editing or configuring.

**SERVICE PROVIDER:** Users can select their DDNS service provider via the drop-down menu in this field.

**USER NAME:** User name for the DDNS service.

**PASSWORD:** Password for the DDNS service.

**HOST NAME:** Reserved host name for the DDNS service.