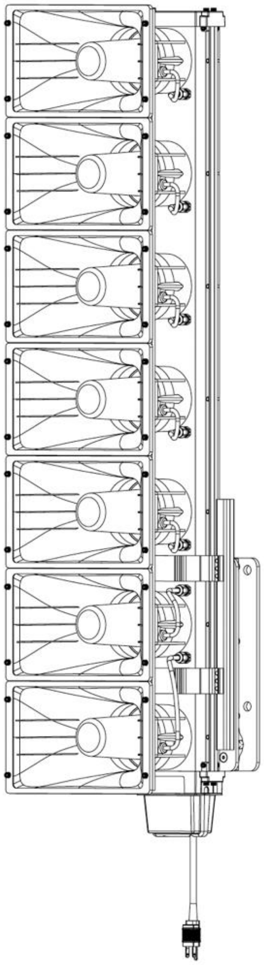
8507 IP Horn Array Speaker

User Guide



UG-8507-06102024
Firmware Version 5.5
support@algosolutions.com
Dec 18, 2024

Algo Communication Products Ltd.
4500 Beedie Street, Burnaby
V5J 5L2, BC, Canada
1-604-454-3790
www.algosolutions.com

Table of Contents

IMPORTANT WARNING AND SAFETY INFORMATION

⚠ Important Notice

The 8507 Horn Array Speaker is AC mains powered. If the power plug is removed for direct connection to a mains supply, the connections should be performed by a qualified electrician according to local building codes.

The 8507 Horn Array Speaker must be mounted securely to a structure capable of supporting its weight. Note that this device is capable of output sound pressure levels in excess of 137 dB at 3 feet (1m). Ensure that the Horn Array is mounted in a location such that nobody is directly in front of or beside the Horn Array including during installation and testing of this device.

If used for emergency communications, the 8507 IP Horn Array Speaker should be routinely tested. SNMP or Algo ADMP supervision is recommended for continuous assurance of proper operation.

The 8507 IP Horn Array Speaker may be used in wet or outdoor environments contingent on electrical and network connections being suitable for wet or outdoor locations. It is strongly recommended that an outdoor-rated network cable be used for network connection.

CAT5 or CAT6 connection wiring to an IEEE 802.3 compliant network PoE/PoE+ switch must not leave the building perimeter without adequate lightning protection consistent with local electrical codes.

⚠ Avis important

L’ensemble de haut-parleurs à pavillon 8507 est alimenté par courant alternatif (CA). Si la fiche d’alimentation est retirée pour être branchée directement sur le secteur, les raccordements doivent être effectués par un électricien qualifié, conformément aux codes de construction locaux.

L’ensemble de haut-parleurs à pavillon 8507 doit être monté solidement sur une structure capable de supporter son poids. Notez que cet appareil est capable d’émettre des niveaux de pression acoustique supérieurs à 137 dB à 1 mètre (3 pieds). Veillez à ce que l’ensemble soit monté à un endroit tel que personne ne se trouve directement devant lui ou à côté de lui, y compris lors de l’installation et de l’essai de l’appareil.

S’il est utilisé pour des communications d’urgence, l’ensemble de haut-parleurs à pavillon IP 8507 doit être testé régulièrement. L’outil de supervision SNMP ou la plateforme de gestion d’appareil ADMP d’Algo sont recommandés pour garantir en permanence le bon fonctionnement.

L’ensemble de haut-parleurs à pavillon IP 8507 peut être utilisé dans des environnements humides ou extérieurs à condition que les connexions électriques et réseau y soient adaptées. Il est fortement recommandé d’utiliser un câble réseau adapté à l’espace extérieur pour la connexion au réseau.

Le câblage de connexion CAT5 ou CAT6 à un commutateur PoE/PoE+ conforme à la norme IEEE 802.3 ne doit pas quitter le périmètre du bâtiment sans une protection adéquate contre la foudre, conformément aux codes électriques locaux.

⚠ Aviso Importante

El Parlante 8507 de Arreglo Bocina “8507 Horn Array Speaker” está operado por energía de C.A. Si se retira el enchufe de energía para conexión directa a tomacorriente, un técnico cualificado deberá realizar las conexiones, de acuerdo con las normas de construcción locales.

El Parlante 8507 de Arreglo Bocina deberá ser montado de forma segura a una estructura con capacidad para soportar su peso. Por favor note que este dispositivo es capaz de proporcionar niveles de presión sonora superiores a 147 dB a 3 pies (1m). Cerciórese de que el Arreglo Bocina “Horn Array” está montado en una dirección tal que nadie esté directamente frente a o detrás del Arreglo Bocina, incluyendo durante la instalación y pruebas de este dispositivo.

Si se usa para comunicaciones de emergencia, el Parlante 8507 Arreglo Bocina IP habrá de probarse rutinariamente. Se recomienda la supervisión SNMP o Algo ADMP para la continua confirmación de su adecuado funcionamiento.

El Parlante 8507 Arreglo Bocina podrá ser utilizado en ambientes húmedos o de exteriores en contingencia con la idoneidad de las conexiones eléctricas y de red para ubicaciones húmedas o exteriores. Se recomienda enfáticamente que se use un cable de red certificado para exteriores para la conexión de red.

El cableado CAT5 o CAT6 a un switch de red que cumpla con IEEE 802.3 PoE/PoE+ no deberá de abandonar el perímetro de edificación sin una protección adecuada contra rayos, consistente con los códigos eléctricos locales.

Disclaimer

The information contained in this document is believed to be accurate in all respects but is not warranted by Algo. The information is subject to change without notice and should not be construed in any way as a commitment by Algo or any of its affiliates or subsidiaries. Algo and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. Algo assumes no liability for damages or claims resulting from any use of this manual or such products, software, firmware, and/or hardware.

No part of this document can be reproduced or transmitted in any form or by any means – electronic or mechanical – for any purpose without written permission from Algo.

For additional information or technical assistance in North America, please contact Algo’s support team:

Algo Technical Support
1-604-454-3792
support@algosolutions.com

1 PRODUCT OVERVIEW

Algo's 8507 IP Horn Array Speaker is a highly durable speaker with wideband audio designed to deliver clear, intelligible audio communication, such as voice paging and emergency notifications in reverberant, loud environments.

The 8507 is IPX9-rated for harsh outdoor environments, including areas with frequent exposure to water, dust, or debris. It can withstand temperatures from -40°C to +50°C. Each Horn Array Speaker is approximately 41 lbs or 46 lbs with the mounting bracket. The outer dimensions are 45.3" x 11" and 10.8" deep without the mounting bracket. With a mounting bracket, the 8507 is 14" deep to a wall when wall-mounted or 16.25" to a pole center when pole-mounted. The 8507 can be used stand-alone or in a cluster configuration, depending on your needs.

Important

This guide provides important safety information that should be read thoroughly before permanently installing the product.

2 SETUP AND INSTALLATION

Included

- 8507 IP Horn Array Speaker
- Array mounting bracket and hardware kit
- Weather resistant ethernet connector
- Wiring shroud

Not Included (Optional)

- Pole-mount bracket kit (8507PMB)

2.1 Getting Started

The 8507 Horn Speaker requires AC Mains power and PoE for full operating power. For configuration and quick testing, the Horn Array Speaker can operate without AC power but will limit its audio output to a single horn driver.

1. Connect the 8507 to a PoE network switch and AC Mains power (optional). The blue LED in the bottom plastic cap will turn on with PoE power until the device boot up is completed. This typically takes about 30 seconds.

2. Once the blue LED turns off, press the reset switch (RST) to hear the IP address over the speaker. The IP address for your device may also be found via the Algo locator tool: www.algosolutions.com/locator. The tool is only available for Windows computers.

3. Type the device IP address into a web browser to access the web interface and configure your device for testing. Note that the 8507 Horn Array may also be configured using centralized provisioning or the Algo Device Management Platform (ADMP).

2.2 Configuration

1. Enter the 8507 IP address into a web browser to access the web interface.
2. Log in using the default password: *algo*.
3. Navigate to **Basic Settings → SIP** and enter the IP address or the domain name for the SIP server (provided by your IT team or hosted provider) into **SIP Domain (Proxy Server)**.
4. Enter the Page and/or Ring credentials **Extension**, **Authentication ID**, and **Authentication Password** (provided by your IT team or hosted provider). If you are not using an extension, leave the fields blank. Note that some SIP servers may say Username instead of Authentication ID.
5. Verify the extension is properly registered with the SIP server in the Status tab. Ensure the SIP registration says **Successful**.
6. Test the adapter by dialing the registered SIP extension from a telephone. The speaker should auto-answer, play the default pre-announce audio, and open a speech path.

2.3 Mounting

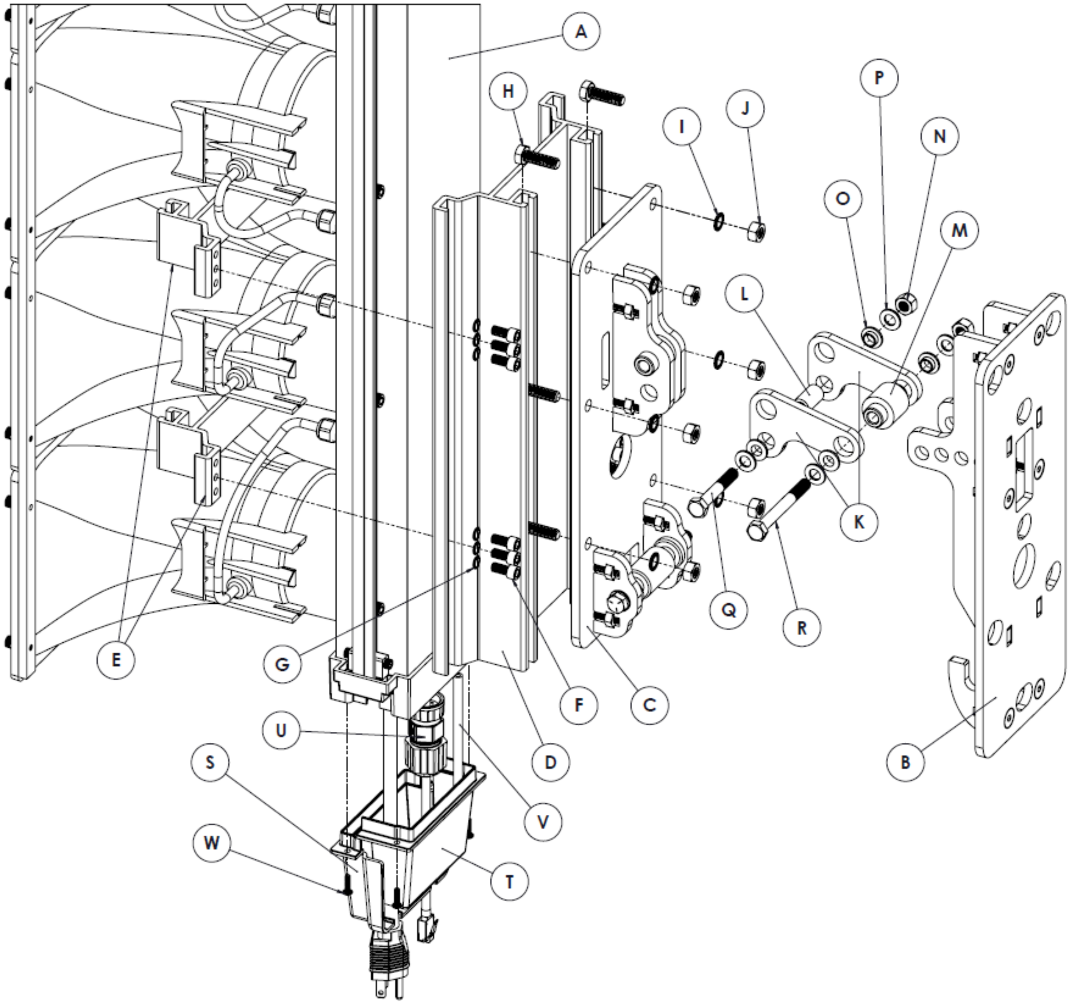
The 8507 is typically installed vertically to create a dispersion pattern with narrow vertical and wide horizontal coverage. It may be tilted downward from 5 to 35 degrees in 5-degree increments.

When surface mounted, an optional bracket component allows up to 90-degree left to right rotation. For pole mount applications, any interfering structures or surfaces will determine the degree of rotation. A pole-mounted 8507 can rotate 90-degrees left to right if the pole center is at least 6 inches from a wall.

To prevent personal harm, it is essential that:

- Due to its weight and size, two people handle, install, and mount the 8507 Horn Array Speaker.
- The mounting surface or material is sufficient to carry the device's weight. The device can be mounted to a solid surface or 2" NPS (2.375" 63.3mm OD) pole.
- Appropriate fasteners are used to prevent the device from falling.
- Contact of dissimilar metals is avoided, especially in outdoor or wet applications, to avoid galvanic corrosion. Note that the mounting brackets and hardware supplied with the Horn Array Speaker are designed to prevent aluminum and stainless-steel components from contacting each other.
- Isolation components are used to ensure long-term performance of the metal bracket components.

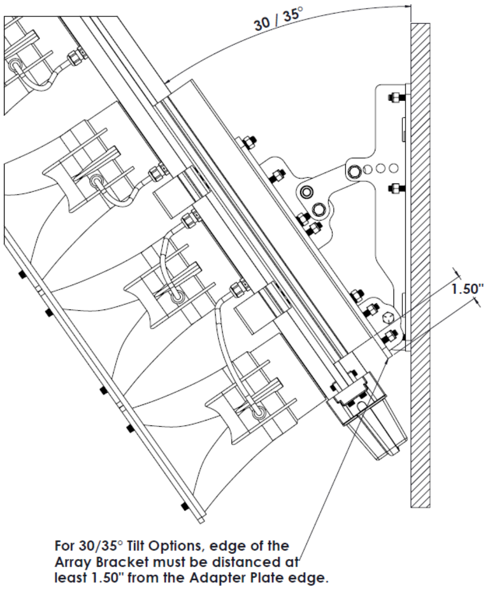
INSTALLATION OF 8507 HORN ARRAY

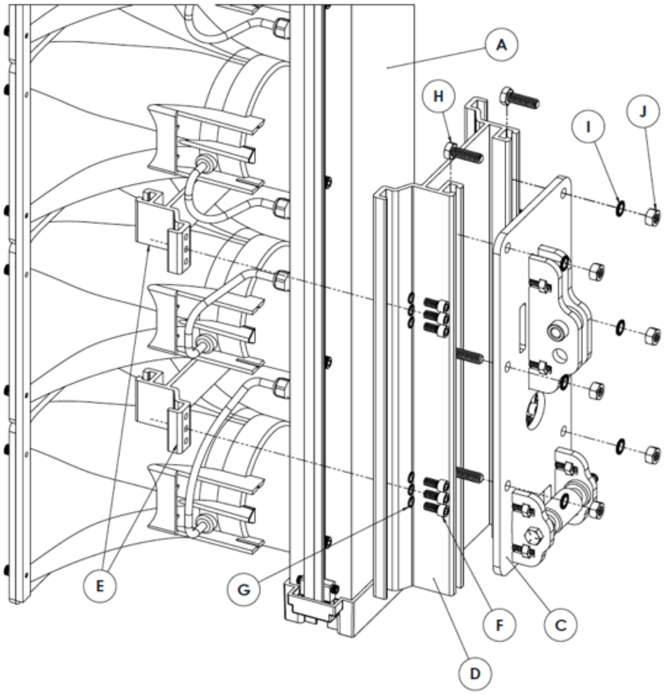


Item	Description	QTY
A	8507 Horn Array	1
B	Mounting Bracket	1
C	Array Bracket	1
D	Adapter Plate	1
E	Adapter Clip	2
F	1/4"-20 x 5/8" Socket Head Bolt	12
G	1/4" Lock Washer	12
H	5/16"-18 x 1" Hex Head Bolt	6
I	5/16" Lock Washer	6
J	6x 5/16" Nut	6
K	Linkage Arm Plate	2
L	Linkage Arm Spacer	1
M	Linkage Arm Bushing	1
N	5/16"-18 Locknut	2
O	5/16" Sleeve Washer	4
P	5/16" Flat Washer	4
Q	5/16"-18 x 2" Hex Head Bolt	1
R	5/16"-18 x 2-3/4" Hex Head Bolt	1
S	Clear Plastic Shroud A	1
T	Clear Plastic Shroud B	1
U	Ethernet Bayonet Plug	1
V	Drain Tube	1
W	6-32 x 1/2" Pan Head Screw	4

Figure 1. Pieces included with the 8507 Horn Array Speaker.

2.3.1 Install the Array Bracket

If no tilt is required, the array bracket may be installed in any position on the array as long as both mounting clips are used. If tilt is required, mount the adapter plate on the bottom of the array as shown below to allow downward tilt from a solid wall by up to 35 degrees. If 30 or 35 degree tilt is required, the array must be mounted onto the adapter plate, as shown in Figure 2. The edge of the array bracket must be distanced at least 1.5 inches from the adapter plate edge to ensure the shroud does not impede and prevent tilting at 30 or 35 degrees. 1. Install the mounting adapter plate (D) to the Horn Array Speaker using the 2 mounting clips (E) and the 12 socket head bolt (F). Torque to 6.5 ft-lbs. 2. Pre-install the 6 hex head bolts (H) loosely with lock washers (I) and nuts (J) into the array bracket (C) to simplify installation. Slide the universal array bracket onto the adapter plate and tighten the bolts into the adapter plate channel to 9.75 ft-lbs.	 30 / 35° 1.50" For 30/35° Tilt Options, edge of the Array Bracket must be distanced at least 1.50" from the Adapter Plate edge. *Figure 2. The array bracket must be mounted at least 1.5 inches from the adapter plate edge.*



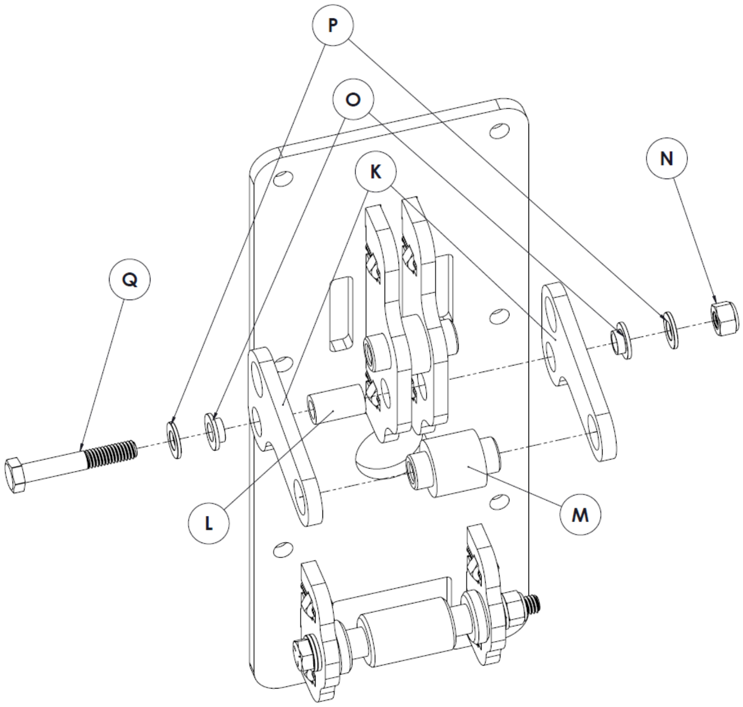
Item	Description	QTY
A	8507 Horn Array	1
C	Array Bracket	1
D	Adapter Plate	1
E	Adapter Clip	2
F	1/4"-20 x 5/8" Socket Head Bolt	12
G	1/4" Lock Washer	12
H	5/16"-18 x 1" Hex Head Bolt	6
I	5/16" Lock Washer	6
J	6x 5/16" Nut	6

Figure 3. Adapter plate and clip assembly.

2.3.2 Assemble Linkage Arm

For tilt angles of 0, 5, 10, and 15 degrees, the linkage arm is not required. For tilt angles of 20, 25, 30, and 35 degrees, the linkage arm is required and must be pre-installed according to the figure below.

1. Slide the linkage spacer (L) between the large hole of the array bracket (C).
2. Slide the two linkage arm plates (K) over the protruding plastic on the array bracket (C), with the linkage bushing (M) wedged in between the plates.
3. Tighten the 5/16”-18 x 2” hex head bolt (Q) through the linkage spacer (L) with the flat washer (P), sleeve washer (O) and 5/16”-18 locknut (N). Torque to 9.75 ft-lbs.



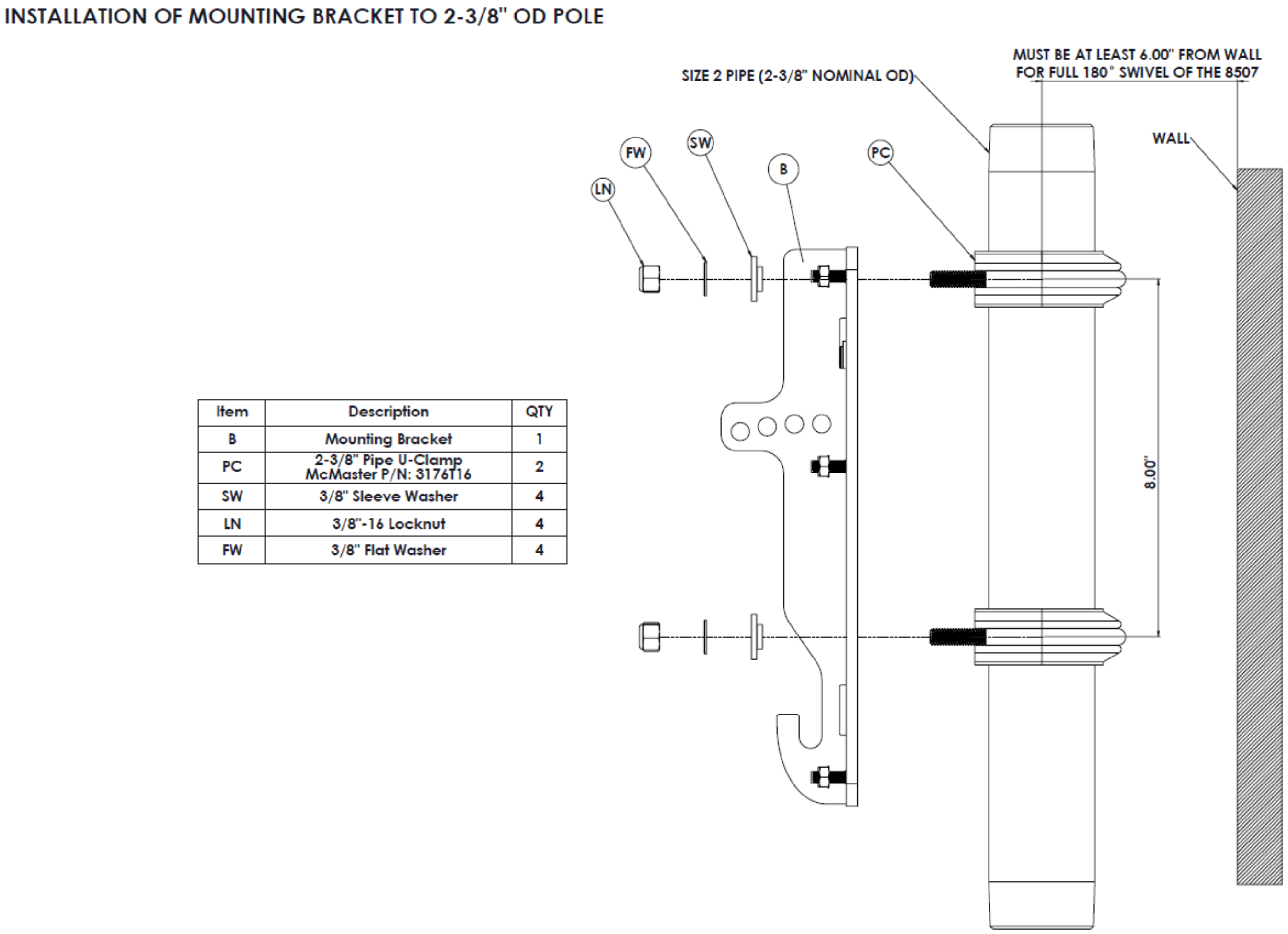
Item	Description	QTY
K	Linkage Arm Plate	2
L	Linkage Arm Spacer	1
M	Linkage Arm Bushing	1
N	5/16"-18 Locknut	1
O	5/16" Sleeve Washer	2
P	5/16" Flat Washer	2
Q	5/16"-18 x 2" Hex Head Bolt	1

Figure 4. Assembly of the linkage arm for 30 or 35-degree tilt.

2.3.3 Install the Mounting Bracket

Pole Mount (2 3/8” OD Pole)

Note that for a full 90-degree rotation, the pole center should be at least 6 inches from any adjacent wall.


INSTALLATION OF MOUNTING BRACKET TO 2-3/8" OD POLE
SIZE 2 PIPE (2-3/8" NOMINAL OD)
MUST BE AT LEAST 6.00" FROM WALL
FOR FULL 180° SWIVEL OF THE 8507
WALL
FW
SW
B
PC
LN
8.00"

Item	Description	QTY
B	Mounting Bracket	1
PC	2-3/8" Pipe U-Clamp McMaster P/N: 3176T16	2
SW	3/8" Sleeve Washer	4
LN	3/8"-16 Locknut	4
FW	3/8" Flat Washer	4

Figure 5. Parts required to mount the 8507 Horn Array Speaker to a pole.

Pole Installation Instructions

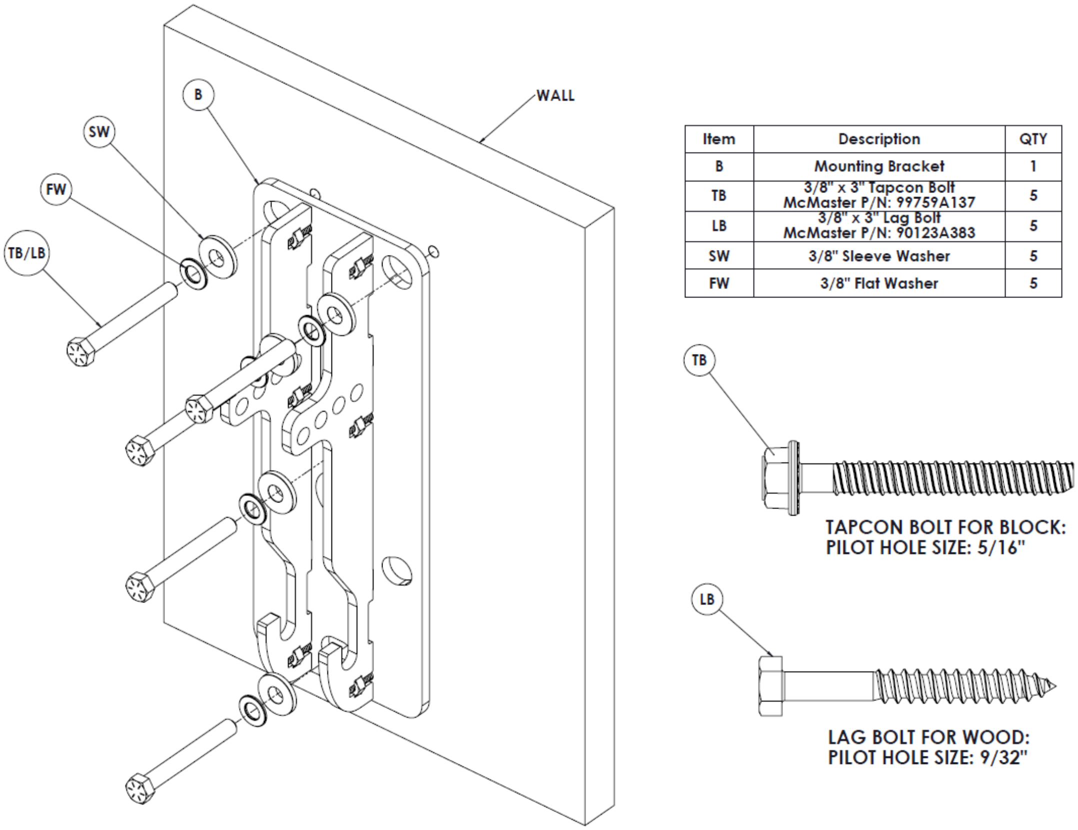
To pole mount the universal mounting bracket, use the pole-mount bracket kit (8507PMB, not included). The kit contains U-clamps (PC), sleeve washers (SW), locknuts (LN), and flat washers (FW).

1. Slide both U-clamps (PC) over the pole, spacing them 8 inches apart.
2. Align the sleeve washers (SW) and flat washers (FW) over the mounting plate and onto the threads of the U-Clamps. The isolating plastic sleeve washers must be used to prevent galvanic corrosion.
3. Tighten the locknuts (LN) to 17.5 ft-lbs. Tightening the locknuts will secure the mounting bracket (B) to the U-clamps and the U-clamps to the pole.

Wall Mount

Note the example kit is meant to mount the Horn Array Speaker to wood, brick, block, or concrete. If the mounting surface is metal other than aluminum and in a wet location, an isolation barrier may be required between the aluminum wall bracket and wall surface to prevent galvanic corrosion.

INSTALLATION OF MOUNTING BRACKET TO WALL



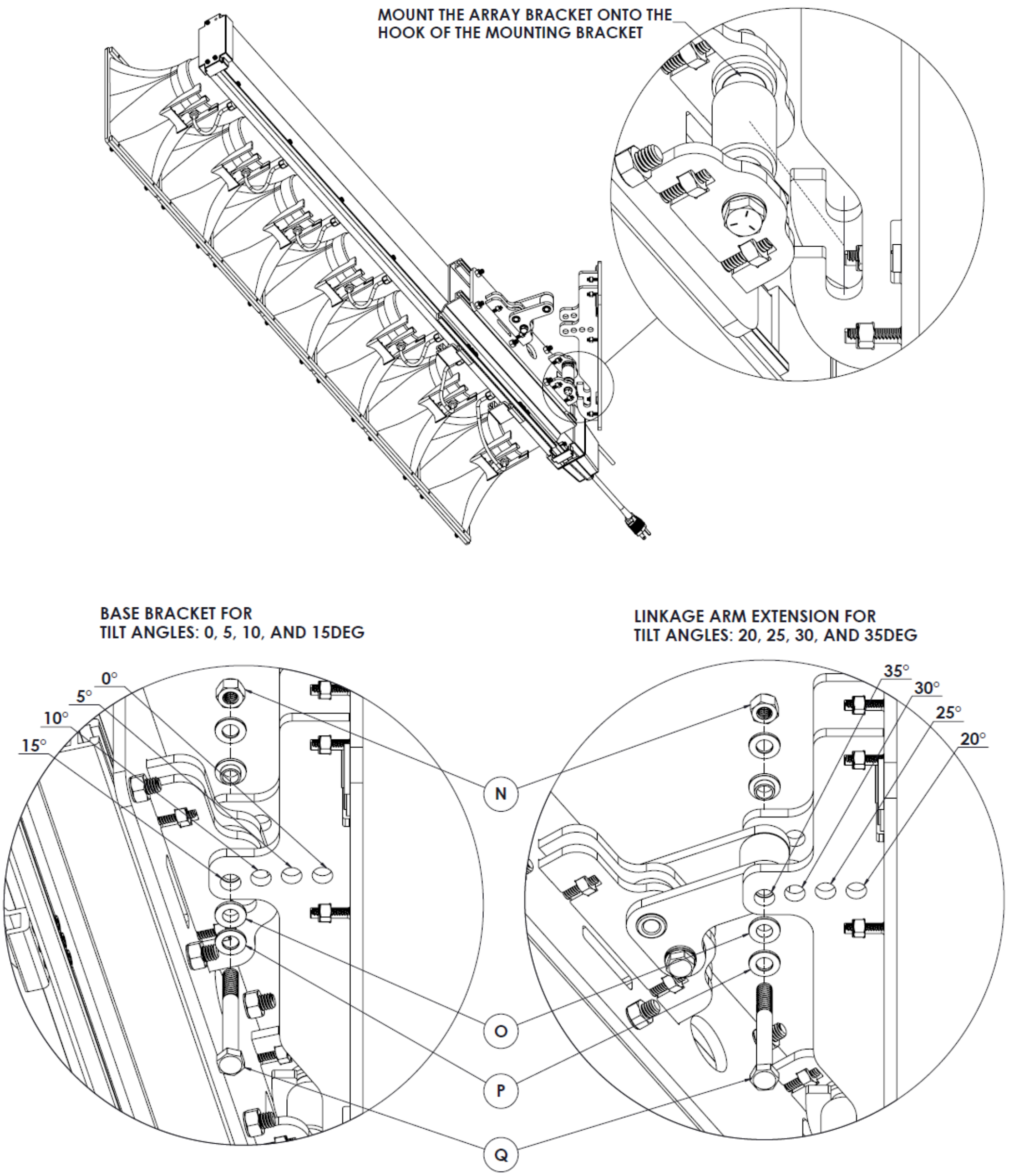
Item	Description	QTY
B	Mounting Bracket	1
TB	3/8" x 3" Tapcon Bolt McMaster P/N: 99759A137	5
LB	3/8" x 3" Lag Bolt McMaster P/N: 90123A383	5
SW	3/8" Sleeve Washer	5
FW	3/8" Flat Washer	5

Figure 6. Parts required to mount the 8507 Horn Array Speaker to a wall.

Wood Installation Instructions	**Concrete, Block, or Brick Installation Instructions**
1. Pre-drill 4 x 9/32” holes into the masonry at least 3” deep. 2. Attach the mounting bracket using (not included) 4 x 3/8” Lag bolt (LB) and isolating flat washers (FW) and sleeve washers (SW).	1. Pre-drill 4 x 5/16” holes into the masonry at least 3” deep. Vacuum any dust or debris from the hole. 2. Attach the mounting bracket using (not included) 4 x 3/8” Tapcon bolt (TB) and isolating flat washers (FW) and sleeve washers (SW).

Install the Horn Array Speaker to the Mounting Bracket

MOUNTING AND FASTENING THE ARRAY


MOUNT THE ARRAY BRACKET ONTO THE
HOOK OF THE MOUNTING BRACKET
BASE BRACKET FOR
TILT ANGLES: 0, 5, 10, AND 15DEG
LINKAGE ARM EXTENSION FOR
TILT ANGLES: 20, 25, 30, AND 35DEG
0°
5°
10°
15°
35°
30°
25°
20°
N
O
P
Q

Item	Description	QTY
N	5/16"-18 Locknut	1
O	5/16" Sleeve Washer	2
P	5/16" Flat Washer	2
Q	5/16"-18 x 2-3/4" Hex Head Bolt	1

Figure 7. How to install the Horn Array Speaker to the mounting bracket.

Use the following instructions to install the array to the mounting bracket:

1. With two people, position the horn array speaker so the black axle of the array bracket slides into the slots of the mounting bracket.
2. Install the hex head bolt (Q) through the corresponding holes in the array and mounting.
3. Install the washer (O) and locknut (N) to the angle adjustment bolt and tighten to 9.75 ft-lbs.

2.4 Wiring

2.4.1 Ethernet Wiring

If the 8507 is installed outdoors or in a wet environment, an outdoor-rated network cable with an LLDPE jacket or equivalent for water and UV protection must be used.

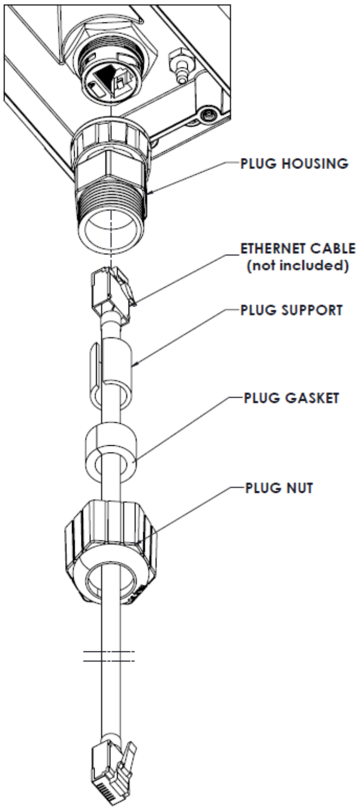
To meet IPX9 ingress protection, the wiring shroud must be installed. To do this, the bayonet plug must be assembled, the drain tube must be installed, and the shroud must be attached.

2.4.2 Bayonet Plug Assembly

For proper bayonet plug assembly, the ethernet cable must *not* have over-moulding or tab cover. To assemble the bayonet plug:

1. Slide the **PLUG NUT** onto the ethernet cable, with the threads facing the connector.
2. Place the **PLUG GASKET** (gray rubber round) over the ethernet cable between the plug nut and the connector.
3. Place the **PLUG SUPPORT** (black plastic tube) over the ethernet cable between the plug gasket and connector.
4. Slide the end of the ethernet cable into the **PLUG HOUSING** so the connector is pushed out the other end with the tab held down. The connector will be approximately half within the housing and half outside.
5. Before tightening the **PLUG NUT** over the **PLUG HOUSING**, ensure the **PLUG SUPPORT** and **PLUG GASKET** sit within the housing spokes. Screw the plug nut onto the housing to hold all pieces in place.
6. Place the end of the ethernet cable with the housing onto the jack. Twist the end of the housing to lock the housing and cable in place.

BAYONET PLUG ASSEMBLY

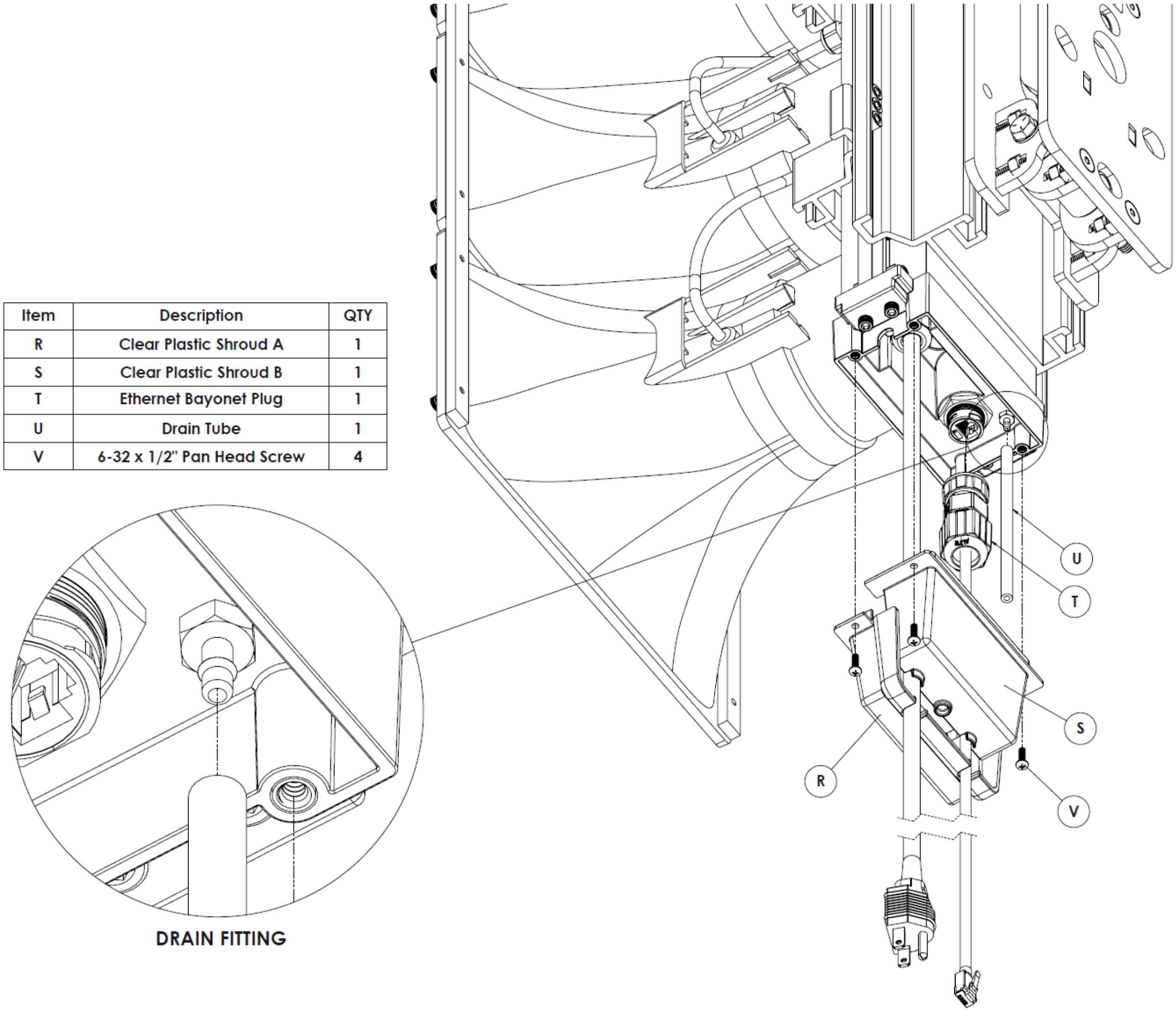


2.4.3 Shroud Assembly

1. Slide the drain tube (U) over the drain fitting. The tube must be clear to drain any moisture that accumulates in the 8507 into the shroud.

2. Attach the shroud (R and S). The smaller hole is for the ethernet cable and the larger hole is for the AC cable. The drain tube should be folded over so the opening is not pressed against the side of the shroud.

3. Use the supplied screws (V) to hold the shroud in place.



Item	Description	QTY
R	Clear Plastic Shroud A	1
S	Clear Plastic Shroud B	1
T	Ethernet Bayonet Plug	1
U	Drain Tube	1
V	6-32 x 1/2" Pan Head Screw	4

2.4.4 AC Electrical Wiring

For quick testing and configuration, the 8507 can operate from PoE power.
For full capability, both AC Mains power 100 V – 240 VAC 50/60Hz and PoE is required. The maximum input current is 4A at 115VAC or 2A at 230VAC. The AC Mains supply must be current limited at 15A by a suitable circuit breaker or fuse.

