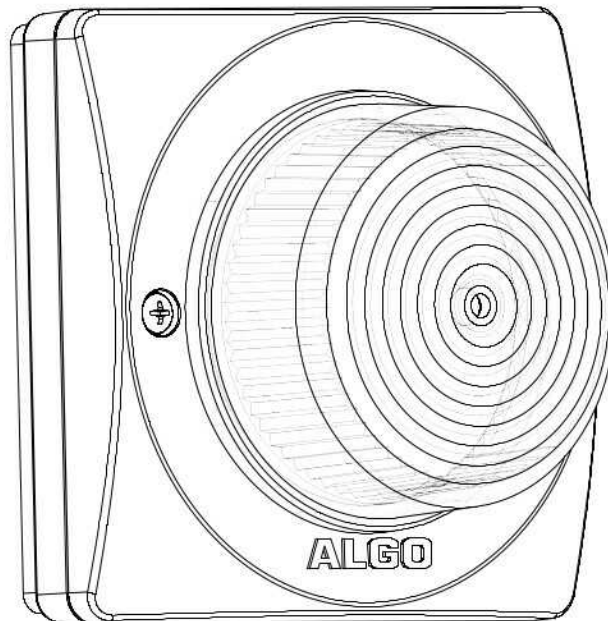


## 8138 SIP Multicolor Strobe Light

### User Guide



## Table of Contents

IMPORTANT SAFETY INFORMATION.....	4
OVERVIEW.....	7
Introduction.....	7
Key Features.....	7
Terminal Block Reset.....	8
SETUP AND INSTALLATION.....	9
Getting Started - Quick Install & Test.....	9
Ceiling and Wall Mounting.....	10
Programming and Configuration.....	10
Inputs/Outputs.....	11
FEATURES.....	12
SIP Paging: One 8138.....	12
SIP Ring Event.....	12
Multicast Overview.....	12
SIP Paging: Multiple 8138 (Using Multicast).....	13
SIP Paging: Multiple Strobe (Using Individual SIP extensions).....	13
SIP Activated Notification Alerts.....	13
TLS for SIP Signaling and Provisioning.....	14
WEB INTERFACE BASIC SETTINGS.....	18
Web Interface Login.....	18
Status.....	19
Basic Settings Tab – SIP.....	19
Basic Settings Tab – Features.....	21
Basic Settings Tab – Strobe.....	22
Basic Settings Tab – Multicast.....	22
Basic Settings Tab – Multicast (Master Settings).....	24
Basic Settings Tab – Multicast (Slave Settings).....	26
WEB INTERFACE ADDITIONAL FEATURES.....	28
Additional Features Tab – Input/Output.....	28
Additional Features Tab – Emergency Alerts.....	31
Additional Features Tab – More Page Extensions.....	33
Additional Features Tab – More Ring Extensions.....	34
WEB INTERFACE ADVANCED SETTINGS.....	35
Advanced Settings Tab – Network.....	35
Advanced Settings Tab – Admin.....	37
Advanced Settings Tab – Time.....	40
Advanced Settings Tab – Provisioning.....	41
Advanced Settings Tab – Advanced Audio.....	43
Advanced Settings Tab – Advanced SIP.....	44
Advanced Settings Tab – Advanced Multicast.....	47
WEB INTERFACE SYSTEM.....	48
System Tab – Maintenance.....	48
System Tab – Firmware.....	49
Advanced Settings Tab – File Manager.....	50

System Tab – System Log.....	51
<b>WIRING CONNECTIONS.....</b>	<b>51</b>
Network Connection.....	51
Connecting Input Devices.....	51
<b>SPECIFICATIONS.....</b>	<b>52</b>
<b>FCC COMPLIANCE STATEMENT.....</b>	<b>53</b>

## Important Safety Information

### Important Safety Information

This product is powered by a certified limited power source (LPS), Power over Ethernet (PoE); through CAT5 or CAT6 connection wiring to an IEEE 802.3at PoE+ or 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](mailto: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 802.3at PoE+ or 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](mailto: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 802.3at PoE+ or 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](mailto: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 802.3at PoE+ or 802.3af-konformen Ethernet-Netzwerkweiche. Das Produkt wurde konzipiert für die Installation innerhalb eines Gebäudes. Alle Kabelverbindungen zum Produkt müssen im selben Gebäude bestehen. Wenn das Produkt jenseits des Gebäudes oder für mehrere Gebäude genutzt wird, müssen die Kabelverbindungen vor Überspannung und Spannungssprüngen geschützt werden. Algo empfiehlt das Produkt von einem qualifizierten Elektriker installieren zu lassenv.

Sollten Sie die englischen Sicherheitsinformationen nicht verstehen, kontaktieren Sie bitte Algo per Email bevor Sie mit der Installation beginnen, um Unterstützung zu erhalten.

Algo kann unter der folgenden E-Mail-Adresse erreicht werden:

[support@algosolutions.com](mailto:support@algosolutions.com).

## **安全须知**

本产品由认证的受限电源（LPS），以太网供电（PoE），通过 CAT5 或 CAT6 线路联接至 IEEE 802.3at PoE+ or 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](mailto:support@algosolutions.com)。

## **EMERGENCY COMMUNICATION**

The 8138 SIP Strobe Light is not intended for fire alarm signaling applications. The 8138 SIP Strobe Light is intended for informative signaling in conjunction with unified communication systems. The 8138 Strobe Light is suitable for OSHA and ADA compliance when properly located and configured

## **DO NOT LOOK DIRECTLY**

Do not look directly at the 8138 SIP Strobe Light while operating in close proximity, as vision may be affected. The LEDs in the 8138 light are classified according to the IEC 62471-2006 standard as “RG-1” for risk group 1. This is defined as “*Low risk. No photobiological hazard under normal behavioral limitations.*”

## PHOTO-SENSITIVITY

Photo-sensitivity in some people with epilepsy can trigger seizures from flashing or flickering lights. It is possible that some flash patterns of the 8138 SIP Strobe Light could trigger a seizure for some individuals under some conditions. High intensity patterns should only be selected if necessary for the 8138 to be effective.

## WET OR OUTDOOR ENVIRONMENTS

The 8138 SIP Strobe Light is intended for indoor or outdoor locations and may be subjected to spray or weather provided the rear wiring cavity is properly sealed to prevent water ingress.

Gaskets included with the 8138 SIP Strobe Light may be effective against water ingress on some, but not all surfaces in which case additional protective measures must be taken such as a perimeter sealant.

