Adtran

Service Delivery Gateways (SDGs) Using SmartOS with 800 Series SDGs

User Manual

6SDGSOS800-29A

November 2022

To the Holder of this Document

The contents of this manual are current as of the date of publication. Adtran reserves the right to change the contents without prior notice.

Trademark Information

“Adtran” and the Adtran logo are registered trademarks of Adtran, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by Adtran’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with Adtran that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall Adtran be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.

Be advised that certain security risks are inherent in the use of any telecommunications or networking equipment, including but not limited to, toll fraud, Denial of Service (DoS) attacks, loss or theft of data, and the unauthorized or illegal use of said equipment. ADTRAN OFFERS NO WARRANTIES, EITHER EXPRESSED OR IMPLIED, REGARDING THE PREVENTION, DETECTION, OR DETERRENCE OF TOLL FRAUD, NETWORKING ATTACKS, OR UNAUTHORIZED, ILLEGAL, OR IMPROPER USE OF ADTRAN EQUIPMENT OR SOFTWARE. THEREFORE, ADTRAN IS NOT LIABLE FOR ANY LOSSES OR DAMAGES RESULTING FROM SUCH FRAUD, ATTACK, OR IMPROPER USE, INCLUDING, BUT NOT LIMITED TO, HUMAN AND DATA PRIVACY, INTELLECTUAL PROPERTY, MATERIAL ASSETS, FINANCIAL RESOURCES, LABOR AND LEGAL COSTS. Ultimately, the responsibility for securing your telecommunication and networking equipment rests with you, and you are encouraged to review documentation regarding available security measures, their configuration and implementation, and to test such features as is necessary for your network.

901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
Phone: (256) 963-8000

Service and Warranty

Warranty information can be found online by visiting www.adtran.com/warranty-terms.

To contact Adtran, choose one of the following methods:

Department	Contact Information	
Customer Care	From within the U.S.: From outside the U.S.:	(888) 4Adtran ((888)-423-8726) +1 (256) 963-8716
Technical Support	Support Community: Product Support:	www.supportcommunity.adtran.com www.adtran.com/support
Training	Email: Adtran University:	training@adtran.com www.adtran.com/training
Sales	For pricing and availability:	1 (800) 827-0807

Document Revision History

Rev A	October 2022	Initial release

Table of Contents

1. Overview

This guide provides information on the installation and configuration of Adtran's SmartOS-based 800 Series Service Delivery Gateways (SDGs). Included in this guide are the steps and configurations necessary to access the device and perform initial set up, navigate the device dashboard, configure wired and Wi-Fi networks, configure various additional network services, and manage the system.

2. Hardware and Software Requirements and Limitations

The SmartOS configurations and features described in this guide are available on 800 Series SDGs running SmartOS 11.2.1.1 and later, as outlined in the *SDG Feature Matrix*, available online in Adtran's Support Community.

NOTE

If your SDG is deployed with PlumeOS firmware installed, refer to PlumeOS documentation available online in Adtran's support community. For hardware information regarding your SDG such as instructions for exterior buttons, ports, LED behavior and cabling diagrams, please refer to the Quick Start Guide associated with your specific model of SDG. This and other related documentation is available for download from the Adtran Support Community *site.*

3. Introduction to the 800 Series Device

First Time Setup

Out of the box, the local Graphical User Interface (GUI) in the SDG is not immediately available. The Quick Start procedure must first be followed.

QuickStart Procedure

The Quickstart menu can be accessed directly at http://192.168.1.1 or via a Smartphone camera. Use the camera to scan the QR code labeled **WiFi QuickStart** located on the back of the unit. You will be presented with a series of self guiding, self documenting steps to select from **Gateway** or **Access Point** mode, to configure the WiFi SSID and passphrase and also to create an account. The credentials you choose for the latter will be used going forward when accessing the SDGs local GUI (described in the next section).

Accessing the Device

To manually configure the SDG, access the browser-based Graphical User Interface (GUI).

1. Connect to the SDG per the instructions in the Quick Start Guide for your specific model. (Quick Start Guides are located in the *SDG Knowledge Base Article* section of the *Adtran Support Community*).
2. Configure your computer's network interface to acquire an IP address automatically using DHCP.
3. Open a web browser application on your PC and enter the SDG's default address: http://192.168.1.1 in the address bar. The sign-in page appears.

4. Enter the username (default username is **admin**) and password you specified during the **WiFi QuickStart** procedure (above).

> **NOTE**
>
> *If you have forgotten the password for this device, select **Forgot password?** and follow the on-screen instructions to reset the SDG to the factory defaults. See Reset the SDG to Factory Default Settings on page 85.*

5. Select **Sign In**. The **Dashboard** page appears, showing data about your system.

Logging out

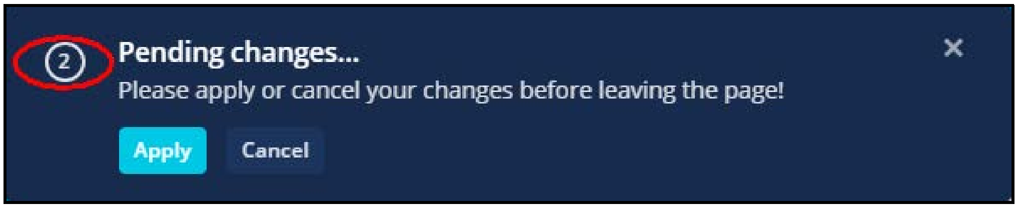
In the top right corner, select the profile name. The **USER PROFILE** drop-down list appears.

Select **Logout**. The **Sign in** dialog box appears

Saving Changes

When any settings are changed, the **Pending changes** dialog box appears at the top of the page. Changes made on the current page must be applied before navigating to a different page. Select **Apply** to apply all changes.

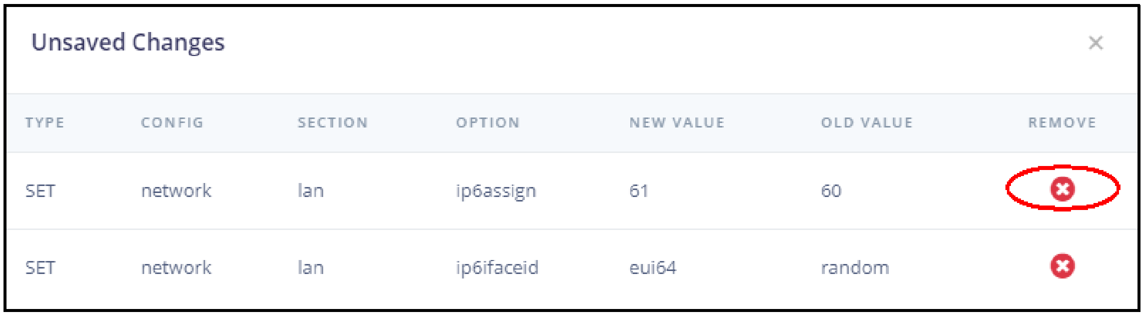
The circled number shown at left indicates the quantity of changes waiting to be applied. To view a list of your unsaved changes, select the circled number.



Pending changes...

Please apply or cancel your changes before leaving the page!

The **Unsaved Changes** pop-up window appears.



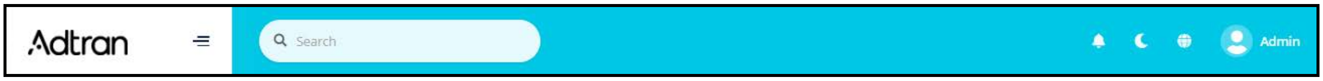
Unsaved Changes

TYPE	CONFIG	SECTION	OPTION	NEW VALUE	OLD VALUE	REMOVE
SET	network	lan	ip6assign	61	60	⊗
SET	network	lan	ip6ifaceid	eui64	random	⊗

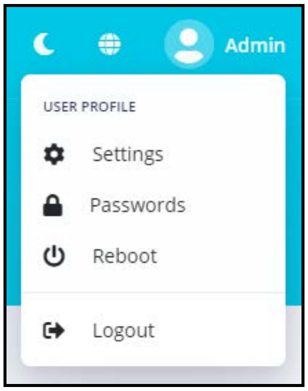
To undo a change in the list, select the red delete icon in the far right column for the line item to be canceled. If all of the changes are removed from the change list, the **Unsaved Changes** window closes and you can proceed to another page.

Setting User Preferences

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

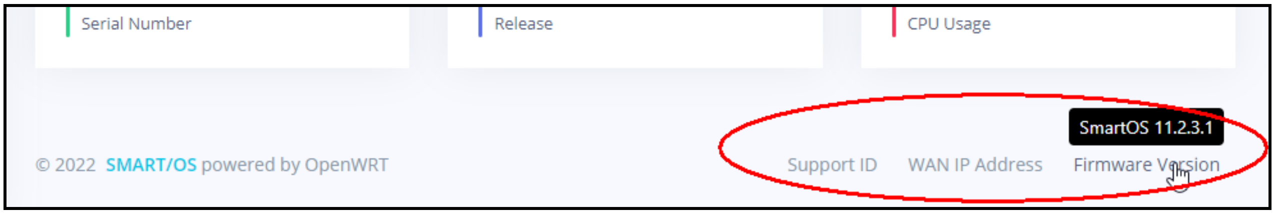


- Select the menu button (icon with 3 lines) next to the logo near the upper-left to minimize or expand the left navigation menu.
- Use the **Search** box to search for features in the GUI. The search returns a list of pages that match the terms entered. Select the feature/page from the list you want to view to link to jump to that feature.
- Select the notifications button (bell icon) to view notifications sent to the logged-in user account.
- Select the dark mode button (crescent moon icon) to engage an alternate color scheme for the GUI. The icon changes to the light mode (sunburst icon). Select the icon again to return to the original color scheme.
- Select the language button (globe icon) to choose your preferred interface language from the drop-down list that appears.
- The extreme upper-right corner of the screen displays the username currently logged in. Select the name to reveal a drop-down list of additional preferences described below.

 Admin USER PROFILE Settings Passwords Reboot Logout	The drop-down list of preferences shown when the currently logged in username is selected offers convenient links to the following features. ■ **Settings**: Save or load a router configuration file. See *Managing System Configurations on page 85*. ■ **Passwords**: Change passwords for SDG access. See *Managing System Passwords on page 87*. ■ **Reboot**: Initiate a reboot of the SDG. See *Rebooting the SDG on page 91*. ■ **Logout**: Ends the current session with the SDG.

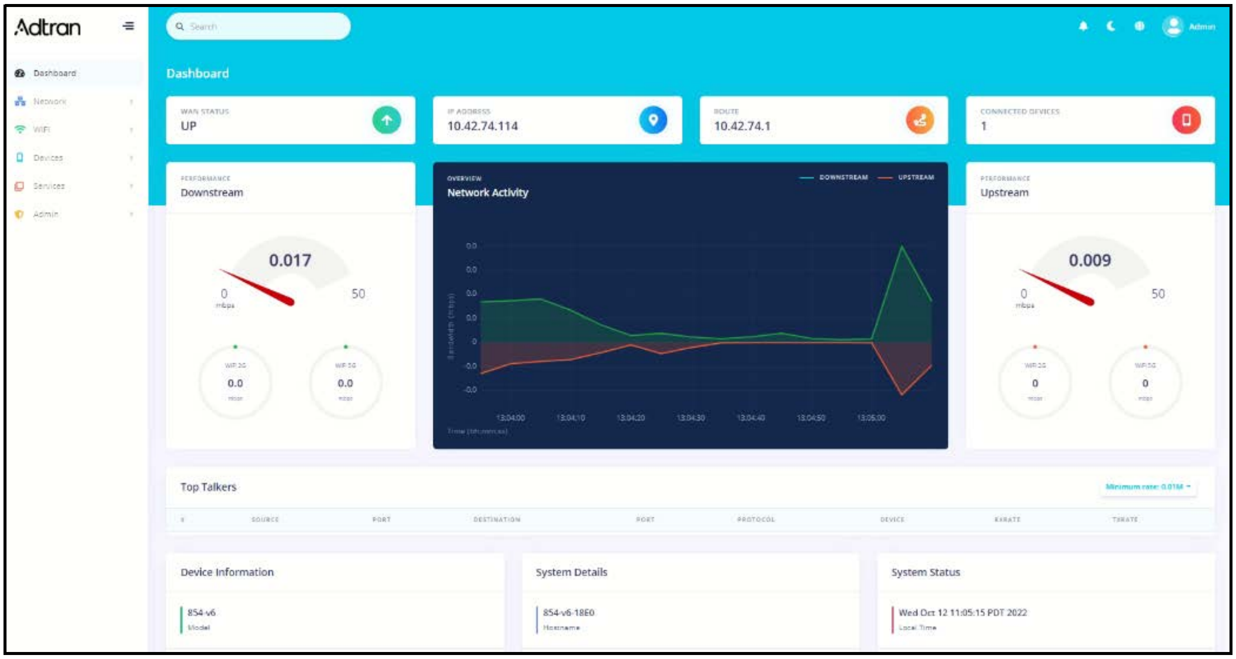
The page footer displays your **Support ID, WAN IP address,** and **Firmware Version**. Hover the cursor over these labels to view the details.

> **NOTE**
>
> *The **Support ID** only appears if the user has enabled Remote Support Diagnostics (**Admin > Support Diagnostics**) when logged in as the support user.*



4. Navigating the Dashboard

Upon successful login the **Dashboard** page appears (see image below).



WAN STATUS UP

IP ADDRESS 10.42.74.114

ROUTE 10.42.74.1

CONNECTED DEVICES 1

PERFORMANCE Downstream 0.017

PERFORMANCE Upstream 0.009

Top Talkers Minimum rate: 0.01M

#	SOURCE	PORT	DESTINATION	PORT	PROTOCOL	DEVICE	RXRATE	TXRATE

Device Information

854-v6
Model

System Details

854-v6-18E0
Hostname

System Status

Wed Oct 12 11:05:15 PDT 2022
Local Time

The central pane contains the **Dashboard** which contains real-time, critical statistics about the status of the device.

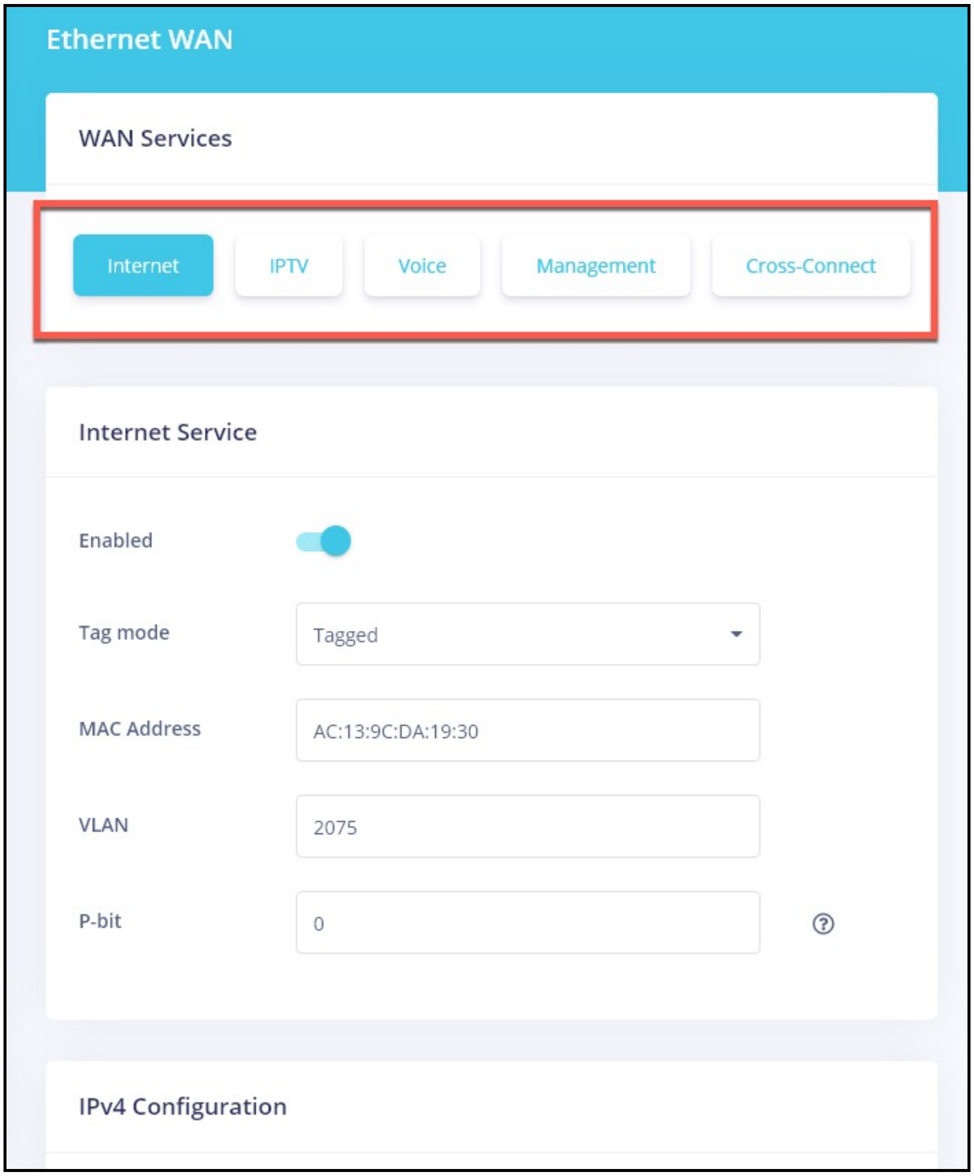
- **WAN STATUS**: Indicates whether the WAN (connection to the service provider) is **UP** or **Down**
- **IP ADDRESS**: Displays the WAN IP address as issued by the service provider to this device.
- **ROUTE**: Displays the default-gateway for this device.
- **CONNECTED DEVICES**: The number of Local Area Network (LAN) devices currently connected to the SDG.
- **Downstream** and **Upstream Performance**: Displays the current utilization of the circuit as seen by the SDG. Expressed as Megabits per second (Mbps)
- **Network Activity**: A time series chart showing real time bandwidth utilization. The blue line on the chart indicates downstream utilization. The red line on the chart indicates upstream utilization.
- **Top Talkers**: This table highlights the most active LAN devices on the network. This table can be sorted by selecting any of the column headers.
- The **Minimum rate** field appears at the top right of the **Top Talkers** frame. Select an option from this drop-down list to alter the threshold for which LAN devices are displayed in the **Top Talkers** table (described above). Optional selections for transmission rate include **None**, **0.01M**, **0.1M**, **1M**, **10M**, and **100M**. The default is **0.01M**
- **Device Information**: This block displays information about your Adtran device hardware-- The **Model** number of the SDG, the **MAC Address** and the **Serial Number**
- **System Details**: This block displays additional facts about the Adtran device hardware and software-- The **Hostname** for the SDG, the version of **Firmware** that is currently installed and the **Release**.
- **System Status**: This block shows the current date and time, the device **Uptime** -how long this SDG has been running, and the current **CPU Usage** for the SDGs processor (expressed as %).

- The left navigation bar contains a list of the SDGs features you can navigate to by expanding the categories and selecting the name of the feature you want. Each of these menu options is described in detail later in this manual. These sidebar options will navigate you away from the **Dashboard** to the selected feature.
- Return to the Dashboard by selecting **Dashboard** from the top of the left navigation bar.

5. Configuring Wired Networks

Information in this chapter includes a description of the controls and options for configuring wired network. This includes both Wide Area Network (WAN) settings as well as Local Area Network (LAN) controls for **Guest**, **Video**, **Multicast**, **Routing** and more.

To access the controls associated with configuring WAN settings, select **Network** > **Ethernet WAN** in the left menu. The following page appears defaulting the display to the first (**Internet**) tab.



Ethernet WAN

WAN Services

Internet Service

Enabled

Tag mode: Tagged

MAC Address: AC:13:9C:DA:19:30

VLAN: 2075

P-bit: 0

IPv4 Configuration

Select and configure the following WAN services by choosing the from the services listed across the top of the page.

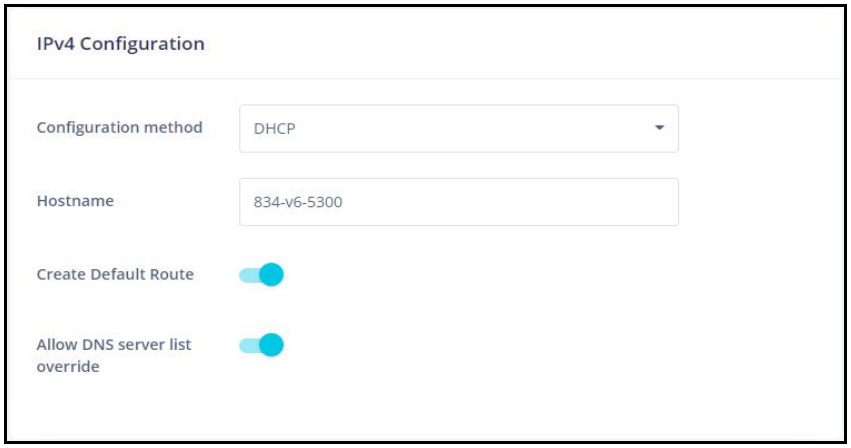
- *Internet*
- *IPTV*
- *Management*
- *Cross-Connect*

Internet

1. Select **Network** > **Ethernet WAN** in the left menu; the Ethernet WAN page appears, showing the Internet settings.
2. By default, the **Internet Service** is enabled. To disable the **Internet** feature, select the toggle next to **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 or select the ID of the appropriate VLAN. Valid values are **1** - **4079**. The default is **2**. Enter or select the P-bit type. Options are **0** - **7**. The default is **0**.
   c. If **DQTagged** is selected, the **CVID** field also appears. Enter or select the Customer VLAN ID (CVID) 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 field is set to your SDG's MAC address.
5. Complete the fields for the **IPv4 Configuration** and **IPv6 Configuration** sections as they apply to your environment, using the information provided below.
6. In the **Configuration method** field, select the appropriate method for your WAN.
   - Options for IPv4 WANs are **DHCP**, **Static Address**, **PPPoE** and **DS-Lite**. The default is **DHCP**.
   - Options for IPv6 WANs are **DHCPv6**, **Static Address**, and **None**. The default is **DHCPv6**.
7. Complete the remaining fields as instructed below for each option:
   - *DHCP for IPv4 WANs*
   - *Static Address for IPv4 WANs*
   - *PPPoE for IPv4 WANs (IPoE)*
   - *DS-Lite for IPv4 WANs*
   - *DHCPv6 for IPv6 WANs*
   - *Static Address for IPv6 WANs*
8. To enable the default route for this WAN, select the toggle to the right of **Create default route**.
9. To allow override of the DNS server list, select the toggle next to **Allow DNS server list ove**rride.
10. Select the **Apply** button in the **Pending change**s 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.



IPv4 Configuration

Configuration method: DHCP

Hostname: 834-v6-5300

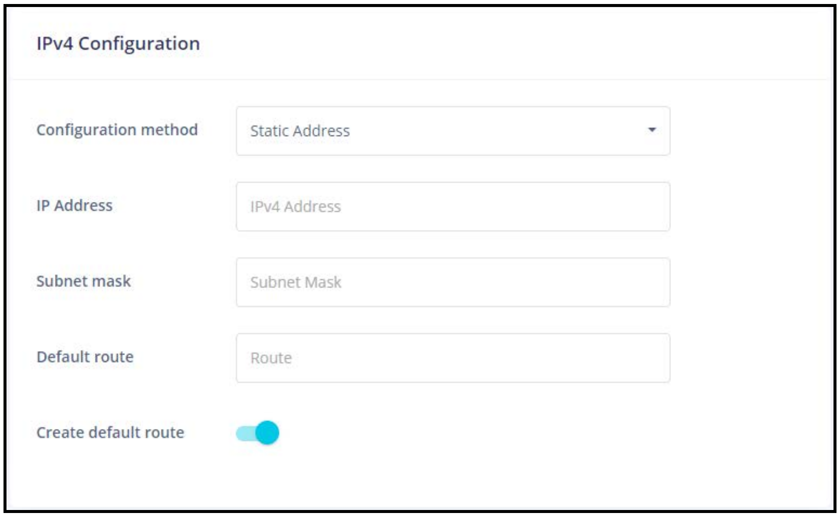
Create Default Route

Allow DNS server list override

1. To use a different host, enter the desired host name to be included in DHCP requests in the **Hostname** field.
2. Select 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.



IPv4 Configuration

Configuration method: Static Address

IP Address: IPv4 Address

Subnet mask: Subnet Mask

Default route: Route

Create default route

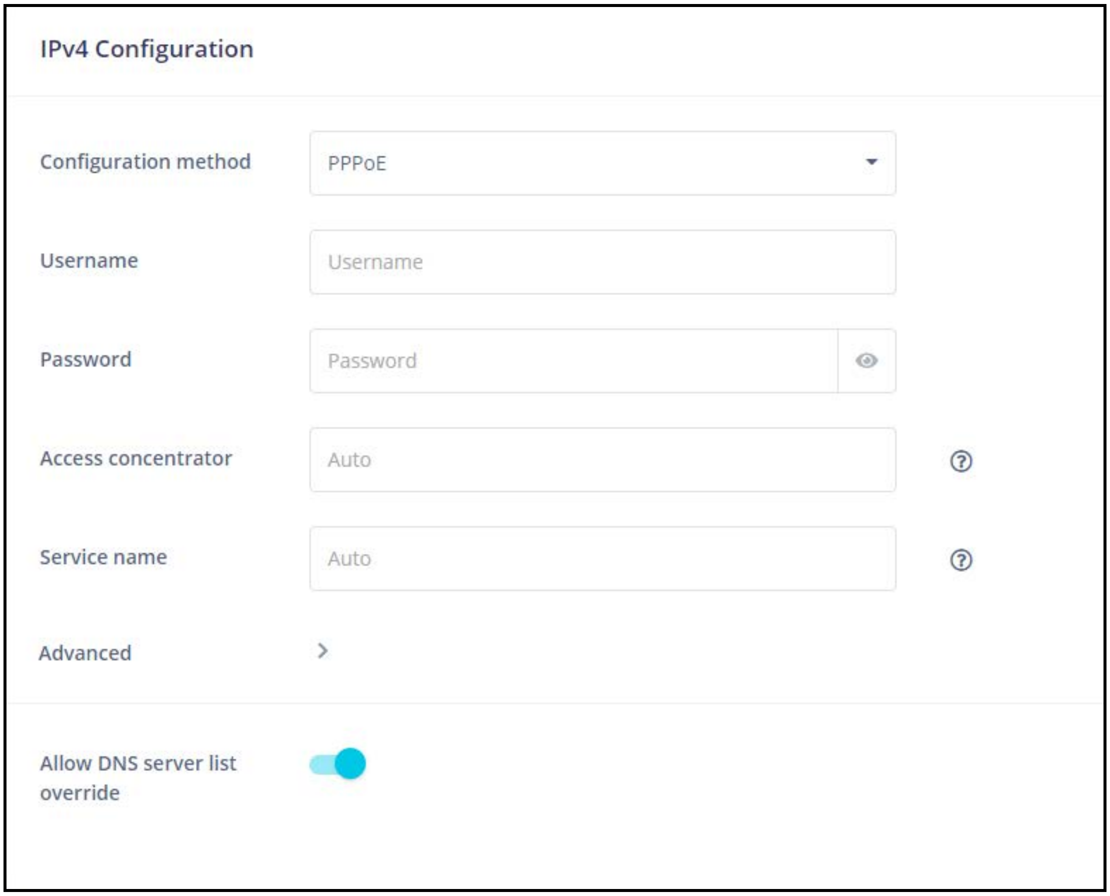
1. Complete the fields using the information in *Table 1*.
2. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Table 1. Static Address for IPv4

Field Name	Description
IP Address	Enter the IP address for IPv4 communications.
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.



IPv4 Configuration

Configuration method: PPPoE

Username: Username

Password: Password

Access concentrator: Auto

Service name: Auto

Advanced

Allow DNS server list override: ●

1. To access LCP and PPP settings, select the arrow next to **Advanced**.
2. Complete the fields using the information in *Table 2* and *Table 3*.
3. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Table 2. PPPoE for IPv4 WANs

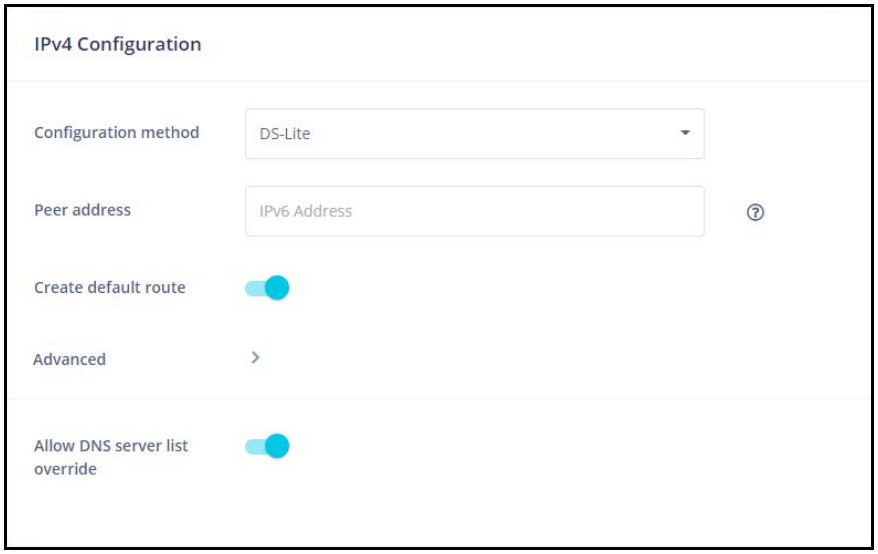
Field	Description
Username	Enter the PPP Username.
Password	Enter the PPP password. To view the password characters, select the show button (eye icon).
Access concentrator	Enter the name of the concentrator application. To have the system detect this automatically, accept the default of **Auto**.
Service name	Enter the name of the service for this interface. To have the system detect this automatically, accept the default of **Auto**.

Table 3. PPPoE for IPv4 WANs - Advanced

Field	Description
LCP Echo Interval	Enter the interval for sending echoes in seconds. Options are **None** and **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, select the toggle.
PPP Holdoff	Enter the number of seconds before attempting to reconnect a dropped call. The default is **zero** (**0**).

DS-Lite for IPv4 WANs

The following fields appear when **DS-Lite** is selected as the configuration method. DS-Lite is a tunneling technology that encapsulates IPv4 packets in IPv6 transports and delivers them to an IPv4 destination.



IPv4 Configuration

Configuration method: DS-Lite

Peer address: IPv6 Address

Create default route: on

Advanced

Allow DNS server list override: on

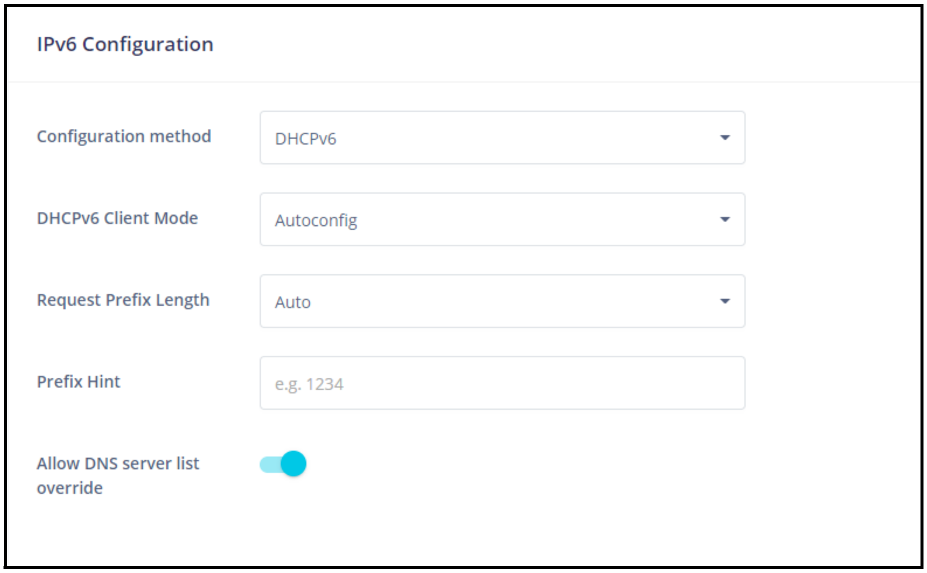
1. To access TTL and MTU settings, select the **arrow** next to **Advanced**.
2. Complete the fields using the information in *Table 4*.
3. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Table 4. DS-Lite for IPv4 WANs - Advanced

Field	Description
Peer Address	Enter the IPv6 address for the peer server.
TTL	Enter the Time to Live value for the packets being sent. This is the number of hops permitted before the packet is discarded. The default is **64**.
MTU	Enter the **MTU (Maximum Transmission Unit) size** for the network. Options are **0** through **2048**. The default is **1500**.