The 8507 has an outdoor-rated electrical cable terminated with a North America NEMA 5-15P plug. For outdoor or wet environments, the AC plug may be removed and the electrical cable can be wired into a waterproof junction box using a cable gland. If you cut the cable you will find the following three color-coded wires:

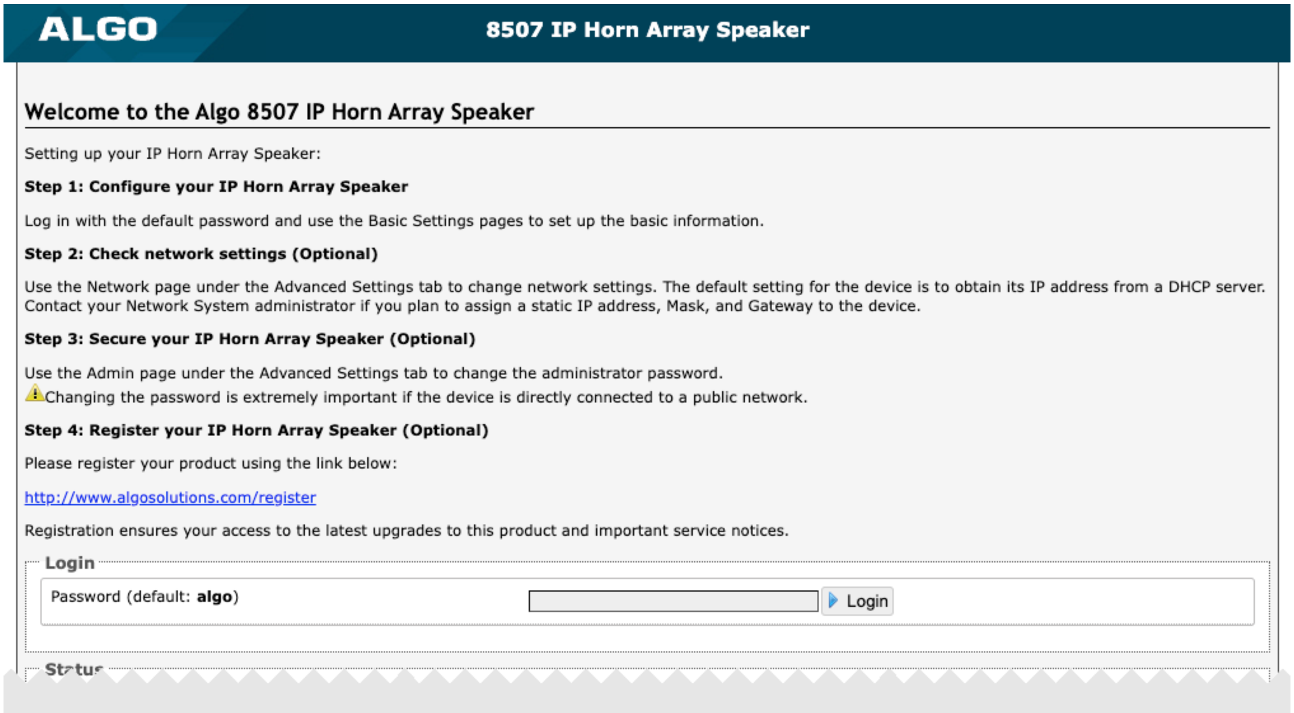
1. Black wire – HOT
2. White wire – NEUTRAL
3. Yellow or green wire – GROUND

2.5 Accessing the Web Interface

After you enter the IP address for your device into your browser, the web interface will appear.

You must log in to view device settings. The default password is *algo*. This password can be changed under **Advanced Settings → Admin** after logging in. Changing the default password is highly recommended if the device is directly connected to a public network.

Important
*The **Save** button must be clicked to apply any changes made in the web interface.*



ALGO 8507 IP Horn Array Speaker

Welcome to the Algo 8507 IP Horn Array Speaker

Setting up your IP Horn Array Speaker:

Step 1: Configure your IP Horn Array Speaker

Log in with the default password and use the Basic Settings pages to set up the basic information.

Step 2: Check network settings (Optional)

Use the Network page under the Advanced Settings tab to change network settings. The default setting for the device is to obtain its IP address from a DHCP server. Contact your Network System administrator if you plan to assign a static IP address, Mask, and Gateway to the device.

Step 3: Secure your IP Horn Array Speaker (Optional)

Use the Admin page under the Advanced Settings tab to change the administrator password.
⚠Changing the password is extremely important if the device is directly connected to a public network.

Step 4: Register your IP Horn Array Speaker (Optional)

Please register your product using the link below:

http://www.algosolutions.com/register

Registration ensures your access to the latest upgrades to this product and important service notices.

Login

Password (default: **algo**)

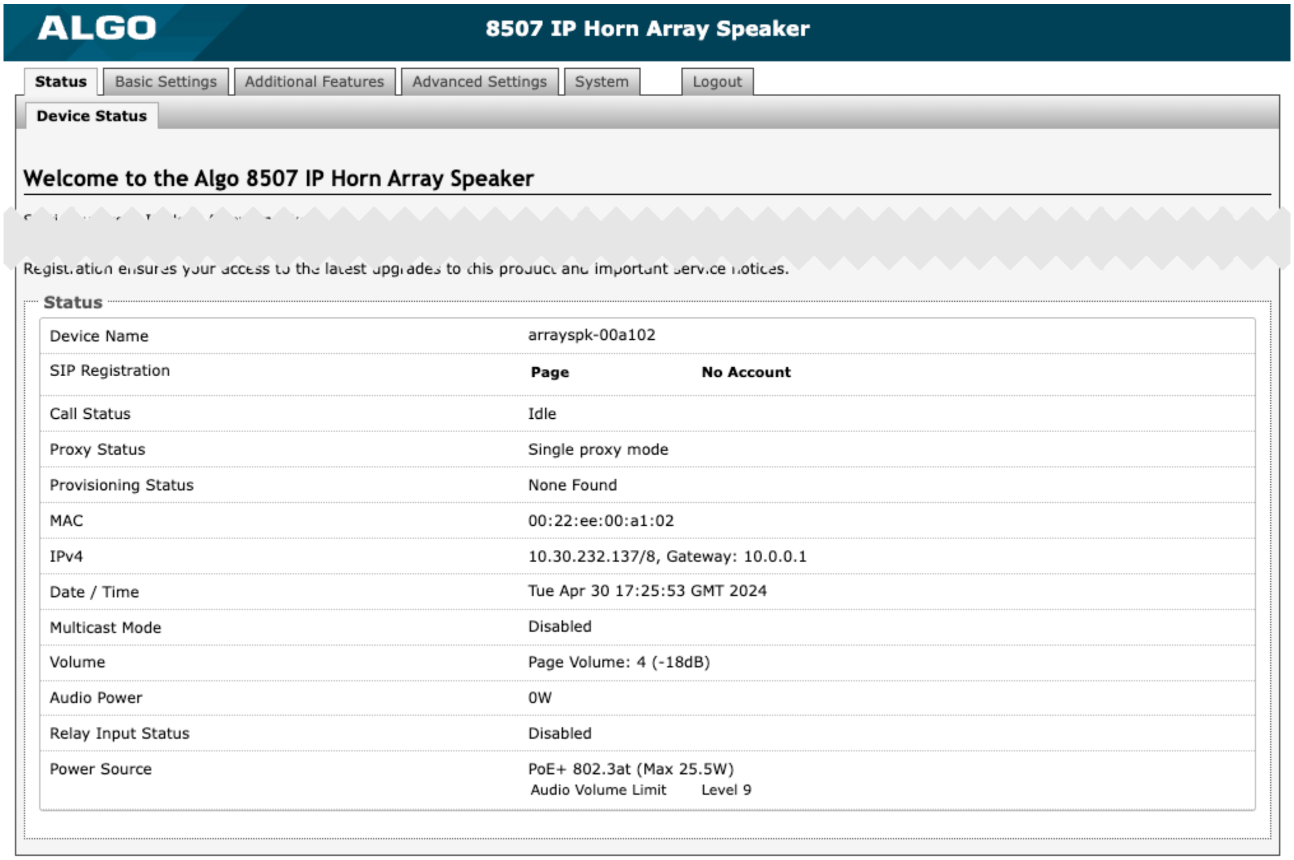
Figure 7: Welcome page of the device's web interface.

2.5.1 Check Device Status

By default, the **Status** page is available with and without a login. The Status page can be made exclusive to logged-in users via **Advanced Settings → Admin → General → Show Status Section on Status Page when Logged Out**.

The **Status** page contains information such as:

- Device Name
- SIP Registration
- Call Status
- Proxy Status
- Provisioning Status
- MAC
- IP Address
- Date/Time
- Multicast Mode
- Volume
- InformaCast License
- ADMP Cloud Monitoring



Welcome to the Algo 8507 IP Horn Array Speaker

Registration ensures your access to the latest upgrades to this product and important service notices.

Status

Device Name	arrayspk-00a102
SIP Registration	**Page** **No Account**
Call Status	Idle
Proxy Status	Single proxy mode
Provisioning Status	None Found
MAC	00:22:ee:00:a1:02
IPv4	10.30.232.137/8, Gateway: 10.0.0.1
Date / Time	Tue Apr 30 17:25:53 GMT 2024
Multicast Mode	Disabled
Volume	Page Volume: 4 (-18dB)
Audio Power	0W
Relay Input Status	Disabled
Power Source	PoE+ 802.3at (Max 25.5W) Audio Volume Limit Level 9

Figure 8: Device status tab on the web interface.

2.6 Register Your Product

You may register your product at https://www.algosolutions.com/product-registration/ to ensure access to the latest upgrades for your device and to receive important service notices.

2.7 Reset

A large, round button located between the AC power cable and ethernet jack at the bottom of the device can only be used to reset the 8507 IP Horn Array Speaker at the time of power-up. To return all the settings in the 8507 to the factory default, reboot or power cycle the 8507. Wait until the button backlight flashes, then press and hold the reset button until the SIP LED begins a double flash pattern. Release the reset button and allow the unit to complete its boot process.

⚠ ***Important***
Do not press the reset button until the SIP LED begins flashing.
A reset will set all configuration options to factory default, including the login password.

Once booting is complete, press the reset button to play the IP address.

2.8 Security

Algo devices use TLS for provisioning and SIP signaling to mitigate cyberattacks by those trying to intercept, replicate, or alter Algo products. Algo devices also come pre-loaded with certificates from a list of trusted certificate authorities (CA) to ensure secure communication with reputable sources. Pre-installed trusted certificates are not visible to users and are separate from those in the ‘certs’ folder.

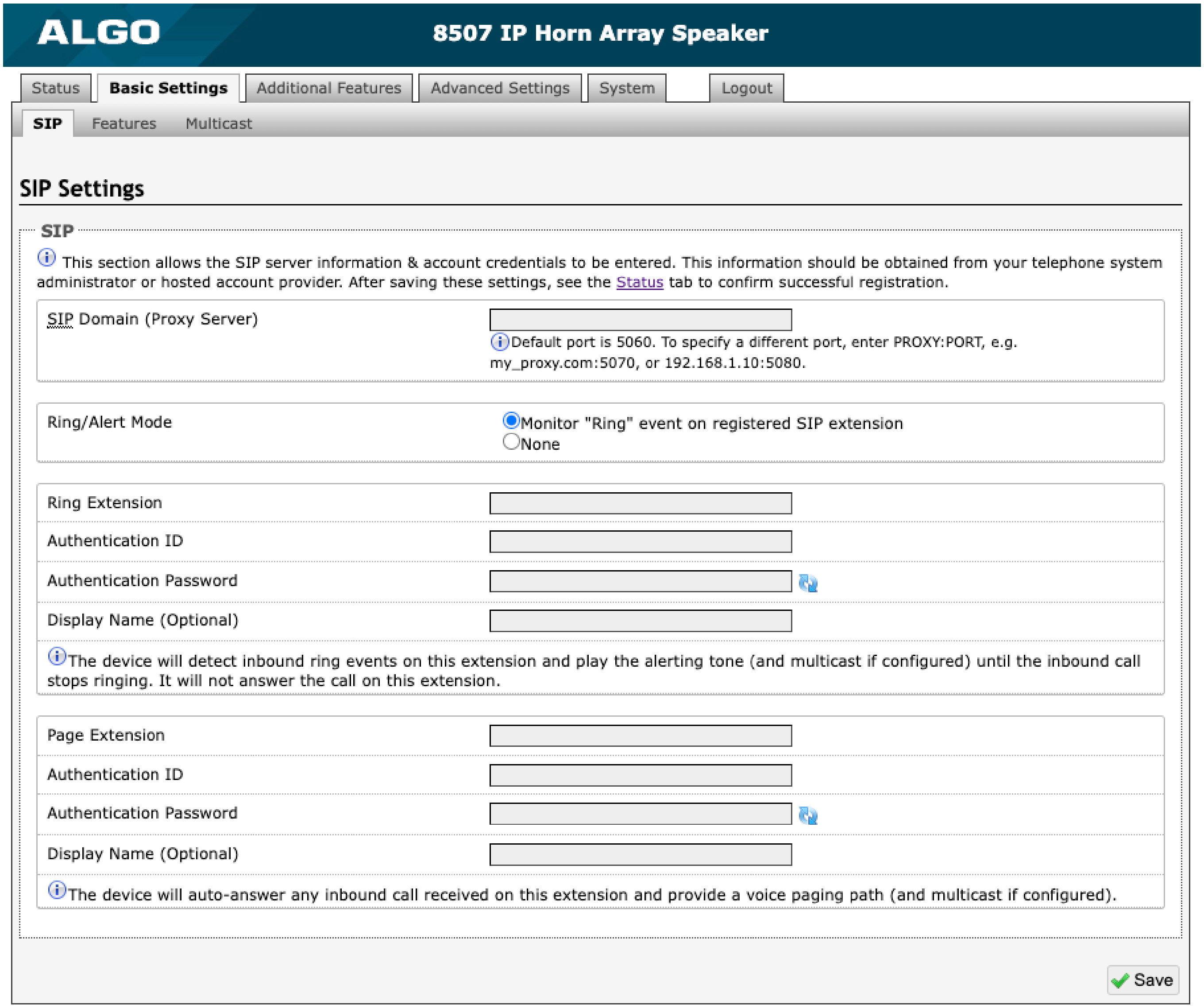
For further details, see Securing Algo Endpoints: TLS and Manual Authentication.

3 SIP CONFIGURATION

SIP signaling is the underlying protocol for transmitting SIP messages between different entities in a network. SIP signaling establishes the call but does not contain the audio.

A SIP endpoint license associated with a UCaaS platform may be required to register the 8507. One license will be required per extension registered. If one device has multiple extensions registered, each registered extension will require a license. On a hosted or cloud platform, the required endpoint extension or seat may be treated the same as any other extension on the system and incur a monthly cost or similar fee.

3.1 Basic Settings



SIP Settings

SIP

This section allows the SIP server information & account credentials to be entered. This information should be obtained from your telephone system administrator or hosted account provider. After saving these settings, see the Status tab to confirm successful registration.

SIP Domain (Proxy Server)

Default port is 5060. To specify a different port, enter PROXY:PORT, e.g. my_proxy.com:5070, or 192.168.1.10:5080.

Ring/Alert Mode ● Monitor "Ring" event on registered SIP extension ○ None

Ring Extension

Authentication ID

Authentication Password

Display Name (Optional)

The device will detect inbound ring events on this extension and play the alerting tone (and multicast if configured) until the inbound call stops ringing. It will not answer the call on this extension.

Page Extension

Authentication ID

Authentication Password

Display Name (Optional)

The device will auto-answer any inbound call received on this extension and provide a voice paging path (and multicast if configured).

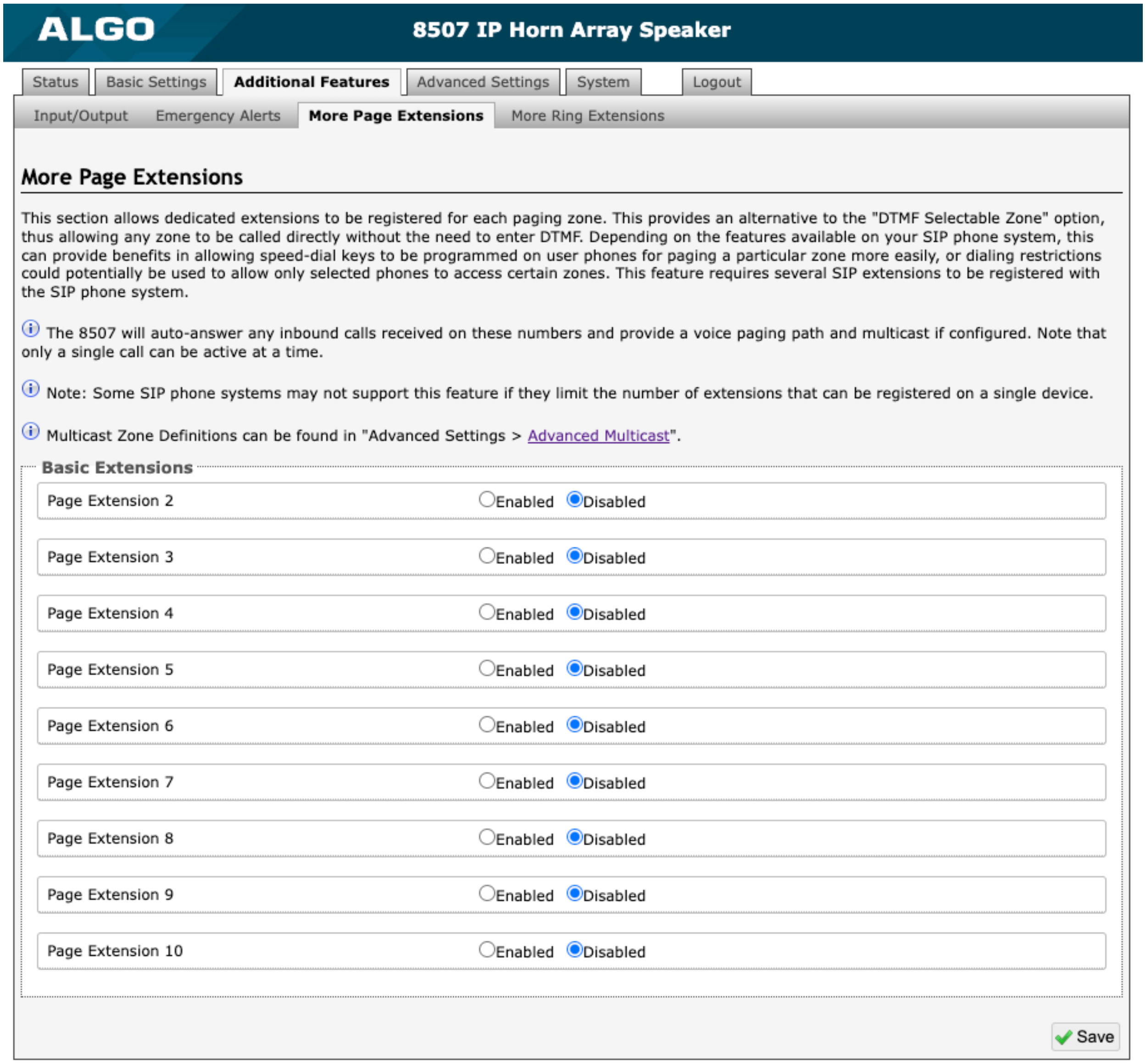
Figure 9: Configure basic SIP settings in the web interface.

Use these SIP settings to enter SIP server information and account credentials. You can ask your system administrator or hosted account provider for more details. After entering the information and saving the settings, check the **Status** tab to confirm the successful registration.

SIP	
SIP Domain (Proxy Server)	The SIP Server's IP address (e.g., 192.168.1.111) or domain name (e.g., myserver.com).
Ring/Alert Mode	Ring extensions do not answer incoming calls but play a customizable, pre-recorded announcement, such as a loud ringer (night bell). Announcements are customizable and can be pre-recorded. Use this setting to add a second SIP extension for a Ring event. If **Monitor "Ring" event on registered SIP extension** is selected, you will see additional settings for Ring extension parameters. **None** is set by default. If set, the device will detect inbound ring events on this extension and play the alerting tone (and multicast if configured) until the inbound call stops ringing. The 8507 will not answer the call on this extension. The 8507 can be a member of a hunt group or ring group to ring in conjunction with a telephone. You may change the alert tone via **Basic Settings → Features**.
Ring Extension	Enter the SIP extension for the ring parameter of the 8507. The device will detect inbound ring events on this extension and play the alerting tone (and multicast if configured) until the inbound call stops ringing. It will not answer the call on this extension.
Page Extension	Page extensions auto-answer and open a voice path, enabling live announcements. Enter the SIP page extension for the 8507 so the device will auto-answer any inbound call received on this extension and provide a voice paging path (and multicast if configured).
Authentication ID	The Authentication ID is a name that represents the page extension. It is also referred to as 'Username' for some SIP servers. This may be the same as the Ring or Page extension in some cases.
Authentication Password	This is the SIP password for the registered SIP account. Up to eight (8) characters can be used. The password can be used to authenticate SIP users. Contact your System Administrator for the password to obtain access.

Display Name (Optional)	Enter the name you want displayed when an SIP call is made. For the display name to be shown, the PBX and phone(s) must be configured to display this message as the Caller ID.

3.2 More Page Extensions



More Page Extensions

This section allows dedicated extensions to be registered for each paging zone. This provides an alternative to the "DTMF Selectable Zone" option, thus allowing any zone to be called directly without the need to enter DTMF. Depending on the features available on your SIP phone system, this can provide benefits in allowing speed-dial keys to be programmed on user phones for paging a particular zone more easily, or dialing restrictions could potentially be used to allow only selected phones to access certain zones. This feature requires several SIP extensions to be registered with the SIP phone system.

ⓘ The 8507 will auto-answer any inbound calls received on these numbers and provide a voice paging path and multicast if configured. Note that only a single call can be active at a time.

ⓘ Note: Some SIP phone systems may not support this feature if they limit the number of extensions that can be registered on a single device.

ⓘ Multicast Zone Definitions can be found in "Advanced Settings > Advanced Multicast".

Basic Extensions

Page Extension 2	○Enabled ●Disabled
Page Extension 3	○Enabled ●Disabled
Page Extension 4	○Enabled ●Disabled
Page Extension 5	○Enabled ●Disabled
Page Extension 6	○Enabled ●Disabled
Page Extension 7	○Enabled ●Disabled
Page Extension 8	○Enabled ●Disabled
Page Extension 9	○Enabled ●Disabled
Page Extension 10	○Enabled ●Disabled

Figure 9: Accessing more page extensions on the device interface.

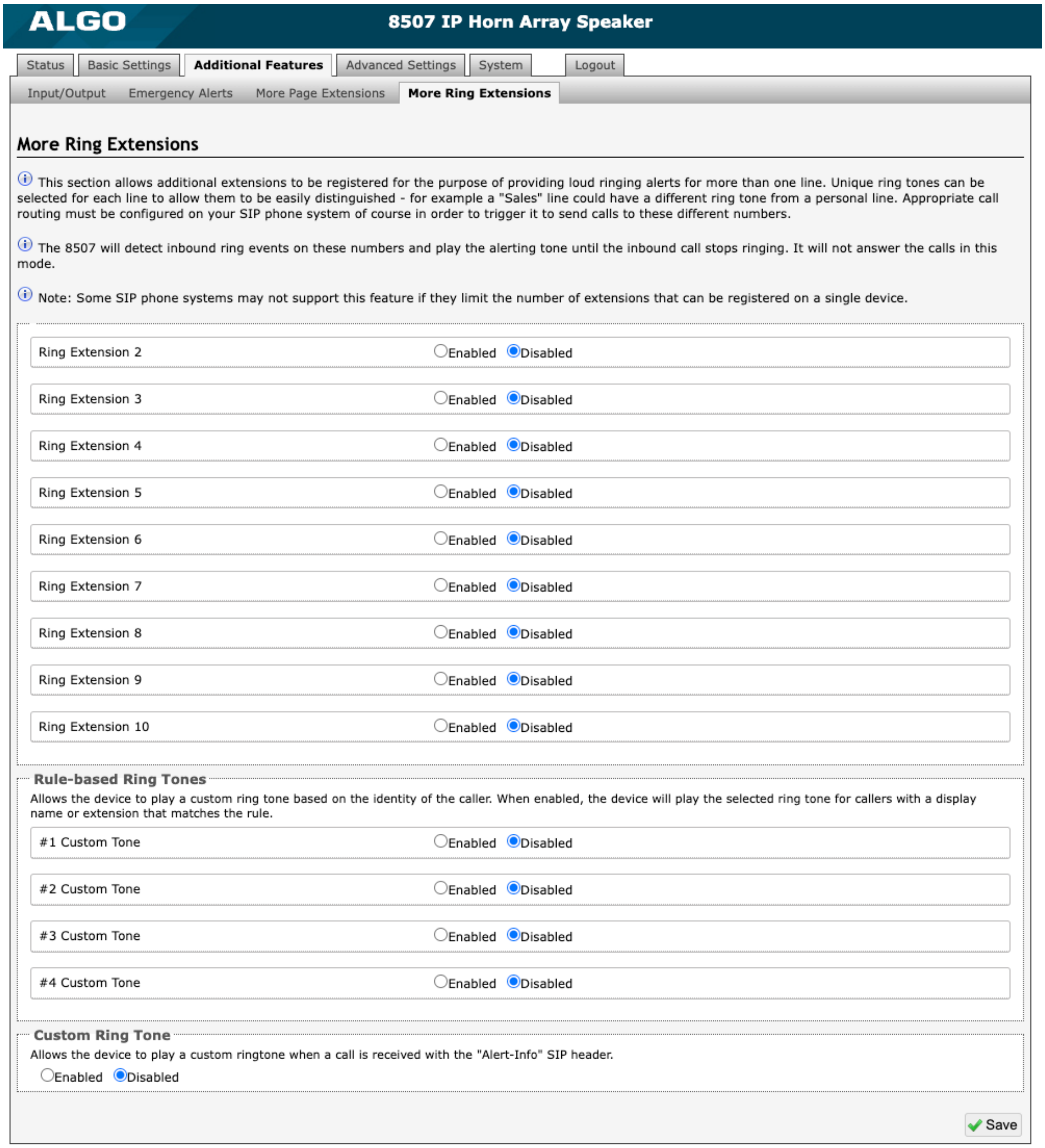
Additional SIP extensions can be registered for each multicast zone. This enables you to dial a zone directly without entering DTMF Codes; however, this may require additional SIP licenses, depending on the SIP provider. Some SIP telephone systems may not support this capability altogether if there is a limit on the number of extensions registered on a single device.

To configure additional page extensions (up to 50):

1. Select **Enable** beside the extension of interest.
2. Enter the **Extension**, **Authentication ID**, and **Authentication Password**. You may enter a Display Name if you'd like.

The 8507 will auto-answer any inbound calls received on these numbers and provide a voice paging path and multicast if configured. Only a single call can be active at a time.

3.3 More Ring Extensions



More Ring Extensions

ⓘ This section allows additional extensions to be registered for the purpose of providing loud ringing alerts for more than one line. Unique ring tones can be selected for each line to allow them to be easily distinguished - for example a "Sales" line could have a different ring tone from a personal line. Appropriate call routing must be configured on your SIP phone system of course in order to trigger it to send calls to these different numbers.

ⓘ The 8507 will detect inbound ring events on these numbers and play the alerting tone until the inbound call stops ringing. It will not answer the calls in this mode.

ⓘ Note: Some SIP phone systems may not support this feature if they limit the number of extensions that can be registered on a single device.

Ring Extension 2 ○Enabled ●Disabled
Ring Extension 3 ○Enabled ●Disabled
Ring Extension 4 ○Enabled ●Disabled
Ring Extension 5 ○Enabled ●Disabled
Ring Extension 6 ○Enabled ●Disabled
Ring Extension 7 ○Enabled ●Disabled
Ring Extension 8 ○Enabled ●Disabled
Ring Extension 9 ○Enabled ●Disabled
Ring Extension 10 ○Enabled ●Disabled

Rule-based Ring Tones

Allows the device to play a custom ring tone based on the identity of the caller. When enabled, the device will play the selected ring tone for callers with a display name or extension that matches the rule.

#1 Custom Tone ○Enabled ●Disabled
#2 Custom Tone ○Enabled ●Disabled
#3 Custom Tone ○Enabled ●Disabled
#4 Custom Tone ○Enabled ●Disabled

Custom Ring Tone

Allows the device to play a custom ringtone when a call is received with the "Alert-Info" SIP header.

○Enabled ●Disabled

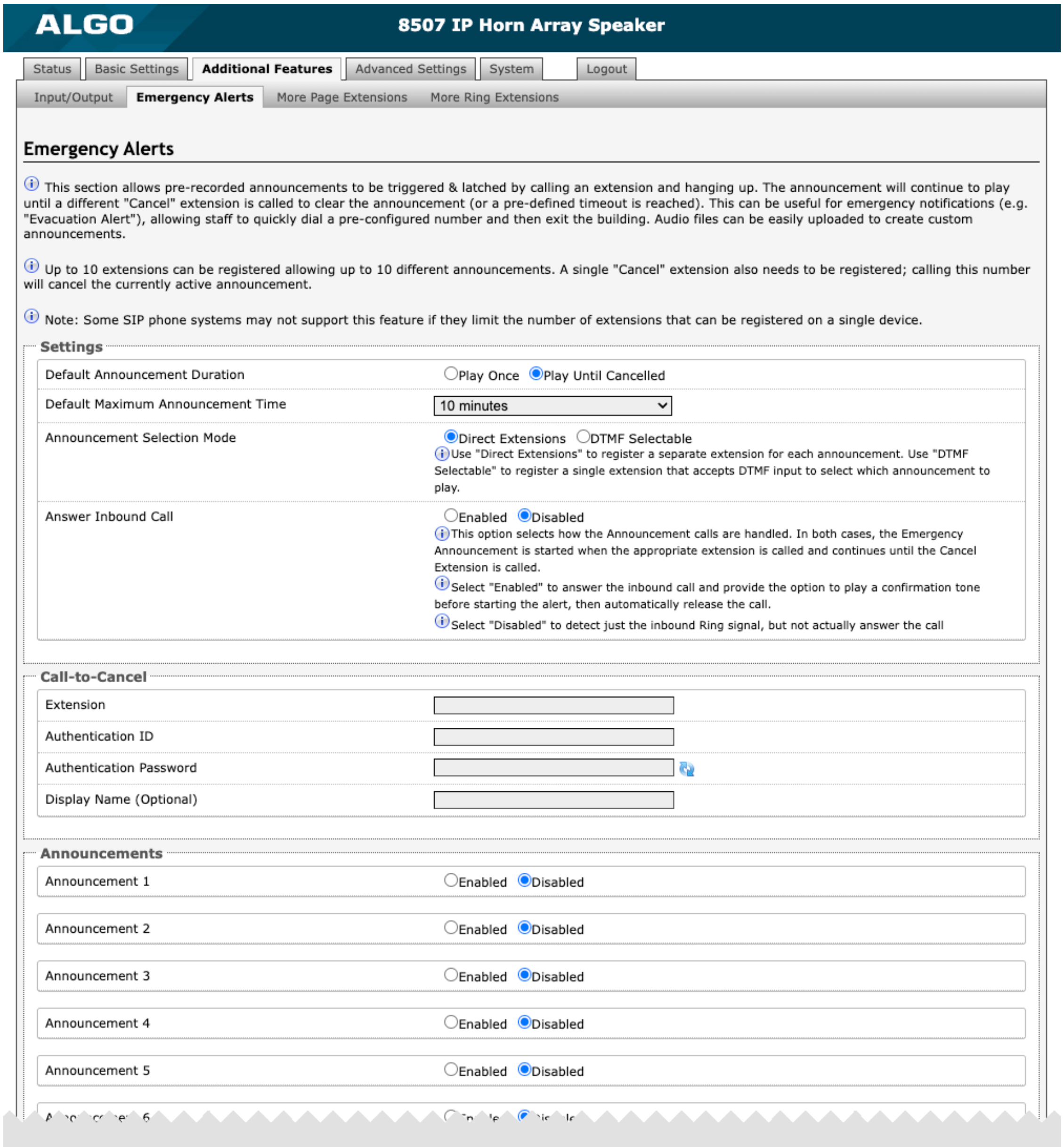
Figure 10: Access more ring extensions on the web interface.

Up to 10 SIP Ring extensions can be registered. To configure additional ring extensions, select **Enabled** beside an extension and enter the Extension, Authentication ID, and Authentication Password. If desired, a unique ringtone and multicast zone can be assigned to each extension.

Set a rule-based ringtone so the device plays a custom ringtone based on the caller's identity. When enabled, the device will play the selected ringtone for callers with a display name or extension that matches the rule.

Enable a custom ring to allow the device to play a custom ringtone when receiving a call with the "Alert-Info" SIP header.

3.4 Emergency Alerts


ALGO
8507 IP Horn Array Speaker
Status | Basic Settings | Additional Features | Advanced Settings | System | Logout
Input/Output | Emergency Alerts | More Page Extensions | More Ring Extensions

Emergency Alerts

ⓘ This section allows pre-recorded announcements to be triggered & latched by calling an extension and hanging up. The announcement will continue to play until a different "Cancel" extension is called to clear the announcement (or a pre-defined timeout is reached). This can be useful for emergency notifications (e.g. "Evacuation Alert"), allowing staff to quickly dial a pre-configured number and then exit the building. Audio files can be easily uploaded to create custom announcements.

ⓘ Up to 10 extensions can be registered allowing up to 10 different announcements. A single "Cancel" extension also needs to be registered; calling this number will cancel the currently active announcement.

ⓘ Note: Some SIP phone systems may not support this feature if they limit the number of extensions that can be registered on a single device.

Settings

Default Announcement Duration	○Play Once ●Play Until Cancelled
Default Maximum Announcement Time	10 minutes
Announcement Selection Mode	●Direct Extensions ○DTMF Selectable ⓘUse "Direct Extensions" to register a separate extension for each announcement. Use "DTMF Selectable" to register a single extension that accepts DTMF input to select which announcement to play.
Answer Inbound Call	○Enabled ●Disabled ⓘThis option selects how the Announcement calls are handled. In both cases, the Emergency Announcement is started when the appropriate extension is called and continues until the Cancel Extension is called. ⓘSelect "Enabled" to answer the inbound call and provide the option to play a confirmation tone before starting the alert, then automatically release the call. ⓘSelect "Disabled" to detect just the inbound Ring signal, but not actually answer the call

Call-to-Cancel

Extension	
Authentication ID	
Authentication Password	
Display Name (Optional)	

Announcements

Announcement 1	○Enabled ●Disabled
Announcement 2	○Enabled ●Disabled
Announcement 3	○Enabled ●Disabled
Announcement 4	○Enabled ●Disabled
Announcement 5	○Enabled ●Disabled
Announcement 6	○Enabled ●Disabled

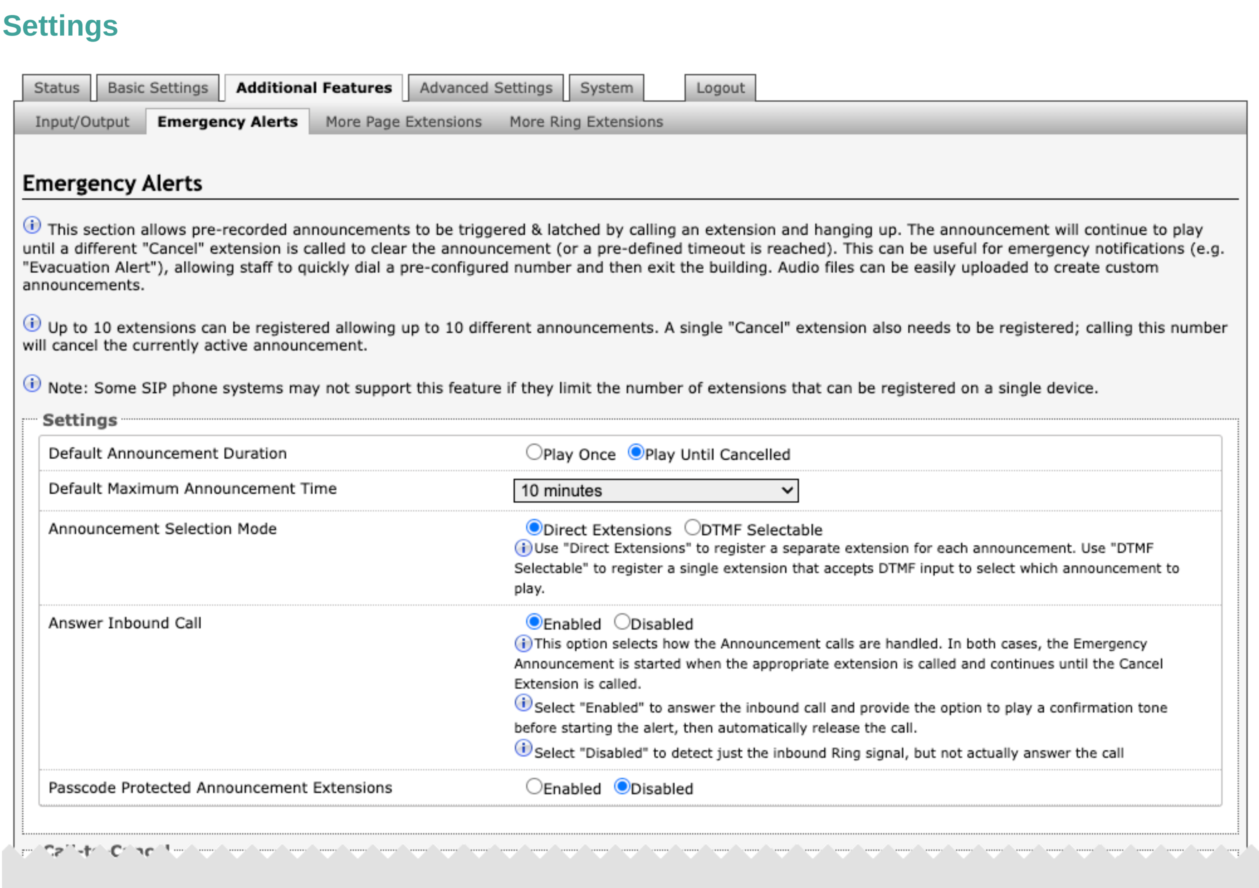
Figure 11: Configure emergency alerts in the web interface.

The 8507 can be used for emergency (e.g., lockdown, evacuation, reverse evacuation), safety (e.g., medical, workplace accident), and security events (e.g., OSHA or similar workplace regulations) alerting.

Emergency alerts notify others of an emergency quickly and efficiently. Users can dial a pre-configured extension number to trigger and latch an emergency alert or announcement. The announcement will continue to play on a loop until a different "Call-to-Cancel" extension is called to clear the announcement or a pre-defined timeout is reached.

Up to 10 extensions can be registered allowing up to 10 different announcements. A single "Call-to-Cancel" extension also needs to be registered. Calling this number will cancel an active announcement.

Note: Some SIP telephone systems may not support this feature if they limit the number of extensions that can be registered on a single device.



Emergency Alerts

ⓘ This section allows pre-recorded announcements to be triggered & latched by calling an extension and hanging up. The announcement will continue to play until a different "Cancel" extension is called to clear the announcement (or a pre-defined timeout is reached). This can be useful for emergency notifications (e.g. "Evacuation Alert"), allowing staff to quickly dial a pre-configured number and then exit the building. Audio files can be easily uploaded to create custom announcements.

ⓘ Up to 10 extensions can be registered allowing up to 10 different announcements. A single "Cancel" extension also needs to be registered; calling this number will cancel the currently active announcement.

ⓘ Note: Some SIP phone systems may not support this feature if they limit the number of extensions that can be registered on a single device.

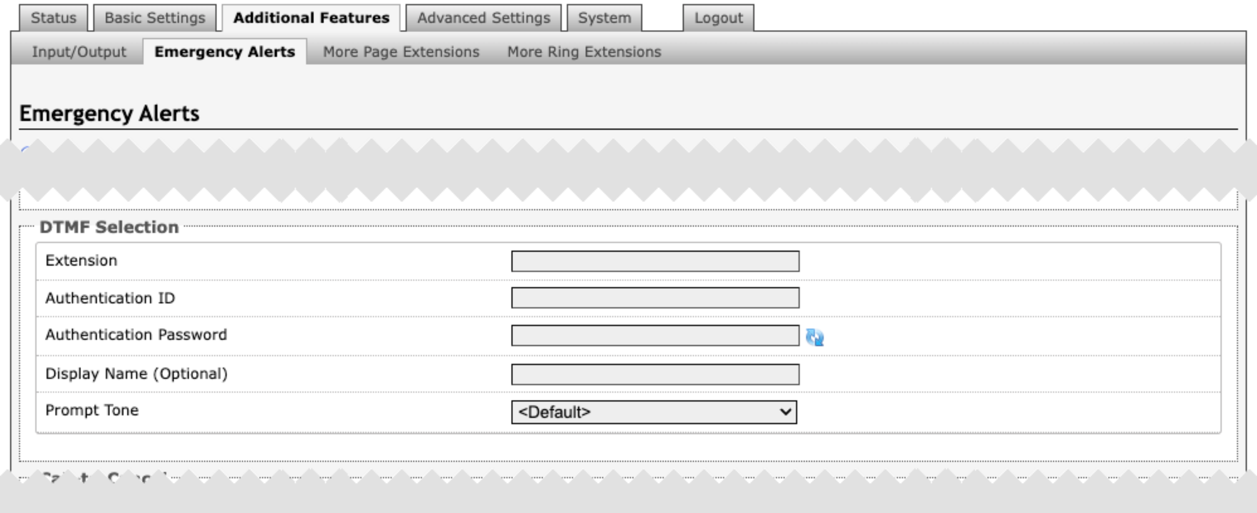
Settings

Default Announcement Duration	○Play Once ●Play Until Cancelled
Default Maximum Announcement Time	10 minutes
Announcement Selection Mode	●Direct Extensions ○DTMF Selectable ⓘUse "Direct Extensions" to register a separate extension for each announcement. Use "DTMF Selectable" to register a single extension that accepts DTMF input to select which announcement to play.
Answer Inbound Call	●Enabled ○Disabled ⓘThis option selects how the Announcement calls are handled. In both cases, the Emergency Announcement is started when the appropriate extension is called and continues until the Cancel Extension is called. ⓘSelect "Enabled" to answer the inbound call and provide the option to play a confirmation tone before starting the alert, then automatically release the call. ⓘSelect "Disabled" to detect just the inbound Ring signal, but not actually answer the call
Passcode Protected Announcement Extensions	○Enabled ●Disabled

Default Announcement Duration	An announcement can be played once or continuously until canceled. Select **Play Once** to play a single cycle of the chosen tone file. If **Play Until Cancelled** is selected, the announcement will continue to play until the "Call-to-Cancel" extension is called to clear the announcement or a defined timeout is reached.

Default Maximum Announcement Time	Select the maximum time an announcement can be played.
Announcement Selection Mode	Select **Direct Extensions** to register a separate extension for each announcement. Select **DTMF Selectable** to register a single extension that accepts DTMF input to select which announcement to play.
Answer Inbound Call	This setting indicates how Announcement calls are handled. In both cases, the Emergency Announcement is started when the appropriate extension is called and continues until the "Call-to-Cancel" extension is called. Select **Enabled** to answer the inbound call and provide the option to play a **Confirmation Tone** before starting the alert, then automatically release the call or request a passcode before playing the announcement. Select **Disabled** to detect the inbound Ring signal but not answer the call. Select **Disabled** to only detect the inbound Ring signal but not answer the call. In both instances, the announcement will play until the time limit is reached or the "Call-to-Cancel" extension is called. Enabling **Answer Inbound Call** can be useful when the caller cannot hear the announcement from their location. However, if the call might go to a group or multiple extension(s) (including this device), the auto-answer may intercept that call and prevent it from ringing on other devices.
Passcode Protected Announcement Extensions	Select **Enabled** to require the caller to enter a passcode after dialing an announcement or "Call-to-Cancel" extension. Setting a passcode helps prevent unintentional announcements.
Announcement Passcode	Enter a passcode that a caller must enter to play or cancel an announcement. When prompted, the caller must enter the passcode followed by the # sign before the announcement will be played or canceled. The passcode prompt will be played before any other action. If the passcode is not correctly entered within 15 seconds, the call will end.
Passcode Prompt Tone	Select a tone to play when the passcode is ready to be entered.