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

**No wiring connected to the 8138 SIP Strobe Light may leave the building perimeter without adequate lightning protection.**

## Overview

### Introduction

The 8138 SIP Strobe Light is a SIP compliant, multicast capable, PoE strobe light. The flash intensity can be chosen to suit the application and environment. There are non-flashing patterns for passive gentle notification and aggressive patterns for maximum conspicuity in busy environments.

The 8138 is typically wall or ceiling mounted. The 360° x 180° visibility, 15 available flash patterns, and 4 color settings makes the 8138 suitable for notification and alerting of telephone, emergency, safety, and security events. Light output is equally intense in every direction unless a directional pattern is chosen.

The 8138 SIP Strobe Light can be activated by:

- SIP Ring
- SIP In-Use (Subscribe Notify)
- Dry contact closure input
- Multicasting

Multiple Algo endpoints in a SIP environment require only one device to register as a SIP extension. Multicasting capabilities allow the SIP registered strobe to flash and simultaneously stream multicast events to the other Algo strobes, speakers and paging adapters in any combination and number of endpoints.

The 8138 SIP Strobe Light is configured using central provisioning features or by accessing a web interface using browsers such as Google Chrome or Firefox.

### Key Features

#### SIP Extensions

The 8138 connects to an on-premise or hosted communication server in the same way as a SIP telephone. To register the 8138 with the server requires the following information:

1. IP address (e.g. 192.168.1.111) or domain name (e.g. myserver.com) of the SIP Server
2. SIP extension (e.g. 3790)
3. Authentication ID
4. Password

The 8138 supports two SIP extensions which behave differently – **RING** and **PAGE**. One or both may be used depending on the application. If the RING extension is called the 8138 will not answer. Instead, it will flash a light pattern until the inbound call stops ringing. Typically the RING extension is programmed as part of a hunt group so that it receives a ring signal simultaneously with one or more devices.

If the PAGE extension is called, the 8138 will answer and flash a light pattern until the call is ended.

## Multicasting

Allows multiple units to simultaneously flash light patterns. The 8138 can be configured as a multicast 'Master' device to send a multicast stream to other slave devices. The 8138 can be configured as a multicast 'Slave' device to flash a light pattern when a stream is received from a multicast 'Master' device. Any number/combination of Algo IP speaker, paging adapter, or strobe endpoint can be configured as multicast 'Slaves'. This feature provides scalability without requiring each endpoint Slave to be registered with a SIP extension.

## Polycom™ Group Paging

The 8138 supports Polycom Group Paging. The 8138 can be added to a Polycom Group Page so that voice paging activates a flash pattern while active.

## Configuration & Provisioning

Configuration can be done through a web interface control panel or central provisioning features. Central provisioning allows units to be pre-configured for a specific server prior to deployment in the field. Configuration files are automatically downloaded from a server (via TFTP, FTP, HTTP, HTTPS) using DHCP.

## Terminal Block Reset

The reset relay terminal on the back can be used to reset the 8138 SIP Strobe light at time of power up. To return all the settings to the factory default for the 8138, wait until the LED flashes, then connect the reset terminals and hold until the 8138 LED begins a double flash pattern. Release the reset connection and allow the unit to complete its boot process.

**A reset will set all configuration options to factory default including the password.**



## Setup and Installation

### Getting Started - Quick Install & Test



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

1. Connect the 8138 SIP Strobe Light to a 802.3af PoE network switch using the RJ45 jack in the back recess of the housing.
2. Allow the 8138 SIP Strobe Light time to boot, about 30 seconds. While booting the Strobe will activate a small dim amber light in the center.
3. If there is no DHCP server found the 8138 SIP Strobe Light will default to the static IP address 192.168.1.111. Most often however the 8138 will be assigned an IP address. The IP address may be discovered by downloading the Algo Locator Tool to find Algo devices on your network: [www.algosolutions.com/locator](http://www.algosolutions.com/locator)
4. Access the 8138 web page by entering the IP address into a browser (Chrome, Firefox etc.) and login using the default password: algo
5. Enter the IP address for the SIP server into the SIP Domain field under the **Basic Settings > SIP** tab.
6. Enter the Ring and/or Page SIP extension and credentials. Leave the credentials blank for either extension if there is no intended use to have both registered.

(Note: The strobe supports multiple Ring, Emergency Alert, and Page SIP extensions. The Page extension auto-answers and flashes a light pattern. The Ring and Emergency Alert extensions will flash a light pattern without answering.)

7. Make a test call from a telephone to the strobe for one or both extensions. The Page SIP extension should auto-answer and flash the light pattern. The Ring SIP extension will flash the light pattern without answering the call.

## Ceiling and Wall Mounting

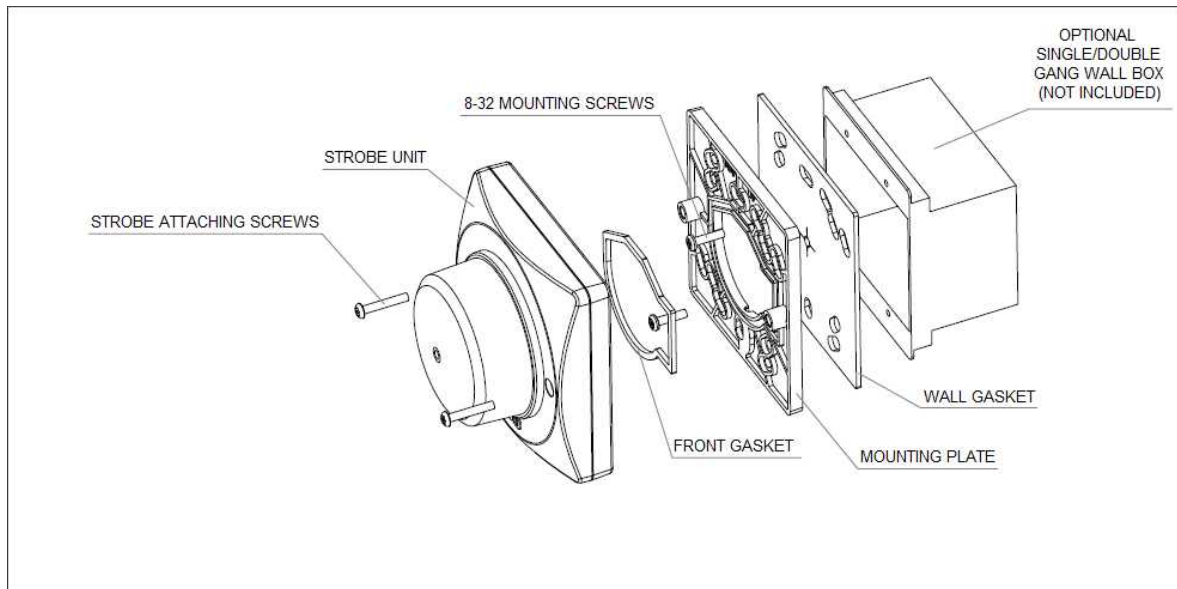
The 8138 SIP Strobe Light can be wall or ceiling mounted. Concealed wiring may enter from the wall into the wiring cavity. Alternatively, surface wiring may enter through a channel from the bottom edge. The channel is intended for cabling 0.2" or 5mm in diameter and is intentionally snug to protect against moisture ingress.

