8301 IP Paging Adapter & Scheduler

User Guide

AL061-UG-GP308301-230508
Firmware Version 5.3.2
support@algosolutions.com
July 25, 2023

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

Information Notices

Warning

Warning indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury

Caution

Caution indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury and/or damage to the equipment or property

Important

Important indicates a key piece of updates, information, and instructions that need to be followed for correct and safe use of the device

Note

Note indicates useful updates, information, and instructions that should be followed

Tips & Tricks

Tips & Tricks indicate helpful instructions that could help you with your device

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

Table of Contents

Tables

Figures

IMPORTANT WARNING AND SAFETY INFORMATION

Important Notice

This product is powered by a certified limited power source (LPS), Power over Ethernet (PoE); through CAT5 or CAT6 connection wiring to an IEEE 802.3af compliant network PoE switch. The product is intended for installation indoors. All wiring connections to the product must be in the same building. If the product is installed beyond the building perimeter or used in an inter-building application, the wiring connections must be protected against overvoltage/transient. Algo recommends that this product is installed by a qualified electrician.

If you are unable to understand the English language safety information, then please contact Algo by email for assistance before attempting an installation support@algosolutions.com.

Consignes de Sécurité Importantes

Ce produit est alimenté par une source d'alimentation limitée certifiée (alimentation par Ethernet); des câbles de catégorie 5 et 6 joignent un commutateur réseau à alimentation par Ethernet homologué IEEE 802.3af Le produit est conçu pour être installé à l'intérieur. Tout le câblage rattaché au produit doit se trouver dans le même édifice. Si le produit est installé au-delà du périmètre de l'édifice ou utilisé pour plusieurs édifices, le câblage doit être protégé des surtensions transitoires. Algo recommande qu'un électricien qualifié se charge de l'installation de ce produit.

Si vous ne pouvez comprendre les consignes de sécurité en anglais, veuillez communiquer avec Algo par courriel avant d'entreprendre l'installation au support@algosolutions.com.

Información de Seguridad Importante

Este producto funciona con una fuente de alimentación limitada (Limited Power Source, LPS) certificada, Alimentación a través de Ethernet (Power over Ethernet, PoE); mediante un cable de conexión CAT5 o CAT6 a un conmutador de red con PoE en cumplimiento con IEEE 802.3af. El producto se debe instalar en lugares cerrados. Todas las conexiones cableadas al producto deben estar en el mismo edificio. Si el producto se instala fuera del perímetro del edificio o se utiliza en una aplicación en varios edificios, las conexiones cableadas se deben proteger contra sobretensión o corriente transitoria. Algo recomienda que la instalación de este producto la realice un electricista calificado.

Si usted no puede comprender la información de seguridad en inglés, comuníquese con Algo por correo electrónico para obtener asistencia antes de intentar instalarlo: support@algosolutions.com.

Wichtige Sicherheitsinformationen

Dieses Produkt wird durch eine zertifizierte Stromquelle mit begrenzter Leistung (LPS – Limited Power Source) betrieben. Die Stromversorgung erfolgt über Ethernet (PoE – Power over Ethernet). Dies geschieht durch eine Cat-5-Verbindung oder eine Cat-6-Verbindung zu einer IEEE 802.3af-konformen Ethernet-Netzwerkweiche. Das Produkt wurde konzipiert für die Installation innerhalb eines Gebäudes. Alle Kabelverbindungen zum Produkt müssen im selben Gebäude bestehen. Wenn das Produkt jenseits des Gebäudes oder für mehrere Gebäude genutzt wird, müssen die Kabelverbindungen vor Überspannung und Spannungssprüngen geschützt werden. Algo empfiehlt das Produkt von einem qualifizierten Elektriker installieren zu lassenv.

Sollten Sie die englischen Sicherheitsinformationen nicht verstehen, kontaktieren Sie bitte Algo per Email bevor Sie mit der Installation beginnen, um Unterstützung zu erhalten. Algo kann unter der folgenden E-Mail-Adresse erreicht werden: support@algosolutions.com.

安全须知

本产品由认证的受限电源(LPS)，以太网供电(PoE)，通过 CAT5 或 CAT6 线路联接至 IEEE 802.3af 兼容的 PoE 网络交换机供电。本产品适用于室内或建筑物周边安装。所有联 接本产品的线路必须源自同一建筑物。本产品如需用于超出建筑物周边范围或跨建筑物的安 装，线路联接部分必须有过压和瞬态保护。Algo 建议本产品由专业电工安装。

如果您对理解英文版安全须知有问题，安装前请通过电子邮件和 Algo 联 系. support@algosolutions.com.

EMERGENCY COMMUNICATION

If used in an emergency communication application, the 8301 IP Paging Adapter & Scheduler should be routinely tested. SNMP supervision is recommended for assurance of proper operation. Contact Algo for other methods of operational assurance.

DRY INDOOR LOCATION ONLY

The 8301 IP Paging Adapter & Scheduler is intended for dry indoor locations only. For outdoor locations Algo offers weatherproof speakers and strobe lights.

CAT5 or CAT6 connection wiring to an IEEE 802.3af (PoE) compliant network PoE switch must not leave the building perimeter without adequate lightning protection.

No wiring connected to the 8301 IP Paging Adapter & Scheduler may leave the building perimeter without adequate lightning protection.

1 GENERAL

1.1 Introduction

Algo's 8301 IP Paging Adapter & Scheduler is a SIP-compliant, multicast-capable endpoint device for integrating consumer, commercial, and professional audio amplifiers into an IP-based Unified Communication (UC) environment for voice paging and notification. Emulating a page port similar to what is found on legacy PBX or key systems, the 8301 connects directly to traditional analog amplifiers, offering a simple and easy interface to a VoIP phone system. The 8301 uses a balanced and isolated line level output that reduces hum and which can connect with any amplifier with an input impedance between 600 Ohm to 10 kOhm.

The 8301 also includes a scheduler, synchronized to NTP, to provide scheduled bells, tones, and customer service or emergency announcements for schools, retail shops, manufacturing facilities, and healthcare institutions. 1 GB of memory is available in the device to store audio files, which can be played via the 8301 Line Out and, if desired, as a multicast to other Algo speakers, paging adapters, and display speakers.

As a 3rd-party, SIP-compliant device, the 8301 is designed to seamlessly integrate into most leading IP-based UC and Mass Notification platforms. The 8301 is easily configured using central provisioning features or by accessing the web interface via a web browser.

The 8301 supports three types of extensions, page, ring, and emergency alerts. The different types of extensions are assigned by entering the SIP credentials on the correct section in the configuration portal. Page extensions by nature auto-answer and open a voice path, allowing for live announcements. Ring extensions don't answer the incoming call, instead they play a configurable pre-recorded announcement. This is traditionally used as a loud ringer/night bell. Lastly, emergency alert extensions are used to communicate critical situations. They use customizable pre-recorded announcements and are generally configured to loop over the announcement until it is cancelled. These extensions can be registered simultaneously but note that some systems limit devices to a single registration.

2 SETUP AND INSTALLATION

What is Included

The following items are included with the purchase of this device:

- 8301 Paging Adapter & Scheduler
- Wall mount bracket and screws
- Network cable
- Two (2) pluggable terminal blocks for relay input and output
- Flat head screwdriver
- Getting Started Sheet

What is Not Included

The following items are not included with the purchase of this device:

- Optional Wall Switch (Algo 1202, 1203, 1204, 1205)
- Optional 2504 Output Cable: XLR-Mini Female to XLR Male
- Optional 2505 Input Cable: XLR-Mini Male to XLR Female

2.1 Getting Started – Quick Install and Test

Important

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

1. Connect the 8301 Paging Adapter & Scheduler to an IEEE 802.3af compliant PoE network switch or PoE Injector. The blue lights on the front will remain on until boot up is completed – about 60 seconds.
2. After the blue lights turn off, press the reset switch (RST) to hear the IP address over the analog outputs (e.g., headset can be connected to the green Aux output port). The IP address may also be discovered by downloading the Algo locator tool or a third-party network scanner to find Algo devices on your network: www.algosolutions.com/locator. Algo device's MAC address starts with 00:22:ee.
3. Connect the adapter Line Out to an amplifier using the mini-XLR connector or pluggable terminal block.
4. Access the 8301 Paging Adapter & Scheduler web page by entering the IP address into a browser (e.g., Chrome, Firefox, or Edge) and login using the default password ***algo.***
5. Enter the IP address or the domain name for the SIP server into the SIP Domain field under the *Basic Settings* → *SIP* tab.
6. Enter the credentials (SIP Extension, Authentication ID, and Password) for the Page and/ or Ring extension. Leave the credentials blank for either extension if there is no intended use to have both registered.

Note

The Authentication ID may also be called Username for some SIP servers, and in some cases may be the same as the SIP extension.

7. Verify the extension is properly registered with the SIP server in the Status tab. Ensure the SIP Registration is “Successful”.
8. Make a call to the adapter by dialing the registered SIP extension of the adapter from a telephone.

2.2 Installation

The 8301 is wall mountable in a horizontal orientation using the supplied bracket.

Figure 1: Wall Mount

Example installation on 1/2” drywall:

Use appropriate drywall anchors for #8 screws, and pre- drill per anchor manufacturer’s instructions. Insert 4 anchors into the wall, and then attach bracket to wall anchors using #8 screws. Snap the 8301 into the bracket.

2.2.1 Programming and Configuration

The 8301 is configurable using the web interface or provisioning features.

After booting up, the blue lights on the front will turn off and the adapter will have obtained an IP address. If there is no DHCP server, the 8301 will default to the static IP address 192.168.1.111.

Press the reset switch (RST) to hear the IP address over the analog outputs (e.g., headset can be connected to the green output port). The IP address may also be discovered by downloading the Algo locator tool to find Algo devices on your network: www.algosolutions.com/locator.

Enter the IP address (e.g., 192.168.1.111) into a browser such as Chrome, Firefox, or Edge. The web interface should be visible, and the default password will be algo in lower case letters.

3 APPLICATIONS

3.1 Connecting Paging Amplifier to UC Environment

The 8301 Paging Adapter & Scheduler is typically used to connect an existing paging amplifier to a UC environment either as a SIP extension or multicast endpoint for voice paging, emergency alerting, night bell / loud ringing, bell scheduling and playing music. It provides a hybrid voice paging solution to integrate analog speaker infrastructure and multicast to Algo IP speakers, strobe lights and paging adapters, in addition to multicast supported IP telephones.

The Line output of the 8301 is connected directly to the dry audio input on an amplifier with an input impedance between 600 Ohm and 10 kOhm.

For amplifiers connected directly to the dry page port of an existing telephone system, the 8301 will provide a very similar interface providing both dry page audio and dry contact closure to activate the amplifier (if required).

For amplifiers connected to a FXS port of ATA through a “telephone answering device”, the 8301 will replace the answering device and eliminate the need for a FXS port or ATA. Please note the 8301 does not provide a FXS port interface.

The 8301 may also be configured as a multicast transmitter to a set of IP endpoints, such as other Algo IP endpoints and certain multicast-capable IP phones.

3.2 Notification

The 8301 is often used for notification alerting for emergency (e.g., lockdown, evacuation, reverse evacuation), safety (e.g., medical, workplace accident), security events (e.g., OSHA or similar workplace regulations).

3.3 Scheduling

The 8301 includes a calendaring functionality synchronized to NTP and can be used to schedule school bells, play automated announcements for retail and healthcare, and notify workplace shift changes and breaks.

3.4 Multicasting

The 8301 can be used as the central multicasting device in Algo endpoint deployments where it is desired to keep the central multicasting device placed in a secure closet or location away from traffic areas.

4 FEATURES

4.1 SIP Paging: Registering an 8301 Device

The 8301 Paging Adapter & Scheduler can be registered as a 3rd-party SIP extension with a hosted or enterprise Communications Server supporting 3rd-party SIP endpoints.

To register the adapter with the SIP server, use the *Basic Settings* → *SIP* tab in the web interface to enter the Communication Server IP address/domain name, extension, username, and password. This information will be available from the IT Administrator.

If VLANs are used, navigate to the *Advanced Settings* → *Network* tab to set VLAN options. (Note, once the adapter is using VLAN you will need to be on the same VLAN to access the web interface.)

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

There are several configurable adapter options, such as:

- Increase or Decrease Volume
- Enable AGC (automatic gain control)
- Ambient noise compensation
- Customize pre-announce tone file
- Passcode protection

The best voice paging quality and intelligibility will be obtained using the G.722 wideband audio codec. Most current IP telephones support G.722 which is sometimes referred to as "HD" voice or audio.

4.2 SIP Paging: Multiple Algo SIP Endpoints (Using Multicast)

Multicast features in the 8301 Paging Adapter & Scheduler require that only the first adapter be registered as a SIP extension. Additional Algo IP endpoints, including any combination of paging adapters, speakers, and visual alerters, may be added as multicast Receivers receiving a stream from the SIP registered Transmitter adapter, provided that only a single audio stream will be active at any given time across any or all of the devices. If multiple unique audio streams are needed simultaneously more than one Transmitter device will be required.

The adapter configured as the transmitter will simultaneously stream audio to the Receiver adapters. The Receiver adapters do not require SIP extensions and do not need to register with the SIP Communication Server.

To enable multicast streaming from the Transmitter adapter, go to the web interface and navigate to the *Basic Settings* → *Multicast* tab. Choose multicast mode '**Transmitter (Sender)**' and pick '**All Call**' for the Transmitter single zone.

To enable multicast monitoring in the Receiver endpoints, go to the web interface for each endpoint and navigate to the *Basic Settings* → *Multicast* tab. This time though, choose multicast mode **'Receiver (Listener)'**. There is no need to select a zone as 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.

Note
*See "**Basic Setting Tab – Multicast**" section below for more configuration options and instructions.*

4.3 SIP Paging: Multiple Algo SIP Endpoints (Using Multicast)

In some cases, it may be desirable for every adapter to have a SIP extension. Multicast may still be used to page multiple Algo IP endpoints, but each endpoint can also be called individually or generate a call when appropriately configured. An Algo IP endpoint configured as a Multicast Receiver will give highest priority to the SIP extension(s) registered.

Communication servers capable of dialing multiple SIP extensions simultaneously for paging may create zones by calling "paging groups" to page telephone speakers in conjunction with speaker endpoints. Certain IP phones are also multicast capable. These can be configured similarly to Algo IP endpoints in receiver mode to participate in the desired zones.

4.4 Background Music Streaming

The 8301 Paging Adapter & Scheduler, set as a Multicast transmitter, can stream background music to other Algo Receiver devices on the network from a music source connected to the 8301's AUX Input. Note music may simultaneously be streamed through the local outputs.

When multicasting music, ensure that Automatic Gain Control (AGC) is 'Disabled' in *Basic Settings* → *Features* tab on all the receiver devices. Meanwhile, on the Multicast sender device, select 'G.722' or 'Opus' for the Sender Output Codec setting in *Advanced Settings* → *Advanced Multicast* tab.

4.5 Multicast Page Zones

The 8301 IP Paging Adapter & Scheduler supports nine 'basic' multicast zones. These zones are defined by the multicast IP addresses.

These zones are defined below but may be used in other ways. The important consideration is that there is a priority hierarchy – streaming activity on a zone higher on the list will be treated as a higher priority than a zone lower down on the list – with music being the lowest priority (multicast receiver side). The multicast transmitter side treats event priority based on the event itself, not the zone. Contact Algo support for more details.

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

There are two options for Paging to multiple zones: 'DTMF Selectable Mode' or via multiple page extensions.

The 'DTMF Selectable Mode' offers a dynamic page zone selection and requires only the Sender device to have a registered SIP Extension. To page, dial the SIP extension of the Sender device and then dial the desired DTMF page zone (e.g., 1, 2, etc.) on the keypad. DTMF digits and their corresponding zone numbers are available in the *Advanced Settings → Advanced Multicast* tab.

Note
DTMF codes for zones 10 and higher start with an "".*

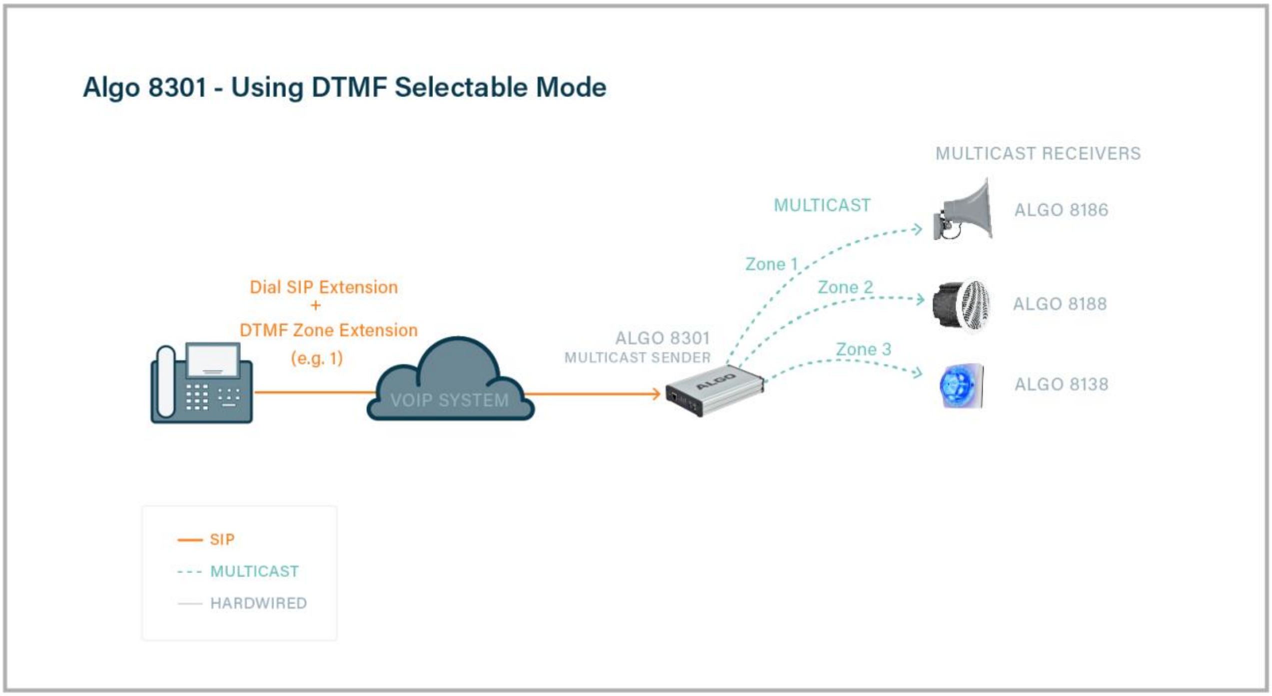


Figure 2: Using DTMF Selectable Mode

Alternatively, multiple SIP extensions can be registered on the Sender device. Each extension is mapped to a unique zone, allowing zones to be called directly (for instance from speed-dial keys) without the use of DTMF. See *Additional Features → More Page Extensions* tab.

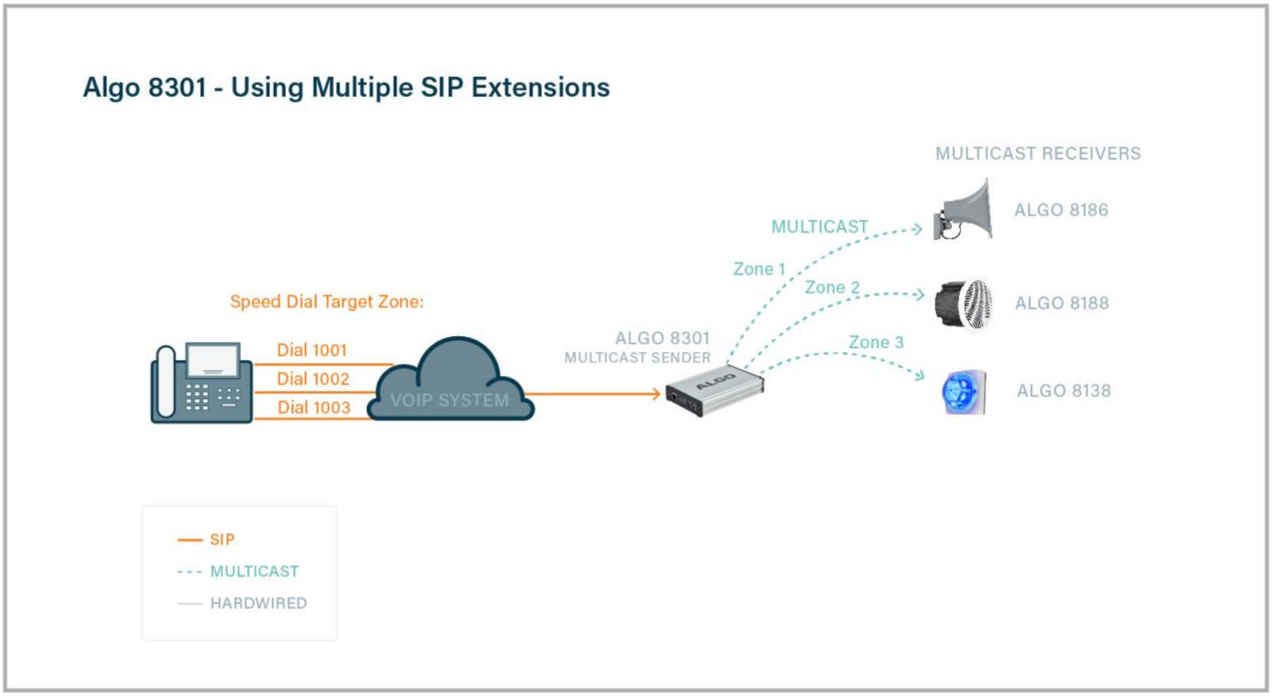


Figure 3: Using Multiple SIP Extensions

'Expanded' zones can also be enabled, allowing up to 50 zones in total. These have the same behaviours as the basic zones but are hidden by default to simplify the interface.

4.6 SIP Ring Event

Set Monitoring Mode to 'Monitor "Ring" event on registered SIP extension' on the *Basic Settings* → *SIP* tab. When a call is made to the SIP extension the 8301 IP Paging Adapter & Scheduler will play the selected audio file from memory (it will not answer the call). Often, the 8301 will be part of a hunt group or ring group to ring in conjunction with a telephone.

4.7 SIP Activated Notification Alerts

In addition to voice paging, the 8301 IP Paging Adapter & Scheduler can play audio files for emergency, safety, and security announcements, customer service, shift changes, etc.

Audio files can be stored in the device's memory and played over a speaker in response to an event such as an inbound call, relay input, or automated schedule, as well as multicast to other Algo SIP endpoints on the network. See *Additional Features* → *Emergency Alerts* and *Additional Features* → *Input / Output* tabs for more details.