DTMF Selection



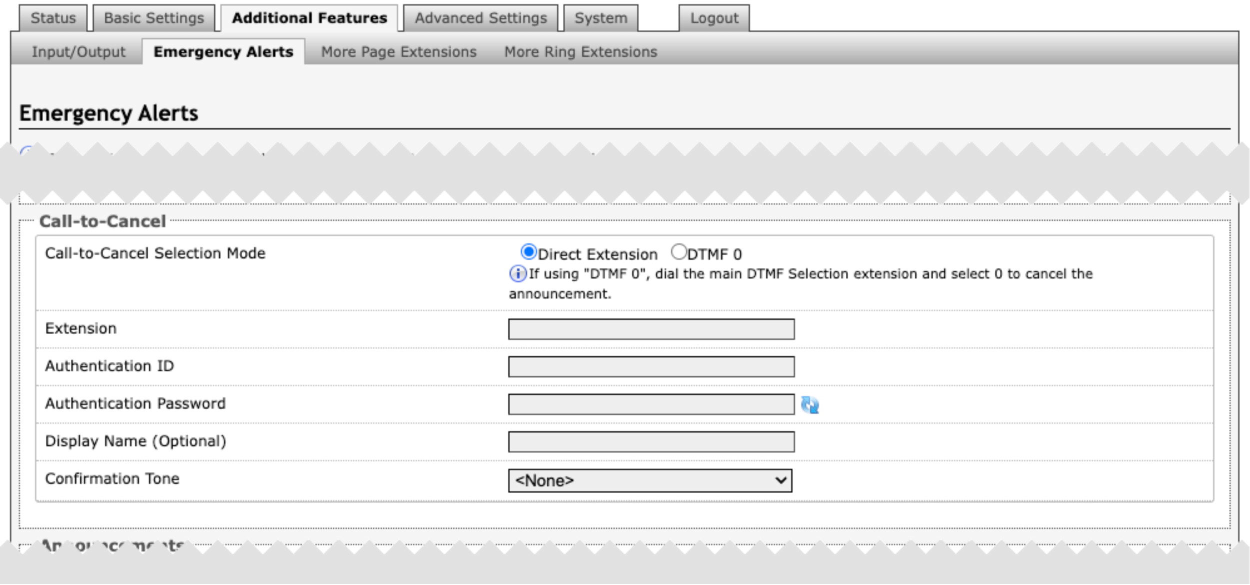
Emergency Alerts

DTMF Selection

Extension	
Authentication ID	
Authentication Password	
Display Name (Optional)	
Prompt Tone	<Default>

Extension	Enter the SIP extension for the DTMF Selection parameter.
Authentication ID	Enter the Authentication ID. It may also be called Username for some SIP servers or may be the same as the extension.
Authentication Password	Enter the SIP password provided by the system administrator for the SIP account.
Display Name (Optional)	Enter a 'Display Name' that will be sent when the SIP call is made. The PBX and phone(s) must be configured to display this message as the Caller ID.
Prompt Tone	Select a tone to play when the passcode is ready to be entered.

Call-to-Cancel



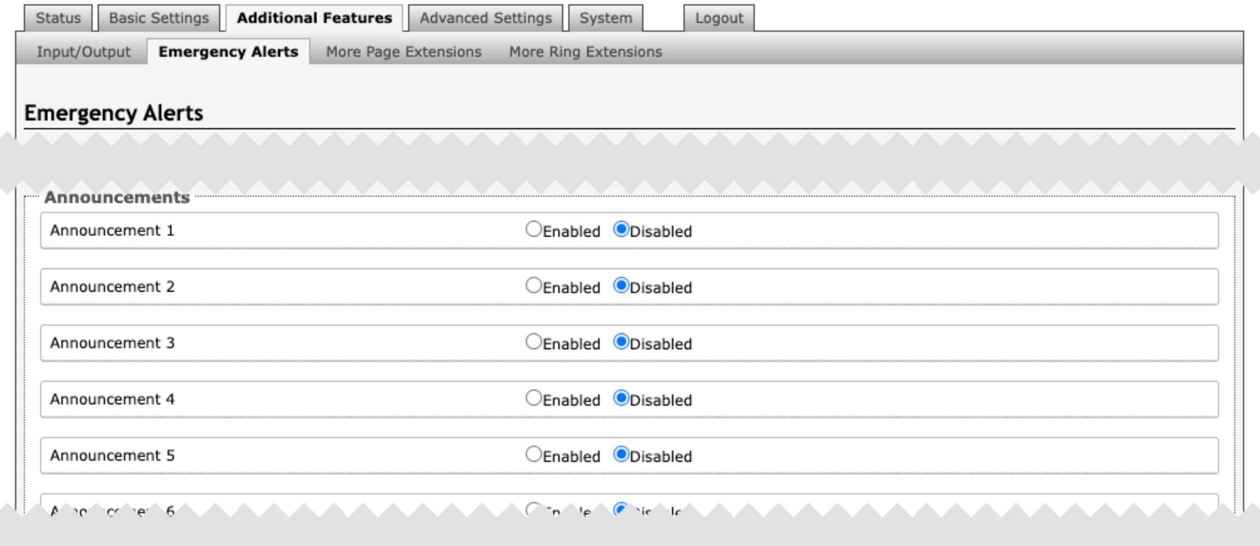
Emergency Alerts

Call-to-Cancel

Call-to-Cancel Selection Mode	● Direct Extension ○ DTMF 0 ⓘ If using "DTMF 0", dial the main DTMF Selection extension and select 0 to cancel the announcement.
Extension	
Authentication ID	
Authentication Password	
Display Name (Optional)	
Confirmation Tone	<None>

Call-to-Cancel Selection Mode	If using “DTMF 0”, the user should dial the main DTMF Selection extension and select ‘0’ to cancel the announcement.
Extension	Enter the SIP extension for the Call-to-Cancel Selection parameter.
Authentication ID	Enter the Authentication ID provided by the System Administrator. It may also be called Username for some SIP servers or may be the same as the extension.
Display Name (Optional)	Enter a ‘Display Name’ that will be sent when the SIP call is made. The PBX and phone(s) must be configured to display this message as the Caller ID.
Confirmation Tone	Select a tone to play to confirm that an alert has been canceled.

Announcements



Emergency Alerts

Announcements

Announcement 1 ○Enabled ●Disabled

Announcement 2 ○Enabled ●Disabled

Announcement 3 ○Enabled ●Disabled

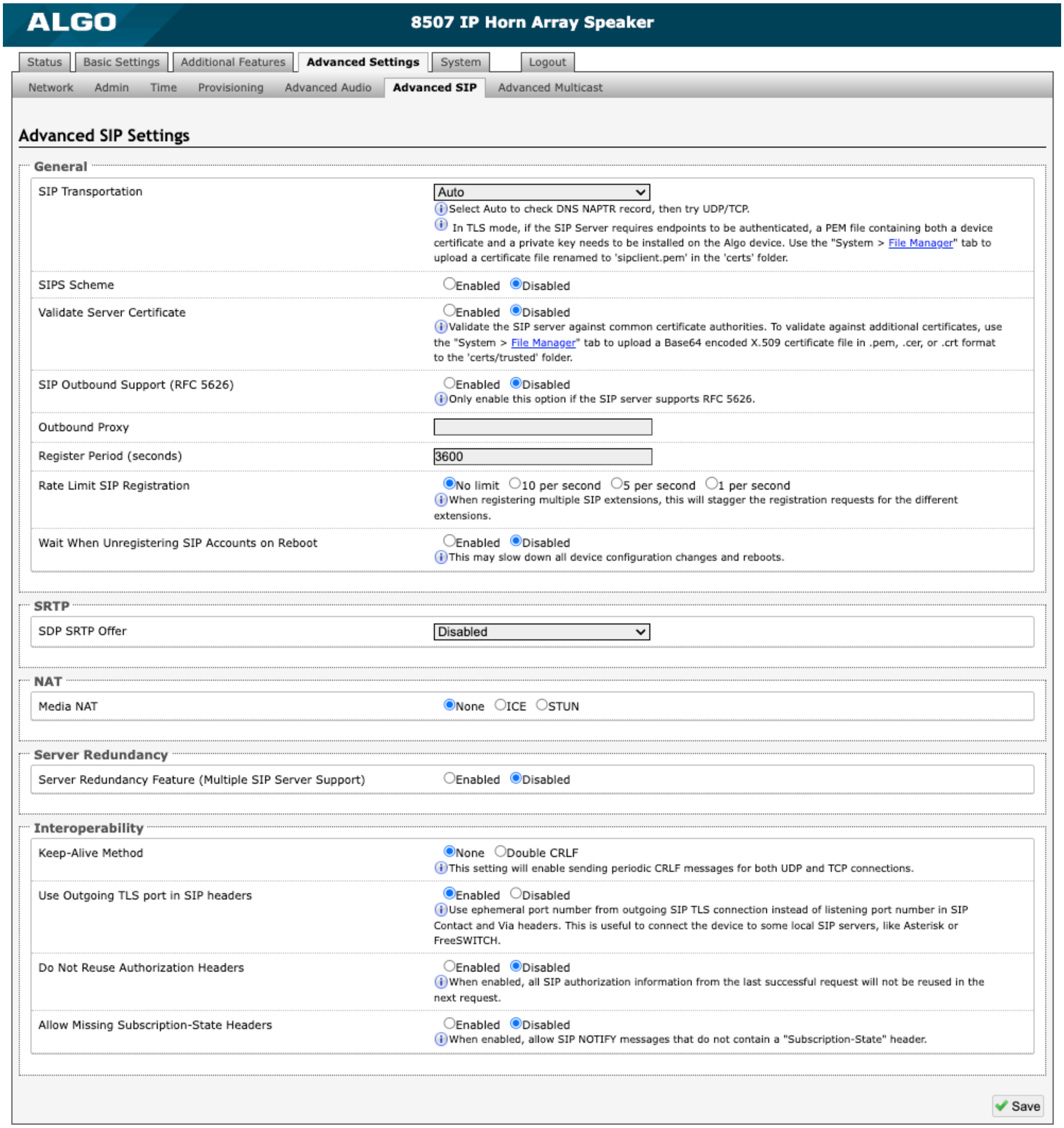
Announcement 4 ○Enabled ●Disabled

Announcement 5 ○Enabled ●Disabled

Announcement 6 ○Enabled ●Disabled

Announcement #	To configure an Emergency Alert extension, select **Enabled** for an announcement number. Up to 10 extensions can be registered allowing up to 10 different announcements. Audio files can be easily uploaded to create custom announcements. Only one 'Call-to-Cancel' extension is needed. Some SIP telephone systems may not support multiple announcements if they limit the number of extensions that can be registered on a single device.
Announcement Duration	Choose the duration of an announcement. The **Default** option follows the behavior configured in **Default Announcement Duration**.
Maximum Announcement Time	Select the maximum announcement time.
Tone/Pre-recorded Announcement	Select a file to use as a ringtone or announcement.
Confirmation Tone	Select a file to use as a confirmation tone.

3.5 Advanced SIP



ALGO
8507 IP Horn Array Speaker
Status | Basic Settings | Additional Features | Advanced Settings | System | Logout
Network | Admin | Time | Provisioning | Advanced Audio | Advanced SIP | Advanced Multicast

Advanced SIP Settings

General

SIP Transportation	Auto ⓘ Select Auto to check DNS NAPTR record, then try UDP/TCP. ⓘ In TLS mode, if the SIP Server requires endpoints to be authenticated, a PEM file containing both a device certificate and a private key needs to be installed on the Algo device. Use the "System > File Manager" tab to upload a certificate file renamed to 'sipclient.pem' in the 'certs' folder.
SIPS Scheme	○Enabled ●Disabled
Validate Server Certificate	○Enabled ●Disabled ⓘ Validate the SIP server against common certificate authorities. To validate against additional certificates, use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder.
SIP Outbound Support (RFC 5626)	○Enabled ●Disabled ⓘ Only enable this option if the SIP server supports RFC 5626.
Outbound Proxy	
Register Period (seconds)	3600
Rate Limit SIP Registration	●No limit ○10 per second ○5 per second ○1 per second ⓘ When registering multiple SIP extensions, this will stagger the registration requests for the different extensions.
Wait When Unregistering SIP Accounts on Reboot	○Enabled ●Disabled ⓘ This may slow down all device configuration changes and reboots.

SRTP

SDP SRTP Offer	Disabled

NAT

Media NAT	●None ○ICE ○STUN

Server Redundancy

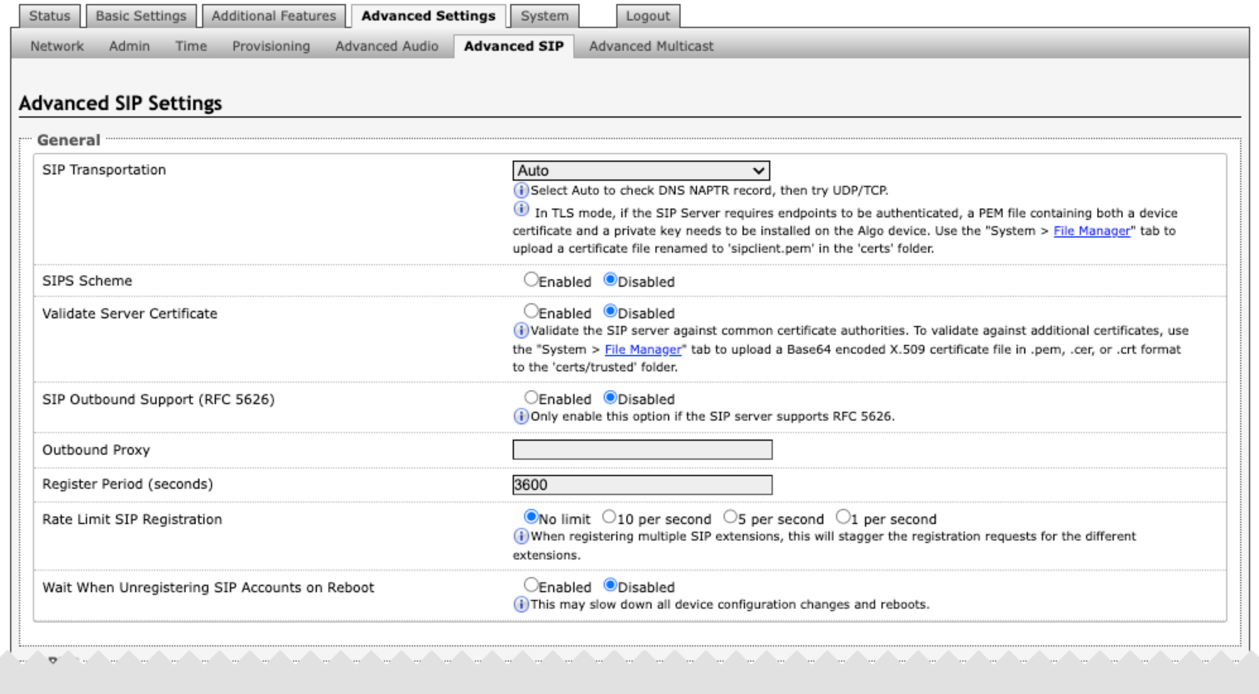
Server Redundancy Feature (Multiple SIP Server Support)	○Enabled ●Disabled

Interoperability

Keep-Alive Method	●None ○Double CRLF ⓘ This setting will enable sending periodic CRLF messages for both UDP and TCP connections.
Use Outgoing TLS port in SIP headers	●Enabled ○Disabled ⓘ Use ephemeral port number from outgoing SIP TLS connection instead of listening port number in SIP Contact and Via headers. This is useful to connect the device to some local SIP servers, like Asterisk or FreeSWITCH.
Do Not Reuse Authorization Headers	○Enabled ●Disabled ⓘ When enabled, all SIP authorization information from the last successful request will not be reused in the next request.
Allow Missing Subscription-State Headers	○Enabled ●Disabled ⓘ When enabled, allow SIP NOTIFY messages that do not contain a "Subscription-State" header.

Figure 12: Configure Advanced SIP settings in the web interface.

General



Advanced SIP Settings

General

SIP Transportation: Auto
ⓘ Select Auto to check DNS NAPTR record, then try UDP/TCP.
ⓘ In TLS mode, if the SIP Server requires endpoints to be authenticated, a PEM file containing both a device certificate and a private key needs to be installed on the Algo device. Use the "System > File Manager" tab to upload a certificate file renamed to 'sipclient.pem' in the 'certs' folder.

SIPS Scheme: ○Enabled ●Disabled

Validate Server Certificate: ○Enabled ●Disabled
ⓘ Validate the SIP server against common certificate authorities. To validate against additional certificates, use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder.

SIP Outbound Support (RFC 5626): ○Enabled ●Disabled
ⓘ Only enable this option if the SIP server supports RFC 5626.

Outbound Proxy:

Register Period (seconds): 3600

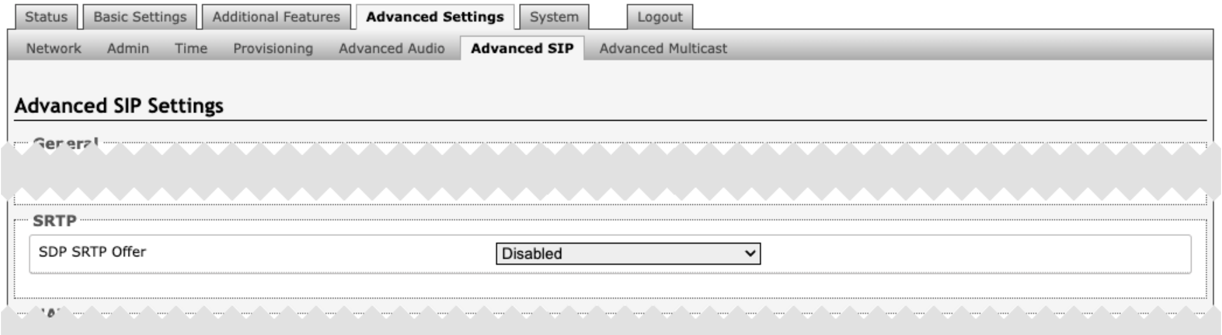
Rate Limit SIP Registration: ●No limit ○10 per second ○5 per second ○1 per second
ⓘ When registering multiple SIP extensions, this will stagger the registration requests for the different extensions.

Wait When Unregistering SIP Accounts on Reboot: ○Enabled ●Disabled
ⓘ This may slow down all device configuration changes and reboots.

SIP Transportation	Select a transport layer protocol to use for SIP messages from the dropdown. These options include: • **Auto**: Will check the DNS NAPTR record, then try UDP/TCP. • **UDP** • **TCP** • **TLS**: Ensures the encryption of SIP traffic. In this mode, if the SIP Server requires endpoints to be authenticated, a PEM file containing both a device certificate and a private key must be installed on the device. Upload a certificate via **System** → **File Manager** and rename it to 'sipclient.pem' in the 'certs' folder.
SIPS Scheme	Only visible when **SIP Transportation** is set to **TLS**. Enable to require the SIP connection from endpoint to endpoint to be secure.
Validate Server Certificate	Enable to validate the SIP server against common certificate authorities. To validate additional certificates, navigate to **System** → **File Manager** to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the **certs** folder.
SIP Outbound Support (RFC 5626)	Enable this option to support best networking practices according to RFC 5626. This option should be enabled if the device is registered with a hosted server or TLS is used for SIP Transportation.

Outbound Proxy	Enter the IP address for an outbound proxy.
Register Period (seconds)	Enter the maximum requested period where the device will re-register with the SIP server. The default setting is 3600 seconds (1 hour). Note that if an Expires header is provided by the SIP response 200 (OK), this time will take precedence over the **Register Period** defined time here. Only change if instructed to do so.
Rate Limit SIP Registration	This option should be used in cases where many SIP extensions are registered (ex. one for each zone). Select a rate limit to stagger registration requests and prevent overloading the server by sending them all at the same time.
Wait When Unregistering SIP Accounts on Reboot	Enable for the device to perform an unregister handshake with the server before shutting down or rebooting. Enabling may cause a slight delay during reboot.

SRTP



Advanced SIP Settings

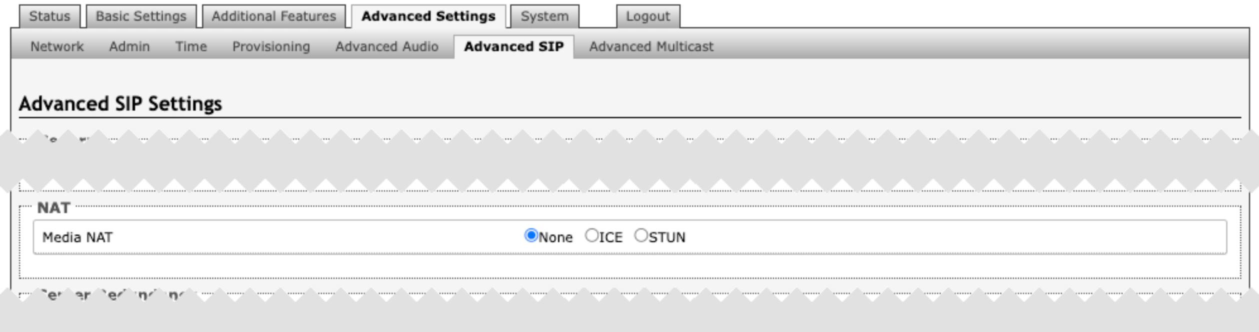
General

SRTP

SDP SRTP Offer: Disabled

SDP SRTP Offer	Select an option from the dropdown menu: • **Disabled** • **Standard**: Encrypts RTP voice data to secure audio RTP packets (SRTP). SIP calls will be rejected if the other party does not support SRTP. This option secures the audio data between parties by ensuring that it's not left out for third parties to reconstruct and listen to. • **Optional** (Non-standard AVP Profile): The SIP call's RTP data will be unencrypted if the other party does not support SRTP.

NAT



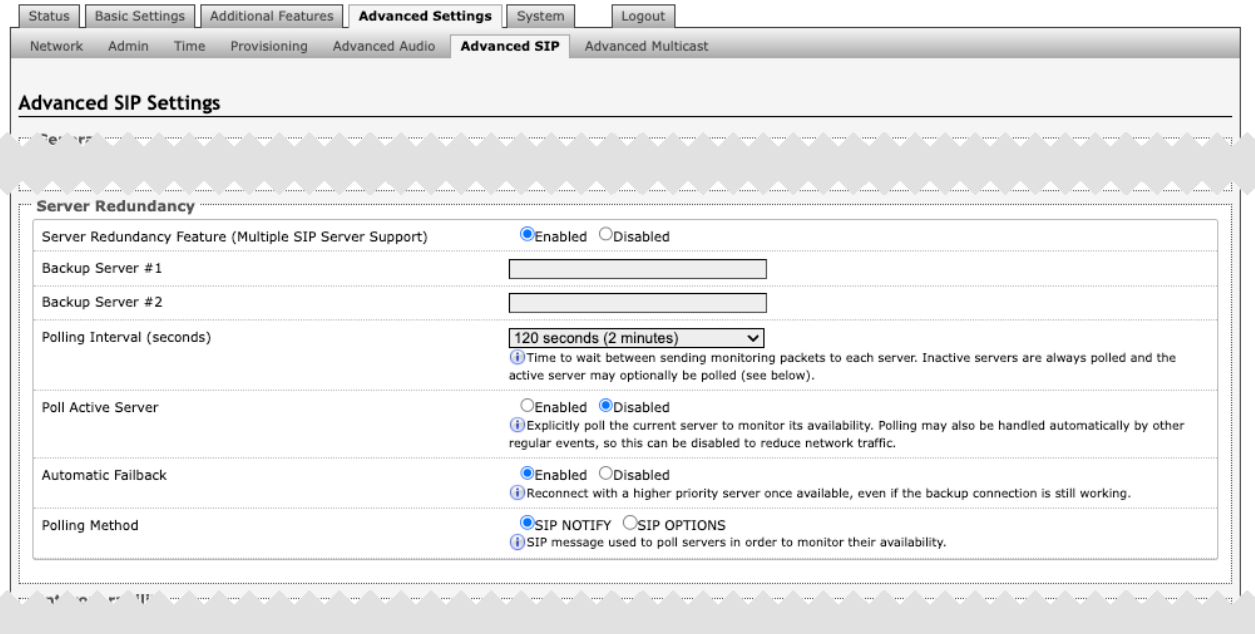
Advanced SIP Settings

NAT

Media NAT ● None ○ ICE ○ STUN

Media NAT	IP address for STUN server if present or IP address/credentials for a TURN server.
ICE – TURN Server	Enter the IP address or domain of the ICE server.
ICE – TURN User	Enter the username.
ICE – TURN Password	Enter the password.
STUN - Server	Enter the IP address or domain of the STUN server.

Server Redundancy



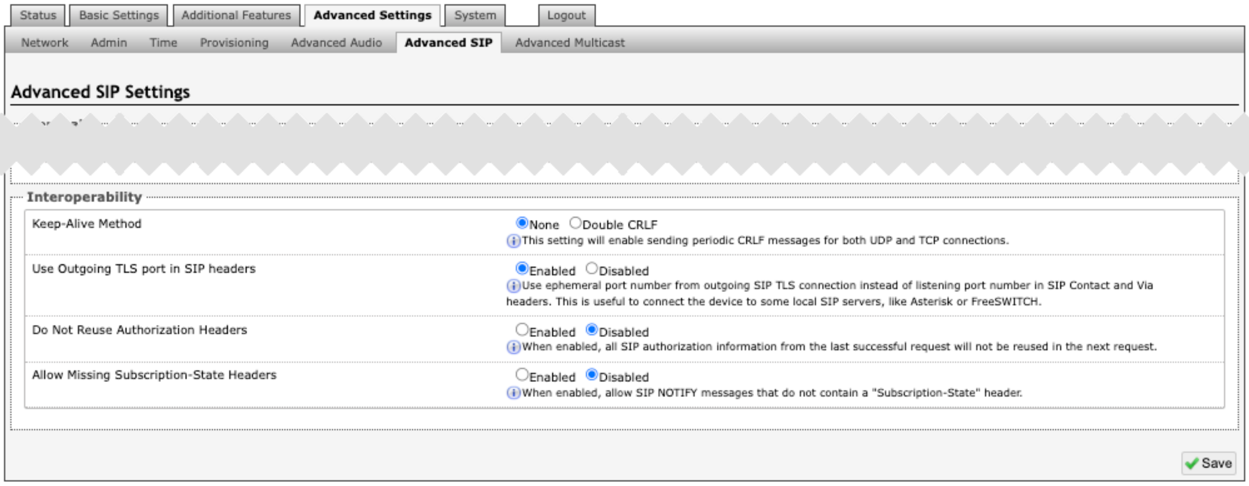
Advanced SIP Settings

Server Redundancy

Server Redundancy Feature (Multiple SIP Server Support)	● Enabled ○ Disabled
Backup Server #1	
Backup Server #2	
Polling Interval (seconds)	120 seconds (2 minutes) Time to wait between sending monitoring packets to each server. Inactive servers are always polled and the active server may optionally be polled (see below).
Poll Active Server	○ Enabled ● Disabled Explicitly poll the current server to monitor its availability. Polling may also be handled automatically by other regular events, so this can be disabled to reduce network traffic.
Automatic Failback	● Enabled ○ Disabled Reconnect with a higher priority server once available, even if the backup connection is still working.
Polling Method	● SIP NOTIFY ○ SIP OPTIONS SIP message used to poll servers in order to monitor their availability.

Server Redundancy Feature	Enable to configure up to two secondary backup servers. When enabled, the device will attempt to register with the primary server but switch to a secondary server when necessary. The configuration allows re-registration to the primary server upon availability or to stay with a server until unresponsive.
Backup Server #1, #2	Provided by your SIP provider or IT team.
Polling Intervals (seconds)	Select the time interval for sending monitoring packets to each server from the dropdown menu. Inactive servers are always polled and the active server may optionally be polled.
Poll Active Server	Enable to explicitly poll the current server to monitor availability. Other regular events may also handle this automatically and can be disabled to reduce network traffic.
Automatic Fallback	Enable to allow the device to reconnect with a higher priority server once available, even if the backup connection is still working.
Polling Method	Select a polling method based on what your SIP provider supports.

Interoperability



Advanced SIP Settings

Interoperability

Keep-Alive Method	● None ○ Double CRLF This setting will enable sending periodic CRLF messages for both UDP and TCP connections.
Use Outgoing TLS port in SIP headers	● Enabled ○ Disabled Use ephemeral port number from outgoing SIP TLS connection instead of listening port number in SIP Contact and Via headers. This is useful to connect the device to some local SIP servers, like Asterisk or FreeSWITCH.
Do Not Reuse Authorization Headers	○ Enabled ● Disabled When enabled, all SIP authorization information from the last successful request will not be reused in the next request.
Allow Missing Subscription-State Headers	○ Enabled ● Disabled When enabled, allow SIP NOTIFY messages that do not contain a "Subscription-State" header.

Keep-Alive Method	Select a keep-alive method: - **None** - **Double CRLF**: The device will send a packet regularly to maintain connection with the SIP Server if behind NAT.
Keep-Alive Interval	Set the interval in seconds that the CRLF message should be sent. 30 seconds is recommended.
Use Outgoing TLS port in SIP Headers	Enable to use the ephemeral port number from an outgoing SIP TLS connection instead of the listening port number in SIP Contact and Via headers. This is useful for connecting the device to some local SIP servers, like Asterisk or FreeSWITCH.
Do Not Reuse Authorization Headers	Enable so all SIP authorization information from the last successful request will not be reused in the next request.
Allow Missing Subscription-State Headers	Enable to allow SIP NOTIFY messages that do not contain a ‘Subscription-State’ header.

4 MULTICAST CONFIGURATION

The 8507 IP Horn Array Speaker can be programmed as a multicast transmitter or receiver to scale communications in a simple and effective way. IP endpoints connected to the 8507 can be grouped into up to 50 multicast zones and paged via DTMF Selectable Mode or multiple SIP extensions.

Dual-tone multi-frequency (DTMF) refers to the sounds or tones a telephone generates when the numbers are pressed. To page with DTMF Selectable Mode, a user can dial the SIP extension of the transmitter device and dial the desired DTMF page zone (e.g., 1, 2, etc.) on the keypad.

Another way to page multiple zones is through multiple registered SIP extensions on the transmitter device. Each extension can be configured to multicast to a unique zone, allowing zones to be called directly.

4.1 Multicast IP Addresses

Each 8507 has a unique IP address and shares a common multicast IP and port number (multicast zone) for multicast packets. The Transmitter units send to a configurable multicast zone, and the Receiver units listen to assigned multicast zones.

The network switches and router see the packet and deliver it to all the group members. The multicast IP and port number must be the same on each group's Transmitter and Receiver units. The user may define multiple zones by picking different multicast IP addresses and/or port numbers.

1. Multicast IP addresses range: 224.0.0.0/4 (from 224.0.0.0 to 239.255.255.255)
2. Port numbers range: 1 to 65535
3. By default, the device is set to use the multicast IP address 224.0.2.60 and the port numbers 50000-50008

Ensure the multicast IP address and port number do not conflict with other services and devices on the same network.

4.2 Enable Multicast Streaming

To use multicast features, only the first endpoint must be registered as a SIP extension. If only one audio stream is active at any given time, additional Algo IP endpoints, including any combination of paging adapters, speakers, and visual alerters, may be added as multicast receivers. If multiple unique audio streams are needed simultaneously, more than one transmitter will be required.

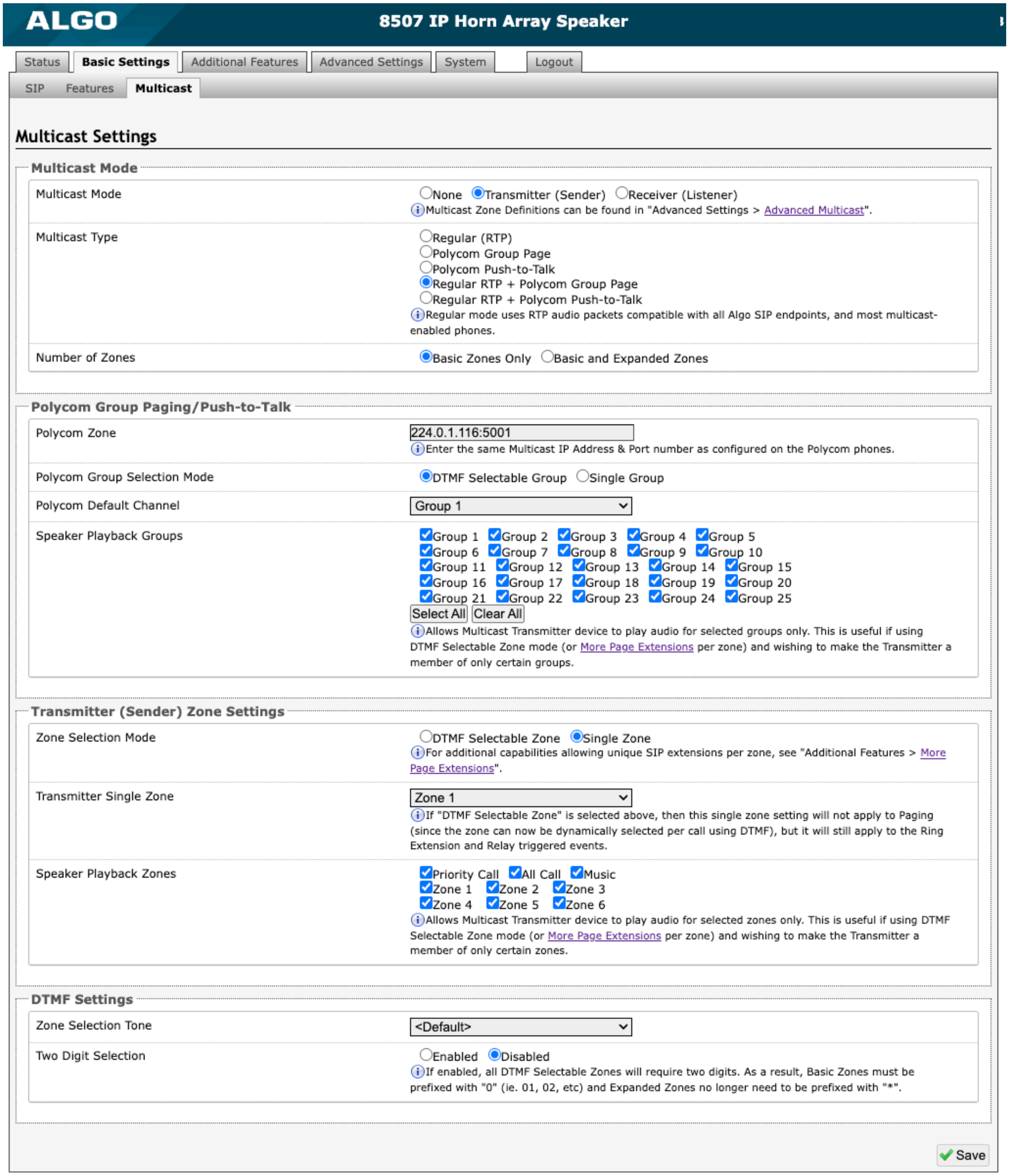
The Algo IP endpoint configured as the transmitter will stream audio to the receivers simultaneously. Receiver endpoints do not require SIP extensions and do not need to register with the SIP Communication Server.

To enable multicast streaming from the transmitter adapter, open the web interface and go to the **Basic Settings → Multicast** tab. For Multicast Mode, select **Transmitter (Sender)**. For Transmitter Single Zone, select **All Call**.

To enable multicast monitoring of the receiver endpoints, go to the web interface for each endpoint and navigate to the **Basic Settings → Multicast** tab. For Multicast Mode, select **Receiver (Listener)**. There is no need to select a Transmitter Single Zone. The endpoint will monitor the **All Call** zone IP address by default.

The page pre-announce tone is generated from the transmitter. The speaker volume can be increased or decreased for each multicast receiver individually.

4.3 Multicast: Transmitter (Sender)



ALGO 8507 IP Horn Array Speaker

Multicast Settings

Multicast Mode

Multicast Mode: ○None ●Transmitter (Sender) ○Receiver (Listener)
ⓘMulticast Zone Definitions can be found in "Advanced Settings > Advanced Multicast".

Multicast Type:
○Regular (RTP)
○Polycom Group Page
○Polycom Push-to-Talk
●Regular RTP + Polycom Group Page
○Regular RTP + Polycom Push-to-Talk
ⓘRegular mode uses RTP audio packets compatible with all Algo SIP endpoints, and most multicast-enabled phones.

Number of Zones: ●Basic Zones Only ○Basic and Expanded Zones

Polycom Group Paging/Push-to-Talk

Polycom Zone: 224.0.1.116:5001
ⓘEnter the same Multicast IP Address & Port number as configured on the Polycom phones.

Polycom Group Selection Mode: ●DTMF Selectable Group ○Single Group

Polycom Default Channel: Group 1

Speaker Playback Groups:
☑Group 1 ☑Group 2 ☑Group 3 ☑Group 4 ☑Group 5
☑Group 6 ☑Group 7 ☑Group 8 ☑Group 9 ☑Group 10
☑Group 11 ☑Group 12 ☑Group 13 ☑Group 14 ☑Group 15
☑Group 16 ☑Group 17 ☑Group 18 ☑Group 19 ☑Group 20
☑Group 21 ☑Group 22 ☑Group 23 ☑Group 24 ☑Group 25
Select All Clear All
ⓘAllows Multicast Transmitter device to play audio for selected groups only. This is useful if using DTMF Selectable Zone mode (or More Page Extensions per zone) and wishing to make the Transmitter a member of only certain groups.

Transmitter (Sender) Zone Settings

Zone Selection Mode: ○DTMF Selectable Zone ●Single Zone
ⓘFor additional capabilities allowing unique SIP extensions per zone, see "Additional Features > More Page Extensions".

Transmitter Single Zone: Zone 1
ⓘIf "DTMF Selectable Zone" is selected above, then this single zone setting will not apply to Paging (since the zone can now be dynamically selected per call using DTMF), but it will still apply to the Ring Extension and Relay triggered events.

Speaker Playback Zones:
☑Priority Call ☑All Call ☑Music
☑Zone 1 ☑Zone 2 ☑Zone 3
☑Zone 4 ☑Zone 5 ☑Zone 6
ⓘAllows Multicast Transmitter device to play audio for selected zones only. This is useful if using DTMF Selectable Zone mode (or More Page Extensions per zone) and wishing to make the Transmitter a member of only certain zones.

DTMF Settings

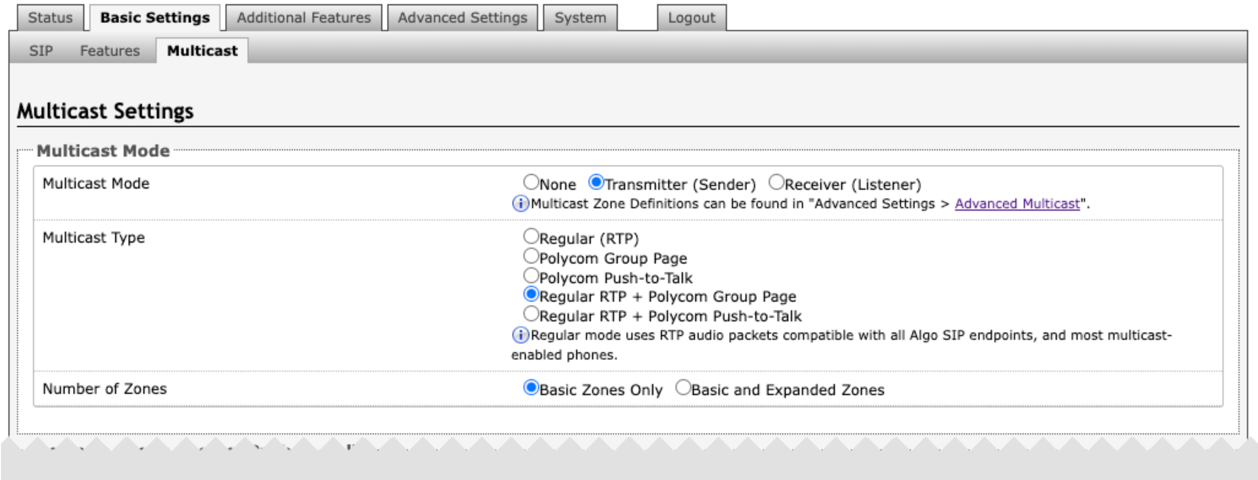
Zone Selection Tone: <Default>

Two Digit Selection: ○Enabled ●Disabled
ⓘIf enabled, all DTMF Selectable Zones will require two digits. As a result, Basic Zones must be prefixed with "0" (ie. 01, 02, etc) and Expanded Zones no longer need to be prefixed with "*".

Figure 13: Multicast transmitter mode settings.

Multicast Mode

Always ensure that the multicast settings on all Receiver devices match those of the Transmitter.



