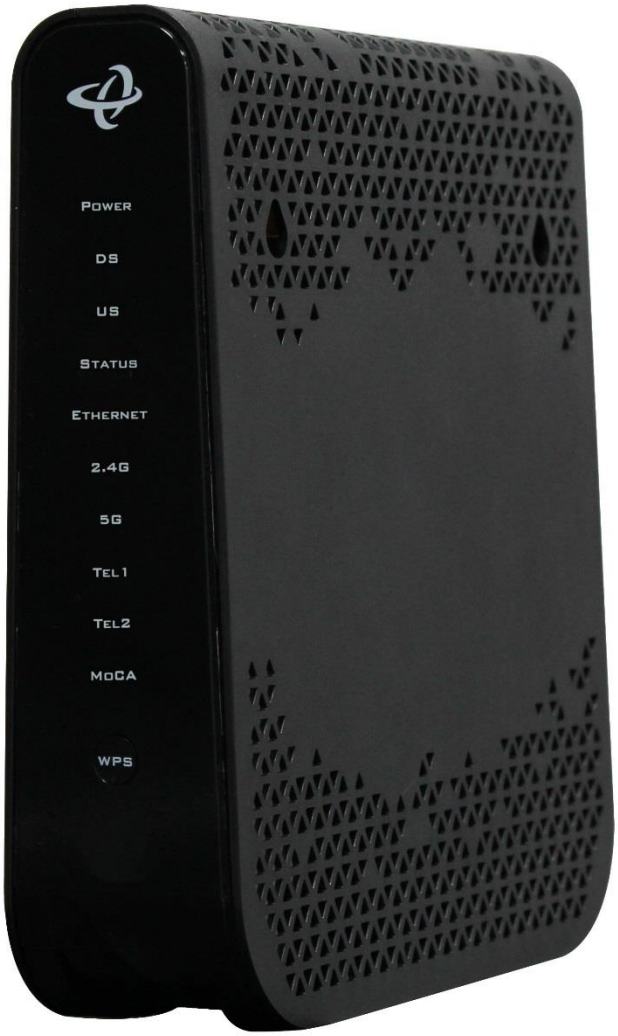
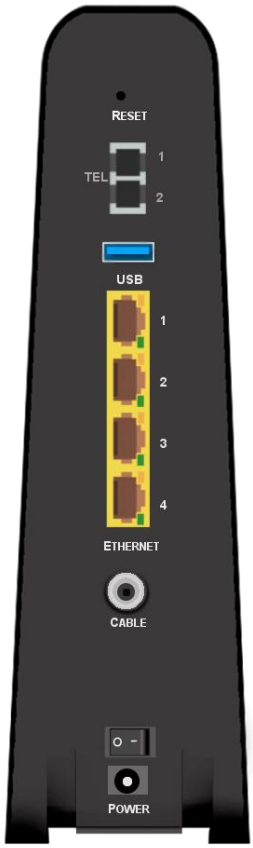
UPC BUSINESS INTERNET DHCP

CHITA MODEM



Inhaltsverzeichnis

1 Anschlüsse und Anzeigen



RESET: Reboot (5s) oder Reset (10s) des Modems

TEL: Anschlüsse inaktiv

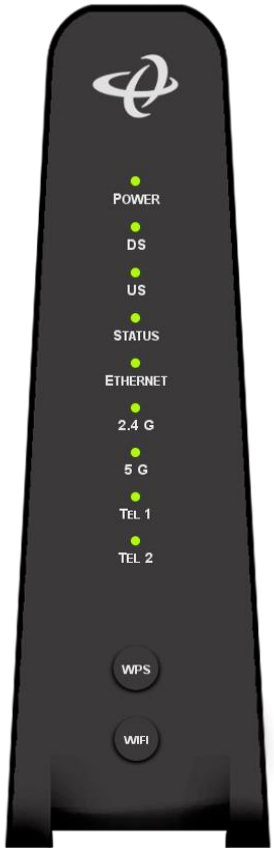
USB: Für UPC Business Mobile Backup (optional)

LAN: Anschlüsse für Clients, SIP-Telefone oder Netzwerk-komponenten

COAX: Anschluss für das Breitband-Anschlusskabel

ON/OFF: Power Schalter

POWER: Stromanschluss



Power

Downstream

Upstream

Online connection

Router/LAN

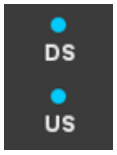
WIRELESS 2.4 GHz

WIRELESS 5 GHz

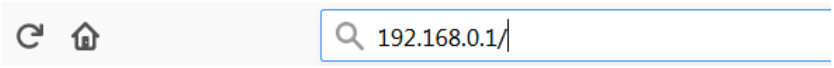
TEL: Inaktiv

WPS

WIFI: ON/OFF (10s)

LED	Status	Beschreibung
	Grün – blinkend	Das Modem befindet sich im Aufstartprozess. Upstream und Downstream werden gesucht. (Bei der Erstinstallation kann es bis zu 30 Minuten dauern.)
	Blau – statisch	Das Modem hat Upstream- und Downstream-Kanäle gefunden.
	Grün – blinkend Grün – statisch	Es wird versucht, eine Verbindung zum Internet aufzubauen. Verbindung zum Internet ist aufgebaut.
	Grün – statisch	Es besteht eine LAN-Verbindung.

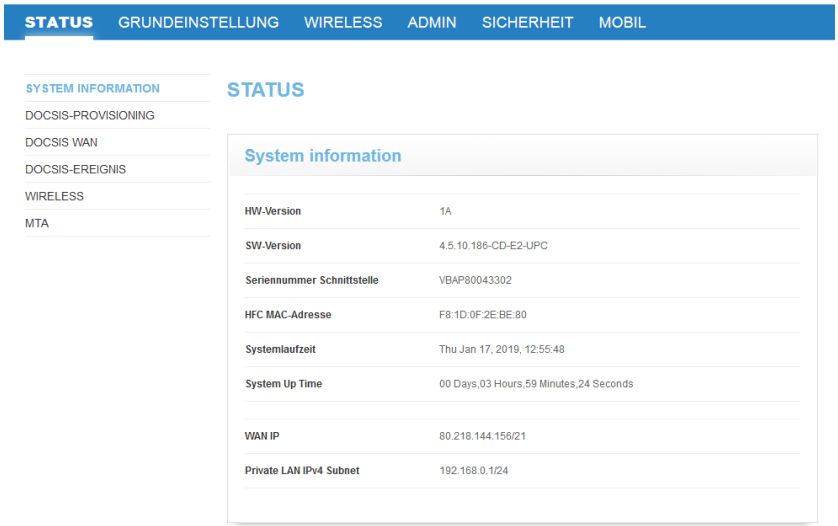
2 Login: Modem



Internet Browser: 192.168.0.1

Username & Passwort von Modem-Rückseite

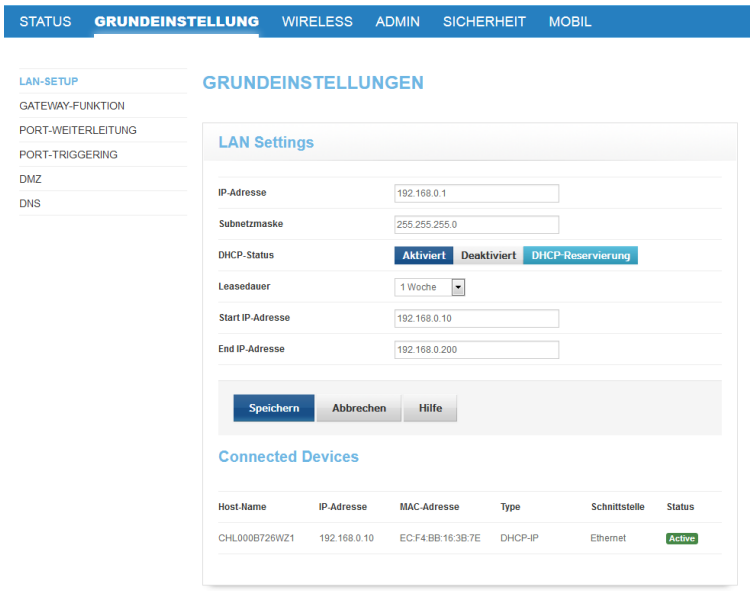
3 Status



4 Grundeinstellung

4.1 LAN-Setup

Der LAN-Setup-Abschnitt enthält die IP-Adressierungsinformationen, die das Gateway an Ihr lokales Netzwerk oder an die Geräte verteilt, die an Ihr Gateway angeschlossen sind.

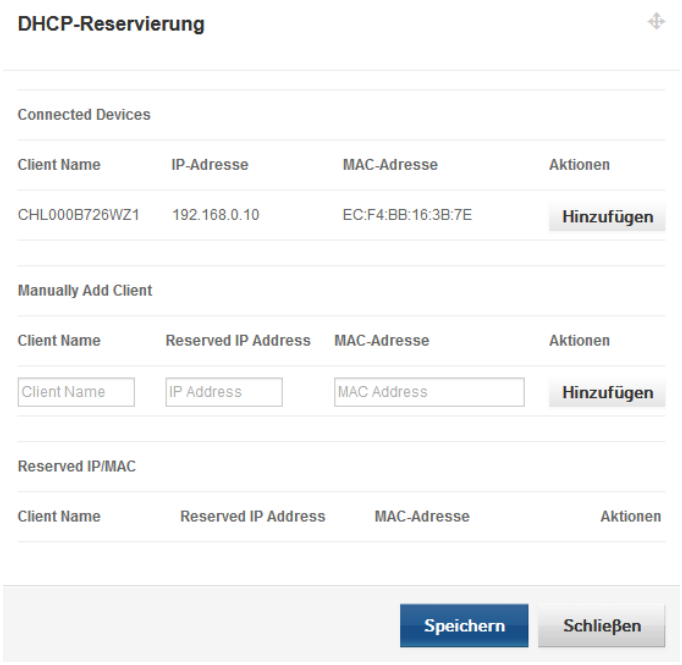


IP-Adresse: Die IP-Adresse ist die LAN-IP-Adresse des Gateways. Mit Ihrem Breitbanddienst verbundene Geräte benötigen DHCP-IP-Adressen, die zu demselben Subnetz wie die private LAN-IP-Adresse Ihres Breitbanddienstes gehören.

Subnetzmaske: Dieses Feld definiert die Grösse des LAN-Subnetzes, welches vom DHCP-Server Ihrer Dienste für die private LAN-Adressierung verwendet wird.