4.8 TLS for SIP Signaling and Provisioning

Algo devices that support firmware 1.6.4 or later support Transport Layer Security (TLS). This feature adds security by ensuring that Algo products can trust the hosted SIP server. This is useful for when third-party devices or attackers may try to intercept, replicate, or alter Algo products and try to connect to the server. TLS protocol will ensure that third parties cannot read/modify any actual data. Previously, security was less of a concern because phone systems were on isolated networks, but hosted services are becoming increasingly more common. Using a hosted SIP service requires traffic to be sent over the public internet and thus much more susceptible to attacks. Signed certificates are important pieces in the operation of Algo devices to ensure the security, integrity, and privacy of device communication. Algo components that use TLS are **Provisioning** and **SIP Signaling**.

Algo devices come pre-loaded with certificates from a list of trusted certificate authorities (CA), which are installed in the hardware at the time of manufacture. Note these pre-installed trusted certificates are not visible to users and are separate from the 'certs' folder.

The TLS handshake happens to make sure that the client and server can trust each other, and once that trust is established, the two parties can freely send encrypted data and decrypt any data that they receive. After the TLS handshake process is complete, a TLS session is established, and the server and client can then exchange messages that are symmetrically encrypted with a shared (pre-sender) secret key.

For further details reference the Algo TLS guide for SIP Signalling and HTTPS Provisioning.

4.8.1 Uploading Public CA Certificates to Algo SIP Endpoints

If the particular CA Certificate is not installed by factory, you can easily upload your own. To install the public CA certificate on the Algo 8301, follow the steps below:

1. Obtain a public certificate from your Certificate Authority (Base64 encoded X.509 .pem, .cer, or .crt).
2. In the web interface of the Algo device, navigate to the *Advanced Settings* → *File Manager* tab.
3. Upload the certificate files into the 'certs/trusted' directory. Click the Upload button in the top left corner of the file manager and browse to the certificate.

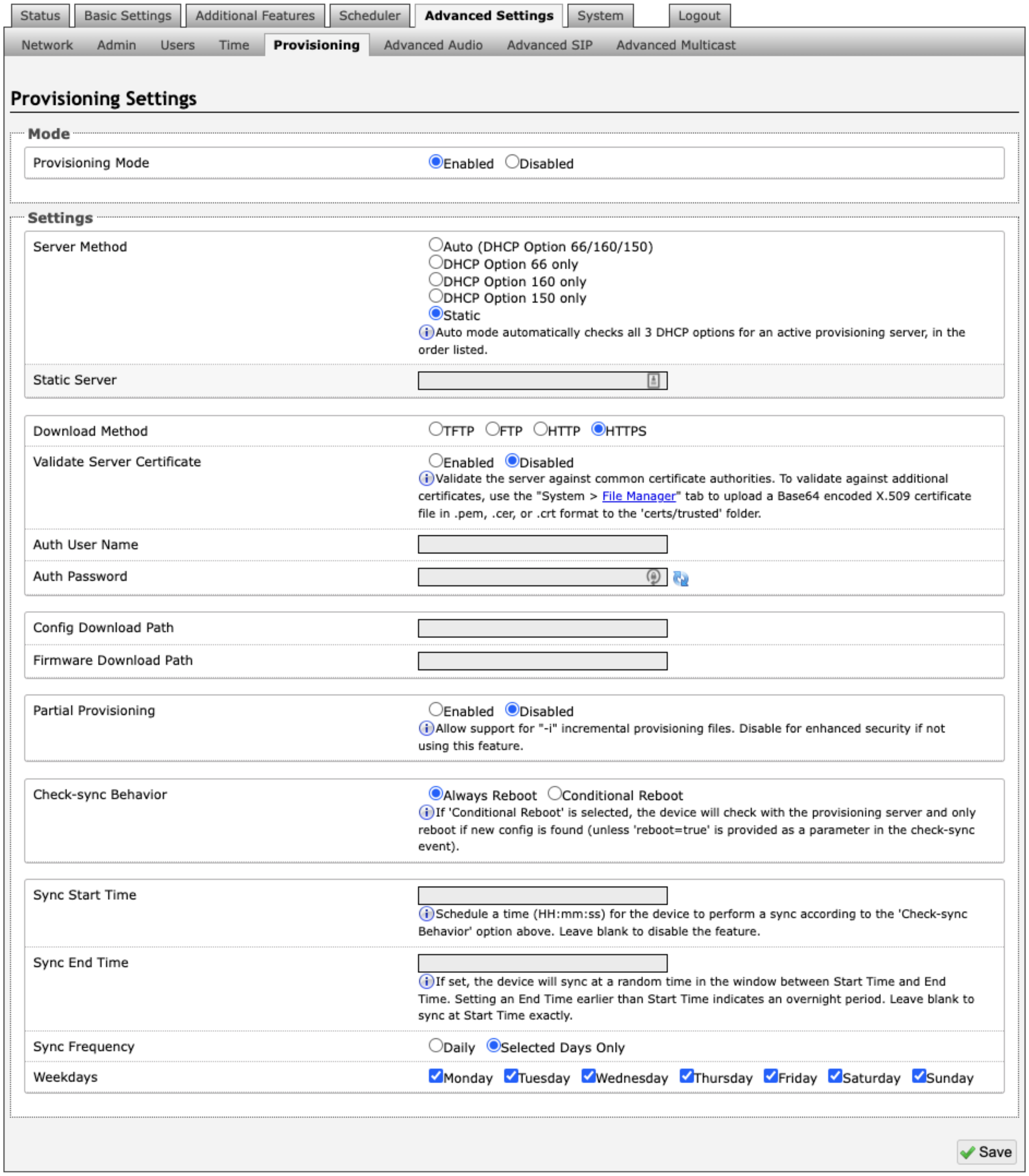
Reach out to support@algosolutions.com to get the complete list of trusted certificate authorities loaded from factory.

For **SIP** TLS, if the 'Validate Server Certificate' option is enabled in *Advanced Settings* → *Advanced SIP* tab, then the device will 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.

For **Provisioning**, if HTTPS is selected and the 'Validate Server Certificate' option is enabled in the *Advanced Settings* → *Provisioning* tab, then the device will 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.

4.8.2 HTTPS Provisioning

Provisioning can be secured by setting the 'Download Method' to 'HTTPS' (under the *Advanced Settings* → *Provisioning* tab). This prevents configuration files from being read by an unwanted third-party. This resolves the potential risk of having sensitive data stolen, such as admin passwords and SIP credentials.



Important

To verify the server 'Enable' the 'Validate Server Certificate' option. This then checks if the certificate that is provided by the server is signed by any of the CAs included in the list of trusted CAs (used by the Debian infrastructure and Mozilla browsers). If we receive a certificate signed by any of these CAs, then that server will be trusted.

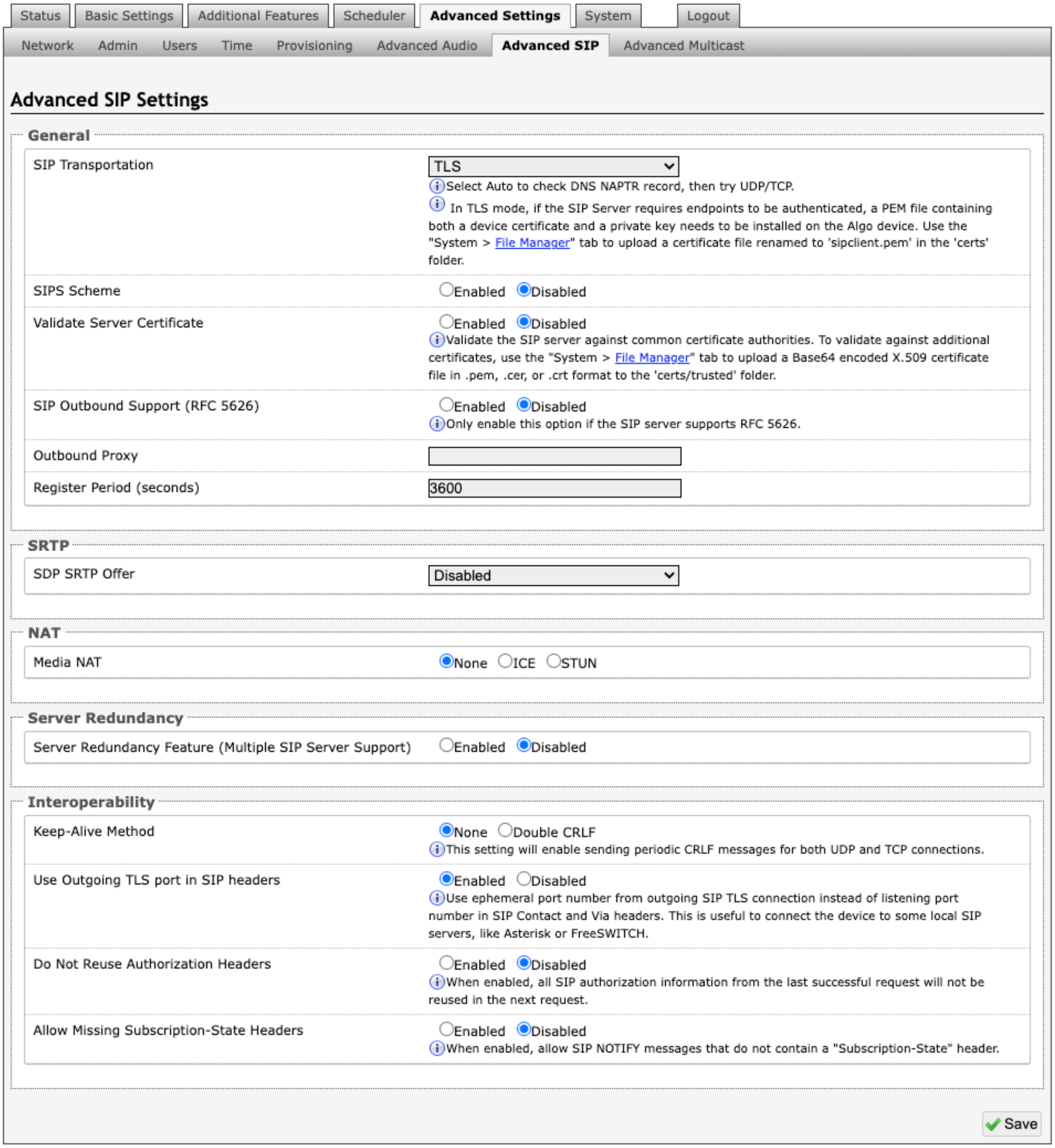
The 'Validate Server Certificate' parameter can also be enabled through provisioning:

Prov.download.cert = 1

4.8.3 Securing SIP Signaling (and RTP Audio)

SIP signalling is secured by setting '**SIP Transportation**' to 'TLS' (under the *Advanced Settings* → *Advanced SIP* tab). SIP transportation refers to the underlying protocol used for transmitting SIP messages between different entities in a network. Setting it to 'TLS' ensures that the SIP traffic will be encrypted. SIP signalling is responsible for establishing the call (the control signals to start and end the call with the other party), but it does not contain the audio.

For the audio (voice) path, use the setting '**SDP SRTP Offer**'. Setting this to '**Optional**' means the SIP call's RTP audio data will be encrypted (using SRTP) if the other party also supports audio encryption. If the other party does not support SRTP, then the call will still proceed, but with unencrypted audio. To make audio encryption mandatory for all calls, set '**SDP SRTP Offer**' to '**Standard**'. In this case, if the other party does not support audio encryption, then the call attempt will be rejected.


Status
Basic Settings
Additional Features
Scheduler
Advanced Settings
System
Logout
Network
Admin
Users
Time
Provisioning
Advanced Audio
Advanced SIP
Advanced Multicast
Advanced SIP Settings
General
SIP Transportation
TLS
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
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.
Save

5 WIRING CONNECTIONS

The wiring diagram below illustrates one of the most common use cases, where the Line Output of the 8301 is connected directly to the dry audio input on an amplifier with an input impedance between 600 Ohm and 10 kOhm. The output level of the 8301 can be adjusted to match the amplifier's input specification. Check the *Basic Settings → Features* section for more details. The optional dry contact closure can be used to activate the amplifier (if required).

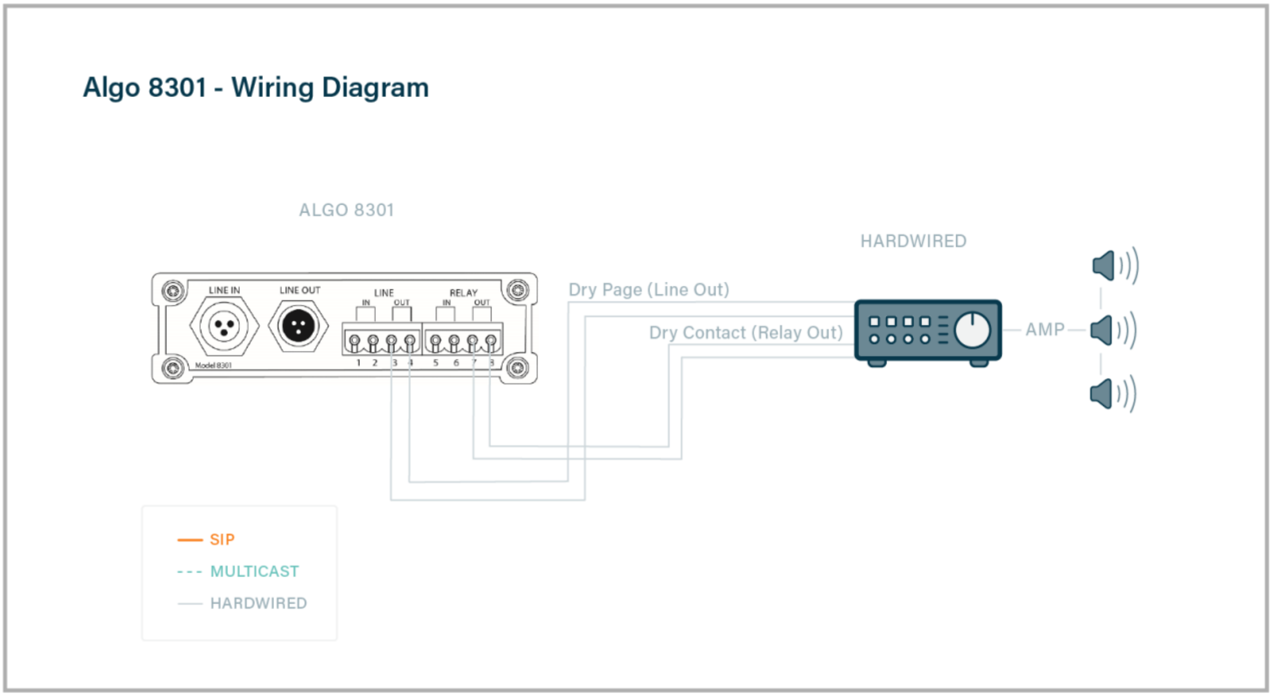


Figure 4: Use Case Wiring Diagram

5.1 Connecting Input Devices to 8301

The relay input of the Algo 8301 IP Paging Adapter & Scheduler can be activated by any normally open or normally closed switch, or one of several Algo input buttons/interfaces (e.g. ,1202 Call Button, 1203 Call Switch, 1204 Volume Control Switch or 1205 Audio Interface). The input switches can be connected to the back of the 8301 via the included Terminal Block on the 'Relay Input' pair. To configure the Relay Input Mode, check the *Additional Features → Input/Output* section.

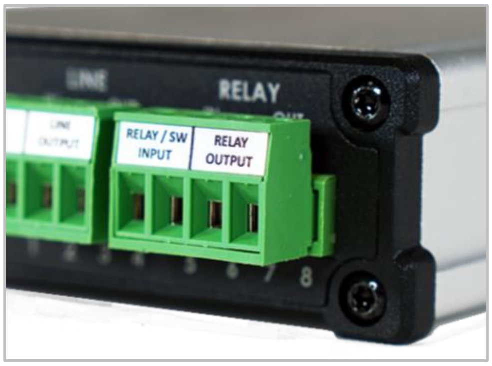


Figure 5: 8301 Relay Input

1202 Call Button

A pair of wires from the terminal block Relay Input on the back of the 8301 can connect to the **center pair** of the modular connector at the back of the Call Button. For more details check the Algo 1202 Installation Sheet.

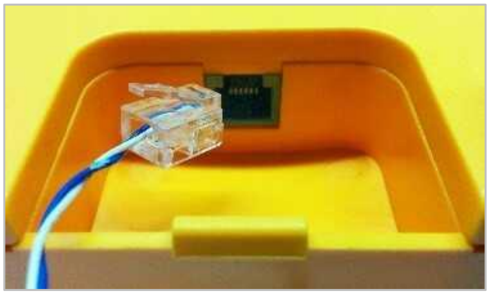


Figure 6: 1202 Call Button Wiring

1203 Call Switch

A pair of wires can be run from the back of the device via a screw output connector to the 8301 via the Relay Input. For more details check the Algo 1203 Getting Started Sheet.

Figure 7: 1203 Call Switch Wiring

1204 Volume Control Switch

Install the 1204 by connecting a single twisted pair wire to its terminal block (not polarity sensitive) and wire it to the Relay Input on the 8301. For more details check the Algo 1204 Getting Started Sheet.

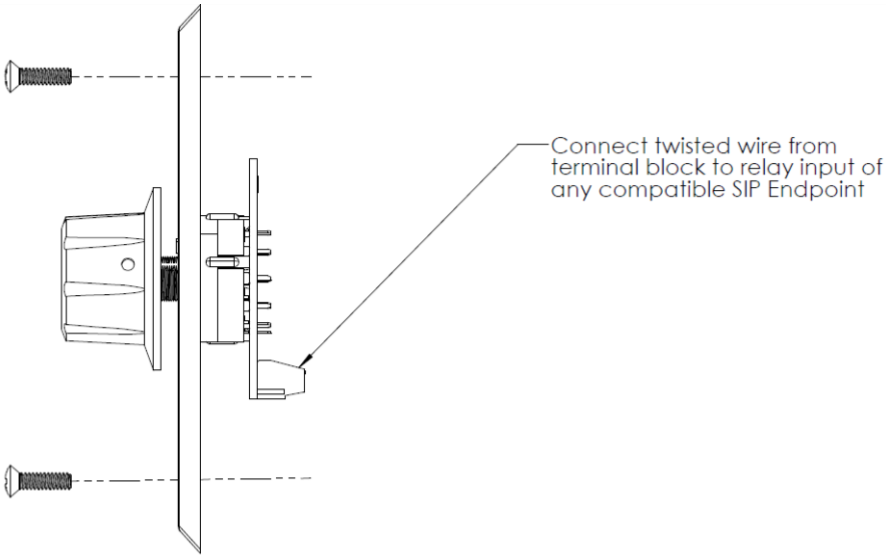


Figure 8: 1204 Volume Control Switch Wiring

1205 Audio Interface

Two pairs of wires connect the 1205 Audio Interface to the 8301. One pair is for balanced audio and one pair is for communicating the rotary switch position.

Connect the Relay Input switch terminals of the 1205 Audio Interface to the “RELAY IN” of the 8301. Next, connect the Line In audio terminals of the 1205 Audio Interface to the Line In of the 8301. Neither of the pair is polarity sensitive. For more details check the Algo 1205 Getting Started Sheet.

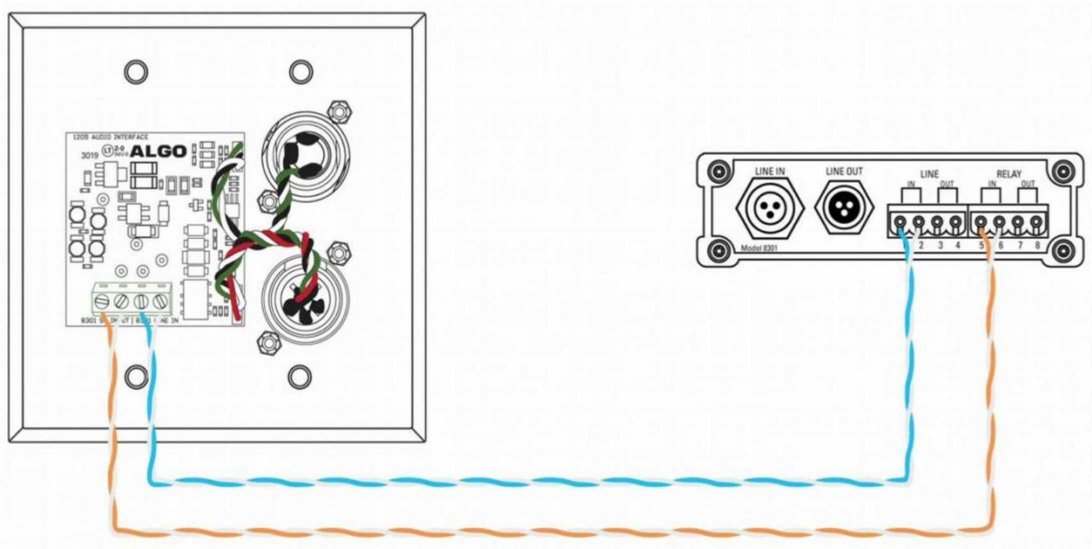


Figure 9: 1205 Audio Interface Wiring

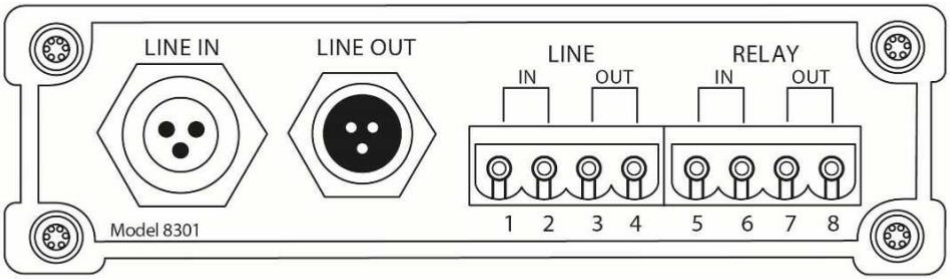


Figure 10: 8301 Paging Adapter & Scheduler Front View

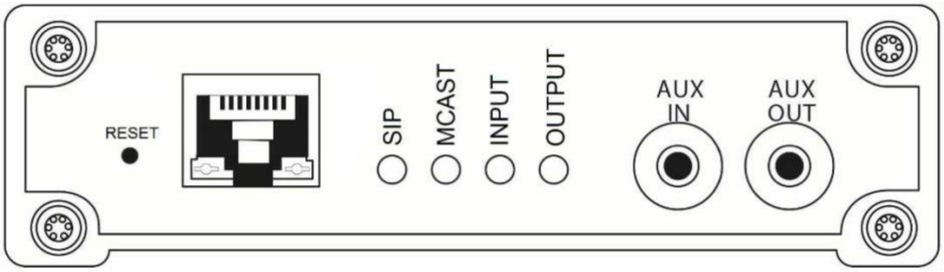


Figure 11: 8301 Paging Adapter & Scheduler Back View

Network Connection

The 8301 provides a RJ45 jack for network connection. A cable run from the switch can be terminated to a modular jack with connection by patch cord or terminated with a RJ45 plug.