The 8138 can be mounted in any orientation but both the bracket and housing identify TOP. This keeps the bracket wiring chase on the bottom and the RJ45 jack on the top side.

The mounting plate may be used to mount over flush or surface mounted electrical boxes or mud rings and fits securely to a 2 gang electrical box (not included) for installation with wiring conduit.

The 8138 SIP Strobe Light is rated for wet locations however care must be taken to ensure that water does not enter the wiring cavity. The supplied gaskets or sealant must be used to protect the wiring cavity in wet environments. In dry indoor environments the gaskets are not required. If the wall gasket is used with surface wiring, then the gasket should be attached after placing the cable into the wiring channel.

The 8138 should not be installed beyond a building perimeter without adequately protecting the building wiring from lightning surge.



## Programming and Configuration

After connecting the 8138 to a network PoE will attempt to obtain an IP address from the DHCP server. If there is no DHCP server or the attempt was unsuccessful, the 8138 will default to the static IP address **192.168.1.111**.



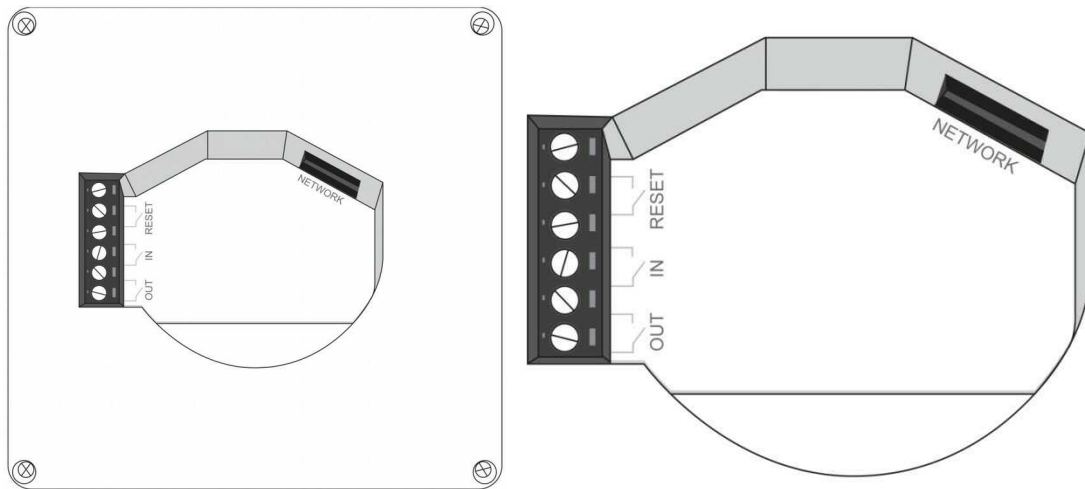
*Note: If you don't have a PoE switch, you'll need a PoE or PoE+ injector installed between the 8138 and the network switch. The PoE injector will supply 48V dc to the 8138. Most PoE injectors are capable of providing more power than the 8138 requires (12.95 W). Ensure that the PoE injector is fully compliant to the IEEE 802.3at PoE+ or 802.3af standard.*

The IP address may be discovered by downloading the Algo locator tool to find Algo devices on your network: [www.algosolutions.com/locator](http://www.algosolutions.com/locator)

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

## Inputs/Outputs

On the back, the 8138 SIP Strobe Light has a relay output, relay input and terminal block reset. Door Control relay.



### 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, or EOL resistor termination.

### Terminal Block Relay Out

By default these terminals provide a contact closure when the 8138 SIP Strobe Light is active.

### Terminal Block Reset

To return all settings to a factory default, use a wire pair to short these terminals at start up—continue until all the 8138 LEDs start a pulsing flash pattern.

## Features

### SIP Paging: One 8138

The 8138 SIP Strobe Light can be registered as a third-party SIP extension with a hosted or enterprise Communications Server supporting 3<sup>rd</sup> party SIP endpoints.

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

If VLAN is used, navigate to the **Advanced Settings > Network** tab to set VLAN options.



*Important: once the strobe is using VLAN you will need to be on the same VLAN to access the web interface.*

The strobe may now be accessed by dialing its assigned extension from a telephone, device, or client. The strobe will auto-answer and flash a light pattern.

There are a number of configurable strobe options:

- Flash Pattern
- Brightness
- Color 1
- Color 2

### SIP Ring Event

Set Monitoring Mode to '**Monitor Ring**' and enter credentials. When a call is made to the SIP extension the 8138 will flash the selected light pattern. Often, the 8138 will be part of a hunt group or ring group to flash in conjunction with a telephone.

### Multicast Overview

In addition to the ring and page features, the 8138 is able to both send and receive IP multicast messages over the network to support larger deployment for both paging and ring/notification. This provides a scalable and efficient method of building large scale notification solutions.

An Algo 8138 can be configured as a Master endpoint. When the SIP Page extension is dialed from a phone, the 8138 will auto-answer, and flash a light pattern in chosen color. Simultaneously, the registered 8138 endpoint broadcasts the audio over the network using RTP multicast to any number/combination of Algo IP speakers, paging adapters, and strobes as required.

The Slave endpoints require a PoE network connection but do not require registration to the communication server.

Multicasting can also be used to distribute loud ring or other alerting (e.g. safety, security, or emergency events) over multiple Algo endpoints (e.g. 8190, 8186, 8188, 8128, 8201, 8301, and 8373).

## SIP Paging: Multiple 8138 (Using Multicast)

To use 8138 multicast feature, setup an 8138 Strobe Light as a Multicast master.

The Master device will flash a light pattern normally while simultaneously streaming audio to the slave speakers. The Slave speakers do not require SIP extensions and do not need to register with the SIP Communication Server.

To enable multicast streaming from the 8138 SIP Strobe Light go to its web interface and navigate to the **Basic Settings > Multicast** tab. Choose multicast mode '**Master/Sender**' and zone '**All Call**'. The multicast addresses pre-populated in the table, under **Advanced Settings > Advanced Multicast** section, will work in most cases and should only be altered for rare cases.

