Adtran

Service Delivery Gateways

Using SmartOS with 800 and 8000 Series SDGs

Document Issue: A
Document Number: 80000082599

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.

“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.

Contents

Preface

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

NOTE

Content and illustrations are current as of the publication date and are subject to change without notice.

This section contains these topics:

Safety Symbol and Message Conventions

These symbols appear throughout this document and include important information related to your safety and the prevention of equipment damage.

All personnel should correctly follow and not ignore any provided safety instructions. Before you work on any equipment, be aware of the hazards involved and be familiar with standard practices for preventing accidents.

Icon	Meaning	Description
	Warning	Means danger and alerts you to a situation that could cause bodily injury.

Icon	Meaning	Description
	Caution	Alerts you to a potentially hazardous situation or condition that may result in minor or moderate injury.
	Documentation	Advises of the importance of carefully reading all instructions before proceeding or provides links to additional information.
	Note	Indicates supplemental information or helpful recommendations.

Documentation

This section contains these topics:

Related Documentation

You can view and download the Adtran product documentation from our documentation portal. To access our documentation portal, click one of these options:

- docs.adtran.com
- My Adtran > Support Community > Technical Documentation

After logging in, select the appropriate product category. Use the Group by option at the top to sort documents by title (default) or release number within the product categories.

Use the robust search engine to find documents by part name or number, alarm name, specifications, procedures, and more. You can refine results by filtering on product **category**, **document type** (title), and **release number.**

Here ares some related documents:

- *SDG SmartOS User Guide*
- *SDG SmartOS Release Note*
- *SDG Feature Matrix*
- *SDG 834-v6 Service Delivery Gateway WiFi 6 Gigabit Router Quick Start Guide*

- *SDG 854-(v)6 Service Delivery Gateway WiFi 6 2.5G Router Quick Start Guide*
- *SDG-8610 Service Delivery Gateway WiFi 6 Gigabit Router Quick Start Guide*
- *SDG-8612 and SDG-8614 Service Delivery Gateway WiFi 6 2.5G Gigabit Routers Quick Start Guide*
- *SDG-8622 Service Delivery Gateway WiFi 6 Mesh AP Quick Start Guide*
- *SDG-8632 Service Delivery Gateway WiFi 6E Mesh AP Quick Start Guide*
- *SDG-8733 and 8734 Service Delivery Gateway WiFi 7 10G Routers Quick Start Guide*
- *SDG 8733A Service Delivery Gateway WiFi 7 10G Mesh AP*
- *SDG-8733v and 8734v Service Delivery Gateway WiFi 7 10G Routers with Voice Quick Start Guide*
- *PlumeOS Release Notes*

Revision History

NOTE

For details about a specific product release, see the respective release notes

Revision	Description
Document Number: 80000082599 **Document Issue:** A **Issue Date: January 2026**	Added: • Caution to Adding Intellifi Satellites regarding DHCP
Document Number: 6SDGSOS800-29A **Document Issue:** A **Issue Date:** November 2022	Initial release

Warranty

Warranty information can be found at: my.adtran.com/warranty

Contact Adtran

Contact	Contact Information
Technical Support	Toll Free: +1-888-423-8726 International: +1-256-963-8716 Europe: +44 20 7523 5358 support@adtran.com adtran.com/GetStarted
Training	training@adtran.com adtran.com/training
Sales	+1-800-827-0807
Other	adtran.com/ContactUs

Chapter 1: 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. This association is outlined in the *SDG Feature Matrix* (located at adtran.docs.com).

If your SDG is deployed with PlumeOS firmware installed, see the PlumeOS documentation for more information.

For hardware information regarding your SDG, such as instructions for exterior buttons, ports, LED behavior and cabling diagrams, see the Quick Start Guide associated with your specific SDG model.

See Related Documentation for information about accessing the online documentation.

Chapter 2: Introduction to the SDG Series Device

This section contains these topics:

First-Time Setup

Out of the box, the local GUI in the SDG is not immediately available. You need to complete a Quick Start setup to gain access to the GUI.

To access the Quick Start menu:

1. See http://192.168.1.1
2. Use a Smartphone camera to scan the QR code labeled Wi-Fi QuickStart located on the back of your unit; or
3. Follow the instructions located within the Intellifi mobile application.

Once you have access, you will see a series of self-guided steps to create an account, choose your account password, select the gateway or access point mode, and configure the Wi-Fi SSID and passphrase. The specified account password is used when you initially log into the SDG GUI.

Accessing the Device

To manually configure the SDG:

1. Connect to the SDG using the instructions in the Quick Start Guide for your specific model.
2. Configure your computer network interface to acquire an IP address automatically using DHCP.
3. Open a web browser application on your PC and enter the SDG default address: **`http://192.168.1.1`** in the address bar.
4. Enter the **username** (default username is **`admin`**) and the password you specified in First-Time Setup.

> **NOTE**
>
> If you forgot the password for this device, click **Forgot password?** and follow the on-screen instructions to reset the SDG to the factory defaults. See Resetting the SDG to Factory Default Settings.

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

Logging Out

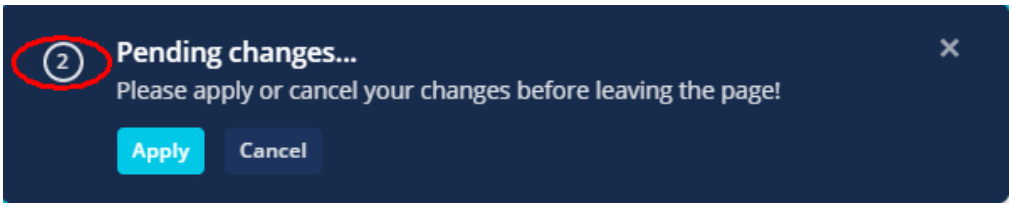
1. Select the profile name in the top, right corner of any GUI screen. The user profile list appears.
2. Click **Logout**. The Sign in dialog box appears.

Saving Changes

When settings are changed, the Pending changes dialog box appears. Apply the changes made on the current page before navigating to a different page. Click **Apply** to apply all changes.

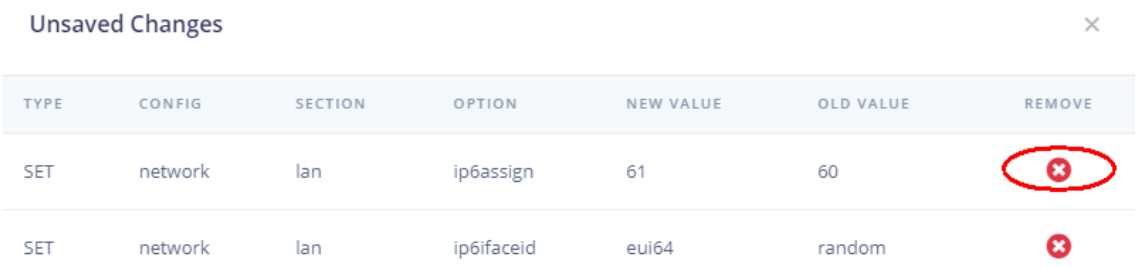
The circled number in Figure 1 indicates the number of pending changes.

Figure 1: Pending Changes Dialog Box



To view a list of your unsaved changes, click the circled number. The Unsaved Changes window appears (Figure 2).

Figure 2: Unsaved Changes Window

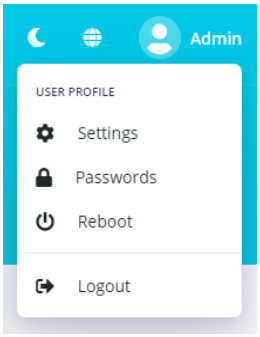


To undo a change for a line item, click the red delete icon next to the line item canceled. After you removed all your changes from the list, the Unsaved Changes window closes.

Setting User Preferences

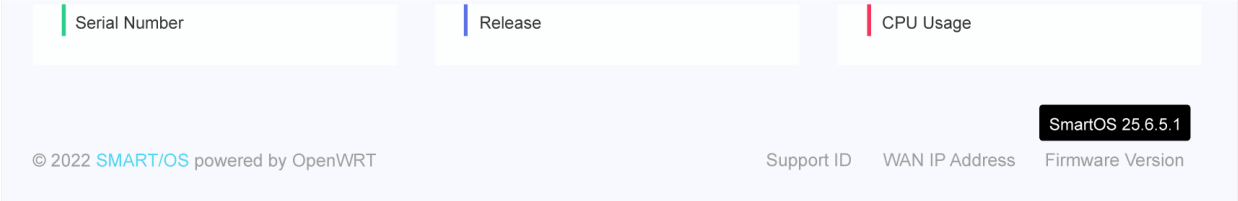
Across the top of your screen, these user preferences are always present:

- **Menu icon** (icon with three lines next to the Adtran logo) — Click to minimize or expand the left navigation menu.
- **Search box** — Use to search for features in the GUI. The search returns a list of pages that match the terms entered. From the list, select the feature or page you want to view.
- **System Errors**(exclamation symbol) — Displays the number of system errors.
- **Notifications icon** (bell symbol) — Click to view notifications sent to the logged-in user account.
- **Dark mode icon** (crescent moon symbol) — Click to engage an alternate color scheme for the GUI. The icon changes to the light mode (sunburst symbol). Click the icon again to return to the original color scheme.
- **Language icon** (globe symbol) — Use to select your preferred interface language.
- **Username** — Displays the username of the person currently logged in. Click the username to access these additional preferences:



  - **Settings** — Use to save or load a router configuration file. See Managing System Configurations.
  - **Passwords** — Use to change passwords for SDG access. See Managing System Passwords.
  - **Reboot** — Use to initiate a reboot of the SDG. See Rebooting the SDG.
  - **Logout** — Use to end the current session with the SDG.

The footer at the bottom of your screen displays your Support ID, WAN IP address, and Firmware Version. Hover your cursor over these labels to view additional details.



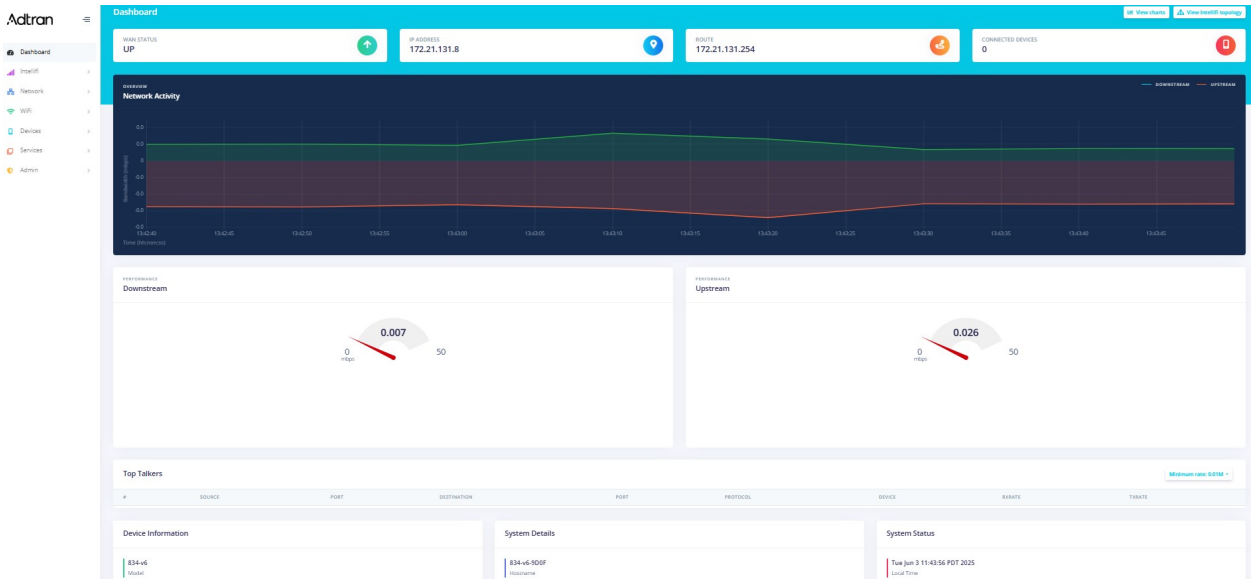
NOTE

The Support ID only appears if you have enabled remote support diagnostics (Admin > Support Diagnostics) when logged in as the support user.

Chapter 3: Navigating the Dashboard

When you successfully log in, the Dashboard appears (see Figure 3) .

Figure 3: Dashboard



The central pane contains these 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 for this device.
- **ROUTE** — Displays the default-gateway for this device.
- **CONNECTED DEVICES** — Displays the number of LAN devices currently connected to the SDG.
- **Network Activity** — Displays 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.
- **Downstream** and **Upstream Performance** — Displays the current utilization of the circuit as seen by the SDG, expressed as Mbps.
- **Top Talkers** — Displays a table that highlights the most active LAN devices on the network. You can sort this table by selecting any of the column headers.
- **Minimum rate** field — Appears at the top right of the **Top Talkers** section. Click to select the options for altering the threshold for which LAN devices are displayed in the Top Talkers table. Optional selections for transmission rate include **None**, **0.01M**, **0.1M**, **1M**, **10M**, and **100M**. The default is **0.01M**.
- **Device Information** section — Displays information about your Adtran device hardware, such as the SDG model number, the MAC address, and the serial number.

- System Details section — Displays additional facts about the Adtran device hardware and software, such as the SDG hostname, the version of firmware that is currently installed, and the release.
- System Status section — Displays the current date and time, the device Uptime (how long this SDG was running), and the current CPU Usage for the SDG processor (expressed as %).
- Left navigation bar — Contains a list of the SDG features that 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 in this guide. These sidebar options navigate you away from the Dashboard to the selected feature. Return to the Dashboard by clicking Dashboard from the top of the left navigation bar.

Chapter 4: Configuring Wired Networks

This section contains these topics:

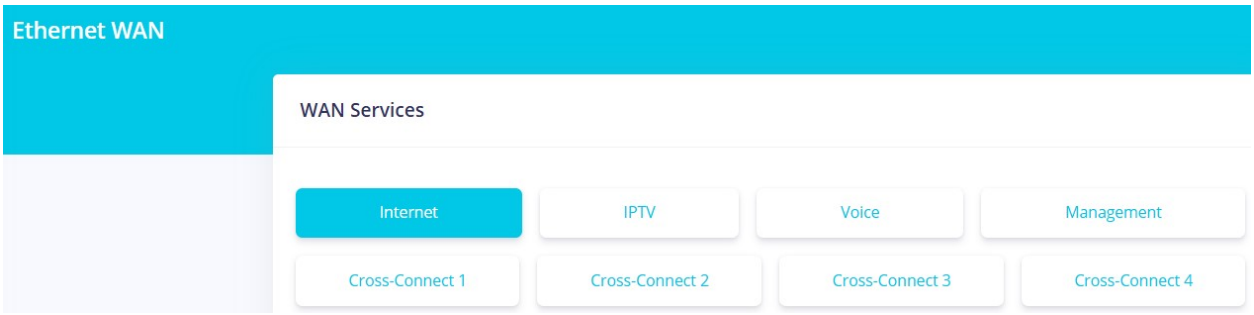
Configuring WAN Settings

This section contains these topics for configuring WAN services:

Accessing WAN Services

To access the controls associated with configuring WAN settings, select **Network > Ethernet WAN**. Figure 4 is the WAN Services screen and defaults to the Internet Services options.

Figure 4: WAN Services Screen



From this screen, you can configure these WAN services using IPv4 and IPv6:

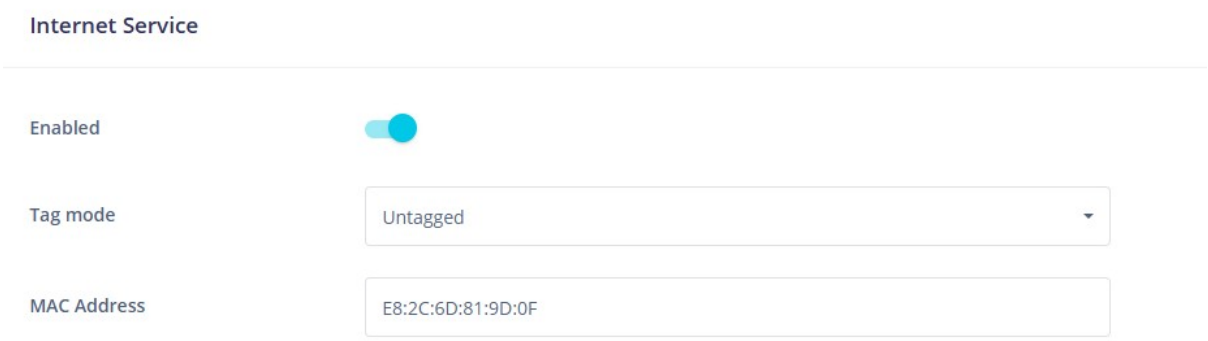
- Internet
- IPTV
- Voice
- Management
- Cross-Connect

Configuring Internet Services

To configure Internet services:

1. Navigate to **Network > Ethernet WAN**.
   The Ethernet WAN page appears showing the **Internet** Service options. By default, the Internet Service setting is enabled and the options appear. Figure 5 shows the IPTV options. IPTV is enabled by default.

   Figure 5: Configuring IPTV



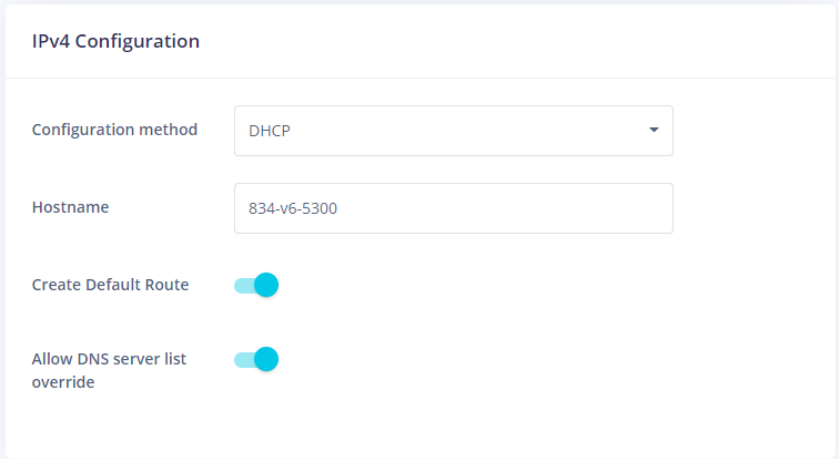
2. Configure these tagging options:
   a. In the **Tag mode** field, select the type of tagging that should be performed. Options are **Untagged**, **Tagged**, and **DQTagged**. The default is **Untagged**.
   b. If you select **Tagged** or **DQTagged**, the **VLAN** and **P-bit** fields appear.
      - **VLAN**: enter or select the ID of the appropriate VLAN. Valid values are **1** to **4079**. The default is **2**.
      - **P-bit**: enter or select the P-bit type. Options are **0** to **7**. The default is **0**.
   c. If you select **DQTagged**, the **CVID** field appears. In the **CVID** field, 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** to **4062**. The default is **0**.
3. (Optional) In the **MAC Address** field, enter the MAC address you want to use with this configuration. By default, this field is set to the MAC address for your SDG.
4. Complete the fields with the provided information for the **IPv4 Configuration** and **IPv6 Configuration** sections as they apply to your environment.
5. In the **Configuration method** field, select the appropriate method for your WAN.
   - **IPv4 WANs** — Options are **DHCP**, **Static Address**, **PPPoE** and **DS-Lite**. The default is **DHCP**.
   - **IPv6 WANs** — Options are **DHCPv6**, **Static Address**, and **None**. The default is **DHCPv6**.

6. For IPv4 and IPv6, complete the remaining fields as instructed for these options:
   - Configuring DHCP for IPv4 WANs
   - Configuring Static Address for IPv4 WANs
   - Configuring PPPoE for IPv4 WANs (IPoE)
   - Configuring DS-Lite for IPv4 WANs
   - Configuring DHCPv6 for IPv6 WANs
   - Configuring Static Address for IPv6 WANs
7. Use the **Create default route** slider to enable the default route for this WAN.
8. Use the **Allow DNS server list override** option to allow override of the DNS server list.
9. Click **Apply** in the Pending changes dialog box.

Configuring DHCP for IPv4 WANs

Figure 6 shows the fields available when **DHCP** is the configuration method. This method is the default for IPv4 WANs. If you want to configure the IPv4 WANs differently, see Configure these options:(below).

Figure 6: DHCP Configuration Fields



1. Configure these options:
   a. In the **Configuration method** field, select the configuration method for IPv4. Options are **DHCP**, **PPPoE**, **DS-Lite** and **Static Address**.
   b. If you select **DHCP** as a configuration method, **Hostname**, **Circuit ID**, **Create Default Route** and **Allow DNS server list override** are the available options.
   c. If you select **PPPoE** as a configuration method, **Username**, **Password**, **Access concentrator**, **Service name**, **Advanced**, and **Allow DNS server list override** are the available options.
      - For **Advanced**, the options are **TTL** and **MTU.**

d. If you select **DS-Lite** as a configuration method, **Peer address**, **Create default route**, **Advanced**, and **Allow DNS list override** are the available options.

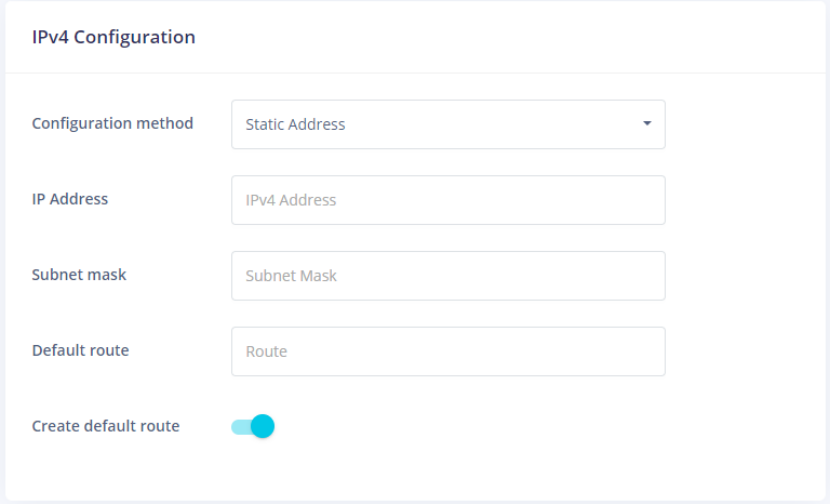
e. If you select **Static Address** as a configuration method, **IP Address**, **Subnet mask**, **Default route** and **Create default route** enable/disable options are the available options.

2. Click **Apply** in the Pending changes dialog box.

Configuring Static Address for IPv4 WANs

Figure 7 shows the fields that appear when you select **Static Address** as the configuration method.

Figure 7: Static Address Fields



1. Complete the fields using the information in Table 1.

Table 1: Static Address for IPv4

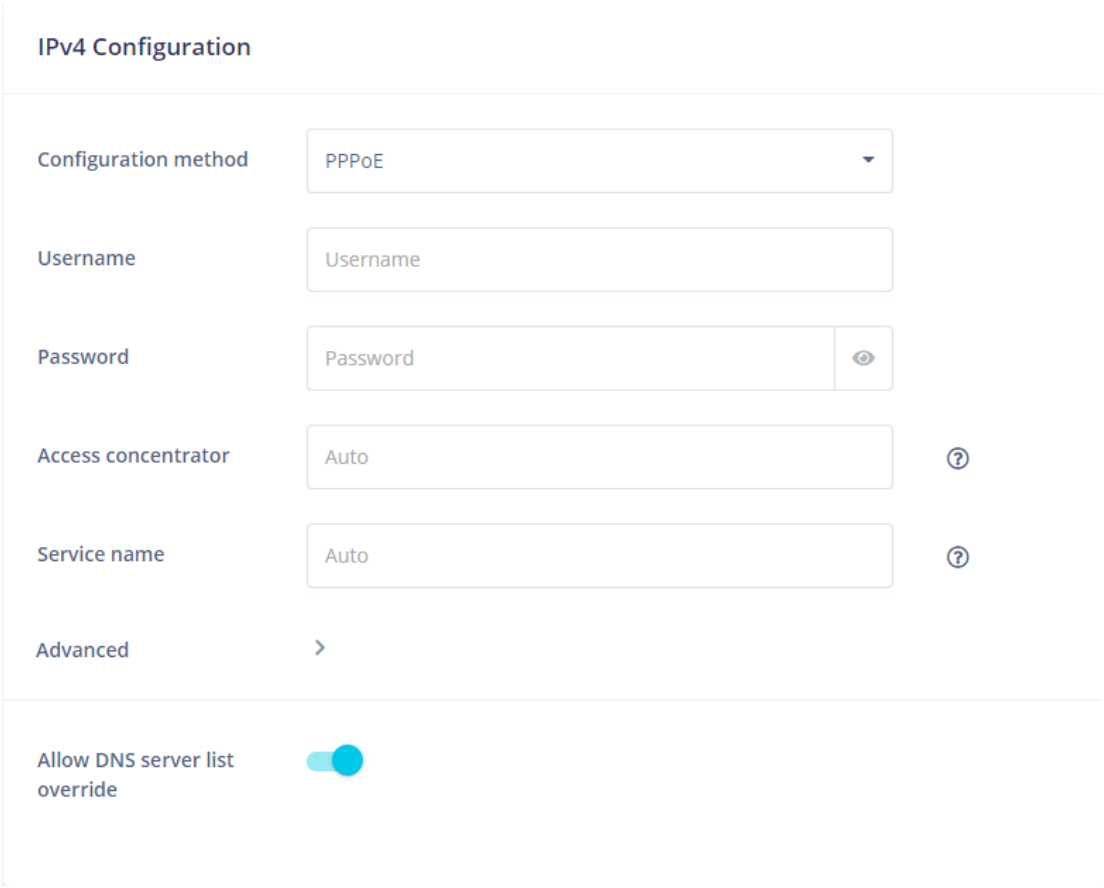
Field Name	Description
IP Address	Enter the IP address for IPv4 communications.
Subnet mask	Enter the IP address for the subnet mask.
Default route	Enter the IP address for the default IPv4 route.

2. Click **Apply** in the Pending changes dialog box.

Configuring PPPoE for IPv4 WANs

Figure 8 shows the field that appear when you select **PPPoE** as the configuration method.

Figure 8: PPPoE Fields



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.

Table 2: PPPoE for IPv4 WANs

Field Name	Description
Username	Enter the PPP Username.
Password	Enter the PPP password. To view the password characters, click 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

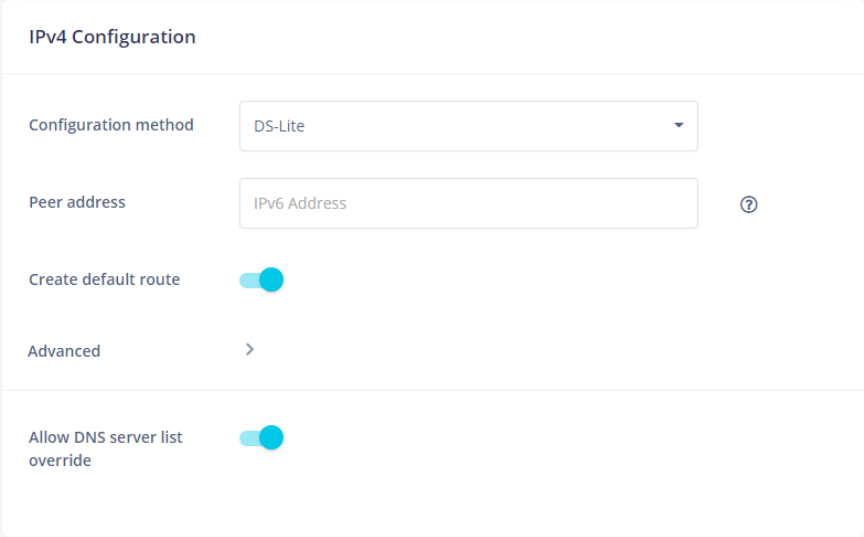
Field Name	Description
LCP Echo Interval	Link Control Protocol (LCP) is used as a "keep-alive" signal between devices connected through PPPoE and echo requests. Enter the interval for sending LCP signals. Options are **None** and **1** to **60** seconds. The default is **None**.
LCP Echo Retry	This is the number of consecutive failed LCP echo requests allowed before the connection between devices is considered down. Enter the number of 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. Use this slider to enable PPP persistence.
PPP Holdoff	Enter the number of seconds before attempting to reconnect a dropped call. The default is **zero** (**0**).

3. Click **Apply** in the Pending changes dialog box.

Configuring DS-Lite for IPv4 WANs

Figure 9 shows the fields that appear when you select **DS-Lite** as the configuration method. DS-Lite is a tunneling technology that encapsulates IPv4 packets in IPv6 transports and delivers them to an IPv4 destination.

Figure 9: DS-Lite Fields



1. To access TTL and MTU settings, select the arrow next to **Advanced**.
2. Complete the fields using the information in Table 4.

Table 4: DS-Lite for IPv4 WANs — Advanced

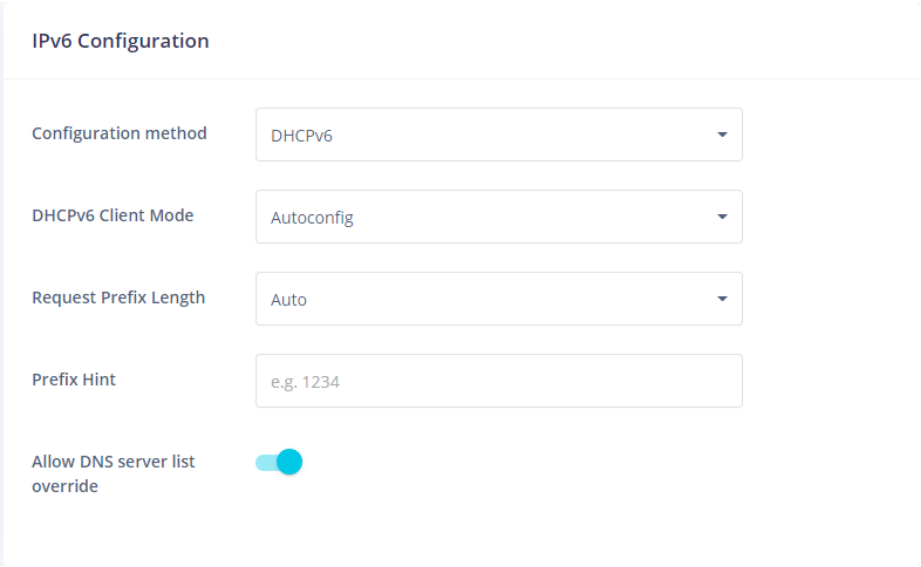
Field Name	Description
Peer Address	Enter the IPv6 address for the peer server.
TTL	Enter the Time to Live value for the packets being sent. This is the number of hops permitted before the packet is discarded. The default is **64**.
MTU	Enter the **MTU (Maximum Transmission Unit) size** for the network.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

3. Click **Apply** in the Pending changes dialog box.

Configuring DHCPv6 for IPv6 WANs

Figure 10 shows the fields that appear when you select **DHCPv6** as the configuration method. This method is the default for IPv6 WANs.

Figure 10: DHCPv6 Fields



1. Complete the fields using the information in Table 5.

Table 5: DHCP v6 for IPv6 WANs

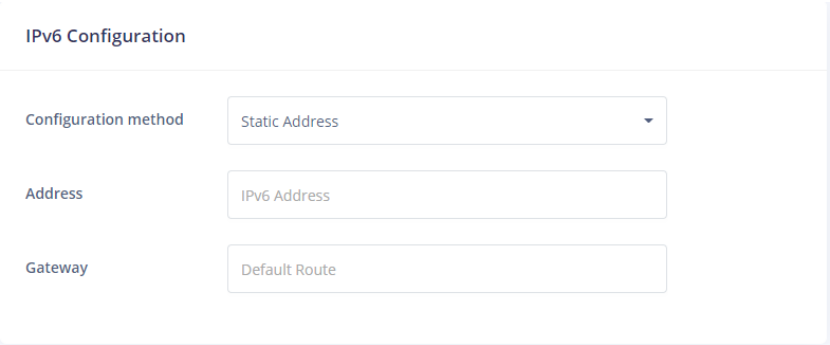
Field Name	Description
DHCPv6 Client Mode	Select the mode for the DHCPv6 client. The options are: • **Autoconfig** — Attempt to use the DHCP server for configuration. If no IP address is provided, use SLACC for configuration. • **Stateful** — Use only the IP address provided by the DHCP server. • **Stateless** — 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** to **64**, and **None**.
Prefix Hint	Enter the 4-digit hint for the subprefix ID.

2. Click **Apply** in the Pending changes dialog box.

Configuring Static Address for IPv6 WANs

Figure 11 shows the fields that appear when you select **Static Address** as the configuration method.

Figure 11: Static Address Fields



1. Complete the fields using the information in Table 6.

Table 6: Static Address for IPv6 WANs

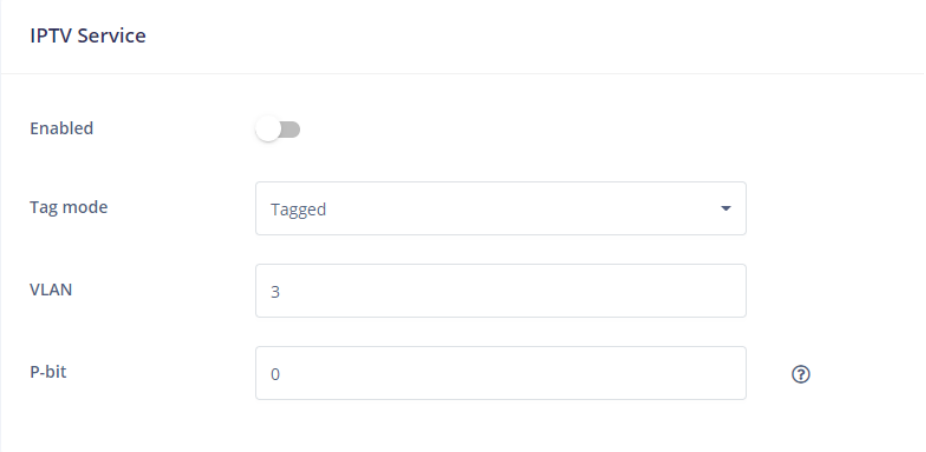
Field Name	Description
Address	Enter the static address for IPv6 communications, such as 2001:db8:a0b:12f0::1.
Gateway	Enter the IP address for the default IPv6 route.

2. Click **Apply** in the Pending changes dialog box.

Configuring the IPTV Settings for Your Ethernet WAN

1. Navigate to **Network > Ethernet WAN**. The Ethernet WAN page appears.
2. Click **IPTV** and the IPTV Service options appear (Figure 12).

