Adtran

800 Series Service Delivery Gateways

PlumeOS User Guide for Operators

Configuration Guide

6SDGPOS800-29A
November 2022

To the Holder of this Document

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

Trademark Information

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

Disclaimer of Liability

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

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

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

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

Service and Warranty

For information on the service and warranty of Adtran products, visit the Adtran website at http://www.adtran.com/warranty-terms.

Contact Information

To contact Adtran, choose one of the following methods:

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

Document Revision History

Rev	Date	Description
Rev A	November 2022	Initial Release

Table of Contents

1. Introduction

This guide provides information on the installation and configuration of Adtran's PlumeOS-based 800 Series Service Delivery Gateways (SDGs). Overviews of both the Frontline and HomePass interfaces are provided in this document, as well as basic troubleshooting information. More information about both Frontline and HomePort is also available in Plume's learning portal, available at https://learning.plume.com/learn/home.

2. Hardware and Software Requirements and Limitations

The features outlined in this guide are available on SDG devices running PlumeOS versions 2.1.0.1 and later as outlined in the *SDG Feature Matrix*, available online at https://supportcommunity.adtran.com.

> **NOTE**
>
> *This guide provides information on using PlumeOS with Adtran's SDGs; if your SDG is using SmartOS, refer to the 800 Series SDG SmartOS User Manual available online in the Adtran Support Community. Hardware information for each SDG model is provided in the Quick Start Guide associated with each SDG model; each Quick Start Guide is also available in the Adtran Support Community.*

3. Adding SDG Devices to the Plume Cloud

This section outlines the steps for adding a supported SDG into the Plume cloud, associating it with a specific customer using Plume's Frontline portal, and then activating the unit using Plume's customer-facing HomePass app. If you do not have access to the Plume cloud tools through Adtran, please contact Adtran Support at https://www.adtran.com/support.

Frontline is an extensive management tool built for service providers so that they can create and manage customer accounts. The application runs in the Plume cloud and has a wide variety of tools that can customize and monitor the customer's network and equipment for the best possible customer experience.

HomePass is the customer-facing smartphone application that allows customers to customize their own network and create profiles for each person and device in the house. This app gives the customer the tools to modify their network for the best possible customer experience.

Prerequisites

The following prerequisites must be met in order to add an SDG unit to the Plume cloud:

- Ensure the SDG is running PlumeOS.
- The SDG device (node) must be allocated to your Partner ID within the **Plume Global Inventory Database**. This is a process that is handled automatically when purchasing the product, so each device should be ready to deploy out of the box. If device is not allocated correctly, contact Adtran Support by following the steps listed in *Troubleshooting on page 32*.
- You must have a Plume account to access Frontline and manage customer devices. If a team member does not have an account, additional accounts can be created by anyone with authorized access to the **Team Management** tool. This tool is located in the **Account** tab in the Plume portal.
- Make sure to have the Media Access Control (MAC) address for the device available. There are stickers on both the box and unit indicating the MAC address. The serial number is NOT used.

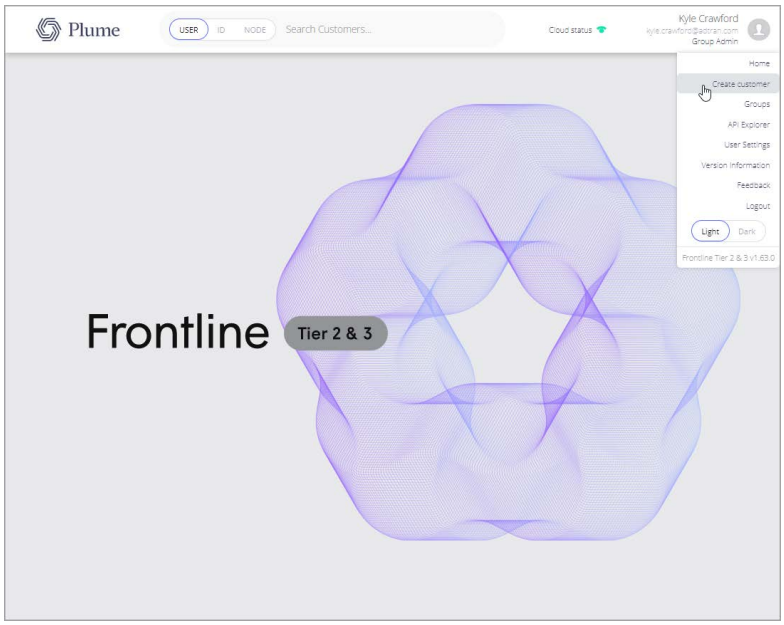
NOTE

Customers will need to create a personal HomePass account within the HomePass app. This personal account will be linked to the Frontline account that the ISP has created during the activation process described in *Activating Units Using HomePass on page 11*.

Creating New Customer Accounts

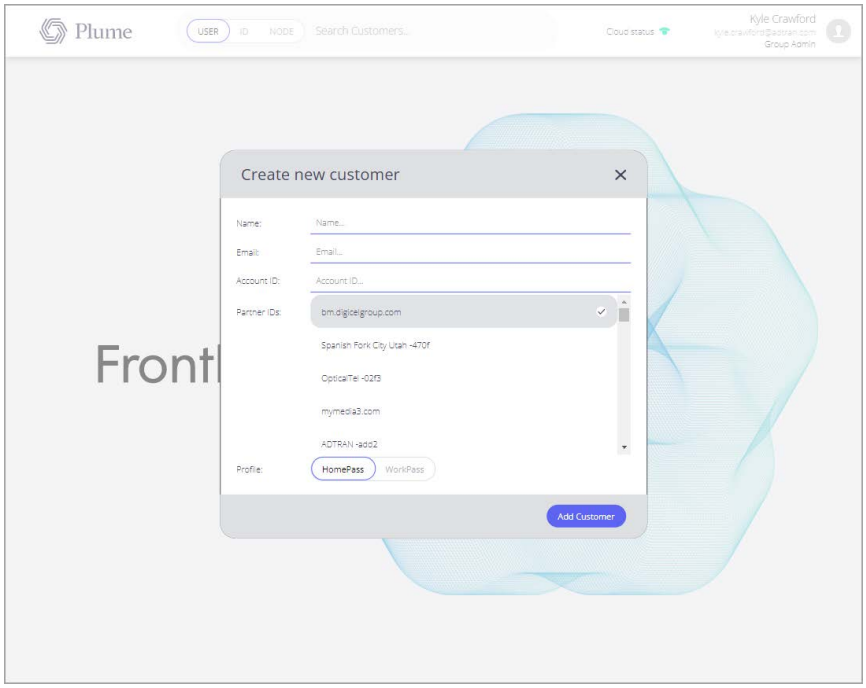
This section provides information about creating Plume accounts for new subscribers. If subscriber already has an account in the Plume portal, you can skip to *Adding Devices to the Plume Cloud (Onboarding) on page 9*.

1. Access the Plume portal at https://portal.plume.com/home and log into your account. If you do not have an account, see the *Prerequisites* section above.
2. Select **Applications** from the menu on the left.
3. In the **My applications** menu, select the **Launch** button under Frontline Tier 2 & 3.
4. In the top-right corner of the main Frontline dashboard, select your avatar icon and then select **Create Customer** from the drop-down menu.



5. A box will appear allowing you to choose if you would like to follow the customer creation with the onboarding process. The onboarding process can be done later if preferred. See *Adding Devices to the Plume Cloud (Onboarding) on page 9* for more information.
6. In the **Create new customer** menu, enter the user's **Name**, **Email**, and **Password**. The **Account ID** field is optional and allows providers to add existing account ID's into the Plume system for easier account

management across multiple platforms. Select your company in the **Partner IDs** box, and make sure the **Profile** toggle switch is set to **HomePass**.

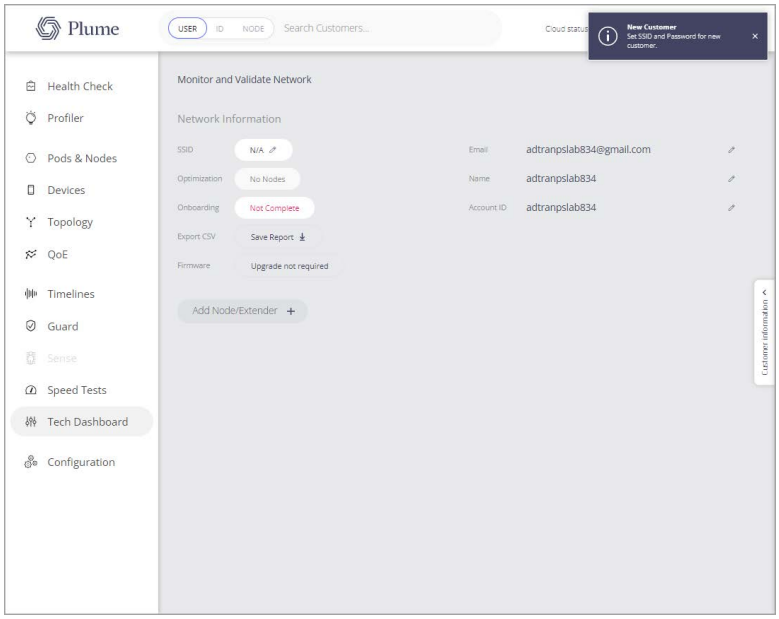


7. After entering the required information, select **Add Customer** to create the customer account.

Adding Devices to the Plume Cloud (Onboarding)

This section is a brief overview on how to add Adtran SDG equipment to the Plume cloud using Plume's Frontline portal. For a full overview of Frontline's features, visit the Plume Academy at http://learning.plume.com/learn/home.