Multicast Settings

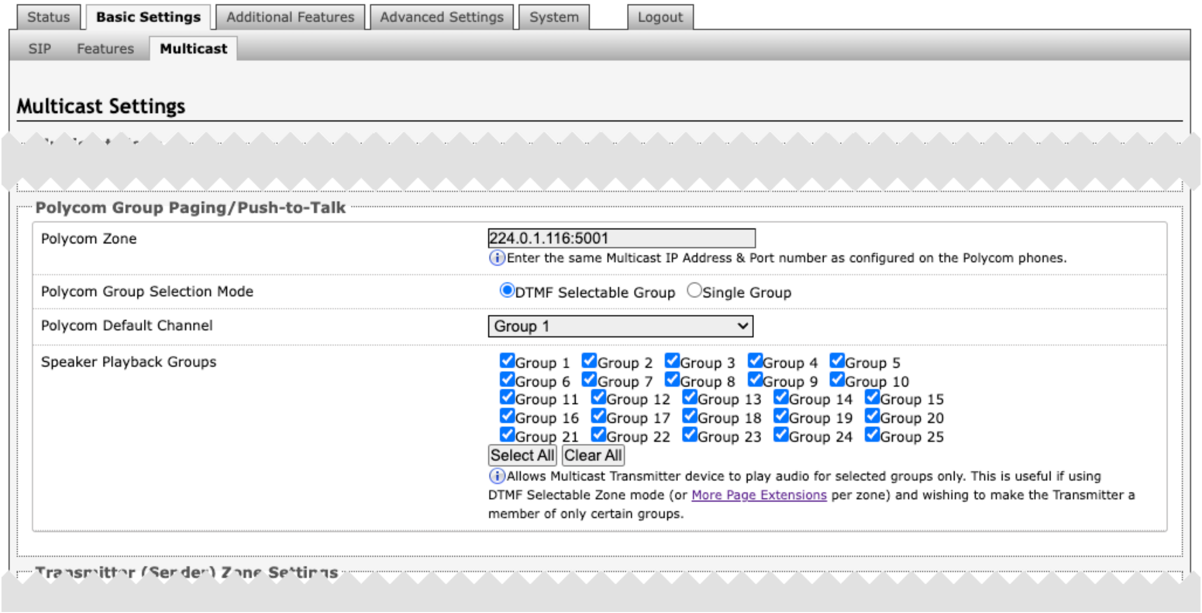
Multicast Mode

Multicast Mode	○ None ● Transmitter (Sender) ○ Receiver (Listener) ⓘ Multicast Zone Definitions can be found in "Advanced Settings > Advanced Multicast".
Multicast Type	○ Regular (RTP) ○ Polycom Group Page ○ Polycom Push-to-Talk ● Regular RTP + Polycom Group Page ○ Regular RTP + Polycom Push-to-Talk ⓘ Regular mode uses RTP audio packets compatible with all Algo SIP endpoints, and most multicast-enabled phones.
Number of Zones	● Basic Zones Only ○ Basic and Expanded Zones

Multicast Mode	If **Transmitter (Sender)** is selected, the device will broadcast an IP stream when activated in addition to playing audio through the audio output. The device cannot be both a multicast Transmitter and Receiver simultaneously.
Multicast Type	The device may broadcast multicast paging compatible with Poly “on-premise group paging” protocol and most multicast-enabled phones that use RTP audio packets. Select **Regular (RTP)** if you are only multicasting to Algo IP endpoints or multicast-enabled phones. To multicast page announcements to Poly phones, select **Poly Group Page** or **Poly Push-to-Talk**. Select **Regular RTP + Poly Group Page** or **Regular RTP + Push-to-Talk** to multicast page audio to Poly phones, Algo IP endpoints, and multicast-enabled phones.
Number of Zones	Select **Basic Zones Only** if configuring nine or fewer multicast zones. Select **Basic and Expanded Zones** to configure up to 50 zones. The expanded zones have the same behavior as the basic Receiver zones but are hidden by default to simplify the interface.

Poly Group Paging/Push-to-Talk

This section is used if the Multicast Type includes Poly Group Page or Poly Push-to-Talk.



Polycom Group Paging/Push-to-Talk

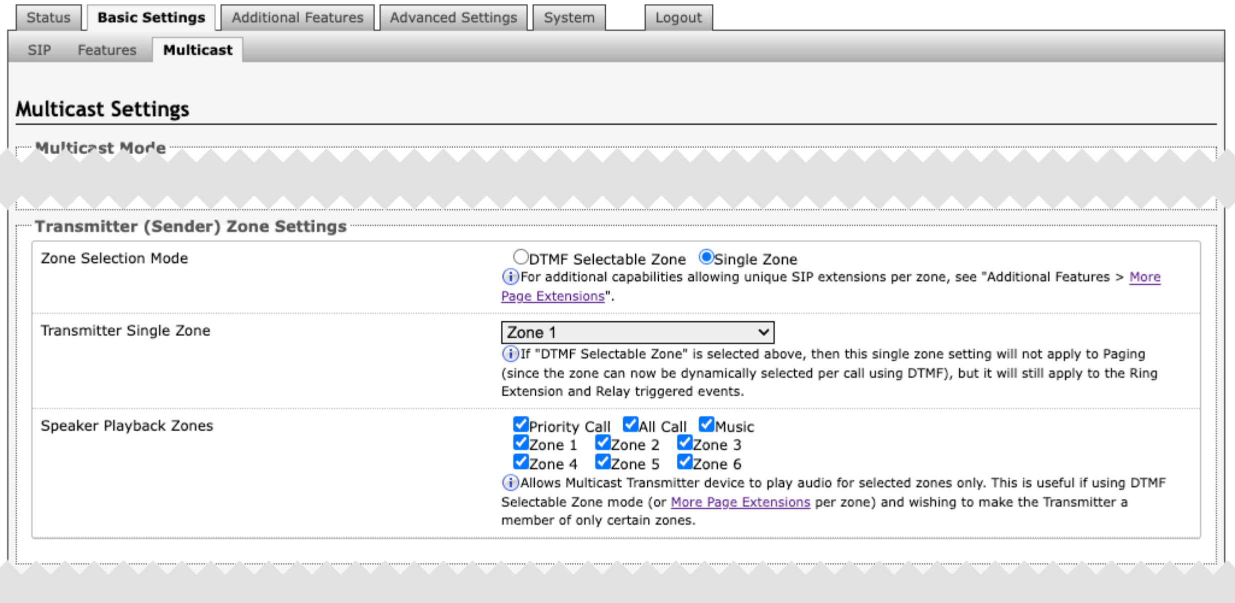
Polycom Zone	224.0.1.116:5001 ⓘEnter the same Multicast IP Address & Port number as configured on the Polycom phones.
Polycom Group Selection Mode	● DTMF Selectable Group ○ Single Group
Polycom Default Channel	Group 1
Speaker Playback Groups	☑Group 1 ☑Group 2 ☑Group 3 ☑Group 4 ☑Group 5 ☑Group 6 ☑Group 7 ☑Group 8 ☑Group 9 ☑Group 10 ☑Group 11 ☑Group 12 ☑Group 13 ☑Group 14 ☑Group 15 ☑Group 16 ☑Group 17 ☑Group 18 ☑Group 19 ☑Group 20 ☑Group 21 ☑Group 22 ☑Group 23 ☑Group 24 ☑Group 25 ⓘAllows Multicast Transmitter device to play audio for selected groups only. This is useful if using DTMF Selectable Zone mode (or More Page Extensions per zone) and wishing to make the Transmitter a member of only certain groups.

Poly Zone	Enter the same Multicast IP Address and Port number configured on the Poly phones.
Poly Group Selection Mode	Select **Single Group** to broadcast on one pre-configured group. Multiple SIP extensions can be registered on the Transmitter device. Each extension is mapped to a unique group, allowing groups to be called directly (e.g., from speed-dial keys). See **Additional Features → More Page Extensions** for additional configuration settings. If **DTMF Selectable Group** is selected, the group is determined by the DTMF selection between 0 – 25. To page using DTMF Selectable Zone: 1. Dial the SIP extension of the Transmitter device 2. Dial the desired DTMF page group number on the keypad when prompted. Groups 10 and higher start with “*”. DTMF group definitions include: • DTMF Extension 1 for Zone 1 • DTMF Extension 2 for Zone 2 …

	- DTMF Extension *10 for Zone 10 - DTMF Extension *11 for Zone 11 All DTMF codes and respective zones are available in **Advanced Settings → Advanced Multicast**.
Poly Default Channel	Select the default group for the multicast stream to be sent to. **If DTMF Selectable Group** is chosen, this single group setting will not apply to paging since the group will be dynamically selected per call using DTMF. The **Single Group** setting will still apply to the ring extension and relay triggered events. The **Poly Default Channel** is the default channel used for multicast actions unless an option is available for a custom channel with specific parameters.
Speaker Playback Groups	Select Speaker Playback Groups to control which specific groups can play audio from the device. This is useful if using the **DTMF Selectable Group** mode or additional page extensions (**Additional Features → More Page Extensions**) per group to make the device a member of only certain zones. In this case, the Transmitter does not participate in the Zone but transmits certain traffic.

Transmitter (Sender) Zone Settings

This section is used if the Multicast Type includes Regular (RTP).



Multicast Settings

Multicast Mode

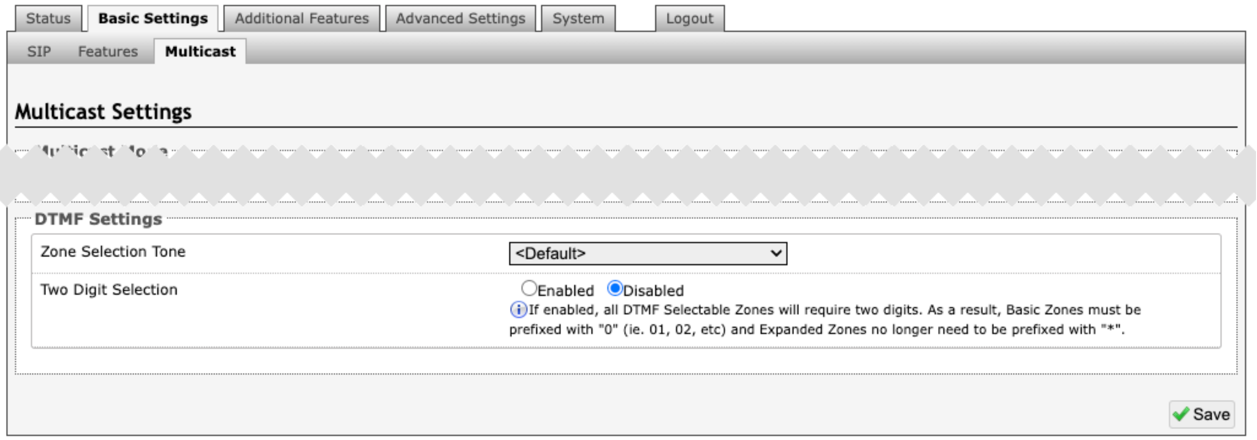
Transmitter (Sender) Zone Settings

Zone Selection Mode	○DTMF Selectable Zone ●Single Zone ⓘFor additional capabilities allowing unique SIP extensions per zone, see "Additional Features > More Page Extensions".
Transmitter Single Zone	Zone 1 ⓘIf "DTMF Selectable Zone" is selected above, then this single zone setting will not apply to Paging (since the zone can now be dynamically selected per call using DTMF), but it will still apply to the Ring Extension and Relay triggered events.
Speaker Playback Zones	☑Priority Call ☑All Call ☑Music ☑Zone 1 ☑Zone 2 ☑Zone 3 ☑Zone 4 ☑Zone 5 ☑Zone 6 ⓘAllows Multicast Transmitter device to play audio for selected zones only. This is useful if using DTMF Selectable Zone mode (or More Page Extensions per zone) and wishing to make the Transmitter a member of only certain zones.

Zone Selection Mode	Select **Single Zone** to broadcast on one pre-configured zone. Multiple SIP extensions can be registered on the Transmitter device. Each extension is mapped to a unique zone, allowing zones to be called directly (e.g., from speed-dial keys). See **Additional Features → More Page Extensions** for more additional configuration settings. If **DTMF Selectable Zone** is selected, the zone is determined by the DTMF selection between 0 – 50. Once multicast Transmitter mode is enabled, navigate to **Advanced Settings → Advanced Multicast** to find the DTMF codes corresponding to each zone. To page using **DTMF Selectable Zone:** 1. Dial the SIP extension of the Transmitter device 2. Dial the desired DTMF page zone number on the keypad when prompted. Zones 10 and higher start with "*". DTMF zone definitions include: • DTMF Extension 9 for Priority Call • DTMF Extension 0 or 8 for All Call • DTMF Extension 1 for Zone 1 • DTMF Extension *10 for Zone 10 • DTMF Extension *11 for Zone 11

	All DTMF codes and respective zones are available in **Advanced Settings → Advanced Multicast**.
Transmitter Single Zone	Select the default zone for the multicast stream to be sent to. If **DTMF Selectable Zone** is chosen, this single zone setting will not apply to Paging since the zone will be dynamically selected per call using DTMF. However, this single zone setting will still apply to the ring extension and relay-triggered events, including the analog audio input. The Transmitter Single Zone is the default zone used for multicast actions unless an option is available for a custom zone with specific parameters.
Speaker Playback Zones	Select Speaker Playback Zones to control which specific zones can play audio. This is useful if using the DTMF Selectable Zone mode or additional page extensions (**Additional Features → More Page Extensions**) per zone to make the device a member of only certain zones. In this case, the Transmitter does not participate in the Zone but transmits certain traffic.

DTMF Settings



Multicast Settings

DTMF Settings

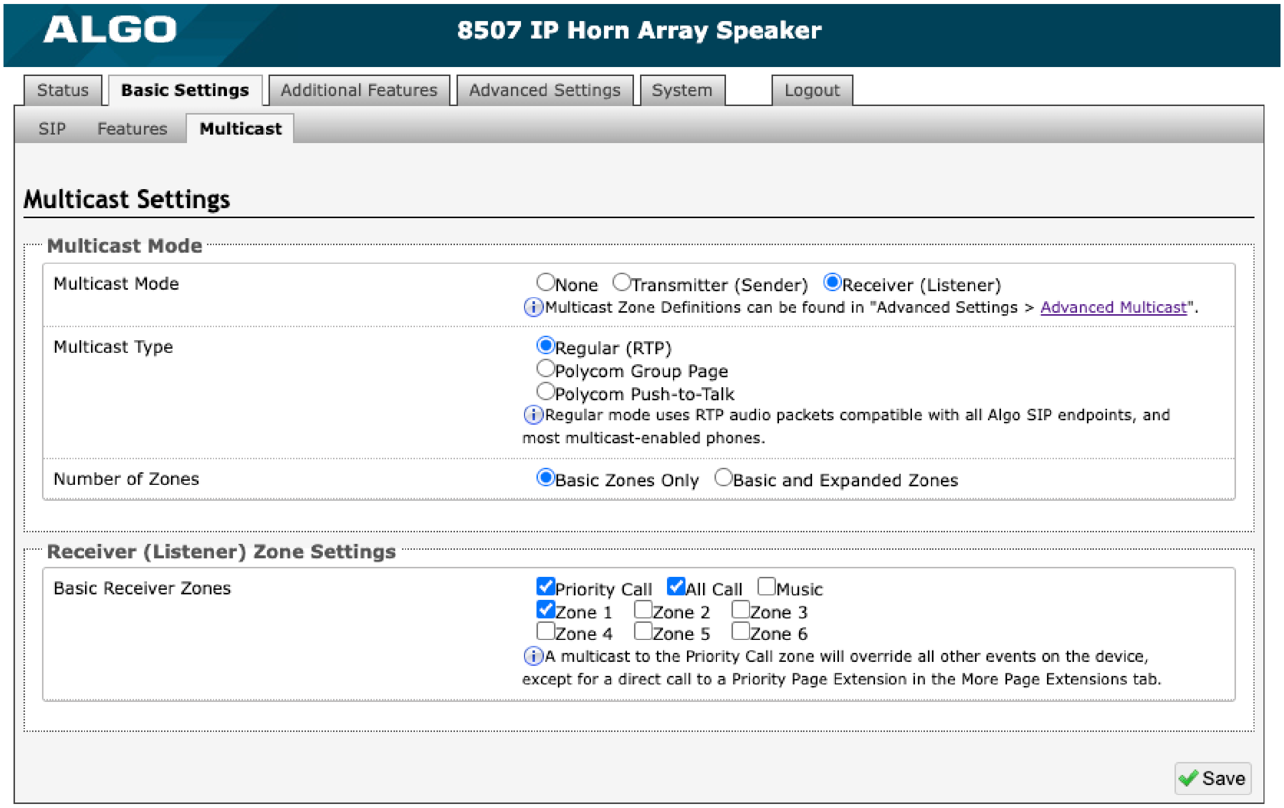
Zone Selection Tone <Default>

Two Digit Selection ○Enabled ●Disabled

If enabled, all DTMF Selectable Zones will require two digits. As a result, Basic Zones must be prefixed with "0" (ie. 01, 02, etc) and Expanded Zones no longer need to be prefixed with "*".

Zone Selection Tone	Select a tone to be played to prompt a user to select a zone to multicast to. This may be used as an interactive voice response (IVR) menu by uploading a custom audio file in the **tones** folder through **System → File Manager**. Each zone may use a different tone. This can be configured in **Advanced Settings → Advanced Multicast**.
Two-Digit Selection	When enabled, all DTMF Selectable Zones will require two digits. As a result, Basic Zones must be prefixed with *0,* and Expanded Zones will no longer need to be prefixed with *.

4.4 Multicast: Receiver (Listener)



ALGO 8507 IP Horn Array Speaker

Multicast Settings

Multicast Mode

Multicast Mode	○None ○Transmitter (Sender) ●Receiver (Listener) ⓘMulticast Zone Definitions can be found in "Advanced Settings > Advanced Multicast".
Multicast Type	●Regular (RTP) ○Polycom Group Page ○Polycom Push-to-Talk ⓘRegular mode uses RTP audio packets compatible with all Algo SIP endpoints, and most multicast-enabled phones.
Number of Zones	●Basic Zones Only ○Basic and Expanded Zones

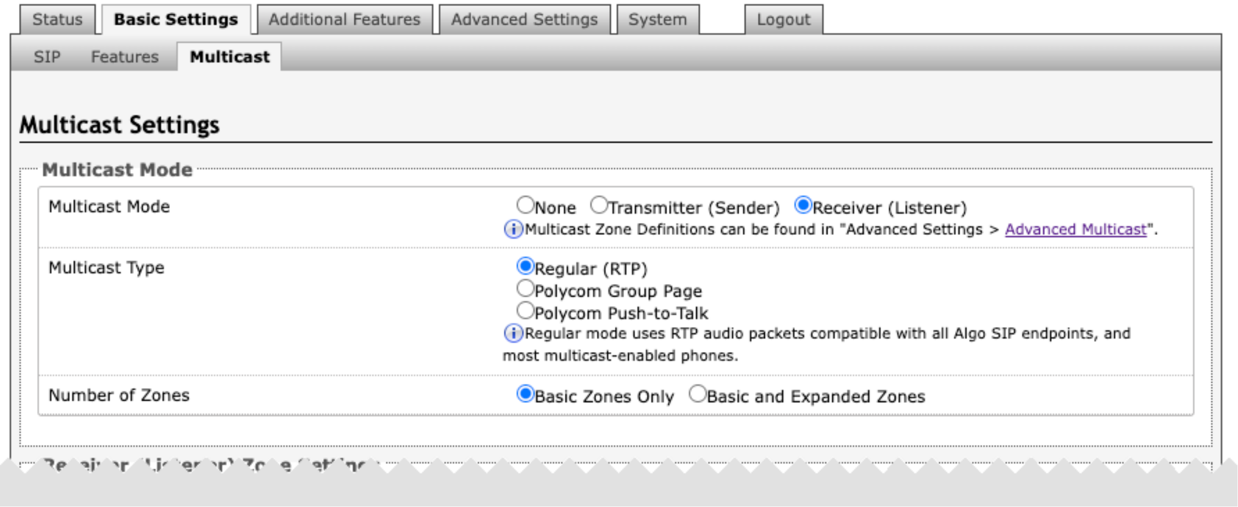
Receiver (Listener) Zone Settings

Basic Receiver Zones	☑Priority Call ☑All Call □Music ☑Zone 1 □Zone 2 □Zone 3 □Zone 4 □Zone 5 □Zone 6 ⓘA multicast to the Priority Call zone will override all other events on the device, except for a direct call to a Priority Page Extension in the More Page Extensions tab.

Figure 14: Multicast receiver mode settings.

Multicast Mode

Always ensure that the multicast settings on all Receiver devices match those of the Transmitter.



Multicast Settings

Multicast Mode

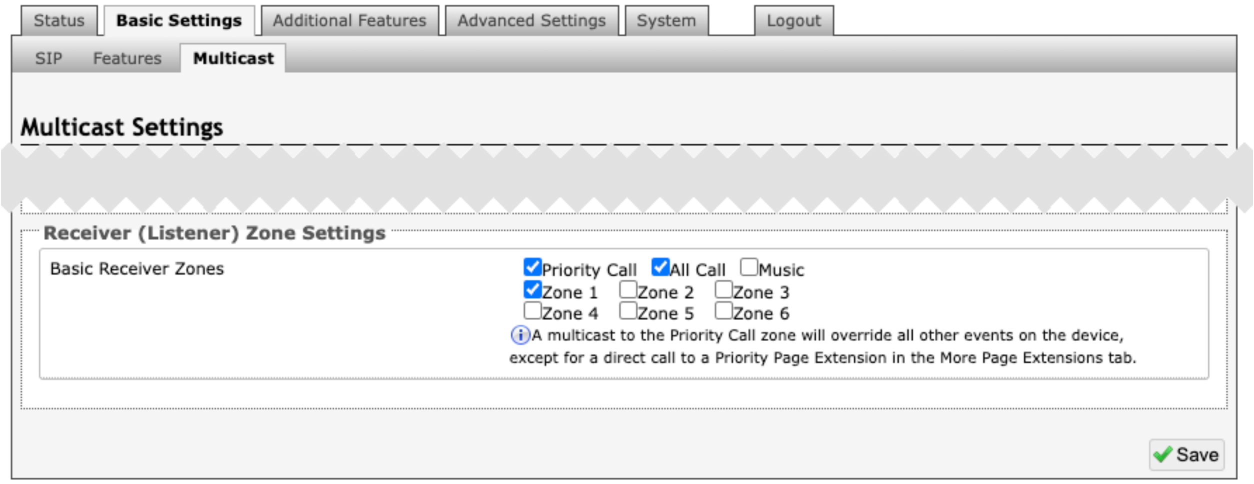
Multicast Mode: ○None ○Transmitter (Sender) ●Receiver (Listener)
ⓘMulticast Zone Definitions can be found in "Advanced Settings > Advanced Multicast".

Multicast Type: ●Regular (RTP) ○Polycom Group Page ○Polycom Push-to-Talk
ⓘRegular mode uses RTP audio packets compatible with all Algo SIP endpoints, and most multicast-enabled phones.

Number of Zones: ●Basic Zones Only ○Basic and Expanded Zones

Multicast Mode	If **Receiver (Listener)** mode is selected, the device will activate when receiving a multicast message. It will mimic the audio stream of the transmitter but use local volume settings. This can be set via **Basic Settings → Features → Page Speaker Volume**.
Multicast Type	Select **Regular** if receiving multicast from other Algo IP endpoint(s) and/or multicast-enabled phone(s) that use RTP audio packets. Select **Poly Group Page** or **Poly Push-to-Talk** if receiving multicast paging compatible with Poly "on-premise group paging" protocol.
Number of Zones	Select **Basic Zones Only** if configuring nine or fewer multicast zones. Select **Basic and Expanded Zones** to configure up to 50 zones. The expanded zones have the same behavior as the basic Receiver zones but are hidden by default to simplify the interface.

Receiver (Listener) Zone Settings



Multicast Settings

Receiver (Listener) Zone Settings

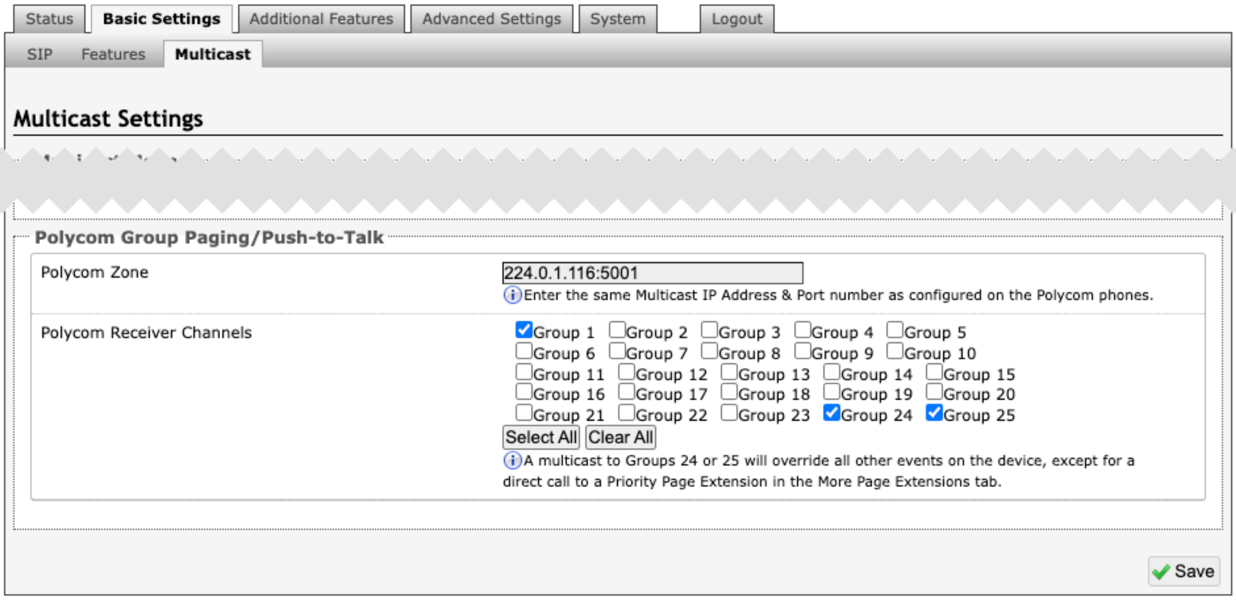
Basic Receiver Zones

☑Priority Call ☑All Call □Music
☑Zone 1 □Zone 2 □Zone 3
□Zone 4 □Zone 5 □Zone 6

ⓘA multicast to the Priority Call zone will override all other events on the device, except for a direct call to a Priority Page Extension in the More Page Extensions tab.

Basic Receiver Zones	Select one or more multicast zones for the device to listen to. Multicast zone priority will be based on the zone definition list order defined in **Advanced Settings → Advanced Multicast**.
Expanded Receiver Zones	Select additional zones (up to 50) for the device to listen to. This is only possible when **Basic and Expanded Zones** is selected.

Poly Group Paging/Push-to-Talk



Multicast Settings

Polycom Group Paging/Push-to-Talk

Polycom Zone: 224.0.1.116:5001

Enter the same Multicast IP Address & Port number as configured on the Polycom phones.

Polycom Receiver Channels:

☑Group 1 □Group 2 □Group 3 □Group 4 □Group 5
□Group 6 □Group 7 □Group 8 □Group 9 □Group 10
□Group 11 □Group 12 □Group 13 □Group 14 □Group 15
□Group 16 □Group 17 □Group 18 □Group 19 □Group 20
□Group 21 □Group 22 □Group 23 ☑Group 24 ☑Group 25

Select All | Clear All

A multicast to Groups 24 or 25 will override all other events on the device, except for a direct call to a Priority Page Extension in the More Page Extensions tab.

Poly Zone	Enter the Poly Zone (IP Address and Port) that matches the configuration of the Poly phones and Channels.
Poly Receiver Channels	If using a Poly telephone as a Multicast Transmitter, a tone may be set for any of the 25 Poly Groups configured on the device. Poly Group Tones can be set in **Advanced Settings → Advanced Multicast**. The Poly telephone used as a page audio source for the device must be configured to use either the G.711 or G.722 audio codec. Note that Poly phone(s) must be configured with the “Compatibility” setting (“ptt.compatibilityMode”) disabled for this codec setting to be applied.

4.5 Using Multicast Page Zones

The 8507 IP Horn Array Speaker can listen to up to 50 paging zones (See **Additional Features → More Page Extensions** for more details). The multicast IP addresses define these zones.

By default, these zones have the names below but can be used however you prefer.

- Priority
- All Call
- Zone 1
- Zone 2
- Zone 3
- Zone 4
- Zone 5
- Zone 6
- Music

When set as a multicast receiver, zones have a priority hierarchy where zones higher on the list will be treated with higher priority, with **Music** being the lowest priority. When set as a multicast transmitter, event priority is based on the event type that initiated the multicast rather than the output multicast channel that will be active.

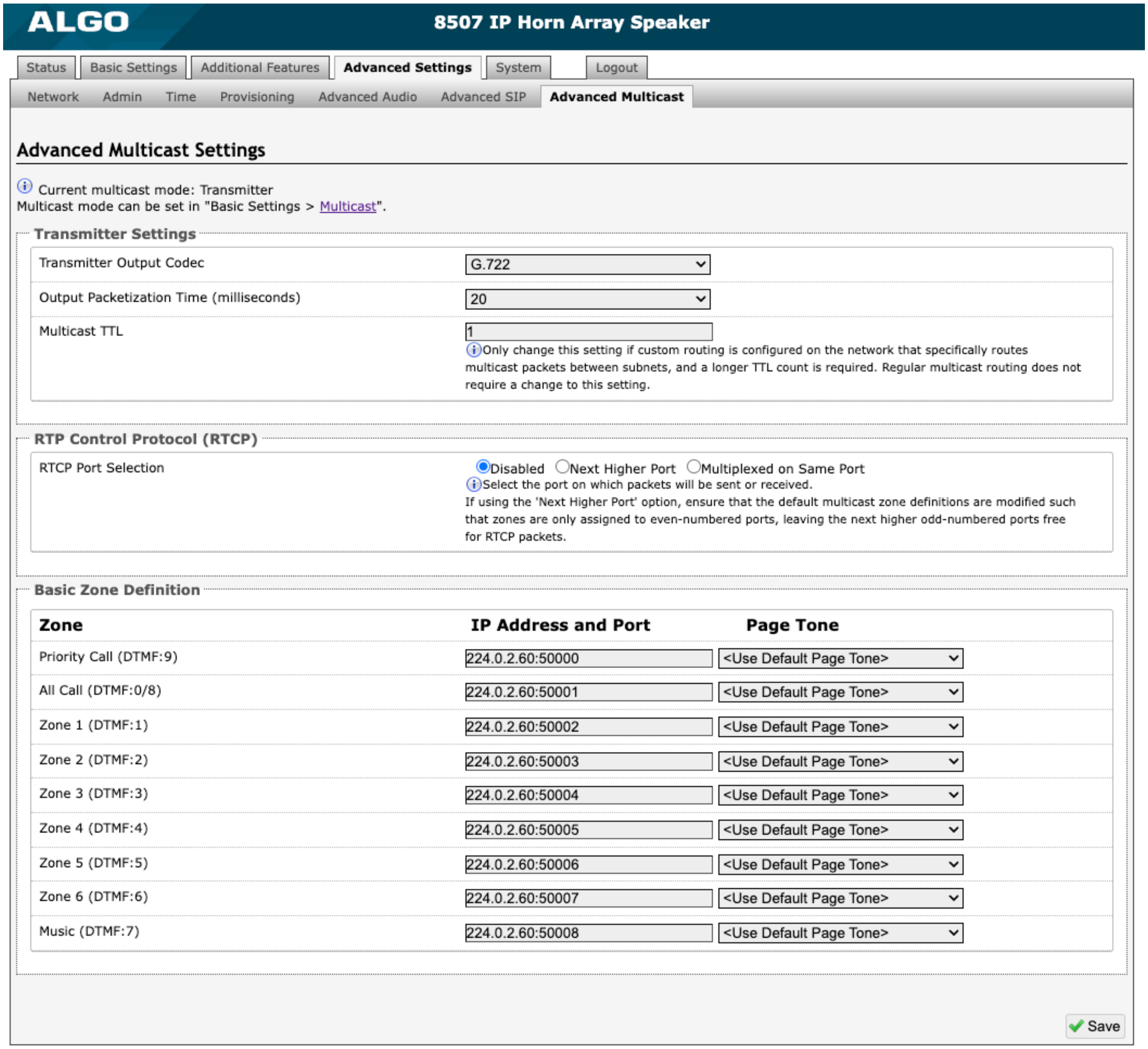
There are two options for paging to multiple zones:

1. DTMF Selectable Mode: Has a dynamic page zone selection and requires only the transmitting device to have a registered SIP extension. To page, dial the SIP extension of the transmitter and dial the desired DTMF page zone (e.g., 1, 2, etc.) on the keypad. DTMF digits and their corresponding zone numbers can be found in the **Advanced Settings → Advanced Multicast** tab of the web interface.

2. Multiple page extensions: Multiple SIP extensions can be registered on the transmitter. Each extension is mapped to a unique zone, allowing zones to be called directly. See **Additional Features → More Page Extensions** tab of the web interface for more details.

4.6 Advanced Multicast

These settings are only visible when in Transmitter or Receiver multicast mode. This can be set in **Basic Settings → Multicast**. The default pre-populated multicast zone IP addresses and ports will work in most cases and should only be altered for rare cases.



Advanced Multicast Settings

Current multicast mode: Transmitter
Multicast mode can be set in "Basic Settings > Multicast".

Transmitter Settings

Transmitter Output Codec	G.722
Output Packetization Time (milliseconds)	20
Multicast TTL	1 Only change this setting if custom routing is configured on the network that specifically routes multicast packets between subnets, and a longer TTL count is required. Regular multicast routing does not require a change to this setting.

RTP Control Protocol (RTCP)

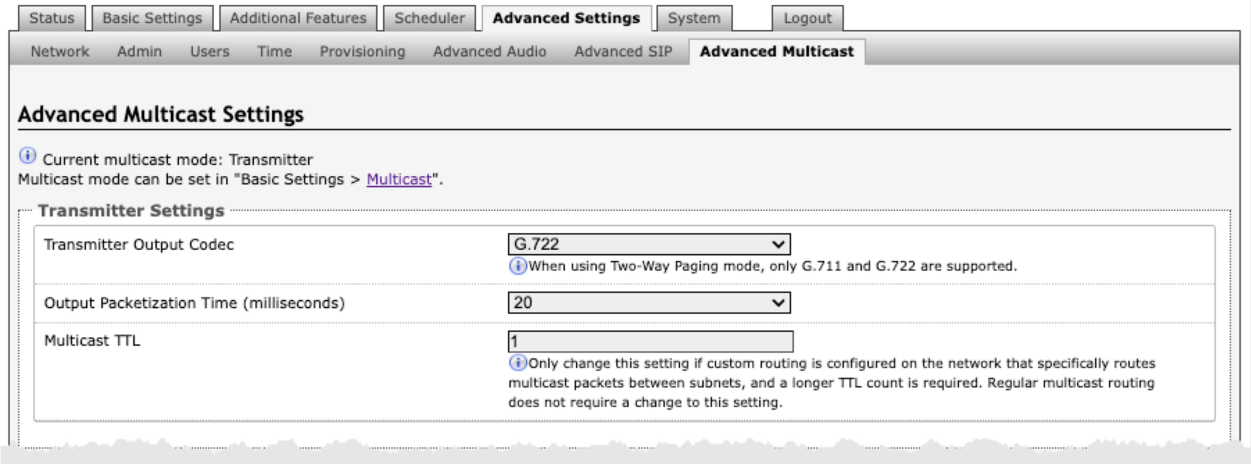
RTCP Port Selection	● Disabled ○ Next Higher Port ○ Multiplexed on Same Port Select the port on which packets will be sent or received. If using the 'Next Higher Port' option, ensure that the default multicast zone definitions are modified such that zones are only assigned to even-numbered ports, leaving the next higher odd-numbered ports free for RTCP packets.

Basic Zone Definition

Zone	IP Address and Port	Page Tone
Priority Call (DTMF:9)	224.0.2.60:50000	<Use Default Page Tone>
All Call (DTMF:0/8)	224.0.2.60:50001	<Use Default Page Tone>
Zone 1 (DTMF:1)	224.0.2.60:50002	<Use Default Page Tone>
Zone 2 (DTMF:2)	224.0.2.60:50003	<Use Default Page Tone>
Zone 3 (DTMF:3)	224.0.2.60:50004	<Use Default Page Tone>
Zone 4 (DTMF:4)	224.0.2.60:50005	<Use Default Page Tone>
Zone 5 (DTMF:5)	224.0.2.60:50006	<Use Default Page Tone>
Zone 6 (DTMF:6)	224.0.2.60:50007	<Use Default Page Tone>
Music (DTMF:7)	224.0.2.60:50008	<Use Default Page Tone>

Figure 15: Advanced multicast - transmitter settings.

Transmitter Settings



Advanced Multicast Settings

Current multicast mode: Transmitter
Multicast mode can be set in "Basic Settings > Multicast".

Transmitter Settings

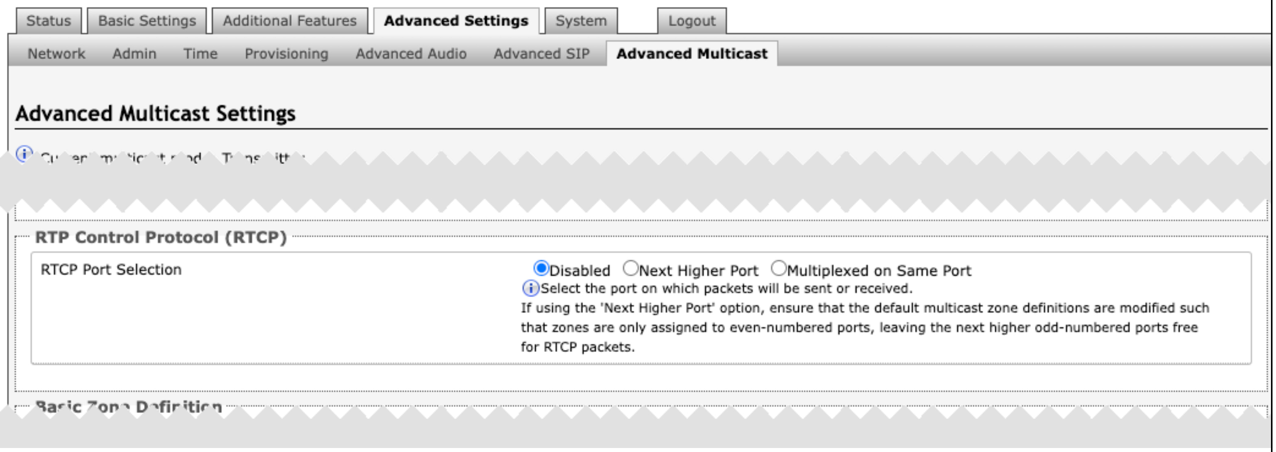
Transmitter Output Codec: G.722
When using Two-Way Paging mode, only G.711 and G.722 are supported.

Output Packetization Time (milliseconds): 20

Multicast TTL: 1
Only change this setting if custom routing is configured on the network that specifically routes multicast packets between subnets, and a longer TTL count is required. Regular multicast routing does not require a change to this setting.

Transmitter Output Codec	Select an audio encoding format for the Transmitter device to use when sending output to the Receivers. Supported formats include: • G.711 ulaw • G.722 • Opus Only G.711 and G.722 are supported when using Two-Way Paging mode.
Output Packetization Time (milliseconds)	Select the size of the audio packets the Transmitter sends to the Receivers from the dropdown menu. The default of 20 milliseconds is recommended unless a different value is specifically required for compatibility with other devices.
Multicast TTL	Only change the multicast time to live (TTL) setting if custom routing is configured on the network that specifically routes multicast packets between subnets and a longer TTL count is required. This ensures packets are not bounced back and forth in a network identity. When the TTL is reached, the router drops the packet.

RTP Control Protocol (RTCP)



Advanced Multicast Settings

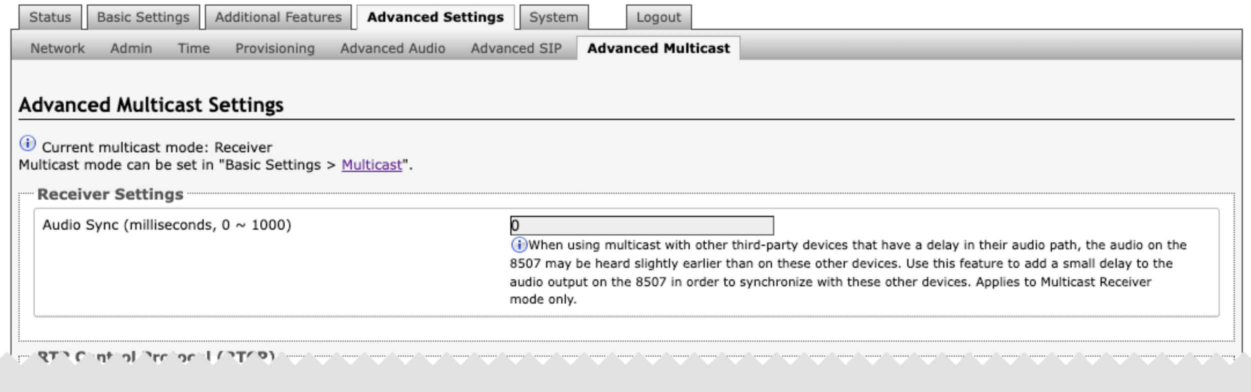
RTP Control Protocol (RTCP)

RTCP Port Selection ● Disabled ○ Next Higher Port ○ Multiplexed on Same Port

Select the port on which packets will be sent or received.
If using the 'Next Higher Port' option, ensure that the default multicast zone definitions are modified such that zones are only assigned to even-numbered ports, leaving the next higher odd-numbered ports free for RTCP packets.

RTCP Port Selection	Select how a port will be chosen to send or receive RTCP packets. Note: If **Next Higher Port** is selected, ensure that the default multicast zone definitions are modified so that zones are only assigned to even-numbered ports, leaving the next higher odd-numbered ports free for RTCP packets.

Receiver Settings



Advanced Multicast Settings

Current multicast mode: Receiver
Multicast mode can be set in "Basic Settings > Multicast".

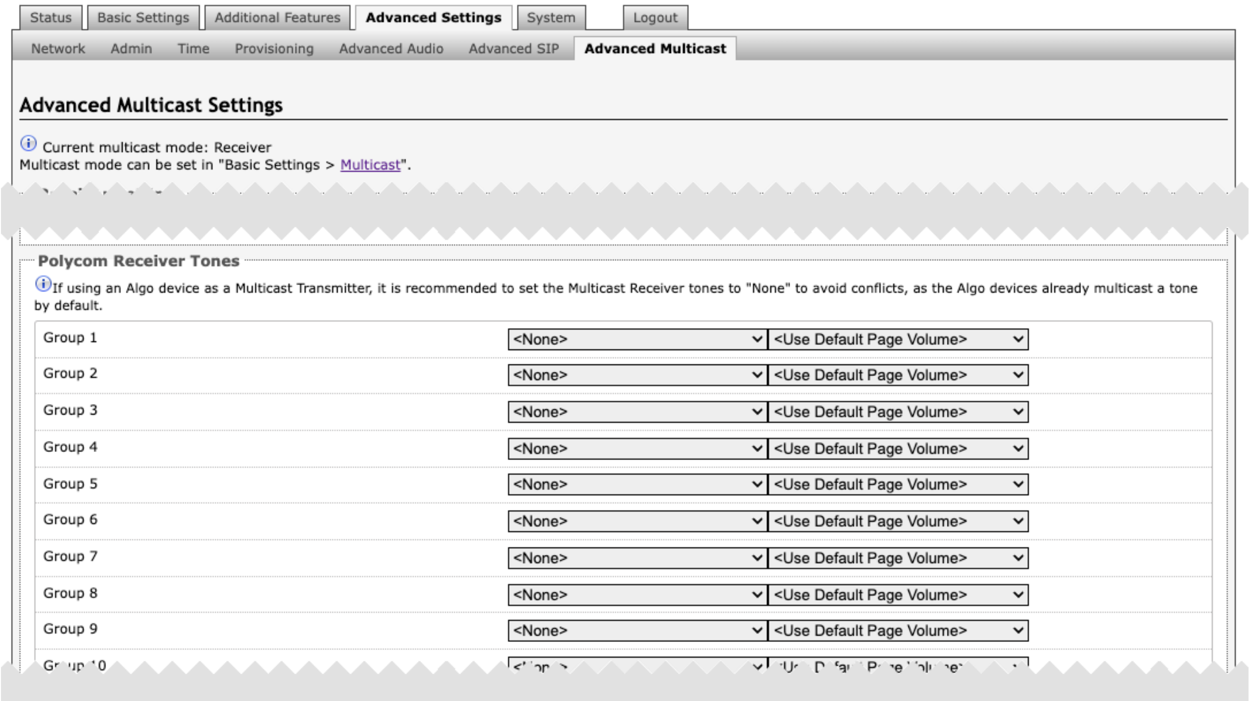
Receiver Settings

Audio Sync (milliseconds, 0 ~ 1000) 0

When using multicast with other third-party devices that have a delay in their audio path, the audio on the 8507 may be heard slightly earlier than on these other devices. Use this feature to add a small delay to the audio output on the 8507 in order to synchronize with these other devices. Applies to Multicast Receiver mode only.