Figure 12: IPTV Service Options



3. Use the **Enabled** option to enable the IPTV feature.
4. Configure these 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 you select **Tagged**, the **VLAN** and **P-bit** fields appear.
      - **VLAN**: enter or select the ID of the appropriate VLAN. Valid values are **1** to **4079**. The default is **3**.
      - **P-bit**: enter or select the P-bit type. Options are **0** to **7**. The default is **0**.
5. In the **IPv4 Configuration** section, configure the settings using the information in Configuring DHCP for IPv4 WANs and Configuring Static Address for IPv4 WANs .
6. Click **Apply** in the Pending changes dialog box.

Configuring Voice Settings for Your Ethernet WAN

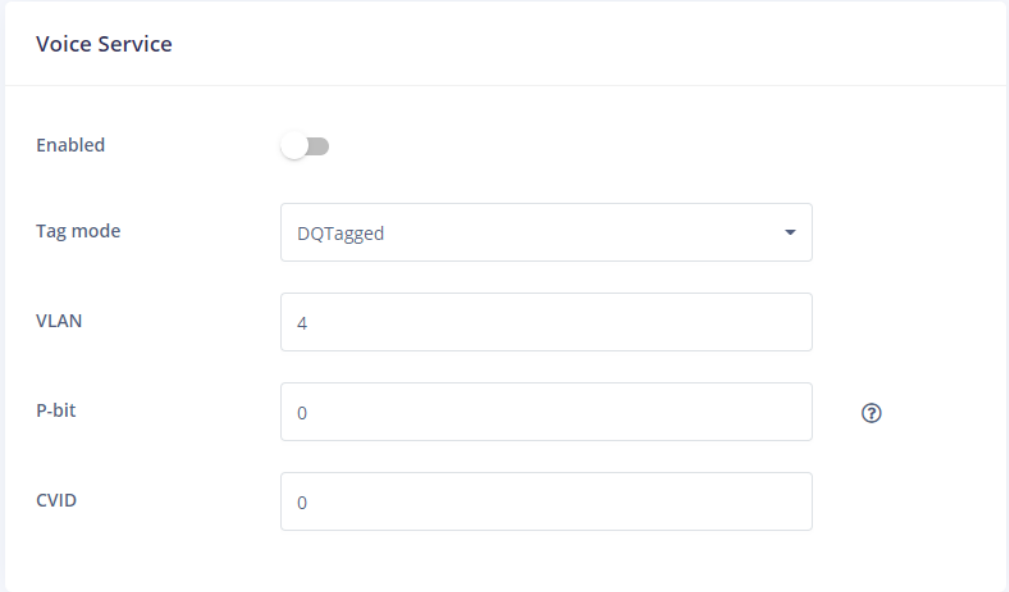
NOTE

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

To configure Voice settings for your Ethernet WAN:

1. Navigate to **Network > Ethernet WAN**. The Ethernet WAN page appears.
2. Click **Voice** and the Voice Service options appear (see Figure 13).

   Figure 13: Voice Service Options



3. Use the **Enabled** option to enable the Voice feature.
4. Configure these 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 you select **Tagged**, the **VLAN** and **P-bit** fields appear.
      - **VLAN**: enter or select the ID of the appropriate VLAN. Valid values are **1** to **4079**. The default is **3**.
      - **P-bit**: enter or select the P-bit type. Options are **0** to **7**. The default is **0**.
   c. If you select **DQTagged**, the **CVID** field appears. In the **CVID** field, 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** to **4062**. The default is **1500**.

5. In the **IPv4 Configuration** section, configure the settings using the information in Configuring DHCP for IPv4 WANs and Configuring Static Address for IPv4 WANs .
6. In the **IPv6 Configuration** section, configure the settings using the information in Configuring DHCPv6 for IPv6 WANs and Configuring Static Address for IPv6 WANs.
7. Click **Apply** in the Pending changes dialog box.

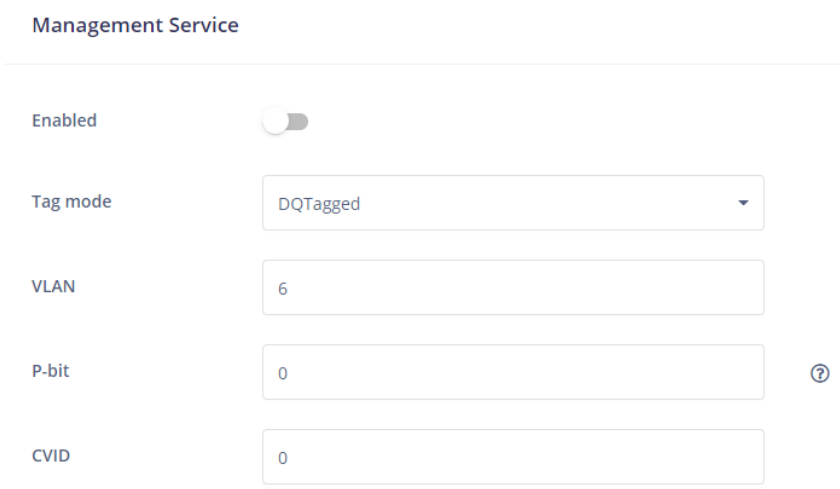
Configuring the Management Settings

This section provides details on how you configure the settings for managing your network and the devices connected to it.

To configure Management settings:

1. Navigate to **Network > Ethernet WAN**. The Ethernet WAN page appears.
2. Click **Management** and the Management Service options appear (see Figure 14).

Figure 14: Management Service Options



3. Configure these 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 you select **Tagged** or **DQTagged**, the **VLAN** and **P-bit** fields appear.
      - **VLAN**: enter the ID of the appropriate VLAN. Valid values are **1** to **4079**. The default is **6**.
      - **P-bit**: enter the P-bit type. Options are **0** to **7**. The default is **0**.
   c. If you select **DQTagged**, the **CVID** field 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** to **4062**. The default is **0**.
4. In the **IPV4 Configuration** section, configure the settings using the information in Configuring DHCP for IPv4 WANs, Configuring Static Address for IPv4 WANs , or Configuring PPPoE for IPv4 WANs.

5. In the **IPV6 Configuration** section, configure the settings using the information in Configuring DHCPv6 for IPv6 WANs or Configuring Static Address for IPv6 WANs.
6. Click **Apply** in the Pending changes dialog box.

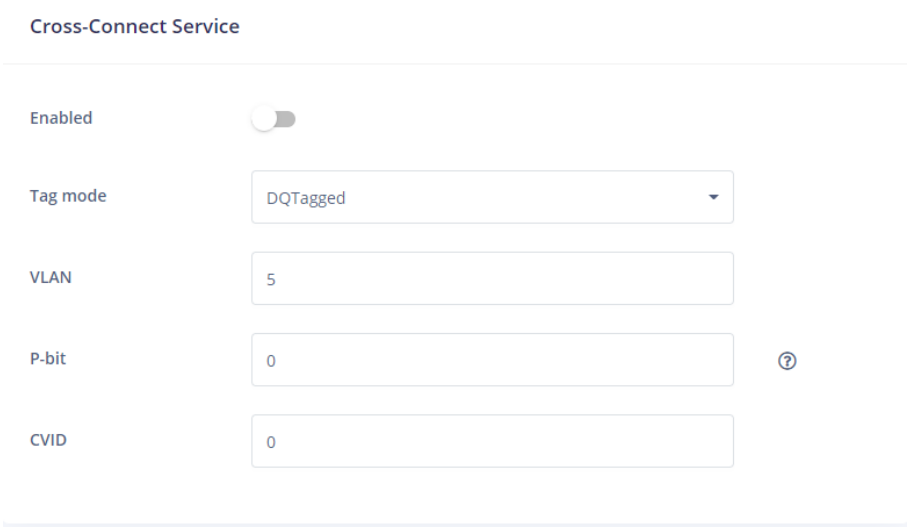
Configuring Cross-Connect Settings

This section provides details on how you configure bridge settings for traffic moving from a WAN-side VLAN to a LAN port. You can use it for bridged IPTV or other services.

To configure Cross-connects settings:

1. Navigate to **Network > Ethernet WAN**. The Ethernet WAN page appears.
2. Click **Cross-Connect** and the cross-connect service options appear (see Figure 15).

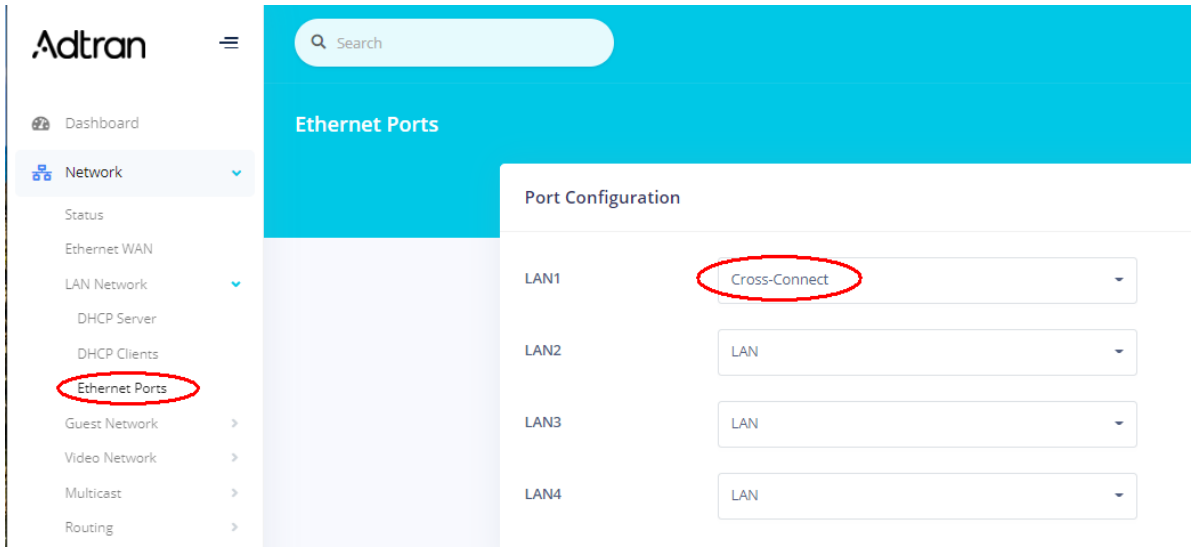
Figure 15: Cross-Connect Service Options



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 you select **Tagged** or **DQTagged**, the **VLAN** and **P-bit** fields appear.
      - **VLAN**: enter the ID of the appropriate VLAN. Valid values are **1** to **4079**. The default is **5**.
      - **P-bit**: enter the P-bit type. Options are **0** to **7**. The default is **0**.
   c. If you select **DQTagged**, the **CVID** field 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** to **4062**. The default is **0**.
4. Click **Apply** in the Pending changes dialog box.

5. Complete the cross-connect by selecting the Ethernet LAN port used for the cross-connect service. Navigate to **Network > LAN Network > Ethernet Ports** and select **Cross-Connect** beside the LAN port used for this option (see Figure 16).

Figure 16: Selecting Cross-Connect Port Configuration



6. Click **Apply** in the Pending changes dialog box.

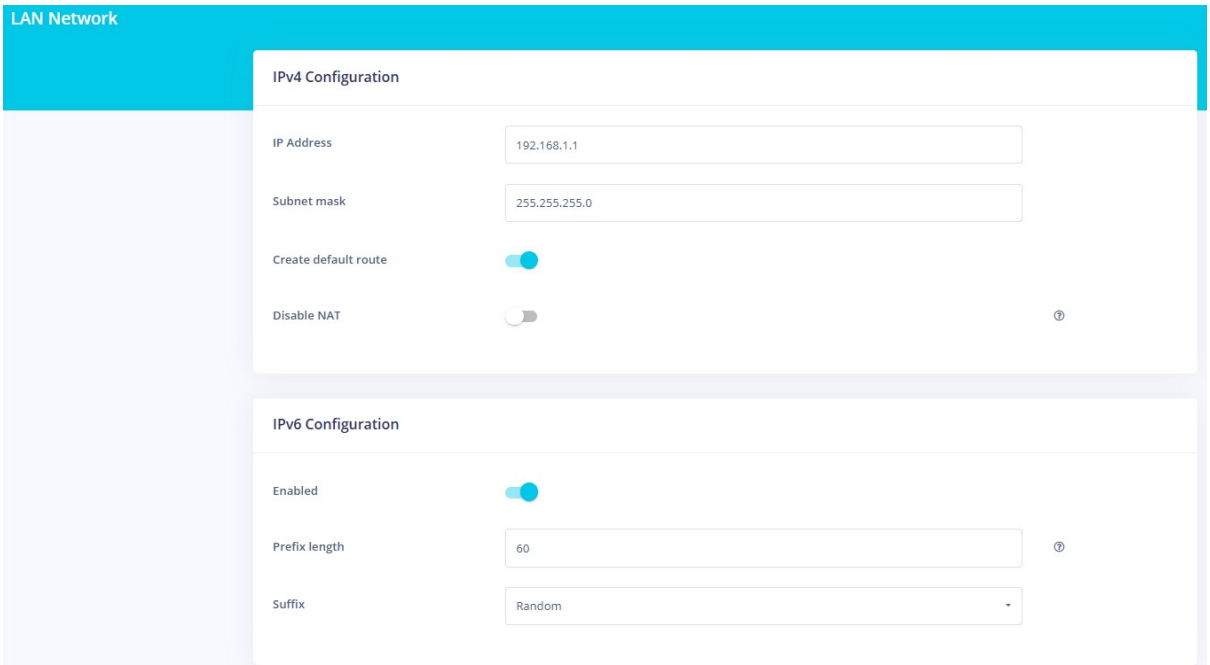
Setting Up the LAN Network

This section includes these topics:

Configuring Basic IPv4 LAN Settings

1. Navigate to **Network > LAN Network**. The LAN Network page appears showing the IPv4 LAN options (see Figure 17).

Figure 17: LAN Network Page



2. Complete the fields using the information in Table 7 and Table 8.

Table 7: IPv4 Configuration

Field Name	Description
IP Address	Enter the IP address for IPv4 communications. The default is **192.168.1.1**.
Subnet mask	Enter the IP subnet mask for this SDG. The default is **255.255.255.0**.
Create default route	(Optional) Use this slider to create the default route for this LAN.
Disable NAT	This option disables Network Access Translation (NAT) for this network and allows normal routing.

Table 8: IPv6 Configuration

Field Name	Description
Enabled	This option is disabled by default. Use this slider to enable IPv6 address configuration. The Prefix length and Suffix fields appear.
Prefix length	Enter the prefix length for this IPv6 address. Options are **0** to **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 *::a:b:c:d* format.

3. Click **Apply** in the Pending changes dialog box.

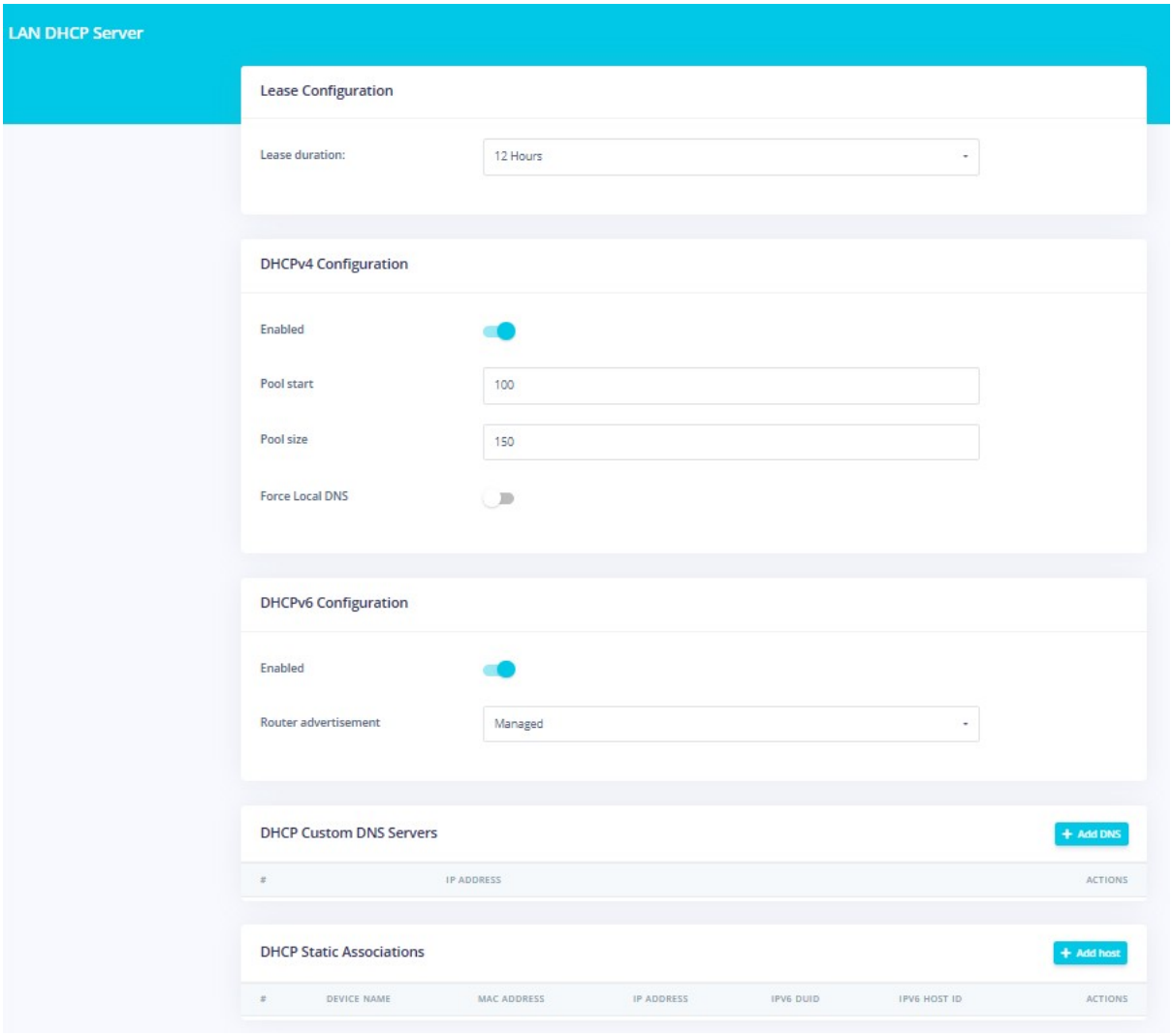
Configuring the DHCP Server

This section provides details on how you configure the DHCP settings for the SDG. The DHCP feature of this SDG automatically assigns LAN IP addresses to host devices as they connect.

To configure the DHCP server:

1. Navigate to **Network > LAN Network > DHCP Server**. The LAN DHCP Server page appears (see Figure 18).

   Figure 18: LAN DHCP Server Page



2. Complete the fields using the information in Table 9.

Table 9: LAN DHCP Server Configuration

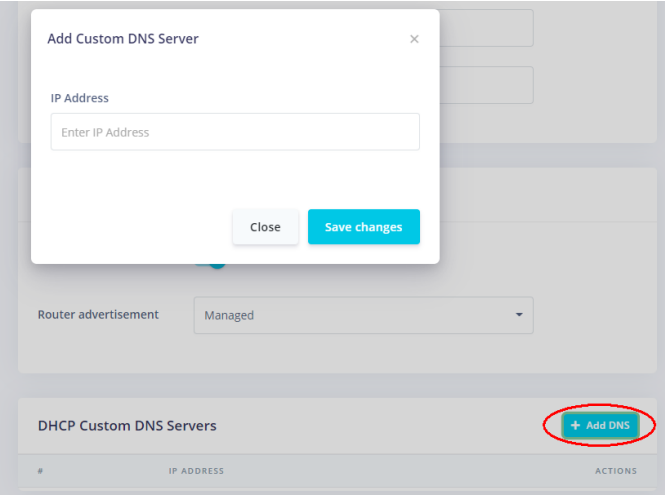
Field Name	Description
Lease Configuration	
Lease duration	Select the amount of time for which an IP address will be leased. Options range from **5 minutes** to **24 hours**. The default is **12 hours**.
DHCPv4 Configuration	
Enabled	This feature is enabled by default. Use this slider to disable this feature.
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.
Force Local DNS	Use the slider to force the system to use the local DNS server list.
DHCPv6 Configuration	
Enabled	This feature is enabled by default. Use this slide to disable 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 Customer DNS Servers	Use this feature to add a customer's IP address for the DNS server.
DHCP Static Associations	(Optional) To define a static DHCP server, see Defining a Static DHCP Association (Optional) .

3. Click **Apply** in the Pending changes dialog box.

Defining a Custom DNS Server (Optional)

1. Navigate to **Network > DHCP Server**and select **Add DNS** in the **DHCP Custom DNS Servers** section. The Add Custom DNS Server dialog box appears (see Figure 19).

   Figure 19: Add Custom DNS Server Dialog Box



2. Enter the IP address of the host device and click **Save changes**.
3. To add another DNS server, repeat steps 1 and 2.

NOTE

To remove a custom server IP address, click the red delete button.

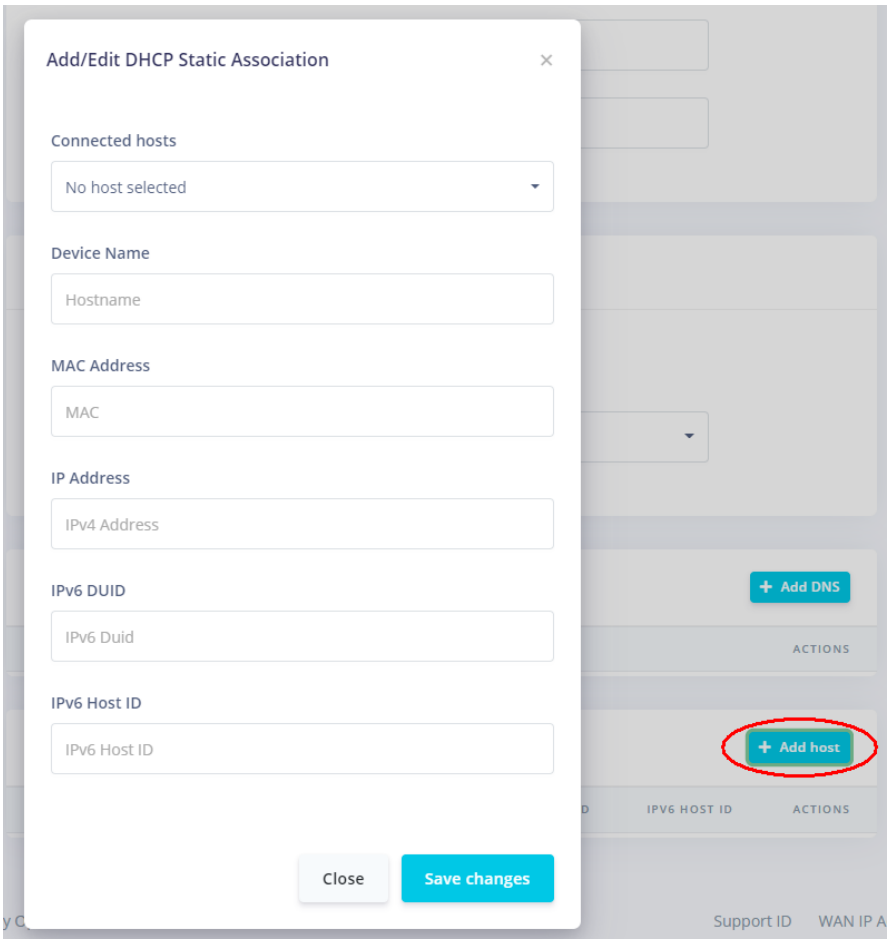
Defining a Static DHCP Association (Optional)

You can associate a static IP address with the a MAC address of a specific LAN host device.

To define a static DHCP association::

1. Navigate to **Network > DHCP Server** and select **Add host** in the **DHCP Static Associations** section. The Add/Edit DHCP Static Association dialog box appears (see Figure 20).

   Figure 20: Add/Edit DHCP Static Association Dialog Box



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 populate with the related information. If the host is currently offline or the **None** option is chosen, the information must be entered manually.
3. Click **Save changes**.
4. To add another static DHCP configuration, repeat steps 1 through 3.
5. To edit a static DHCP IP address:
   a. Click **Edit** next to the IP address. The Add/Edit dialog box appears.
   b. Change the entries as needed and click **Save Changes**.

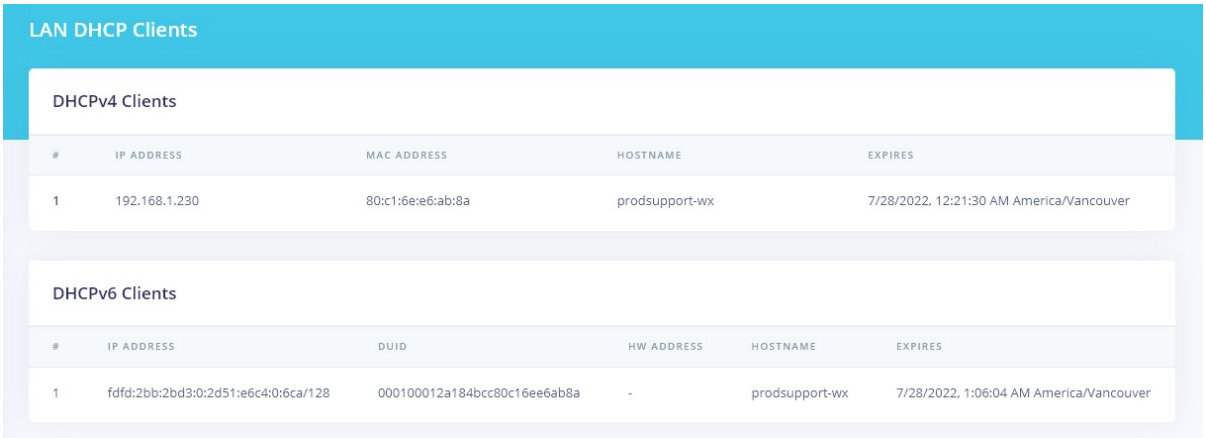
NOTE

To remove a static DHCP IP address, click the red delete button. Click **Apply** in the Pending changes dialog box.

Viewing IPv4 and IPv6 DHCP Clients

To view the IPv4 and IPv6 DHCP clients connected to your LAN, navigate to **Network > LAN Network > Guest DHCP Clients**. The LAN DHCP Clients screen appears (see Figure 21).

Figure 21: LAN Guest DHCP Clients Page

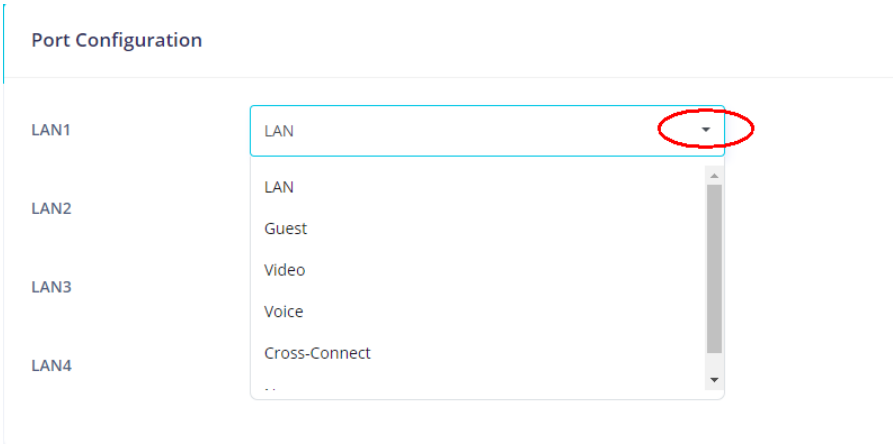


Selecting Services for Ethernet Ports

To select which service to run for each interface defined on your SDG (see Figure 22):

1. Navigate to **Network > LAN Network > Ethernet Ports**. The Port Configuration page appears.

   Figure 22: Port Configuration Page



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

NOTE

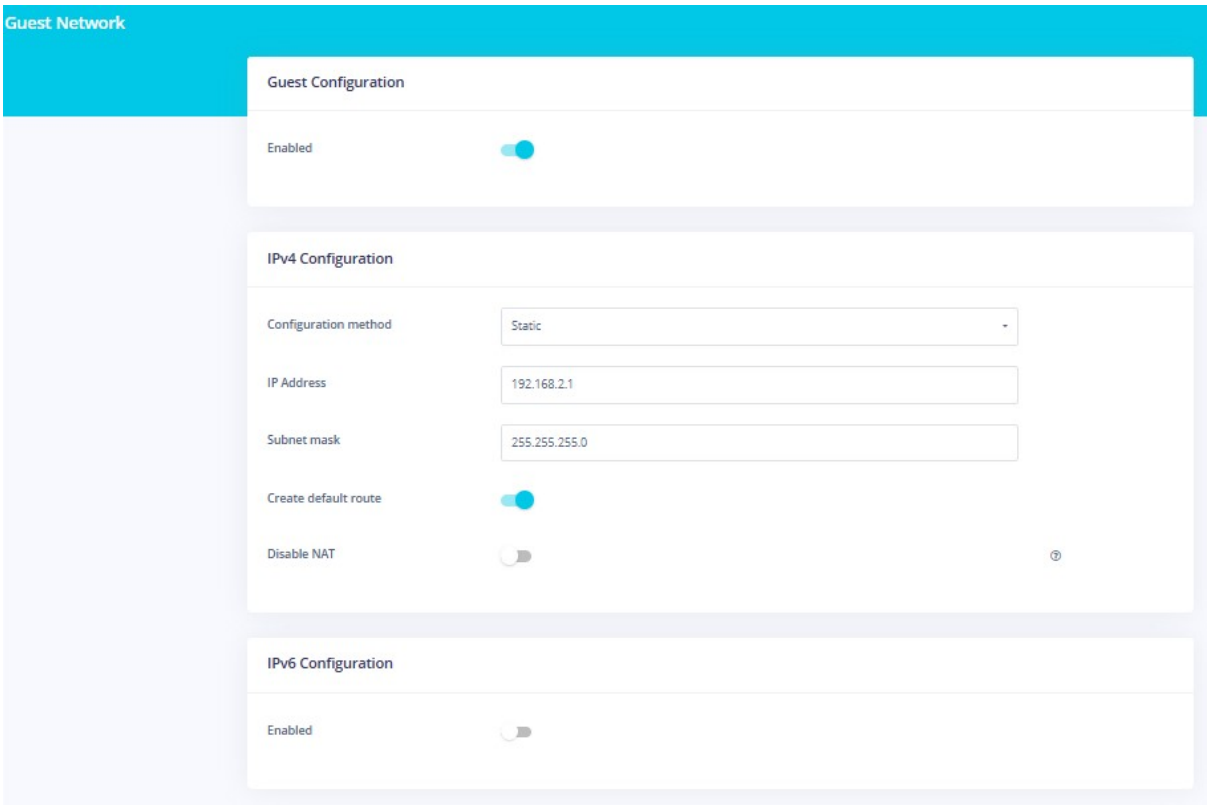
If Cross-Connect is selected, the cross connect service will need to be enabled on the WAN. For more information, see Configuring Cross-Connect Settings.

3. Click **Apply** in the Pending changes dialog box.

Configuring Guest Network Settings

1. Navigate to **Network > Guest Network**. The Guest Configuration page appears (see Figure 23). This feature is enabled by default.

Figure 23: Guest Configuration Page



2. Complete the fields using the information in Table 10.

Table 10: Guest Network Settings

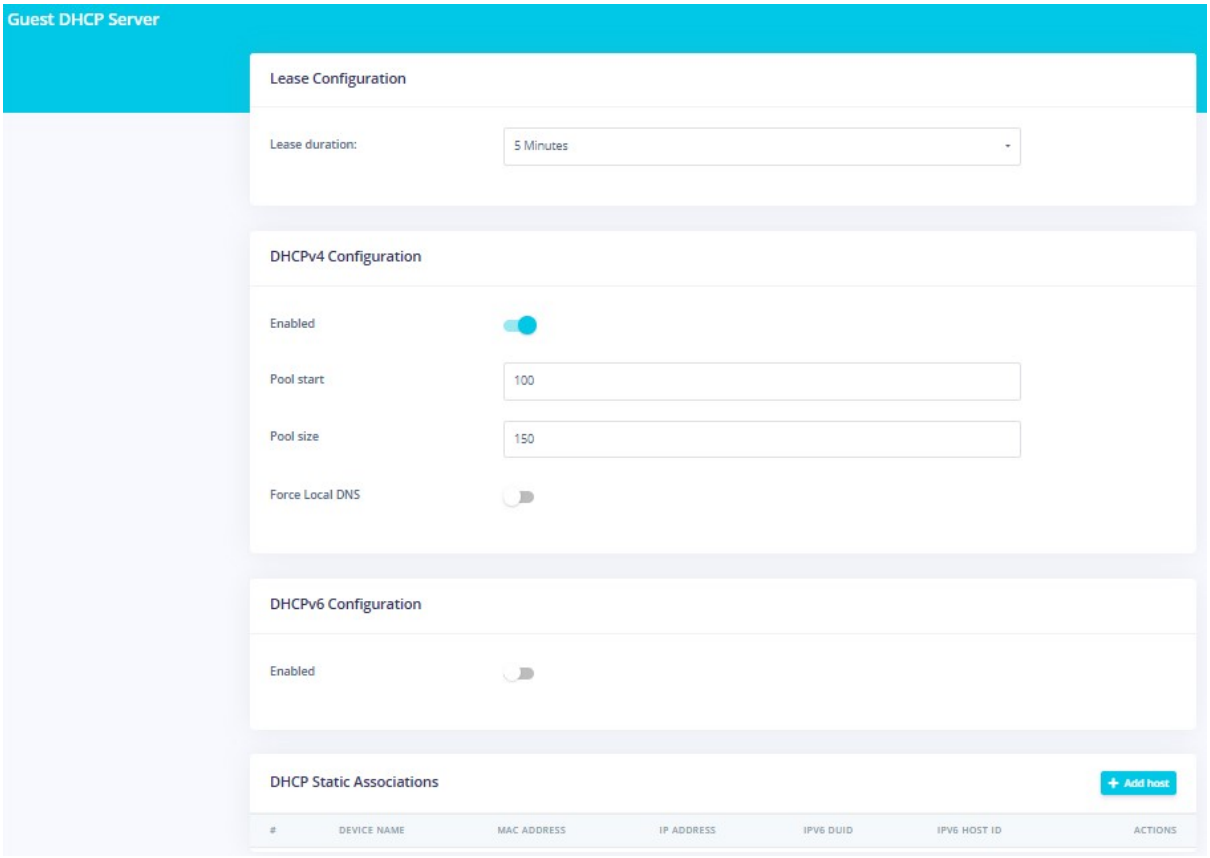
Field Name	Description
IPv4 Configuration	
Configuration method	Select the appropriate method for your WAN. The page refreshes to show the fields that apply for the selected method. Options are **Static**, **DHCP**, and **None**. The default is **Static**.
Static Configuration Method	
IP Address	Enter 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	Use this slider to create a default route for this LAN.
Disable NAT	Use this slider to disable Network Address Translation (NAT) for this network and allow normal routing.
DHCP Configuration Method	
Hostname	Enter the host name to be included in DHCP requests.
IPv6 Configuration Method	
Enabled	This feature is disabled by default. Use this slider to enable IPv6 address configuration.
Prefix length	Enter the prefix length for this IPv6 address. Options are **0** to **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 *::a:b:c:d* format.