To enable multicast monitoring in the 8138, go to the web interface for each strobe and again navigate to the **Basic Settings > Multicast** tab. This time though, choose multicast mode '**Slave/Receiver**' There is no need to select a zone as the strobe will automatically monitor the '**All Call**' zone IP address.



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

## SIP Paging: Multiple Strobe (Using Individual SIP extensions)

In some cases, it may be desirable for every strobe to have a SIP extension. Multicast may still be used to page multiple strobes but each strobe can also be called individually or generate a call when appropriately configured.

A strobe configured as a SIP Multicast Slave will give its highest priority to the 'Priority Call' zone. Other than the 'Priority Call' zone, a page using its SIP extension, has priority over all other multicast zones.

Communication Servers with the capability of dialing many SIP extensions simultaneously for paging may be able to create zones by calling "page groups" and also page telephone speakers in conjunction with overhead speakers.

## SIP Activated Notification Alerts

In addition to voice paging, the 8138 can multicast audio files for emergency, safety, and security announcements, customer service, shift changes, etc.

Audio WAV files can be stored in strobe memory and also multicast to other Algo SIP endpoints on the network. See **Additional Features > Emergency Alerts** and **Additional Features > Input/Output** for more details.

## Polycom™ Group Paging

The 8138 SIP Strobe Light has been designed to support Polycom Group Paging.

The 8138 can be added to a Polycom Group Page so that voice paging is heard over Polycom telephone speakers and visually alerted simultaneously.



## 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 an important piece in the Algo device's operation, to ensure the security, integrity, and privacy of its communication. Algo components that use TLS are **Provisioning** and **SIP Signaling**.

These Algo devices each 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 shared (pre-master) secret key.

## Provisioning


Provisioning is secured by setting the 'Download Method' to 'HTTPS' (under the **Advanced Settings > Provisioning** tab)

The screenshot shows the 'Provisioning Settings' page. At the top, there are tabs for 'Status', 'Basic Settings', 'Additional Features', 'Advanced Settings' (selected), 'System', and 'Logout'. Below these are sub-tabs for 'Network', 'Admin', 'Time', 'Provisioning' (selected), 'Advanced Audio', 'Advanced SIP', and 'Advanced Multicast'. The main content area is titled 'Provisioning Settings' and contains several sections:

- Mode:** A section with a 'Provisioning Mode' label and two radio buttons: 'Enabled' (selected) and 'Disabled'.
- Settings:** A section containing:
  - Server Method:** Radio buttons for 'Auto (DHCP Option 66/160/150)' (selected), 'DHCP Option 66 only', 'DHCP Option 160 only', 'DHCP Option 150 only', and 'Static'. Below this is an information icon and text: 'Auto mode automatically checks all 3 DHCP options for an active provisioning server, in the order listed.'
  - Download Method:** Radio buttons for 'TFTP' (selected), 'FTP', 'HTTP', and 'HTTPS'.
  - Config Download Path:** An empty text input field.
  - Firmware Download Path:** An empty text input field.
  - Partial Provisioning:** Radio buttons for 'Enabled' and 'Disabled' (selected). Below this is an information icon and text: 'Allow support for "-i" incremental provisioning files. Disable for enhanced security if not using this feature.'

At the bottom right of the form is a 'Save' button with a green checkmark icon.

Setting provisioning to 'HTTPS' prevents configuration files from being read by unwanted third-party devices/ attackers. This resolves the potential risk of having sensitive data: admin passwords and SIP credentials stolen.

 **Important:** To verify the server you must '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. Certificates can also be manually uploaded using the 'File Manager'.



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

```
prov.download.cert = 1
```

## SIP Signaling

SIP Signaling is secured by setting 'SIP Transportation' to 'TLS' (under the **Advanced Settings >Advanced SIP** tab)

The screenshot displays the 'Advanced SIP Settings' page in a web browser. The top navigation bar includes 'Status', 'Basic Settings', 'Additional Features', 'Advanced Settings', 'System', and 'Logout'. Below this, a secondary navigation bar shows 'Network', 'Admin', 'Time', 'Provisioning', 'Advanced Audio', 'Advanced SIP', and 'Advanced Multicast'. The main content area is titled 'Advanced SIP Settings' and is divided into several sections:

- General**:
  - SIP Transportation**: A dropdown menu is set to 'Auto'. Below it, a help icon and text state: "Select Auto to check DNS NAPTR record, then try UDP/TCP. In TLS mode, if the SIP Server requires endpoints to be authenticated, a PEM file containing both a device certificate and a private key needs to be installed on the Algo device. Use the 'System > File Manager' tab to upload a certificate file renamed to 'sipclient.pem' in the 'certs' folder."
  - SIPS Scheme**: Radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected.
  - Validate Server Certificate**: Radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected. A help icon and text state: "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."
  - Force Secure TLS Version**: Radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected. A help icon and text state: "Enable this option to require TLS connections to use TLSv1.2."
  - SDP SRTP Offer**: A dropdown menu is set to 'Disabled'.
  - SIP Outbound Support (RFC 5626)**: Radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected. A help icon and text state: "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**: An empty text input field.
  - Register Period (seconds)**: A text input field containing '3600'.
- NAT**:
  - Media NAT**: Radio buttons for 'None', 'ICE', and 'STUN', with 'None' selected.
- Server Redundancy**:
  - Server Redundancy Feature (Multiple SIP Server Support)**: Radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected.
- Interoperability**:
  - Keep-Alive Method**: Radio buttons for 'None', 'Double CRLF', with 'None' selected. A help icon and text state: "This setting will enable sending periodic CRLF messages for both UDP and TCP connections."
  - Use Outgoing TLS port in SIP headers**: Radio buttons for 'Enabled' and 'Disabled', with 'Enabled' selected. A help icon and text state: "Use ephemeral port number from outgoing SIP TLS connection instead of listening port number in SIP Contact and Via headers. This is useful to connect the device to some local SIP servers, like Asterisk or FreeSWITCH."
  - Do Not Reuse Authorization Headers**: Radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected. A help icon and text state: "When enabled, all SIP authorization information from the last successful request will not be reused in the next request."
  - Allow Missing Subscription-State Headers**: Radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected. A help icon and text state: "When enabled, allow SIP NOTIFY messages that do not contain a 'Subscription-State' header."

A green 'Save' button with a checkmark is located at the bottom right of the settings area.



Setting 'SIP Transportation' from 'Auto' (default) to 'TLS', ensures the encryption of SIP traffic. Setting 'SDP SRTP Offer' to 'Standard' or '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.