Schaltflächen zum Aktivieren/Deaktivieren von LAN-DHCP: Verwenden Sie diese Schaltflächen, um die DHCP-Serverfunktion für private LAN-IP-Adressen zu aktivieren/deaktivieren. Wenn der DHCP-Server aktiviert ist, werden den Geräten LAN-IP-Adressen und DNS-Informationen zugewiesen.

Schaltfläche für die DHCP-Reservierung: Durch Klicken auf diese Schaltfläche wird ein Pop-up-Fenster geöffnet, in dem IP-Adressen für bestimmte Geräte fix zugewiesen werden können.



Lease-Zeit: Dies ist die vom LAN-DHCP zugewiesene IP-Lease-Zeit. Die Angabe definiert, wie lange eine bestimmte IP-Adresse für einen Client reserviert ist. Bis dann muss sich der Client erneut beim Server melden und eine «Verlängerung» beantragen. Meldet er sich nicht, wird die Adresse frei und kann an einen anderen (oder auch denselben) Client neu vergeben werden.

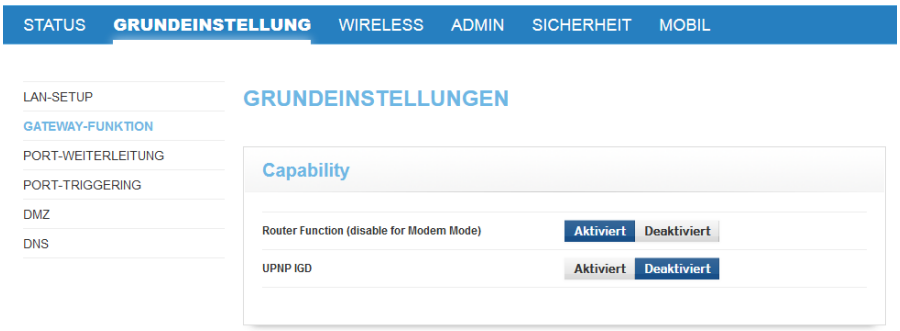
DHCP-Start-IP: Hier wird die erste verfügbare LAN-IP-Adresse definiert, die vom LAN-DHCP zugewiesen wird.

DHCP-End-IP: Definiert die letzte verfügbare LAN-IP-Adresse, die vom LAN-DHCP zugewiesen wird. Die Anzahl der IP-Adressen zwischen der DHCP-Start-IP und der DHCP-End-IP bestimmt die Grösse des DHCP-IP-Adresspools.

4.2 Gateway-Funktion (Bridge)

Router-Mode ist der Standardmodus. Router, Firewall-Funktionen und WiFi des Hitron sind verfügbar. Bei Deaktivierung befindet sich das Hitron im Modem-Modus (Bridge-Modus). Diese Einstellung ist bei der Verwendung eines eigenen Routers/Firewall notwendig. Im Bridge-Modus ist ein Zugriff auf das

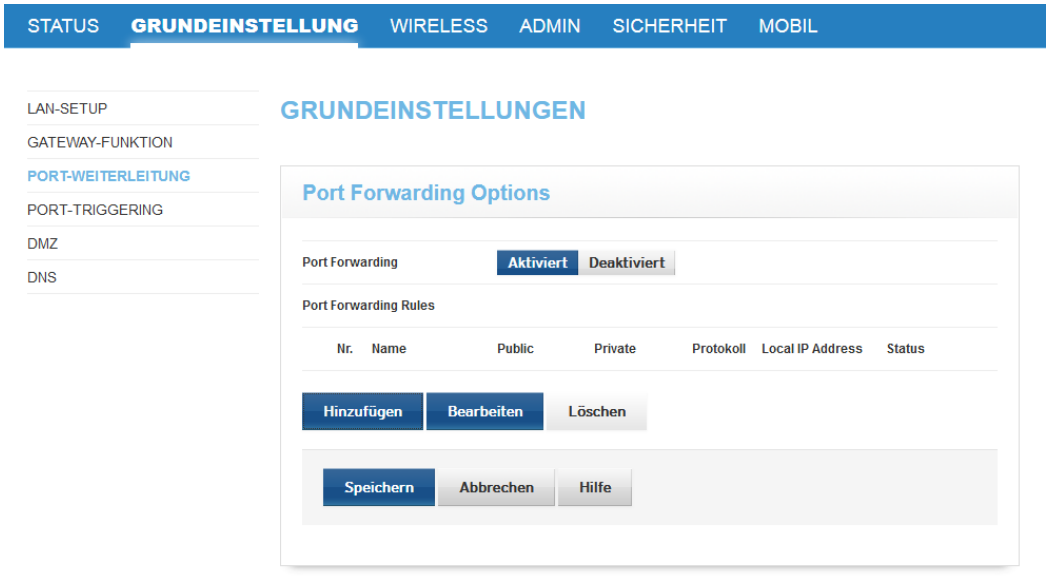
Modem-Interface nicht mehr möglich. Zurücksetzen in den Router-Modus ist durch Modem-Reset möglich.



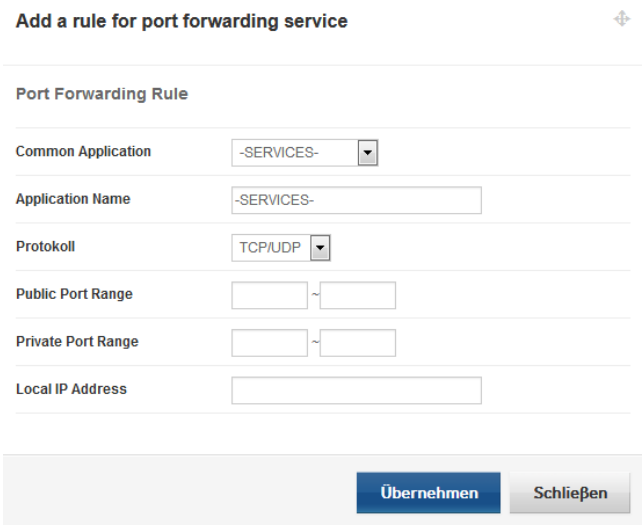
UPnP bedeutet Universal Plug and Play und bezeichnet einen Standard, über den ein Gerät im LAN automatisch Port-Weiterleitungen im Hitron konfigurieren kann (und damit auch die Firewall beeinflusst!). Hier wird definiert, ob das Hitron UPnP zulässt oder nicht.

4.3 Port-Weiterleitung

Die Port-Weiterleitung wird verwendet, um den eingehenden Datenverkehr an die entsprechenden Server oder spezifisch identifizierten Anwendungen innerhalb Ihres Netzwerks umzuleiten.



Aktiviert/Deaktiviert: Mit diesen Buttons können Sie konfigurierbare Details der Port-Forwarding-Tabelle hinzufügen/bearbeiten. Mit den Optionen zum Hinzufügen/Bearbeiten können Sie auf ein Pop-up-Fenster zugreifen, in dem Sie die Regeln für die Port-Weiterleitung in einer Tabelle konfigurieren können.



Common Applications: Für allgemeine und bekannte Anwendungen können über diese Funktion Regeln definiert werden, die speziell für sie definiert sind. Die Anwendung kann über ein Drop-down-Menü zur Verfügung gestellt werden. Nach Auswahl der Anwendung werden der Anwendungsname, das Protokoll und der öffentliche Port-Bereich automatisch ausgefüllt.

Protokoll: Dieses Feld definiert den Internetprotokolltyp, der für die Weiterleitungsregel verwendet wird. Die Beispiele für Protokolle sind TCP, UDP, TCP/UDP, GRE und ESP.

Public Port Range: Der öffentliche Port-Bereich definiert die Ports, die verwendet werden können, um den von Ihnen erstellten LAN-Service über die Port-Weiterleitung zu verbinden. Die zuweisbaren Ports liegen zwischen 1 und 65535.

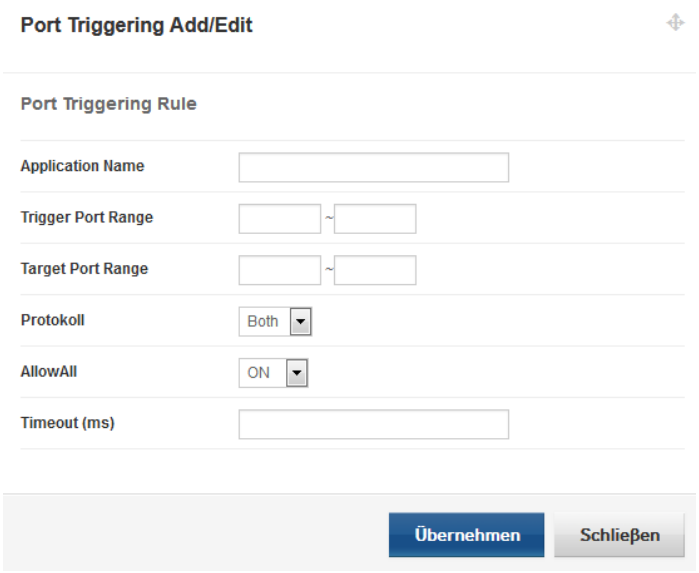
Private Port Range: Der private Port-Bereich definiert den Port-Bereich auf dem Gerät, an den die Regel den Verkehr weiterleitet. Die Grösse des privaten Port-Bereichs muss mit der Grösse des öffentlichen Port-Bereichs übereinstimmen und wird automatisch für Sie berechnet.

Local IP Address: Dieses Feld definiert das Gerät, an das der Datenverkehr weitergeleitet werden soll.

4.4 Port Triggering

Mit Port Triggering können Sie die dynamische Port-Weiterleitung für bestimmte Dienste/Anwendungen aktivieren. Das Modem überwacht den ausgehenden Datenverkehr an den im Auslösebereich angegebenen Ports. Wenn Aktivitäten an diesen Ports festgestellt werden, wird die IP-Adresse des Geräts, das die Daten sendet, gespeichert und der eingehende Datenverkehr an den Ports im Zielbereich an diese IP-Adresse in Ihrem Netzwerk weitergeleitet. Der Ziel-Port-Bereich wird geöffnet, damit der vom Internet ausgelöste Datenverkehr die Firewall des Routers innerhalb der Time-out-Zeit passieren kann.

Aktiviert/Deaktiviert: Mit diesen Buttons können Sie konfigurierbare Details der Port-Triggering-Tabelle hinzufügen/bearbeiten.



Application Name: Dieses Feld wird zur Identifizierung dieser Port-Auslöser-Regel verwendet.

Trigger Port Range: Dieses Feld definiert den ausgehenden Port-Bereich, durch den diese Regel den Ziel-Port-Bereich für eingehende Verkehrssitzungen öffnet.