Audio Sync	Available if **Multicast Mode** is set to **Receiver (Listener)** and **Multicast Type** is set to **Poly Group Page** or **Poly Push-to-Talk** (under **Basic Settings → Multicast**). When using multicast with other third-party devices that have a delay in their audio path, the audio on the device may be heard slightly earlier than on these other devices. Use this feature to add a small delay to the audio output on the device to synchronize with these other devices.

Polycom Receiver Tones



Advanced Multicast Settings

Current multicast mode: Receiver
Multicast mode can be set in "Basic Settings > Multicast".

Polycom Receiver Tones

If using an Algo device as a Multicast Transmitter, it is recommended to set the Multicast Receiver tones to "None" to avoid conflicts, as the Algo devices already multicast a tone by default.

Group 1	<None>	<Use Default Page Volume>
Group 2	<None>	<Use Default Page Volume>
Group 3	<None>	<Use Default Page Volume>
Group 4	<None>	<Use Default Page Volume>
Group 5	<None>	<Use Default Page Volume>
Group 6	<None>	<Use Default Page Volume>
Group 7	<None>	<Use Default Page Volume>
Group 8	<None>	<Use Default Page Volume>
Group 9	<None>	<Use Default Page Volume>
Group 10	<None>	<Use Default Page Volume>

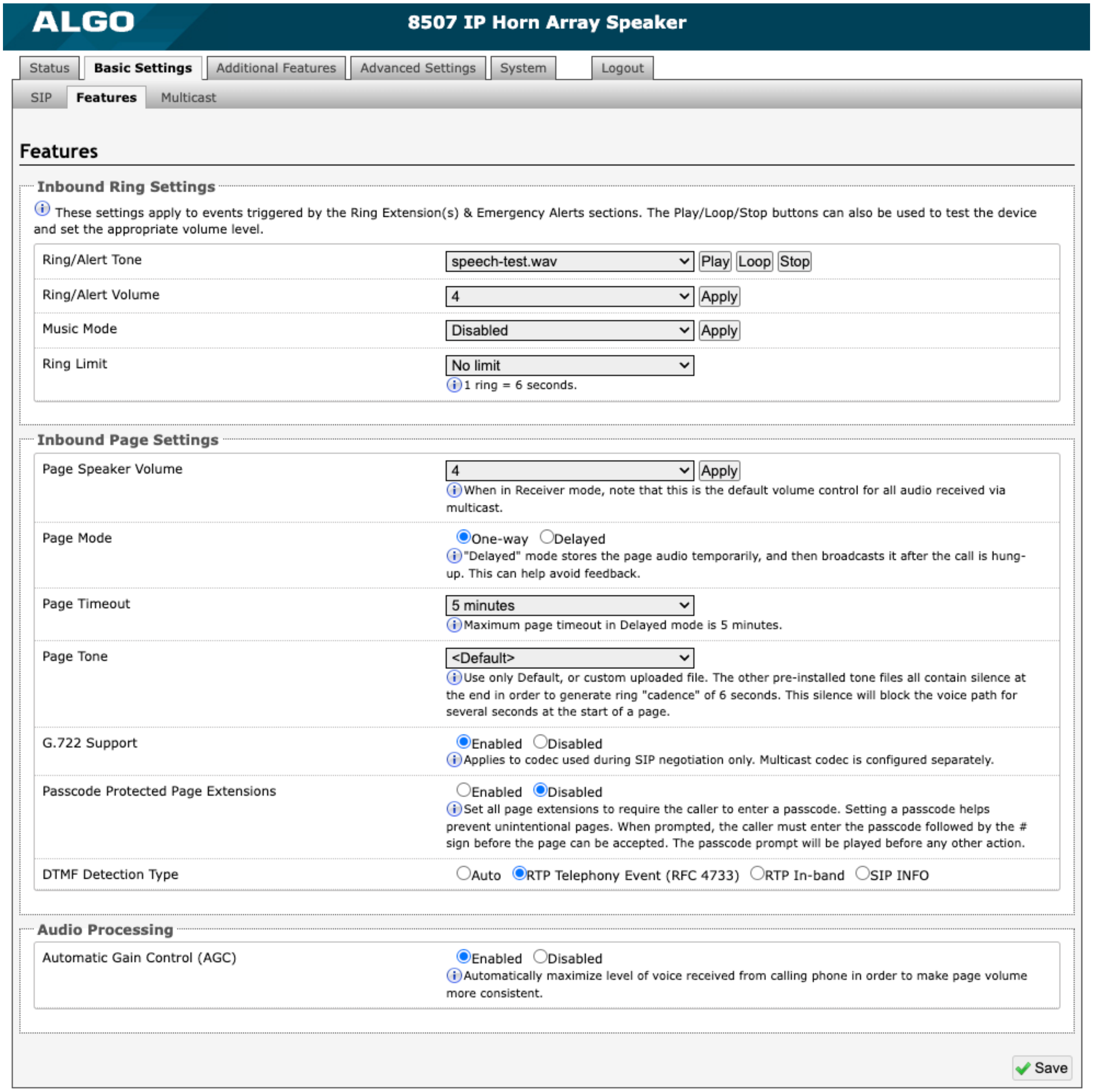
Poly Receiver Tones	Available if under **Basic Settings → Multicast** the **Multicast Mode** is set to **Receiver (Listener)** and **Multicast Type** is set to **Poly Group Page** or **Poly Push-to-Talk**. A tone may be set for any of the 25 Poly Groups. If using an Algo device as a Multicast Transmitter, it is recommended to set the Receiver tones to **None** to avoid conflicts, as the Algo devices already multicast a tone by default.

5 AUDIO CONFIGURATION

In addition to voice paging, the 8507 IP Horn Array Speaker can play audio files for notifications such as emergency alerts, safety and security announcements, or shift changes. Audio files can be stored on the speaker and played in response to an event such as a ring, relay input, or automated schedule.

The 8507 can also connect to a visual alerter or strobe light via multicast to accompany audio notifications.

5.1 Basic Audio Settings



Features

Inbound Ring Settings

ⓘ These settings apply to events triggered by the Ring Extension(s) & Emergency Alerts sections. The Play/Loop/Stop buttons can also be used to test the device and set the appropriate volume level.

Ring/Alert Tone	speech-test.wav [Play] [Loop] [Stop]
Ring/Alert Volume	4 [Apply]
Music Mode	Disabled [Apply]
Ring Limit	No limit ⓘ1 ring = 6 seconds.

Inbound Page Settings

Page Speaker Volume	4 [Apply] ⓘWhen in Receiver mode, note that this is the default volume control for all audio received via multicast.
Page Mode	● One-way ○ Delayed ⓘ"Delayed" mode stores the page audio temporarily, and then broadcasts it after the call is hung-up. This can help avoid feedback.
Page Timeout	5 minutes ⓘMaximum page timeout in Delayed mode is 5 minutes.
Page Tone	<Default> ⓘUse only Default, or custom uploaded file. The other pre-installed tone files all contain silence at the end in order to generate ring "cadence" of 6 seconds. This silence will block the voice path for several seconds at the start of a page.
G.722 Support	● Enabled ○ Disabled ⓘApplies to codec used during SIP negotiation only. Multicast codec is configured separately.
Passcode Protected Page Extensions	○ Enabled ● Disabled ⓘSet all page extensions to require the caller to enter a passcode. Setting a passcode helps prevent unintentional pages. When prompted, the caller must enter the passcode followed by the # sign before the page can be accepted. The passcode prompt will be played before any other action.
DTMF Detection Type	○ Auto ● RTP Telephony Event (RFC 4733) ○ RTP In-band ○ SIP INFO

Audio Processing

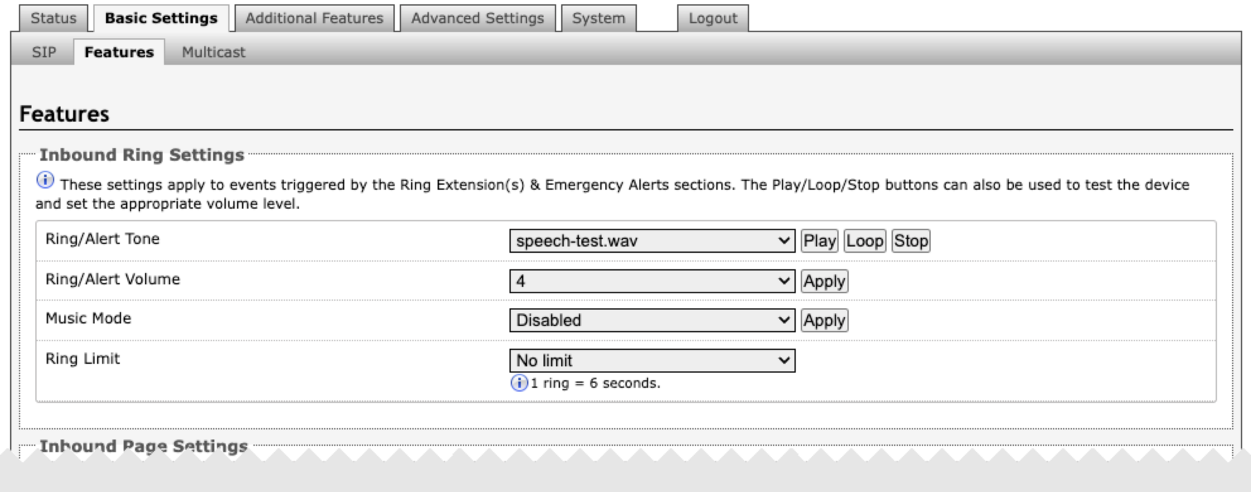
Automatic Gain Control (AGC)	● Enabled ○ Disabled ⓘAutomatically maximize level of voice received from calling phone in order to make page volume more consistent.

✓ Save

Figure 16: Basic Settings → Features.

Inbound Ring Settings

Ring settings apply to events triggered by Ring Extensions and Emergency Alerts. Emergency Alert tones are configured under **Additional Features → Emergency Alerts**.



Features

Inbound Ring Settings

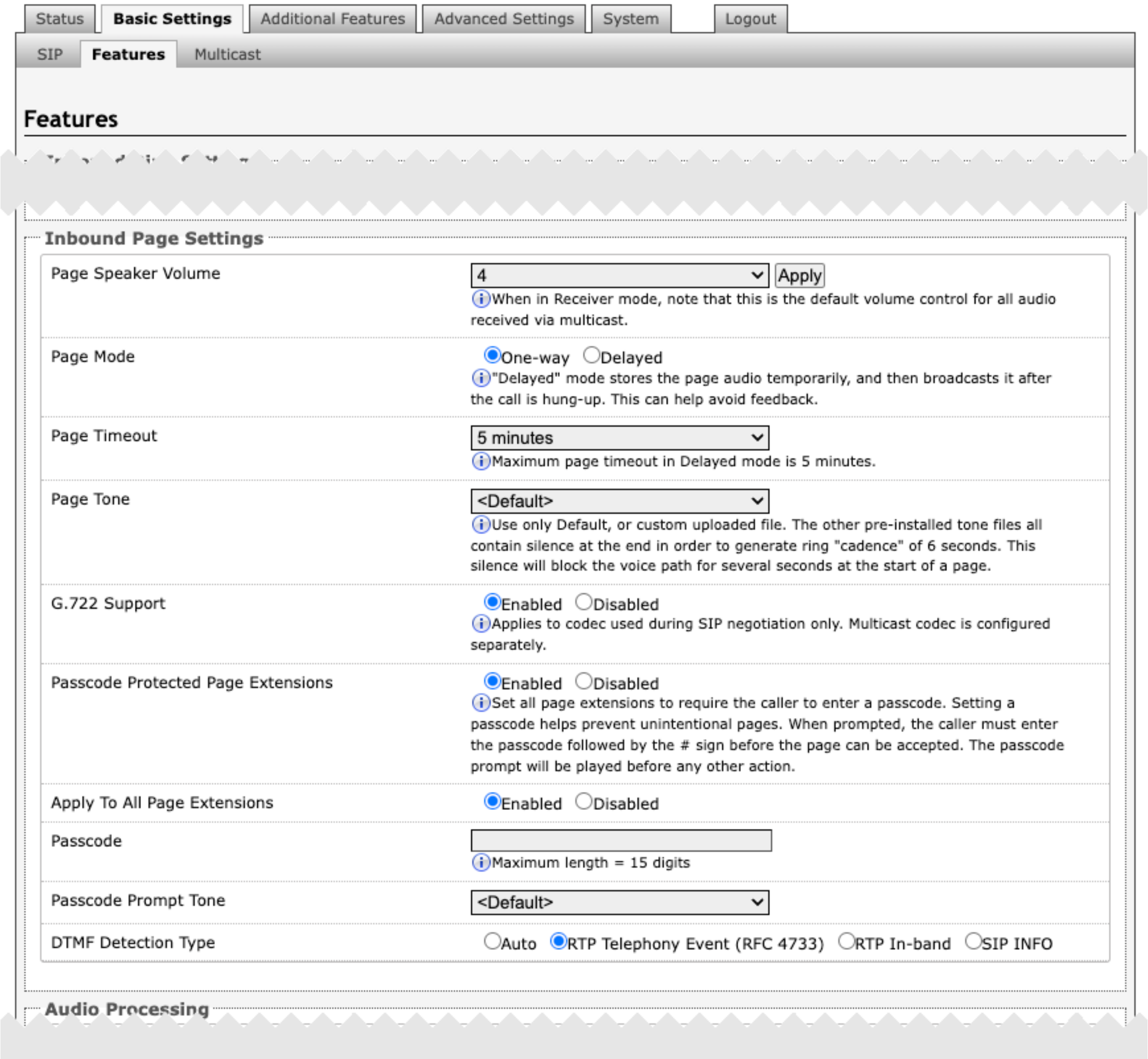
ⓘ These settings apply to events triggered by the Ring Extension(s) & Emergency Alerts sections. The Play/Loop/Stop buttons can also be used to test the device and set the appropriate volume level.

Ring/Alert Tone	speech-test.wav [Play] [Loop] [Stop]
Ring/Alert Volume	4 [Apply]
Music Mode	Disabled [Apply]
Ring Limit	No limit ⓘ 1 ring = 6 seconds.

Inbound Page Settings

Ring/Alert Tone	Select an audio file to play when a ring event is detected on the SIP Ring Extension. Test the audio file immediately using the Play, Loop, and Stop buttons. During multicast, the device will broadcast an audio stream using the Transmitter's selected ringtone. This is the default tone that will be played if selected in the settings **Multicast → Additional Ring Extension**.
Ring/Alert Volume	Set the volume for a SIP Ring event using the dropdown. This setting is for gain control and the output level depends on the levels recorded into the source audio file played from memory. This setting is only used for local tones, not multicast. See Page Speaker Volume below for multicast settings.
Ring Limit	Typically set to no limit. Ring Limit will limit how long the speaker will ring before timing out. A new ring event must occur for the speaker to play the audio file again.

Inbound Page Settings



Features

Inbound Page Settings

Page Speaker Volume	4 [Apply] ⓘWhen in Receiver mode, note that this is the default volume control for all audio received via multicast.
Page Mode	● One-way ○ Delayed ⓘ"Delayed" mode stores the page audio temporarily, and then broadcasts it after the call is hung-up. This can help avoid feedback.
Page Timeout	5 minutes ⓘMaximum page timeout in Delayed mode is 5 minutes.
Page Tone	<Default> ⓘUse only Default, or custom uploaded file. The other pre-installed tone files all contain silence at the end in order to generate ring "cadence" of 6 seconds. This silence will block the voice path for several seconds at the start of a page.
G.722 Support	● Enabled ○ Disabled ⓘApplies to codec used during SIP negotiation only. Multicast codec is configured separately.
Passcode Protected Page Extensions	● Enabled ○ Disabled ⓘSet all page extensions to require the caller to enter a passcode. Setting a passcode helps prevent unintentional pages. When prompted, the caller must enter the passcode followed by the # sign before the page can be accepted. The passcode prompt will be played before any other action.
Apply To All Page Extensions	● Enabled ○ Disabled
Passcode	ⓘMaximum length = 15 digits
Passcode Prompt Tone	<Default>
DTMF Detection Type	○ Auto ● RTP Telephony Event (RFC 4733) ○ RTP In-band ○ SIP INFO

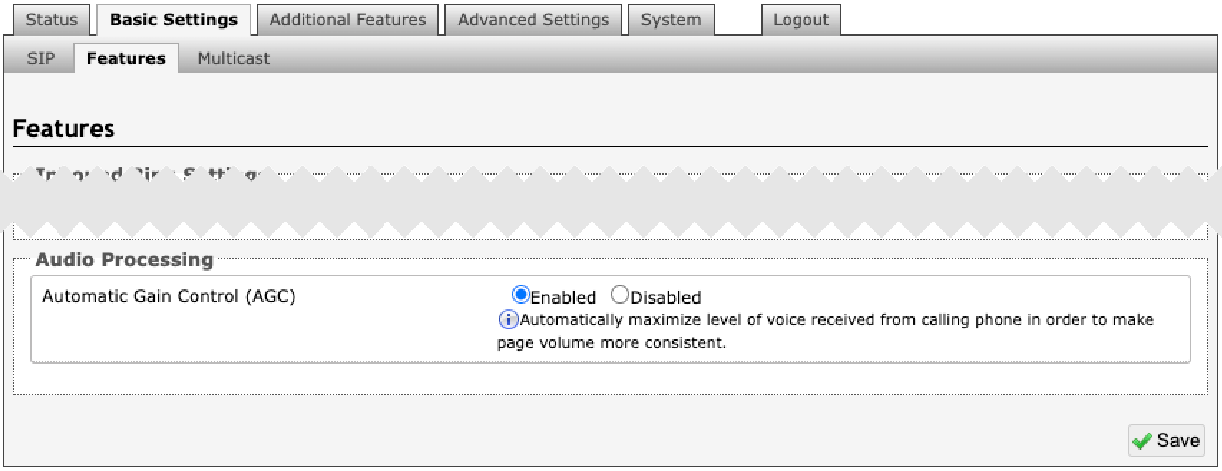
Audio Processing

Page Speaker Volume	This setting is for gain control for SIP or multicast paging. The output level will depend on the streaming level. Page Speaker Volume will apply to all inbound multicast streams (for Receiver mode only) regardless of audio source or type.
Page Mode	Set calls to the SIP page extension as one-way, two-way (using an external microphone), or delayed. In delayed mode, the speaker will record a message to be played after disconnecting. The device will buffer an announcement up to 5 minutes long. To cancel a page while in delay mode, press "*" while recording to prevent it from being sent after hanging up.

Page Timeout	Set the maximum duration for a page. The page will end when the timeout limit has been reached. This is useful to ensure the paging system is not stuck in an active state in cases where someone accidentally forgets to hang up.
Page Tone	Select a pre-page tone to be played when a page is starting. Use only the Default or custom uploaded files. Other pre-installed tone files contain silence at the end to generate a ring "cadence" of 6 seconds. This silence will block the voice path for several seconds at the start of a page. The “Default” tone is set to page-notif.wav. The **Default Page Tone** in **Advanced Multicast** will play the tone set here.
G.722 Support	Enable or disable the G.722 codec. G.722 enables wideband audio for optimum speech intelligibility.
Passcode Protected Page Extensions	When **Enabled**, the caller must enter the set passcode followed by the # sign before the page can be made. Setting a passcode helps prevent unintentional pages.
Apply to All Page Extensions	Only visible when **Passcode Protected Page Extensions** is set to **Enabled**. Enable or disable a passcode for all page extensions.
Passcode	Only visible when **Passcode Protected Page Extensions** is set to **Enabled**. Passcodes can be up to 15 digits and must be numbers only.
Passcode Prompt Tone	Only visible when **Passcode Protected Page Extensions** is set to **Enabled**. Select the tone to be played to prompt the user to enter the passcode before paging.
DTMF Detection Type	Select the preferred dual-tone multi-frequency (DTMF) detection method. DTMF is a technology used with touch-tone phones (the sound made when pressing a number key). The device uses this for multi-zone selection, passcode, etc.

<table>
<tr><td colspan="2">

Audio Processing



Features

Audio Processing

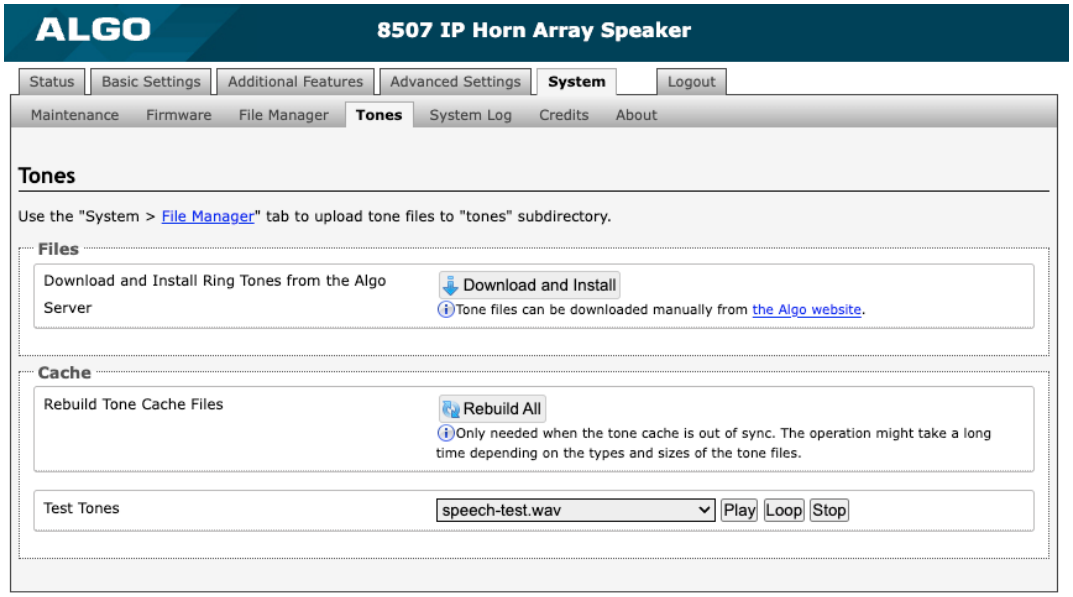
Automatic Gain Control (AGC) ● Enabled ○ Disabled

Automatically maximize level of voice received from calling phone in order to make page volume more consistent.

</td></tr>
<tr><td>Automatic Gain Control (AGC)</td><td>Enable or disable AGC to normalize the audio level. Enabling ensures the speaker is always played at a consistent volume.</td></tr>
</table>

5.2 Tones

The 8507 includes several pre-loaded audio files that can be selected to play for various events. The web interface allows you to select a file and play it immediately over the speaker for testing, which is available in **Basic Settings → Features**. Files may also be added, deleted, or renamed. For more information, see section 8.8 File Manager.



Tones

Use the "System > File Manager" tab to upload tone files to "tones" subdirectory.

Files

Download and Install Ring Tones from the Algo Server — Tone files can be downloaded manually from the Algo website.

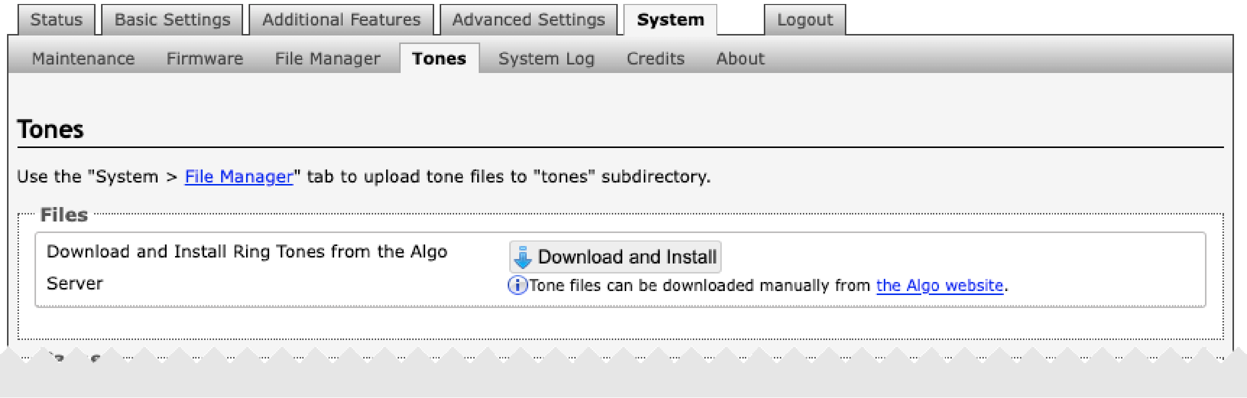
Cache

Rebuild Tone Cache Files — Only needed when the tone cache is out of sync. The operation might take a long time depending on the types and sizes of the tone files.

Test Tones: speech-test.wav

Figure 17: Configure tone settings in the web interface.

Files



Tones

Use the "System > File Manager" tab to upload tone files to "tones" subdirectory.

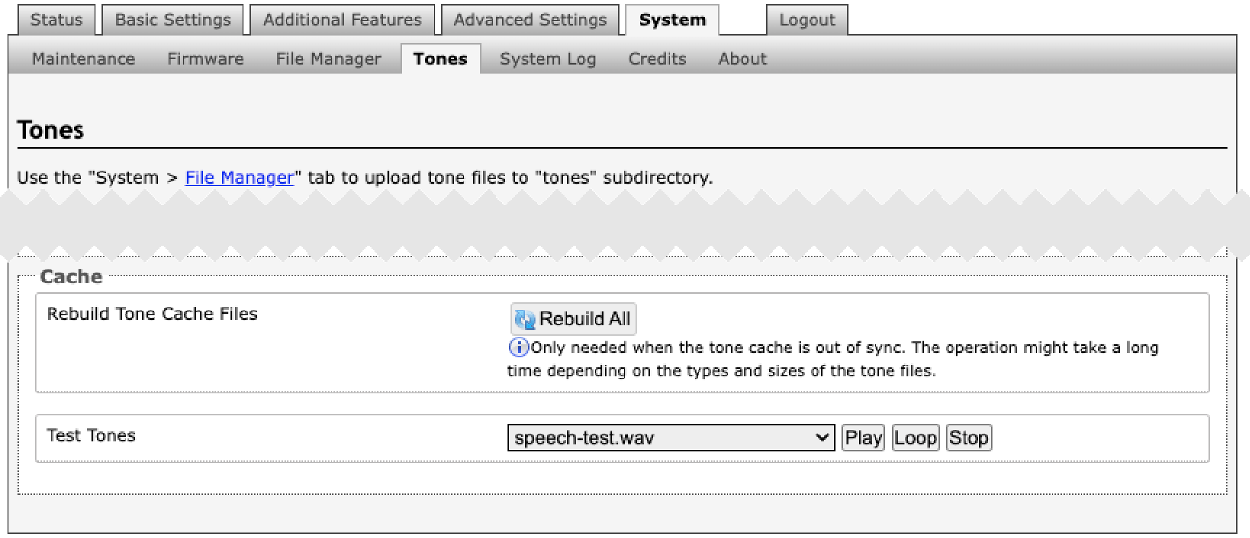
Files

Download and Install Ring Tones from the Algo Server

ⓘTone files can be downloaded manually from the Algo website.

Download and Install Ring Tones from the Algo Server	Tone files can be downloaded manually from the Algo website.

Cache



Tones

Use the "System > File Manager" tab to upload tone files to "tones" subdirectory.

Cache

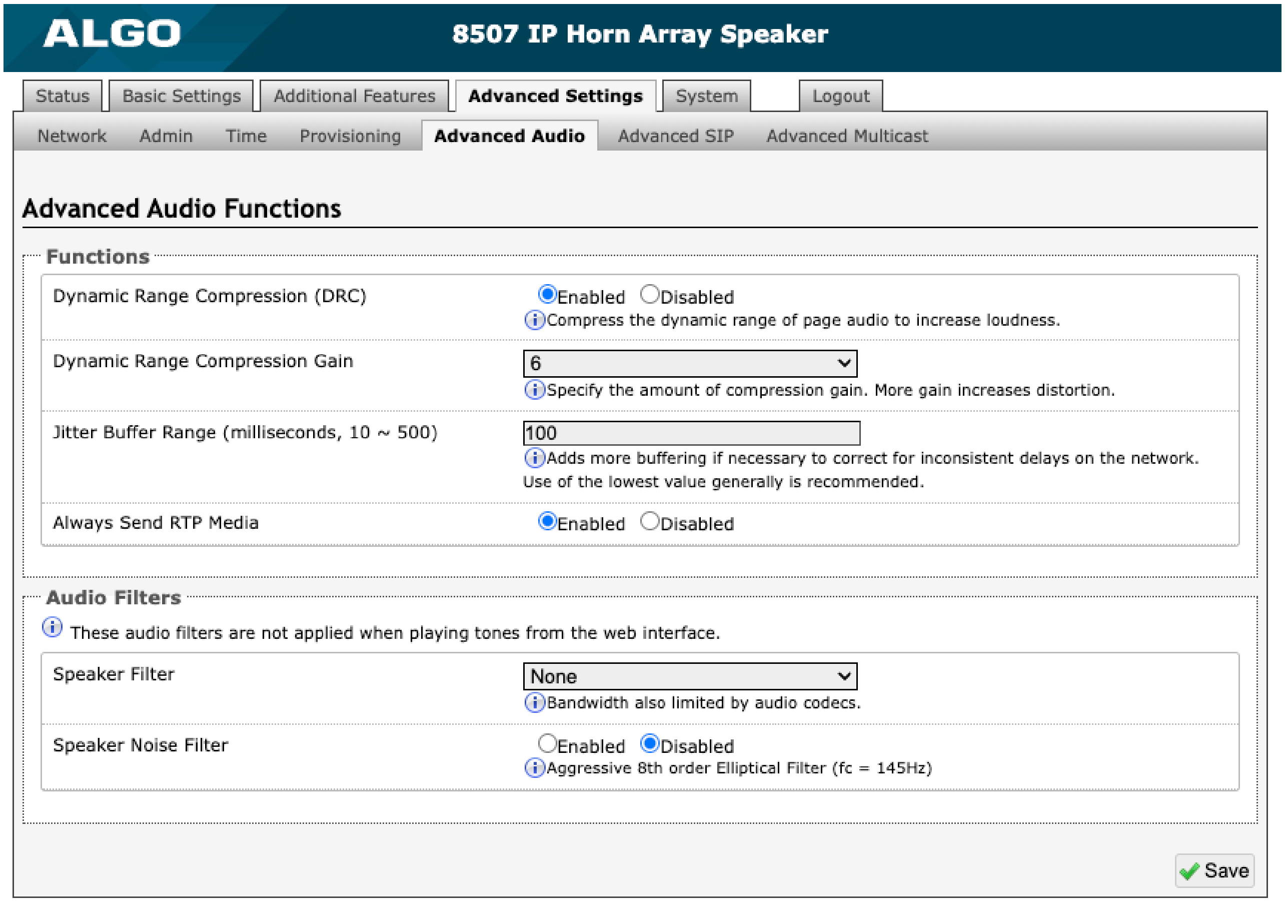
Rebuild Tone Cache Files

ⓘOnly needed when the tone cache is out of sync. The operation might take a long time depending on the types and sizes of the tone files.

Test Tones: speech-test.wav

Rebuild Tone Cache Files	Only needed when the tone cache is out of sync. The operation might take a long time, depending on the types and sizes of the tone files.
Test Tones	Listen to uploaded audio files before selecting them for your system.

5.3 Advanced Audio



Advanced Audio Functions

Functions

Dynamic Range Compression (DRC)	● Enabled ○ Disabled Compress the dynamic range of page audio to increase loudness.
Dynamic Range Compression Gain	6 Specify the amount of compression gain. More gain increases distortion.
Jitter Buffer Range (milliseconds, 10 ~ 500)	100 Adds more buffering if necessary to correct for inconsistent delays on the network. Use of the lowest value generally is recommended.
Always Send RTP Media	● Enabled ○ Disabled

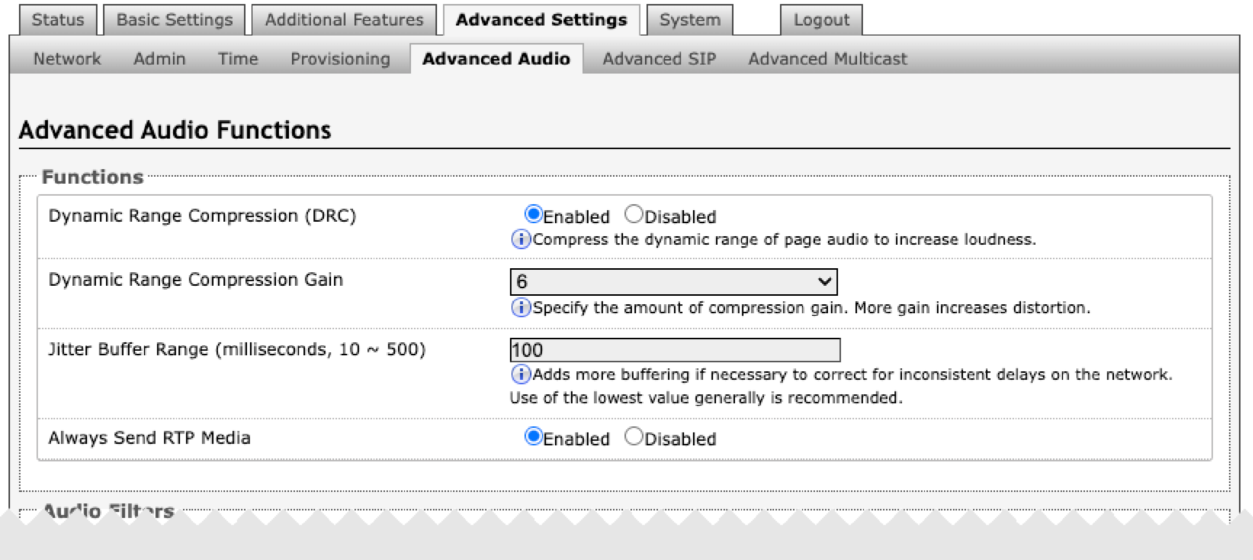
Audio Filters

These audio filters are not applied when playing tones from the web interface.

Speaker Filter	None Bandwidth also limited by audio codecs.
Speaker Noise Filter	○ Enabled ● Disabled Aggressive 8th order Elliptical Filter (fc = 145Hz)

Figure 18: Configure advanced audio settings in the web interface.

Functions



Advanced Audio Functions

Functions

Dynamic Range Compression (DRC) ● Enabled ○ Disabled
ⓘ Compress the dynamic range of page audio to increase loudness.

Dynamic Range Compression Gain: 6
ⓘ Specify the amount of compression gain. More gain increases distortion.

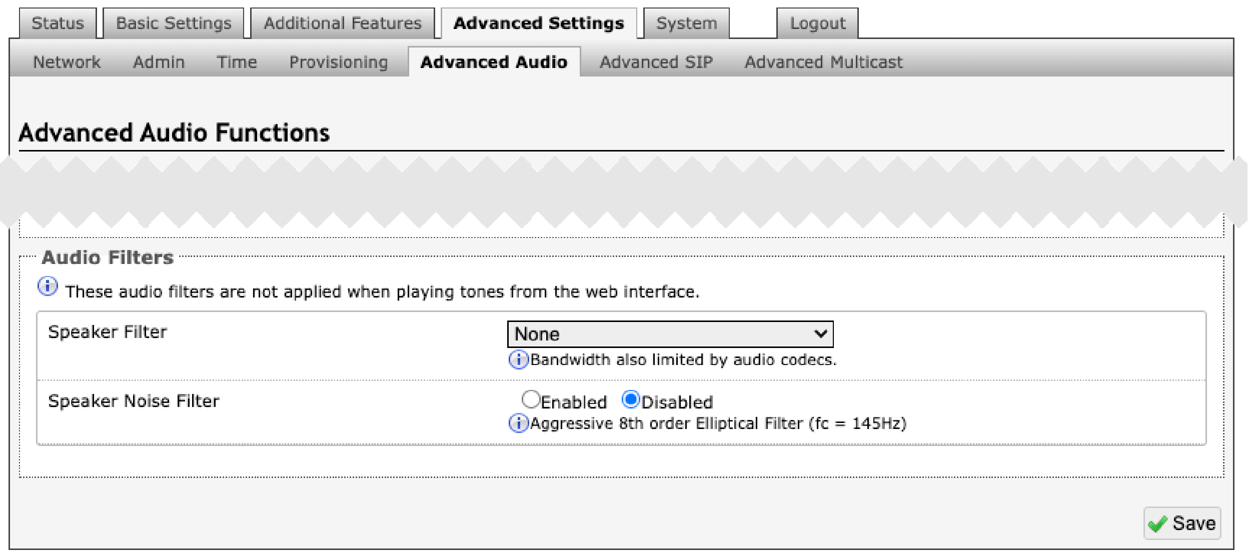
Jitter Buffer Range (milliseconds, 10 ~ 500): 100
ⓘ Adds more buffering if necessary to correct for inconsistent delays on the network. Use of the lowest value generally is recommended.

Always Send RTP Media ● Enabled ○ Disabled

Audio Filters

Dynamic Range Compression (DRC)	Enable to compress the dynamic range of page audio to increase loudness.
Dynamic Range Compression Gain	Select the amount of compression gain from the dropdown menu. More gain increases distortion.
Jitter Buffer Range	Enter a value between 10-500 to add more buffering if necessary to correct for inconsistent delays on the network. It is recommended to use the lowest value.
Always Send RTP Media	Enable to send audio packets at all times, even during one-way paging mode. This option is needed when the server expects to always see audio packets.

Audio Filters



Advanced Audio Functions

Audio Filters

ⓘ These audio filters are not applied when playing tones from the web interface.

Speaker Filter: None
ⓘBandwidth also limited by audio codecs.

Speaker Noise Filter: ○Enabled ●Disabled
ⓘAggressive 8th order Elliptical Filter (fc = 145Hz)

Speaker Filter	Select a frequency from the dropdown to apply a high-pass filter to the speaker output. This setting reduces audio artifacts like humming or buzzing by filtering out unwanted frequencies.
Speaker Noise Filter	Enable to filter below 145 Hz to reduce mains-induced noise like fans.

6 INTEGRATION

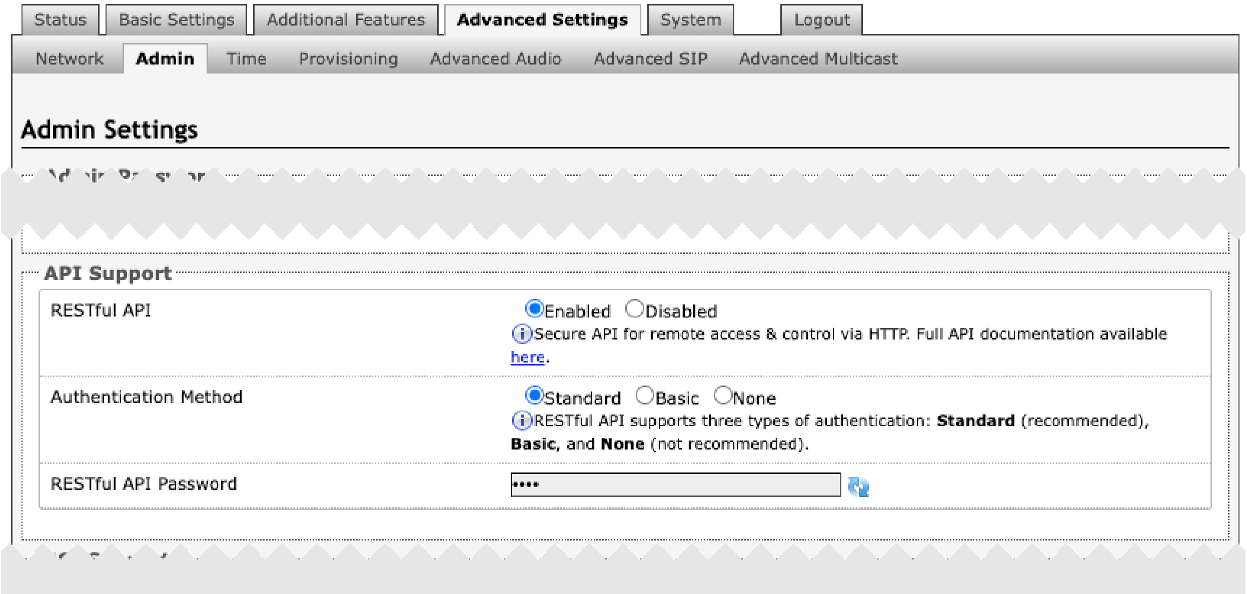
6.1 API

Algo RESTful API can be used to access, manipulate, and trigger Algo endpoints on your network through HTTP/HTTPS requests.

Requesting systems can interact with Algo devices through a uniform and predefined set of stateless operations. See the Algo RESTful API Guide for more details.

To configure API settings on your 8507 IP Horn Array Speaker, use the web interface and navigate to **Advanced Settings → Admin → API Support**.