1. Use search bar to find customer. Once customer is selected, you will be taken to their profile. Here you will see multiple dashboards that will allow you to customize the customer's account.
2. Select **Tech Dashboard** (see *Tech Dashboard on page 23*) from the left sidebar. The **Monitor and Validate** menu appears.



3. Enter network information in the **Monitor and Validate Network** menu and then select **Add Node/Extender** from the bottom of the page. Enter the MAC address(es) for the Adtran SDG to be added to this customer's account into the **Node ID** field. (Do not use the device serial number.)

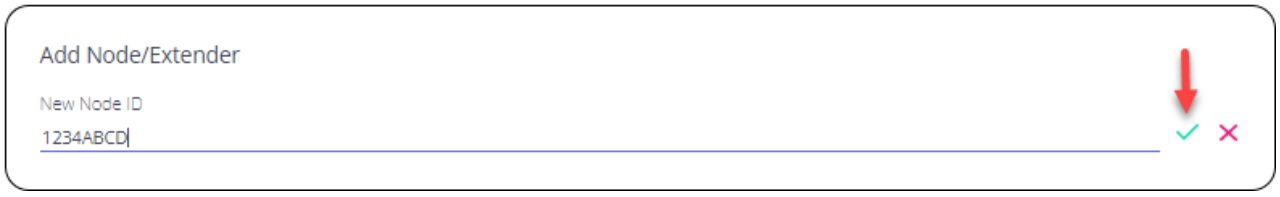
NOTE

If you receive one of the following errors and aren't able to rectify the problem, speak to a support engineer, open a ticket with Adtran Support by following the instructions provided on the Adtran Support website.

*- **Claimed by another account** - Someone else is already using that MAC in the same customer partner ID.*
*- **Could not find node with ID** - Device has not been added to the Plume cloud.*
*- **Node PartnerID Mismatch** - Node is assigned to another Partner, most likely Adtran in the case of an 841-t6.*

NOTE

*MAC addresses should be entered using all capitalized letters and without colons; for example, **12:34:56:AB:CD:EF** should be **123456ABCDEF**.*



4. After entering the MAC address(es) in the **Node ID** field, select the green check mark to apply the changes. The device will be provisioned into this customer's account. Customers can now complete the rest of the device activation using the Plume HomePass app, or a field technician can complete those steps.

> **NOTE**
>
> *SSID may be edited here if desired. Customer may also edit their SSID and password through the HomePass app. Default SSID can be found on the bottom of the unit.*

Activating Units Using HomePass

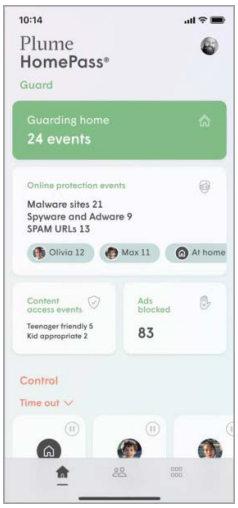
This section describes how to activate Adtran SDG equipment with the HomePass app once it has been added to the Plume cloud. For a full overview of everything HomePass offers, visit the Plume Academy at https://learning.plume.com/learn/home.

1. Download and install the Plume HomePass application on your smartphone or tablet. The HomePass app can be found in the Google Play Store or the Apple App Store.
2. Confirm that Bluetooth is enabled on the smartphone.
3. Open the HomePass app and follow the prompts to create an account.
4. Log into the HomePass app using the credentials you created in Step 3 above.
5. Connect the Ethernet and power cables to the 800 Series SDG per the instructions in the Quick Start Guide for your specific model of SDG. The unit will begin powering up.
6. If you are adding 841-t6's as extenders, it is recommended to plug in and set the gateway up before turning on and discovering the 841-t6s. This is so the 841-t6 extenders have a stable network connection to receive configuration and download firmware.

> **NOTE**
>
> *With the exception of the 841-t6 model, the rest of the 800 Series SDGs do not have an external power switch. The unit should immediately begin booting upon connection of the power cable.*

7. After power is connected, a single blue LED on the face of the unit will light briefly, then turn off for approximately **45 seconds**. When the LED lights up a second time, it will remain lit. The SDG is now in discovery mode and ready to be linked with the HomePass smartphone app.
8. In the HomePass app, under **Other Setup Options**, select the **Next** button. The other instructions at the top of that first screen (for example **Restart your modem**) should be ignored.
9. The app will make an initial connection with the SDG via Bluetooth in a few moments.
10. The HomePass app will progress to the **It's time to Wi-Fi** screen. Follow the on-screen prompts to choose a Wi-Fi name (SSID) and a Wi-Fi password. Complete both fields, then tap the **Next** button at the bottom of the screen.
11. Wait approximately **2 minutes** for the final setup process to complete. The steady LED on the face of the SDG mentioned in step 6 above remains lit during this time.
12. The final setup process is complete when the LED turns off. Return to the HomePass app on your smartphone.

13. If there are additional Plume Pods or Wi-Fi extenders that will be used in your network, follow the prompts in the HomePass app to configure these devices.
14. Select the **All done** button when it becomes available.
15. The setup is completed when a screen that resembles the following is displayed.



The SDG is now connected to the Internet and Wi-Fi is operational.

Verifying the Device is Connected to the Plume Cloud

There are two ways to verify the unit is working correctly in the Plume cloud. They are as follows:

- Check the unit status in Frontline or HomePass. Unit should appear online in both applications.
- Secure Shell (SSH) into the router from the LAN side via its IP address. Run the **show ovsh-table Manager** command. This test will show whether the unit is connected or not. For a more detailed command reference guide, please see the *Administrative Interface* document in the *Adtran Support Community*.

NOTE

Cloud and device may take a few minutes to fully synchronize. If problems continue to persist, see Troubleshooting on page 32.

Specifying Device Router or Extender Mode

Plume automatically determines if a unit is a router or an extender. If a router is already configured, and another router is plugged in, Plume will try to configure the second unit as an extender (if that unit supports extender mode). Currently, only the SDG 841-t6 supports extender mode.

NOTE

If you only want extenders in your network, you can select the extender only option in the Plume cloud. This is found under Configuration > WAN and Ethernet > Bridge.

4. Frontline Interface Overview

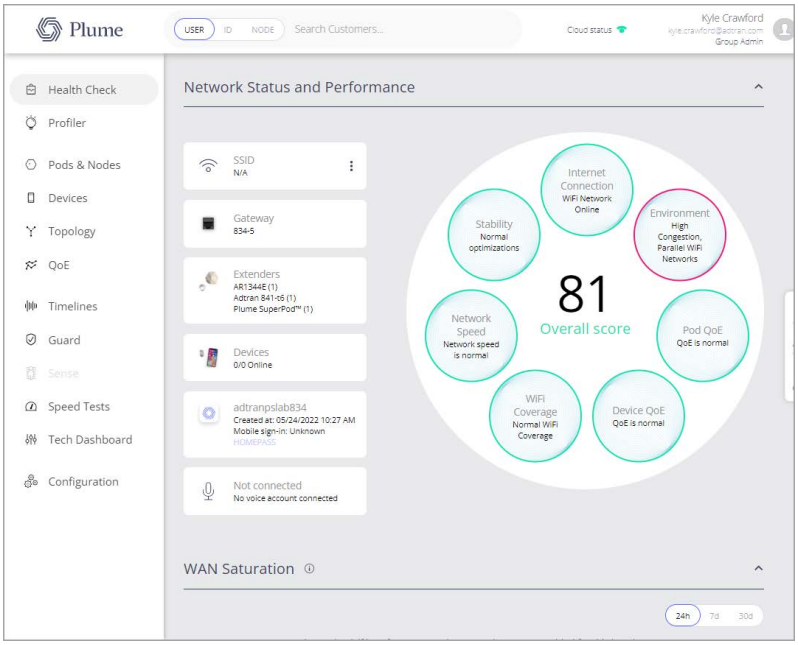
Frontline is Plume's solution for managing customers and their devices. It's built to give providers the tools they need to easily manage and troubleshoot any PlumeOS based equipment in their network for the best possible customer service. This section provides a brief overview of the features provided in Frontline. For a more detailed guide on all Frontline features, take the Frontline courses available online in Plume's Academy at http://learning.plume.com/learn/home.