Target Port Range: Dieses Feld definiert den Port, an den der eingehende Datenverkehr auf dem lokalen Client-PC weitergeleitet wird.

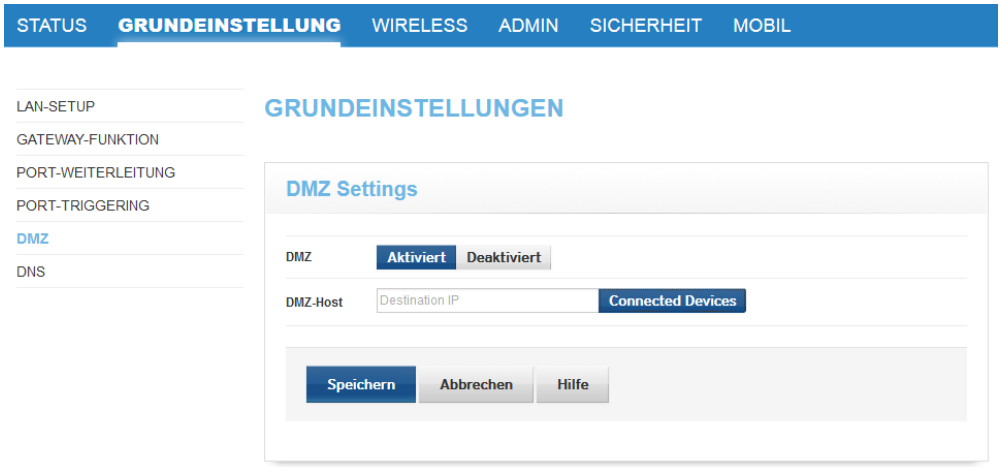
Protokoll: Dieses Feld definiert das für diese Regel verwendete Protokoll.

Timeout: Dieses Feld definiert den Wert der effektiven Zeit für ausgelöste und weitergeleitete Ports.

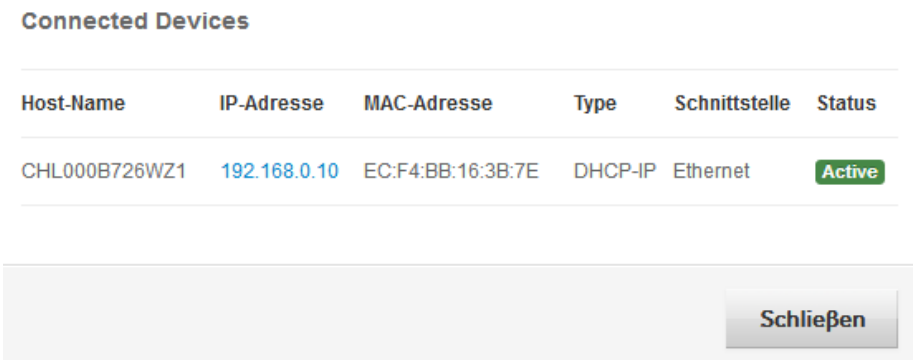
4.5 DMZ

DMZ (Demilitarized Zone) ermöglicht einem ausgewählten Gerät, Firewall-Funktionen zu umgehen, und erlaubt den uneingeschränkten Zugriff aus dem Internet. Wenn ein lokaler Client eine Internetanwendung nicht ordnungsgemäss hinter einer NAT-Firewall ausführen kann, kann dieser Client mit uneingeschränktem bidirektionalem Internetzugang eingerichtet werden, indem er als DMZ-Host eingerichtet wird.

Aktiviert/Deaktiviert: Das Feld kann nur bearbeitet werden, wenn «DMZ» aktiviert ist.



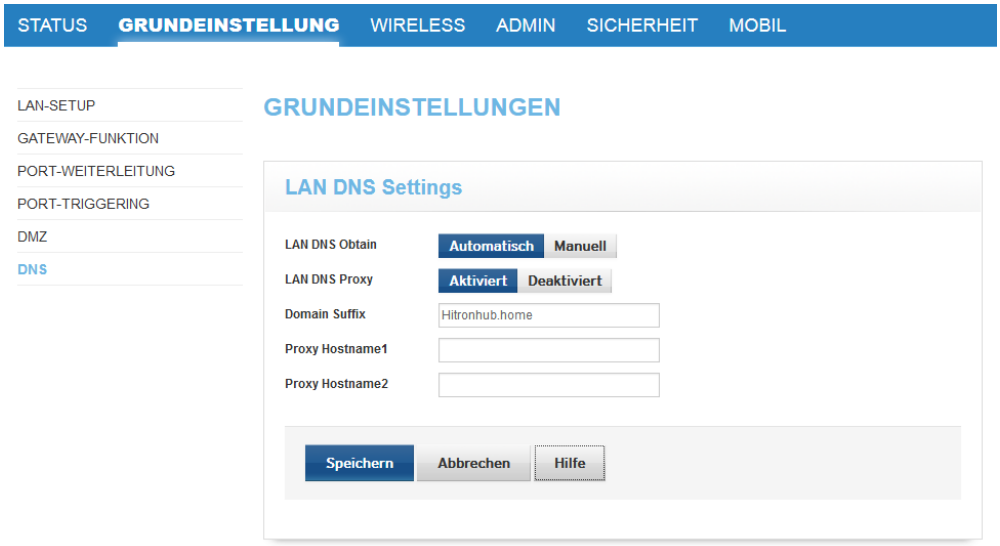
«Connected Devices»-TASTE: Mit dieser Schaltfläche wird ein Pop-up-Fenster mit dem Titel «Connection Information» (Verbindungsinformationen) angezeigt. In diesem Fenster werden die angeschlossenen Geräte in Ihrem Netzwerk angezeigt. Benutzer können die IP-Adresse der angeschlossenen Geräte auswählen, um sie in das Feld «DMZ-Host» einzutragen.



Alternativ können Sie manuell eine IP-Adresse eingeben, die sich im privaten LAN-Subnetz Ihres Netzwerks befinden muss.

4.6 DNS

DNS (Domain Name System) wird verwendet, um Namenskonventionen für Websites in numerische IP-Adressen zu übersetzen. DNS-Informationen können vom DNS-Server abgeleitet und direkt auf dem Endbenutzergerät bereitgestellt werden.



LAN DNS Obtain: Wenn die Schaltfläche «Automatisch» ausgewählt ist und der LAN DNS Proxy deaktiviert ist, wird die vom Router verwendete DNS-Server-Adresse automatisch ausgefüllt. Wenn die Schaltfläche «Manuell» ausgewählt ist, können die vom Router verwendeten DNS-Server-Adressen eingegeben werden.

LAN DNS Proxy: Wenn «Enabled» ausgewählt ist, fungiert Ihr Router als DNS-Proxyserver. Bei dieser Einstellung wird die private LAN-IP-Adresse des Routers als DNS-Server für die im Netzwerk befindlichen Geräte bereitgestellt. Wenn «Deaktiviert» ausgewählt ist, fungiert der Router nicht als DNS-Proxyserver, und die vom Router abgerufenen Adressen werden den Geräten im Netzwerk über das LAN-DHCP bereitgestellt.

Domain Suffix: Dieses Feld definiert den Domänennamen des Dienstes. Es wird Geräten im Netzwerk über LAN-DHCP bereitgestellt. Wenn die Proxy-Hostnamen nicht definiert wurden, erhalten sie ein Standard-Domänensuffix für den Zugriff auf das Internet. Ein Domain Suffix besteht aus einem Sub-Domain-Namen und einem Top-Level-Domain-Namen, getrennt durch Punkte (z.B. myoffice.com).

Proxy Hostname1: Dieses Feld sollte die Einstellung «Domain Suffix» enthalten. Endbenutzer können diese Einstellung zusammen mit dem Domänensuffix verwenden, um einen vollqualifizierten Domänennamen (FQDN) zu bilden, um auf die GUI des Routers für die Verwaltung zuzugreifen. Wenn dieses Feld beispielsweise «host1» heisst und das Domänensuffix «myoffice.com» ist, lautet der FQDN für den lokalen Webzugriff http://host1.myoffice.com.

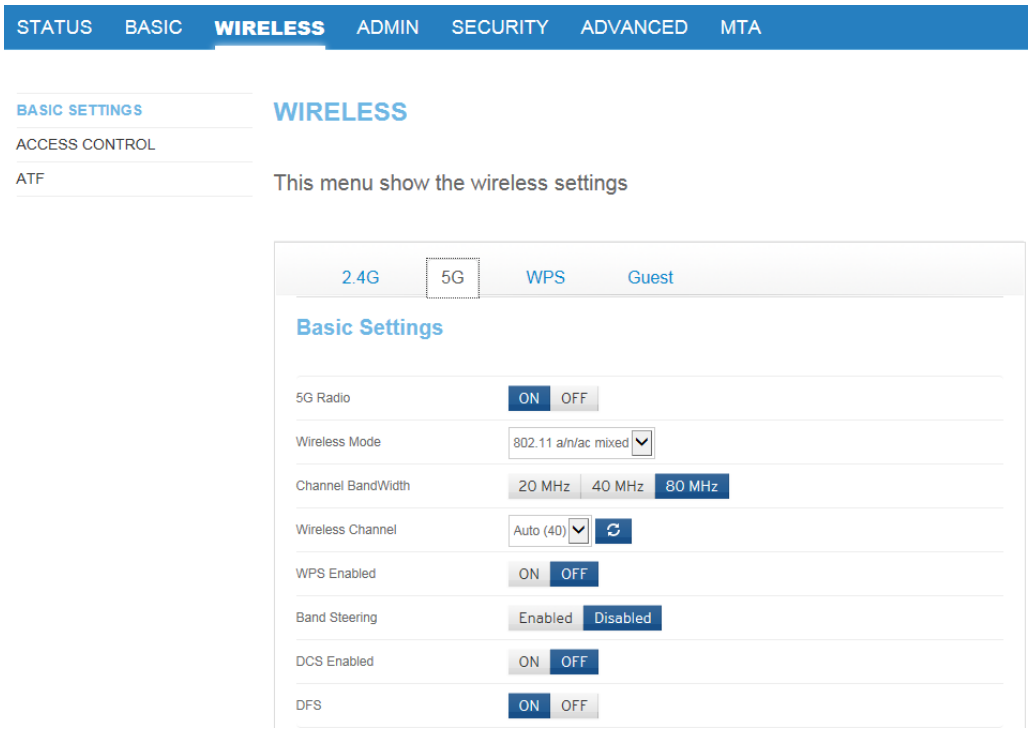
Proxy Hostname2: Dieses Feld sollte die Einstellung «Domain Suffix» enthalten. Endbenutzer können diese Einstellung zusammen mit dem Domänensuffix verwenden, um einen vollqualifizierten Domänennamen (FQDN) zu bilden, um auf die GUI des Routers für die Verwaltung zuzugreifen. Wenn dieses Feld beispielsweise «host2» heisst und das Domänensuffix «myoffice.com» ist, lautet der FQDN für den lokalen Webzugriff http://host2.myoffice.com.

