

8301 IP Paging Adapter & Scheduler

User Guide



AL061-UG-GP308301-230508 Firmware Version 5.3.2 <u>support@algosolutions.com</u> 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

3

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

 ${\small @2023} \ \mbox{Algo} {\small \circledast}$ is a registered trademark of Algo Communication Products Ltd.

All Rights Reserved. All other trademarks are the property of their respective owners. All specs are subject to change without notice.



Table of Contents

1	Ge	eneral.		1
	1.1	Intro	duction	1
2	Se	tup an	d Installation	1
	2.1	Getti	ng Started – Quick Install and Test	2
	2.2	Insta	lation	2
	2.2	2.1	Programming and Configuration	3
3	Ap	oplicati	ons	4
	3.1	Conn	ecting Paging Amplifier to UC Environment	4
	3.2	Notif	ication	4
	3.3	Schee	duling	4
	3.4	Multi	casting	4
4	Fe	atures		5
	4.1	SIP P	aging: Registering an 8301 Device	5
	4.2	SIP P	aging: Multiple Algo SIP Endpoints (Using Multicast)	5
	4.3	SIP P	aging: Multiple Algo SIP Endpoints (Using Multicast)	6
	4.4	Back	ground Music Streaming	6
	4.5	Multi	cast Page Zones	6
	4.6	SIP R	ing Event	8
	4.7	SIP A	ctivated Notification Alerts	8
	4.8	TLS fo	or SIP Signaling and Provisioning	8
	4.8	8.1	Uploading Public CA Certificates to Algo SIP Endpoints	9
	4.8	8.2	HTTPS Provisioning	9
	4.8	8.3	Securing SIP Signaling (and RTP Audio)	11
5	W	iring Co	onnections	13
	5.1	Conn	ecting Input Devices to 8301	13
	5.2	Blue	LED Indicators	17
	5.3	Reset	t	17
6	W	eb Inte	rface	18
	6.1	Stats		18
	6.3	1.1	Device Status	18
	6.2	Basic	Settings	19
	6.2	2.1	SIP	19
	6.2	2.2	Features	22
	6.2	2.3	Multicast	25
	6.3	Multi	cast (Transmitter/Sender Settings)	27
	6.4	Multi	cast (Receiver Settings)	30
	6.5	Addit	ional Features	32
	6.	5.1	Input/Output	32



8301 IP Paging Adapter & Scheduler

	6.5.2	Emergency Alerts	. 39
	6.5.3	More Page Extensions	. 43
	6.5.4	More Ring Extensions	. 44
6.	6 Sched	duler TAB	. 45
	6.6.1	Calendar	. 45
	6.6.2	Schedules	. 46
	6.6.3	Data	. 47
6.	7 Advar	nced Settings	. 48
	6.7.1	Network	. 48
	6.7.2	Admin	. 52
	6.7.3	Users	. 56
	6.7.4	Time	. 56
	6.7.5	Provisioning	. 58
	6.7.6	Advanced Audio	. 61
	6.7.7	Advanced SIP	. 63
	6.7.8	Advanced Multicast	. 67
6.	8 Systei	m	. 69
	6.8.1	Maintenance	. 69
	6.8.2	Firmware	. 71
	6.8.3	File Manager	. 72
	6.8.4	Tones	. 73
	6.8.5	System Log	. 74
6.	9 Logou	Jt	. 74
7	Specificat	tions	75
8	FCC Comp	pliance Statement	77

Tables

Table 1: 8301 Specification Table	.75
-----------------------------------	-----

Figures

Figure 1: Wall Mount	2
Figure 2: Using DTMF Selectable Mode	7
Figure 3: Using Multiple SIP Extensions	8
Figure 4: Use Case Wiring Diagram	13
Figure 5: 8301 Relay Input	13
Figure 6: 1202 Call Button Wiring	14
Figure 7: 1203 Call Switch Wiring	14
Figure 8: 1204 Volume Control Switch Wiring	14
Figure 9: 1205 Audio Interface Wiring	15



Figure 10: 8301 Paging Adapter & Scheduler Front View	15
Figure 11: 8301 Paging Adapter & Scheduler Back View	15
Figure 12: Status	18
Figure 13: Basic Settings \rightarrow SIP	20
Figure 14: Basic Settings → Features	22
Figure 15: Multicast transmitter mode settings	27
Figure 16: Multicast receiver mode settings	30
Figure 17: Input settings	33
Figure 18: 1203 Call Switch	34
Figure 19: 1202 Call Button – the insert card is interchangeable	34
Figure 20: 1204 Volume Control	35
Figure 21: 1205 Audio Interface	35
Figure 22: Emergency Alerts	39
Figure 23: More page extensions	43
Figure 24: More ring extensions	44
Figure 25: Network settings	48
Figure 26: Admin settings	52
Figure 27: Users settings	56
Figure 28: Time settings	57
Figure 29: Provisioning settings	58
Figure 30: Advanced audio settings	61
Figure 31: Advanced SIP Setting	63
Figure 32: Advanced multicast - transmitter settings	67
Figure 33: Maintenance settings	69
Figure 34: Firmware settings	71
Figure 35: File manager settings	72
Figure 36: Tones settings	73
Figure 37: System log settings	74

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 Spannungsprüngen 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.



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.
- 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* \rightarrow *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: <u>www.algosolutions.com/locator</u>.

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* \rightarrow *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* \rightarrow *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 \rightarrow 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* \rightarrow *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* \rightarrow *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* \rightarrow *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 <u>priority</u> <u>hierarchy</u> – 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

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

- Zone 4
- Zone 5
- Zone 6
- Music



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 \rightarrow 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 \rightarrow 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* \rightarrow *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 \rightarrow Emergency Alerts and Additional Features \rightarrow 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 \rightarrow 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 <u>support@algosolutions.com</u> 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* \rightarrow *Advanced SIP* tab, then the device will validate the SIP server against common certificate authorities. To validate against additional certificates, use the *System* \rightarrow *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* \rightarrow *Provisioning* tab, then the device will validate the server against common certificate authorities. To validate against additional certificates, use the *System* \rightarrow *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 \rightarrow 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.



tatus	Basic Setting	s Add	litional	Features	Sche	eduler	Advan	ced S	Settings	Syste	m	Logo	but					
etwork	Admin I	Jsers	Time	Provisi	oning	Adv	anced Aud	lio	Advance	d SIP	Advanc	ed Mult	ticast		_		_	_
0V1S10	ning Sett	ings																
lode									~									
Provisio	ning Mode						Enal	bled	ODisabl	ed								
ettina	15																	
Server N	Method) (DH P Op P Op P Op	CP Optio tion 66 o tion 160 tion 150	n 66/16 nly only only	0/150)							
							Stat Auto r order list	ic mode ed.	automatio	ally chec	ks all 3 C	OHCP op	itions fo	r an act	ive prov	isioning	server, i	n the
Static S	erver										±.]						
Downloa	ad Method						Oteti	p ()	FTP Он	ττρ 💽	ITTPS							
Validate	e Server Cert	ificate					OEnabled Disabled Validate the server against common certificate authorities. To validate against additional certificates, use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file in .pemcer. or .ct format to the 'certs/trusted' folder.											
Auth Us	er Name																	
Auth Pa	ssword										٩	3						
Confia D	Download Pat	th										7						
Firmwar	re Download	Path																
Partial P	Provisioning						OEnal (i) Allow using this	bled suppo s feat	Disable ort for "-i" ure.	ed increme	ntal provi	isioning	files. D	isable fo	or enhan	ced sec	urity if no	pt
Check-s	ync Behavio	r					OAlwa i If 'Cor reboot if event).	ays Randition new o	eboot C nal Rebool config is fo	Condition t' is select cound (unl	onal Reb ted, the ess 'rebo	oot device v ot=true	vill chec ' is prov	k with t vided as	he provi a paran	sioning neter in	server ar the chec	nd only :k-sync
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 En	d Time						i If set, Time. Se sync at S	, the d tting a Start 1	levice will an End Tir 'ime exact	sync at a me earlie tly.	a random r than Sta	time in art Time	the wir e indicat	idow be ies an o	tween S vernight	tart Tin period.	e and En Leave bl	nd Iank to
Sync Fre	equency						ODail	у 🔘	Selected	Days Or	nly							
Weekda	ys						Mon	day	Tuesda	ay 🗹 we	ednesda	у 🔽ті	hursday	/ 🔽 Fri	dav 🔽	Saturd	ay 🔽 Si	unday



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 \rightarrow 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 Settir	ngs	Additional	Features	Scheduler	Advanced	d Settings	Syst	em	L	ogout			
Network	Admin	User	s Time	Provision	ing Advar	nced Audio	Advanced	SIP	Adva	anced N	Multicas	t		
Advanc	ed SIP Se	ttin	gs											
Gener	al													
SIP Tra	ansportation					TLS				~				
						i Select A	uto to check	DNS NA	PTR re	record, t	then try	UDP/TCP.		
						In TLS both a devi	mode, if the !	SIP Ser	ver rec	quires e e key ne	endpoints eds to b	to be authentica e installed on the	ted, a PEM file c	ontaining e the
						"System >	File Manager	' tab to	uploa	ad a cert	tificate fi	le renamed to 'sip	client.pem' in t	ne 'certs'
						folder.	~							
SIPS S	Scheme					OEnable	ed ODisabl	ed						
Validat	te Server Ce	rtifica	te			OEnable	ed ODisabl	ed er agair	st con	mmon o	ertificate	authorities. To v	alidate against a	dditional
						certificates,	, use the "Sy	tem >	File Ma	lanager	" tab to u	upload a Base64 e	ncoded X.509 c	ertificate
						file in .pem	, .cer, or .crt	format	to the	e 'certs/t	trusted'	folder.		
SIP Ou	tbound Sup	port (I	RFC 5626)			OEnable	ed ODisabl	ed In if the	SID	server o	upporte	PEC 5626		
0	und Decore						une uns optio		. 517 5		apports	N C 3020.		
Outbo	und Proxy													
Registe	er Period (se	conds	;)			3600								
SRTP														
SDP S	RTP Offer					Disabled				*				
NAT						A	<u></u>							
Media	NAT					ONone	OICE OS	TUN						
Sarva	r Podunda	neu												
Server	Redundance	v Eest	ure (Multin	e SID Sen	(er Support)	OEnable	ad ODisabl	od						
Sciver	Redundanc	y i cut			ver supporty	CENTRO		<u>u</u>					*****	
Intero	perability	r												
Keep-A	Alive Method					None	ODouble C	RLF						
						(i)This sett	ting will enab	e send	ng per	riodic C	RLF mes	sages for both UI	OP and TCP conn	ections.
Use Ou	utgoing TLS	port ir	n SIP heade	rs		Enable	d ODisabl	ed .						
						number in :	emeral port r SIP Contact a	umber nd Via	from o header	outgoing ers. This	g SIP TL is usefu	S connection inste I to connect the d	evice to some lo	oort ocal SIP
						servers, lik	e Asterisk or	FreeSW	птсн.	•				
Do Not	t Reuse Auth	orizat	ion Header	5		OEnable	ed ODisabl	ed						
						(i) When er reused in ti	habled, all SI he next reque	' autho st.	rizatio	on inforn	mation fr	om the last succe	sstul request wi	i not be
Allow I	Missing Subs	criptio	on-State He	aders		OEnable	ed ODisabl	ed						
	-					(i)When er	nabled, allow	SIP NO	TIFY m	message	es that d	o not contain a "S	ubscription-Stat	e" header.
														A So
														v 3a



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* \rightarrow *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 <u>Algo 1202 Installation</u> <u>Sheet</u>.