PoE (Power over Ethernet) must be 48 V 350 mA IEEE 802.3af compliant whether provided by the network switch or injector.

There are two lights on the Ethernet jack:
Green light: On when Ethernet is working, flickers off to indicate activity on the port.

Amber light: Off when successful 100Mbps link is established. Typically, on only briefly at power up. *(Exception: the amber LED behaviour will be reversed on “Rls 1” hardware)*

Under normal conditions, the Amber light will turn on immediately after the Ethernet cable is first connected. This indicates that PoE power has been successfully applied. Once the device connects to the network, it will switch to the Green light instead, which will typically flicker indicating traffic on the network.

AUX IN 3.5 mm Jack (Front)

Analog line level input from a smartphone or similar device for music input. Non-isolated.

AUX OUT 3.5 mm Jack (Front)

Analog line level output for compatible PC speakers or headset. Non-isolated.

LINE IN XLR-MINI (Back)

Balanced and isolated audio (Page or music) input can be configured for pass-through to Line Out (when paging is idle), and/or for broadcast via multicast.

Line OUT XLR-MINI (Back)

Balanced and isolated audio output to external amplifier. Locking mini-XLR female to standard XLR male cable available. Output level defined using web interface.

Terminal Block Line In

Balanced and isolated wire pair input parallel to XLR-MINI LINE IN (polarity independent).

Terminal Block Line Out

Balanced and isolated wire pair output parallel to XLR-MINI LINE OUT (polarity independent).

Terminal Block Relay In

By default, these terminals are inactive. Connection options are a normally closed switch, normally open switch, 1202 Call Button, 1203 Call Switch, 1204 Volume Control Switch, 1205 Audio Interface or EOL resistor termination.

Terminal Block Relay Out

By default, these terminals provide a contact closure when the 8301 IP Paging Adapter is active. Please note this is a normally open relay only.

5.2 Blue LED Indicators

All four (4) blue lights will be on during power up and boot process.

SIP

A steady light will appear when a SIP extension is registered. The light will blink when the device is engaged in a SIP call.

MCAST

A steady light will appear when the 8301 receives multicast messages as a Receiver. The light will blink when the 8301 sends output to Receivers as a Transmitter.

INPUT

The input light will be 'on' when the device is actively using an analog input port based on the configuration set in the web interface and the active state (it does not detect a physical connection to the audio jack by default).

OUTPUT

The output light will be on when analog output is enabled.

5.3 Reset

A recessed reset button (RST) next to the Ethernet Jack can only be used to reset the 8301 IP Paging Adapter & Scheduler at the time of power up. To return all the settings in the 8301 to the factory default, reboot, or power cycle the 8301. Wait until the SIP LED flashes and 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 has completed, press the reset button to cause the device to speak its IP address over the analog output ports.

6 WEB INTERFACE

6.1 Stats

6.1.1 Device Status

Web Interface Login

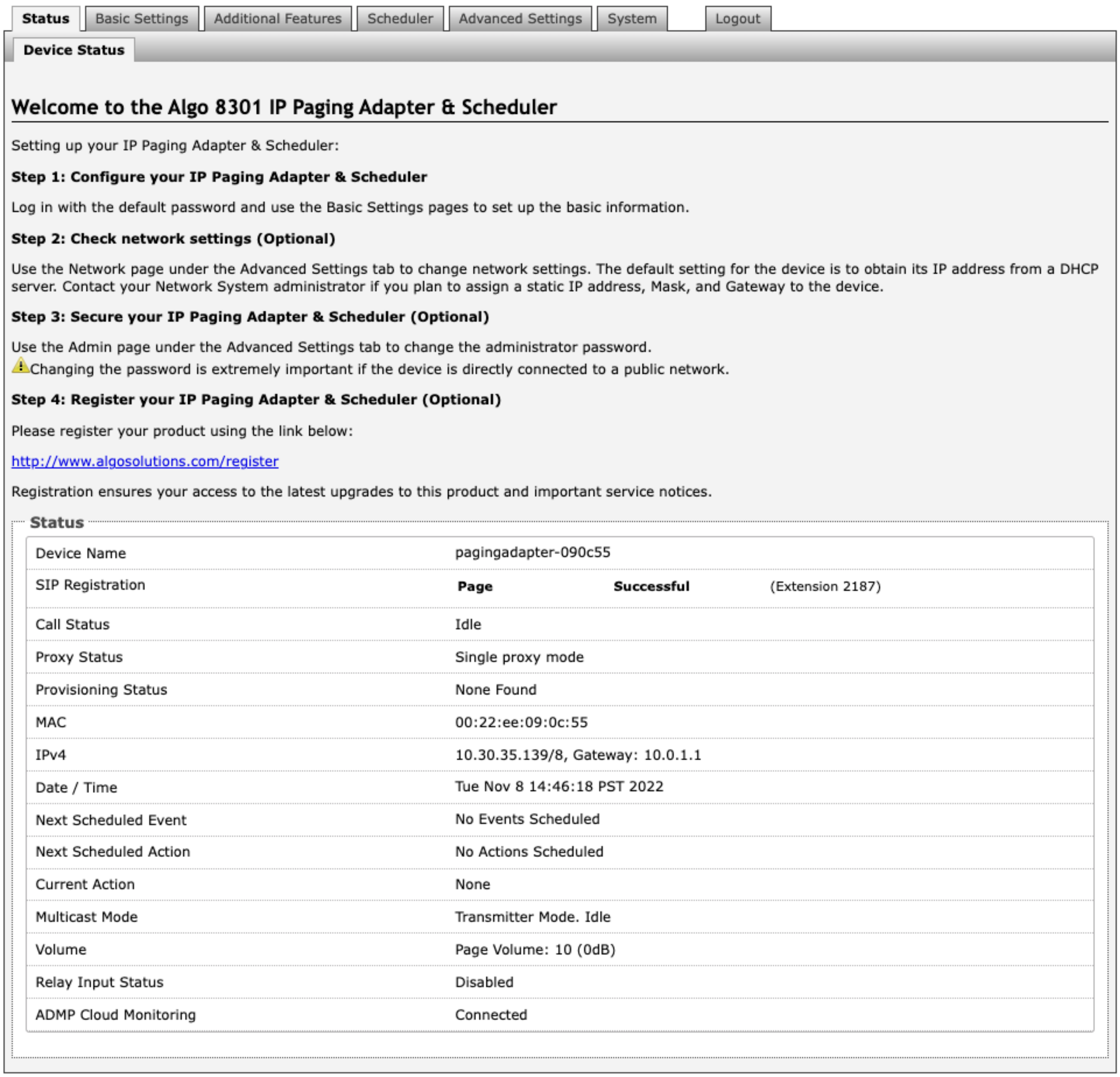


Figure 12: Status

The web interface of the 8301 requires a password to login to see the device settings. The default password is **'algo'**. This password can be changed in *Advanced Settings* → *Admin* tab after logging in the first time.

Note

Web Interface is accessed by entering the 8301 IP Address into a web browser.

Important

It is highly recommended to change the default password if the device is directly connected to a public network.

Status

By default, the *Status* page of the 8301 will be available before and after logging on. This section can be used to check the status of the 8301 for the following:

- Device Name
- SIP Registration
- Call Status
- Proxy Status
- Provisioning Status
- MAC
- IPv4
- Date/Time
- Next Scheduled Event
- Multicast Mode
- Volume
- Relay Input Status
- InformaCast License
- ADMP Cloud Monitoring

Note

*For security purposes, the Status page can be hidden when logged out through the settings under the **Advanced Settings → Admin** tab.*

These options may change depending on how the device is configured.

6.2 Basic Settings

6.2.1 SIP

The *SIP* tab under *Basic Settings* allows for the SIP server information and account credentials to be entered. This information can be obtained from your telephone system administrator or hosted account provider. After entering the information and saving the settings, go to the *Status* tab to confirm the registration was successful.

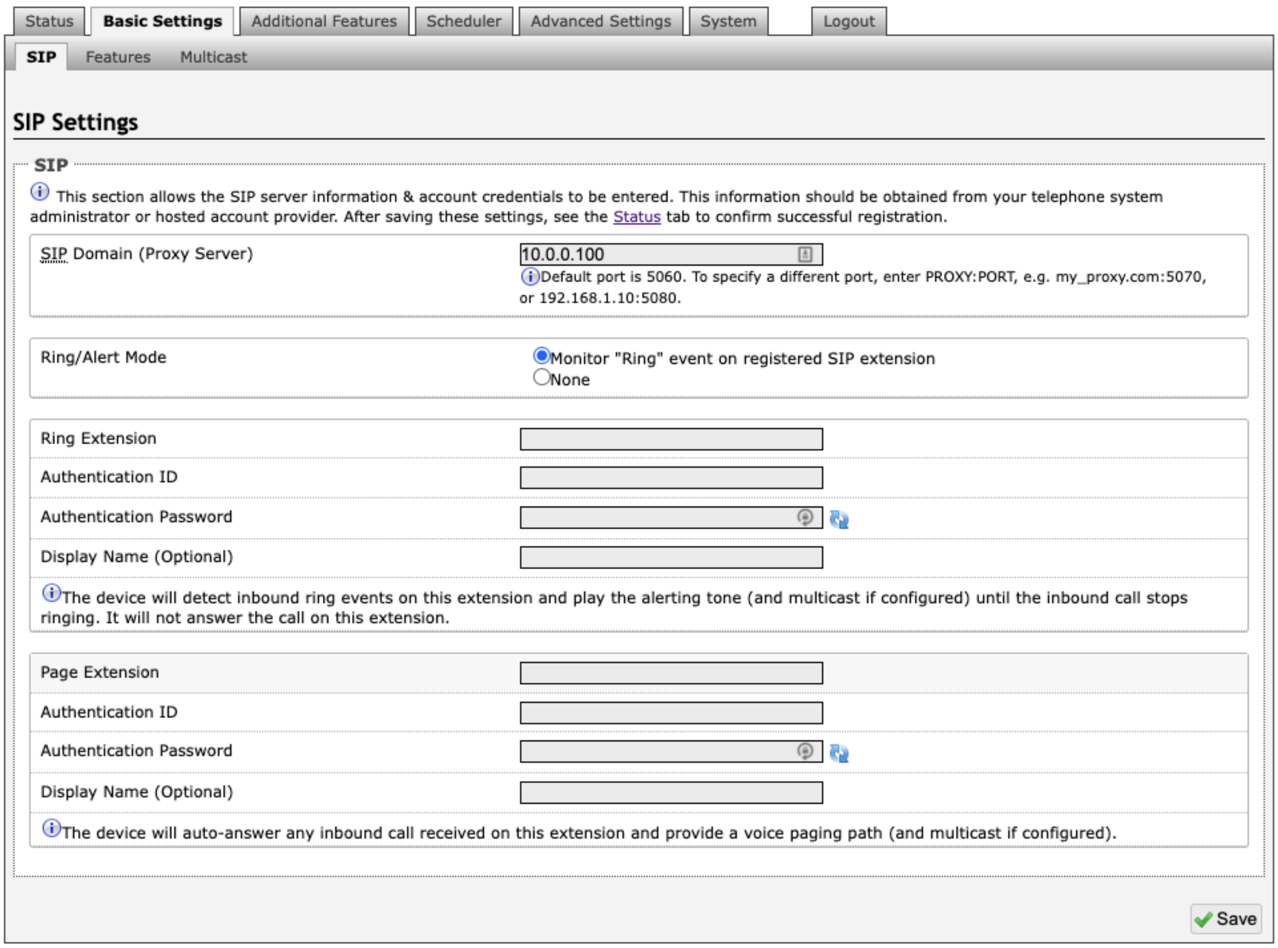


Figure 13: Basic Settings → SIP

Important

*Anytime changes are made to settings in the web interface the **'Save'** button must be clicked to save the changes.*

SIP Domain (Proxy Server)

The IP address (e.g., 192.168.1.111) or domain name (e.g., myserver.com) of the SIP Server.

Ring / Alert Mode

This is the option for adding a second SIP extension for a Ring event. If activated ("Monitor" is selected), the screen expands to show blocks for SIP extension parameters for a Ring/Alert Extension to be entered.

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. The alert tone may be configured in *Basic Settings → Features*.

Ring Extension

This is the SIP extension for the Ring parameter of the 8301.

Page Extension

This is the SIP extension for the Page parameter of the 8301. The device will auto-answer any inbound call received on this extension and provide a voice paging path (and multicast if configured). Different page modes and options are available in *Basic Settings* → *SIP*.

Authentication ID

Also referred to as 'Username' for some SIP servers, this, in some cases, may be the same as the Ring and/or Page extension. The authentication is a name you choose to represent the page extension.

Authentication Password

This is the SIP password provided by the system administrator for the registered SIP account. Up to eight (8) characters can be implemented. The password can be used to authenticate SIP users.

Display Name

The Display Name is what is shown on a receiving phone to which a SIP call is made. For the display name to be shown, the PBX and phone(s) need to be configured to display this message as the Caller ID. The desired Display Name should be entered in this field.

6.2.2 Features

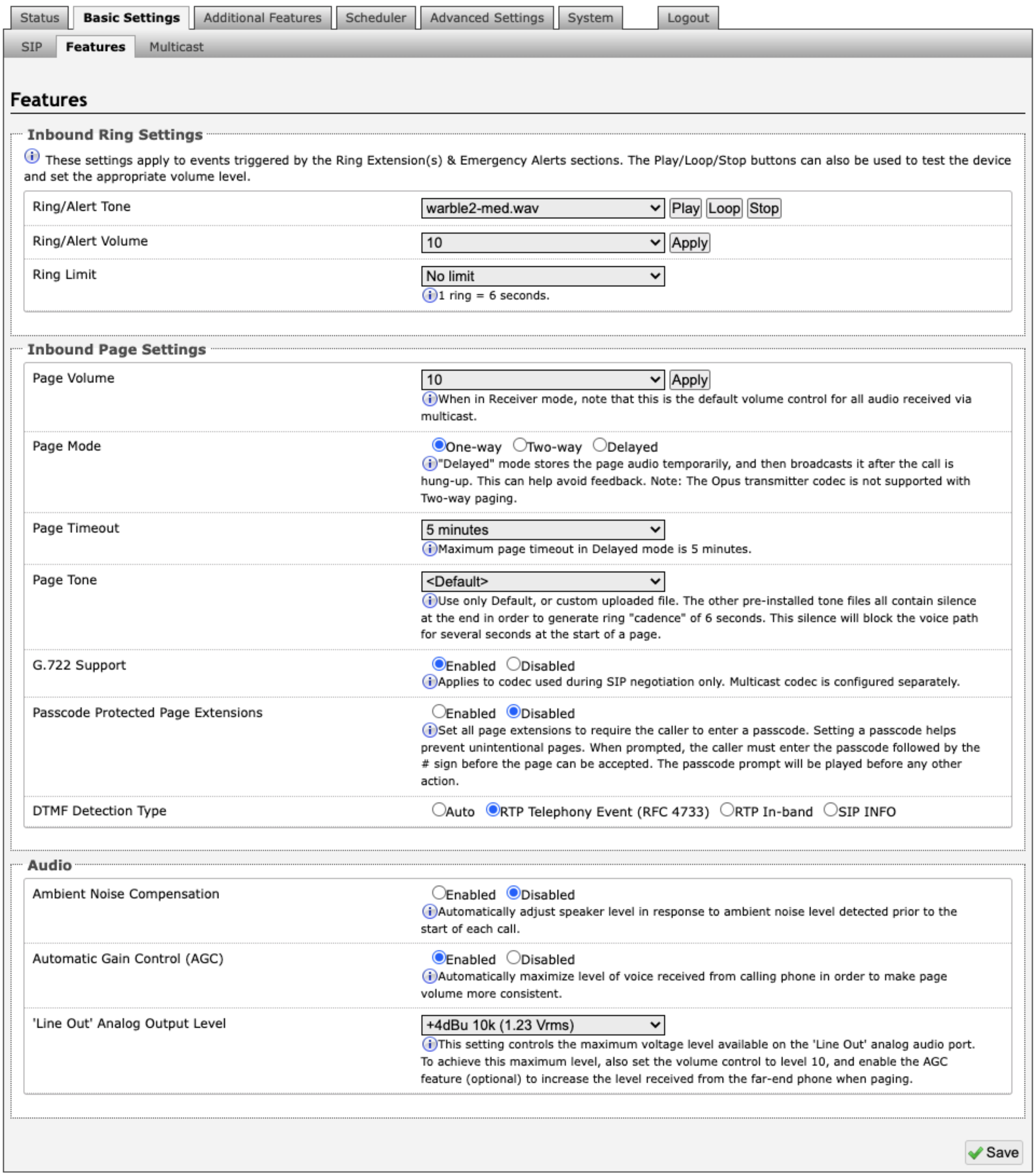


Figure 14: Basic Settings → Features

Inbound Ring Settings

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

Ring/Alert Tone

Select an audio file to play when a ring event is detected on the SIP Ring Extension. The audio file may be played immediately to an associated speaker from the web interface for test purposes using the Play, Loop, and Stop buttons. During multicast, the device will broadcast an audio stream using the Sender's selected ring tone.

Note
This is the "Default" tone that will be played if selected for Multicast, Additional Ring Extension settings.

Ring/Alert Volume

Set the volume for a SIP Ring event. This setting is an amplifier gain control, and the output level will depend on the levels recorded into the source audio file played from memory. This setting is only used for local tones, and not when receiving multicast (see Page Speaker Volume below).

Ring Limit

Typically set to no limit, this feature can be used to set a limit on how long the speaker will ring before timing out. A new ring event is required before the speaker will play the audio file again.

Inbound Page Settings

Page Speaker Volume

This is the Page Speaker Volume control for SIP or multicast paging. This setting is an amplifier gain control, and the output level will depend on the streaming level. This setting will apply to all inbound multicast streams (for Receiver mode only), regardless of content.

Page Mode

A call to the SIP page extension can be one-way, two-way (using an external microphone), or delayed. In delay mode, the speaker will store a page in its memory and then play after disconnecting.

Delayed Page

Delayed Page allows for a user to record a message before it is played over the speakers. To cancel a page while in delay mode, press "*" while the recording state is in process to prevent it from being sent after hanging up.

Page Timeout

Page Timeout is the maximum duration for a page. The call will be terminated when the timeout occurs whether anyone is speaking or not. This is useful for situations when someone accidentally forgets to hang up, preventing the paging system from getting stuck in the active state. A time limit may be set for an active page.

Page Tone

Select a pre-announce tone for paging. This tone will play to announce a Page is starting. Use only the Default or custom uploaded files. Other pre-installed tone files contain silence at the end to generate ring "cadence" of 6 seconds. This silence will block the voice path for several seconds at the start of a page. The “Default” tone will play the page-notif.wav file.

Note
The “Default Page Tone”, in Advanced Multicast, will play the tone set here.

G.722 Support

G.722 enables wideband audio for optimum speech intelligibility. Enable or disable the G.722 codec.

Passcode Protected Page Extensions

When enabled, the caller must enter the passcode followed by the # sign before the page can be accepted. Setting a passcode helps prevent unintentional pages. Passcodes can be up to 15 digits and must be numbers only.

Apply to All Page Extensions

Only visible when ‘Passcode Protected Page Extensions’ is set to ‘Enabled’. Choose to apply a passcode to all page extensions.

Passcode

Only visible when ‘Passcode Protected Page Extensions’ is set to ‘Enabled’. Enter the desired numerical passcode (maximum length of 15 digits).

Passcode Prompt Tone

Only visible when ‘Passcode Protected Page Extensions’ is set to ‘Enabled’. Select the tone to be played to notify 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, best known to users as the sound made when pressing a number key. In the 8301, this is used for multi-zone selection, passcode, etc.

Audio Processing

Ambient Noise Compensation

Ambient Noise compensation will allow the speaker level to adjust automatically in response to ambient noise levels detected at the device prior to the start of each call. The 8301 requires an external microphone wired in.

Ambient Noise Compensation No Loss

Configure the Ambient Noise Compensation algorithm to only use levels at or above the current volume. The current volume is the minimum volume when this setting is enabled.

Ambient Noise Compensation Max Volume

Based on ambient noise levels, a maximum volume can be set.

Automatic Gain Control (AGC)

AGC normalizes the audio level. This ensures the audio level heard near the speaker is always at a consistent level, independent of the phone that is used to call.

'Line Out' Analog Output Level

The following output levels are available, allowing the 8301 to interface with a wide variety of amplifiers:

- +4dBu 10k (1.23 Vrms)
- 0dBu 10k (0.775 Vrms)
- 0dBV 10k (1.0 Vrms)
- -10dBV 10k (0.316 Vrms)
- 0dBm 600 ohm (0.755 Vrms)
- -10dBm 600 ohm (0.245 Vrms)
- -20dBm 600 ohm (0.077 Vrms)

6.2.3 Multicast

Multicast IP Addresses

Each 8301 has its own IP address and shares a common multicast IP and port number (multicast zone) for multicast packets. The Sender transmits to a configurable multicast zone, and the Receiver units listen to all the multicast zones assigned to them.

The network switches and router see the packet and deliver it to all the members of the group. The multicast IP and port number must be the same on all the Transmitter and Receiver units of one group. 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 8301 is set to use the multicast IP address 224.0.2.60 and the port numbers 50000-50008

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

Multicast Page Zones

The 8301 supports nine (9) 'basic' multicast zones. These zones are defined by the multicast IP addresses.

Somewhat arbitrarily, these zones are defined below but may be used in other ways. The important consideration is that there is a priority hierarchy – streaming activity on a zone higher on the list, will be treated as a higher priority than a zone lower down on the list – with music being the lowest priority.

1. Priority
2. All Call
3. Zone 1
4. Zone 2
5. Zone 3
6. Zone 4
7. Zone 5
8. Zone 6
9. Music

"Expanded" zones can also be enabled, in *Basic Settings* → *Multicast*, allowing up to 50 zones in total. These have the same behaviors as the basic zones but are hidden by default to simplify the interface.

