SMART/RG
An ADTRAN Company

501 SE Columbia Shores Boulevard, Suite 500
Vancouver, Washington 98661 USA
+1 360 859 1780 / smartrg.com

/ Gateway User Manual

Model: SR905acv

Release: 2.2

January 2021

Software Version: 10.8.8.1

Table of Contents

SMART/RG
An ADTRAN Company

Table of Contents

Welcome!

Thank you for purchasing this SmartRG product.

SmartRG offers solutions that simplify the complex Internet ecosystem. Our solutions include hardware, software, applications, enhanced network insights, and security delivered via a future-proof operating system. Based in the USA, SmartRG provides local, proactive software development and customer support. We proudly offer the best, most innovative broadband gateways available. Learn more at www.SmartRG.com.

Purpose & Scope

This User Manual provides SmartRG customers with installation, configuration and monitoring information for their SR905acv gateway.

Intended Audience

The information in this document is intended for Network Architects, NOC Administrators, Field Service Technicians and other networking professionals responsible for deploying and managing broadband access networks. Readers of this manual are assumed to have a basic understanding of computer operating systems, networking concepts and telecommunications.

Getting Assistance

The ADTRAN Support Community provides how-to information, forums, documentation and software downloads.

- **Subscribers:** If you require further help with this product, please contact your service provider.
- **Service providers:** if you require further help with this product, please open a support request.

Copyright and Trademarks

Disclaimer

SmartRG does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor patent rights of others. SmartRG further reserves the right to make changes to any products described herein without notice. This publication is subject to change without notice.

Any trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Important Safety Instructions

When using your telecommunications equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

1. Use only the power adaptor that is included with the device.
2. Do not use this product near water, for example, near a bathtub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
3. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
4. Do not use the telephone to report a gas leak in the vicinity of the leak.
5. **CAUTION** - To Reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.

The socket-outlet shall be installed near the equipment and shall be easily accessible.

WEEE Statement

The WEEE logo (shown at the left) appears on the product to indicate that this product must not be disposed of or dumped with your other household wastes. You are required to dispose of your electronic or electrical waste equipment by delivering it to the specified collection point for recycling of such hazardous waste.

Importantes Mesures de Sécurité

tre prises pendant l'utilisation de matérial télécommunications afin de réduire les risques d'incendie, de choc électrique Certaines mesures de sécurité doivent et de blessures. En voici quelquesunes:

1. Utilisez uniquement l'adaptateur secteur fourni avec l'appareil.
2. Ne pas utiliser l'appareil près de l'eau, p.ex., près d'une baignoire, d'un lavabo, d'un évier de cuisine, d'un bac à laver, dans un sous-sol humide ou près d'une piscine.
3. Éviter d'utiliser le téléphone (sauf s'il s'agit d'un appareil sans fil) pendant un orage électrique. Ceci peut présenter un risque de choc électrique causé par la foudre.
4. Ne pas utiliser l'appareil téléphonique pour signaler une fuite de gaz s'il est situé près de la fuite.
5. **ATTENTION** - Pour réduire les risques d'incendie, utiliser uniquement des conducteurs de télécommunications 26 AWG au de section supérleure.

le socle de prise de courant doit être installé à proximité du matériel et doit être aisément accessible.

DEEE Statement

Le logo DEEE (illustré à gauche) apparaît sur le produit pour indiquer que ce produit ne doit pas être jeté ou jeté avec vos autres déchets ménagers. Vous êtes tenu de vous débarrasser de vos déchets d'équipements électroniques ou électriques en les livrant au point de collecte spécifié pour le recyclage de ces déchets dangereux.

Getting Familiar with your Gateway

This section explains the SR905acv gateway's lights, ports, and buttons.

LED Indicators

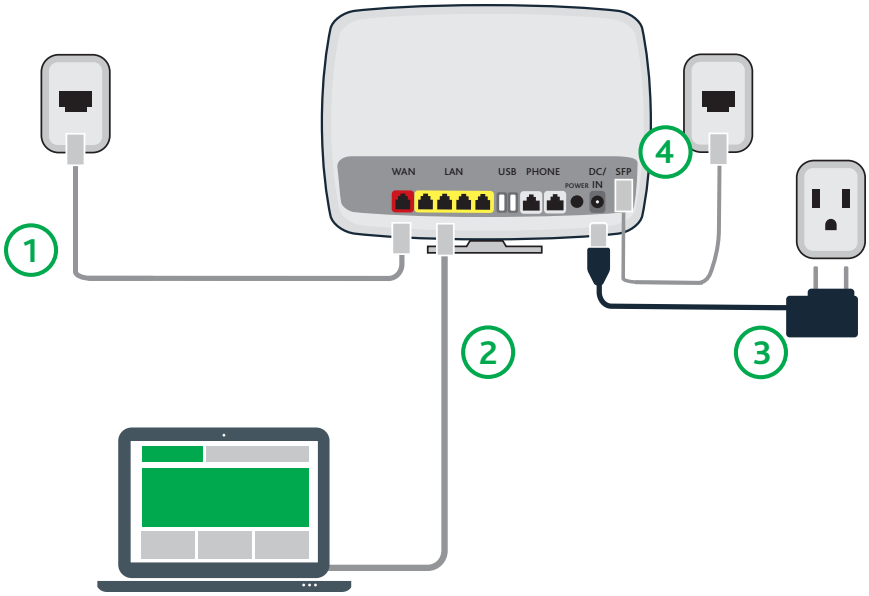
Your SR905acv gateway has several status indicators (LEDs) on its top which are described below.

Legend: ○ White ⚙ White blinking ● Green ⚙ Green blinking ● Red

LED	Action	Explanation
Power	⚙	Device in CFE mode
	○	Device powered on and ready for use
Internet	⚙	Data being transferred
	●	Internet authentication / connection has failed
Lan 1-4	○	LAN Ethernet connected (at 1000 BASE-T)
	⚙	Data being transferred (at 1000 BASE-T)
	●	LAN Ethernet connected (at 10/100BASE-T)
	⚙	Data being transferred (at 10/100BASE-T)
WAN	○	Device online (at 1000 BASE-T)
	●	Device online (at 10/100 BASE-T)
	○	WAN Ethernet connected (at 1000 BASE-T)
	⚙	Data being transferred (at 1000 BASE-T)
	●	WAN Ethernet connected (at 10/100BASE-T)
	⚙	Data being transferred (at 10/100BASE-T)
2.4 GHz 5 GHz	○	WiFi enabled
	⚙	Data being transferred
((·🔒·)) (locked WiFi / WPS)	○	WPS enabled
	⚙	Data being transferred
SS 1 & 2	○	USB 3.0 device connected
	⚙	Data being transferred
Phone 1 & 2	○	Phone line connected
	⚙	Phone line in use
SFP	○	SFP (fiber optic) connected
	⚙	Data being transferred

Connections

The SR905acv's exterior ports are shown in the following cabling diagram and explained below.



LAN

The four yellow RJ45 Ethernet ports located on the back of the gateway (labelled LAN1, LAN2, LAN3, LAN4) are used to connect client devices such as computers and printers.

WAN

The red RJ45 port labeled WAN is used to connect the SR905acv gateway to another network device using a RJ45/Ethernet cable.

USB 1 & 2

Two USB ports (two 3.0 ports on back) are used to connect USB storage devices to the gateway for transferring data. They also provide +5 VDC for charging other devices.

POWER

- Use ONLY the dedicated power supply included with your gateway (3-amp 12 v). Intended for indoor use only.
- Do NOT open the device. Opening or removing covers can expose dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.

External Buttons

The SR905acv gateway provides push-button controls on its exterior for critical features. These buttons provide a convenient means to trigger WPS mode, toggle the WiFi radios on and off, or reset the gateway. The button functions are described below.

WPS Button (5 GHz Band)

WiFi Protected Setup™ (WPS) is a standard means for creating secure connections between the gateway and various wireless client devices. It is designed to simplify the pairing process between devices. This button is located on the left side of the gateway.

Press this button for 1-3 seconds, the **5 GHz** LED starts to flash. If no client pairs with the gateway after 2 minutes, the **5 GHz** LED turns off. When the gateway pairs successfully with a client, the **5 GHz** LED glows solid for 5 minutes and then turns off.

WiFi Button (2.4 GHz Band)

The **WiFi** button toggles the 2.4 GHz WiFi radio on and off. This button is located on the left side of the gateway. Look at the **2.4 GHz** LED indicator to determine the current state of the WiFi radio.

To activate the radio, press and hold the **WiFi** button for 3-5 seconds then release. Expect a 1-3 second delay before the **2.4 GHz** LED turns on. The WiFi radio is now on.

To deactivate the radio, press and hold the **WiFi** button for 3-5 seconds then release. Expect a 1-3 second delay before the **2.4 GHz** LED turns off. The WiFi radio is now off.

On/Off Button

The **On/Off** button turns the gateway on and off. This button is located on the left side of the gateway.

Reset Button

Warning: Do not press the **Reset** button unless you want to clear the current settings.

The **Reset** button returns the gateway to its default settings. This button is in a small circular hole in the back of the gateway with the actual button mounted behind the surface. This style of push button prevents the gateway from being inadvertently reset during handling.

To restore the current default settings, insert a thin wire (such as a paper clip) into the hole, press for 1 second, then release the button. The gateway reboots and returns to the current defaults.

To return the gateway to factory default settings, press the **Reset** button until the LEDs flash red and orange. The gateway reboots and returns to the default settings applied in the factory. This process may take a few minutes.

Installing your SR905acv Gateway

1. Connect the gateway to incoming services:
   - For Ethernet services, connect one end of an Ethernet cable to the **WAN** port on the gateway and connect the other end of the cable to the wall jack installed by your provider.
   - For fiber services:
     a. Slide open the small door at the right end of the gateway's back.
     b. Insert the SFP transceiver (included with the gateway) into the port.
     c. Connect one end of the fiber cable to the SFP transceiver and connect the other end of the cable to the wall jack installed by your provider.
2. Connect a LAN port on the gateway to your PC using an Ethernet cable.
3. Plug the power adapter to the wall outlet and then connect the other end of it to the **Power** port of the gateway.
4. Turn on the unit by pressing the **Power** button on the side of the gateway.

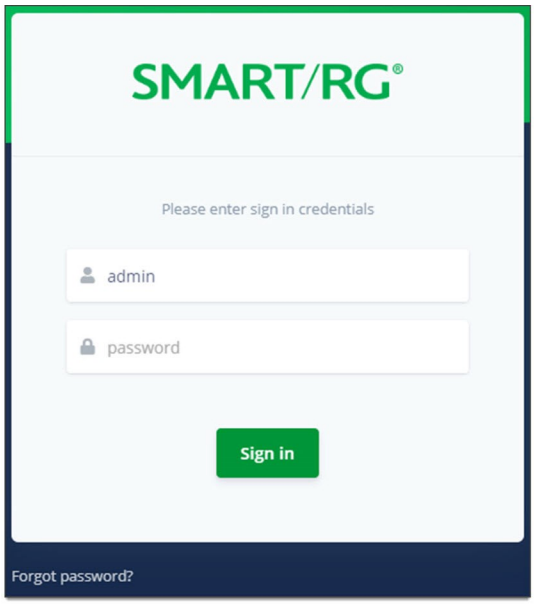
The gateway is now automatically being set up to connect to the Internet. This process may take a few minutes to complete before you can begin using your Internet applications (browser, email, etc.).

If connection to the Internet is unsuccessful, verify that all cable connections are in place and the gateway's power is turned on.

Logging in to the SR905acv Interface

To manually configure the SR905acv gateway, you must access the gateway's Web-based UI.

1. Configure your computer's IP interface to acquire an IP address automatically using DHCP.
2. Open a browser and enter the gateway's default address: http://192.168.1.1 in the address bar. The sign-in page appears.



3. Enter the default username and password.
   - For the administrator user, these are "admin" and "admin".
   - For the support user, these are "support" and the last three octets of the MAC address. The MAC address is located on a label on the back of the gateway. Make sure to enter the letters in all caps and include the separating colons (e.g., AA:BB:CC).

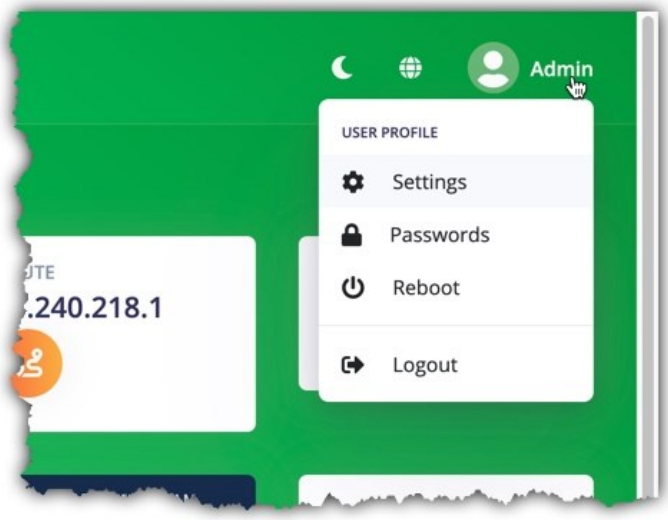
   To review the end user license agreement, click the **License Agreement link** at the bottom right corner of the browser window. The agreement appears in a separate tab.

   Note: If you have forgotten the password, click **Forgot password?** and follow the instructions to reset the gateway to the factory defaults. Then, enter the credentials provided with the gateway when it first arrived.
4. Click **Sign In**. The Dashboard page appears, showing data about your system.

User Preferences

The top of the screen displays various options that are always present:

- Next to the logo in the upper-left is the **Menu** button ( ). Click to minimize or reveal the left navigation menu.
- To the right is a **Search** box which returns a list of pages/gateway features that match the search terms entered.
- Next is the **Dark Mode** icon ( ). Click to engage an alternate color scheme for the UI. The icon changes to the **Light Mode** icon ( ). Click it to return to the original color scheme.
- Next is the **Language** icon( ). Click to select the preferred interface language from the list.
- The far right corner displays the username currently logged in (typically "Admin"). Click the name to reveal a list of additional preferences.



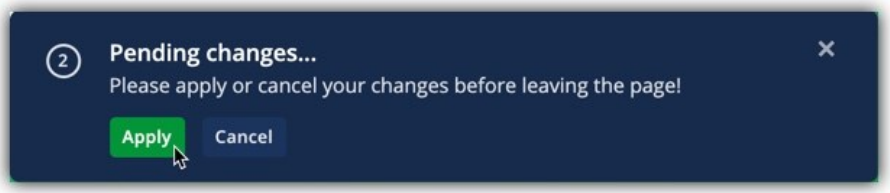
The preferences under the **User Profile** link to options also found under **Admin** in the left menu.

- **Settings**: Save or load a router configuration file. See instructions here.
- **Passwords**: Change passwords for gateway access. See instructions here.
- **Reboot**: Initiate a reboot of the gateway. See instructions here.
- **Logout**: Ends the current session with the gateway.

The page footers display the WAN IP address and firmware version. Mouse over the labels to view the details.

Saving Your Changes

When you change settings, the **Pending changes** dialog box appears at the top of the page.



Changes made on a page must be applied before you can navigate to a different page.

The circled number shown at left indicates the quantity of changes waiting to be applied. To view a list of your unsaved changes, click the circled number. The Unsaved Changes pop-up window appears.

To undo a change in the list, click the **trash can** icon in the far right column for the line item to be cancelled. If you remove all of the changes from the change list, the Unsaved Changes window closes and you can proceed to another page.

Dashboard

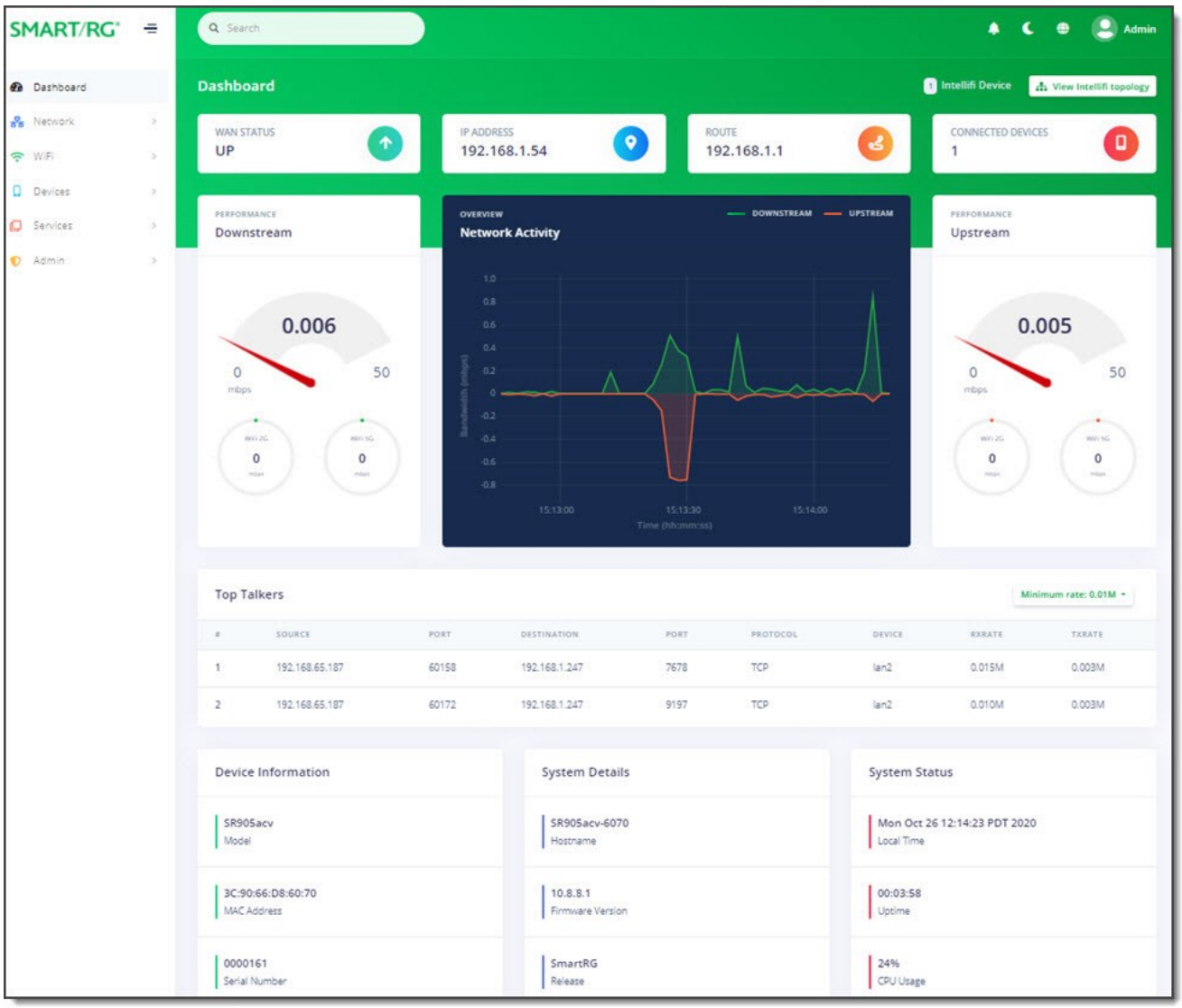
When you log in to the gateway, the following Dashboard landing page appears. On this page, you can view the IP address, route, number of connected devices, WAN and WiFi traffic, device and system information, system status, and memory statistics. You can also reach this page by clicking **Dashboard** in the left menu.

At the top right of the page, you will find the number of Intellifi devices connected to your gateway plus the **View Intellifi topology** button that will take you to the Intellifi Devices page.

A list of top talkers appears below the WiFi information.

- To sort this table, click on any of the headings.
- The **Minimum rate** field appears at the top right of the **Top Talkers** frame. Select a different transmission rate from the drop-down list if desired. Options are **None**, **0.01M**, **0.1M**, **1M**, **10M**, and **100M**. The default is **0.01M**.

At the bottom of the page are the WAN IP address and the firmware version. Mouse over the labels to view the information.



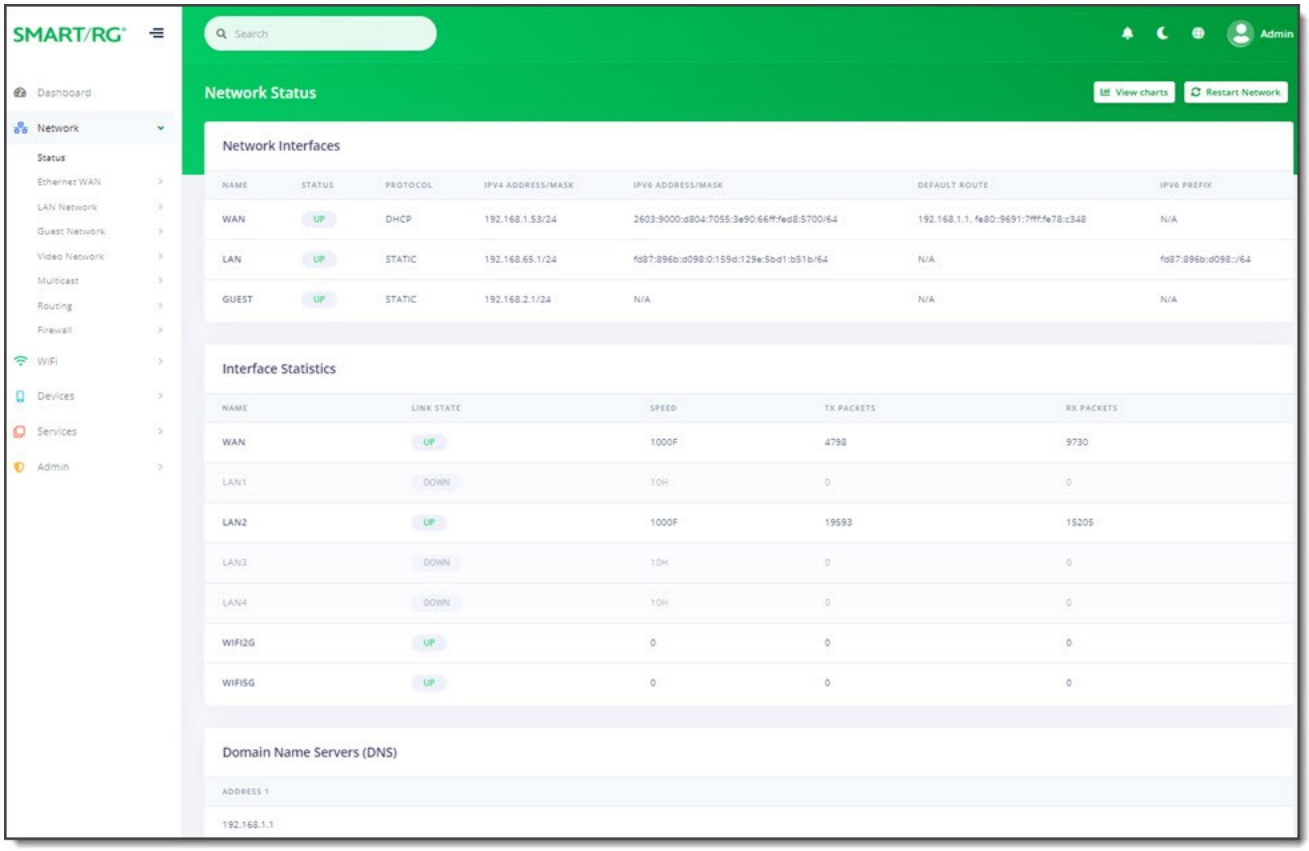
Network

In this section, you can view and configure information about your gateway connections.

Status

On this page, you can view the status and detailed information for gateway connections.

In the left menu, click **Network** > **Status**. The following page appears.



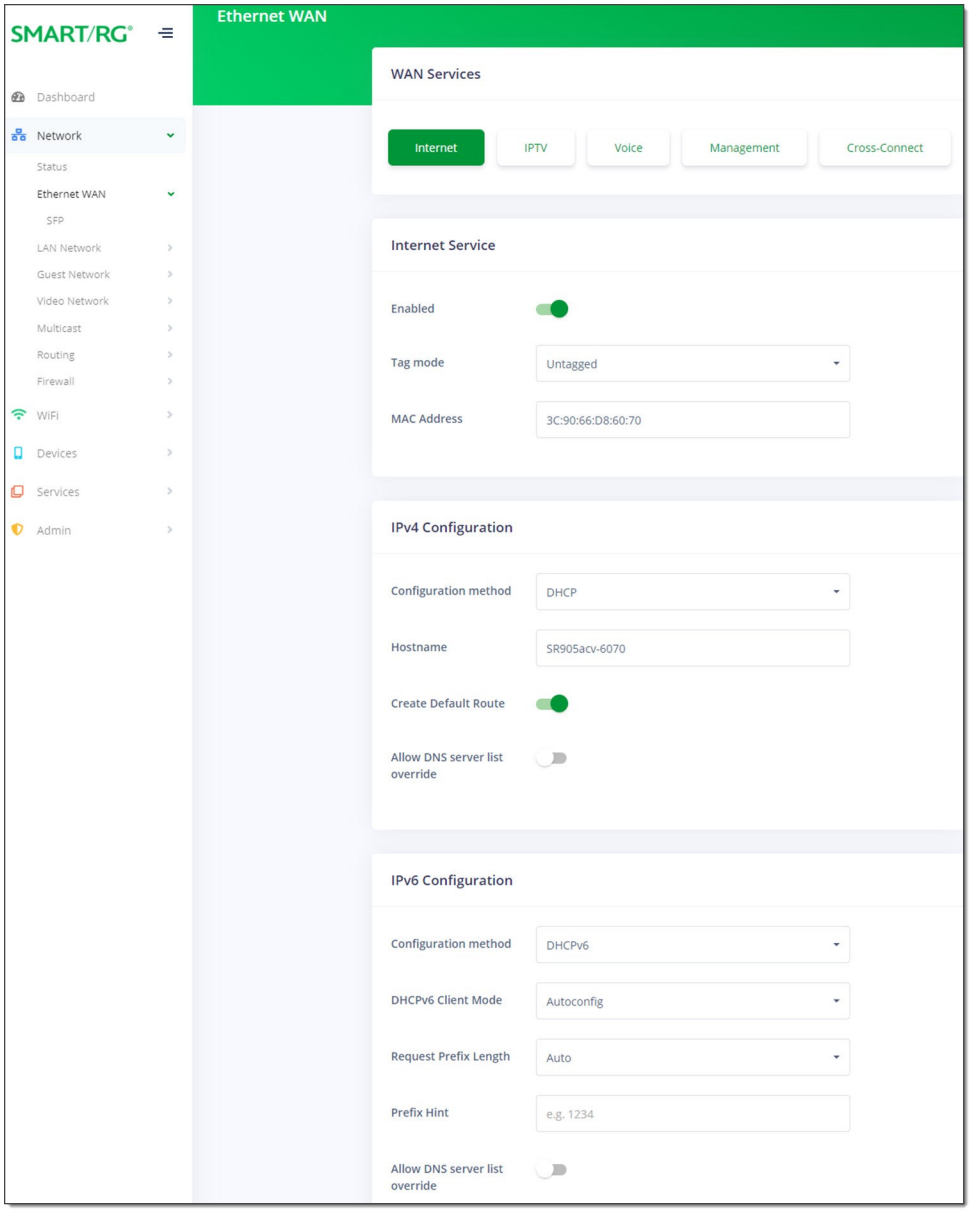
To restart your network, click the **Restart Network** button near the upper right. A Warning message appears. Click **Ok, restart** to proceed. The **STATUS** column for WAN may briefly change to **PENDING** and then back to the previous status.

To view detailed transmission data for the individual interfaces, click the **View Charts** button near the upper-right. The netdata window opens in a new tab, showing information about the overall SR905acv system, memory, CPUs, firewall, IPv4 networking, etc. Use the navigation menu at right to select the statistics that you want to view.

Ethernet WAN

On this page, you can configure WAN settings for connecting to the Internet via Ethernet.

To access this page, click **Network** > **Ethernet WAN** in the left menu. The following page appears, showing the **Internet** settings.



By clicking the buttons across the top of the page, you can select and configure the following WAN services. Click the links below to see the instructions for each service:

Internet

1. When you select **Network** > **Ethernet WAN** in the left menu, the Ethernet WAN page appears with the **Internet** settings displayed.
2. By default, the **Internet Service** is *enabled*. To *disable* the Internet feature, click the **slide button** to the right of **Enabled**.
3. Configure the tagging options:
    a. In the **Tag mode** field, select the type of tagging that should be performed. Options are **Untagged**, **Tagged**, and **DQTagged**. The default is **Untagged**.
    b. If **Tagged** or **DQTagged** is selected, the **VLAN** and **P-bit** fields appear. Enter the ID of the appropriate VLAN. Valid values are **1** - **4079**. The default is **2**. Enter the P-bit type. Options are **0** - **7**. The default is **0**.
    c. If **DQTagged** is selected, the **CVID** field also appears. Enter the Customer VLAN ID or the first in a range of CVIDs that will be accepted and mapped to the specified WAN. Valid values are **1** - **4062**. The default is **0**.
4. (*Optional*) In the **MAC Address** field, enter the MAC address to be used with this configuration. By default, this value is the gateway MAC address.
5. Complete the fields for **IPv4 Configuration** and **IPv6 Configuration** sections as they apply to your environment, using the information provided below.
    a. In the **Configuration method** field, select the appropriate method for your WAN.

    Options for IPv4 WANs are **DHCP**, **Static Address**, and **PPPoE**. The default is **DHCP**.

    Options for IPv6 WANs are **DHCPv6**, **Static Address**, and **None**. The default is **DHCPv6**.

    b. Complete the remaining fields as instructed below for each option:
        - "DHCP for IPv4 WANs" (IPoE)
        - "Static Address for IPv4 WANs"
        - "PPPoE for IPv4 WANs"
        - "DHCPv6 for IPv6 WANs"
        - "Static Address for IPv6 WANs"
6. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

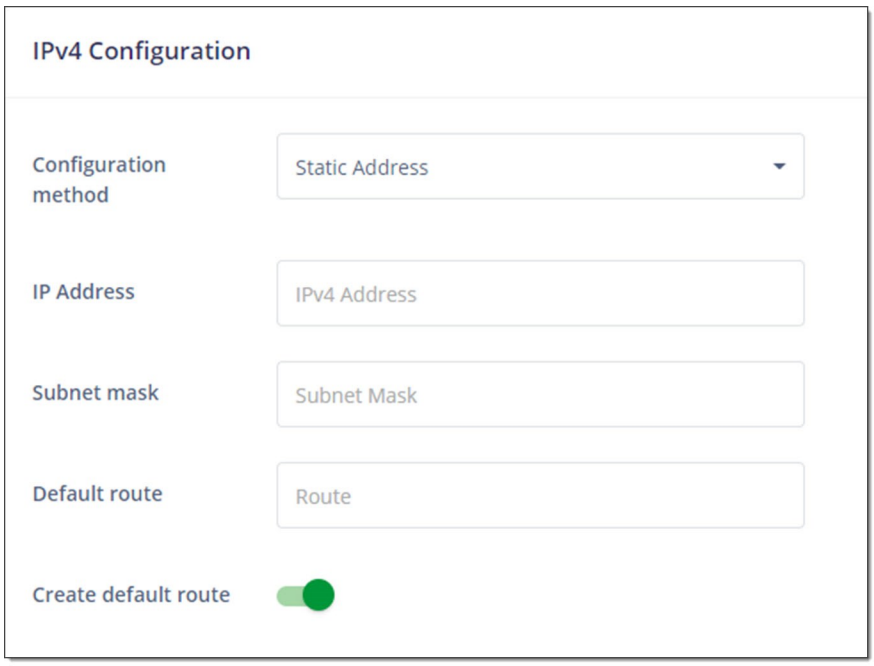
DHCP for IPv4 WANs

The following fields appear when **DHCP** is selected as the configuration method. This method is the default for IPv4 WANs.

1. To use a different host, enter the host name that you want to include in DHCP requests in the **Hostname** field.
2. To *disable* the default route for this WAN, click the **slide button** next to **Create default route**.
3. To *allow* override of the DNS server list, click the **slide button** next to **Allow DNS server list override**. To *prevent* override, click the **slide button** again.
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Static Address for IPv4 WANs

The following fields appear when **Static Address** is selected as the configuration method.



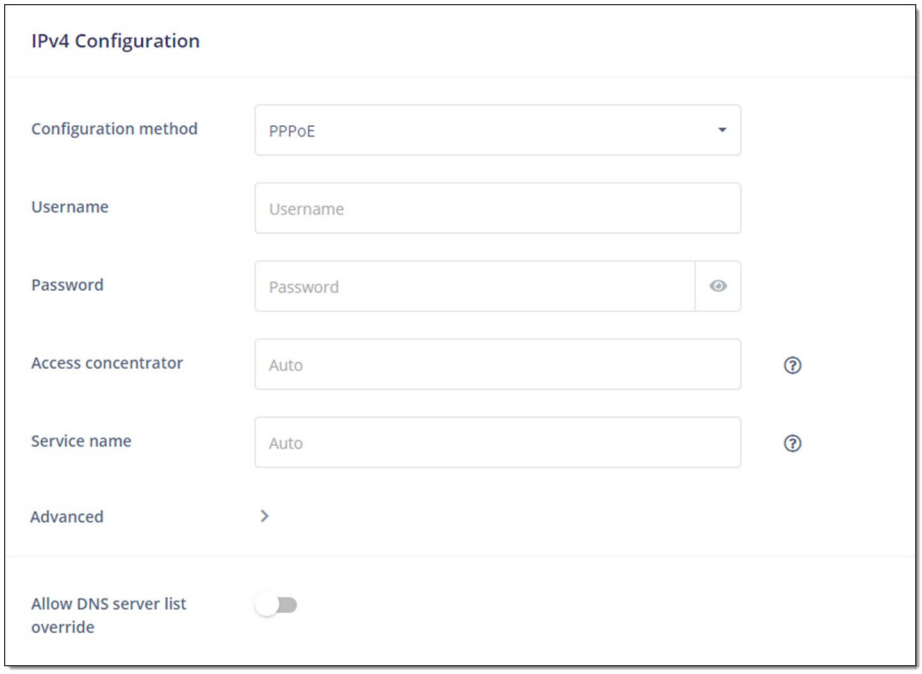
1. Complete the fields using the information in the table below.
2. To *disable* the default route for this WAN, click the **slide button** to the right of **Create default route**.
3. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

The fields for this option are explained in the table below.

Field	Description
IP Address	Enter the IP address for IPv4 communications (such as 192.168.1.44).
Subnet mask	Enter the IP address for the subnet mask.
Default route	Enter the IP address for the default IPv4 route.

PPPoE for IPv4 WANs

The following fields appear when **PPPoE** is selected as the configuration method.



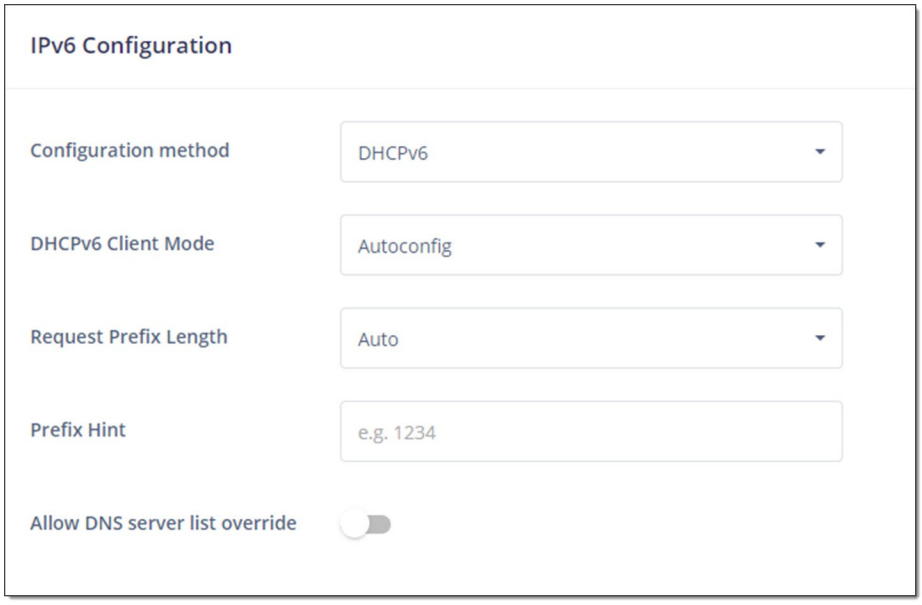
1. To access LCP and PPP settings, click the down arrow next to Advanced.
2. Complete the fields using the information in the table below.
3. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

The fields for this option are described in the following table.

Field	Description
Username	Enter the user ID for this WAN.
Password	Enter the password for this WAN. To view the password characters, click the **Show** icon ( ).
Access concentrator	Enter the name of the concentrator application. To have the system detect this automatically, accept the default of **Auto**
Service name	Enter the name of the service for this interface. To have the system detect this automatically, accept the default of **Auto**
Advanced section	
LCP Echo Interval	Enter the interval for sending echoes in seconds. Options are **1** - **60** seconds. The default is **None**.
LCP Echo Retry	Enter the number of ping retries before the connection is identified as down. The default is **None**.
PPP Persist	PPP persistent dialing ensures that a dropped call link is rebuilt. To *enable* PPP persistence, click the **slide button**.
PPP Holdoff	Enter the number of seconds before attempting to reconnect a dropped call. The default is **zero (0)**.
Allow DNS server list override	(*Optional*) To *allow* override of the DNS server list, click the **slide button**. To *prevent* override, click the **slide button** again.

DHCPv6 for IPv6 WANs

The following fields appear when **DHCPv6** is selected as the configuration method. This method is the default for IPv6 WANs.



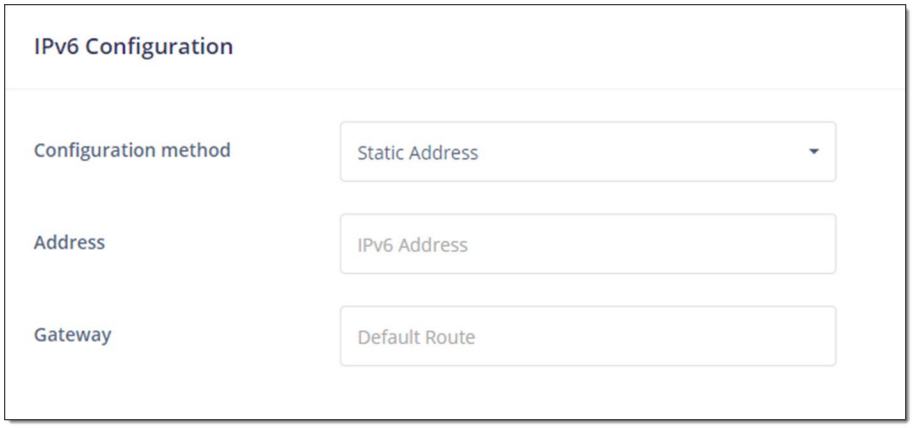
1. Complete the fields using the information in the table below.
2. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

The fields for this option are described in the following table.