*Important: In order for a SIP server to validate the Algo device, an additional certificate has to be installed on the Algo device manually. For Firmware v1.7, the only way to add this user certificate file is to use a '.pem' file type extension and have the file named 'sipclient'. This is done by manually adding a file named 'sipclient.pem', which contains a device certificate and private key, to the 'certs' folder (under the 'Advanced Settings' tab File Manager). In the future, '.crt', '.cer', and '.der' certificate extensions will also be supported and you will not be restricted to naming the file 'sipclient.pem'.*

## Web Interface Basic Settings

### Web Interface Login

The web interface requires a password which is 'algo' by default. This password can be changed in the **Admin** tab after logging in the first time.

Status
Basic Settings
Additional Features
Advanced Settings
System
Logout

Device Status

### Welcome to the Algo 8138 SIP Multicolor Strobe Control Panel

Setting up your SIP Multicolor Strobe:

**Step 1: Configure your SIP Multicolor Strobe**

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

**Step 2: Check network settings (Optional)**

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

**Step 3: Secure your SIP Multicolor Strobe (Optional)**

Use the Admin page under the Advanced Settings tab to change the administrator password.

Changing the password is extremely important if the device is directly connected to a public network.

**Step 4: Register your SIP Multicolor Strobe (Optional)**

Please register your product using the link below:

<http://www.algosolutions.com/register>

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

**Status**


Device Name	sipstrobe-eva	
SIP Registration	<b>Page</b>	<b>No Account</b>
Call Status	Idle	
Proxy Status	Single proxy mode	
Security	TLS	Disabled
	SRTP	Disabled
Provisioning Status	None Found	
MAC	00:22:ee:0f:00:20	
IPv4	10.30.27.198/8, Gateway: 10.0.0.1	
IPv6	fdb4:1f1d:4df6:100:dc:0:ffff:cd49	
Date / Time	Mon Sep 9 18:09:45 GMT 2019	
Multicast Mode	Disabled	
Relay Input Status	Disabled	

*Web Interface is accessed by entering 8138's IP Address into the web browser.*

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

## Status

The device's Status page will be available before and after log on. The section can be used to check 8138's SIP Registration status of the Ring/Page extensions, Call Status, Multicast Mode, Relay Input Status, Proxy Status, and general MAC, IP, Netmask, Date/Time, and Timezone information.

 *The Status page can be hidden when logged out for security purposes under the **Advanced Settings > Admin** tab.*

## Basic Settings Tab – SIP

SIP Server information and Credentials should be obtained from your telephone system administrator or hosted account provider. After saving the settings, see the Status page to confirm that the registration was successful.

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

SIP
Features
Strobe
Multicast

### SIP Settings

**SIP**

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

SIP Domain (Proxy Server)

*ⓘ* Default port is 5060. To specify a different port, enter PROXY:PORT, e.g. my\_proxy.com:5070, or 192.168.1.10:5080.

Alert Mode

Monitor "Ring" event on registered SIP extension


Use "Subscribe/Notify" dialog event (RFC 4235) to monitor event on different extension

Use "Subscribe/Notify" presence event (RFC 3856/3863 PIDF) to monitor event on different extension

None

Ring/Alert Extension

Authentication ID


Authentication Password  

Display Name (Optional)

*ⓘ* The device will detect inbound ring events on this extension and flash a light pattern until the inbound call stops ringing. It will not answer the call on this extension.


Base/Page Extension

Authentication ID

Authentication Password  

Display Name (Optional)

*ⓘ* The device will auto-answer any inbound call received on this extension and flash a pattern.

 *Important: Any time 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**

Option for enabling/disabling/or subscribing to a Ring/Alert SIP extension. If activated, screen expands to enter SIP extension parameters for a Ring/Alert Extension.

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

## **Subscribe Notify**

Can subscribe to and notify, for when a Ring Extension is dialed ('Ring') and/or when the Ring is answered ('Both Ring & In-Use' or 'In-Use').

You must first configure a 'Page Extension', and then can configure a 'Ring/Alert Extension' to subscribe to.

You can subscribe to just the 'Ring' Alert Event, for which when the ring extension is called. You can subscribe to just an 'In-Use' Alert Event as well, for which when the ring extension is called, the 8138 will only flash a light pattern once the ring is actually answered. Lastly, you can subscribe to both Alert Events by using 'Both Ring & In-Use', for which the 8138 will flash a light pattern, when the subscribed ring extension, is being called and when its in-use.

## **Ring Extension**

This is the SIP extension for the 8138 strobe's Ring parameter. The device will detect inbound ring events on this extension and flash a light pattern (and multicast the alerting tone if configured) until the inbound call stops ringing. It will not answer the call on this extension.

## **Page Extension**

This is the SIP extension for the 8138 strobe. The device will auto-answer any inbound call received on this extension and flash a light pattern and provide a voice paging path for multicast (if configured).

## **Authentication ID**

May also be called Username for some SIP servers and in some cases may be the same as the SIP extension used for the associated Ring and/or Page parameter.

## **Authentication Password**

SIP password provided by the system administrator for the SIP account used for the associated Ring and/or Page parameter.

## Basic Settings Tab – Features

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

SIP
**Features**
Strobe
Multicast

### Features

**Inbound Ring Settings**

*i* These settings apply to events triggered by the Ring Extension(s) & Emergency Alerts sections.

Ring Limit No limit

*i* 1 ring = 6 seconds.

**Inbound Page Settings**

Page Timeout 5 minutes

G.722 Support  Enabled  Disabled

*i* Applies to codec used during SIP negotiation only. Multicast codec is configured separately.

DTMF Detection Type  Auto  RTP Telephony Event (RFC 4733)  RTP In-band  SIP INFO

**Strobe**

Strobe Pattern 1 - Multi-strobe Fast Amber

Idle Pattern <None>

Save

### Ring Limit

Typically set to no limit, this feature can be used to set a limit on how long the strobe will ring before timing out. A new ring event is required before the strobe will flash a light pattern and play the WAV file again

### Page Timeout

A time limit may be set for an active page.

### G.722 Support

Enable or disable the G.722 codec.

### DTMF Detection Type

Different DTMF detection options are given.

## Strobe Pattern

Select strobe pattern to flash when page/ring event is detected on the SIP Page/Ring extension.

## Idle Pattern

Select strobe pattern to flash when 'Call Status' is in Idle mode.

## Basic Settings Tab – Strobe

### Pattern Definitions

Several different strobe patterns can be configured with a Flash Pattern, Brightness, and one or two colors.

Configured strobe patterns are named to simplify the selection elsewhere.

On the 8138 a drop down option **Strobe Pattern** is displayed next to features that allow patterns to be associated with actions such as page, ring, or multicast.