DHCPv6 for IPv6 WANs

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



IPv6 Configuration

Configuration method: DHCPv6

DHCPv6 Client Mode: Autoconfig

Request Prefix Length: Auto

Prefix Hint: e.g. 1234

Allow DNS server list override

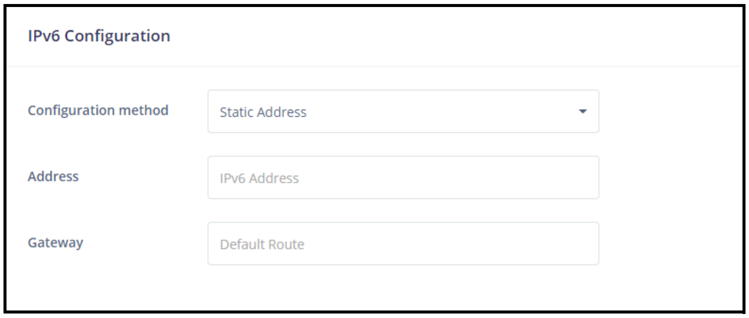
1. Complete the fields using the information in *Table 5*.
2. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Table 5. DHCP v6 for IPv6 WANs

Field Name	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. ■ **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**.
Prefix Hint	Enter the 4-digit hint for the subprefix ID.

Static Address for IPv6 WANs

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



IPv6 Configuration

Configuration method: Static Address

Address: IPv6 Address

Gateway: Default Route

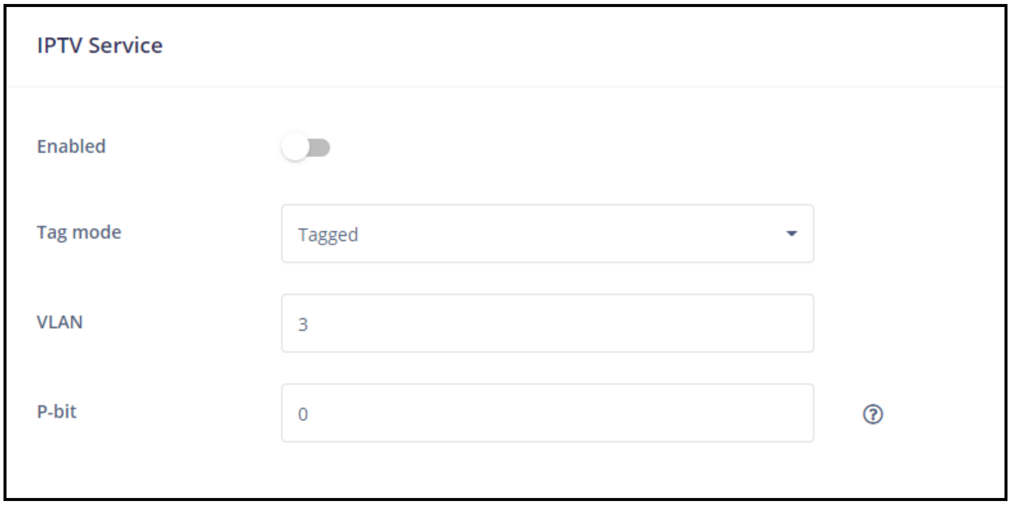
1. Complete the fields using the information in *Table 6*.
2. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Table 6. Static Address for IPv6 WANs

Field Name	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. The following page appears when you select the IPTV button:



IPTV Service

Enabled

Tag mode: Tagged

VLAN: 3

P-bit: 0

1. In the left menu, select **Network** > **Ethernet WAN**. The Ethernet WAN page appears showing the Internet settings.
2. Select the **IPTV** button.
3. To enable the IPTV feature, select the toggle 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 or select the ID of the appropriate VLAN. Valid values are **1** - **4079**. The default is **3**. Enter or select 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. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

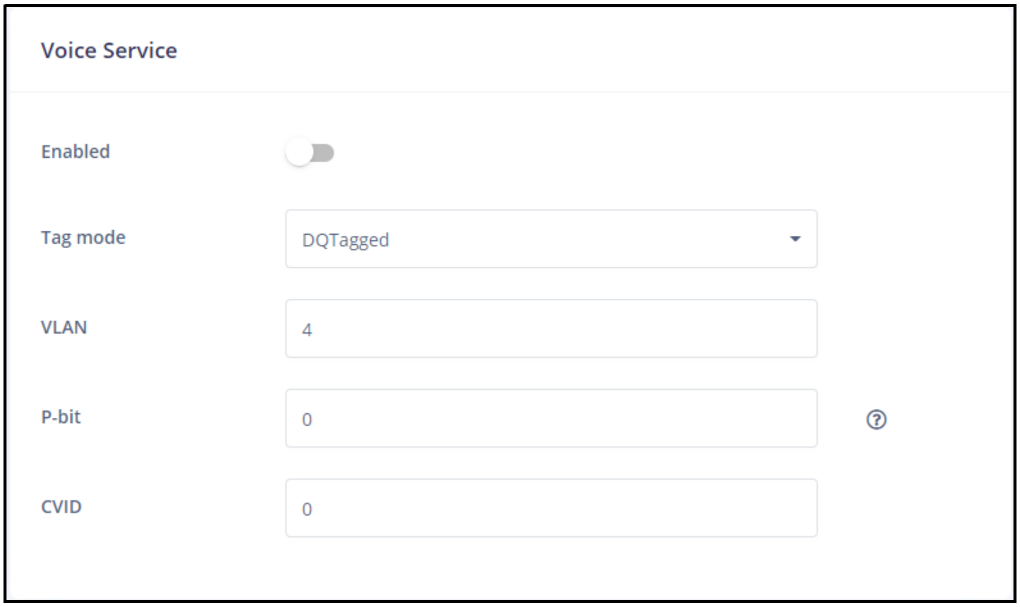
Voice

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

NOTE

This feature is supported only by VOIP-capable SDG models including the 834-v6 and 854-v6.

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



Voice Service

Enabled

Tag mode: DQTagged

VLAN: 4

P-bit: 0

CVID: 0

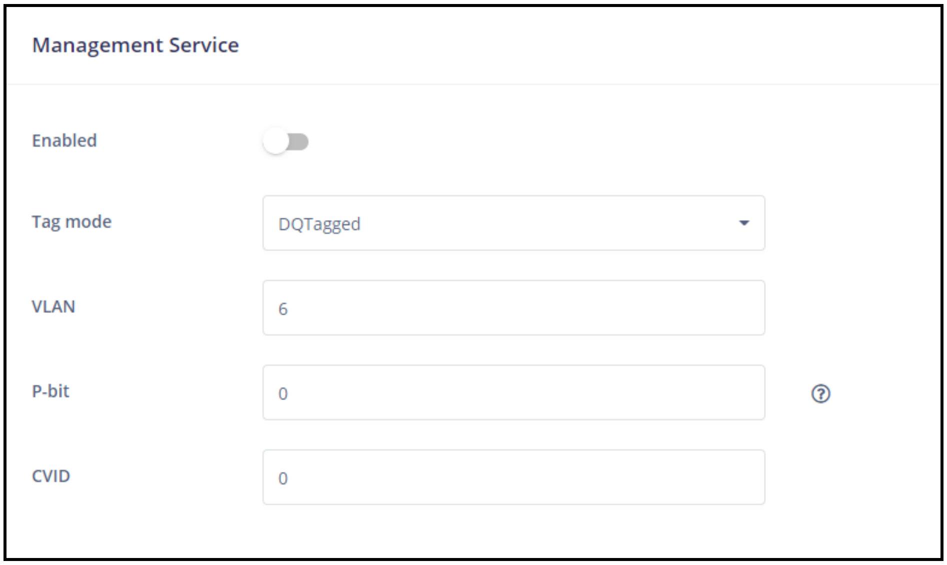
3. To enable the Voice feature, select the toggle to the right of **Enabled**.
4. Configure the tagging options:
    a. In the **Tag mode** field, select the type of tagging that should be performed. Options are **Untagged**, **Tagged** and **DQTagged**. The default is **Tagged**.
    b. If **Tagged** is selected, the **VLAN** and **P-bit** fields become available. Enter or select the ID of the appropriate VLAN. Valid values are **1** - **4079**. The default is **3**. Enter or select 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 (CVID) or the first in a range of CVIDs that will be accepted and mapped to the specified WAN. Valid values are **1** - **4062**. Default value is **1500**.
5. In the **IPv4 Configuration** section, configure the settings using the information in *DHCP for IPv4 WANs* and *Static Address 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*.

Select 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.The following page appears when you select the Management butto

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



Management Service

Enabled

Tag mode: DQTagged

VLAN: 6

P-bit: 0

CVID: 0

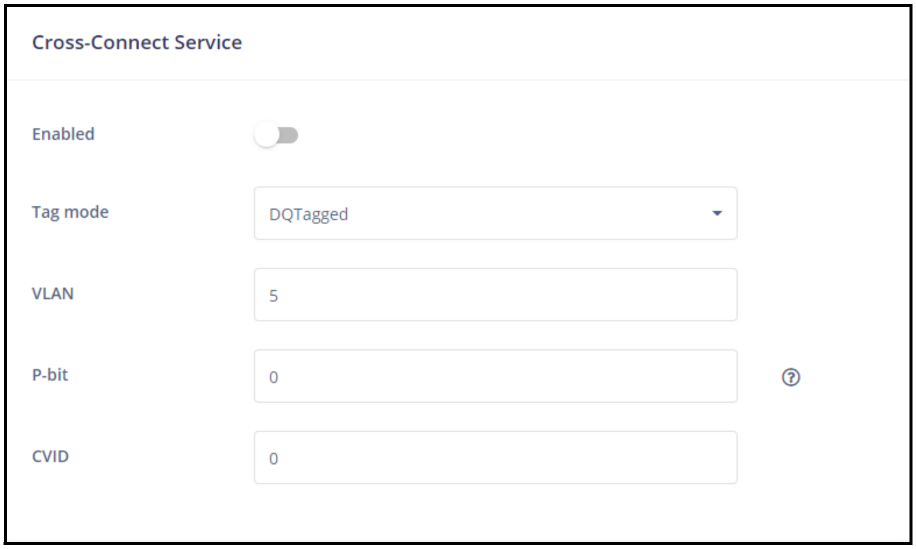
3. Configure the tagging options:
    a. In the **Tag mode** field, select the type of tagging that should be performed. Options are **Untagged**, **Tagged**, and **DQTagged**. The default is **Tagged**.
    b. If **Tagged** or **DQTagged** is selected, the **VLAN** and **P-bit** fields appear. Enter the ID of the appropriate VLAN. Valid values are **1** - **4079**. The default is **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 (CVID) 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. 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*.
5. In the **IPV6 Configuration** section, configure the settings using the information in *DHCPv6 for IPv6 WANs* or *Static Address for IPv6 WANs*.
6. Select 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, select **Network** > **Ethernet WAN**. The Ethernet WAN page appears showing the Internet settings.

2. Select the **Cross-Connect** button



Cross-Connect Service

Enabled

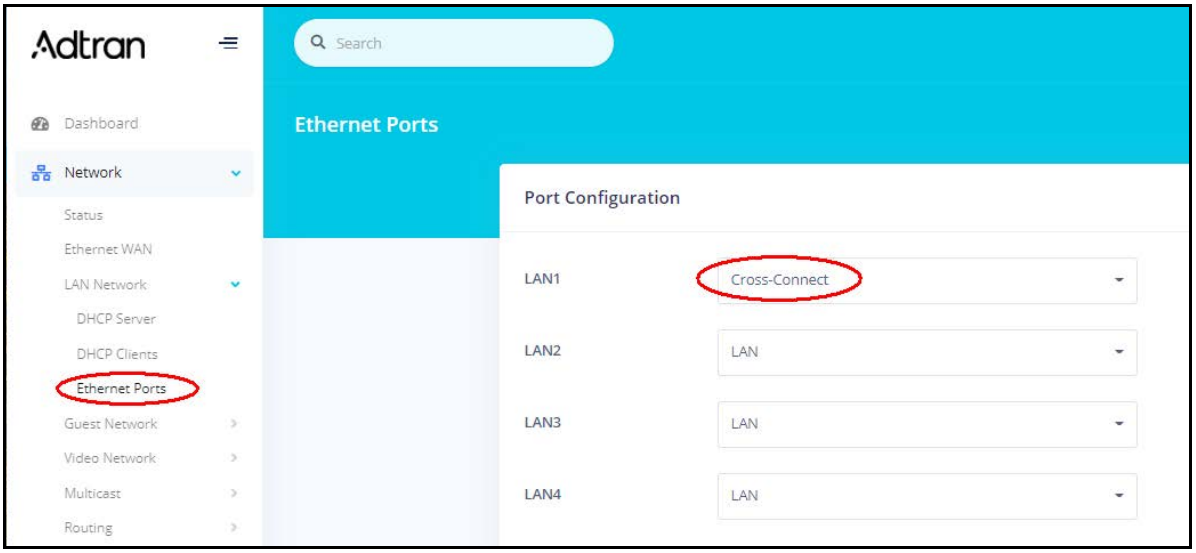
Tag mode: DQTagged

VLAN: 5

P-bit: 0

CVID: 0

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 **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 (CVID) 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. Select the **Apply** button in the **Pending changes** dialog box to save your settings.
5. Complete the cross-connect by selecting the Ethernet LAN port that will be used for the cross-connect service. **Navigate to Network > LAN Network > Ethernet Ports** and select **Cross-Connect** beside the LAN port that will be used.



Port Configuration

LAN1: Cross-Connect

LAN2: LAN

LAN3: LAN

LAN4: LAN

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

LAN Network Setup

Information in this section includes a description for configuration of:

Basic IPv4 LAN settings on page 19

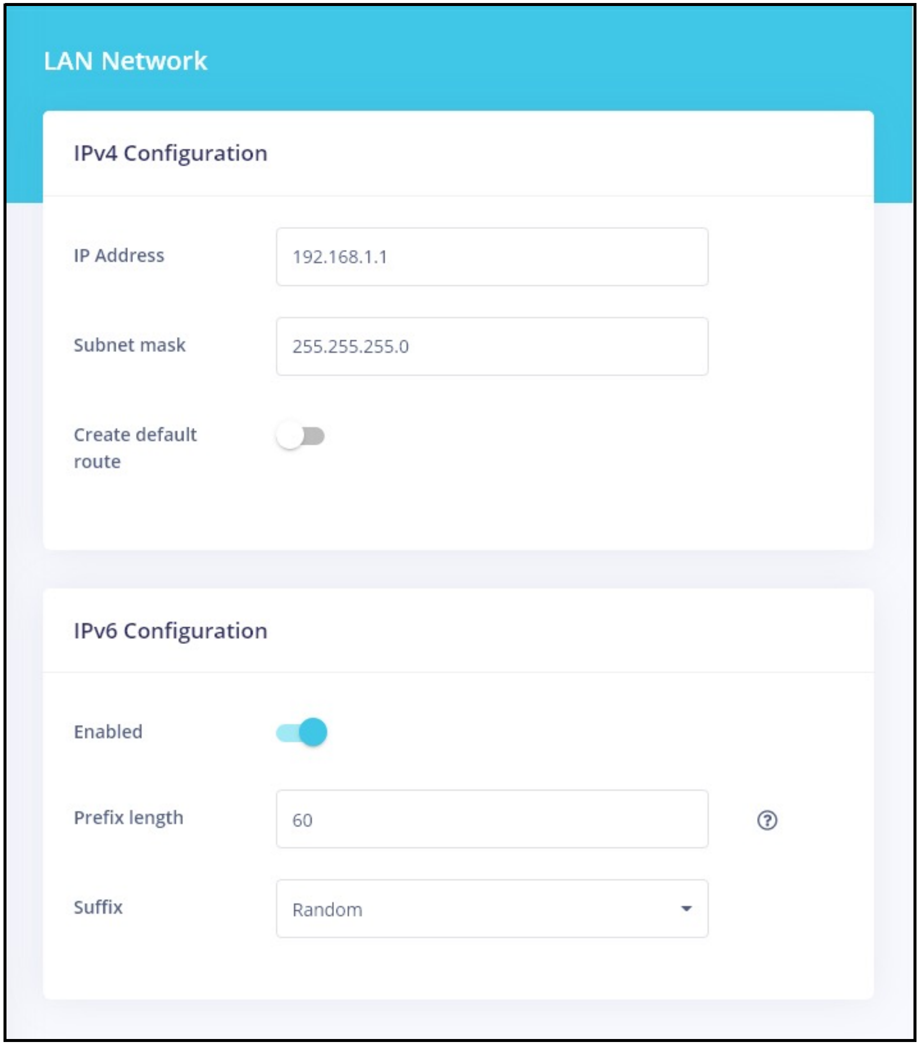
DHCP Server on page 21

DHCP Clients on page 23

Ethernet Ports on page 24

Basic IPv4 LAN settings

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



LAN Network

IPv4 Configuration

IP Address: 192.168.1.1

Subnet mask: 255.255.255.0

Create default route: ○ (off)

IPv6 Configuration

Enabled: ● (on)

Prefix length: 60

Suffix: Random

2. Fill in the fields using the information in *Table 7* and *Table 8*.

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

Table 7. IPv4 Configuration

Field	Description
IP Address	Enter the IP address for IPv4 communications. The default is t192.168.1.1.
Subnet mask	Enter the IP subnet mask for this SDG. The default is **255.255.255.0**.
Create default route	(Optional) To create the default route for this LAN, select the toggle.

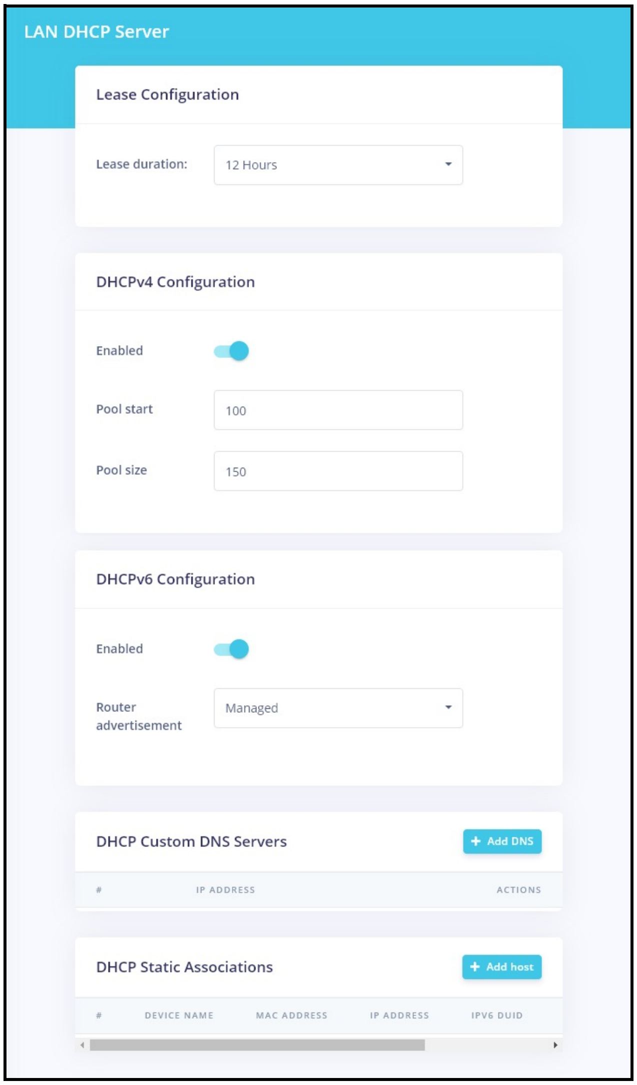
Table 8. IPv6 Configuration

Field	Description
Enabled	This option is disabled by default. To enable IPv6 address configuration, select the toggle to the right of **Enabled**. The **Prefix length** and **Suffix** fields appear.
Prefix length	Enter the prefix length for this IPv6 address. 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, configure the DHCP settings for the SDG. The Dynamic Host Control Protocol Server (DHCP) feature of this SDG will automatically assign LAN IP addresses to host devices as they connect.

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



LAN DHCP Server

Lease Configuration

Lease duration: 12 Hours

DHCPv4 Configuration

Enabled

Pool start 100

Pool size 150

DHCPv6 Configuration

Enabled

Router advertisement Managed

DHCP Custom DNS Servers

#	IP ADDRESS	ACTIONS

DHCP Static Associations

#	DEVICE NAME	MAC ADDRESS	IP ADDRESS	IPV6 DUID

2. Fill in the fields using the information in *Table 9*.
3. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Table 9. LAN DHCP Server Configuration

Field	Description
Lease duration	Select the amount of time for which an IP address will be leased. Options range from **5 minutes** to **24 hours**. The default is **12 hours**.
	DHCPv4 Configuration
Enabled	This feature is enabled by default. To disable this feature, select the toggle.
Pool start	Enter the beginning of the class-C IP address range to be assigned by the DHCP server. The default is **100**.

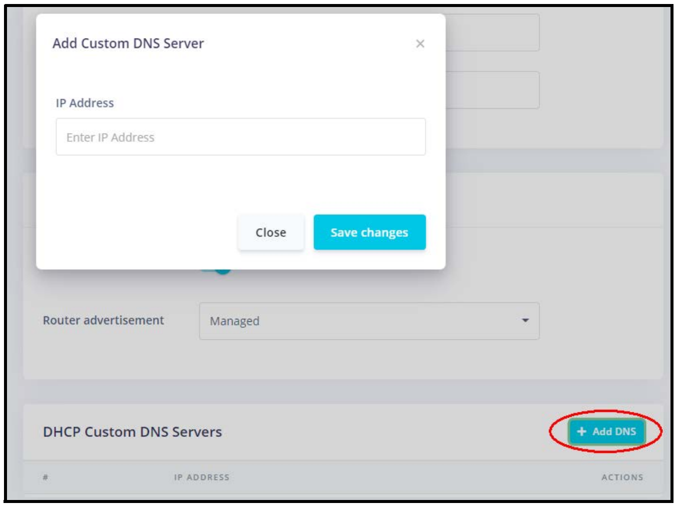
Table 9. LAN DHCP Server Configuration (Continued)

Field	Description
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, select the toggle.
Router advertisement	Select how this SDG will be advertised through this DHCPv6 server. Options are: ■ **Assisted**: Advertises this SDG with all configuration, with stateless auto-configuration, or both. ■ **Managed**: Advertises this SDG with all configuration. This is the default. ■ **Unmanaged**: Advertises this SDG with only stateless auto-configuration.
DNS and Static Associations	
Custom DNS Servers	(Optional) To define a custom 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 Association*.

Defining a Custom DNS Server

Defining custom DNS server(s) is an optional step.

1. To define a custom DNS server, select **Add DNS** to the right of the **DHCP Custom DNS Servers** section heading. The **Add Custom DNS Server** dialog box appears.



Add Custom DNS Server

IP Address: Enter IP Address

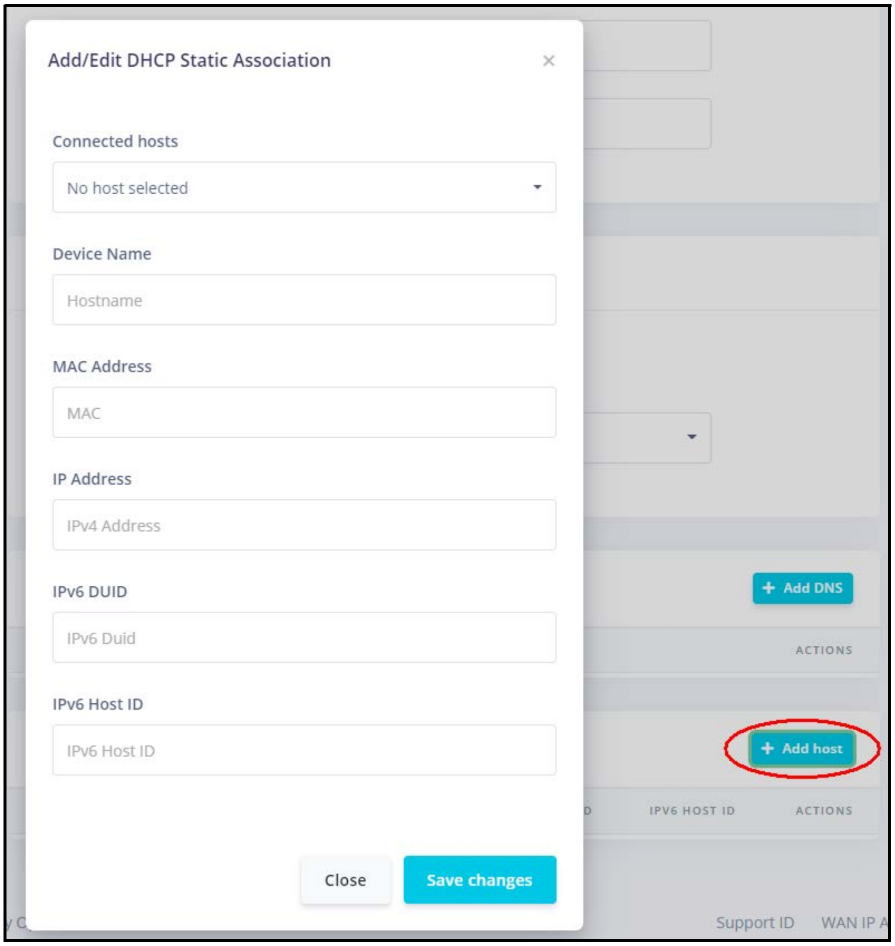
Router advertisement: Managed

2. Enter the IP address of the host device.
3. Select **Save changes** to commit your changes.
4. To add another DNS server, repeat Steps 1-3.
5. To remove a custom server IP address, select the red delete button.

Defining a Static DHCP Association

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

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

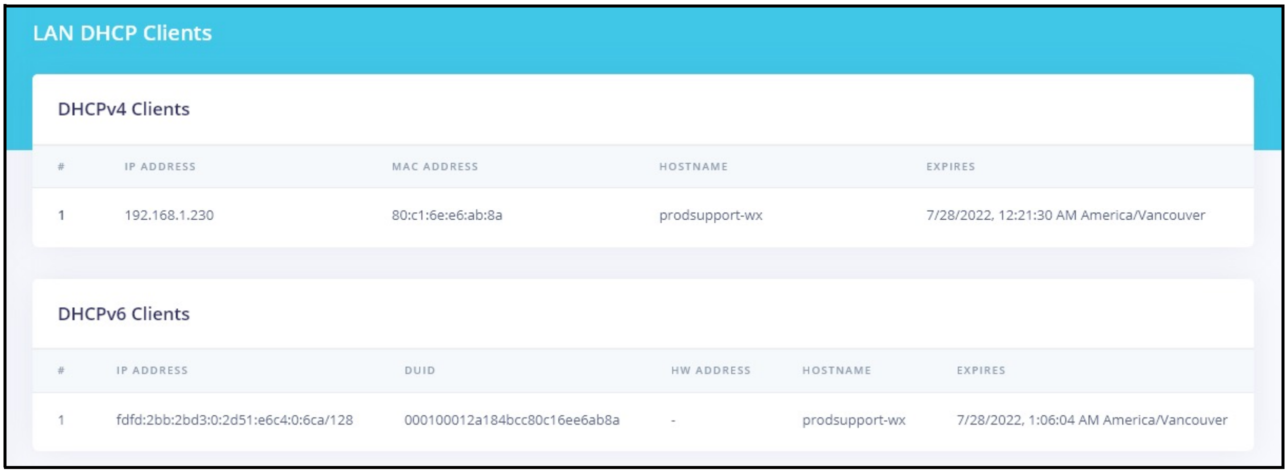


2. In the **Connected Hosts** field, select the host server to use as a static host. When a connected host is selected, the other fields in the dialog box are populated with the related information. If the host is currently offline or the **None** option is chosen, the information must be entered manually.
3. Select **Save changes** to commit your changes.
4. To add another static DHCP configuration, repeat Steps 1-3.
5. To edit a static DHCP IP address, select the blue adjacent edit button. The **Add/Edit** dialog box appears. Change the entries as needed and select **Save Changes** to commit your changes.
6. To remove a static DHCP IP address, select the red delete button.
7. Select 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, select **Network** > **LAN Network** > **DHCP Clients**. The following page appears.



LAN DHCP Clients

DHCPv4 Clients

#	IP ADDRESS	MAC ADDRESS	HOSTNAME	EXPIRES
1	192.168.1.230	80:c1:6e:e6:ab:8a	prodsupport-wx	7/28/2022, 12:21:30 AM America/Vancouver

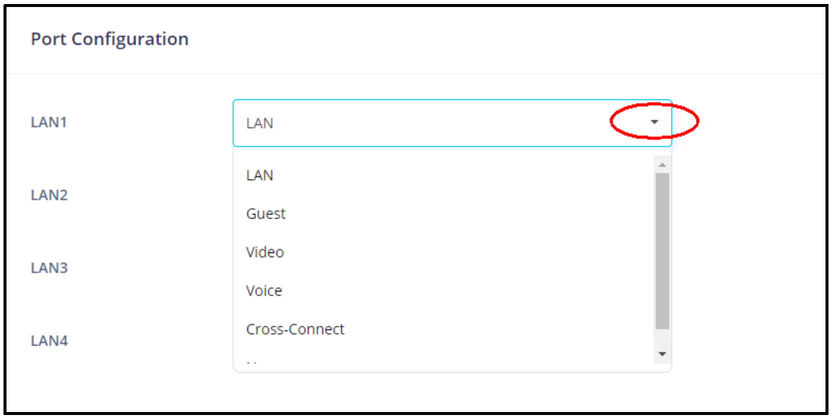
DHCPv6 Clients

#	IP ADDRESS	DUID	HW ADDRESS	HOSTNAME	EXPIRES
1	fdfd:2bb:2bd3:0:2d51:e6c4:0:6ca/128	000100012a184bcc80c16ee6ab8a	-	prodsupport-wx	7/28/2022, 1:06:04 AM America/Vancouver

Ethernet Ports

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

1. In the left menu, select **Network** > **LAN Network** > **Ethernet Ports**.



Port Configuration

LAN1: LAN

LAN2

LAN3

LAN4

2. Select an option for each LAN port where a particular service is to be defined. Available options are **LAN**, **Guest**, **Video**, **Voice**, **Cross-Connect,** and **None**. The default is **LAN**.

NOTE

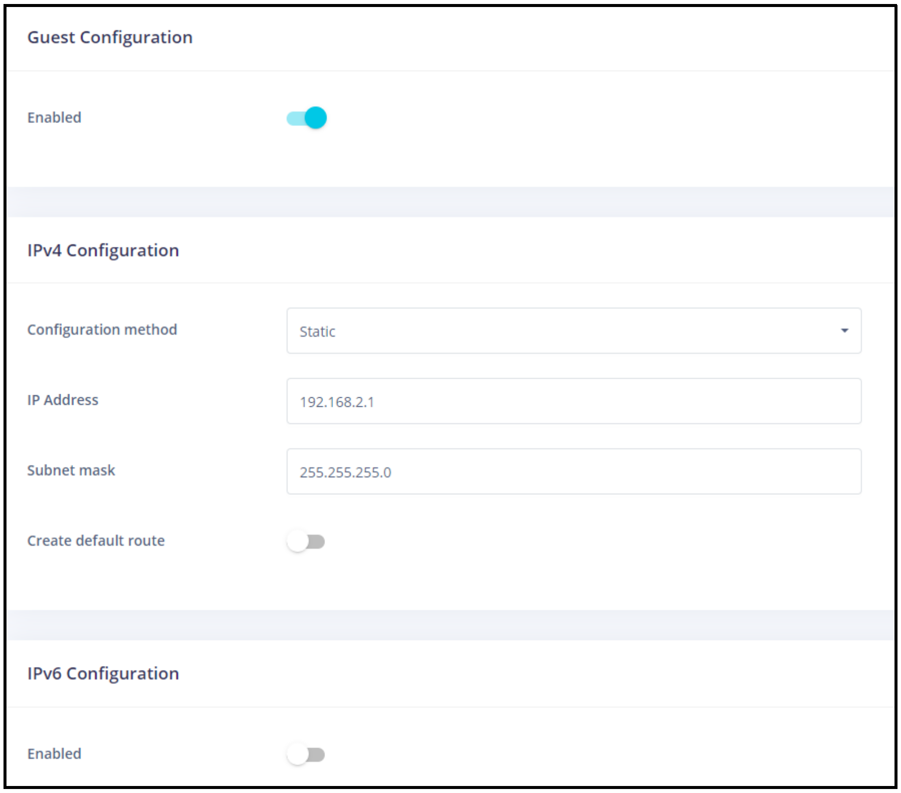
If Cross-Connect is selected, the cross connect service will need to be enabled on the WAN as shown in Cross-Connect on page 17.