3. Click **Apply** in the Pending changes dialog box.

Configuring the Guest Network DHCP Server

1. Navigate to **Network > Guest Network > DHCP Server**. The Guest DHCP Server page appears (see Figure 24).

Figure 24: Guest DHCP Server Page



2. Complete the fields using the information in Table 11.

Table 11: Guest Network DHCP Server Settings

Field Name	Description
Lease Configuration	
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. Use this slider to disable this feature.
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.

Table 11: Guest Network DHCP Server Settings (continued)

Field Name	Description
Force Local DNS	This option enables you to force the system to use the DNS server in stead of the DHCP server.
DHCPv6 Configuration	
Enabled	Use this slider 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, see Defining a Static DHCP IP Address Association for a Guest Network Host .

3. Click **Apply** in the Pending changes dialog box.

Editing a DHCP Host

1. Select the Add host option adjacent to the DHCP Static Associations field.
2. Edit the fields using the information in Table 11.

Table 12: Add DHCP Static Association

Field Name	Description
Connected host	This is the name of the DHCP host.
Device Name	This is the user-defined name for the DHCP host.
MAC Address	This is the MAC address of the DHCP host.
IPv6 DUID	This is the unique DHCP identifier.
IPv6 Host ID	This is the DHCP host identifier.

3. Select **Save changes**.

Adding a DHCP Host

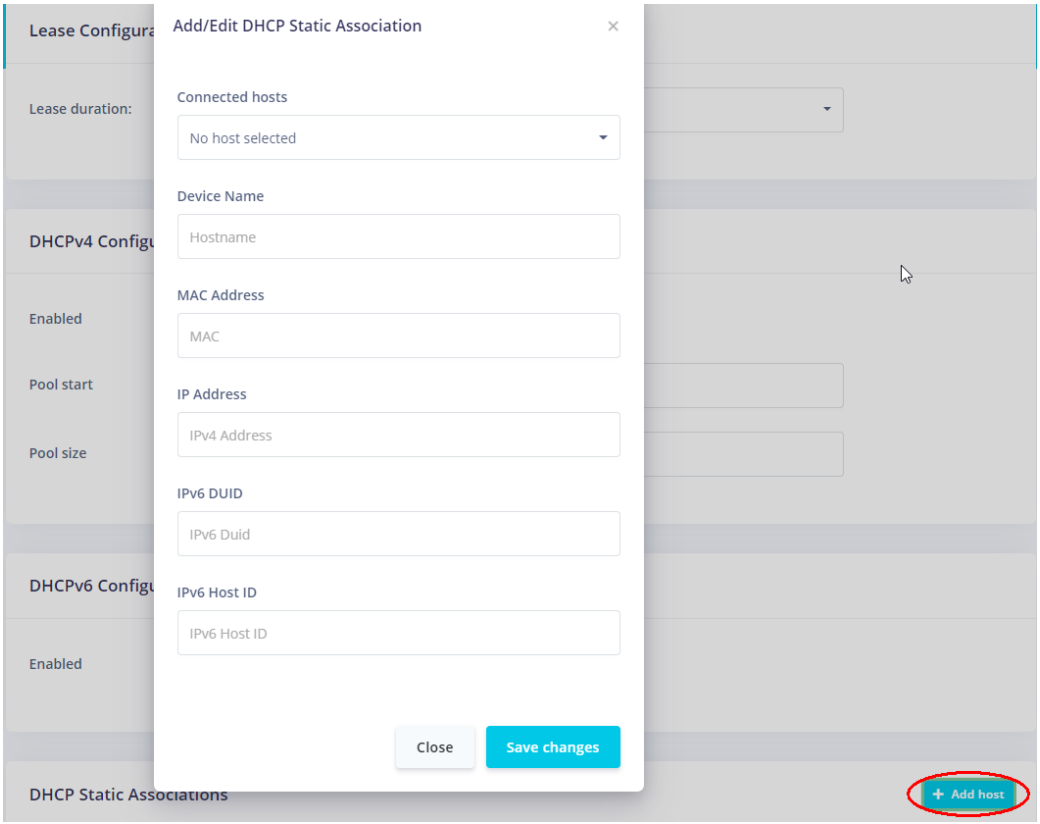
1. Select the **Add host** option adjacent to the **DHCP Static Associations** field.
2. In the **Connected hosts** field, select the **Add Connected Host** option.
3. In the **Add Connected Host** field, enter a user-defined name for the host.
4. In the **MAC Address** field, enter the MAC address of the host.
5. In the Edit the fields using the information in Table 11. field, enter the IP address of the host.
6. In the **IPv6 DUID**, enter the DHCP unique identifier for the host.
7. In the **IPv6 Host ID** field, enter the identification for the IPv6 Host.
8. Select **Save changes.**

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

To define a static IP address to be associated with the MAC address of one of your Guest Network host devices:

1. Select a LAN client device and click **Add host** in the **DHCP Static Associations** section. The Add/Edit DHCP Static Association dialog box appears (see Figure 25).

   Figure 25: Add/Edit DHCP Static Association Dialog Box



2. In the **Connected Hosts** field, select the host server to use as a static host. When a connected host is selected, the fields in the dialog box populate 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 13.

Table 13: Define a Static DHCP IP Address Association for a Guest Network Host

Field Name	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.

4. Click **Save changes**.
5. To add another static DHCP configuration, repeat steps 1 through 4.
6. To edit a static DHCP IP address:
   a. Click the blue edit button. The Add/Edit dialog box appears.
   b. Change the entries as needed and click **Save Changes**.

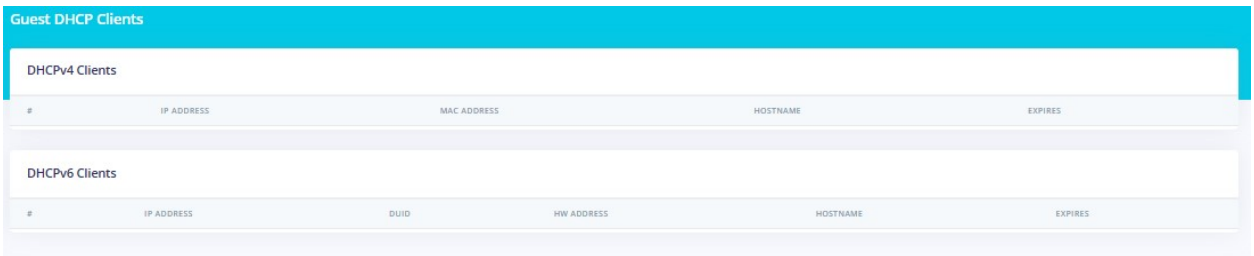
NOTE

To remove a static DHCP IP address, click the red delete button. Click **Apply** in the Pending changes dialog box.

Viewing IPv4 and IPv6 DHCP Clients

To view the IPv4 and IPv6 DHCP clients connected to your SDG, navigate to **Network > Guest Network > DHCP Clients**. The Guest DHCP Clients page appears and displays the IPv4 LAN and IPv6 LAN client devices in separate tables (see Figure 26).

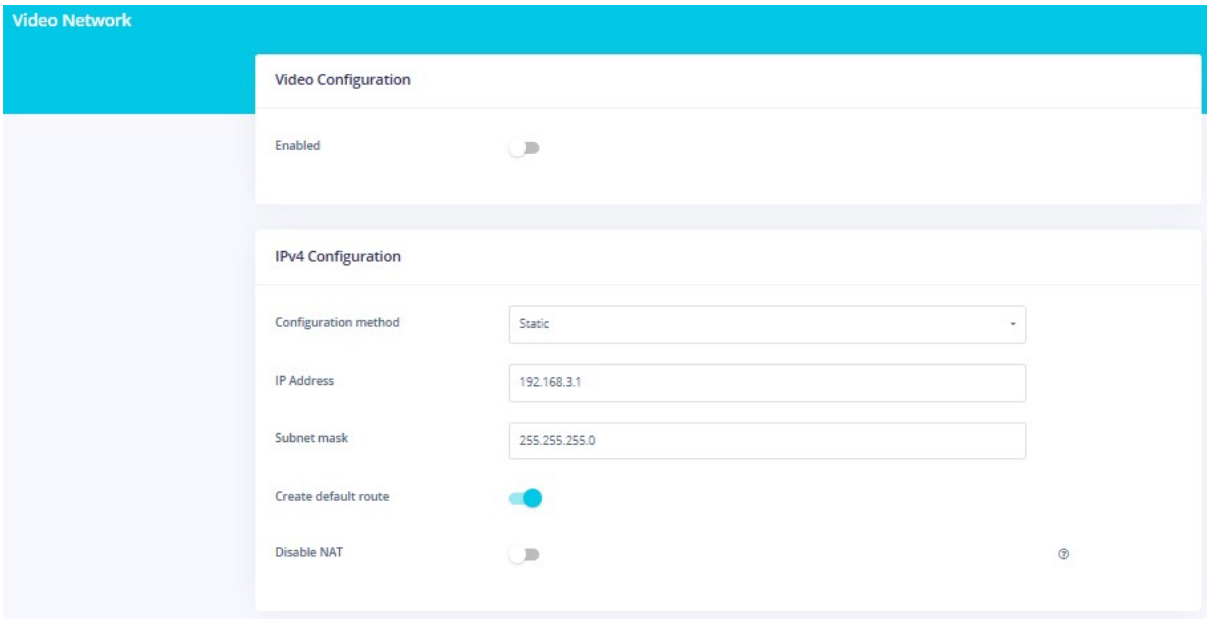
Figure 26: Guest DHCL Clients



Configuring Video Network Settings

1. Navigate to **Network > Video Network**. The Video Configuration page appears. This feature is disabled by default.

   Figure 27: Video Configuration Page



2. Use the slider to enable this feature.
3. In the **Configuration method** field, select the appropriate method for your WAN. Options are **Static**, **DHCP**, and **None**. The default is **Static**.

   The page refreshes to show the fields that apply for the selected method. If you select **None**, the other fields are hidden.
4. If you select **Static** for your **Configuration method**, complete the fields using the information in Table 14.

Table 14: Static IP Parameters for Voice

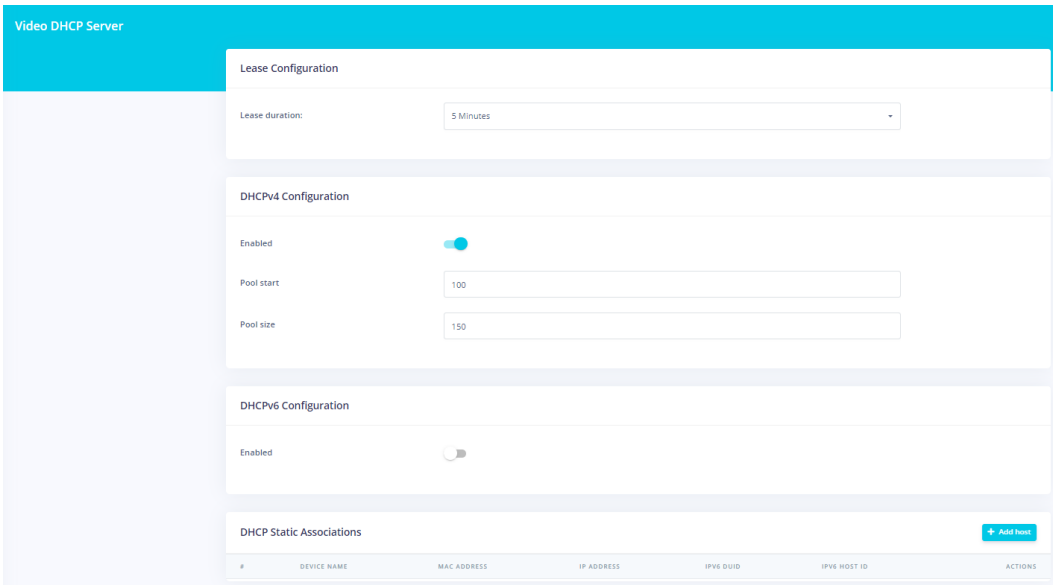
Field Name	Description
IP Address	Enter the IP address for IPv4 communications. The default IP address is **192.168.3.1.**
Subnet mask	Enter the IP address for the subnet mask.
Create default route	Use this slider to enable the default route for this network.
Disable NAT	Use this slider to disable Network Address Translation (NAT) for this network and allow normal routing.

5. (Optional) If you select **DHCP**for your **Configuration method**, enter the host name to be included in DHCP requests in the **Hostname** field.
6. Use the **Create default route** slider to enable the default route for this network.
7. Click **Apply**.

Configuring the Video DHCP Server

1. Navigate to **Network > Video Network > DHCP Server**. The Video DHCP Server page appears (see Figure 28).

Figure 28: Video DHCP Server Page



2. Complete the fields using the information in Table 15.

Table 15: DHCP Server for Voice

Field Name	Description
Lease Configuration	
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. Use this slider to disable this feature.
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. Use this slider to enable this feature.
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, see Defining a Static DHCP IP Address Association for a Video Host.

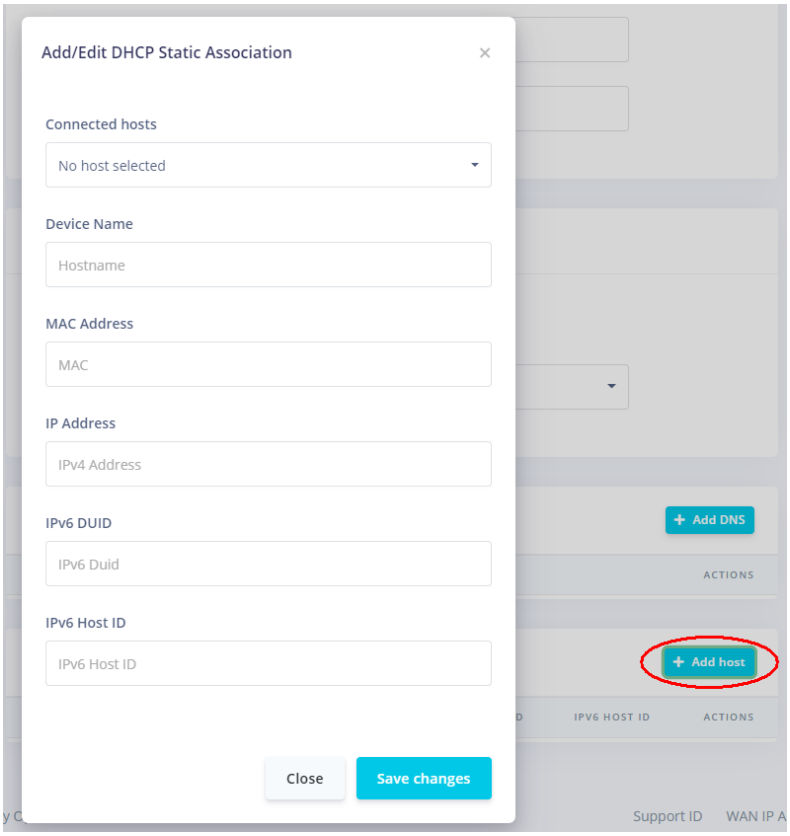
3. Click **Apply** in the Pending changes dialog box.

Defining a Static DHCP IP Address Association for a Video Host

To define a static DHCP IP address to be associated with the MAC address of a specific video host device:

1. To select a LAN client device, click **Add host** in the **DHCP Static Associations** section. The Add/Edit DHCP Static Association dialog box appears (see Figure 29).

   Figure 29: Add/Edit DHCP Static Association Dialog Box



2. In the **Connected Hosts** field, select the host server to use as a static host. When a connected host is selected, the fields in the dialog box populate 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 16.

Table 16: Defining a Static DHCP IP Address Association for a Video Host

Field Name	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.

4. Select **Save changes** to commit your changes.
5. To add another static DHCP configuration, repeat steps 1 through 4.
6. To edit a static DHCP IP address:
   a. Click the blue edit button. The **Add/Edit** dialog box appears.
   b. Change the entries as needed and click **Save Changes**.

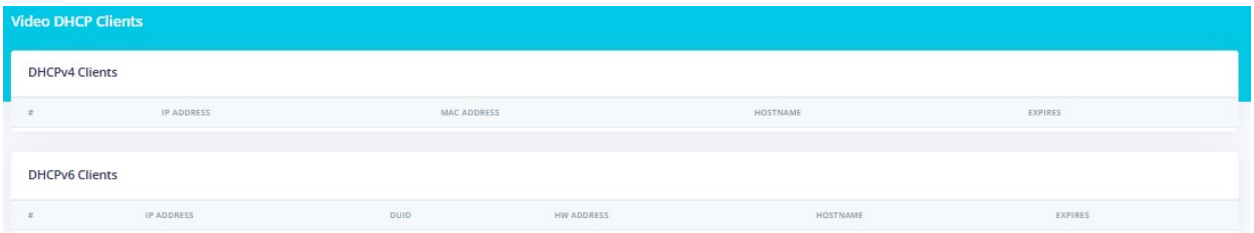
NOTE

To remove a static DHCP IP address, click the red delete button. Click **Apply** in the Pending changes dialog box.

Viewing IPv4 and IPv6 Video DHCP Clients

To view the IPv4 and IPv6 DHCP clients connected to the video network, navigate to **Network > Video Network > DHCP Clients**. The Video DHCP Clients page appears and displays the IPv4 LAN and IPv6 LAN client devices in separate tables (see Figure 30).

Figure 30: Video DHCP Clients



Specifying Wired Network Settings

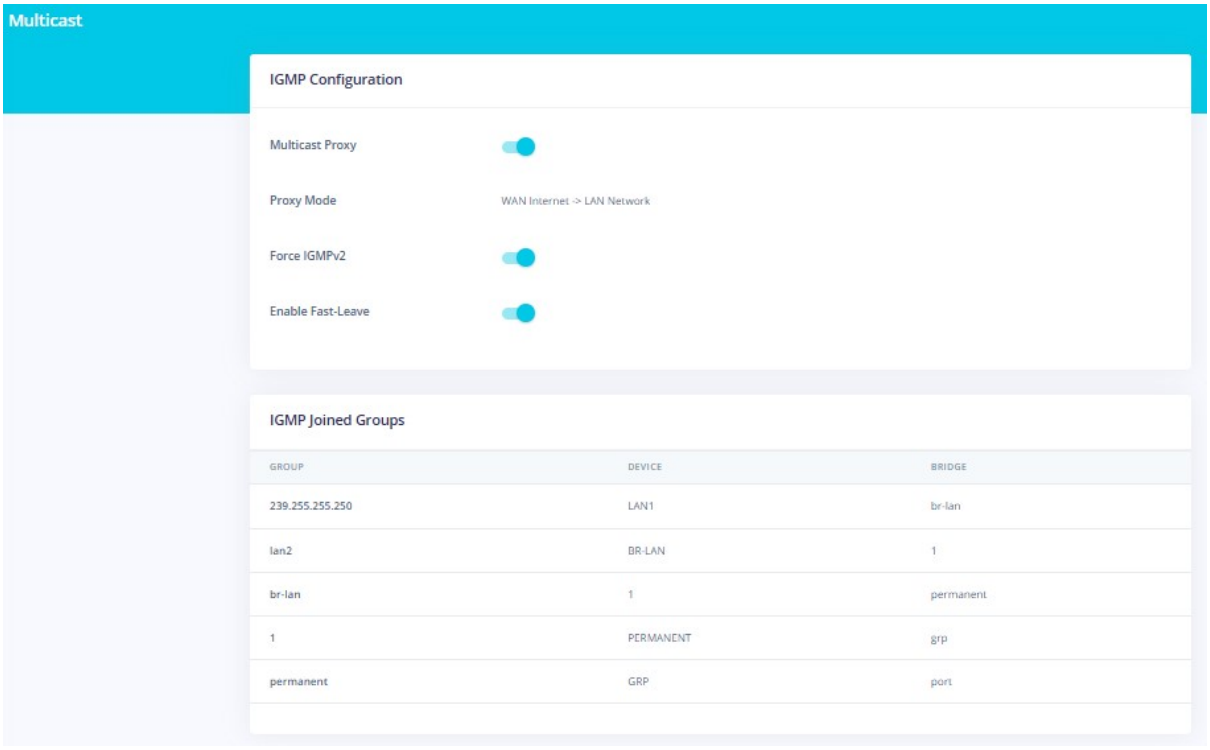
These sections provide details for configuring additional network settings:

Configuring Multicast Settings

To configure IGMP settings, such as the Fast-Leave option, and to view details of the joined groups including IP address, device name, and bridge ID:

1. Navigate to **Network > Multicast**. The Multicast page appears.

   Figure 31: Multicast Page



Complete the fields using the information in Table 17.

Table 17: Configuring Multicast Settings

Field Name	Description
Multicast Proxy	Use this slider to enable a single packet to route to multiple destinations.
Proxy Mode	Use this slider to choose between Explicit and Transparent proxy modes.
Force IGMP2	Use this slider to enable IGMP2 as a multicast option.
Enable Fast-Leave	Use this slider to enable a quicker departure from a host multicast group.
IGMP Joined Groups	
Group	These fields display information about the IGMP Group.
Device	These fields display information about the Device associated with the IGMP Group.
Bridge	These fields display information about the IGMP Bridge used for multicast message forwarding.

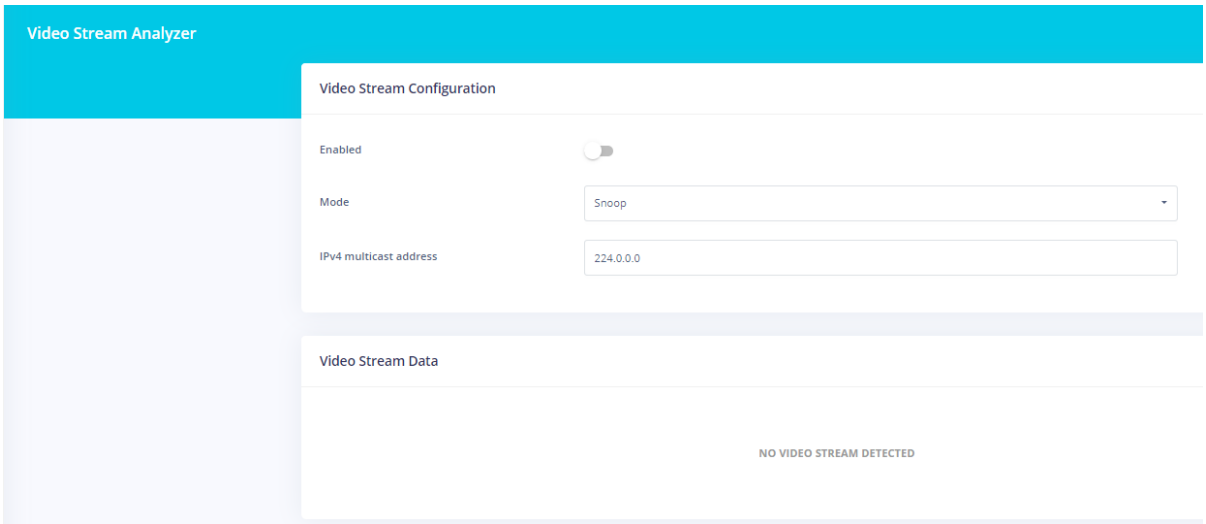
2. Both the **Force IGMPv2** and **Enable Fast-Leave** are optional.
3. Click **Apply** in the Pending changes dialog box.

Configuring Video Analyzer

To configure the IP multicast video streams:

1. Navigate to **Network > Multicast > Video Analyzer**. The Video Stream Analyzer page appears.

Figure 32: Video Stream Analyzer Page



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

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

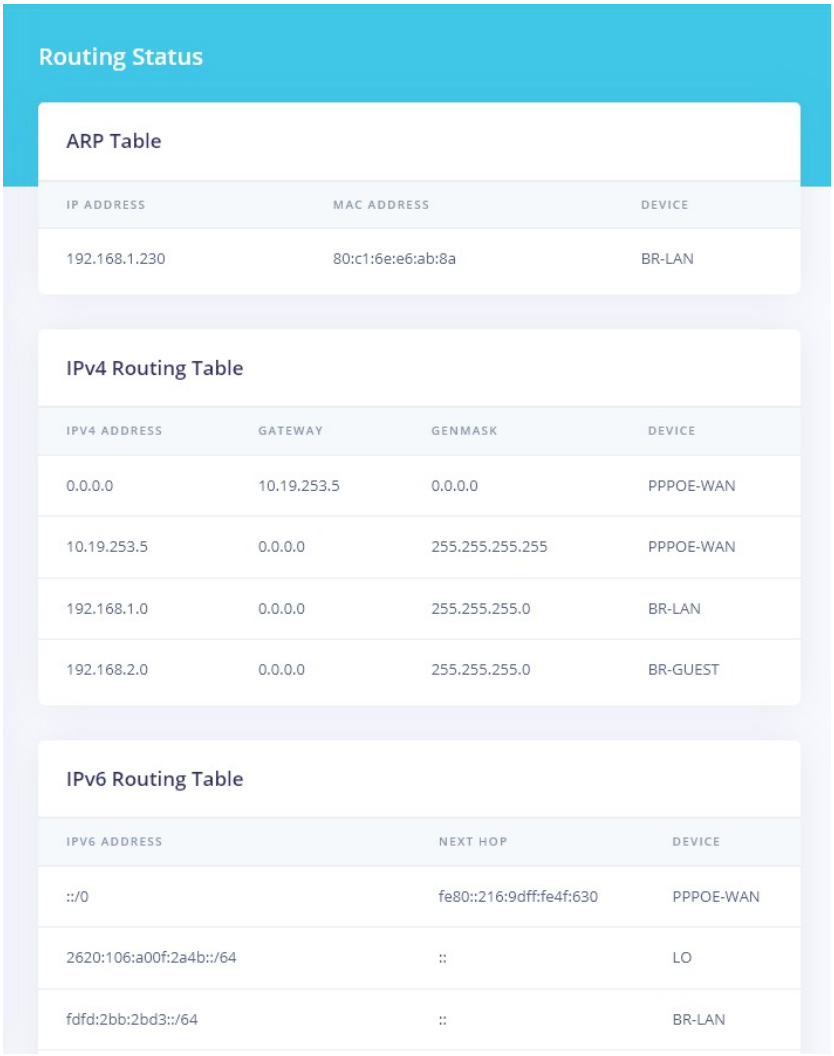
NOTE

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

Configuring Routing Settings

To view the static routes provisioned for the network, navigate to **Network** > **Routing**. The Routing Status page appears displaying the ARP Table, IPv4 Routing Table, IPv6 Routing Table and an IPv6 Neighbors Table.

Figure 33: Routing Status Page



Configuring Static Routes

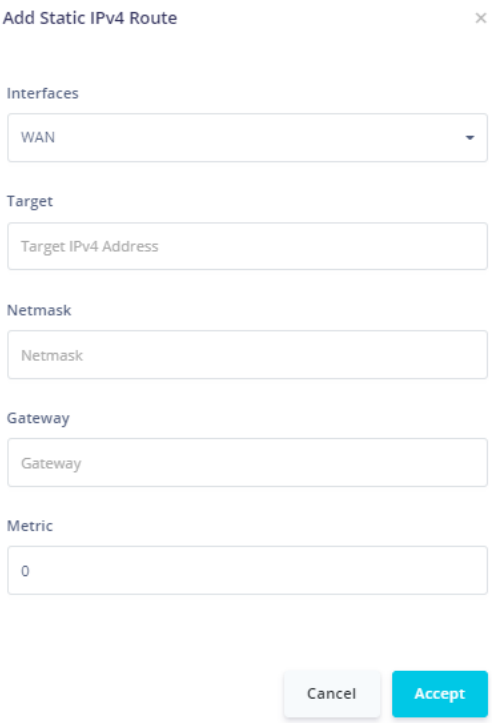
You can specify the routes over which interface and SDG for a certain host or network can be reached. When several networks are accessible from the SDG, static routes become useful to ensure packets get correctly routed between them.

To configure a static route:

1. Navigate to **Network** > **Routing** > **Static Routes**. Tables appear for both IPv4 static routes and IPv6 static routes.

2. Click **Add Route** next to the desired IP version. The appropriate Add Static IPv4 Route page appears.

Figure 34: Add Static IPv4 Route Page Example



3. Complete the fields using the information provided in Table 18.

Table 18: Add Static Route

Field Name	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. For example, enter **`192.168.1.0`** to identify that subnet as the target.
Netmask	Enter the net mask for the target IP address. This field appears for IPv4 routes only.
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. Click **Accept** and the Static Routes page appears.
5. To edit an existing route:

a. Click the blue edit button next to the appropriate route. The Add Static Route dialog box appears.

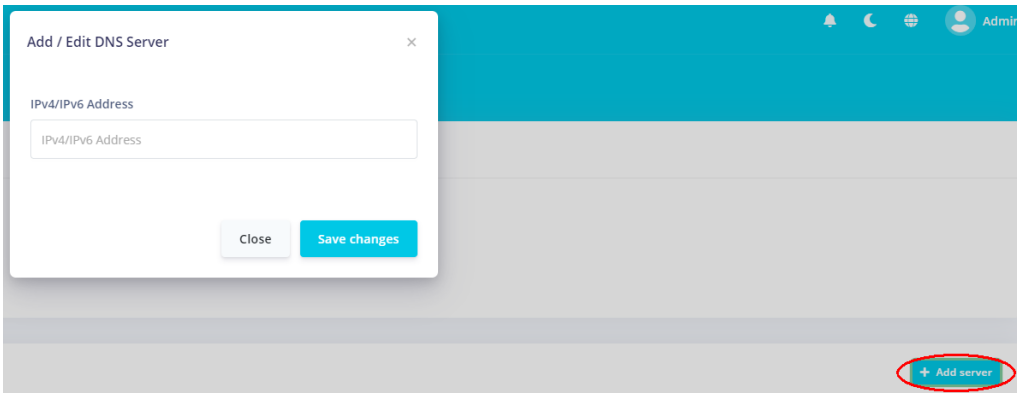
b. Modify the fields as needed and then click **Accept**.

NOTE

To delete a route, click the red delete button next to the appropriate route. Click **Apply** in the Pending changes dialog box.

Configuring Network DNS Servers

1. Navigate to **Network > Routing > DNS**.
2. Enable the **Enable Rebind Protection** slider.
   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:
   a. In the Custom DNS Servers section, click **Add server**. The Add/Edit DNS Server dialog box appears.



   b. Enter the IP address of the custom DNS server and click **Save changes**.
   c. To add another IP address, repeat steps a and b.
4. To edit a DNS server address:
   a. Click the appropriate blue edit button. The Add/Edit dialog box appears.
   b. Enter the new server address and click **Save Changes**.

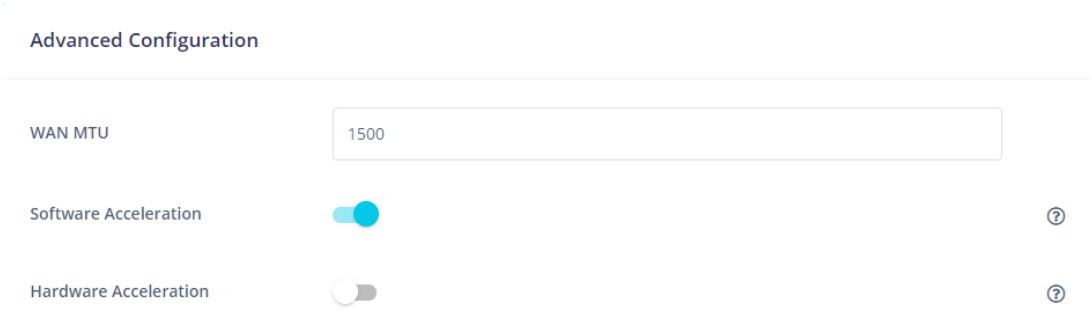
NOTE

To remove a server, click the red delete button next to the appropriate server. Click **Apply** in the Pending changes dialog box.

Configuring Advanced Settings

1. Navigate to **Network** > **Routing** > **Advanced**. The Advanced Configuration page appears see Figure 35).

   Figure 35: Advanced Configuration Page



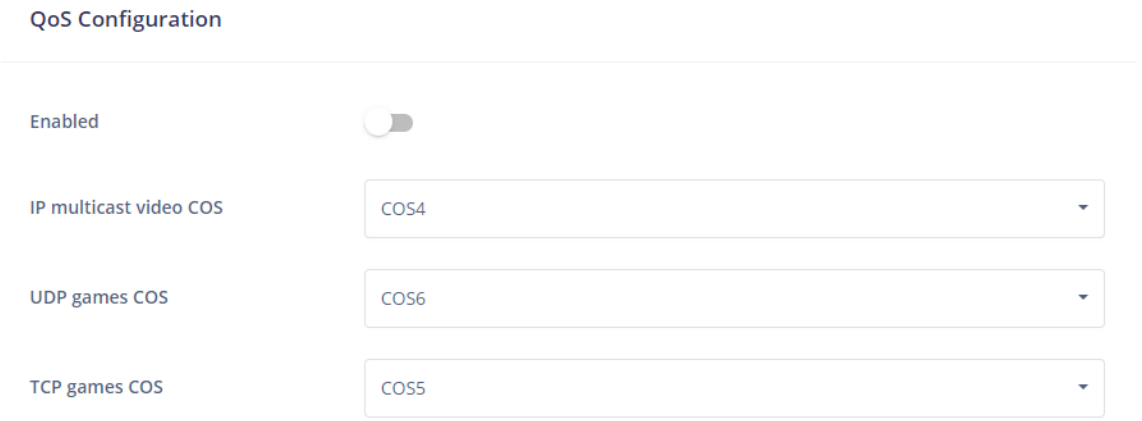
2. Enter the **WAN MTU** for the network. Options are **0** to **2048**. The default is **1500**.
3. Software acceleration of routed flows to wired LAN clients is enabled by default. Use the slider to disable software acceleration .
4. Hardware acceleration of routed flows to wired LAN clients is disabled by default. Use the slider to enable hardware acceleration.
5. Click **Apply** in the Pending changes dialog box.

Configuring Downstream QoS

This option contains both Quality of Service (QoS) and Class of Service (CoS) provisioning. QoS shapes traffic, administers policies for monitoring traffic flow, and manages congestion by prioritizing traffic. CoS operates at Layer 2 and is used to identify traffic priorities in a network, By setting CoS values (0 to 7, 0 being the lowest priority and 7 the highest) devices can sort and prioritize network traffic to improve overall performance.