General Navigation

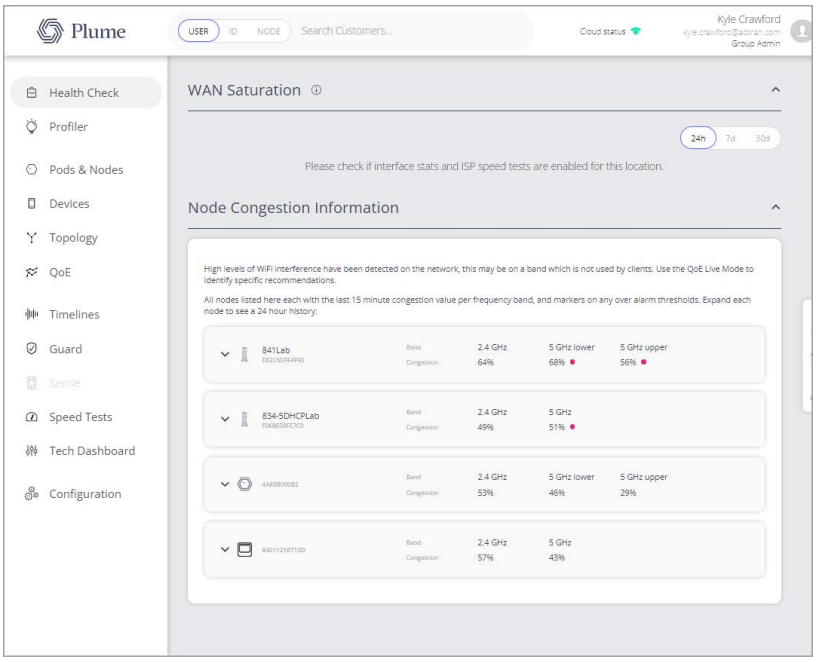
To access Frontline, refer back to steps 1 through 3 in *Creating New Customer Accounts* on *page 8*. Once logged in, you may search any customer by entering their customer ID, location, or node in the search bar. Selecting a customer will open their profile and you will see the menus listed below.

Health Check Menu

The **Health Check** menu provides basic information about the customer's network and determines an overall health score for the network. This score is based off of multiple variables that can be seen in the image below, green signifying good health and red signifying a potential issue. Any categories showing red can be selected and a list of alarms and errors will be displayed. For a list of alarms and troubleshooting methods, visit the *Health Check KPIs and Troubleshooting approach* article in the Plume cloud.

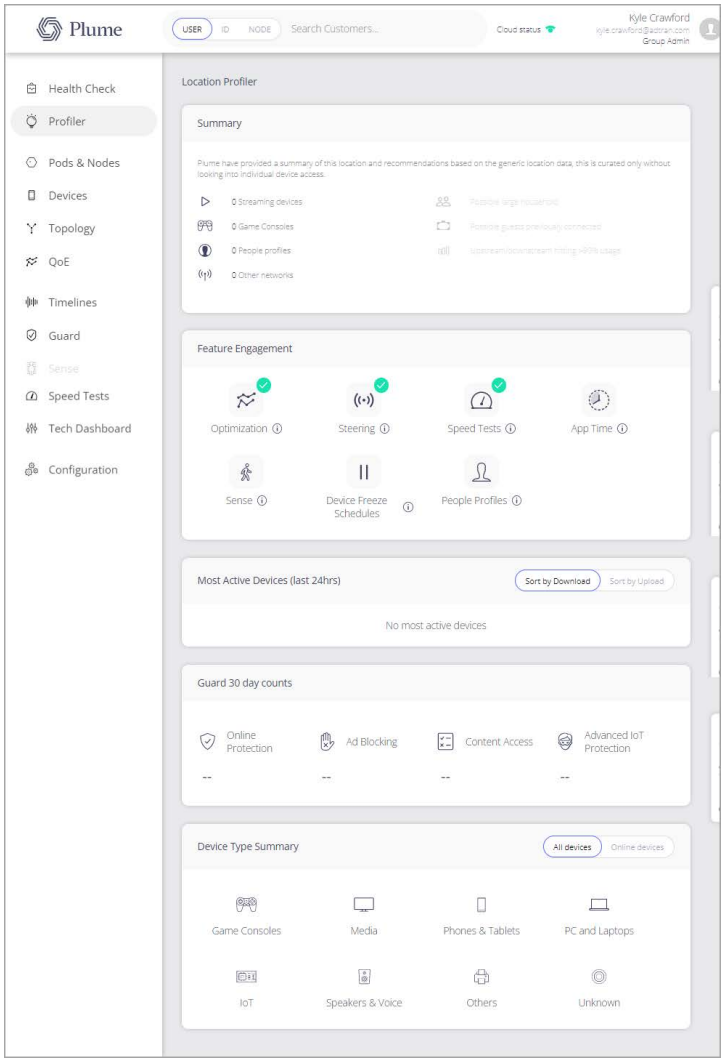


Below the health score wheel, you'll find the WAN Saturation and Node Congestion Information menus. These are both tools to help further determine the network's health.



Profiler Menu

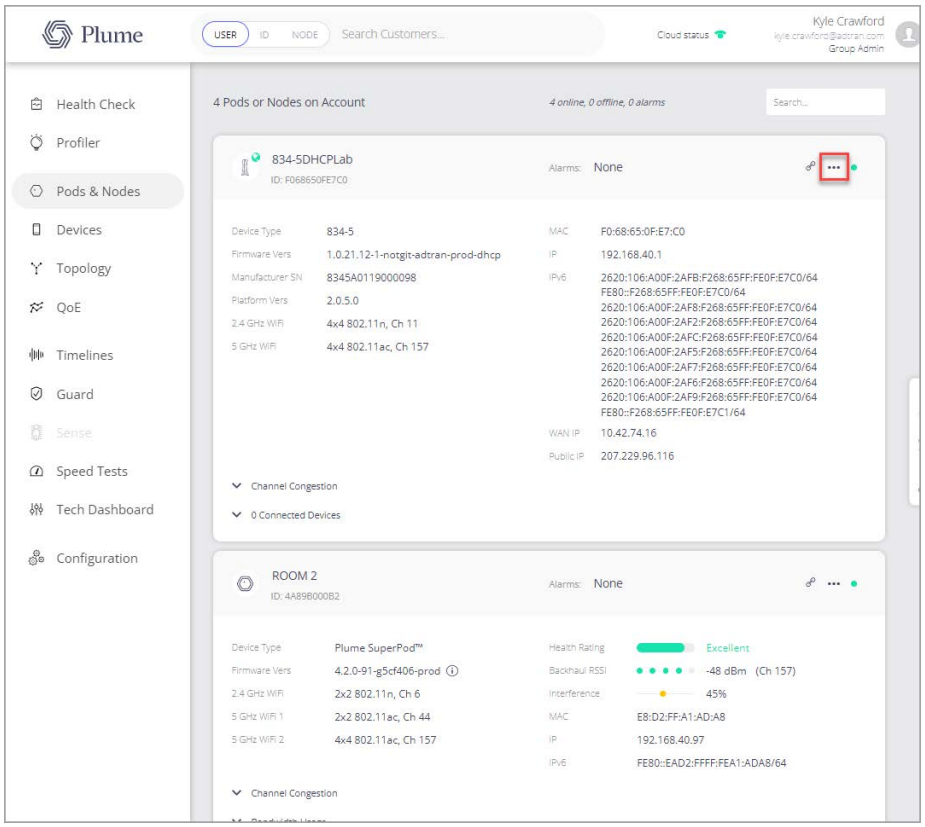
The **Profiler** dashboard automatically sorts all devices, users, and networks attached to the customer into function-based profiles for a more organized and streamlined look at the customer's network(s). This menu also displays a list of features the customer is using and general usage information.



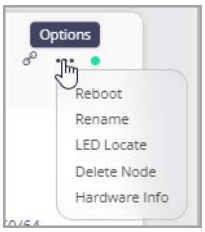
The Profiler is a useful tool for gathering customer data that can be used for improving customer service. The Feature Engagement area shows what features the customer is using in their network. The Guard area shows how active the customer's security is and how many times it has saved them from potential threats in the last month.

Pods and Nodes Menu

The **Pods and Nodes** menu displays information about the nodes on the account, including the IP address, MAC address, firmware version, and device serial number. A graph showing channel congestion over the past day/week and a list of all connected devices are also displayed.



There are also several tools within this dashboard. Select the three dots in the top right of any device window to open the **Options** drop-down menu to access these tools.