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 <u>Algo 1203 Getting</u> <u>Started Sheet</u>.



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 <u>Algo 1204 Getting Started Sheet</u>.



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 <u>Algo 1205 Getting Started Sheet</u>.



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

	Status Basic Settings Additional Features Schedule	r Advanced Settings Sys	stem	Logout
Γ	Device Status		_	
<u> </u>	elcome to the Algo 8301 IP Paging Adapte	r & Scheduler		
s	etting up your IP Paging Adapter & Scheduler:			
s	tep 1: Configure your IP Paging Adapter & Scheduler			
L	og in with the default password and use the Basic Settings	pages to set up the basic info	ormation.	
s	tep 2: Check network settings (Optional)			
U se	se the Network page under the Advanced Settings tab to ch rver. Contact your Network System administrator if you pla	ange network settings. The c an to assign a static IP addres	default sett ss, Mask, a	tting for the device is to obtain its IP address from a DHCP and Gateway to the device.
s	tep 3: Secure your IP Paging Adapter & Scheduler (O	ptional)		
U	se the Admin page under the Advanced Settings tab to cha	nge the administrator passwo	ord.	
6	Changing the password is extremely important if the device	Ontional)	public netwo	work.
D	ease register your product using the link below:	optional)		
h	to://www.algosolutions.com/register			
R	egistration ensures your access to the latest upgrades to th	is product and important serv	vice notices	25.
	Status	- F F		
	Device Name	pagingadapter-090c55		
	SIP Registration	Page Su	uccessful	(Extension 2187)
	Call Status	Idle		
	Proxy Status	Single proxy mode		
	Provisioning Status	None Found		
	MAC	00:22:ee:09:0c:55		
	IPv4	10.30.35.139/8, Gateway	y: 10.0.1.1	1
	Date / Time	Tue Nov 8 14:46:18 PST 2	2022	
	Next Scheduled Event	No Events Scheduled		
	Next Scheduled Action	No Actions Scheduled		
	Current Action	None		
	Multicast Mode	Transmitter Mode. Idle		
	Volume	Page Volume: 10 (0dB)		
	Relay Input Status	Disabled		
	ADMP Cloud Monitoring	Connected		

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* \rightarrow *Admin* tab after logging in the first time.

ALGO



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** \rightarrow **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.



tatus Basic Settings	Additional Features	Scheduler Adv	anced Settings	System	Logout		
IP Features Multica	st						
PSettings							
SIP							
This section allows the sadministrator or hosted acc	SIP server information & ount provider. After sav	account credential ng these settings,	s to be entered. T see the <u>Status</u> tab	his information to confirm s	on should be ob uccessful regist	ained from your teleph ation.	one system
SIP Domain (Proxy Serve	er)	10.0 (i)Du or 19	.0.100 efault port is 5060. 2.168.1.10:5080.	To specify a d	lifferent port, en	er PROXY:PORT, e.g. my	_proxy.com:5070,
Ring/Alert Mode			4onitor "Ring" ev None	ent on regist	ered SIP exten	sion	
Ring Extension							
Authentication ID							
Authentication Password					(P)		
Display Name (Optional)							
The device will detect ringing. It will not answe	inbound ring events or r the call on this exten	n this extension ar sion.	d play the alertir	ng tone (and	multicast if cor	figured) until the inbo	und call stops
Page Extension							
Authentication ID							
Authentication Password					P 🚯		
Display Name (Optional)							
iThe device will auto-a	nswer any inbound cal	received on this e	extension and pro	ovide a voice	paging path (a	nd multicast if configu	red).
							A 0.

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* \rightarrow *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* \rightarrow *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

Status Basic Settings A	dditional Features	Scheduler	Advanced Settings	System	Logout							
SIP Features Multicast												
Features												
Inbound Ring Settings												
These settings apply to even and set the appropriate volume	nts triggered by the Ri e level.	ing Extension	(s) & Emergency Aler	ts sections. The	Play/Loop/Stop	buttons can also be	used to test the device					
Ring/Alert Tone			warble2-med.wav		V Play Loop	Stop						
Ring/Alert Volume		-	10		Apply							
Ring Limit		[No limit 1 ring = 6 seconds.		•							
Inbound Page Settings												
Page Volume		((10 When in Receiver moulticast.	ode, note that th	✓ Apply is is the default vertex	olume control for all	audio received via					
Page Mode		(h Tr	•One-way OTwo)"Delayed" mode stor ung-up. This can help wo-way paging.	way ODelaye res the page aud avoid feedback.	d o temporarily, and Note: The Opus to	d then broadcasts it ransmitter codec is n	after the call is lot supported with					
Page Timeout		(5 minutes (i) Maximum page timeout in Delayed mode is 5 minutes.									
Page Tone		a fo	<default> Use only Default, or the end in order to gor several seconds at the seconds accords accords at the seconds accords accords</default>	custom uploaded enerate ring "cad he start of a pag	✓ d file. The other pi dence" of 6 second e.	re-installed tone files ds. This silence will b	all contain silence block the voice path					
G.722 Support		(Enabled Obisation Disation Obisation Description Obisation Disation Obisation Dis	eled d during SIP neg	otiation only. Mult	ticast codec is config	ured separately.					
Passcode Protected Page Ext	tensions	(P # a	OEnabled ODisat Set all page extension revent unintentional p sign before the page ction.	oled ons to require the ages. When pror can be accepted	e caller to enter a npted, the caller r . The passcode pr	passcode. Setting a nust enter the passc ompt will be played	passcode helps ode followed by the before any other					
DTMF Detection Type			OAuto ORTP Tele	phony Event (R	FC 4733) ORT	P In-band OSIP 1	NFO					
Audio												
Ambient Noise Compensatio	n	(s	OEnabled ODisab Automatically adjust tart of each call.	lled : speaker level in	response to ambi	ent noise level detec	ted prior to the					
Automatic Gain Control (AG	C)	(v	Enabled Obisat Automatically maxin olume more consisten	lled nize level of voice t.	e received from ca	lling phone in order	to make page					
'Line Out' Analog Output Lev	/el	Ti fe	+4dBu 10k (1.23 Vrr This setting controls o achieve this maximu eature (optional) to ind	ns) the maximum vo im level, also set crease the level r	Ditage level availa the volume contr eceived from the	ble on the 'Line Out' ol to level 10, and er far-end phone when	analog audio port. nable the AGC paging.					
							Save					
							↓ cave					

Figure 14: Basic Settings \rightarrow Features



Inbound Ring Settings

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



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

Ring/Alert Volume

Note

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)
- OdBV 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* \rightarrow *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)

Status Basic Settings	Additional Features Scheduler Advanced Settings System Logout
SIP Features Multica	st
Aulticast Settings	
Multicast Mode	
Multicast Mode	○None ●Transmitter (Sender) ○Receiver (Listener) ④Multicast Zone Definitions can be found in "Advanced Settings > <u>Advanced Multicast</u> ".
Multicast Type	 Regular (RTP) Polycom Group Page Polycom Push-to-Talk Regular RTP + Polycom Group Page Regular RTP + Polycom Push-to-Talk Regular RTP + Polycom Push-to-Talk Regular mode uses RTP audio packets compatible with all Algo SIP endpoints, and most multicast-enabled phones.
Number of Zones	Basic Zones Only OBasic and Expanded Zones
Transmitter (Sender	Zone Settings
Zone Selection Mode	OTMF Selectable Zone Osingle Zone For additional capabilities allowing unique SIP extensions per zone, see "Additional Features > More Page Extensions ".
Transmitter Single Zone	Priority Call (I) If "DTMF Selectable Zone" is selected above, then this single zone setting will not apply to Paging (since the zone can now be dynamically selected per call using DTMF), but it will still apply to the Ring Extension and Relay triggered events, including the analog audio input.
Speaker Playback Zones	 Priority Call Call Music Zone 1 Zone 2 Zone 3 Zone 4 Zone 5 Zone 6 Allows Multicast Transmitter device to play audio for selected zones only. This is useful if using DTMF Selectable Zone mode (or <u>More Page Extensions</u> per zone) and wishing to make the Transmitter a member of only certain zones.
DTMF Settings	
Zone Selection Tone	<default> V</default>
Two Digit Selection	OEnabled OEnabled If enabled, all DTMF Selectable Zones will require two digits. As a result, Basic Zones must be prefixed with "0" (ie. 01, 02, etc) and Expanded Zones no longer need to be prefixed with "*".
	√ Sav

Figure 15: Multicast transmitter mode settings



Note

See Advanced Settings \rightarrow 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 \rightarrow 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 \rightarrow 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* \rightarrow *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 \rightarrow 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* \rightarrow *File Manager* in the Tones folder. Each zone may use a different tone. This can be configured in *Advanced Settings* \rightarrow *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)

Status Basic Settings Additiona	l Features Scheduler Advanced Settings System Logout
SIP Features Multicast	
Multicast Settings	
Multicast Mode	
Multicast Mode	ONone Orransmitter (Sender) Receiver (Listener) Multicast Zone Definitions can be found in "Advanced Settings > Advanced Multicast".
Multicast Type	 Regular (RTP) Polycom Group Page Polycom Push-to-Talk Regular mode uses RTP audio packets compatible with all Algo SIP endpoints, and most multicast-enabled phones.
Number of Zones	Basic Zones Only Basic and Expanded Zones
Receiver (Listener) Zone Sett	ings
Basic Receiver Zones	✓Priority Call ✓All Call ✓Music ✓Zone 1 □Zone 2 □Zone 3 □Zone 4 □Zone 5 □Zone 6 ④A multicast to the Priority Call zone will override all other events on the device, except for a direct call to a Priority Page Extension in the More Page Extensions tab.
	✓ Save

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* \rightarrow *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.