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

Guest Network

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

1. In the left menu, select **Network** > **Guest Network**. This feature is enabled by default.



Guest Configuration

Enabled ●

IPv4 Configuration

Configuration method: Static

IP Address: 192.168.2.1

Subnet mask: 255.255.255.0

Create default route ○

IPv6 Configuration

Enabled ○

2. To disable the guest network feature, select the toggle next to **Enabled**.
3. Fill in the fields using the information in *Table 10*.
4. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Table 10. Guest Network Settings

Field	Description
	IPv4 Configuration
Configuration method	Select the appropriate method for your WAN. The page refreshes to show the fields that apply for the selected method. Options are **Static**, **DHCP**, and **None**. The default is **Static**.
	Static Configuration Method
IP Address	Enter the IP address for IPv4 communications. The default IP address is 192.168.2.1.
Subnet mask	Enter the IP subnet mask for this SDG. The default is **255.255.255.0**.
Create default route	To create a default route for this LAN, select the toggle.
	DHCP Configuration Method
Hostname	Enter the host name to be included in DHCP requests.
	IPv6 Configuration Method

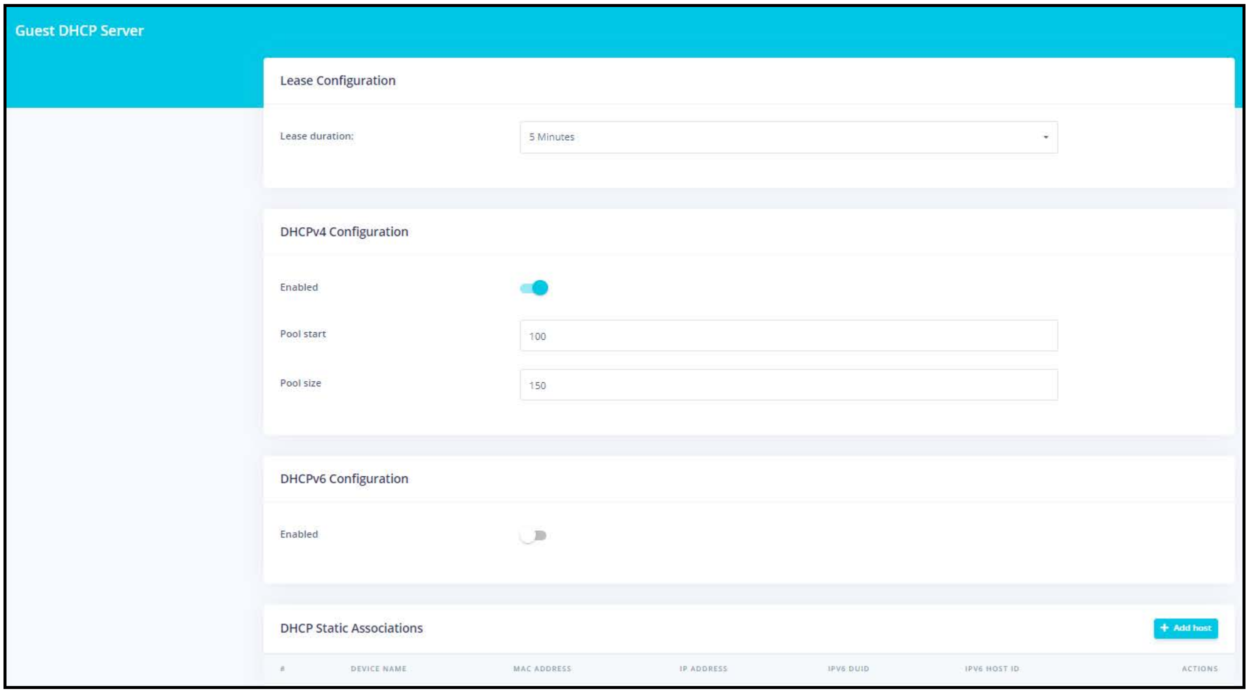
Table 10. Guest Network Settings (Continued)

Field	Description
Enabled	This feature is disabled by default. To enable IPv6 address configuration, select the toggle.
Prefix length	Enter the prefix length for this IPv6 address. Options are **0** - **64**.
Suffix	Select the interface identifier for this IPv6 address. Options are **Random**, **MAC Based**, and **Suffix Address**. The default is **Random**. When you select **Suffix Address**, the **Suffix Address** field appears. Enter the address in format: "::a:b:c:d".

Guest DHCP Server

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

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



Guest DHCP Server

Lease Configuration

Lease duration: 5 Minutes

DHCPv4 Configuration

Enabled

Pool start 100

Pool size 150

DHCPv6 Configuration

Enabled

DHCP Static Associations

2. Fill in the fields using the information in *Table 11*.
3. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Table 11. Guest Network DHCP Server Settings

Field	Description
Lease duration	Select the amount of time for which 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, select the toggle to the right of **Enabled**.
Pool start	Enter the beginning of the class-C IP address range to be assigned by the DHCP server. The default is **100**.

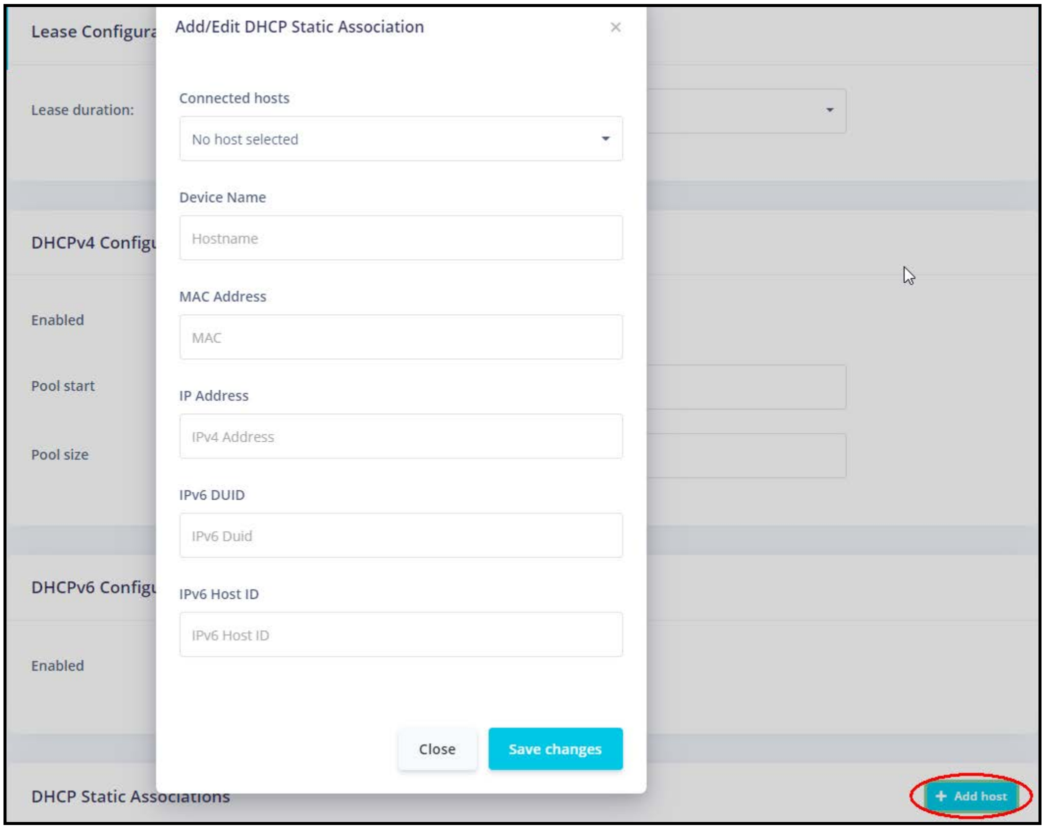
Table 11. Guest Network DHCP Server Settings (Continued)

Field	Description
Pool size	Enter the size of the DHCP pool. The maximum size allowed is 252. The default is **150**.
DHCPv6 Configuration	
Enabled	Select the toggle to enable this feature.
Router advertisement	Select how this SDG will be advertised through this DHCPv6 server. Options are: ■ **Assisted**: Advertises this SDG with all configuration, with stateless auto-configuration, or both. ■ **Managed**: Advertises this SDG with all configuration. This is the default. ■ **Unmanaged**: Advertises this SDG with only stateless auto-configuration.
DHCP Static Associations	
DHCP Static Associations	(Optional) To define a static DHCP server, follow the steps in *Defining a Static DHCP IP Address Association for a Guest Network Host on page 27*.

Defining a Static DHCP IP Address Association for a Guest Network Host

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

1. To select a LAN client device, select **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 a connected host is selected, the fields in the dialog box are populated with the necessary information. If the host is currently offline or the **None** option is chosen, the information must be entered manually.
3. Complete the fields, using the information in *Table 12*.
4. Select **Save changes** to commit your changes.

Table 12. Define a Static DHCP IP Address Association for a Guest Network Host

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. 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 server.

5. To add another static DHCP configuration, repeat Steps 1-4.
6. To edit a static DHCP IP address, select the blue edit button. The **Add/Edit** dialog box appears. Change the entries as needed and select **Save Changes** to commit your changes.
7. To remove a static DHCP IP address, select the red delete button.
8. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Guest DHCP Clients

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

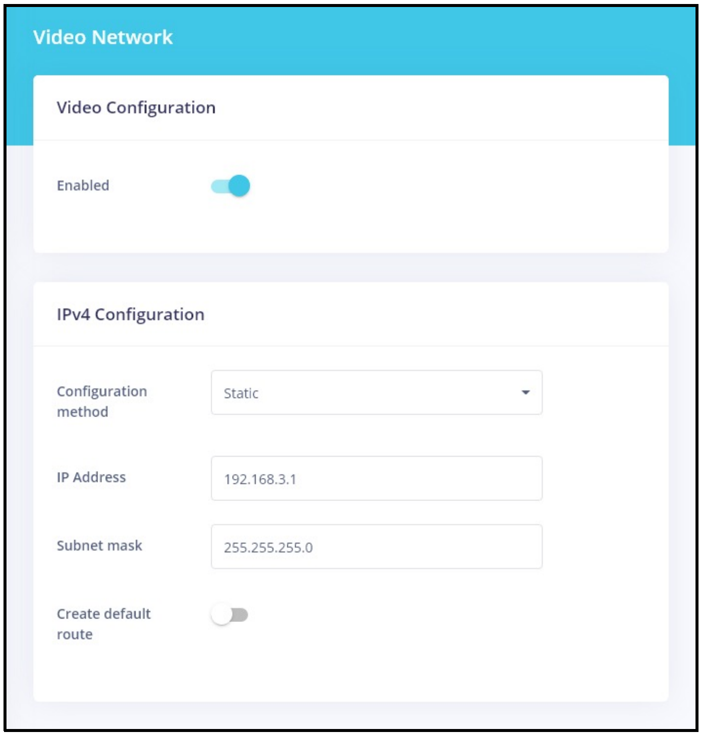
In the left menu, select **Network** > **Guest Network** > **DHCP Clients**. The subsequent page that appears displays two tables

The upper table lists active IPv4 LAN client devices. The lower table lists active IPv6 LAN client devices.

Video Network

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

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



Video Network

Video Configuration

Enabled

IPv4 Configuration

Configuration method: Static

IP Address: 192.168.3.1

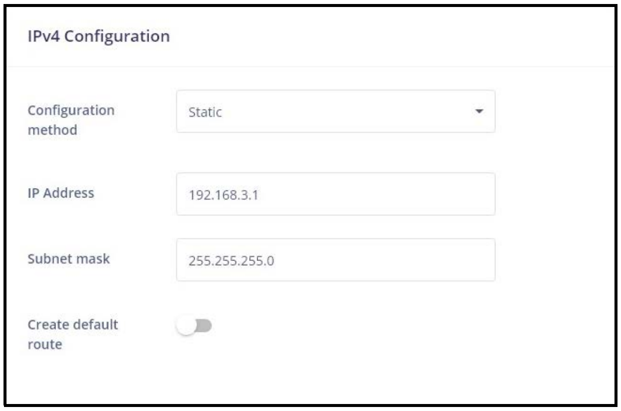
Subnet mask: 255.255.255.0

Create default route

2. To enable this feature, select the toggle to the right of **Enabled**.
3. In the 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. If you select **None**, the other fields are hidden.
4. Fill in the other fields as explained below for each option:
   - *Static*
   - *DHCP*

Static

When **Static** is selected for the **Configuration method**, the following fields are displayed:



IPv4 Configuration

Configuration method: Static

IP Address: 192.168.3.1

Subnet mask: 255.255.255.0

Create default route

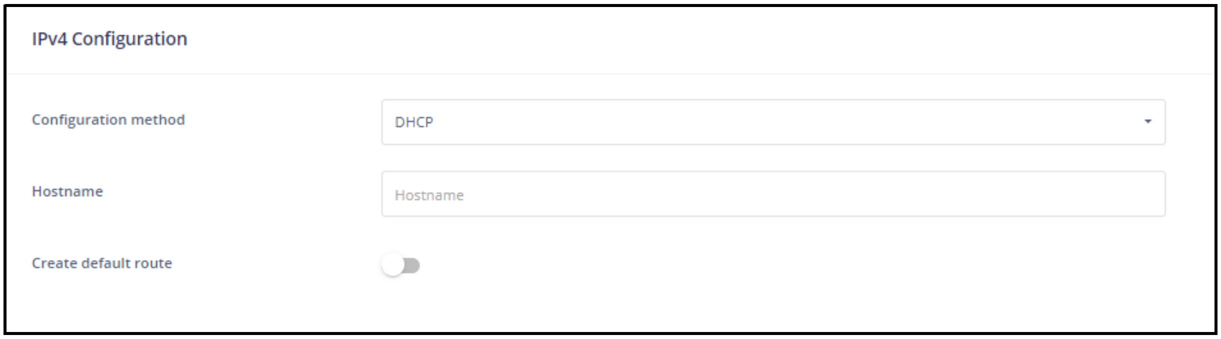
1. Modify the fields using the information in *Table 13*.
2. Go to Step 5 below.

Table 13. Static IP Parameters for Voice

Field	Description
IP Address	Enter the IP address for IPv4 communications. The default IP address is 192.168.3.1.
Subnet mask	Enter the IP address for the subnet mask.

DHCP

When **DHCP** is selected for the **Configuration method**, the following fields are displayed.



IPv4 Configuration

Configuration method: DHCP

Hostname: Hostname

Create default route

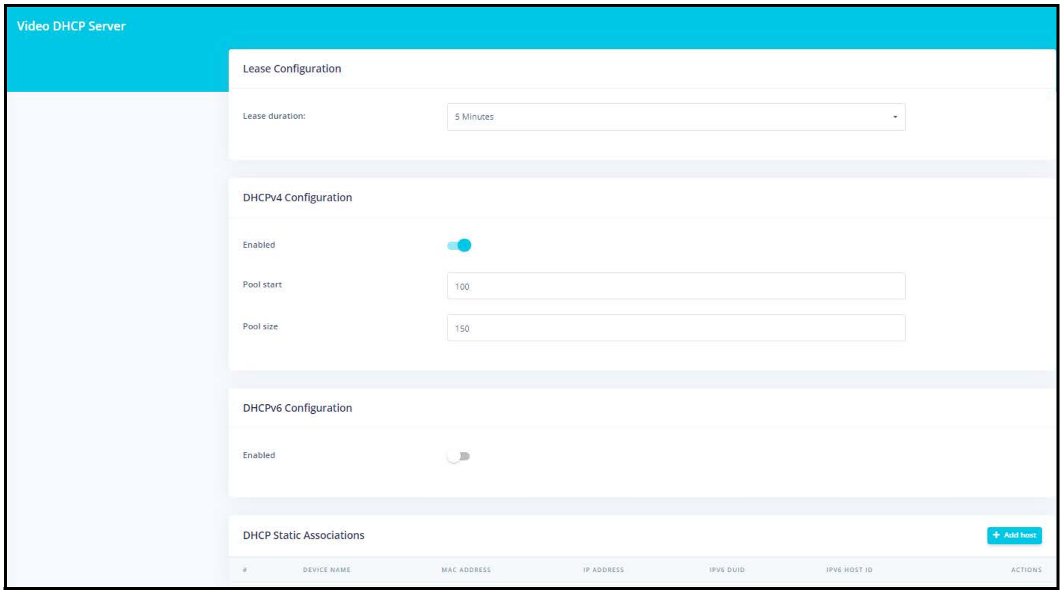
1. (Optional) In the **Hostname** field, enter the host name to be included in DHCP requests.
2. Go to Step 5 below.

5. To enable the default route for this network, select the toggle to the right of **Create default route**.
6. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Video DHCP Server

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

1. In the left menu, select **Network** > **Video Network** > **DHCP Server**.



Video DHCP Server

Lease Configuration

Lease duration: 5 Minutes

DHCPv4 Configuration

Enabled

Pool start: 100

Pool size: 150

DHCPv6 Configuration

Enabled

DHCP Static Associations

#	DEVICE NAME	MAC ADDRESS	IP ADDRESS	IPV6 DUID	IPV6 HOST ID	ACTIONS

2. Fill in the fields using the information in *Table 14*.
3. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

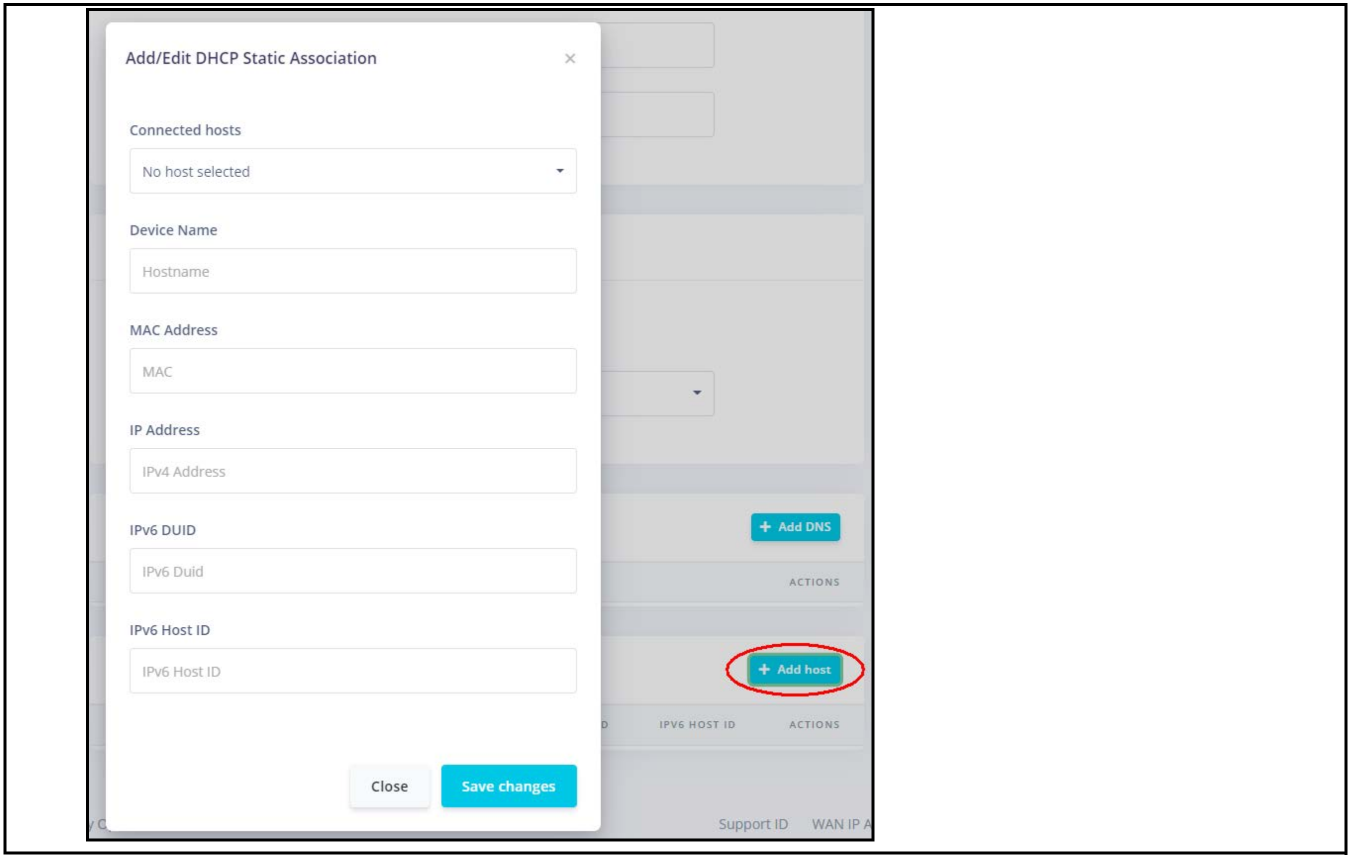
Table 14. DHCP Server for Voice

Field	Description
Lease duration	Enter the amount of time for which 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, select the toggle.
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 disabled by default. To enable this feature, select the toggle to the right of **Enabled**.
Router advertisement	(Appears when **Enabled** is set to **On**) Select how this SDG 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
DHCP Static Associations	(Optional) To define a static DHCP server, follow the steps in *Defining a Static DHCP IP Address Association for a Video Host on page 32*.

Defining a Static DHCP IP Address Association for a Video Host

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

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



2. When a connected host is selected, the fields in the dialog box are populated with the necessary information. If the host is currently offline or the **None** option is chosen, the information must be entered manually.

3. Complete the fields, using the information in *Table 15*.

4. Select **Save changes** to commit your changes.

Table 15. Defining a Static DHCP IP Address Association for a Video Host

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. 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 server.

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

6. To edit a static DHCP IP address, select the adjacent blue edit button. The **Add/Edit** dialog box appears. Change the entries as needed and select **Save Changes** to commit your changes.
7. To remove a static DHCP IP address, select the adjacent red delete button.
8. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Video DHCP Clients

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

In the left menu, select **Network** > **Video Network** > **DHCP Clients**. The subsequent page that appears displays two tables.

The upper table lists active IPv4 LAN client devices. The lower table lists active IPv6 LAN client devices.

Specifying Wired Network Settings

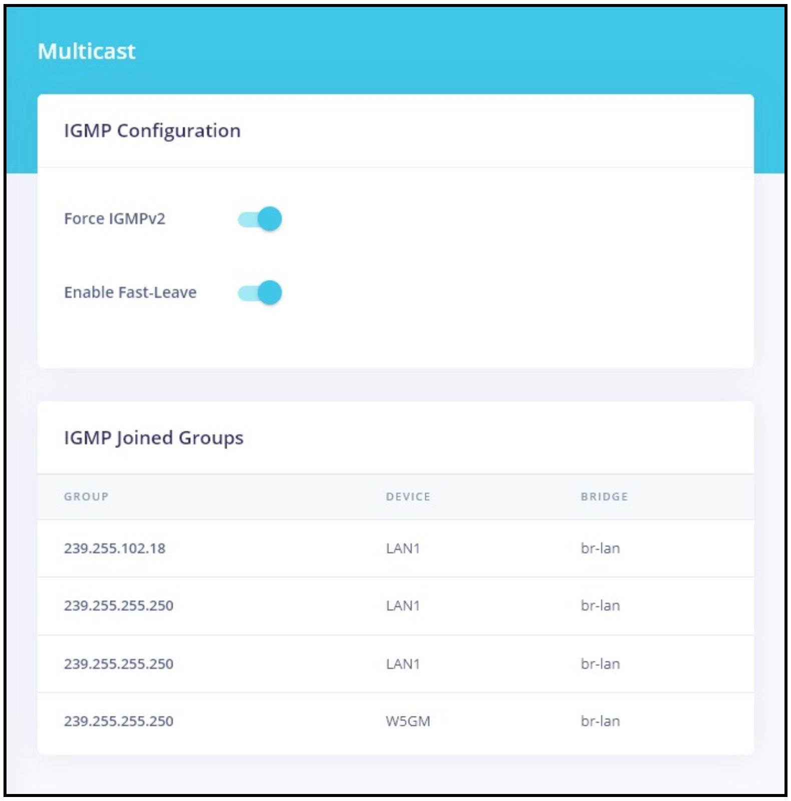
In this section, additional network settings are discussed including configuration instructions for:

- *Multicast on page 33*
- *Routing on page 35*
- *Firewall on page 38*

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, select **Network** > **Multicast**. The following page appears.



Multicast

IGMP Configuration

Force IGMPv2 ●

Enable Fast-Leave ●

IGMP Joined Groups

GROUP	DEVICE	BRIDGE
239.255.102.18	LAN1	br-lan
239.255.255.250	LAN1	br-lan
239.255.255.250	LAN1	br-lan
239.255.255.250	W5GM	br-lan

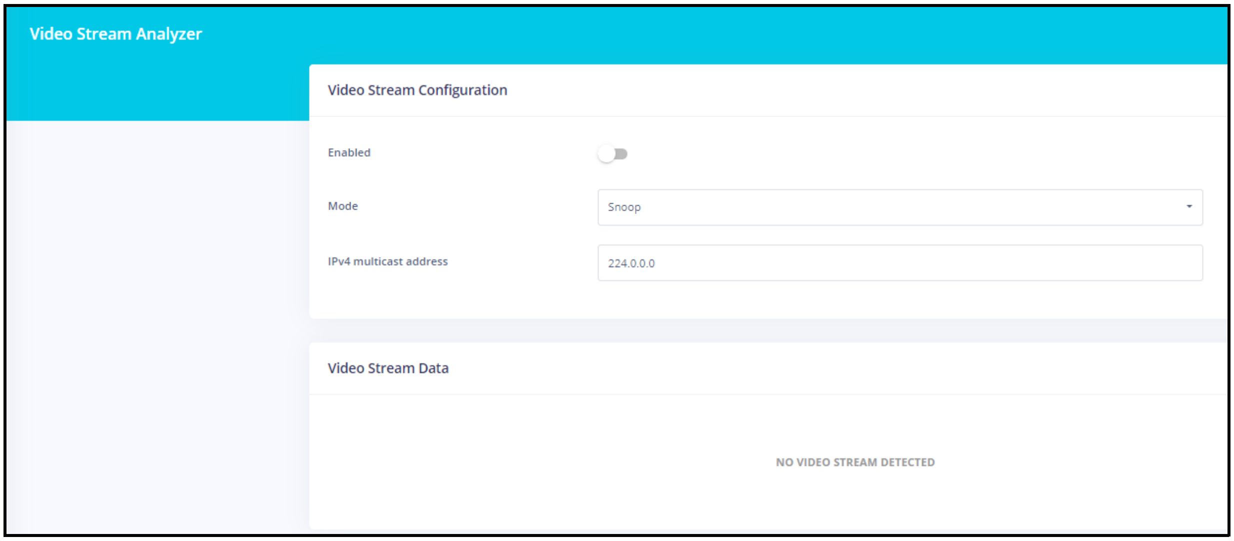
2. (Optional) To enable the IGMPv2 feature, select the toggle next to **Force IGMPv2**.

3. (Optional) To enable the Fast-Leave feature, select the toggle next to **Enable Fast-Leave**.
4. Select 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, select **Network** > **Multicast** > **Video Analyzer**. The following page appears.



Video Stream Analyzer

Video Stream Configuration

Enabled

Mode: Snoop

IPv4 multicast address: 224.0.0.0

Video Stream Data

NO VIDEO STREAM DETECTED

If video is configured for your SDG, data about the video stream appears in the bottom section of the page.

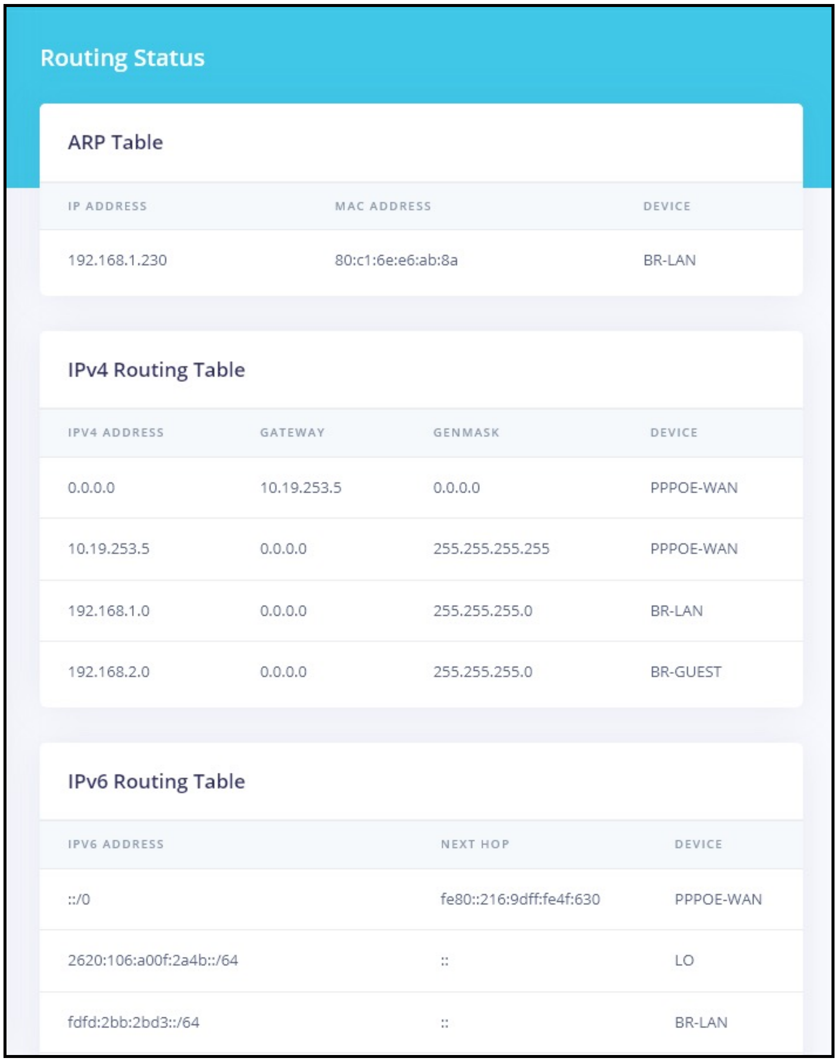
2. To enable this feature, select the toggle to the right of **Enabled**.
3. In the **Mode** field, select the analyzer mode. Options are **Snoop** and **Join**. The default is **Snoop**.
4. (Optional) In the **IPv4 multicast address** field, enter the IP address. Options range from **224.0.0.0** through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

When a video stream is active, the stream summary is shown in the **Video Stream Data** section, along with information about the stream rate, media delivery index, packet header, and PID counters display.

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, select **Network** > **Routing**. The following page appears displaying the **ARP Table**, **IPv4 Routing Table**, **IPv6 Routing Table** and an **IPv6 Neighbors Table**.



Routing Status

ARP Table

IP ADDRESS	MAC ADDRESS	DEVICE
192.168.1.230	80:c1:6e:e6:ab:8a	BR-LAN

IPv4 Routing Table

IPV4 ADDRESS	GATEWAY	GENMASK	DEVICE
0.0.0.0	10.19.253.5	0.0.0.0	PPPOE-WAN
10.19.253.5	0.0.0.0	255.255.255.255	PPPOE-WAN
192.168.1.0	0.0.0.0	255.255.255.0	BR-LAN
192.168.2.0	0.0.0.0	255.255.255.0	BR-GUEST

IPv6 Routing Table

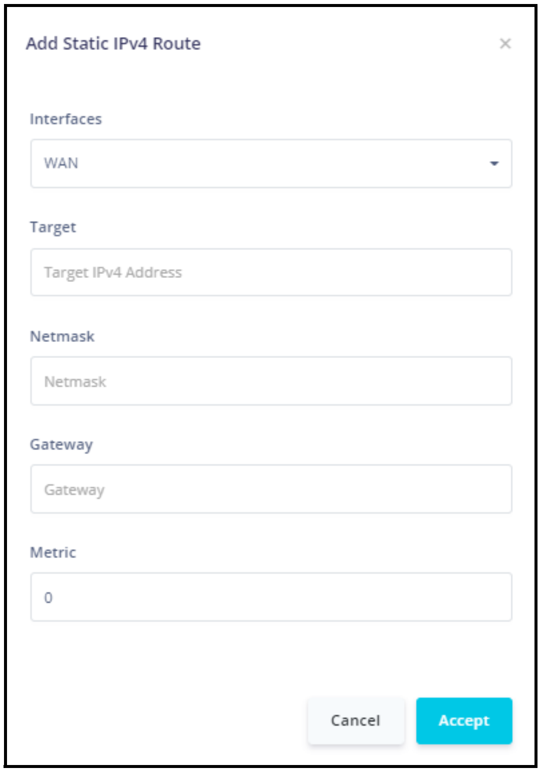
IPV6 ADDRESS	NEXT HOP	DEVICE
::/0	fe80::216:9dff:fe4f:630	PPPOE-WAN
2620:106:a00f:2a4b::/64	::	LO
fdfd:2bb:2bd3::/64	::	BR-LAN

Static Routes

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

1. In the left menu, select **Network** > **Routing** > **Static Routes**. The subsequent page that appears displays tables for **IPv4 Static Routes** and **IPv6 Static Routes**.