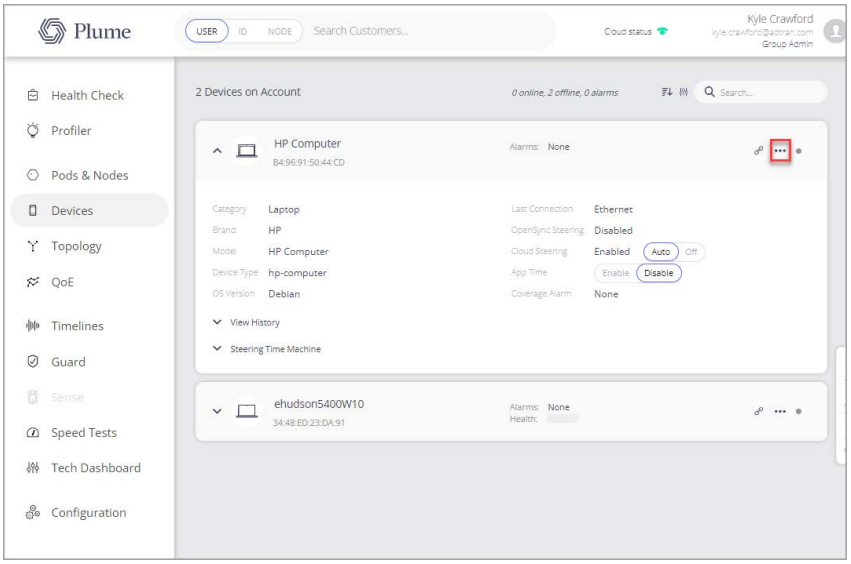


NOTE

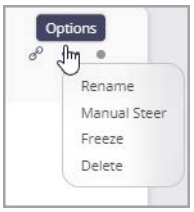
For a more detailed guide on all Frontline features, take the Frontline courses available online in Plume's Academy at http://learning.plume.com/learn/home.

Devices

The **Devices** dashboard shows each device and its corresponding networking and operating system information. This tab also allows manual steering of units and freezing users. For more information on steering and freezing, visit Plume's Academy at http://learning.plume.com/learn/home. History of connections, data consumption, and steering events are also displayed here.

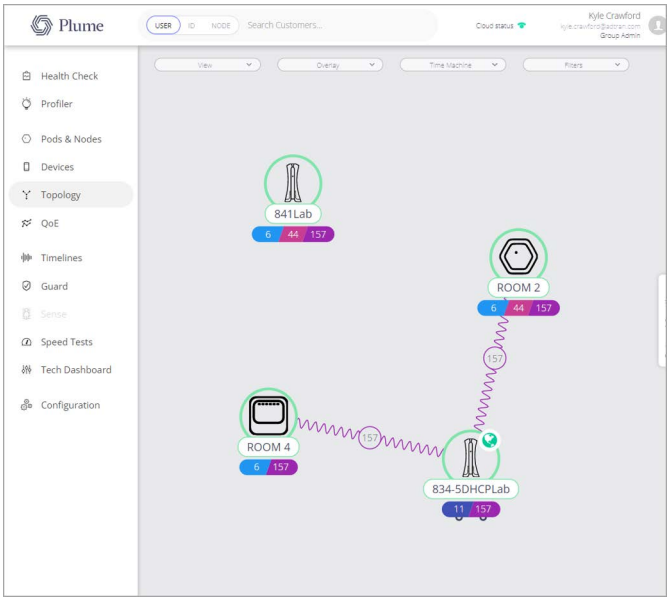


There are also several device management tools within this dashboard. Select the three dots in the top right of any device window to open the **Options** drop-down menu to access these tools. Here you can rename the device, toggle manual steering, freeze, or delete the device from the network.

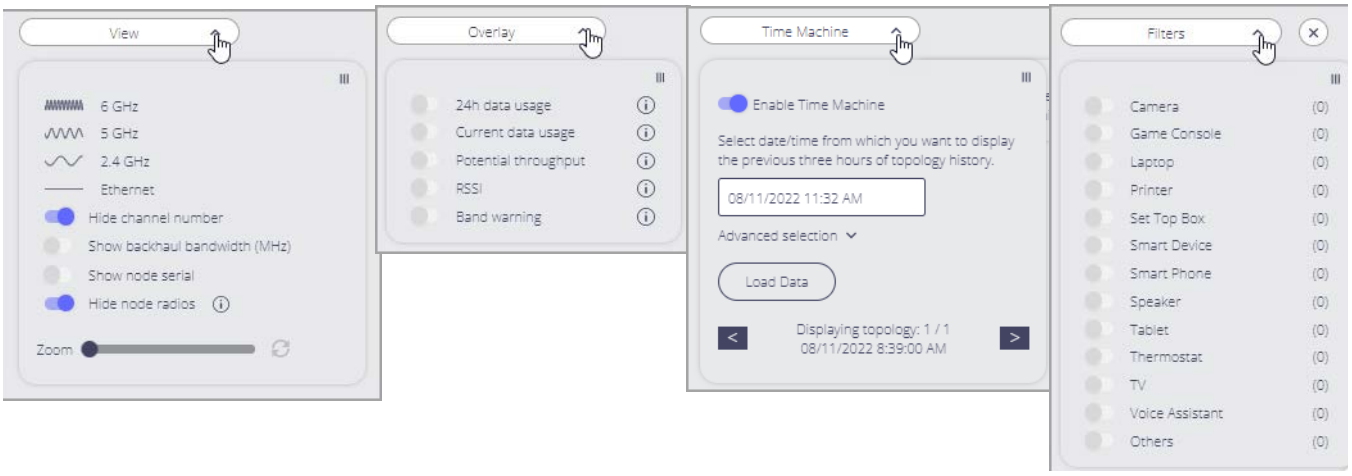


Topology

The **Topology** dashboard shows a topology view of the network with options to add views and overlays. This tool is used to get a quick visual representation of the network and the devices connected to it. Connections are shown as lines. A key can be seen in the **View** menu shown below.



Across the top of the screen, there are four different tabs: **View**, **Overlay**, **Time Machine**, and **Filters**. Each tab opens a menu that provides various tools for customizing the information displayed on this page.



View - This tab provides a key for reading different connection types and a few toggle switches to hide/show basic information. This tab also provides a zoom tool for the network.

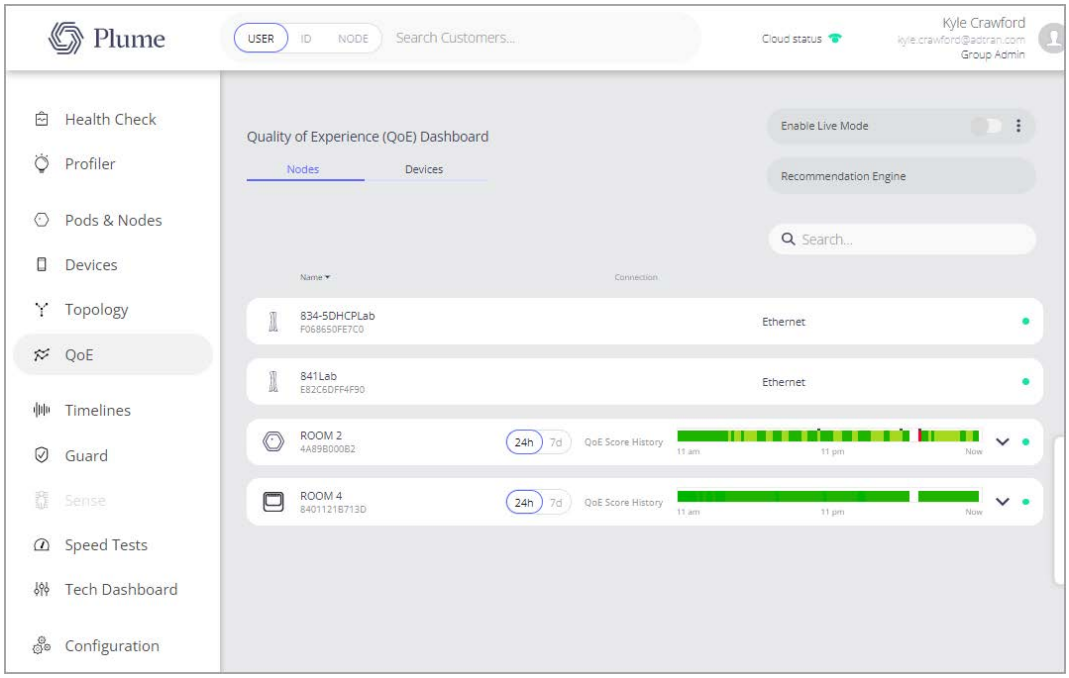
Overlay - This tab provides six toggle switches that will allow you to overlay different usage data values on the network topology map.

Time Machine - This tab lets you look into the history of the network and how it interacted with any devices that connected. Note that **Overlay** and **Filter** options do not work while in **Time Machine** mode.

Filters - This tab provides a large list of device Profiles (see) that you can toggle on or off. This helps filter what devices are being seen on the network topology map.