Status Basic Settings	Additional Features Scheduler Advanced Settings System Logout
IP Features Multica	st
ulticast Settings	
Multicast Mode	
Multicast Mode	○None ○Transmitter (Sender) ●Receiver (Listener) ④Multicast Zone Definitions can be found in "Advanced Settings > <u>Advanced Multicast</u> ".
Multicast Type	Regular (RTP) Polycom Group Page OPolycom Push-to-Talk Regular mode uses RTP audio packets compatible with all Algo SIP endpoints, and most multicast-enabled phones.
Polycom Group Pagi Polycom Zone	g/Push-to-Talk 224.0.1.116:5001 (i) Enter the same Multicast IP Address & Port number as configured on the Polycom phones.
Polycom Receiver Chann	Is Image: Group 1 Group 2 Group 3 Group 4 Group 5 Group 6 Group 7 Group 8 Group 9 Group 10 Group 11 Group 12 Group 13 Group 14 Group 15 Group 16 Group 17 Group 18 Group 19 Group 20 Group 21 Group 22 Group 23 Group 24 Group 25 Select All Clear All (i) A multicast to Groups 24 or 25 will override all other events on the device, except for a direct call to a Priority Page Extension in the More Page Extensions tab.
	∢ Sa

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 \rightarrow 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 \rightarrow 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.

	_	stungs			Scheduler	Advanced Settings	System		Logout					
nput/Ou	utput	Emerge	ency Alerts	More Page	e Extensions	More Ring Extensions		-						
put/Ou	utput													
Genera	1					~								
Relay Input Mode						Disabled Relay Normally Open Relay Normally Open with Supervision (e.g. Algo 1203 Call Switch) Relay Normally Closed Relay Normally Closed with Supervision Mute Switch Mute Switch with Supervision Algo 1202 Call Button Algo 1204 Volume Control Switch Algo 1204 Volume Control Switch with Supervision Algo 1205 Audio Interface Switch Algo 1205 Audio Interface Switch with Supervision Algo 2507 Ring Detector								
Audio S	Stream	ing												
Audio Al	lways O	n			(C S	OEnabled ODisable PAudio Always On" will configured. Input port and section. "Scheduled" mod	d OScheo play sound d volume ca e will enable	duled on the n be c e strea	e Line Out onfigured ming at th	and Aux Ou below in the e times set	ut ports as e "Audio Ir t in the sch	well as m nput Settin neduler tab	ulticast if gs"	
Action \	When	Input	Triggered											
Action						Play Tone Make Two-Way SIP Make SIP Call with	Voice Call							
					(r	Stream Audio Play Tone" and "Stream multicast if configured.	m Audio" wi	ill play	sound on	the Line Ou	ut and Aux	Out ports	as well as	
Tone/Pre	e-record	led Ann	ouncement		(,	Stream Audio Stream Audio Play Tone" and "Strea multicast if configured. chime.wav	m Audio" wi	ill play	sound on	the Line Ou	ut and Aux	Out ports	as well as	
Tone/Pre Tone Du	e-record	led Ann	ouncement		(r [Stream Audio Transmission Play Tone" and "Streamulticast if configured. chime.wav Play Once OPlay N	m Audio" wi	ill play	sound on ay Until C	the Line Ou ompletion	ut and Aux	Out ports	as well as	
Tone/Pre	e-record	ded Ann	Duncement		(r	Stream Audio Stream Audio Play Tone" and "Stream multicast if configured. chime.wav Play Once OPlay M	m Audio" wi While Held	ill play	sound on ay Until C	the Line Ou	ut and Aux	Out ports	as well as	
Tone/Pre Tone Du Action 1 Wiring F	e-record uration When Fault Su	ded Anno Tampe pervision	r Detecter n Mode	d	(r [Orteam Audio Stream Audio Tran Audio Play Tone" and "Stream multicast if configured. chime.wav Play Once Play V Detect Open Circuit Opetect Both Open Ci Open Circuit detection with The nominal source voltage	While Held Fault Only Circuit & Sf will trigger wh ge on the Re	OPIa OPIa when the elay In	sound on ay Until C ircuit Fau the curren current d put circuit	the Line Ou completion ts : draw is <br raw is >36r is 13V, with	ut and Aux 4mA. mA. h a 40mA /	Out ports	as well as	
Tone/Pre Tone Du Action 1 Wiring F	e-record uration When Fault Su	ded Anno Tampe pervision	r Detecter	4		Stream Audio Stream Audio Stream Audio Play Tone* and "Strea multicast if configured. chime.wav Play Once Play N Detect Open Circuit Detect Both Open C Open Circuit detection will The nominal source voltag Play Tone Make Two-Way SIP Make SIP Call with * Play Tone* and "Strea multicast if configured. N ff the fault is resolved wit	While Held While Held Fault Only Circuit & Sf will trigger Il trigger wh ge on the Re Voice Call Tone m Audio" wi be that this hin 5 secon	OPI2	sound on ay Until C ircuit Fau the curren current d put circuit sound on will occur s action wi	the Line Ou ompletion ts : draw is < raw is >36r is 13V, with the Line Ou 5 seconds Il not occur	4mA. mA. h a 40mA i ut and Aux after a wi	Out ports	as well as it. as well as s detected.	
Tone/Pre Tone Du Action 1 Wiring F Action	e-record uration When Fault Su	ded Anno Tampe pervision	r Detecter n Mode	4		Otream Audio Stream Audio Stream Audio Play Tone" and "Stream multicast if configured. chime.wav OPlay Once OPlay M Open Circuit Open Circuit detection Short Circuit detection will The nominal source voltag OPlay Tone Make Two-Way SIP Make TP Call with Play Tone" and "Strea multicast if configured. N if the fault is resolved wit buzzer.wav	While Held While Held Fault Only Circuit & Sf will trigger I trigger wh ge on the Re Voice Call Tone m Audio" wi te that this hin 5 secon	Ill play	sound on ay Until C ircuit Fau the current current d put circuit sound on will occur s action wi	the Line Ou ompletion ts : draw is <br raw is >36r is 13V, with the Line Ou 5 seconds II not occur	4mA. nA. h a 40mA i ut and Aux after a wi	Out ports	as well as it. as well as s detected.	
Tone/Pre Tone Du Action 1 Wiring F Action Tone/Pre Tone Du	e-record When Fault Su	ded Anno Tampe pervision	n Mode	1		Stream Audio Stream Audio Stream Audio Stream Audio Play Tone* and "Stream multicast if configured. chime.wav Play Once Play V Open Circuit Open Circuit detection will Common and the term Short Circuit detection will The nominal source voltag Play Tone Make Two-Way SIP Make SIP Call with P'Play Tone* and "Stream multicast if configured. Not the fault is resolved wit buzzer.wav Play Once Play V	While Held While Held Crouit & S Will trigger I trigger wh ge on the Re Voice Call Tone m Audio" wi de that this hin 5 secon While Held	Ill play	sound on ay Until C ircuit Fau the curren current d put circuit sound on a will occur s action w	the Line Ou ompletion ts : draw is >36r is 13V, with the Line Ou 5 seconds II not occur ompletion	4mA. nA. h a 40mA i after a wi	Out ports	as well as it. as well as s detected.	
Tone/Pre Tone Du Action 1 Wiring F Action Tone/Pre Tone Du	e-record When Fault Su e-record uration	ded Anne Tampe pervision ded Anne	n Mode	4	(r (S T (r I I I	Stream Audio Stream Audio Stream Audio Stream Audio Play Tone* and "Streamulticast if configured. Chime.wav Play Once Play N Detect Doen Circuit Detect Both Open C Open Circuit detection will The nominal source voltage Play Tone Make Two-Way SIP Make SIP Call with *Play Tone* and "Streamulticast if configured. N If the fault is resolved wit buzzer.wav Play Once Play N	While Held While Held Fault Only Circuit & SF will trigger Il trigger wh ge on the Re Voice Call Tone m Audio" wild the that this hin 5 second While Held	OPIz	sound on ay Until C ircuit Fau the curren current d put circuit sound on will occur s action wi ay Until C	the Line Ou ompletion ts : draw is < aw is >36r is 13V, with the Line Ou 5 seconds Il not occur	4mA. mA. h a 40mA i ut and Aux after a wi	Out ports	as well as it. as well as s detected.	
Tone/Pre Tone Du Action N Wiring F Action Tone/Pre Tone Du	e-record When Fault Su e-record uration	ded Anno Tampe pervision ded Anno st Setti	n Mode	1		Stream Audio Stream Audio Stream Audio Stream Audio Play Tone" and "Stream multicast if configured. chime.wav Play Once Play M Detect Open Circuit Detect Both Open C Open Circuit detection with The nominal source voltag Play Tone Make SIP Call with Play Tone" and "Stream multicast if configured. N ff the fault is resolved wit buzzer.wav Play Once Play M	While Held Fault Only Fault Only Fault Only Frouit & SF will trigger wh ge on the Re Voice Call Tone m Audio" wi tote that this hin 5 second While Held	Pla Pla	sound on ay Until C ircuit Fau the curren current d put circuit sound on a will occur s action wi	the Line Ou ompletion ts draw is <a aw is >36r is 13V, with the Line Ou 5 seconds II not occur ompletion</a 	4mA. nA. h a 40mA i ut and Aux after a wi	Out ports	as well as it. as well as s detected.	
Tone/Pre Tone Du Action 1 Wiring F Action Tone/Pre Tone Du Use Sep	e-record when Fault Su e-record uration ulticas	ded Anno Tampe pervision ded Anno st Setti	n Mode	1		Stream Audio Stream Audio Stream Audio Stream Audio Play Tone" and "Stream multicast if configured. chime.wav Play Tone" and "Stream Play Once Play V Play Tone Make SIP Call with Play Tone Audio Stream Multicast if configured. N. If the fault is resolved with Play Once Play V Play Once Play V 	While Held While Held Fault Only Circuit & ST Will trigger I trigger wh ge on the Re Voice Call Tone m Audio" wi to that this hin 5 secon While Held d t to be playe	ill play	sound on ay Until C ircuit Fau the current d put circuit sound on a will occur s action w ay Until C multicast o	the Line Ou ompletion ts : draw is >36r is 13V, with the Line Ou 5 seconds II not occur ompletion	4mA. nA. h a 40mA i after a wi c	Out ports	as well as it. as well as s detected. as a	
Tone/Pre Tone Du Action N Wiring F Action Tone/Pre Tone Du Use Sep Output	e-record When Fault Su e-record uration bulticas	ded Anno Tampe pervision ded Anno st Setti	Duncement r Detecter h Mode buncement ngs			Stream Audio Stream Audio Stream Audio Stream Audio Play Tone* and *Strea multicast if configured. Chime.wav Play Once Play N Detect Both Open C Open Circuit detection will The nominal source voltage Play Tone Make TWO-Way SIP Make SIP Call with *Play Tone Play Tone Make SIP Call with *Play Tone Play Play	While Held While Held Fault Only Circuit & SF Will trigger I trigger wh ge on the Re Voice Call Tone MAUdio" wi to that this hin 5 secon While Held d t to be playe	III play	sound on ay Until C ircuit Fau the curren current d put circuit sound on will occur s action wi ay Until C multicast o	the Line Ou ompletion : draw is < aw is >36r is 13V, with the Line Ou 5 seconds Il not occur ompletion	4mA. mA. mA a 40mA a ut and Aux after a wi device is co	Out ports	as well as it. as well as s detected. IS a	

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* \rightarrow *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 \rightarrow 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 preconfigured 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 prerecorded 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* \rightarrow *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* \rightarrow *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