No	Description	Application		Intensity/Strobe		
		Wall	Ceiling	High	Med	Low
1	Rotate Fast		•		•	
2	Rotate Slow		•		•	
3	Multicolor Spin	•	•	•		
4	Multi-strobe Fast (One color)	•	•	•	•	
5	Multi-strobe Fast (Two colors)	•	•	•	•	
6	Multi-strobe Slow(One color)	•	•	•	•	
7	Multi-strobe Slow (Two colors)	•	•	•	•	
8	Rotating Strobe	•	•	•		
9	Steady (One color)	•	•			•
10	Steady (Two colors)	•	•			•
11	Side to Side	•			•	
12	Flashing	•	•		•	
13	Classic Strobe Fast	•	•		•	
14	Classic Strobe Medium	•	•		•	
15	Classic Strobe Slow	•	•		•	

## Basic Settings Tab – Multicast

### Multicast IP Addresses

Each 8138 SIP Strobe Light has its own IP address, and shares common multicast IP and port numbers (multicast zone) for multicast packets. The master device transmits to a configurable multicast zone, and the slave 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 master and slave 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 8138 SIP Strobe Light 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 8138 SIP Strobe Light supports nine “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 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 the **Basic Settings > Multicast tab**, 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.

## Basic Settings Tab – Multicast (Master Settings)

The screenshot displays the 'Multicast Settings' configuration page. At the top, there are navigation tabs: 'Status', 'Basic Settings' (selected), 'Additional Features', 'Advanced Settings', 'System', and 'Logout'. Below these, there are sub-tabs: 'SIP', 'Features', 'Strobe', and 'Multicast' (selected). The main content area is titled 'Multicast Settings' and is divided into two sections: 'Multicast Mode' and 'Master/Sender Zone Settings'. In the 'Multicast Mode' section, 'Multicast Mode' is set to 'Master/Sender', 'Multicast Type' is 'Regular (RTP)', and 'Number of Zones' is 'Basic Zones Only'. In the 'Master/Sender Zone Settings' section, 'Zone Selection Mode' is 'Single Zone' and 'Master Single Zone' is 'Zone 1'. A 'Save' button is located at the bottom right of the form.

### Multicast Mode (Master/Sender Selected)

If master is enabled the 8138 SIP will broadcast an IP stream when activated and flash a light pattern.

### Multicast Type – Regular

Select 'Regular (RTP)' if solely multicasting to Algo SIP endpoint(s) and/or multicast enabled phone(s) that use RTP audio packets.

### 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 Slave zones, but are hidden by default to simplify the interface.



## Basic Settings Tab – Multicast (Slave Settings)

**Multicast Settings**

**Multicast Mode**

Multicast Mode:  None  Master/Sender  Slave/Receiver  
 ⓘ 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

**Slave/Receiver Zone Settings**

Basic Slave Zones:  Priority Call  All Call  Music  
 Zone 1  Zone 2  Zone 3  
 Zone 4  Zone 5  Zone 6

Expanded Slave Zones:  Zone \*10  Zone \*11  Zone \*12  Zone \*13  Zone \*14  
 Zone \*15  Zone \*16  Zone \*17  Zone \*18  Zone \*19  
 Zone \*20  Zone \*21  Zone \*22  Zone \*23  Zone \*24  
 Zone \*25  Zone \*26  Zone \*27  Zone \*28  Zone \*29  
 Zone \*30  Zone \*31  Zone \*32  Zone \*33  Zone \*34  
 Zone \*35  Zone \*36  Zone \*37  Zone \*38  Zone \*39  
 Zone \*40  Zone \*41  Zone \*42  Zone \*43  Zone \*44  
 Zone \*45  Zone \*46  Zone \*47  Zone \*48  Zone \*49  
 Zone \*50

Select All Clear All

Save

### Multicast Mode (Slave Selected)

If Slave is enabled the 8138 will activate when receiving a multicast message and flash a light pattern.

### Multicast Type – Regular

Select 'Regular (RTP)' if solely receiving from Algo SIP endpoint(s) and/or multicast enabled phone(s) that use RTP audio packets.

The screenshot displays the 'Multicast Settings' page. At the top, there are navigation tabs: Status, Basic Settings (selected), Additional Features, Advanced Settings, System, and Logout. Below these are sub-tabs: SIP, Features, Strobe, and Multicast (selected). The main content area is titled 'Multicast Settings' and is divided into several sections:

- Multicast Mode:** Radio buttons for 'None', 'Master/Sender', and 'Slave/Receiver' (selected). A note indicates that Multicast Zone Definitions can be found in 'Advanced Settings > Advanced Multicast'.
- Multicast Type:** Radio buttons for 'Regular (RTP)', 'Polycom Group Page' (selected), and 'Polycom Push-to-Talk'. A note states that Regular mode uses RTP audio packets compatible with all Algo SIP endpoints and most multicast-enabled phones.
- Polycom Group Paging/ Push-to-Talk:**
  - Polycom Zone:** A text input field containing '224.0.1.116:5001'. A note below it says: 'Enter the same Multicast IP Address & Port number as configured on the Polycom phones.'
  - Polycom Slave Channels:** A grid of radio buttons for Groups 1 through 25. Groups 1, 24, and 25 are checked. Below the grid are 'Select All' and 'Clear All' buttons.

A 'Save' button with a green checkmark is located at the bottom right of the settings area.

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

The 8138 may receive multicast paging compatible with Polycom **“on premise group paging”** protocol.

To configure the 8138 as a slave to receive 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.

## 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 Slave zones, but are hidden by default to simplify the interface.

## Slave Zones

Select one or more multicast zones for the 8138 SIP Strobe Light to monitor. Note that multicast zone priority is based on the zone definition list order (top to bottom).

## Web Interface Additional Features

### Additional Features Tab – Input/Output

The screenshot shows the 'Additional Features' tab in the web interface, specifically the 'Input/Output' section. The interface includes a navigation bar with tabs for 'Status', 'Basic Settings', 'Additional Features', 'Advanced Settings', 'System', and 'Logout'. Below the navigation bar, there are sub-tabs for 'Input/Output', 'Emergency Alerts', 'More Page Extensions', and 'More Ring Extensions'. The 'Input/Output' section is divided into four main areas:

- General:** 'Relay Input Mode' is set to 'Relay Normally Open with Supervision (e.g. Algo 1203 Call Switch)'. Other options include Disabled, Relay Normally Open, Relay Normally Closed, Relay Normally Closed with Supervision, and Algo 1202 Call Button.
- Action When Input Triggered:** The 'Action' is 'Start Flash Pattern' and the 'Start Flash Pattern' is set to '1 - Multi-strobe Fast Amber'.
- Action When Tamper Detected:** 'Wiring Fault Supervision Mode' is set to 'Detect Open Circuit Fault Only'. The 'Action' is 'Start Flash Pattern'. A note states: 'Note that 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.' The 'Start Flash Pattern' is set to '1 - Multi-strobe Fast Amber'.
- Output:** 'Output Relay' is set to 'Enabled'.