Field	Description
DHCPv6 Client Mode	Select the mode for the DHCPv6 client. Options are: • **Autoconfig**: Attempt to use the DHCP server for configuration. If no IP address is provided, then use SLACC for configuration. This is the default. • **Stateful**: Use only the IP address provided by the DHCP server. • **Stateless**: Use only SLACC for configuration.
Request Prefix Length	Select the length of the prefix sent with the request. Options are **Auto, 48**, **52**, **56**, **59** - **64**, and **None**. The default is **Auto**.
Prefix Hint	Enter the 4-digit hint for the subprefix ID.
Allow DNS server list override	(*Optional*) To *allow* override of the DNS server list, click the **slide button**. To *prevent* override, click the **slide button** again.

Static Address for IPv6 WANs

The following fields appear when **Static Address** is selected as the configuration method.



1. Complete the fields using the information in the table below.
2. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

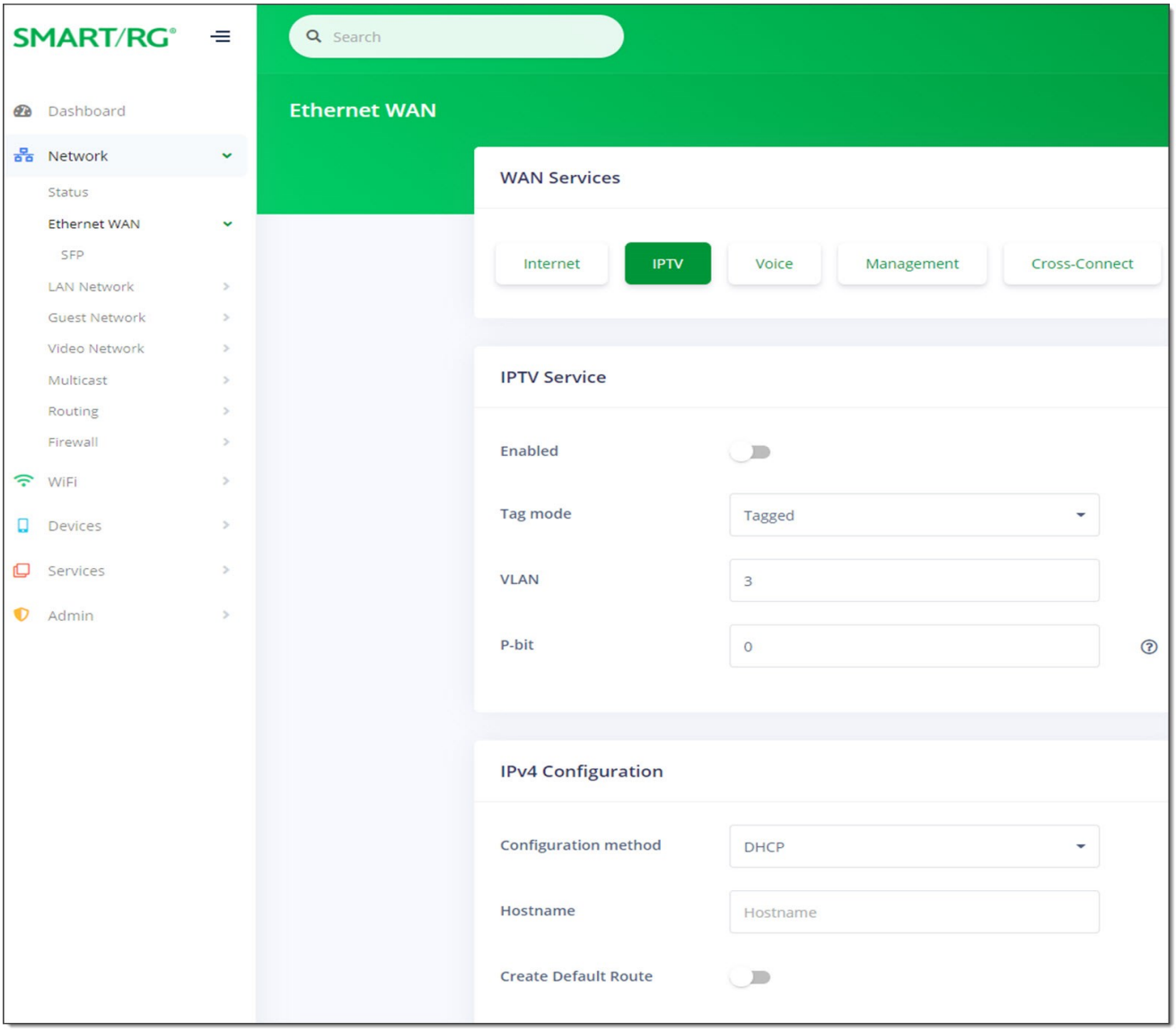
Complete the fields using the information in the table below.

Field	Description
Address	Enter the static address for IPv6 communications (such as 2001:db8:a0b:12f0::1).
Gateway	Enter the IP address for the default IPv6 route.

IPTV

On this page, you can configure the IPTV settings for your Ethernet WAN.

1. In the left menu, click **Network** > **Ethernet WAN**. The Ethernet WAN page appears, showing the **Internet** settings.
2. Click the **IPTV** button. The following page appears.



3. To *enable* the IPTV feature, click the **slide button** to the right of **Enabled**.
4. Configure the tagging options:
    a. In the **Tag mode** field, select the type of tagging that should be performed. Options are **Untagged** and **Tagged**. The default is **Tagged**.

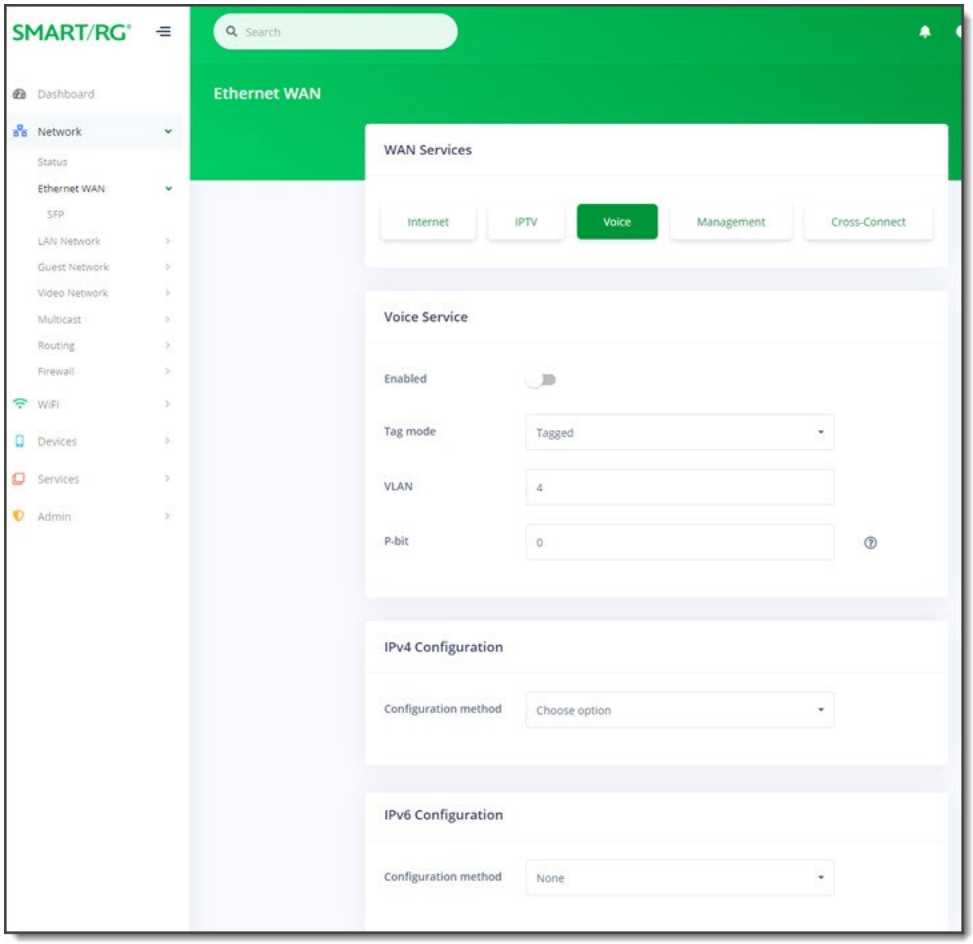
b. If **Tagged** is selected, the **VLAN** and **P-bit** fields appear. Enter the ID of the appropriate VLAN. Valid values are **1** - **4079**. The default is **3**. Enter the P-bit type. Options are **0** - **7**. The default is **0**.

5. In the **IPV4 Configuration** section, configure the settings using the information in "DHCP for IPv4 WANs" and "Static Address for IPv4 WANs".
6. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Voice

On this page, you can configure the voice settings for your Ethernet WAN.

1. In the left menu, click **Network** > **Ethernet WAN**. The Ethernet WAN page appears, showing the **Internet** settings.
2. Click the **Voice** button. The following page appears.



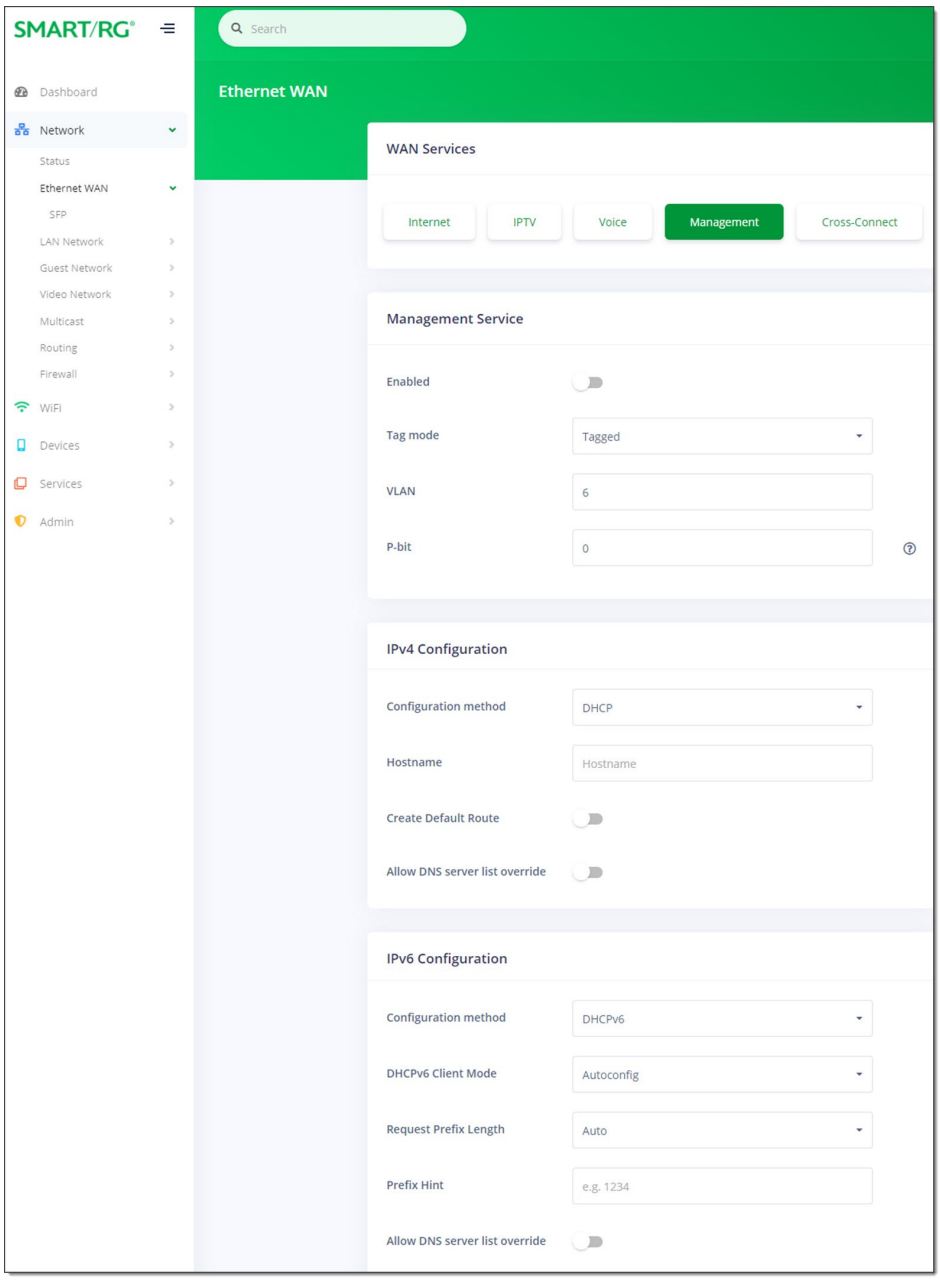
3. To *enable* the Voice feature, click the **slide button** to the right of **Enabled**.
4. Configure the tagging options:
    a. In the **Tag mode** field, select the type of tagging that should be performed. Options are **Untagged**, **Tagged**, and **DQTagged**. The default is **Tagged**.

   b. If **Tagged** or **DQTagged** is selected, the **VLAN** and **P-bit** fields appear. Enter the ID of the appropriate VLAN. Valid values are **1** - **4079**. The default is **4**. Enter the P-bit type. Options are **0** - **7**. The default is **0**.
   c. If **DQTagged** is selected, the **CVID** field also appears. Enter the Customer VLAN ID or the first in a range of CVIDs that will be accepted and mapped to the specified WAN. Valid values are **1** - **4062**.
   The default is **0**.
5. In the **IPV4 Configuration** section, configure the settings using the information in "DHCP for IPv4 WANs", "Static Address for IPv4 WANs", or "PPPoE for IPv4 WANs".
6. In the **IPV6 Configuration** section, configure the settings using the information in "DHCPv6 for IPv6 WANs" and "Static Address for IPv6 WANs".
7. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Management

On this page, you can configure the settings for managing your network and the devices connected to it.

1. In the left menu, click **Network** > **Ethernet WAN**. The Ethernet WAN page appears, showing the **Internet** settings.
2. Click the **Management** button. The following page appears.



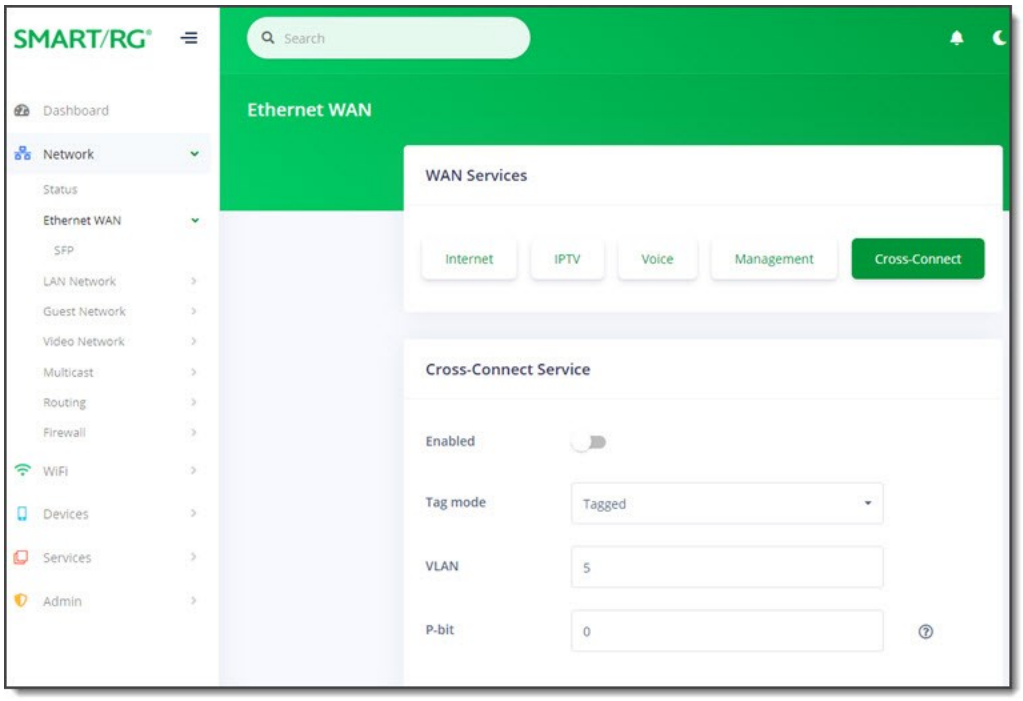
1. To *enable* the Management feature, click the **slide button** to the right of **Enabled**.
2. Configure the tagging options:
    a. In the **Tag mode** field, select the type of tagging that should be performed. Options are **Untagged**, **Tagged**, and **DQTagged**. The default is **Tagged**.

   b. If **Tagged** or **DQTagged** are selected, the **VLAN** and **P-bit** fields appear. Enter the ID of the appropriate VLAN. Valid values are **1** - **4079**. The default is **6**. Enter the P-bit type. Options are **0** - **7**. The default is **0**.
   c. If **DQTagged** is selected, the **CVID** field also appears. Enter the Customer VLAN ID or the first in a range of CVIDs that will be accepted and mapped to the specified WAN. Valid values are **1** - **4062**. The default is **0**.
3. In the **IPV4 Configuration** section, configure the settings using the information in "DHCP for IPv4 WANs", "Static Address for IPv4 WANs", or "PPPoE for IPv4 WANs".
4. In the **IPV6 Configuration** section, configure the settings using the information in "DHCPv6 for IPv6 WANs" and "Static Address for IPv6 WANs".
5. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Cross-Connect

On this page, you can configure bridge settings for traffic moving from a WAN-side VLAN to a LAN port. This can be used for bridged IPTV or other services.

1. In the left menu, click **Network** > **Ethernet WAN**. The Ethernet WAN page appears, showing the **Internet** settings.
2. Click the **Cross-Connect** button. The following page appears.



3. To *enable* the Cross-Connect feature, click the **slide button** to the right of **Enabled**.
4. Configure the tagging options:
   a. In the **Tag mode** field, select the type of tagging that should be performed. Options are **Untagged**, **Tagged**, and **DQTagged**. The default is **Tagged**.
   b. If **Tagged** or **DQTagged** is selected, the **VLAN** and **P-bit** fields appear. Enter the ID of the appropriate VLAN. Valid values are **1** - **4079**. The default is **5**. Enter the P-bit type. Options are **0** - **7**. The default is **0**.

c. If **DQTagged** is selected, the **CVID** field also appears. Enter the Customer VLAN ID or the first in a range of CVIDs that will be accepted and mapped to the specified WAN. Valid values are **1** - **4062**. The default is **0**.

5. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

SFP

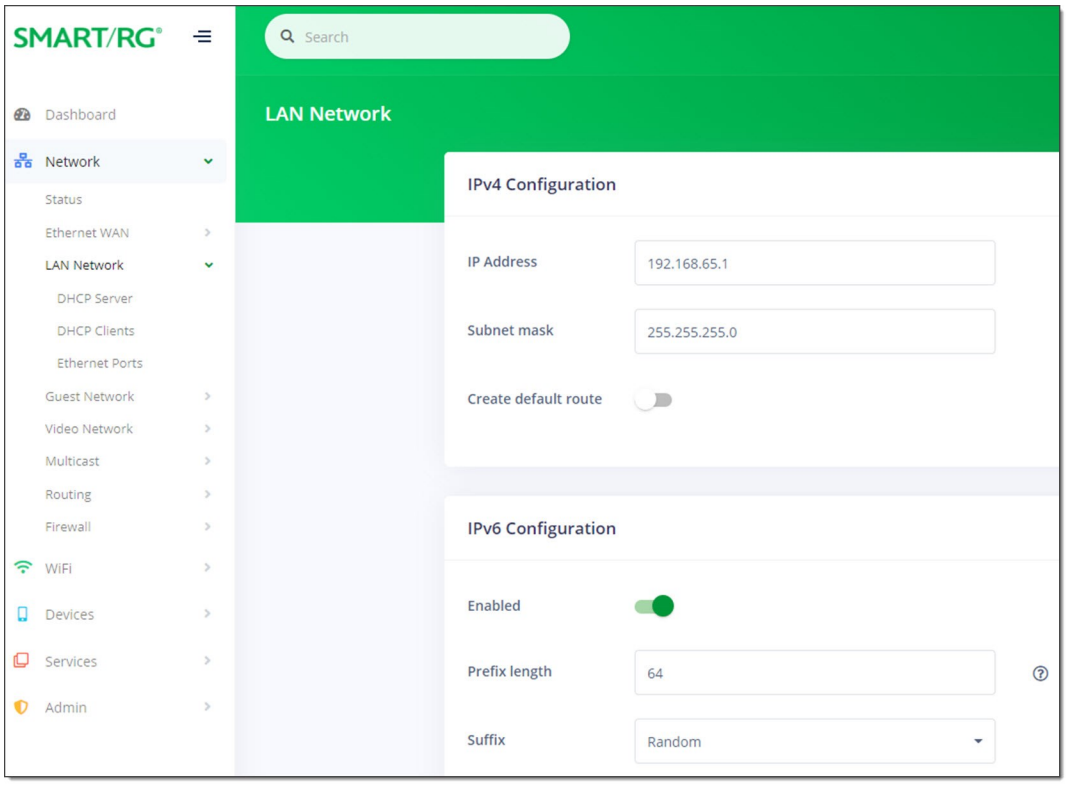
On this page, you can view SFP status and statistics for your fiber service including fiber length, vendor details, and transmission power. SM8 GPON and off-the-shelf Gigabit Ethernet modules are supported.

In the left menu, click **Network** > **Ethernet WAN** > **SFP**. The following page appears. If an SFP module is connected to the gateway, detailed information appears on this page.

LAN Network

In this section, you can view and configure information about the DHCP server, DHCP clients and Ethernet ports.

1. In the left menu, click **Network** > **LAN Network**. The following page appears.



2. Fill in the fields using the information in the table below.
3. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

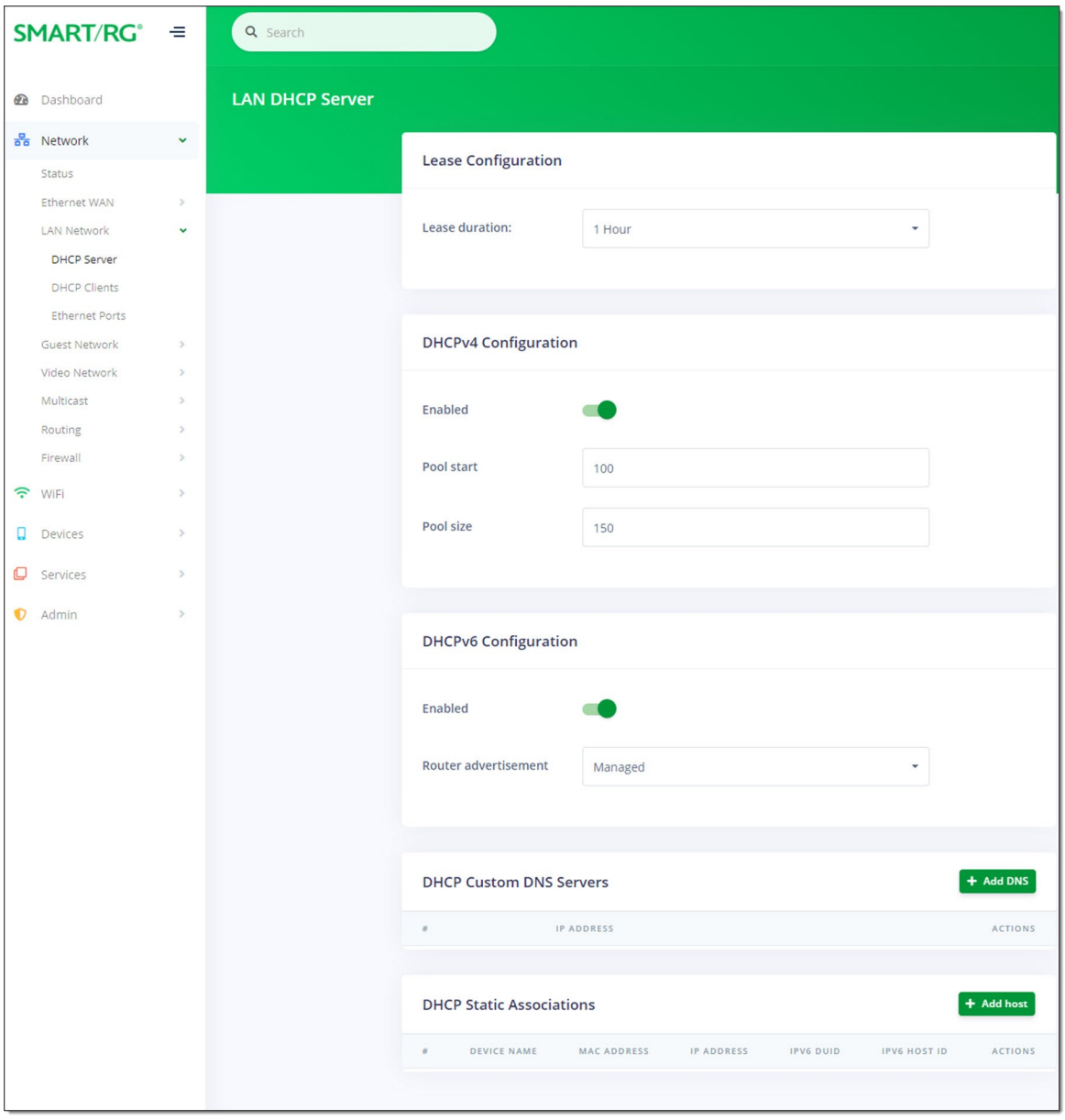
Field	Description
IPv4 Configuration section	
IP Address	Enter the IP address for IPv4 communications (such as 192.168.1.44). The default is the address assigned to the gateway.
Subnet mask	Enter the IP subnet mask for this gateway. The default is **255.255.255.0**.
Create default route	To create a default route for this WAN, click the **slide button** to the right of **Create default route**.
IPv6 Configuration section	
Enabled	This option is *enabled* by default. To *disable* IPv6 address configuration, click the **slide button** to the right of **Enabled**. The **Prefix length** and **Suffix** fields are hidden.
Prefix length	Enter the prefix length for this IPv6 address. Options are **0** - **64**. The default is **64**.

Field	Description
Suffix	Select the interface identifier for this IPv6 address. Options are **Random**, **MAC Based**, and **Suffix Address**. The default is **Random**. If you select **Suffix Address**, the **Suffix Address** field appears. Enter the address in format: "::a:b:c:d".

DHCP Server

On this page, configure the DHCP settings for the gateway. The Dynamic Host Control Protocol Server (DHCP) feature of this gateway will automatically assign LAN IP addresses to host devices as they connect.

1. In the left menu, click **Network** > **LAN Network** > **DHCP Server**. The following page appears.



2. Fill in the fields using the information in the table below.
3. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

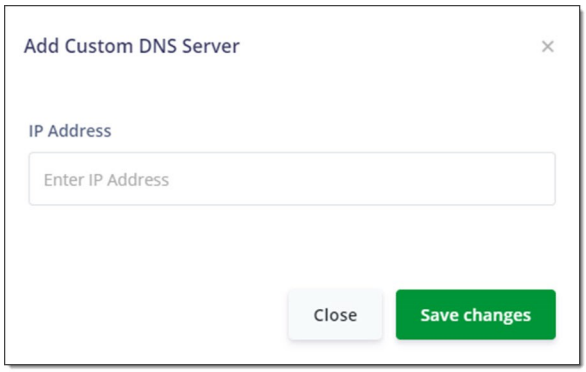
Field	Description
Lease duration	Select how long an IP address will be leased. Options range from **5 minutes** to **24 hours**. The default is **1 Hour**.

Field	Description
DHCPv4 Configuration	
Enabled	This feature is *enabled* by default. To *disable* this feature, click the **slide button**.
Pool start	Enter the beginning of the class-C IP address range to be assigned by the DHCP server. The default is **100**.
Pool size	Enter the size of the DHCP pool. The maximum size allowed is **252**. The default is **150**.
DHCPv6 Configuration	
Enabled	This feature is *enabled* by default. To *disable* this feature, click the **slide button**.
Router advertisement	Select how this gateway will be advertised through this DHCPv6 server. Options are: • **Assisted**: Advertises this gateway with all configuration, with stateless auto-configuration, or both. • **Managed**: Advertises this gateway with all configuration. This is the default. • **Unmanaged**: Advertises this gateway with only stateless auto-configuration.
DHCP Custom DNS Servers	(*Optional*) To define a DNS server, follow the steps in "Defining a Custom DNS Server".
DHCP Static Associations	(*Optional*) To define a static DHCP server, follow the steps in "Defining a Static DHCP IP Address".

Defining a Custom DNS Server

If desired, a static IP address may be associated with the MAC address of a specific LAN host device.

1. To select a LAN client device, click **Add DNS** to the right of the **DHCP Custom DNS Servers** section heading. The Add Custom DNS Server dialog box appears.



2. Enter the IP address of the host device (such as 192.168.1.44).
3. Click **Save changes** to commit your changes.

To add another DNS server, repeat Steps 1-3.

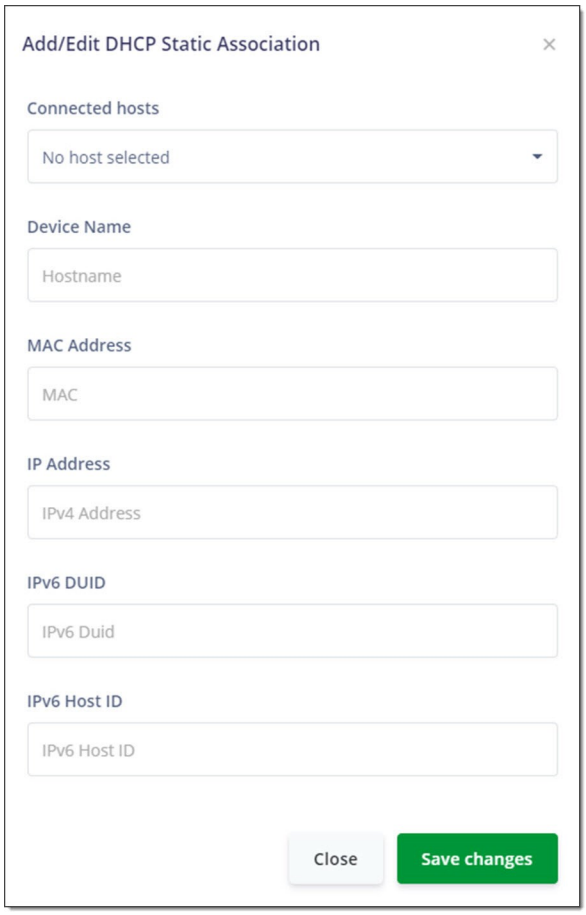
To edit a static DHCP IP address, click the **Edit** () icon next to it. The Add/Edit dialog box appears. Change the entries as needed and click **Save Changes** to commit your changes.

To remove a custom server IP address, click the **Delete** icon ()next to it.

Defining a Static DHCP IP Address

You can define a static IP address to be associated with the MAC address of a specific LAN host device.

1. To select a LAN client device, click **Add host** to the right of the **DHCP Static Associations** section heading. The **Add/Edit DHCP Static Association** dialog box appears.



2. In the **Connected Hosts** field, select the host server that you want to use as a static host. When you select a connected host, the other fields in the dialog box are populated with the necessary information. If the host is currently offline or you select **None** in this field, you must enter the information manually.
3. Click **Save changes** to commit your changes.

To add another static DHCP configuration, repeat Steps 1-4.

To edit a static DHCP IP address, click the **Edit** icon ( ) next to it. The Add/Edit dialog box appears. Change the entries as needed and click **Save Changes** to commit your changes.

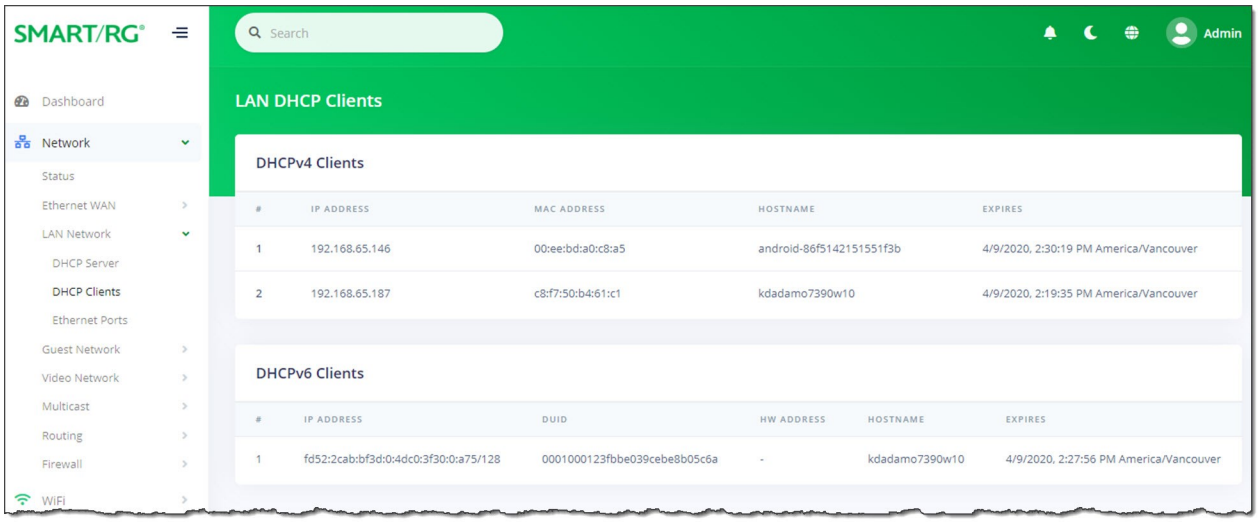
To remove a static DHCP IP address, click the **Delete** icon ( )next to it.

Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

DHCP Clients

On this page, you can view the IPv4 and IPv6 DHCP clients connected to your LAN.

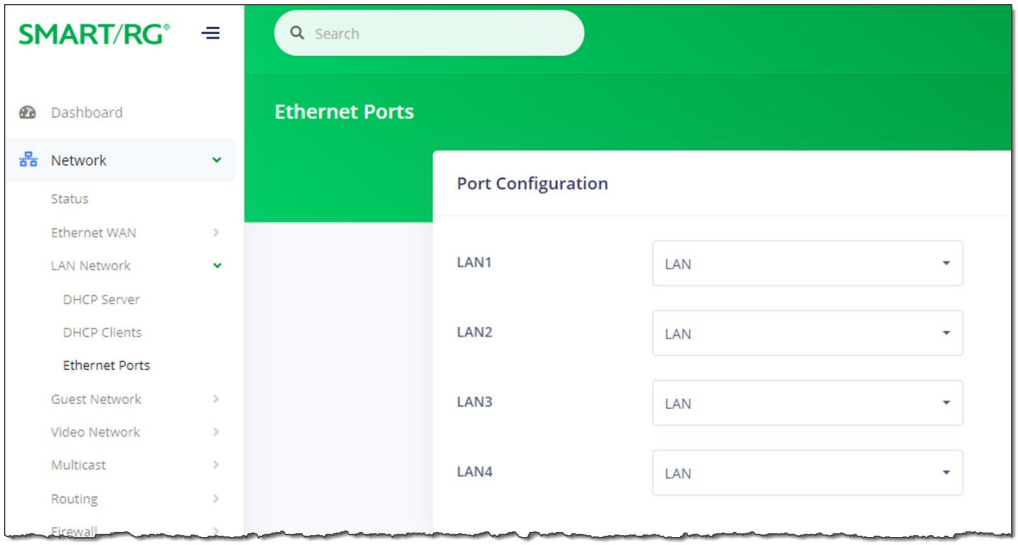
In the left menu, click **Network** > **LAN Network** > **DHCP Clients**. The following page appears.



Ethernet Ports

On this page, you can select which service to run for each interface defined on your gateway.