QoE

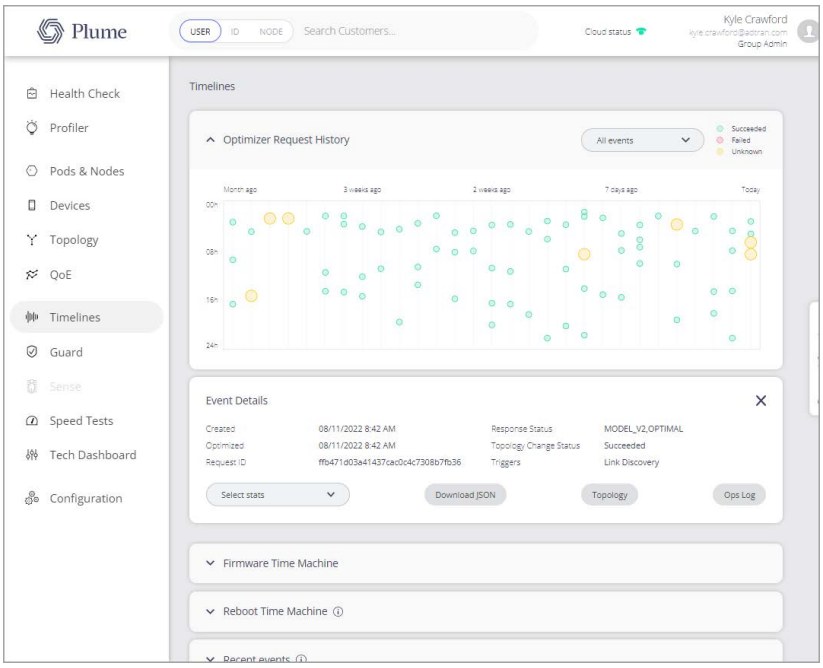
The **QoE** (Quality of Experience) dashboard allows you to view a QoE score over time for each device in the system's history. It also provides a live view of the expected experience for the device.



QoE scores range from 1 to 5 and are determined by factoring the "happiness" of devices on the network. A device is considered "happy" if the network is currently meeting its idle and active needs. The Plume QoE metric determines a device's needs while active and inactive, constantly measures that information over time, and determines the devices "happiness". This shows a much more accurate score than the standard QoS (Quality of Service) metric, and can tell a provider whether each and every connected device in a home is getting the throughput it needs. Better diagnostic information for the provider means better quality of service for the customer. More information on QoE scores can be found online at https://www.plume.com/measuring-quality-of-experience-with-plume.

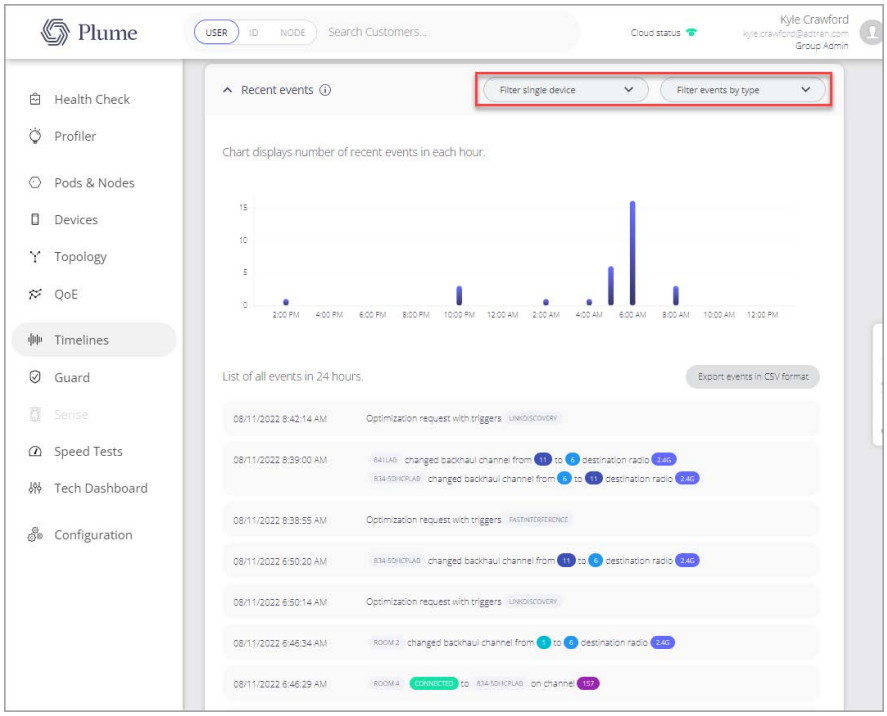
Timelines

The **Timelines** dashboard displays a full history of optimizations, a timeline of any reboots, and a list of any events (connections, optimizations, alarms, reboots, etc.) that occurred in the last 24 hours.



Optimizations are automatic scans of the network to make sure it is running as efficiently as possible. If any adjustments need to be made to improve the connectivity of Pods or devices, the optimizer will automatically make those changes. The network will run an automatic optimization at least once a day (default behavior) and will also run an optimization if the Plume cloud server detects any changes in the network. To view more information about network optimizations, select an Optimization Event. As shown below, general event details are displayed for each Optimization Event. This will include date/time, an automatically generated **Request ID**, response and topology statuses, and triggers. You'll also be able to download a .JSON event report, view any changes in the network topology map, or view the log of the optimization by selecting the applicable link (shown below) if desired.

At the bottom of the **Timelines** page, the **Recent Events** tab can be expanded to show a time-based chart of network events. Events include connections/disconnections, optimizations, alarms, reboots, and any other activity that might alter the network. These events can be filtered by device or event type by selecting the drop-down menus on the top-right of the tab. You can also create a CSV (Comma-Separated Values) file by clicking the **Export events in CSV format** button.



> **NOTE**
>
> *Thermal reboots are currently not supported in the **Reboot Time Machine** timeline.*

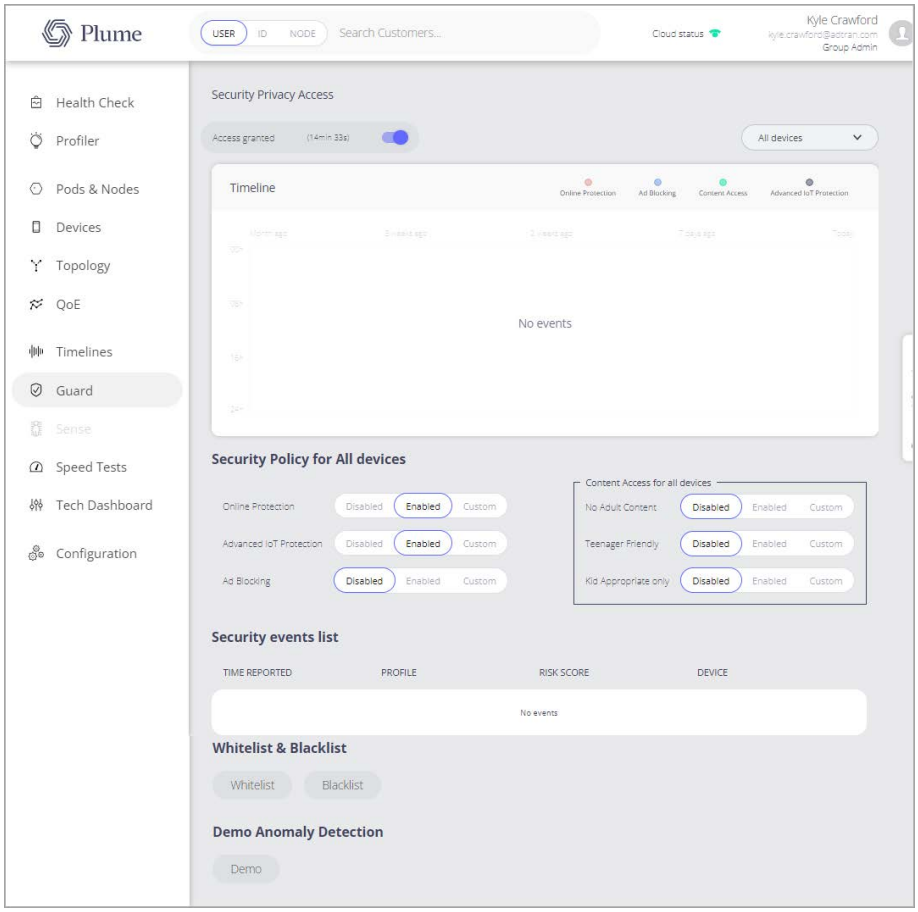
> **NOTE**
>
> *The **Firmware Time Machine** tab is also available on this dashboard, but anything upgraded via ACS is not currently supported. However, a **Firmware Upgrade** event will appear in the **Reboot Time Machine** timeline whenever an upgrade takes place.*

Guard

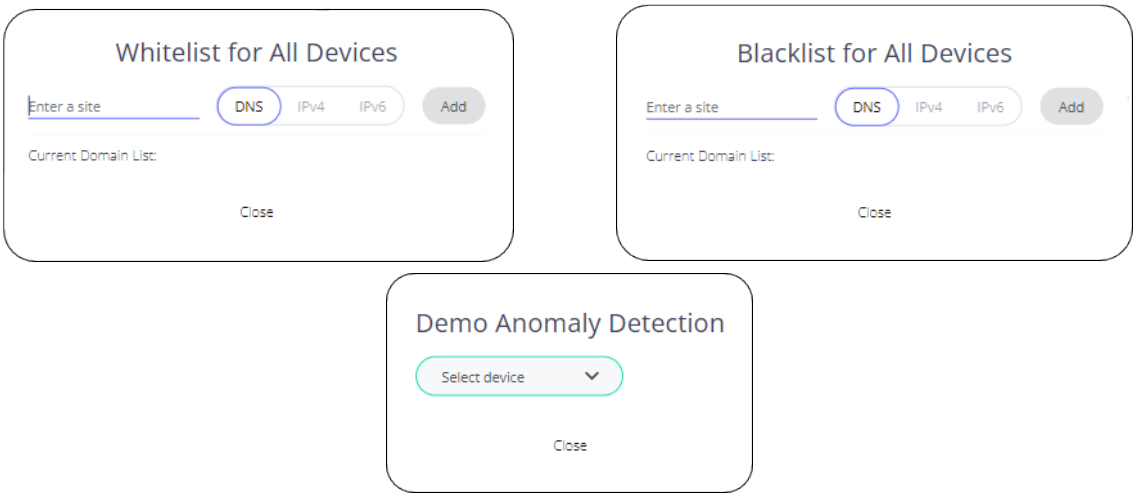
The **Guard** dashboard gives the power to edit various security options and block certain content to all devices or specified devices. To edit these settings, the **Enable access** switch must be toggled on. Once this switch is on, a **15** minute timer begins. After the 15 minutes, all security options return to their locked state until the **Enable access** switch is flipped again. This page provides a timeline showing any security-related events that have occurred within the past month, and a variety of tools used to customize security protocols and control content. All of these tools can be easily toggled on and off with default settings, or set to custom if custom settings are desired. If any security events take place, they will appear in the **Security events list**, below the tool toggle switches.