API Support



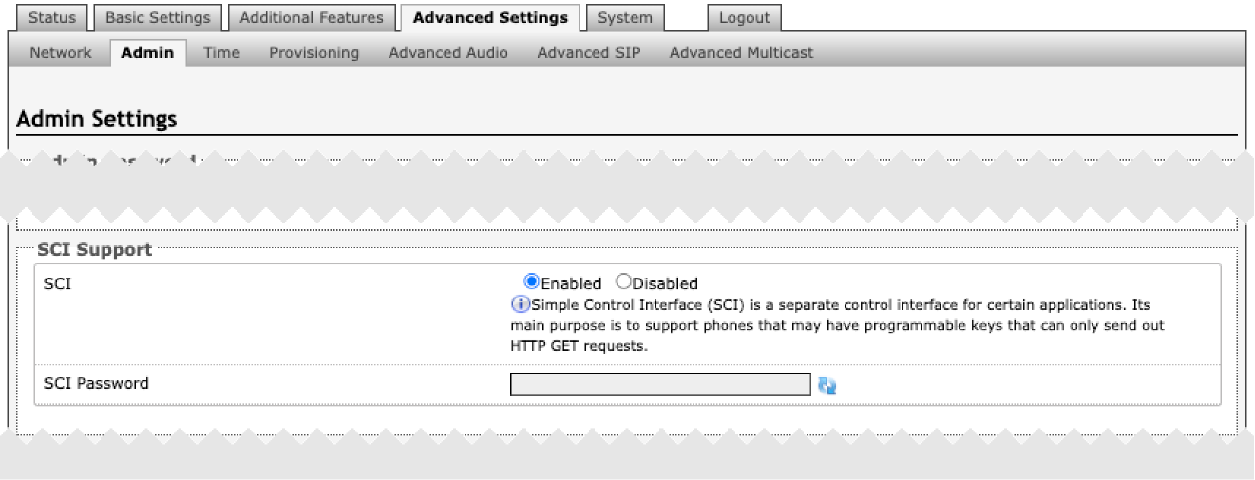
Admin Settings

API Support

RESTful API	● Enabled ○ Disabled Secure API for remote access & control via HTTP. Full API documentation available here.
Authentication Method	● Standard ○ Basic ○ None RESTful API supports three types of authentication: **Standard** (recommended), **Basic**, and **None** (not recommended).
RESTful API Password	••••

RESTful API	Enable a secure API for remote access and device control via HTTP. For more information, see the Algo RESTful API Guide.
Authentication Method	Speak to your IT Administrator for more information.
RESTful API Password	Speak to your IT Administrator for more information.

SCI Support



Admin Settings

SCI Support

SCI ● Enabled ○ Disabled

Simple Control Interface (SCI) is a separate control interface for certain applications. Its main purpose is to support phones that may have programmable keys that can only send out HTTP GET requests.

SCI Password

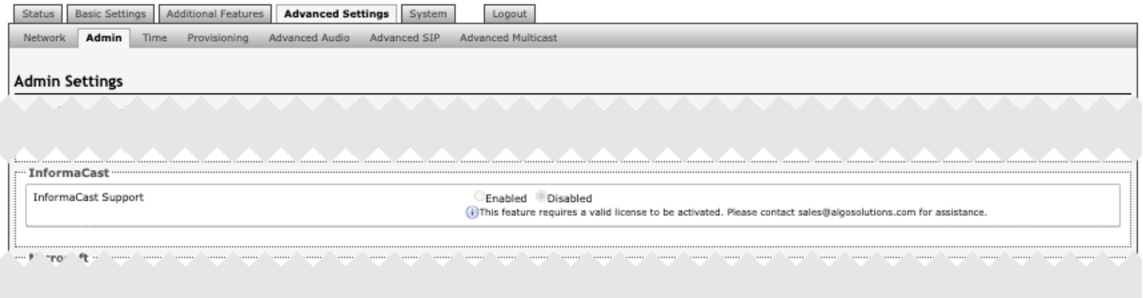
SCI	Simple Control Interface (SCI) is a separate control interface for certain applications. Its primary purpose is to support phones that may have programmable keys that can only send out HTTP GET requests.

6.2 InformaCast

As a Singlewire Solutions Partner, Algo products have been certified for compatibility and interoperability.

To set up your device with Informacast, use the web interface and navigate to **Advanced Settings → Admin → InformaCast**.

InformaCast



Admin Settings

InformaCast

InformaCast Support ○ Enabled ● Disabled

This feature requires a valid license to be activated. Please contact sales@algosolutions.com for assistance.

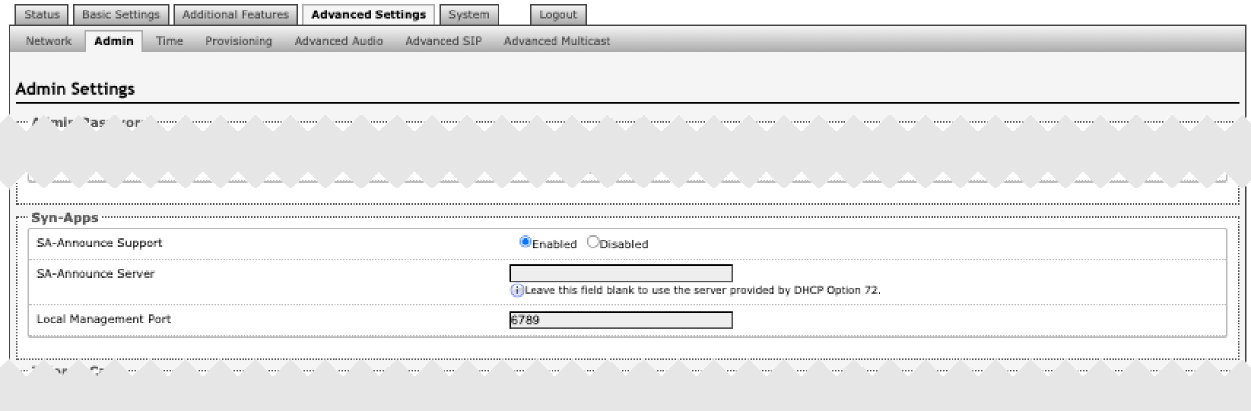
InformaCast Support	This feature requires a valid InformaCast license to be activated. Please contact sales@algosolutions.com for assistance.

6.3 Syn-Apps

As a Syn-Apps Partner, Algo products have been Syn-Apps Certified for compatibility and interoperability.

Syn-Apps

The SA-Announce feature cannot be used when Multicast Transmitter mode or Poly mode is enabled. To enable SA-Announce mode, set **Multicast Mode** to **None** in **Basic Settings → Multicast**.



Admin Settings

Syn-Apps

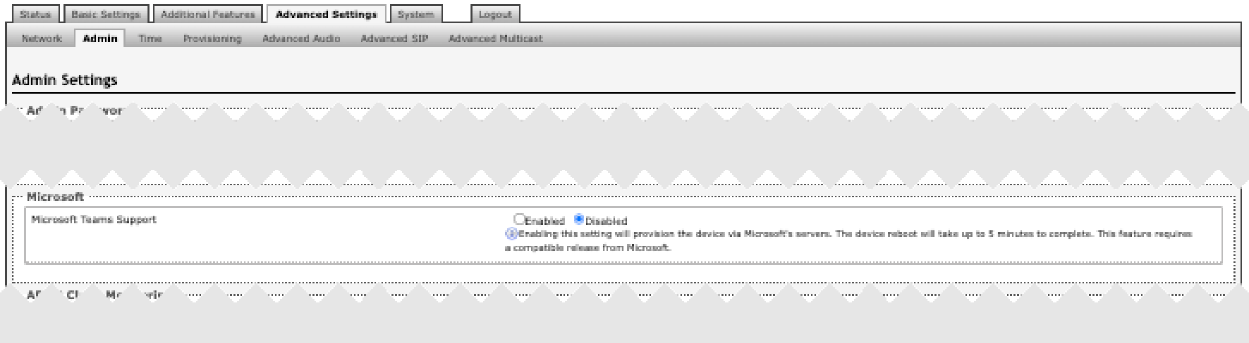
SA-Announce Support	● Enabled ○ Disabled
SA-Announce Server	Leave this field blank to use the server provided by DHCP Option 72.
Local Management Port	6789

SA-Announce Support	Enable to convert unicast streams to multicast and deliver them to the target endpoints.
SA-Announce Server	Enter the SA-Announce Server to use the Syn-Apps paging feature. Leave the field blank to use the server provided by the DHCP Option 72.
Local Management Port	Enter the local management port for the SA-Announce Server.

6.4 Microsoft Teams

Algo devices are certified by and compatible with Microsoft Teams. When registered in the Microsoft Teams SIP Gateway, the 8507 can be configured to deliver Teams-based communication throughout facilities.

Microsoft



Admin Settings

Microsoft

Microsoft Teams Support ○Enabled ●Disabled

Enabling this setting will provision the device via Microsoft's servers. The device reboot will take up to 5 minutes to complete. This feature requires a compatible release from Microsoft.

Microsoft Teams Support	Enable to provision the device via Microsoft's servers. The device reboot will take up to 5 minutes to complete, as the device will communicate several times with the Microsoft server. This feature requires a compatible release from Microsoft.

7 DEVICE MANAGEMENT

7.1 ADMP

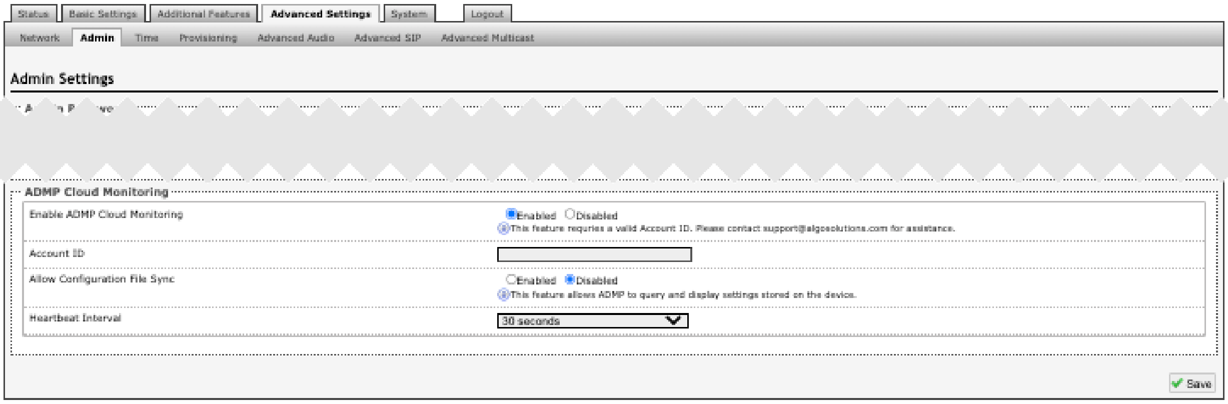
The Algo Device Management Platform (ADMP) is a cloud-based device management solution to manage, monitor, and configure Algo IP endpoints from any location. Devices can be easily grouped via a tagging functionality, allowing devices to be coded by district, department, or function to easily oversee many devices. Devices can be supervised for connectivity and email-based notifications can be sent should devices go offline, allowing for a real-time overview of device status.

To connect your device to your ADMP account, use the web interface and navigate to **Advanced Settings → Admin → ADMP Cloud Monitoring**.

Note that if you choose to use ADMP to manage your devices, the Algo 8300 IP Controller cannot be used at the same time.

To learn more about ADMP and how to purchase a license, visit the website.

ADMP Cloud Monitoring



Admin Settings

ADMP Cloud Monitoring

Enable ADMP Cloud Monitoring ● Enabled ○ Disabled
This feature requries a valid Account ID. Please contact support@algosolutions.com for assistance.

Account ID

Allow Configuration File Sync ○ Enabled ● Disabled
This feature allows ADMP to query and display settings stored on the device.

Heartbeat Interval 30 seconds

Enable ADMP Cloud Monitoring	The Algo Device Management Platform (ADMP) simplifies the process of managing, monitoring, and maintaining Algo devices from any location. This feature requires a valid Account ID. To learn more about ADMP and how to purchase a license, visit the website.

7.2 Algo 8300 IP Controller

The Algo 8300 IP Controller is designed for centralized on-premise or local network Algo endpoint monitoring and supervision. Any Algo SIP endpoint device, including the 8507, can be monitored on the network via the 8300 dashboard.

Note that if you choose to use the Algo 8300 IP Controller to manage your devices, ADMP cannot be used at the same time.

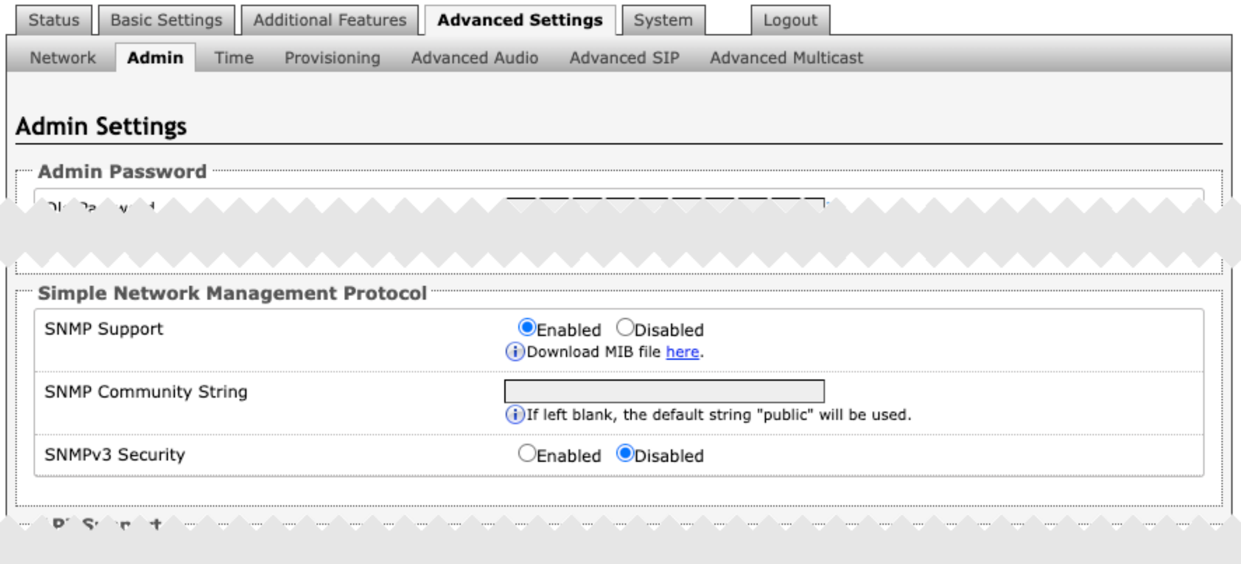
Learn more about the Algo 8300 IP Controller.

7.3 SNMP

Simple Network Management Protocol (SNMP) can be used to monitor and manage the 8507.

To configure your SNMP settings, use the web interface and navigate to **Advanced Settings → Admin → Simple Network Management Protocol**.

Simple Network Management Protocol



Admin Settings

Admin Password

Simple Network Management Protocol

SNMP Support ● Enabled ○ Disabled
ⓘ Download MIB file here.

SNMP Community String
ⓘ If left blank, the default string "public" will be used.

SNMPv3 Security ○ Enabled ● Disabled

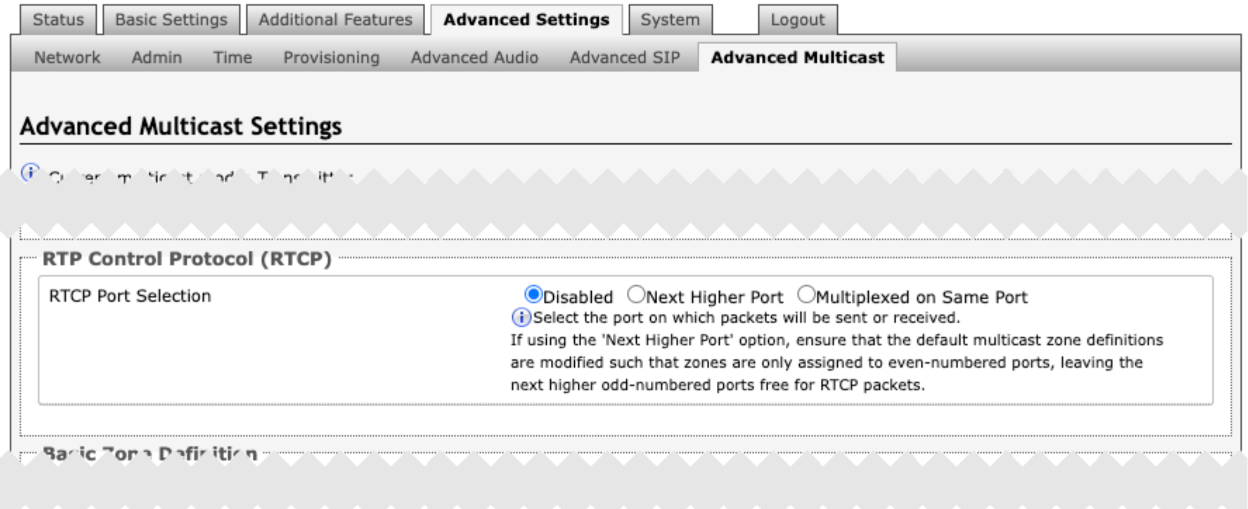
SNMP Support	The existing setting will respond to a simple status query for automated supervision.
SNMP Community String	Speak to your IT Administrator for more information.
SNMPv3 Security	Speak to your IT Administrator for more information.

7.4 RTCP

Real-Time Transport Control Protocol (RTCP) can be used to monitor data delivery on the 8507.

To configure your RTCP settings, use the web interface and navigate to **Advanced Settings → Admin → RTP Control Protocol (RTCP)**.

RTP Control Protocol (RTCP)



Advanced Multicast Settings

RTP Control Protocol (RTCP)

RTCP Port Selection ● Disabled ○ Next Higher Port ○ Multiplexed on Same Port

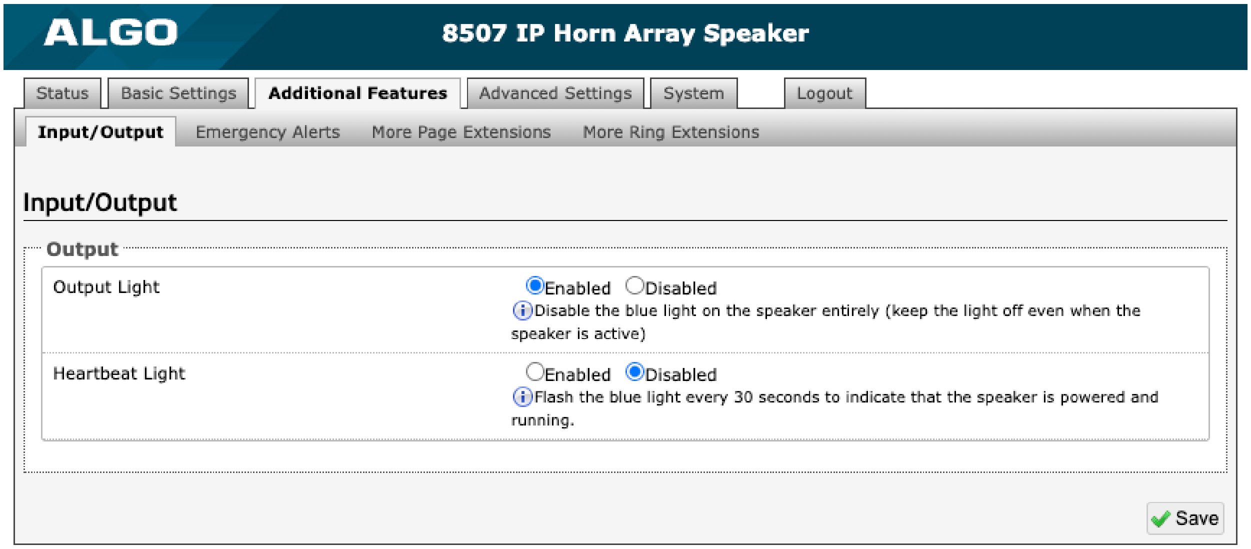
Select the port on which packets will be sent or received.
If using the 'Next Higher Port' option, ensure that the default multicast zone definitions are modified such that zones are only assigned to even-numbered ports, leaving the next higher odd-numbered ports free for RTCP packets.

RTCP Port Selection	Select how a port will be chosen to send or receive RTCP packets. Note: If **Next Higher Port** is selected, ensure that the default multicast zone definitions are modified so that zones are only assigned to even-numbered ports, leaving the next higher odd-numbered ports free for RTCP packets.

8 SYSTEM CONFIGURATION

8.1 Input/Output

Output



Input/Output

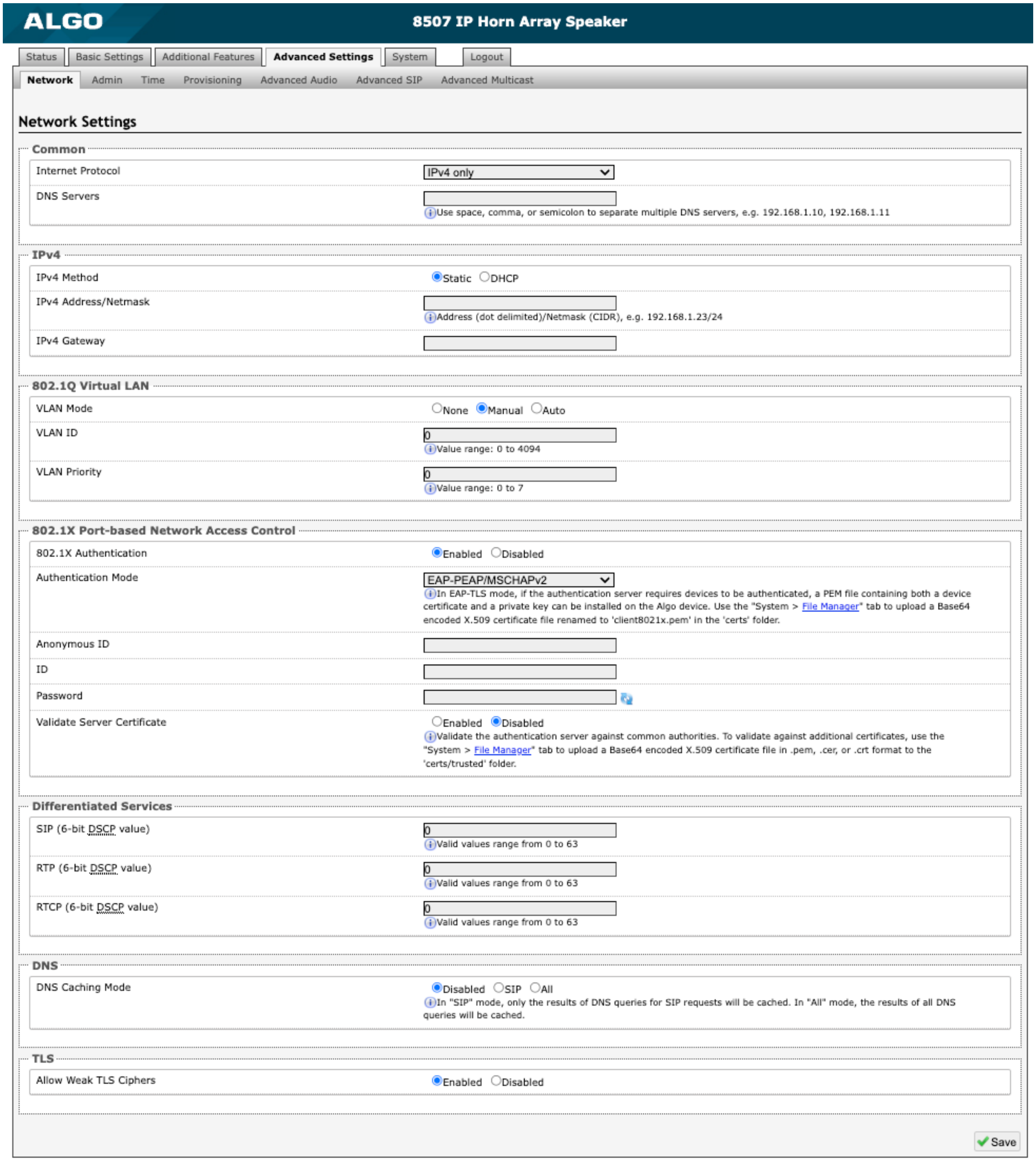
Output

Output Light ● Enabled ○ Disabled
Disable the blue light on the speaker entirely (keep the light off even when the speaker is active)

Heartbeat Light ○ Enabled ● Disabled
Flash the blue light every 30 seconds to indicate that the speaker is powered and running.

Output Light	Enable or disable the backlight on the button. If disabled, the light remains off even when the speaker is active.
Heartbeat Light	Enable this feature to have the blue light flash every 30 seconds. This is used to indicate that the speaker is powered and running. Note this feature is not available if the **Output Light** is disabled.

8.2 Network Settings



Network Settings

Common

Internet Protocol	IPv4 only
DNS Servers	Use space, comma, or semicolon to separate multiple DNS servers, e.g. 192.168.1.10, 192.168.1.11

IPv4

IPv4 Method	● Static ○ DHCP
IPv4 Address/Netmask	Address (dot delimited)/Netmask (CIDR), e.g. 192.168.1.23/24
IPv4 Gateway	

802.1Q Virtual LAN

VLAN Mode	○ None ● Manual ○ Auto
VLAN ID	0 Value range: 0 to 4094
VLAN Priority	0 Value range: 0 to 7

802.1X Port-based Network Access Control

802.1X Authentication	● Enabled ○ Disabled
Authentication Mode	EAP-PEAP/MSCHAPv2 In EAP-TLS mode, if the authentication server requires devices to be authenticated, a PEM file containing both a device certificate and a private key can be installed on the Algo device. Use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file renamed to 'client8021x.pem' in the 'certs' folder.
Anonymous ID	
ID	
Password	
Validate Server Certificate	○ Enabled ● Disabled Validate the authentication server against common authorities. To validate against additional certificates, use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder.

Differentiated Services

SIP (6-bit DSCP value)	0 Valid values range from 0 to 63
RTP (6-bit DSCP value)	0 Valid values range from 0 to 63
RTCP (6-bit DSCP value)	0 Valid values range from 0 to 63

DNS

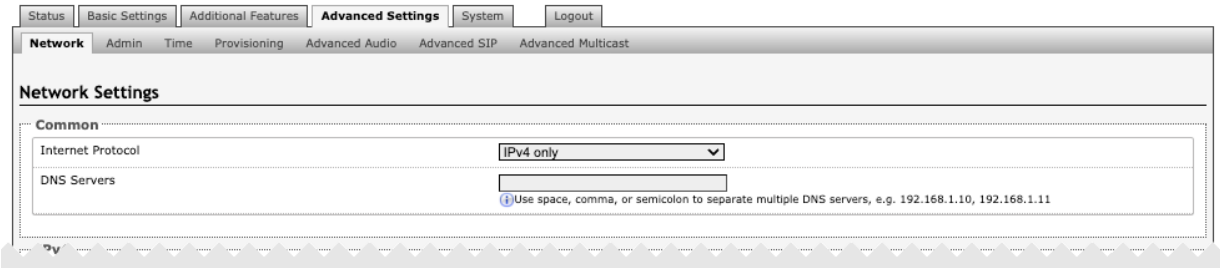
DNS Caching Mode	● Disabled ○ SIP ○ All In "SIP" mode, only the results of DNS queries for SIP requests will be cached. In "All" mode, the results of all DNS queries will be cached.

TLS

Allow Weak TLS Ciphers	● Enabled ○ Disabled

Figure 19: Configure network settings in the web interface.

Common



Network Settings

Common

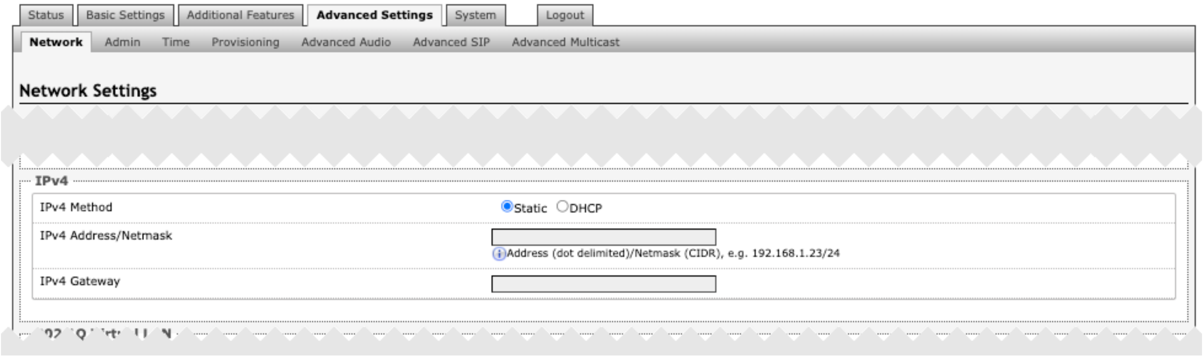
Internet Protocol: IPv4 only

DNS Servers

Use space, comma, or semicolon to separate multiple DNS servers, e.g. 192.168.1.10, 192.168.1.11

Internet Protocol	Use the dropdown to select **IPv4 Only** or **IPv4 and IPv6**. If IPv6 is also configured, it will have to be set up via DHCP or statically, similarly to the IPv4.
DNS Servers	Add one or multiple DNS servers when **Supersede DNS provided by DHCP** is enabled. Separate each server by a space, comma, or semicolon.

IPv4



Network Settings

IPv4

IPv4 Method: ● Static ○ DHCP

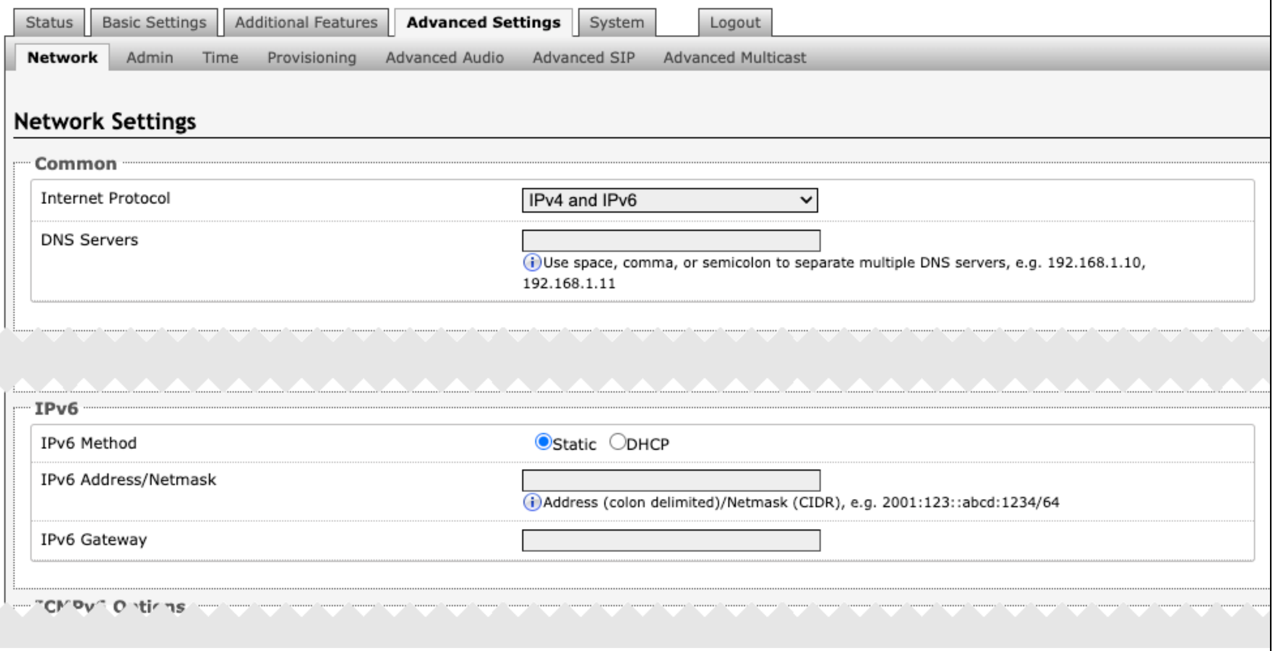
IPv4 Address/Netmask

Address (dot delimited)/Netmask (CIDR), e.g. 192.168.1.23/24

IPv4 Gateway

IPv4 Method	The device can be set to a static or DHCP IP address. DHCP is an IP standard designed to simplify the administration of IP addresses. When selected, **DHCP** will automatically configure IP addresses for each device on the network. DHCP is selected by default. When **Static** is selected, the device will use the IP address entered in the fields below.
IPv4 Address/Netmask	Enter the static IP address and netmask (CIDR format) for the device (e.g., 192.168.1.23/24).
IPv4 Gateway	Enter the gateway address.

IPv6



Status | Basic Settings | Additional Features | **Advanced Settings** | System | Logout

Network | Admin | Time | Provisioning | Advanced Audio | Advanced SIP | Advanced Multicast

Network Settings

Common

Internet Protocol	IPv4 and IPv6
DNS Servers	ⓘUse space, comma, or semicolon to separate multiple DNS servers, e.g. 192.168.1.10, 192.168.1.11

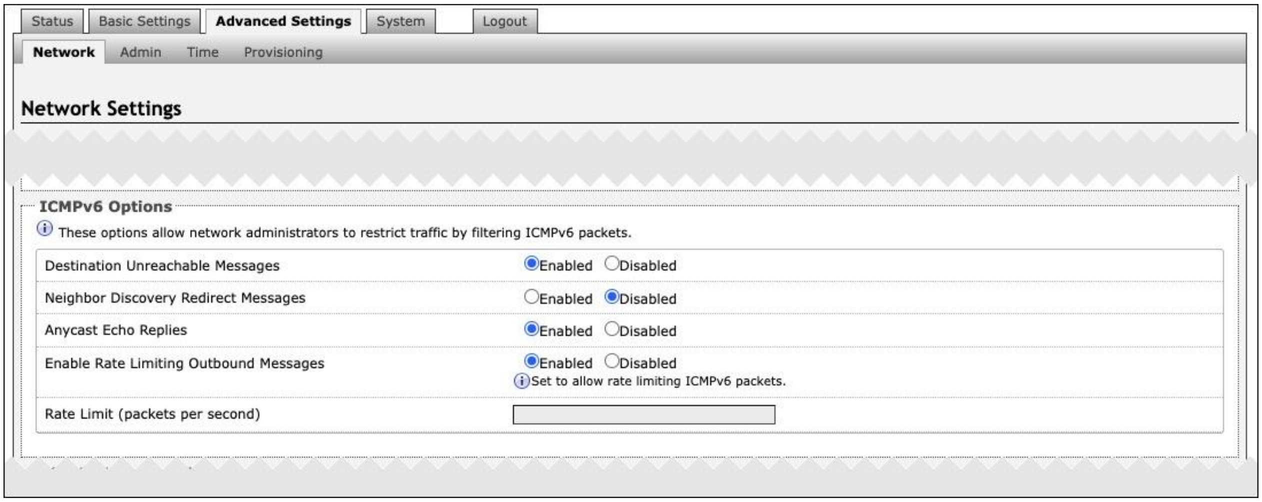
IPv6

IPv6 Method	● Static ○ DHCP
IPv6 Address/Netmask	ⓘAddress (colon delimited)/Netmask (CIDR), e.g. 2001:123::abcd:1234/64
IPv6 Gateway	

ICMPv6 Options

IPv6 Method	The device can be set to a static or DHCP IP address. DHCP is an IP standard designed to simplify the administration of IP addresses. When selected, **DHCP** will automatically configure IP addresses for each device on the network. When **Static** is selected, the device will use the IP address entered in the fields below.
IPv6 Address/Netmask	Enter the static IP address and netmask (CIDR format) for the device (e.g., 2001:123::abcd:1234/64).
IPv6 Gateway	Enter the gateway address.

ICMPv6 Options



Network Settings

ICMPv6 Options

These options allow network administrators to restrict traffic by filtering ICMPv6 packets.

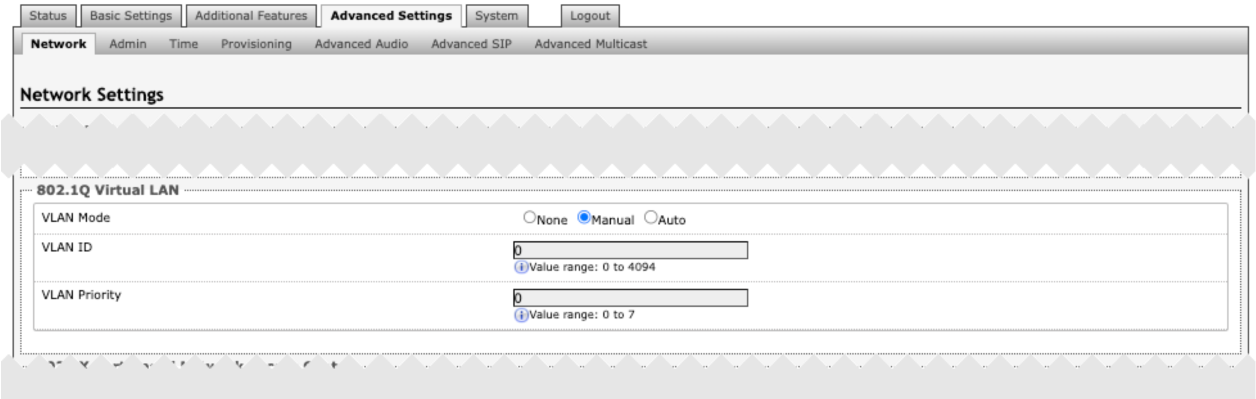
Destination Unreachable Messages	● Enabled ○ Disabled
Neighbor Discovery Redirect Messages	○ Enabled ● Disabled
Anycast Echo Replies	● Enabled ○ Disabled
Enable Rate Limiting Outbound Messages	● Enabled ○ Disabled Set to allow rate limiting ICMPv6 packets.
Rate Limit (packets per second)	

Destination Unreachable messages	Enable to restrict traffic by filtering ICMPv6 packets.
Neighbor Discovery Redirect messages	Enable to restrict traffic by filtering ICMPv6 packets.
Anycast Echo Replies	Enable to restrict traffic by filtering ICMPv6 packets.
Enable Rate Limiting Outbound Messages	Enable to limit the device to respond to other network devices at the specified rate below and prevent it from receiving multiple requests at the same time.
Rate Limit (packets per second)	Specify the packets per second allowed for Rate Limiting Outbound Messages.

802.1Q Virtual LAN

If set, the speaker can be accessed by dialing its assigned extension from a telephone, device, or client. The speaker will auto-answer, play the default pre-announce tone, and allow voice paging until disconnected.

If the device is using VLAN, you will need to be on the same VLAN to access the web interface.



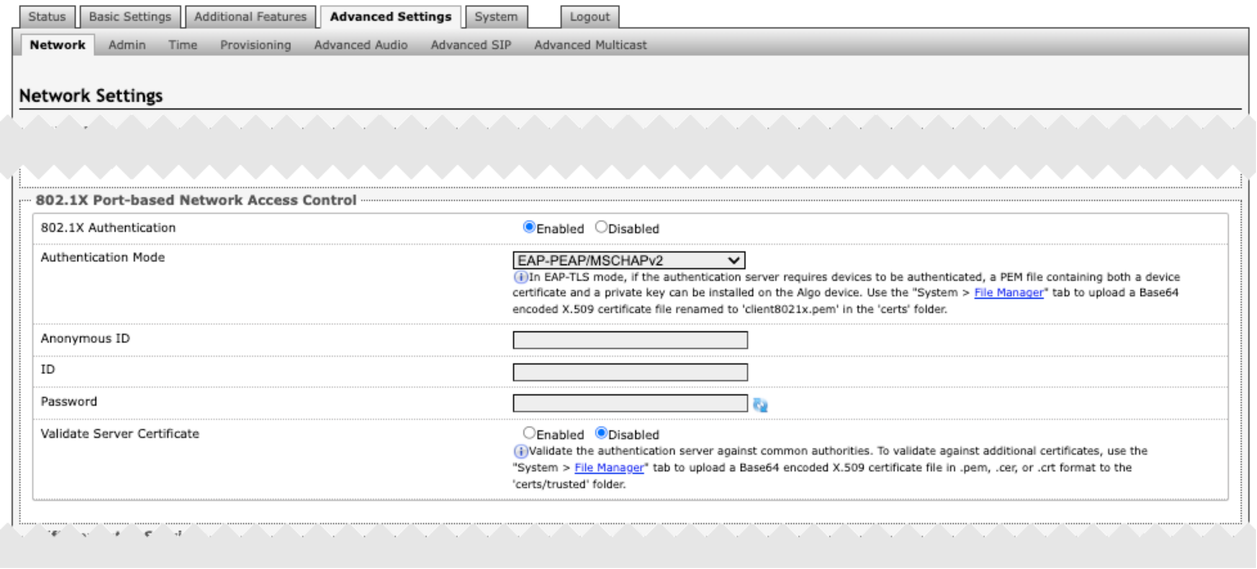
Network Settings

802.1Q Virtual LAN

VLAN Mode	○None ●Manual ○Auto
VLAN ID	0 Value range: 0 to 4094
VLAN Priority	0 Value range: 0 to 7

VLAN Mode	VLAN tagging is the networking standard that supports Virtual LANs (VLANs) on an Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames. The standard also provides provisions for a quality-of-service prioritization scheme known as IEEE 802.1p and defines the Generic Attribute Registration Protocol.
VLAN ID	Specify the VLAN that the Ethernet frame belongs to. The hexadecimal values 0x000 and 0xFFF are reserved. All other values may be used as VLAN identifiers, allowing up to 4094 VLANs. The reserved value 0x000 indicates that the frame does not belong to any VLAN. In this case, the 802.1Q tag specifies only a priority and is referred to as a priority tag.
VLAN Priority	Set the frame priority level. Otherwise known as Priority Code Point (PCP), VLAN Priority is a 3-bit field that refers to the IEEE 802.1p priority or frame priority level. Values are from 0 (lowest) to 7 (highest).

802.1X Port-based Network Access Control



Network Settings

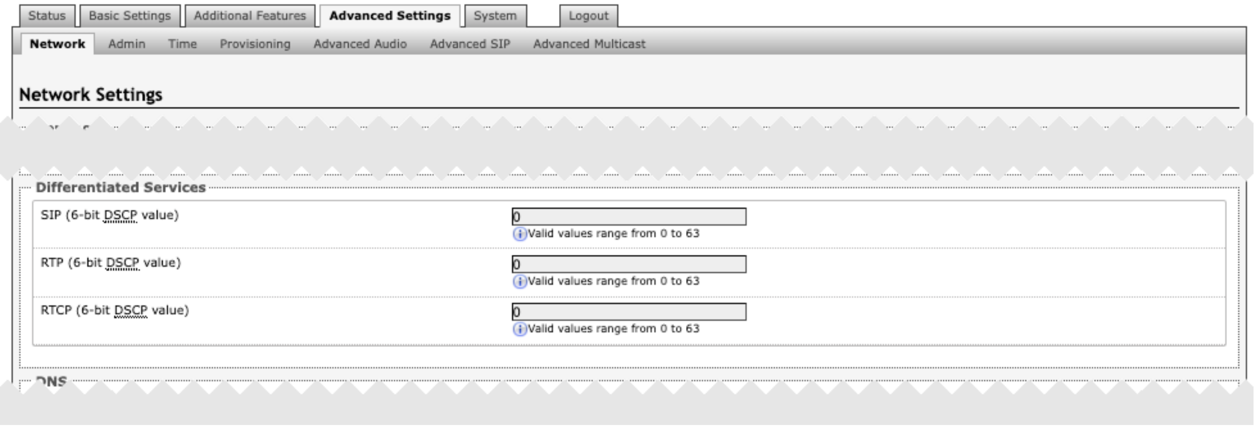
802.1X Port-based Network Access Control

802.1X Authentication	● Enabled ○ Disabled
Authentication Mode	EAP-PEAP/MSCHAPv2 In EAP-TLS mode, if the authentication server requires devices to be authenticated, a PEM file containing both a device certificate and a private key can be installed on the Algo device. Use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file renamed to 'client8021x.pem' in the 'certs' folder.
Anonymous ID	
ID	
Password	
Validate Server Certificate	○ Enabled ● Disabled Validate the authentication server against common authorities. To validate against additional certificates, use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder.