Status	Bi	asic S	Settings	Additio	nal Feature	s Scheduler	Advanced Settings	System		Logout		
Input/0	Outpu	ut	Emerge	ncy Alerts	More Pag	ge Extensions	More Ring Extensions		_	_	_	
Emerg	imergency Alerts											
This : announc files can	section cerment be e	on all nt (or asily	lows pre r a pre-d uploade	-recorded a lefined time d to create	announceme eout is reach e custom ann	ents to be triggened). This can be nouncements.	red & latched by callir e useful for emergenc	ng an exter y notificatio	nsion an ons (e.g	id hangir 9. "Evacu	ng up. The ar uation Alert")	nnouncement will continue to play until a different "Cancel" extension is called to clear the), allowing staff to quickly dial a pre-configured number and then exit the building. Audio
• Up to	5 10 1	exten	isions ca	n be regist	tered allowin	g up to 10 airre	rent announcements.	A single "C	ancer	extensio	on also needs	s to be registered; calling this number will cancel the currently active announcement.
Note: Sotti	: Son	ne SI	P phone	systems n	nay not supp	port this feature	if they limit the numb	per of exter	nsions t	hat can	be registered	d on a single device.
Anno	ounce	men	t Duratio	n					Once 🤇	Play Ur	ntil Cancelled	
Maxi	mum	Ann	ounceme	ent Time				10 minut	tes		~	- -
Anno	ounce	men	t Selectio	on Mode				Opirec	t Extens	sions 🧿	DTMF Select	table
								(i)Use "Di extension	irect Extended that acc	ensions" epts DTM	to register a se IF input to sele	eparate extension for each announcement. Use "DTMF Selectable" to register a single ect which announcement to play.
Passe	code	Prote	ected An	nounceme	nt Extension	s		OEnab	led 🔍	Disabled		
DTM	F Se	lect	ion									
Exter	nsion											
Auth	entic	ation	ID									
Auth	entic	ation	Passwo	rd							()	0
Displ	lay N	ame	(Optiona	al)								
Prom	npt To	one						<default< td=""><td>t></td><td></td><td>~</td><td>2</td></default<>	t>		~	2
Call-	to-C	anc	el									
Call-	to-Ca	ancel	Selectio	n Mode				 Direc If using 	t Extens) "DTMF	sion Ot 0", dial ti	DTMF 0 he main DTMF	Selection extension and select 0 to cancel the announcement.
Exter	nsion	1										
Auth	entic	ation	ID									
Auth	entic	ation	Passwo	rd							9	2 💀
Displ	lay N	ame	(Optiona	i)								
Confi	irmat	tion T	one					<none></none>			~	2
Anno	ounc	eme	onts									
Anno	ounce	men	1					OEnab	led 🔍	Disabled		
Anno	ounce	men	1 2					OEnab	led 🔍	Disabled		
Anno	ounce	men	t 3					Enab	led 🔍	Disabled		
Anno	ounce	men	t 4					OEnab	led 🔍	Disabled		
Anno	ounce	men	t 5					OEnab	led 🔍	Disabled		
Anna	ounce	men	t 6					OEnabl	led 🔍	Disabled		
Anco	unce	mer	7					OEash		Disabled		
Anno	- and e	mar						OFactor		Neatled		L
Anno	unce	mor								Visabled		L
Anno	unce	men	. 9					∪Enab	180 🔍	vsabled		
Anno	ounce	men	t 10					OEnabl	led 🔍	Disabled use 0 to	select this anr	nouncement.
												Save

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

Status Basic Settings Additional Features Scheduler	Advanced Settings System Logout									
Input/Output Emergency Alerts More Page Extensions	More Ring Extensions									
More Page Extensions										
his section allows dedicated extensions to be registered for each paging zone. This provides an alternative to the "DTMF Selectable Zone" option, thus llowing any zone to be called directly without the need to enter DTMF. Depending on the features available on your SIP phone system, this can provide enefits in allowing speed-dial keys to be programmed on user phones for paging a particular zone more easily, or dialing restrictions could potentially be sed to allow only selected phones to access certain zones. This feature requires several SIP extensions to be registered with the SIP phone system. The 8301 will auto-answer any inbound calls received on these numbers and provide a voice paging path and multicast if configured. Note that only a ingle call can be active at a time.										
Note: Some SIP phone systems may not support this feature	e if they limit the number of extensions that can be registered on a single device.									
(i) Multicast Zone Definitions can be found in "Advanced Setting	gs > <u>Advanced Multicast</u> ".									
Basic Extensions										
Priority Call Page Extension	 Enabled Disabled A call to the Priority Extension will override all other events on the device. 									
Extension										
Authentication ID										
Authentication Password										
Display Name (Optional)										
All Call Page Extension	OEnabled Disabled									
Zone 1 Page Extension	OEnabled OEnabled									
Zone 2 Page Extension	OEnabled OEnabled									
Zone 3 Page Extension	OEnabled OEnabled									
Zone 4 Page Extension	OEnabled OEnabled									
Zone 5 Page Extension	OEnabled OEnabled									
Zone 6 Page Extension	OEnabled OEnabled									
Music Page Extension	OEnabled OEnabled									
	✓ Save									

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

Status B	asic Settings	Additional Features	Scheduler	Advanced S	Settings	System		Logout				
Input/Outpu	ut Emergeno	y Alerts More Page	Extensions	More Ring Ex	tensions				_	_	_	
More Ring	g Extensior	ns										
This section the selected for estimation of the section of the	on allows addit each line to alle nust be configu	tional extensions to be ow them to be easily o red on your SIP phon	registered for istinguished - 1 e system of co	the purpose for example a urse in order	of providir "Sales" li to trigger	ig loud rir ne could l it to send	nging al have a c calls to	erts for i different o these d	nore than one l ring tone from ifferent number	line. Unique rir a personal line rs.	ig tones can be 2. Appropriate	
D The 8301 his mode.	The 8301 will detect inbound ring events on these numbers and play the alerting tone until the inbound call stops ringing. It will not answer the calls in is mode.											
D Note: Sor	ne SIP phone :	systems may not supp	ort this feature	if they limit	the numbe	er of exte	nsions t	hat can	be registered o	n a single devi	ce.	
Ring Exte	nsion 2				Oisable	d						
Ring Exte	nsion 3				Oisable	d						
Ring Exte	nsion 4			OEnabled	Oisable	d						
Ring Exte	nsion 5				Oisable	d						
Ring Exte	nsion 6				Oisable	d						
Ring Exte	nsion 7			OEnabled	Oisable	d						
Ring Exte	nsion 8			OEnabled	Oisable	d						
Ring Exte	nsion 9			OEnabled	Olisable	d						
Ring Exte	nsion 10			OEnabled	Olisable	d						
Rule-bas	ed Ring Tor	18										
Allows the or ex	device to play a tension that ma	custom ring tone base atches the rule.	d on the identit	y of the caller.	When ena	bled, the	device w	vill play t	he selected ring	tone for callers	with a display	
#1 Custo	m Tone			OEnabled	Olisable	d						
#2 Custo	m Tone			OEnabled	Oisable	d						
#3 Custo	m Tone			OEnabled	Olisable	d						
#4 Custo	m Tone			OEnabled	Olisable	d						
											✓ Save	

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.

Stat	us Basic Settings A	dditional Features Sch	Advanced Set	tings System	Logout			
Cale	endar Schedules Da	ata						
						Wed 16 Nov, 2022	11:40:47 (System T	ïme)
Тс	oday < 🗲	November 2	2022	Friday	~	Single	ng	
	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	
			1	2	3	4	5	
	6	7	8	9	10	11 Regular Weekday Friday	12	
	13	14 Regular Weekday	15 Regular Weekday	16 Regular Weekday	17 Regular Weekday	18 Friday	19	
	20	21 Regular Weekday	22 Regular Weekday	23 Regular Weekday	24 Regular Weekday	25 Friday	26	
	27	28 Regular Weekday	29 Regular Weekday	30 Regular Weekday				
Rec	urrence: O Daily	• • Weekly OM	onthly 🗆 S 🗆 M	□ T □ W □ T	🗹 F 🗆 S Every	1 weeks end o	date: 2022-12-16 Save	

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

Status	Basic Settings	Addition	al Features	Scheduler	Advanced Setti	ngs System	L	_ogout				
Calenda	r Schedules	Data										
									Wed 1	16 Nov, 2022 1	l1:41:24 (S	ystem Time)
Colour	Schedule Name			Current Sch	edule: Regula	r Weekday						
	Regular Weeko	da 🚺	×	Event Descript	ion		Time	1	Audio		Page Zone	
	Friday			Lunch Bell			12:30	:00	bell-na.wav	~	1 ~	× 🛍
	Thuay		کنی ک	Action		Start 1	End	1				
						-	This sche	edule cu	rrently has no actions			
Cre	ate Schedule			Add	Event	Add /	Action					Save

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

Testore							
1 Convert							
(i) Restore scheduler data with a backup file from the previous version of the scheduler.							
Na Clear							

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

Status	Basic Settings	Additio	nal Features	Scheduler	Advanced	Settings	Syste	em	Logout			
Network	k Admin	Users Tir	me Provisi	ioning Adv	anced Audio	Advanced	SIP	Advand	ced Multica	st		
letwor	k Settings											
Comm	on											
Interne	et Protocol				IP	v4 only			~			
DNS S	ervers								*			
					(i) (Jse space, co	omma,	or semic	olon to sep	arate multiple DNS servers, e.g. 192.168.1.10, 192.168.1.11		
IPv4	lathad				6	Ch-H-						
IPV4 M	ddrose/Networ	ale.					нср					
IPV4 A	doress/ Netmas	5K			(i),	Address (dot	delimit	ted)/Netr	mask (CIDR), e.g. 192.168.1.23/24		
IPv4 G	ateway											
802.1	Q Virtual LA	N										
VLAN M	Mode				C	None OM	anual	OAuto)			
VLAN I	۱D				0							
					(1)	/alue range:	0 to 40	094				
VLAN F	Priority				0 (i))	/alue range:	0 to 7					
L				*****								
802.1	X Port-based	d Networ	k Access C	ontrol								
802.1X	(Authenticatio	n			C	Enabled	Disab	oled				
Auther	ntication Mode				EA	P-PEAP/M	SCHA	Pv2	~			
					(i)]	(i) In EAP-TLS mode, if the authentication server requires devices to be authenticated, a PEM file containing both a device certificate and a private key can be installed on the Algo device. Use the "System > File						
					Mar	Manager" tab to upload a Base64 encoded X.509 certificate file renamed to 'client8021x.pem' in the 'certs' folder						
	10				TOIO	er.						
Anonyi	mous ID											
ID												
Passwo	ord								٩	<u>62</u>		
Validat	e Server Certif	ficate				Enabled	Disab	oled	erver again	st common authorities. To validate against additional certificates.		
					use	use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt						
					TOPT	nat to the 'ce	erts/tru	isted fold	uer.			
Differe	entiated Ser	vices										
SIP (6	-bit DSCP value	e)			0							
		-			(i)	/alid values r	ange fr	rom 0 to	63	•		
RTP (6	-bit DSCP valu	e)			0	tellat en t			()			
DTOD (c his peop				10	valid values r	ange fr	rom 0 to	63			
RTCP (6-bit DSCP val	ue)			0 (i)	/alid values r	ange fr	rom 0 to	63			
L												
DNS												
DNS C	aching Mode					Disabled	SIP		14 6 P			
					(i)) of a	In "SIP" mod II DNS querie	e, only es will t	the resu be cache	uts of DNS (d.	queries for SIP requests will be cached. In "All" mode, the results		
L												
										✓ Save		

Figure 25: Network settings



<u>Common</u>

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* \rightarrow *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.