Die Einstellungen für Hostnamen können nur verwendet werden, wenn die LAN-DNS-Proxy-Einstellung auf «Aktiviert» gesetzt ist. Wenn sie deaktiviert ist, können Endbenutzer diese nicht definieren und müssen IP-Adressen für den Zugriff auf die GUI verwenden.

5 WIRELESS

5.1 WiFi-Grundeinstellungen

Das WiFi ist in der Standardkonfiguration bereits aktiviert. Die Login-Informationen finden Sie auf der Rückseite des Modems. Verwenden Sie die An-/Aus-Tasten, um WLAN zu aktivieren oder zu deaktivieren.



2.4G- und 5G-Registerkarten: Wechseln Sie die Registerkarte, um das Frequenzband auszuwählen, das Sie konfigurieren möchten.

Wireless Mode: Wählen Sie den Standard, den Ihr Gerät unterstützt. Die Standardeinstellung ist «802.11b/g/n gemischt» für das 2,4-GHz-Band und «802.11n/ac gemischt» für das 5-GHz-Band.

Channel BandWidth: Für die 2,4-GHz-Frequenz werden 20 MHz und 20/40 MHz unterstützt. 20/40 MHz wird als Standardeinstellung verwendet. Für die 5-GHz-Frequenz werden 20 MHz, 40 MHz und 80 MHz unterstützt. 80 MHz wird als Standardeinstellung verwendet.

Wireless Channel: Wählen Sie den Funkkanal aus, den Ihr Gerät verwenden soll. Bei der Einstellung «Auto» scannt Ihr Dienst die Umgebung und wählt den besten verfügbaren WLAN-Kanal aus. Diese Einstellung ist standardmässig auf «Auto» eingestellt. Im 5-GHz-Band kann es (je nach Kanal) nach dem manuellen Auswählen bis zu zehn Minuten dauern, bis das WLAN sichtbar wird.

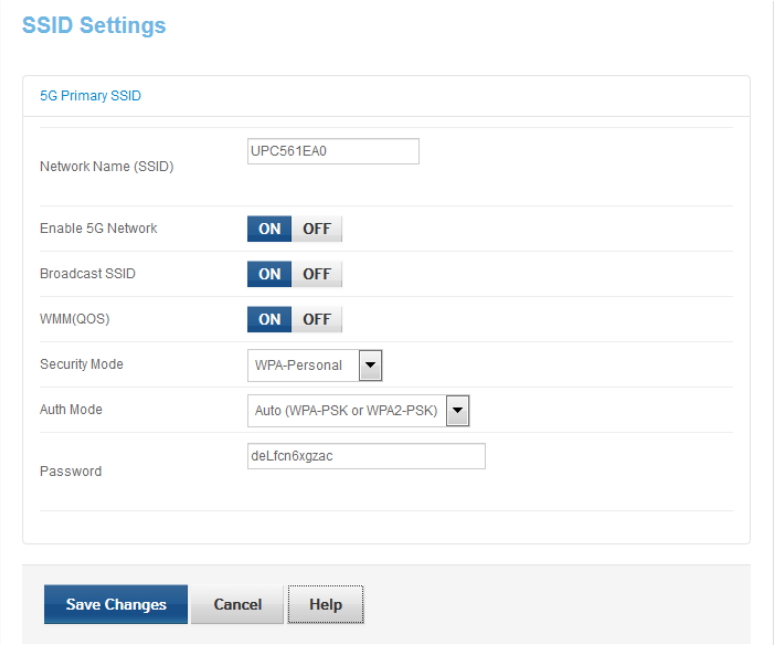
WPS Enabled: Genereller WPS ON/OFF Schalter

Band Steering: verbindet Ihre Geräte automatisch mit der besten verfügbaren WLAN-Frequenz - 2,4 GHz und 5 GHz - und fordert Sie auf, eine Auswahl zu treffen, wenn Sie ein Gerät an Ihr Netzwerk anschließen.Wenn diese Option aktiviert ist, müssen Sie nicht auswählen, welche Frequenz Ihr Gerät am besten unterstützt. Das Modem führt dies automatisch aus.

DCS Enabled: Aktivieren / Deaktivieren der DCS-Unterstützung (Dynamic Channel Selection). Dynamic Channel Selection ist eine Funktion, die den Störpegel auf dem Kanal überwacht und das Gateway automatisch auf einen sauberen Kanal umschaltet.

DFS (DYNAMIC FREQUENCY SELECTION): Diese Funktion ist nur für das 5-GHz-Band verfügbar und dient zur Vermeidung von Interferenzen. Mit den An-/Aus-Tasten können Sie diese Einstellung aktivieren und deaktivieren. Bei ausgeschalteter DFS wird die Sendeleistung gesenkt und die Anzahl verfügbarer Kanäle stark reduziert.

5.2 SSID Settings



Network Name (SSID): Legen Sie hier Ihren SSID-Namen fest.

Enable 2.4G/5G Network: Verwenden Sie die An-/Aus-Tasten, um das WiFi-Netzwerk zu aktivieren/deaktivieren. Sind beide Netzwerke 2.4G und 5G deaktiviert, ist das WiFi komplett ausgeschaltet.

Broadcast SSID: Verwenden Sie die An-/Aus-Tasten, um die Übertragung einer bestimmten SSID zu aktivieren/deaktivieren. Bei «Aus» wird diese SSID von Geräten nicht erkannt.

WMM(QoS): Wi-Fi Multimedia (WMM) ist eine drahtlose QoS-Funktion (Quality of Service), die die Qualität von Audio-, Video- und Sprachanwendungen durch Priorisierung des drahtlosen Datenverkehrs verbessert. Der Einrichtungsabschnitt enthält die IP-Informationen, die vom Gateway an Ihr lokales Netzwerk verteilt werden.

Security Mode: In der angezeigten Tabelle können Sie die Art der drahtlosen Sicherheit auswählen, die Sie verwenden möchten. DRAHTLOSER SICHERHEITSMODUS: Über das Drop-down-Menü können Benutzer zwischen «KEINE», «WEP» und «WPA-Personal» wählen. Bei Auswahl von «NONE» wird kein Sicherheitsmechanismus angewendet, und jeder WLAN-Client kann eine Verbindung zu diesem AP herstellen. Wenn Sie «WEP» oder «WPA-Personal» auswählen, wird die entsprechende Tabelle zur weiteren Einstellung angezeigt.

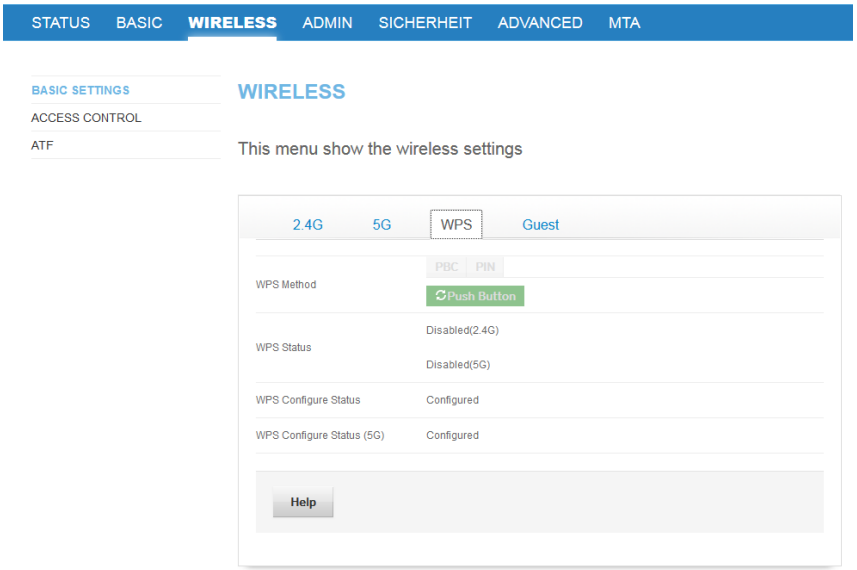
Authentifikation: Benutzer können WPA-PSK (WPA Pre-Shared Key), WPA2-PSK oder Auto (kompatibel mit WPA-PSK- und WPA2-PSK-Client) wählen.

Password: Dies ist das Passwort, das von der WPA-/WPA2-Verschlüsselung verwendet wird. Das Standardpasswort kann überschrieben werden.

5.3 WPS Conectivity

Für den WPS-Betrieb wird die PBC-Funktion (Push-Button Configuration) über die WPS-Taste (an der Modemfront oder virtuell) gestartet. Wenn diese Taste gedrückt wird, beginnt das Gerät die WPS-Aushandlung mit einem anderen WLAN-Client, auf dem auch der PBC-Modus ausgeführt wird.

Wenn die PIN-Taste gedrückt wird, öffnet das Gerät ein Dialogfeld, in dem Benutzer einen 8-stelligen PIN-Code für die WPS-Aushandlung eingeben können. Gleichzeitig muss der WLAN-Client denselben PIN-Code für die WPS-Aushandlung verwenden.

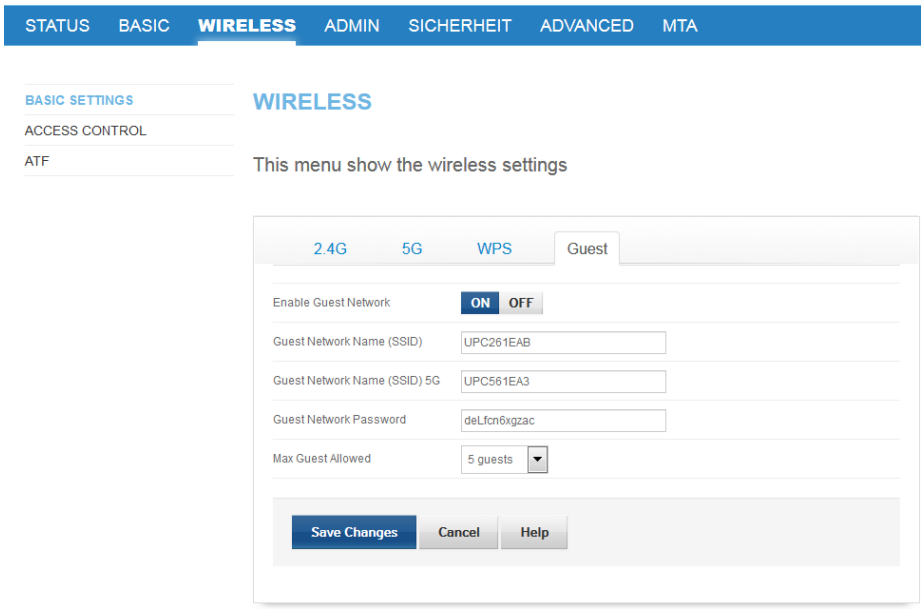


WPS PBC: Push Button Configuration.