1. In the left menu, click **Network** > **LAN Network** > **Ethernet Ports**. The following page appears.

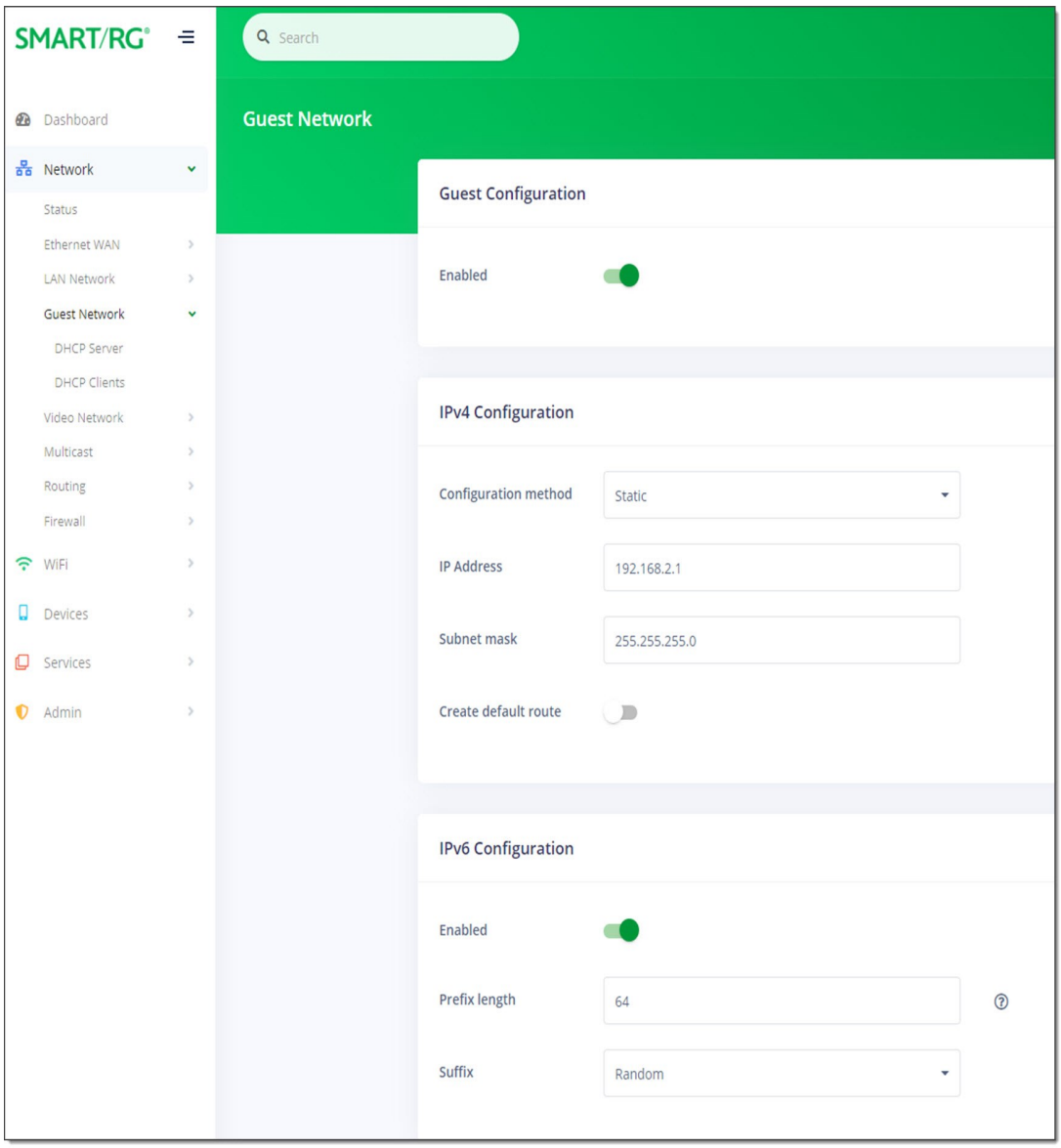


2. Select an option for each port where a particular service is to be defined.
   Options are **LAN**, **Guest**, **Video**, **Voice**, **Cross-Connect**, and **None**. The default is **LAN**.
3. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Guest Network

In this section, you can configure settings for a guest network including a DHCP server.

1. In the left menu, click **Network** > **Guest Network**. The following page appears. This feature is *enabled* by default.



2. To *disable* this feature, click the **slide button** next to **Enabled**.
3. In the **Configuration method** field, select the method for the IPv4 server. Options are **Static**, **DHCP** and **None**. The default is **Static**.

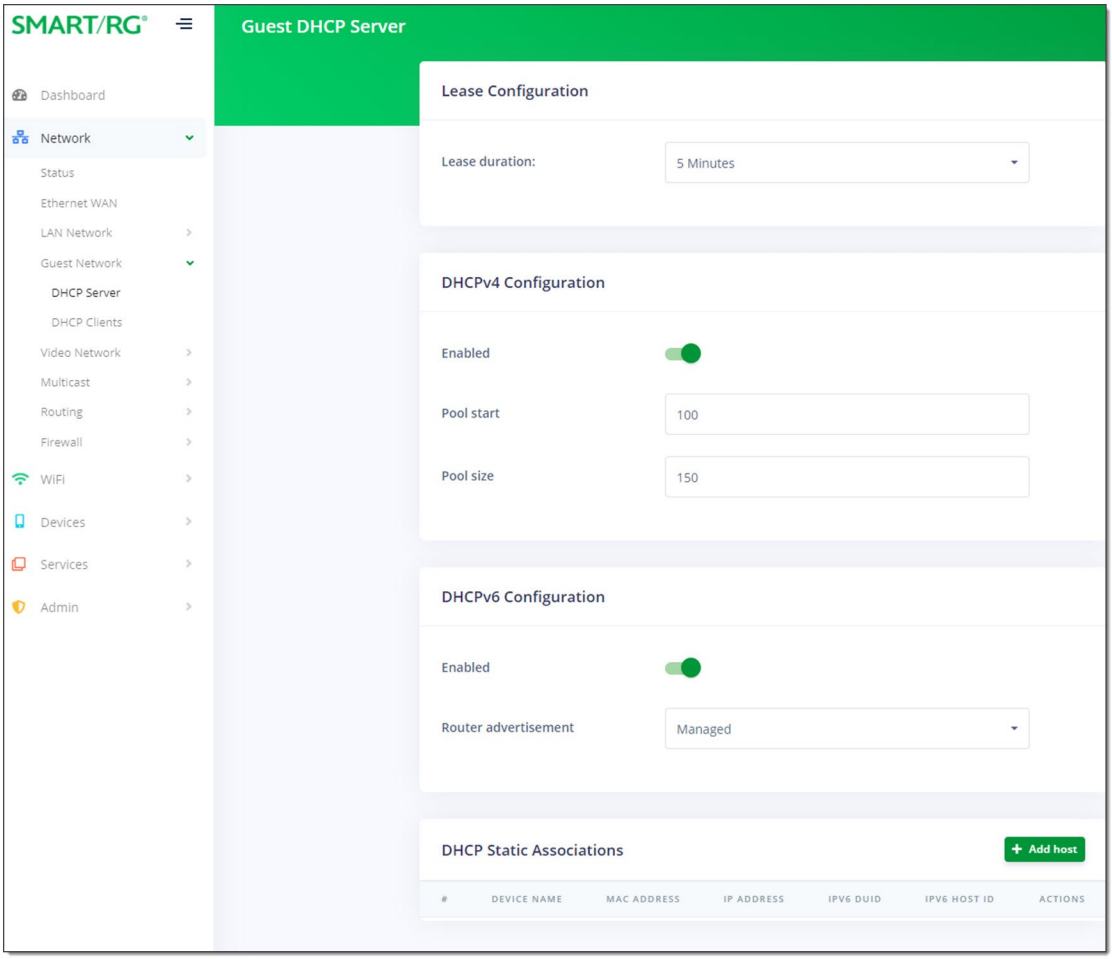
   Note: If you select **None**, the other fields in this section are hidden.
4. To create a default route for this LAN, click the **slide button** to the right of **Create default route**.
5. Fill in the fields using the information in the table below.
6. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Field	Description
IPv4 Settings section - for **Static** configuration method	
IP Address	Enter the IP address for IPv4 communications (such as 192.168.1.1). The default is the address assigned to the gateway.
Subnet Mask	Enter the IP subnet mask for this gateway. The default is **255.255.255.0**.
IPv4 Settings section - for **DHCP** configuration method	
Hostname	(*Optional*) Enter the host name that will display to your users.
IPv6 Settings section	
Enabled	This option is *enabled* by default. To *disable* IPv6 address configuration, click the **slide button** to the right of **Enabled**. The **Prefix Length** and **Suffix** fields are hidden.
Prefix length	Enter the prefix length for the IPv6 server. Options are **0** - **64**.The default is **64**.
Suffix	Select the interface identifier for this IPv6 address. Options are **Random**, **MAC Based**, and **Suffix Address**. The default is **Random**. If you select **Suffix Address**, the **Suffix Address** field appears. Enter the address in format: "::a:b:c:d".

DHCP Server

On this page, you can configure DHCP settings for your guest network.

1. In the left menu, click **Network** > **Guest Network** > **DHCP Server**. The following page appears.



2. Fill in the fields using the information in the table below.
3. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

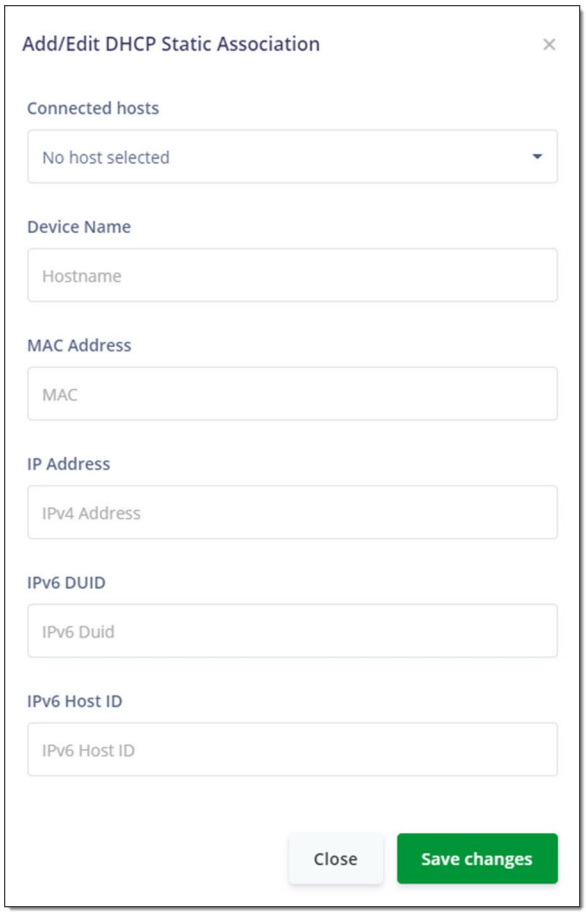
Field	Description
Lease duration	Select how long an IP address will be leased. Options range from **5 minutes** to **24 hours**. The default is **5 minutes**.
DHCPv4 Configuration	
Enabled	This feature is *enabled* by default. To *disable* this feature, click the **slide button**.
Pool start	Enter the beginning of the class-C IP address range to be assigned by the DHCP server. The default is **100**.
Pool size	Enter the size of the DHCP pool. The maximum size allowed is **252**. The default is **150**.
DHCPv6 Configuration section	
Enabled	This feature is *enabled* by default. To *disable* this feature, click the **slide button**.

Field	Description
Router Advertisement	Select how this gateway will be advertised through this DHCPv6 server. Options are **Assisted**, **Managed**, and **Unmanaged**. The default is **Managed**. The **Assisted** option advertises this router with all configuration through a DHCPv6 server *and/or* stateless auto configuration.
DHCP Static Associations	(*Optional*) To define a static DHCP server, follow the steps in "Defining a Static DHCP IP Address".

Defining a Static DHCP IP Address

You can define a static IP address to be associated with the MAC address of one of your LAN host devices.

1. To select a LAN client device, click **Add host** to the right of the **DHCP Static Associations** section heading. The **Add/Edit DHCP Static Association** dialog box appears.



2. In the **Connected Hosts** field, select the host server that you want to use as a static host. When you select a connected host, the fields in the dialog box are populated with the necessary information. If the host is currently offline or you select **None** in this field, you must enter the information manually.
3. Complete the fields, using the information in the table below.
4. Click **Save changes** to commit your changes.

The fields in this dialog box are described in the following table.

Field	Description
Device Name	Enter a name for the host device.
MAC Address	Accept the displayed address or enter the MAC address of the host device (such as 00:23:6A:A3:7C:C3). The MAC address of the device selected in Step 2 appears in this field.
IP Address	Accept the displayed address or enter the IP address of the host device (such as 192.168.1.44). The IP address of the device selected in Step 2 appears in this field.
IPv6 DUID	Enter the DHCP Unique Identifier (DUID) for the IPv6 server.
IPv6 Host ID	Enter the ID for the IPv6 host server.

To add another static DHCP configuration, repeat Steps 1-4.

To edit a static DHCP IP address, click the **Edit** icon ( ) next to it. The Add/Edit dialog box appears. Change the entries as needed and click **Save Changes** to commit your changes.

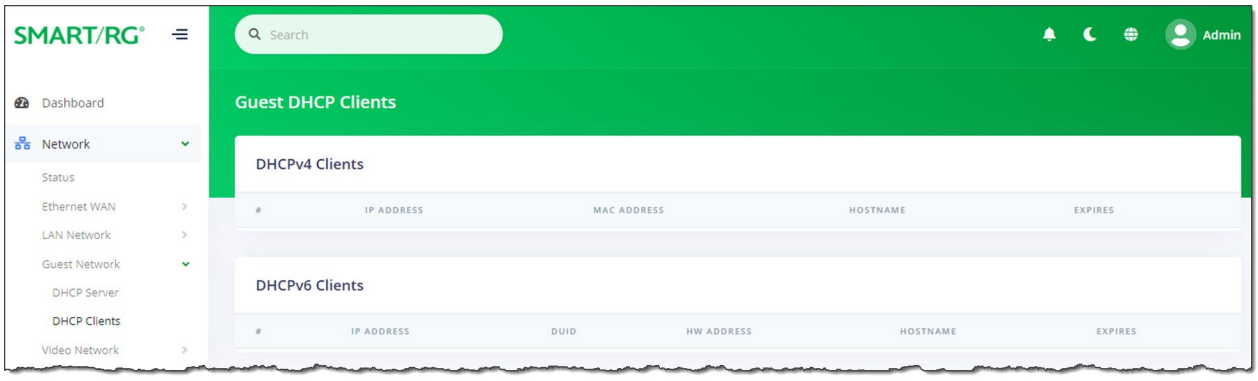
To remove a static DHCP IP address, click the **Delete** icon ( )next to it.

Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

DHCP Clients

On this page, you can view the IPv4 and IPv6 DHCP clients connected to your gateway.

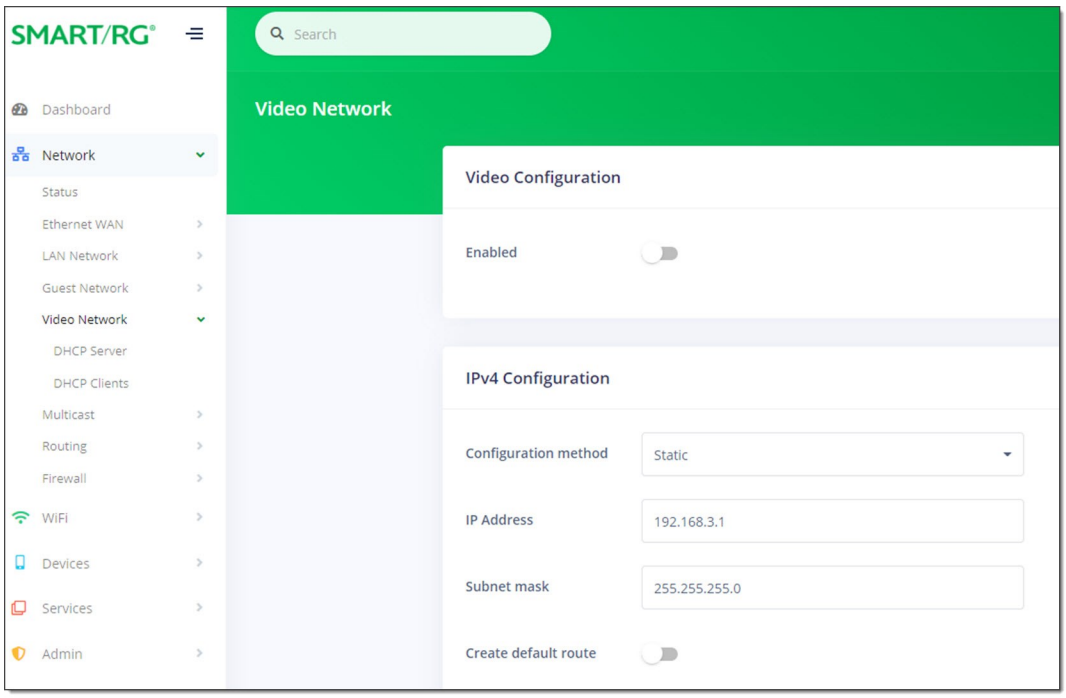
In the left menu, click **Network** > **Guest Network** > **DHCP Clients**. The following page appears.



Video Network

In this section, you can configure WAN settings for video data.

1. In the left menu, click **Network** > **Video Network**. The following page appears. This feature is *disabled* by default.

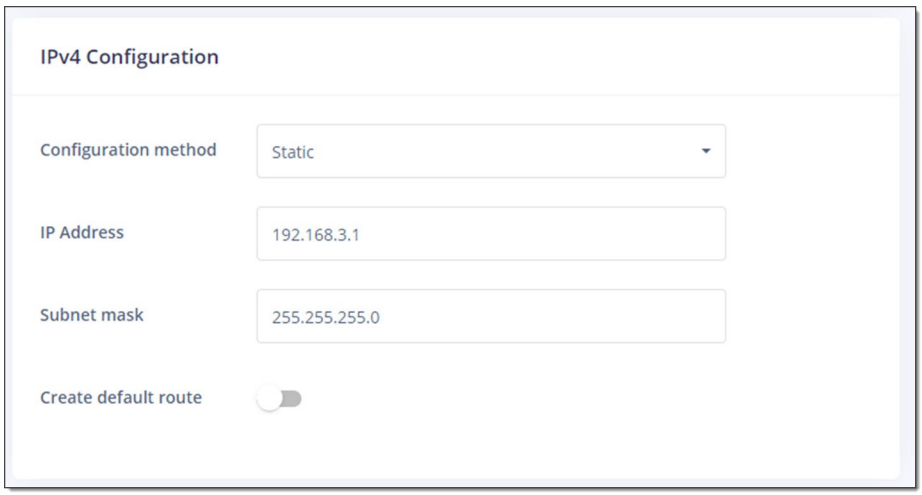


2. To *enable* this feature, click the **slide button** to the right of **Enabled**.
3. In the **Configuration method** field, select the appropriate method for your WAN. Options are **Static**, **DHCP**, and **None**. The default is **Static**. The page refreshes to show the fields that apply for the selected method.

   Note: If you select **None**, the other fields are hidden.
4. Fill in the other fields as explained below for each option:
   - "Static"
   - "DHCP"
5. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Static

When you select **Static** in the **Configuration method** field, the following fields appear.

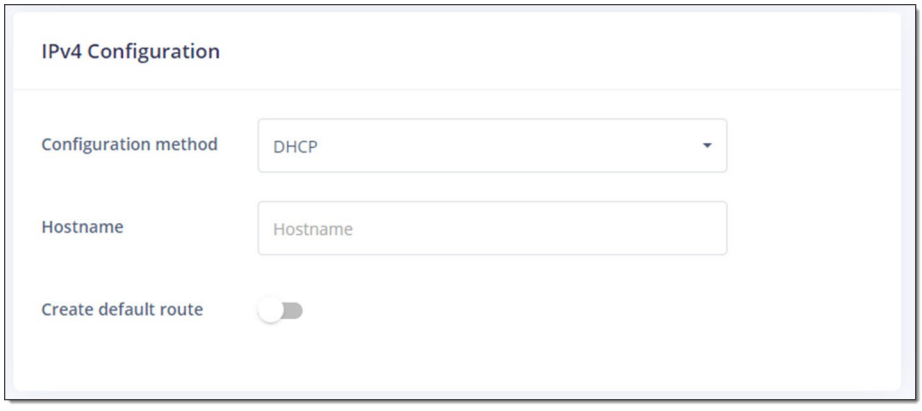


1. Modify the fields using the information in the table below.
2. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Field	Description
IP Address	Enter the IP address for IPv4 communications (such as 192.168.1.44).
Subnet mask	Enter the IP address for the subnet mask.
Create default route	To create a default route for this WAN, click the **slide button** next to **Create default route**.

DHCP

When you select **DHCP** in the **Configuration method** field, the following fields appear.

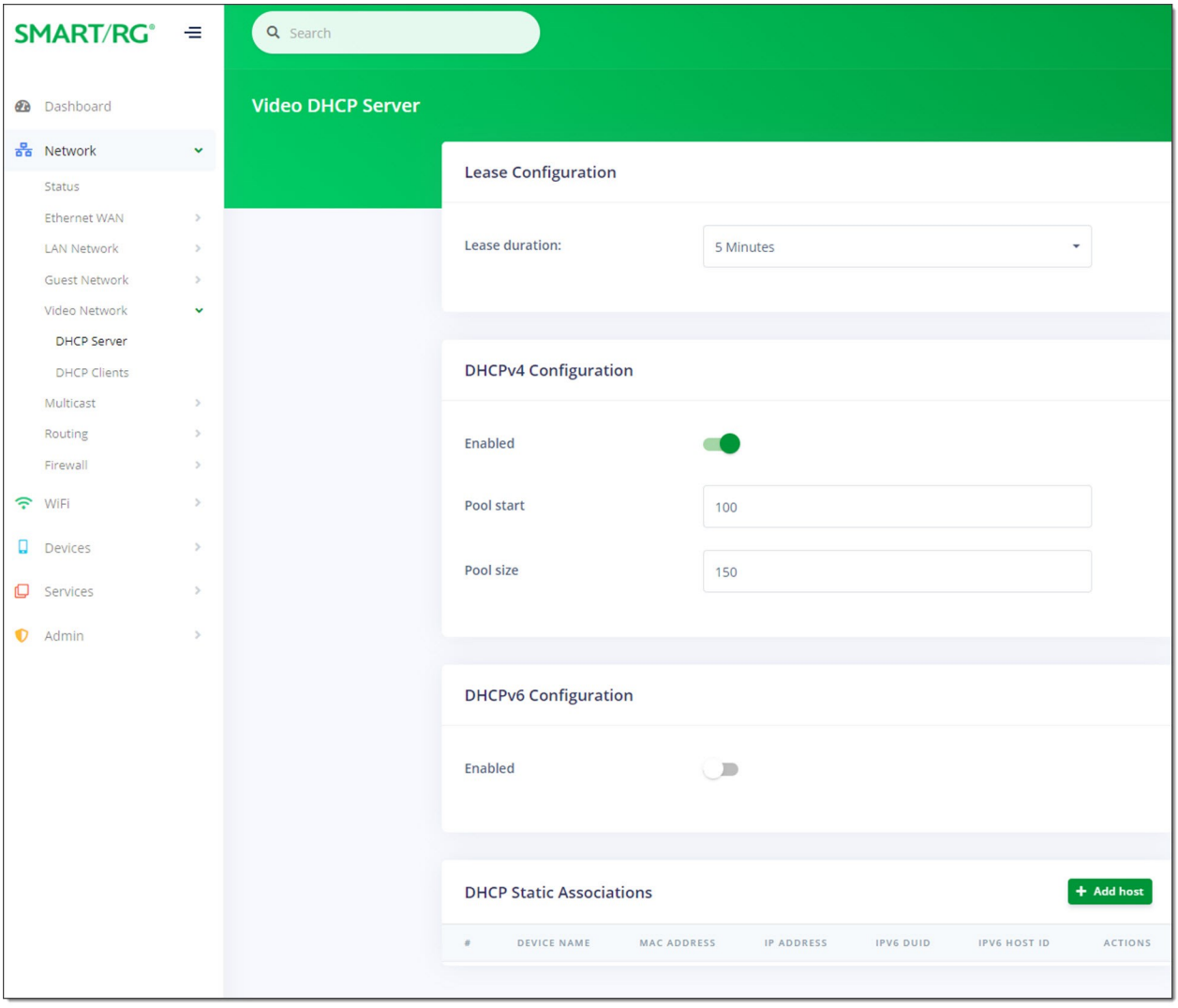


1. (*Optional*) In the **Hostname** field, enter the host name to be included in DHCP requests.
2. To create a default route for this WAN, click the **slide button** next to **Create default route**.
3. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

DHCP Server

On this page, you can configure DHCP settings for the video network.

1. In the left menu, click **Network** > **Video Network** > **DHCP Server**. The following page appears.



2. Fill in the fields using the information in the table below.
3. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

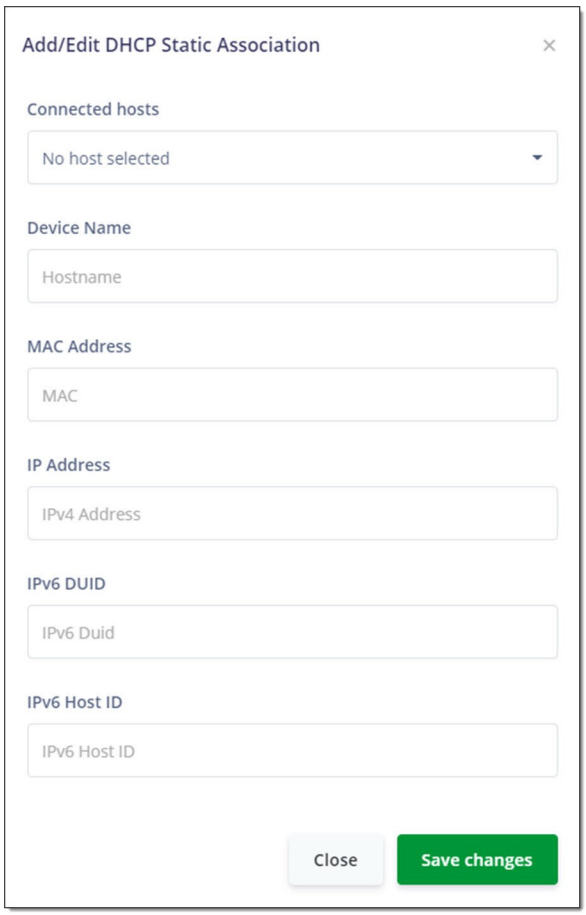
Field	Description
Lease duration	Select how long an IP address will be leased. Options range from **5 minutes** to **24 hours**. The default is **5 minutes**.

Field	Description
DHCPv4 Configuration section	
Enabled	This feature is *enabled* by default. To *disable* this feature, click the **slide button**.
Pool start	Enter the beginning of the class-C IP address range to be assigned by the DHCP server. The default is **100**.
Pool size	Enter the size of the DHCP pool. The maximum size allowed is **252**. The default is **150**.
DHCPv6 Configuration section	
Enabled	This feature is *disabled* by default. To *enable* this feature, click the **slide button**.
Router advertisement	(*Appears when **Enabled** is set to **On***) Select how this gateway will be advertised through this DHCPv6 server. Options are **Assisted**, **Managed**, and **Unmanaged**. The **Assisted** option advertises this router with all configuration through a DHCPv6 server *and/or* stateless auto configuration.
DHCP Static Associations	(*Optional*) To define a static DHCP server, follow the steps in "Defining a Static DHCP IP Address".

Defining a Static DHCP IP Address

You can define a static IP address to be associated with the MAC address of one of your LAN host devices.

1. To select a LAN client device, click **Add host** to the right of the **DHCP Static Associations** section heading. The Add/Edit DHCP Static Association dialog box appears.



2. In the **Connected Hosts** field, select the host server that you want to use as a static host. When you select a connected host, the fields in the dialog box are populated with the necessary information. If the host is currently offline, you must enter the information manually.
3. Complete the fields, using the information in the table below.
4. Click **Save changes** to commit your changes.

To add another static DHCP configuration, repeat Steps 1-4.

To edit a static DHCP IP address, click the **Edit icon** ( ) next to it. The Add/Edit dialog box appears. Change the entries as needed and click **Save Changes** to commit your changes.

To remove a static DHCP IP address, click the **Delete** icon ( ) next to it.

Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

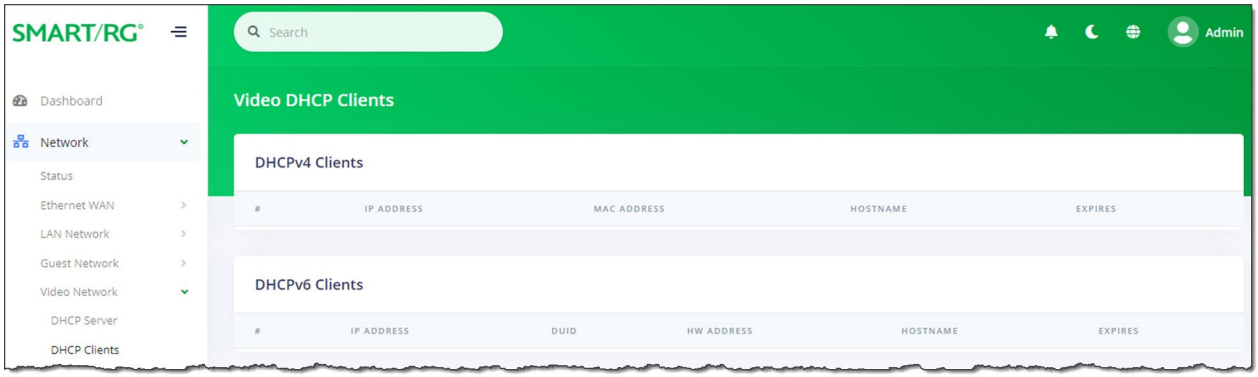
The fields in this dialog box are described in the following table.

Field	Description
Device Name	Enter a name for the host device.
MAC Address	Enter the MAC address of the host device (such as 00:23:6A:A3:7C:C3).
IP Address	Enter the IP address of the host device (such as 192.168.1.44).
IPv6 DUID	Enter the DHCP Unique Identifier (DUID) for the IPv6 server.
IPv6 Host ID	Enter the ID for the IPv6 server.

DHCP Clients

On this page, you can view the IPv4 and IPv6 DHCP clients connected to the video network.

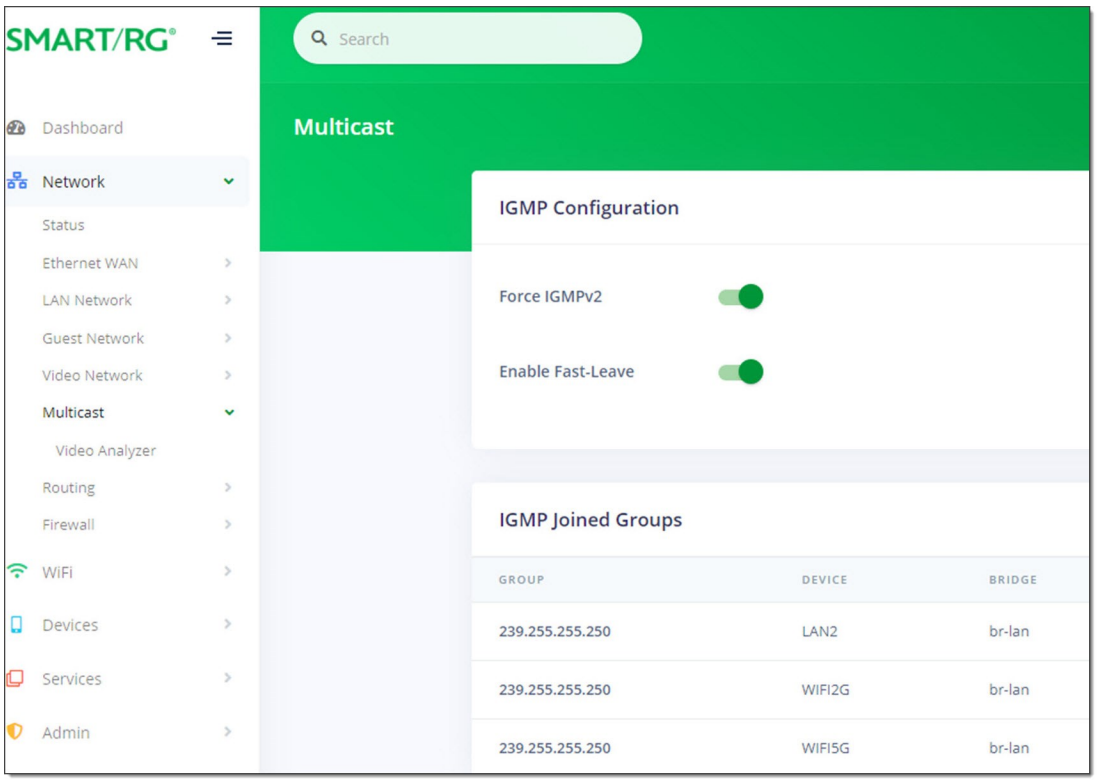
In the left menu, click **Network** > **Video Network** > **DHCP Clients**. The following page appears, showing any active video clients.



Multicast

On this page, you can configure IGMP settings such as the Fast-Leave option and view details of the joined groups including IP address, device name, and bridge ID.

1. In the left menu, click **Network** > **Multicast**. The following page appears.

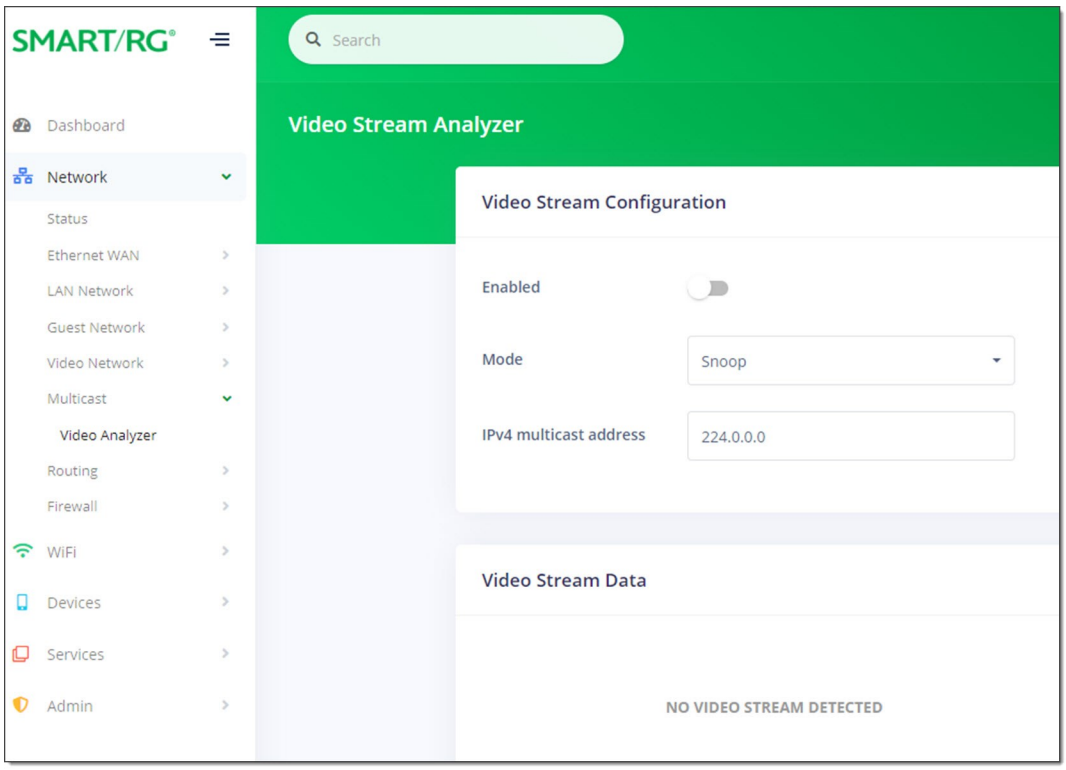


2. (*Optional*) To *disable* the IGMPv2 feature, click the **slide button** next to **Force IGMPv2**.
3. (*Optional*) To *disable* the Fast-Leave feature, click the **slide button** next to **Enable Fast-Leave**.
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Video Analyzer

On this page, you can configure the IP multicast video streams.

1. In the left menu, click **Network** > **Multicast** > **Video Analyzer**. The following page appears. If video is configured for your gateway, data about the video stream appears in the bottom section of the page.



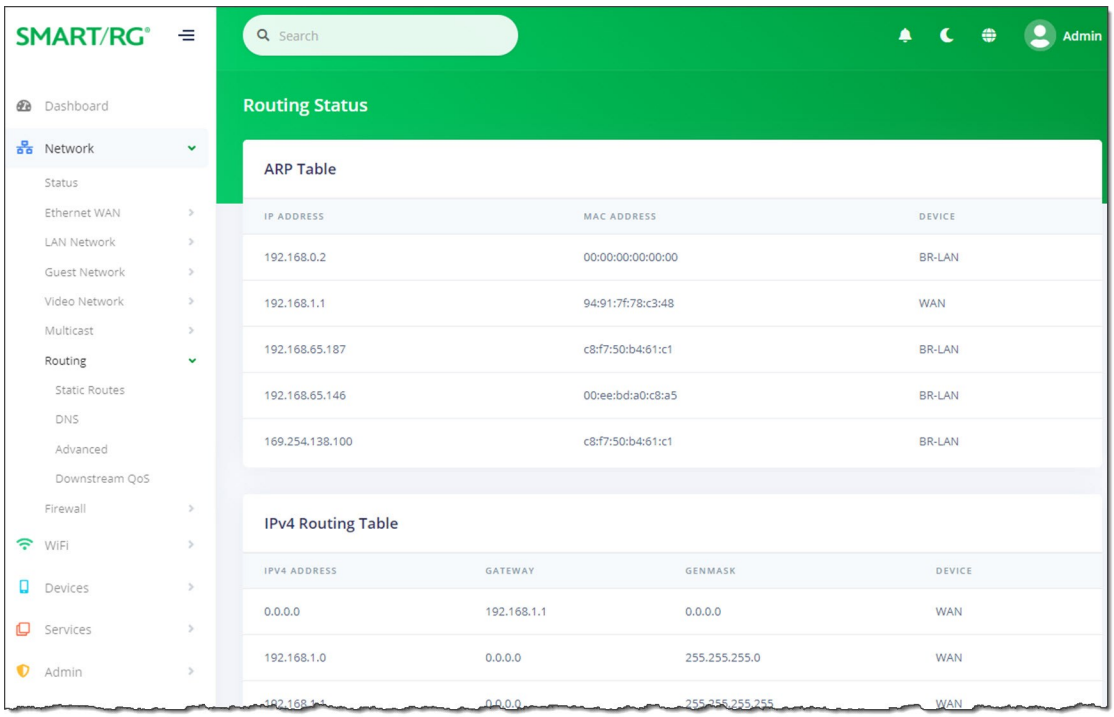
2. To *enable* this feature, click the **slide button** to the right of **Enabled**.
3. In the **Mode** field, select the analyzer mode. Options are **Snoop** and **Join**. The default is **Snoop**.
4. (*Optional*) In the **IPv4 multicast address** field, enter the IP address. Options range from **224.0.0.0** through **239.255.255.255**. The default is **224.0.0.0**.
5. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

In the **Video Stream Data** section, when a video stream is active, the stream summary plus information about the stream rate, media delivery index, packet header, and PID counters are shown.

Routing

On this page, you can view the static routes configured for the network (including tables for ARP, IPv4, IPv6, and IPv6 Neighbors).