A 'Save' button with a green checkmark is located at the bottom right of the form.

#### Input Relay Terminal Function

When triggered by an input relay, the 8138 can flash a light pattern.

#### Relay Input Mode

The input relay to the 8138 SIP Strobe Light can be prompted by any normally open or normally closed switch. For the 8138, Algo offers the 1202 Call Button and the 1203 Call Switch with supervision. Via supervision settings, flash patterns 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 8138, the 1203 can prompt a single action with one-touch, or a continuous action if the button is held.

## 1202 Call Button



The 1202 Call Button is a one-touch button for event notification and response. It can be used with the 8138 for improved customer service, emergency notification, and non-emergency alerting. The Call Button's one-touch button can trigger a flash pattern action, which can be halted via the small cancel/reset button located below the main call button.

## Action when Input Triggered

The relay input may be used to trigger the 8138 SIP Strobe Light only while the input is active.

## Action When Tamper Detected (Supervision)

In addition to the main events, the device can be configured with supervision to also execute a strobe action in case the device goes offline due to wiring failure or after being tampered with. 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.

## Output Relay

Enable or disable the output relay.

## Additional Features Tab – Emergency Alerts

Status
Basic Settings
Additional Features
Advanced Settings
System
Logout

Input/Output
Emergency Alerts
More Page Extensions
More Ring Extensions

### Emergency Alerts

*(i)* This section allows a strobe pattern to be triggered & latched by calling an extension and hanging up. The pattern will continue to flash until a different "Cancel" extension is called to stop the pattern (or a pre-defined timeout is reached). This can be useful for emergency notifications, allowing staff to quickly dial a pre-configured number and then exit the building.

*(i)* Up to 10 extensions can be registered allowing up to 10 different flash patterns. A single "Cancel" extension also needs to be registered; calling this number will cancel the currently active flash pattern.

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

**Settings**

Announcement Duration  Play Once  Play Until Cancelled

Maximum Announcement Time 10 minutes ▾

Answer Inbound Call  Enabled  Disabled

*(i)* 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.

*(i)* 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.

*(i)* Select "Disabled" to detect just the inbound Ring signal, but not actually answer the call

**Call-to-Cancel**

Extension	
Authentication ID	
Authentication Password	
Display Name (Optional)	

**Announcements**

Announcement 1  Enabled  Disabled

Announcement 2  Enabled  Disabled

Emergency Alerts allow for an announcement (chosen strobe to be triggered & latched by calling a pre-configured Emergency extension and hanging up. The announcement will continue to flash a light pattern until a different "Cancel" extension is called to clear the announcement (or a defined timeout is reached). The 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.

If the "Answer Inbound Call" option is "Enabled" the call is auto-answered and a confirmation tone is played through multicast (if configured) 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 stay active 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 extensions (including this device), the auto-answer may intercept that call and prevent it from ringing on other devices.

Up to 10 extensions can be registered allowing up to 10 different announcements.



*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.*



*Note: The 8138 does not have speaker mounted. If using both Algo audio and visual devices, both audible and visual alerting can be achieved.*

## Additional Features Tab – More Page Extensions

Status
Basic Settings
Additional Features
Advanced Settings
System
Logout

Input/Output
Emergency Alerts
More Page Extensions
More Ring Extensions

### More Page Extensions

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

- i The 8128 will auto-answer any inbound calls received on these numbers and provide a voice paging path and multicast if configured. Note that only a single call can be active at a time.
- i 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.
- i Multicast Zone Definitions can be found in "Advanced Settings > [Advanced Multicast](#)".

#### Basic Extensions

Priority Call Page Extension	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extension	<input style="width: 100%;" type="text"/>
Authentication ID	<input style="width: 100%;" type="text"/>
Authentication Password	<input style="width: 100%;" type="password"/> <span style="float: right; color: #0070C0;">🔑</span>
Display Name (Optional)	<input style="width: 100%;" type="text"/>
Strobe Pattern	<Use Default Strobe Pattern> ▾

All Call Page Extension  Enabled  Disabled

Zone 1 Page Extension  Enabled  Disabled

Zone 2 Page Extension  Enabled  Disabled

Zone 3 Page Extension  Enabled  Disabled

Zone 4 Page Extension  Enabled  Disabled

Zone 5 Page Extension  Enabled  Disabled

Zone 6 Page Extension  Enabled  Disabled

Music Page Extension  Enabled  Disabled

#### Expanded Extensions

Zone 10 Page Extension  Enabled  Disabled

Zone 11 Page Extension  Enabled  Disabled

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 (e.g. speed-dial keys can be used), but may require additional SIP licenses depending on the SIP provider.

To configure additional page extensions (up to 50) click “Enable” beside the target extension and enter the Extension, Authentication ID, and Authentication password.

The 8138 will auto-answer any inbound calls received on these numbers and provide a voice paging path and multicast if configured.



*Note: that only a single call can be active at a time.*

## Additional Features Tab – More Ring Extensions

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

Input/Output Emergency Alerts More Page Extensions **More Ring Extensions**

### More Ring Extensions

**i** This section allows additional extensions to be registered for the purpose of providing loud ringing alerts for more than one line. Unique flash patterns can be selected for each line to allow them to be easily distinguished. Appropriate call routing must be configured on your SIP phone system of course in order to trigger it to send calls to these different numbers.

**i** The 8128 will detect inbound ring events on these numbers and activate the strobe light until the inbound call stops ringing. It will not answer the calls in this mode.

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

Ring Extension 2	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extension	<input type="text"/>
Authentication ID	<input type="text"/>
Authentication Password	<input type="password"/>
Display Name (Optional)	<input type="text"/>
Strobe Pattern	<Use Default Strobe Pattern>
Multicast Zone	<Use Default Multicast Zone>
Ring Extension 3	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Ring Extension 4	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Ring Extension 5	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Ring Extension 6	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Ring Extension 7	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Ring Extension 8	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Ring Extension 9	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Ring Extension 10	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Save

Up to 10 SIP Ring extensions can be registered. To configure additional ring extensions, click “Enable” beside the target extension and enter the Extension, Authentication ID, and Authentication password. A unique Ring Tone can be assigned to each extension if desired.