ALGO

6.7.2 Admin

Interverk Admin Users Time Provisioning Advanced Au Intra Settings Admin Password Image: Setting Seting Seting Setting Setting Seting Set ing Set ing Set ing Set ing	iii Advanced SIP Advanced Multicast Advanced SIP Advanced Nulticast Advanced SIP Advanced Multicast Advanced SIP Advanced SIP Advanced Multicast Advanced SIP Advanced Multicast Advanced SIP A
dmin Settings Admin Password Old Password Password Confirmation General Device Name (Hostname) Introduction Section on Status Page Show Status Section on Status Page Web Interface Session Timeout Play Tone at Startup Ug Level Log Settings Log Settings Log Setver Management Web Interface Protocol Simple Network Management Protocol SimP Community String SimP Support RESTful API System Integrity System Integrity System Integrity	adapter-\$mac\$ adapter-\$mac\$ adapter-\$mac\$ adapter-\$mac\$ orr orr orr orr abled ©Disabled abled ©Disabled abled ©Disabled abled ©Disabled abled ©Disabled
Admin Password Old Password Old Password Confirmation General Device Name (Hostname) Introduction Section on Status Page Option Show Status Section on Status Page Option Display Switch Port ID on Status Page Web Interface Session Timeout Play Tone at Startup Cog Settings Log Level Log Method Log Server Management Web Interface Protocol Force Strong Password Allow Secure SIP Passwords Simple Network Management Protocol Simple Support RESTful API RESTful API System Integrity System Integrity Checking	adapter-\$mac\$ ad
Old Password Old Password Old Password Confirmation General Device Name (Hostname) Device Name (Hostname) Display Switch Port ID on Status Page (Port ID on Status Page) (P	adapter-\$mac5 a
Password Confirmation Confirmation General Device Name (Hostname) Introduction Section on Status Page Op Show Status Section on Status Page @ Op Display Switch Port ID on Status Page Web Interface Session Timeout Play Tone at Startup Play Tone at Startup Log Settings Log Level Log Method Log Server Management Web Interface Protocol Force Strong Passwords Force Strong Passwords Simple Network Management Protocol SIMP Support SIMP Support RESTful API RESTful API System Integrity System Integrity Checking Confirmation	adapter-\$macS
Confirmation Confirmation Confirmation Confirmation General Device Name (Hostname) Introduction Section on Status Page OD Show Status Section on Status Page OD Display Switch Port ID on Status Page Web Interface Session Timeout Play Tone at Startup Cog Settings Log Level Log Method Log Server CManagement Web Interface Protocol Force Strong Passwords Simple Network Management Protocol Simple Network Management Protocol Simple Network Management Protocol Simple Network Management Protocol Simple Community String Simple Network Management Protocol Simple Support RESTful API RESTful API System Integrity System Integrity Checking Community String Community Community String Community Co	adapter-SmacS a
Contrination Centrimation Centr	adapter-\$mac\$ adapter-\$mac\$ orr orr orr orr bisabled or f bisabled th HTTP and HTTPS OHTPS Only abled © Disabled bisabled bisabl
General Device Name (Hostname) pagin Introduction Section on Status Page ©O Show Status Section on Status Page when Logged Out ©O Display Switch Port ID on Status Page OO Display Switch Port ID on Status Page OO Web Interface Session Timeout I hoo Play Tone at Startup @Page Cog Settings Cer Log Level Cer Log Method Cer Management Web Interface Protocol Web Interface Protocol @Bac Simple Network Management Protocol @Er System Integrity String @If if System Integrity @Er System Integrity Cer <t< td=""><td>adapter-\$mac\$ Off Off Off Off Off Off Off Off Off Of</td></t<>	adapter-\$mac\$ Off Off Off Off Off Off Off Off Off Of
Device Name (Hostname) Pagin Introduction Section on Status Page O O Show Status Section on Status Page O O Display Switch Port ID on Status Page O O U Display Switch Port ID on Status Page O O U Display Switch Port ID on Status Page O O U Display Switch Port ID on Status Page O O U Display Switch Port ID on Status Page O O U Display Switch Port ID on Status Page O O U Display Switch Port ID on Status Page O O U Display Switch Port ID on Status Page O O U Display Switch Port ID on Status Page O O U Display Switch Port ID on Status Page O O U Display Switch Port ID on Status Page O O U Display Support C D SNMP Community String D SNMP Community String System Integrity O E C D System Integrity Checking O D S D D D D D D D D D D D D D D D D	adapter-\$mac\$ Orf Orf @orf aires the device to be connected to a switch that supports LLDP or CDP. rematcally log out web interface after period of inactivity. abled @Disabled ne can be played at starup to confirm that the device has booted. This can be useful string or configure a device, but might not be desirable if the device is connected to an il amplifier and paging system. or (Lowest) Onotice ("Event") @Info ("SIP") ODebug (Highest) cal Onetwork @Both th HTTP and HTTPS OHIY abled @Disabled renabling this option, it is recommended to re-enter SIP passwords and their onding realm to store the passwords securely. abled Obisabled
Introduction Section on Status Page Or Show Status Section on Status Page when Logged Out Or Display Switch Port ID on Status Page Or Web Interface Session Timeout Interface Session Timeout Interface Session Timeout Or Or Or Or Or Or Or Or Or Or Or Or Or O	Orf Orf @orf aires the device to be connected to a switch that supports LLDP or CDP. r matcally log out web interface after period of inactivity. abled ●Disabled ne can be played at startup to confirm that the device has booted. This can be useful string or configuring a device, but might not be desirable if the device is connected to an il amplifier and paging system. or (Lowest) ●Notice ("Event") ●Info ("SIP") ●Debug (Highest) cal ●Network ●Both th HTTP and HTTPS ●HTTPS Only abled ●Disabled renabling this option, it is recommended to re-enter SIP passwords and their onding realm to store the passwords securely. abled ●Disabled
Show Status Section on Status Page when Logged Out Display Switch Port ID on Status Page Web Interface Session Timeout Play Tone at Startup Cog Settings Log Level Log Method Log Server Management Web Interface Protocol Simple Network Management Protocol Simple	Orf irres the device to be connected to a switch that supports LLDP or CDP. irres the device to be connected to a switch that supports LLDP or CDP. irrestriction irrestriction abled If Disabled irrestriction or (Lowest) Notice ("Event") If Info ("SIP") Obebug (Highest) cal Network Bold Obsabled enabling this option, it is recommended to re-onter SIP passwords and their onding realm to store the passwords securely. abled Obsabled
Display Switch Port ID on Status Page Or @Req Web Interface Session Timeout I flou Play Tone at Startup OF @Data Log Log Settings Log Log Log I OF Log Method C C Log Method C C Log Server I Management Web Interface Protocol @Bc Force Strong Password OF Allow Secure SIP Passwords OF SIMP Support OF SNMP Community String OF SNMP Security OF API Support RESTful API OF System Integrity Checking OF System Integrity Checking OF Enabling OF OF Control Control Contr	Off irres the device to be connected to a switch that supports LLDP or CDP. irres the device to be connected to a switch that supports LLDP or CDP. irrestically log out web interface after period of inactivity. abled © Disabled ne can be played at startup to confirm that the device has booted. This can be useful susting or configure a device, but might not be desirable if the device is connected to an all amplifier and paging system. or (Lowest) Notice ("Event") ® Info ("SIP") Obebug (Highest) cal Network ® Both th HTTP and HTTPS OHIY abled ® Disabled renabling this option, it is recommended to re-enter SIP passwords and their onding realm to store the passwords securely. abled O Disabled
Web Interface Session Timeout I hou Play Tone at Startup Er Play Tone at Startup Er Log Settings Er Log Settings Er Log Level Er Log Method Log Settings Er Management Brock Web Interface Protocol Brock Force Strong Password Er Allow Secure SIP Passwords Er Simple Network Management Protocol ShMP Support SNMP Community String If If SNMP V3 Security Er API Support Er System Integrity Er System Integrity Checking Er	
Play Tone at Startup Play Tone at Startup Play Tone at Startup Play Tone at Startup Cog Settings Log Settings Log Level Log Method Log Server Management Web Interface Protocol Force Strong Password Allow Secure SIP Passwords Simple Network Management Protocol SIMP Support SIMP Support SIMP Security Free SIMP Security SIMP Security System Integrity System Integrity Checking Play Security Play	abled ©Disabled ne can be played at startup to confirm that the device has booted. This can be useful issting or configuring a device, but might not be desirable if the device is connected to an lamplifier and paging system. or (Lowest) Notice ("Event") @Info ("SIP") Obebug (Highest) cal Network @Both th HTTP and HTTPS OHTPS Only abled @Disabled renabling this option, it is recommended to re-enter SIP passwords and their onding realm to store the passwords securely. abled Obisabled
Log Settings Log Level CFr Log Method Log Server Management Web Interface Protocol BFR Force Strong Password EFr Allow Secure SIP Passwords Simple Network Management Protocol SIMP Support SIMP Support SIMP Security EFr API Support RESTful API Bassword System Integrity Checking EFr Emablin	or (Lowest) Notice ("Event") Info ("SIP") Debug (Highest) cal Network Both th HTTP and HTTPS OHTTPS Only abled Disabled renabling this option, it is recommended to re-enter SIP passwords and their onding realm to store the passwords securely. abled Disabled
Log Level Creatings Log Level Creatings Log Log Method Log Server Log Method Log Server Management Web Interface Protocol Broce Strong Password Creating Force Strong Passwords Creating Simple Network Management Protocol SNMP Support SNMP Community String SNMPV3 Security Creating SNMPV3 Security Creating SSTul API Creating System Integrity Checking Creating Crea	or (Lowest) Notice ("Event") Info ("SIP") Debug (Highest) cal Network Both th HTTP and HTTPS OHTTPS Only abled Disabled enabling this option, it is recommended to re-enter SIP passwords and their onding realm to store the passwords securely. abled Disabled
Log Levei OFF Log Method OL Log Server Management Web Interface Protocol Bassword OFF Force Strong Password OFF Allow Secure SIP Passwords OFF OFF SIMP Support OFF SIMP Support OFF SIMP Community String OFF SIMP Security OFF VPI Support RESTful API OFF RESTful API OFF System Integrity Checking OFF OFF	or (Lowest) Notice ("Event") ©Info ("SIP") Obebug (Highest) cal ONetwork @Both cal ONEtwork @Both cal ONETRIC ONLY cal Disabled cal Obsabled
Log Method Log Server	al Wetwork Both
Log Server Management Web Interface Protocol Force Strong Password Allow Secure SIP Passwords Simple Network Management Protocol SNMP Support SNMP Community String SNMPV3 Security FI Support RESTful API Estruit API System Integrity System Integrity Checking String	th HTTP and HTTPS OHTPS Only abled Disabled abled Disabled renabling this option, it is recommended to re-enter SIP passwords and their onding realm to store the passwords securely. abled Obisabled
Management Web Interface Protocol Force Strong Password Allow Secure SIP Passwords Simple Network Management Protocol SNMP Support SNMP Community String SNMP Community String SNMPV3 Security PET SNMPV3 Security EXTRA PI SSTful API @Er @Er System Integrity Checking @Er @The Security System Integrity Checking System Integrity C	th HTTP and HTTPS Only abled Disabled abled Disabled renabling this option, it is recommended to re-enter SIP passwords and their onding realm to store the passwords securely. abled Obisabled
Management Web Interface Protocol Force Strong Password Force Strong Passwords Allow Secure SIP Passwords Simple Network Management Protocol Simple Network Management Protocol SNMP Support SNMP Community String SNMPv3 Security API Support RESTful API @Sec System Integrity System Integrity Checking	th HTTP and HTTPS OHTPS Only abled Disabled abled Disabled enabling this option, it is recommended to re-enter SIP passwords and their onding realm to store the passwords securely. abled Obisabled
wee interface Protocol Bg Force Strong Password	th HTTP and HTTPS OHY abled Disabled abled Disabled enabling this option, it is recommended to re-enter SIP passwords and their onding realm to store the passwords securely. abled Disabled
Force Strong Password Er Force Strong Passwords Er Allow Secure SIP Passwords Er SIMP Enter Strong Passwords Er SIMP Support Er SIMP Community String Er SIMP Community String Er SIMP V3 Security Er SIMP Security Er SIMP Security Er SIMP Security Er SIMP Security Er Simple Network Management Protocol SIMP Security Er SIMP Security Er SIMP Security Er Simple Network Management Protocol SIMP Support Er SIMP Support Er S	abled Disabled abled Disabled enabling this option, it is recommended to re-enter SIP passwords and their onding realm to store the passwords securely. abled Disabled
Allow Secure SIP Passwords	abled [©] Disabled enabling this option, it is recommended to re-enter SIP passwords and their onding realm to store the passwords securely.
Simple Network Management Protocol SNMP Support SNMP Community String SNMPV3 Security PI Support RESTful API System Integrity System Integrity Checking	abled ODisabled
SNMP Support SNMP Support SNMP Community String SNMP Community String SNMPV3 Security CEr API Support RESTful API System Integrity System Integrity Checking	abled Obisabled
(a) Dow SNMP Community String (a) If it SNMPv3 Security (b) Fr API Support RESTful API System Integrity System Integrity Checking (c) Fr	
SNMP Community String Office SNMPv3 Security Office API Support RESTful API System Integrity System Integrity Checking	nload MIB file <u>here</u> .
SNMPV3 Security OEr API Support RESTful API OEr System Integrity System Integrity Checking OEr Enablia	t blank, the default string "public" will be used.
API Support RESTful API Best RESTful API Password System Integrity System Integrity Checking	abled Cisabled
API Support RESTful API RESTful API System Integrity System Integrity Checking	
RESTful API (e)Sec RESTful API Password System Integrity Checking System Integrity Checking Erablin	_
RESTful API Password System Integrity System Integrity Checking	abled Obisabled ire API for remote access & control via HTTP. Contact Algo Support for more information
System Integrity OFF System Integrity Checking OFF @Thin Enablin	©] 🗞
System Integrity Checking OEr @This Enable	
System integrity crecking (e)Thi Enablin Enablin	abled
results	Substance = Substance feature verifies installed system packages to ensure they have not been tampered with, g this feature may cause reboots and upgrades to take 30 seconds longer. Verification can be found on the Status page.
Syn-Apps	
iA-Announce Support he SA-Announce feature cannot be used when Multicast Transmitter r lone in "Basic Settings > <u>Multicast</u> ".	ode or Polycom mode is enabled. To enable SA-Announce mode, set Multicast Mode to
InformaCast	
InformaCast Support Er InformaCast Support	abled
ADMP Cloud Monitoring	
Enable ADMP Cloud Monitoring	abled ODisabled
Account ID Degra	70704444000044 447 0 070
Heartbeat Interval 30 se	a/9/91441f89281ba14/c0a8/fu
	a/9/91441189281ba14/c0a8/10 conds