6.3 Multicast (Transmitter/Sender Settings)

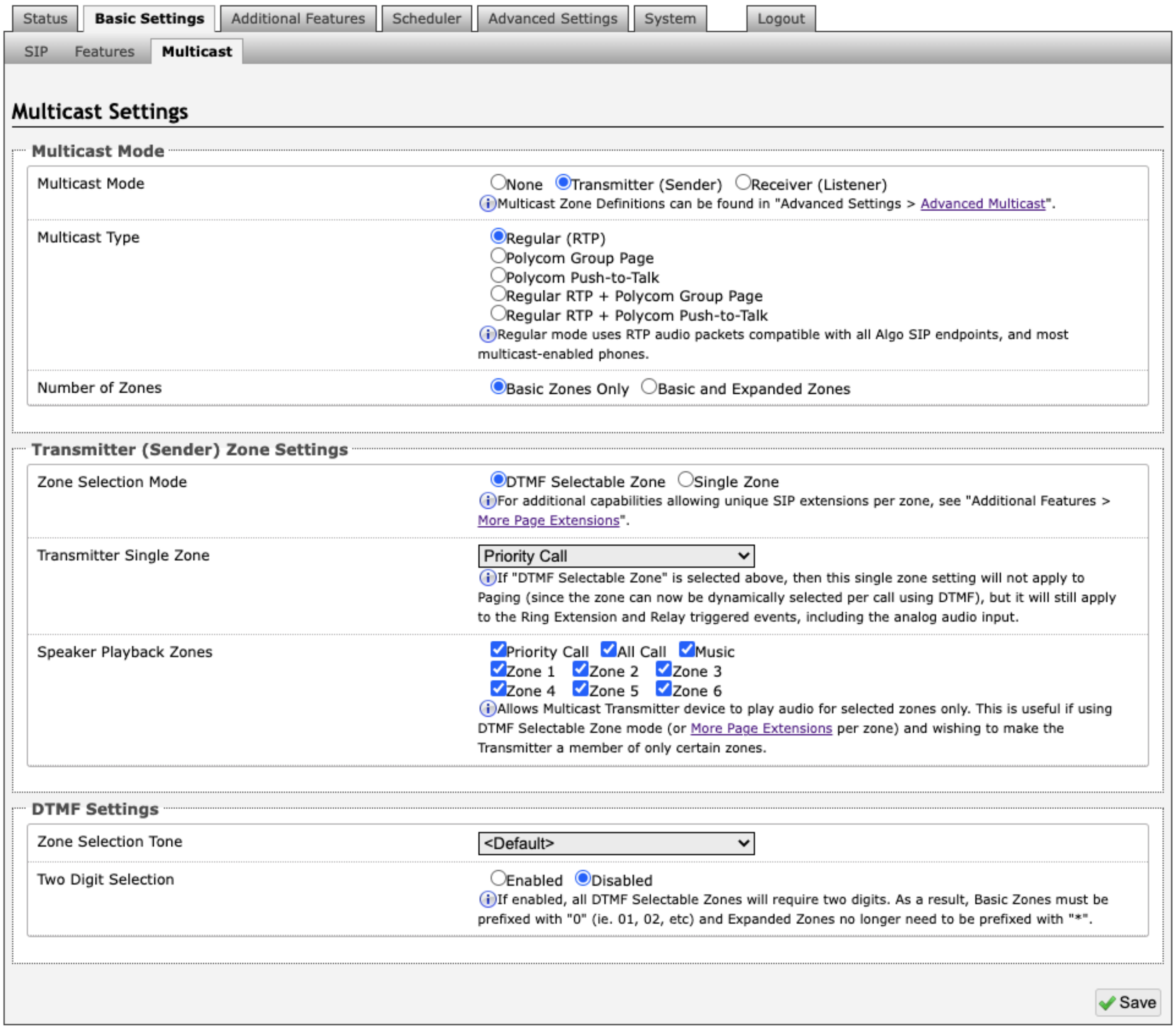


Figure 15: Multicast transmitter mode settings

Note

See Advanced Settings → Advanced Multicast *for more information on populated IP values.*

Multicast Mode

Multicast Mode (Transmitter/Sender Selected)

If the Transmitter mode is enabled, the 8301 will broadcast an IP stream when activated in addition to playing the audio through the audio output (Note that the 8301 cannot be both a multicast Transmitter and Receiver simultaneously).

Multicast Type

The 8301 may broadcast multicast paging, compatible with Polycom ***"on premise group paging"*** protocol and most multicast-enabled phones that use RTP audio packets.

Select 'Regular' if solely multicasting to Algo IP endpoints and/or multicast-enabled phones.

To multicast page announcements solely to Polycom phones, select 'Poly Group Page' or 'Push-to-Talk'. Then, configure the 8301 with the 'Poly Zone' (IP Address and Port) and 'Polycom Default Channel'.

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

Select 'Regular RTP + Poly Group Page/Push-to-Talk' to multicast page audio to both Polycom phones, Algo IP endpoints, and multicast-enabled phones.

Number of Zones

Select 'Basic Zones Only' if configuring nine or fewer multicast zones (shown beside 'Speaker Playback Zones') or 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.

Transmitter (Sender) Zone Settings

Zone Selection Mode

'Single Zone' always broadcasts on one pre-configured zone. In 'DTMF Selectable Zone' mode, 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.

Zone Selection Mode

"Single Zone" mode always broadcasts on one IP address.

Note
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.

'DTMF Selectable Zone' mode, offers dynamic zone selection and requires only the Transmitter device to have a registered SIP Extension. The zone definitions can be found in the *Advanced Settings* → *Advanced Multicast* tab.

In 'DTMF Selectable Mode', to page, dial the SIP extension of the Transmitter device: ####, then dial the desired DTMF page zone (e.g., 1, 2, etc.) on the keypad when prompted.

1. Press DTMF Extension 9 for Priority Call
2. Press DTMF Extension 0 (or 8) for All Call
3. Press DTMF Extension 1 for Zone 1
4. Press DTMF Extension *10 for Zone 10

5. Press DTMF Extension *11 for Zone 11

Note
DTMF codes for zones 10 and higher start with an ""*
All DTMF codes and respective zones are available in Advanced Settings → Advanced Multicast.

Zone Selection Tone

Only visible when 'Zone Selection Mode' is set to 'DTMF Selectable Zone'. The tone played over the phone to prompt the user to select a zone to multicast to.

Transmitter Single Zone

The zone that multicast stream will be sent to by default. If 'DTMF Selectable Zone' is chosen above, this setting will not apply to Paging, since the zone now must be dynamically selected per call via DTMF. However, the specified Transmitter 'Single Zone' setting is still used for any multicast events triggered by the Ring, analog input, or the relay input.

Note
The Transmitter Single Zone is the default zone used for any multicast actions unless an option is available for a custom zone with specific parameters.

Speaker Playback Zones

The Speaker Playback Zones allows the Transmitter device to play audio for selected zones only. This is useful if using the DTMF Selectable Zone mode (or More Page Extensions per zone) with the intention of making the Transmitter unit a member of only certain zones. In this case, the Transmitter does not participate in the Zone, but it transmits certain traffic.

Expanded Speaker Playback Zones

Up to 50 zones can be shown and are only visible when 'Basic and Expanded Zones' is selected.

DTMF Settings

Zone Selection Tone

This is the prompt to select a zone. This may be used as an interactive voice response (IVR) menu by uploading a custom audio file through *System → File Manager* in the Tones folder. 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 '*'.

6.4 Multicast (Receiver Settings)

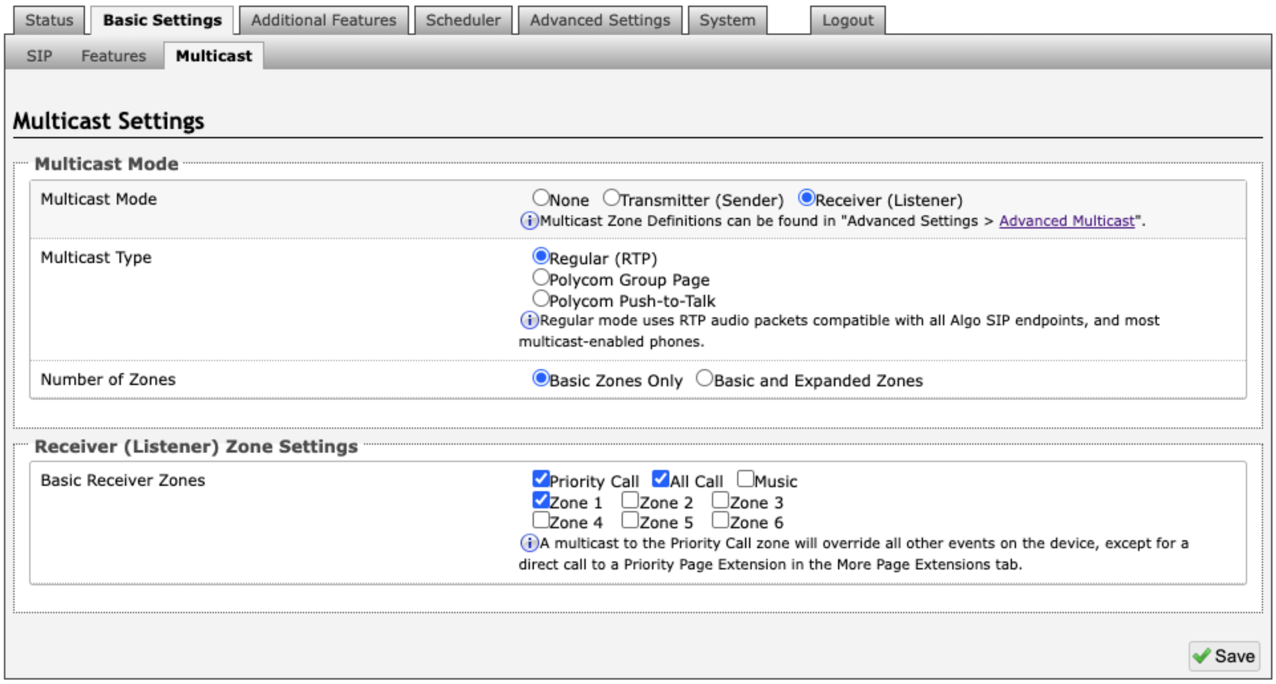


Figure 16: Multicast receiver mode settings

Multicast Mode

Multicast Mode (Receiver Selected)

If Receiver mode is enabled, the 8301 will activate when receiving a multicast message. It will mimic the audio stream of the transmitter but use local volume settings (‘Page Speaker Volume’ in *Basic Settings* → *Features*).

Multicast Type - Regular

Select “Regular” if receiving multicast from other Algo IP endpoint(s) and/or multicast- enabled phone(s) that use RTP audio packets.

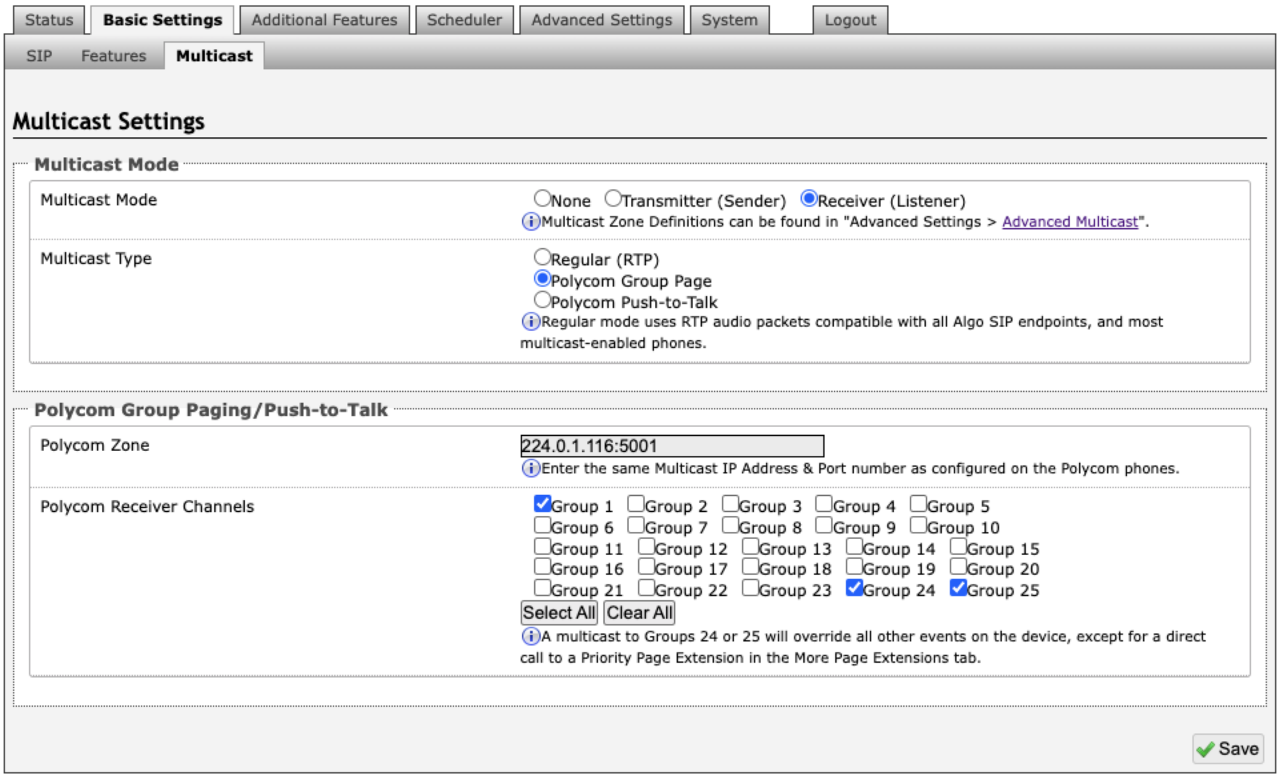
Number of Zones

Select ‘basic’ zones if configuring nine or fewer multicast zones or ‘expanded’ 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.

Multicast Type – Polycom Group Paging/Push-to-Talk

The 8301 may receive multicast paging compatible with Polycom ***“on premise group paging”*** protocol.

To configure the 8301 as a Receiver to play Polycom page announcements, select ‘Group Page’ or ‘Push-to-Talk’. Then enter the Polycom Zone (IP Address and Port) that matches the configuration of the Polycom phones and Channels. The ‘Default Channel’ is the target group in a Polycom paging environment.



The Polycom phone used as page audio source for the 8301 must be configured to use either the G.711 or G.722 audio codec. **The Polycom phone(s) must also be configured with the "Compatibility" setting ("ptt.compatibilityMode") disabled** in order for this codec setting to be applied.

If using a Polycom phone as the Multicast Transmitter, a tone may be set for any of the 25 Polycom Groups configured on the Algo device. If an Algo device is used as a Multicast Transmitter, a tone does not have to be set as the Algo Transmitter will provide its own tone. Polycom Group Tones can be set in *Advanced Settings* → *Advanced Multicast*.

Receiver (Listener) Zone Settings

Basic Receiver Zones

Select one or more multicast zones for the 8301 to subscribe to.

Note

Multicast zone priority is based on the zone definition list order (from top to bottom) in Advanced Settings → Advanced Multicast.

Expanded Receiver Zones

Up to 50 zones can be shown, however, they are only visible when 'Basic and Expanded Zones' is selected.

6.5 Additional Features

6.5.1 Input/Output

The *Input* terminals allow external accessories to be connected to the 8301. This is a dry contact input which can be configured as ‘normally open’ or ‘normally closed’ mode. Algo offers accessories, such as the 1202, 1203, 1204, 1205 and 2507. Third-party accessories/systems may also be used provided they have a dry contact output.

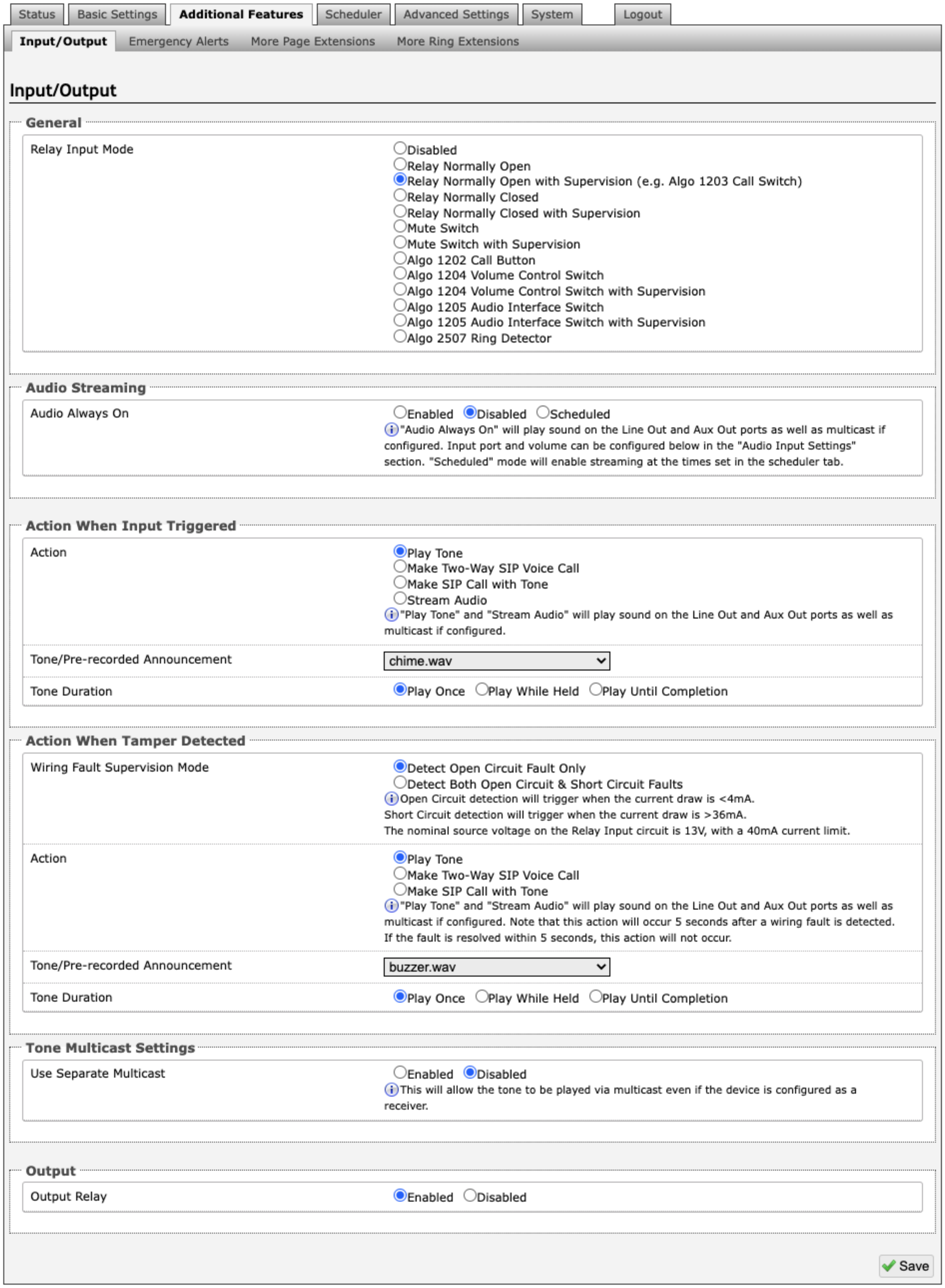


Figure 17: Input settings

General

Relay Input Mode

The input relay to the 8301 can be activated by any normally open or normally closed switch. Algo offers the 1202 Call Button, the 1203 Call Switch, 1204 Volume Control Switch, or the 1205 Audio Interface with supervision. Via supervision settings, notification actions can also be triggered if the input switch is disconnected.

1203 Call Switch

The 1203 Call Switch is a simple contact closure switch with an illuminated button and supervision capabilities. When used in conjunction with the 8301, the 1203 can prompt a single action with one-touch, or a continuous action if the button is held.

Figure 18: 1203 Call Switch

Mute Switch

Apply an external switch (short-circuit) across the Relay Input terminals in order to mute the 8301. This allows a temporary "disable" switch to control the device if desired, for example in a boardroom to block paging during important meetings.

Leave the Relay Input terminals open (no-connect) for regular full-volume operation when in this mode.

Multicast Override

Allow selected multicast zones to override the Mute Switch settings for the selected zones.

1202 Call Button

The 1202 Call Button is a one-touch button for event notification and response. It can be used with the 8301 for improved customer service, emergency notification, and non-emergency alerting. The Call Button's one-touch button can trigger a single or continuous action, which can be halted via the small cancel/reset button located below the main call button.

Figure 19: 1202 Call Button – the insert card is interchangeable

While the 8301 can be configured to play the audio file only once, it can also be enabled to play it continuously with just a press of the 1202 Call Button. The action can then be stopped via the smaller oval cancel button located below the main call button on the 1202 Call Button.

1204 Volume Control

The 1204 Volume Control Switch is a simple two terminal potentiometer that will allow attenuation below the maximum volume level (configured under *Basic Settings* → *Features*).

Figure 20: 1204 Volume Control

Mute On Lowest Setting

Enabling 'Mute On Lowest Setting' allows audio to be completely muted when volume control switch is turned all the way down.

Wire Length

This allows you to calibrate impedance for 24 AWG.

Multicast Override

Multicast Override allows selected multicast zones to override the 1204 Volume Control settings for the selected zones.

Remote Volume Settings

Configure the device to subscribe to a remote 1204 volume input or to notify remote devices of 1204 volume input.

Note
RESTful API must be enabled in the Advanced Settings → Admin *tab.*

Notify (Local 1204) → remote device RESTful API password

Subscribe (Remote 1204)

- IP address
- Remote device RESTful API password

1205 Audio Interface Switch

The 1205 Audio Interface provides a method for connecting a music source and live microphone to the 8301 Paging Adapter for multicast broadcast over the network to IP speakers or IP enabled legacy paging systems.

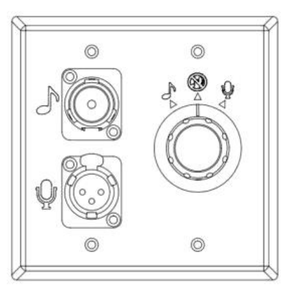


Figure 21: 1205 Audio Interface

The Algo 1205 rotary control knob has three positions (music, microphone and off). The 8301 will automatically detect the control knob position to start multicast for either the microphone or music input as selected or stop multicast in the off state.

The music input uses a 3.5 mm stereo input jack compatible with AppleTM iPodTM and other sources. Left and right stereo channels are combined into a balanced mono signal compatible with public address infrastructure. The music volume is adjusted by both the Audio Input Volume setting in the web interface of the 8301 and manual adjustment of the source level.

The microphone input uses an XLR connector compatible with dynamic microphones such as the SennheiserTM E835 and similar microphones that do not require phantom power.

Audio Streaming

Audio Always On

Primarily used to play background music, this feature will play sound on the Line Out and Aux Out ports as well as multicast if configured. The input port and volume can be configured below in the "Audio Input Settings" section.