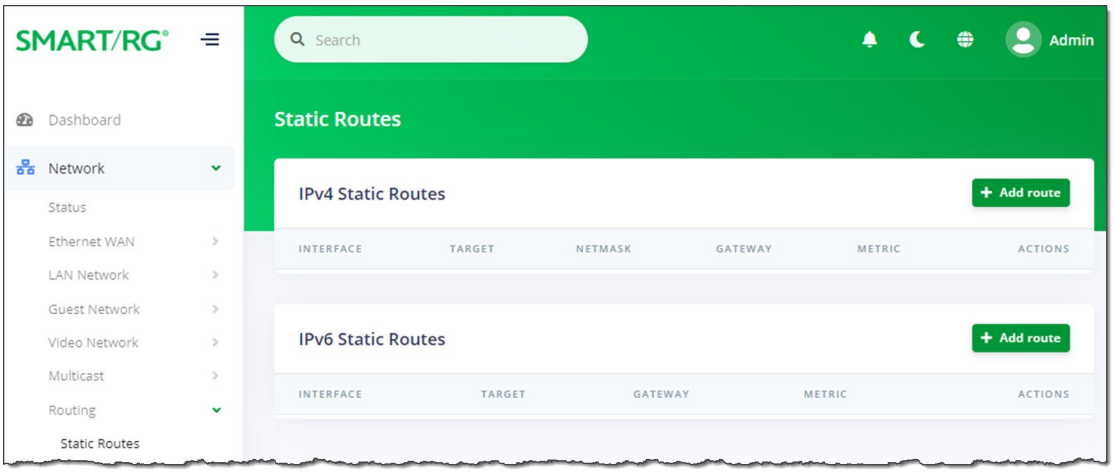
In the left menu, click **Network** > **Routing**. The following page appears.



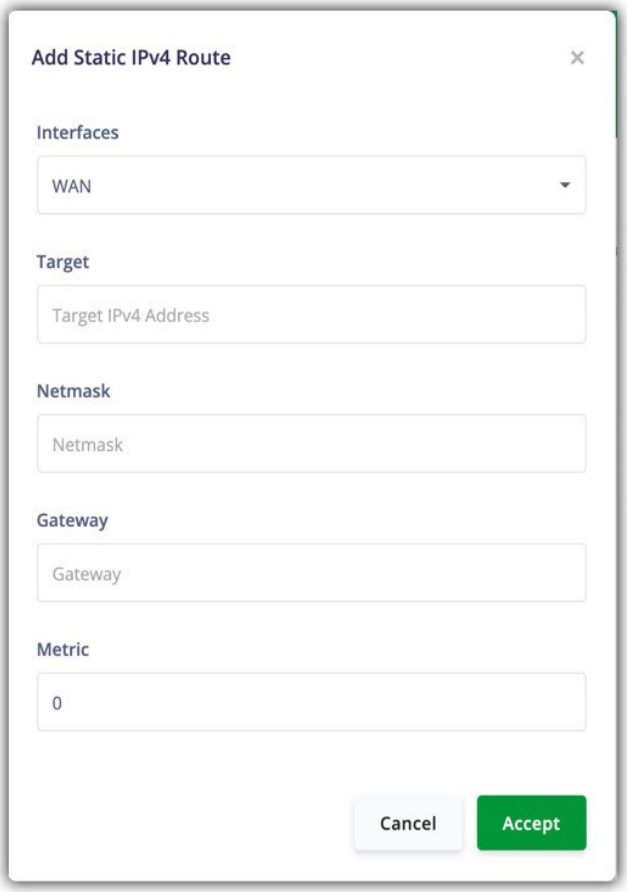
Static Routes

On this page, you can specify the routes over which interface and gateway for a certain host or network can be reached. When several networks are accessible from the gateway, this option is useful to ensure packets get correctly routed between them.

1. In the left menu, click **Network** > **Routing** > **Static Routes**. The following page appears, showing sections for **IPv4 Static Routes** and **IPv6 Static Routes**.



2. Click the **Add Route** button to the right of the heading for the desired IP version. The appropriate Add Static Route dialog box appears.



   a. Complete the fields, using the information provided in the table below.
   b. Click **Accept** to save your changes. You are returned to the Static Routes page.
3. To edit an existing route:
   a. Click the **Edit** icon ( ) to the right of the entry to be edited. The Add Static Route dialog box appears.
   b. Modify the fields as needed and then click **Accept**.
4. To delete a route, click the **Delete** icon ( ) to the right of the entry to be deleted.
5. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

The following table describes the fields on this page.

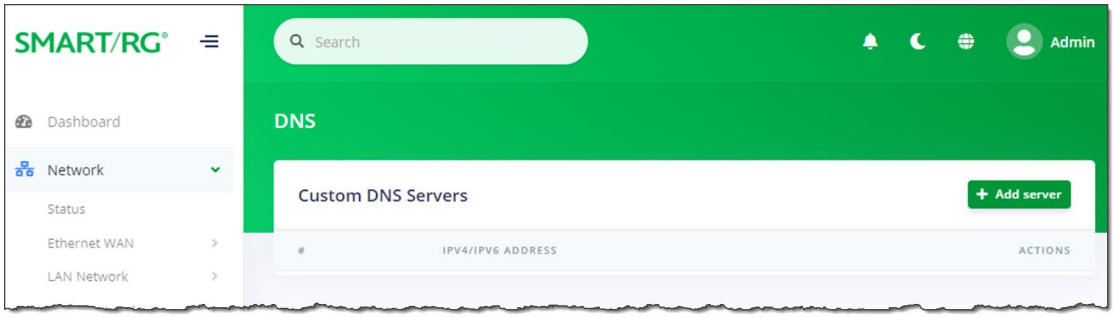
Field Name	Description
Interfaces	Select the interface for the static route.

Field Name	Description
Target	Enter the host IP or network address. Enter specific IP addresses for a single device or identify an entire subnet. e.g., enter 192.168.1.0 to identify that subnet as the target.
Netmask	(*Appears for IPv4 routes only*) Enter the net mask for the target IP address.
Gateway	Enter the gateway address for the route.
Metric	Enter the number of hops needed to reach the default gateway. The default is **0**.

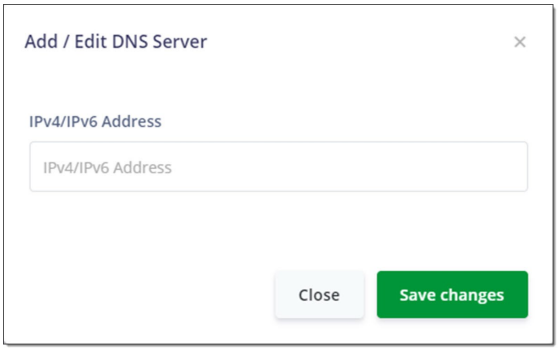
DNS

On this page, you can configure network DNS servers.

1. In the left menu, click **Network** > **Routing** > **DNS**. The following page appears.



2. To add a custom DNS server:
   a. Click the **Add server** button. The **Add/Edit DNS Server** dialog box appears.



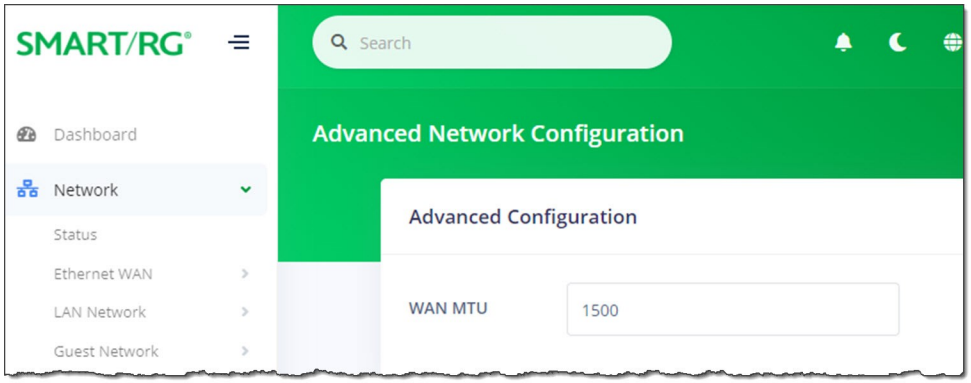
   b. Enter the IP address of the custom DNS server.
   c. Click **Save changes**.
   d. To add another IP address, repeat steps a - c.
3. To change a DNS server address:
   a. Click the **Edit** ( ) icon next to it. The Add/Edit dialog box appears.
   b. Enter the new server address
   c. Click **Save Changes** to commit your changes.

4. To remove a server, click the **Delete** icon ( ) next to it. The list is refreshed.
5. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Advanced

On this page, you can configure the WAN MTU setting.

1. In the left menu, click **Network** > **Routing** > **Advanced**. The following page appears.

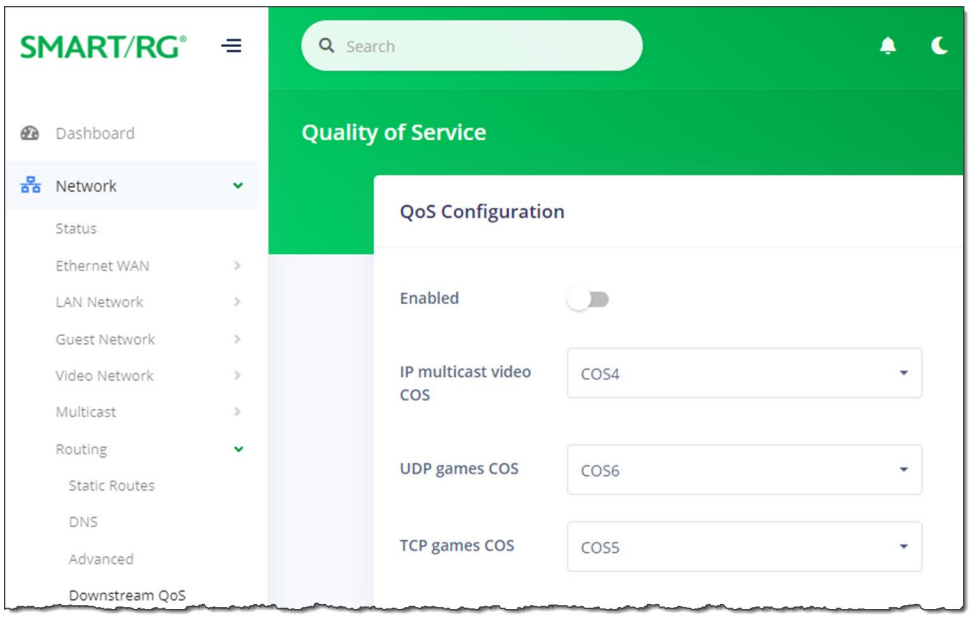


2. Enter or select the MTU (Maximum Transmission Unit) size for the network. Options are **0** - **2048**. The default is **1500**.
3. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Downstream QoS

On this page, configure how traffic is prioritized over wireless networks to improve quality of service.

1. In the left menu, click **Network** > **Routing** > **Downstream QoS**. The following page appears.

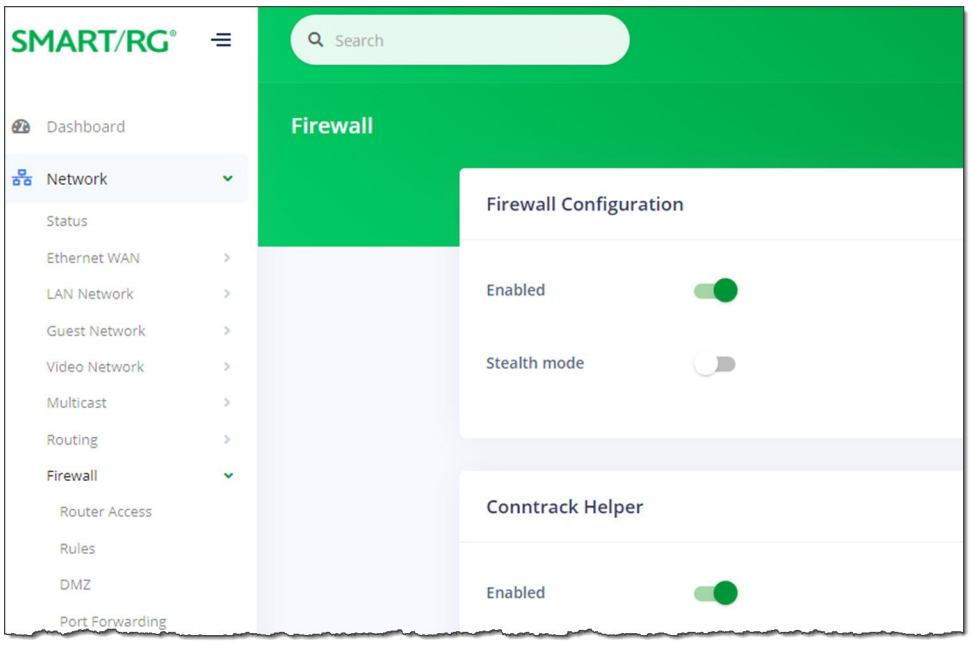


2. To *enable* the quality of service feature, click the **slide button** to the right of **Enabled**.
3. In the three remaining fields, select the appropriate COS (priority) level. Options are **COS7** - **COS0**. The default settings work for most systems.
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Firewall

In this section, you can configure router access, rules, DMZ settings, and port forwarding settings.

1. In the left menu, click **Network** > **Firewall**. The following page appears. The firewall is *enabled* by default.

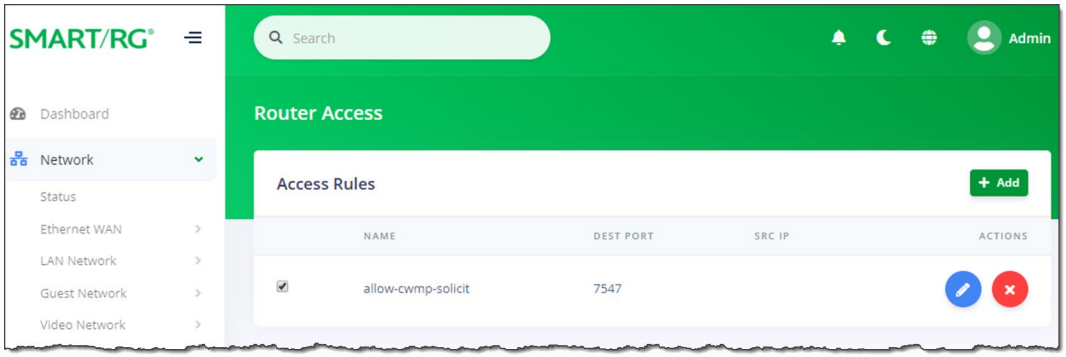


2. To *disable* the firewall, click the **slide button** next to **Enabled**.
3. To prevent malicious users from discovering information about your network and its devices and service, click the **slide button** next to **Stealth mode**.
4. The Conntrack Helper feature is *enabled* by default. To *prevent* these modules from assisting the firewall in tracking the various protocols used to establish traffic flow. click the **slide button**.
5. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

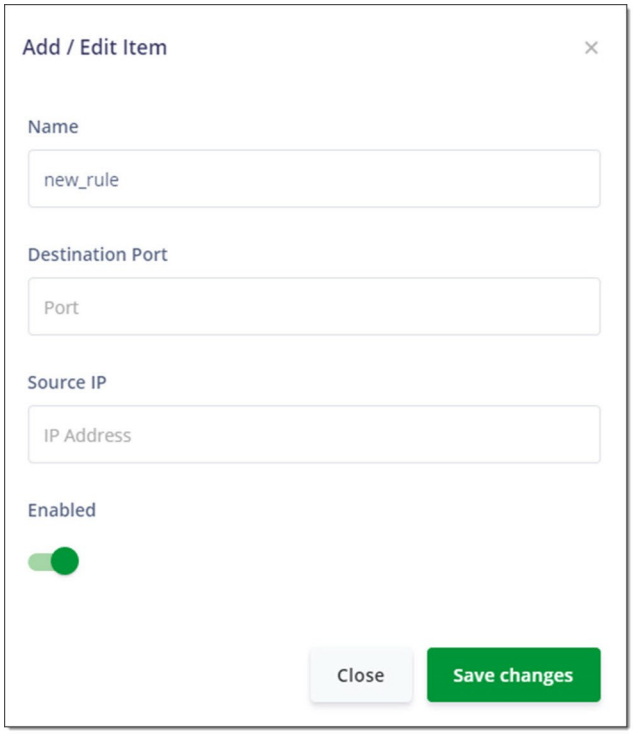
Router Access

On this page, you can configure a destination port and source IP address for router access.

1. In the left menu, click **Network** > **Firewall** > **Router Access**. The following page appears.



2. To add a mapping, click the **Add** button at the right side of the page. The **Add / Edit Item** dialog box appears.



3. Fill in the fields using the information provided in the table below. All fields are optional.
4. Click **Save changes**. The dialog box closes and the new mapping appears in the **Router Access** list.

5. To edit a mapping:
   a. Click the **Edit** icon ( ) next to the line item to be changed. The **Add / Edit Item** dialog box appears.
   b. Modify the fields as needed.
   c. Click **Save changes**. The updated values appear on the page.
6. To *disable* a mapping, clear the checkbox in the far left column for the mapping you wish to suspend. The mapping definition remains on the page but is not active.
7. To *remove* a mapping, click the **Delete** icon ( ) at the end of the row to be deleted. The mapping definition is removed.
8. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

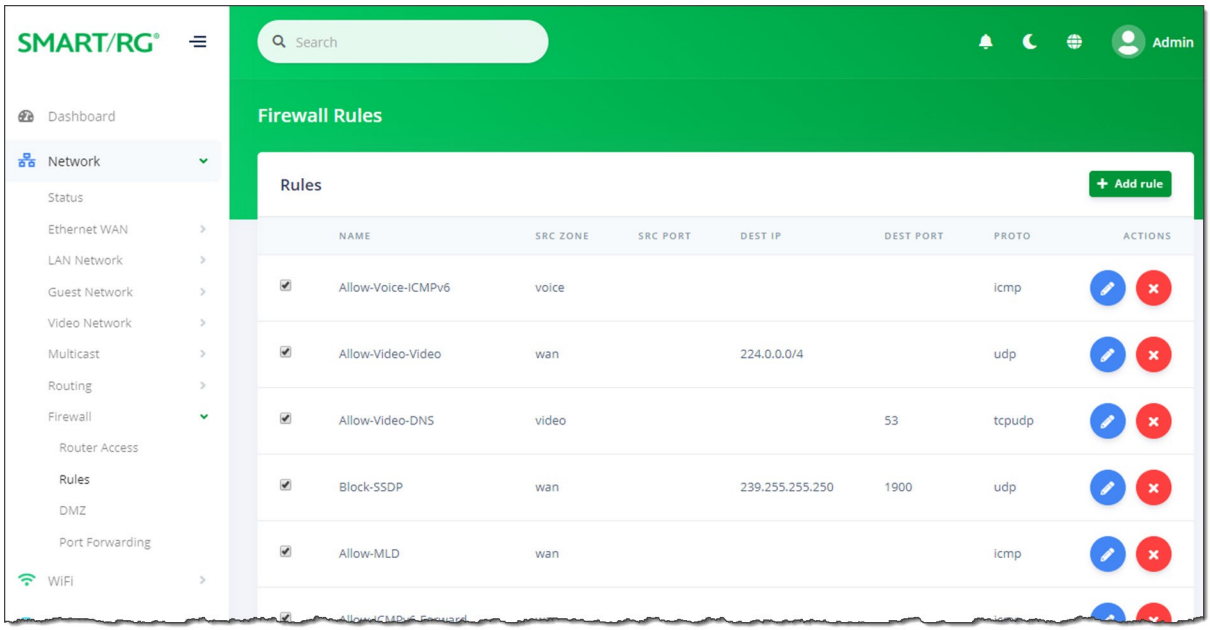
The fields on this page are explained in the following table.

Field Name	Description
Name	Enter a descriptive name for this rule. No spaces are allowed.
Destination Port	Enter the destination port for this rule.
Source IP	Enter the IP address for the source device (such as 192.168.1.44).
Enabled	New rules are *enabled* by default. To *disable* this rule but save the settings, click the **slide button**.

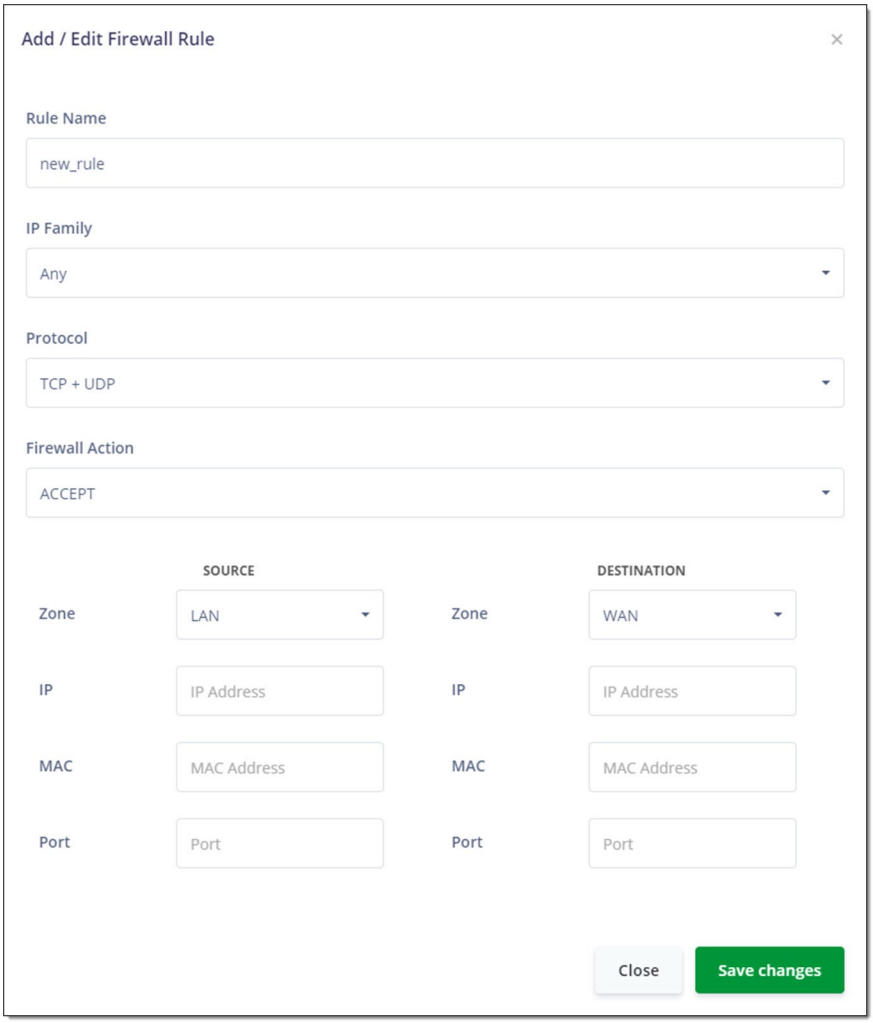
Rules

On this page, you can define firewall rules to filter traffic.

1. In the left menu, click **Network** > **Firewall** > **Rules**. The following page appears.



2. To create a new rule:
    a. Click the **Add rule** button to the right of the **Rules** section heading. The **Add / Edit Firewall Rule** dialog box appears.



    b. In the **Rule Name** field, enter a descriptive name for the rule.
    c. Fill in the other fields using the information in the table below.
    d. Click **Save changes**.
3. To edit a mapping:
    a. Click the **Edit** icon ( ) next to the entry you want to change. The **Add / Edit Item** dialog box appears.
    b. Modify the fields as needed.
    c. Click **Save changes**. The updated values appear on the page.
4. To *remove* a rule, click the **Delete** icon ( ) next to the entry you want to delete. The rule is removed.
5. To *disable* a rule, clear the checkbox in the far left column. The rule remains on the page but is not active.

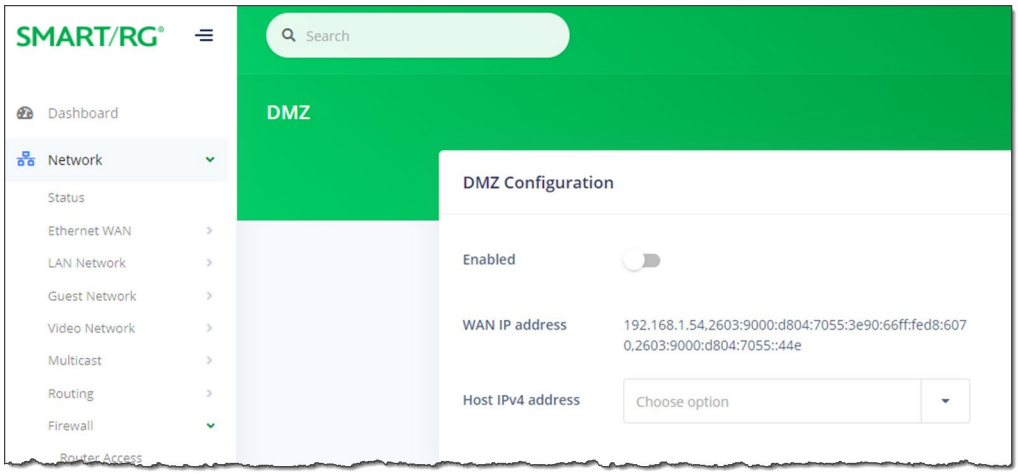
6. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Field Name	Description
IP Family	Select the address family. Options are **Any**, **IPv4**, and **IPv6**.
Protocol	Select the protocol for this rule. Options are **UDP**, **TCP**, **ICMP**, **TCP + UDP**, and **ESP**.
Firewall Action	Select the action to be performed when this rule is triggered. Options are **ACCEPT**, **REJECT**, **FORWARD**, and **DROP**. The default is **ACCEPT**.
SOURCE section	
Zone	Select the source zone. Options are **Unspecified**, **Any**, **GUEST**, **VIDEO**, **WAN**, **MGMT**, **LAN** and **VOICE**. The default is **LAN**.
IP	Enter the source IP address for this rule.
MAC	(*Optional*) To associate a source MAC address (such as 00236AA37CC3) with this rule, enter the MAC address for your gateway. If an IP address has been entered, the related MAC address appears in this field. To change the source MAC address, enter a new address.
Port	(*Optional*) To associate a source port with this rule, click the checkbox next to the entry field and then enter the port number for the source address.
DESTINATION section	
Zone	Select the destination zone. Options are **Unspecified**, **Any**, **GUEST**, **VIDEO**, **WAN, MGMT**, **LAN**, and **VOICE**. The default is **WAN**.
IP	Enter the destination IP address for this rule.
MAC	*Optional*) To associate a source MAC address (such as 00236AA37CC3) with this rule, enter the MAC address for your gateway. If an IP address has been entered, the related MAC address appears in this field. To change the source MAC address, enter a new address.
Port	(*Optional*) To associate a destination port with this rule, enter the port number for the destination address.

DMZ

On this page, you can configure DMZ settings for your gateway. For security reasons, it is recommended that you create a static IP address for the host server that you enter on this page.

1. In the left menu, click **Network** > **Firewall** > **DMZ**. The following page appears. The WAN IP Address is read-only.



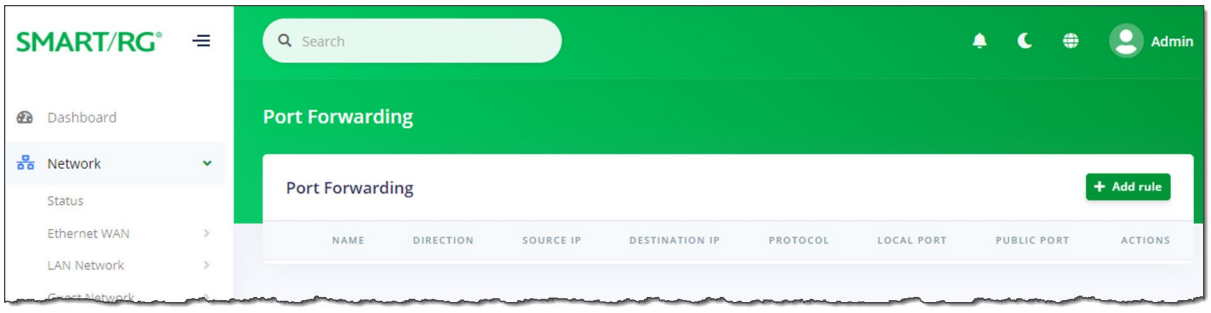
2. To *enable* this feature, click the **slide button** to the right of **Enabled**.
3. In the **Host IPv4 Address** field, select or enter the IP address for which unrestricted Internet access is to be allowed.

   Note: It is recommended to create a static DHCP association to this host address.
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

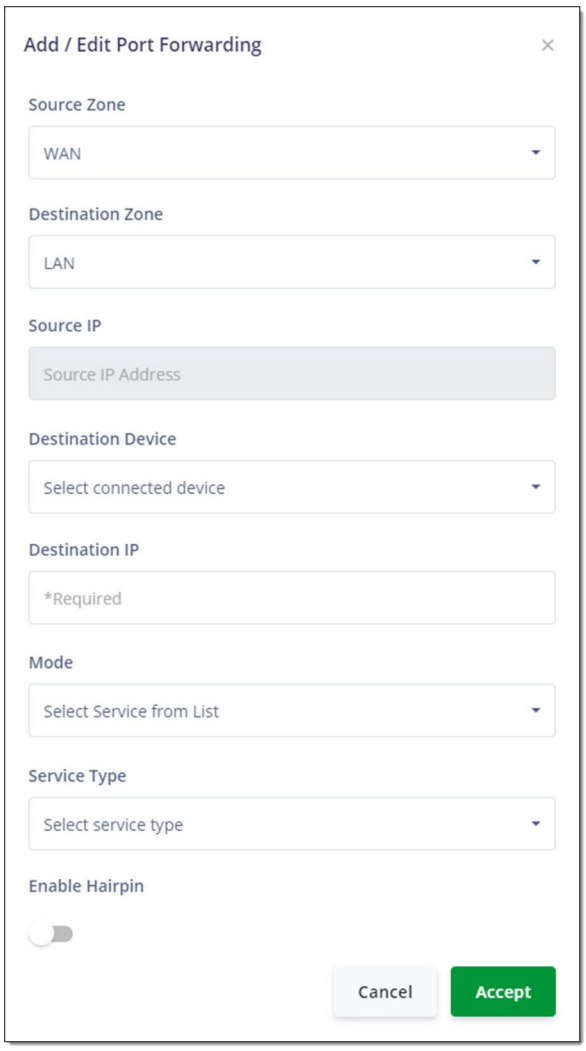
Port Forwarding

On this page, you can configure a local network device to have unrestricted access to the Internet. This is useful when local network devices cannot run an Internet application properly behind the firewall. This is also known as *exposed host* or *virtual server*.

1. In the left menu, click **Network** > **Firewall** > **Port Forwarding**. The following page appears.



2. To add a mapping, click the **Add Rule** button to the right of the **Port Forwarding** section heading. The **Add/Edit Port Forwarding** dialog box appears.



3. Fill in the fields using the information provided in the table below. All fields are optional.
4. Click **Accept**. The dialog box closes and the new mapping appears in the **Port Forwarding** list.

Field Name	Description
Source Zone	Select the source zone from the drop-down list of zones defined on this network. Options are **GUEST**, **VIDEO**, **WAN**, **MGMT**, **LAN** and **VOICE**. The default is **WAN**.
Destination Zone	Select the destination zone from the drop-down list of zones. Options are **GUEST**, **VIDEO**, **WAN**, **MGMT**, **LAN** and **VOICE**. The default is **LAN**.
Source IP	Enter the IP address for the source device (such as 192.168.1.44).
Destination Device	Select a connected device from the devices available in the selected zone.
Destination IP	This field is populated when a destination device is selected. To change this address, type a different address in the field.

Field Name	Description
Mode	Select whether to use the settings defined for a service or to define the port settings manually. Options are **Select Service From List** and **Configure Manually**. The default is **Select Service From List**.
Fields defined for using a service	
Service Type	Select the type of service. The **Service** field appears. Options are **Server**, **Consoles**, **Remote Access**, **VPN**, **Messaging Telephone**, and **Audio and Video**.
Service	Select the service for the service type selected. The options vary by the type of service.
Fields defined for configuring the rule manually	
Public port/ Public port range	(*Appears when **Configure Manually** is selected in the **Mode** field*) Enter the applicable port number or range of numbers. Options are **1** - **65535**.
Protocol	(*Appears when **Configure Manually** is selected in the **Mode** field*) Select the correct protocol. Options are **UDP**, **TCP**, and **TCP + UDP**.
Local port/ Local port range	(*Appears when **Configure Manually** is selected in the **Mode** field*) Enter the local port number or range of numbers. Options are **1** - **65535**.
Port Type	(*Appears when **Configure Manually** is selected in the **Mode** field*) Select whether to enter a single port or a range of ports. If **Port range** is clicked, the **Public port** field changes to the **Public port range** fields and the **Local port** field changes to the **Local port range** fields.
Enable Hairpin	To *enable* hairpin protocol, click the **slide button**.

1. To edit a mapping:
   a. Click the icon to the right of the mapping entry. The **Add/Edit Port Forwarding** dialog box appears.
   b. Modify the fields as needed, and then click **Save**. The updated values appear on the page.
2. To *disable* a mapping, clear the checkbox that appears before the **Name** column. The mapping definition remains on the page but is not active.
3. To *remove* a mapping, click the **Delete** icon ( ) at the end of the row to be deleted. The rule is removed.
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

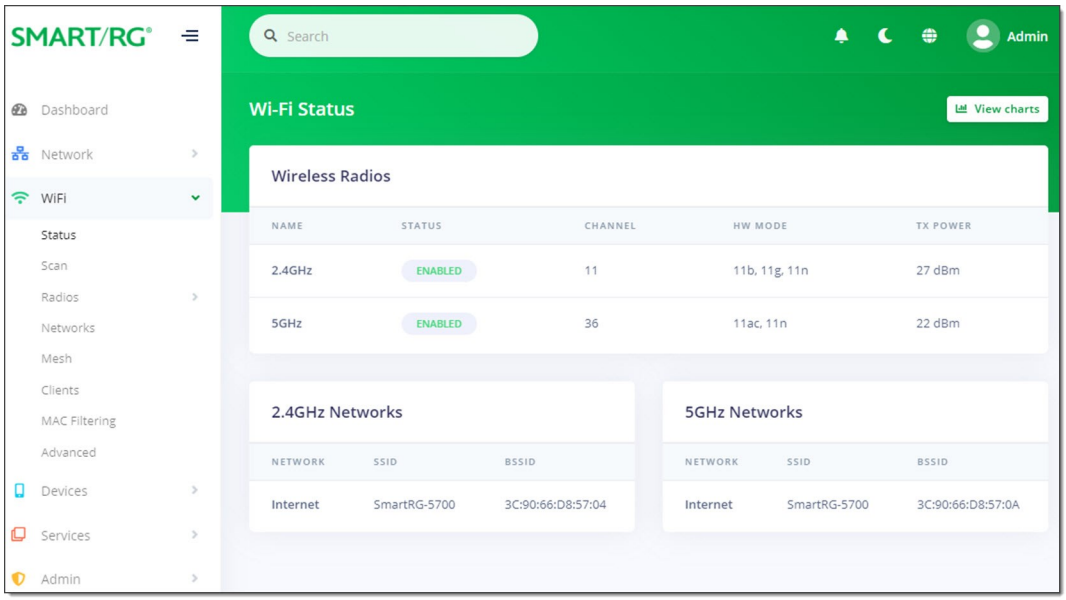
WiFi

In this section, you can adjust settings and view performance associated with the WiFi network(s) configured on this gateway.

Status

On this page, you can view status information about the wireless networks connected to your system.

In the left menu, click **WiFi** > **Status**. The following page appears, showing the information for the 2.4 GHz and 5 GHz wireless networks.

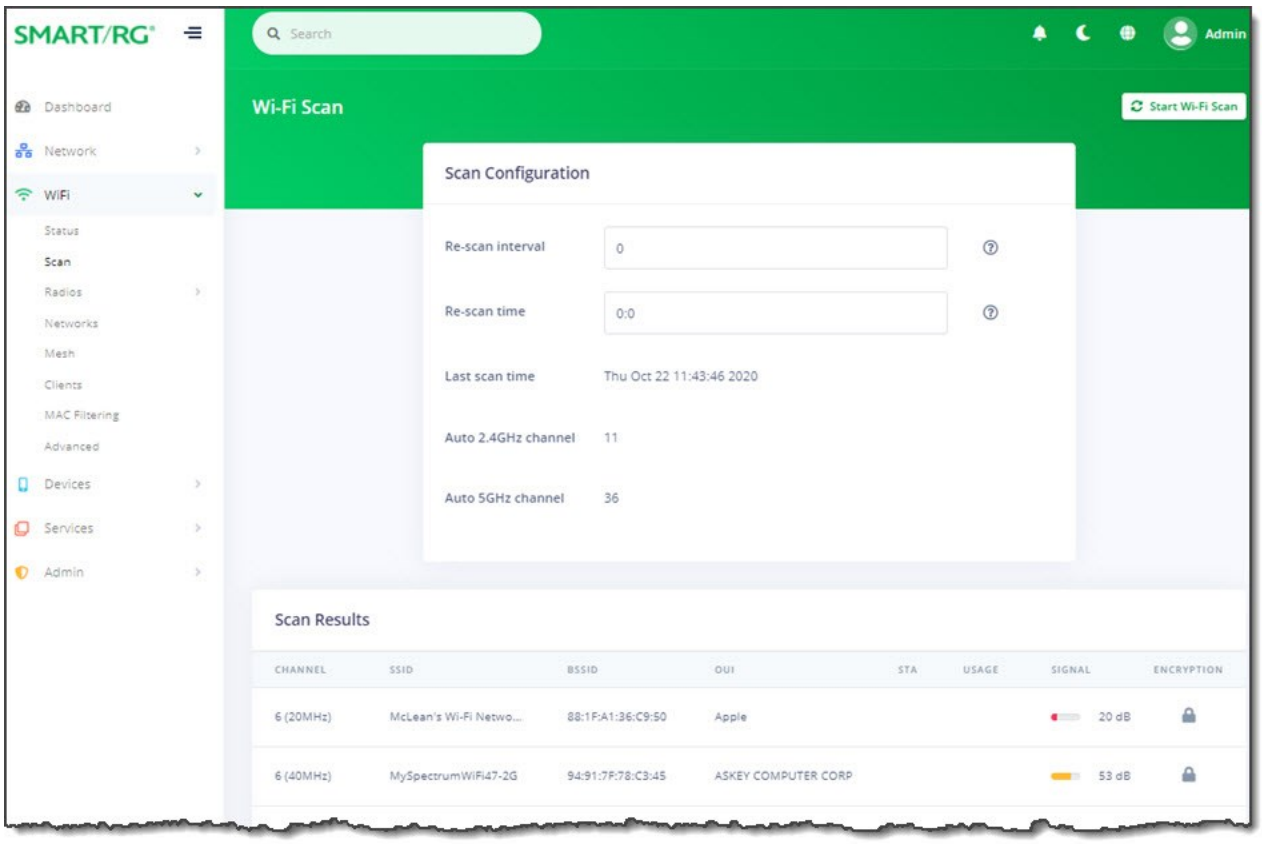


To view detailed transmission data for the individual interfaces, click the **View charts** button (View Charts) at the top right. The netdata window opens in a new tab, showing information about the overall SR905acv system, memory, CPUs, firewall, IPv4 networking, etc. Use the navigation menu at right to select the desired statistics to be displayed.