WPS-Client-PIN: Geben Sie die von Ihrem Clientgerät generierte PIN ein.

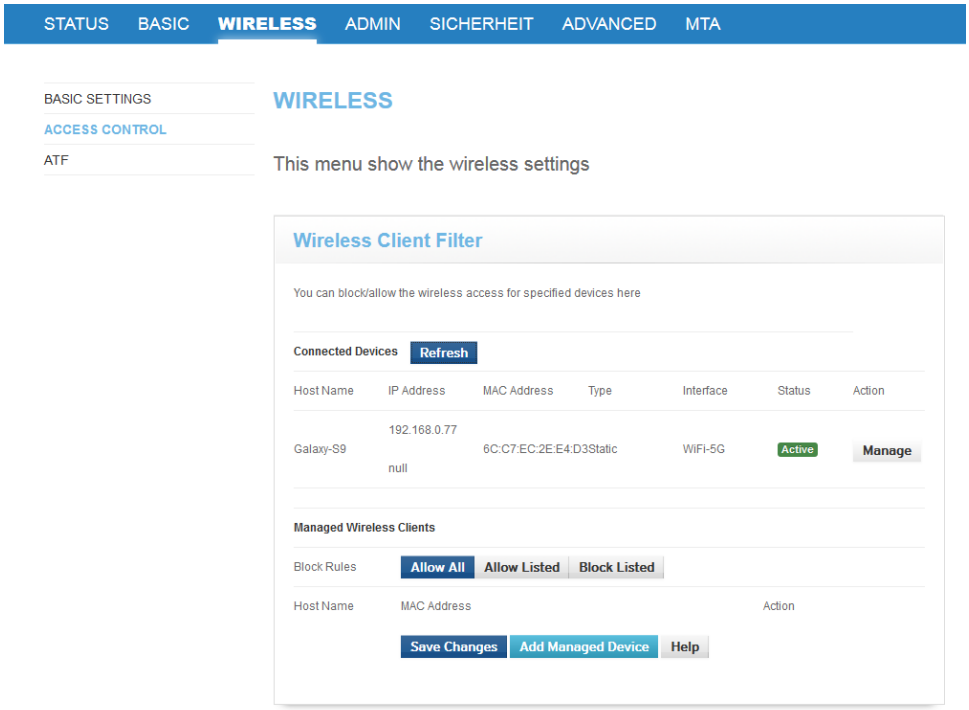
5.4 Gastnetzwerk

Über den Gastzugang können sich Besucher mit dem Internet verbinden, ohne Zugriff auf andere Computer oder persönliche Daten zu erhalten. Sie können sich mit Ihrem Gastnetzwerk verbinden, online gehen und im Internet surfen. Das Gäste-LAN ist ein separiertes Netz.



5.5 Access-Kontrolle

In diesem Abschnitt können Sie angeben, welche Benutzer und Geräte auf bestimmte SSIDs zugreifen können.



Über die Schaltfläche **«Block Listed»** (Sperren) können bestimmte Geräte auf das Gateway zugreifen. Über «Allow Listed» können Sie auf die Geräte in dieser Liste zugreifen. **«Allow All»** ermöglicht den Gateway-Zugriff auf alle mit dem Gateway verbundenen Geräte.

Geräte können auf zwei verschiedene Arten in die Regeltabelle eingefügt werden:

Die erste Methode ist die Verwendung der Schaltfläche **«Manage»** des Geräts in der Tabelle «Verbundene Geräte». Sobald diese Schaltfläche gedrückt wird, erscheint ein Pop-up-Fenster mit den folgenden zu konfigurierenden Feldern:

MAC-Adresse: Dieses Feld wird mit den MAC-Adressen aus der Tabelle «Verbundene Geräte» gefüllt.

Die zweite Methode ist die Auswahl der Schaltfläche «Add Managed Device». Ein Pop-up-Fenster wird geöffnet und zeigt keine Informationen im Feld «Host-Name» und eine vordefinierte MAC-Adresse mit «00: 00: 00: 00: 00: 00» an. Endbenutzer müssen die Einstellungen in diese beiden Felder manuell eingeben. Die anderen Felder in diesem Pop-up-Fenster können auf dieselbe Weise wie bei der ersten Methode oben konfiguriert werden.

Drücken Sie zur Bestätigung «Übernehmen» oder zum Ignorieren «Schliessen». Benutzer müssen zur Seite «Zugriffskontrolle» zurückkehren und auf «Änderungen speichern» klicken, um die Änderungen zu aktivieren. Erweiterte Wireless-Einstellungen

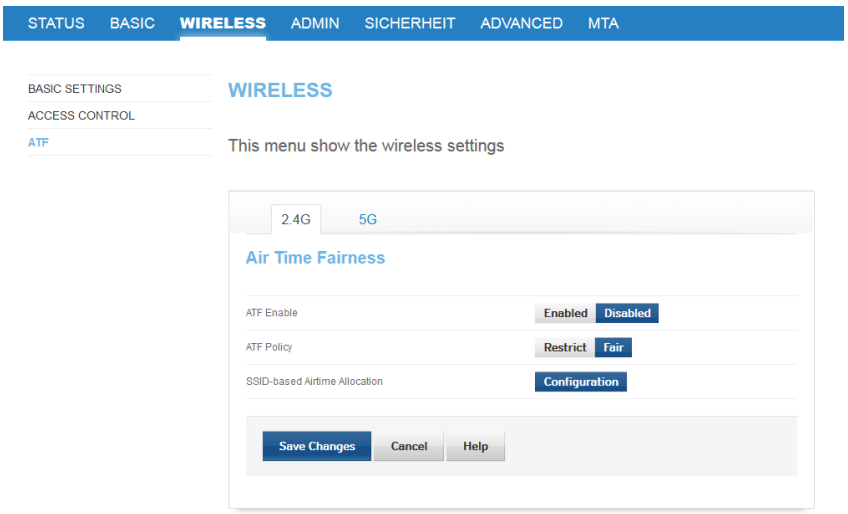
Diese Seite bietet einige erweiterte Funktionen von WiFi.

WIFI SITE SURVEY: Wenn diese Taste gedrückt wird, kann Ihr Router die Umgebung nach anderen Signalen durchsuchen und diese anzeigen.

WIFI-CLIENTS: Damit haben Sie Informationen über alle mit WLAN verbundenen Clients via die GUI.

5.6 ATF Air Time Fairness

Die Air Time Fairness (ATF) konzentriert sich in erster Linie auf die Planung der Fairness für die Übertragung von Verkehr des Access Point (AP) sowie auf die effiziente Nutzung der WiFi-Bandbreite. Der Algorithmus befasst sich nicht mit der Übertragung von Frames von anderen Clients.



ATM-Algorithmus-Typ: Dieser Parameter wird verwendet, um den ATM-Algorithmus zu deaktivieren oder den Typ des ATM-Algorithmus zu konfigurieren, der zum Anwenden von Air Time Fairness verwendet werden muss. Dieser Parameter **muss** die folgenden Werte annehmen: Disable, Global Fairness oder Weighted Fairness.

ATF-Policy steuert zwei verschiedene Zeitplanungsalgorithmen, die sich gegenseitig ausschliessen: strikte Warteschlange und faire Warteschlange. Die strikte Warteschlange folgt einer strengen Sendezeitzuweisung, wie vom Benutzer konfiguriert, und versucht nicht, ungenutzte Bandbreite zu verwenden. Der «fair queue»-Algorithmus hingegen garantiert die konfigurierte Sendezeit in überlasteten Umgebungen und nutzt auch ungenutzte Bandbreite.

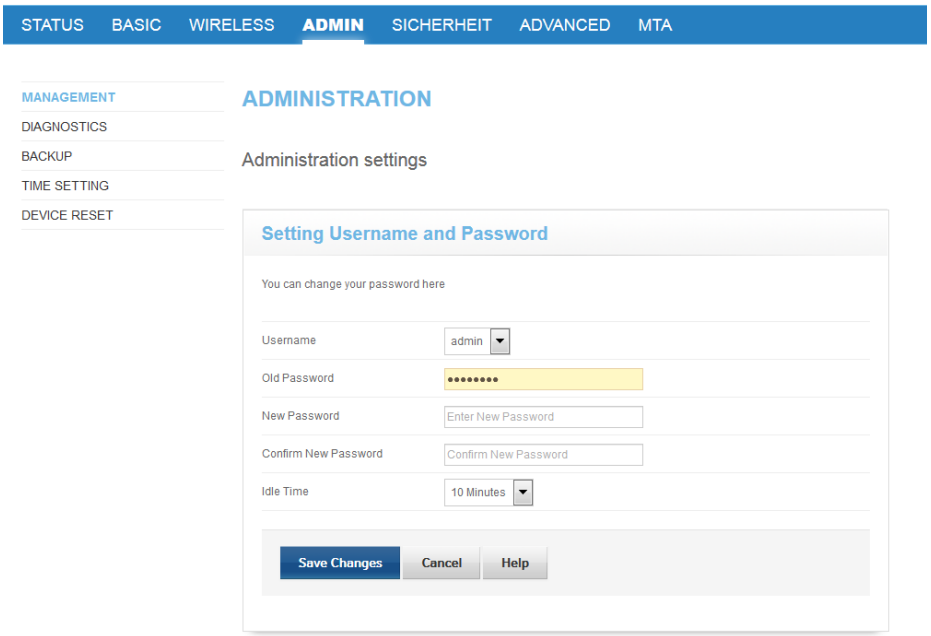
SSID-basierte Air-Time-Zuweisung: Mit diesem Parameter wird die Gewichtung für jede SSID konfiguriert. Die ATM-Gewichtung einer SSID **muss** ein Wert zwischen 5 und 100 sein. Wenn Sie die Schaltfläche «Löschen» drücken, wird der Air-Time-Prozentsatz dieser SSID zu –1. Das bedeutet, dass der Air-Time-Prozentsatz dieser SSID gelöscht wird. Wenn Sie für eine SSID eine Sendezeit festlegen möchten, müssen Sie zuerst die Set-Taste drücken. Wenn der SSID-Status deaktiviert ist, ist die Sendezeit der von Ihnen festgelegten SSID ungültig.