Note

Audio Streaming Always On cannot be used when the Relay Input Mode is set to 1205 Audio Interface Switch or when the relay trigger action 'Stream Audio'. To enable Audio Streaming Always On, set Relay Input Mode to 'Disabled', or set Action When Input Triggered to 'Play Tone', 'Make Two-Way SIP Voice Call', or 'Make SIP Call with Tone'.

Action When Input Triggered

Action

Play Tone

When the 8301 input is triggered, a tone or a pre-recorded audio file will play over the speaker or multicast if enabled. This function can be used to request support/assistance in service or retail environments, notify about an emergency at a specific location in medical or educational facilities, or sound an alarm during an intrusion.

- Action When Input Triggered:
    - Tone/Pre-recorded Announcement
    - Tone Duration

Make SIP Voice Call

When the 8301 input is triggered, a voice path will open for an intercom-like call via an external microphone to a pre-configured phone extension. This option can be used when a call needs to be made from a public place where a phone would not be practical to use.

- Action When Input Triggered:
    - Extension to Dial
    - Call Mode

  - Allow 2nd Button Press
- Outbound SIP Call Settings:
  - Outbound Ring Limit
  - Ringback Tone
  - Maximum Call Duration

Make SIP Call with Tone

When the 8301 input is triggered, a private call can be generated to a pre-configured phone extension with a pre-recorded message. For instance, a call to a supervisor's phone notifying about an emergency or intrusion at some location.

- Action When Input Triggered:
  - Extension to Dial
  - Allow 2nd Button Press
  - Tone/Pre-recorded Announcement
  - Interval Between Tones (seconds)
  - Maximum Tone Duration
- Outbound SIP Call Settings:
  - Outbound Ring Limit

Allow 2nd Button Press

If enabled, the 2nd button press will either simply End Call or End and Restart Call. Therefore, if an input is triggered for the second time the SIP call will either simply be terminated or terminated and immediately called again.

Action When Tamper Detected (Supervision)

In addition to the main events, the device can be configured with supervision to also execute one of the above three actions ('Play Tone', 'Make Two-Way SIP Voice Call', 'Make SIP Call with Tone') in case the device goes offline due to wiring failure or after being tampered with. For example, a tone could sound over the speaker(s), or a private pre-recorded message could be sent to a specified phone extension. The supervision configuration options will appear once a relay option with supervision is selected. See the Electrical Specification section for details on supervision detection circuit.

Wiring Fault Supervision Mode

Short circuit detection will be triggered when the current draw is <4 mA. Short circuit detection will trigger when the current draw is >36 mA. The nominal source voltage on the Relay Input circuit is 13 V, with 40 mA current limit.

Action

"Play Tone" will play a recorded audio file to a local speaker and multicast if configured. "Stream Mic Audio" will stream microphone audio to multicast only, so it requires multicast "Transmitter" mode to be enabled in *Basic Settings → Multicast*.

Note

This action will occur 5 seconds after a wiring fault is detected. If the fault is resolved within 5 seconds, this action will not occur.

- Play Tone
- Make SIP Voice Call
- Make SIP Call with Tone

Tone/Pre-recorded Announcement (Action – Play Tone / Make SIP call with Tone)

Select a recording or tone to use. Custom audio files may be used and uploaded though *System* → *File Manager*.

Extension to Dial (Action – Make SIP Voice Call)

SIP account required in Page Extension fields in order to make a call. Can be configured if 'Make SIP Voice Call' or 'Make SIP Call with Tone' actions are enabled under 'Call Button Settings'.

Interval Between Tones (Action –Make SIP call with Tone)

Specify the time delay (seconds) between tones. Can be configured if 'Play Tone' or 'Make SIP Call with Tone' actions are enabled under 'Call Button Settings'.

Maximum Tone Duration (Action – Play Tone / Make SIP call with Tone)

Select the maximum tone duration. The tone will be terminated once the maximum time is reached. Can be configured if 'Play Tone' or 'Make SIP Call with Tone' actions are enabled.

Tone Multicast Settings

Use Separate Multicast

This allows the tone to be played via multicast even if the 8301 is configured as receiver. See additional options when enabled.

- Multicast Mode
- IP Address
- Port

Outbound SIP Call Settings

Outbound Ring Limit

Typically set to ensure that a call will not reach voicemail. This feature, under 'Outbound SIP Call Settings', can be used to set a limit on how long the speaker will ring before timing out.

Ringback Tone

If enabled, under 'Outbound SIP Call Settings', a ringback tone will play over the speaker during an outbound SIP call, while waiting for the far-end party to answer.

6.5.2 Emergency Alerts

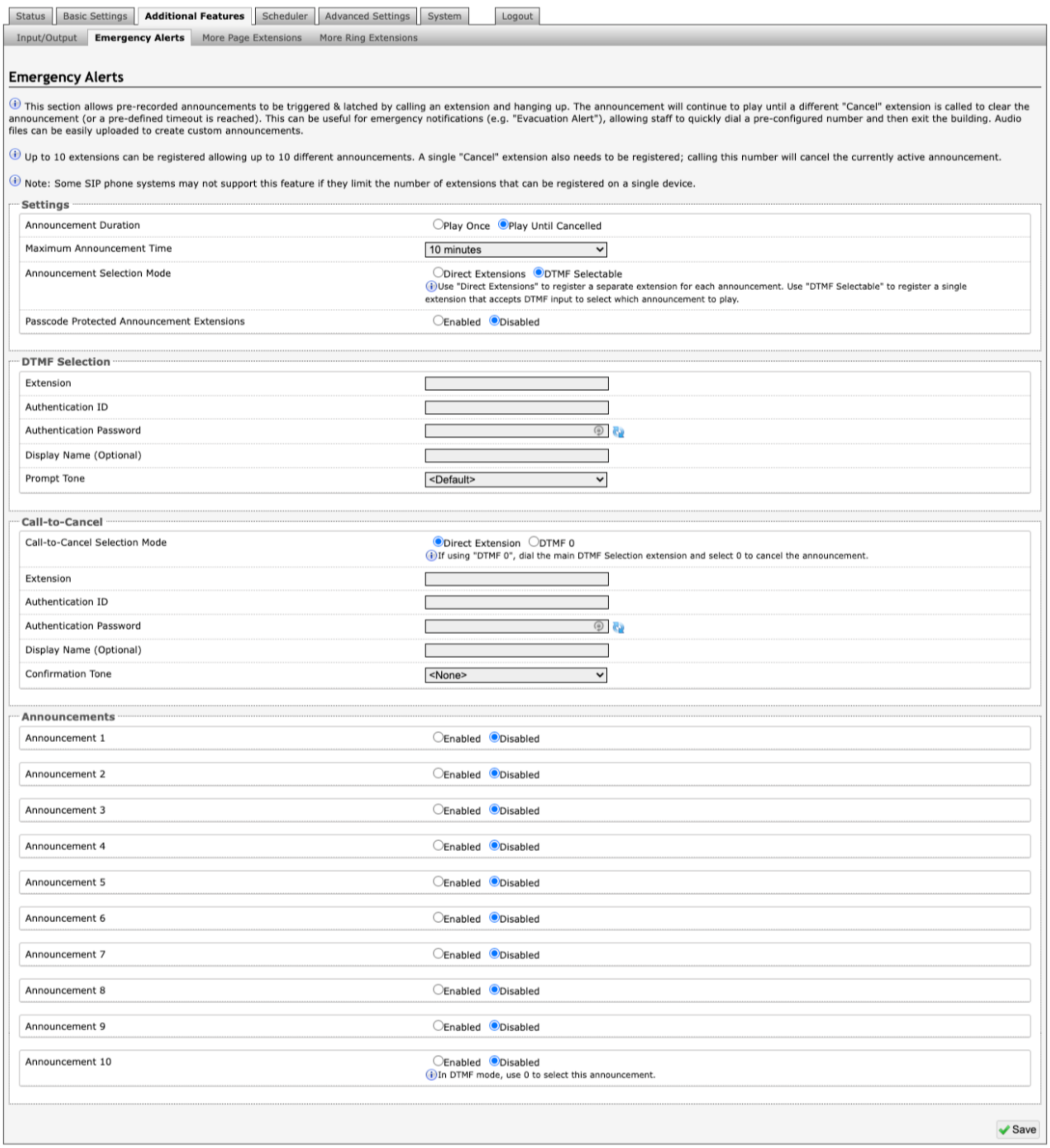


Figure 22: Emergency Alerts

Emergency Alerts allow for an announcement to be triggered and latched by calling a pre-configured Emergency extension and hanging up. Emergency Alerts are useful for emergency notifications (e.g., evacuation, lock down, medical emergency, etc.), allowing staff to quickly dial a pre-configured number under such circumstances.

Settings

Default Announcement Duration

The announcement can be chosen to play once or to play until cancel. 'Play Once' mode will play a single cycle of the chosen tone file, despite of its duration. 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

This represents the duration for how long the announcement plays for.

Announcement Selection Mode

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

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 or to require a passcode before releasing the announcement. Select 'Disabled' to detect just the inbound Ring signal, but not actually answer the call.

If the 'Answer Inbound Call' option is 'Enabled' the call is auto answered and a configurable confirmation tone is played before starting the alert. If 'Disabled', the alert is triggered just by the inbound ring, without answering the call. (In both instances, the announcement will play until the time limit is reached or the 'Cancel Extension' is called). The auto-answering option can be useful when the caller cannot hear announcement from their location. However, in instances where the call might go to a group/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

When enabled, this setting requires the caller to enter a passcode after dialing an announcement or call-to-cancel extension. Setting a passcode helps prevent unintentional announcements.

Announcement Passcode

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 be ended.

Passcode Prompt Tone

Select a tone to play when the passcode is ready to be entered.

DTMF Selection

Extension

This is the SIP extension for the DTMF Selection parameter of the 8301.

Authentication ID

The Authentication ID may also be called Username for some SIP servers and in some cases may be the same as the extension.

Authentication Password

This is 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) will have to 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

Call-to-Cancel Selection Mode

If using "DTMF 0", dial the main DTMF Selection extension and select '0' to cancel the announcement.

Extension

This is the SIP extension for the Call-to-Cancel Selection parameter of the 8301. .

Authentication ID

The Authentication ID may also be called Username for some SIP servers and in some cases may be the same as the extension.

Authentication Password

The SIP password is 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) will have to 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.

Announcements

Announcement 1

To configure an emergency alert extension, select 'Enable' beside the target announcement and enter the Extension, Authentication ID, and Authentication password.

Up to 10 extensions can be registered allowing up to 10 different announcements. Audio files can also be easily uploaded to create custom announcements. Only one 'Call-to-Cancel' extension is needed, despite the number of the alert extensions.

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.

Announcement Duration

Choose how long to allow for the announcement duration. An announcement can:

- Play Once
- Play Until Cancelled
- Default (this option follows the behavior configured in 'Default Announcement Duration')

Extension

This is the SIP extension for the announcement parameter of the 8301.

Authentication ID

The Authentication ID may also be called Username for some SIP servers and in some cases may be the same as the extension.

Authentication Password

The SIP password is 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) will have to be configured to display this message as the Caller ID.

6.5.3 More Page Extensions

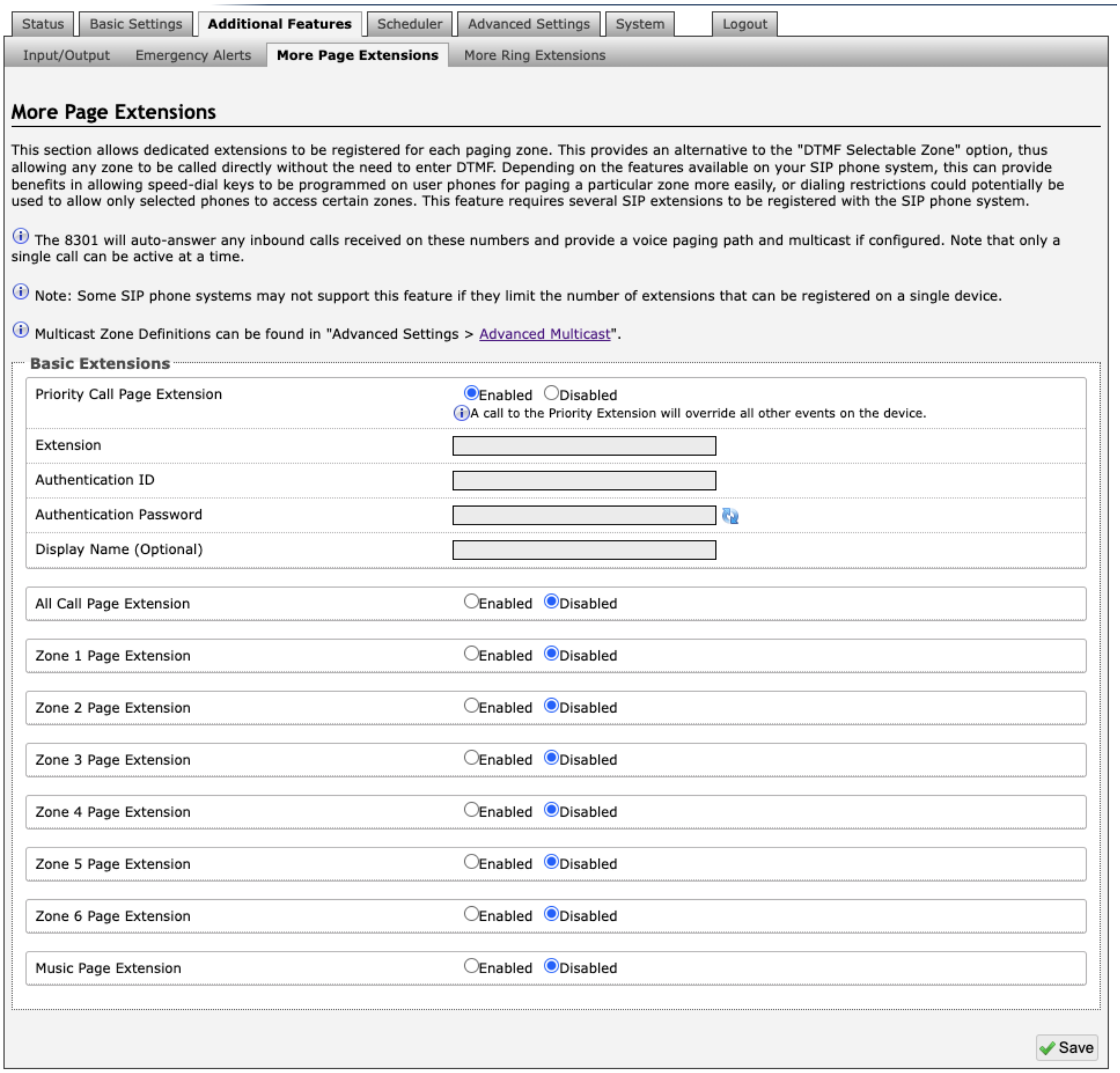


Figure 23: More page extensions

Additional SIP extensions can be registered for each multicast zone that will be used. This allows the advantage of dialing directly to a zone without needing to enter DTMF Codes (e.g., speed-dial keys can be used), but this may require additional SIP licenses depending on the SIP provider.

To configure additional page extensions (up to 50), select ‘Enable’ beside the target extension and enter the Extension, Authentication ID, and Authentication password.

The 8301 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.

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.

6.5.4 More Ring Extensions

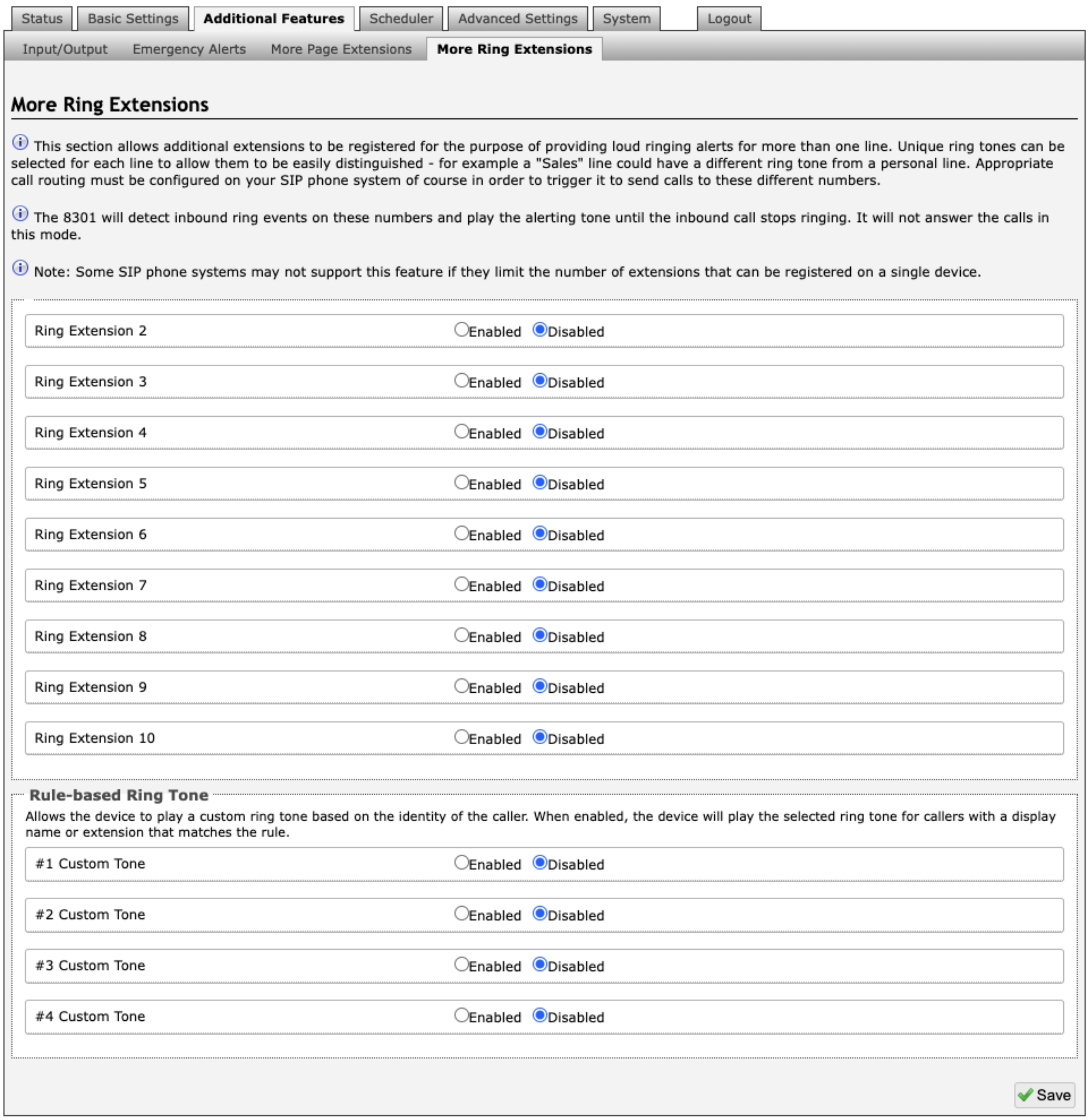


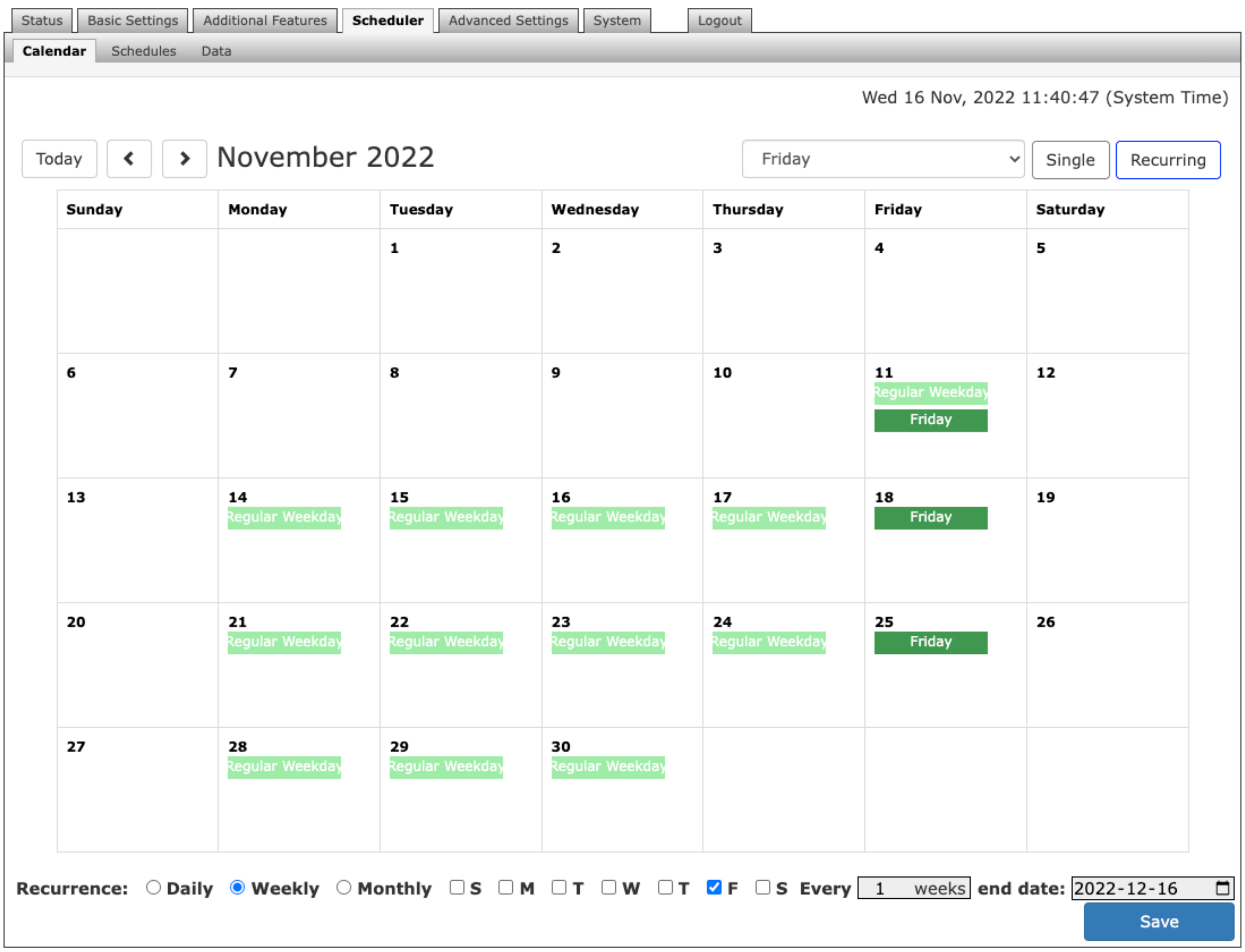
Figure 24: More ring extensions

Up to 10 SIP Ring extensions can be registered. To configure additional ring extensions, select 'Enable' beside the target extension and enter the Extension, Authentication ID, and Authentication Password. A unique Ring Tone and Multicast Zone can be assigned to each extension if desired.