NOTE

The default view in the **Guard** dashboard shows all devices. You can select a specific device as needed to disable **Guard** and edit settings. This will allow you to keep **Guard** up for the rest of the network while modifying a single device.

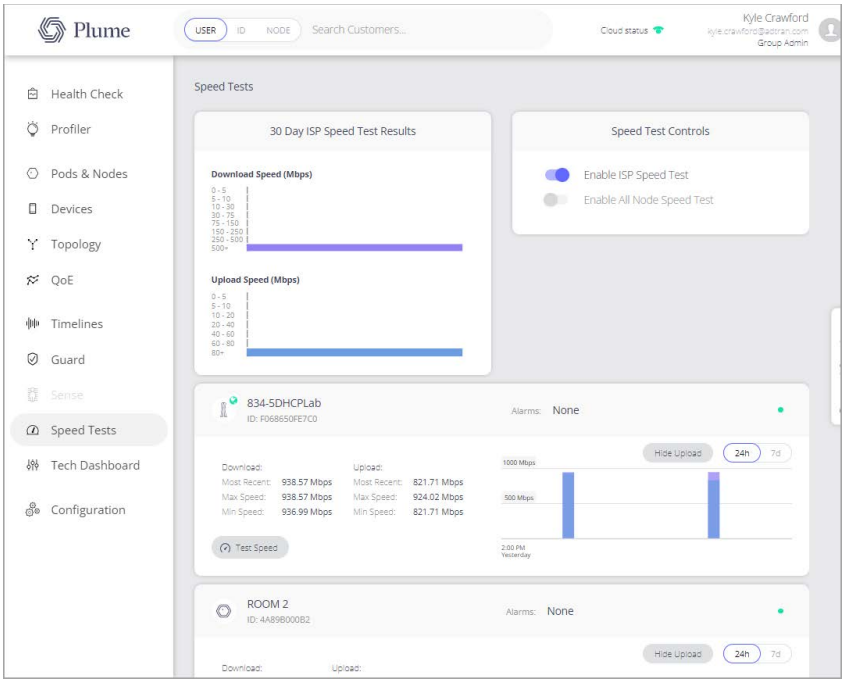


Tools for whitelisting and blacklisting are available on this page to allow or deny access to specific sites (shown below). Whitelisting can be useful if prior security settings are preventing access to a site you would like to access. Blacklisting can be a powerful tool to deny access to an untrustworthy or potentially dangerous site. A demo anomaly detection tool is provided to test the parameters that have been set on this dashboard. You may choose a device to simulate and the network will respond as it would if that device were pushing the security boundaries set. This is helpful to ensure security features are set up in the intended manner.



Speed Tests

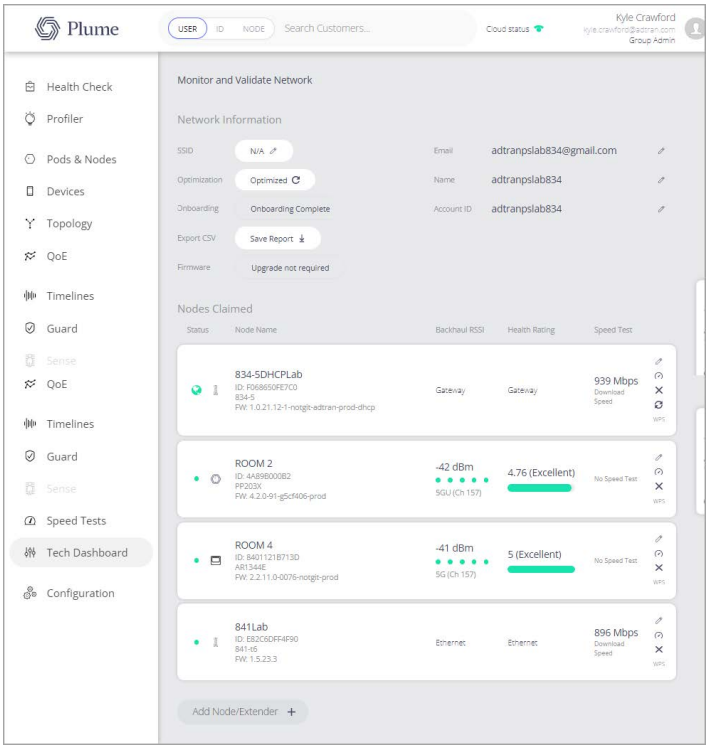
The **Speed Tests** dashboard displays the results of speed tests from each pod in the network. You can also enable **ISP** and **All Node** tests with the toggle switches on the right. The bottom of the page will show each network device and the speed test statistics on that device. You may also initiate a speed test on any of the devices listed by selecting the **Test Speed** option on the bottom-left of each device window. By default, the OpenWRT Ookla client is used to select a server with the best possible latency. This helps ensure accurate test results.



Tech Dashboard

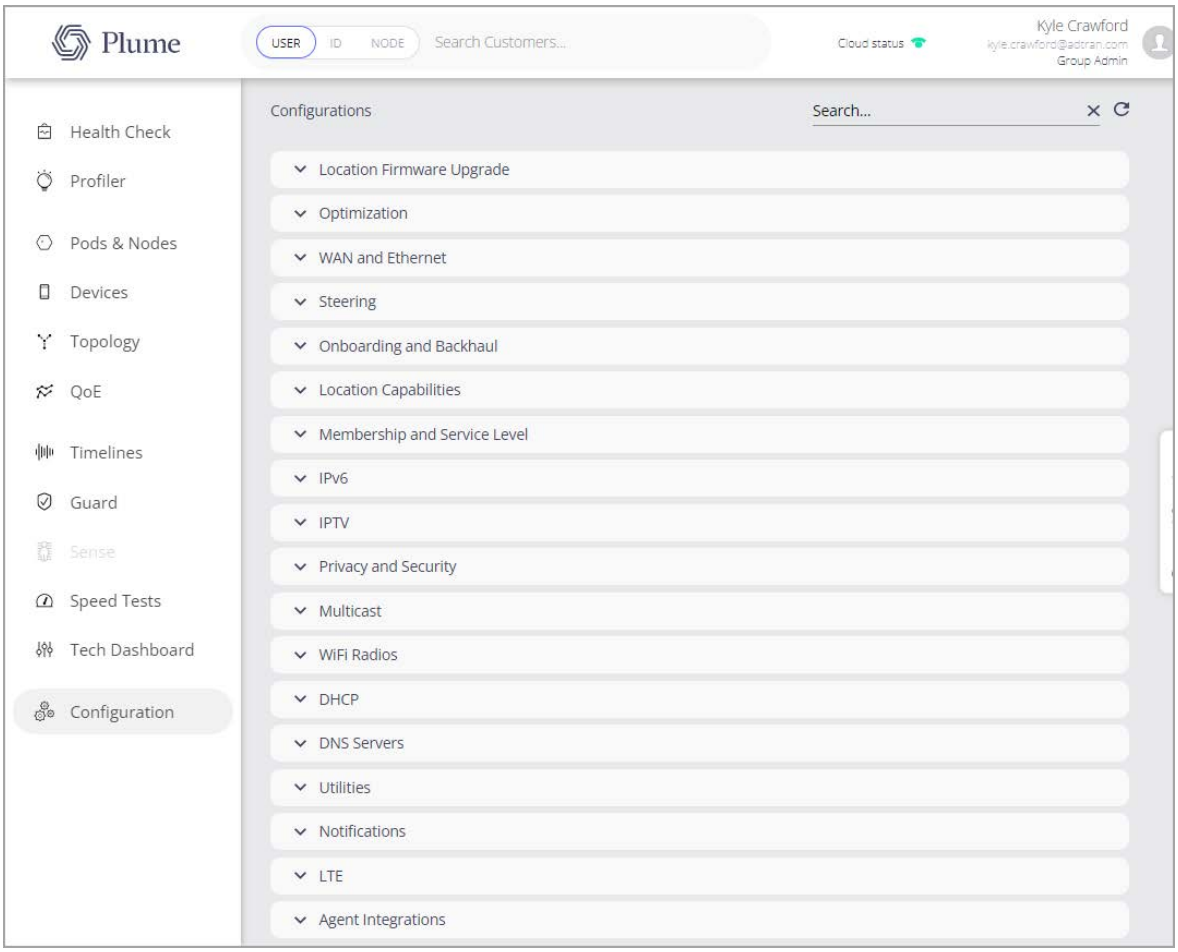
The **Tech Dashboard** displays account level information and nodes claimed on that account. This page gives the ability to edit network (SSID, optimization, onboarding) and account information (email, name, account ID,

etc), export a CSV status report, add/remove network devices (nodes), and manually run a Plume optimization scan.