Scan

On this page, you can scan for nearby wireless access points. The available data includes the channel number, SSID, BSSID, OUI, STA, usage, signal, and encryption.

1. In the left menu, click **WiFi** > **Scan**. The following page appears, showing the wireless access points found during the most recent scan. You can find the latest scan date and time in the top section next to **Last scan time**. The channels currently in use are displayed below that field.



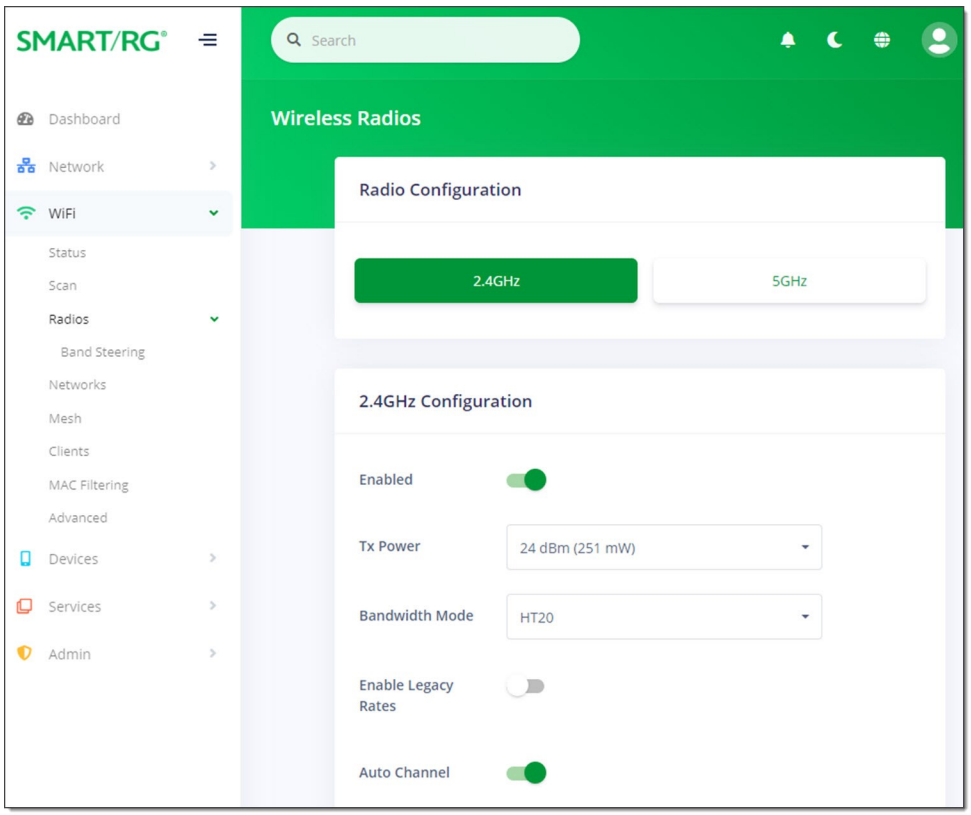
2. Do any of the following:
   - To re-scan for wireless access points near your location, click the **Start Wi-Fi Scan** button at the top right. The list refreshes in a few moments.
   - To define how often the scan should occur, in the **Re-scan interval** field, enter the number of hours between scans. To disable scanning, enter **zero** (**0**) in this field. This is the default.
   - To define the time of day when the scan should occur, in the **Re-scan time** field, enter the time in hh:mm format. Options are **00:01** - **23:59**. The default is **0:0** (disabled).
3. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Radios

On this page, you can configure 2.4 or 5 GHz wireless networks for the primary SSID.

Note: The maximum number of connected devices for each network is *28*. To connect more than 28 devices, create an additional access point.

1. In the left menu, click **WiFi** > **Radios**. The following page appears, showing the fields for the 2.4 GHz radio. To view and adjust 5 GHz settings, click the **5GHz** button.



2. Fill in the fields, using the information in the following table. The same fields are used for both 2.4 GHz and 5 GHz configurations.
3. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

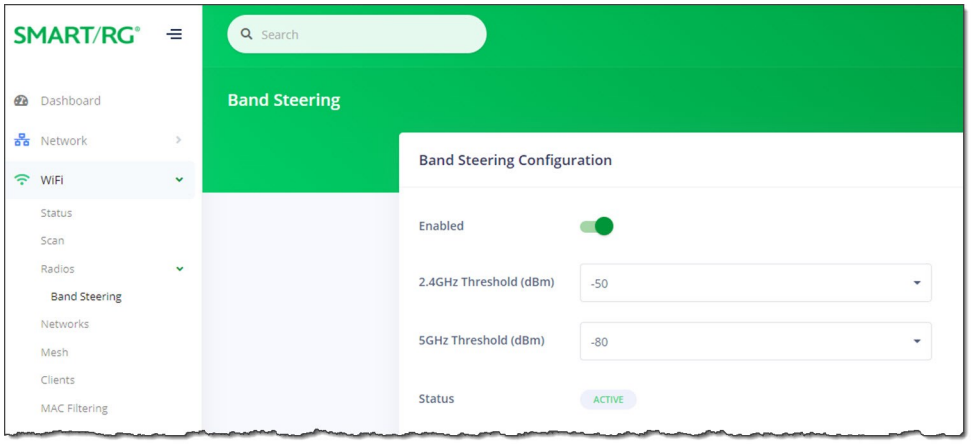
Field Name	Description
Enabled	Each radio is *enabled* by default. To *disable* a radio, click the **slide button**.
TX Power	Select the maximum rate at which transmission is allowed. Options range from **15 dBm (31 mw)** to **30 dBm (1000 mw)**. The default is **24 dBm (251 mW)** for the 2.4GHz radio and **22 dBm (158 mW)** for the 5 GHz radio.
Bandwidth Mode	**2.4 GHz radio:** Select the "high throughput" (HT) bandwidth mode for this device. Options are **HT20** and **HT40** (MHz). The default is **HT20**. **5 GHz radio:** Select the "very high throughput" (VHT) bandwidth mode for this device. Options are **VHT20**, **VHT40**, and **VHT80**. The default is **VHT80**.
Enable Legacy Rates	This feature is *disabled* by default. To set the gateway to cut transmission briefly when changing channels, click the **slide button**. This is useful for legacy WiFi clients, enabling them to connect more effectively to a new channel.

Field Name	Description
Auto Channel	This feature is *enabled* by default. To *disable* automatic channel selection , click the **slide button**. The **Channel** field appears.
Channel	(*Available only when **Auto Channel** is disabled*) Select the channel for this device. **2.4 GHz radio:** Options include **Channel 1 (2.412 GHz)** - **Channel 11 (2.462 GHz)**. **5 GHz radio:** Options include **Channel 36 (5.18 GHz)** - **Channel 48 (5.24 GHz)** and **Channel 149 (5.745 GHz)** - **Channel 165 (5.825 GHz)**.

Band Steering

On this page, you can configure the band steering settings for your wireless radios.

1. In the left menu, click **WiFi > Radios** > **Band Steering**. The following page appears. The status of this feature is shown in the **Status** field at the bottom of the page.

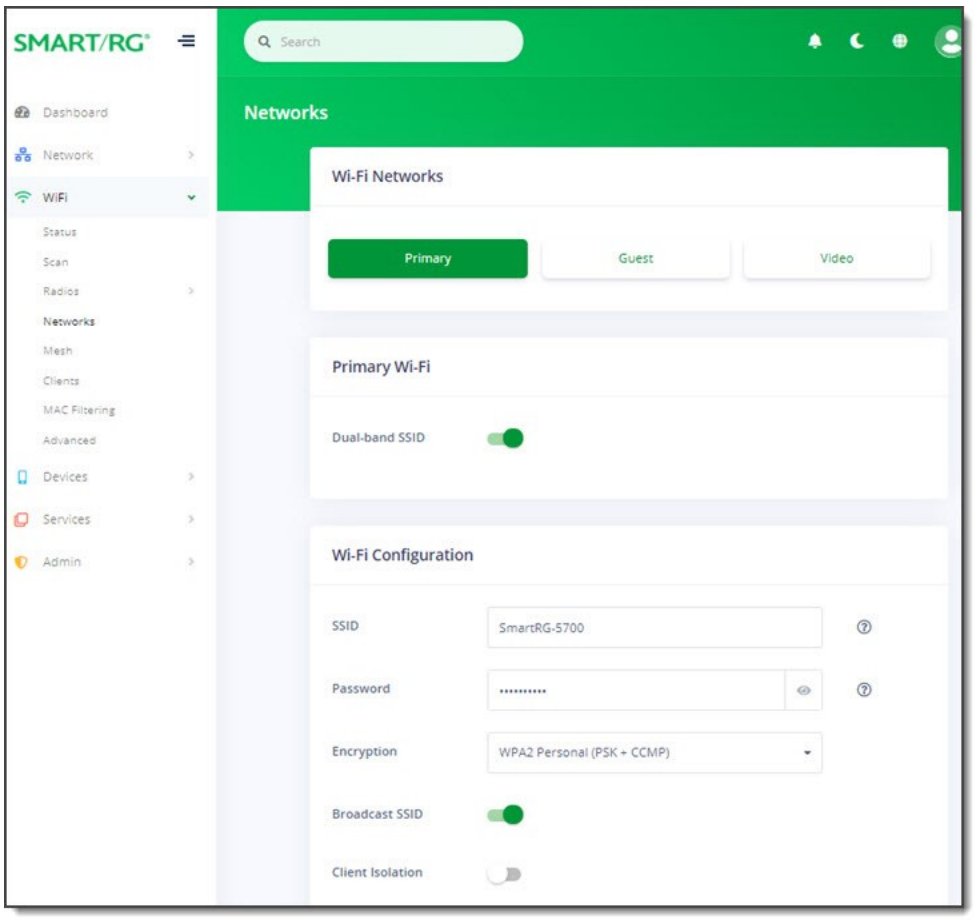


2. To *disable* band steering, click the **slide button** to the right of **Enabled**.
3. In the **2.4GHz** and **5GHZ Threshold (dBm)** fields, select the dBm value.
   - For the **2.4GHz Threshold** field, options are **-55** to **-40**. The default is **-50**.
   - For the **5GHz Threshold** field, options are **-85** to **-70**. The default is **-80**.
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Networks

On this page, you can configure the Primary, Guest and Video wireless networks.

1. In the left menu, click **WiFi** > **Networks**. The following page appears, showing the information for the primary wireless network.



2. Fill in the fields for the primary network, using the information provided in the table below. The same fields are provided for 2 GHZ and 5 GHz radios.
3. To configure the guest network, click the **Guest** button and modify the fields as needed, using the information provided in the table below.
4. To configure the video network, click the **Video** button and modify the fields as needed, using the information provided in the table below.
5. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

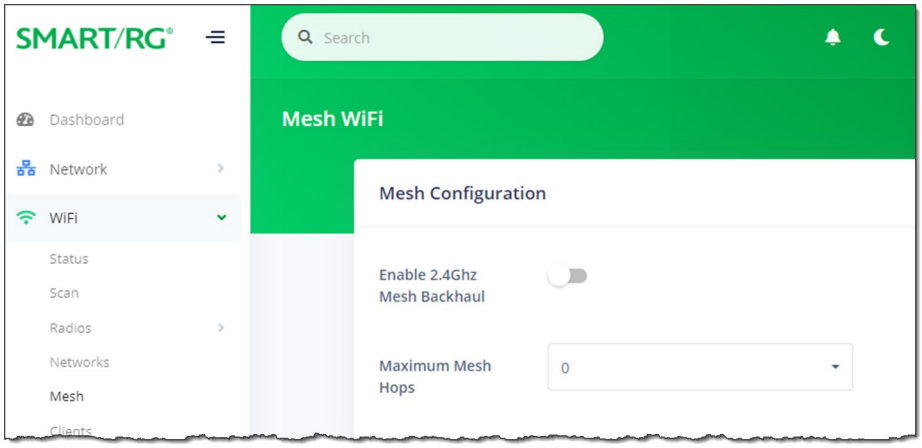
Field Name	Description
Dual-band SSID	This feature is *enabled* by default. To *disable* the dual-band feature for these networks, click the **slide button**.
Enabled	(*Appears on the **Guest** and **Video** pages only*) To enable the Wi-Fi configuration, click the **slide button**.
Wi-Fi Configuration section	
SSID	(*Optional*) Customize the wireless network ID. This field cannot contain quotes (") or back slashes (\) but can contain most other special characters. It is recommended that this ID be no more than 32 characters.

Field Name	Description
Password	Enter the passphrase for this connection. To show the key characters, click the **Show/Hide** icon ( ). This field cannot contain the following characters: " \ ( ) ; & | < > but spaces are allowed.
Encryption	Select the encryption protocol (mode and cypher) for this connection. Options are **None** and **WPA2 Personal (PSK + CCMP)**. The default is **WPA2 Personal (PSK + CCMP)**.
Broadcast SSID	This option is *enabled* by default. To *hide* the SSID from end users, click the **slide button**.
Client Isolation	This option is *disabled* by default for the **Primary** and **Video** networks and *enabled* for the **Guest** network. To change this setting, click the **slide button**.

Mesh

On this page, you can configure WiFi options for your mesh network.

1. In the left menu, click **WiFi** > **Mesh**. The following page appears.



2. To *enable* the 2.4 GHz mesh backhaul feature, click the **slide button** next to **Enable 2.4Ghz Mesh Backhaul**.
3. (Optional) In the **Maximum Mesh Hops** field, select the maximum number of hops allowed for the mesh network. Options are **1** - **3** and **Unlimited**. The default is **Unlimited**.
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Clients

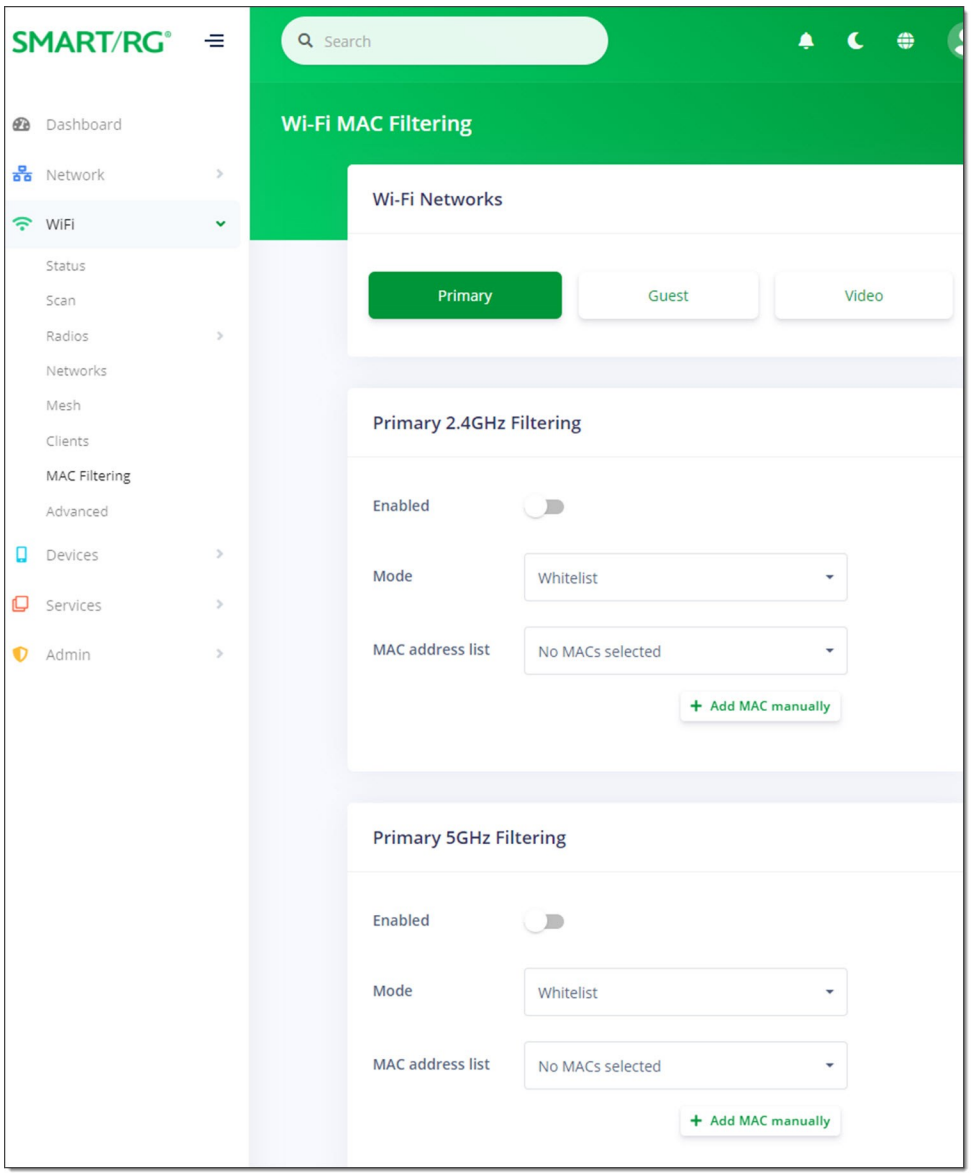
On this page, you can view information about the clients connected to the network via wireless interfaces.

In the left menu, click **WiFi > Clients**. The following page appears, listing the clients currently connected to your network.

MAC Filtering

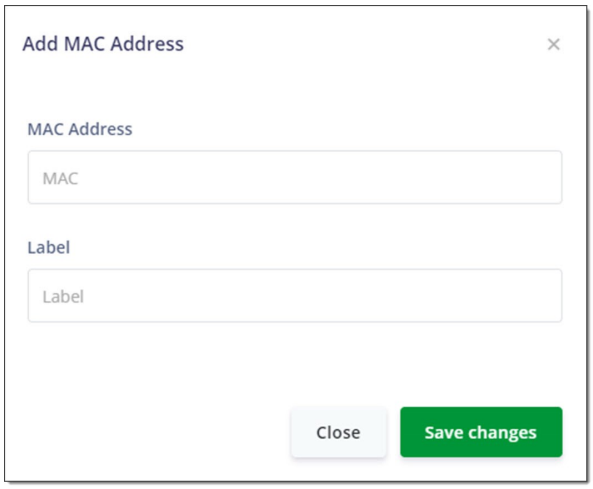
On this page, you can configure whether wireless clients are allowed to access the wireless networks of the gateway.

1. In the left navigation bar, click **WiFi** > **MAC Filtering**. The following page appears, showing the **Primary** tab.

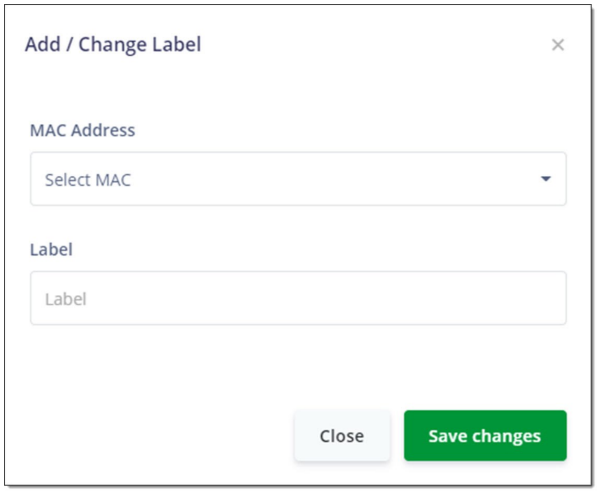


2. Click the button for the network for which you want to configure whitelist and blacklist addresses.
3. To enable filtering, click the **slide button** next to **Enabled**.

4. Select the **Mode**. Options are:
   - **Blacklist**: Disable wireless MAC address filtering.
   - **Whitelist**: Allow the wireless clients in the **MAC Address** list to access the wireless network. This is the default.
     Note: For this option to work, you must add at least one MAC address to this page.
5. To add a **MAC Address** to the filter list:
   a. In the **filtering** section for the band you want to configure, click the **Add MAC manually** button below the **MAC address list** field. The Add MAC Address dialog box appears.



   b. Enter the **MAC Address** of the wireless client.
   c. (*Optional*) In the **Label** field, enter the name that you want displayed to your users.
   d. Click **Save changes** to save the address to the list. You are returned to the Wireless MAC Filtering page.
6. To change the label of a MAC address:
   a. Below the **MAC address list** field, click **Add/change MAC label**. The Add/Change Label dialog box appears.



   b. In the **MAC Address** field, select the MAC address that you want to change.

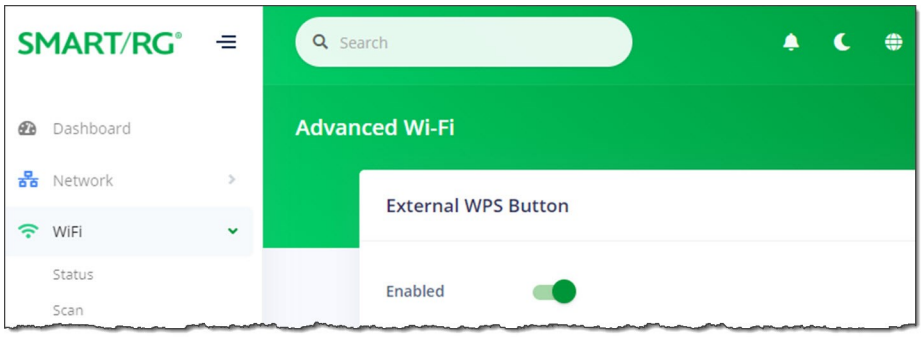
c. In the **Label** field, enter the new label.
d. Click **Save changes**. You are returned to the Wi-Fi MAC Filtering page.

7. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Advanced

On this page, you can configure advanced WiFi options for the gateway.

1. In the left menu, click **WiFi** > **Advanced**. The following page appears.



2. To *disable* the physical WPS button on the outside of the gateway, click the **slide button** next to **Enabled**.
3. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Devices

In this section, you can configure and manage the devices connected to your gateway. You can group and manage LAN devices as well as Intellifi mesh network devices.

Intellifi Devices

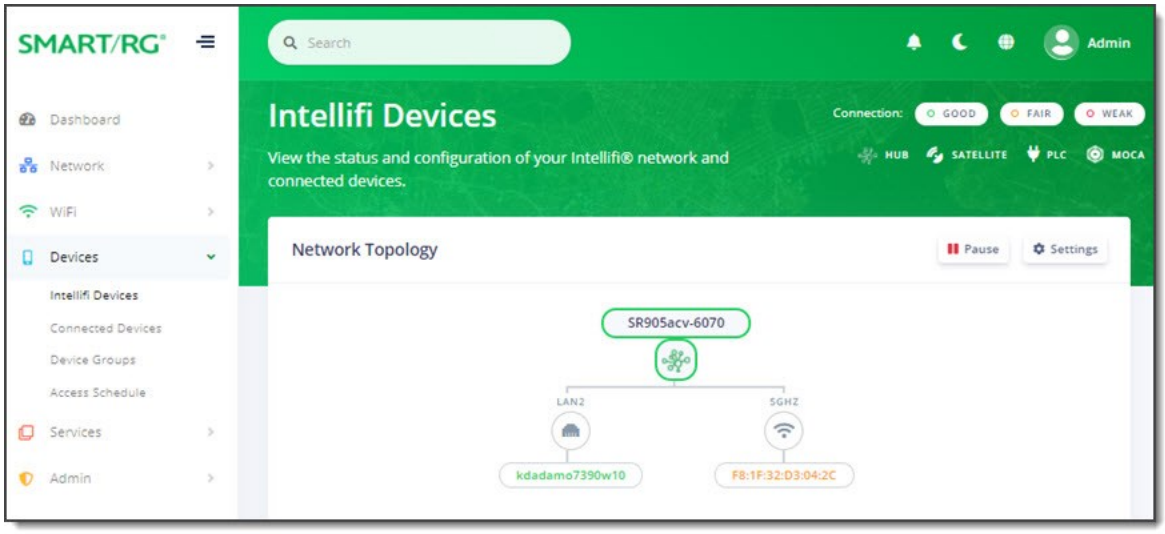
On this page, you can view the Intellifi mesh devices connected to the network.

Note: To extend the network, you can connect a satellite to a satellite.

1. In the left menu, click **Devices** > **Intellifi Devices**. The following page appears showing a diagram of the connected devices.

   If a device is connected via wireless, the WiFi band appears as the name instead of LAN or WAN. The device colors identify the connection status. The **Connection Status** legend at the top right of the page explains the colors. Below that legend is the **device identifier** legend, showing symbols for HUB, SATELLITE, PLC, and MOCA devices.

   There are two views: the simple view (the default) and the detailed view. (The detailed view shows the IP addresses for each device.) This map refreshes every 10 seconds.



2. To switch between the simple view and the detailed view:
   a. Click the **Settings** button at the top right of the **Network Topology** section. The Topology Settings diagram box appears.
   b. Click the **slide button** below **Show Detailed View**.
   c. Click **Save Changes**.
3. To change the refresh interval:
   a. Click the **Settings** button at the top right of the **Network Topology** section. The Topology Settings diagram box appears.

b. In the **Refresh Interval** field, select the new interval. Options are **10 seconds** to **1 minute**. The default is **10 seconds**.
c. Click **Save Changes**.

4. To pause the traffic with the Intellifi network, click **Pause** to the right of the **Network Topology** heading. The **Pause** button changes to a **Play** button. Click the **Play** button to restart traffic.
5. To view details of a device, click the device label. The **DEVICE DETAILS** pane appears.

   You can edit the host name, click the IP address to log into the device, or click **Internet Access** to pause access to this device.
6. When finished, close the pane.

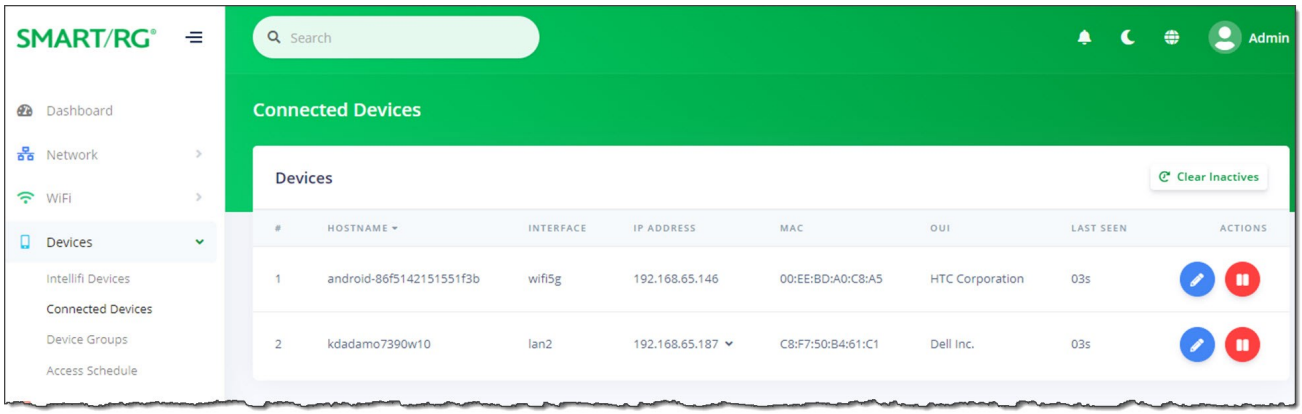
Connected Devices

This page displays a list of devices connected to the LAN.

Note: Before you can assign a device to a group, you must configure an access schedule, then configure a device group, and finally assign the schedule to the group.

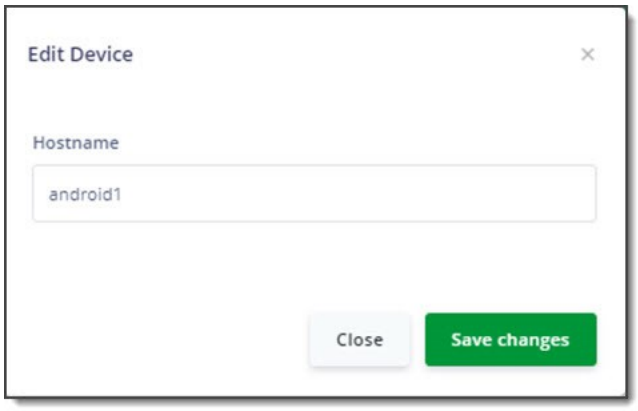
Warning: Pausing access for LAN devices not only restricts access to the Internet but LAN access as well. This in turn prevents you from logging in to the SmartRG gateway to make changes from any LAN clients included in the pause. With this in mind, users are strongly advised against pausing all LAN devices at the same time. Instead, exclude at least one browser-equipped LAN device from the Device Group to ensure that a means to modify access schedules, device groups and timeout periods is preserved.

1. In the left menu, click **Devices** > **Connected Devices**. The following page appears.

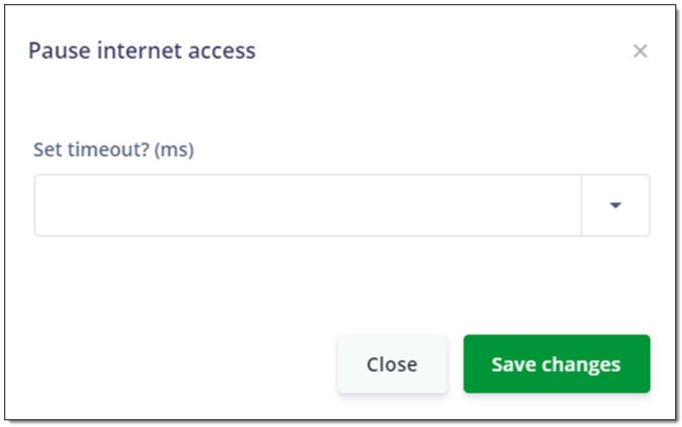


2. To refresh the list to show only active devices, click the **Clear Inactives** button (Clear Inactives) to the right of the table title.

3. To edit a device host name:
   a. Click the **Edit** icon ( ) to the right of the entry that you want to edit. The **Edit device** dialog box appears.



   b. In the **Hostname** field, enter a descriptive name for the device.
   c. Click **Save changes**.
4. To pause access for a device temporarily:
   a. Click the **Pause** icon ( ) to the right of the device for which you want to halt access. The Pause internet access dialog box appears.



   b. In the **Set timeout** field, select how long you want access paused. Options are **None**, **15 - 60 minutes**, **2-8 hours**, and **1 day**.
   c. Click **Save changes**.
5. To restart access, click the **Play** icon ( ) to the right of the line item for which you wish to resume Internet access. The **Pause** icon ( ) re-appears.

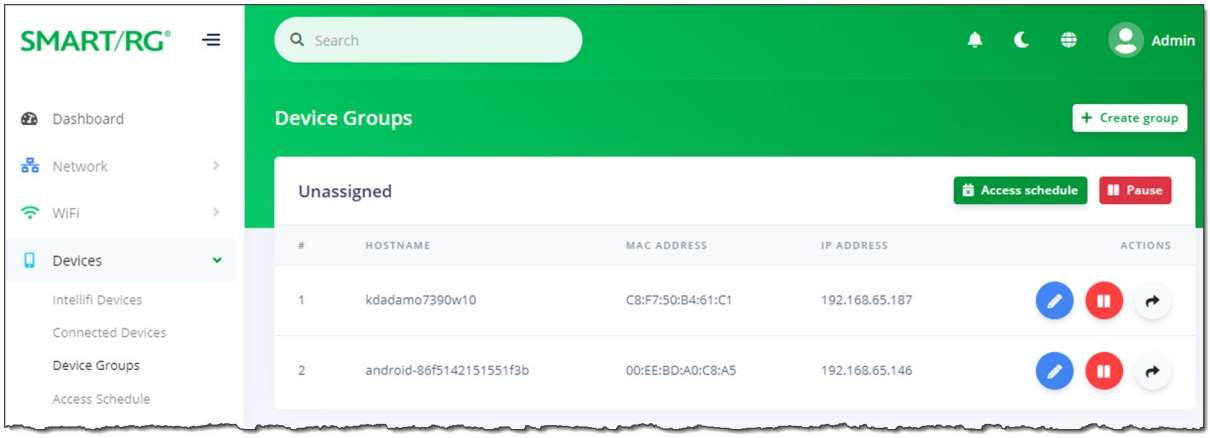
Device Groups

On this page, you can create device groups, assign devices to groups, pause access for devices, delete groups

Note: Before it is possible to assign a device to a group, configuring an access schedule is required first, then configure a device group, and finally assign the schedule to the group.

Warning: Pausing access for LAN devices not only restricts access to the Internet but LAN access as well. This in turn prevents you from logging in to the SmartRG gateway to make changes from any LAN clients included in the pause. With this in mind, users are strongly advised against pausing all LAN devices at the same time. Instead, exclude at least one browser-equipped LAN device from the Device Group to ensure that a means to modify access schedules, device groups and timeout periods is preserved.

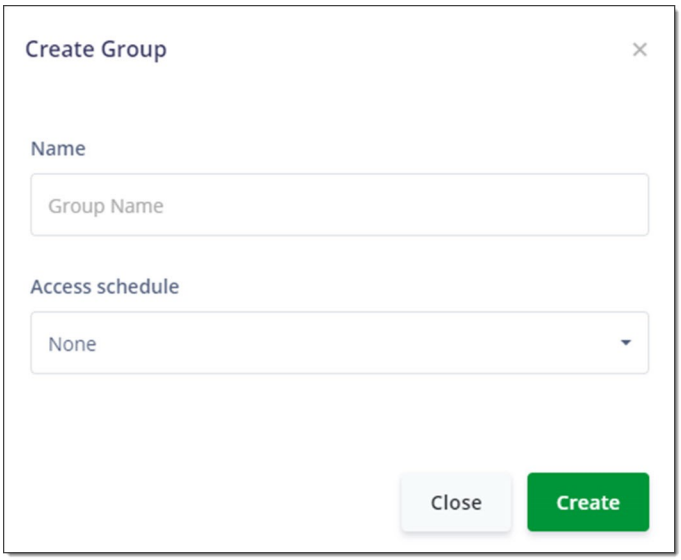
1. In the left menu, click **Devices** > **Device Groups**. The following page appears.



Note: You cannot delete or rename the unassigned (default) group but you can assign a schedule to it and pause/restart it.

2. To add a new device group:
    a. Click the **Create group** button (

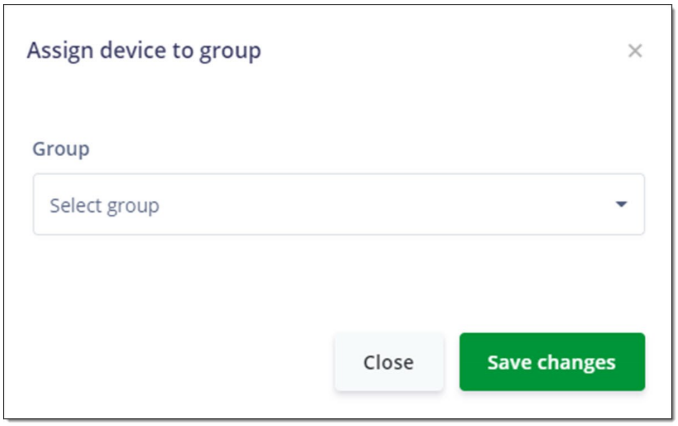
) to the right of the page title. The Create Group dialog box appears.



    b. In the **Name** field, enter a descriptive name for the device group.
    c. To assign a schedule to the device group, select the schedule in the **Access schedule** field.

    Note: If you do not see the schedule that you want, go to the Devices > Access Schedule page and create it. Then, return to this page.

    d. Click **Create**. The new group appears at the top of the list and a **Delete group** button (
) appears at the top right.
3. To add a device to a group:
    a. Click the **Assign** button (
) at the far right of the device that you want to add to a device group. The **Assign device to group** dialog box appears.



b. In the **Group** field. select a group.

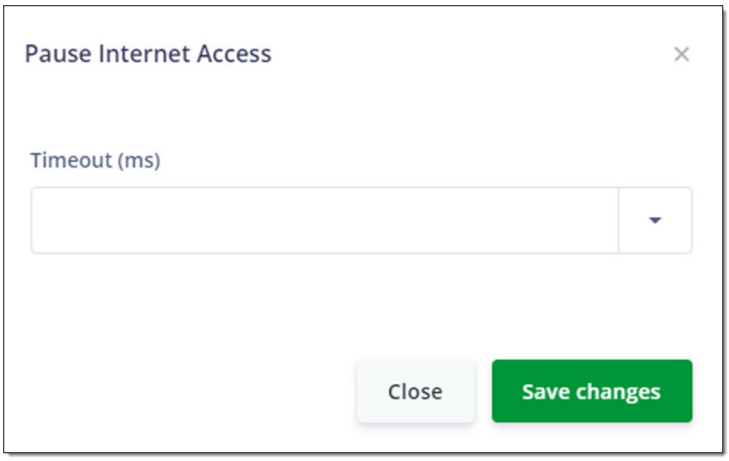
Note: If you do not see the group that you want, create it, following the steps provided above.

c. Click **Save changes**.

4. To define a timeout period for a *group*:

Before proceeding, read the **Warning** above.

a. Click the **Pause** button ( ) next to the section heading for which you want to withhold Internet access. The **Pause Internet Access** dialog box appears.



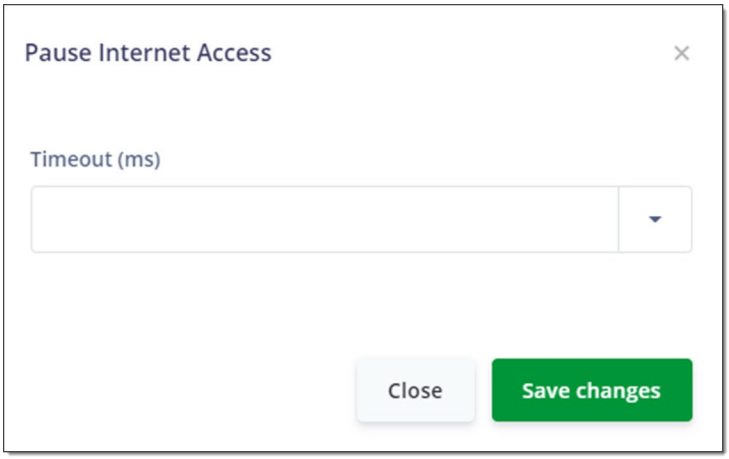
b. In the **Timeout** field, select the duration of the pause. Options are **None**, **15** - **60** minutes, **2 - 8 hours**, and **1 day**.

c. Click **Save changes**.