To configure how traffic over wireless networks works to improve quality of service (QoS):

1. Navigate to **Network > Routing > Downstream QoS**.
   Figure 36: QoS Configuration Page



2. Use the slider to enable the QoS feature.
3. For **IP multicast video COS**, select the appropriate COS (priority) level. Options are **COS7** to **COS0**. The default value is **COS4**. The default settings work for most systems.
4. For Unity Multiplayer **(UDP) games COS**, select the appropriate COS (priority) level. Options are **COS7** to **COS0**. The default value is **COS6**. The default settings work for most systems.
5. For Transmission Control Protocol (**TCP**) **games COS**, select the appropriate COS (priority) level. Options are **COS7** to **COS0**. The default value is **COS5**. The default settings work for most systems.
6. Click **Apply** in the Pending changes dialog box.

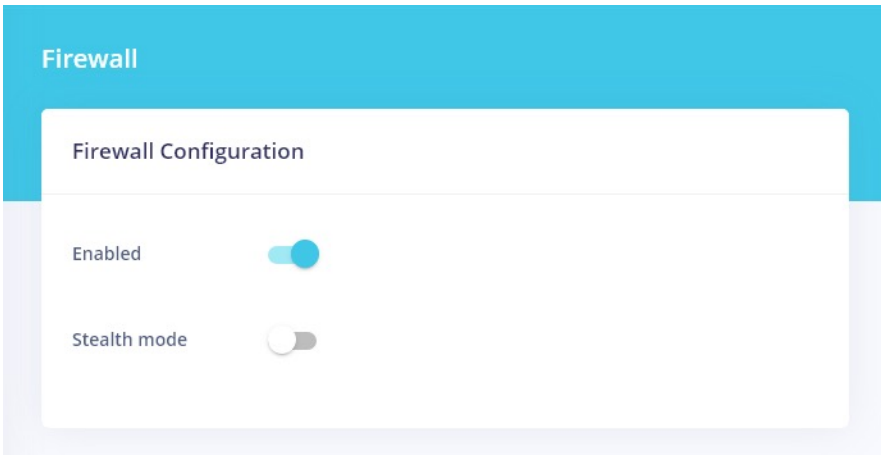
Configuring Firewall Settings

These sections provide details about the Firewall configuration elements:

Enabling the Firewall for Your System

1. Navigate to **Network** > **Firewall**. The Firewall page appears.

   Figure 37: Firewall Page

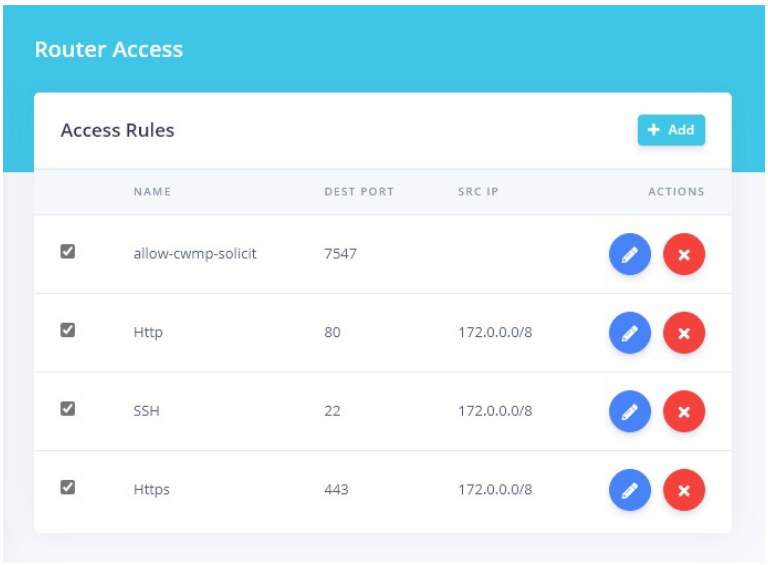


2. Disable the firewall. The firewall is enabled by default.
3. To prevent malicious users from discovering information about your network and its devices and services, enable the **Stealth mode** slider.
4. If configured for your system, the **Contact Helper** section is visible. This feature is disabled by default. Enable this slider to allow these modules to assist the firewall in tracking the various protocols used to establish traffic flow.
5. Click **Apply** in the Pending changes dialog box.

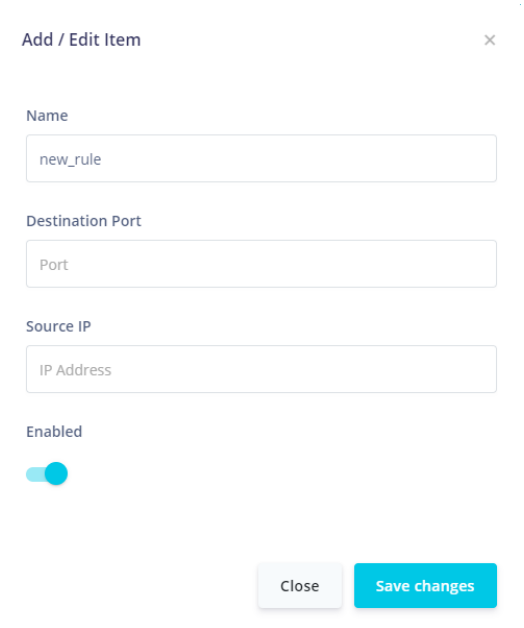
Configuring Router Access

To configure a destination port and source IP address for router access:

1. Navigate to **Network > Firewall > Router Access**. The Router Access page appears.
   Figure 38: Router Access Page



2. To add a mapping, click **Add**. The Add/Edit Item dialog box appears.
   Figure 39: Add/Edit Item Dialog Box



3. Complete the fields using the information in Table 19. All fields are optional.

Table 19: Router Access Parameters

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

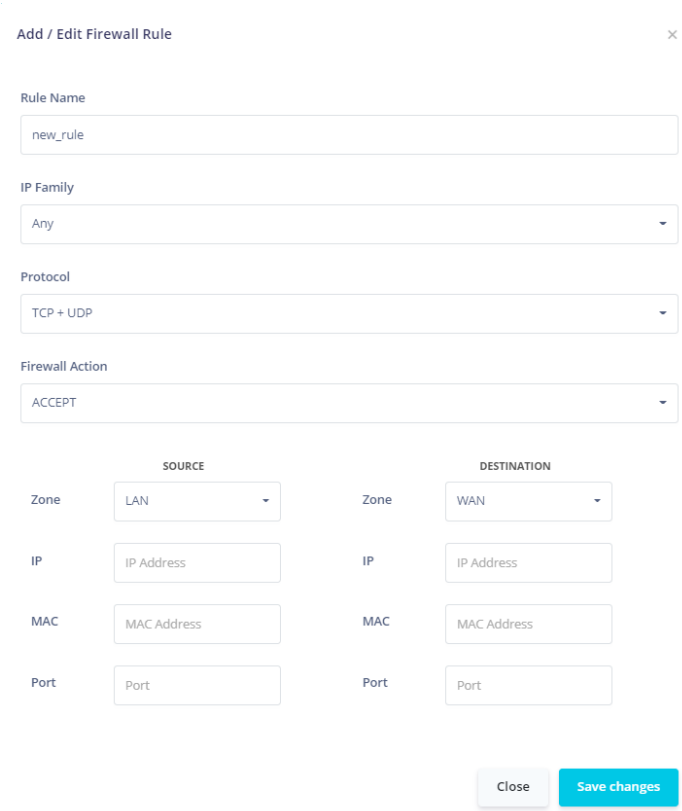
4. Click **Save changes**. The dialog box closes and the new mapping appears in the Router Access list.
5. To edit a mapping:
   a. Click the appropriate blue edit button. The Add/Edit Item dialog box appears.
   b. Modify the fields as needed and click **Save changes**. The updated values appear on the page.
6. To disable a mapping, clear the option next to the appropriate mapping. The mapping definition remains on the page but is not active.

NOTE

To remove a mapping, select the red delete button next to the appropriate mapping. Click **Apply** in the Pending changes dialog box.

Defining Firewall Rules to Filter Traffic

1. Navigate to **Network > Firewall > Rules**.
2. To create a new rule:
   a. Click **Add rule**. The Add/Edit Firewall Rule dialog box appears.
   Figure 40: Add/Edit Firewall Rule Dialog Box



   b. In the **Rule Name** field, enter a descriptive name for the rule.

c. Complete the fields using the information in Table 20.

Table 20: Add a Firewall Rule

Field Name	Description
IP Family	Select the address family. Options are **Any**, **IPv4**, and **IPv6**.
Protocol	Select the protocol for this rule. Options are **UDP**, **TCP**, **ICMP**, **TCP + UDP**, and **ESP**. 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 with this rule, such as 00236AA37CC3, 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 with this rule, such as 00236AA37CC3, 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.

d. Click **Save changes**.

3. To edit a rule:
   a. Click the appropriate blue edit button. The Add/Edit Item dialog box appears.
   b. Modify the fields as needed and click **Save changes**. The updated values appear on the page.
4. To disable a rule, clear the checkbox next to the appropriate rule. The rule remains on the page but is not active.

NOTE

To remove a rule, select the red delete button next to the appropriate rule. Click **Apply** in the Pending changes dialog box.

Configuring DMZ Settings

1. Navigate to **Network > Firewall > DMZ**. The WAN IP address shown is read-only.
2. Enable this feature.
3. In the **Host IPv4 address** field, select or enter the IP address for which unrestricted Internet access is to be allowed.

NOTE

For security reasons, Adtran recommends that you create a static IP address for the host server entered on this page.

4. Click **Apply** in the Pending changes dialog box.

Configuring Port Forwarding

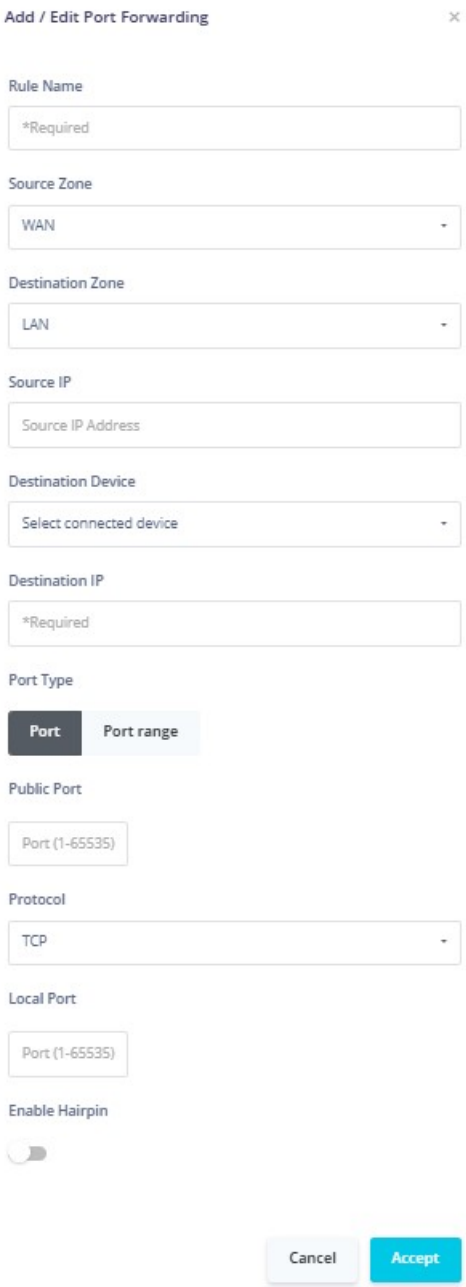
You can configure a local network device to have unrestricted access to the Internet. This is useful when local network devices cannot run an Internet application properly behind the firewall. This is also known as exposed host or virtual server.

To configure port forwarding:

1. Navigate to **Network > Firewall > Port Forwarding**.

2. To add a mapping, click **Add rule**. The Add/Edit Port Forwarding dialog box appears.

Figure 41: Add/Edit Port Forwarding Dialog Box



3. Complete the fields using the information provided in Table 21. All fields are optional.

Table 21: Add/Edit Port Forwards

Field Name	Description
Rule Name	Enter a rule name associated with Port Forwarding.

Table 21: Add/Edit Port Forwards (continued)

Field Name	Description
Source Zone	Select the source zone from the zones list 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 zones list. 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 populates when a destination device is selected. To change this address, type a different address in the field.
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** to **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** to **65535**.
Enable Hairpin	Use this slider to enable hairpin protocol.

4. Click **Accept**. The dialog box closes and the new mapping appears in the Port Forwarding list.
5. To edit a mapping:
   a. Click the appropriate blue edit button. The Add/Edit Port Forwarding dialog box appears.
   b. Modify the fields as needed, and click **Save**. The updated values appear on the page.
6. To disable a mapping, clear the appropriate mapping option. The mapping definition remains on the page but is not active.
7.

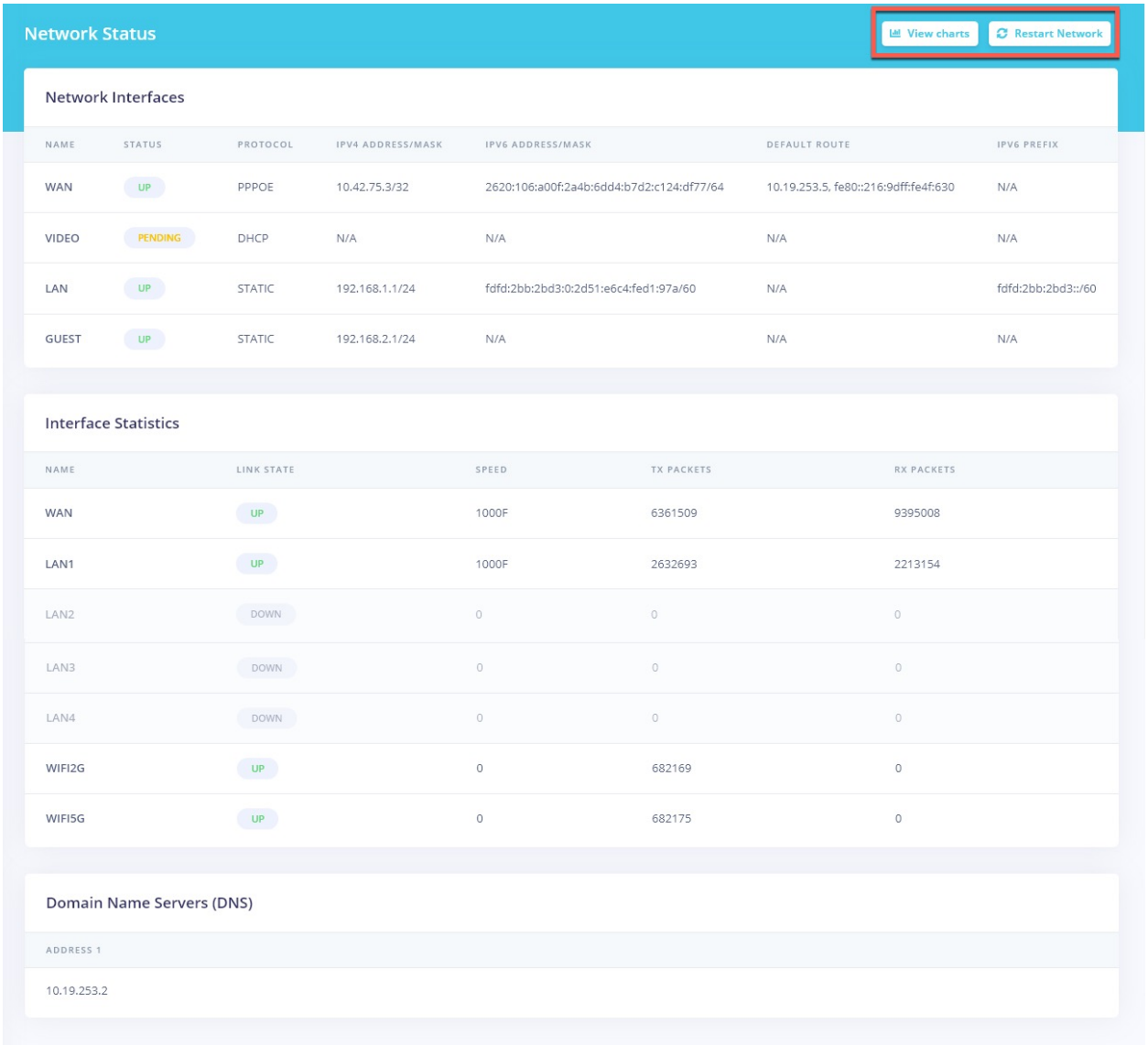
NOTE

To remove a mapping, click the red delete button next to the appropriate mapping. Click **Apply** in the Pending changes dialog box.

Viewing Network Status

To view the status and detailed information for SDG connections, navigate to **Network > Status**. The Network Status page appears.

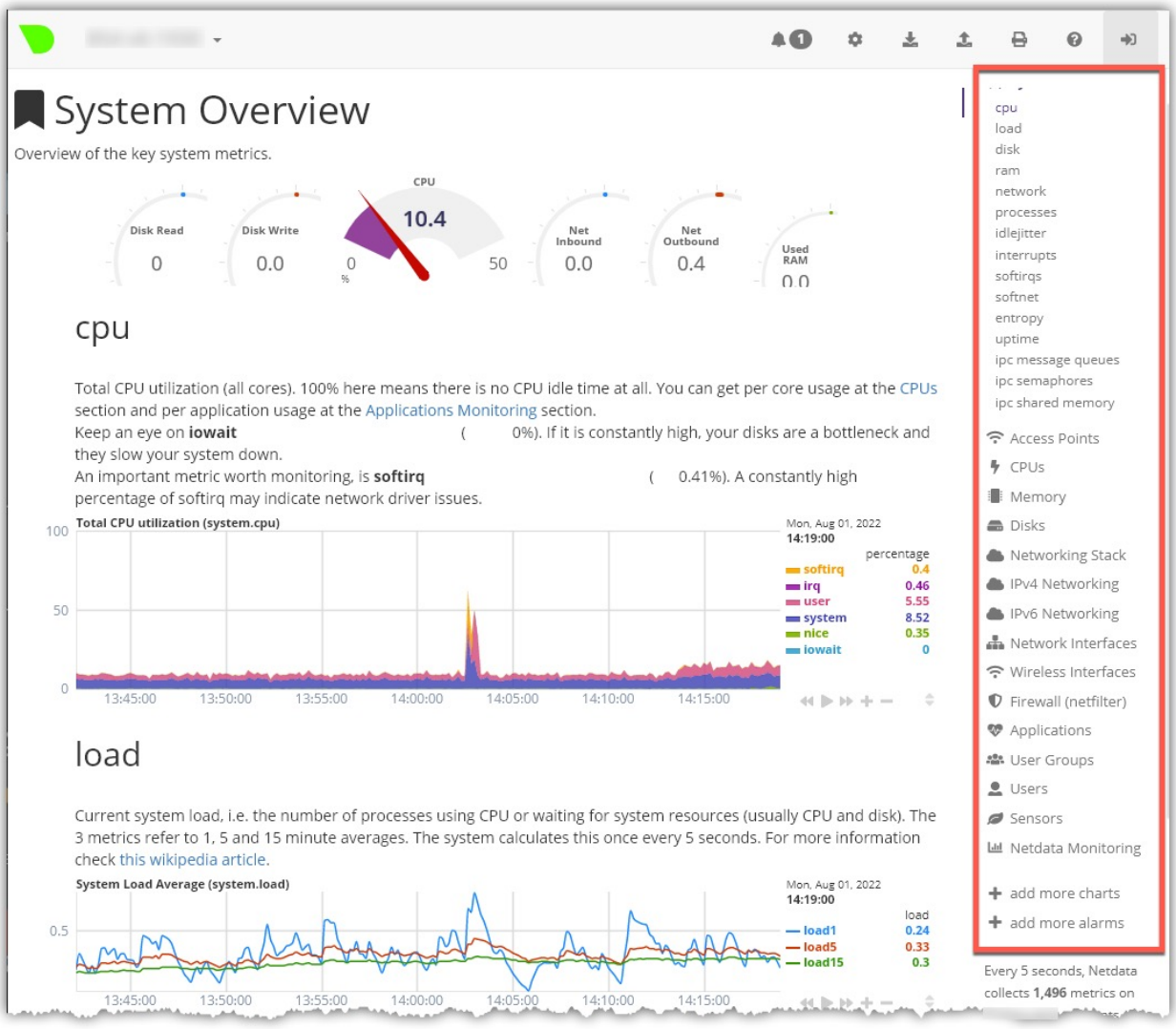
Figure 42: Network Status Page



To restart the local network, click **Restart Network**. A confirmation message appears. Click **Ok, restart** to proceed. The Status column for WAN might briefly change to Pending and then back to the previous status.

To view detailed transmission data for the individual interfaces, click **View Charts**. The netdata System Overview window opens in a new tab, showing information about the overall SDG system, memory, CPUs, firewall, IPv4 networking, and so forth. Use the navigation menu to select the statistics you want to view, as shown in Figure 43.

Figure 43: System Overview Window



Chapter 5: Configuring Wi-Fi Networks

This section contains these topics:

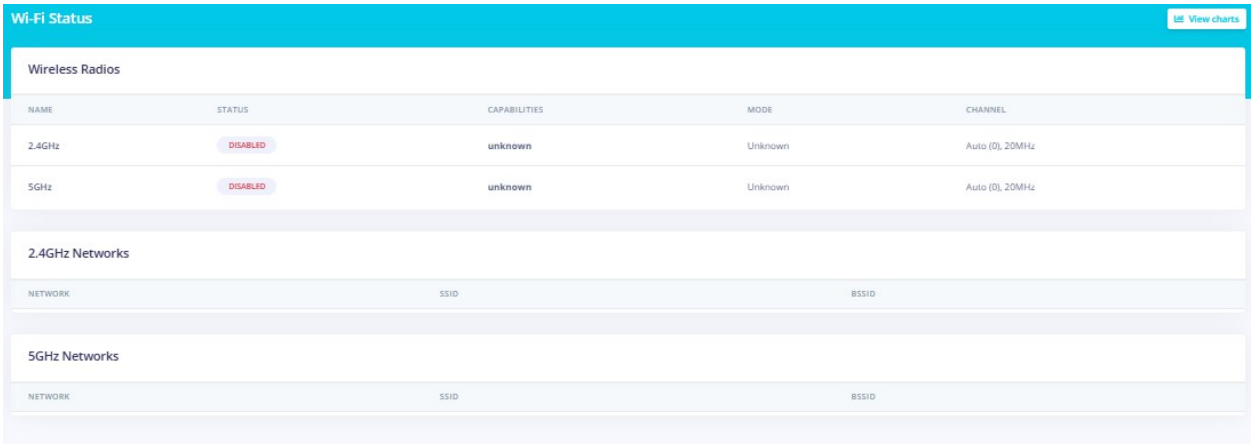
Viewing Wi-Fi Network Status and Scan for Nearby Access Points

These sections describe features associated with viewing performance information on the Wi-Fi networks configured on your SDG, as well as scanning for nearby Wi-Fi access points:

Viewing Wireless Network Status

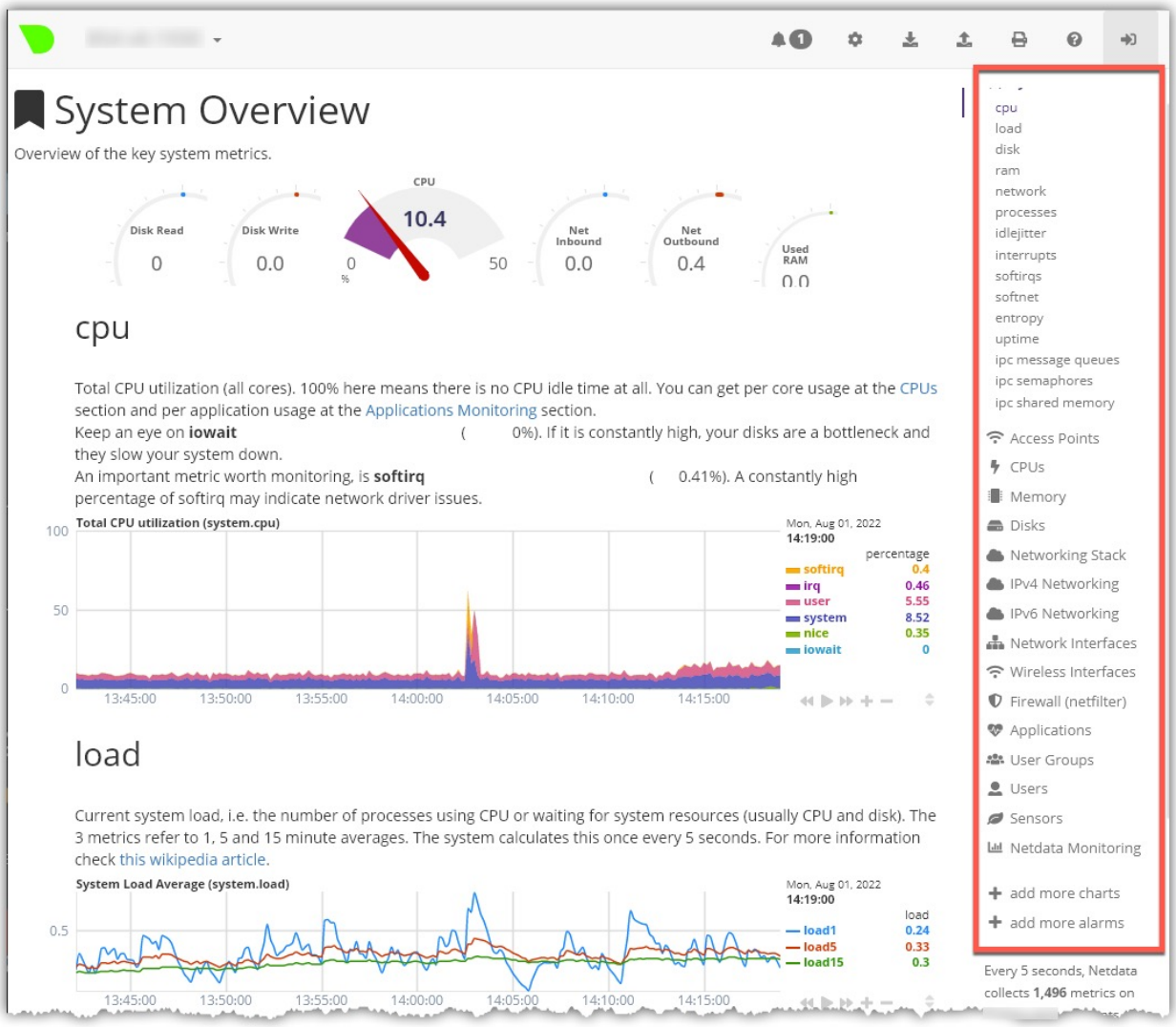
To view the status and detailed information about the wireless networks configured on your SDG, navigate to **Wi-Fi > Status**. The Wi-Fi Status page appears, providing information for the 2.4 GHz and 5 GHz wireless networks.

Figure 44: Wi-Fi Status Page



To view detailed transmission data for the individual interfaces, click **View charts**. The netdata System Overview window opens in a new tab, showing information about the overall SDG system, memory, CPUs, firewall, IPv4 networking, and so forth. Use the navigation menu to select the statistics you want to view, as shown in Figure 45.

Figure 45: System Overview Window



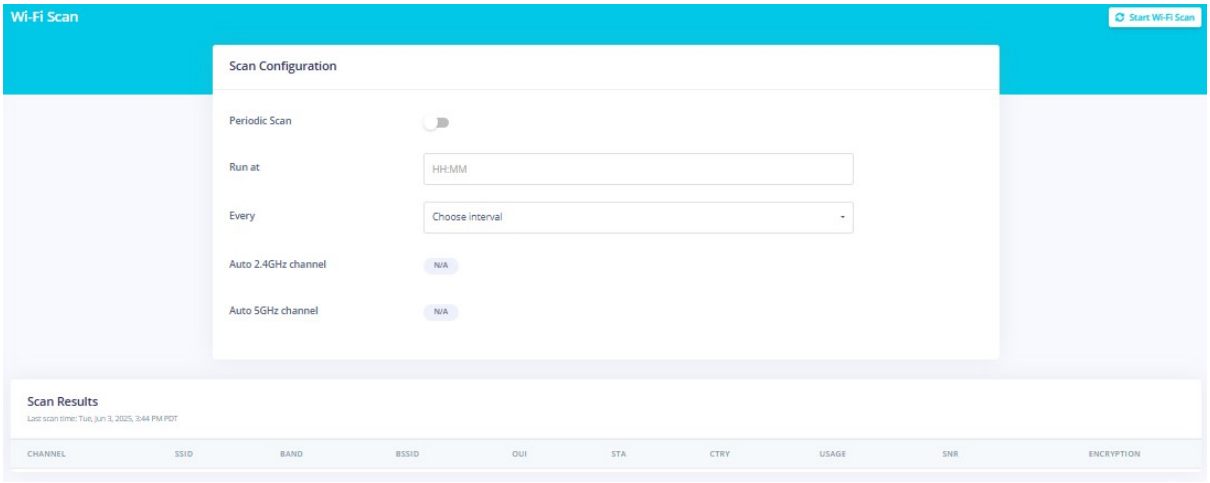
Scanning for Access Points

You can scan for nearby wireless access points. A scan can return data about the channel number, SSID, BSSID, OUI, STA, usage, signal, and encryption. In addition to other useful application, knowing the Wi-Fi channels in use by other nearby access points enables you to strategically choose a lesser utilized channel in your SDG Wi-Fi settings.

To scan for access points:

1. Navigate to **Wi-Fi > Scan**. The Scan Configuration page appears, showing the wireless access points found during the most recent scan.

Figure 46: Scan Configuration



NOTE

You can find the latest scan date and time under the Scan Configuration section, next to Last scan time. The channels currently in use by all nearby access points displayed under the **Best channel selection** field.

2. To re-scan for wireless access points near your location, click **Start Wi-Fi Scan**. The list refreshes.
3. To define how often to run a scan, enter the HH:MM in the **Run at** field.

   To define how often the scan should occur, enter the number of hours between scans in**Every** field. To disable scanning, enter **zero** (**0**) in this field. This is the default.
4. To define the time of day when the scan should occur, enter the time in hh:mm format in the **Re-scan time** field. Options are **00:01** to **23:59**. The default is **0:0** (disabled).
5. Select either the **Auto 2.4GHz channel** or the **Auto 5GHz channel** to scan.
6. Click **Apply** in the Pending changes dialog box.

Configuring Radio and SSID Settings

This section contains these topics:

Configuring Wireless Radios

You can configure 2.4 GHz or 5 GHz wireless networks for the primary SSID.

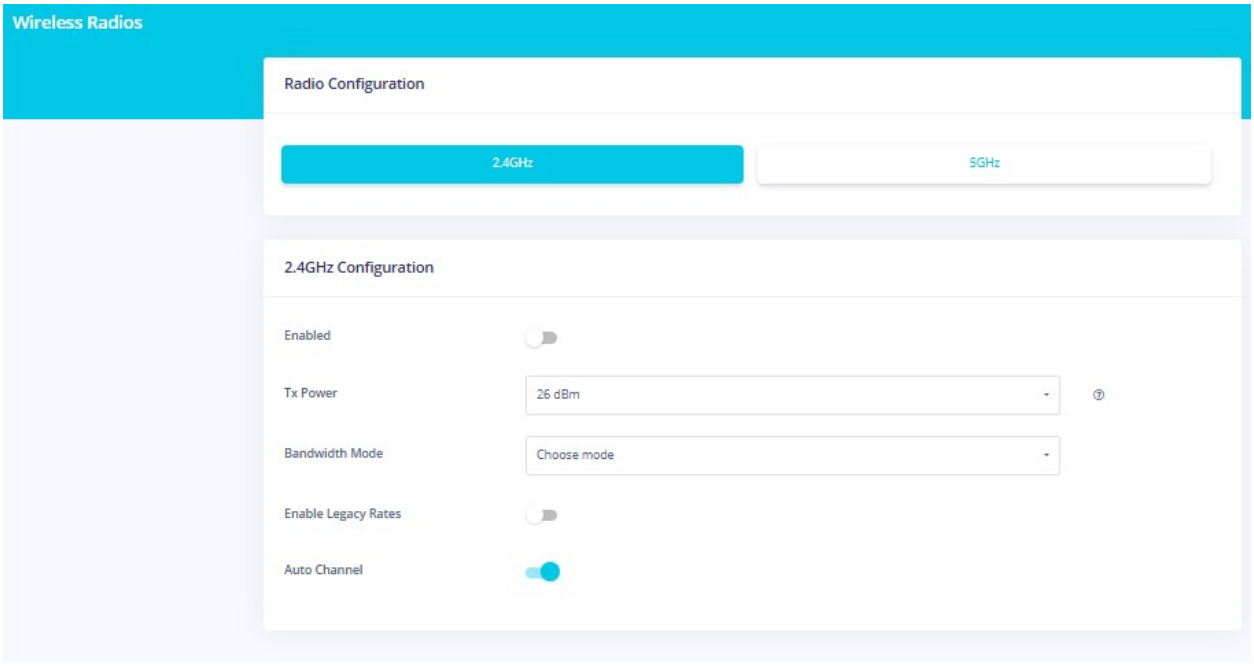
NOTE

The maximum number of connected devices for each network is 128. To connect more than 128 devices, you will need to create an additional network.

To configure a wireless radio:

1. Navigate to **Wi-Fi > Radios**. The Wireless Radios page appears, showing the fields for the 2.4 GHz radio.

Figure 47: Wireless Radios Page



NOTE

To view and adjust 5 GHz settings, click **5GHz**.

2. Complete the fields using the information in Table 22. The same fields are used for both 2.4 GHz and 5 GHz configurations.