Sendezeitzuweisung pro Station: Dieser Mechanismus soll in erster Linie dazu verwendet werden, um sicherzustellen, dass den STAs ausreichend Bandbreite für die Ausführung ihrer jeweiligen Aufgaben (Videostreaming usw.) zugewiesen wird. Mit diesem Parameter werden die Gewichtungen für die einzelnen STAs festgelegt. Die Sendezeit von STAs, die mit einer SSID verbunden sind, **darf nicht** 100% überschreiten.

6 ADMIN

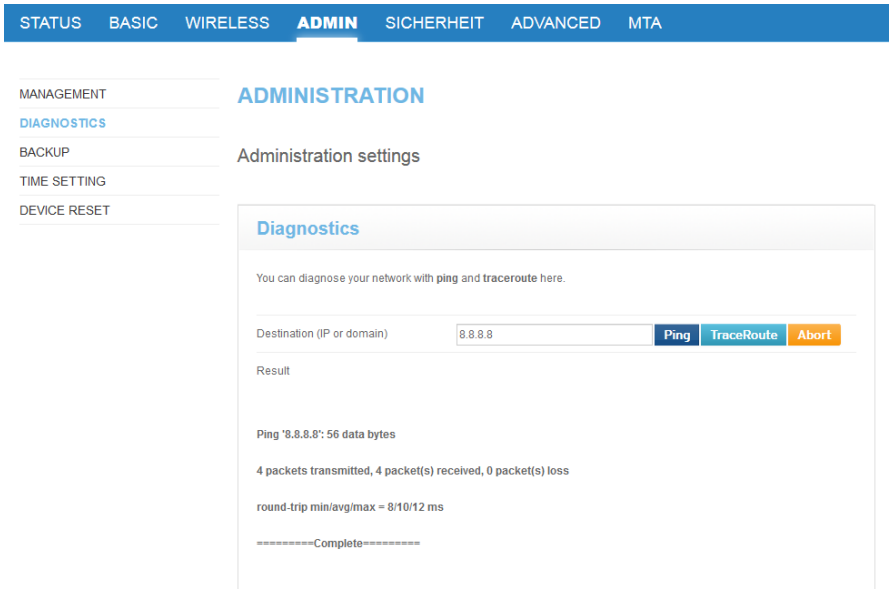
6.1 Management

Benutzer können diesen Abschnitt verwenden, um ihr Passwort für den Zugriff auf die GUI zu ändern. Die Einstellungen für Username und GUI Idle Timeout können nur vom Benutzer geändert werden.



6.2 Diagnose

Ping oder Traceroute für eine Verbindungsprüfung.



6.3 Backup

Hier können die Konfigurationen des Hitron Modems lokal gespeichert werden. Mit der Wiederherstellungsoption kann der gespeicherte Zustand jederzeit wiederhergestellt werden.

6.4 Time Setting

Benutzer können auf dieser Seite zwischen zwei Zeiteinstellungsprotokollen wählen, ToD und SNTP. Für jedes Zeiteinstellungsprotokoll können Benutzer die Zeitzone auswählen, in der sie sich befinden. Das ToD-Protokoll wird standardmässig basierend auf den DOCSIS-Provisioning-Einstellungen ausgewählt.

Diese Seite enthält auch die Sommerzeitfunktion. Wenn diese Funktion aktiviert ist, folgt der Dienst der für jede Zeitzone definierten Sommerzeitregel, sodass Benutzer die Uhrzeit anpassen können.

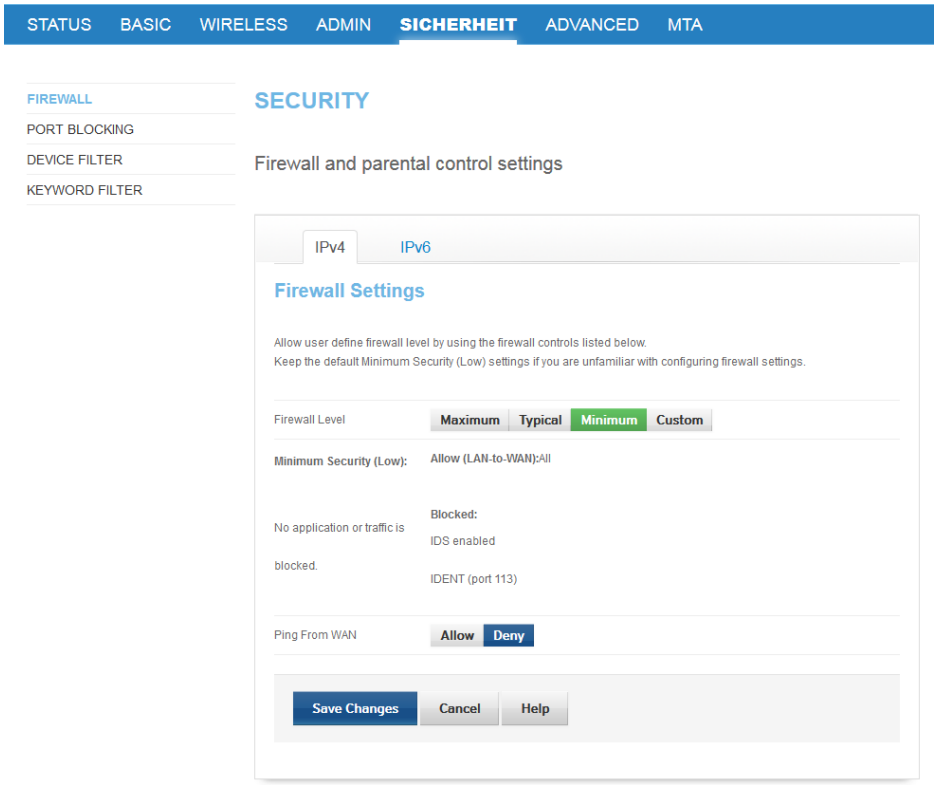
6.5 Zurücksetzen

Neustart des Modems oder Zurückstellen auf die Werkseinstellungen.

7 SICHERHEIT

7.1 Firewall

Benutzer können die Firewall-Sicherheitsstufe definieren, die für ihren Dienst erforderlich ist. Es gibt drei vordefinierte Firewall-Ebenen: Maximum, Standard und Minimum. Mit der benutzerdefinierten Einstellung können Benutzer ihre eigenen Firewall-Regeln definieren.



Maximale Sicherheit: Von LAN zu WAN werden alle Anwendungen einschliesslich Sprachanwendungen (z.B. GTalk, Skype) und P2P-Anwendungen blockiert. Diese Einstellung ermöglicht das Surfen im Internet, E-Mail-, VPN-, DNS- und iTunes-Dienste.

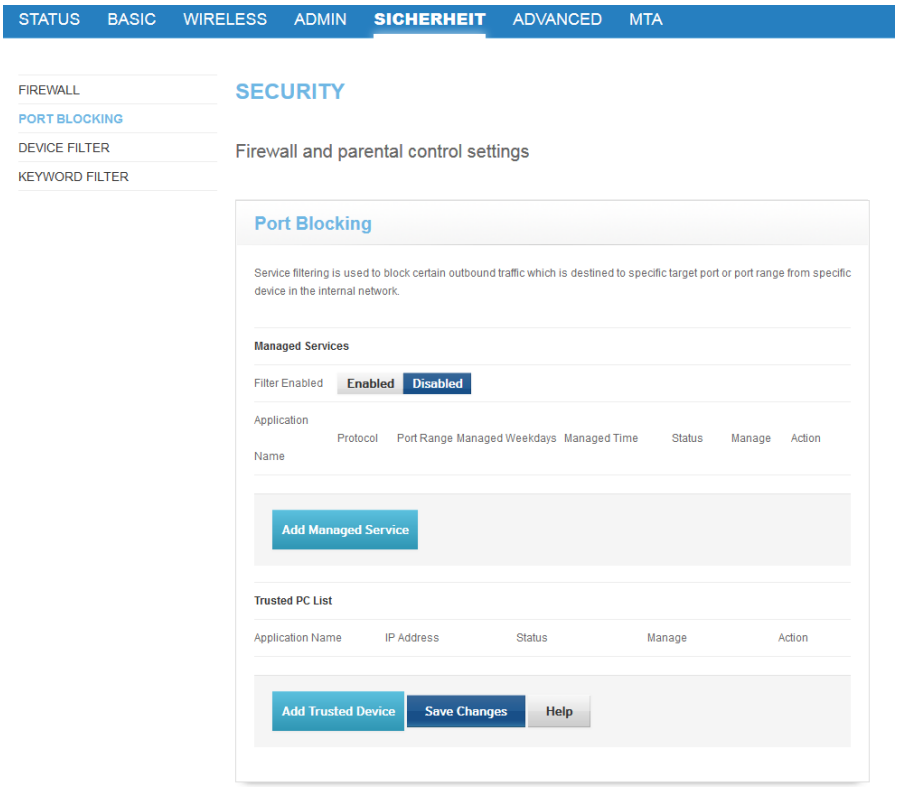
Typische Sicherheit: Von LAN zu WAN werden P2P-Anwendungen und Ping zum Gateway blockiert, der gesamte Datenverkehr wird jedoch zugelassen.

Mindestsicherheit: Von LAN zu WAN wird keine Anwendung oder kein Verkehr blockiert. Dies ist die Standardkonfiguration.

Benutzerdefinierte Sicherheit: Häufig verwendete Anwendungen können durch Klicken auf die Schaltfläche «Ablehnen» blockiert werden. Alle anderen Dienste können standardmässig aktiviert werden. Um einen bestimmten Port zu blockieren, kann die Option «Service-Filter» verwendet werden.