Configuration

The **Configuration** dashboard allows the configuration of various network features (listed in the image below). Configurations are location specific, not device specific, so if changes are enabled, they are applied to all devices. For more detailed information on all of the configuration settings, take the Frontline courses located in the Plume Academy at http://learning.plume.com/learn/home.



Below

Table 1: Configuration Dashboard

Feature	Configuration Options
Location Firmware Upgrade	Not Currently Supported
Optimization	Enable/Disable automatic optimization and edit optimizer settings. Also allows you to run a manual optimization and reset any link failures.
WAN and Ethernet	Configure Network Mode, Ethernet LAN, UPnP, and persistent configuration settings.
Steering	Enable/Disable OpenSync and Cloud Steering.
Onboarding and Backhaul	Configuration options for WDS (if capable), Profile type, Dynamic Beaconing, Onboard Network, BLE Mode, WPS, and DPP Easy Connect. Onboarding status is also displayed.
Location Capabilities	A full list of all capabilities present at the location. Filterable by Capable/Not Capable.

Table 1: Configuration Dashboard (Continued)

Feature	Configuration Options
Membership and Service Level	A brief overview of the customer's membership and service level. Includes Service Level, Charge ID, Effective/Expiration Dates, and any equipment authorized on the account.
IPv6	Addressing, DNS, and IPv6 settings. Can also view IPv6 data.
IPTV	IPTV name and Enable/Disable information.
Privacy and Security	A long list of privacy and security settings that can be toggled and customized.
Multicast	Multicast and Unicast settings including IGMP and MLD.
WiFi Radios	WiFi radio options include uAPSD (power saving), Group ReKey, and Fast Transition. 2.4G and Control Mode options are also available.
DHCP	View and edit Subnet, Netmask, and Start/End IP. Create DHCP reservations and view DHCP data. Port forwarding is also configured in this section.
DNS Servers	View and edit primary and secondary DNS information. Shows DNS source and data.
Utilities	Quick tools for location management. Includes location reboot, unclaim all nodes option, neighbor's report, customer groups, email status, password reset, controller resync, and audit logs. Also allows you to generate a logpull for the location and view a history of logpulls performed.
Notifications	Customize notifications for new devices connected and locally administered MAC's.
Agent Integrations	Enable/Disable any third party integrated systems (for example, SamKnows).

NOTE

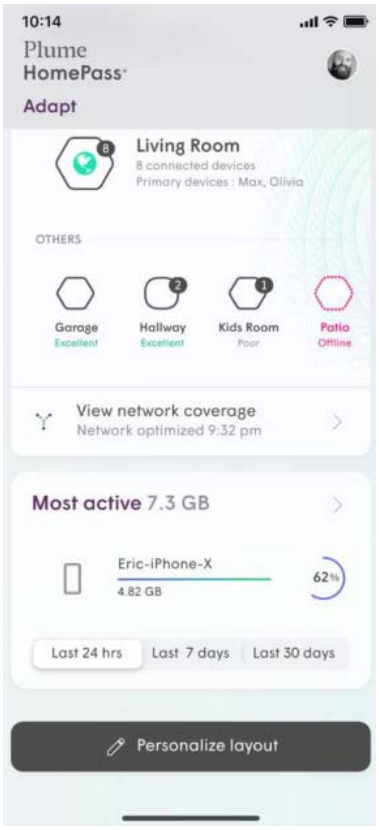
If using a Plume Pod or OpenSync device, some features may show supported which are not supported in the Adtran hardware. See the SDG Feature Matrix on the Adtran Support Community for a detailed breakdown of supported features.

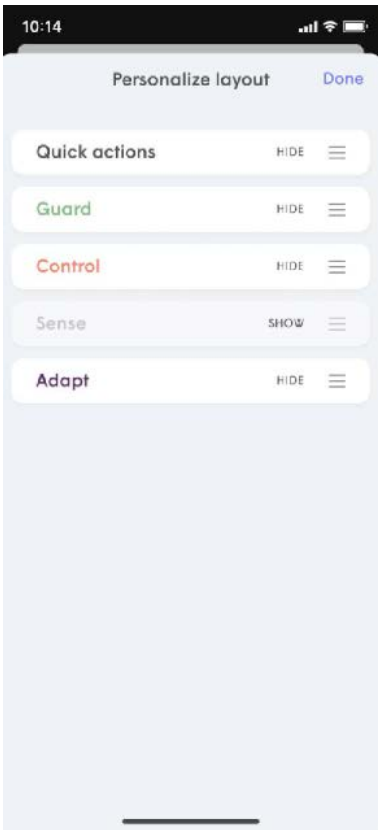
5. HomePass Interface Overview

This section provides a brief overview of the features provided in the HomePass app. For more detailed information about HomePass features, visit the Plume learning portal online at http://learning.plume.com/learn/home.

Home Screen

This is the screen you will be presented with when opening the app. This customizable screen provides an overview of the current status of the network and provides a high-level view of **Guard** events, **Control**, **Sense**, and **Adapt**. To customize the layout of the **Home** screen, scroll to the bottom and choose **Personalize Layout**.

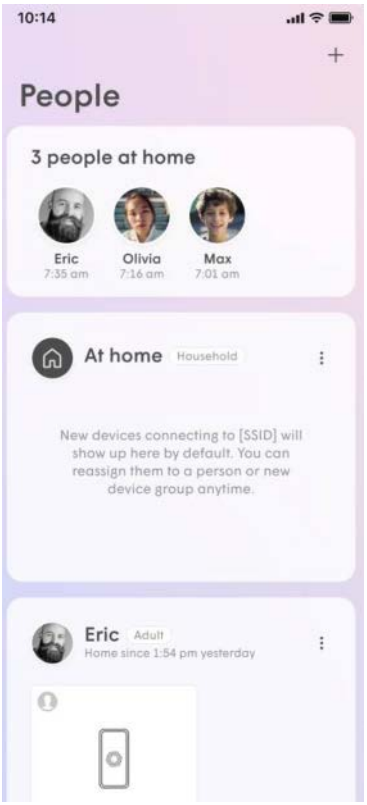


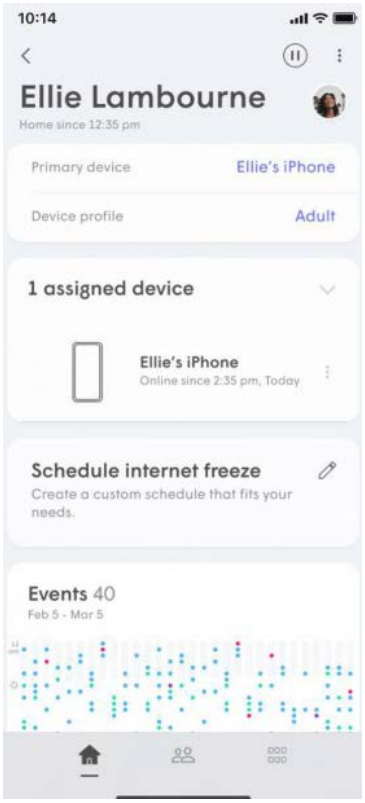


People

The **People** menu is where individual users of the network can be managed. Control-related functions include tools such as **Time Outs** and **Internet Freezes**. This screen is broken into three categories: **People at Home**, **At Home**, and **People Cards**.

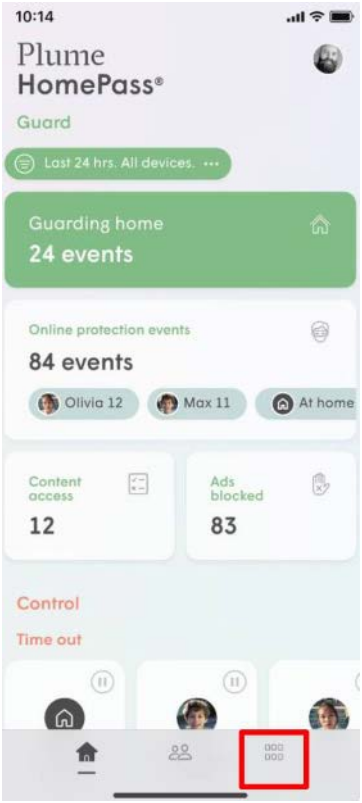
- **People at Home** - Displays a list of all people currently at home, based on their primary device connection status to the network.
- **At Home** - Used for unassigned devices. All new devices that connect to the network are added to this card until they are assigned to a person.
- **People Cards** - Displays a summary of each person on the network. Selecting someone's card allows you to easily change their assigned devices, set up device profiles, create time outs, enable freezes, and send them invitations to the HomePass app.