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 reentered in *Basic Settings* \rightarrow *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 \rightarrow 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 <u>sales@algosolutions.com</u> 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 <u>sales@algosolutions.com</u> for assistance.

6.7.3 Users

Status Basic Settings Addition	al Features Scheduler Advanced	Settings System	Logout
Network Admin Users Tim	ne Provisioning Advanced Audio	Advanced SIP Advar	vanced Multicast
User Management			
Scheduler			
These settings enable a separate	e login account with limited access that al	lows the user to only me	modify the device scheduler
User Login	Enabled		
Username	Scheduler		
Password	••••		
I			
			√ Sav

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.



Lettorik Advances Advances Advances Advances Advances and Advances	tus Basic Settings Addi	tional Features Schedule	Advanced Settings	System Logout
me Settings General	CHOIR Admin Oscis	The Trovisioning Ad		
Seneral Timezone US/Pacific NTP Time Server 1 0.debian.pool.ntp.org NTP Time Server 2 1.debian.pool.ntp.org NTP Time Server 3 2.debian.pool.ntp.org NTP Time Server 4 3.debian.pool.ntp.org Supersede NTP provided by DHCP CEnabled ©Disabled •By default, if an NTP Server address is provided via DHCP Option 42, it will be used instee of the NTP servers listed above. Enable this option to ignore DHCP Option 42. Device Date/Time Mon Dec 12 09:34:33 2022 Manually Override Time 09:34:19 Manually Set Time () Manual time and date are intended for testing purpose only. Time will be lost upon power down if NTP server is reachable.	ne Settings			
Timezone US/Pacific NTP Time Server 1 0.debian.pool.ntp.org NTP Time Server 2 1.debian.pool.ntp.org NTP Time Server 3 2.debian.pool.ntp.org NTP Time Server 4 3.debian.pool.ntp.org Supersede NTP provided by DHCP OEnabled Obisabled Option 42, it will be used instee of the NTP servers listed above. Enable this option to ignore DHCP Option 42, it will be used instee of the NTP servers listed above. Enable this option to ignore DHCP Option 42. Device Date/Time Mon Dec 12 09:34:33 2022 Sync with browser Manually Override Time 09:34:19 Manually Set Time () Manual time and date are intended for testing purpose only. Time will be lost upon power down if NTP server is reachable. Nor perver is reachable.	eneral			
NTP Time Server 1 O.debian.pool.ntp.org NTP Time Server 2 1.debian.pool.ntp.org NTP Time Server 3 2.debian.pool.ntp.org NTP Time Server 4 3.debian.pool.ntp.org Supersede NTP provided by DHCP OEnabled Obisabled OP Supersede NTP provided by DHCP OEnabled Obisabled OP Supersede NTP provided by DHCP OEnabled Obisabled OP Supersede NTP provided by DHCP OP Sate of the NTP Server address is provided via DHCP Option 42, it will be used instead of the NTP Servers listed above. Enable this option to ignore DHCP Option 42. Device Date/Time Mon Dec 12 09:34:33 2022 Sync with browser Manually Override Time OP Sat:19 Manually Set Time Of Manual time and date are intended for testing purpose only. Time will be lost upon power down if NTP server is reachable.	limezone		US/Pacific	v
NTP Time Server 2 1.debian.pool.ntp.org NTP Time Server 3 2.debian.pool.ntp.org NTP Time Server 4 3.debian.pool.ntp.org Supersede NTP provided by DHCP OEnabled ©Disabled	ITP Time Server 1		0.debian.pool.ntp.org	
NTP Time Server 3 2.debian.pool.ntp.org NTP Time Server 4 3.debian.pool.ntp.org Supersede NTP provided by DHCP OEnabled @Disabled @By default, if an NTP Server address is provided via DHCP Option 42, it will be used instead of the NTP servers listed above. Enable this option to ignore DHCP Option 42. Device Date/Time Mon Dec 12 09:34:33 2022 Manually Override Time 09:34:19 Manually Coverride Time @Manual time and date are intended for testing purpose only. Time will be lost upon power down if NTP server is reachable.	ITP Time Server 2		1.debian.pool.ntp.org	
NTP Time Server 4 3.debian.pool.ntp.org Supersede NTP provided by DHCP OEnabled @Disabled @By default, if an NTP Server address is provided via DHCP Option 42, it will be used instered of the NTP servers listed above. Enable this option to ignore DHCP Option 42. Device Date/Time Mon Dec 12 09:34:33 2022 Manually Override Time 09:34:19 @Manual time and date are intended for testing purpose only. Time will be lost upon power down if NTP server is reachable.	NTP Time Server 3		2.debian.pool.ntp.org	
Supersede NTP provided by DHCP OEnabled @Disabled Image: Supersede NTP provided by DHCP Image: Supersede NTP server address is provided via DHCP Option 42, it will be used instead of the NTP servers listed above. Enable this option to ignore DHCP Option 42. Device Date/Time Mon Dec 12 09:34:33 2022 Manually Override Time Image: Op:34:19 Image: Image: Op:34:19 Image: Image: Op:34:19 Image: Image: Image: Op:34:19 Image: Image: Image: Op:34:19 Image: Image: Image: Image: Image: Op:34:19 Image: I	NTP Time Server 4		3.debian.pool.ntp.org	
Device Date/Time Mon Dec 12 09:34:33 2022 Sync with browser Manually Override Time 09:34:19 Manually Set Time (i) Manual time and date are intended for testing purpose only. Time will be lost upon power down if NTP server is reachable. Time will be lost upon power	Supersede NTP provided by D	нср	OEnabled ODisable (a) By default, if an NTP S of the NTP servers listed	ed Server address is provided via DHCP Option 42, it will be used instead above. Enable this option to ignore DHCP Option 42.
Manually Override Time (i) Manual time and date are intended for testing purpose only. Time will be lost upon power down if NTP server is reachable.	Device Date/Time		Mon Dec 12 09:34:33 2022	Sync with browser
	1anually Override Time		09:34:19 (i) Manual time and date down if NTP server is rea	Manually Set Time are intended for testing purpose only. Time will be lost upon power achable.
				V Sé

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

tatus Basic Settings Additional Feat	ures Scheduler Advanced Settings System Logout
letwork Admin Users Time Pr	ovisioning Advanced Audio Advanced SIP Advanced Multicast
en del en la a Cattle au	
ovisioning Settings	
Mode	
Provisioning Mode	Enabled Disabled
Settings	
Server Method	 Auto (DHCP Option 66/160/150) DHCP Option 66 only DHCP Option 160 only DHCP Option 150 only Static
	(i) Auto mode automatically checks all 3 DHCP options for an active provisioning server, in the order listed.
Static Server	
Download Method	OTFTP OFTP OHTTP OHTTPS
Validate Server Certificate	OEnabled Disabled OEnabled the server against common certificate authorities. To validate against additional certificates, use the "System > <u>File Manager</u> " tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder.
Auth User Name	
Auth Password	۰
Config Download Path	
Firmware Download Path	
Partial Provisioning	OEnabled OEnabled Isabled Isable for enhanced security if not using this feature.
Check-sync Behavior	Always Reboot Oconditional Reboot (a) If 'Conditional Reboot' is selected, the device will check with the provisioning server and only reboot if new config is found (unless 'reboot=true' is provided as a parameter in the check-sync event).
Sync Start Time	Schedule a time (HH:mm:ss) for the device to perform a sync according to the 'Check-sync Behavior' option above. Leave blank to disable the feature.
Sync End Time	If set, the device will sync at a random time in the window between Start Time and End Time. Setting an End Time earlier than Start Time indicates an overnight period. Leave blank to sync at Start Time exactly.
Sync Frequency	Obaily Selected Days Only
Weekdays	☑Monday ☑Tuesday ☑Wednesday ☑Thursday ☑Friday ☑Saturday ☑Sunday
	✓ S

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.