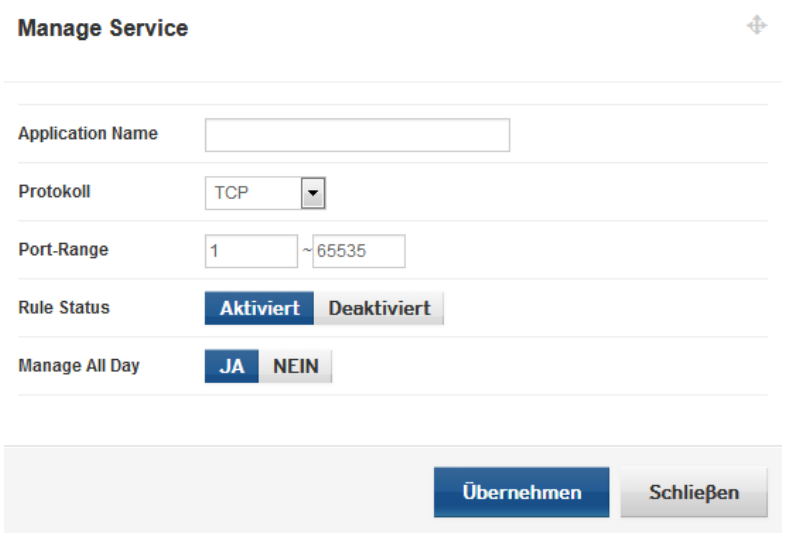
7.2 Port Blocking

Die Dienstfilterung wird verwendet, um bestimmten abgehenden Datenverkehr zu blockieren, der von einem Computer im internen Netzwerk an einen bestimmten Ziel-Port oder Port-Bereich gerichtet ist. Bei der Liste der vertrauenswürdigen PCs wird der in die Liste eingetragene PC von der in der Service-Filter-Tabelle festgelegten Filterung ausgenommen.



So konfigurieren Sie Service-Filter-Regeln:

Die Dienstfilterung wird verwendet, um bestimmten abgehenden Datenverkehr zu blockieren, der von einem Computer im internen Netzwerk an einen bestimmten Ziel-Port oder Port-Bereich gerichtet ist. Wenn die Filterregel aktiviert ist, können Benutzer die Schaltfläche «Managed Service hinzufügen» drücken, um eine Service-Filter-Regel hinzuzufügen. Ein Pop-up-Fenster wird angezeigt, um unterhalb der Einstellungen zu arbeiten.



Anwendungsname: In diesem Feld wird die Regel angegeben.

Protokoll: Benutzer können das Protokoll (TCP, UDP oder TCP/UDP) für die Filterregel auswählen.

Port-Range: Mit dieser Einstellung können Benutzer den Port-Bereich einrichten, der die Einstellung von 1 bis 65535 erlaubt.

Regelstatus: In diesem Feld wird diese bestimmte Regel aktiviert/deaktiviert.

Ganztägig verwalten: Dieses Feld wird verwendet, um die Zeitplanung für die Anwendung dieser Regel zu steuern. Wenn Sie die Schaltfläche «JA» auswählen, stehen für die Zeitplanverwaltung mehr Kontrollfelder zur Verfügung.

Die zusätzliche Planungseinstellung, einschliesslich der Wochentagseinstellung und der Start-/ Endzeiteinstellung.

Verwaltete Wochentage: Wenn «Ganztägig verwalten» auf «JA» eingestellt ist, wird dieses Feld angezeigt. Benutzer können die Tage auswählen, an denen die Regel angewendet werden soll. Die Wochentage umfassen Sonntag bis Samstag.

Verwaltete Zeit: Dieses Feld wird verwendet, um die Startzeit und die Endzeit für die Anwendung der Regel zu steuern.

Nachdem Sie die obige Einstellung festgelegt haben, klicken Sie auf die Schaltfläche «Übernehmen», um die Einstellung in die Service-Filter-Tabelle zu übernehmen, oder drücken Sie auf «Schliessen», um die Einstellung zu ignorieren. Wenn Sie die Regel löschen möchten, wählen Sie einfach die Schaltfläche «Deaktiviert» für das Feld «Regelstatus» aus.

Nach der Rückkehr zur Service-Filter-Seite müssen Benutzer noch auf «Änderungen speichern» klicken, um die Einstellung wirksam zu machen.

So konfigurieren Sie eine Liste mit vertrauenswürdigen PCs:

Benutzer können auf die Schaltfläche «Vertrauenswürdiges Gerät hinzufügen» klicken, um Geräte zur Liste hinzuzufügen. Wenn Sie auf die Schaltfläche «Vertrauenswürdiges Gerät hinzufügen» klicken, wird ein Pop-up-Fenster angezeigt, in dem Benutzer die Einstellungen wie unten beschrieben vornehmen können.

Host-Name: In diesem Feld wird der Hostname des hinzugefügten Geräts angegeben.

MAC-Adresse: Dieses Feld enthält die MAC-Adresse des vertrauenswürdigen PCs.

Regelstatus: Benutzer können diese Regel über die Schaltflächen «Aktiviert»/«Deaktiviert» aktivieren/deaktivieren.

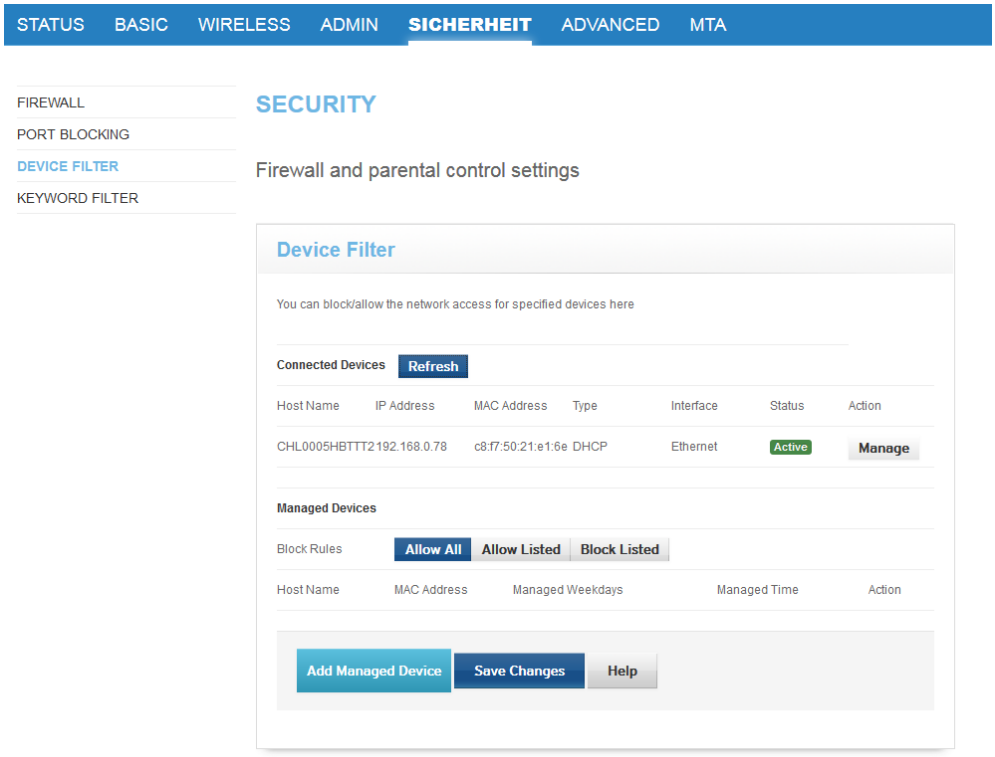
Nachdem Sie die obige Einstellung festgelegt haben, klicken Sie auf die Schaltfläche «Übernehmen», um die Einstellung in die Liste der vertrauenswürdigen PCs zu übernehmen, oder drücken Sie auf «Schliessen», um die Einstellung zu ignorieren.

Nach der Rückkehr zur Service-Filter-Seite müssen Benutzer noch auf «Änderungen speichern» klicken, um die Einstellung wirksam zu machen.

Schaltfläche «Löschen»: Löscht eine vorhandene Regel aus der Liste der vertrauenswürdigen PCs.

7.3 Device-Filter

Mit der Einstellung «Gerätefilter» können Sie angeben, auf welchen Computern der Zugriff auf das Internet und Ihr Netzwerk gesperrt werden darf. Ausserdem kann die Einstellung das Blockieren/Zulassen steuern basierend auf dem Zeitplan, der durch die Regel definiert wurde.

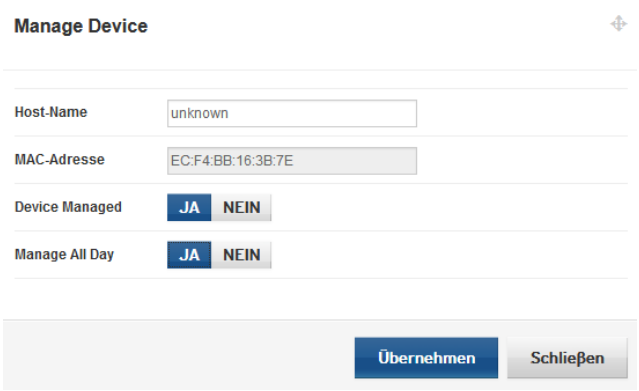

STATUS
BASIC
WIRELESS
ADMIN
SICHERHEIT
ADVANCED
MTA
FIREWALL
PORT BLOCKING
DEVICE FILTER
KEYWORD FILTER
SECURITY
Firewall and parental control settings
Device Filter
You can block/allow the network access for specified devices here
Connected Devices
Refresh
Host Name
IP Address
MAC Address
Type
Interface
Status
Action
CHL0005HBTTT2
192.168.0.78
c8:f7:50:21:e1:6e
DHCP
Ethernet
Active
Manage
Managed Devices
Block Rules
Allow All
Allow Listed
Block Listed
Host Name
MAC Address
Managed Weekdays
Managed Time
Action
Add Managed Device
Save Changes
Help

So konfigurieren Sie die Gerätefiltereinstellung:

Mithilfe des Gerätefilters können Sie eine Liste von Computern erstellen, denen die Verbindung zum Gateway über die LAN-Switch-Ports verweigert wird. Alle Computer, die in der Liste aufgeführt sind, können keine Verbindung zu Ihrem Gateway herstellen, wenn Sie auf die Schaltfläche **«Block Listed»** klicken und die Zugriffszeit den in der Regel festgelegten Zeitplan erfüllt. Jeder in der Liste angegebene Computer kann eine Verbindung zu Ihrem Gateway herstellen, wenn Sie auf die Schaltfläche **«Allow Listed»** klicken und die Zugriffszeit den in der Regel festgelegten Zeitplan erfüllt. Wenn die Schaltfläche **«Allow All»** (Alle zulassen) gedrückt wird, können alle Computer, unabhängig von den Einstellungen in der Regeltabelle, eine Verbindung zum Gateway herstellen.

Es gibt zwei verschiedene Methoden, um den PC in die Regeltabelle einzufügen.