6.6 Scheduler TAB

6.6.1 Calendar

The Scheduler can be deployed along with Algo IP speakers, paging adapters, and strobes to provide bell scheduling and automated announcements.



Once a bell schedule has been configured in the Schedules tab (see below), it can be added to the desired dates on the calendar. Multiple different schedules can be created. For example, Fridays might have a different schedule than the other weekdays.

From the drop-down menu at the top of the calendar, select a schedule (e.g., Regular weekday), then click on the calendar dates to implement the schedule. When finished, click Save.

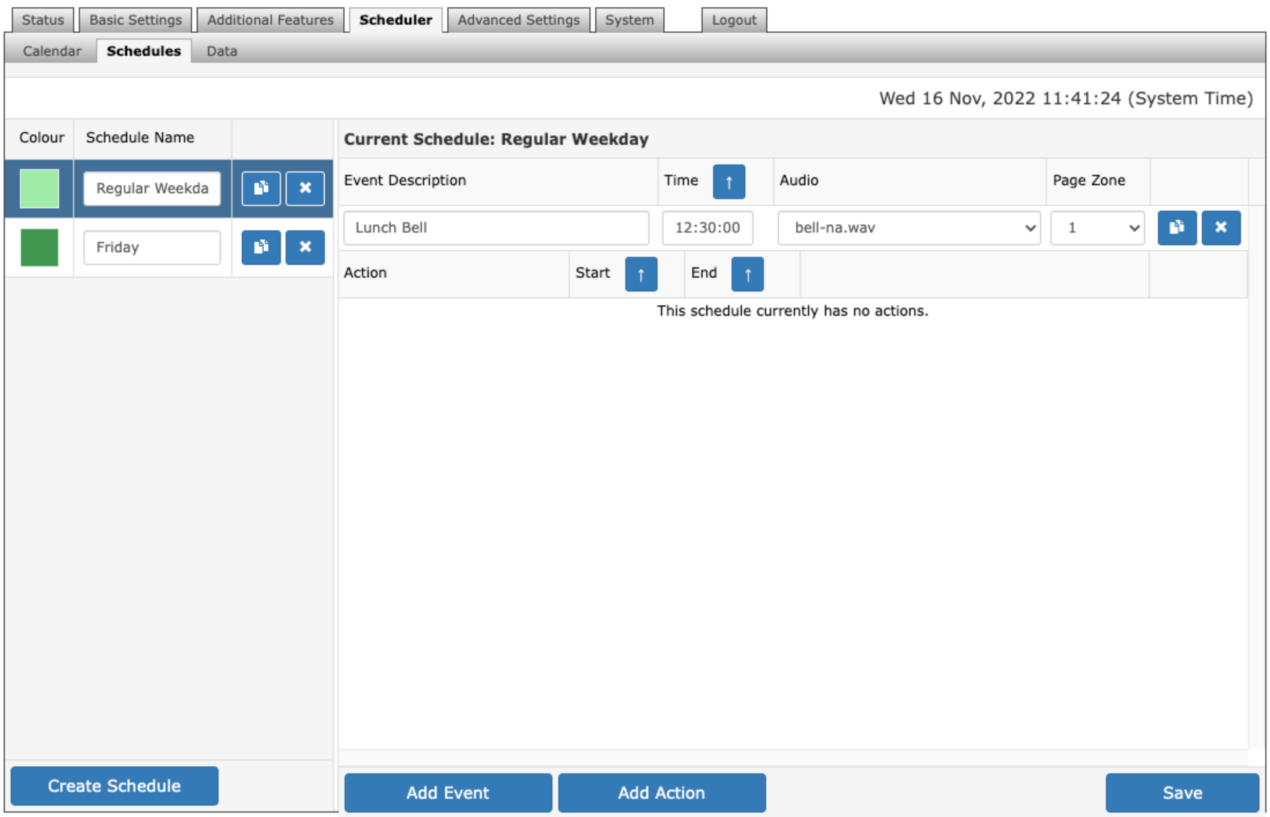
To clear the schedule from the entire month, select **None (clear)** from the drop-down menu, and click on the dates to clear.

The ‘All Weekdays’ or ‘All’ buttons can be used instead of clicking individual dates to implement a specific schedule throughout the month or to clear existing schedule for the whole month.

The schedule will need to be applied to each month separately.

Recurrent schedules are also supported. Select the desired schedule from the drop-down menu and select "Recurring" from the button on the top right. Once selected, configure the recurrency settings underneath the calendar. To apply, click on the starting day on the calendar. The schedule will now be populated onto the calendar. Save the settings.

6.6.2 Schedules



Press **Create Schedule** to add a bell schedule that will be implemented on specific calendar days. Give a ‘Schedule Name’ and pick a ‘Color in Calendar’ to represent the schedule on the calendar.

Select the schedule, and in the ‘Current Schedule’ section, add events (bells) to the schedule. Specify the event **Description, Time, Audio** files to be played, and the **Page Zone** (if Multicast Transmitter mode is enabled).

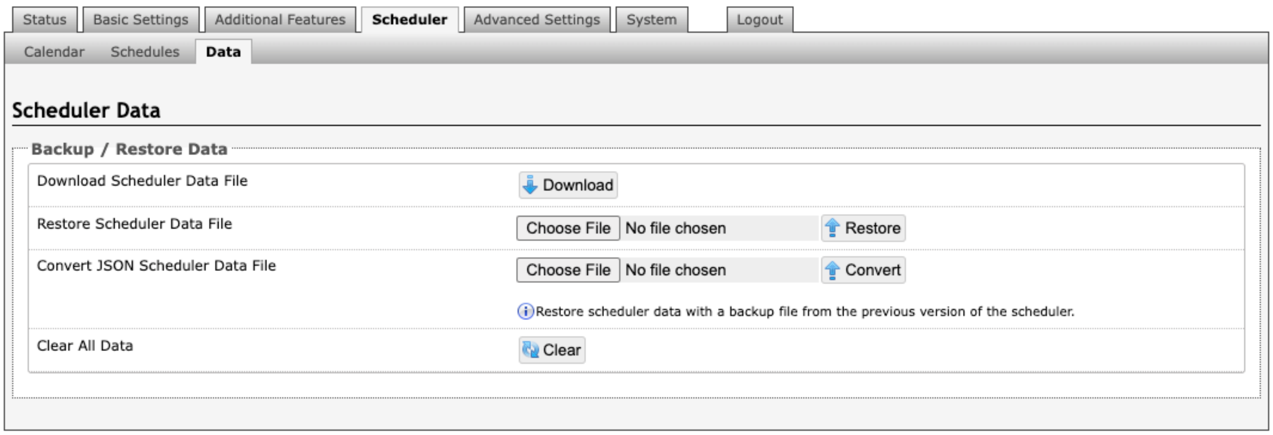
The chosen audio file will be played locally (e.g., amplifier connected to the 8301) and/or over the network via multicast to all other Algo endpoints (e.g., 8186, 8188, 8180, 8128, etc.) or RTP multicast compatible third-party equipment that are configured as Receivers on this zone.

 Delete schedule or event button

 Copy event button

Note
Each schedule may contain up to 500 events (bells) and up to 30 schedules may be created.

6.6.3 Data



Download

Allows a backup of the schedule with events, times, and calendar dates to be downloaded for backup purposes. Note that this backup is independent from the rest of the configuration backup on the device.

Restore

Upload and restore a saved Scheduler data file.

Clear All Data

Clears all the Scheduler data, including saved schedules and set calendar dates.

6.7 Advanced Settings

6.7.1 Network

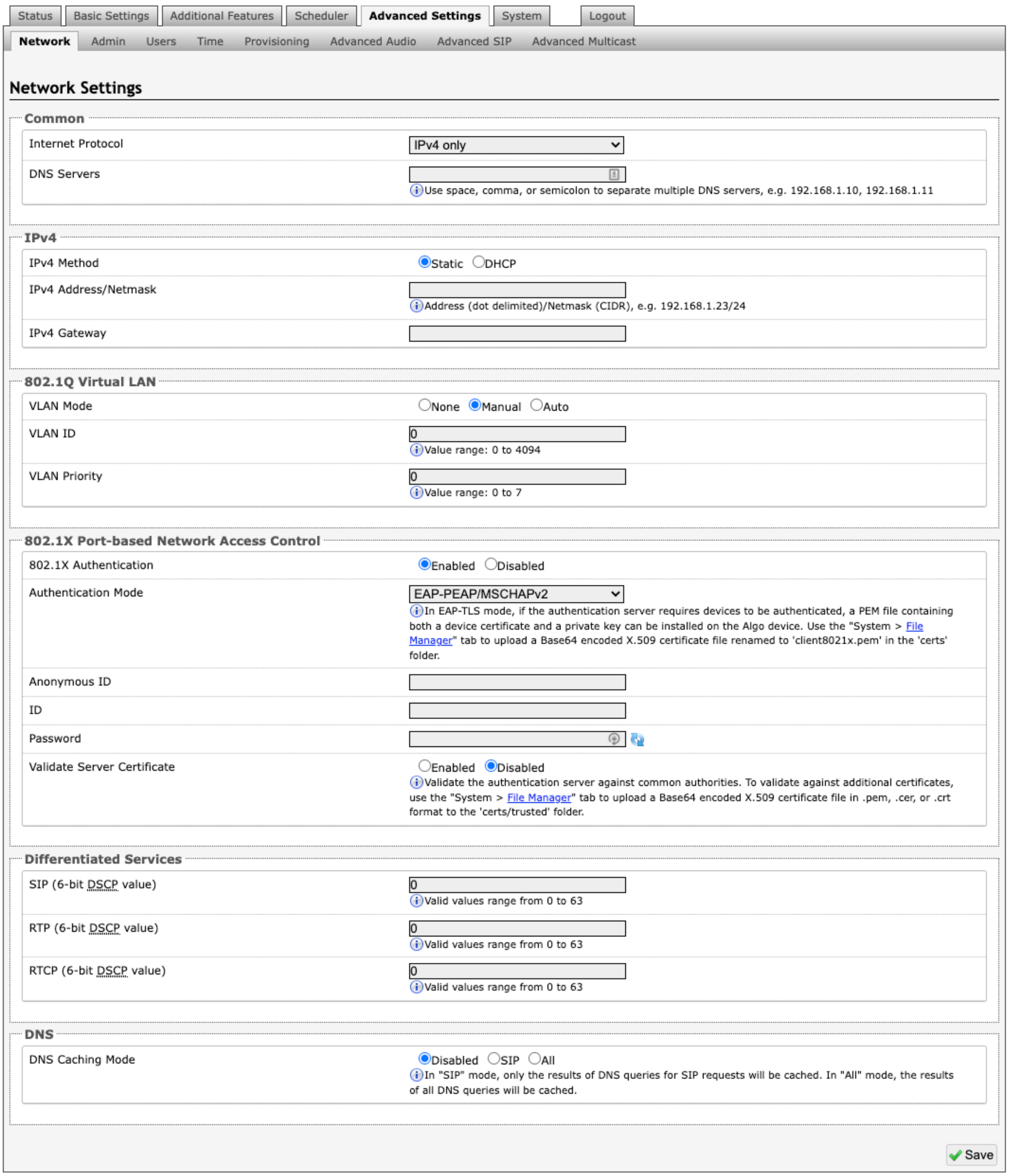


Figure 25: Network settings

Common

Internet Protocol

DHCP is an IP standard designed to make administration of IP addresses simpler. When selected, DHCP will automatically configure IP addresses for each 8301 on the network. Alternatively, the 8301 can be set to a static IP address.

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.

Supersede DNS provided by DHCP

Only available when DHCP is enabled. Use this option to enter a custom DNS server address and supersede the one sent via DHCP.

DNS Servers

Add one or multiple DNS servers. Separate each server by a space, comma, or semicolon.

IPv4

IPv4 Method

The 8301 can be set to a DHCP or a static IP address. When DHCP is selected, the DHCP will automatically configure IP addresses for the 8301 on the network.

IPv4 Address/Netmask

Enter the static IP address and netmask (CIDR format) for the 8301 (e.g., 192.168.1.23/24).

IPv4 Gateway

Enter the gateway address.

IPv6

IPv6 Method

The 8301 can be set to a DHCP or a static IP address. When DHCP is selected, the DHCP will automatically configure IP addresses for the 8301 on the network.

IPv6 Address/Netmask

Enter the static IP address and netmask (CIDR format) for the 8301 (e.g., 2001:123::abcd:1234/64).

IPv6 Gateway

Enter the gateway address.

802.1Q Virtual LAN

VLAN Mode

Enables or Disables VLAN Tagging. 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 commonly known as IEEE 802.1p and defines the Generic Attribute Registration Protocol.

VLAN ID

Specifies the VLAN to which the Ethernet frame belongs. A 12-bit field specifying the VLAN to which the Ethernet frame belongs. The hexadecimal values of 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

Sets the frame priority level. Otherwise known as Priority Code Point (PCP), VLAN Priority is a 3-bit field which refers to the IEEE 802.1p priority. It indicates the frame priority level. Values are from 0 (lowest) to 7 (highest).

802.1X Port-based Network Access Control

802.1x Authentication

Credentials to access LAN or WLAN that have 802.1X network access control (NAC) enabled. This information will be available from the IT Administrator.

Authentication Mode

Select the desired authentication mode.

Anonymous ID

If configured, the 8301 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.

Password

Enter the password.

Validate Server Certificate

Validate the authentication server against common authorities. To validate against additional certificates, go to the *System → File Manger* to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder.

Differentiated Services

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

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

DNS Caching Mode

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.

6.7.2 Admin

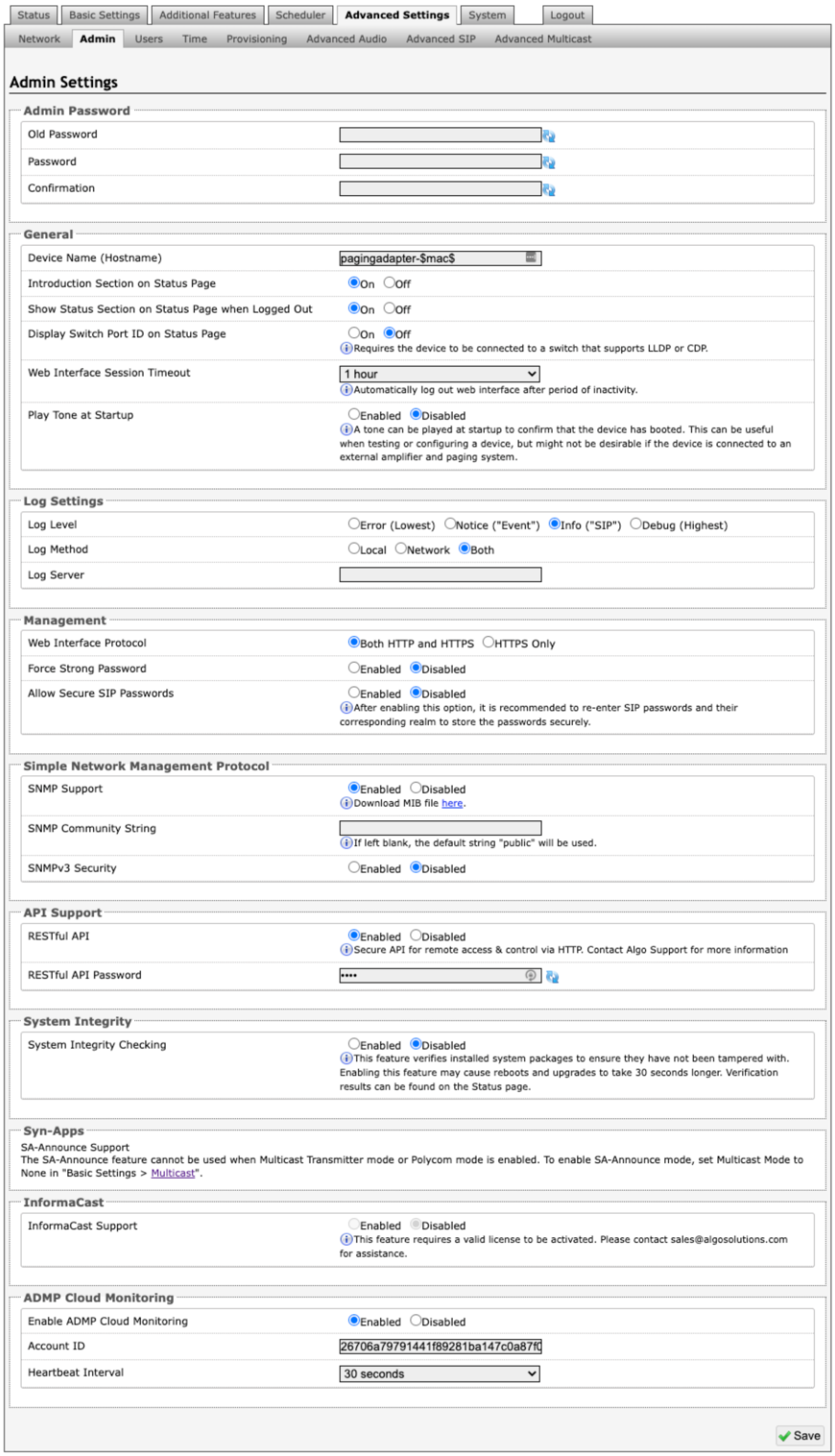


Figure 26: Admin settings

Admin Password

Old Password

Enter the old password.

Password

Password to log into the 8301 web interface. You should change the default password ***algo*** to secure the device on the network. If you have forgotten your password, you will need to perform a reset using the **Reset Button** to restore the password (as well as all other settings) back to the original factory default conditions.

For additional password security see "Force Strong Password" below.

Confirmation

Re-enter network admin password.

General

Device Name (Hostname)

Name to identify the device in the Algo Network Device Locator Tool.

Introduction Section on Status Page

Allows the introduction text to be hidden from the login screen.

Show Status Section on Status Page when Logged Out

Use this option if you wish to block access to the status page when logged out. The settings and configurations, on the status page, will be hidden entirely unless you're logged in – this feature is useful when you want only trusted users to view possible sensitive device information.

Display Switch Port ID on Status Page

Enable this option to display the Switch Port ID. This option requires the 8301 to be connected to a switch that supports LLDP or CDP.

Web Interface Session Timeout

Set the maximum period of inactivity after which the web interface will log out automatically.

Play Tone at Startup

A tone can be played at start up to confirm that the device has booted.

Log Settings

Log Level

The Log Level is to be used on the advice of Algo technical support only.

Log Method

Allows the 8301 to write to external Syslog server if the option for external (or both) is selected.

Log Server

If ‘Network’ or ‘Both’ is selected this is the address of the Syslog server on the network.

Management

Web Interface Protocol

HTTPS is always enabled on the device. Use ‘HTTPS Only’ mode to disable HTTP, then requests will be automatically redirected to HTTPS. Also note that since the device can have any address on the local network, no security certificate exists, and thus most browsers will provide a warning when using HTTPS.

Force Strong Password

When enabled, ensures that a secure password is provided for the device’s web interface for additional protection. The password requirements 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

Allows SIP passwords to be stored in the configuration file in an encrypted format, to prevent viewing and recovery. Once enabled, the SIP ‘Realm’ field should be entered and all the configured Authentication Password(s) must be re-entered in *Basic Settings* → *SIP*, and any other locations where SIP extensions have been configured, to save the encrypted password(s).

If the Realm is changed at a later time, all the passwords will also need to be re-entered again to save the passwords with the new encryption.

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.

Simple Network Management Protocol

SNMP Support

Additional SNMP support is anticipated for future. The current setting of the 8301 will respond to a simple status query for automated supervision. Contact Algo technical support for more information.

API Support

RESTful API

Secure API for remote access and control via HTTP.

System Integrity

System Integrity Checking

This feature verifies installed system packages to ensure they have not been tampered with by running 'Perform 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

SA-Announce Support

Syn-Apps SA-Announce paging application converts unicast streams to multicast and delivers them to the target endpoints. The feature can only be used on the 8301 when Multicast Sender Mode is disabled (set to 'None') in the *Basic Settings* → *Multicast* tab.

SA-Announce Server

Enter the SA-Announce Server to use the Syn-Apps paging feature. To use the server provided by the DHCP Option 72, leave the field blank.

Local Management Port

Enter the local management port for the SA-Announce Server.

InformaCast

InformaCast Support

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

Microsoft

Microsoft Teams Support

Enabling this setting will provision the device via Microsoft's servers. The device reboot will take up to 5 minutes to complete.

ADMP Cloud Monitoring

Enable ADMP Cloud Monitoring

This feature requires a valid Account ID. Please contact sales@algosolutions.com for assistance.

6.7.3 Users

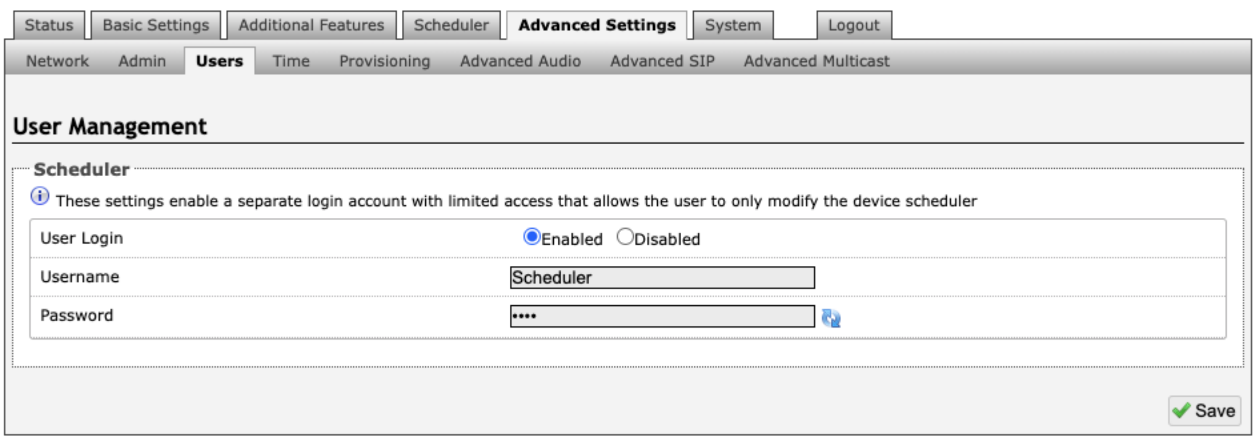


Figure 27: Users settings

A separate login account with limited access can be set up. The user will only be able to modify the device scheduler.