<u>Mode</u>

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 <u>http://myserver.com/config-path</u> 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

Status Basic Settings Additional Features	Scheduler Advanced Settings System Logout	
Network Admin Users Time Provision	g File Manager Advanced Audio Advanced SIP Advanced Multicast	
Advanced Audio Functions		
Functions		
Dynamic Range Compression (DRC)	 Enabled O bisabled Compress the dynamic range of page audio to increase loudness. 	
Dynamic Range Compression Gain	6 • Specify the amount of compression gain. More gain increases distortion.	
Jitter Buffer Range (milliseconds, $10 \sim 500$)	100 (i)Adds more buffering if necessary to correct for inconsistent delays on the network. Use of the lowest value generally is recommended.	ie
Generate In-Band DTMF Tones	 Enabled ODisabled Play DTMF tones during a SIP Call to allow interoperability with DTMF-controlled multi-zone amplifiers 	
Always Send RTP Media	• Enabled O Disabled	
Audio Filters		
Speaker Filter	None	
Speaker Noise Filter	 Enabled Oisabled Iggressive 8th order Elliptical Filter (fc = 145Hz) 	
Microphone Filter	None 🔽	
Microphone Noise Filter	○ Enabled ● Disabled (i)Aggressive 8th order Elliptical Filter (fc = 145Hz)	
	•	✔ Save

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

	ng Advanced Audio Advanced SIP Advanced Multicast
etwork Admin Users Time Provisionin	
vanced SIP Settings	
ieneral	
SIP Transportation	Auto
	 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 > Eile Manager" tab to upload a certificate file renamed to 'sinclinet pem' in the 'serte'
	folder.
SIPS Scheme	
Validate Server Certificate	
	(i) 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)	OEnabled ODisabled
	(i) Only enable this option if the SIP server supports RFC 5626.
Outbound Proxy	
Register Period (seconds)	3600
SDP SRTP Offer	Disabled V
Media NAT	
erver Redundancy	•None CICE OSTUN
Server Redundancy Server Redundancy Feature (Multiple SIP Serve	Support) Enabled Obisabled
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1	•None OICE OSTUN rr Support) •Enabled ODisabled
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2	• None OICE OSTUN • r Support) • Enabled ODisabled
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2	r Support) eEnabled Disabled
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds)	•None OICE OSTUN •r Support) •Enabled ODisabled 120 seconds (2 minutes) •) Time to wait between sending monitoring packets to each server. Inactive servers are
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds)	None OICE OSTUN Support) Enabled Disabled 120 seconds (2 minutes) () Time to wait between sending monitoring packets to each server. Inactive servers are aiways polled and the active server may optionally be polled (see below).
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server	None OICE OSTUN Support) Enabled Disabled 120 seconds (2 minutes) filme to wait between sending monitoring packets to each server. Inactive servers are always polled and the active server may optionally be polled (see below). OEnabled Disabled
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server	None OICE OSTUN Strong OICE OSTUN
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server Automatic Failback	None OICE OSTUN er Support) Enabled Obisabled 120 seconds (2 minutes) (1) Time to wait between sending monitoring packets to each server. Inactive servers are always polled and the active server may optionally be polled (see below). OEnabled Obisabled Explicitly poll the current server to monitor its availability. Polling may also be handled automatically by other regular events, so this can be disabled to reduce network traffic. OEnabled Obisabled
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server Automatic Failback	None OICE OSTUN er Support) Enabled Obisabled 120 seconds (2 minutes) 4) Time to wait between sending monitoring packets to each server. Inactive servers are always polled and the active server may optionally be polled (see below). On Enabled Obisabled (*) Explicitly poll the current server to monitor its availability. Polling may also be handled automatically by other regular events, so this can be disabled to reduce network traffic. One Enabled Obisabled (*) Explicitly poll the current server once available, even if the backup connection is still
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server Automatic Failback	Invore OICE OSTUN er Support) Enabled Disabled 120 seconds (2 minutes) Image to wait between sending monitoring packets to each server. Inactive servers are always polled and the active server may optionally be polled (see below). Enabled Disabled Image connect with a higher priority server once available, even if the backup connection is still working.
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server Automatic Failback Polling Method	None OICE OSTUN er Support) Enabled Disabled 120 seconds (2 minutes) (i) Time to wait between sending monitoring packets to each server. Inactive servers are always polled and the active server may optionally be polled (see below). Enabled Disabled (i) Explicitly poll the current server to monitor its availability. Polling may also be handled automatically by other regular events, so this can be disabled to reduce network traffic. Enabled Disabled (i) Reconnect with a higher priority server once available, even if the backup connection is still working. (i) SIP MOTIPY OSIP OPTIONS (i) SIP message used to poll servers in order to monitor their availability.
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server Automatic Failback Polling Method	None OICE OSTUN er Support) Enabled Disabled 120 seconds (2 minutes) Image: Interpret in the second sec
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server Automatic Failback Polling Method Interoperability	None OICE OSTUN er Support) Enabled Obisabled 120 seconds (2 minutes) Image: Interpret in the second se
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server Automatic Failback Polling Method Interoperability Keep-Alive Method	None OICE OSTUN er Support) Enabled Disabled 120 seconds (2 minutes) 120 seconds (2 minutes) 11me to wait between sending monitoring packets to each server. Inactive servers are always polled and the active server may optionally be polled (see below). Enabled Disabled Enab
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server Automatic Failback Polling Method nteroperability Keep-Alive Method Keen Alive Leberge (second in)	None OICE OSTUN er Support) Enabled ODisabled 120 seconds (2 minutes) (1) Time to wait between sending monitoring packets to each server. Inactive servers are always polled and the active server may optionally be polled (see below). Enabled Disabled (2) Enabled Disabled (3) Enabled Disabled (3) Exabled ODisabled (3) EXP message used to poll servers in order to monitor their availability. Onone ODuble CRLF (4) This setting will enable sending periodic CRLF messages for both UDP and TCP connections.
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server Automatic Failback Polling Method Interoperability Keep-Alive Interval (seconds)	None OICE OSTUN er Support) Enabled ODisabled 120 seconds (2 minutes) ③Time to wait between sending monitoring packets to each server. Inactive servers are always polled and the active server may optionally be polled (see below). Enabled ●Disabled ③Enabled ●Disabled ③SIP NOTIFY OSIP OPTIONS ④SIP NOTIFY OSIP OPTIONS ④SIP message used to poll servers in order to monitor their availability. Onone ●Double CRLF ④This setting will enable sending periodic CRLF messages for both UDP and TCP connections.
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server Automatic Failback Polling Method Reep-Alive Method Keep-Alive Interval (seconds) Use Outgoing TLS port in SIP headers	None OICE OSTUN er Support) Enabled Disabled 120 seconds (2 minutes) 13 Time to wait between sending monitoring packets to each server. Inactive servers are always polled and the active server may optionally be polled (see below). Enabled Disabled Enabled CRLF This setting will enable sending periodic CRLF messages for both UDP and TCP connections. Enabled Disabled Enabled Disabled Enabled Disabled Enabled Disabled Enabled Disabled Other Enabled Stated Enabled Disabled Enabled State Provide State Presence Provide State Presence Presence Provide Presence P
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server Automatic Failback Polling Method Interoperability Keep-Alive Method Keep-Alive Interval (seconds) Use Outgoing TLS port in SIP headers	None OICE OSTUN er Support) Enabled Disabled 120 seconds (2 minutes) (1)Time to wait between sending monitoring packets to each server. Inactive servers are always polled and the active server may optionally be polled (see below). Enabled Disabled (a)Time to wait between server to monitor its availability. Polling may also be handled automatically by other regular events, so this can be disabled to reduce network traffic. Enabled Disabled (a)Time Size Dottions (b) SIP NOTIFY OSIP OPTIONS (c) SIP NOTIFY OSIP OPTIONS (c) SIP message used to poll servers in order to monitor their availability. Onone Double CRLF (a) This setting will enable sending periodic CRLF messages for both UDP and TCP connections. (c) 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 or remere Will device to a some INUTCH
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server Automatic Failback Polling Method Interoperability Keep-Alive Method Keep-Alive Interval (seconds) Use Outgoing TLS port in SIP headers	None OICE OSTUN er Support) Enabled Disabled 120 seconds (2 minutes) 17 Time to wait between sending monitoring packets to each server. Inactive servers are always polled and the active server may optionally be polled (see below). Enabled Disabled Enabled Disabled Enabled Disabled Enabled Disabled Enabled Disabled Enabled Disabled SIP NOTIFY OSIP OPTIONS SIP NOTIFY OSIP OPTIONS This setting will enable sending periodic CRLF messages for both UDP and TCP connections. Enabled Disabled Once Double CRLF This setting will enable sending periodic CRLF messages for both UDP and TCP connections. Enabled Disabled Osservers, like Asterisk or FreeSWITCH.
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server Automatic Failback Polling Method Interoperability Keep-Alive Interval (seconds) Use Outgoing TLS port in SIP headers Do Not Reuse Authorization Headers	None OICE OSTUN er Support) Enabled Disabled 120 seconds (2 minutes) It and the active server may optionally be polled (see below). Enabled Disabled Enabled CLEF This setting will enable sending periodic CRLF messages for both UDP and TCP connections. Enabled Disabled Was express, like Asterisk or FreeSWITCH. Enabled Disabled Enabled Disabled When enabled, all SIP authorization information from the last successful request will not be
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server Automatic Failback Polling Method Interoperability Keep-Alive Method Keep-Alive Interval (seconds) Use Outgoing TLS port in SIP headers Do Not Reuse Authorization Headers	None OICE OSTUN er Support) Enabled Disabled 120 seconds (2 minutes) If Time to wait between sending monitoring packets to each server. Inactive servers are always polled and the active server may optionally be polled (see below). Enabled Disabled When enabled, all SIP authorization information from the last successful request will not be reused in the next request.
Server Redundancy Server Redundancy Feature (Multiple SIP Serve Backup Server #1 Backup Server #2 Polling Interval (seconds) Poll Active Server Automatic Failback Polling Method Interoperability Keep-Alive Method Keep-Alive Interval (seconds) Use Outgoing TLS port in SIP headers Do Not Reuse Authorization Headers Allow Missing Subscription-State Headers	None OICE OSTUN er Support) Enabled Disabled 120 seconds (2 minutes) 120 met to wait between sending monitoring packets to each server. Inactive servers are always polled and the active server may optionally be polled (see below). Enabled Disabled 120 Enabled Disabled 120 Seconect with a higher priority server to monitor its availability. Polling may also be handled automatically by other regular events, so this can be disabled to reduce network traffic. 120 Seconect with a higher priority server once available, even if the backup connection is still working. 120 SIP NOTIFY OSIP OPTIONS 121 SIP message used to poll servers in order to monitor their availability.