Table 22: Radio Settings

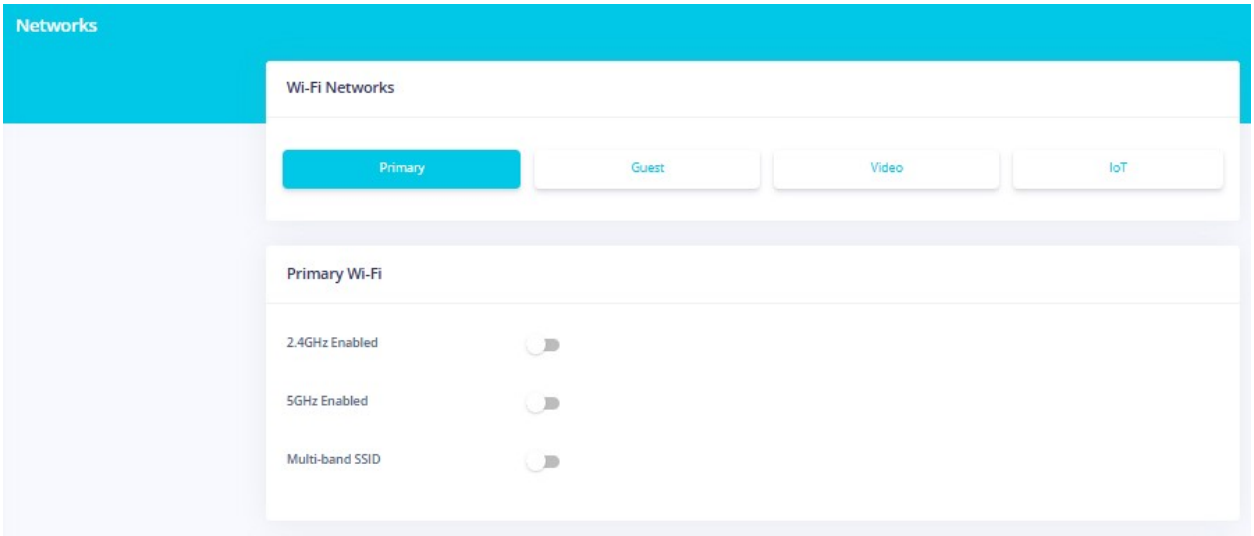
Field Name	Description
Enabled	Each radio is enabled by default. Use this slider to disable a radio.
TX Power	Select the maximum allowed transmission rate. Options range from **6 dBm (4 mw)** to **26 dBm (398 mw)**. The default is **24 dBm (251 mw)** for the 2.4 GHz radio and **22 dBm (158 mw)** for 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. Use this slider to set the SDG to cut transmission briefly when changing channels. This is useful for legacy Wi-Fi clients, enabling them to connect more effectively to a new channel.
Auto Channel	This feature is enabled by default. Use this slider to disable automatic channel selection and 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. Use this slider to allow the SDG to select the best channel for legacy clients.

3. Click **Apply** in the Pending changes dialog box.

Specifying Network Settings for Primary, Guest, Video or Mesh

To configure network settings for primary, guest, video, and mesh, navigate to **Wi-Fi > Networks**. The Networks Page appears showing the primary wireless network options as default.

Figure 48: Networks Page

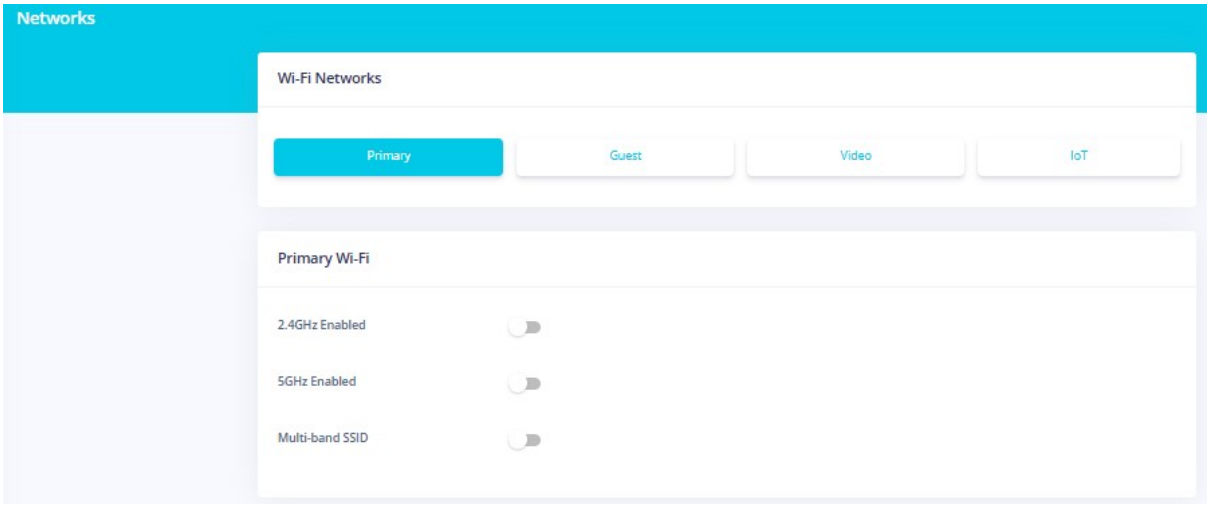


This section contains these topics:

Configuring the Primary Network

1. Navigate to **Wi-Fi > Networks**. The Networks Page appears showing the primary wireless network options as the default.

Figure 49: Networks Page



2. Complete the fields using the information provided in Table 23.

Table 23: Primary, Guest, Video, and IoT Network Settings

Field Name	Description
Primary	
Primary	This option is enabled for the **Primary** network. Use this slider to enable Wi-Fi configuration for the **Guest** and **Video** networks.
2.5GHz Enabled	This option enables 2.5GHz for these networks. Use this slider to enable this option.
5GHz Enabled	This option enables 5GHz for these networks. Use this slider to enable this option.
Multi-band SSID	This option is enabled by default. Use this slider to hide the SSID from end users. When selected, an **SSID network name** and **password** for that system are displayed.
Guest	
2.4GHz/5GHz	Description
SSID	This is the name of the WiFi networks.
Password	This is the password for these WiFi networks.
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)**.

Table 23: Primary, Guest, Video, and IoT Network Settings (continued)

Field Name	Description
Broadcast SSID	This option is enabled by default. Use this slider to hide the SSID from end users. When selected, an **SSID network name** and **password** for that system are displayed.
Client Isolation	This option is disabled by default for the **Primary** and **Video** networks and enabled for the **Guest** network. Use this slider to enable client isolation for the **Primary** or **Video** networks.
Fast Roaming (802.11r)	This option enables fast roaming which allows devices to switch between access points without needing re-authentication. Use this slider to enable this feature.

3. Click **Apply** in the Pending changes dialog box.

Configuring the Guest Network

1. Navigate to **Wi-Fi > Networks**. The Networks Page appears showing the primary wireless network options as the default.
2. Click **Guest** and the guest network configuration options appear.
3. Complete the fields using the information provided in Table 23.
4. Click **Apply** in the Pending changes dialog box.

Configuring the Video Network

1. Navigate to **Wi-Fi > Networks**. The Networks Page appears showing the primary wireless network options as the default.
2. Click **Video** and the video network configuration options appear.
3. Complete the fields using the information provided in Table 23.
4. Click **Apply** in the Pending changes dialog box.

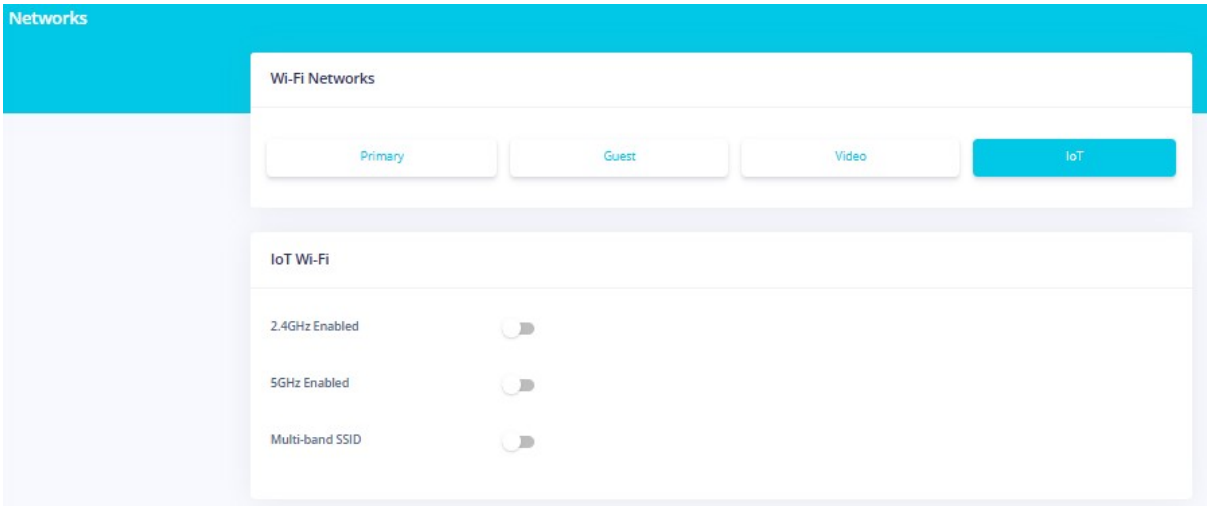
Configuring Mesh IoT

Internet of Things (IoT) is a collection of devices with processing abilities that connect and exchange data with other devices and systems over the Internet, or other communication networks.

To configure Mesh IoT:

1. Navigate to **Wi-Fi > IoT**. The WiFi Networks page appears.

   Figure 50: IoT Wi-Fi Page



2. Use the slider to enable either the 2.4 GHz or the 5GHz feature.
3. Use the slider to enable either the Multi-band SSID feature.
4. Complete the fields using the information provided in Table 23.
5. Click **Apply**.

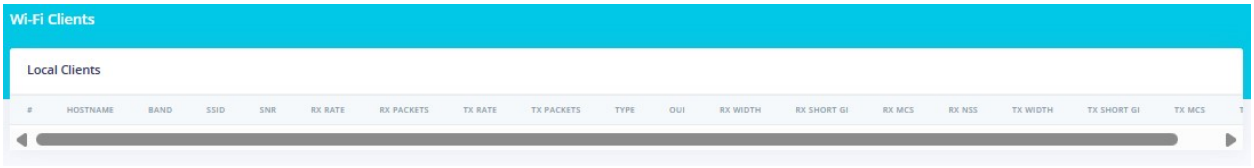
Viewing Client Connections

This section contains these topics:

Viewing Connected Clients

To view information about the clients connected to the network through wireless interfaces, navigate to **Wi-Fi > Clients**. The Wi-Fi Clients page appears, listing the clients currently connected to your network.

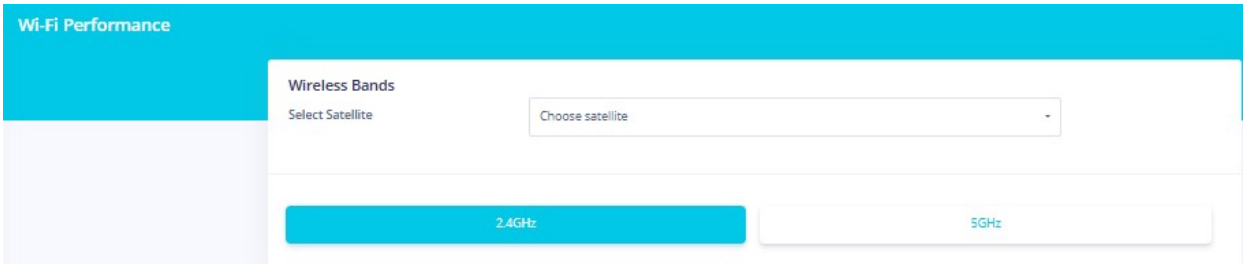
Figure 51: Wi-Fi Clients Page



Wireless Bands

To view information about wireless bands (Satellites) connected to the network, navigate to **Wi-Fi > Performance**. The Wireless Bands page appears.

Figure 52: Wireless Bands

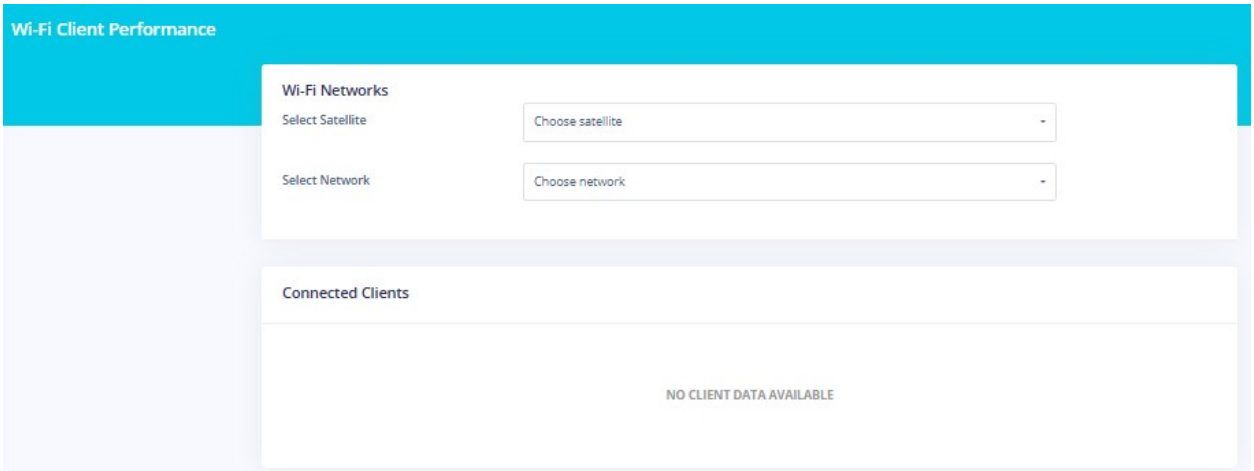


1. In the Select Satellite window, select the satellite used for wireless connectivity.
2. Select either 2.4GHz or 5GHz for the transmission speed.
3. Click **Apply**.

Client Performance

To view information about a client performance from a satellite connected to the network, navigate to **Wi-Fi > Client Performance**. The Wi-Fi Client Performance page appears.

Figure 53: Client Performance



1. In the **Select Satellite** field, choose the satellite whose performance you want to check.
2. In the **Select Network** field,

Connectivity performance for this satellite's network is displayed in the **Connected Clients** window.

Managing Client Access

You can configure whether wireless clients are allowed to access the SDG wireless network. You can achieve this by filtering using the Wi-Fi client hardware address (MAC address).

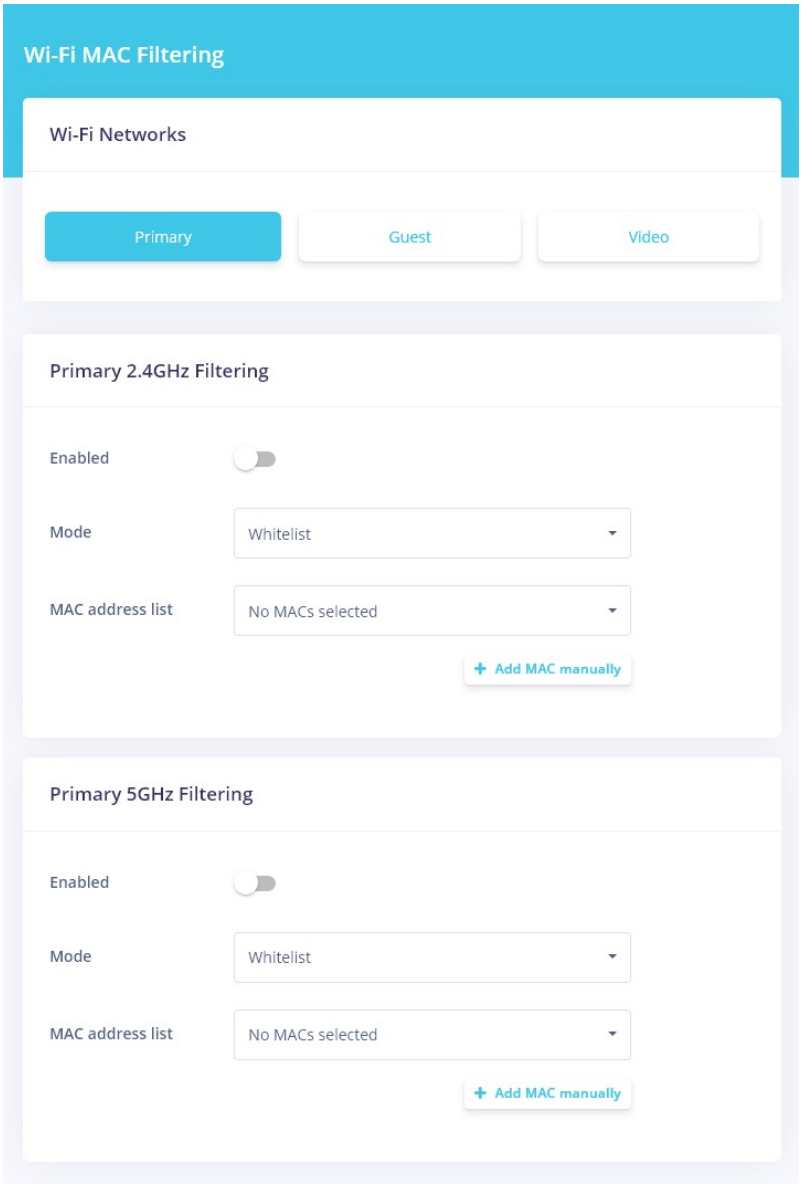
To manage client access:

1. Navigate to **Wi-Fi > MAC Filtering**. The Wi-Fi MAC Filtering page appears, showing information for the **Primary** network.

NOTE

Click **Guest, Video** or **IoT** to view information about those respective networks.

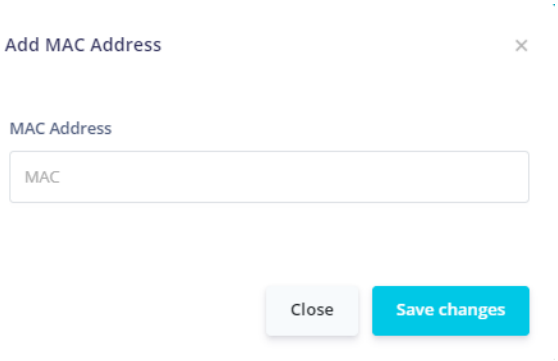
Figure 54: Wi-Fi MAC Filtering Page



2. Use the slider to enable MAC filtering for the network you want to configure — 2.4 GHz or 5 GHz.
3. In the section for the network 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.

Figure 55: Add MAC Address Dialog Box



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

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

5. To edit the label for a MAC address:

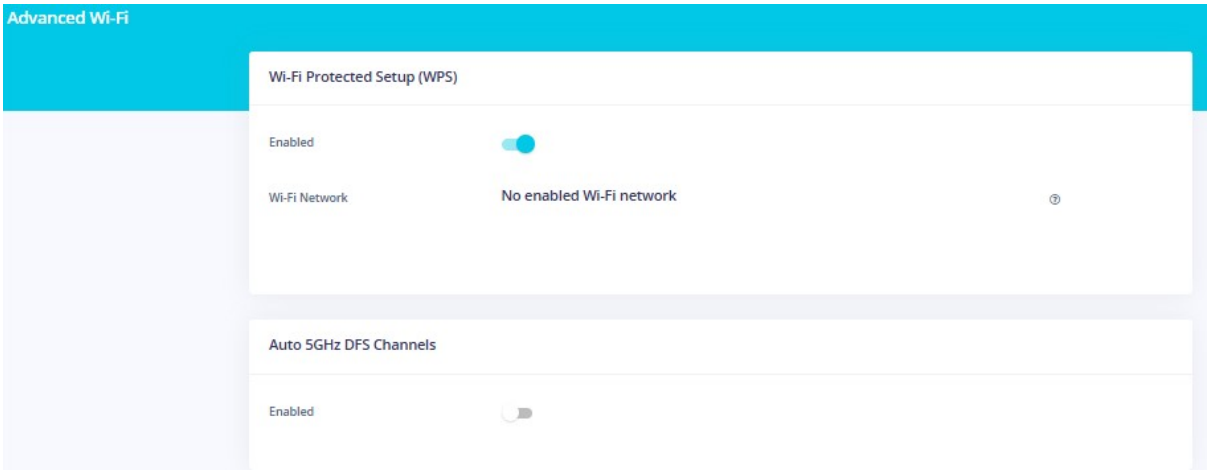
a. Click **Add/change label**. The **Add/Change Label** dialog box appears.

b. In the **Label** field, type a descriptive label and click **Save changes**.

Configuring WPS

1. Navigate to **Wi-Fi > Advanced**. The Advanced Wi-Fi page appears.

Figure 56: Advanced Wi-Fi Page



2. Disable the physical WPS button on the outside of the SDG. It is enabled by default.
3. To activate WPS on the wireless radio, click the Enable button for **Auto 5GHz WPS Channels**.
4. Click **Apply** in the Pending changes dialog box.

Viewing Wi-Fi Performance Statistics

These sections describe display statistics for various aspects of your Wi-Fi networks:

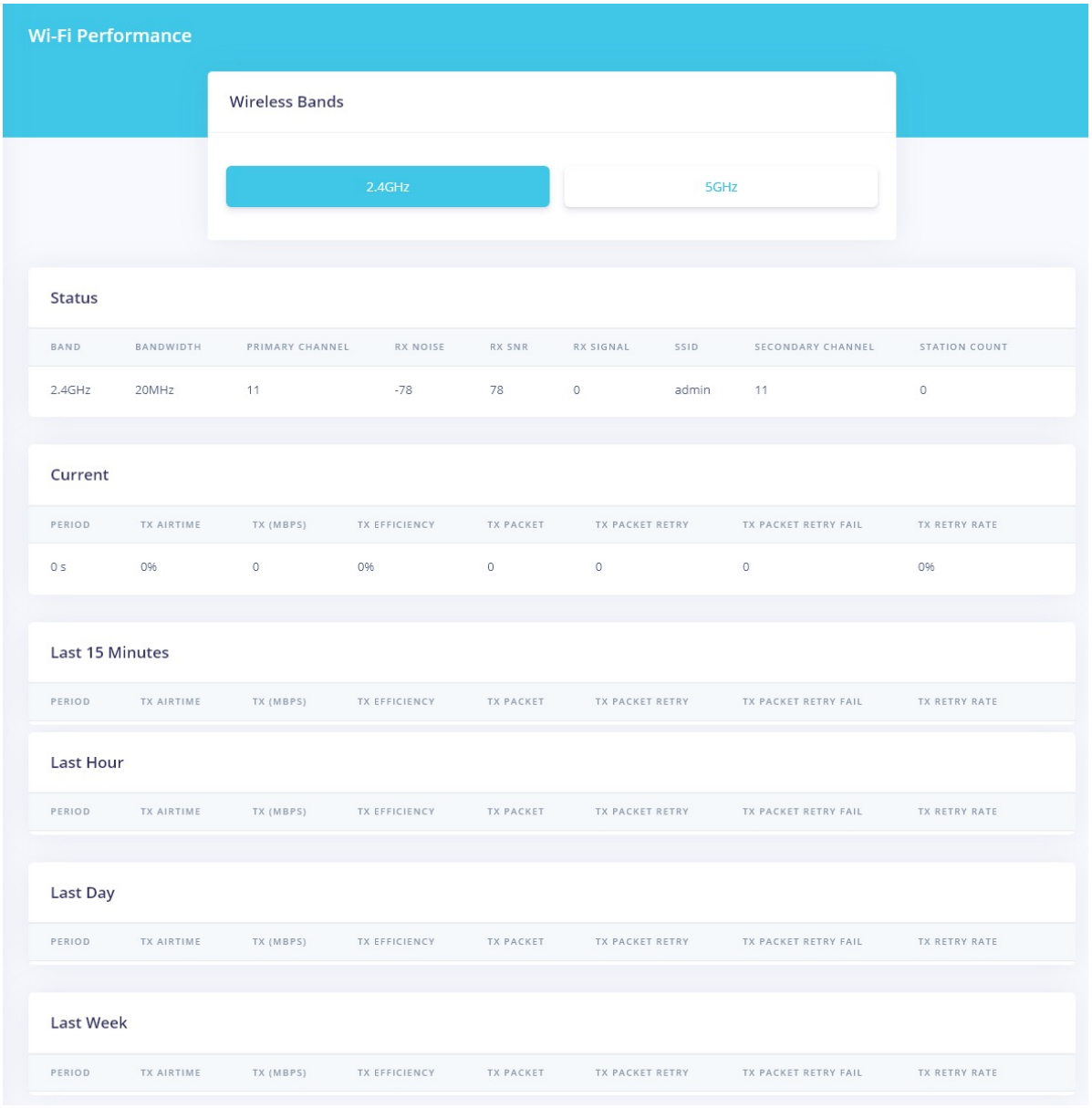
Viewing Performance Statistics

To view performance information about the wireless networks connected to your system, navigate to **Wi-Fi > Performance**. The Wi-Fi Performance page appears with the 2.4 GHz wireless network pre-selected.

NOTE

To view information about the 5 GHz network, click **5GHz**.

Figure 57: Wi-Fi Performance Page



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

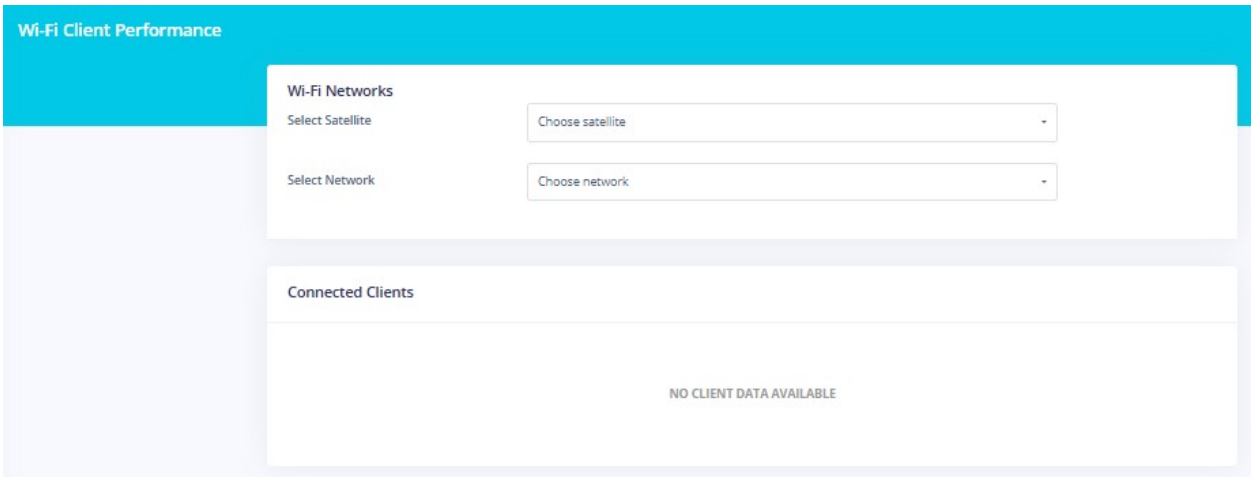
Viewing Network Status

To view information about the performance of clients connected to the network via wireless interfaces, navigate to **Wi-Fi > Client Performance**. The Wi-Fi Client Performance page appears, showing information for the LAN client devices connected to the 2.4 GHz network. As an example, Figure 58 shows the 5GHZ information.

NOTE

To view details about a different band (5GHz, and Guest [2.4GHz and 5GHz]), click the appropriate button.

Figure 58: Wi-Fi Client Performance Page



Devices

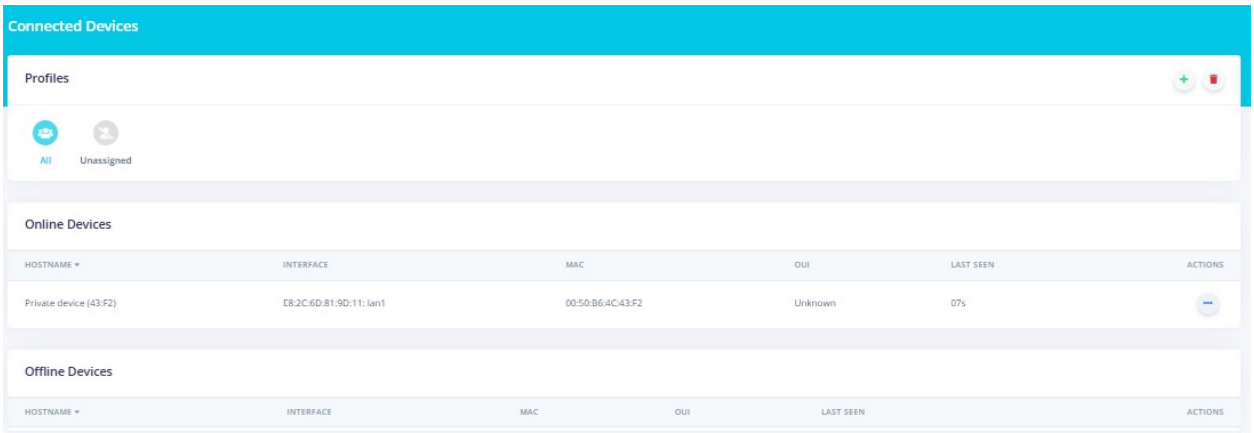
These sections describe Profiles for devices and Schedule Configuration on your Wi-Fi networks:

Online Devices

Navigate to **Devices** > **Connected Devices**. The Connected Devices profiles page appears.

This screen lists profiles for all online and offline devices.

Figure 59: Advanced Wi-Fi Page



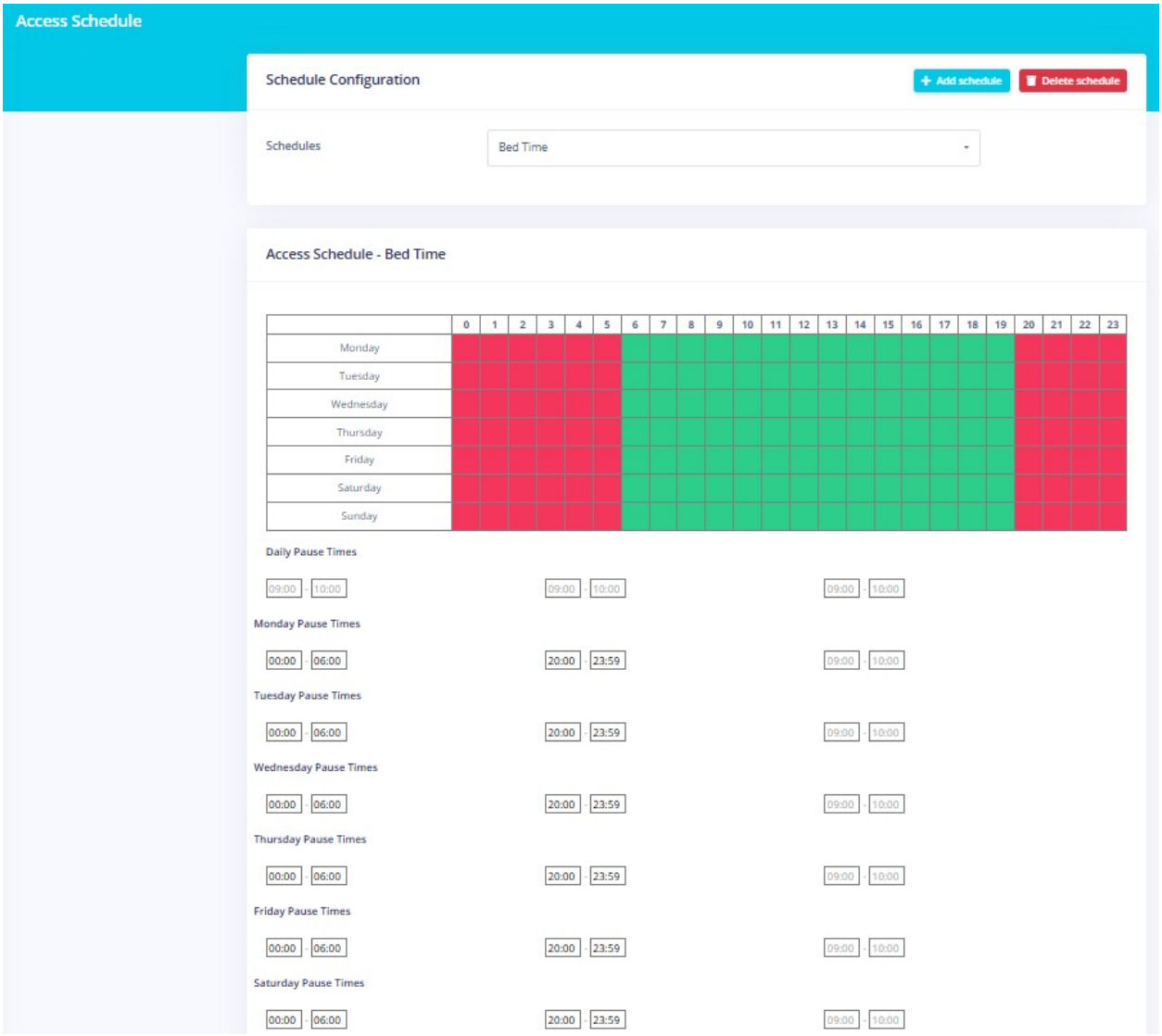
1. To display a list of all Unassigned devices, select the **Unassigned** icon.
2. Select Access schedule.
3. Determine which **Profile** you want to change and select **Save Changes**.

Access Schedule

Navigate to **Devices** > **Connected Devices**. The Schedule Configuration page appears.

This screen displays weekly schedule configuration on an hourly basis based on military time references. For example, 0 is the time between midnight and 1 a.m.; 10 is 10 a.m. 18 is 6 p.m and 22 is 11 p.m.

Figure 60: Schedule Configuration



1. To change a pre-set schedule, select **Schedules**, and select an item from the menu. The screen automatically updates.
2. To create a new schedule, select **Add schedule**.
3. Enter a new schedule name and select **Save Changes**.
4. In the **Daily Pause Time** boxes, enter the time you want the service to be unavailable. You can either pause services for an entire week, or on a daily basis.

   For example, if you want to pause services on Monday from 6 a.m to 8 p.m for the entire week, in the **Daily Pause Times** boxes, you would enter 06:00 and 20:00.

   If you wanted activate services on Wednesday from Noon to 5 p.m. you would select the **Wednesday Pause Time** boxes and enter 12:00 and 17:00.
5. Click **Apply** in the Pending changes dialog box.

Chapter 6: Configuring Network Services

This section contains these topics:

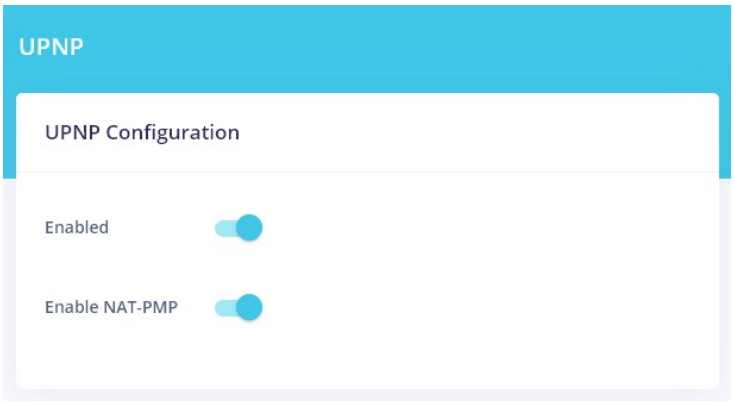
Configuring UPnP Services

You can configure the Universal Plug and Play (UPnP) 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.

To configure UPnP services:

1. Navigate to **Services** > **UPnP**. The UPNP Configuration page appears. This feature is enabled by default.

   Figure 61: Wi-Fi Page



NOTE

Use this slider to disable the UPNP Configuration feature.