5. To define a timeout period for a *device*:

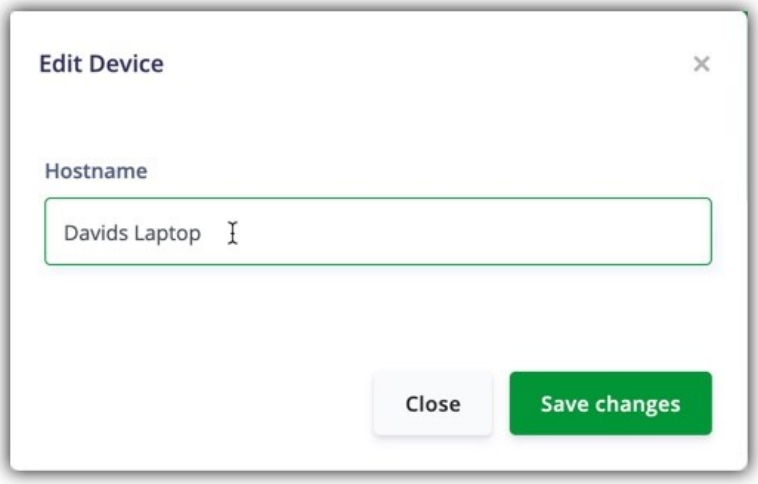
Before proceeding, read the **Warning** above.

a. Click the **Pause** button ( ) next to the device for which you want to withhold Internet access. The **Pause Internet Access** dialog box appears.



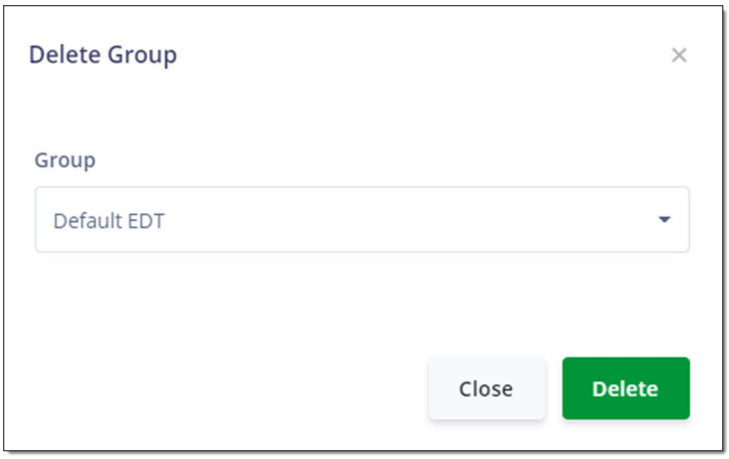
b. In the **Timeout** field, select the duration of the pause. Options are **None**, **15** - **60** minutes, **2 - 8 hours**, and **1 day**.
c. Click **Save changes**.

6. To customize the host name for a device:
   a. Click the icon next to the device you want to customize. The **Edit Device** dialog box appears.



   b. Enter the desired host name.
   c. Click **Save changes**.

7. To delete a device group:
    a. Click the **Delete group** button ( ) at the top of the device pane. The **Delete Group** dialog box appears.



    b. In the **Group** field, select the group to be deleted.
    c. Click **Delete**. The device list on the Device Group page refreshes.
8. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

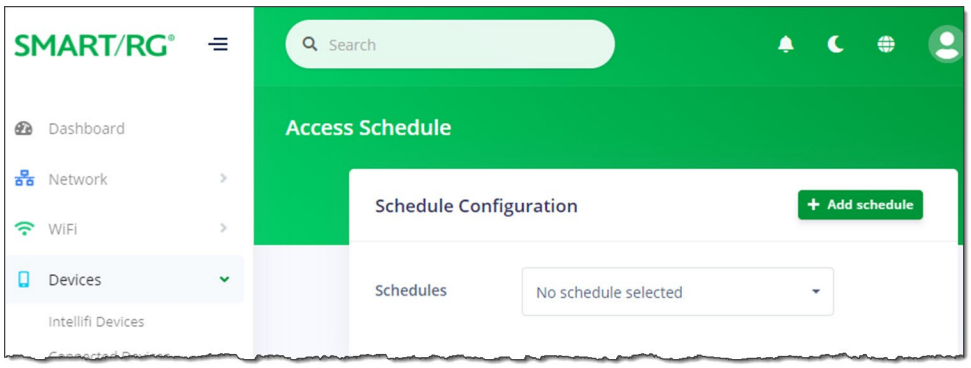
Access Schedule

On this page, you can configure the access schedules that are needed to control access for LAN device groups.

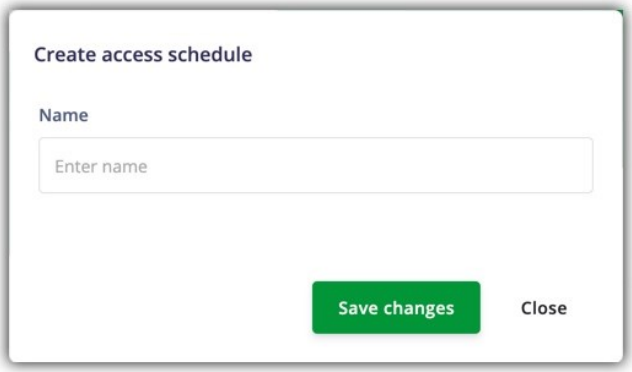
Make sure that the time zone is set correctly for this gateway before configuring an access schedule. You can access the Timezone setting on the **Admin** > **Time** page in the GUI. Instructions are provided in the Time topic.

Warning: Pausing access for LAN devices not only restricts access to the Internet but LAN access as well. This in turn prevents you from logging in to the SmartRG gateway to make changes from any LAN clients included in the pause. With this in mind, users are strongly advised against pausing all LAN devices at the same time. Instead, exclude at least one browser-equipped LAN device from the Device Group to ensure that a means to modify access schedules, device groups and timeout periods is preserved.

1. In the left menu, click **Devices** > **Access Schedule**. The following page appears.

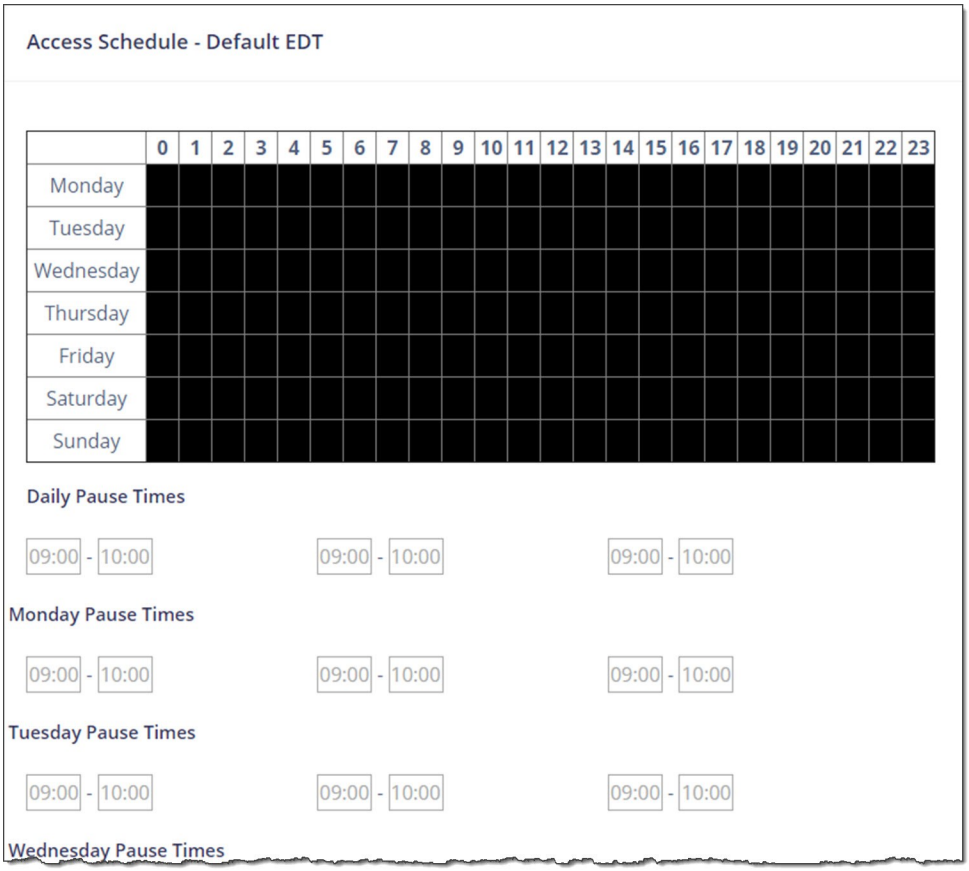


2. To create an access schedule:
   a. Click the **Add schedule** button at the top right. The Create access schedule dialog box appears.



   b. Enter a descriptive name for the new schedule and click **Save changes**. Additional fields appear on the Access Schedule page for configuring blocked access time for every day or for specific days. The **Delete schedule** button

appears at the top right of the pane.



3. Enter start and end times in the fields below the **Pause Times** labels. Use 24-hour format. The separating colon is added for you as you type the numbers.

   The entered time periods are shown in **red** on the grid in whole-hour blocks only. When times are entered in the **Daily Pause Times** fields, that period changes to **red** for *every* day.

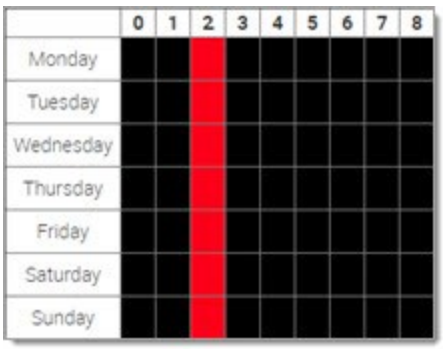
   For example, to prevent access between 2 am and 3 am, enter "0200" in the first (start) field and "0259" in the second (end) field for either every day (daily) or specific days. The grid refreshes to show that access is blocked for the 2:00 hour.

   If you enter "0300" in the second field, a 2-hour block is selected in the grid, from 2:00 - 4:00 am.

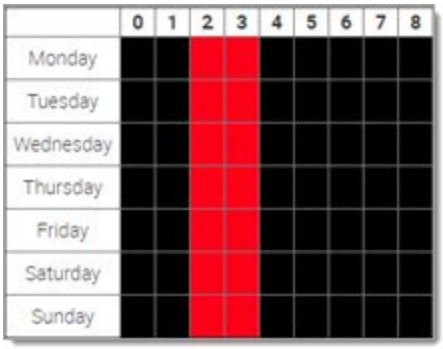
   The maximum number of blocked periods allowed per day is 3.

   To add another blocked period *for the same day*, enter values in the 2nd and 3rd time fields.

   Example of a 1-hour block (entered as 02:00 to 02:59)



Example of a 2-hour block (entered as 02:00 to 03:00)



4. To change a schedule, select it in the **Access Schedule** field and modify the fields.
5. To delete a schedule, select it in the **Access Schedule** field and click the **Delete schedule** button (Delete schedule) at the top right.
   Note: If you delete a schedule that is assigned to a device group, it is removed from the device group configuration.
6. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

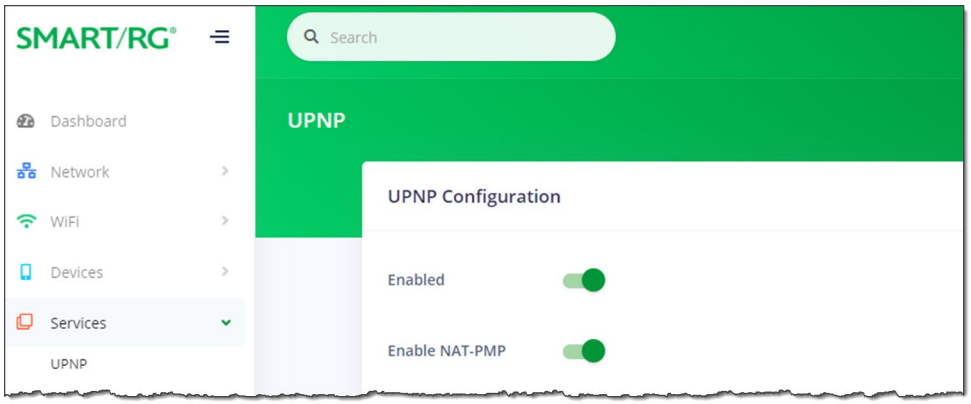
Services

In this section, you can configure the various services for the network including UPnP, TR-069, SNMP, hosts, DDNS, and others.

UPNP

On this page, you can manage the UPnP (Universal Plug and Play) service so that third-party devices on the LAN that support this standard can connect. Common devices include gaming consoles, IP cameras, printers, and so on.

1. In the left menu, click **Services** > **UPNP**. The following page appears.



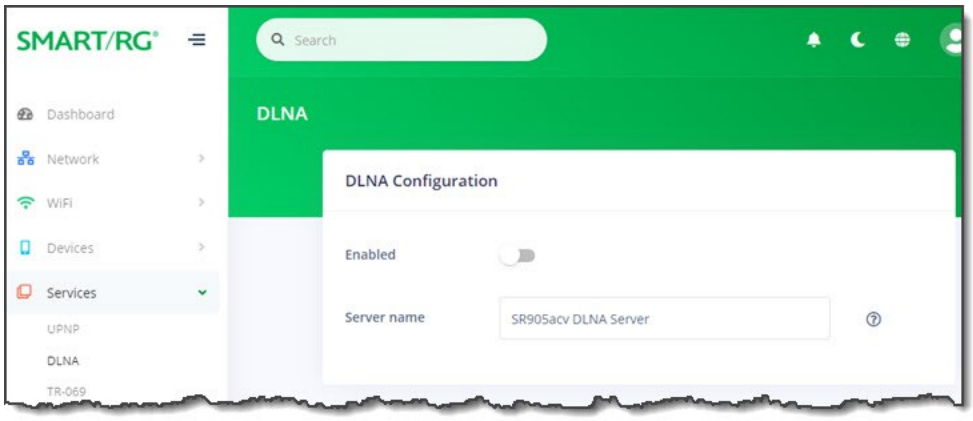
2. To *disable* UPnP, click the **slide button** to the right of **Enabled**.
3. To *disable* the automatic configuration of NAT settings, click the **slide button** to the right of **Enable NAT-PMP**.
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

DLNA

On this page, you can configure the DLNA (Digital Living Network Alliance) server software.

Note: You must reboot the gateway to implement any changes made on this page.

1. In the left menu, click **Services** > **DLNA**. The following page appears.



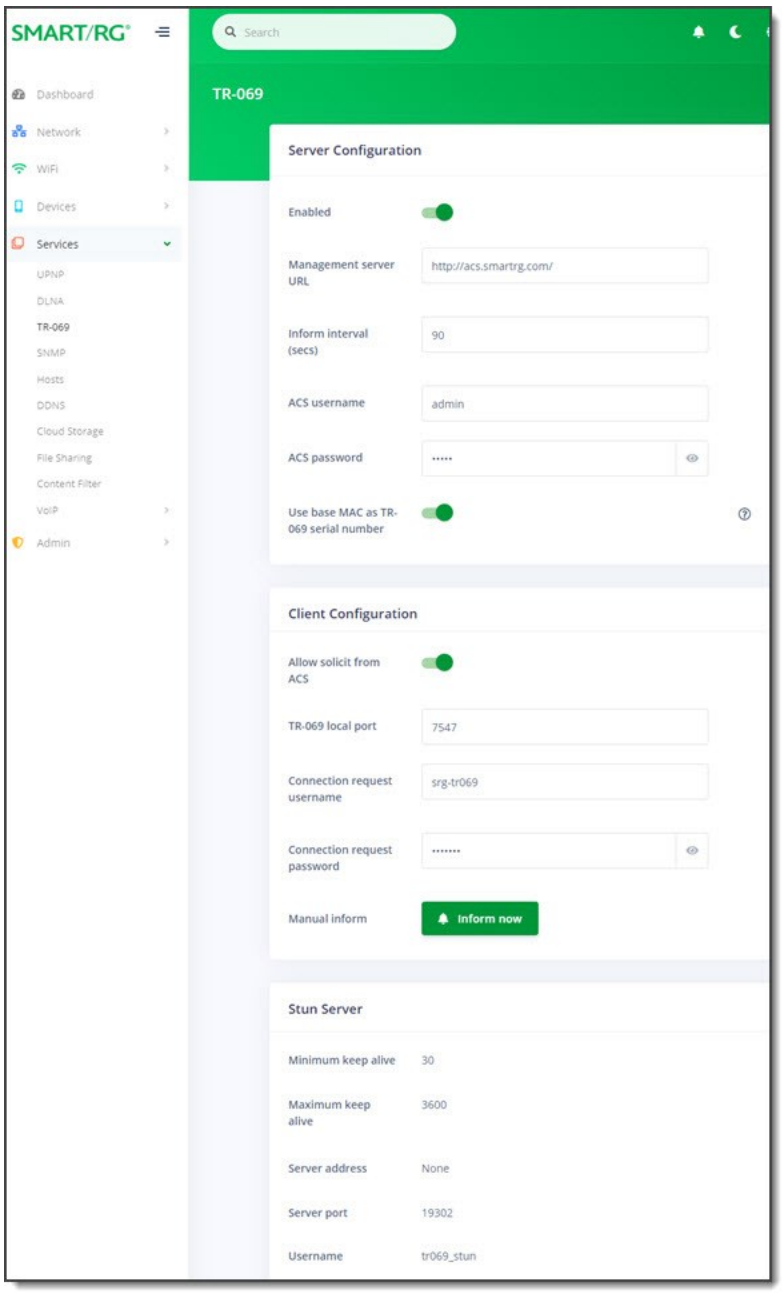
2. To *enable* this option, click the **slide button** to the right of **Enabled**.
3. (*Optional*) In the **Server name** field, enter a descriptive name for this network that end users will see.
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

TR-069 Configuration

On this page, you can configure the gateway with details about the management server to which this gateway will be linked.

Note: You must reboot the gateway to implement any changes made on this page.

1. In the left menu, click **Services** > **TR-069**. The following page appears.



2. Fill in the fields, using the information in the following table. Values appear in the **Stun Server** section if that feature is configured for your system.
3. To connect to the ACS, in the **Client Configuration** section, click the **Inform now** button.

4. Management by ACS is *enabled* by default. To *disable* this option, click the **slide button** to the right of **Enabled** near the top of the page.
5. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Field Name	Description
Server Configuration section	
Management server URL	Enter the URL of the management server such as http://youracsname.youracsprovider.com.
Inform interval (secs)	Enter the number of seconds for how often the gateway contacts the host server. The default setting is whatever interval is defined on your ACS.
ACS username	Enter the user name for the ACS. **Note:** If you clear this field and the **ACS Password** field, the ACS will populate these fields on the next inform.
ACS password	Enter the password for the ACS.
Use base MAC as TR-069 serial number	This option is *enabled* by default. The base MAC address of your device is used as the serial number. To use the device's actual serial number instead, click the **slide button** to the right which disables this option.
Client Configuration section	
Allow solicit from ACS	This feature is *enabled* by default. To *prevent* solicitation transactions from your ACS, click the **slide button**.
TR-069 local port	Enter the port number for the local port as defined for your ACS. The default is **7547**.
Connection request username	Enter the user name for requesting the connection. **Note:** If you clear this field and the **Connection request password** field, the ACS will re-populate these fields on the next inform.
Connection request password	Enter the password for requesting the connection.

Stun Server

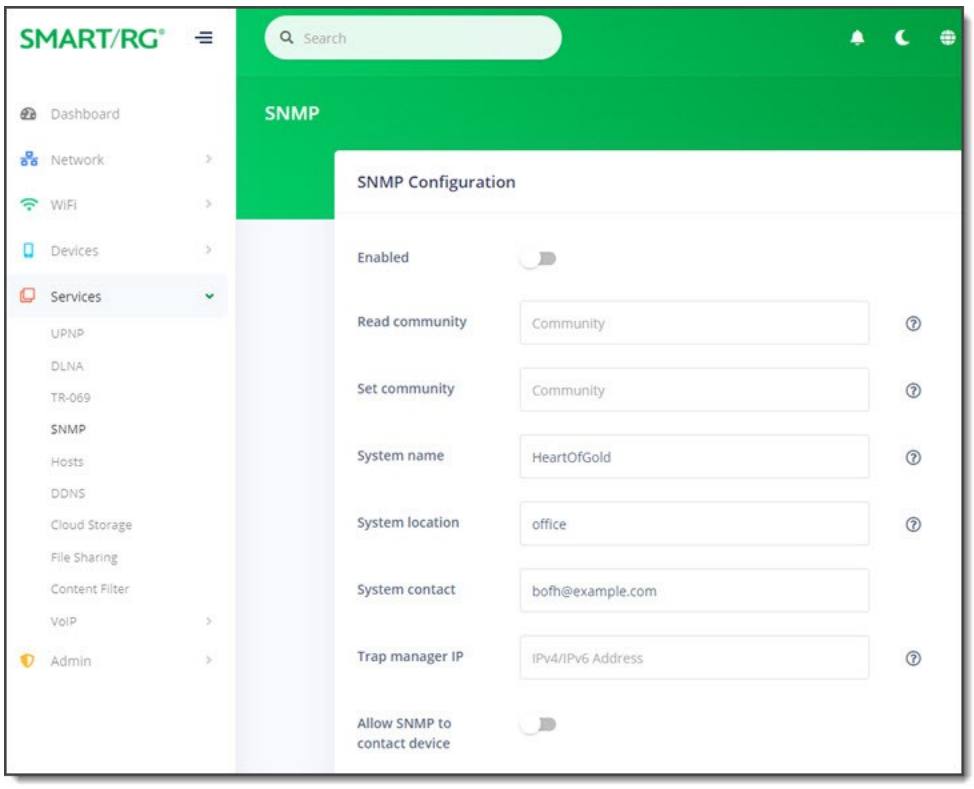
Note: Values appear for these fields *only* when a STUN server is configured.

Minimum keep alive	The minimum time(in seconds)that the keepalive function should be active. Options are **0** - **Unlimited**. The default is **30** seconds.
Maximum keep alive	The maximum time(in seconds)that the keepalive function should be active. Options are **0** - **Unlimited**. The default is **3600** seconds.
Server address	The assigned network address of the physical STUN server. An invalid address will produce an immediate on-page error message from the gateway. Maximum length is 256 characters.
Server port	The port number associated with your STUN server infrastructure. Options are **0** - **64435**. The default is **19302**.
Username	The user name by which the gateway accesses the STUN infrastructure. Maximum length is 256 characters. Special characters are allowed.

SNMP

On this page, you can configure an SNMP service for the gateway.

1. In the left menu, click **Services** > **SNMP**. The following page appears.



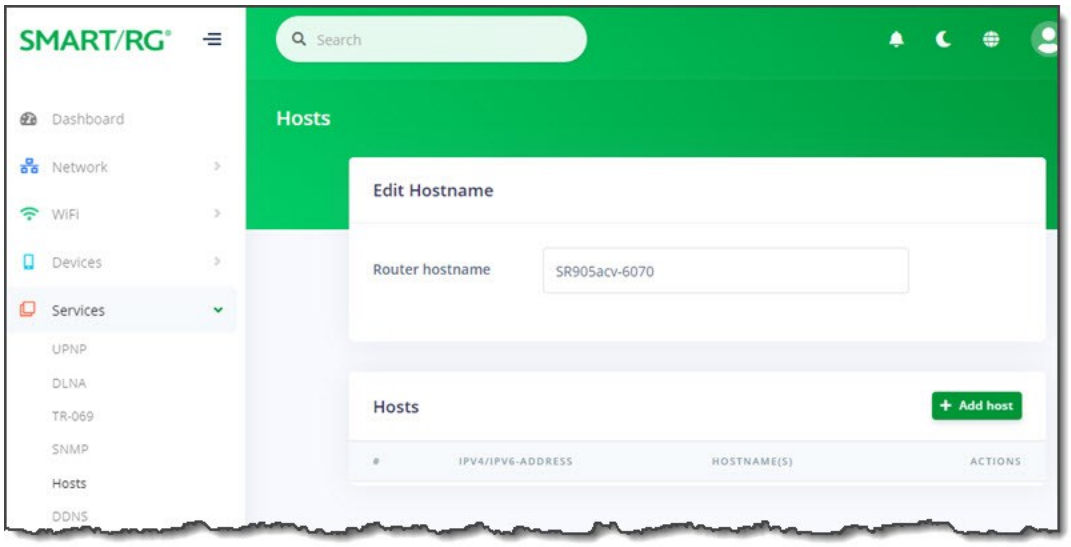
2. To *enable* the SNMP service, click the **slide button** to the right of **Enabled**.
3. Fill in the fields, using the information in the following table. All fields are optional.
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Field Name	Description
Read community	Enter the SNMP community string for your network which allows read-only access.
Set community	Enter the SNMP community string for your network which allows read-write access.
System name	Modify the name of the gateway.
System location	Modify the default location of this service.
System contact	Enter the email address for the contact person.
Trap manager IP	Enter the IP address of the server where the SNMP trap manager is located.
Allow SNMP to contact device	This option is *disabled* by default. To *enable* this option, click the **slide button**.

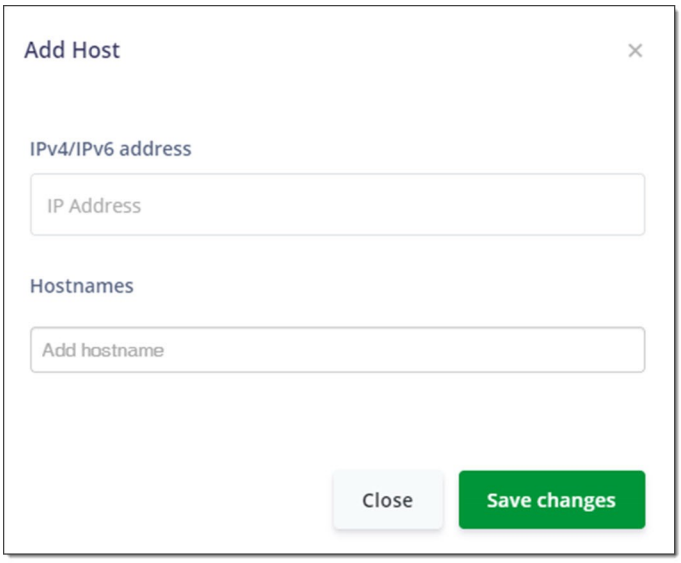
Hosts

On this page, you can configure the hostname of the gateway and add IP addresses for other hosts on the gateway. To begin, configure the host servers in the **Network** section.

1. In the left menu, click **Services** > **Hosts**. The following page appears.



2. To add a host:
   a. Click the **Add Host** button to the right of the Hosts section heading. The **Add Host** dialog box appears.



   b. In the **IPv4/IPv6 address** field, enter the host IP address.

c. In the **Hostnames** field, enter the host name and press **Enter** or **Tab**. The name is added and the cursor moves to a new **Add hostname** entry field. To add more hosts, repeat this step as needed.

Note: No spaces are allowed.

You can also delete names from this field by clicking the **X** next to the name.

d. Click **Save changes**.

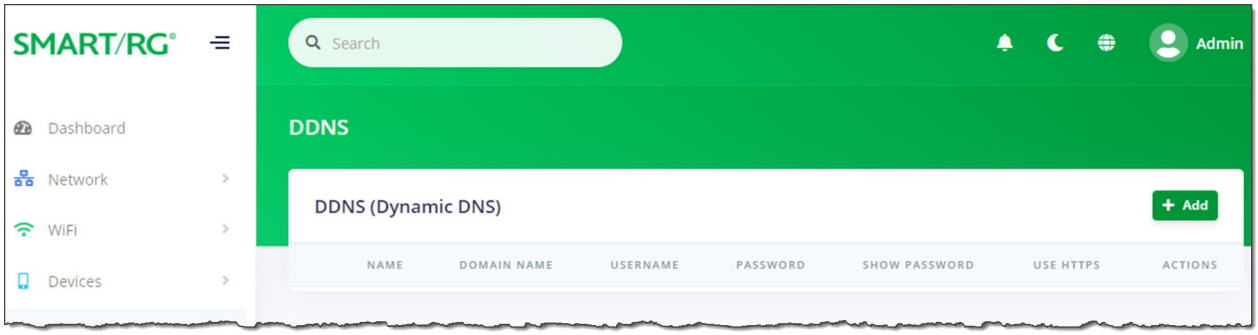
3. To edit the details of a host:
   a. Click the **Edit** icon ( ) next to the host that you want to edit. The **Add/Edit Item** dialog box appears.
   b. Modify the fields as needed.
   c. Click **Save changes**.
4. To delete a host, click the **Delete** icon ( ) next to the host that you want to delete.
5. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

DDNS

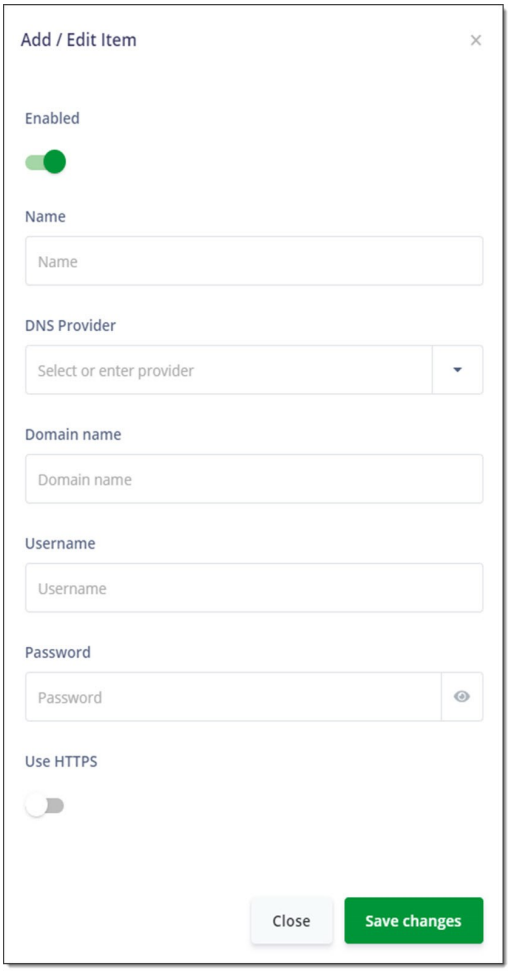
On this page, you can configure the DDNS settings for the gateway.

Dynamic DNS allows remote access the router from the Internet using a domain name instead of an IP address. An account on a DDNS service provider is required to implement this feature.

1. In the left menu, click **Services** > **DDNS**. The following page appears.



2. To add a dynamic DNS server:
   a. Click the **Add** button to the right of the **DDNS (Dynamic DNS)** section heading. The **Add / Edit Item** dialog box appears. New server definitions are enabled by default.



b. Fill in the fields, using the information in the table below.
c. Click **Save changes**.

3. To edit the details of a server:
   a. Click the **Edit** icon ( ) next to the server that you want to edit. The **Add/Edit Item** dialog box appears.
   b. Modify the fields as needed, using the information in the table below.
   c. Click **Save changes**.
4. To delete a server, click the **Delete** icon ( ) to the right of the server that you want to delete.
5. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Field Name	Description
Enabled	New server definitions are *enabled* by default. To *disable* a configuration, click the **slide button**.
Name	Enter a descriptive name for this entry.
DNS Provider	*(Optional)* Select or enter the DNS provider.

Field Name	Description
Domain name	Enter the URL or name of the domain.
Username	Enter the user name required to access the domain.
Password	Enter the password required to access the domain. To display the password, click the **Show/Hide** icon ( ).
Use HTTPS	(*Optional*) To *enable* HTTPS security, click the **slide button**.

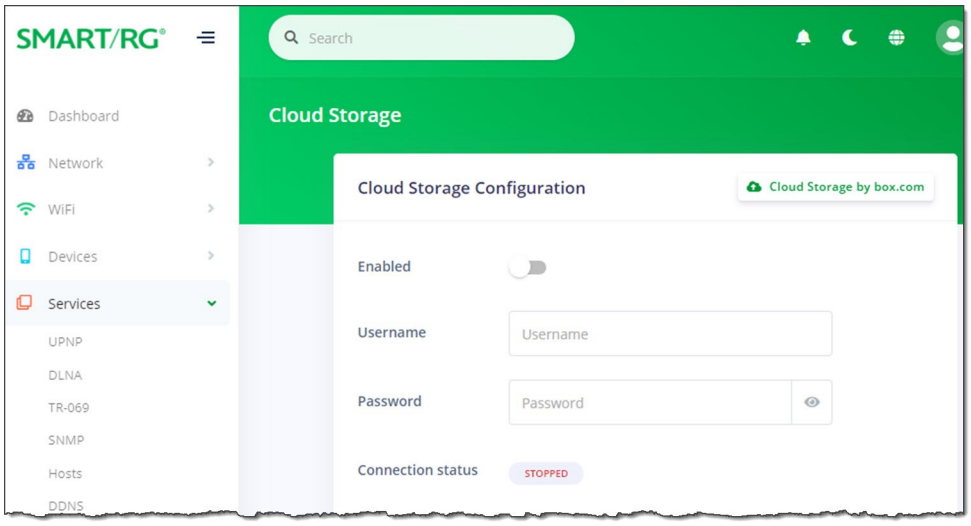
Cloud Storage

On this page, you can configure access to a cloud storage account. Cloud storage is supported by box.com.

To create an account, click the **Cloud Storage by box.com** button at the top of this page.

Warning: To link a box.com account with this gateway, enable the BOX share on the Services > File Sharing page first. Then return to this page and enter the related credentials. If you don't follow this sequence, you may have to perform a factory reset (FRESET) of the gateway.

1. In the left menu, click **Services** > **Cloud Storage**. The following page appears. The connection status for existing cloud storage accounts is displayed at the bottom of the page.



2. To *enable* cloud storage, click the **slide button** to the right of **Enabled**.
3. In the **Username** field, enter the user name for accessing your cloud storage account.
4. In the **Password** field, enter the password for accessing your cloud storage account.
   To display the password, click the **Show/Hide** icon ( ).
5. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

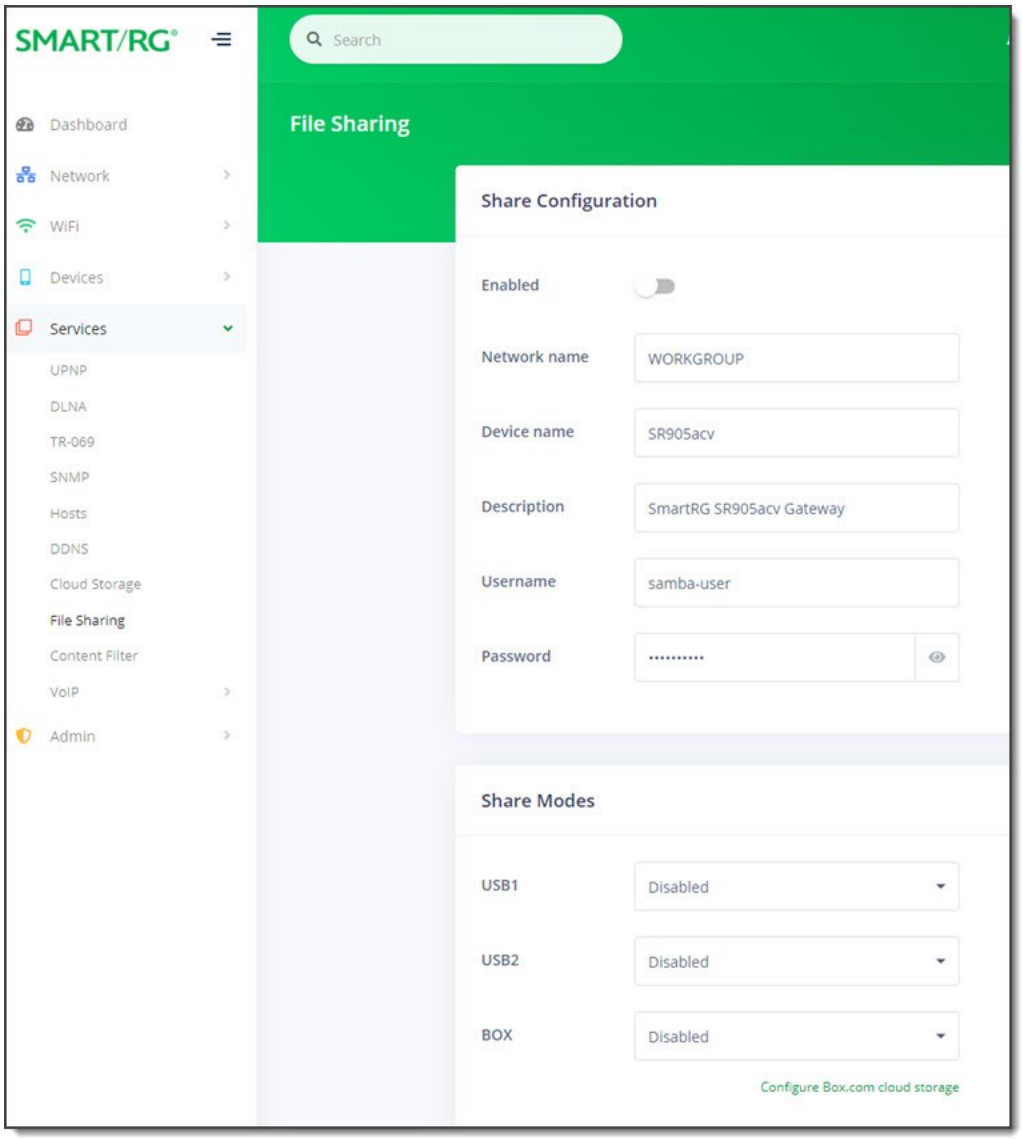
File Sharing

On this page, you can configure network settings and shares (on box.com) settings for sharing files.

Warning: To link a box.com account with this gateway, enable the BOX share on this page *first*. *Then* go to the Services > Cloud Storage page and enter the related credentials. If you don't follow this sequence, recovering your device may require a factory reset (FRESET) of the gateway.