802.1x Authentication	Enable to add credentials to access LAN or WLAN that have 802.1X network access control (NAC). You can ask your IT Administrator for this information
Authentication Mode	Select the desired authentication mode.
Anonymous ID	If configured, the device will send the anonymous ID to the authenticator instead of the 802.1X client username.
ID	The ID should contain a string identifying the IEEE 802.1X authenticator originating the request. Ask your IT administrator for details.
Password	Ask your IT administrator for details.
Validate Server Certificate	Enable to validate the authentication server against common authorities. To validate additional certificates, go to the **System → File Manager** to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the '**certs**' folder.

Differentiated Services

Differentiated Services provide quality of service if the DSCP protocol is supported on your network. Differentiated Services can be specified independently for SIP control packets and RTP and RTCP audio packets.



Network Settings

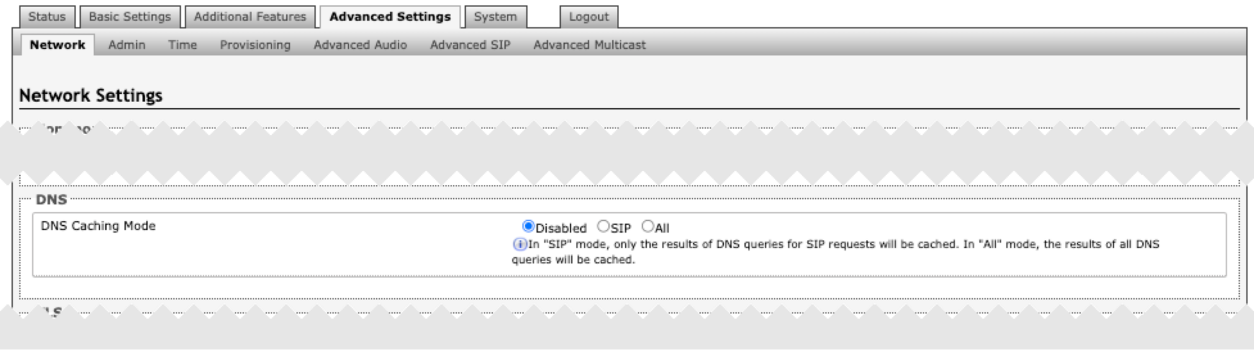
Differentiated Services

SIP (6-bit DSCP value)	0 Valid values range from 0 to 63
RTP (6-bit DSCP value)	0 Valid values range from 0 to 63
RTCP (6-bit DSCP value)	0 Valid values range from 0 to 63

DNS

SIP (6-bit DSCP value)	Enter the DSCP value for SIP packets.
RTP (6-bit DSCP value)	Enter the DSCP value for RTP packets.
RTCP (6-bit DSCP value)	Enter the DSCP value for RTCP packets.

DNS



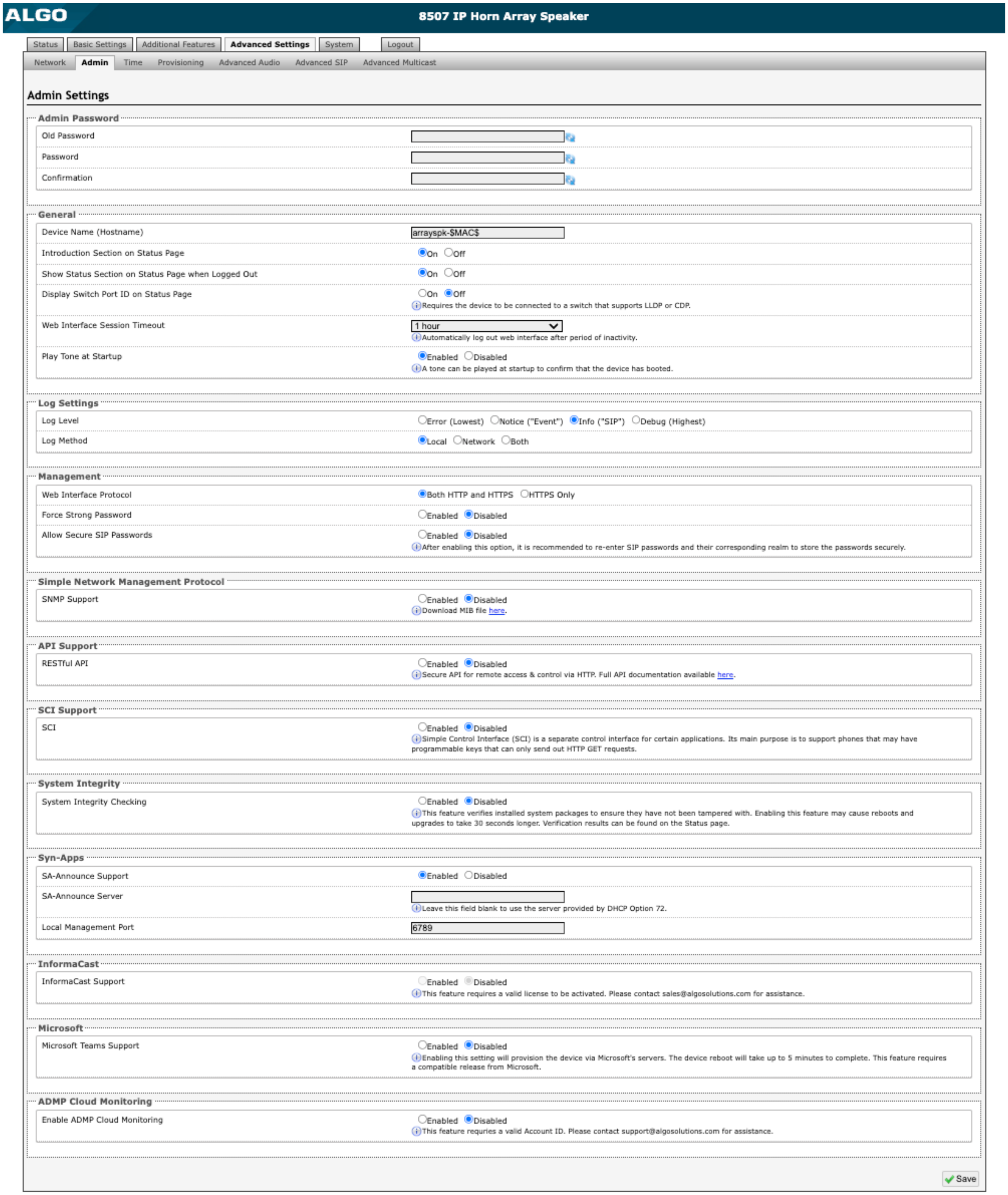
Network Settings

DNS

DNS Caching Mode	● Disabled ○ SIP ○ All In "SIP" mode, only the results of DNS queries for SIP requests will be cached. In "All" mode, the results of all DNS queries will be cached.

DNS Caching Mode	There are three mode options: 1. **Disabled**: No DNS queries will be cached. 2. **SIP**: Only the results of DNS queries for SIP requests will be cached. 3. **All**: The results of all DNS queries will be cached.

8.3 Admin



Admin Settings

Admin Password

Old Password	
Password	
Confirmation	

General

Device Name (Hostname)	arrayspk-MAC
Introduction Section on Status Page	● On ○ Off
Show Status Section on Status Page when Logged Out	● On ○ Off
Display Switch Port ID on Status Page	○ On ● Off Requires the device to be connected to a switch that supports LLDP or CDP.
Web Interface Session Timeout	1 hour Automatically log out web interface after period of inactivity.
Play Tone at Startup	● Enabled ○ Disabled A tone can be played at startup to confirm that the device has booted.

Log Settings

Log Level	○ Error (Lowest) ○ Notice ("Event") ● Info ("SIP") ○ Debug (Highest)
Log Method	● Local ○ Network ○ Both

Management

Web Interface Protocol	● Both HTTP and HTTPS ○ HTTPS Only
Force Strong Password	○ Enabled ● Disabled
Allow Secure SIP Passwords	○ Enabled ● Disabled After enabling this option, it is recommended to re-enter SIP passwords and their corresponding realm to store the passwords securely.

Simple Network Management Protocol

SNMP Support	○ Enabled ● Disabled Download MIB file here.

API Support

RESTful API	○ Enabled ● Disabled Secure API for remote access & control via HTTP. Full API documentation available here.

SCI Support

SCI	○ Enabled ● Disabled Simple Control Interface (SCI) is a separate control interface for certain applications. Its main purpose is to support phones that may have programmable keys that can only send out HTTP GET requests.

System Integrity

System Integrity Checking	○ Enabled ● Disabled This feature verifies installed system packages to ensure they have not been tampered with. Enabling this feature may cause reboots and upgrades to take 30 seconds longer. Verification results can be found on the Status page.

Syn-Apps

SA-Announce Support	● Enabled ○ Disabled
SA-Announce Server	Leave this field blank to use the server provided by DHCP Option 72.
Local Management Port	6789

InformaCast

InformaCast Support	○ Enabled ○ Disabled This feature requires a valid license to be activated. Please contact sales@algosolutions.com for assistance.

Microsoft

Microsoft Teams Support	○ Enabled ● Disabled Enabling this setting will provision the device via Microsoft's servers. The device reboot will take up to 5 minutes to complete. This feature requires a compatible release from Microsoft.

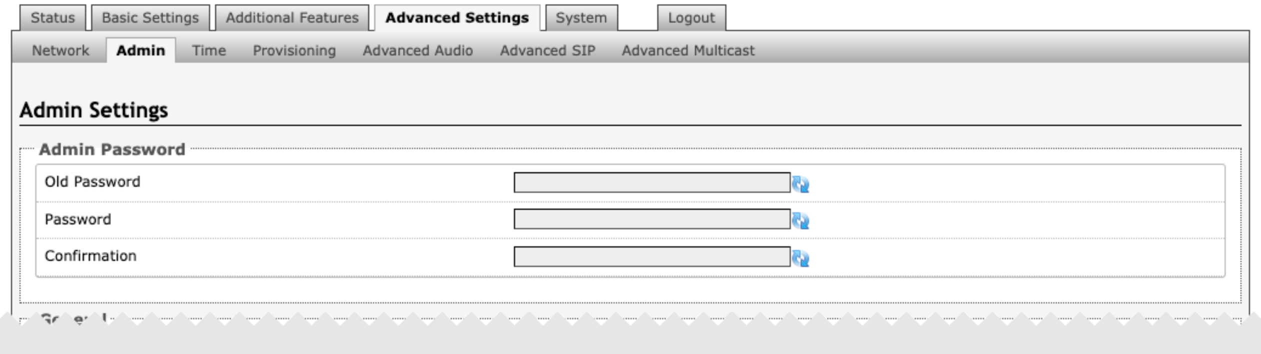
ADMP Cloud Monitoring

Enable ADMP Cloud Monitoring	○ Enabled ● Disabled This feature requries a valid Account ID. Please contact support@algosolutions.com for assistance.

Figure 20: Configure admin settings in the web interface.

Admin Password

Use this section to change the admin password for logging into your 8507 web interface. It’s recommended that you change the admin password from the default to secure the device on your network.



Admin Settings

Admin Password

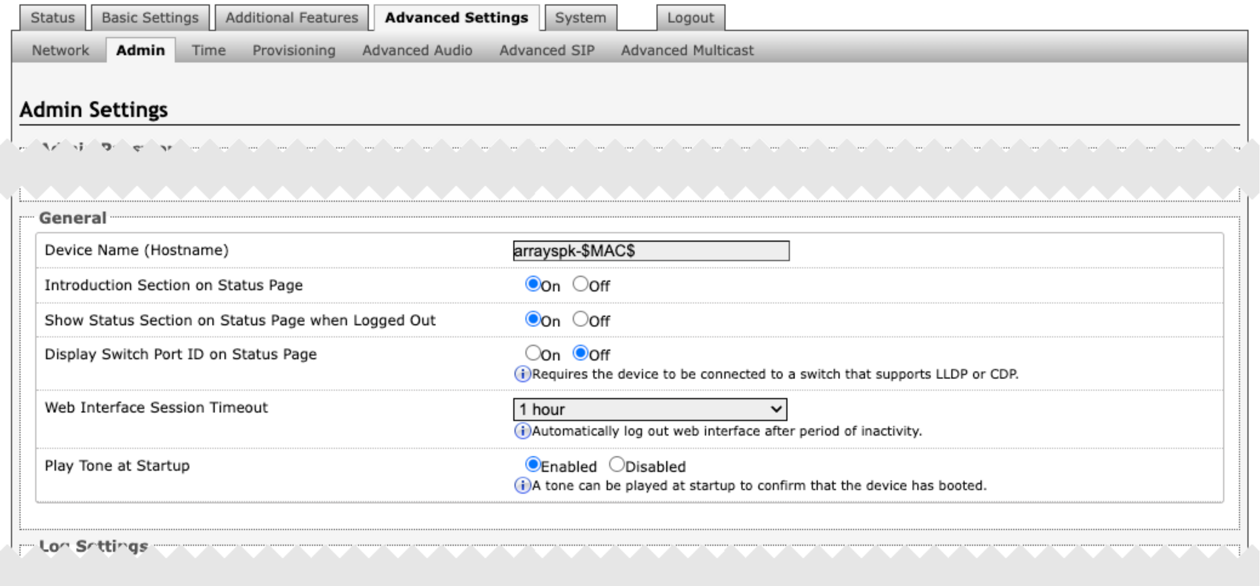
Old Password

Password

Confirmation

Old Password	Enter the old admin password. The default password when you first get the device is *algo*.
Password	Enter a new admin password to log into the device web interface. Make sure the new password is stored safely. If the password is forgotten, you must reset the device entirely with the Reset Button to restore the default password. All other settings will be reset to the original default settings as well. For additional password security, see the setting: Force Strong Password.
Confirmation	Re-enter your new admin password.

General



Admin Settings

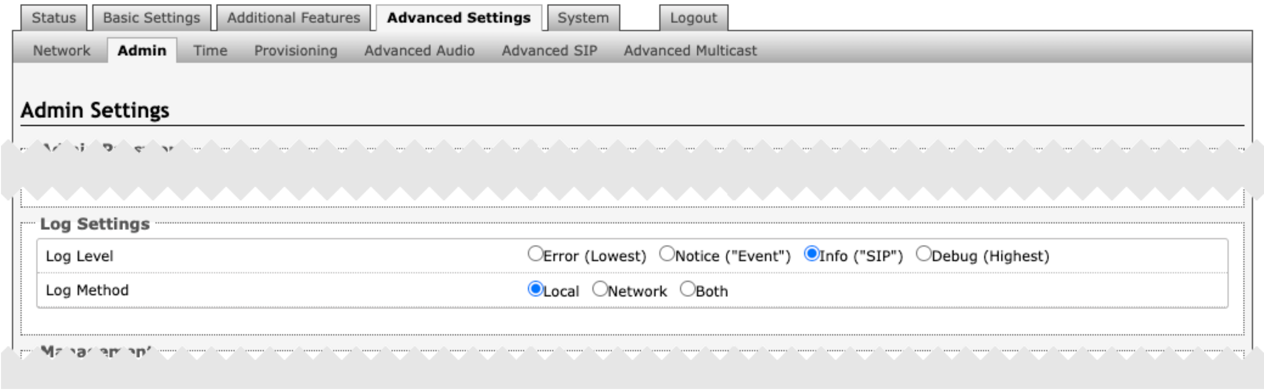
General

Device Name (Hostname)	arrayspk-MAC
Introduction Section on Status Page	● On ○ Off
Show Status Section on Status Page when Logged Out	● On ○ Off
Display Switch Port ID on Status Page	○ On ● Off Requires the device to be connected to a switch that supports LLDP or CDP.
Web Interface Session Timeout	1 hour Automatically log out web interface after period of inactivity.
Play Tone at Startup	● Enabled ○ Disabled A tone can be played at startup to confirm that the device has booted.

Log Settings

Device Name (Hostname)	Add a name to identify the device in the Algo Network Device Locator Tool.
Introduction Section on Status Page	Turn **On** to show the introduction text on the login screen.
Show Status Section on Status Page when Logged Out	Turn **On** to allow others to view the status page without logging in. If turned **Off**, the settings and configurations on the status page will be hidden entirely unless a user is logged in to ensure only trusted users can view device information.
Display Switch Port ID on Status Page	Turn **On** to display the Switch Port ID on the Status Page. This option is only possible if the device is connected to a switch that supports LLDP or CDP.
Web Interface Session Timeout	Set the maximum duration of inactivity to log a user out of the web interface automatically.
Play Tone at Startup	Enable to play a tone at start-up to confirm that the device has booted. This can be useful when testing or configuring a device but might not be desirable if the device is connected to an external legacy communication system and paging system.

Log Settings



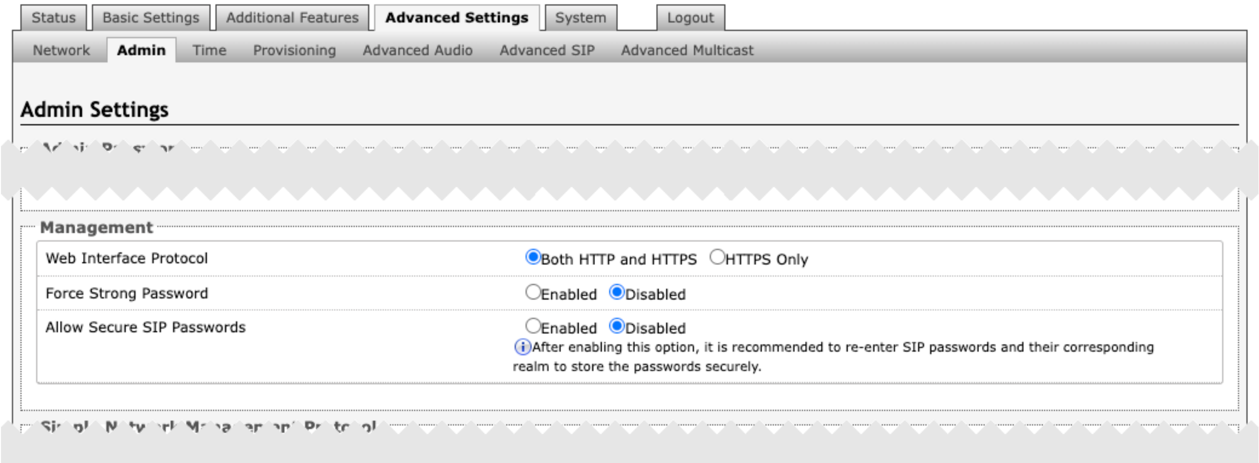
Admin Settings

Log Settings

Log Level	○Error (Lowest) ○Notice ("Event") ●Info ("SIP") ○Debug (Highest)
Log Method	●Local ○Network ○Both

Log Level	This setting should only be used after consulting with the Algo support team.
Log Method	Select a Log Method: - Local: The log file is saved in RAM on the device. - Method: Send the log file to a server repeatedly so settings are not lost if the device is rebooted. - Both: Use both methods.
Log Server	Enter the Syslog server address provided by your IT administrator.

Management



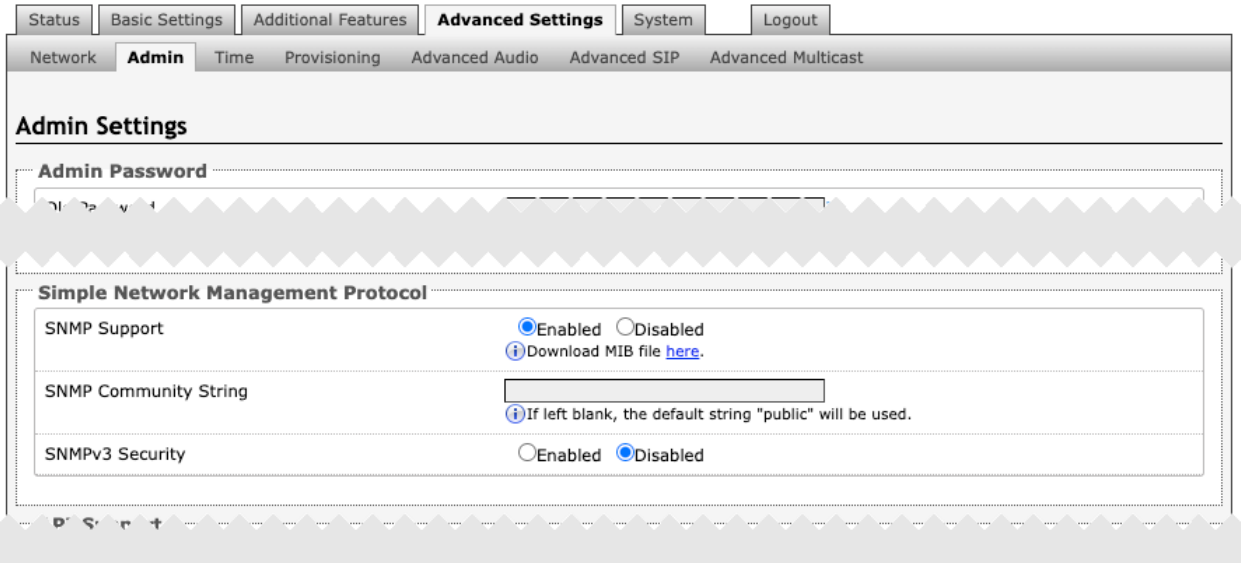
Admin Settings

Management

Web Interface Protocol	● Both HTTP and HTTPS ○ HTTPS Only
Force Strong Password	○ Enabled ● Disabled
Allow Secure SIP Passwords	○ Enabled ● Disabled ⓘ After enabling this option, it is recommended to re-enter SIP passwords and their corresponding realm to store the passwords securely.

Web Interface Protocol	HTTPS is always enabled on the device. HTTP is enabled by default but may be disabled. To do so, select **HTTPS Only** mode so requests are automatically redirected to HTTPS. Note that no security certificate exists since the device can have any address on the local network. Therefore, most browsers will provide a warning when using HTTPS.
Force Strong Password	When **Enabled,** you can enforce a secure password for the device web interface for additional protection. The password requirements for a strong password are: • Must contain at least 10 characters • Must contain at least 1 uppercase character • Must contain at least 1 digit (0 – 9) • Must contain at least 1 special character
Allow Secure SIP Password	When **Enabled,** SIP passwords are stored in the configuration file in an encrypted format to prevent viewing and recovery. If enabled, navigate to **Basic Settings** → **SIP** and fill out the field **Realm.** To obtain your SIP Realm information, contact your SIP Server administrator or check the SIP log file for a registration attempt. The Realms may be the same or different for all the extensions used. All the configured Authentication Password(s) must be re-entered here as well as any other locations where SIP extensions have been configured to save the encrypted password(s). If the **Realm** is changed later, all passwords must be re-entered to save the passwords with the new encryption.

Simple Network Management Protocol



Admin Settings

Admin Password

Simple Network Management Protocol

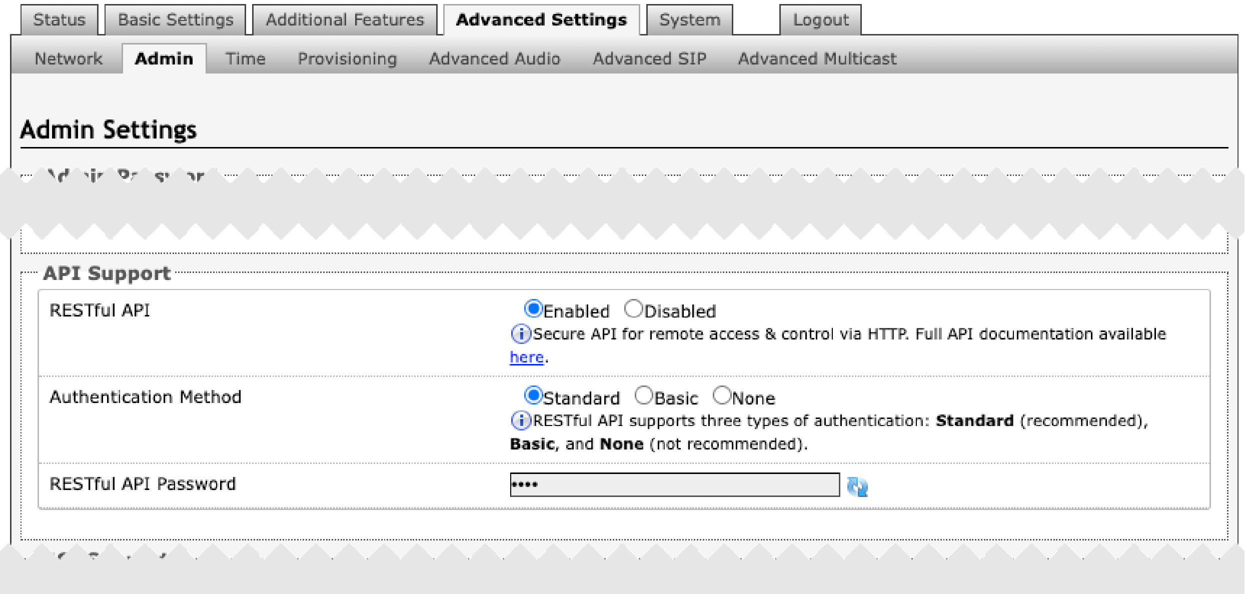
SNMP Support ● Enabled ○ Disabled
Download MIB file here.

SNMP Community String
If left blank, the default string "public" will be used.

SNMPv3 Security ○ Enabled ● Disabled

SNMP Support	The existing setting will respond to a simple status query for automated supervision.
SNMP Community String	Speak to your IT Administrator for more information.
SNMPv3 Security	Speak to your IT Administrator for more information.

API Support



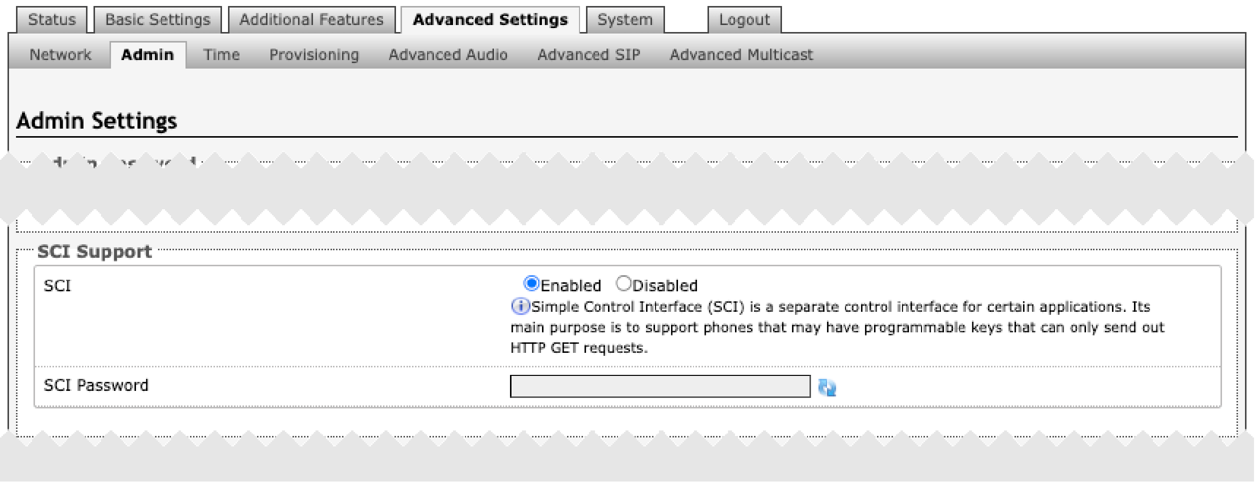
Admin Settings

API Support

RESTful API	● Enabled ○ Disabled ⓘSecure API for remote access & control via HTTP. Full API documentation available here.
Authentication Method	● Standard ○ Basic ○ None ⓘRESTful API supports three types of authentication: **Standard** (recommended), **Basic**, and **None** (not recommended).
RESTful API Password	••••

RESTful API	Enable a secure API for remote access and device control via HTTP. For more information, see the Algo RESTful API Guide.
Authentication Method	Speak to your IT Administrator for more information.
RESTful API Password	Speak to your IT Administrator for more information.

SCI Support



Admin Settings

SCI Support

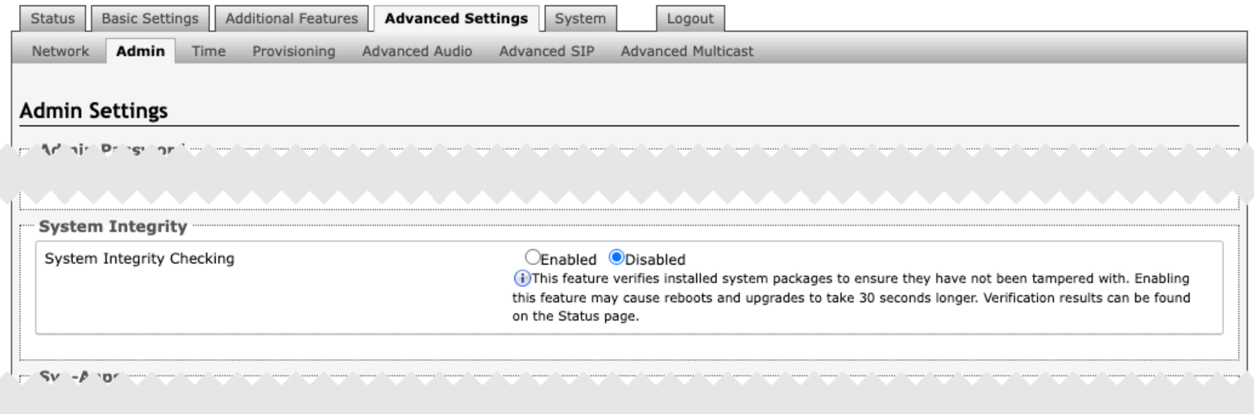
SCI ● Enabled ○ Disabled

ⓘ Simple Control Interface (SCI) is a separate control interface for certain applications. Its main purpose is to support phones that may have programmable keys that can only send out HTTP GET requests.

SCI Password

SCI	Simple Control Interface (SCI) is a separate control interface for certain applications. Its primary purpose is to support phones that may have programmable keys that can only send out HTTP GET requests.

System Integrity



Admin Settings

System Integrity

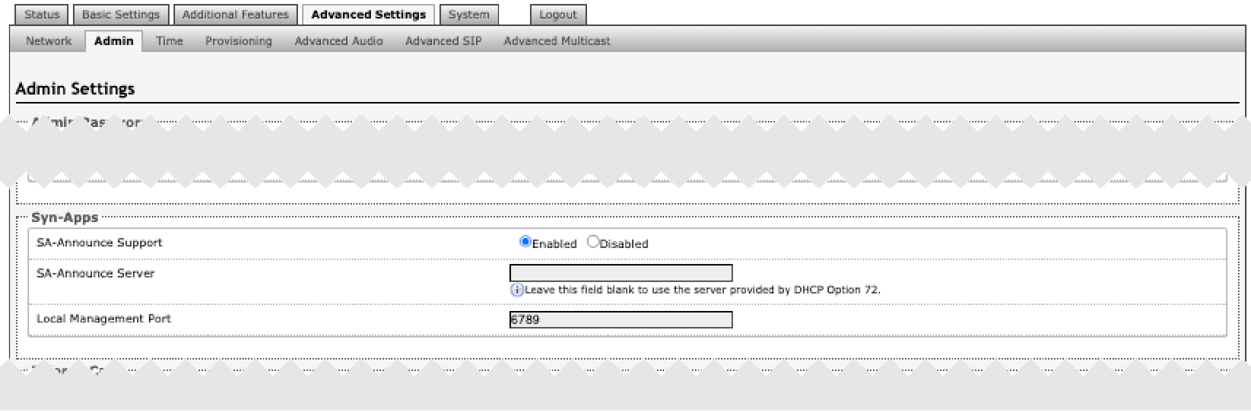
System Integrity Checking ○ Enabled ● Disabled

ⓘ This feature verifies installed system packages to ensure they have not been tampered with. Enabling this feature may cause reboots and upgrades to take 30 seconds longer. Verification results can be found on the Status page.

System Integrity Checking	Enable this feature to verify that installed system packages have not been tampered with by running a check. Enabling this feature may cause reboots and upgrades to take 30 seconds longer. Verification results can be found on the **Status** tab.

Syn-Apps

The SA-Announce feature cannot be used when Multicast Transmitter mode or Poly mode is enabled. To enable SA-Announce mode, set **Multicast Mode** to **None** in **Basic Settings → Multicast**.



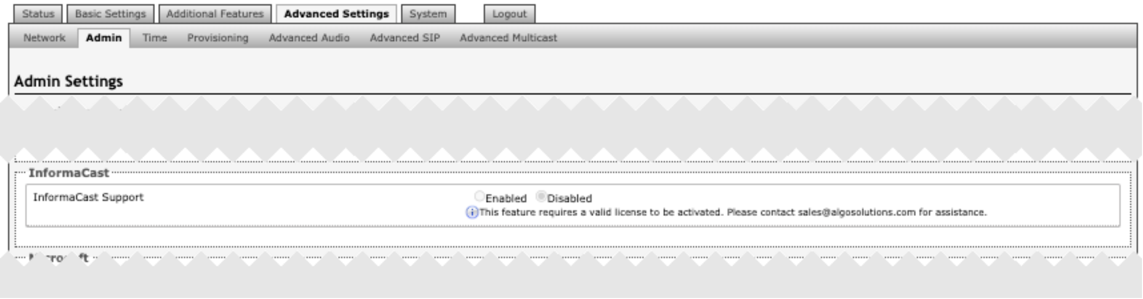
Admin Settings

Syn-Apps

SA-Announce Support	● Enabled ○ Disabled
SA-Announce Server	ⓘ Leave this field blank to use the server provided by DHCP Option 72.
Local Management Port	6789

SA-Announce Support	Enable to convert unicast streams to multicast and deliver them to the target endpoints.
SA-Announce Server	Enter the SA-Announce Server to use the Syn-Apps paging feature. Leave the field blank to use the server provided by the DHCP Option 72.
Local Management Port	Enter the local management port for the SA-Announce Server.

InformaCast



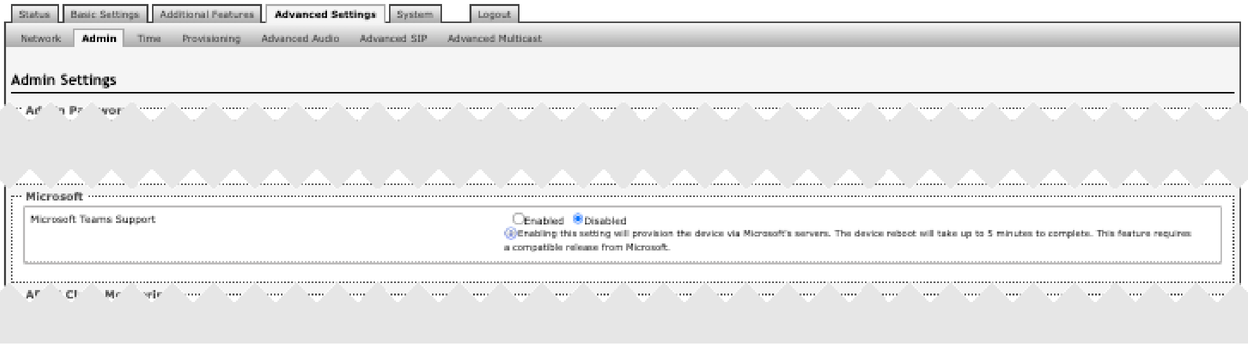
Admin Settings

InformaCast

InformaCast Support	○ Enabled ○ Disabled ⓘ This feature requires a valid license to be activated. Please contact sales@algosolutions.com for assistance.

InformaCast Support	This feature requires a valid InformaCast license to be activated. Please contact sales@algosolutions.com for assistance.

Microsoft



Admin Settings

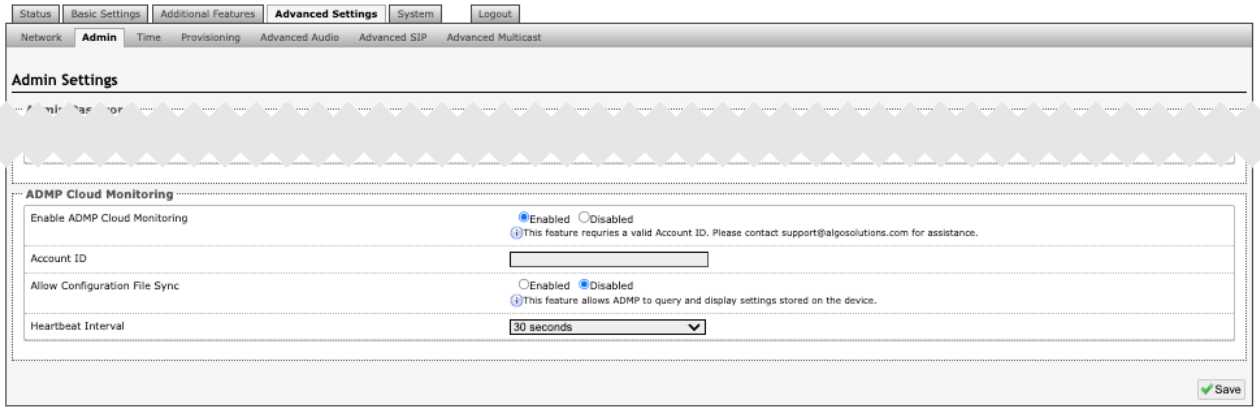
Microsoft

Microsoft Teams Support ○Enabled ●Disabled

ⓘEnabling this setting will provision the device via Microsoft's servers. The device reboot will take up to 5 minutes to complete. This feature requires a compatible release from Microsoft.

Microsoft Teams Support	Enable to provision the device via Microsoft's servers. The device reboot will take up to 5 minutes to complete. This feature requires a compatible release from Microsoft.

ADMP Cloud Monitoring



Admin Settings

ADMP Cloud Monitoring

Enable ADMP Cloud Monitoring ●Enabled ○Disabled

ⓘThis feature requries a valid Account ID. Please contact support@algosolutions.com for assistance.

Account ID

Allow Configuration File Sync ○Enabled ●Disabled

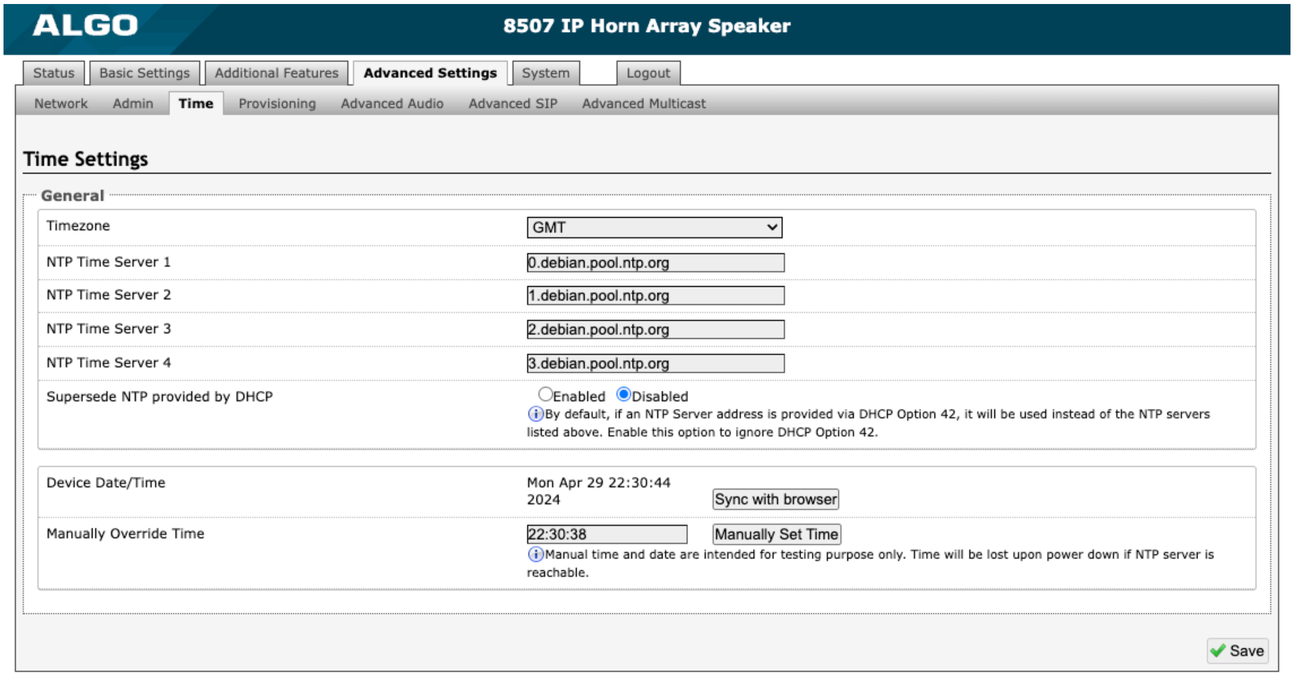
ⓘThis feature allows ADMP to query and display settings stored on the device.

Heartbeat Interval 30 seconds

Enable ADMP Cloud Monitoring	The Algo Device Management Platform (ADMP) simplifies the process of managing, monitoring, and maintaining Algo devices from any location. This feature requires a valid Account ID. To learn more about ADMP and how to purchase a license, visit the website.
Account ID	Enter the account ID listed on the **Settings** page of your ADMP account.
Allow Configuration File Sync	Enable ADMP to query and display settings stored on the device.
Heartbeat Interval	Select how often ADMP should check the status of your device.

8.4 Time

Time and date are used for logging.