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



Add Static IPv4 Route

Interfaces: WAN

Target: Target IPv4 Address

Netmask: Netmask

Gateway: Gateway

Metric: 0

3. Complete the fields, using the information provided in *Table 16*.

Table 16. Add Static Route

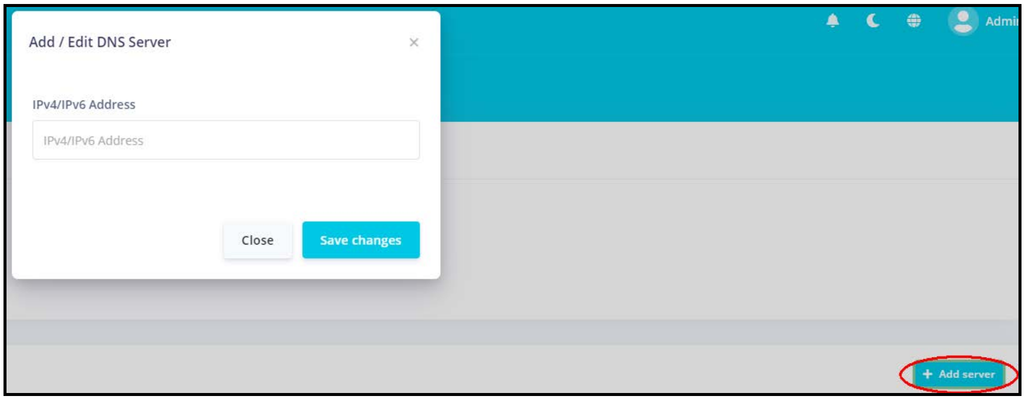
Field	Description
Interfaces	Select the interface for the static route. The default is **WAN**.
Target	Enter the host IP or network address. Enter specific IP addresses for a single device or identify an entire subnet, e.g., enter 192.168.1.0 to identify that subnet as the target.
Netmask	(Appears for 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**.

4. Select **Accept** to save your changes. You are returned to the Static Routes page.
5. To edit an existing route:
   a. Select the blue edit button to the right of the entry to be edited. The **Add Static Route** dialog box appears.
   b. Modify the fields as needed and then select **Accept**.
6. To delete a route, select the red delete button to the right of the entry to be deleted.
7. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

DNS

On this page, you can configure network DNS servers.

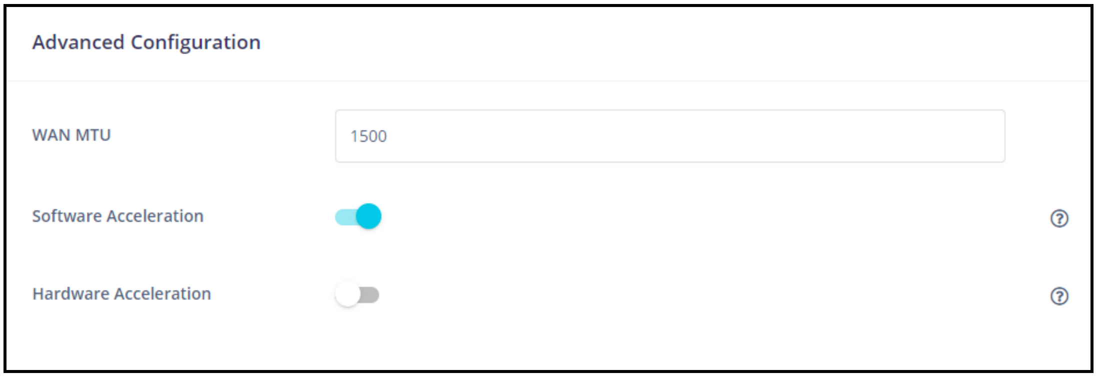
1. In the left menu, select **Network** > **Routing** > **DNS**.
2. Enable Rebind Protection by selecting the toggle to the right. Rebind protection protects against an attack known as DNS rebinding. Enabling Rebind protection blocks the use of private IP ranges by public domains.
3. To add a custom DNS server, in the **Custom DNS Servers** section:
    a. Select the **Add server** button. The **Add/Edit DNS Server** dialog box appears.



    b. Enter the IP address of the custom DNS server and select **Save changes**.
    c. To add another IP address, repeat steps a and b.
4. To edit a DNS server address, select the adjacent blue edit button. The **Add/Edit** dialog box appears. Enter the new server address and select **Save Changes** to commit your changes.
5. To remove a server, select the adjacent red delete button.
6. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Advanced

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


Advanced Configuration

WAN MTU: 1500

Software Acceleration: ● on

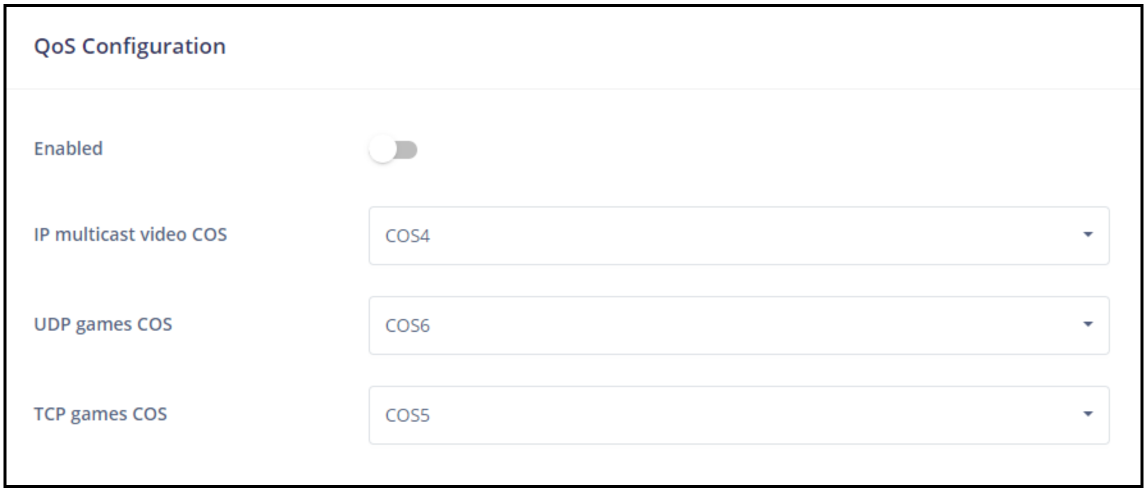
Hardware Acceleration: ○ off

1. In the left menu, select **Network** > **Routing** > **Advanced**.
2. Enter the **WAN MTU** for the network. Options are **0** - **2048**. The default is **1500**.
3. Software acceleration of routed flows to wired LAN clients is enabled by default. Select the toggle to disable software.

4. Hardware acceleration of routed flows to wired LAN clients is disabled by default. Select the toggle to enable hardware acceleration.
5. Select 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 (QoS).



QoS Configuration

Enabled

IP multicast video COS: COS4

UDP games COS: COS6

TCP games COS: COS5

1. In the left menu, select **Network** > **Routing** > **Downstream QoS**.
2. To enable the quality of service feature, select the toggle to the right of **Enabled**.
3. In the three remaining fields for **IP multicast video COS**, **UDP games COS** and **TCP games COS**, select the appropriate COS (priority) level. Options are **COS7 - COS0**. The default value for IP multicast video is **COS4**, UDP games is **COS6**, TCP games is **COS5**. The default settings work for most systems.
4. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Firewall

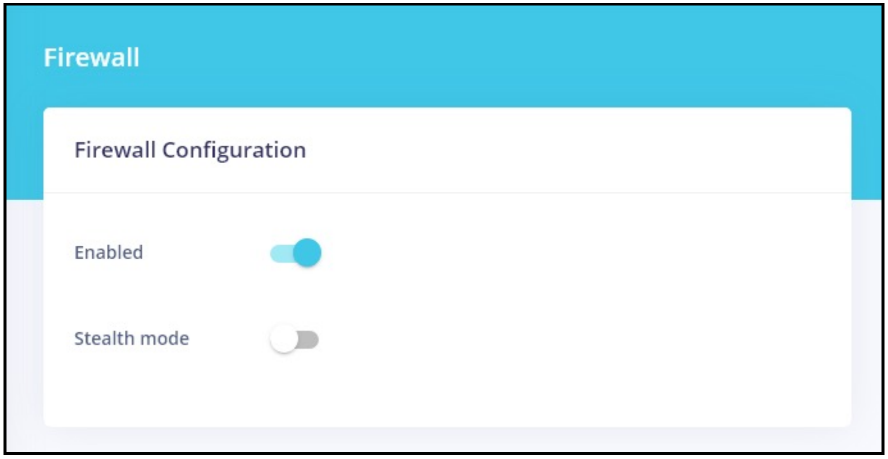
In this section, learn about settings for the following Firewall configuration elements:

- *Firewall Settings on page 39*
- *Firewall Rules on page 40*
- *DMZ on page 42*
- *Port Forwarding on page 43*
- *Viewing Wired Network Statistics on page 44*

Firewall Settings

On this page, you can enable the firewall for your system.

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



Firewall

Firewall Configuration

Enabled

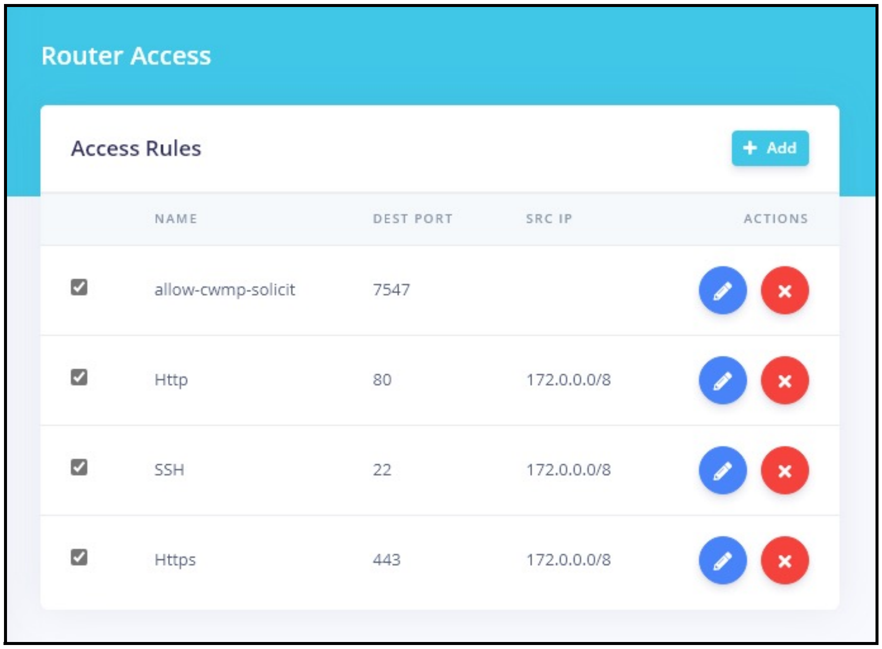
Stealth mode

2. To disable the firewall, select the toggle next to **Enabled**.
3. To prevent malicious users from discovering information about your network and its devices and services, select the toggle next to **Stealth mode**.
4. If configured for your system, the **Conntrack Helper** section is visible. This feature is disabled by default. To allow these modules to assist the firewall in tracking the various protocols used to establish traffic flow, select the toggle.
5. Select 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, select **Network** > **Firewall** > **Router Access**. The following page appears.

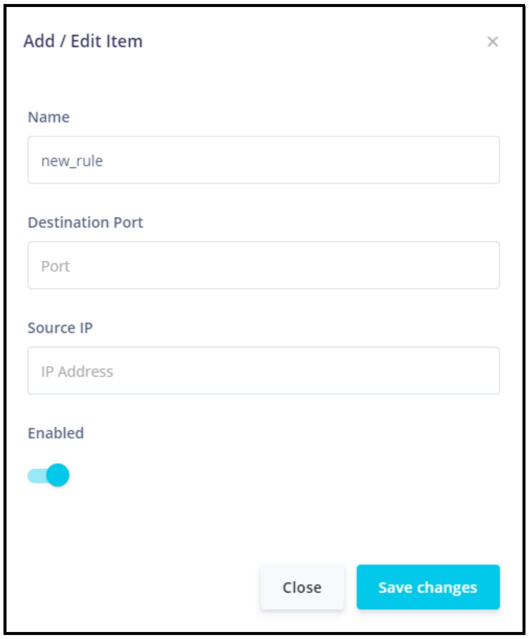


Router Access

Access Rules

	NAME	DEST PORT	SRC IP	ACTIONS
☑	allow-cwmp-solicit	7547		
☑	Http	80	172.0.0.0/8	
☑	SSH	22	172.0.0.0/8	
☑	Https	443	172.0.0.0/8	

2. To add a mapping, select the **Add button** near the upper-right corner. The **Add / Edit Item** dialog box appears.



Add / Edit Item

Name

new_rule

Destination Port

Port

Source IP

IP Address

Enabled

3. Fill in the fields using the information provided in *Table 17*. All fields are optional.
4. Select **Save changes**. The dialog box closes and the new mapping appears in the **Router Access** list.
5. To edit a mapping:
    a. Select the blue edit button next to the line item to be changed. The **Add / Edit Item** dialog box appears.
    b. Modify the fields as needed.
    c. Select **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 to be suspend. The mapping definition remains on the page but is not active.
7. To remove a mapping, select the red delete button at the end of the row to be deleted. The mapping definition is removed.
8. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Table 17. Router Access Parameters

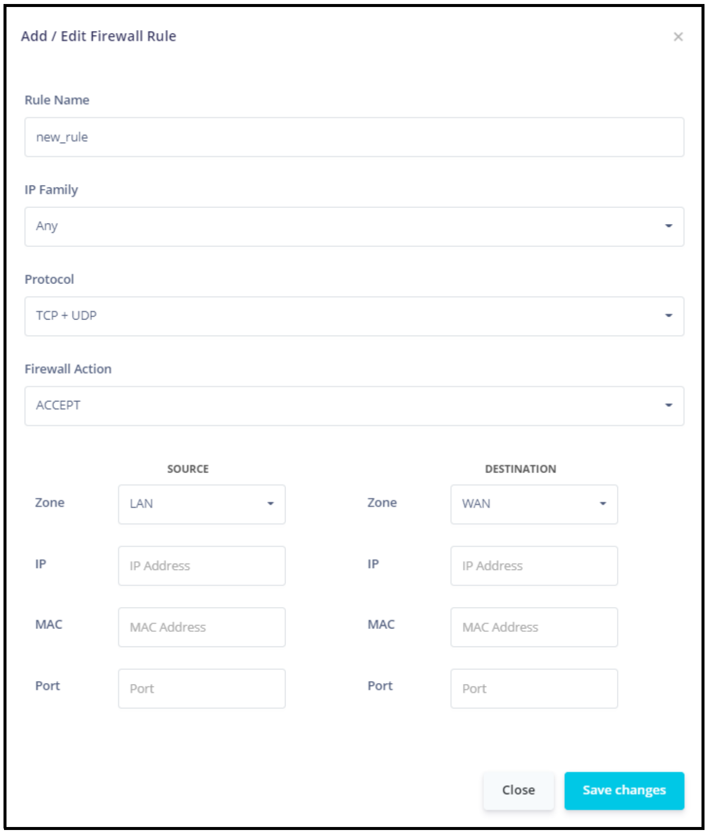
Field	Description
Name	Enter a descriptive name for this rule. No spaces are allowed.
Destination Port	Enter the destination port for this rule.
Source IP	Enter the IP address of the remote network that will be used for access.
Enabled	New rules are enabled by default. To disable this rule but save the settings, select the toggle.

Firewall Rules

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

1. In the left menu, select **Network** > **Firewall** > **Rules**.

2. To create a new rule:
    a. Select the **Add rule** button near the upper-right corner. The **Add / Edit Firewall Rule** dialog box appears.



Add / Edit Firewall Rule

Rule Name: new_rule

IP Family: Any

Protocol: TCP + UDP

Firewall Action: ACCEPT

	SOURCE		DESTINATION
Zone	LAN	Zone	WAN
IP	IP Address	IP	IP Address
MAC	MAC Address	MAC	MAC Address
Port	Port	Port	Port

    b. In the **Rule Name** field, enter a descriptive name for the rule.
    c. Fill in the other fields using the information in *Table 18*.
    d. Select **Save changes**.

3. To edit a rule:
    a. Select the blue edit button next to the line item to be changed. The **Add / Edit Item** dialog box appears.
    b. Modify the fields as needed.
    c. Select **Save changes**. The updated values appear on the page.

4. To remove a rule, select the red delete button at the end of the row to be deleted. 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. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Table 18. Add a Firewall Rule

Field	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**. The default is **TCP + UDP**.
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	
Zone	Select the source zone. Options are **Unspecified**, **Any**, **MGMT**, **VOICE**, **WAN**, **VIDEO**, **GUEST**, and **LAN**. 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 SDG. 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, enter the port number for the source address.
DESTINATION	
Zone	Select the destination zone. Options are **Unspecified**, **Any**, **MGMT**, **VOICE**, **WAN**, **VIDEO**, **GUEST**, and **LAN**. 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 SDG. 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 SDG. For security reasons, it is recommended that you create a static IP address for the host server entered on this page.

1. In the left menu, select **Network** > **Firewall** > **DMZ**. The WAN IP address shown is read-only.
2. To enable this feature, select the toggle 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.

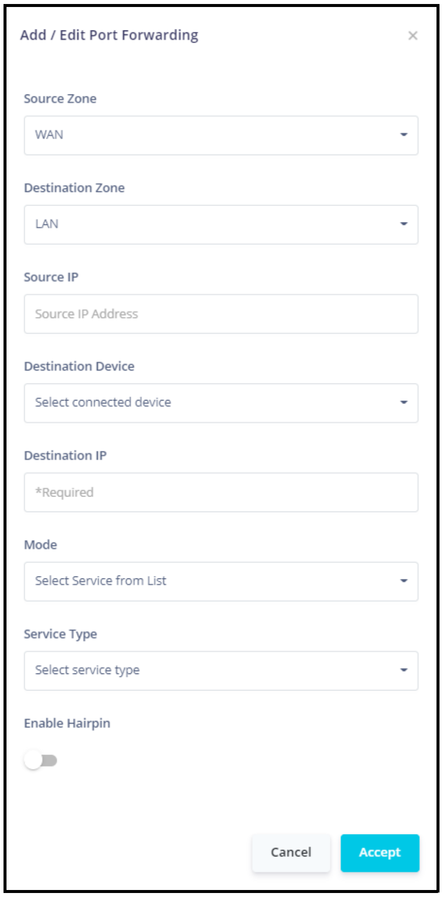
> **NOTE**
>
> *It is recommended to create a static DHCP association to this host address.*

4. Select 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, select **Network** > **Firewall** > **Port Forwarding**.
2. To add a mapping, select the **Add rule** button near the upper-right corner. The **Add/Edit Port Forwarding** dialog box appears.



Add / Edit Port Forwarding

Source Zone: WAN

Destination Zone: LAN

Source IP: Source IP Address

Destination Device: Select connected device

Destination IP: *Required

Mode: Select Service from List

Service Type: Select service type

Enable Hairpin

3. Fill in the fields using the information provided in *Table 19*. All fields are optional.

Table 19. Add/Edit Port Forwards

Field	Description
Source Zone	Select the source zone from the drop-down list of zones defined on this network. Options are **MGMT**, **VOICE**, **WAN**, **VIDEO**, **GUEST**, and **LAN**. The default is **WAN**.
Destination Zone	Select the destination zone from the drop-down list of zones. Options are **MGMT**, **VOICE**, **WAN**, **VIDEO**, **GUEST**, and **LAN**. The default is **LAN**.
Source IP	Enter the IP address for the remote device.
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.

Table 19. Add/Edit Port Forwards (Continued)

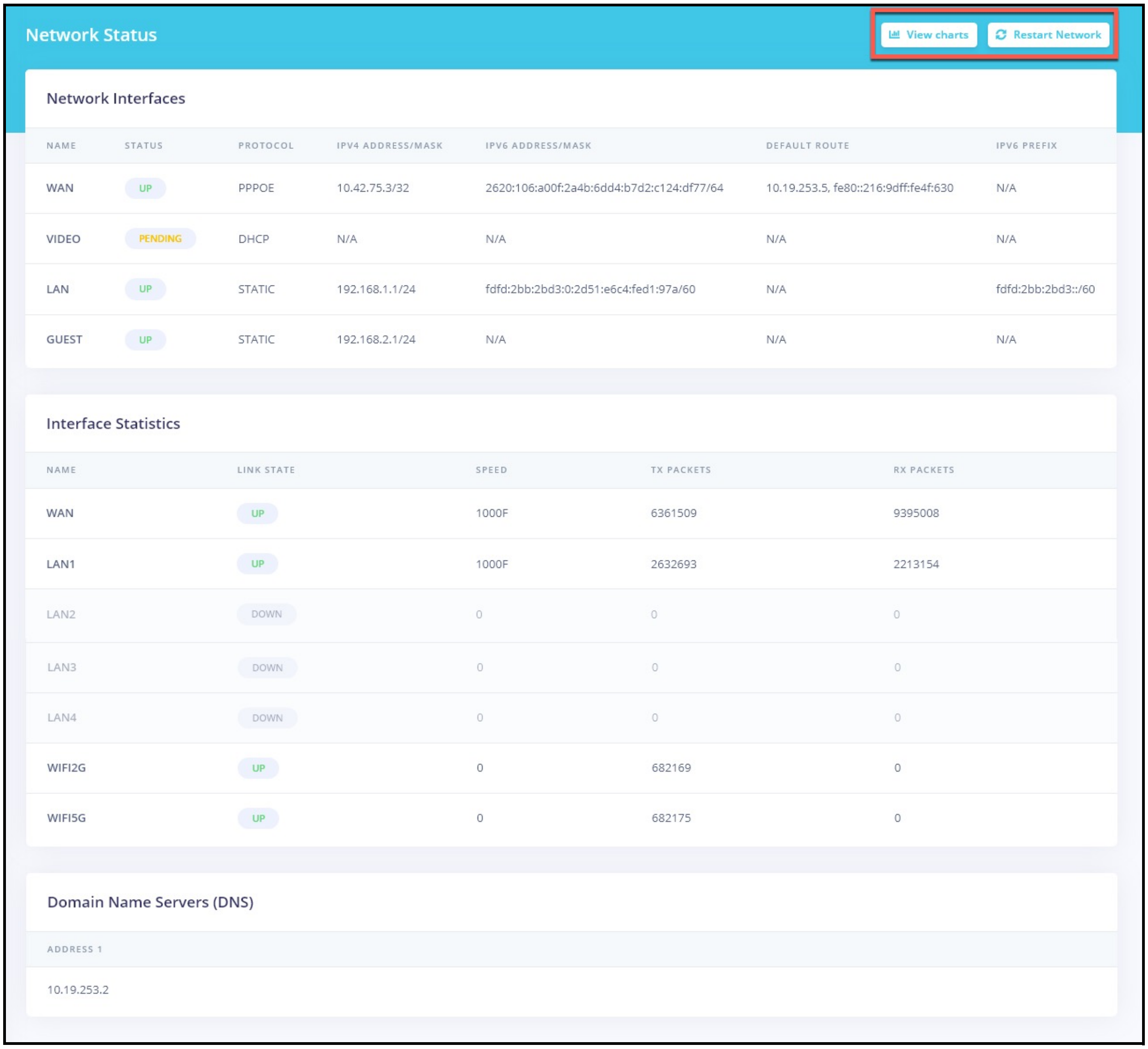
Field	Description
Mode	Select whether to use the settings defined for a service or to define the port settings manually. Options are **Select Service From List** and **Configure Manually**. The default is **Select Service From List**.
Fields defined for using a service	
Service Type	Select the type of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

4. Select **Accept**. The dialog box closes and the new mapping appears in the **Port Forwarding** list.
5. To edit a mapping:
   a. Select the blue edit button to the right of the mapping entry. The **Add/Edit Port Forwarding** dialog box appears.
   b. Modify the fields as needed, and then select **Save**. The updated values appear on the page.
6. To disable a mapping, clear the **checkbox** that appears before the **Name** column. The mapping definition remains on the page but is not active.
7. To remove a mapping, select the red delete button at the end of the row to be deleted. The rule is removed.
8. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Viewing Wired Network Statistics

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

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



Network Interfaces

NAME	STATUS	PROTOCOL	IPV4 ADDRESS/MASK	IPV6 ADDRESS/MASK	DEFAULT ROUTE	IPV6 PREFIX
WAN	UP	PPPOE	10.42.75.3/32	2620:106:a00f:2a4b:6dd4:b7d2:c124:df77/64	10.19.253.5, fe80::216:9dff:fe4f:630	N/A
VIDEO	PENDING	DHCP	N/A	N/A	N/A	N/A
LAN	UP	STATIC	192.168.1.1/24	fdfd:2bb:2bd3:0:2d51:e6c4:fed1:97a/60	N/A	fdfd:2bb:2bd3::/60
GUEST	UP	STATIC	192.168.2.1/24	N/A	N/A	N/A

Interface Statistics

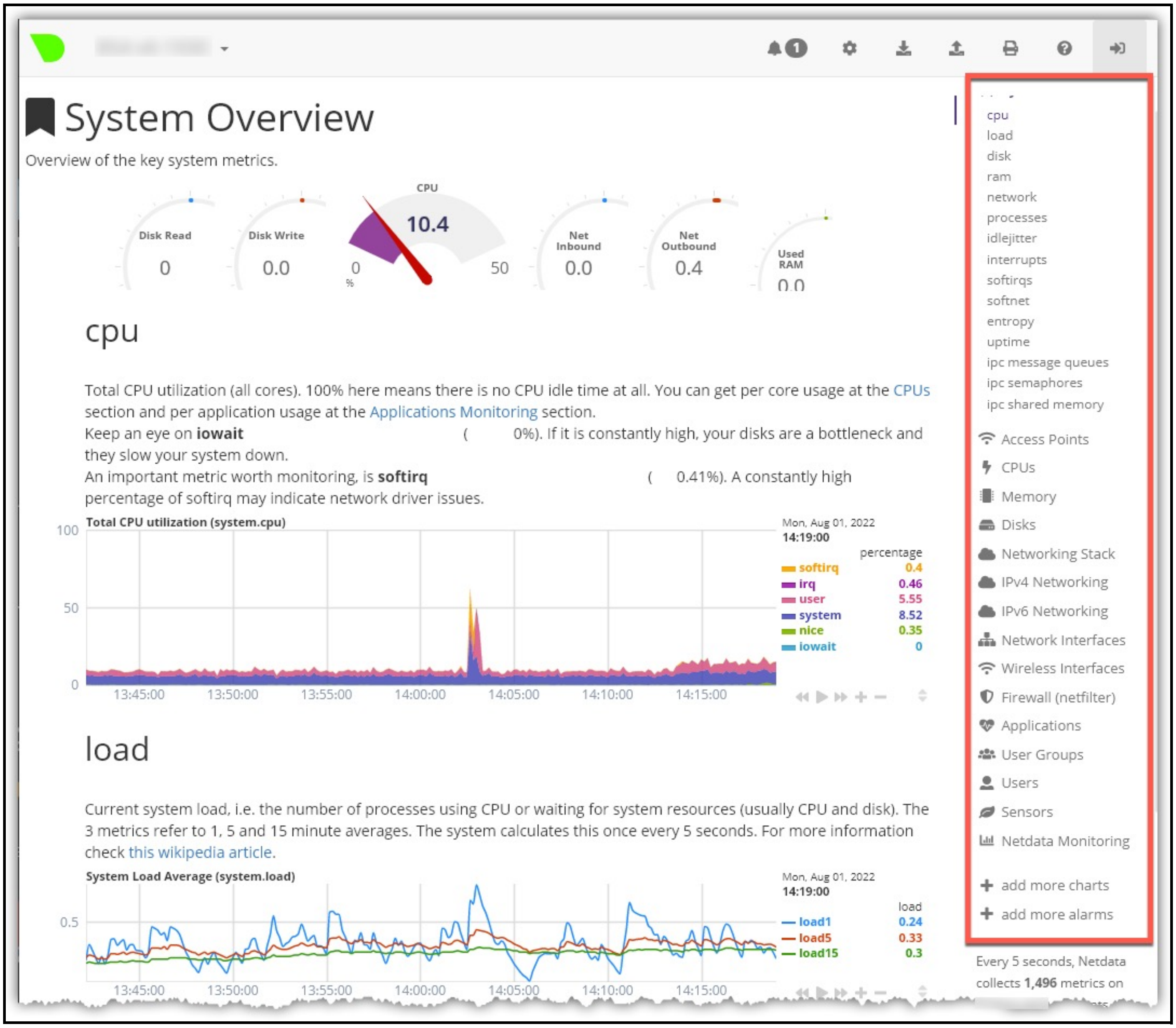
NAME	LINK STATE	SPEED	TX PACKETS	RX PACKETS
WAN	UP	1000F	6361509	9395008
LAN1	UP	1000F	2632693	2213154
LAN2	DOWN	0	0	0
LAN3	DOWN	0	0	0
LAN4	DOWN	0	0	0
WIFI2G	UP	0	682169	0
WIFI5G	UP	0	682175	0

Domain Name Servers (DNS)

ADDRESS 1
10.19.253.2

Select the **Restart Network** button at the upper right to restart the local network. The confirmation message appears. Select **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, select the **View Charts** button at the upper-right.



System Overview

Overview of the key system metrics.

cpu

Total CPU utilization (all cores). 100% here means there is no CPU idle time at all. You can get per core usage at the CPUs section and per application usage at the Applications Monitoring section.
Keep an eye on **iowait** (0%). If it is constantly high, your disks are a bottleneck and they slow your system down.
An important metric worth monitoring, is **softirq** (0.41%). A constantly high percentage of softirq may indicate network driver issues.

load

Current system load, i.e. the number of processes using CPU or waiting for system resources (usually CPU and disk). The 3 metrics refer to 1, 5 and 15 minute averages. The system calculates this once every 5 seconds. For more information check this wikipedia article.

Every 5 seconds, Netdata collects **1,496** metrics on

The netdata **System Overview** window opens in a new tab, showing information about the overall SDG's system, memory, CPUs, firewall, IPv4 networking, etc. Use the navigation menu at right to select the statistics you want to view.

6. Configuring Wi-Fi Networks

In this section, instructions are provided for adjusting settings and viewing performance associated with the Wi-Fi networks configured on your SDG. Topics include:

- *Viewing Network Status on page 47*
- *Scan for Access Points on page 48*
- *Configuring Radio and SSID Settings on page 50*
- *Viewing Client Connections on page 54*
- *Managing Client Access on page 55*

- *WPS Configuration on page 56*
- *Performance Statistics on page 57*

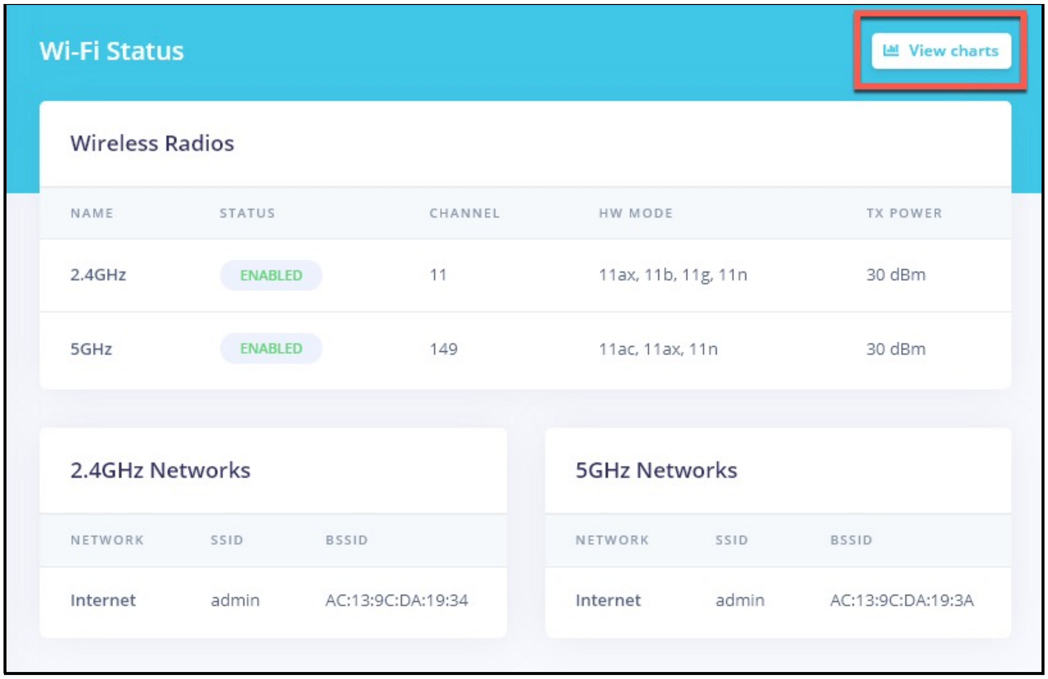
View WiFi Network Status and Scan for Nearby Access Points

This section describes features associated with viewing performance information on the WiFi networks configured on your SDG and also how to scan for nearby WiFi access points.

Viewing Network Status

On this page, you can view information about the wireless networks configured on your SDG..