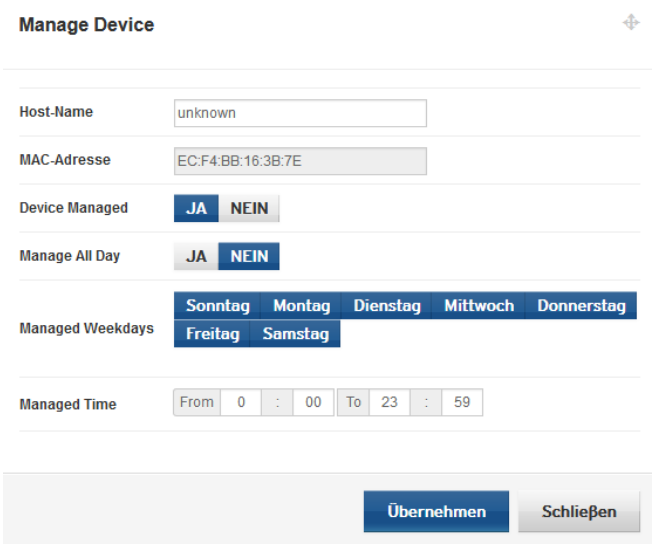
Die erste besteht darin, die Schaltfläche «Manage» des gelernten PCs in der Tabelle «Connected Devices» zu drücken. Nachdem Sie auf die Schaltfläche «Manage» geklickt haben, wird ein Pop-up-Fenster mit dem folgenden Feld angezeigt:



MAC-Adresse: Dieses Feld wird mit der erlernten MAC aus der Tabelle der verbundenen Geräte ausgefüllt.

Gerät verwaltet: Wenn Sie hier die Schaltfläche «JA» drücken, wird die Zeile «Ganztägig verwalten» erstellt. Wenn die Schaltfläche «NO» gedrückt wird und die Schaltfläche «Apply» ebenfalls gedrückt wird, wird die Regel in der Gerätefiltertabelle gelöscht.

Ganztägig verwalten: Die Standardeinstellung ist «YES». Dies bedeutet, dass die Regel sieben Tage pro Woche und 24 Stunden pro Tag angewendet wird. Wenn Sie die Schaltfläche «NO» drücken, werden die Zeilen «Managed Weekdays» und «Time» angezeigt, und der Benutzer kann den Zeitplan für die Regel festlegen.



Verwaltete Wochentage: Benutzer können eine beliebige Kombination der sieben Tasten drücken (Sonntag bis Samstag).

Verwaltete Zeit: Benutzer können die Stunden und Minuten des Tages für den Zeitplan der Regel auswählen.

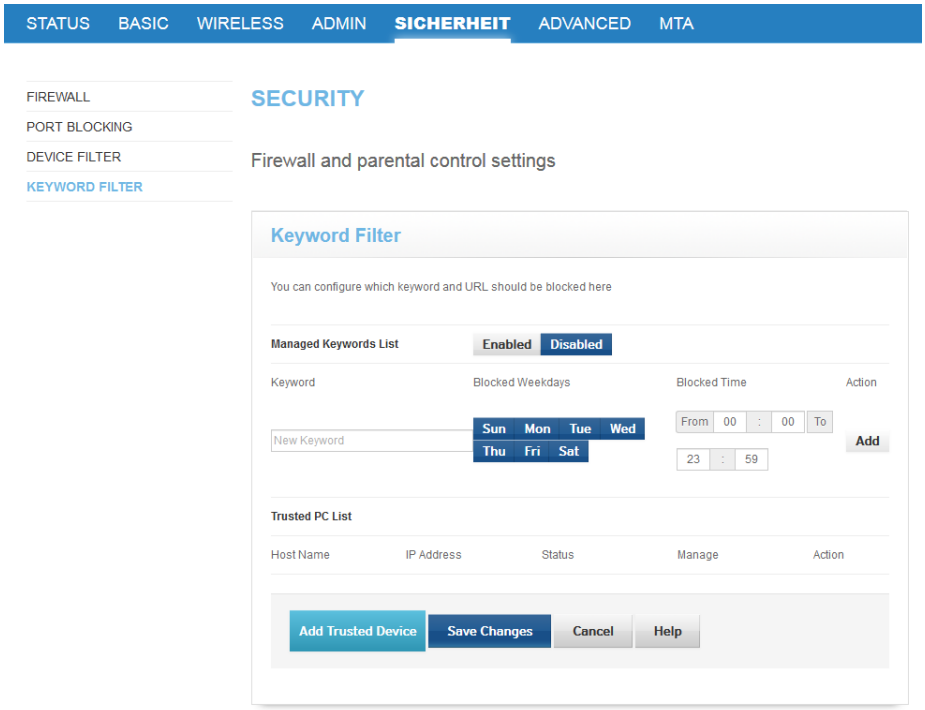
Die zweite Methode ist das Klicken auf die Schaltfläche **«Add Managed Device».** Ein Pop-up-Fenster, das das manuelle Hinzufügen erlaubt.

Nachdem Sie die obige Einstellung festgelegt haben, drücken Sie bitte die Schaltfläche **«Übernehmen»**, um die Einstellung in die Gerätefiltertabelle zu übernehmen, oder drücken Sie **«Schliessen»**, um die Einstellung zu ignorieren. Wenn Sie die Regel löschen möchten, wählen Sie einfach die Schaltfläche «NEIN» für das Feld «Gerät verwaltet».

Nach der Rückkehr zur Gerätefilterseite müssen Benutzer noch auf **«Änderungen speichern»** klicken, damit die Einstellung wirksam wird.

7.4 Keyword-Filter

Benutzer können konfigurieren, welches Schlüsselwort gesperrt werden soll, wenn es in der URL verwendet wird. Gleichzeitig können Benutzer einen Zeitplan einrichten, der zusammen mit der Regel verwendet wird. Wenn Benutzer möchten, dass einige Computer von der Schlüsselwortsperrung ausgeschlossen werden, kann dies in der Liste der vertrauenswürdigen PCs konfiguriert werden.



So konfigurieren Sie den Keyword-Filter:

Wenn Sie ein oder mehrere Schlüsselwörter festlegen möchten, müssen Sie zunächst auf die Schaltfläche **«Aktiviert»** klicken. Geben Sie dann das Schlüsselwort ein, das Sie blockieren möchten, und wählen Sie die Uhrzeit aus. Klicken Sie abschliessend auf die Schaltfläche **«Hinzufügen».** Benutzer können diesen Vorgang wiederholen, um das Schlüsselwort einzeln hinzuzufügen.

So konfigurieren Sie eine Liste mit vertrauenswürdigen PCs:

Benutzer können auf die Schaltfläche **«Vertrauenswürdiges Gerät hinzufügen»** klicken, um Geräte zur Liste hinzuzufügen. Wenn Sie auf die Schaltfläche **«Vertrauenswürdiges Gerät hinzufügen»** klicken, wird ein Pop-up-Fenster angezeigt, in dem Benutzer die Einstellungen wie unten beschrieben vornehmen können.

Host-Name: Dieses Feld gibt den Hostnamen des Computers an.

MAC-Adresse: Dieses Feld muss mit der MAC-Adresse des Computers ausgefüllt werden, die von der Schlüsselwortfilterung ausgenommen wird.

Regelstatus: Benutzer können diese Regel über die Schaltflächen «Aktiviert»/«Deaktiviert» aktivieren/deaktivieren.

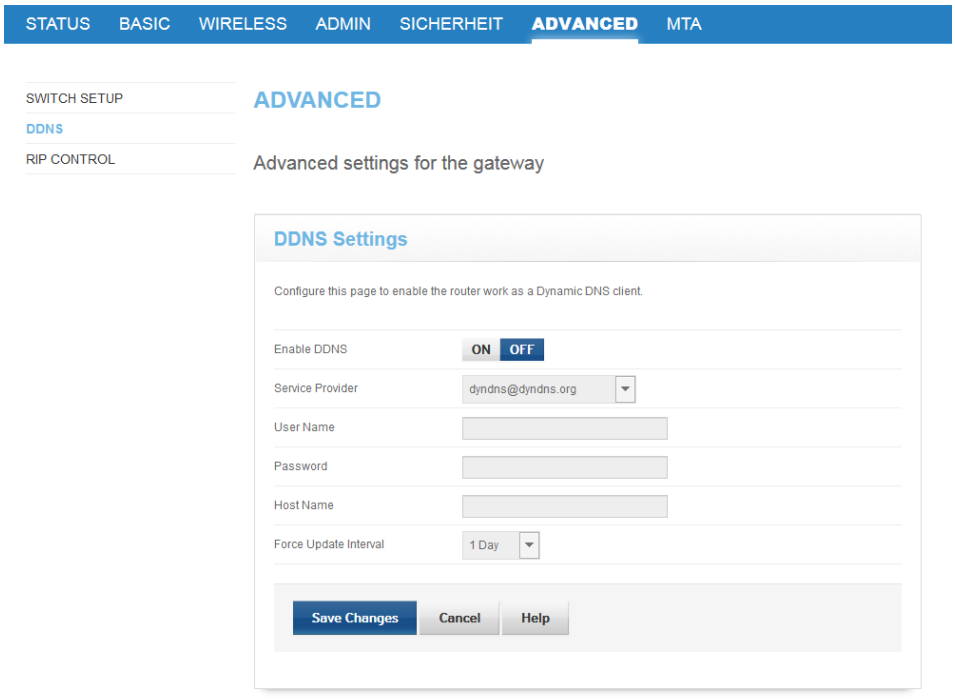
Nachdem Sie die obige Einstellung festgelegt haben, klicken Sie auf die Schaltfläche «Übernehmen», um die Einstellung in die Liste der vertrauenswürdigen PCs zu übernehmen, oder drücken Sie auf «Schliessen», um die Einstellung zu ignorieren.

Nach der Rückkehr zur Keyword-Filter-Seite müssen Benutzer noch auf «Änderungen speichern» klicken, um die Einstellung wirksam zu machen.

Schaltfläche «Löschen»: Löscht eine vorhandene Regel aus der Liste der vertrauenswürdigen PCs.

7.5 DDNS

Dynamisches DNS oder DDNS ist eine Technik, um Domains im Domain Name System (DNS) dynamisch zu aktualisieren. Der Zweck ist, dass ein Computer (bspw. ein PC oder ein Router) nach dem Wechsel seiner IP-Adresse automatisch und schnell den dazugehörigen Domaineintrag ändert.



DDNS: Verwenden Sie die An-/Aus-Tasten, um den DDNS-Dienst zu aktivieren/deaktivieren. Wenn der DDNS-Dienst deaktiviert ist, stehen die verbleibenden Felder nicht zum Bearbeiten oder Konfigurieren zur Verfügung.

Service Provider: Benutzer können ihren DDNS-Serviceprovider über das Drop-down-Menü in diesem Feld auswählen.

Benutzername: Benutzername beim DDNS-Dienst.

Password: Passwort beim DDNS-Dienst.

Host-Name: Beim DDNS-Dienst reservierter Hostname.