2. Use the **Enable NAT-PMP** slider (Enabled by Default) to disable the automatic configuration of NAT settings.

3. Click **Apply** in the Pending changes dialog box.

Configuring CWMP

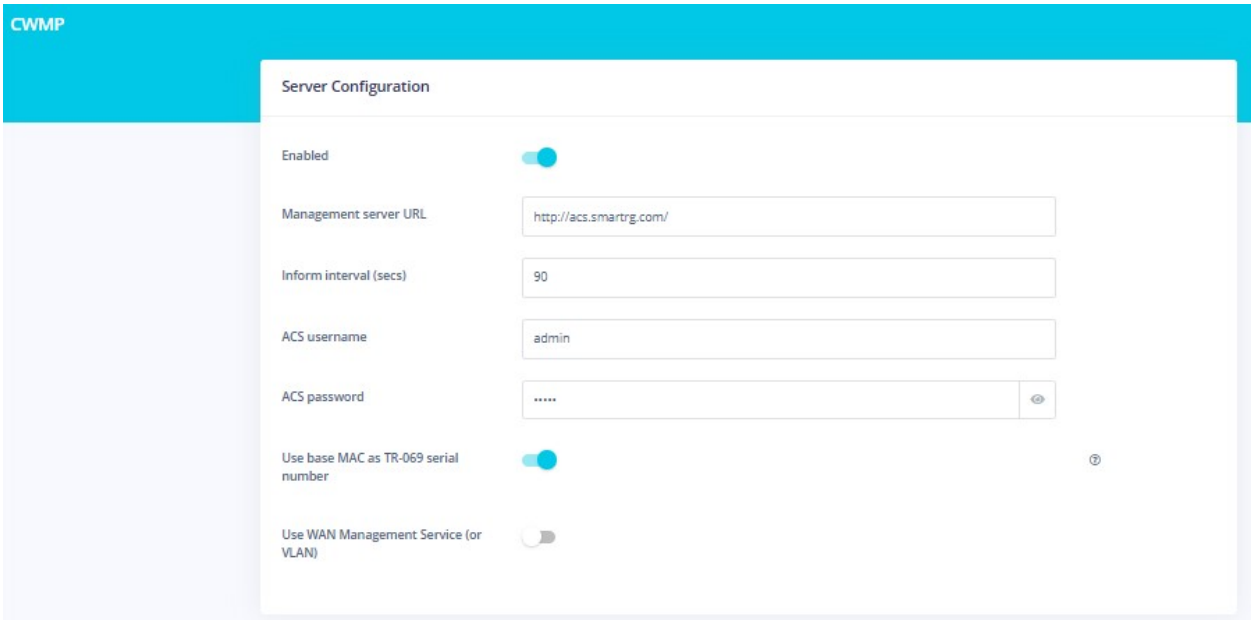
Customer Premises Equipment (CPE) Wan Management Protocol (CWMP) is a bidirectional protocol that enables communications between CPEs and auto-configured servers.

1. Navigate to **Services** > **CWMP**. The **Server Configuration** page appears (see Figure 62 through).

The Server Configuration screen consists of these three screens:

- CWMP Server Configuration
- CWMP Client Configuration
- CWMP Stun Server

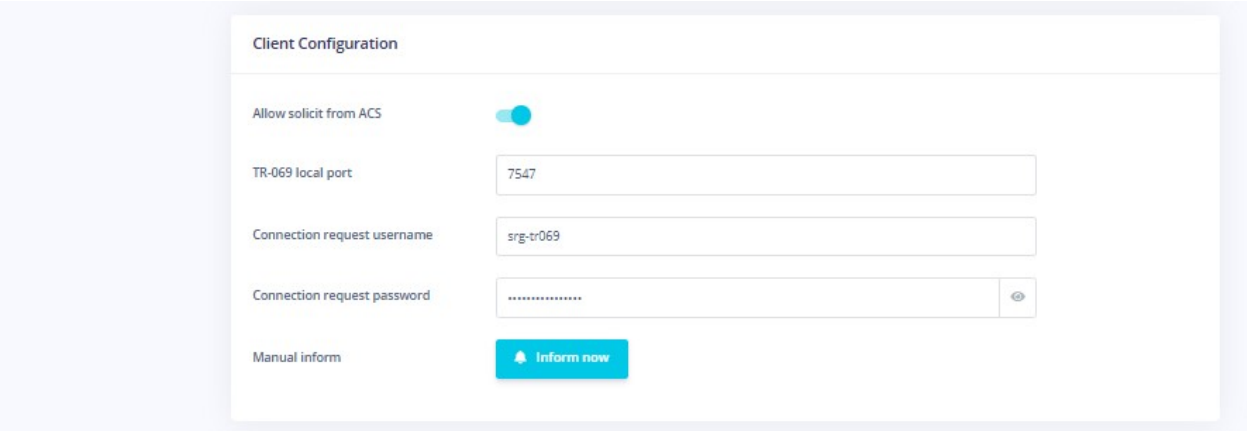
Figure 62: Server Configuration (page 1 of 3)



To provision Server Configuration, see Figure 62:

1. In the **Management server URL** field, enter the IP address for the server.
2. In the **Inform interval (secs)** field, enter the interval (in seconds) at which the CPE sends inform messages to the server.
3. In the **ACS user name** field, enter the ACS user name for the server.
4. In the **ACS password** field, enter the password the server.
5. Use the slide to enable or disable the **Use base MAC as TR-069 serial number** option. When enabled, the TR-069 serial number field is populated with the base MAC address. When disabled, the TR-069 serial number field is populated with the device serial number. The option is enabled by default.
6. Use the slide to enable **Use WAN Management Service (for VLAN)** option. WAN management is used for managing and monitoring network devices. When enabled, VLAN management will revert to WAN Management. This may require additional system configuration. The option is disabled by default.

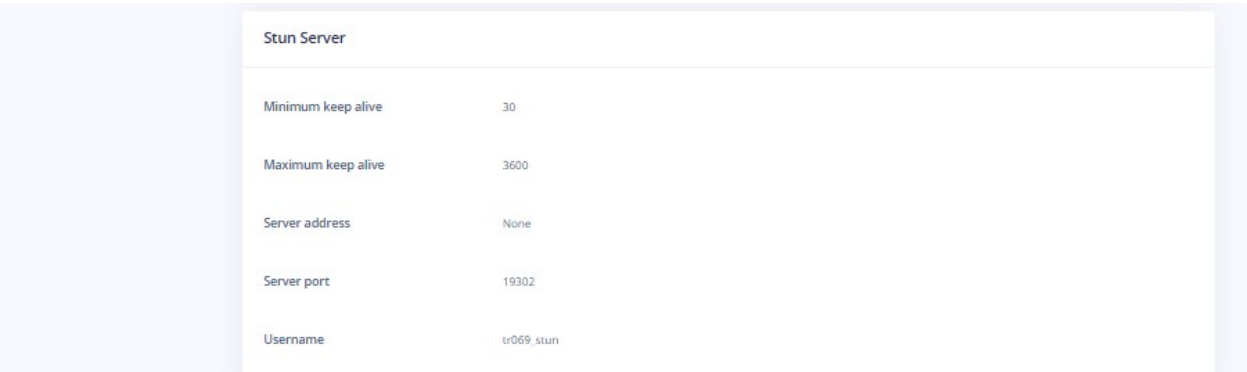
Figure 63: Server Configuration (page 2 of 3)



To provision Client Configuration, see Figure 63:

1. Use the slide to Enable **Allow solicit from ACS**. This option is enabled by default.
2. In the **TR-069 local port** field, enter the port number associated with TR-069 service.
3. In the **Connection request username**, enter the user ID for accessing the server.
4. In the **Connect ion request password**, enter the user password for accessing the server.
5. In the **Manual inform** field, select the Inform now option.

Figure 64: Server Configuration (page 3 of 3)



To provision the Stun Server, see :

1. In the **Minimum keep alive** field, enter the minimum amount of time the connection to the Stun Server will remain open
2. In the **Maximum keep alive** field, enter the maximum amount of time the connection to the Stun Server will remain open.
3. In the **Server address** field, enter the IP address of the Stun Server,
4. In the **Server port** field, enter the port on the Stun Server services are connected to.
5. In the **Username** field, enter the user name associated with the Stun server.

a. This feature is enabled by default. Disable this feature.

b. Complete the fields using the information in Table 24. Values appear in the **STUN Server** section if that feature is configured for your system.

Table 24: TR-069 Settings for ACS Connectivity

Field Name	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 populates 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. Use this slider to disable this option if you want to use the actual serial number for the device.
Client Configuration	
Allow solicit from ACS	This feature is enabled by default. Use this slider to prevent solicitation transactions from your ACS.
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 re-populates 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.	

Table 24: TR-069 Settings for ACS Connectivity (continued)

Field Name	Description
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**.
Server address	The assigned network address of the physical STUN server. The default is **None**. An invalid address produces 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 the SDG uses to access the STUN infrastructure. Maximum length is 256 characters. Special characters are allowed.

c. To connect to the ACS, click **Inform now** in the Client Configuration section.

d. Click **Apply** in the Pending changes dialog box.

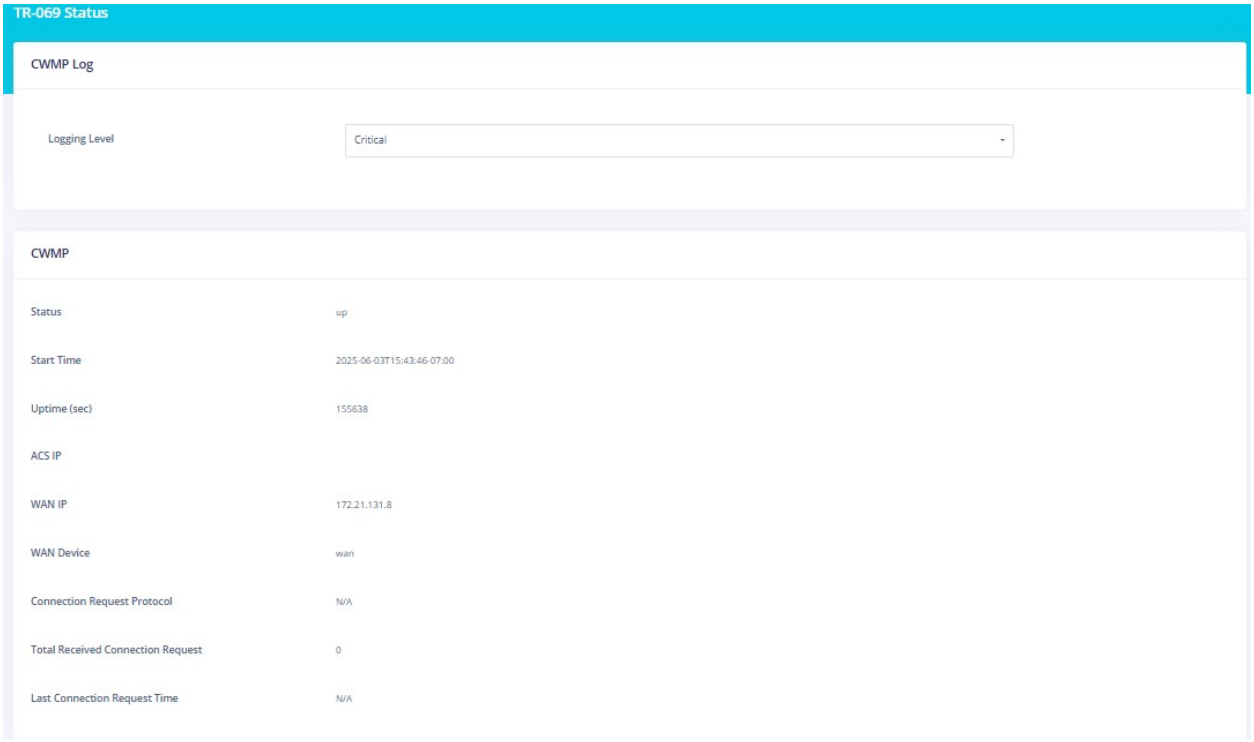
Viewing TR-069 Status table

TR-069 status monitors the CPE WAN Management Protocol (CWMP) Log for Critical, Warning, Notice, Information, and Debug logging levels. To view TR-069 status, navigate to **Services** > **CWMP** >**Status**. The TR-069 Status pages appear (see Figure 65 through Figure 68).

The TR-069 Status screen consists of the following four screens:

- CWMP Log
- Sessions
- Standard Diagnostics
- NPT Diagnostics

Figure 65: TR-069 Status (page 1 of 4)



Refer to Table 25Viewing TR-069 Status table for a description of the fields in Figure 1.

Figure 66: Sessions (Page 2 of 4)

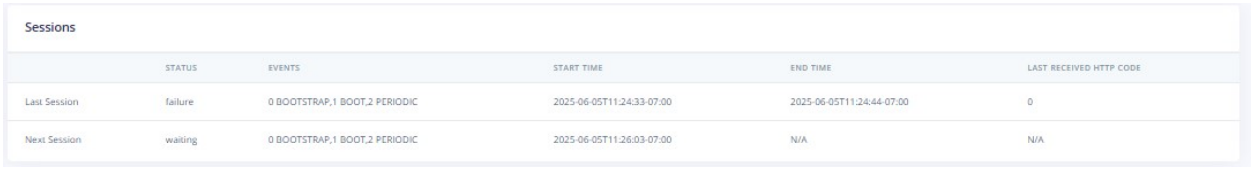


Figure 67: Standard Diagnostics (page 3 of 4)

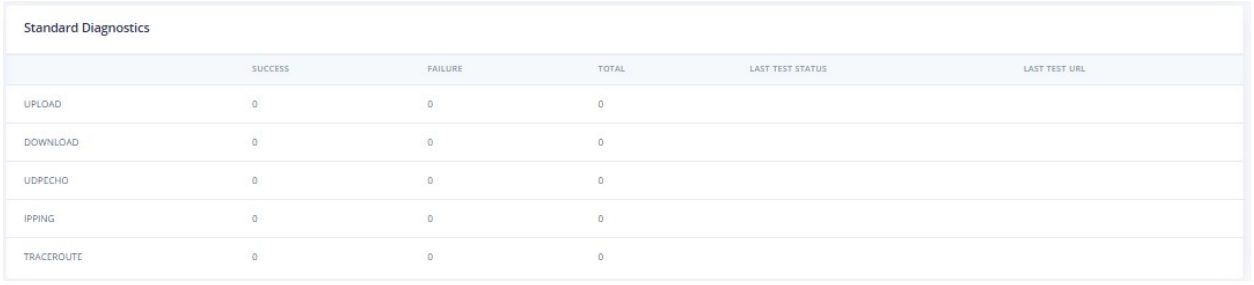


Figure 68: NPT Diagnostics Standard Diagnostics (page 4 of 4)

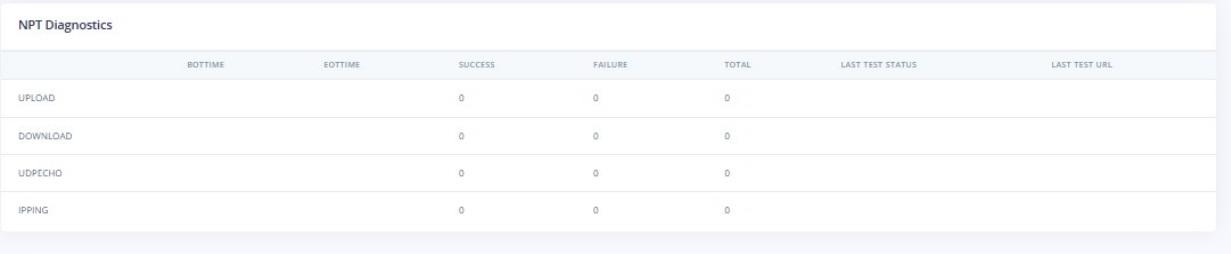


Table 25 lists all the information displayed in the TR-069 Status screens.

Table 25: TR-069 Status

Field Name	Description
CWMP Log	
Logging Level	This is level of information logged by CWMP. Possible levels are: • Critical (Default) • Warning • Notice • Information • Debug
CWMP	
Status	This is the status of the TR-069 service.
Start Time	This is the start time of the TR-069 service.
Uptime	This is the amount of time (in seconds) the connection has been available.
ACS IP	This is the IP address of the Auto Configuration Server (ACS). ACS provides secure auto-configuration between the VoIP service and the Control router.
WAN IP	This is the IP address for the WAN.
WAN Devices	This is the IP address for the server.
Connection Request Protocol	This is the protocol (normally SSL) used by the VoIP device to connect to the VoIP device.
Total Received Connection Request	This is the number of connection requests made by the VoIP device.

Table 25: TR-069 Status (continued)

Field Name	Description
Last Connection Request Time	This is the time of the last connection request sent by the VoIP device.
Sessions	
Last Session/ Next Session	Values: • Status - status of the session • Events - name of event occurring during the session • Start Time -time event started • End Time - time event ended • Last Received HTTP Code - http code from the last device identification

Table 26: TR-069 Status

Field Name	Description
Standard Diagnostics	
UPLOAD	This is the number of successful diagnostics uploads.
DOWNLOAD	This is the number of successful diagnostics downloads.
UDPECHO	This reports test and connectivity results between the VoIP client and the server.
IPPING	This is the number of IP pings the VoIP client has sent to the server.
TRACEROUTE	This is the number traceroute successes and failures between the VoIP client and the server.
NTP Diagnostics	
BOTTIME	This is the time transmissions began.
EOTTIME	This is the time transmissions ended.
UPLOAD	This is the number of successful uploads recorded by the Network Time Protocol (NTP) software.
DOWNLOAD	This is the number of successful downloads recorded by the Network Time Protocol (NTP) software.

Table 26: TR-069 Status (continued)

Field Name	Description
UDPECHO	This is the number of successful and failed communication attempts between the NTP software and the VoIP client.
IPPING	This is the number of IP pings the VoIP client has sent to the NTP software.

User Service Platform

The User Service Platform (USP) is a layer protocol and data model for remote management of connected devices. TR-369 is the technical specification that covers USP.

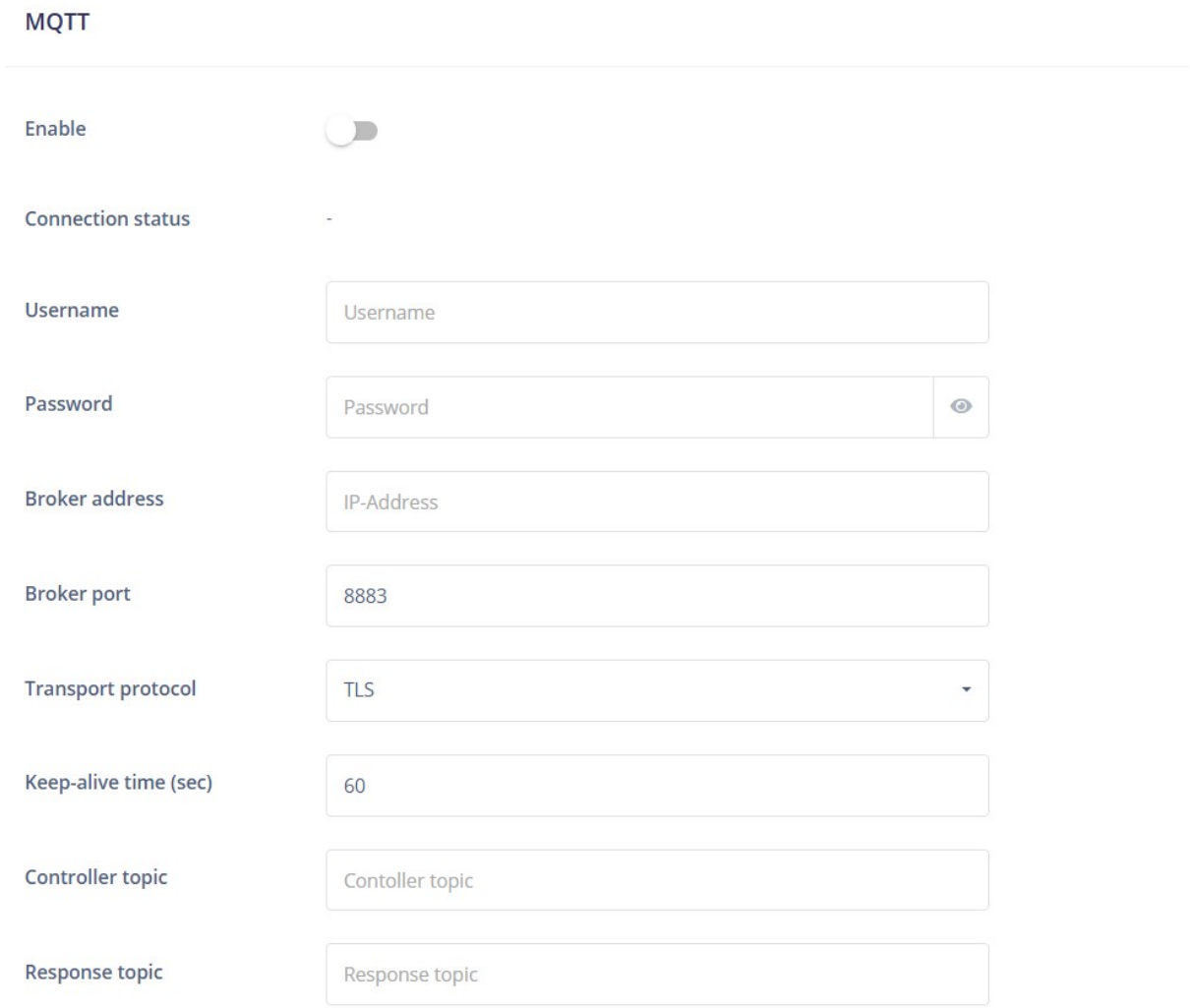
Message Queuing Telemetry Transport (MQTT) is a messaging protocol designed for communication between devices where bandwidth is limited.

To configure an USP (TR-369):

1. Navigate to **Services > USP**. The Controller page for USP (TR-369) appears.
   The TR-069 Status screen consists of these two screens (see Figure 69 and Figure 70):
   - Controller
   - MQTT

   Figure 69: Controller 1 of 2

Figure 70: Controller 2 of 2



2. Complete the fields using the information in Table 27.

Table 27: USP (TR-369)

Field Name	Description
Controller	
Endpoint ID	This is the user-defined name for the Control router that all VoIP devices are connected to through remote monitoring.
Periodic notification interval	This is the time (in seconds) between transmissions from VoIP remote devices to the Control router.
MQTT	

Table 27: USP (TR-369) (continued)

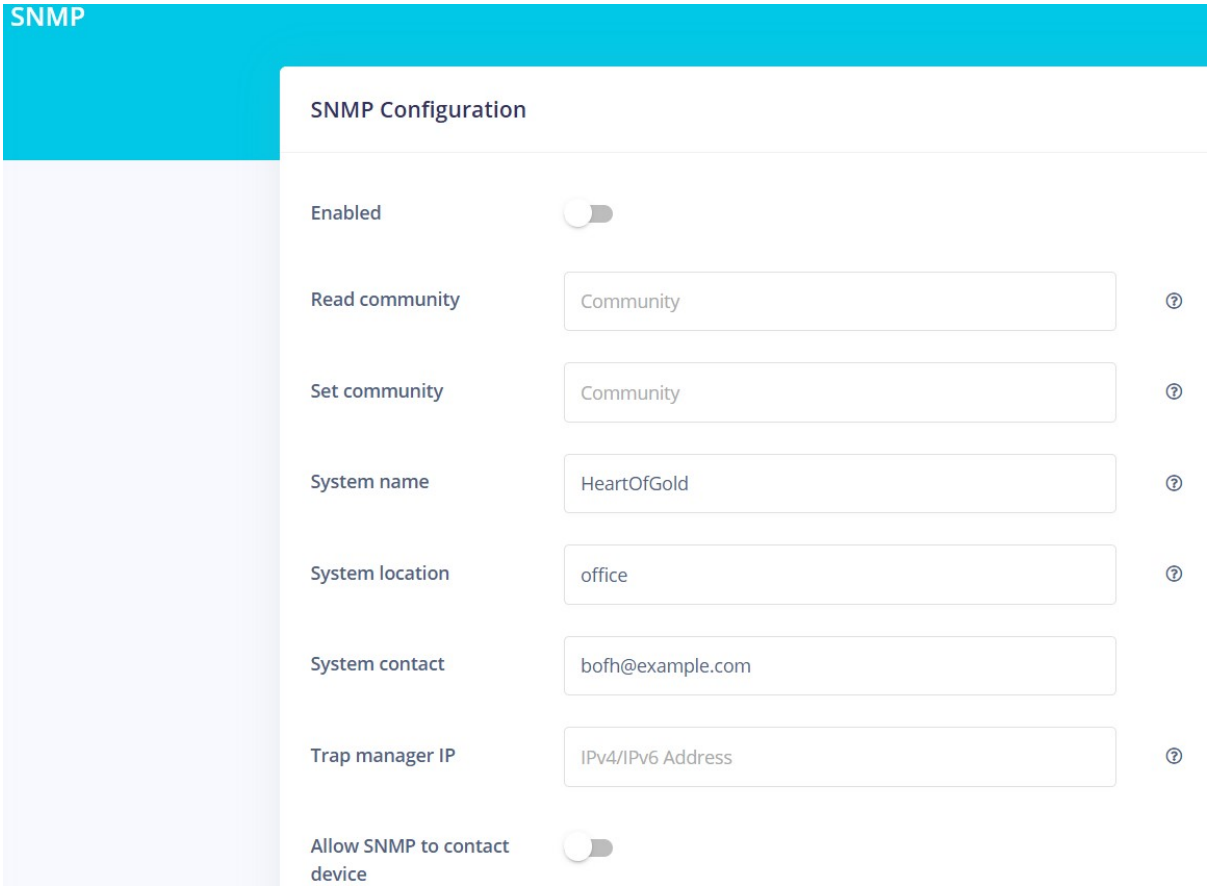
Field Name	Description
Enable	By default MOTT is Disabled. When enabled, MQTT establishes communications between multiple VoIP devices that have low bandwidth and low power requirements.
Connection status	These fields display information on VoIP devices connected to the Control router.
Username	This is the user-defined name for the VoIP device.
Password	This is the user-defined password for the VoIP device.
Broker address	This is the IP address of the central hub in the MQTT architecture. This device receives input and filters that input to the VoIP network.
Broker port	This is the port on the Control router that transmits information to the VoIP devices. The default is 8883.
Transport protocol	This is the transport protocol used by all devices in the VoIP network. Available options are: • TLS (Default) • TCP/IP
Keep-alive time (sec)	This refers to the interval when the Control router sends messages to VoIP devices to determine connectivity. The Default is 60 seconds.
Controller topic	This is a user-defined identification that enables the Control router to route messages based on this identifier. However, the VoIP device must have a the same "Response topic" (see below) as the Controller topic.
Response topic	This is a user-defined identification that enables a VoIP device to receive conformation from the Controller.

3. Click **Apply** in the Pending changes dialog box

Configuring SNMP Services

1. Navigate to **Services > SNMP**. The SNMP Configuration page appears (see Figure 71).

Figure 71: SNMP Configuration



2. Use the **Enabled** slider to enabled this service.
3. In the **Read community** field, enter a community identifier for SNMP network.
4. In the **Set community** field, enter a community identifier for the SNMP device.
5. In the **System name** field, enter a user-defined name for your system.
6. In the **System location** field, enter the location of your device .
7. In the **System contact** field, enter the email address of the person responsible for administering this network.
8. In the **Trap manager IP** field, enter the IP address for the IPv4 or IPv6 management software.
9. Enable the **Allow SNMP to contact device** slider.
10. Click **Apply** in the Pending changes dialog box.

11. Complete the fields using the information in Table 28. All fields are optional.

Table 28: SNMP Conf

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 preferred, modify the name of the SDG.
System location	If preferred, 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. Use this slider to enable this option.

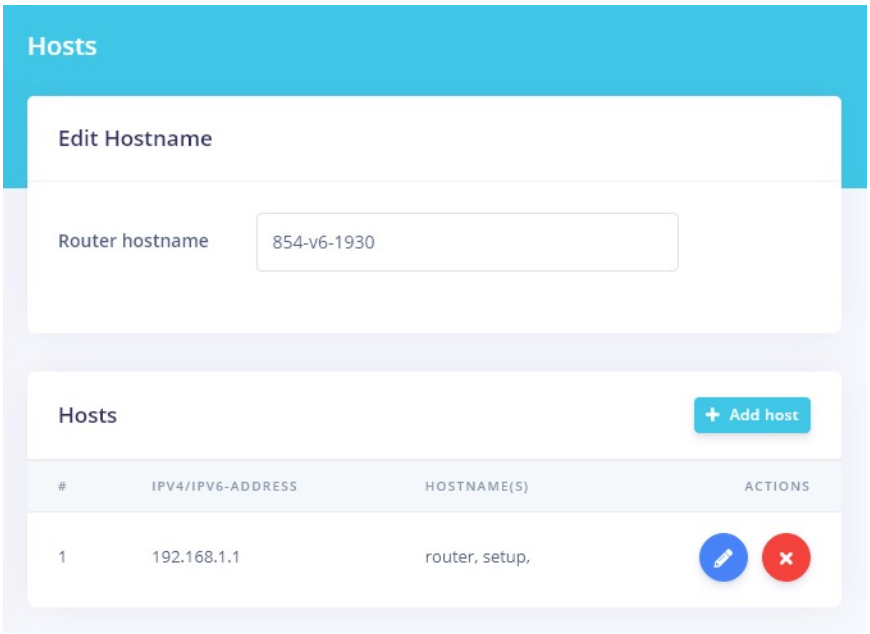
12. Click **Apply** in the Pending changes dialog box.

Configuring Hosts Services

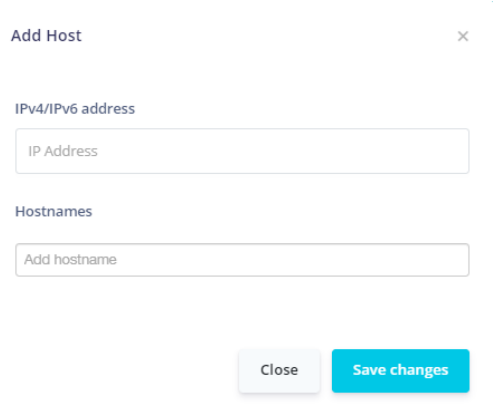
You can configure the hostname of the SDG and add IP addresses for other hosts on the SDG.

To configure the host servers in the **Network:**

1. Navigate to **Services > Hosts**. The Hosts page appears (see Figure 73).
   Figure 72: Hosts Page



2. To add a host:
   a. Click **Add Host**. The **Add Host** dialog box appears (see Figure 73),
      Figure 73: Add Host Dialog Box



   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. Spaces are not permitted.

The name is added and the cursor moves to a new **Add hostname** entry field. To add more hosts, repeat this step as needed.

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

d. Click **Save changes**.

3. To edit the details of a host:

a. Click the blue edit button next to the appropriate host. The **Add/Edit Item** dialog box appears.

b. Modify the fields as needed.

c. Click **Save changes**.

NOTE

To delete a host, click the red delete button next to the appropriate host. Click **Apply** in the Pending changes dialog box.

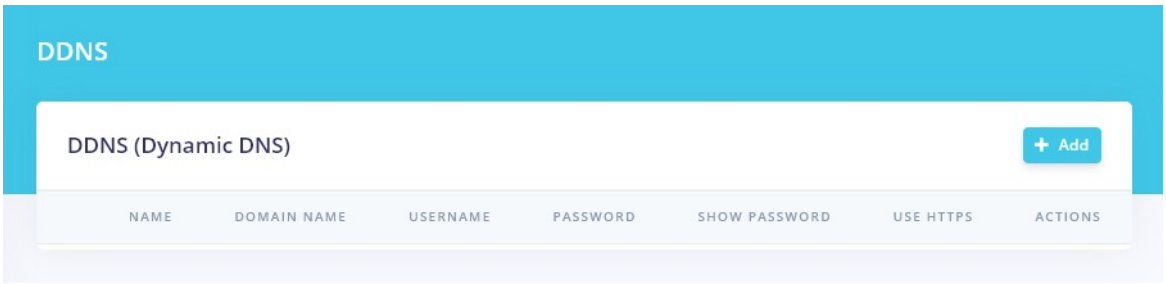
Configuring Dynamic DNS Services

You can configure the Dynamic DNS (DDNS) settings for the SDG. DDNS allows remote access to 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.

To configure a Dynamic DNS server:

1. Navigate to **Services > DDNS**. The DDNS page appears (see Figure 74).

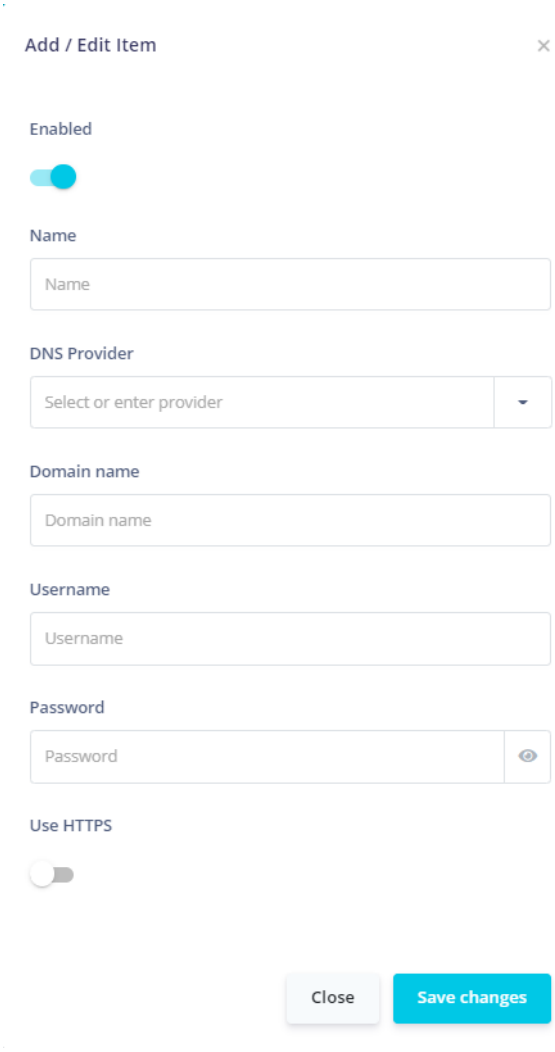
Figure 74: DDNS Page



2. To add a dynamic DNS server:

a. Click **+ Add**. The Add/Edit Item dialog box appears (see Figure 75).

Figure 75: Add / Edit Item Dialog Box



b. Complete the fields using the information in Table 29.

Table 29: Dynamic DNS Server Configuration Settings

Field Name	Description
Enabled	New server definitions are enabled by default. Use this slider to disable a configuration.
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.