To create an account, click the **Cloud Storage by box.com** link at the bottom of this page.

1. In the left menu, click **Services** > **File Sharing**. The following page appears. This feature is *disabled* by default.



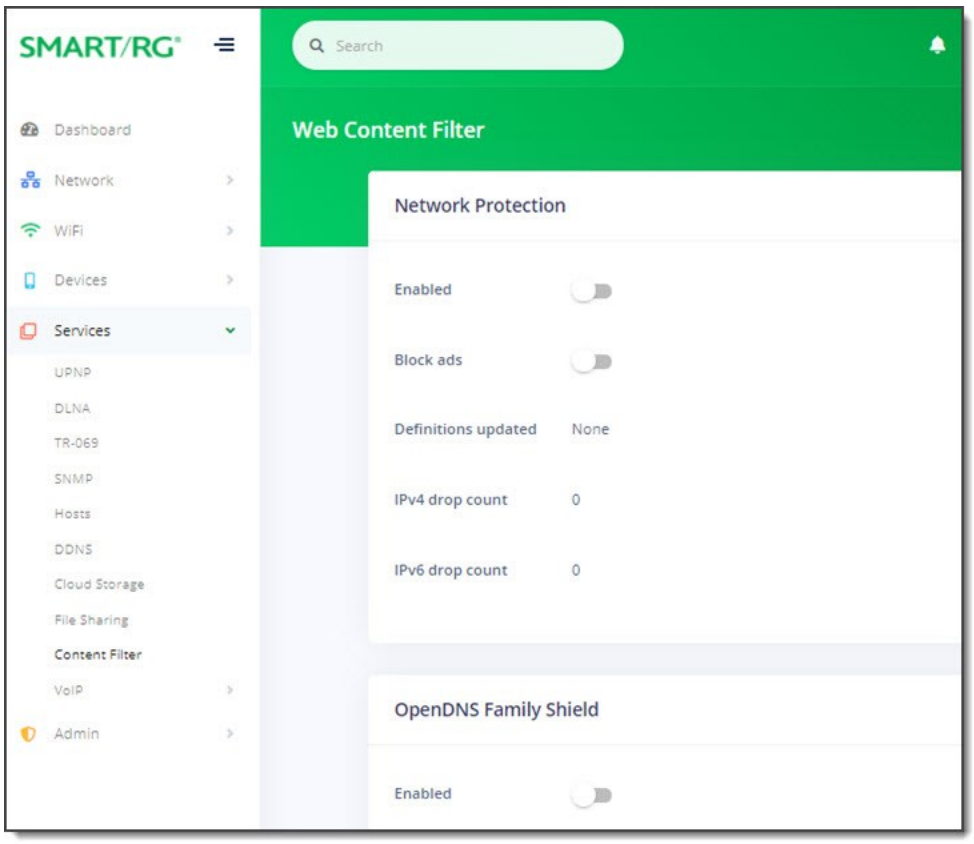
2. To *enable* file sharing, click the **slide button** to the right of **Enabled**.
3. Modify the fields as needed, using the information provided in the following table.
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Field Name	Description
Share Configuration section	
Network name	Enter the name of the network used for file sharing.
Device name	Enter the device name.
Description	Enter a brief description of the device.
Username	Enter the user name for your cloud storage account.
Password	Enter the password for your cloud storage account. To display the password, click the **Show/Hide** icon ().
Share Modes section	
USB1 USB2 BOX	Select whether this share is disabled, read-only or read & write. The USB port to which you connect first is designated as USB1 and the other port is designated as USB2. The gateway uses either port equally. Options are **Disabled**, **Read only**, and **Read / Write**. The default is **Disabled**. **Note:** To use the **BOX** option, create a box.com cloud storage account first. To do so, click the **Cloud Storage by box.com** link near the bottom of the page.

Content Filter

On this page, you can configure web content filtering, i.e., parental controls. If you enable **Network Protection** (and optionally the **Block ads** feature), approximately 20 thousand domains are blocked. The domains are gathered from a few crowd-sourced databases of sites known to serve malware, randomware, adware, etc. The feature is similar to pihole and adguard.

1. In the left menu, click **Services** > **Content Filter**. The following page appears.



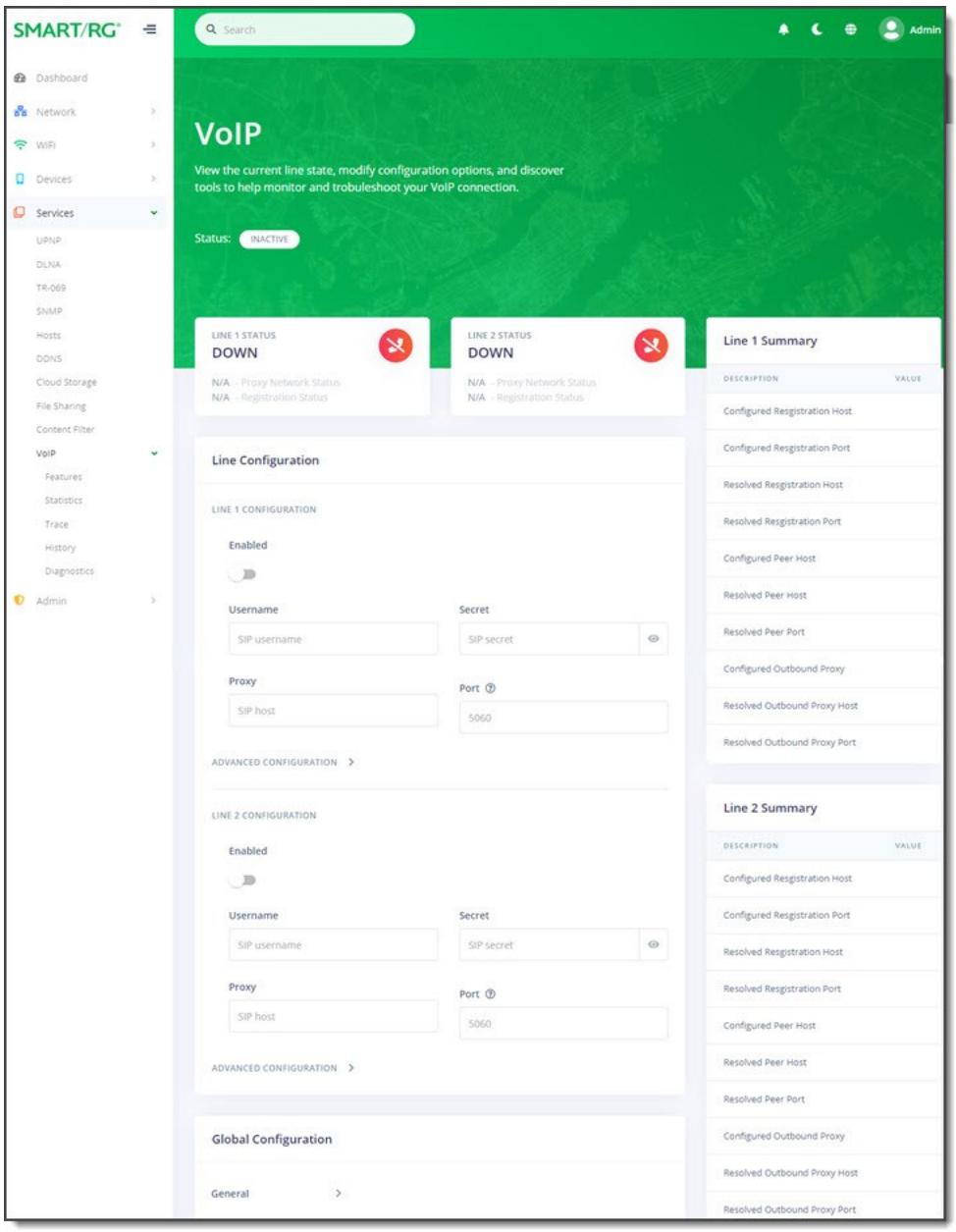
2. To *enable* network protection, click the **slide button** to the right of **Enabled**.
3. Fill in the fields, using the information in the table below.
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Field Name	Description
Block ads	To *enable* the advertisement blocking feature, click the **slide button**.
Definitions updated	The date and time when the filter definitions were last updated. If the definitions were never updated, "None" appears in the field.
IPv4 drop count	The number of dropped packets on the IPv4 network.
IPv6 drop count	The number of dropped packets on the IPv6 network.
OpenDNS Family Shield section	
Enabled	To *enable* the adult content blocking feature, click the **slide button**.

VoIP

On this page, you can configure the VoIP settings for your gateway.

1. In the left menu, click **Services** > **VoIP**. The following page appears. The **Line Summary** sections list the phone features.



2. In the **Line Configuration** section for the line you want to enable, to enable VoIP service click the **slide button** below **Enabled**. The status of the service is displayed in the **Line Status** sections.
3. Modify the settings as needed, using the information in the table below. Click the **ADVANCED CONFIGURATION** heading to view and configure the settings for each line. G
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Field Name	Description
Username	Enter the user name for the authorized SIP user.
Secret	Enter the SIP secret. To display the secret, click the **Show/Hide** icon ().
Proxy	Enter the SIP host.
Port	Enter the SIP port. If you enter a port number in this field, SRV lookup is disabled.
SIP Configuration section	
Outbound proxy	Enter the SIP outbound proxy.
Outbound proxy port	Enter the SIP outbound port. If you enter a port number in this field, SRV lookup is disabled.
Auth username	Enter the default username for this phone.
Caller ID Name	Enter the name to display as the caller ID.
Registrar	Enter the SIP registrar.
Registrar Port	Enter the port for the SIP registrar to use when SRV lookup is not desired.
Session max expires	Enter the number of seconds that can elapse before a session is considered expired. The default is **1800** seconds.
Session min interval	Enter the minimum interval for closing a conversation. This value must be **90 seconds** or greater. The default is **90 seconds**.
SIP Codecs section	
SIP codec table	The table lists 4 codecs in priority order. To edit a codec selection, click the **Edit** icon (). The Edit SIP Codec dialog box appears. In the **SIP Codec** field, select the G.7xx codec that you want used. Then, click **Save changes**.
SIP Features section	
Three-way conference enabled	This feature is *disabled* by default. To *enable* 3-way conferencing, click the **slide button**.
Caller transfer enabled	This feature is *disabled* by default. To *enable* call transfer, click the **slide button**.
Caller ID enabled	This feature is *enabled* by default. To *disable* the transfer features, click the **slide button**.
Block caller ID delivery enabled	This feature is *disabled* by default. Click the **slide button** to *enable* users to temporarily block the display of their caller ID for a single call. Options are: • **On:** Caller ID blocking is managed locally. • **Off:** Caller ID blocking is managed by the remote switch.
Call park	This feature is *disabled* by default. To *enable* call parking, click the **slide button**.
Call hold enabled	This feature is *disabled* by default. To *enable* call holding, click the **slide button**.
Dial Options section	
Digit map	Enter the digit map for your phone system.

Field Name	Description
Interdigit timeout	Enter the number of seconds that can elapse between digits being entered by the caller. The default is **4000** seconds.
SIP DTMF mode	Select the Dual Tone Multi Frequency mode. Options are **INFO**, **RFC 2833**, **inband**, and **auto**. The default is **RFC 2833**.
Message Waiting Indication section	
AMWI	This feature is *disabled* by default. To *enable* the Active Message Waiting Indicator, click the **slide button**.
VMWI	This feature is *disabled* by default. To *enable* the Voice Mail Waiting Indicator, click the **slide button**.
VMWI refresh interval (minutes)	Enter how long in minutes between checks for voice mail. This setting is in addition to the interval set at the system level.
MWI subscribe	This feature is *disabled* by default. To *enable* the MWI subscription, click the **slide button**.
MWI unsolicited notify	This feature is *disabled* by default. To *enable* the receipt of unsolicited messages, click the **slide button**.
Fax/Modem section	
T.38 fax	This feature is *disabled* by default and instructs the gateway to accept faxes using the T.38 protocol. To *enable* it, click the **slide button**.
Fax passthrough	This feature is *enabled* by default and allows faxes that do not use the T.38 protocol to be received. To *disable* it, click the **slide button**.
Modem passthrough	This feature is *disabled* by default and allows modem signals to be transmitted using pulse code modulation (PCM) packets. To *enable* it, click the **slide button**.
Fax/Modem call waiting block	This feature is *disabled* by default and disables the call waiting actions while the fax or modem is in active use. To *enable* it, click the **slide button**.
Call Waiting section	
Enable call waiting	This feature is *enabled* by default. To *disable* call waiting, click the **slide button**.
Enable call waiting caller ID	This feature is *disabled* by default. To *enable* display caller ID for waiting calls, click the **slide button**.
Enable cancel call waiting	This feature is *disabled* by default. To *enable* the Cancel Call Waiting feature, click the **slide button**.
Do Not Disturb section	
Enabled	This feature is *disabled* by default. To *enable* this feature, click the **slide button**.
Status	This feature is *disabled* by default. To *allow* users to set the status of the Do Not Disturb feature, click the **slide button**.
Anonymous Blocking section	
Enabled	This feature is *disabled* by default. To *allow* anonymous calls to be received, click the **slide button**.
Status	This feature is *disabled* by default. To allow users to set the status of the Anonymous Blocking feature, click the **slide button**.
Cal Forwarding No Answer section	
Enabled	This feature is *disabled* by default. To *enable* forwarding of calls when the target line is not answered, click the **slide button**.

Field Name	Description
No answer timeout	Enter the length of time (in seconds) that the system will wait to forward an unanswered call.
Status	Indicates whether the Call Forwarding No Answer feature is active on this line.
Forwarding extension	Enter the extension to which an unanswered call will be transferred.
Forwarding code	Enter the star code that users must enter to activate this feature. The default is ***92**.
Call Forwarding Busy section	
Enabled	This feature is *disabled* by default. To *enable* forwarding of calls when the target line is engaged, click the **slide button**.
Status	Indicates whether the Call Forwarding Busy feature is active on this line.
Forwarding extension	Enter the extension to which unanswered calls will be transferred.
Forwarding code	Enter the star code that users must enter to activate this feature. The default is ***90**.
Call Forwarding Unconditional section	
Enabled	This feature is *disabled* by default. To *enable* forwarding all calls, click the **slide button**.
Status	Indicates whether the Call Forwarding Unconditional feature is active on this line.
Forwarding extension	Enter the extension to which all calls will be transferred.
Forwarding code	Enter the star code that users must enter to activate this feature. The default is ***72**.
Speed Dial section	
Speed dial 8 enabled	This feature is *disabled* by default. To *enable* speed dialing, click the **slide button**. Enter the phone numbers for each digit in the fields below.
Speed Dial 1 -9	(*Appears when the **Speed dial 8 enabled** feature is activated*) Enter the phone number for each speed dialing option.
Line Configuration section	
Rx gain	Select the gain value for received transmissions. Options are **-12** - **0**. The default is **-9**.
TX gain	Select the gain value for received transmissions. Options are **-12** - **0**. The default is **-3**.
VAD	This feature is *enabled* by default. To *disable* voice activated detection, click the **slide button**.
On-hook min	The minimum number of milliseconds required to validate an on-hook event. The default is **1100 milliseconds**.
Off-hook min	The minimum number of milliseconds required to validate an off-hook event. The default is **350 milliseconds**.
Hook flash max	Enter the maximum length of time that the hook flash has to operate. The default is **1099 milliseconds**.
Hook flash min	Enter the minimum length of time that the hook flash has to operate. The default is **151 milliseconds**.
Pulse digit break max	Enter the maximum length of time that the break between digits being dialed will last. The default is **60 milliseconds**.
Pulse digit break min	Enter the minimum length of time that the break between digits being dialed will last. The default is **40 milliseconds**.

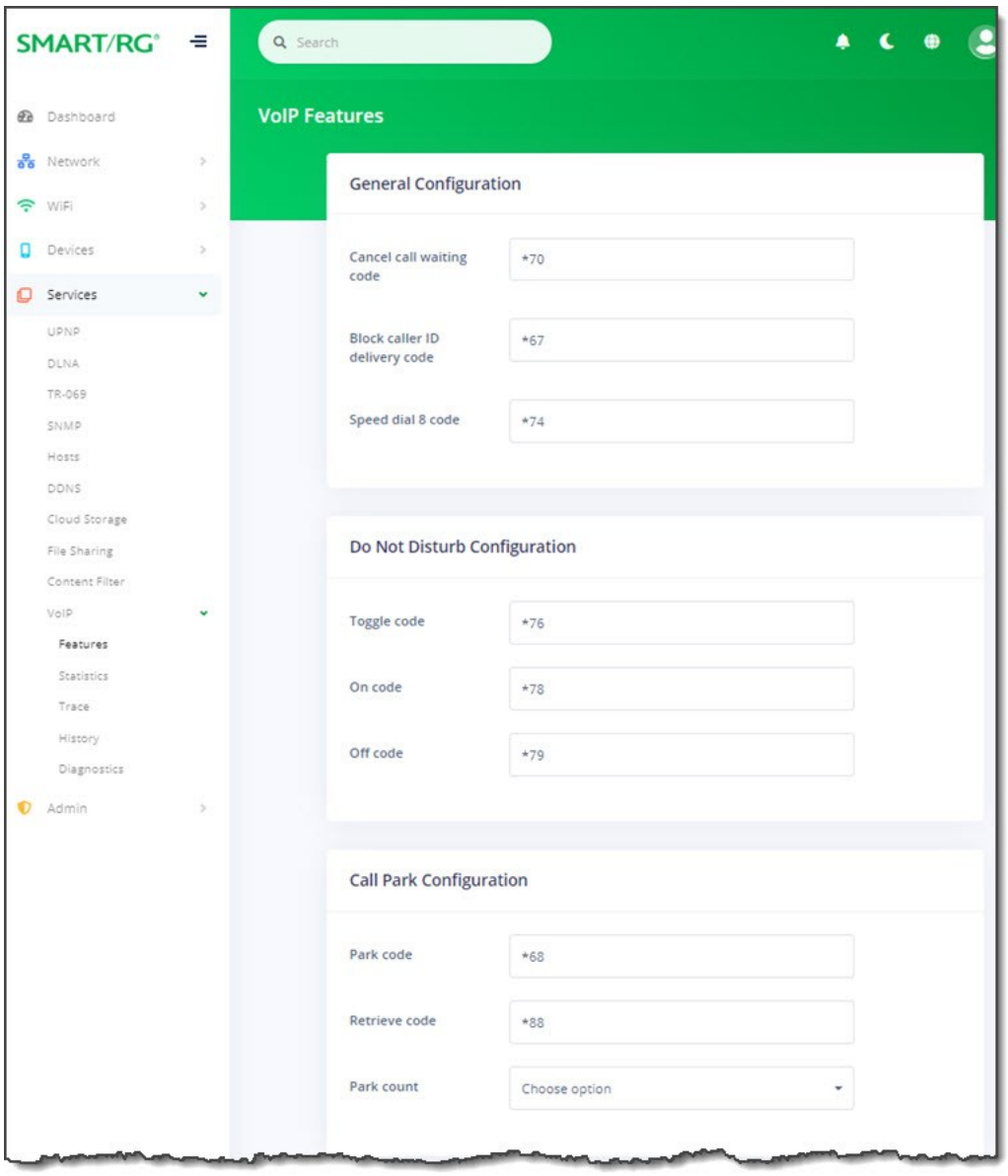
Field Name	Description
Pulse digit make max	Enter the maximum length of time that the make between digits being dialed will last. The default is **60 milliseconds**.
Pulse digit make min	Enter the minimum length of time that the make between digits being dialed will last. The default is **40 milliseconds**.
Pulse Interdigit min	Enter the minimum length of time that can elapse between digits being dialed. The default is **250 milliseconds**.
Global Configuration section	
General subsection	
Region	Select the location where your VoIP phone is located.
FXS port impedance	Select the impedance value for the FX port. Options are **600 Ohm (20 Hz)**, **600 Ohm (25 Hz)**, and **ETSI (25 Hz)**.The default is **600 Ohm (20 Hz)**.
CID standard	Select caller ID standard. Options are **Telcordia**, **ETSI FSK**, **ETSI DTMF**, and **SIN 227**. The default is **Telcordia**.
ETSI CID alert signal	Select when Caller ID information is sent to the destination phone. Options are **Full Ring**, **Ring Pulse**, **Dual Tone**, and **Line Reversal + Dual Tone**. The default is **Full Ring**.
ETSI WMWI alert signal	Select when Message Waiting information is sent to the destination phone. Options are **Dual Tone**, **Ring Pulse**, and **Line Reversal + Dual Tone**. The default is **Dual Tone**.
Flash services profile	Select which profile will be used for flashing devices. Options are **North America** and **Digit Directed A**.
ADVANCED CONFIGURATION subsection	
Log level	Select the degree of logging. Options are **DTMF**, **Debug**, **Notice**, **Warning**, and **Error**. The default is **Warning** + **Error**.
DNS Management section	
DNS management enabled	This feature is *disabled* by default. To *enable* DNS management, click the **slide button**.
DNS refresh interval	Select or enter how long between DNS refresh tasks. The default is **1800** seconds.
SIP Registration section	
Dialtone Without Registration	This feature is *disabled* by default. To *enable* a dial tone without SIP registration, click the **slide button**.
Registration expiry	Select or enter the number of seconds by which a registration must be refreshed to remain active. The default is **3600**.
Registration attempts	Select or enter the number of registrations attempts before the session is cancelled. The default is **zero** (**0**) or unlimited.
Registration retry interval	Select or enter how long in seconds the gateway waits before retrying to register a SIP connection. The default is **20**.
Registration refresh percentage	Select or enter the percentage of the Registration Expiry value when the system will send a refresh request. This is how long before expiration the request will be sent. The default is **zero** (**0**).
SIP Query section	

Field Name	Description
Query enabled	This feature is *enabled* by default. To *disable* SIP queries, click the **slide button**.
Query frequency seconds	Select or enter how long in seconds the gateway waits before retrying to send a SIP query. The default is **600**.
Query timeout (ms)	Select or enter how long in seconds the gateway waits before timing out a SIP connection. The default is **2000**.
Use registration expire pct	Select or enter the percentage of the Registration Expiry value when the system will send a refresh request. This is how long before expiration the request will be sent. The default is **zero** (**0**).
Fail over max queries	Select or enter the maximum number of queries before failover is initiated. The default is **2**.
Failed state query frequency	Select or enter how long in seconds the gateway waits before retrying to send a SIP query. The default is **300**.
Failed state registration expire pct	Select or enter the percentage of the Registration Expiry value when the system will send a refresh request. This is how long before expiration the request will be sent. The default is **zero** (**0**).
Call Waiting section	
Call waiting alert interval	Select how often the call waiting alert will sound, in seconds. The default is **10**.
Call waiting tone repetition	Select how many times the call waiting alert will sound. The default is **2**.
QOS section	
SIP	Select the priority level for SIP.
RTP	Select the priority level for RTP.
SIP PRACK	This option is *disabled* by default. To *enable* provisional responses, click the **slide button**.
SIP Alert-Info Prefix	Enter the prefix for SIP alerts.

Features

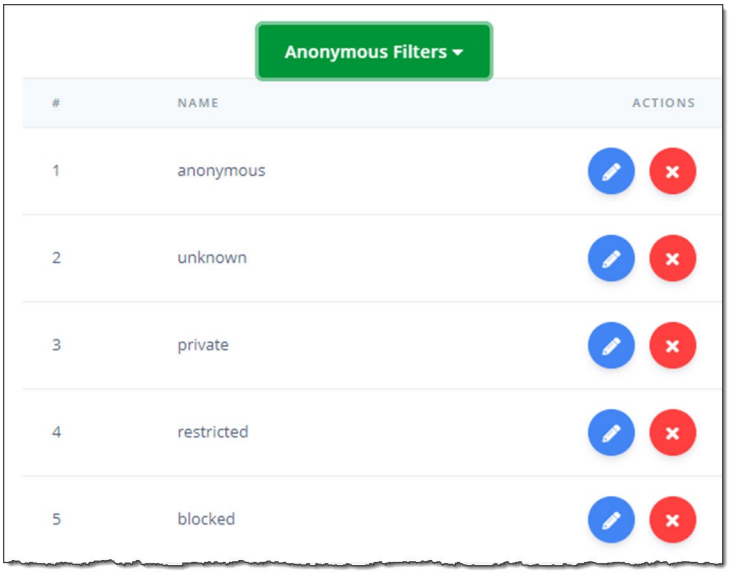
On this page, you can configure VoIP features such as call waiting for your gateway.

1. In the left menu, click **Services** > **VoIP** > **Features**. The following page appears.



2. Modify the settings using the information in the following table.

3. To view and manage the anonymous filters defined for your gateway:
   a. Click **Anonymous Filters** at the bottom of the page. A list of the filters appears.



   b. To change a filter name, click the **Edit** icon ( ). The Edit Name dialog box appears. Enter the new name and click **SAVE**.
   c. To delete a filter, click the **Delete** icon ( ) next to the host that you want to delete.
   d. To add a filter, click the **Add** icon ( ) next at the bottom of the section where you want to add it. The Add dialog box appears. Enter the name and click **SAVE**.
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

The fields on this page are described in the table below.

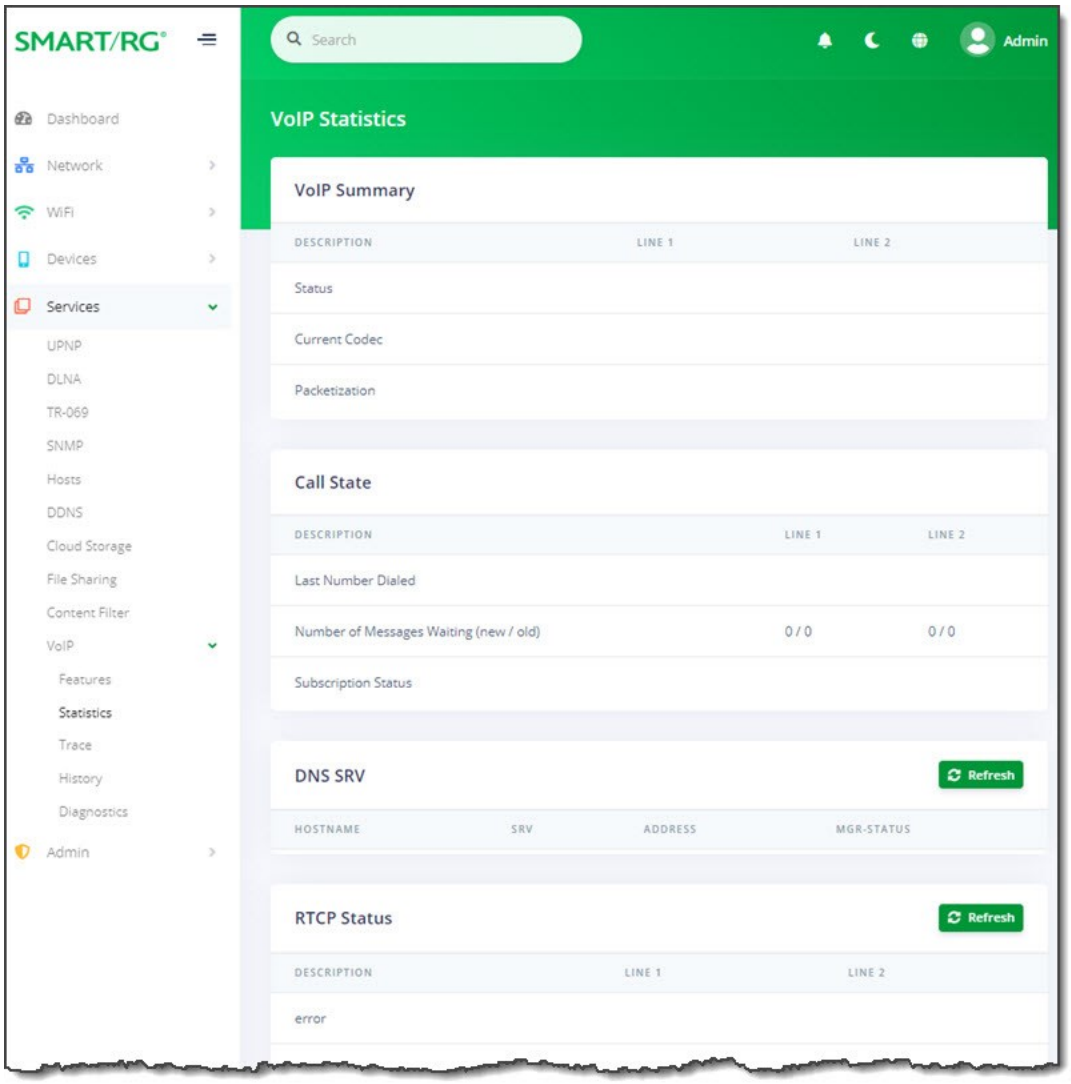
Field Name	Description
General Configuration section	
Cancel call waiting code	Enter the star code for canceling call waiting. The default is ***70**.
Block caller ID delivery code	Enter the star code for blocking caller ID. The default is ***67**.
Speed dial 8 code	Enter the star code for enabling speed dialing. The default is ***74**.
Do Not Disturb Configuration	
Toggle code	Enter the star code for enabling this feature. The default is ***76**
On code	Enter the star code for activating this feature. The default is ***78**.
Off code	Enter the star code for de-activating this feature. The default is ***79**.

Field Name	Description
Call Park Configuration section	
Park code	Enter the star code for parking a call. The default is ***68**.
Retrieve code	Enter the star code for retrieving a parked call. The default is ***88**.
Park count	Select the number of calls that can be parked at one time. Options are **1** - **3**.
Call Hold Configuration section	
Activate call on hold	Enter the star code for enabling the hold option. The default is ***43**.
Deactivate call on hold	Enter the star code for disabling the hold option. The default is ***44**.
Call Forwarding Configuration section	
Unconditional code	Enter the star code for forwarding all calls. The default is ***72**.
Unconditional cancel code	Enter the star code for canceling call forwarding. The default is ***73**.
Busy code	Enter the star code for forwarding calls when a phone is engaged. The default is ***90**.
Busy cancel code	Enter the star code for canceling the forwarding-when-busy option. The default is ***91**.
No answer code	Enter the star code for forwarding calls when a call is not answered. The default is ***92**.
No answer cancel code	Enter the star code for canceling the forwarding-when-no-answer option. The default is ***93**.
No answer timeout code	Enter the star code for enabling the timeout setting for the no-answer forwarding option. The default is ***94**.
Custom Call Blocking section	
Anonymous blocking on code	Enter the star code to enable the blocking of anonymous calls. The default is ***77**.
Anonymous blocking off code	Enter the star code to disable the blocking of anonymous calls. The default is ***87**.

Statistics

On this page, you can view VoIP statistics for your gateway including call state, RTCP status, and Jitter status.

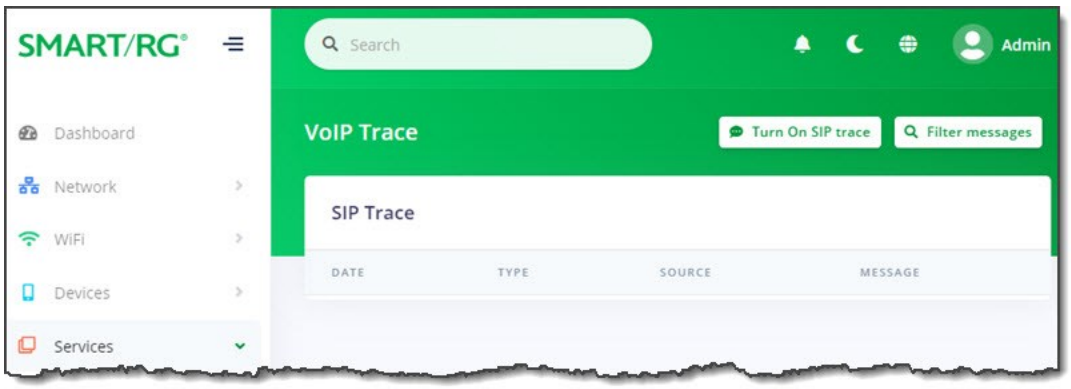
In the left menu, click **Services** > **VoIP** > **Statistics**. The following page appears. To update the data, click a **Refresh** button.



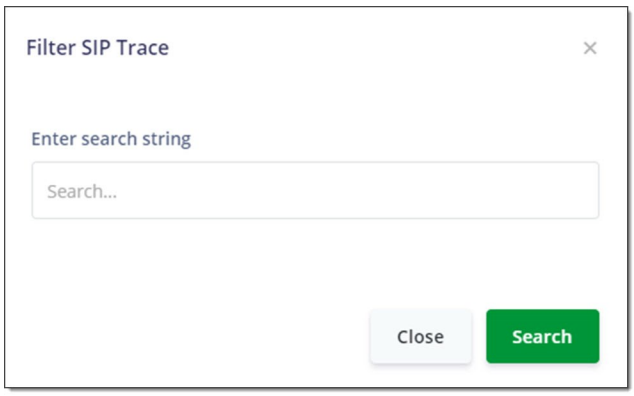
Trace

On this page, you can view the VoIP log for your gateway and configure the log settings.

1. In the left menu, click **Services** > **VoIP** > **Trace**. The following page appears.



2. To enable SIP tracing, click the **Turn On SIP trace** button at the top right. The button label changes to **Turn Off SIP trace**.
3. To filter the message list:
   a. Click the **Filter messages** button. The Filter SIP Trace dialog box appears.

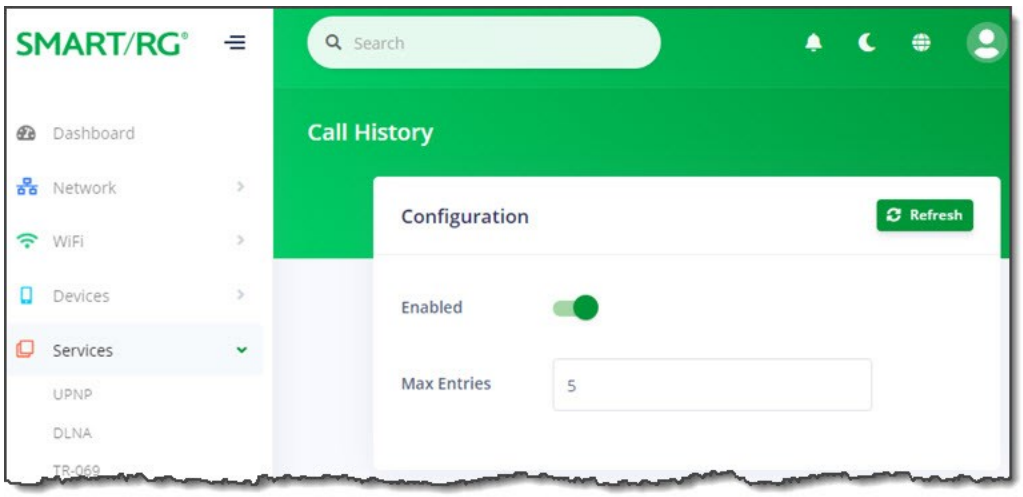


   b. Enter a search string and click **Search**. The message list refreshes to show the entries that match the string.
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

History

On this page, you can configure the call history settings.

1. In the left menu, click **Services** > **VoIP** > **History**. The following page appears.

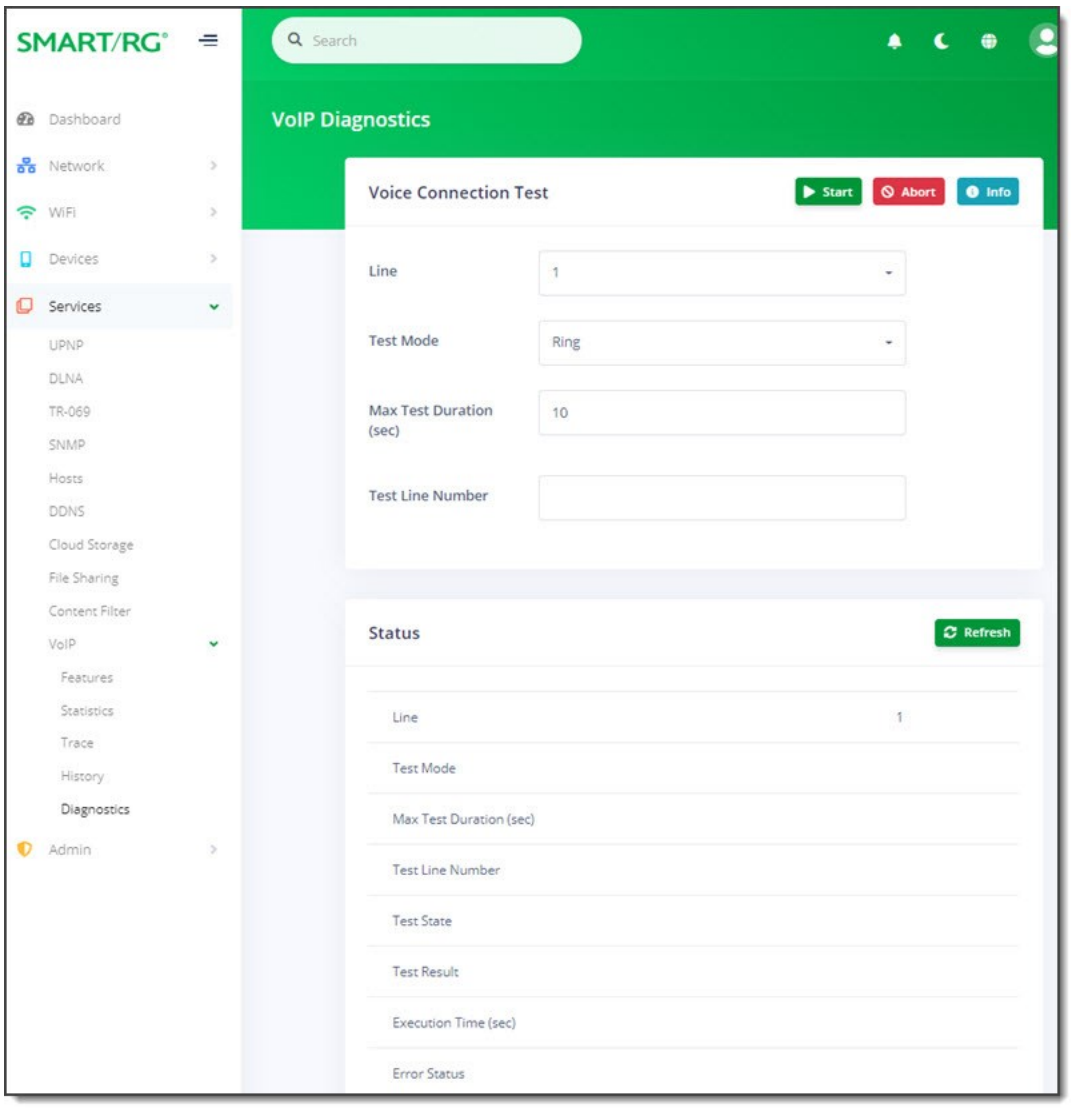


2. This feature is *enabled* by default. To *disable* SIP tracing, click the **slide button** next to **Enabled**.
3. (*Optional*) Enter the maximum number of entries kept in the call history file. Options are **0** (disabled) - **50**. The default is **5**.
4. To refresh the history, click the **Refresh** button to the right of the **Configuration** section heading.
5. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Diagnostics

On this page, you can configure the settings for testing voice connection to a remote test line and view the diagnostic statistics.