6.7.4 Time

Network time is used for logging events into memory for troubleshooting.

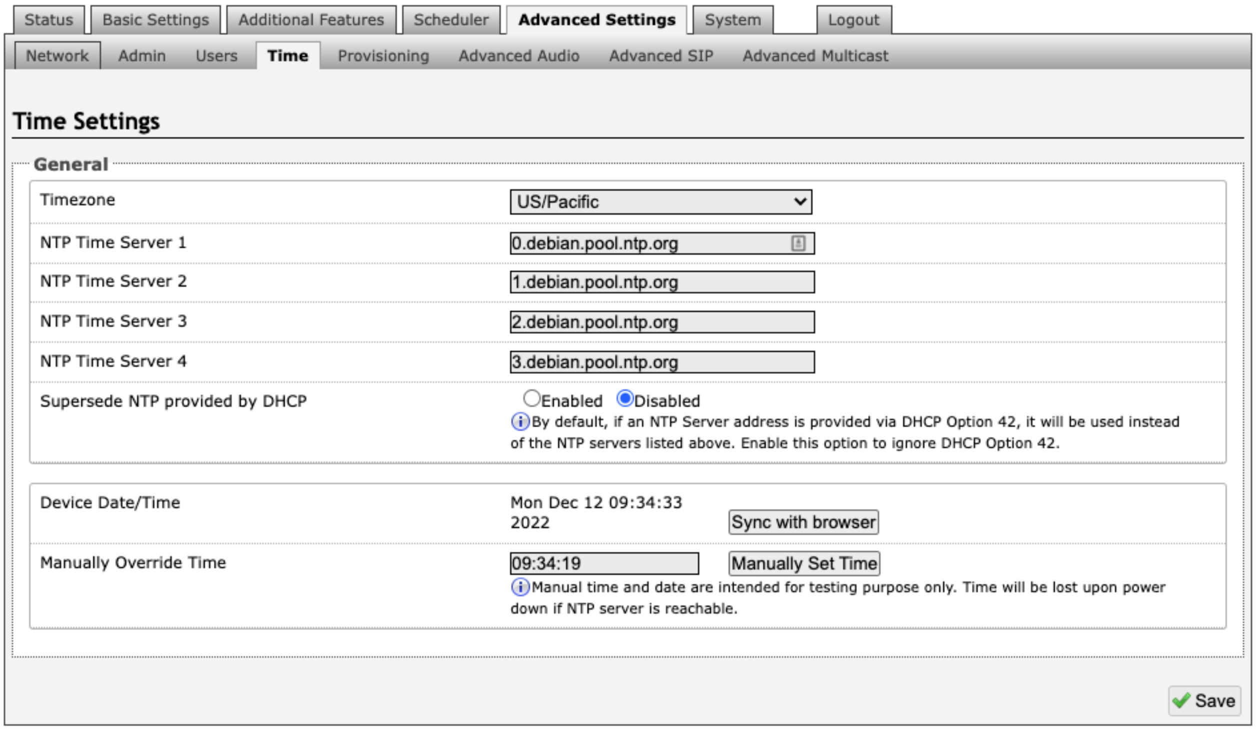


Figure 28: Time settings

Timezone

Select a time zone to be used.

NTP Time Servers 1/2/3/4

The interface will attempt to use Timer Server 1 and work down the list if one or more of the time servers become unresponsive.

Supersede NTP provided by DHCP

When 'Use DHCP Option 42' is chosen, if an NTP Server address is provided via the DHCP Option 42, that NTP Server will be used instead of the four (4) mentioned above. Alternatively, 'Ignore DHCP Option 42' can be chosen to only use servers mentioned above.

Device Date/Time

This field shows the current time and date as set on the device. If testing the device on a lab network that may not have access to an external NTP server, the "Sync with browser" button can be used to temporarily set the time on the device.

Note

This time value will be lost at power down or overwritten if NTP is currently active. Time and date are used for logging purposes and for the scheduler feature.

6.7.5 Provisioning

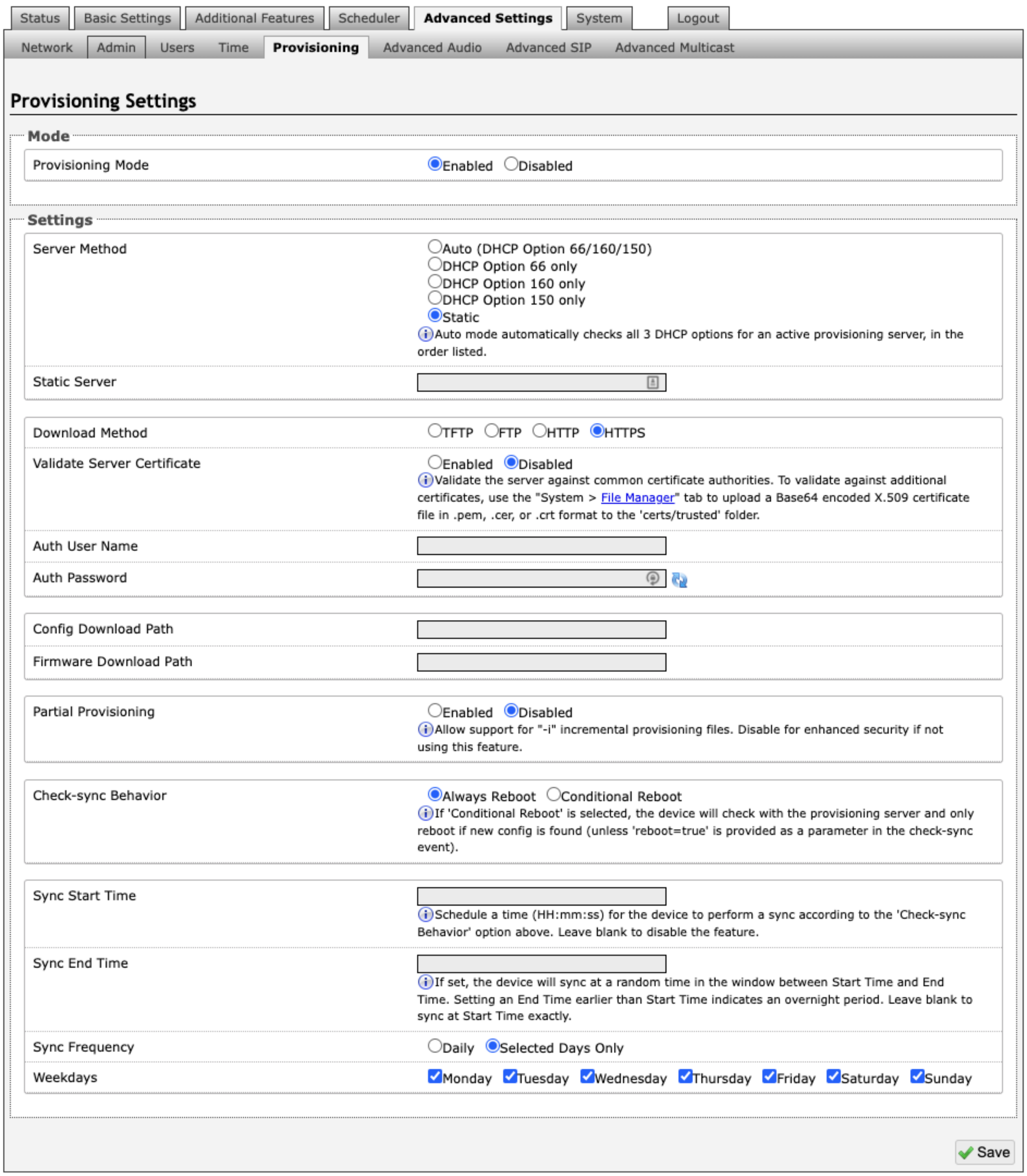


Figure 29: Provisioning settings

Note

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.

Mode

Provisioning Mode

Provisioning allows installers to pre-configure the 8301 units prior to installation on a network. It is typically used for large deployments to save time and ensure consistent setups.

Settings

Server Method

The device can be provisioned via the Auto mode (where all three DHCP options (Option 66/160/150) will be automatically checked for an active provisioning server), just one of the three specified DHCP options, or a Static Server. In addition, there are four different ways to download provisioning files from a “Provisioning Server”: TFTP (Trivial File Transfer Protocol), FTP, HTTP, or HTTPS.

Static Server

Enter the server address or domain.

Download Method

The 8301 configuration files can be automatically downloaded from a TFTP server using DHCP Option 66. This option code (when set) supplies a TFTP boot server address to the DHCP client to boot from.

Important
DHCP must be enabled if using DHCP Option 66/160/150, in order for Provisioning to work.

One of two files can be uploaded on the Provisioning Server (for access via TFTP, FTP, HTTP, or HTTPS):

- Generic (for all Algo 8301 IP Paging Adapter & Scheduler) **algop8301.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.

Config Download Path

Enter the path where the configuration file Is located within the provisioning server (e.g. algo/config/8301).

Firmware Download Path

Enter the path where the firmware file Is located within the provisioning server (e.g. algo/firmware/8301).

Partial Provisioning

Allow support for “-i” incremental provisioning files. Disable for enhanced security if not using this feature.

Check-sync Behavior

If 'Conditional Reboot' is selected, the device will check with the provisioning server and only reboot if a 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 the Start Time indicates an overnight period. Leave blank to sync at Start Time exactly.

Sync Frequency

Choose the frequency for which this setting should occur. Select between daily or go to 'Sync Days' to choose specific days of the week.

Sync Days

Select the days of the week to apply this setting for.

MD5 Checksum

In addition to the **.conf** file, an **.md5** checksum file must also be uploaded to the Provisioning server (for TFTP mode only). This checksum file is used to verify that the **.conf** file is transferred correctly without error.

A tool such as can be found at the website address below and may be used to generate this file: http://www.fourmilab.ch/md5

The application doesn't need an installation. To use the tool, simply unzip and run the application (md5) from a command prompt. The proper .md5 file will be generated in the same directory.

If using the above tool, be sure to use the "-l" parameter to generate lower case letters.

Generating a generic configuration file

If using a generic configuration file, extensions and credentials have to be entered manually once the 8301 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 8301 with the MAC address specified in the configuration file name. Since all the necessary settings can be included in this file, the 8301 will be ready to work immediately after the configuration file is downloaded. The MAC address of each 8301 can be found on the back label of the unit.

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

6.7.6 Advanced Audio

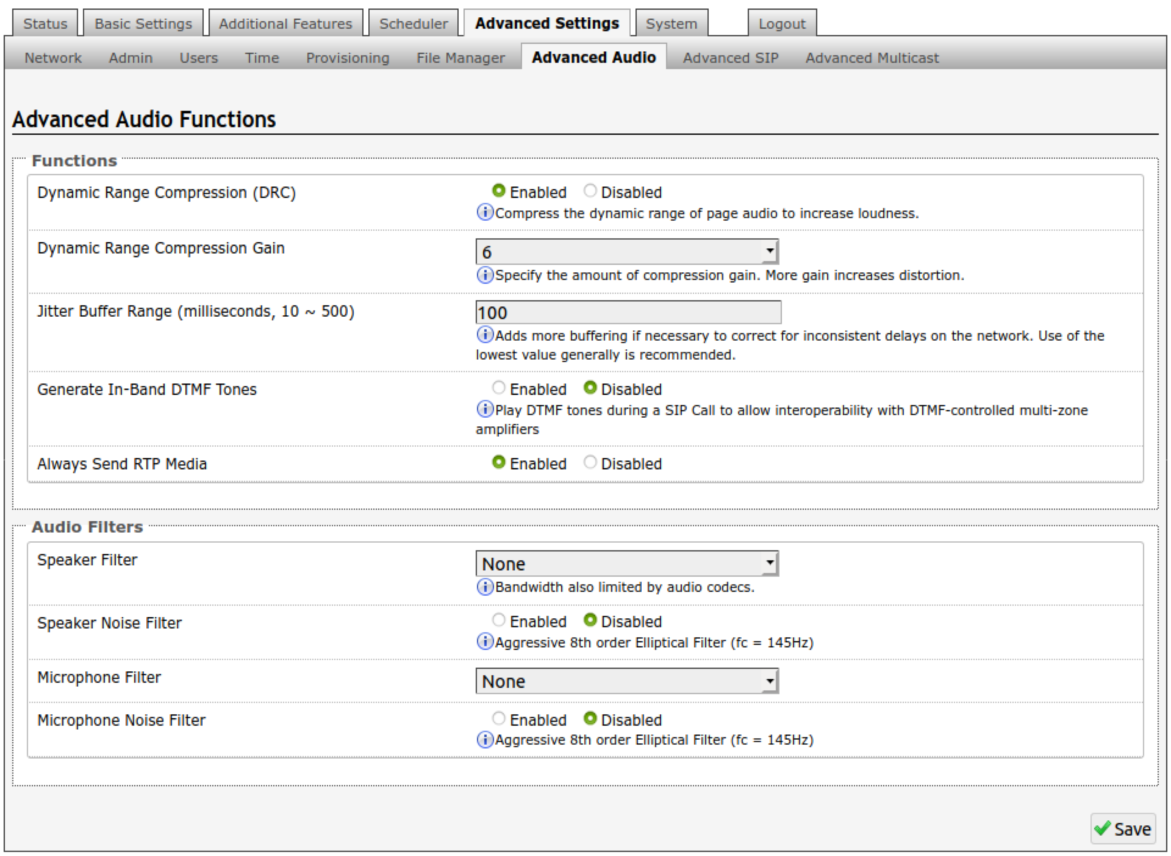


Figure 30: Advanced audio settings

Functions

Dynamic Range Compression (DRC)

If enabled, compresses the dynamic range of page audio to increase loudness.

Dynamic Range Compression Gain

Higher compression gain increases distortion.

Jitter Buffer Range

The jitter buffer removes the jitter in arriving network packets by temporarily storing them. This process corrects the inconsistent delays on the network. It is recommended to use the lowest value.

Always Send RTP Media

If enabled, audio packets will be sent at all times, even during one-way paging mode. This option is needed in cases when the server expects to see audio packets at all times.

Audio Filters

Speaker Filter

Applies a high-pass filter to the speaker output. Used to reduce audio artifacts like humming or buzzing by filtering out unwanted frequencies.

Speaker Noise Filter

Enables heavy filtering below 145 Hz to reduce mains induced noise (fans).

Microphone Filter

Applies a high-pass filter to the microphone input. Used to reduce audio artifacts like humming or buzzing by filtering out unwanted frequencies.

Microphone Noise Filter

Enables heavy filtering below 145 Hz to reduce mains induced noise (fans).

Microphone

Global Microphone Mute

Enabling this will disable the microphone entirely.

Microphone Volume

Select a volume for the microphone.

6.7.7 Advanced SIP

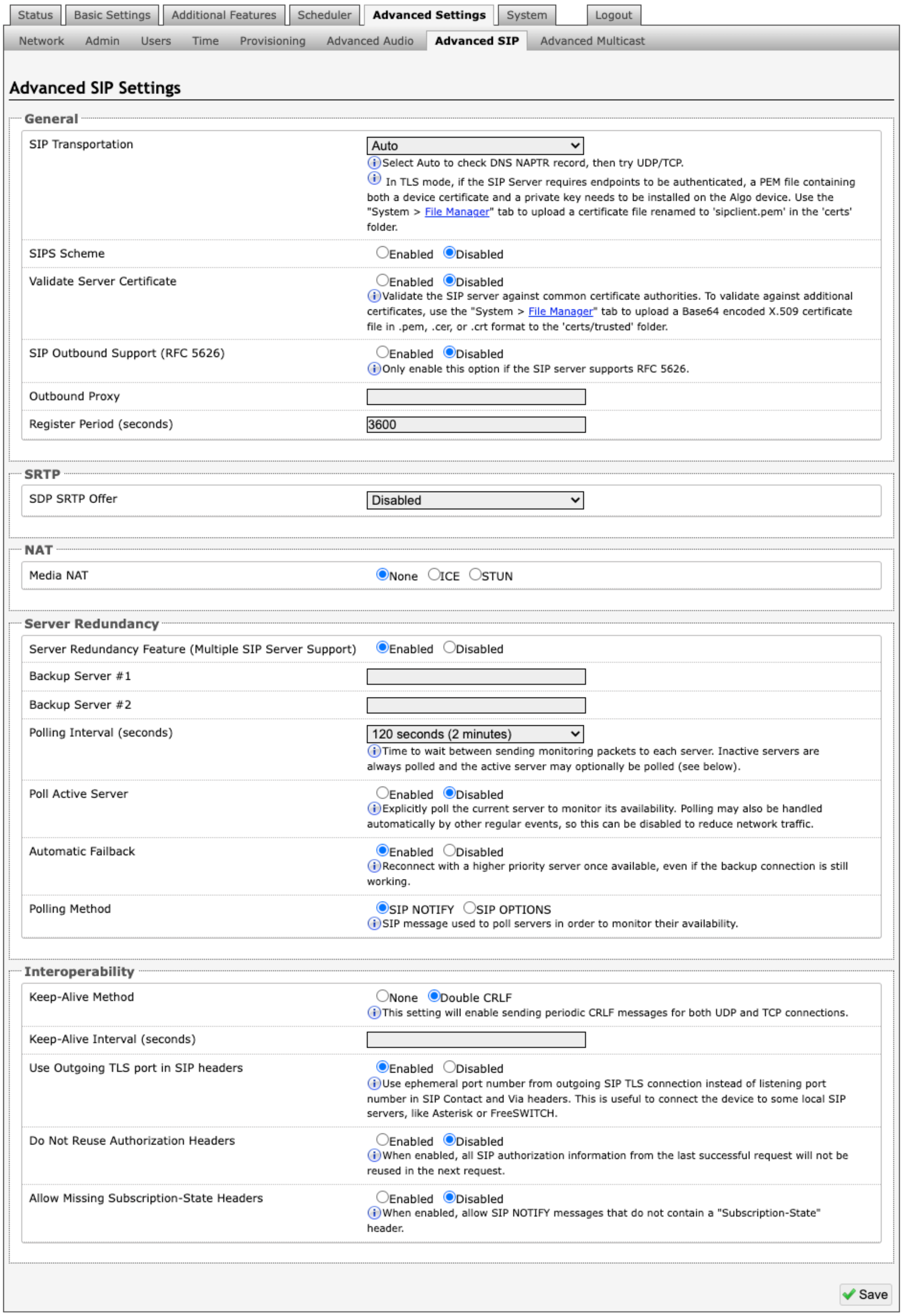


Figure 31: Advanced SIP Setting

General

SIP Transportation

Which transport layer protocol to use for SIP messages. Setting ‘SIP Transportation’ to ‘TLS’, ensures the encryption of SIP traffic.

SIPS Scheme

Only visible when ‘SIP Transportation’ set to ‘TLS’. Enabling SIPS Scheme requires the SIP connection from endpoint to endpoint to be secure.

Validate Server Certificate

Validate the SIP server against common certificate authorities.

SIP Outbound Support (RFC 5626)

Enable this option to support best networking practices according to RFC 5626. This option should generally be enabled if the Algo device is being registered with a hosted server or if TLS is being used for SIP Transportation.

Outbound Proxy

IP address for outbound proxy. A proxy (server) stands between a private network and the internet.

Register Period (seconds)

Maximum requested period of time where the 8301 will re-register with the SIP server. Default setting is 3600 seconds (1 hour). Only change if instructed otherwise.

SRTP

SDP SRTP Offer

Setting ‘SDP SRTP Offer’ to ‘Optional’, means the SIP call’s RTP data will be left unencrypted if the other party does not support SRTP. Setting ‘SDP SRTP Offer’ to ‘Standard’, encrypts RTP voice data, meaning the normal audio RTP packets will now be secure (SRTP). This means SIP calls will be rejected if other party does not support SRTP. The ‘Standard’ option secures the audio data between parties, by making sure that it’s not left out in the open for third parties to later reconstruct and listen to.

NAT

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

Server Redundancy Feature

Two secondary SIP servers may be configured. The 8301 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.

If Server Redundancy is selected the web page will expand as shown below.

Backup Server #1

If the primary server is unreachable, the 8301 will attempt to register with the backup servers. If enabled, the 8301 will always attempt to register with the highest priority server.

Backup Server #2

If backup server #1 is unreachable, the 8301 will attempt to register with the 2nd backup server. If enabled, the 8301 will always attempt to register with the highest priority server.

Polling Intervals (seconds)

The time period between sending monitoring packets to each server. Non-active servers are always polled, and active server may optionally be polled (see below).

Poll Active Server

Explicitly poll current server to monitor availability. This may also be handled automatically by other regular events and can be disabled to reduce network traffic.

Automatic Fallback

This enables device to reconnect with a higher priority server once available, even if the backup connection is still fine.

Polling Method

A SIP message used to poll servers to monitor availability.

Interoperability

Keep-Alive Method

If Double CRLF is selected, the 8301 will send a packet every 30 seconds (recommended value) to maintain connection with the SIP Server if behind NAT.

Keep-Alive Interval

This is the interval in seconds that the CRLF message should be sent.

Use Outgoing TLS port in SIP Headers

Use ephemeral port number from outgoing SIP TLS connection instead of the 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

When enabled, all SIP authorization information from the last successful request will not be reused in the next request.

Allow Missing Subscription-State Headers

When enabled, this allows SIP NOTIFY messages that do not contain a ‘Subscription-State’ header.