Table 29: Dynamic DNS Server Configuration Settings (continued)

Field Name	Description
Username	Enter the user name required to access the domain.
Password	Enter the password required to access the domain. To display the password, click the show/hide button (eye icon).
Use HTTPS	(Optional) Use this slider to enable HTTPS security.

c. Click **Save changes**.

3. To edit the details of a server:

   a. Click the blue edit button next to the appropriate server. The Add/Edit Item dialog box appears.

   b. Modify the fields as needed, using the information in Table 29.

   c. Click **Save changes**.

NOTE

To delete a server, click the red delete button next to the appropriate server. Click **Apply** in the Pending changes dialog box.

Configuring VoIP Services

This section contains this topics for configuring Voice over IP settings (VoIP) on supported SDG models:

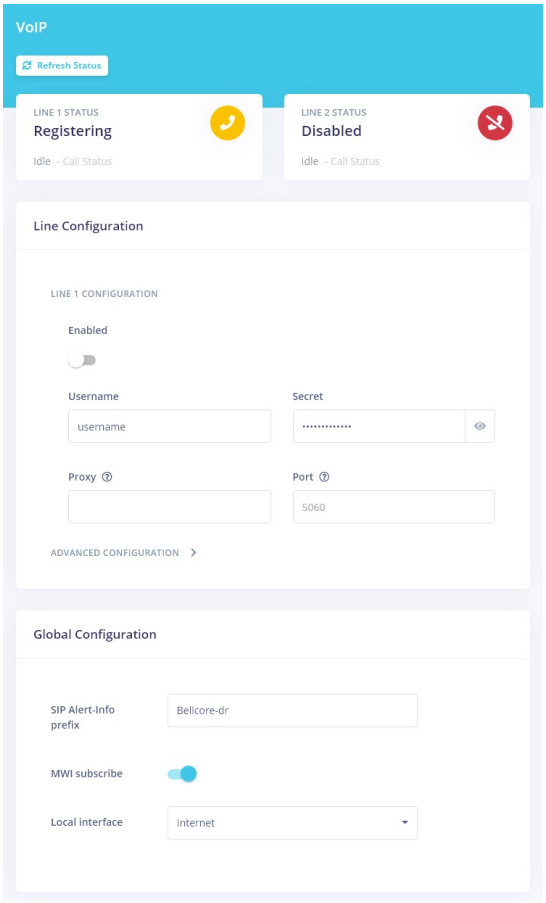
NOTE

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

Configuring Basic VoIP Services

1. Navigate to **Services > VoIP**. The VoIP page appears (see Figure 76).

Figure 76: VoIP Page



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

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

2. Complete the VoIP configuration using the information in Table 30.

Table 30: VoIP Configuration - Basic

Field Name	Description
LINE 1 and LINE 2 Configuration	
Enabled	Use this slider to enable this VoIP line on your SDG. Use this slider to enable and configure just one line or both lines, if needed.

Table 30: VoIP Configuration - Basic (continued)

Field Name	Description
Username	Enter the username for this line of service to access the service provider VoIP network.
Secret	Enter the passphrase for this line of service to access the service provider 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**.
Advanced Configuration Line 1 and Line 2	
SIP Configuration	Options are: • Domain • Auth username • Outbound proxy • Outbound proxy port • Registrar • Registrar port • Local port (Default is 5060) • Registration expiration (Default is 3600) • PRACK (Default is Disabled) • Session max tsec (Default is 120) • Session min timer sec (Default is 90) • Session Refresher (Options: Unspecified, UAC. UAS. Default is UAC
QoS	Options are: • SIP ToS (Default is 104) • RTP ToS (Default is 184) • RTCP ToS (Default is 184)
Codecs	Options are: • G.711 Mu-Law • G.726 • G.711 A-Law • G.729 • Silence suppression

Table 30: VoIP Configuration - Basic (continued)

Field Name	Description
Dial Options	Options are: • Digit Map • Digit escape mode • Start digit timer (sec) Default is 16 • Short digit timer (Default is 4) • Long digit timer (Default is 16) • DTMF relay. Options are: INFO, RFC 2833, Inband. Inband is Default)
Caller ID	Options are: • Local CID • Outgoing CID • Outgoing CID Name
Multi Party Features	Options are: • 3-Way conference: Options are: Disabled, Enabled, Enabled with call transfer (Default) • Call waiting (Disabled is the Default) • Flash relay mode. Options are: Disabled, RFE-2833, SIP INFO (Default)
Message Waiting Indication	Options are: • Audible message waiting indication (AMWI) • Visible message waiting indication (VMWI)
Fax	T-38 fax relay is the only option
Warmline	Options are: • Warmtime: Enabled/Disabled • Warmtime number • Warmtime timer in sec (Default is 8)
Line Gains	Options are: • Rx gain. Default is -9 dB • TX gain. Default is -3dB • RX 0.5 dB additional loss (Default is Disable) • TX 0.5 dB additional loss (Default is Disable)

Table 30: VoIP Configuration - Basic (continued)

Field Name	Description
Global Configuration	
SIP Alert-Info prefix	Bellcore-dr is the only option
MWI subscribe	Default is Disable.
SIP Options interval (sec)	Default is zero.
SIP transport	Options are: • UDP (Default) • TCP • TLS
Local interface	Options are: • Internet (Default) • Voice
TLS	Options are: • SRTP (Default is Disabled) • TLS certificate file URL • TLS certificate server password • TLS server verification (Default is Disabled)
Security	Options are: • Restricted source (Default is Disabled) • Active source filter (Default is Disabled) • keepalive (Default is 60 seconds)

3. Click **Apply** in the Pending changes dialog box.

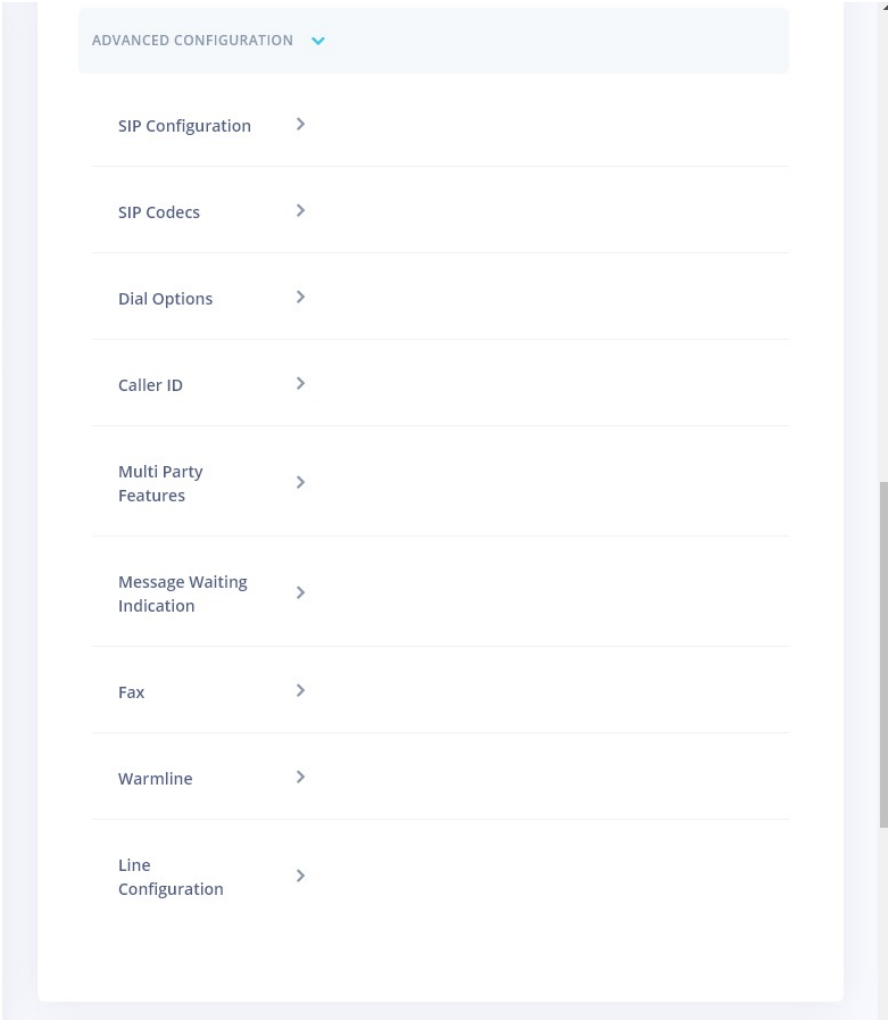
Configuring Advanced VoIP Services

When a detailed VoIP configuration is required, expand the Advanced configuration section on the VoIP page. This section provides additional settings to customize the voice behavior of the SDG. The additional settings are categorized under these sections: SIP Configuration, Codecs, Dial Options, Caller ID, Multi Party Features, Message Waiting Indication, Fax, Warmline, and Line Configuration.

To configure advanced VoIP services:

1. Expand the ADVANCED CONFIGURATION section. The Advanced Configuration Section - VoIP page appears (see Figure 77).

Figure 77: Advanced Configuration Section — VoIP Page



1. Complete the sections under Advanced Configuration using the information in Table 31.

Table 31: 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	Use this slider 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.

Table 31: VoIP Configuration - Advanced (continued)

Field Name	Description
QoS	
SIP ToS	This is a Type of Service (ToS) setting for SIP packets. ToS is related to QoS where priority 0 is the lowest priority and 7 is the highest.
RTP ToS	This is a Type of Service (ToS) setting for RTP packets. ToS is related to QoS where priority 0 is the lowest priority and 7 is the highest.
RTCP ToS	This is a Type of Service (ToS) setting for RTCP packets. ToS is related to QoS where priority 0 is the lowest priority and 7 is the highest.
SIP Codecs	
Use the slider 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 (for example, 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 timeout. Default value is **16 seconds**.
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**.

Table 31: VoIP Configuration - Advanced (continued)

Field Name	Description
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). Select inband, INFO, or RFC 2833.
Caller ID	
Local CID	Use this slider to enable the generation of the CID signal locally.
Outgoing CID	Use this slider 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	Use this slider to Disable flash-hook services handled by the softswitch (such as Metasphere).
Call waiting	Use this slider 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	Use this slider to enable stutter dial tone MWI indication.
VMWI	Use this slider to generate MWI FSK signal to the CPE.
Fax	
T.38 fax relay	Use this slider to enable T.38 fax relay.
Warmline	
Warmline	Use this slider 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.

Table 31: VoIP Configuration - Advanced (continued)

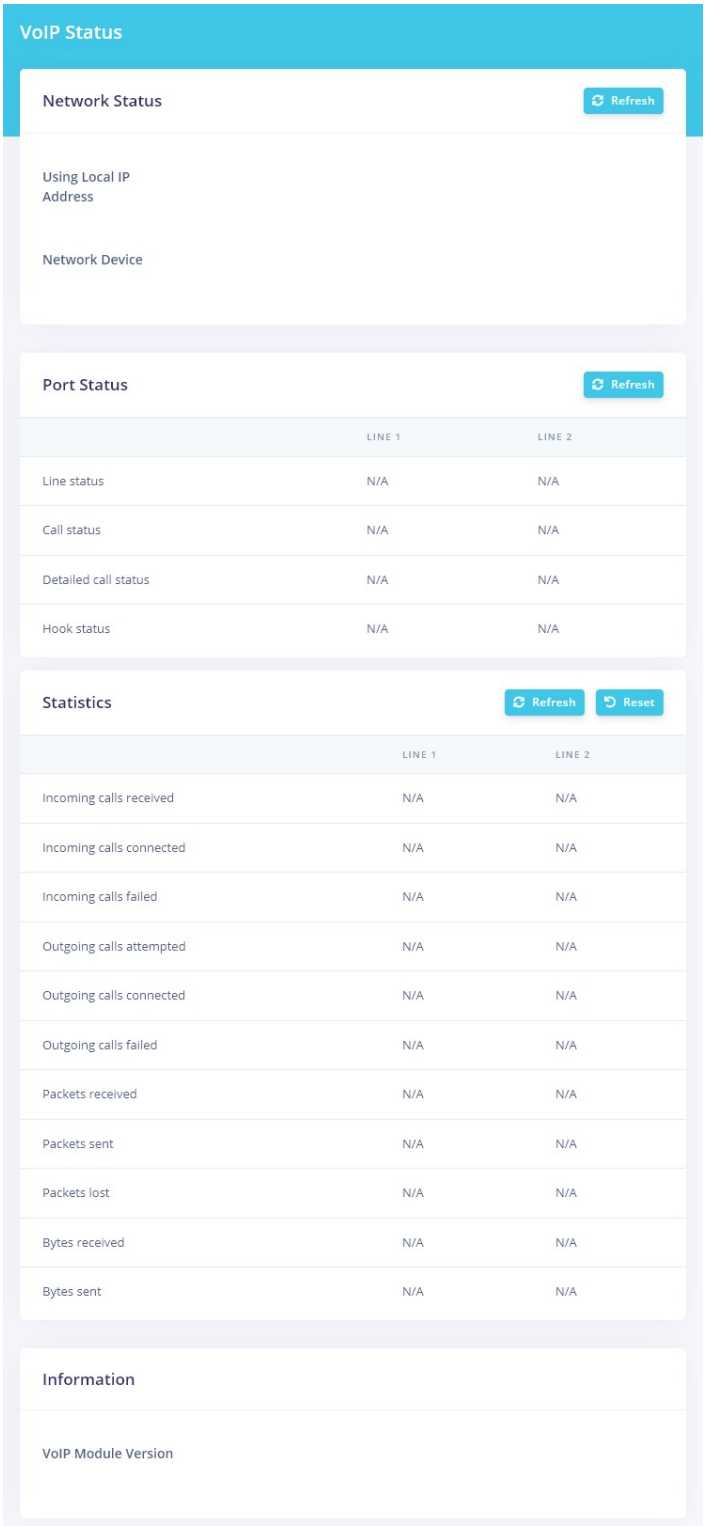
Field Name	Description
Warmline timer (sec)	Enter the warmline timeout. Default is **8 seconds**.
Line Configuration	
RX gain (dB)	Select the RX gain for the line. Range is **0** to **–12dB**. Default value is **–9dB**.
TX gain (dB)	Select the TX gain for the line. Range is **0** to **–12dB**. Default value is **-3dB**.

2. Click **Apply** in the Pending changes dialog box.

Viewing VoIP Statistics

Navigate to **Services** > **VoIP**. The VoIP Status page appears (see Figure 78).

Figure 78: VoIP Statistics



Cabling and Pinouts

The VoIP-capable models are equipped with an RJ11 port on the back panel of the device. If a POTS device is required for your installation, use an RJ11 cable (not included) to connect the telephony device to the SDG port labeled **Tel 1/2** on the rear of the units.

A Y-cable is 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 might be equipped with ports conforming to the RJ11 standard. Consult your PBX or KSU vendor documentation to confirm cabling requirements.

Chapter 7: Managing Connected Devices

This section contains these topics:

Configuring and Managing Intellifi Mesh Devices

This section details the configuration and management of your mesh network and includes these topics:

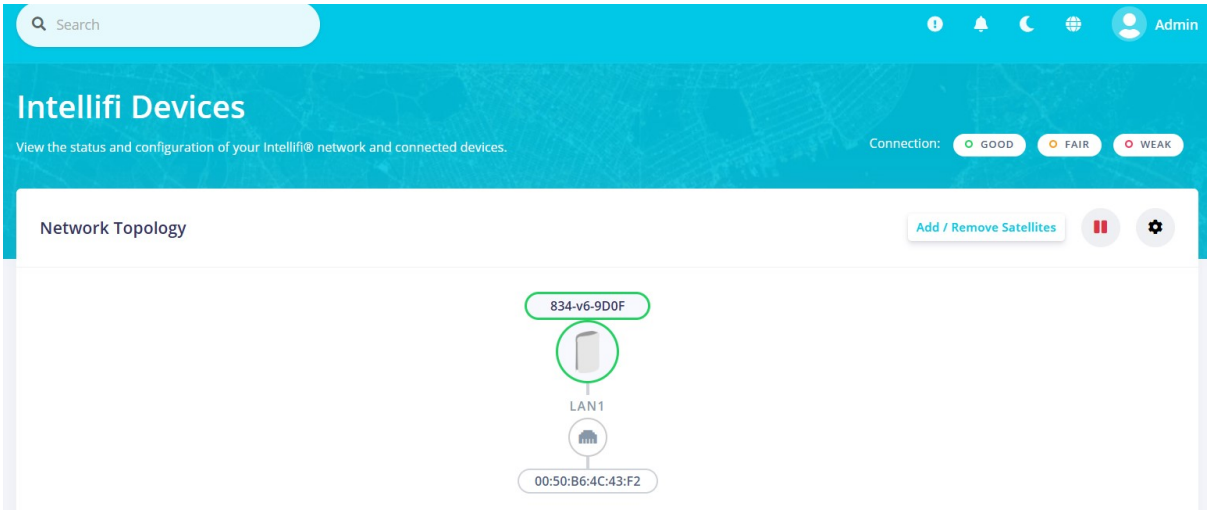
Viewing Connected Intellifi Mesh Devices

NOTE

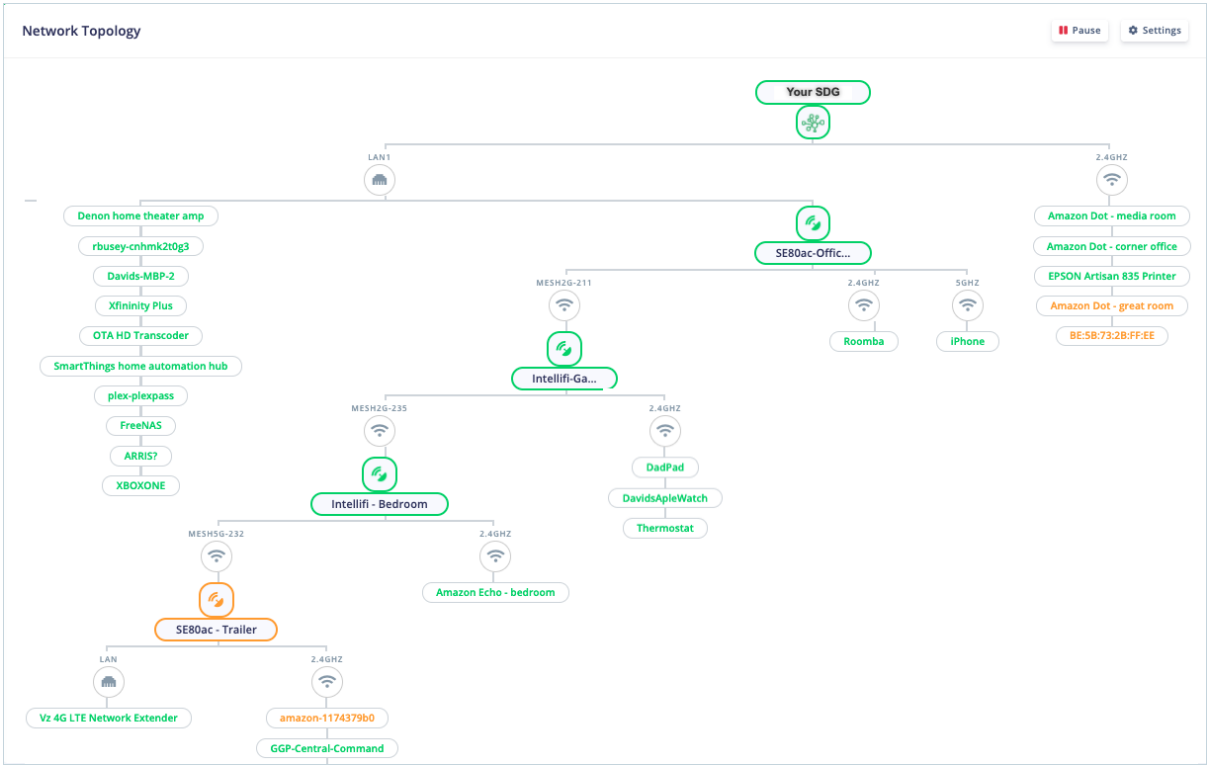
To extend the network, a satellite can be linked to another satellite.

1. Navigate to **Devices > Intellifi Devices**. The Intellifi Devices page appears, showing a diagram of the connected devices (see Figure 79). Connection status and device type legends appear in the top right of the page.

Figure 79: Intellifi Devices Page



If a wireless LAN device is connected, the Wi-Fi band information appears as the name instead of LAN or WAN. The device colors identify the device status. The connection legend in the top right explains the colors. The device identifier legend appears below the connection legend, showing symbols for HUB, SATELLITE, PLC, and MOCA devices.



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

2. To switch between the simple view and the detailed view:
   a. Click **Settings** at the top right of the Network Topology section. The Topology Settings dialog box appears.
   b. Enable the **Show Detailed View** slider and click **Save Changes**.
3. To change the refresh interval of the network topology:
   a. Click **Settings** 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. Click **Save Changes**.
4. 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.

NOTE

See Pausing Mesh Network Access for information about pausing Internet access.

Managing Satellite Devices — Mesh Extenders

This section contains these topics:

Adding Intellifi Satellites

Satellites require that DHCP be enabled to function properly.

Satellites require the controller's DHCP to function properly and to maintain connection with that controller. Without DHCP, new satellites cannot be added and current satellites will lose connectivity after their lease expires.

NOTE

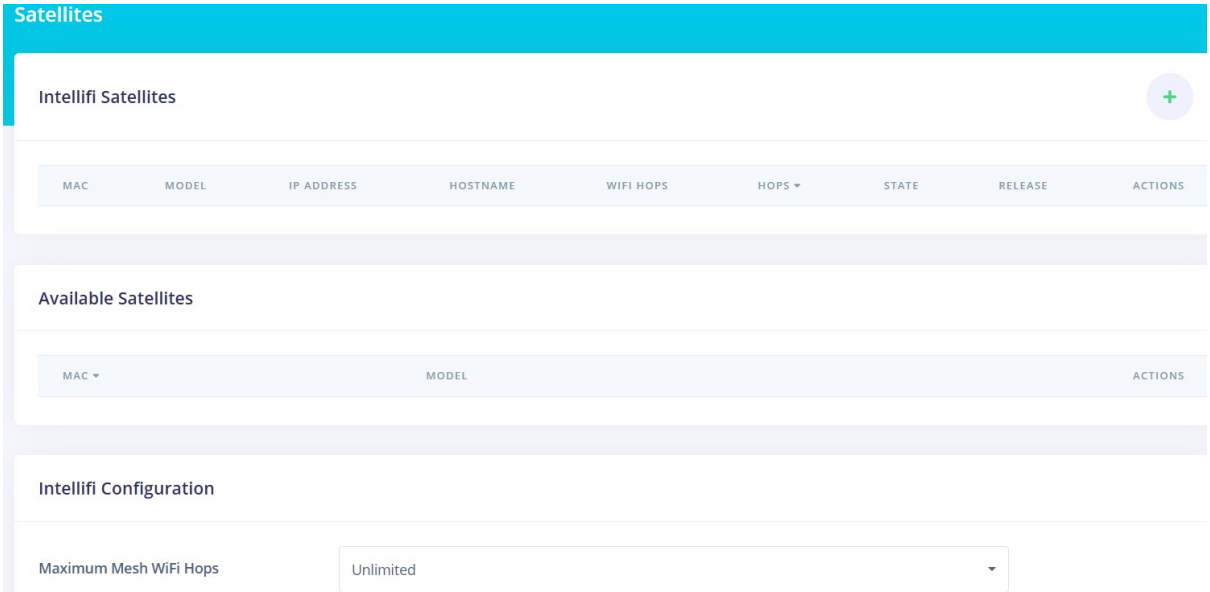
Configure your computer network interface to automatically acquire an IP address using DHCP.

Any available satellite is displayed in the Available Satellites field. If you do not see an expected satellite, reset the unit to its factory settings.

To add satellites to your Intellifi network:

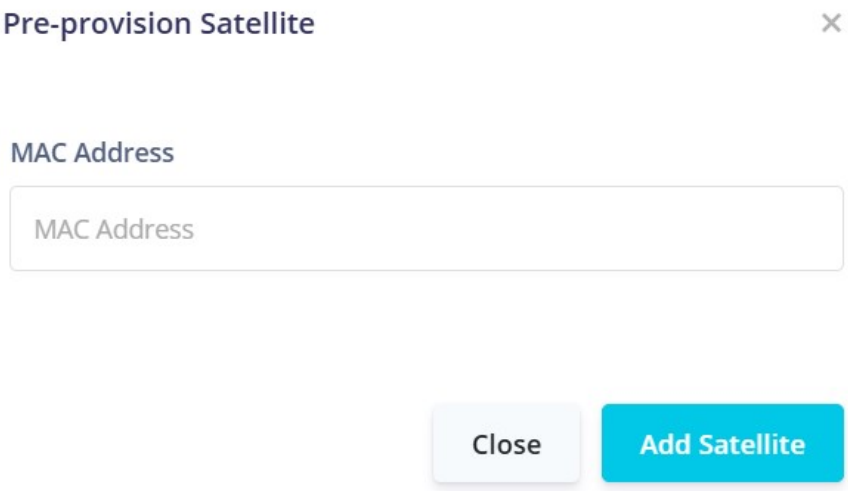
1. Navigate to **Intellifi > Topology > Add/Remove Satellite**. The Intellifi Satellites page appears (see Figure 80).

Figure 80: Add Intellifi Satellite



2. In the Available Satellites field, select the **+** next to the satellite you want to add. This will enable you to add the satellite to the network (see). This could take up to 5 minutes.

   Figure 81: Pre-provision Satellite



3. Click **Add Satellite**

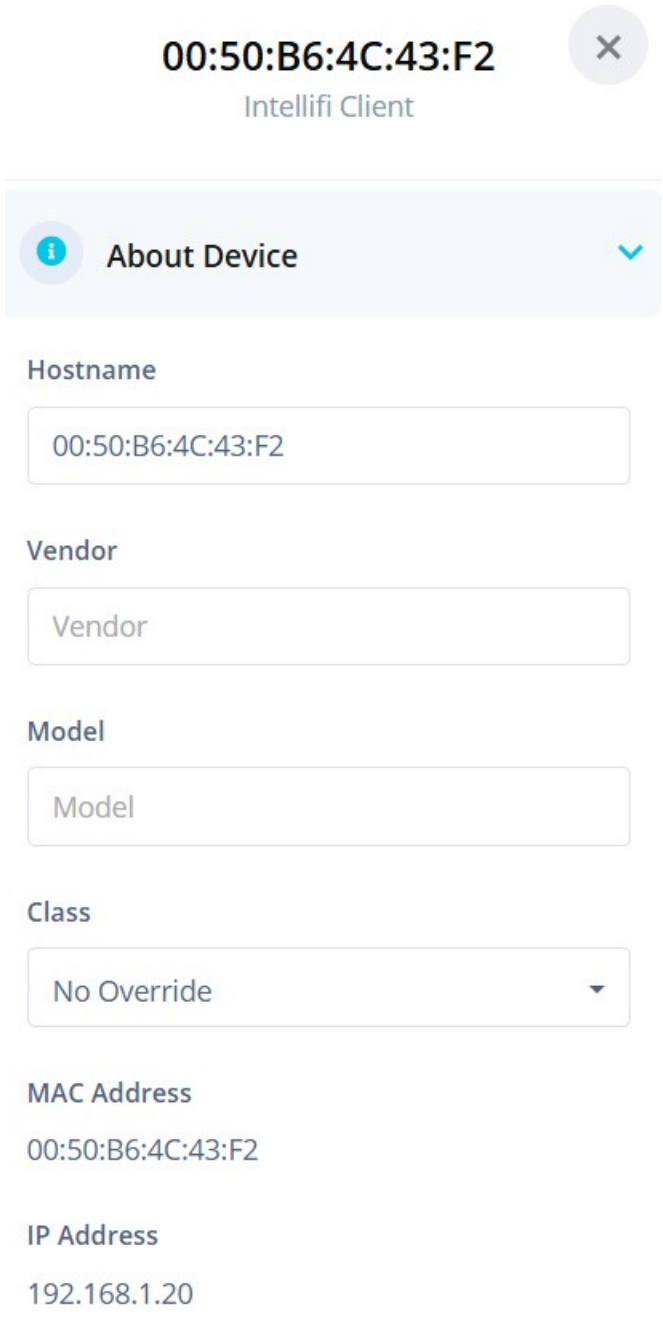
Viewing Device Settings

To view the device host name, MAC address, and IP address:

1. Navigate to **Intellifi > Topology**. The Topology page appears.
2. Select the device label in the topology diagram. The details pane appears below the device label.
3. Double click the image and deadline about the device appear on the right side of the screen and Figure 82 is displayed.

4. Select **DEVICE DETAILS** and the **DEVICE DETAILS** pane expands.

Figure 82: Intellifi Device Details

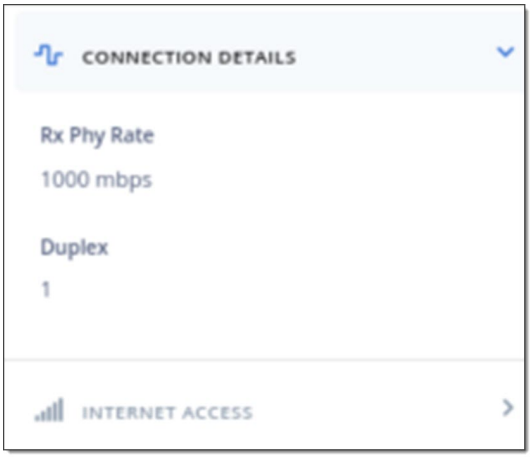


5. In this pane, either edit the host name or select the IP address to log into the device and view status and statistics.
6. The **Internet Access** option. is located at the bottom of this pane. Click the **Connection Status** to change the connection if needed.
7. To refresh the screen, select the gear icon at the right of the screen and enter a new **Refresh Interval**.
8. Click **Save changes**.

Viewing Connection Details

1. Navigate to **Intellifi > Topology**. The CONNECTION DETAILS page appears (see Figure 83).
2. Select the label next to the device you want. The device information pane appears.
3. To view the connection details, select **CONNECTION DETAILS** to expand the pane. The transmission rates and signal data appear.

Figure 83: Connection Details



Pausing Mesh Network Access

This section contains these topics:

Pausing the Intellifi Network

To pause the entire Intellifi network from Internet access, on the Network Topology menu, click the double bar to the right of the **Add/Remove Satellites** option. When clicked, pause changes to play. The network access pauses.

To restart the network, click the icon again.

Pausing Device Internet Access Remove

To pause access to a specific device for a specified duration:

1. Select the label next to the device you want. The device information pane appears (see Figure 84).
2. To view the access details, select **INTERNET ACCESS** to expand the pane.

Figure 84: Pausing a Device

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

Configuring and Managing LAN-Connected Devices

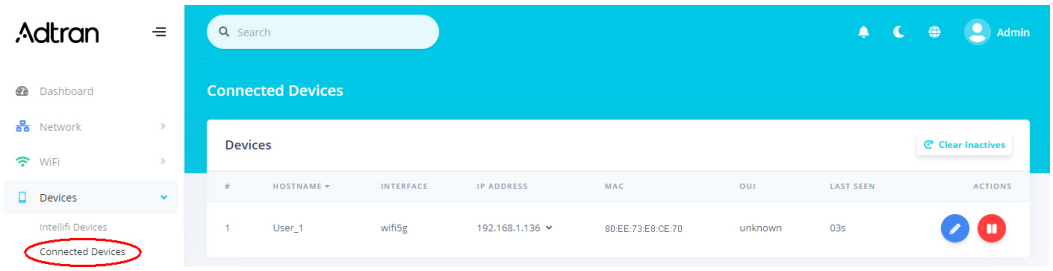
This section details the configuration and management of your LAN client devices and includes these topics:

Viewing LAN-Connected Devices

To view a list of devices connected to the LAN:

1. Navigate to **Devices > Connected Devices**. The Connected Devices page appears (see Figure 85).

   Figure 85: Connected Devices Page



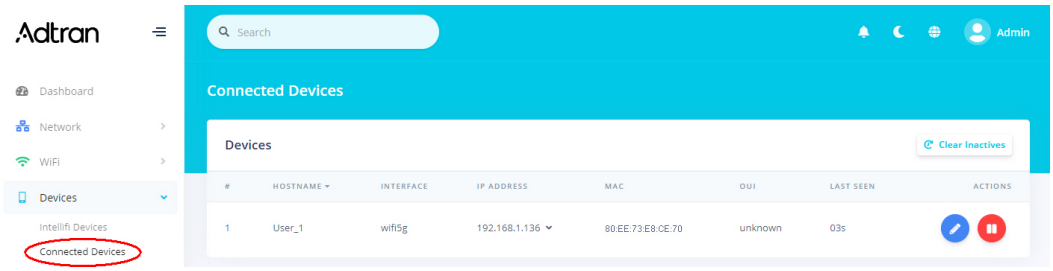
2. Click **Clear Inactives** to refresh the list to show only active devices.

Editing a Device Name

To view and edit a list of devices connected to the LAN:

1. Navigate to **Devices > Connected Devices**. The Connected Devices page appears (see Figure 86).

   Figure 86: Connected Devices Page

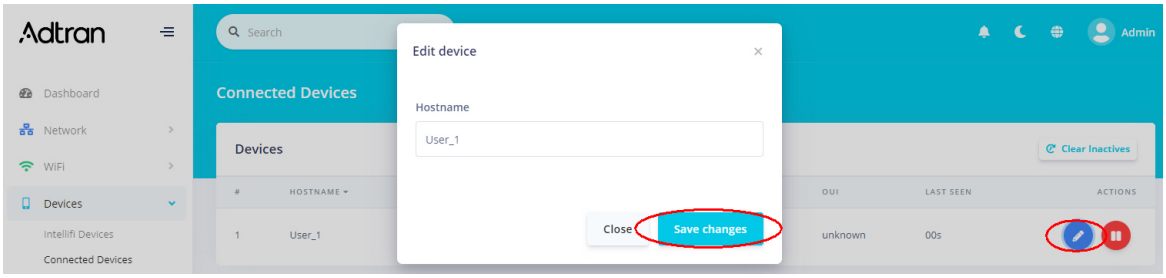


2. Click **Clear Inactives** to refresh the list to show only active devices.

3. To edit the host name for a device:

   a. Click the blue **Edit** icon next to the device you want to edit. The Edit device dialog box appears (see Figure 87).

   Figure 87: Edit Connected Devices



   b. Enter the host name and click **Save changes**.

Managing Connected Devices

This section contains these topics:

NOTE

Before assigning a device to a group, complete this steps:

1. Create or modify an access schedule.
2. Create a device group and add devices.
3. Assign the schedule to the device group.