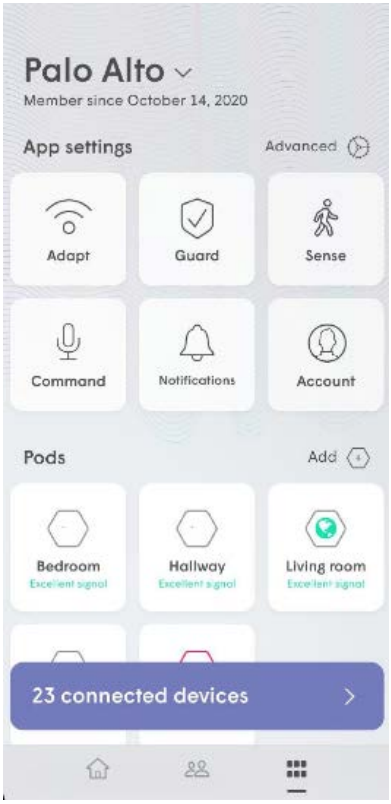

10:14
People
3 people at home
Eric
7:35 am
Olivia
7:16 am
Max
7:01 am
At home
Household
New devices connecting to [SSID] will show up here by default. You can reassign them to a person or new device group anytime.
Eric
Adult
Home since 1:54 pm yesterday


10:14
Ellie Lambourne
Home since 12:35 pm
Primary device
Ellie's iPhone
Device profile
Adult
1 assigned device
Ellie's iPhone
Online since 2:35 pm, Today
Schedule internet freeze
Create a custom schedule that fits your needs.
Events 40
Feb 5 - Mar 5

More

The **More** menu is where all HomePass features and settings are managed. To navigate to this menu, click on the right icon at the bottom of the screen (red box below). For more information on the features provided by HomePass, visit the Plume learning portal at http://learning.plume.com/learn/home.





Below

Table 2: HomePass Settings

Setting	Configuration Options
Adapt	Change the SSID. Manage and create passwords for WiFi access.
Guard	Online Protection, Advanced IoT Protection, Ad Blocking, and Privacy Mode.
Sense	Motion detection.
Command	Control your HomePass network using voice assistants.
Notifications	Manage push notifications sent from HomePass network.
Account	Log out of the account or switch between locations. View membership information if applicable.
Advanced	Reservations and port Forwarding, Networking Mode, DNS, UPnP Settings.

6. SDG Status LEDs with PlumeOS

Adtran's SDG units are equipped with a multifunction status LED that represents the unit's current status. The table below describes the patterns and colors of this LED.

Table 3: Multifunction Status LED for PlumeOS

Color	LED State	Event
Blue	Solid	Power is on.
Green	Pulsing	Attempting to connect.
Green	Blinking (double)	During device naming (this device) and waiting for optimization to finish.
N/A	Off	During device naming (other devices).
N/A	Off	Internet is working.
White	Pulsing after 3 minutes	Internet is down (with power) or Internet is still connected but lost cloud connection.
N/A	Off	Cloud planned outage.
Green	Pulsing	Claimed device (by another account).
Red	Rapid Blinking	TFTP/recovery blink.

NOTE

If reset button is pressed for around 5 seconds, all LEDs will turn off and device will reboot. If reset is held for more than 60 seconds, the device will be reverted to previous image and LED will blink white continuously.

7. SDG 841-t6 Extender

Adtran's SDG 841-t6 Router/Extender is designed to work seamlessly with PlumeOS as a stand-alone router or an extender. This section will be going over Plume's extender features and how the 841-t6 will behave as an extender. Adding an SDG extender to the Plume cloud is done the same way as adding any other SDG device. See *Adding SDG Devices to the Plume Cloud on page 7* for more information.

Extender Placement

Extenders should be placed **21**-**30** feet apart through walls and **42**-**59** feet apart in open spaces. Be sure to position extenders in central locations along interior walls for the best coverage. Adjust extender placement if the extender is not receiving optimal signal strength (see *Extender Troubleshooting on page 31* for more information).

NOTE

Extender placement will vary on a case-by-case basis due to housing arrangements. Best practice is to achieve a Received Signal Strength Indicator (RSSI) value of no worse than ***-70****. When reading RSSI values, the closer you are to zero the better. This value can be found in Frontline for each extender under the* ***Pods and Nodes*** *dashboard.*

Access Through Secure Shell (SSH)

To access any SDG 841-t6 through SSH, it must first be added to the Plume cloud. See *Adding SDG Devices to the Plume Cloud on page 7* for guidance. If you are on the LAN side, you can access your unit from the LAN IP locally. Once accessed, an admin user can run basic show commands and perform simple troubleshooting. You may also upgrade software while accessing through SSH. The login information for accessing your unit will be:

Username: admin

Password: adtran-plos

For a more detailed guide on how SSH works with PlumeOS, please see the *Administrative Interface* document in the *Adtran Support Community*.

Extender Troubleshooting

There are a few extender-specific errors and alarms that may occur. If this section does not cover what you are looking for or problems persist, please see *Troubleshooting on page 32*.

Internet Connection Alarms

If the **Internet Connection** tile on the **Health Check** dashboard (see *page 13*) turns amber in color, one or more of the nodes is having trouble connecting to the Internet. This could be because of extender placement, bad Ethernet connectivity, or power issues. To troubleshoot this issue, follow these steps:

1. Check to see if the node is connected via Ethernet.
2. If yes, check the Ethernet connection between the extender and router.
3. Power cycle the extender. This will cause the unit to renegotiate its Ethernet connection.

Failed Optimization

If you receive the error message **Network Unstable: Failed Optimization**, this may be due to an extender issue. This can happen if one of the extenders is fluctuating in and out of range, excessive interference is causing connection issues, or if one or more of the units are offline. Within the error message there will be a **Reference log record** link you can copy into a browser. This will give detailed on-screen prompts of what needs to be done to fix the issue. Follow the prompts and then reboot the router. This will be followed by an automatic optimization. If the optimization is successful, the errors will go away. If the optimization fails, the previous steps will repeat so other adjustments can be made.

Low Extender Broadband Efficiency/Low Extender Speed

These alarms are often due to over-extending the range of an extender. This issue will cause lower speeds for any device connected to the extender. To fix this issue, move the extender closer to the router or other extender so the unit can receive a stronger signal. Once repositioned, an Optimization will be triggered and a Speed Test can be run. If results do not change, the customer may need additional extenders.

8. Upgrading Device Firmware

All PlumeOS software requires the use of an Auto Configuration Server (ACS) or command-line interface (CLI) to upgrade and manage device firmware. For information on performing the upgrade via Mosaic Device Manager (MDM), refer to the *Updating Firmware* article included in the MDM online help. MDM is based on the TR-069 open standard. Below is a list of features provided.

- Functions supported
  - Solicit/Inform
  - Reboot
  - Upgrade/Downgrade
  - PPPoE Credential Provisioning
  - Voice Provision
- Device Menu Options
  - Control Panel
  - Announcements
  - Gateway Information
  - Gateway Status
  - Speed Test
  - Replace Device
  - Reboot Device
  - Upgrade Firmware
  - Event Logs
  - Factory Default Device
  - Parameter Browser
  - Script
  - Synchronization

NOTE

For 841-t6 units running PlumeOS, if the customer does not have an ACS they can utilize our TR69 Auto Update service. Units are automatically opted in for this service. For more information on how PlumeOS Auto Update works, visit the PlumeOS Auto Update Feature for the 841-t6 article on the Adtran Support Community.

9. Troubleshooting

This section describes how to take a log pull through Frontline and open a support ticket through the Adtran portal. For a more detailed command reference guide, please see the *Administrative Interface* document in the *Adtran Support Community*.

Conducting a Logpull

To take a logpull, first use the search bar to find the customer for which a log is required. Once a customer's profile has been opened, navigate to the **Configuration** dashboard. Scroll down and expand the **Utilities** tab. Here you can submit a log pull request by selecting the **Generate Logpull** button. Once completed, the log pull will appear in the **Logpull History**. From the history, log pulls can be downloaded or a link to the log can be copied.

Opening a Support Ticket

To speak to a support engineer, open a ticket with Adtran Support by following the instructions provided on the *Adtran Support* website. Tickets can be submitted online or via phone.

10. Additional References

Below is a list of additional references.

Table 4: Additional References

Name	Link
SDG Feature Matrix	https://supportcommunity.adtran.com/t5/Service-Delivery-Gateway-SDG/bd-p/sdg-feature-matrix
PlumeOS Admin Interface Guide	https://supportcommunity.adtran.com/t5/PlumeOS/PlumeOS-Admin-Interface-Command-Reference-Guide/ta-p/37671
Adtran Support Community	https://supportcommunity.adtran.com/
Adtran Support	https://www.adtran.com/support
Plume Academy	http://learning.plume.com/learn/home
Plume Portal	https://portal.plume.com