6.7.8 Advanced Multicast

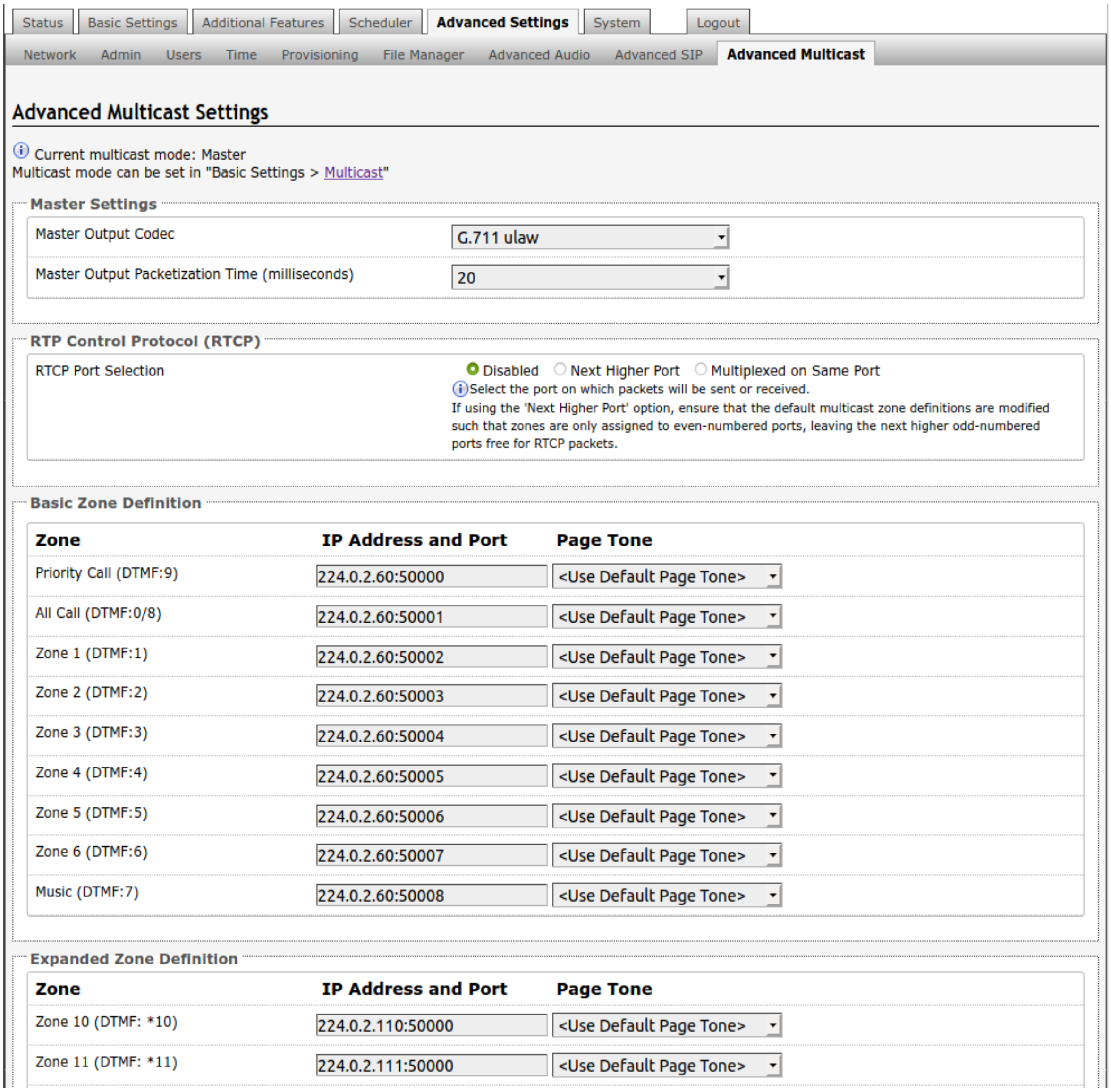


Figure 32: Advanced multicast - transmitter settings

Note

The settings on this tab are only visible when in Sender or Receiver multicast mode.

The default pre-populated multicast addresses above will work in most cases and should only be altered for rare cases.

Transmitter Settings

Transmitter Output Codec

This is the audio encoding format used by the Transmitter device when sending output to the Receivers.

Output Packetization Time (milliseconds)

The size of the audio packets sent by the Transmitter to the Receivers. The default of 20 ms is recommended unless a different value is specifically required for compatibility with other devices.

Multicast TTL

The multicast time to live (TTL) setting should only be changed 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.

Receiver Settings

RTCP Port Selection

Select the port on which RTCP 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.

Polycom Receiver Tones

Available if Multicast Receiver and ‘Polycom Group Page’ or ‘Polycom Push-to-Talk’ are selected in the *Basic Settings* → *Multicast* tab. A tone may be set for any of the 25 Polycom Groups. If using an Algo device as a Multicast Sender, it is recommended to set the Receiver tones to ‘None’ to avoid conflicts, as the Algo devices already multicast a tone by default.

Basic Zone Definitions

Zones

The ‘Expanded’ Receiver zones can be enabled/disabled in *Basic Settings* → *Multicast*. Default IP addresses and ports may be revised for any given zone in the table.

Important
Ensure that the Address and Port settings are the same for all Sender and Receiver devices.

Page Tone and Page Volume

Sender Mode: By default, the same tone can be set for all Receiver zones in the *Basic Settings* → *Features* tab. Unique paging tones may be revised for any given zone in the table above.

Receiver Mode: When an Algo device is the multicast Sender, a page tone will play on the Receiver device, so it is recommended to set the Receiver tone to ‘None’. If a page is received from a non-Algo device that doesn’t send a tone, a tone can be inserted on the Receivers (above) each time they detect page audio starting, allowing them to play a tone.

By default, the same page volume can be set for all Receiver zones in the *Basic Settings* → *Features* → *Page Volume*. Unique page volumes may be revised on a per-zone basis in the table above. For instance, emergency pages can be louder on certain Receiver speakers.

6.8 System

6.8.1 Maintenance

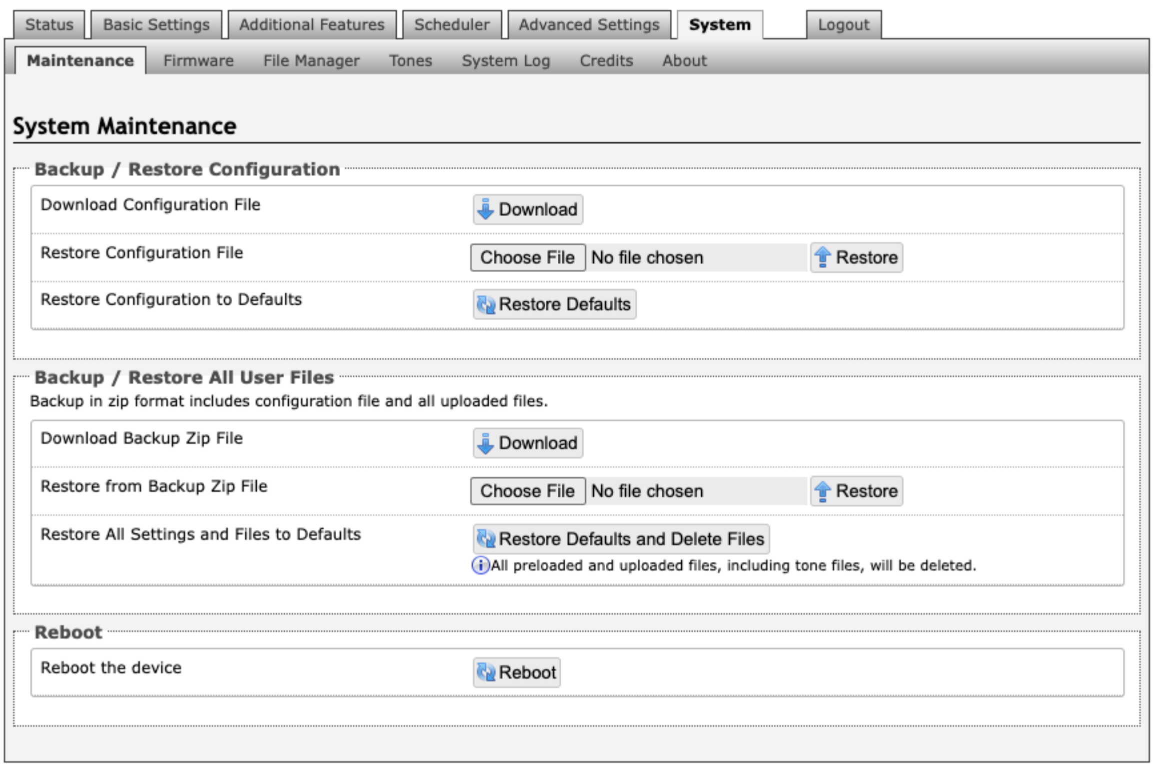


Figure 33: Maintenance settings

Backup / Restore Configuration

Download Configuration File

Save the device settings to a text file for backup or to setup a provisioning configuration file.

Restore Configuration File

Restore settings from a backup file.

Restore Configuration to Defaults

Resets all 8301 IP Paging Adapter & Scheduler settings to factory default values.

Backup / Restore All User Files

Download Backup Zip File

Saves the device settings (configuration) and all the files in File Manager: certificates, licenses, and tones to a backup zip file.

Restore from Backup Zip File

Restores the device settings (configuration) and all the files in *File Manager*: certificates, licenses, and tones from a backup zip file.

Restore All Settings and Files to Defaults

Resets the device settings (configuration) and all the files in *File Manager*: certificates, licenses, and tones to factory default values.

Reboot

Reboot the Device

Reboots the device.

6.8.2 Firmware

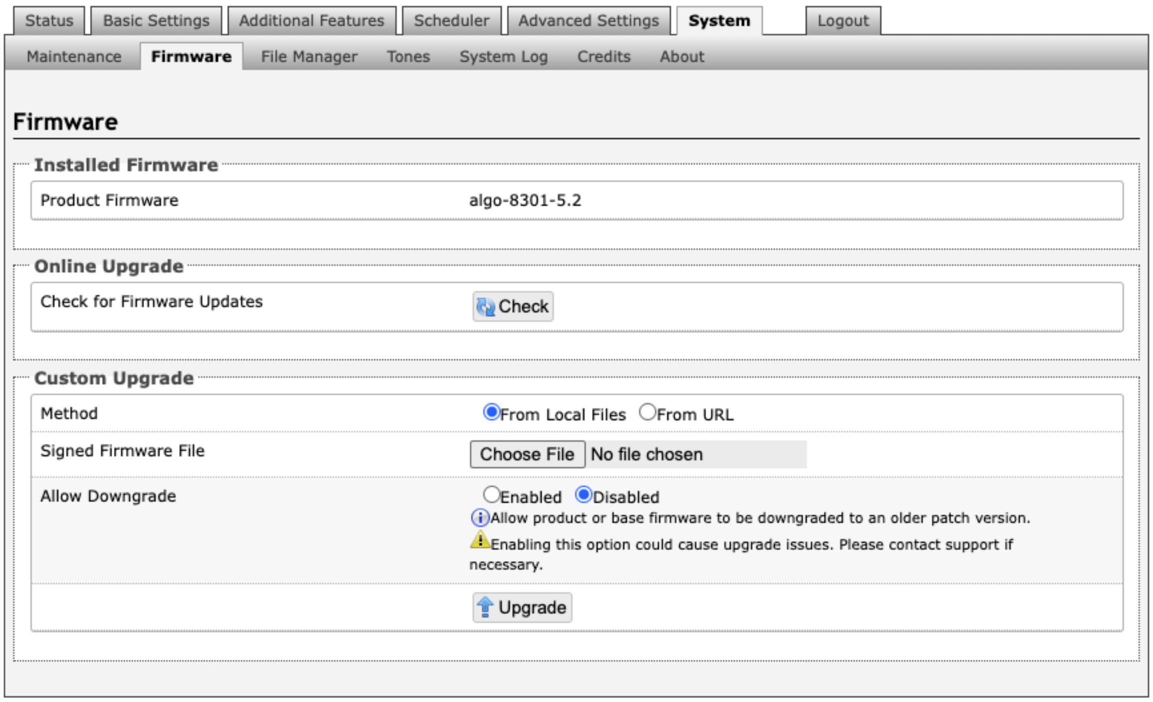


Figure 34: Firmware settings

Installed Firmware

Product Firmware

Shows the current firmware on the device.

Online Upgrade

Check for Firmware Updates

Check for the latest firmware. If firmware is current, **Latest Firmware** will show as 'Firmware up to date'. If firmware needs to be upgraded, the new firmware availability will be listed. Internet connection is required.

Custom Upgrade

Method

For firmware upgrades. Specify whether the firmware files will be downloaded from the local computer or a remote URL.

Signed Firmware File

How to upgrade Firmware

1. From the top menu, go to *System* → *Firmware*.
2. In the Upgrade section, press **Choose File** and select the 8301 firmware file to upload. Note that both FW firmware and MD5 checksum files must be loaded.
3. Press **Upgrade.**
4. After the upgrade is complete, confirm that the firmware version has changed (refer to top right of Control Panel).

Allow Downgrade

Allow product or base firmware to be downgraded to an older patch version. Enabling this option could cause upgrade issues.

6.8.3 File Manager

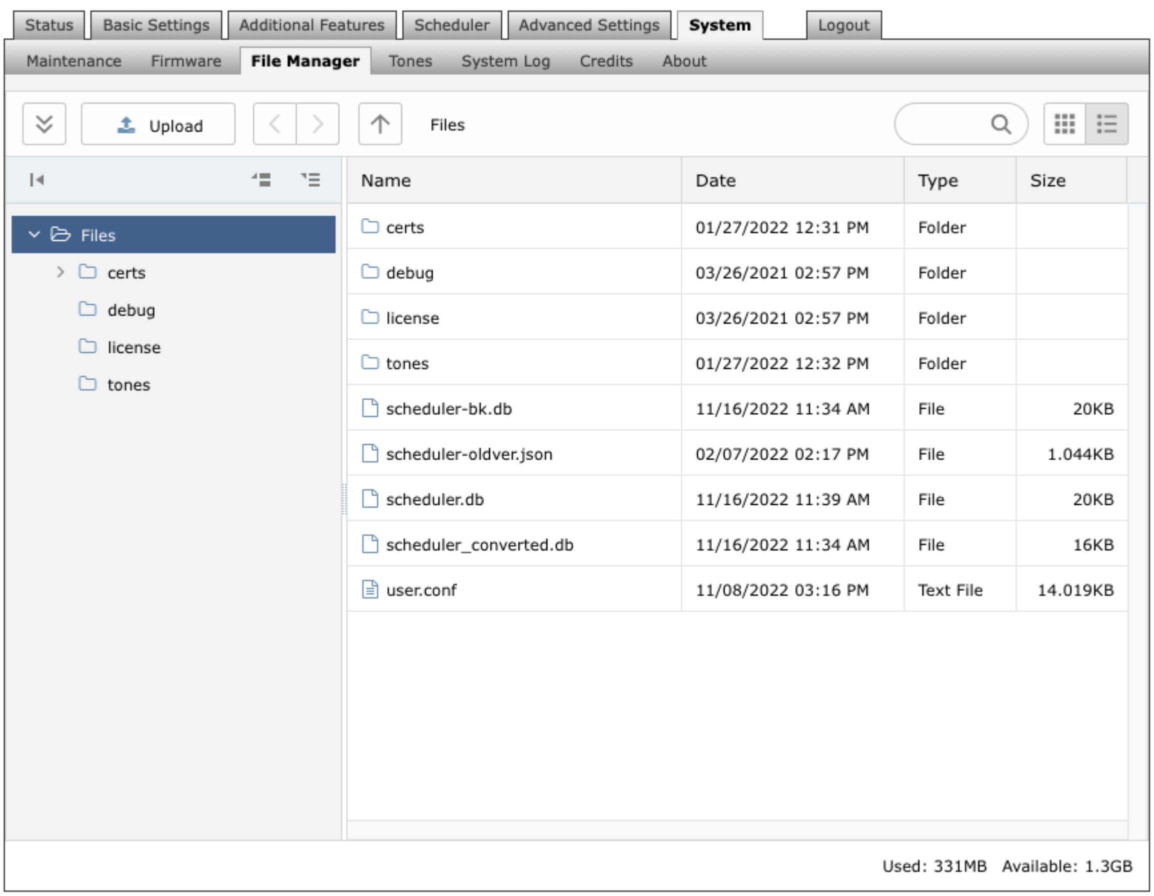


Figure 35: File manager settings

Uploading Custom Audio Files

Custom audio files may be uploaded into memory (1 GB) to play for notification applications. Place your audio files into the **tones** directory.

An existing file may also be modified. Download the original file and right clicking the tone and selecting 'Download', making the desired changes, and then uploading the new version with a different name. 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.

6.8.4 Tones

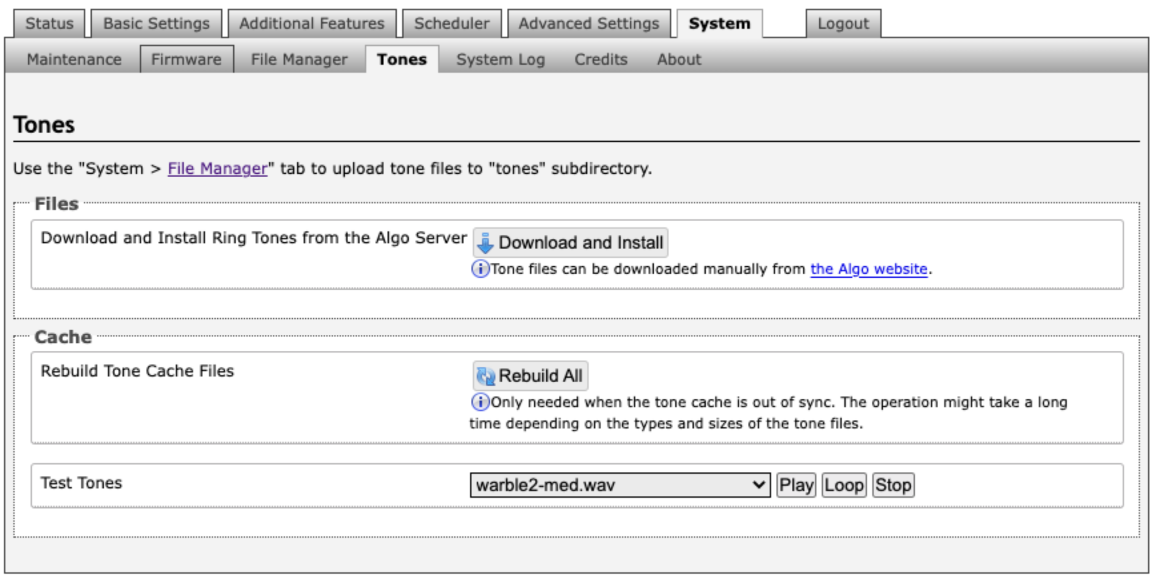


Figure 36: Tones settings

Tone Files Included in Memory

The 8301 includes several pre-loaded audio files that can be selected to play for various events. The web interface allows selection of the file and the ability to play it immediately over the speaker for testing (available in *Basic Settings → Features*). Files may also be deleted or renamed.

6.8.5 System Log

System log files are automatically created and assist with troubleshooting in the event the 8301 does not behave as expected.

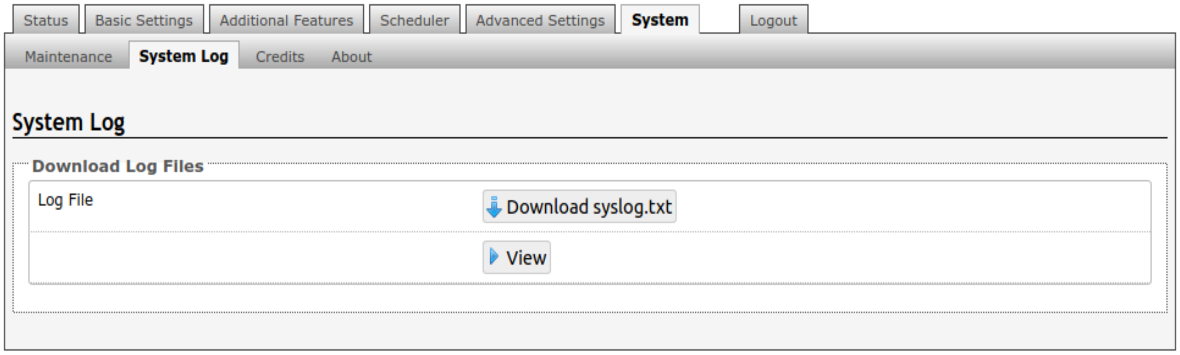


Figure 37: System log settings

6.9 Logout

Log out of the 8301 web interface.

7 SPECIFICATIONS

Table 1: 8301 Specification Table

Power	
PoE-Powered	PoE (IEEE 802.3af Class 0) 48V, 12.95W (Max 4 W - Idle nominal 2W)
SIP	
SIP Extensions	50 Page & 10 Alerting/Ring extensions with multicast scalability
Transport Protocols	UDP, RTP, TCP
Security	TLS, MTLS, SRTP
Multicast Compatibility	
Multicast	RTP Multicast (Send and Receive 50 Zones)
Third-Party Multicast	Poly™ Group Page, Singlewire™ InformaCast, Syn-Apps™ Revolution
Digital IO	
Relay Configured as Input	Normally open or normally closed dry contact supervision. Compatible with Algo 1202, 1203, 1204, and 1205 Accessories.
API	
API	RESTful
Audio	
Audio Codes	G.711 A-law, G.711 u-law, G.722, Opus 48 kHz.
Audio Memory & Format	1 GByte audio storage for WAV or MP3 files
Audio Controls	Volume, AGC, Latency, LF Cut
Anti-Feedback Delay	Cache to memory and release
Audio Delay	Programmable 1-1000 ms synchronization delay
Network	
Network	IPv4, IPv6, DHCP, VLAN, MDNS
Link Layer	LLDP, CDP
QOS	DSCP (SIP, RTP, RTCP)
Web Interface	HTTP, HTTPS
Provisioning	TFTP, FTTP, HTTP, HTTPS, DHCP Options 66, 150, 160 Reboot via SIP Check-sync
NAT	STUN, TURN, CRLF Keep Alive, SIP Outbound
Address Resolution	DNS, SRV Record
Supervision	SNMP V1.3, RTCP, Algo 8300, ADMP
Redundancy	Secondary and tertiary SIP server
Input/Output	
Female RJ45 Jack	
Aux In	3.5 mm jack for analog line level input for music input. Non-isolated.
Aux Out	3.5 mm jack for analog line level output for compatible PC speakers or headset. Non-isolated.

Line In XLR-Mini	Balanced and isolated audio (Page or music) input can be configured for pass-through to Line Out (when paging is idle) or for broadcast via multicast.
Line Out XLR-Mini	Balanced and isolated audio output to external amplifier. Locking mini-XLR female to standard XLR male cable available. Output level defined using web interface.
Terminal Block Line In	Balanced and isolated wire pair input parallel to XLR-Mini Line In (polarity independent).
Terminal Block Line Out	Balanced and isolated wire pair output to external amplifier. Parallel to XLR-Mini Line Out (polarity independent).
Relay Output	Max 30 V 50 mA (normally open)
Environmental & Mechanical	
Environmental	0 to +40° degree C (32 to 104° F), 10-95% Relative Humidity, non-condensing. Dry indoor locations only.
Dimensions (Product)	6.75” x 4.3” x 1.18” (17.2 cm x 10.9 cm x 3.0 cm)
Weight (Product)	0.95 lbs (0.4 kg)
Weight (Shipping)	1.5 lbs (0.7 kg)
Mounting	Snap mounting bracket included.
Compliance	
RoHS, CE, FCC Class A, CISPR 22 Class A, CISPR 24, CSA/UL (USA & Canada), EN60950	
Firmware	
These specifications refer to the Algo 8301 running on firmware 5.2 and above.	

8 FCC COMPLIANCE STATEMENT

his 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.