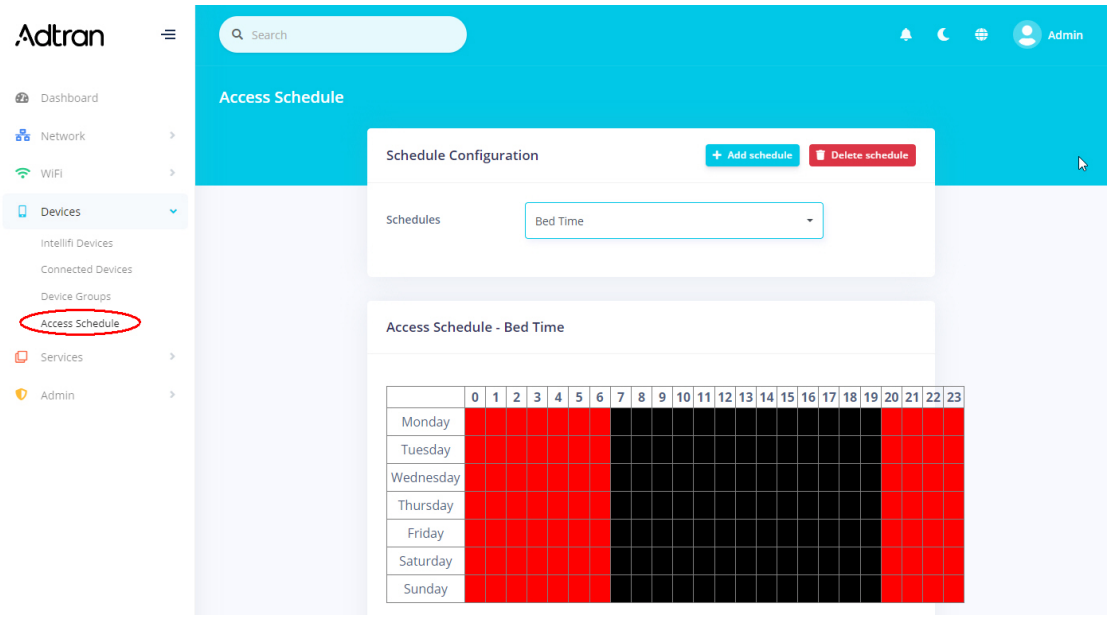
Creating or Modifying a Schedule

Make sure you set the time zone correctly for the SDG before configuring an access schedule. You can access the Timezone setting on the **Admin > Time** page.

You need the access schedule to control access for LAN device groups. To create a new access schedule or modify an existing default schedule:

1. Navigate to **Devices > Access Schedule**. The Access Schedule appears.

Figure 88: Access Schedule Page



Two default schedules exist in the system: Bed Time and School Nights.

2. To create a new schedule:

   a. Click **Add schedule**. The Create access schedule dialog box appears.

   b. In the **Name** field, enter a name for the new schedule and click **Save changes**. Additional fields appear on the Access Schedule page for configuring blocked access time for every day or for specific days.

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

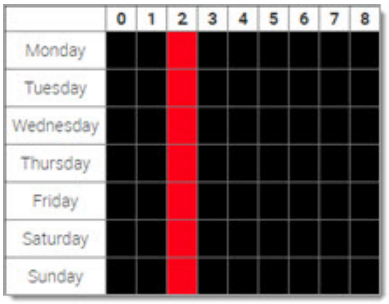
      The entered time periods appear in red on the grid in whole-hour blocks only. When times are entered in the **Daily Pause Times** fields, that period changes to red for each day.

      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.

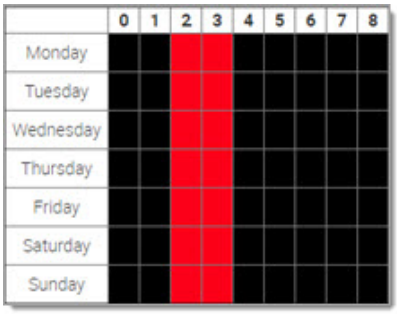
      If you enter **0300** in the second field, a 2-hour block is selected in the grid, from 2:00 to 4:00 am. The maximum number of blocked periods allowed per day is 3.

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)



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



3. To modify a schedule, select it in the **Access Schedule** field and modify the fields.
4. Click **Apply**.

NOTE

To delete a schedule, select it in the **Access Schedule** field and click **Delete schedule**. If you delete a schedule that is assigned to a device group, it is removed from the device group configuration.

Creating a Device Group and Adding Devices

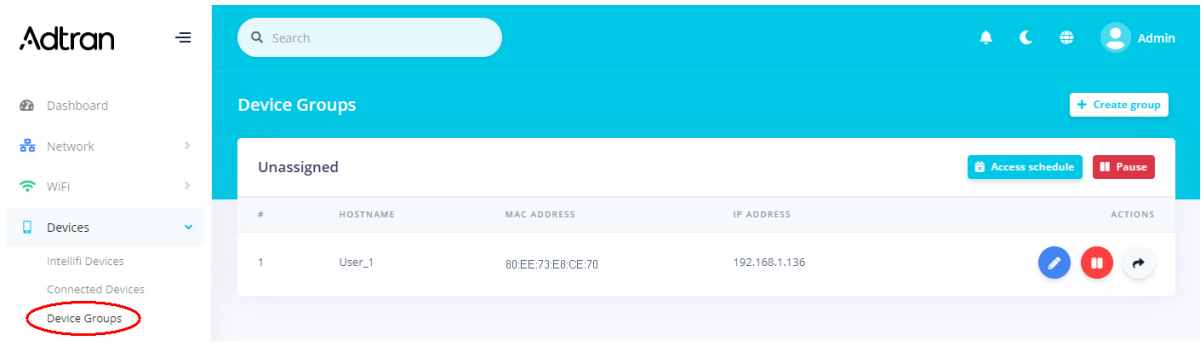
NOTE

This procedure assumes that you have already created the access schedule to assign to your device group. If you have not, see Creating or Modifying a Schedule before continuing with this procedure.

To create device groups, assign devices to groups, and assign schedules to groups:

1. Navigate to **Devices > Device Groups**. The Device Groups page appears (see Figure 89).

Figure 89: Device Group Page



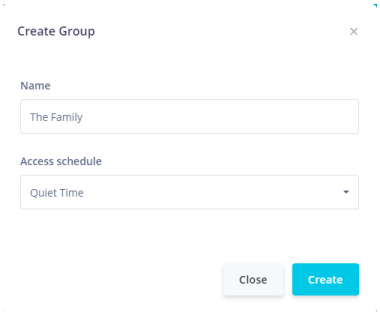
NOTE

You cannot delete or rename the unassigned (default) group . You can, however, assign a schedule and pause or restart it.

2. To create a new device group:

   a. Click **Create group**. The Create Group dialog box appears (see Figure 90).

Figure 90: Create Group



   b. In the **Name** field, enter a descriptive name for the device group.

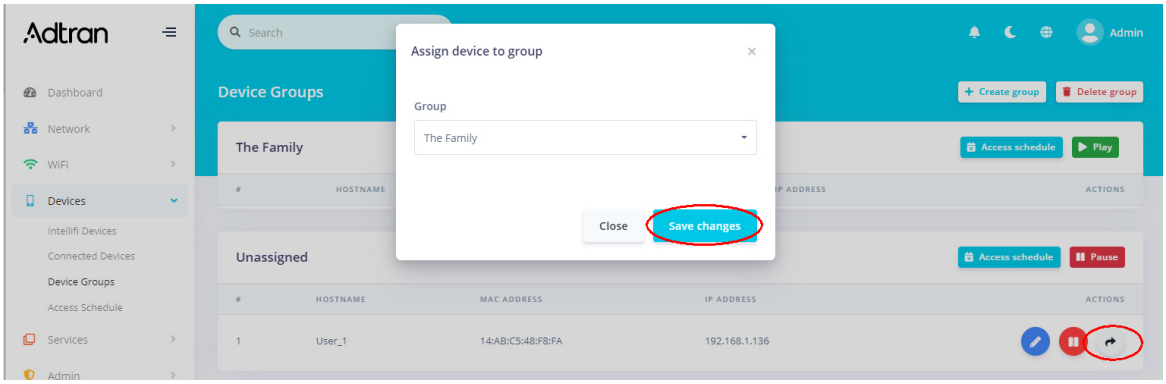
   c. To assign a schedule to the device group, select the schedule in the **Access schedule** field.

   d. Click **Create**. The new device group appears on the page.

3. Add a device to the group:

   a. Click 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 (see Figure 91).

Figure 91: Assign Device to a Group



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

c. Click **Save changes**.

NOTE

To delete a device group:

1. Click **Delete group** at the top of the device pane. The Delete Group dialog box appears.
2. Select the group that you want to delete from the drop-down list.
3. Click **Delete**.
4. Click **Apply**.

Applying an Access Schedule to a Device Group

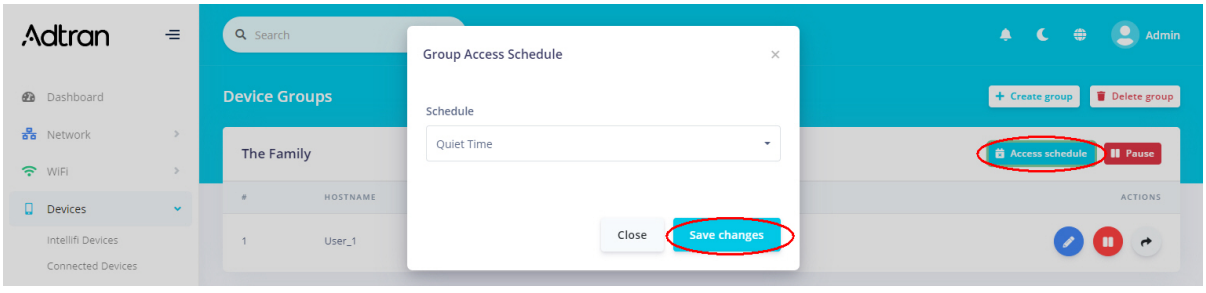
NOTE

This procedure assumes that you have already created the access schedule to assign to your device group. If you have not, see Creating or Modifying a Schedule before continuing with this procedure.

To change or apply an access schedule to a device group (see Figure 92):

1. Click **Access schedule**.

Figure 92: Group Access Schedule



2. Select the name of the schedule you wish to apply and click **Save changes**.

Pausing Internet Access

WARNING!

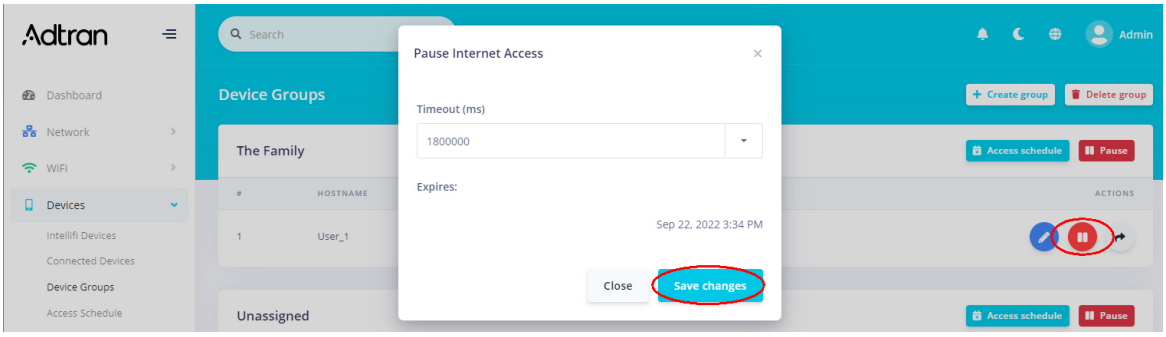
Pausing access for LAN devices not only restricts access to the Internet but access to the LAN as well. This action prevents logging in to the SDG to make changes from any LAN client included in the pause. With this in mind, Adtran strongly advises against pausing all LAN devices at the same time. Instead, 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.

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. To pause Internet access for a single device (see Figure 93):
   a. Select the red pause button at the far right next to the device you want to pause. The Pause Internet Access dialog box appears.

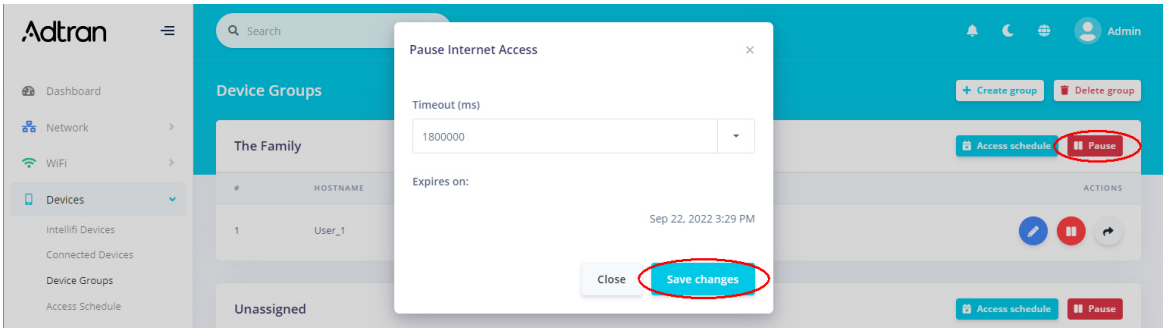
   Figure 93: Pausing Internet Access (1 of 2)



   b. In the **Timeout (ms)** field, select how long you want Internet access paused. Options are **None**, **15 minutes** through **60 minutes**, **2 hours** through **8 hours**, and **1 day**. Your selection displays in milliseconds.
   c. Click **Save changes**. The red pause button is replaced by the green play button.

2. To pause Internet access for a device group:
   a. Select the red pause button at the far right next to the device group name you want to pause. The Pause Internet Access dialog box appears (see):

Figure 94: Pause Internet Access (2 of 2)



b. In the **Timeout (ms)** field, select how long you want Internet access paused. Options are **None**, **15 minutes** through **60 minutes**, **2 hours** through **8 hours**, and **1 day**. Your selection displays in milliseconds.

c. Click **Save changes**. The red pause button is replaced by the green play button.

3. To restart Internet access for a device or a device group, click the green play button.

Chapter 8: Managing System Settings

This section includes these topics:

Updating SDG Firmware

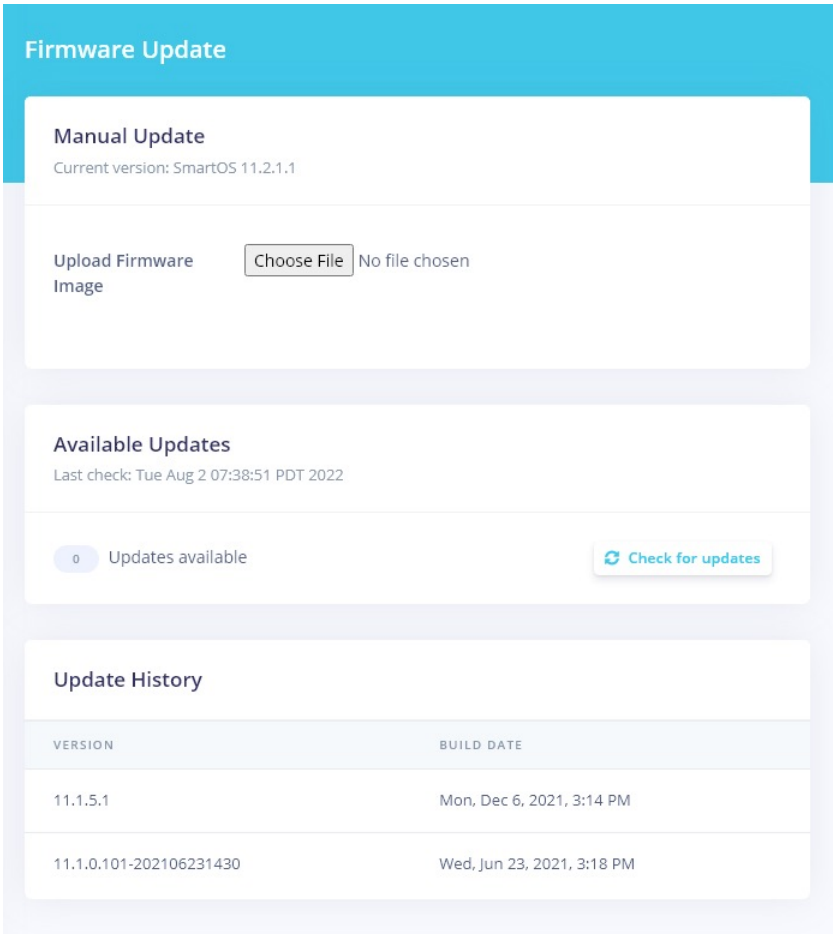
NOTE

You can download software updates from the Adtran Support Community site.

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

Navigate to **Admin > Update** to view the current firmware version and build date, available updates, and update history (see Figure 95). The current firmware version is listed below the Manual Update heading.

Figure 95: Firmware Update



To check for available firmware updates:

1. In the Available Updates section, click **Check for updates**. 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.

2. If updates are available, click **Install Updates**. A confirmation message appears.

3. Click **Yes** and the installing message appears. When the installation has finished, the SDG reboots.

To manually update your firmware:

1. Download the firmware update from the Adtran Support Community site.
2. In the Manual Update section, click **Choose File**. An Open or File Upload dialog box appears.
3. Navigate to and select the firmware image file that you want to install and then click **Open**. A progress bar and a Cancel button appears.
4. When the file completed loading, click **Start Upgrade**. You will see the Upgrading progress bar.

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

Managing System Configurations

This section contains these topics:

Backing Up the Current Configuration

NOTE

Before making changes to your SDG configuration, Adtran recommends that you back up your current configuration.

1. Navigate to the **Admin** section in the left navigation bar.
2. Select **Configuration > Save Configuration**.
3. Click **Download**. The file containing the working configuration parameters for your SDG was downloaded to your local drive.

Restoring a Saved Configuration

1. Navigate to the **Admin** section in the left navigation bar.
2. Select **Configuration > Restore Configuration**.
3. Click **Browse**, navigate to the saved configuration file, and click **Open**.

   The saved configuration file uploads and will be active on your SDG.

Resetting the SDG to Factory Default Settings

1. Navigate to the **Admin** section in the left navigation bar.
2. Select **Configuration > Factory Default**.
3. Click **Factory Reset** and the confirmation dialogue appears.
4. Click **Yes, reset**. After the reset, your SDG reboots. Allow a few minutes for this process to complete.

NOTE

You cannot access the local GUI of the SDG until the Quick Start Procedure is performed.

You can accomplish this with the Quickstart Wizard or the Inteffifi App.

Creating Custom Gateway Default Settings

You can customize the gateway defaults settings. You can define and upload these defaults with the GUI, CLI, or CWMP support of the gateway. To create a custom set of default settings:

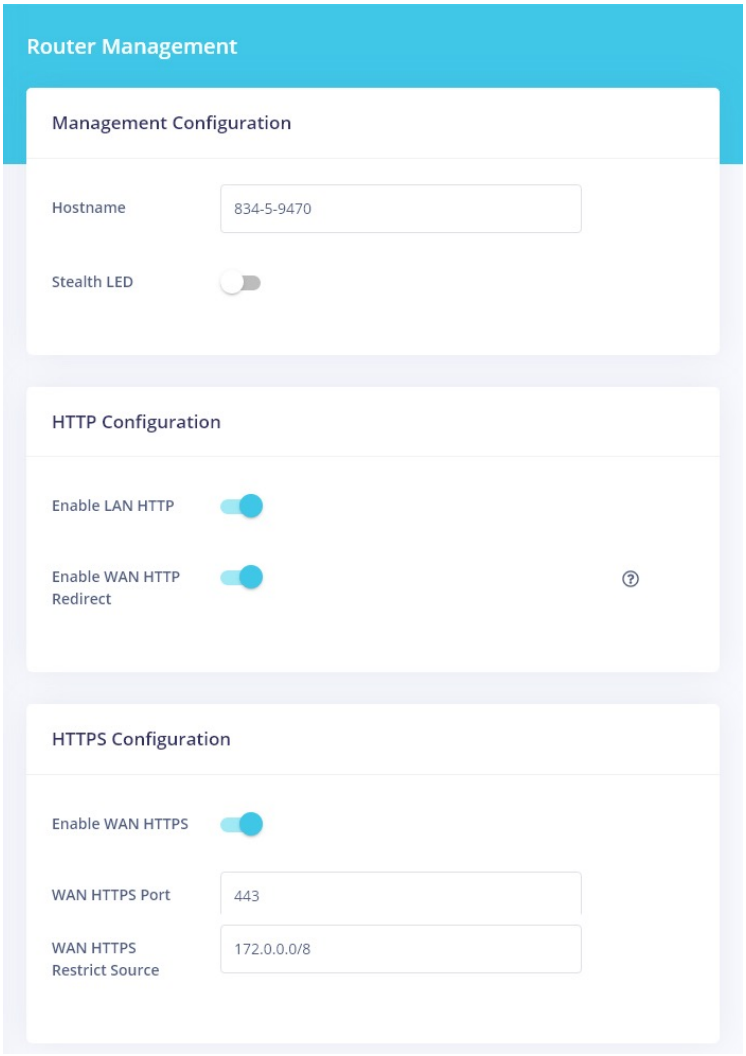
1. Configure the gateway as required.
2. Download the current configuration to your local drive using the instructions in Backing Up the Current Configuration.
3. Restore the configuration you just saved using the instructions in Restoring a Saved Configuration.

   The gateway now uses your custom settings as the default.

Configuring SDG HTTP Settings

1. Navigate to **Admin > Router Management**. The Router Management page appears.

Figure 96: Router Management Page



2. Complete the fields using the information provided in Table 32.

Table 32: 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. The default is disabled. Use this slider to prevent the LEDs from shining.
HTTP Configuration	
Enable LAN HTTP	This feature is enabled by default. Use this slider to disable LAN HTTP.
Enable WAN HTTP redirect	This feature is disabled by default. Use this slider to redirect WAN HTTP port 80 to a WAN HTTPS port.
HTTPS Configuration	
Enable WAN HTTPS	This feature is disabled by default. Use this slider to enable WAN HTTPS.
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.

3. Click **Apply** in the Pending changes dialog box.

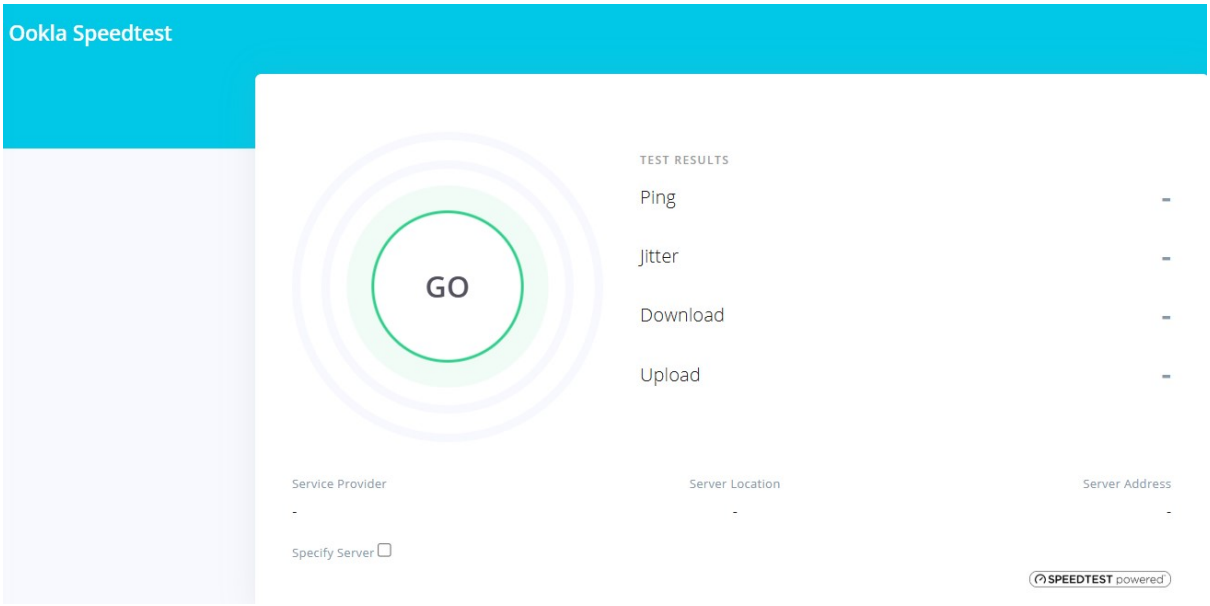
Managing System Passwords

1. Navigate to **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. Click **Save Changes**. The new password takes effect immediately.

Performing an Ookla Speedtest

1. Navigate to **Admin > Speedtest**. The Ookla Speedtest page appears.

   Figure 97: Speedtest Page



2. Click **Go**. Statistics are returned for ping, jitter, download speed, and upload speed. You can run this test as often as needed.
3. To specify a specific server, select the Specify Server option and enter that server <hostname> <port>. Then click **Go**.

Speedwave

Speedwave is an Adtran proprietary speed testing protocol that uses public servers or private ISP-devices deployed to accurately test speeds to and from the gateway.

To run Speedwave for your SDG:

1. Navigate to **Admin > Speedwave**.
2. Select **Go**.
3. Results are displayed on the screen.

Testing Network Connectivity — Ping and Traceroute

You can ping a server and use the traceroute utility to display a packet path over the IP network and measure route transit delays that may be present.

To test the network connectivity using Ping and Tracerouts:

1. Navigate to **Admin > Net Tools**.
2. In the Ping section:
   a. Enter an IP address or host name in the **IP/Hostname** field.
   b. Click **Start** and 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. In the Traceroute section:
   a. Enter an IP address or host name in the **IP/Hostname** field.
   b. Click **Start** and the trace results appear.

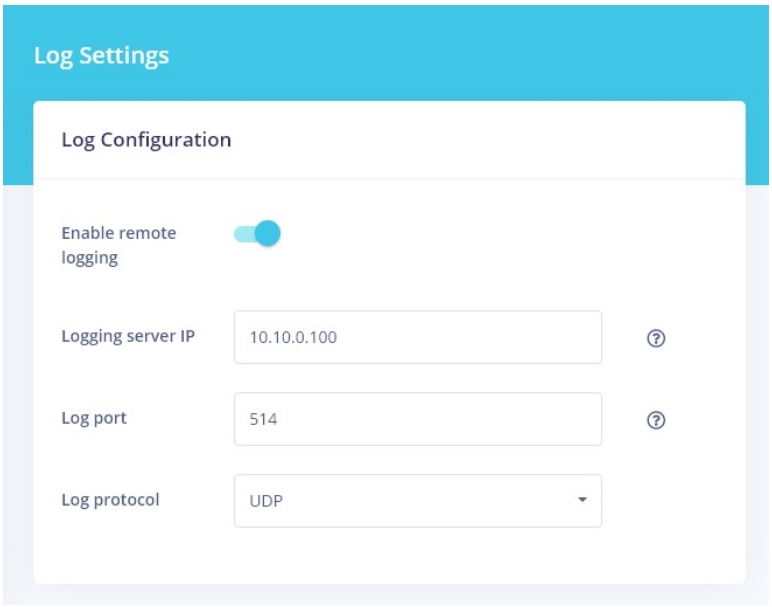
```
traceroute to 192.168.1.44 (192.168.1.44), 30 hops max, 46 byte packets
 1  *
 2  *
 3  *
 4  192.168.1.1  60.268 ms !H
```

Configuring System Logs

This section contains these topics:

Enabling Remote Logging (Optional)

1. Navigate to **Admin > Event Log > Log Settings**.
2. Use the **Enable remote logging** slider to activate remote logging. Additional fields appear.

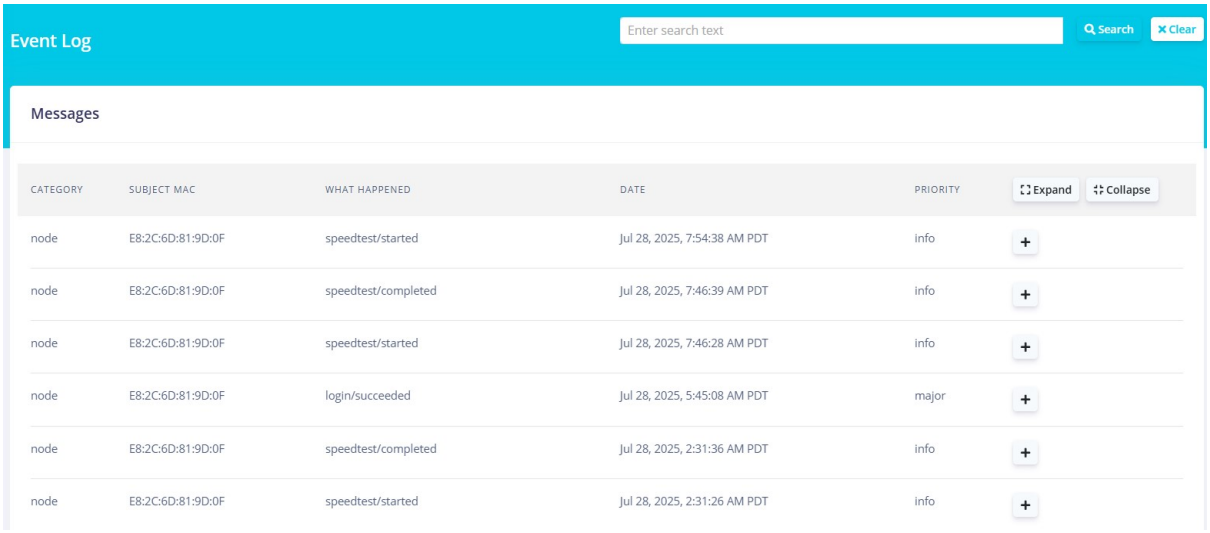


3. In the **Logging server IP** field, enter the IP address (such as 192.168.1.21) of the syslog server to which the log messages should be sent. Log messages are sent to this server in addition to the default local destination.
4. In the **Log port** field, enter or select the port number for the specified logging server. Options are **1** to **9999**.
5. In the **Log protocol** field, select the protocol. Options are **TCP** and **UDP**. The default is **UDP**.
6. Click **Apply** in the Pending changes dialog box.

Viewing Event Logs

1. Navigate to **Admin > Event Log**. The Event Log page appears.

   Figure 98: Event Log Page



2. To filter the displayed messages:
   a. Click **Search log messages** and the **Search log messages** dialog box appears.
   b. Enter a search string and click **Search**. The list refreshes to show the matching entries. As new entries are added to the event log file, the list refreshes to display them.
3. To clear the current filter, click **Clear search**.

Active Alarms

Active alarms displays any active alarm.

Alarm History

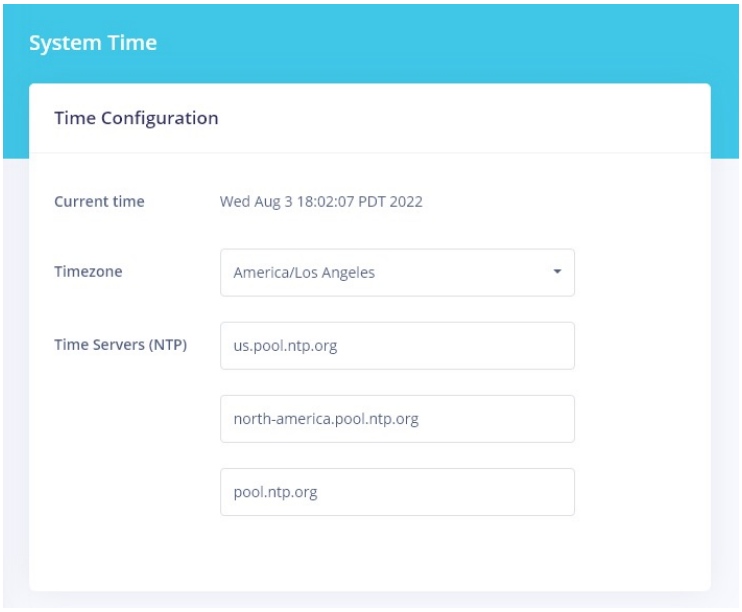
Alarm History displays a history for each alarm recorded by the system.

Specifying Time Settings

To select a time zone and manage connections to the reliable clocking servers available on the Internet:

1. Navigate to **Admin > Time**. The System Time page appears. All fields on this page are optional.

Figure 99: System Time Page



2. To change the time zone, select the appropriate zone in the **Timezone** field.
3. To change or remove time servers, modify or delete the addresses in the **Time Servers (NTP)** fields to point to the timeserver of your choice.
4. Click **Apply** in the Pending changes dialog box.

Specifying the SDG Operating Mode

To select whether the SDG operates as a router or a wireless access point:

1. Navigate to **Admin > Operating Mode**.
2. To configure how this SDG should operate, select the appropriate setting in the **Operating Mode** field. Options are **Router**, **Bridge** and **DSL Bridge**. The default is **Router**.

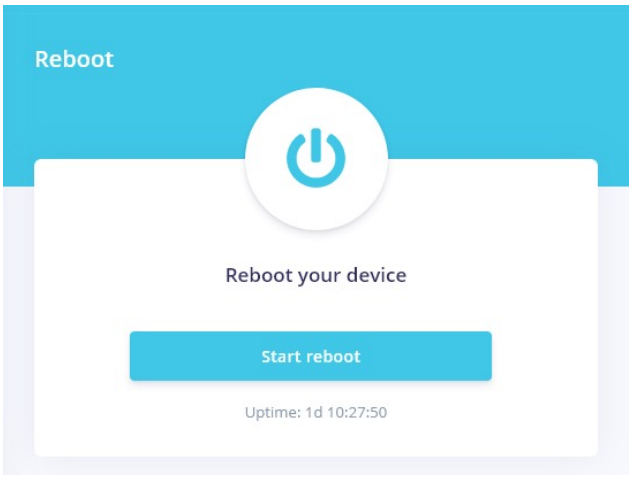
   In **Router** mode, this device functions as a router between your ISP WAN and your home network LAN. It provides firewall, NAT server, DHCP server, UPnP, DDNS, and other services. Select this option if you do not currently have a router.
3. To configure this SDG as part of a mesh network, select the appropriate setting in the **Intellifi Mode** field. Options are **None**, **Mesh 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 Wi-Fi coverage at this location.
4. The Intellifi Mode Auto feature is enabled by default. Enable this slider to prevent the SDG from automatically switching from **Intellifi Controller** mode to the managed **Satellite** mode.
5. Click **Apply** in the Pending changes dialog box.

Rebooting the SDG

1. Navigate to **Admin > Reboot**. The Reboot screen appears. The amount of time that the SDG was connected appears in the **Uptime** line below the **Start reboot** button.

   Figure 100: Reboot Screen



2. Click **Start reboot**. The restart confirmation dialog box appears, stating that rebooting takes approximately 3 minutes.
3. Click **Yes, reset**. The rebooting dialog box appears, showing the time remaining until completion. When your SDG is ready, the Sign In dialog box appears.