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



Wireless Radios

NAME	STATUS	CHANNEL	HW MODE	TX POWER
2.4GHz	ENABLED	11	11ax, 11b, 11g, 11n	30 dBm
5GHz	ENABLED	149	11ac, 11ax, 11n	30 dBm

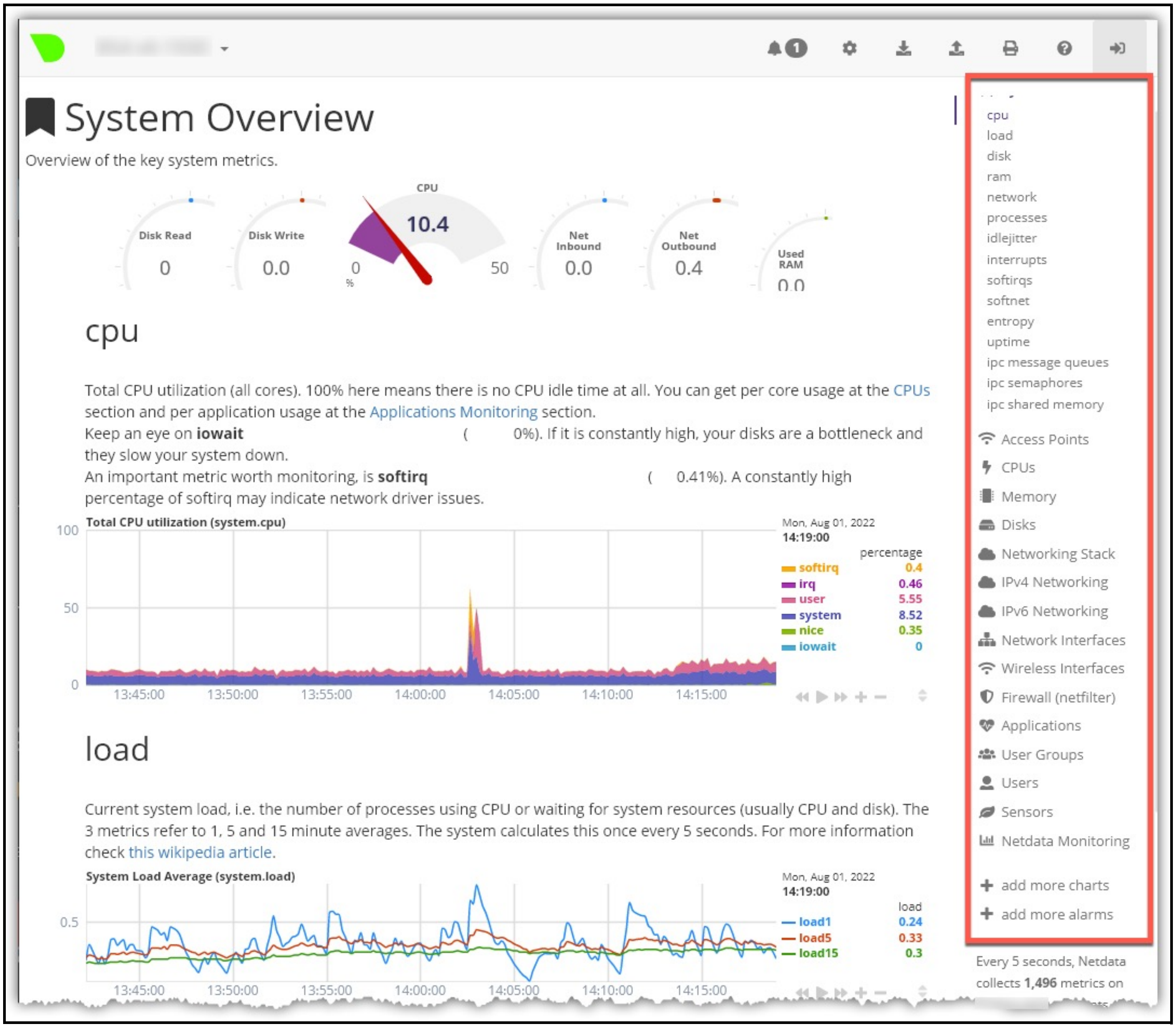
2.4GHz Networks

NETWORK	SSID	BSSID
Internet	admin	AC:13:9C:DA:19:34

5GHz Networks

NETWORK	SSID	BSSID
Internet	admin	AC:13:9C:DA:19:3A

To view detailed transmission data for the individual interfaces, select the **View charts** button at the top right.



System Overview

Overview of the key system metrics.

cpu

Total CPU utilization (all cores). 100% here means there is no CPU idle time at all. You can get per core usage at the CPUs section and per application usage at the Applications Monitoring section.
Keep an eye on **iowait** (0%). If it is constantly high, your disks are a bottleneck and they slow your system down.
An important metric worth monitoring, is **softirq** (0.41%). A constantly high percentage of softirq may indicate network driver issues.

load

Current system load, i.e. the number of processes using CPU or waiting for system resources (usually CPU and disk). The 3 metrics refer to 1, 5 and 15 minute averages. The system calculates this once every 5 seconds. For more information check this wikipedia article.

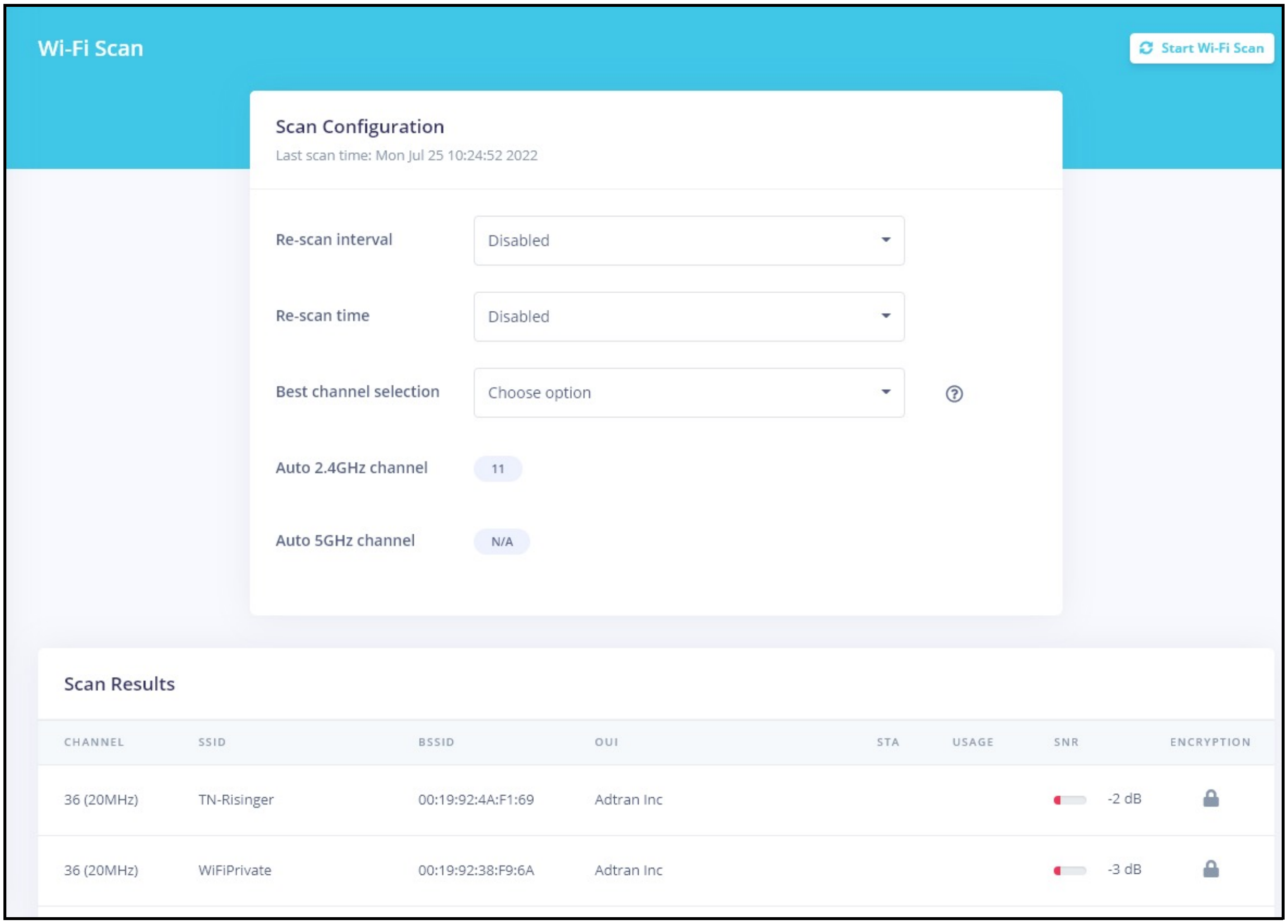
The netdata **System Overview** window opens in a new tab, showing information about the overall status of your SDG's, memory, CPUs, firewall, IPv4 networking, etc. Use the navigation menu at right to select the statistics to be displayed.

Scan for Access Points

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. Amongst other useful applications, knowing the WiFi channels in use by other nearby access points enables you to strategically choose a lesser utilized channel in your SDG's WiFi settings.

1. In the left menu, select **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 below the **Scan Configura-**

tion section heading (next to **Last scan time**). The channels currently in use by all nearby access points are displayed below the **Best channel selection** field.



Scan Configuration

Last scan time: Mon Jul 25 10:24:52 2022

Re-scan interval	Disabled
Re-scan time	Disabled
Best channel selection	Choose option
Auto 2.4GHz channel	11
Auto 5GHz channel	N/A

Scan Results

CHANNEL	SSID	BSSID	OUI	STA	USAGE	SNR	ENCRYPTION
36 (20MHz)	TN-Risinger	00:19:92:4A:F1:69	Adtran Inc			-2 dB	🔒
36 (20MHz)	WiFiPrivate	00:19:92:38:F9:6A	Adtran Inc			-3 dB	🔒

2. Do any of the following:
   - To re-scan for wireless access points near your location, select 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).
   - To select the method by which the best channel is selected, on the **Best channel selection** field, select the preferred method. Options are **AP count** (number of access points) and **QBSS** (QOS enhanced basic service set). The default is **AP count**.

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

Configuring Radio and SSID Settings

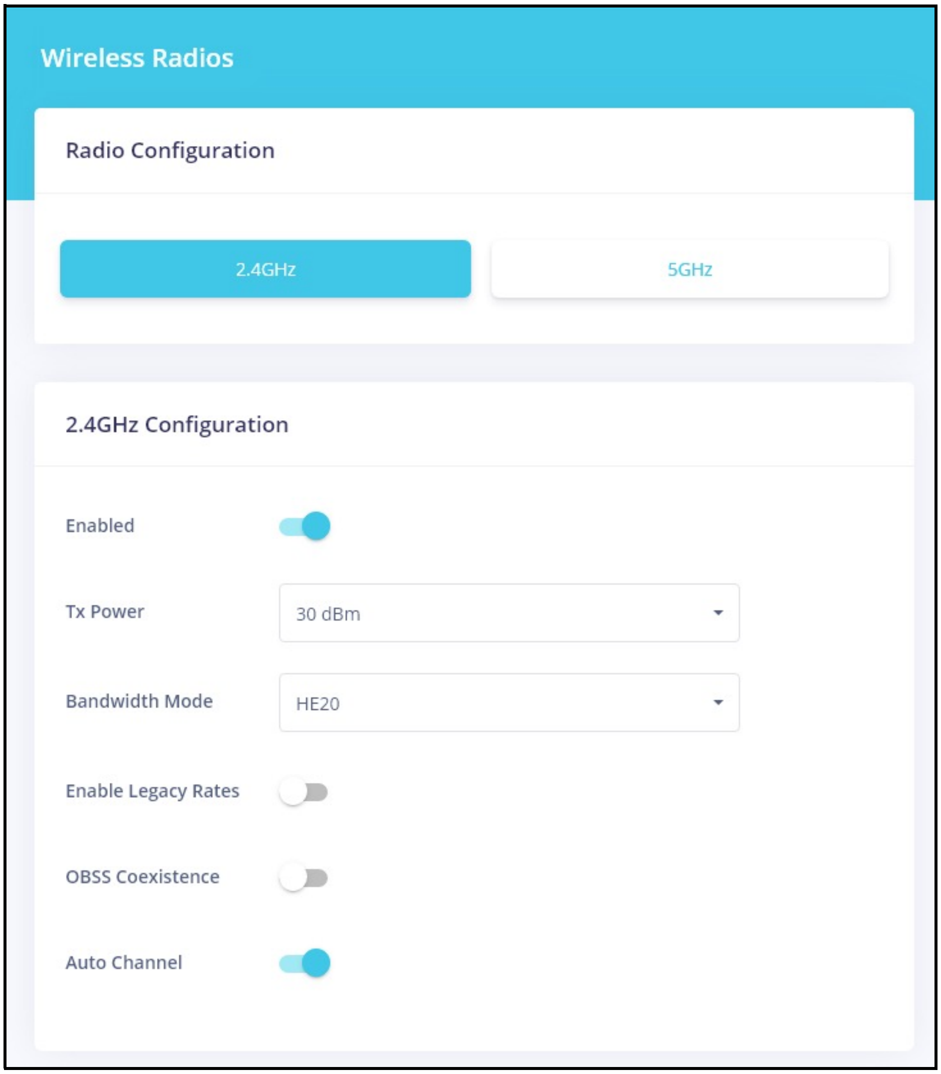
Radio

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 128. To connect more than 128 devices, create an additional network..

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



Wireless Radios

Radio Configuration

2.4GHz Configuration

Enabled ●

Tx Power: 30 dBm

Bandwidth Mode: HE20

Enable Legacy Rates ○

OBSS Coexistence ○

Auto Channel ●

2. Fill in the fields, using the information in *Table 20*. The same fields are used for both 2.4 GHz and 5 GHz configurations.

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

Table 20. Radio Settings

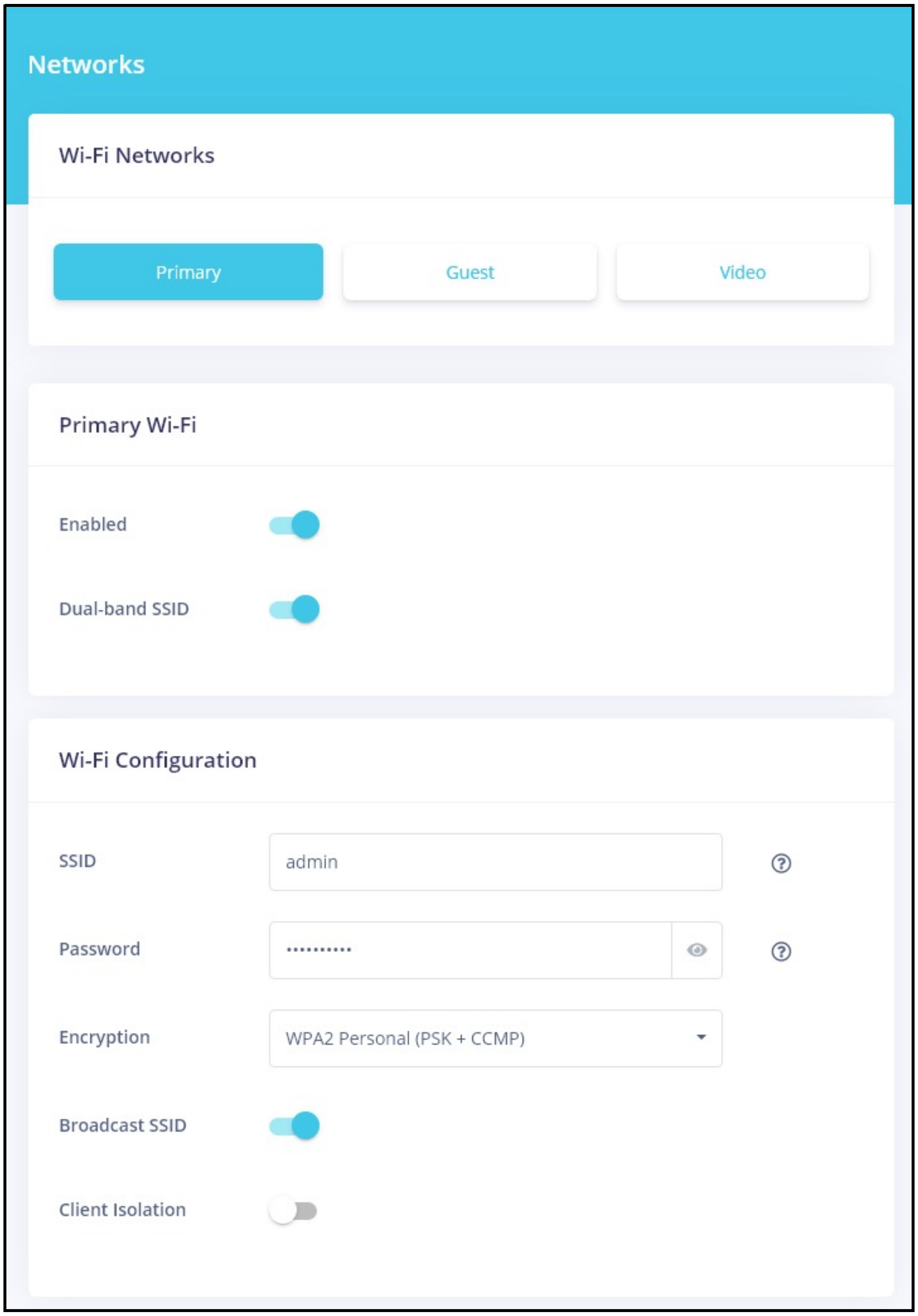
Field	Description
Enabled	Each radio is enabled by default. To disable a radio, select the toggle.
TX Power	Select the maximum rate at which transmission is allowed. Options range from **6 dBm (4 mw)** to **26 dBm (398 mw)**. The default is **24 dBm (251 mw)** for the 2.4 GHz radio and **22 dBm (158 mw)** for the 5 GHz radio.
Bandwidth Mode	Select the radio bandwidth: ■ **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** (MHz). The default is **VHT80**.
Enable Legacy Rates	This feature is disabled by default. To set the SDG to cut transmission briefly when changing channels, select the toggle. This is useful for legacy WiFi clients, enabling them to connect more effectively to a new channel.
Auto Channel	This feature is enabled by default. To disable automatic channel selection, select the toggle. 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 64 (5.32 GHz)** and **Channel 100 (5.5 GHz)** - **Channel 165 (5.825 GHz)**.
Legacy Client Auto Channel Mode	(Appears for **2.4GHz** only) This feature is disabled by default. To allow the SDG to select the best channel for legacy clients, select the toggle.

Specifying Network Settings

On this page, you can configure the network settings for

- *Primary on page 52*
- *Guest on page 53*
- *Video on page 53*
- *Mesh on page 53*

In the left menu, select **WiFi** > **Networks**. The following page appears showing the primary wireless network tab. Select from the horizontal row of tabs for the network you want to configure.



Networks

Wi-Fi Networks

Primary Wi-Fi

Enabled: on

Dual-band SSID: on

Wi-Fi Configuration

SSID: admin

Password: ••••••••••

Encryption: WPA2 Personal (PSK + CCMP)

Broadcast SSID: on

Client Isolation: off

Primary

Use the following steps to configure the Primary network.

1. In the left menu, select **WiFi** > **Networks**. primary wireless network tab is selected by default.
2. Complete the fields for the primary network configuration, using the information provided in *Table 21*.

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

Table 21. Primary, Guest and Video Network Settings

Field	Description
Enabled	This option is enabled for the **Primary** network. To enable Wi-Fi configuration for the **Guest** and **Video** networks, select the toggle.
Dual-band SSID	This feature is enabled by default. To disable the dual-band feature for these networks, select the toggle.
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.
Password	Enter the passphrase for this connection. To show the key characters, select the **Show/Hide** button (eye 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, select the toggle.
Client Isolation	This option is disabled by default for the **Primary** and **Video** networks and enabled for the **Guest** network. To enable client isolation for the **Primary** or **Video** networks, select the toggle.

Guest

Use the following steps to configure the Guest network.

1. In the left menu, select **WiFi** > **Networks**. primary wireless network tab is selected by default.
2. Select the **Guest** tab and complete the fields for the Guest network configuration, using the information provided in *Table 21* (above).

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

Video

Use the following steps to configure the Video network.

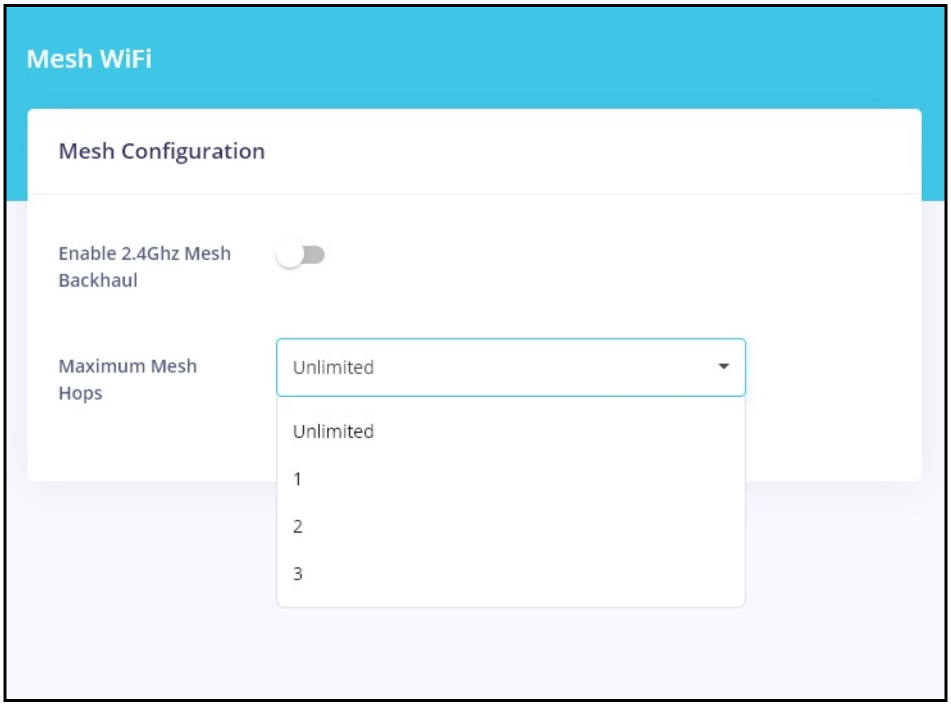
1. In the left menu, select **WiFi** > **Networks**. primary wireless network tab is selected by default.
2. Select the **Video** tab and complete the fields for the Video network configuration, using the information provided in *Table 21* (above).

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

Mesh

On this page, you can enable 2.4GHz backhaul for your Intellifi network.

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



Mesh WiFi

Mesh Configuration

Enable 2.4Ghz Mesh Backhaul

Maximum Mesh Hops: Unlimited

2. To enable the 2.4 GHz mesh backhaul feature, select the toggle 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 **Unlimited** and **1** through **3**. The default is **Unlimited**.
4. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

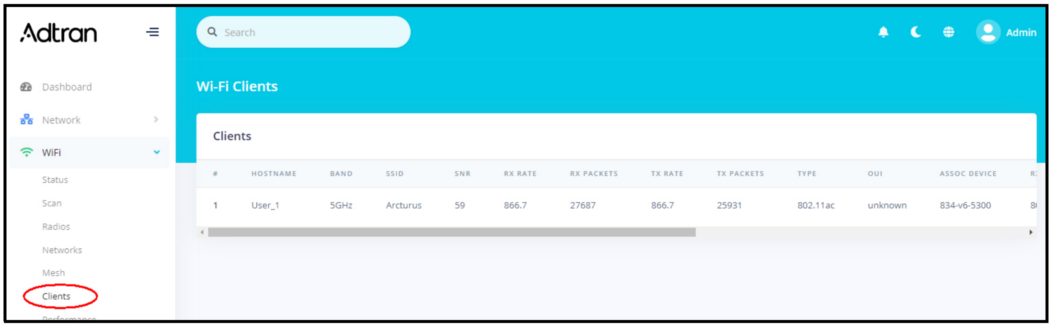
Viewing Client Connections

This section discusses viewing and managing the client devices connected to the LAN.

Viewing Connected Clients

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

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



Wi-Fi Clients

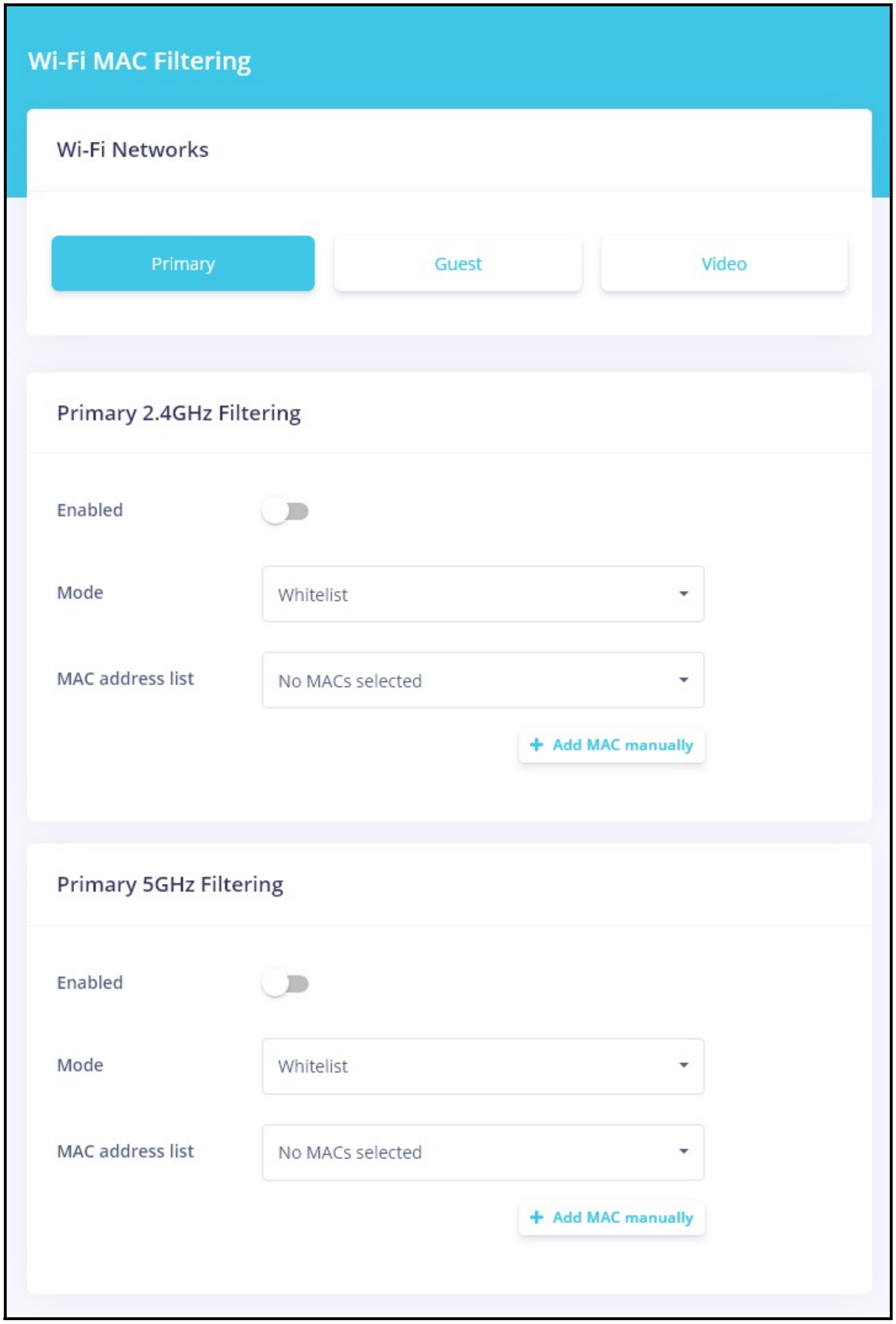
Clients

#	HOSTNAME	BAND	SSID	SNR	RX RATE	RX PACKETS	TX RATE	TX PACKETS	TYPE	OUI	ASSOC DEVICE
1	User_1	5GHz	Arcturus	59	866.7	27687	866.7	25931	802.11ac	unknown	834-v6-5300

Managing Client Access

On this page, you can configure whether wireless clients are allowed to access the wireless network of the SDG. This is achieved by a filtering using the hardware address (MAC Address) of the WiFi client.

1. In the left menu, select **WiFi** > **MAC Filtering**. The following page appears, showing information for the **Primary** network. To view information about the **Guest** and **Video** networks, click the related button.



Primary 2.4GHz Filtering

Enabled

Mode: Whitelist

MAC address list: No MACs selected

Primary 5GHz Filtering

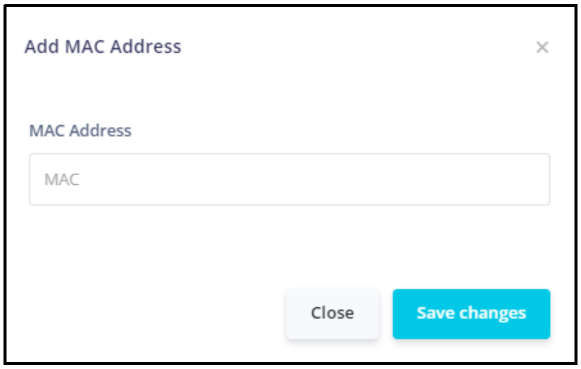
Enabled

Mode: Whitelist

MAC address list: No MACs selected

2. To enable MAC filtering, select the toggle next to **Enabled** for the network you want to configure.
3. In the section for the radio you want to configure, select the **Mode**. Options are **Whitelist** and **Blacklist**.
4. To add a MAC Address to the filter list:

a. Click **Add MAC manually**. The **Add MAC Address** dialog box appears.



Add MAC Address

MAC Address

MAC

b. Enter the **MAC address** of the wireless client.

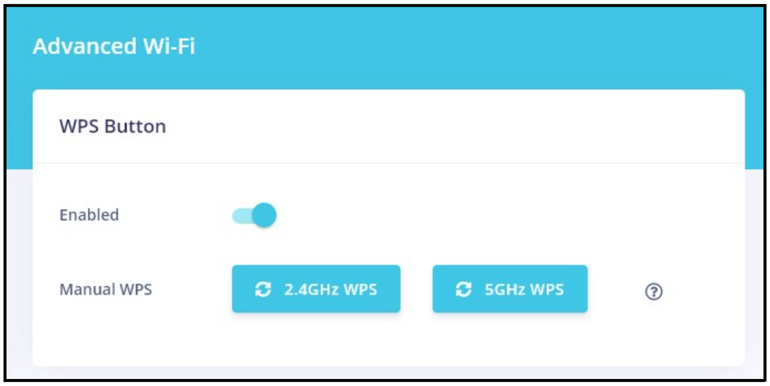
c. Click **Save changes** to save the address to the list. You are returned to the **Wi-Fi MAC Filtering** page.

To edit the label for a MAC address, select the **Add/change label** button. The **Add/Change Label** dialog box appears. In the **Label** field, type a descriptive label and select **Save changes**.

WPS Configuration

On this page, you can configure advanced wireless options for the SDG.

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



Advanced Wi-Fi

WPS Button

Enabled

Manual WPS

2. To disable the physical WPS button on the outside of the SDG, select the toggle next to **Enabled** below **WPS Button**.
3. To activate manual WPS on either of the wireless radios, click the appropriate button next to **Manual WPS**. The button label changes to **2.4GHz WPS is running** or **5GHz WPS is running.** Select the buttons again to deactivate manual WPS.
4. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Viewing Wi-Fi Performance Statistics

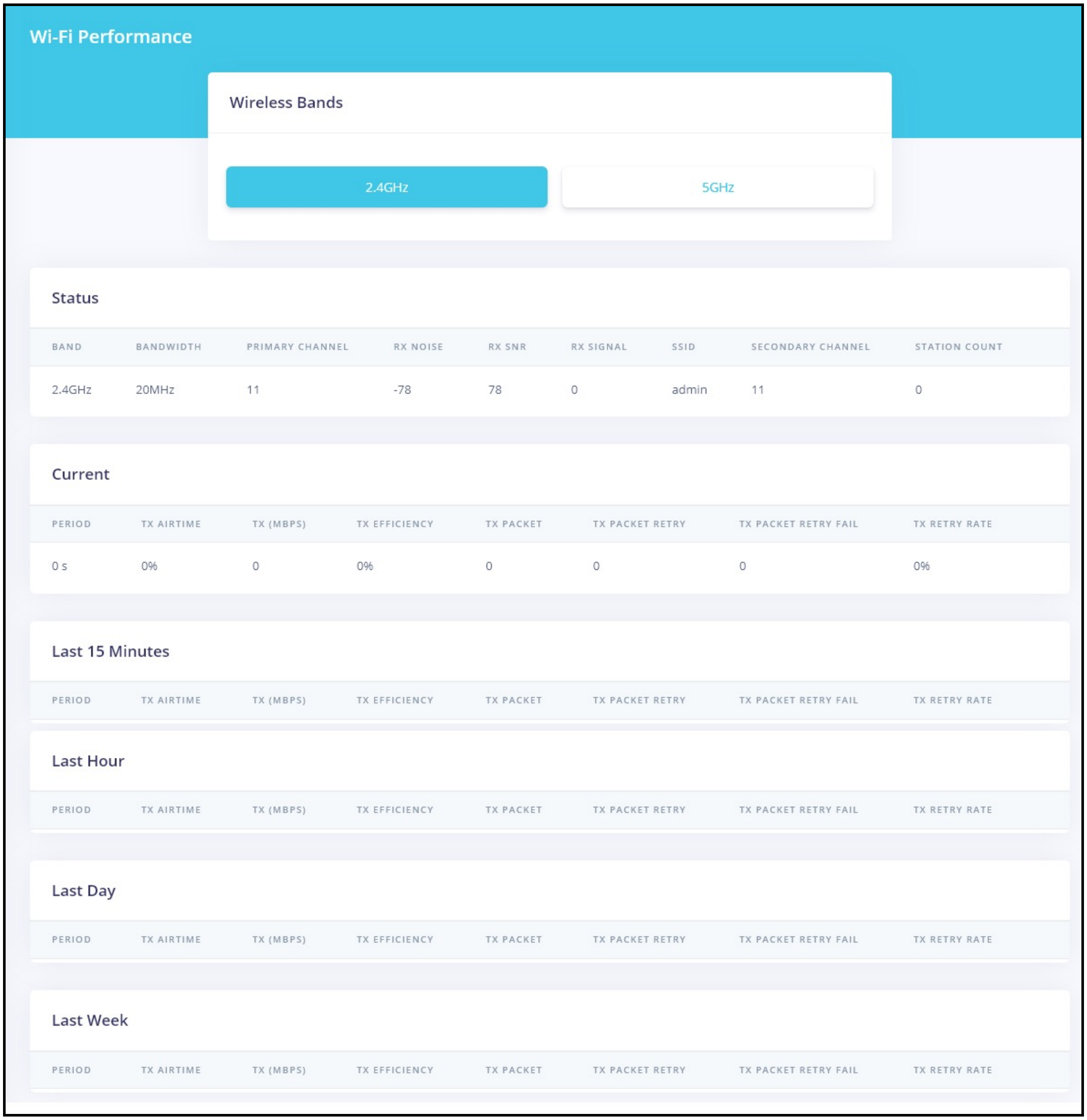
The features described in this section display statistics for various aspects of your WiFi Networks including

- *Performance Statistics on page 57*
- *Viewing Network Status on page 58*

Performance Statistics

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

In the left menu, select **WiFi** > **Performance**. The following page appears, the 2.4 GHz wireless network is pre-selected. To view information about the 5 GHz network, select the **5GHz** button.