1. In the left menu, click **Services** > **VoIP** > **Diagnostics**. The following page appears. You can view helpful information about test configuration by clicking the **Info** button (Info) at the top right.



2. Modify the settings using the information in the following table.
3. To start a voice connection test, click the **Start** button (Start) at the top right.
4. To cancel a voice connection test, click the **Abort** button (Abort) at the top right.
5. To refresh the status data, click the **Refresh** button to the right of the **Status** section heading.
6. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Field	Description
Line	Select which of the two lines that you want to test.

Field	Description
Test Mode	Select the function that you want to test. Options are: • **Ring mode:** Verifies that the remote test line rings. This is the default. • **Answer mode:** Verifies that the remote test line answers. • **Tone mode:** Verifies that the remote test line generates a 2100 Hz tone.
Max Test Duration (sec)	Enter the maximum length allowed for the test in seconds. The default is **10**.
Test Line Number	Enter the phone number of the line you want to test.

Admin

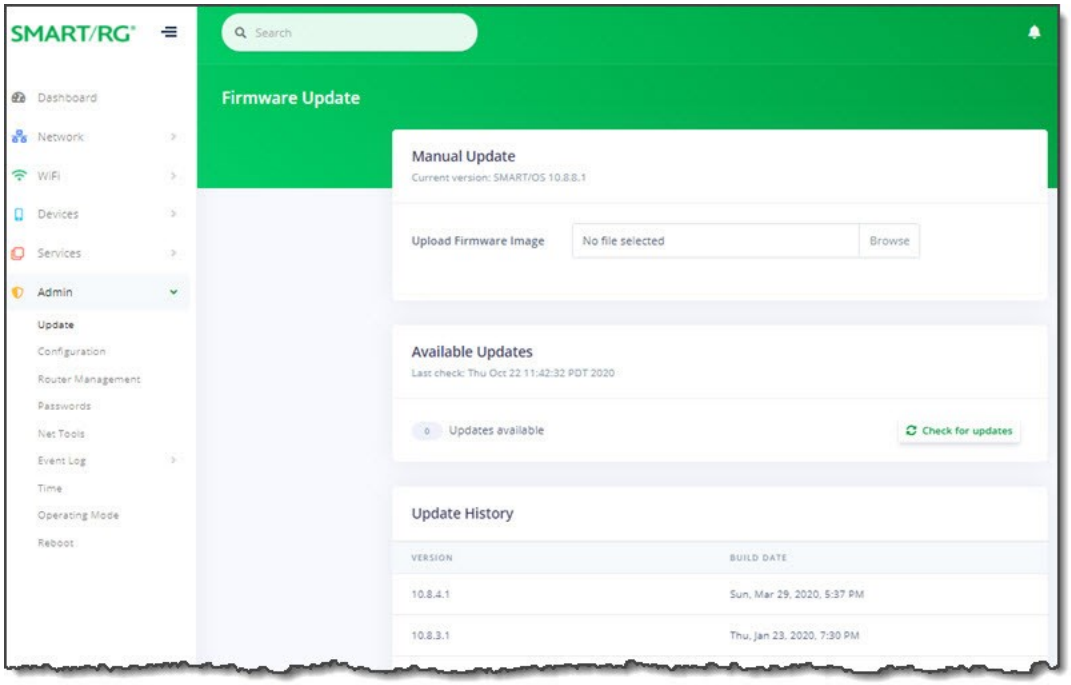
In this section, you can update firmware on your gateway, manage passwords, run diagnostics, and view the event log.

Update

On this page, you can update the firmware of your SmartRG gateway. Software updates for SmartRG products are available for download in the ADTRAN Support Community via your Customer Dashboard.

Note: Following a firmware upgrade, the gateway reboots; rebooting takes approximately 6 minutes.

1. In the left menu, click **Admin** > **Update**. The following page appears, showing the **Update History** at the bottom of the page. The version number and build date are listed for each update.



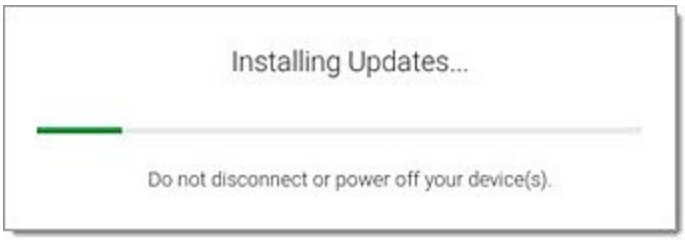
   Note: The current firmware version is listed below the **Manual Update** heading.

2. To update firmware manually:
   a. In the **Manual Update** section, click **Browse**. An Open dialog box appears.
   b. Navigate to and select the firmware image file to be installed and then click **Open**.
   A progress bar and a **Cancel** button appears.
   c. Click **Start Upgrade**. The Please wait popup appears, showing the Upgrading progress bar.

      Note: If the failed message appears, click the message to clear it. Then try downloading the file again and repeating the above steps.

3. To check for available updates:
    a. In the **Available Updates** section, click the **Check for updates** button. The CHECKING FOR UPDATES message appears. The **Update status** field refreshes to show a list of available updates or the 0 Updates available message.
    b. If updates are available, click **Install Updates**. A confirmation message appears.

    c. Click **Yes**. The installing message appears.

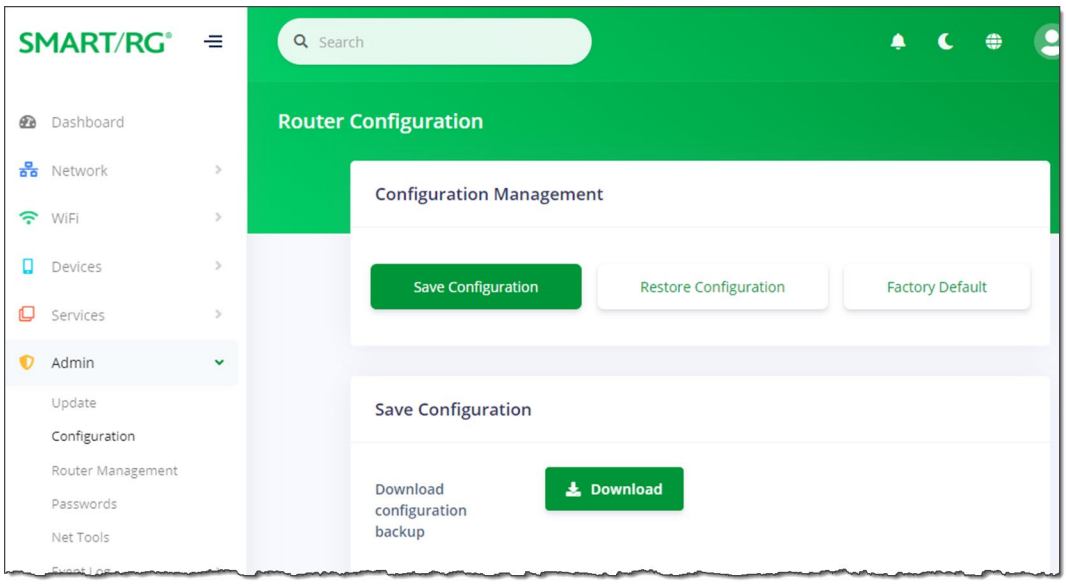


    When the installation has finished, the gateway reboots.

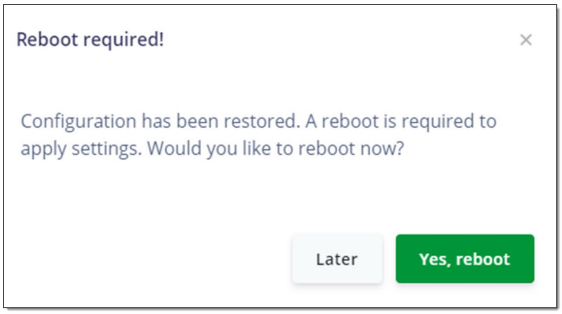
Configuration

You can save your settings (back up) to a local computer, restore previously saved settings, and reset your device to its factory settings. It is recommended that you save your settings as a first step whenever you plan to change the configuration.

1. In the left menu, click **Admin** > **Configuration**. The following page appears.



2. To back up your settings:
   a. Click the **Save Configuration** button.
   b. Click the **Download** button. The zipped .tar file is saved (.gz.zip format) to your default download location and is named "backup" followed by the gateway model number and the date in *yyyy-mm-dd* format, e.g., backup-SR905acv-2020-10-15.tar.gz.
3. To restore settings saved previously saved:
   a. Click the **Restore Configuration** button.
   b. In the **Restore Configuration** section, click **Browse** to select a file to upload, e.g., backup-SR905acv-2020-10-15.tar.gz and then click **Open**. The Reboot required dialog box appears.

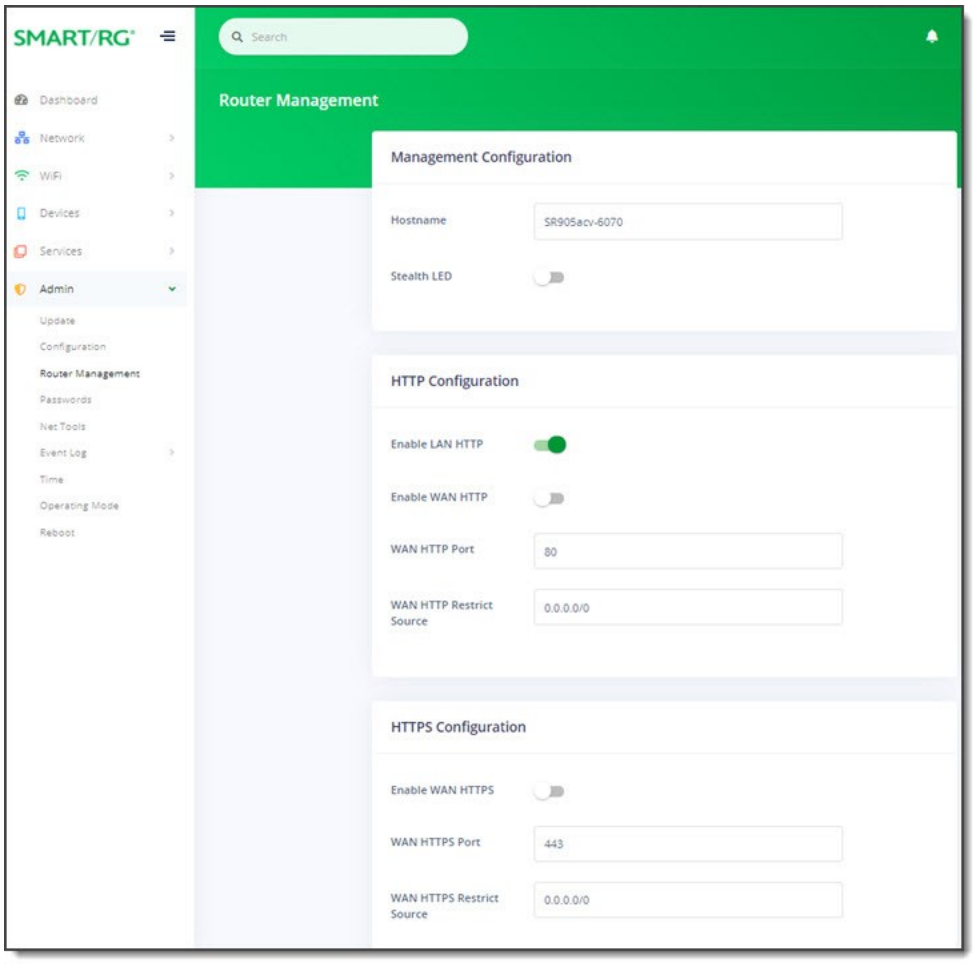


   c. Click **Yes, reboot**. The selected configuration is applied and the gateway reboots.
4. To restore the device to factory default settings:
   a. Click the **Factory Default** button.
   b. In the **Factory Default** section, click the **Factory reset** button. The factory reset warning dialog box appears.
   c. Click **Yes, reboot**. The device is restored to default configuration.

Router Management

On this page, you can enable or disable WAN HTTP and mobile management.

1. In the left menu, click **Admin** > **Router Management**. The following page appears.



2. Fill in the fields using the information in the table below.
3. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

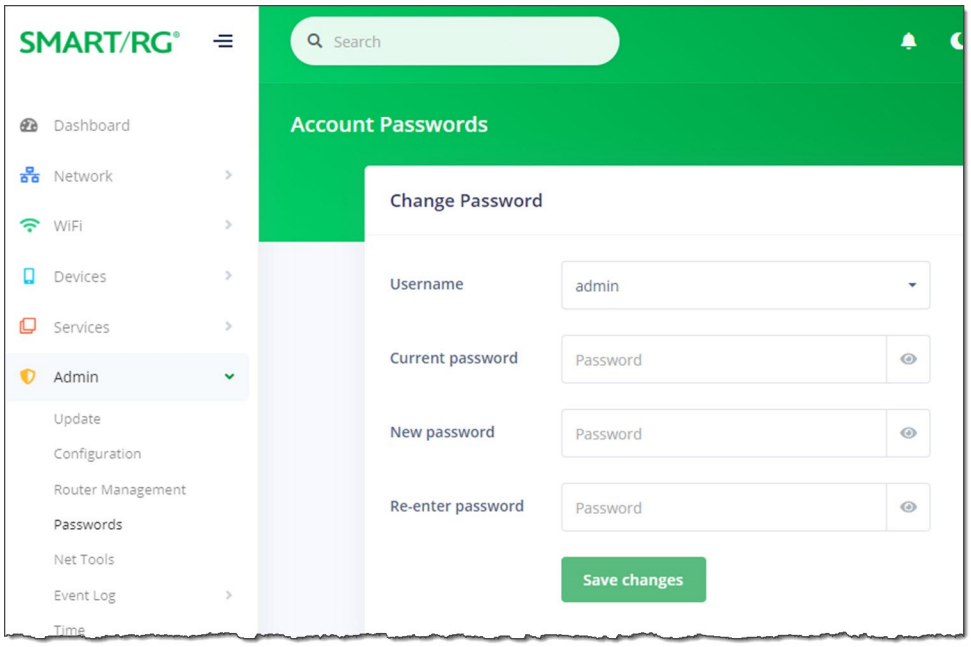
Field	Description
Management Configuration section	
Hostname	(*Optional*) Enter a new name for the host.
Stealth LED	This option *prevents* the LEDs on the gateway from shining. It is *disabled* by default. To *prevent* the LEDs from shining, click the **slide button**.

Field	Description
Enable Mobile Management	This option is *enabled* by default. It allows or denies the gateway to be remotely managed. To *disable* mobile management, click the **slide button**.
HTTP Configuration section	
Enable LAN HTTP	This feature is *enabled* by default. To *disable* LAN HTTP, click the **slide button**.
Enable WAN HTTP	This feature is *disabled* by default. To *enable* WAN HTTP, click the **slide button**.
WAN HTTP Port	(*Optional*) Enter a different port number for the WAN. The default is **80**.
WAN HTTP Restrict Source	(*Optional*) Enter the IP address for which you want access restricted.
HTTPS Configuration section	
Enable WAN HTTPS	This feature is *disabled* by default. To *enable* WAN HTTPS, click the **slide button**.
WAN HTTPS Port	(*Optional*) Enter a different port number for the secure WAN. The default is **443**.
WAN HTTPS Restrict Source	(*Optional*) Enter the IP address for which you want access restricted.

Passwords

On this page, you can change the passwords used to access your device.

1. In the left menu, click **Admin** > **Passwords**. The following page appears.

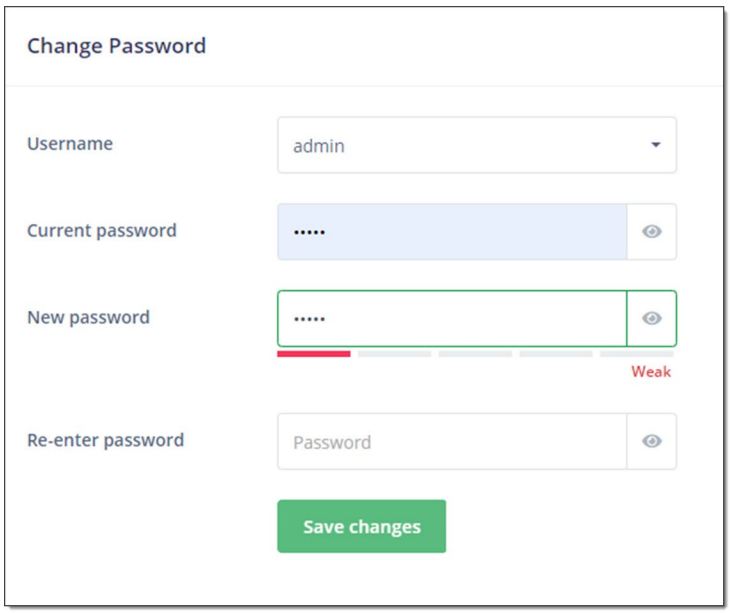


2. In the **Username** field, select the user password that you want to modify.
3. In the **Current password** field, either enter the current password for the selected user, or click in the field to select a stored password.

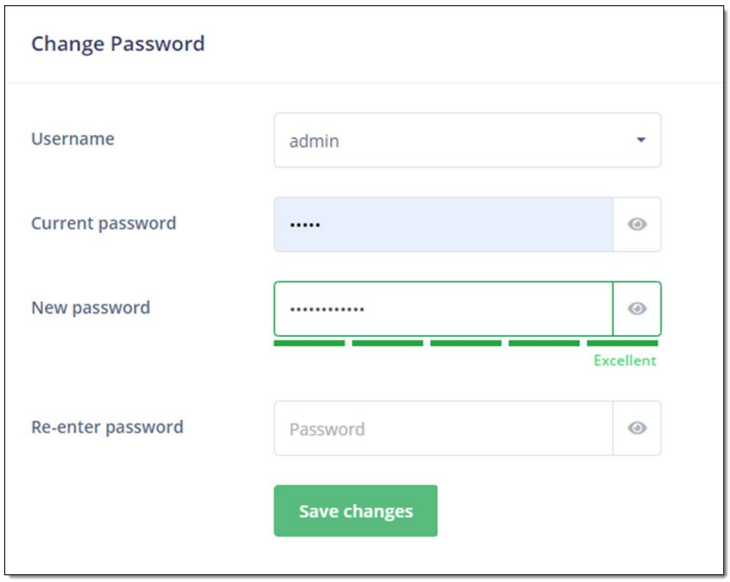
   Note: If you click the **Manage passwords** link in the Sign In dialog box, the Settings window opens for your browser. You can change passwords there as well.

4. In the **New password** and **Re-enter password** fields, enter the new password.
   The password strength rating located below each of these fields refreshes automatically as each character is typed.

   Weak password example



Strong password example

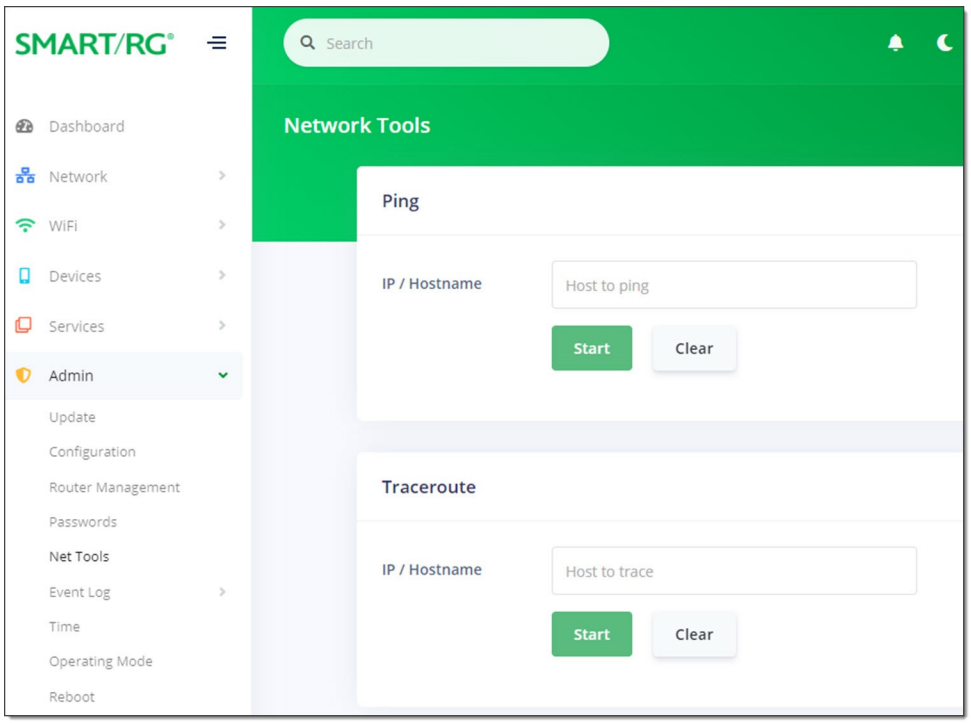


5. Click **Save Changes**. The new password takes effect immediately.

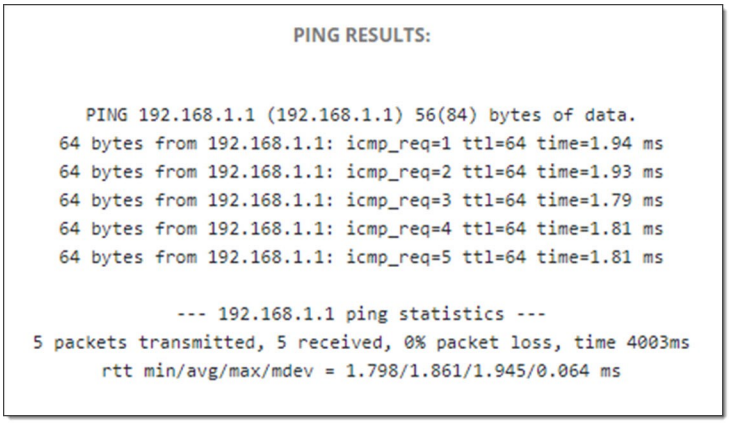
Net Tools

On this page, you can ping a server and use the traceroute utility to display a packet's path over the IP network and measure route transit delays that may be present.

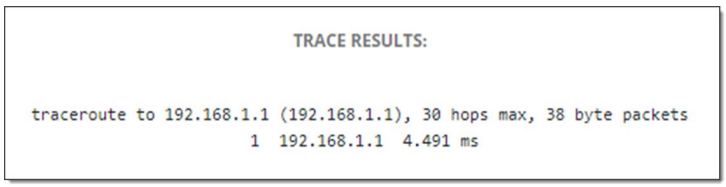
1. In the left menu, click **Admin** > **Net Tools**. The following page appears.



2. To ping a server, in the **Ping** section:
   a. Enter an IP address or host name in the **IP/Hostname** field (such as 192.168.1.44).
   b. Click the **Start** button in this section. The **PING RESULTS** appear.



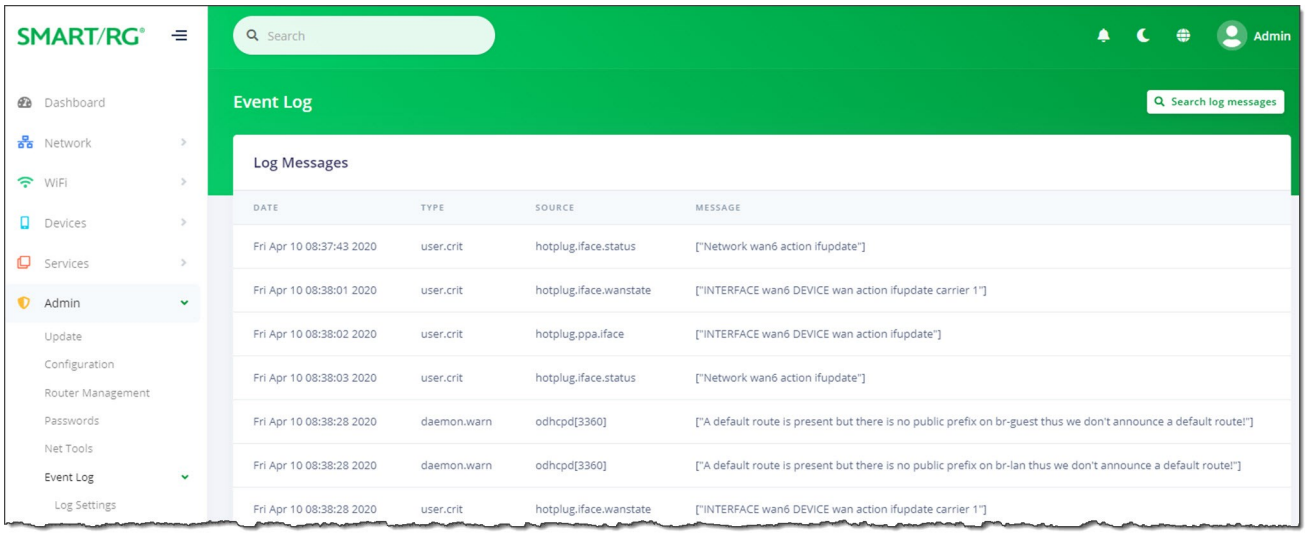
3. To trace a transmission, in the **Traceroute** section:
    a. Enter an IP address or host name in the **IP/Hostname** field (such as 192.168.1.44).
    b. Click the **Start** button in this section. The **TRACE RESULTS** appear.



Event Log

On this page, you can view the event log (system log) and configure how the log entries are displayed.

1. In the left menu, click **Admin** > **Event Log**. The following page appears.



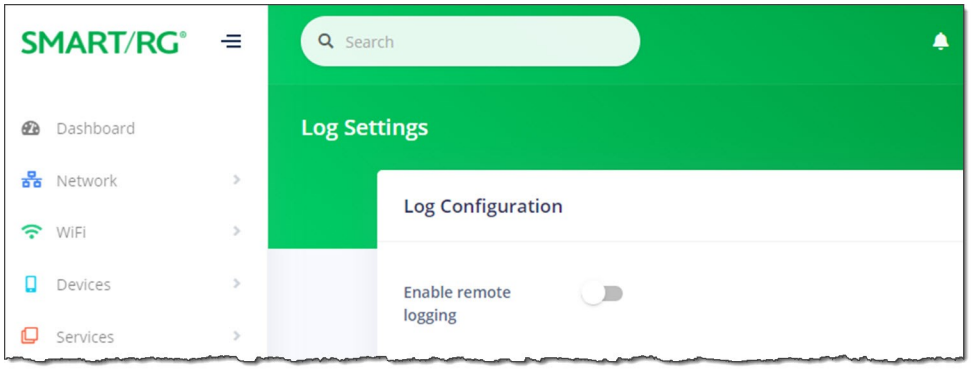
2. To filter the displayed messages:
    a. Click the **Search log messages** button at top right. The Search log messages dialog box appears.
    b. Enter a search string and click **Search**. The list refreshes to show the matching entries. The **Clear search** button appears next to the **Search log messages** button.
3. To clear the current filter, click the **Clear search** button at the top right.
4. To configure log settings, follow the "Configuring Log Settings" instructions below.

As new entries are added to the event log file, the list refreshes to display them.

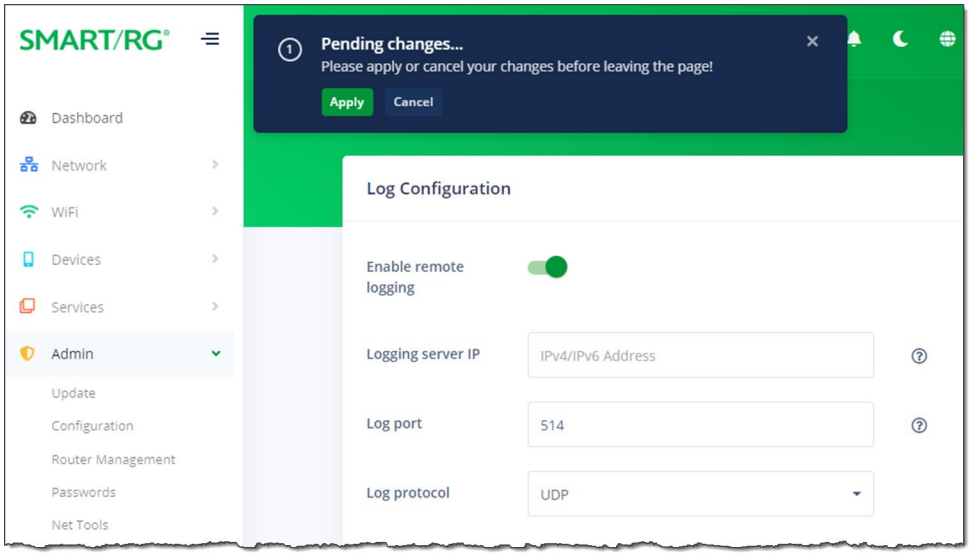
Configuring Log Settings

On this page, you can enable remote logging.

1. In the left menu, click **Admin** > **Event Log** > **Log Settings**. The following page appears.



2. (*Optional*) To activate remote logging, click the **slide button** next to **Enable remote logging**. Additional fields appear.

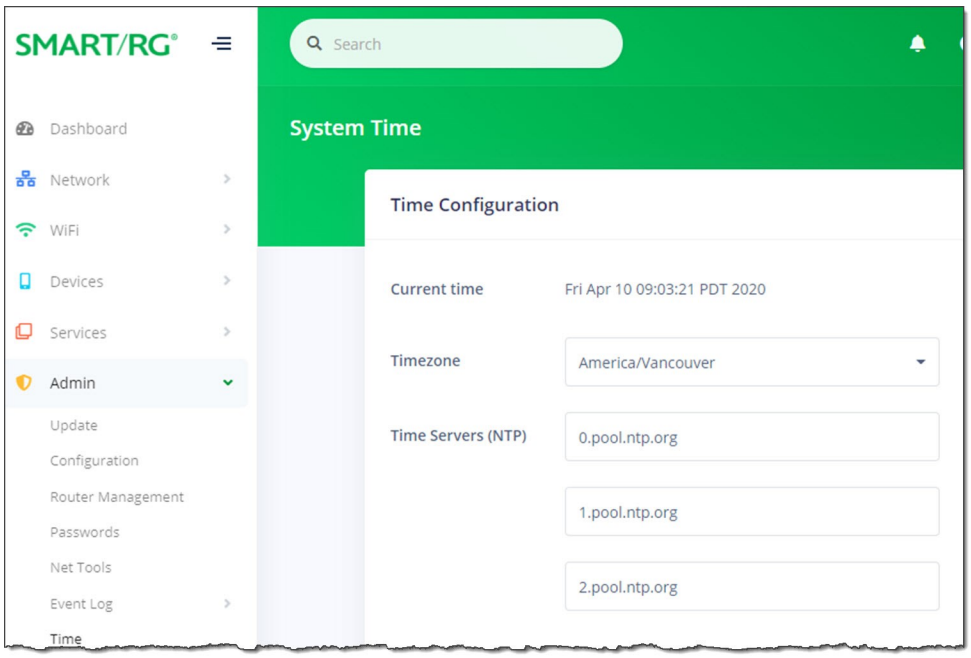


3. In the **Logging server IP** field, enter the IP address (such as 192.168.1.44) of the syslog server to which the log messages should be sent. Log messages are sent to this server in addition to the default local destination.
4. In the **Log port** field, enter or select the port number for the specified logging server. Options are **1** - **9999**. The default is **514**.
5. In the **Log protocol** field, select the protocol to be used for logging. Options are **TCP** and **UDP**. The default is **UDP**.
6. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Time

On this page, you can select a timezone and manage connections to the reliable clocking servers available on the Internet.

1. In the left menu, click **Admin** >**Time**. The following page appears. All fields on this page are optional.

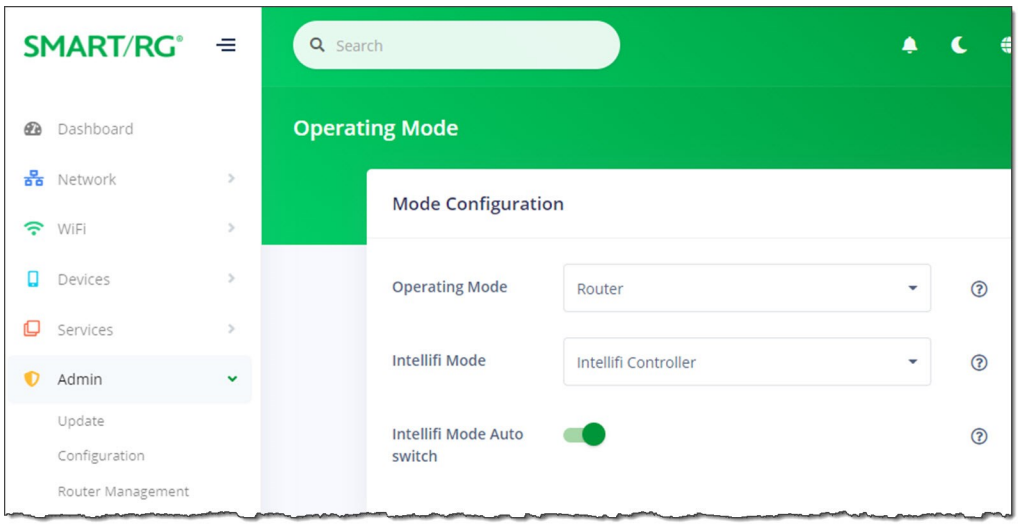


2. To change the time zone, in the **Timezone** field, select the appropriate zone.
3. To change or remove time servers, in the **Time servers (NTP)** section, modify or delete the addresses in the fields.
4. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Operating Mode

On this page, you can select whether the gateway operates as a router or a wireless access point.

1. In the left menu, click **Admin** > **Operating Mode**. The following page appears.



2. To configure how this gateway should operate, in the **Operating Mode** field, select the appropriate setting. Options are **Router** and **Wireless Access Point**. The default is **Router**.

   In **Router** mode, this device functions as a router between your ISP's WAN and your home network LAN. It provides firewall, NAT server, DHCP server, UPnP, DDNS, Cloud File Sharing and other services. Select this option if you do not currently have a router.

   Warning: When you change this setting, a Warning message appears, stating that the gateway will reboot upon applying this setting.

3. To configure this gateway as part of a mesh network, in the **Intellifi Mode** field, select the appropriate setting. Options are **None**, **Intellifi Controller** and **Satellite**. **Satellite** is only available when you select **Wireless Access Point** in the **Operating Mode** field. The default setting is **Intellifi Controller**.

   In **Intellifi Controller** mode, this device also becomes the central control center for your Intellifi network. Select this option if you are deploying Intellifi mesh nodes to support WiFi coverage at this location.

4. The **Intellifi Mode Auto switch** feature is *enabled* by default. To *prevent* the gateway from automatically switching from the Intellifi Controller mode to the managed Satellite mode, click the **slide button**.

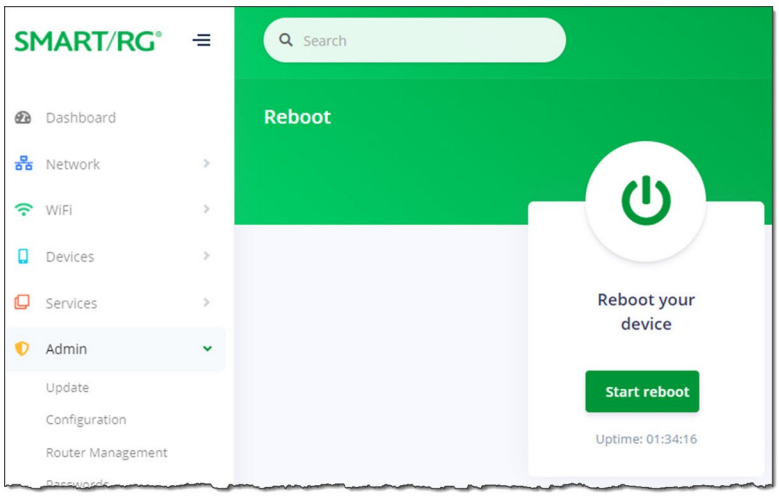
   To learn more about Intellifi network configuration, refer to the "How to set up an Intellifi mesh network (SR400ac)" How-To article available in the ADTRAN Support Community.

5. Click the **Apply** button in the **Pending changes...** dialog box to save your settings.

Reboot

On this page, you can reboot your device.

1. In the left menu, click **Admin** > **Reboot**. The following screen appears. The amount of time that the gateway has been connected is shown in the **Uptime** line below the **Start reboot** button.



2. Click the **Start reboot** button.
   The restart confirmation dialog box appears, stating that rebooting takes approximately three minutes.
3. Click the **Yes, reboot** button. The Rebooting dialog box appears, showing the time remaining until completion. When your gateway is ready, the sign-in page appears.

Logging out

1. In the top right corner of the interface, click the profile name. The USER PROFILE pane appears.
2. Click **Logout**. The Sign in dialog box appears.

Appendix: Compliance Statements

FCC Interference Statement

This device complies with Part 15 of the Federal Communications Commission (FCC) Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numrique de la classe B est conforme Ã la norme NMB-003 du Canada.

FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules.

- This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
- This equipment should be installed an operated with a minimum distance of 20cm between the radiator and your body.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution! Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

5GHz

5150-5250 MHz band is restricted to indoor operations only.

Revision History

Rev	Date	Description
2.2	January 2021	Updated to match SmartRG firmware release 10.8.8.1.
2.1	March 2020	Updated to match release 10.8.4.1.
2.0	January 2020	New screen captures and updated navigation paths reflect the GUI facelift for release 10.8.3.1. Related content was also updated.
1.1	June 2019	Updated to match release 10.7.1.1.
1.0	December 2018	Initial document release.