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.

<u>SRTP</u>

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.

<u>NAT</u>

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

Status Basic Settings Additional Feat	tures Scheduler Adv	anced Settings	System Lo	gout
Network Admin Users Time Pr	ovisioning File Manager	Advanced Aud	o Advanced SIP	Advanced Multicast
Advanced Multicast Settings				
Ourrent multicast mode: Master Multicast mode can be set in "Basic Setting	gs > <u>Multicast</u> "			
Master Settings				
Master Output Codec	C	G.711 ulaw 🛃		•
Master Output Packetization Time (milli	seconds) 2	20 🔽		•
RTP Control Protocol (RTCP)				
RTCP Port Selection	(i If su po	• Disabled N Select the port on using the 'Next Hig ch that zones are o rts free for RTCP pa	ext Higher Port which packets will be : her Port' option, ensur nly assigned to even-r ckets.	Multiplexed on Same Port sent or received. e that the default multicast zone definitions are modified numbered ports, leaving the next higher odd-numbered
Basic Zone Definition				
Zone	IP Address and	Port Pa	ge Tone	
Priority Call (DTMF:9)	224.0.2.60:50000	<u< td=""><th>se Default Page To</th><td>one> 🔽</td></u<>	se Default Page To	one> 🔽
All Call (DTMF:0/8)	224.0.2.60:50001	<u< td=""><th>se Default Page To</th><td>one> 🔽</td></u<>	se Default Page To	one> 🔽
Zone 1 (DTMF:1)	224.0.2.60:50002	<u< td=""><th>se Default Page To</th><td>one> •</td></u<>	se Default Page To	one> •
Zone 2 (DTMF:2)	224.0.2.60:50003	<u< td=""><th>se Default Page To</th><td>one> 🔽</td></u<>	se Default Page To	one> 🔽
Zone 3 (DTMF:3)	224.0.2.60:50004	<u< td=""><th>se Default Page To</th><td>one> •</td></u<>	se Default Page To	one> •
Zone 4 (DTMF:4)	224.0.2.60:50005	<u< td=""><th>se Default Page To</th><td>one> 🔽</td></u<>	se Default Page To	one> 🔽
Zone 5 (DTMF:5)	224.0.2.60:50006	<u< td=""><th>se Default Page To</th><td>one> 🔽</td></u<>	se Default Page To	one> 🔽
Zone 6 (DTMF:6)	224.0.2.60:50007	<u< td=""><th>se Default Page To</th><td>one> •</td></u<>	se Default Page To	one> •
Music (DTMF:7)	224.0.2.60:50008	<u< td=""><th>se Default Page To</th><td>one> 🔽</td></u<>	se Default Page To	one> 🔽
Expanded Zone Definition				
Zone	IP Address and	Port Pa	ge Tone	
Zone 10 (DTMF: *10)	224.0.2.110:50000	<u< td=""><th>se Default Page To</th><td>one> •</td></u<>	se Default Page To	one> •
Zone 11 (DTMF: *11)	224.0.2.111:50000	<u< td=""><th>se Default Page To</th><td>one> •</td></u<>	se Default Page To	one> •

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* \rightarrow *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* \rightarrow *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* \rightarrow *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* \rightarrow *Features* \rightarrow *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

Additional Features	Scheduler Advanced Settings System Logout
Download Configuration File	Jownload
Restore Configuration File	Choose File No file chosen
Restore Configuration to Defaults	Restore Defaults
ackup in zip format includes configuration file and Download Backup Zip File Restore from Backup Zip File	all uploaded files.
Restore All Settings and Files to Defaults	 Restore Defaults and Delete Files All preloaded and uploaded files, including tone files, will be deleted.
Reboot	
Reboot the device	Reboot

Figure 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

Maintenance Firmware File Manager Tones System Log Credits About Firmware Installed Firmware Installed Firmware algo-8301-5.2 Online Upgrade Check for Firmware Updates Image: Check Custom Upgrade Image: Check Image: Check Method Image: From Local Files Image: Check Signed Firmware File Choose File No file chosen Allow Downgrade Image: Check or bits option could cause upgrade issues. Please contact support if necessary. Image:	Status Basic Settings Additional Features	Scheduler Advanced Settings System Logout
Firmware Installed Firmware Product Firmware algo-8301-5.2 Online Upgrade Check for Firmware Updates Custom Upgrade Method From Local Files From URL Signed Firmware File Choose File No file chosen Allow Downgrade Chabled Allow product or base firmware to be downgraded to an older patch version. Allow Downgrade Installed Chabled Disabled Disabled	Maintenance Firmware File Manager To	ones System Log Credits About
Installed Firmware Product Firmware algo-8301-5.2 Online Upgrade Check for Firmware Updates Check Custom Upgrade Check Method ©From Local Files Signed Firmware File Choose File Allow Downgrade CEnabled Online Upgrade Chabled Image: Choose File No file chosen Allow Downgrade Cenabled Option could cause upgrade issues. Please contact support if necessary.	Firmware	
Product Firmware algo-8301-5.2 Online Upgrade Check Check for Firmware Updates Check Custom Upgrade Check Method Image: Check Signed Firmware File Choose File Allow Downgrade Chabled Online Upgrade Chabled Image: Check Choose File No file chosen Choose File Allow Downgrade Chabled Image: Check Optimizer for base firmware to be downgraded to an older patch version. Image: Check Image: Check Image: Check Image: Check	Installed Firmware	
Online Upgrade Check for Firmware Updates Check Custom Upgrade Method From Local Files From URL Signed Firmware File Choose File No file chosen Allow Downgrade Cenabled Objabled	Product Firmware	algo-8301-5.2
Check for Firmware Updates Check Custom Upgrade Image: Check Method Image: Check Signed Firmware File Choose File No file chosen Allow Downgrade Cenabled Disabled Image: Allow Downgrade Cenabled Disabled Image: Check Choose File No file chosen Choose File No file chosen Allow Downgrade Cenabled Disabled Output or base firmware to be downgraded to an older patch version. Image: Check Check Check Choose File No file chosen Check Choose File No file chosen Allow Downgrade Cenabled Disabled Output or base firmware to be downgraded to an older patch version. Image: Check Choose File No file chosen Choose File No file chosen Choose File No file chosen Image: Check Choose File No file chosen Choose File No file chosen Choose File No file chosen Image: Check Choose File No file chosen Choose File No file chosen Choose File No file chosen Image: Check Choose File No file Choose File No file chosen Choose File No file chosen Choose File No file chosen Image: Check Choose File No file Choose File No file chosen Choose File No file choosen Choose File No file choosen <t< td=""><td>Online Upgrade</td><td></td></t<>	Online Upgrade	
Custom Upgrade Method From Local Files From URL Signed Firmware File Choose File No file chosen Allow Downgrade Cenabled	Check for Firmware Updates	Re Check
Method Image: Choose File OFrom URL Signed Firmware File Choose File No file chosen Allow Downgrade OEnabled Image: OEnabled I	Custom Upgrade	
Signed Firmware File Choose File No file chosen Allow Downgrade CEnabled Image: Comparison of the part of the	Method	From Local Files OFrom URL
Allow Downgrade CEnabled Disabled Allow product or base firmware to be downgraded to an older patch version. Another the source of the sou	Signed Firmware File	Choose File No file chosen
P Upgrade	Allow Downgrade	 Cenabled Disabled (i) Allow product or base firmware to be downgraded to an older patch version. A Enabling this option could cause upgrade issues. Please contact support if necessary.
		1 Upgrade
		· · · · · · · · · · · · · · · · · · ·

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 \rightarrow 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

Status Basic Settings Additional Features Scheduler Advanced Settings System Logout				
Maintenance Firmware File Manager Tones System Log Credits About				
🕹 Upload < 🗦	↑ Files		٩	
I∢ "≣ "≘	Name	Date	Туре	Size
∽ 🗁 Files	🗅 certs	01/27/2022 12:31 PM	Folder	
> 🗅 certs	🗅 debug	03/26/2021 02:57 PM	Folder	
🗅 debug	🗅 license	03/26/2021 02:57 PM	Folder	
C license	🗅 tones	01/27/2022 12:32 PM	Folder	
	🗋 scheduler-bk.db	11/16/2022 11:34 AM	File	20KB
	scheduler-oldver.json	02/07/2022 02:17 PM	File	1.044KB
	🗋 scheduler.db	11/16/2022 11:39 AM	File	20KB
	scheduler_converted.db	11/16/2022 11:34 AM	File	16KB
	🖹 user.conf	11/08/2022 03:16 PM	Text File	14.019KB
		Us	ed:331MB Av	ailable: 1.3GB

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

Status Basic Settings Additional Features Sched	uler Advanced Settings System Logout	
Maintenance Firmware File Manager Tones S	System Log Credits About	
Tones Use the "System > File Manager" tab to upload tone files to "tones" subdirectory. Files Download and Install Ring Tones from the Algo Server Download and Install () Tone files can be downloaded manually from the Algo website.		
Cache Rebuild Tone Cache Files	Rebuild All	
	Only needed when the tone cache is out of sync. The operation might take a long time depending on the types and sizes of the tone files.	
Test Tones	warble2-med.wav V Play Loop Stop	

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* \rightarrow *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.

Status	Basic Settings Additional Features Scheduler Advanced Settings System Logout
Mainten	ance System Log Credits About
System	l Log
Down	
Down	
Log Fi	le 🕹 Download syslog.txt
	View

Figure 37: System log settings

6.9 Logout

Log out of the 8301 web interface.

7 SPECIFICATIONS

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		
АРІ	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.	

Table 1: 8301 Specification Table



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.