Status

BAND	BANDWIDTH	PRIMARY CHANNEL	RX NOISE	RX SNR	RX SIGNAL	SSID	SECONDARY CHANNEL	STATION COUNT
2.4GHz	20MHz	11	-78	78	0	admin	11	0

Current

PERIOD	TX AIRTIME	TX (MBPS)	TX EFFICIENCY	TX PACKET	TX PACKET RETRY	TX PACKET RETRY FAIL	TX RETRY RATE
0 s	0%	0	0%	0	0	0	0%

Last 15 Minutes

PERIOD	TX AIRTIME	TX (MBPS)	TX EFFICIENCY	TX PACKET	TX PACKET RETRY	TX PACKET RETRY FAIL	TX RETRY RATE

Last Hour

PERIOD	TX AIRTIME	TX (MBPS)	TX EFFICIENCY	TX PACKET	TX PACKET RETRY	TX PACKET RETRY FAIL	TX RETRY RATE

Last Day

PERIOD	TX AIRTIME	TX (MBPS)	TX EFFICIENCY	TX PACKET	TX PACKET RETRY	TX PACKET RETRY FAIL	TX RETRY RATE

Last Week

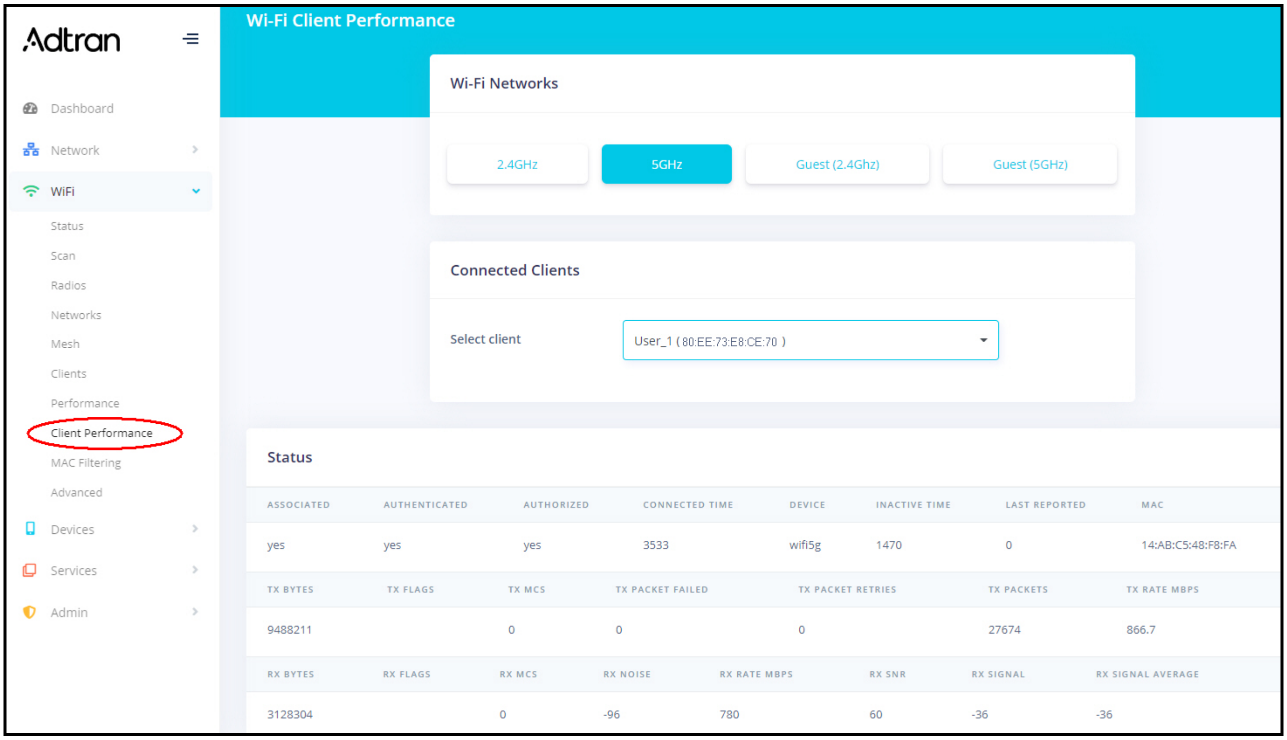
PERIOD	TX AIRTIME	TX (MBPS)	TX EFFICIENCY	TX PACKET	TX PACKET RETRY	TX PACKET RETRY FAIL	TX RETRY RATE

To view detailed information about each network, scroll through the **Current**, **Last 15 minutes**, **Last Hour, Last Day**, and **Last Week sections**.

Viewing Network Status

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

In the left menu, select **WiFi** > **Client Performance**. The Client Performance page appears, showing information for the LAN client devices connected to the 2.4 GHz network. To view details about a different band (5GHz, and Guest [2.4GHz and 5GHz]), select the appropriate button. The example below shows the 5GHZ information.



Wi-Fi Client Performance

Wi-Fi Networks

Connected Clients

Select client: User_1 (80:EE:73:E8:CE:70)

Status

ASSOCIATED	AUTHENTICATED	AUTHORIZED	CONNECTED TIME	DEVICE	INACTIVE TIME	LAST REPORTED	MAC
yes	yes	yes	3533	wifi5g	1470	0	14:AB:C5:48:F8:FA

TX BYTES	TX FLAGS	TX MCS	TX PACKET FAILED	TX PACKET RETRIES	TX PACKETS	TX RATE MBPS
9488211		0	0	0	27674	866.7

RX BYTES	RX FLAGS	RX MCS	RX NOISE	RX RATE MBPS	RX SNR	RX SIGNAL	RX SIGNAL AVERAGE
3128304		0	-96	780	60	-36	-36

7. Configuring Network Services

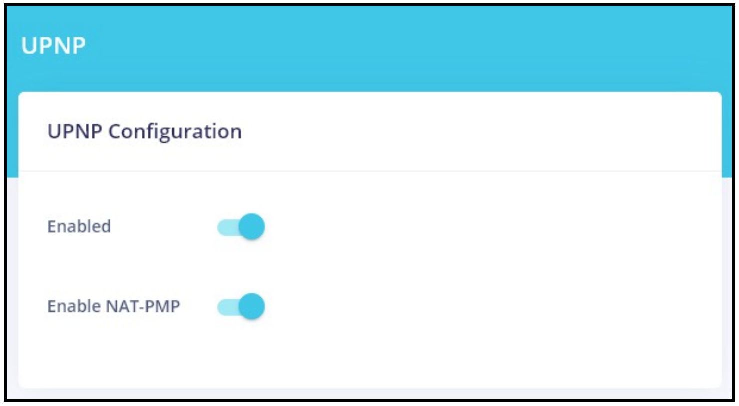
In this chapter, configuration of various services for your network are discussed including

- *UPNP Configuration on page 58*
- *TR-069 Configuration on page 59*
- *SNMP Configuration on page 61*
- *Hosts Configuration on page 62*
- *Dynamic DNS Configuration on page 63*

UPNP Configuration

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, select **Services** > **UPnP**. The following page appears.



UPNP

UPNP Configuration

Enabled

Enable NAT-PMP

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

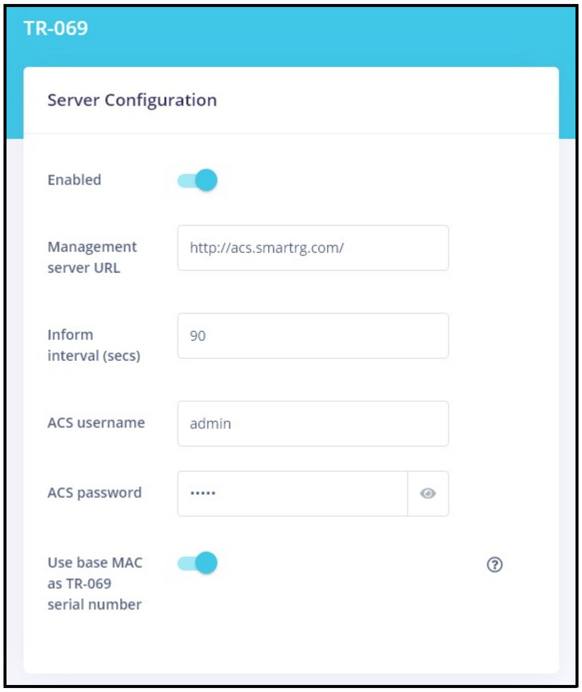
TR-069 Configuration

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

NOTE

To implement any changes made on this page, the SDG must be rebooted after the change is made.

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



TR-069

Server Configuration

Enabled

Management server URL: http://acs.smartrg.com/

Inform interval (secs): 90

ACS username: admin

ACS password: •••••

Use base MAC as TR-069 serial number

2. Management by ACS is enabled by default. To disable this option, select the toggle to the right of **Enabled** near the top of the page.
3. Fill in the fields, using the information in *Table 22*. Values appear in the **Stun Server** section if that feature is configured for your system.
4. To connect to the ACS, in the **Client Configuration** section, select the **Inform now** button.
5. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Table 22. TR-069 Settings for ACS Connectivity

Field	Description
	Server Configuration
Management server URL	Enter the URL of the management server such as http://youracsname.youracsprovider.com.
Inform interval (in secs)	Enter the number of seconds for how often the SDG 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, select the toggle to the right to disable this option.
	Client Configuration
Allow solicit from ACS	This feature is enabled by default. To prevent solicitation transactions from your ACS, select the toggle.
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 Settings
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** through **Unlimited**. The default is **30 seconds**.
Maximum keep alive	The maximum time(in seconds) that the keepalive function should be active. Options are **0** through **Unlimited**. The default is **3600 seconds**.

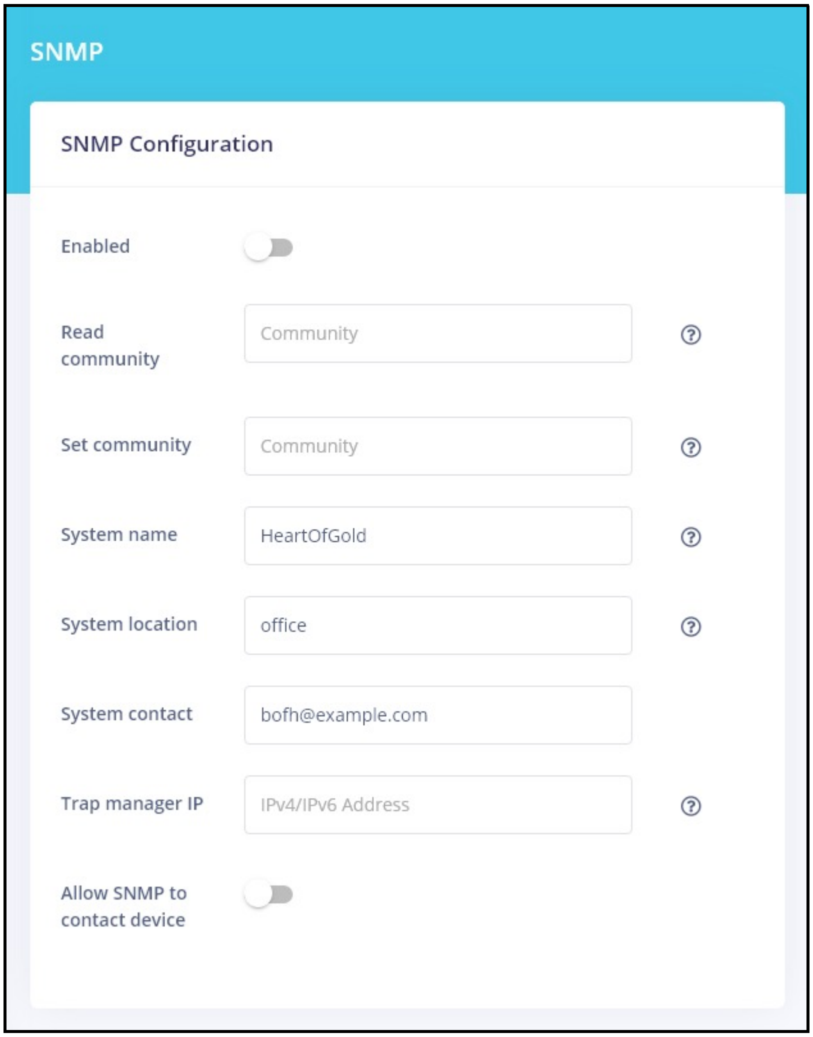
Table 22. TR-069 Settings for ACS Connectivity (Continued)

Field	Description
Server address	The assigned network address of the physical STUN server. The default is **None**. An invalid address will produce an immediate on-screen error message from the SDG. Maximum length is 256 characters.
Server port	The port number associated with your STUN server infrastructure. Options are **0** through **64435**. The default is **19302**.
Username	The user name by which the SDG accesses the STUN infrastructure. Maximum length is 256 characters. Special characters are allowed.

SNMP Configuration

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

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



SNMP

SNMP Configuration

Enabled

Read community: Community

Set community: Community

System name: HeartOfGold

System location: office

System contact: bofh@example.com

Trap manager IP: IPv4/IPv6 Address

Allow SNMP to contact device

2. To enable the SNMP service, select the toggle to the right of **Enabled**.

3. Fill in the fields, using the information in *Table 23*. All fields are optional.

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

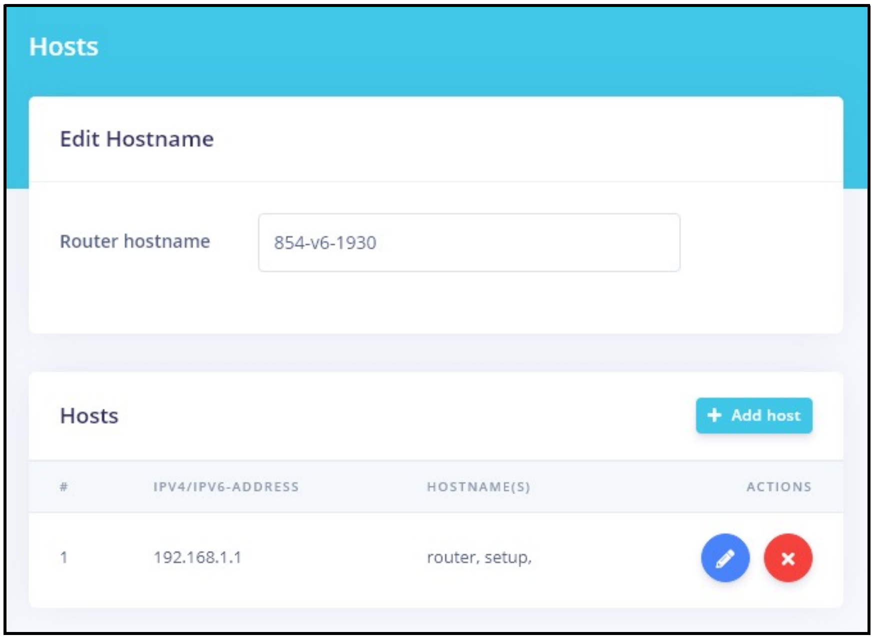
Table 23. SNMP Configuration

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	If desired, modify the name of the SDG.
System location	If desired, 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, select the toggle.

Hosts Configuration

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

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



Hosts

Edit Hostname

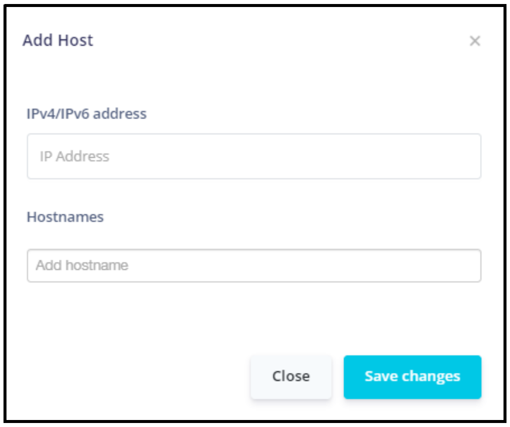
Router hostname: 854-v6-1930

Hosts

#	IPV4/IPV6-ADDRESS	HOSTNAME(S)	ACTIONS
1	192.168.1.1	router, setup,	

2. To add a host:

a. Select 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.

Spaces are not permitted.

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

e. Select **Save changes**.

3. To edit the details of a host:

a. Select the blue edit button next to the host that you want to edit. The **Add/Edit Item** dialog box appears.

b. Modify the fields as needed.

c. Select **Save changes**.

4. To delete a host, select the red delete button to the right of the host that you want to delete.

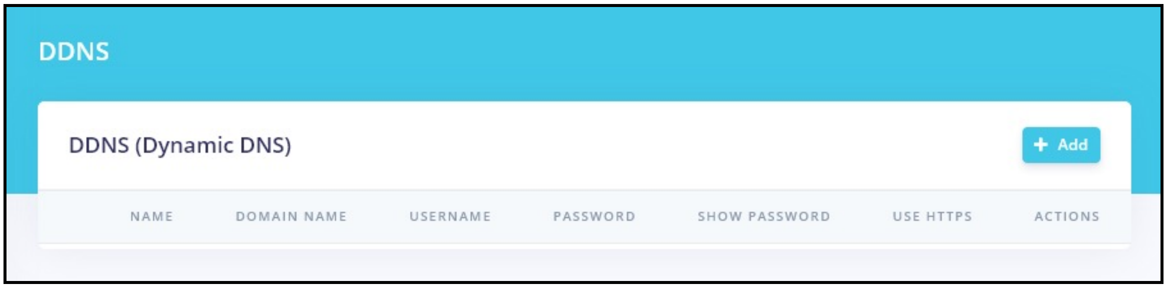
5. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Dynamic DNS Configuration

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

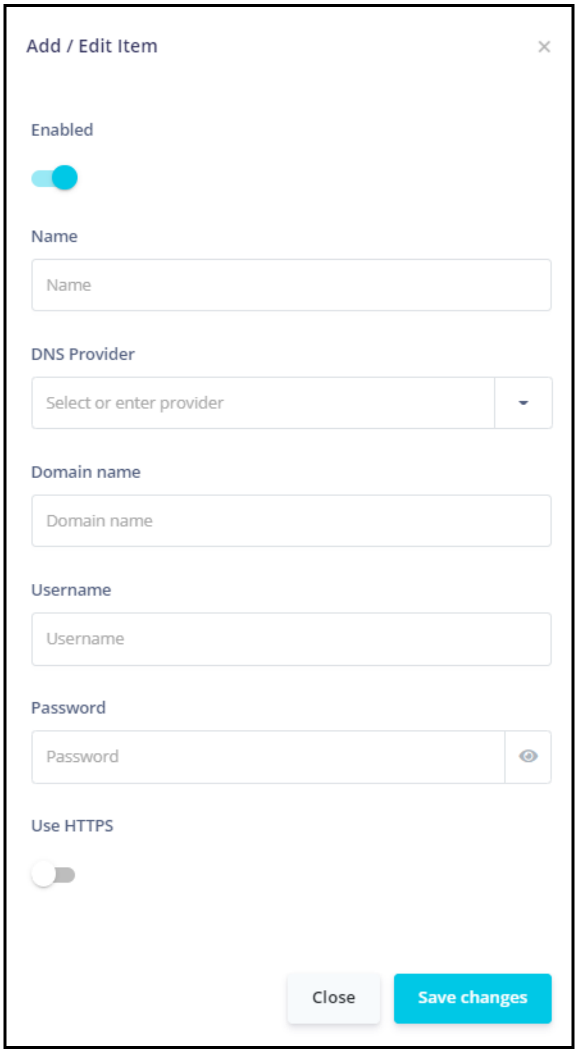
Dynamic DNS allows remote access the router from the Internet using a domain name instead of an IP address. An account on a DDNS service provider is required to implement this feature.

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



2. To add a dynamic DNS server:

   a. Select the **+ Add** button near the upper-right corner. The **Add / Edit Item** dialog box appears.



Add / Edit Item ×

Enabled

Name

Name

DNS Provider

Select or enter provider

Domain name

Domain name

Username

Username

Password

Password

Use HTTPS

   b. Fill in the fields, using the information in *Table 24*.

   c. Select **Save changes**.

3. To edit the details of a server:

   a. Select the blue edit button 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 *Table 24*.

   c. Select **Save changes**.

4. To delete a server, select the red delete button to the right of the server that you want to delete.

5. Select the **Apply** button in the **Pending Changes** dialog box to save your settings.

Table 24. Dynamic DNS Server Configuration Settings

Field Name	Description
Enabled	New server definitions are enabled by default. To *disable* a configuration, select the toggle.
Name	Enter a descriptive name for this entry.
DNS Provider	*(Optional*) Select or enter the URL of your DDNS provider.
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, select the show/hide button (eye icon).
Use HTTPS	(Optional) To *enable* HTTPS security, select this toggle.

VOIP

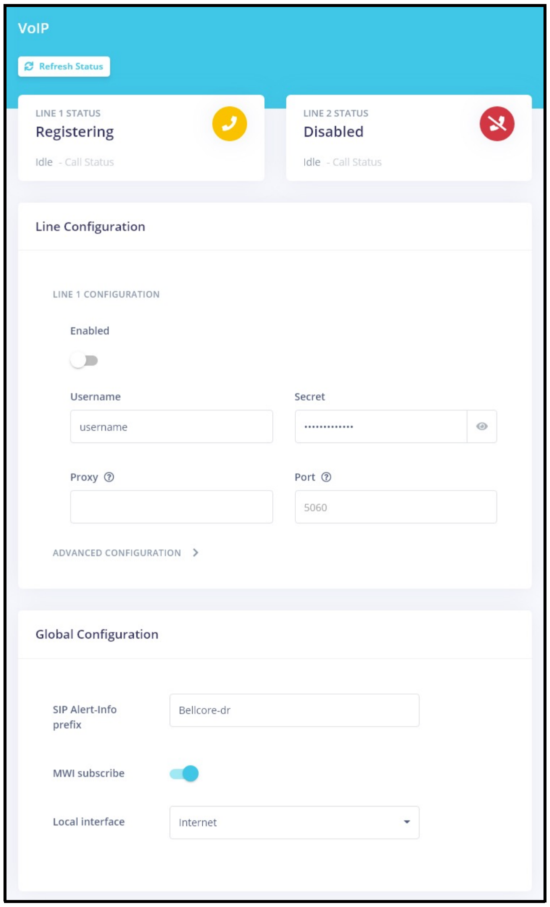
On this page, you can configure Voice over IP settings (VoIP) on supported SDG models.

NOTE

This feature is supported only by VOIP-capable SDG models including the 834-v6 and 854-v6.

Basic Configuration

1. From the left side-menu select, Services > VoIP. The following page appears.



LINE 1 STATUS: Registering
Idle - Call Status

LINE 2 STATUS: Disabled
Idle - Call Status

LINE 1 CONFIGURATION

Enabled: ○

Username: username

Secret: ••••••••••••••

Proxy:

Port: 5060

SIP Alert-Info prefix: Bellcore-dr

MWI subscribe: ●

Local interface: Internet

2. The upper section of the screen displays the current state of the two lines in the **LINE 1 STATUS** and **LINE 2 STATUS** tiles. The status of each line may vary from **Disabled**, **Registering**, and **Up**.

   The **Call Status** display for each port may vary from **Idle**, **Connected,** or **Alerting** to indicate the state of the voice port.

   1. Complete the VoIP configuration using the information in *Table 25*.
   2. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Table 25. VoIP Configuration - Basic

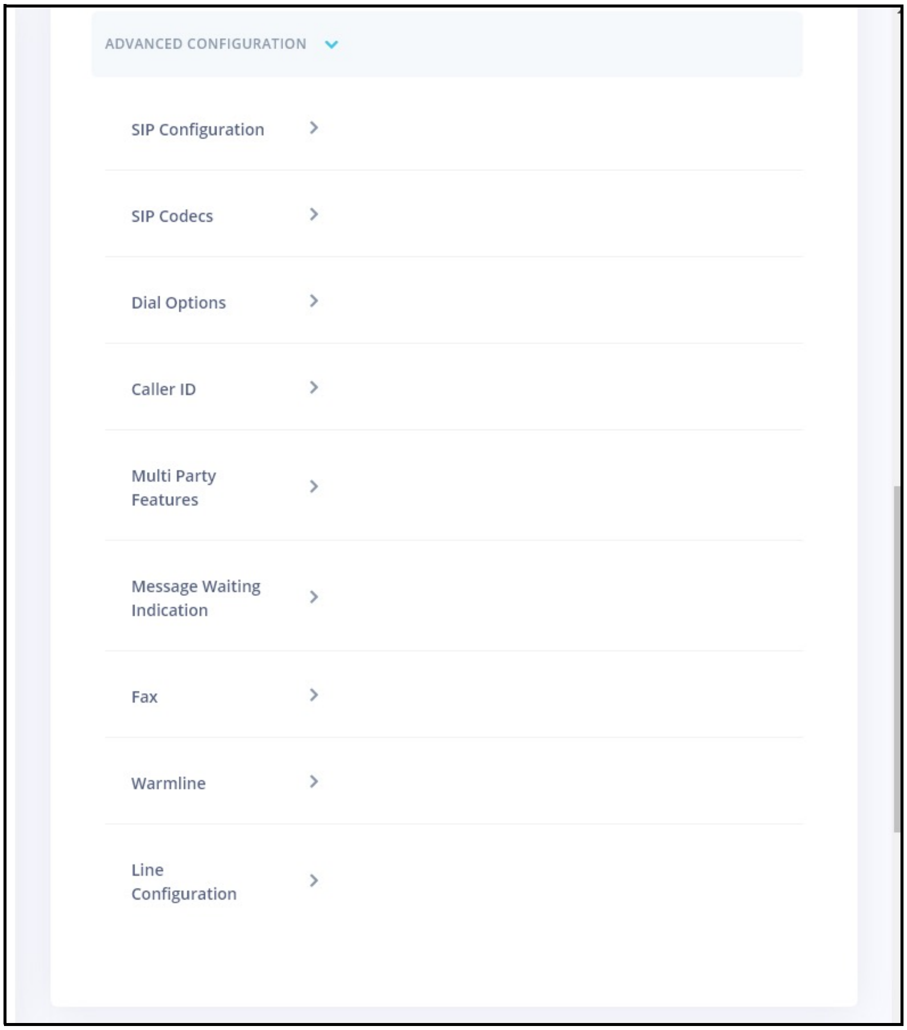
Field Name	Description
LINE 1 and LINE 2 Configuration	
Enabled	Select this toggle to enable this VoIP line on your SDG. You can enable and configure just one line or both lines if needed.
Username	Enter the username for this line of service to access the service provider’s VoIP network.
Secret	Enter the passphrase for this line of service to access the service provider’s VoIP network.
Proxy	Specify the IP or Fully Qualified Domain Name (FQDN) of a record or SRV record.
Port	Specify the Port Number. Leave this field blank for SRV lookups. Default value is 5060.

Table 25. VoIP Configuration - Basic (Continued)

Field Name	Description
Global Configuration	
SIP Alert Info Prefix	String prefix in SIP INVITE Alert-Info header used for distinctive ring. Allows the user to define a string to match what the softswitch is sending.
MWI Subscribe	Toggle on to have SIP SUBSCRIBE request for MWI service in the case of solicited or unsolicited SIP NOTIFY. Usually defer to softswitch setting.
Local Interface	Select Internet or Voice to choose which VLAN/Interface to send/receive VoIP traffic.

Advanced Configuration

When detailed VoIP configuration is required, expand the ADVANCED CONFIGURATION section toward the middle of the VoIP page. Additional settings are available here to customize the voice behavior of the SDG. The additional settings are categorized under sections titled SIP Configuration, Codecs, Dial Options, Caller ID, Multi Party Features, Message Waiting Indication, Fax, Warmline, and Line Configuration.



1. Complete the sections under Advanced Configuration using the information in *Table 26*.

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

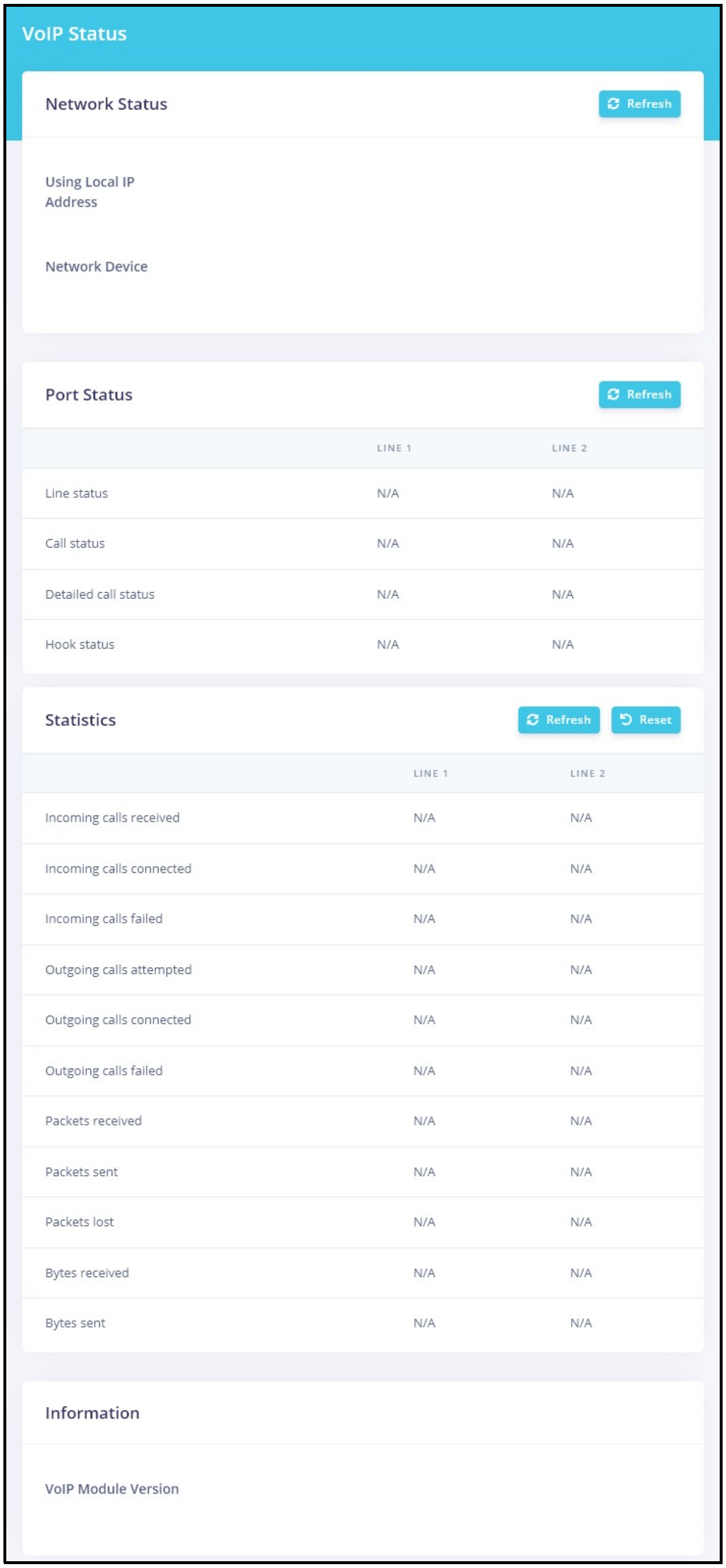
Table 26. VoIP Configuration - Advanced

Field Name	Description
SIP Configuration	
Domain	Specify the domain name for SIP users.
Auth Username	Specify the username that will be required as authentication for registration to the SIP server.
Outbound proxy	Specify the FQDN or IP address of the outbound proxy server to which all SIP messages are sent.
Registrar	Specify the FQDN or IP address of the SIP registrar server. This entry is required for SRV failover..
Registrar port	Specify the UDP port number of the registrar server. Default value is 5060. **Note:** If this port exists, SRV lookups will be automatically disabled. SRV lookups require the user does not provide SIP port information.
Registration expiration	Specify the duration of the registration that is requested in the REGISTER sent to the SIP server. Default value is 3600.
PRACK	Toggle on to enable Provisional Response Acknowledgment (PRACK). Enabling PRACK adds 100rel option tag in the SIP 18x response. If the user agent (UA) is in the User Agent Server (UAS) role, the 1XX response will include ‘Require:100rel’. For User Agent Client (UAC), PRACK is always supported. UAS will reply with PRACK when a 1XX response is received with ‘Require:100rel’.
Session max timer	Enter the maximum amount of time that can occur between session refresh requests in a dialog before the session will be considered timed out. Note: This is the RFC 4028 session expiration. Supports UPDATE method. Leave blank to disable session refresher.
Session min timer	Enter the minimum time for the session interval.
Session refresher	Specify whether the UAC or UAS sends the session refresher.
SIP Codecs	
Select the toggle adjacent to each CODEC to enable or disable them as needed for your environment. For the enabled CODEC, a priority must be chosen to indicate the likelihood of which CODEC will be utilized to facilitate the voice services. A priority selection of 1 indicates this CODEC will most likely be used when it is supported by the rest of the infrastructure supporting the call. If the priority 1 CODEC is not supported end-to-end, the SDG will shift to the priority 2 CODEC and so forth. The **G.711 Mu-Law** codec is enabled by default and may not be turned off. Other, optional CODECs include **G.726**, **G.111 A-Law** and **G.728**.	
Dial Options	
Digit map	The default map is *xx.T|x.T. Digit ‘#’ terminates dialing unless it matches a pattern in the digit map (e.g., service code #21#)
Start digit timer	Specifies the maximum amount of time allowed to begin entering a digit sequence. Default value is 16 seconds.
Short digit timer	Specifies the maximum amount of time allowed between dialed digits, when at least one viable digit sequence is completed as dialed. Also known as the interdigit timout. Default value is 16 seconds.