Time Settings

General

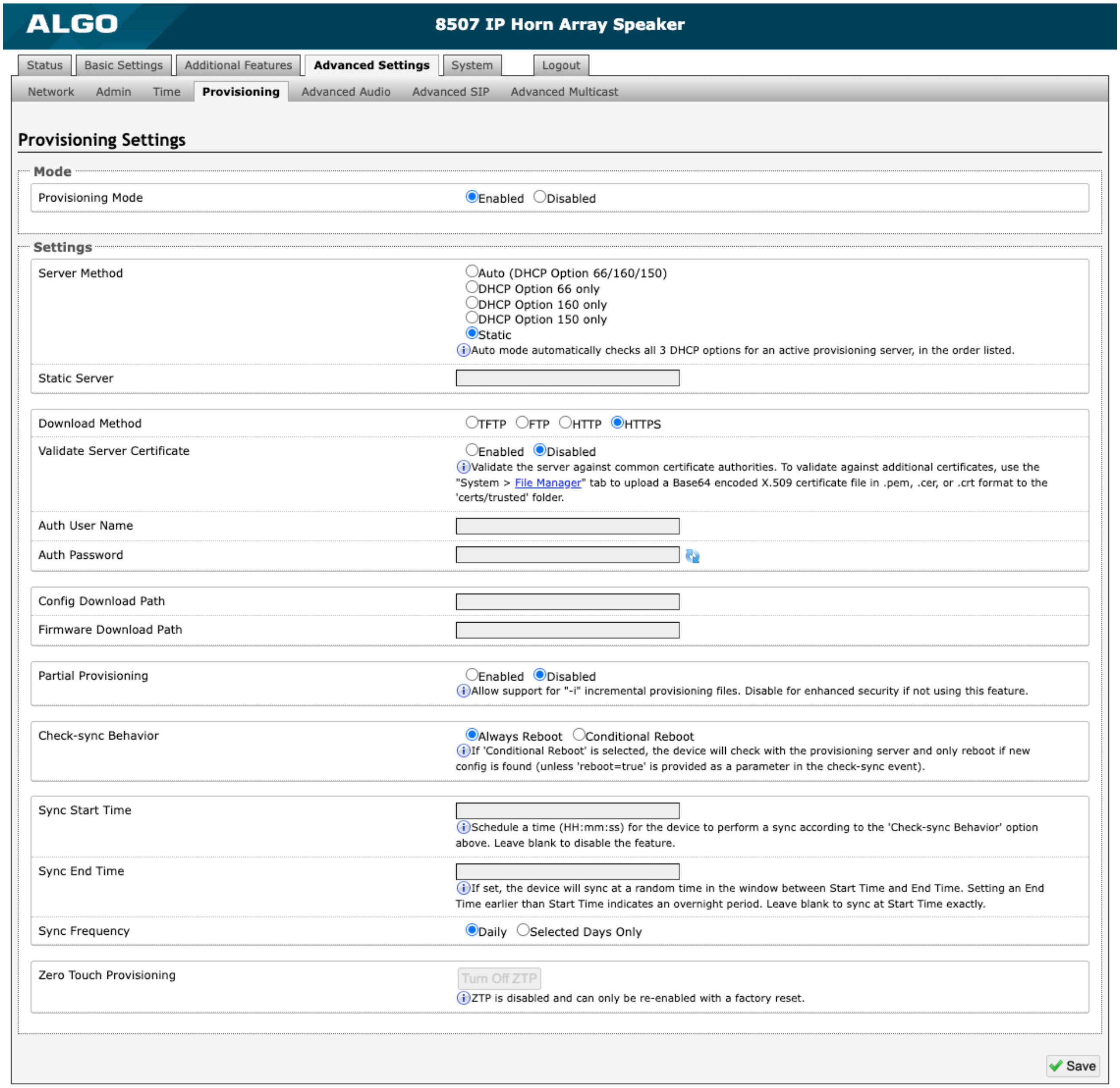
Timezone	GMT
NTP Time Server 1	0.debian.pool.ntp.org
NTP Time Server 2	1.debian.pool.ntp.org
NTP Time Server 3	2.debian.pool.ntp.org
NTP Time Server 4	3.debian.pool.ntp.org
Supersede NTP provided by DHCP	○Enabled ●Disabled By default, if an NTP Server address is provided via DHCP Option 42, it will be used instead of the NTP servers listed above. Enable this option to ignore DHCP Option 42.
Device Date/Time	Mon Apr 29 22:30:44 2024
Manually Override Time	22:30:38 Manual time and date are intended for testing purpose only. Time will be lost upon power down if NTP server is reachable.

Figure 25: Configure time settings in the web interface.

General	
Timezone	Select a time zone for your device to use.
NTP Time Servers 1/2/3/4	The device will attempt to use Timer Server 1 and work down the list if one or more of the time servers become unresponsive. These settings are pre-populated with public NTP servers hosted on the internet. To use these, the device requires an internet connection. Alternatively, this can be customized to point the device to any other NTP server hosted or premise-based.
Supersede NTP provided by DHCP	By default, if an NTP Server address is provided via DHCP Option 42, it will be used instead of the NTP servers listed above. Enable this option to ignore DHCP Option 42.
Device Date/Time	This field shows the current time and date set on the device. If you are testing the device on a lab network that does not have access to an external NTP server, click **Sync with browser** to temporarily set the time on the device.

	This time value will be lost at power down or overwritten if a connection to the NTP server is available. Time and date are used for logging purposes and the scheduler feature.
Manually Override Time	Manual time and date are intended for testing purposes only. Time will be lost upon power down if the NTP server is reachable.

8.5 Provisioning



Provisioning Settings

Mode

Provisioning Mode: ● Enabled ○ Disabled

Settings

Server Method: ○ Auto (DHCP Option 66/160/150) ○ DHCP Option 66 only ○ DHCP Option 160 only ○ DHCP Option 150 only ● Static
ⓘ Auto mode automatically checks all 3 DHCP options for an active provisioning server, in the order listed.

Static Server:

Download Method: ○ TFTP ○ FTP ○ HTTP ● HTTPS

Validate Server Certificate: ○ Enabled ● Disabled
ⓘ Validate the server against common certificate authorities. To validate against additional certificates, use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder.

Auth User Name:

Auth Password:

Config Download Path:

Firmware Download Path:

Partial Provisioning: ○ Enabled ● Disabled
ⓘ Allow support for "-i" incremental provisioning files. Disable for enhanced security if not using this feature.

Check-sync Behavior: ● Always Reboot ○ Conditional Reboot
ⓘ If 'Conditional Reboot' is selected, the device will check with the provisioning server and only reboot if new config is found (unless 'reboot=true' is provided as a parameter in the check-sync event).

Sync Start Time:
ⓘ Schedule a time (HH:mm:ss) for the device to perform a sync according to the 'Check-sync Behavior' option above. Leave blank to disable the feature.

Sync End Time:
ⓘ If set, the device will sync at a random time in the window between Start Time and End Time. Setting an End Time earlier than Start Time indicates an overnight period. Leave blank to sync at Start Time exactly.

Sync Frequency: ● Daily ○ Selected Days Only

Zero Touch Provisioning: Turn Off ZTP
ⓘ ZTP is disabled and can only be re-enabled with a factory reset.

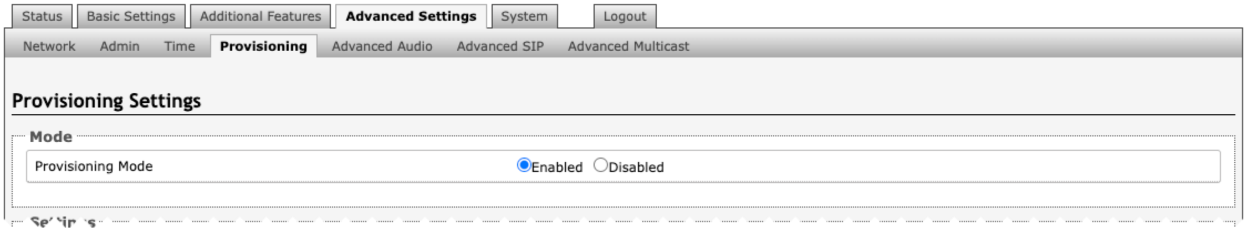
Figure 21: Configure provisioning settings in the web interface.

Algo devices can be provisioned through a provisioning server or zero-touch provisioning (ZTP).

System administrators can provision multiple Algo devices together, eliminating the need to log into each endpoint web interface. After configuration or firmware files are placed on a provisioning server, Algo devices can be instructed to fetch these files and apply the settings.

Algo also offers a ZTP service that is meant to be used as a redirection service to your provisioning server or to configure your device with an Algo Device Management Platform (ADMP) account. ZTP is enabled by default and occurs before any other provisioning step. It will be disabled automatically after any other provisioning settings are changed on the device for the first time.

Mode



Provisioning Settings

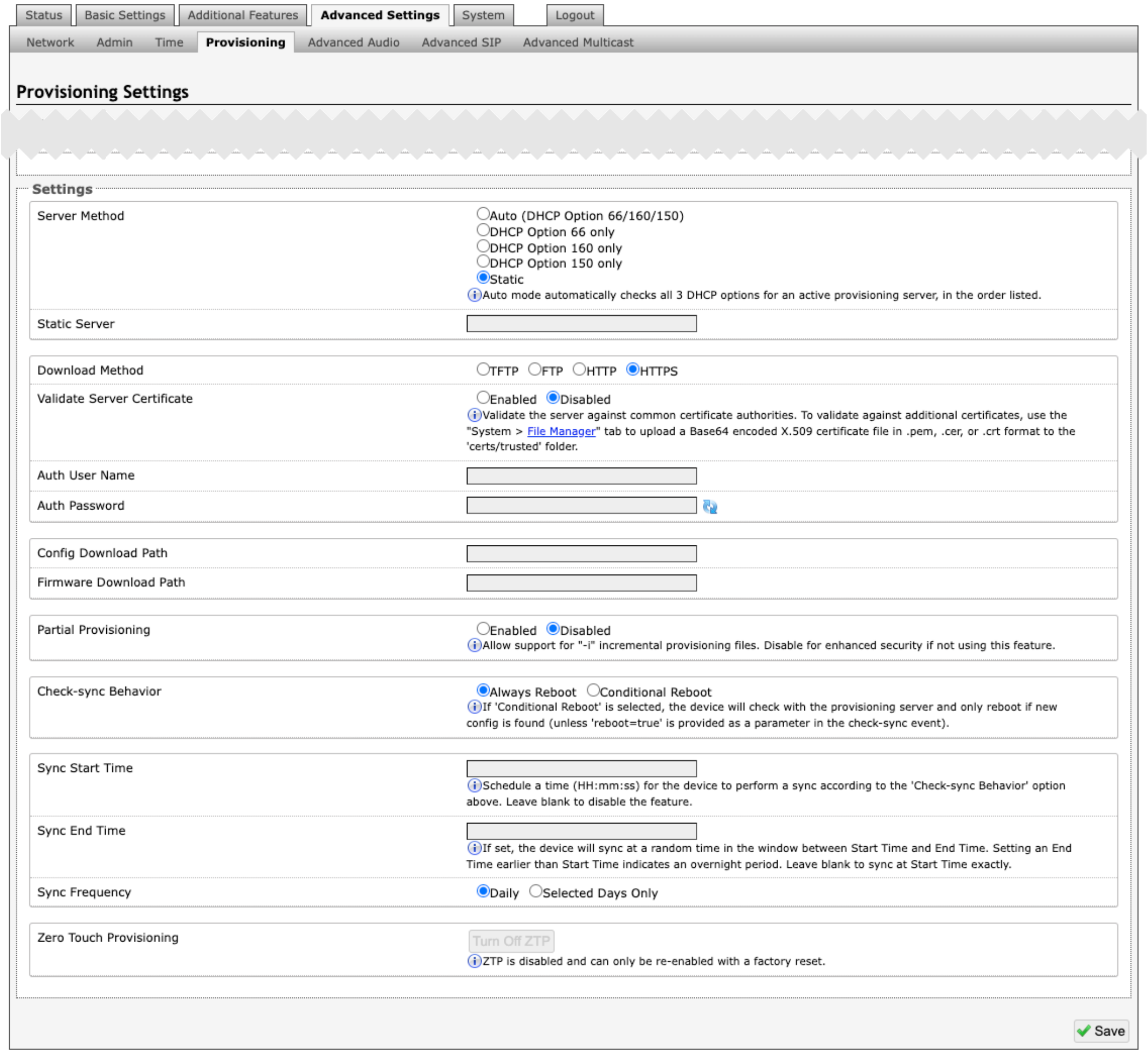
Mode

Provisioning Mode ● Enabled ○ Disabled

Settings

Provisioning Mode	Enabling provisioning allows installers to pre-configure the device on a network before installation. This is typically done for large deployments to save time and ensure consistent setups. It is recommended that **Provisioning Mode** be set to **Disabled** if this feature is not in use. This will prevent unauthorized re-configuration of the device if DHCP is used. Visit the Algo Provisioning Guide for more information.

Settings



Provisioning Settings

Settings

Server Method	○Auto (DHCP Option 66/160/150) ○DHCP Option 66 only ○DHCP Option 160 only ○DHCP Option 150 only ●Static ⓘAuto mode automatically checks all 3 DHCP options for an active provisioning server, in the order listed.
Static Server	
Download Method	○TFTP ○FTP ○HTTP ●HTTPS
Validate Server Certificate	○Enabled ●Disabled ⓘValidate the server against common certificate authorities. To validate against additional certificates, use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder.
Auth User Name	
Auth Password	
Config Download Path	
Firmware Download Path	
Partial Provisioning	○Enabled ●Disabled ⓘAllow support for "-i" incremental provisioning files. Disable for enhanced security if not using this feature.
Check-sync Behavior	●Always Reboot ○Conditional Reboot ⓘIf 'Conditional Reboot' is selected, the device will check with the provisioning server and only reboot if new config is found (unless 'reboot=true' is provided as a parameter in the check-sync event).
Sync Start Time	ⓘSchedule a time (HH:mm:ss) for the device to perform a sync according to the 'Check-sync Behavior' option above. Leave blank to disable the feature.
Sync End Time	ⓘIf set, the device will sync at a random time in the window between Start Time and End Time. Setting an End Time earlier than Start Time indicates an overnight period. Leave blank to sync at Start Time exactly.
Sync Frequency	●Daily ○Selected Days Only
Zero Touch Provisioning	Turn Off ZTP ⓘZTP is disabled and can only be re-enabled with a factory reset.

Server Method	Select a Server Method. • **Auto**: All three DHCP options (66, 160, 150) will be automatically checked for an active provisioning server • **DHCP Option 66 Only**: Only DHCP Option 66 will be checked for a provisioning server • **DHCP Option 160 Only**: Only DHCP Option 160 will be checked for a provisioning server • **DHCP Option 150 Only**: Only DHCP Option 150 will be checked for a provisioning server

	- **Static**: Only the specified static server will be checked for a provisioning server For provisioning to work with a DHCP option, DHCP must be enabled under **Advanced Settings → Network → IPv4**.
Static Server	Enter the server address or domain.
Download Method	Select your preferred method for downloading provisioning files. The options are: - TFTP (Trivial File Transfer Protocol) — See MD5 Checksum below for more details. - FTP - HTTP - HTTPS — This may help prevent configuration files from being read by an unwanted third party and having sensitive data stolen. The device configuration files can be automatically downloaded from a provisioning server using DHCP Option 66. This option code (when set) supplies a TFTP boot server address to the DHCP client to boot from. One of two files can be uploaded on the provisioning server (for access via TFTP, FTP, HTTP, or HTTPS): - Generic (for all Algo 8507 IP Horn Array) **algop8507.conf** - Specific (for a specific MAC address) **algom[MAC].conf** Both protocol and path are supported for Option 66, allowing for http://myserver.com/config-path to be used.
Validate Server Certificate	Enable to verify the server. This checks if the certificate provided by the server is signed by any CAs included in the list of trusted CAs (used by the Debian infrastructure and Mozilla browsers). If a certificate signed by any of these CAs is received, that server will be trusted. This parameter can also be enabled through provisioning: Prov.download.cert = 1
(FTP) Auth User Name	Speak to your IT Administrator for more information.
(FTP) Auth Password	Speak to your IT Administrator for more information.
(HTTP) Auth User Name	Speak to your IT Administrator for more information.

(HTTP) Auth Password	Speak to your IT Administrator for more information.
(HTTPS) Validate Server Certificate	Speak to your IT Administrator for more information.
(HTTPS) Auth User Name	Speak to your IT Administrator for more information.
(HTTPS) Auth Password	Speak to your IT Administrator for more information.
Config Download Path	Enter the path where the configuration file is located within the provisioning server (e.g., algo/config/8507).
Firmware Download Path	Enter the path where the firmware file is located within the provisioning server (e.g., algo/firmware/8507).
Partial Provisioning	**Enable** to allow support for “-i” incremental provisioning files. **Disable** for enhanced security if this is not required.
Check-sync Behavior	Select **Always Reboot** to set the device to always reboot despite other settings. Select **Conditional Reboot** to set the device and check the provisioning server. Only reboot if a new config is found (unless “reboot=true” is provided as a parameter in the check-sync event).
Sync Start Time	Set a time (HH:mm:ss) for the device to perform a sync according to the **Check-sync Behavior** setting. Leave this blank if not needed.
Sync End Time	If set, the device will sync randomly in the window between Sync Start Time and Sync End Time. Setting an End Time earlier than the Start Time indicates an overnight period. Leave blank to lank to sync exactly at the set start time.
Sync Frequency	Select the sync frequency. Frequency can be set to **Daily** or **Selected Days Only.**
Sync Days	Select the days of the week for syncs to occur.

MD5 Checksum

If using TFTP as a download mode, a **.md5** checksum file must be uploaded to the provisioning server In addition to the **.conf** file. This checksum file is used to verify that the **.conf** file is transferred correctly without error.

To generate a .md5 file, you can use tools such as http://www.fourmilab.ch/md5. To use this tool, simply download and unzip the .md5 program in a command prompt. The correct .md5 file will be generated in the same directory. To generate lowercase letters, use the “-l” parameter.

Generating a generic configuration file

This configuration file is device-generic in terms of MAC address and will be used by all connected 8507 devices.

If using a generic configuration file, extensions and credentials must be entered manually once the 8507 has automatically downloaded the configuration file.

To see Algo’s SIP endpoint provisioning guide, visit www.algosolutions.com/provision.

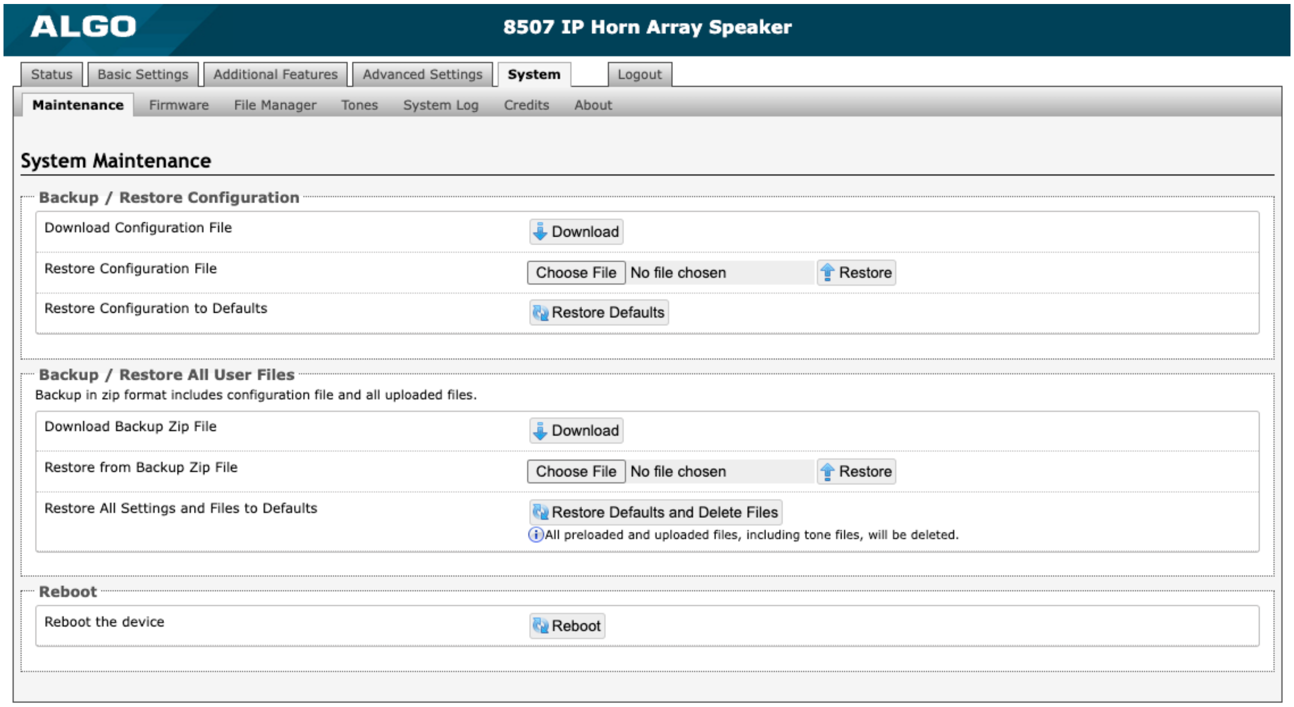
Generating a specific configuration file

The specific configuration file will only be downloaded by the 8507 with the MAC address specified in the configuration file name.

Since all necessary settings can be included in this file, the 8507 will be ready to work immediately after downloading the configuration file. The MAC address of each 8507 can be found on the back label of the unit.

To see Algo’s SIP endpoint provisioning guide, visit www.algosolutions.com/provision.

8.6 Maintenance



System Maintenance

Backup / Restore Configuration

Download Configuration File	Download
Restore Configuration File	Choose File No file chosen Restore
Restore Configuration to Defaults	Restore Defaults

Backup / Restore All User Files

Backup in zip format includes configuration file and all uploaded files.

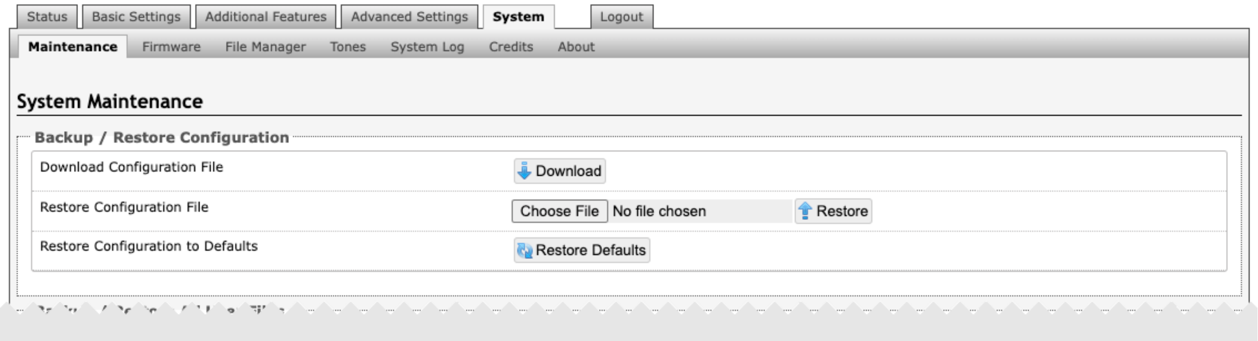
Download Backup Zip File	Download
Restore from Backup Zip File	Choose File No file chosen Restore
Restore All Settings and Files to Defaults	Restore Defaults and Delete Files ⓘAll preloaded and uploaded files, including tone files, will be deleted.

Reboot

Reboot the device	Reboot

Figure 22: Maintenance settings.

Backup/Restore Configuration



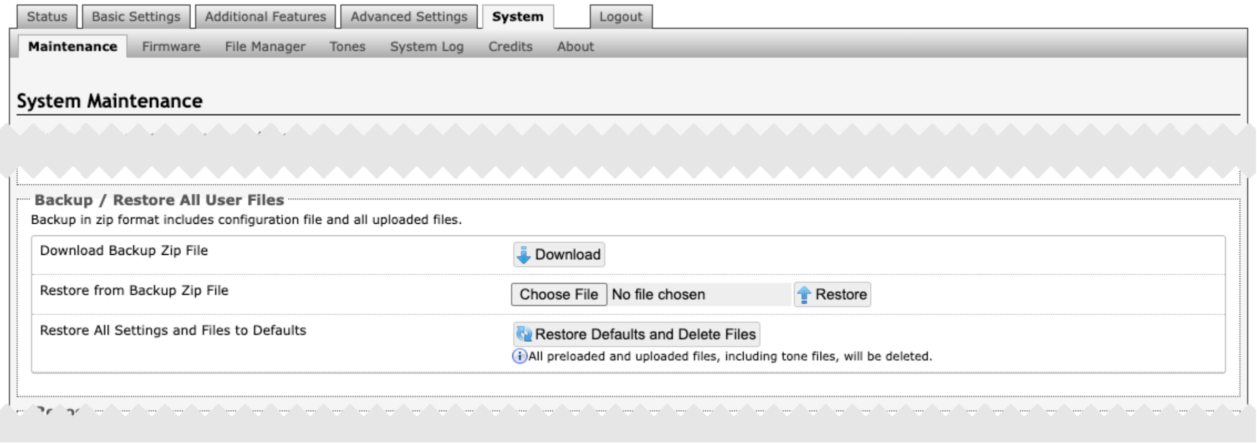
System Maintenance

Backup / Restore Configuration

Download Configuration File	Download
Restore Configuration File	Choose File No file chosen Restore
Restore Configuration to Defaults	Restore Defaults

Download Configuration File	Save configuration settings to a text file for backup or to set up a provisioning configuration file.
Restore Configuration File	Restore settings by uploading a backup file.
Restore Configuration to Defaults	Reset all device settings to factory default values.

Backup/Restore All User Files



System Maintenance

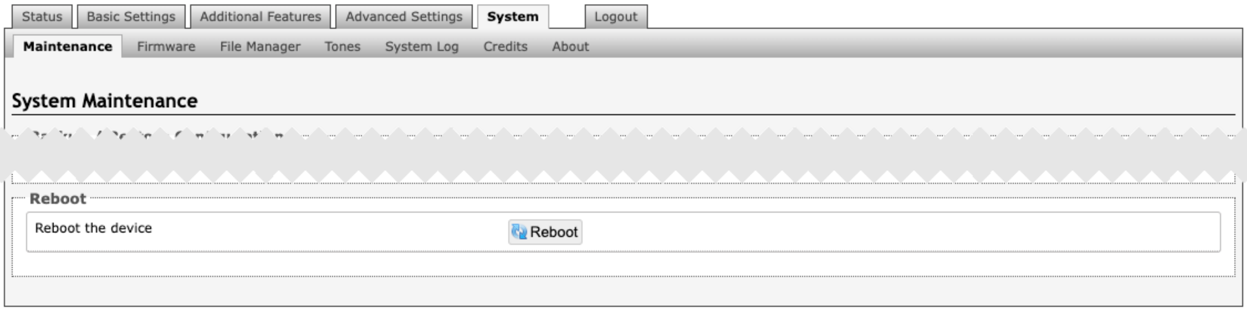
Backup / Restore All User Files

Backup in zip format includes configuration file and all uploaded files.

Download Backup Zip File	Download
Restore from Backup Zip File	Choose File No file chosen Restore
Restore All Settings and Files to Defaults	Restore Defaults and Delete Files ⓘAll preloaded and uploaded files, including tone files, will be deleted.

Download Backup Zip File	Download the device configuration settings and the files in File Manager (ex., certificates, licenses, and tones) to a backup ZIP file.
Restore from Backup Zip File	Restore the device configuration settings and files in File Manager (ex., certificates, licenses, and tones) by uploading a backup zip file.
Restore All Settings and Files to Defaults	Reset the device configuration settings. All preloaded and uploaded files, including tone files, will be deleted

Reboot



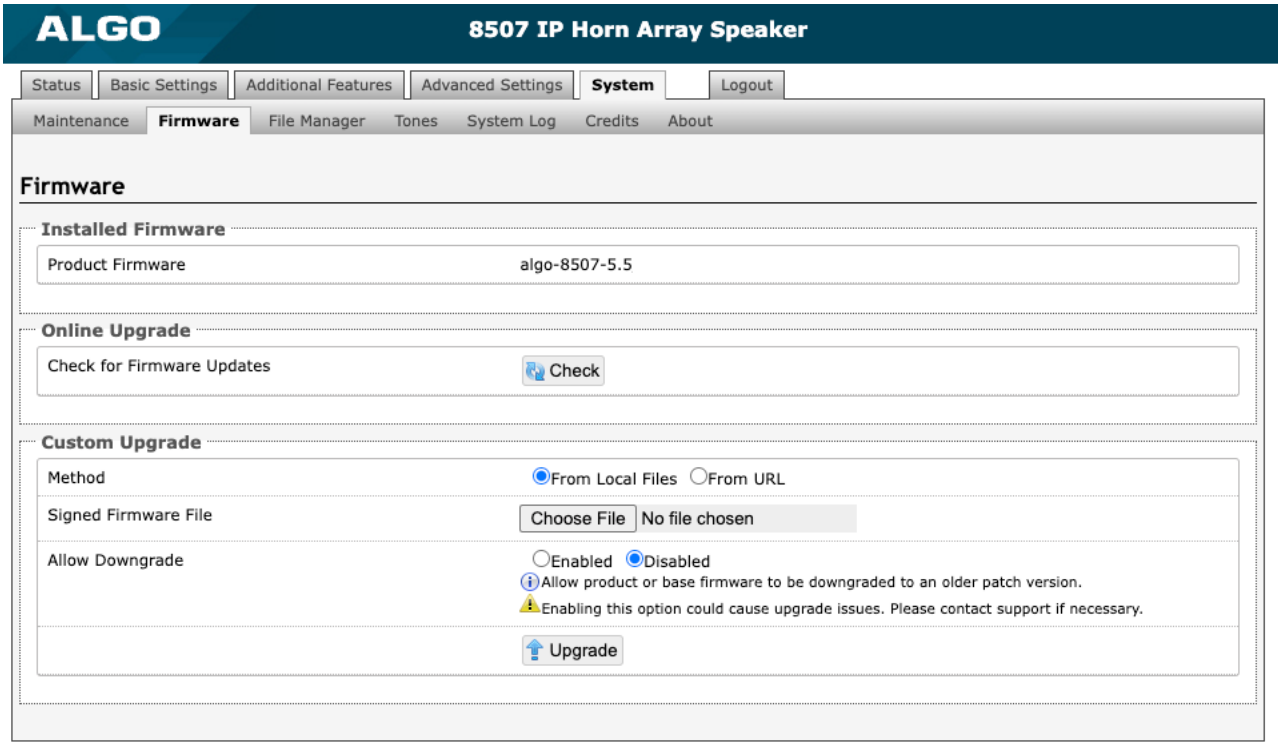
System Maintenance

Reboot

Reboot the device	Reboot

Reboot the Device	Reboots the device.

8.7 Firmware



Firmware

Installed Firmware

Product Firmware algo-8507-5.5

Online Upgrade

Check for Firmware Updates

Custom Upgrade

Method ● From Local Files ○ From URL

Signed Firmware File No file chosen

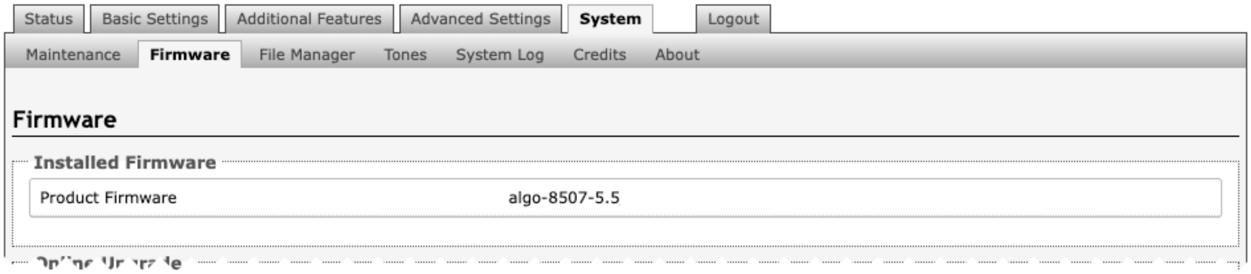
Allow Downgrade ○ Enabled ● Disabled

Allow product or base firmware to be downgraded to an older patch version.

Enabling this option could cause upgrade issues. Please contact support if necessary.

Figure 23: Configure firmware settings in the web interface.

Installed Firmware



Firmware

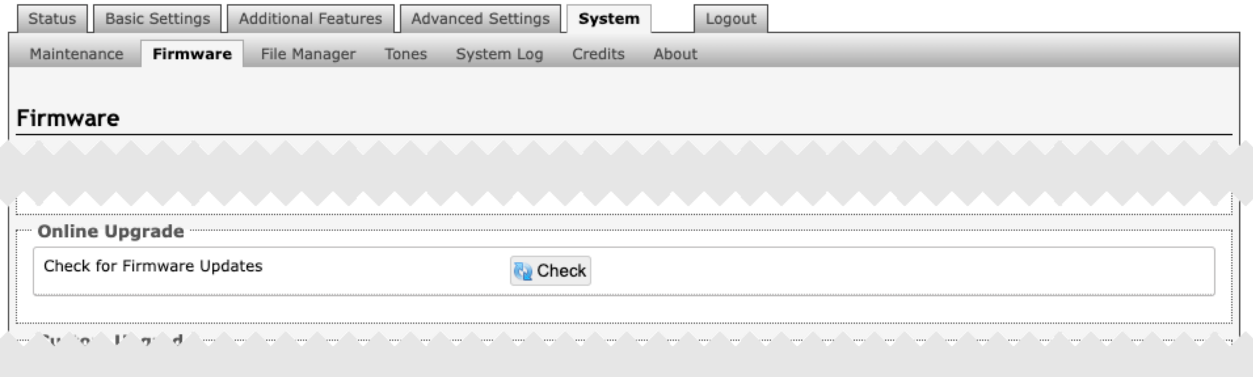
Installed Firmware

Product Firmware algo-8507-5.5

Online Upgrade

Product Firmware	Displays the current firmware on the device.

Online Upgrade



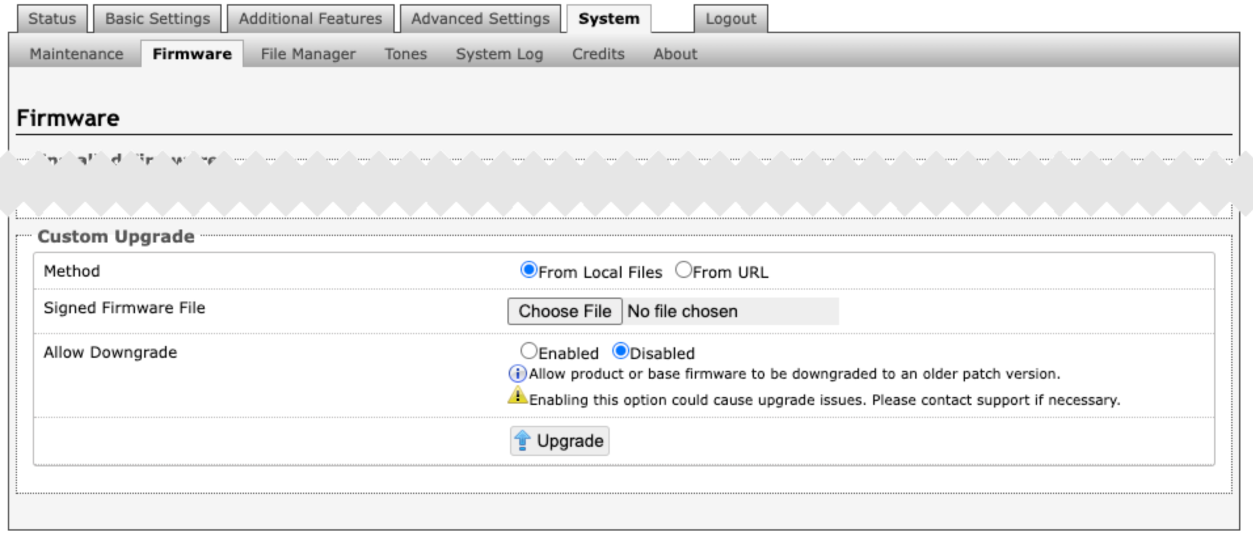
Firmware

Online Upgrade

Check for Firmware Updates

Check for Firmware Updates	Click **Check** to check for the latest firmware. If the firmware is up to date, **Latest Firmware** will state **Firmware up to date**. If your firmware is outdated, the new firmware availability will be listed. Internet connection is required.

Custom Upgrade



Firmware

Custom Upgrade

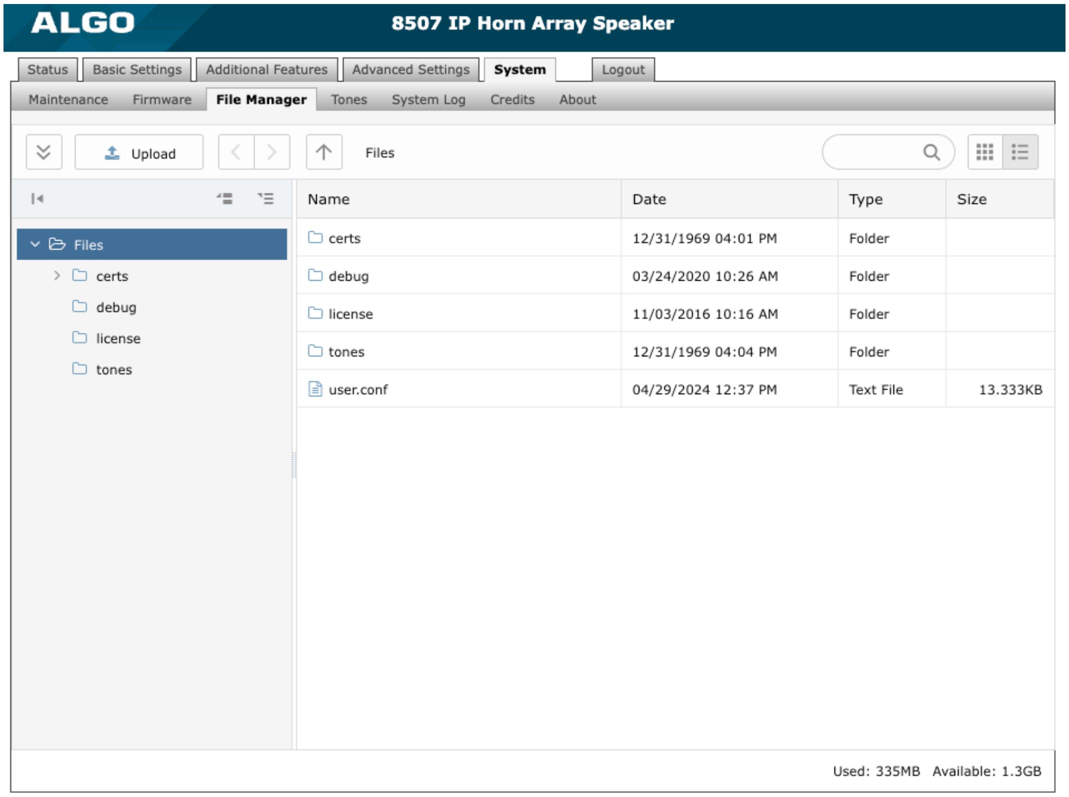
Method	● From Local Files ○ From URL
Signed Firmware File	Choose File No file chosen
Allow Downgrade	○ Enabled ● Disabled ⓘ Allow product or base firmware to be downgraded to an older patch version. ⚠ Enabling this option could cause upgrade issues. Please contact support if necessary.

Method	Select a method for firmware upgrades to occur. This can be done **From Local Files** or **From URL.**
Signed Firmware File	Use to upgrade firmware from a local file. To do this, download the firmware file from https://www.algosolutions.com/firmware-downloads/ then upload the file by clicking on **Choose File** and selecting the firmware file.

	Click **Upgrade** at the bottom of the interface. Once the upgrade is complete, you can confirm the firmware version is changed by looking at the top right of the web interface.
Upgrade URL	Instead of downloading the firmware file https://www.algosolutions.com/firmware-downloads/, you may add the download link here instead. Click **Upgrade** at the bottom of the interface. Once the upgrade is complete, you can confirm the firmware version is changed by looking at the top right of the web interface.
Allow Downgrade	Enable to allow product or base firmware to be downgraded to an older patch version. Enabling this option could cause future upgrade issues. If you require downgrading, please contact support@algosolutions.com for assistance.

8.8 File Manager

The 8507 has 1GB of storage space for additional files.



Name	Date	Type	Size
certs	12/31/1969 04:01 PM	Folder	
debug	03/24/2020 10:26 AM	Folder	
license	11/03/2016 10:16 AM	Folder	
tones	12/31/1969 04:04 PM	Folder	
user.conf	04/29/2024 12:37 PM	Text File	13.333KB

Used: 335MB Available: 1.3GB

Figure 24: View files in the ***File Manager*** *tab.*

certs Folder

If you have enabled **Validate Server Certificate** under **Advanced Settings → Advanced SIP** or **Advanced Settings → Provisioning** and want to validate against additional certificates, you can upload them here.

To install a public CA certificate on the Algo device, follow the steps below:

1. Obtain a public certificate from your Certificate Authority (Base64 encoded X.509 .pem, .cer, or .crt).
2. Open the **certs** folder in the web interface by going to **System → File Manager**.
3. Upload the certificate files into the **certs** folder by clicking **Upload** in the top left corner of the file manager and select the certificate.

Reach out to support@algosolutions.com to get the complete list of pre-loaded trusted certificates**.**

debug Folder

If you have any challenges with the device and work with the Algo support team to overcome or fix them, the debug folder will be used. The device will generate files containing information about the device and put them in the debug folder. You do not need to use this folder unless directed to by the Algo support team.

license Folder

If you would like to use Informacast on a device that hasn't been bundled with an Informacast license, you will need to purchase a license and put it into the license folder in the file manager.

tones Folder

Custom audio files may be uploaded to play notifications. Audio files should be stored in the **tones** directory.

Existing files may be modified by downloading the original file, making the desired changes, then uploading the updated file with a different name. To download, right-click the tone and click **Download**.

Audio files must be in the following format:

- WAV or MP3 format
- Smaller than 200 MB

File names must be limited to 32 characters, with no spaces.

For further instructions, reference the Custom Tone Conversion and Upload Guide.

8.9 System Log

System log files are automatically created and can assist with troubleshooting if the device does not behave as expected.

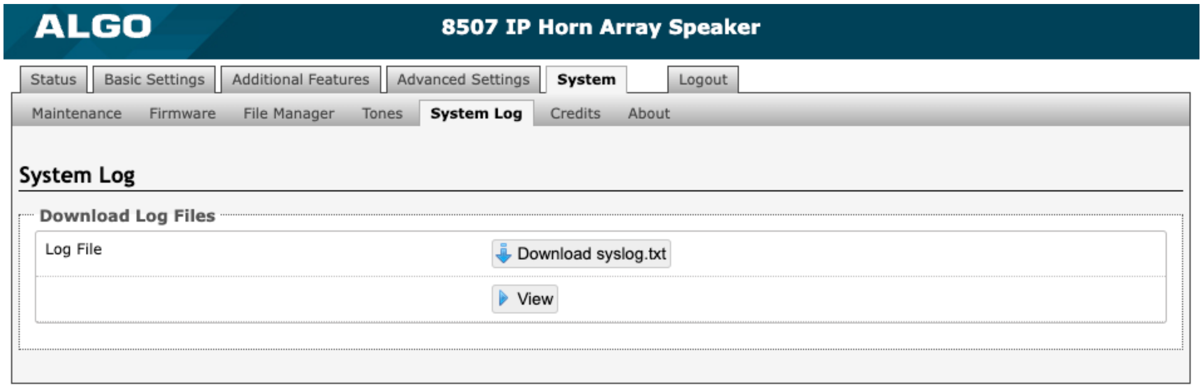


Figure 25: Configure system log settings in the web interface.

8.10 Logout

Log out of the web interface.

9 SPECIFICATIONS

View 8507 technical specifications.

10 FCC COMPLIANCE STATEMENT

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operations of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his or her own expense.