Table 26. VoIP Configuration - Advanced (Continued)

Field Name	Description
Long digit timer	Specifies the maximum amount of time allowed between dialed digits, when no viable digit sequence has been entered yet. Default value is 16 seconds.
DTMF relay	Specify the method by which dual- tone multi-frequency (DTMF) events are relayed. Inband - DTMF events are relayed inband in the RTP stream. OOB using named telephone events (NTE) - not sure if this is RFC 2833 or INFO. Select inband, INFO, or RFC 2833.
Caller ID	
Local CID	Toggle on to enable the generation of the CID signal locally.
Outgoing CID	Toggle on to enable ‘Outgoing CID Name’ appended to the ‘From’ SIP header. May be overridden by the softswitch.
Outgoing CID Name	Enter the name for the outgoing Caller ID.
Multi-Party Features	
3-Way conference	Toggle off to have flash-hook services handled by the softswitch (e.g., Metasphere)
Call waiting	Toggle off to disable call waiting.
Flash Relay Mode	Select Disabled, SIP INFO (out of band), or RFC-2833 (in-band via RTP). Applicable when 3-WAY conference is disabled. Follows DTMF Relay if DTMF relay is INFO.Disabled if DTMF relay is disabled.
Message Waiting Indication	
AMWI	Toggle on to enable stutter dial tone MWI indication
VMWI	Toggle on to generate MWI FSK signal to the CPE.
Fax	
T.38 fax relay	Toggle on to enable T.38 fax relay.
Warmline	
Warmline	Toggle on to enable warmline.Warmline calls a set destination after a phone has been off-hook for longer than the time specified for the warmline timer.
Warmline number	Enter the destination number to call.
Warmline timer (sec)	Enter the warmline timeout. Default is **8 seconds**.
Line Configuration	
RX gain (dB)	Select the RX gain for the line. Range is 0 to -12dB. Default value is **-9dB**.
TX gain (dB)	Select the TX gain for the line. Range is 0 to -12dB. Default value is **-3dB**.

Statistics



VoIP Status

Network Status

Using Local IP Address

Network Device

Port Status

	LINE 1	LINE 2
Line status	N/A	N/A
Call status	N/A	N/A
Detailed call status	N/A	N/A
Hook status	N/A	N/A

Statistics

	LINE 1	LINE 2
Incoming calls received	N/A	N/A
Incoming calls connected	N/A	N/A
Incoming calls failed	N/A	N/A
Outgoing calls attempted	N/A	N/A
Outgoing calls connected	N/A	N/A
Outgoing calls failed	N/A	N/A
Packets received	N/A	N/A
Packets sent	N/A	N/A
Packets lost	N/A	N/A
Bytes received	N/A	N/A
Bytes sent	N/A	N/A

Information

VoIP Module Version

Cabling and Pinout

The VoIP-capable SDG models are equipped with an RJ-11 port on the back panel of the device. If a POTS device is required for your installation, use an RJ-11 cable (not included) to connect the telephony device to the SDG’s port labeled **Tel 1/2** on the rear of the 834-v6 or 854-v6.

A “Y” cable will be required to connect two individual telephone sets or individual, single line POTS ports on a Private Branch Exchange (PBX) or Key System Unit (KSU). However, your PBX or KSU may be equipped with ports conforming to the RJ-11 standard as described above. Consult the PBX / KSU vendor’s documentation to confirm cabling requirements.

8. Managing Connected Devices

In this chapter, management of your connected LAN devices is discussed and broken down as follows

- *Mesh (Intellifi) Devices on page 71*
- *LAN-Connected Devices on page 75*

Mesh (Intellifi) Devices

In this section, configuration and management of your mesh network is discussed and broken down as follows:

- *Viewing Connected Devices (Device Map) on page 71*
- *Managing Satellite Devices (Mesh Extenders) on page 73*
- *Pausing Mesh Network Access on page 74*

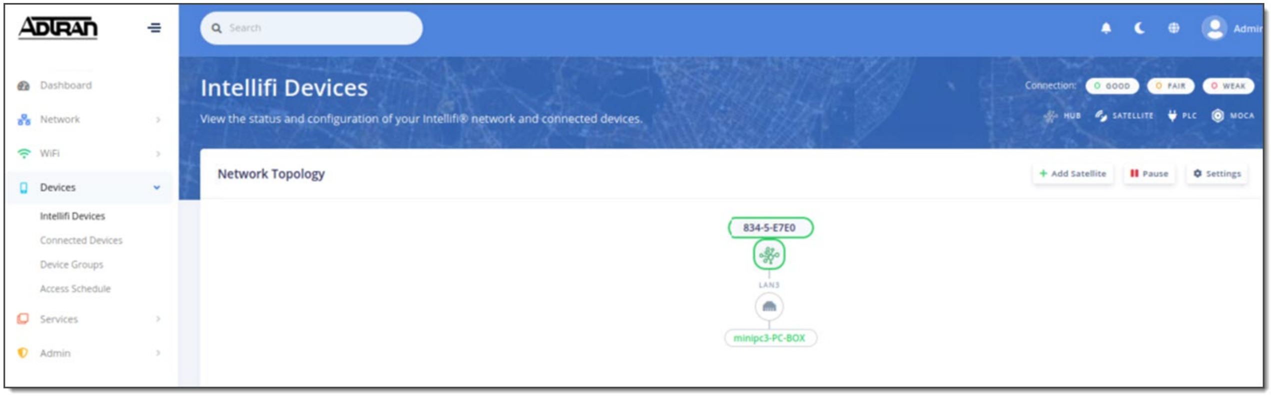
Viewing Connected Devices (Device Map)

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

NOTE

To extend the network, a satellite can be linked to another satellite.

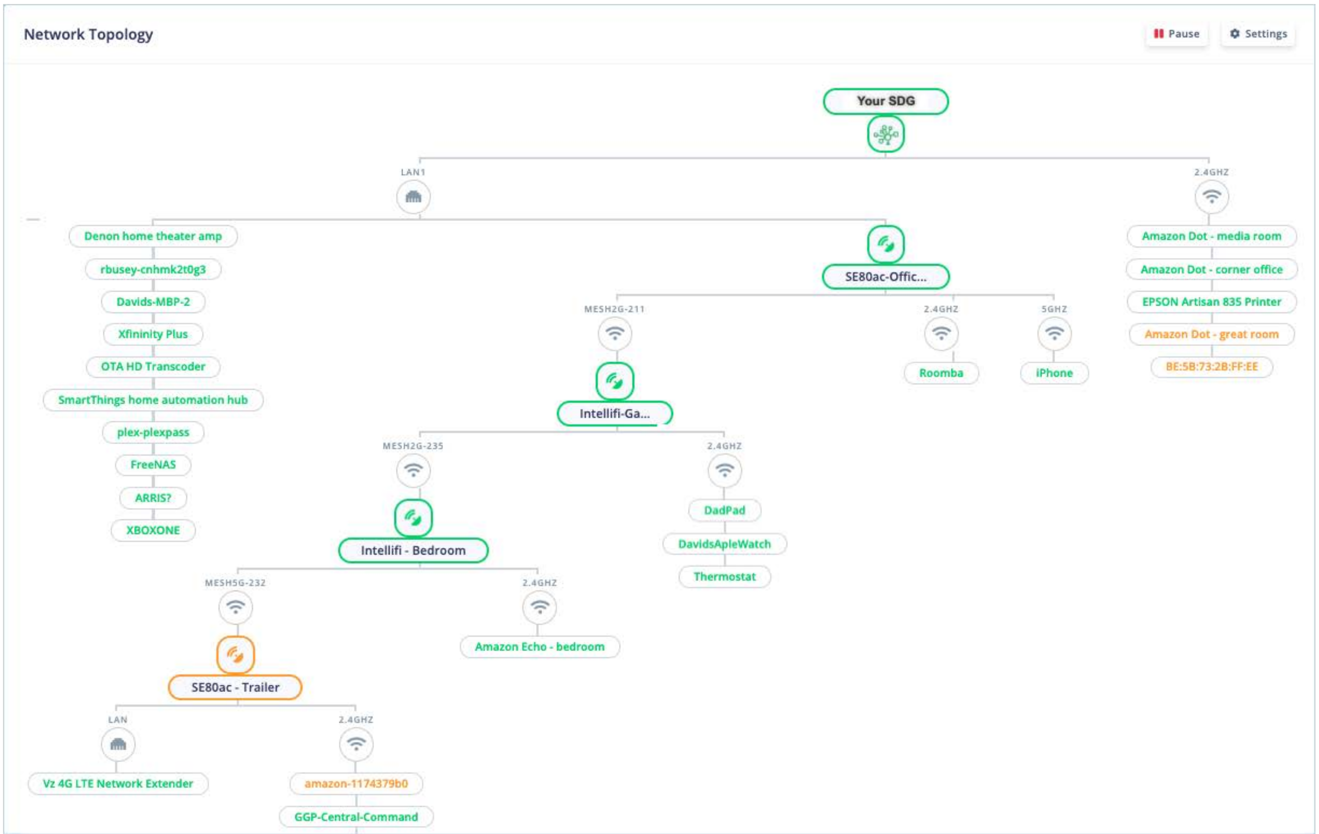
1. In the left menu, select **Devices** > **Intellifi Devices**. The following page appears, showing a diagram of the connected devices.Connection status and device type legends appear at the top right.



Intellifi Devices

View the status and configuration of your Intellifi® network and connected devices.

If a LAN device is connected via wireless, the WiFi band information appears as the name instead of LAN or WAN. The device colors identify the device status. The **Connection** 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. Select the **Settings** button at the top right of the **Network Topology** section. The **Topology Settings** dialog box appears.

   b. Select the toggle below **Show Detailed View** and then select **Save Changes**.

3. To change the refresh interval:

   a. Select the **Settings** button at the top right of the **Network Topology** section. The **Topology Settings** dialog 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. Select **Save Changes**.

4. To pause traffic with the Intellifi network, select the **Pause** button to the right of the **Network Topology** heading. The **Pause** button changes to a **Play** button. Select the **Play** button to restart traffic.

5. To view details of a device, select the device label. The **DEVICE DETAILS** pane appears.

   You can edit the host name, select the IP address to log into the device, or expand the **CONNECTION DETAILS** or **INTERNET ACCESS** sections to access other functions. For detailed information about the available information and functions, see Accessing Device Information below.

6. When finished, close the pane.

Managing Satellite Devices (Mesh Extenders)

Device Pairing

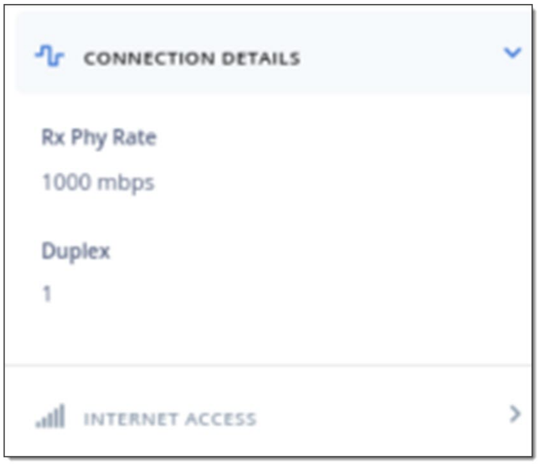
You can add satellites (mesh extenders) to your Intellifi network.

1. Select the **View Intellifi topology** button at the top right.
2. Select the **Add Satellite** button at the top right of the **Network Topology** section. The **Pair a new Intellifi Satellite** wizard appears.
3. Follow the on-screen, self-guiding prompts, selecting the **Continue to next step** button to proceed.
4. On the **Start pairing** pane, you can choose to pair the satellite device using a wired connection. Do either of the following:
   - To use a wired connection, select the **Or pair using a wired connection** link.
   - To continue with wireless pairing, select the **GO** button.

   Once pairing is completed, a **checkmark** appears on the **Finish pairing** pane.
5. Close the pane.

Viewing Device Settings

1. Select the **View Intellifi topology** button at the top right.
2. Select the label for the LAN device you want to work with. The device information pane appears to the right.
3. To view the connection details, select **CONNECTION DETAILS** to expand the pane. The transmission rates and signal data are shown.



CONNECTION DETAILS

Rx Phy Rate

1000 mbps

Duplex

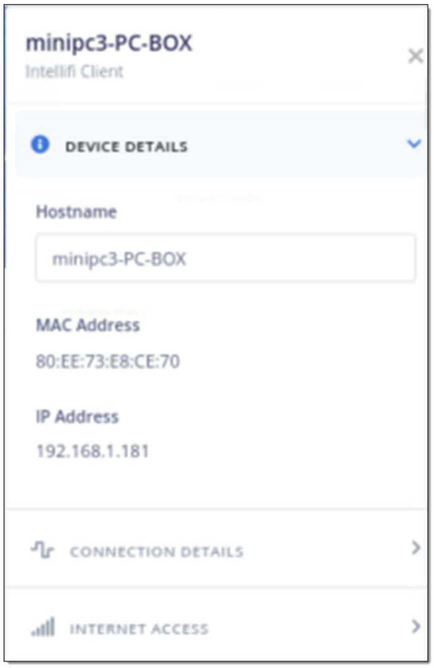
1

INTERNET ACCESS

To view the device's host name, MAC address, and IP address follow these steps:

1. Select the **View Intellifi topology** button at the top right.
2. Select the device label in the topology diagram. The details pane opens to the right.

3. Select **DEVICE DETAILS**. The **DEVICE DETAILS** pane expands.



minipc3-PC-BOX
Intellifi Client

Hostname
minipc3-PC-BOX

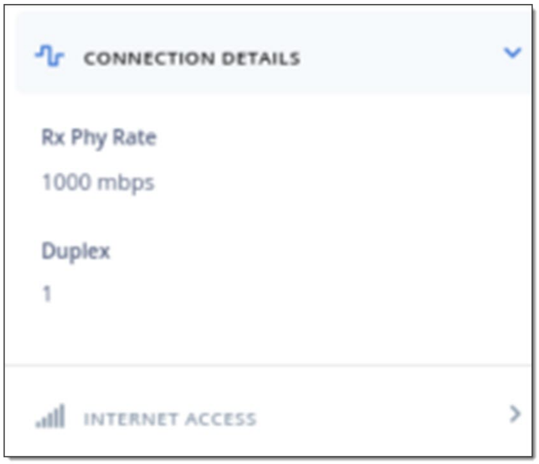
MAC Address
80:EE:73:E8:CE:70

IP Address
192.168.1.181

4. You can edit the host name or select the IP address to log into the device and view status and statistics.

Viewing Connection Details

1. Select the label for the device you want to work with. The device information pane appears to the right.
2. To view the connection details, select **CONNECTION DETAILS** to expand the pane. The transmission rates and signal data are shown.



Rx Phy Rate
1000 mbps

Duplex
1

Pausing Mesh Network Access

Pausing Intellifi Network

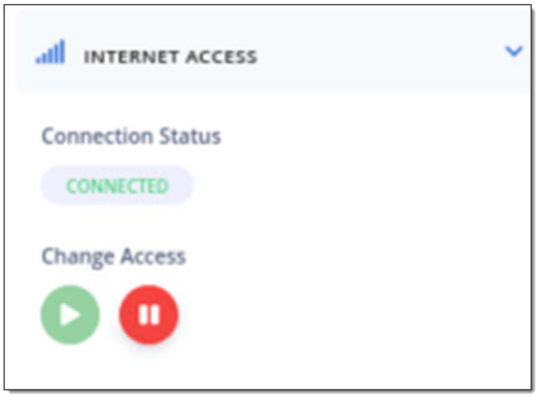
To pause the entire Intellifi network from accessing the Internet, select the **Pause** button at the top right of the **Network Topology** section. The network access is paused.

To restart the network, select the **Pause** button again.

Pausing Device Internet Access

You can pause access to the Internet for an individual LAN device and a specified duration.

1. Select the label for the device you want to work with. The device information pane appears to the right.
2. Select **INTERNET ACCESS** to expand the pane. The access details are shown.



3. Select the red pause button. The **Set Timeout(ms)** field appears.
4. Select a time period. Option are **15 minutes** - **1 day**. Your selection appears in milliseconds.
5. Select the red pause button below the field. The play button becomes active.
6. To resume Internet access for this LAN device, select the green play button.
7. Close the device details pane.

LAN-Connected Devices

In this section, configuration and management of your LAN client devices is discussed and broken down as follows:

- *Viewing Connected Devices on page 75*
- *Managing Connected Devices on page 76*
- *Pausing Internet Access on page 82*

Viewing Connected Devices

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

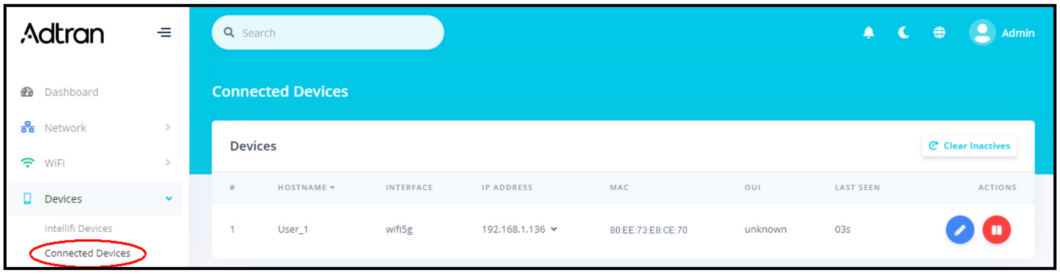
NOTE

Before assigning a device to a group, an access schedule must be configured, 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 access to the LAN as well. This in turn prevents logging in to the SDG 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 groups to ensure that a means to modify access schedules, device groups and timeout periods is preserved.

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

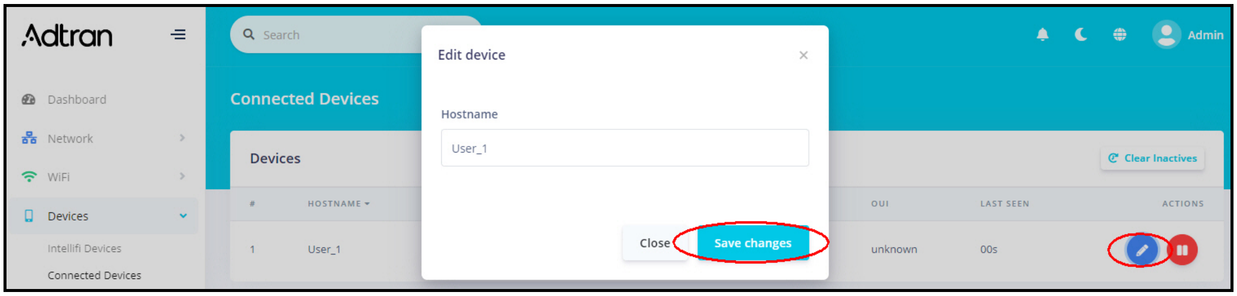


Connected Devices

Devices

#	HOSTNAME	INTERFACE	IP ADDRESS	MAC	OUI	LAST SEEN	ACTIONS
1	User_1	wifi5g	192.168.1.136	80:EE:73:E8:CE:70	unknown	03s	

2. Refresh the list to show only active devices by clicking the **Clear Inactives** button above the table on the right.
3. To edit the host name for a device:
    a. Select the blue **Edit** icon next to the device you want to edit. The **Edit Device** dialog box appears.



Connected Devices

Devices

Edit device

Hostname: User_1

#	HOSTNAME	OUI	LAST SEEN	ACTIONS
1	User_1	unknown	00s	

    b. Enter the desired host name.
    c. Select **Save changes**.
4. To pause access for a device temporarily:
    a. Select the red pause button 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** through **60 minutes**, **2** through **8 hours**, and **1 day**. Your selection displays in milliseconds.
    c. Select **Save changes**. The pause button is replaced by the play button.
5. To restart access, select the green play button to the right of the line item for which you wish to resume Internet access. The red pause button re-appears.

Managing Connected Devices

The series of features discussed in this section enable you to create groupings of LAN devices to help make management of the devices more efficient.

Along with creating device groups, you'll learn how to assign devices to groups, delete groups, and assign access schedules to groups.

> **NOTE**
>
> *Before you can assign a device to a group, an access schedule must be configured, then configure a device group, and finally assign the schedule to the group. Each of these procedures is discussed immediately below.*

⚠ **WARNING!**

Pausing access for LAN devices not only restricts access to the Internet but access to the LAN as well. This in turn prevents you from logging in to the SDG 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 groups to ensure that a means to modify access schedules, device groups and timeout periods is preserved.

Learn more using the links below.

- *Creating a Schedule on page 77*
- *Creating a Device Group and Adding Devices on page 79*
- *Applying an Access Schedule to a Device Group on page 81*

Creating a Schedule

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

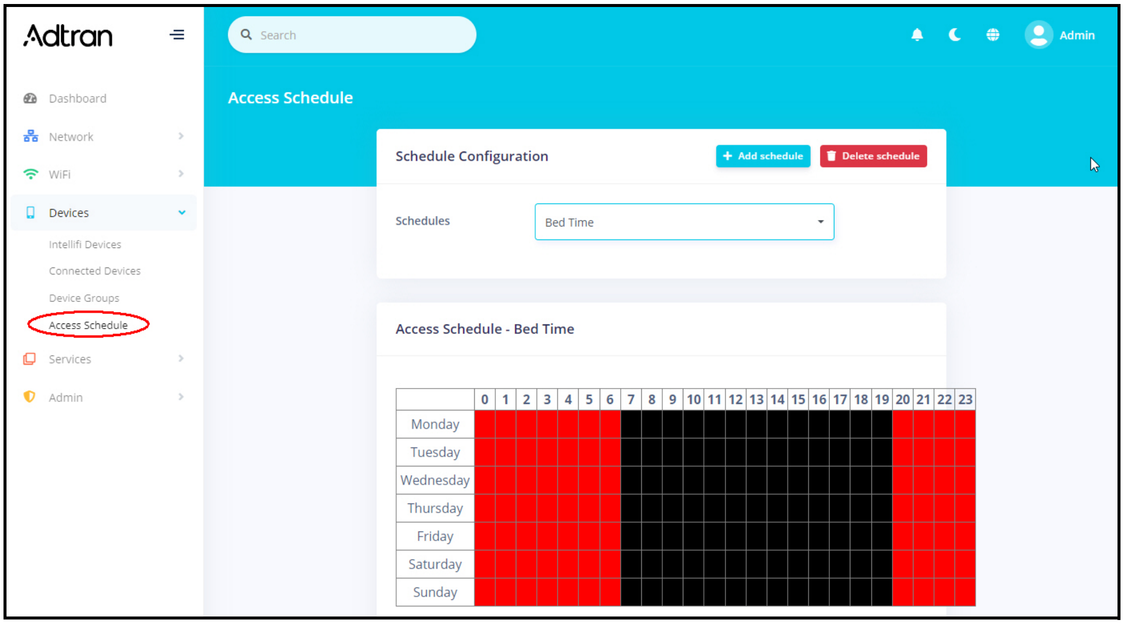
NOTE

Make sure that the time zone is set correctly for this SDG before configuring an access schedule. You can access the **Timezone** *setting on the* **Admin** > **Time** *page in the GUI. Instructions are provided in Specifying Time Settings on page 90.*

⚠ **WARNING!**

Pausing access for LAN devices not only restricts access to the Internet but access to the LAN as well. This in turn prevents you from logging in to the SDG 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 groups to ensure that a means to modify access schedules, device groups and timeout periods is preserved.

1. In the left menu, select **Devices** > **Access Schedule**. The following page appears. Two default schedules exist in the system: **Bed Time** and **School Nights**.



Access Schedule

Schedule Configuration

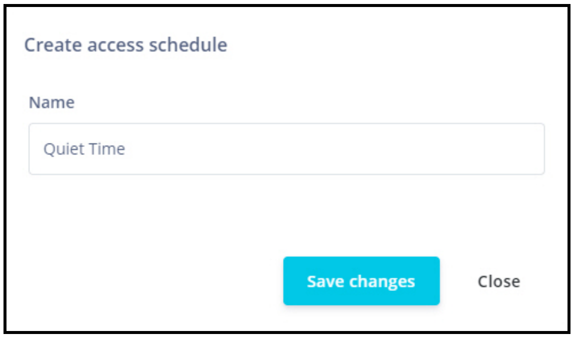
Schedules: Bed Time

Access Schedule - Bed Time

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Monday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	🟥	🟥	🟥	🟥
Tuesday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	🟥	🟥	🟥	🟥
Wednesday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	🟥	🟥	🟥	🟥
Thursday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	🟥	🟥	🟥	🟥
Friday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	🟥	🟥	🟥	🟥
Saturday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	🟥	🟥	🟥	🟥
Sunday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	🟥	🟥	🟥	🟥

2. You can modify the existing default schedules or create a new access schedule. To create a new schedule:

   a. Select the **Add schedule** button at the top right. The **Create access schedule** dialog box appears.



Create access schedule

Name: Quiet Time

   b. Enter a descriptive name for the new schedule and select **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.

   c. 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.

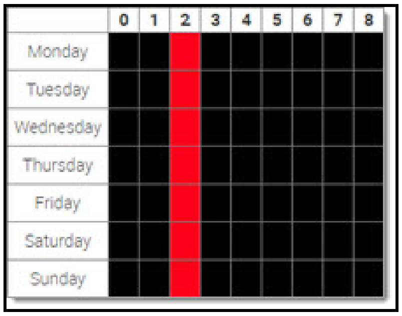
   For example, to prevent access between 2 am and 3 am, enter “0200” in the first (start) field and “0259” in the second (end) field for either every day (daily) or specific days. The grid refreshes and displays red, indicating that access is blocked for the 2:00 hour.

   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.

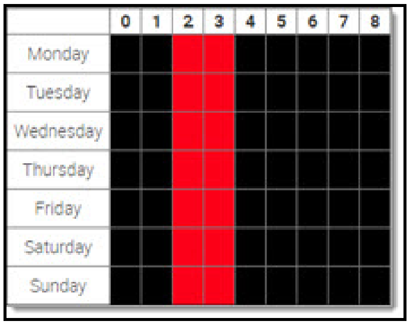
   d. To add another blocked period for the same day, enter values in the **2nd** and **3rd time** fields.

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



	0	1	2	3	4	5	6	7	8
Monday	⬛	⬛	🟥	⬛	⬛	⬛	⬛	⬛	⬛
Tuesday	⬛	⬛	🟥	⬛	⬛	⬛	⬛	⬛	⬛
Wednesday	⬛	⬛	🟥	⬛	⬛	⬛	⬛	⬛	⬛
Thursday	⬛	⬛	🟥	⬛	⬛	⬛	⬛	⬛	⬛
Friday	⬛	⬛	🟥	⬛	⬛	⬛	⬛	⬛	⬛
Saturday	⬛	⬛	🟥	⬛	⬛	⬛	⬛	⬛	⬛
Sunday	⬛	⬛	🟥	⬛	⬛	⬛	⬛	⬛	⬛

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



	0	1	2	3	4	5	6	7	8
Monday	⬛	⬛	🟥	🟥	⬛	⬛	⬛	⬛	⬛
Tuesday	⬛	⬛	🟥	🟥	⬛	⬛	⬛	⬛	⬛
Wednesday	⬛	⬛	🟥	🟥	⬛	⬛	⬛	⬛	⬛
Thursday	⬛	⬛	🟥	🟥	⬛	⬛	⬛	⬛	⬛
Friday	⬛	⬛	🟥	🟥	⬛	⬛	⬛	⬛	⬛
Saturday	⬛	⬛	🟥	🟥	⬛	⬛	⬛	⬛	⬛
Sunday	⬛	⬛	🟥	🟥	⬛	⬛	⬛	⬛	⬛

3. To change a schedule, select it in the **Access Schedule** field and modify the fields.
4. To delete a schedule, select it in the **Access Schedule** field and select the **Delete schedule** button (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.*

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

Creating a Device Group and Adding Devices

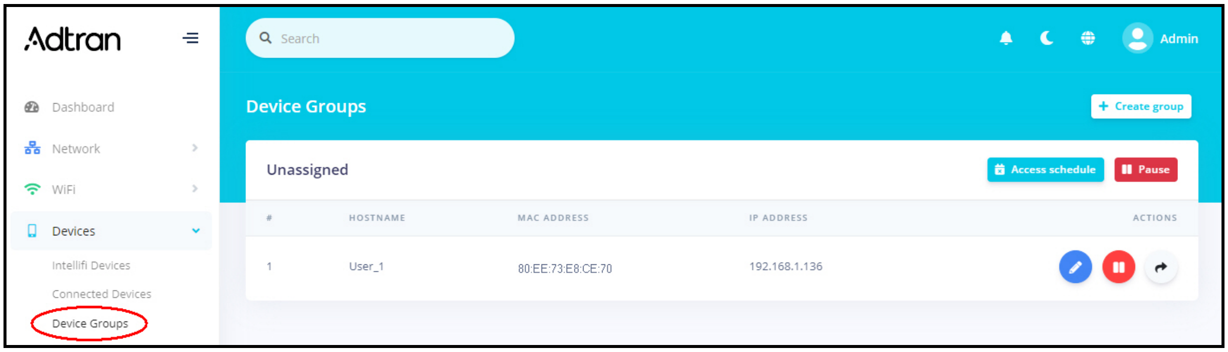
On this page, you can create device groups, assign devices to groups, pause access for devices, delete groups, and assign schedules to groups.

> **NOTE**
>
> *Before you can assign a device to a group, an access schedule must be configured, 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 access to the LAN as well. This in turn prevents you from logging in to the SDG 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 groups to ensure that a means to modify access schedules, device groups and timeout periods is preserved.

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



#	HOSTNAME	MAC ADDRESS	IP ADDRESS	ACTIONS
1	User_1	80:EE:73:E8:CE:70	192.168.1.136	

NOTE

The unassigned (default) group cannot be deleted or renamed. You can, however, assign a schedule and pause/restart it.

2. To add a new device group:

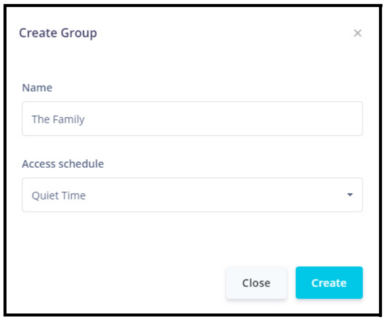
   a. Select the **Create group** button at the upper right. The **Create Group** dialog box appears.

   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.

   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 and select it.

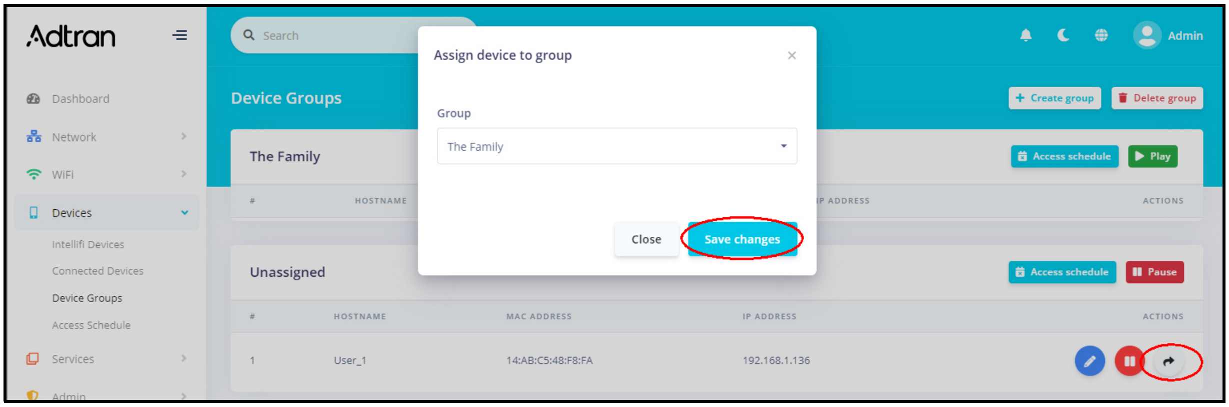
   d. Select **Create**. The new group appears on the page and a **Delete group** button appears at the top right.



Name: The Family

Access schedule: Quiet Time

3. To add a device to a group:
    a. Select the **black arrow** button at the far right next to the device that you want to add to a device group. The **Assign device to group** dialog box appears.



Assign device to group

Group: The Family

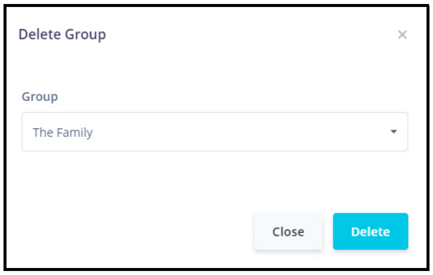
#	HOSTNAME	MAC ADDRESS	IP ADDRESS	ACTIONS
1	User_1	14:AB:C5:48:F8:FA	192.168.1.136	

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

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

    c. Select **Save changes**.

4. To delete a device group:
    a. Select the **Delete group** button at the top of the device pane. The **Delete Group** dialog box appears.



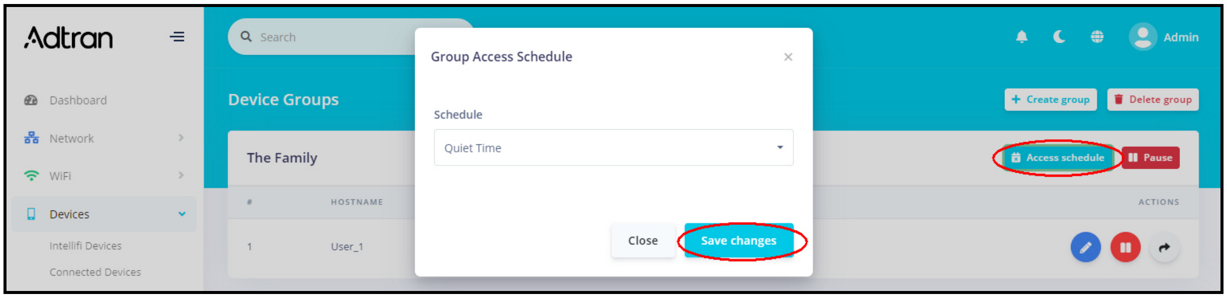
Delete Group

Group: The Family

    b. Select the group to be deleted from the drop-down list.
    c. Select **Delete**.
    d. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Applying an Access Schedule to a Device Group

1. To change or apply an access schedule to a device group, select the **Access schedule** button to the right of the name of the device group.



Group Access Schedule

Schedule: Quiet Time

#	HOSTNAME	ACTIONS
1	User_1	

a. Select the name of the schedule you wish to apply. Select **Save changes**.

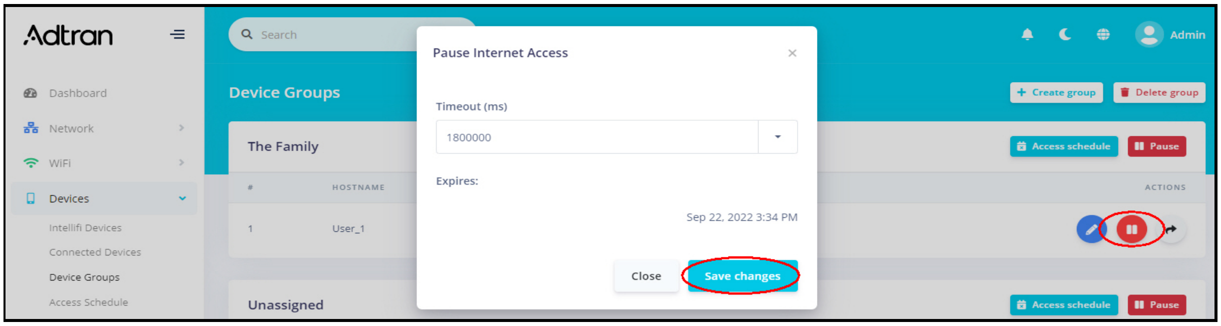
If you do not see the schedule that you want, go to the **Devices** > **Access Schedule** page and create it. Then, return to this page and select it.

Pausing Internet Access

Internet Access can be paused for a single device or an entire device group.

You can pause Internet Access for a single device from either the **Connected Devices** page or the **Device Groups** page.

1. You can pause Internet Access for a single device from either the **Connected Devices** page or the **Device Groups** page. To pause Internet Access, select the red pause button at the far right next to the device you want to pause.



Pause Internet Access

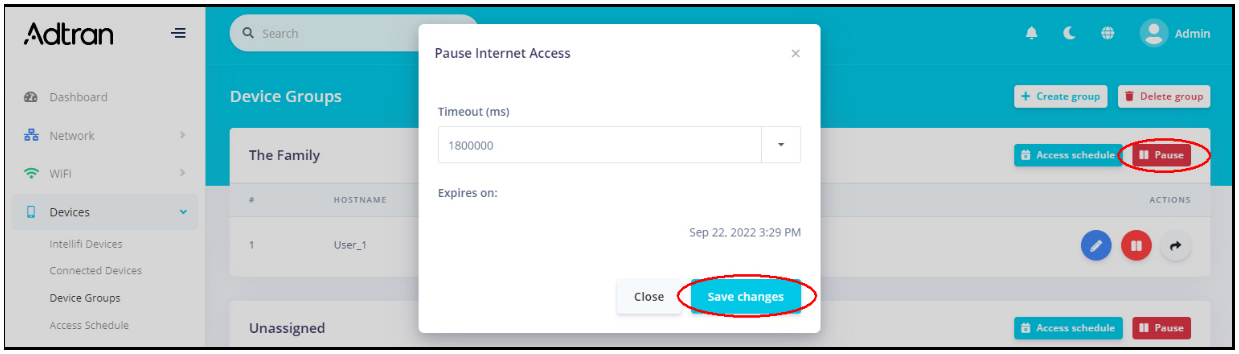
Timeout (ms): 1800000

Expires: Sep 22, 2022 3:34 PM

   a. Select how long you want Internet access paused. Options are **None**, **15** through **60 minutes**, **2** through **8 hours**, and **1 day**. Your selection displays in milliseconds.

   b. Select **Save changes**.

2. You can pause Internet Access for a device group by selecting the pause button at the far right next to the name of the device group you wish to pause.



Pause Internet Access

Timeout (ms): 1800000

Expires on: Sep 22, 2022 3:29 PM

   a. Select how long you want Internet access paused. Options are **None**, **15** through **60 minutes**, **2** through **8 hours**, and **1 day**. Your selection displays in milliseconds.

   b. Select **Save changes**.

9. Managing System Settings

The series of features discussed in this section govern general system-wide settings on your SDG and other general utilities including:

- *Updating SDG Firmware on page 83*
- *Managing System Configurations on page 85*
- *Configuring SDG HTTP Settings on page 86*
- *Managing System Passwords on page 87*
- *Performing a Speed Test on page 88*
- *Testing Network Connectivity (Ping and Traceroute) on page 88*
- *Configuring System Logs on page 89*
- *Specifying Time Settings on page 90*
- *Specifying SDG Operating Mode on page 91*
- *Rebooting the SDG on page 91*

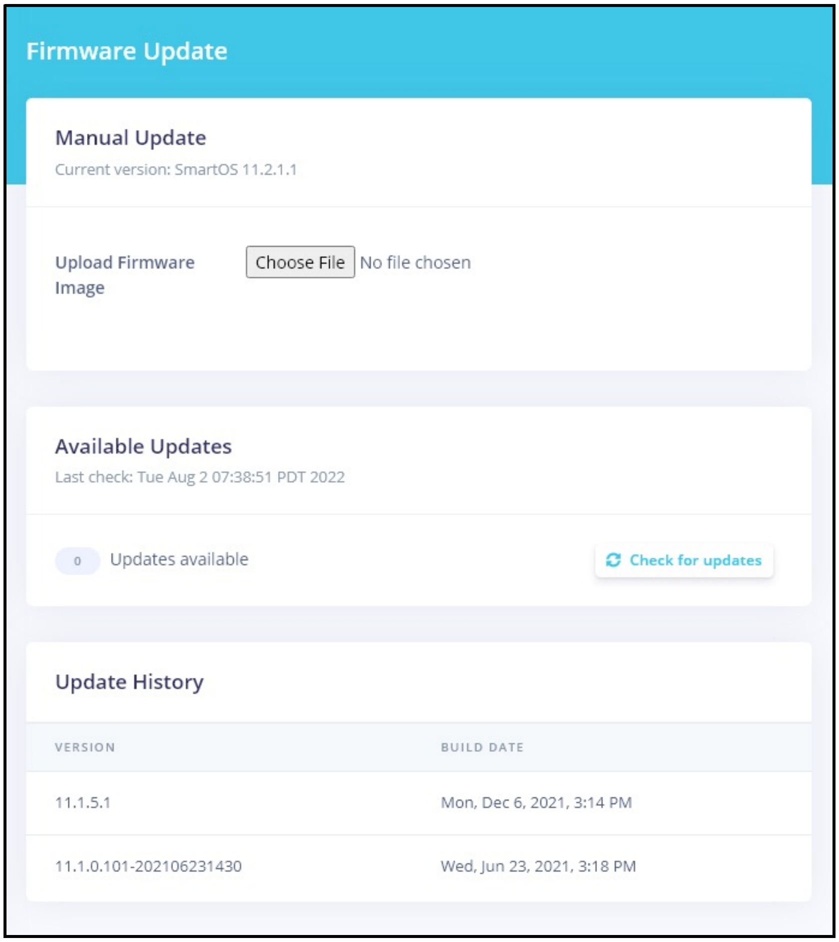
Updating SDG Firmware

On the **Update** page, you can update the firmware of your SDG. Software updates are available for download from the Adtran Support Community site.

NOTE

Following a firmware upgrade, the SDG automatically reboots. Allow for approximately 6 minutes of down time for the reboot to complete.

In the left menu, select **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.



Firmware Update

Manual Update

Current version: SmartOS 11.2.1.1

Upload Firmware Image [Choose File] No file chosen

Available Updates

Last check: Tue Aug 2 07:38:51 PDT 2022

0 Updates available

Update History

VERSION	BUILD DATE
11.1.5.1	Mon, Dec 6, 2021, 3:14 PM
11.1.0.101-202106231430	Wed, Jun 23, 2021, 3:18 PM

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

1. To update firmware manually:
   a. In the **Manual Update** section, select **Browse**. An **Open** or **File Upload** dialog box appears.
   b. Navigate to and select the firmware image file to be installed and then select **Open**. A progress bar and a **Cancel** button appears. When the file has completed loading, the **Start Upgrade** button appears.
   c. Select **Start Upgrade**. The **Please wait** popup appears, showing the **Upgrading** progress bar.

If the failed message appears, select the message to clear it. Then try downloading the file again and repeat the above steps.

2. To check for available updates:
   a. In the **Available Updates** section, select the **Check for updates** button. The **CHECKING FOR UPDATES** message appears. The **Available Updates section** refreshes to show either a list of available updates or the **0 Updates available** message.
   b. If updates are available, select **Install Updates**. A confirmation message appears.
   c. Select **Yes**. The installing message appears. When the installation has finished, the SDG reboots.

Managing System Configurations

In this section, functions associated with backing up the config for your SDG and restoring a saved config file are covered here. It is recommended that settings be saved as a first step before making changes to the configuration of your SDG.

Backup The Current Configuration

To backup the current settings of your SDG, follow these steps.

1. Expand the **Admin** section in the left navigation bar
2. Select **Configuration** > **Save Configuration** and finally the **Download** button located in the lower portion of the screen.

The file containing the working config parameters for your SDG has now been downloaded to your local drive.

Restore Settings From a Saved Config

To restore the settings for your SDG from a previously saved config made using the above method, follow these steps.

1. Expand the **Admin** section in the left navigation bar
2. Select **Configuration** > **Restore Configuration** and finally the **Browse** button located in the lower portion of the screen.
3. A standard open file dialogue appears. Navigate to the configuration file you saved in Step 2 then select the **Open** button.

In a few moments, the saved configuration will be uploaded and active on your SDG.

Reset the SDG to Factory Default Settings

You can restore factory defaults to the SDG by following these stesp:

1. Expand the **Admin** section in the left navigation bar
2. Select **Configuration** > **Factory Default** and finally the **Factory Reset** button located in the lower portion of the screen.
3. Acknowledge the confirmation dialogue that appears.

The reset will take place, followed by a reboot. Allow a few minutes for this to be completed.

NOTE

You will be unable to access the local GUI of the SDG until the *QuickStart Procedure on page 5* has been performed.

Reset the SDG to Custom Default Settings

The custom defaults feature allows the establishment of a set of defaults to the gateway that are restored when the Restore Default Settings operation is activated. This set of defaults can be defined and updated via the GUI, CLI, or CWMP support of the gateway. To create a custom set of default settings, follow these steps:

1. Configure the gateway as required.
2. Download the current configuration to your local drive using the instructions described above. See *Backup The Current Configuration on page 85*.

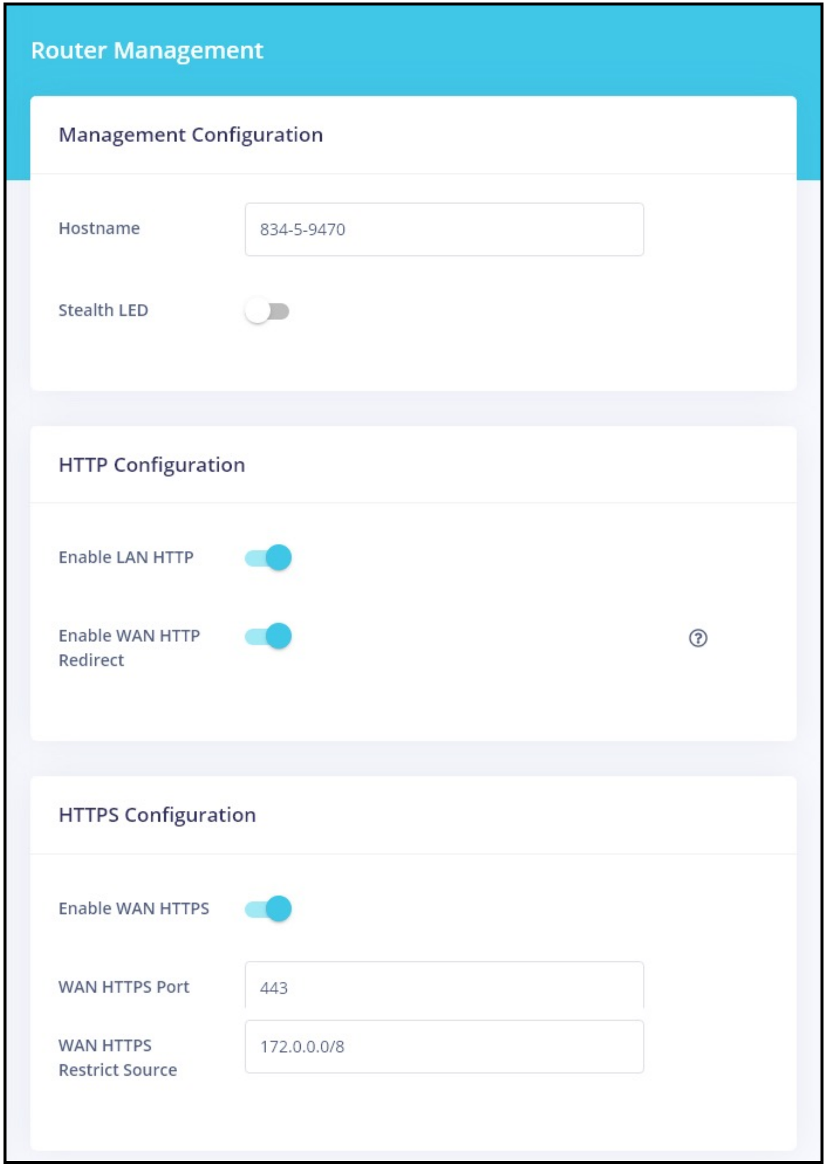
3. Restore the configuration you just saved using the instructions described above. See *Restore Settings From a Saved Config on page 85*.

The gateway now uses your custom settings as the custom default whenever the Restore Default Settings operation is invoked.

Configuring SDG HTTP Settings

On the **Router Management** page, you can enable or disable WAN HTTP and mobile management.

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



Router Management

Management Configuration

Hostname	834-5-9470
Stealth LED	○

HTTP Configuration

Enable LAN HTTP	●
Enable WAN HTTP Redirect	●

HTTPS Configuration

Enable WAN HTTPS	●
WAN HTTPS Port	443
WAN HTTPS Restrict Source	172.0.0.0/8

2. Fill in the fields using the information in *Table 27*.

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

Table 27. Router Management

Field Name	Description
Management Configuration	
Hostname	(Optional) Enter a new name for the host.
Stealth LED	This option prevents the LEDs on the SDG from shining. It is disabled by default. To prevent the LEDs from shining, select the toggle.
HTTP Configuration	
Enable LAN HTTP	This feature is enabled by default. To disable LAN HTTP, select the toggle.
Enable WAN HTTP Redirect	This feature is disabled by default. To redirect WAN HTTP port 80 to a WAN HTTPS port, select the toggle.
HTTPS Configuration	
Enable WAN HTTPS	This feature is disabled by default. To enable WAN HTTPS, select the toggle.
WAN HTTPS Port	(Optional) Enter a different port number for the secure WAN. The default is **443**.
WAN HTTPS Restrict Source	Enter the IP address for which you want access restricted.

Managing System Passwords

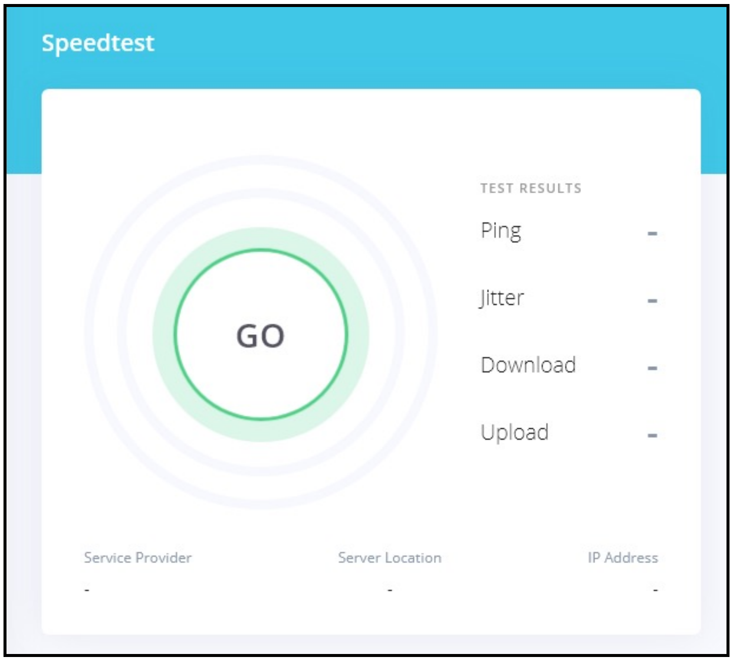
On the **Passwords** page, you can change the passwords used to access your device.

1. In the left menu, select **Admin** > **Passwords**.
2. In the **Username** field, select the user name for the password that you want to modify.
3. In the **Current password** field, enter the current password for the selected user.
4. In the **New password** and **Re-enter password** fields, enter the new password.
5. Select **Save Changes**. The new password takes effect immediately.

Performing a Speed Test

On the **Speed Test** page, you can run transmission speed tests for your SDG. Statistics are returned for ping, jitter, download and upload speeds.

1. In the left menu, select **Admin** > **Speed Test**. The following page appears.

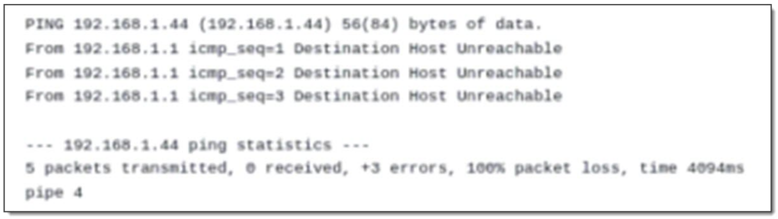


2. Select the **Go** button. The test results appear next to the parameters.You can run this test as often as needed.

Testing Network Connectivity (Ping and Traceroute)

On the **Net Tools** 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, select **Admin** > **Net Tools**.
2. To ping a server, perform the following steps in the **Ping** section:
   a. Enter an IP address or host name in the **IP/Hostname** field.
   b. Select the **Start** button in this section. The ping results appear.

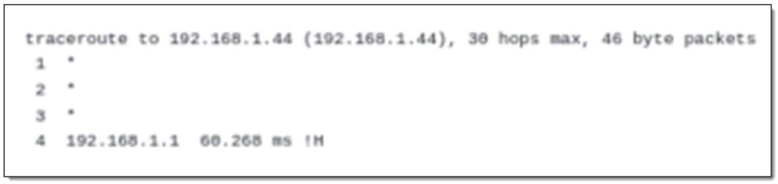


```
PING 192.168.1.44 (192.168.1.44) 56(84) bytes of data.
From 192.168.1.1 icmp_seq=1 Destination Host Unreachable
From 192.168.1.1 icmp_seq=2 Destination Host Unreachable
From 192.168.1.1 icmp_seq=3 Destination Host Unreachable

--- 192.168.1.44 ping statistics ---
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time 4094ms
pipe 4
```

3. To trace a transmission, perform the following steps:in the **Traceroute** section:
   a. Enter an IP address or host name in the **IP/Hostname** field.

b. Select the **Start** button in this section. The trace results appear.



```
traceroute to 192.168.1.44 (192.168.1.44), 30 hops max, 46 byte packets
 1  *
 2  *
 3  *
 4  192.168.1.1  60.268 ms !H
```

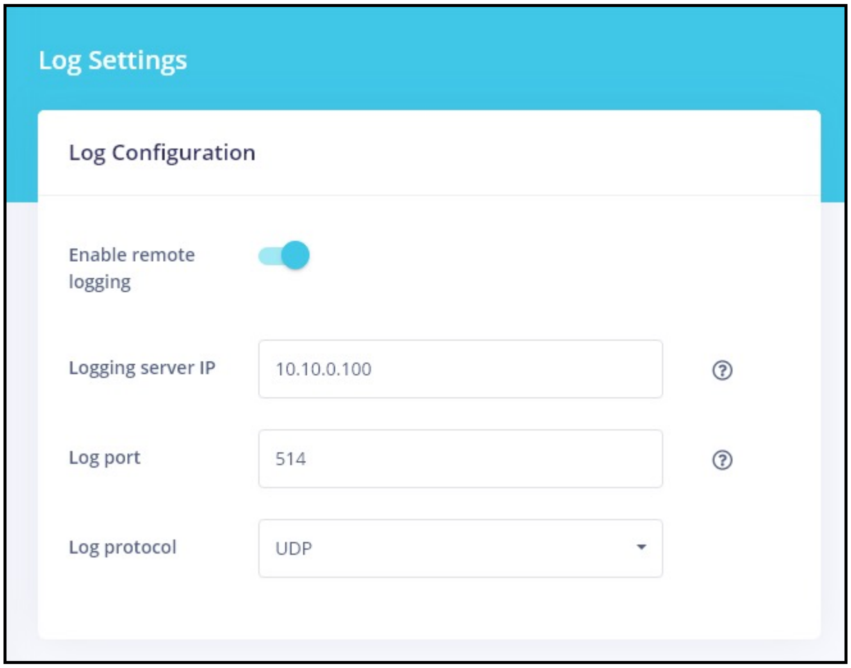
Configuring System Logs

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

Log Settings

On the **Log Settings** page, you can enable remote logging.

1. In the left menu, select **Admin** > **Event Log** > **Log Settings**.
2. (Optional) To activate remote logging, select the toggle next to **Enable remote logging**. Additional fields appear.



Log Settings

Log Configuration

Enable remote logging

Logging server IP: 10.10.0.100

Log port: 514

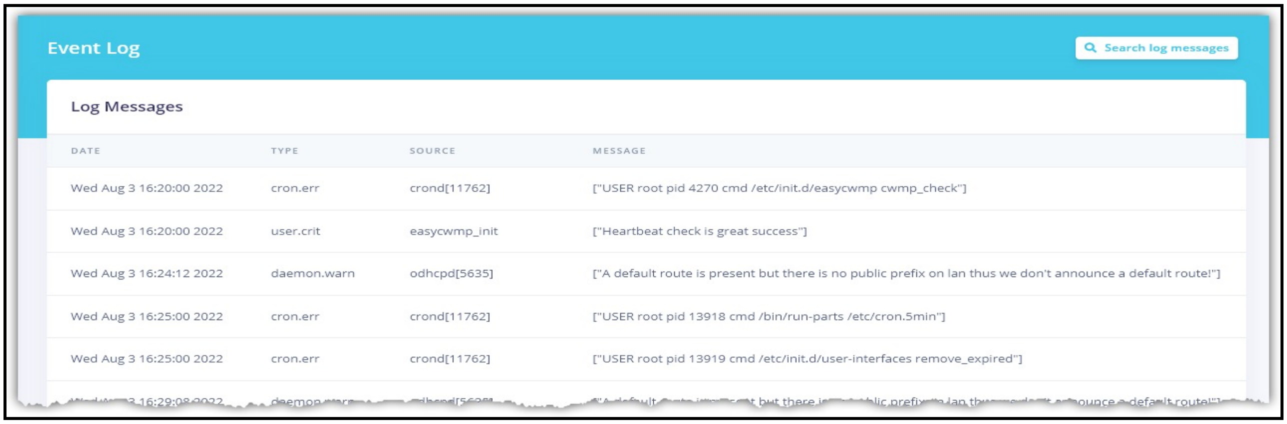
Log protocol: UDP

3. In the **Logging server IP** field, enter the IP address (such as 192.168.1.21) 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**.
5. In the **Log protocol** field, select the protocol. Options are **TCP** and **UDP**. The default is **UDP**.
6. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Viewing Logs

To view the Event Log, follow these steps:

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



Log Messages

DATE	TYPE	SOURCE	MESSAGE
Wed Aug 3 16:20:00 2022	cron.err	crond[11762]	["USER root pid 4270 cmd /etc/init.d/easycwmp cwmp_check"]
Wed Aug 3 16:20:00 2022	user.crit	easycwmp_init	["Heartbeat check is great success"]
Wed Aug 3 16:24:12 2022	daemon.warn	odhcpd[5635]	["A default route is present but there is no public prefix on lan thus we don't announce a default route!"]
Wed Aug 3 16:25:00 2022	cron.err	crond[11762]	["USER root pid 13918 cmd /bin/run-parts /etc/cron.5min"]
Wed Aug 3 16:25:00 2022	cron.err	crond[11762]	["USER root pid 13919 cmd /etc/init.d/user-interfaces remove_expired"]
Wed Aug 3 16:29:08 2022	daemon.warn	odhcpd[5635]	["A default route is present but there is no public prefix on lan thus we don't announce a default route!"]

2. To filter the displayed messages:

   a. Select the **Search log messages** button at top right. The **Search log messages** dialog box appears.

   b. Enter a search string and select **Search**. The list refreshes to show the matching entries. The **Clear search** button appears next to the **Search log messages** button.

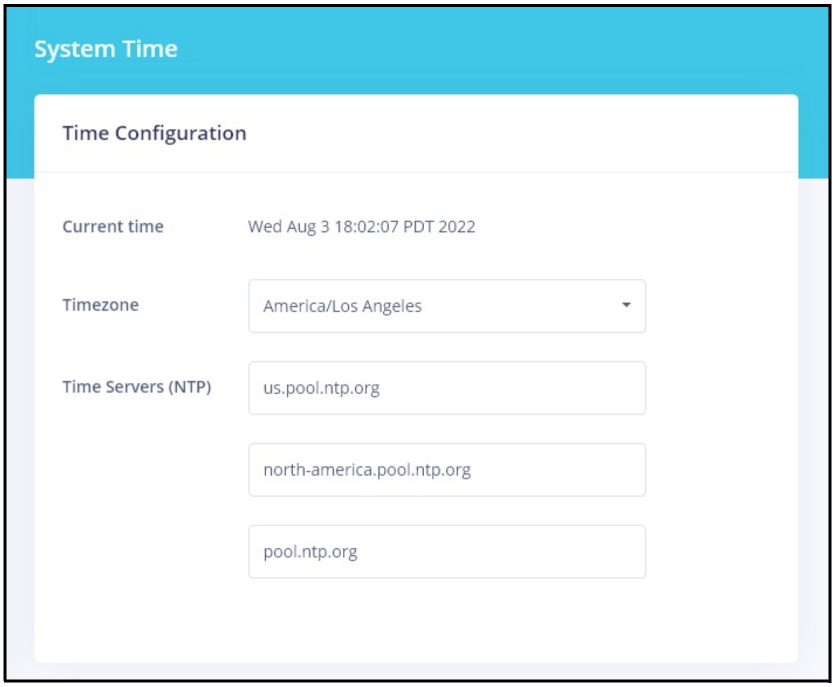
3. To clear the current filter, select the **Clear search** button at the top right.

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

Specifying Time Settings

On the **Time** page, you can select a time zone and manage connections to the reliable clocking servers available on the Internet.

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



Time Configuration

Current time Wed Aug 3 18:02:07 PDT 2022

Timezone America/Los Angeles

Time Servers (NTP) us.pool.ntp.org

north-america.pool.ntp.org

pool.ntp.org

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 to point to the timeserver of your choice.
4. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Specifying SDG Operating Mode

On the **Operating Mode** page, you can select whether the SDG operates as a router or a wireless access point.

1. In the left menu, select **Admin** > **Operating Mode**. The following page appears.
2. To configure how this SDG should operate, in the **Operating Mode** field, select the appropriate setting. Options are **Router** and **Wireless Access Point**. The default is **Router**.

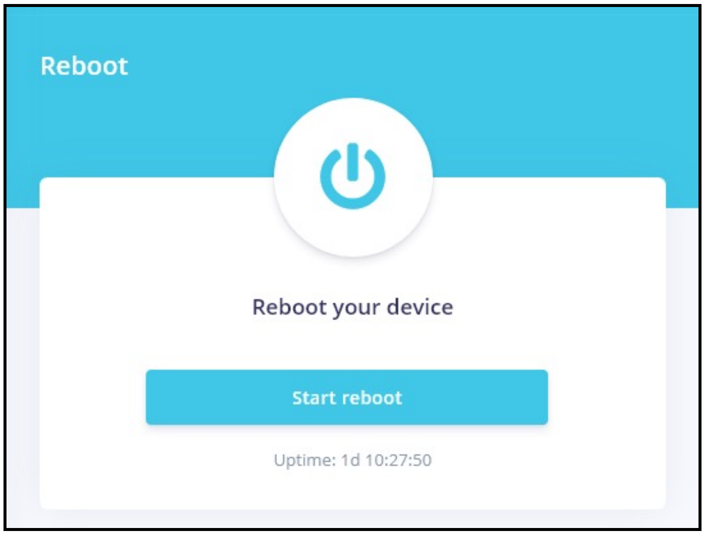
   In **Router** mode, this device functions as a router between your ISP's WAN and your home network LAN. It provides firewall, NAT server, DHCP server, UPnP, DDNS and other services. Select this option if you do not currently have a router.
3. To configure this SDG as part of a mesh network, in the **Intellifi 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 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 SDG from automatically switching from **Intellifi Controller** mode to the managed **Satellite** mode, select the toggle.
5. Select the **Apply** button in the **Pending changes** dialog box to save your settings.

Rebooting the SDG

On the **Reboot** page, you can reboot your SDG.

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



Reboot

Reboot your device

Uptime: 1d 10:27:50

2. Select the **Start reboot** button.
   The restart confirmation dialog box appears, stating that rebooting takes approximately three minutes.

3. Select the **Yes, reset** button. The rebooting dialog box appears, showing the time remaining until completion. When your SDG is ready, the **Sign In** dialog box appears.