## Web Interface Advanced Settings

### Advanced Settings Tab – Network

The screenshot displays the 'Advanced Settings' tab for the 'Network' section. The 'Network Settings' panel is expanded, showing several configuration areas:

- Network Interface:** Internet Protocol is set to 'IPv4 and IPv6'. DHCP is checked as 'Enabled'.
- 802.1Q Virtual LAN:** VLAN Mode is set to 'Auto'.
- 802.1X Port-based Network Access Control:** 802.1X Authentication is checked as 'Disabled'.
- Differentiated Services:** SIP (6-bit DSCP value), RTP (6-bit DSCP value), and RTCP (6-bit DSCP value) are all set to '0'. Each field has a tooltip indicating 'Valid values range from 0 to 63'.
- DNS:** DNS Caching Mode is checked as 'Disabled'. A tooltip explains: '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.'

A 'Save' button with a green checkmark is located at the bottom right of the settings panel.

#### Protocol

DHCP is an IP standard designed to make administration of IP addresses simpler. When selected, DHCP will automatically configure IP addresses for each 8138 on the network. Alternatively, the 8138 can be set to a static IP address.

## 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 0xFF 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. On bridges, VLAN 1 (the default VLAN ID) is often reserved for a management VLAN; this is vendor specific.

## 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 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.

## Differentiated Services (6-bit DSCP value)

Provides quality of service if the DSCP protocol is supported on your network. Can be specified independently for SIP control packets versus RTP audio packets.

## 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.

## Advanced Settings Tab – Admin

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

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

### Admin Settings

**Admin Password**

Password

Confirmation

**General**

Device Name (Hostname)

Introduction Section on Status Page  On  Off

Show Status Section on Status Page when Logged Out  On  Off

Display Switch Port ID on Status Page  On  Off  
Requires the device to be connected to a switch that supports LLDP or CDP.

Web Interface Session Timeout   
Automatically log out web interface after period of inactivity.

Play Tone at Startup  Enabled  Disabled  
A tone can be played at startup to confirm that the device has booted.

**Log Settings**

Log Level  Error (Lowest)  Notice ("Event")  Info ("SIP")  Debug (Highest)

Log Method  Local  Network  Both

**Management**

Web Interface Protocol  Both HTTP and HTTPS  HTTPS Only

Force Strong Password  Enabled  Disabled

Allow Secure SIP Passwords  Enabled  Disabled  
After enabling this option, it is recommended to re-enter SIP passwords and their corresponding realm to store the passwords securely.

**Simple Network Management Protocol**

SNMP Support  Enabled  Disabled  
Download MIB file [here](#).

**System Integrity**

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

**InformaCast**

InformaCast Support  Enabled  Disabled  
This feature requires a valid license to be activated. Please contact [sales@algosolutions.com](mailto:sales@algosolutions.com) for assistance.

Save

## Password

Password to log into the 8138 SIP Strobe Light web interface. You should change the default password **algo** in order to secure the device on the network. If you have forgotten your password, you will need to perform a reset using the Reset Button in order 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.

## 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

Switch port ID can be displayed on the status page, however the switch must support LLDP or CDP.

## Web Interface Session Timeout

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

## Log Level

Use on the advice of Algo technical support only.

## Log Method

Allows the 8138 to write to external Syslog server if the option for external (or both) is selected.

## Log Server

If external (or both) is selected this is the address of the Syslog server on the network.

## Web Interface Protocol

HTTPS is always enabled on the device. Use this setting to disable HTTP. When HTTP is disabled, requests will be automatically redirected to HTTPS. Also note that since the

device can have any address on the local network, no security certificate exists, and thus most browsers will provide a warning when using HTTPS.

## Force Strong Password

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

- Must contain at least 10 characters
- Must contain at least 1 uppercase character
- Must contain at least 1 digit (0 – 9)
- Must contain at least 1 special character

## Allow Secure SIP Password

Allows SIP passwords to be stored in the configuration file in an encrypted format, to prevent viewing and recovery. Once enabled, the SIP "Realm" field should be entered and all the configured Authentication Password(s) must be re-entered in the Basic Settings > SIP tab, and any other locations where SIP extension 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.

## SNMP Support

Additional SNMP support is anticipated for future, but the 8138 SIP Strobe Light will respond to a simple status query for automated supervision. Contact Algo technical support for more information.

## 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 page.

## Local Management Port

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

## InformaCast Support

This feature requires a valid InformaCast license to be activated. Please contact [sales@algosolutions.com](mailto:sales@algosolutions.com) for assistance.

## Advanced Settings Tab – Time

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

### Time Zone

Select time zone.

### NTP Time Servers 1/2/3/4

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

### NTP Time Server Source

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 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.

## Manually Override Time

For testing purpose, you may also override the time setting.



*Note: This time value will be lost at power down, or overwritten if NTP is currently active. Time and date are used only for logging purposes and are not typically required.*

## Advanced Settings Tab – Provisioning

Status
Basic Settings
Additional Features
Advanced Settings
System
Logout

Network
Admin
Time
Provisioning
Advanced Audio
Advanced SIP
Advanced Multicast

### Provisioning Settings

**Mode**

Provisioning Mode  Enabled  Disabled

**Settings**

Server Method

- Auto (DHCP Option 66/160/150)
- DHCP Option 66 only
- DHCP Option 160 only
- DHCP Option 150 only
- Static

**i** Auto mode automatically checks all 3 DHCP options for an active provisioning server, in the order listed.

Static Server

Download Method  TFTP  FTP  HTTP  HTTPS

Config Download Path

Firmware Download Path

Partial Provisioning  Enabled  Disabled

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



*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.*

Provisioning allows installers to pre-configure 8138 SIP Strobe Light units prior to installation on a network. It is typically used for large deployments to save time and ensure consistent setups.

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.

For example, 8138 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 8138 Strobes)                      **algot8138.conf**

Specific (for a specific MAC address)                      **algot[MAC].conf**

Both protocol and path is supported for Option 66, allowing for <http://myserver.com/config-path> to be used.

## MD5 Checksum

In addition to the **.conf** file, an **.md5** checksum file must also be uploaded to the Provisioning server. 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 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

1. Connect 8138 to the network
2. Access the 8138 Web Interface Control Panel
3. Configure the 8138 with desired options
4. Click on the System tab and then Maintenance.
5. Click “Download” to download the current configuration file
6. Save the file settings.txt
7. Rename file settings.txt to algot8138.conf
8. File algot8138.conf can now be uploaded onto the Provisioning server



If using a generic configuration file, extensions and credentials have to be entered manually once the 8138 SIP Strobe Light has automatically downloaded the configuration file.

### Generating a specific configuration file

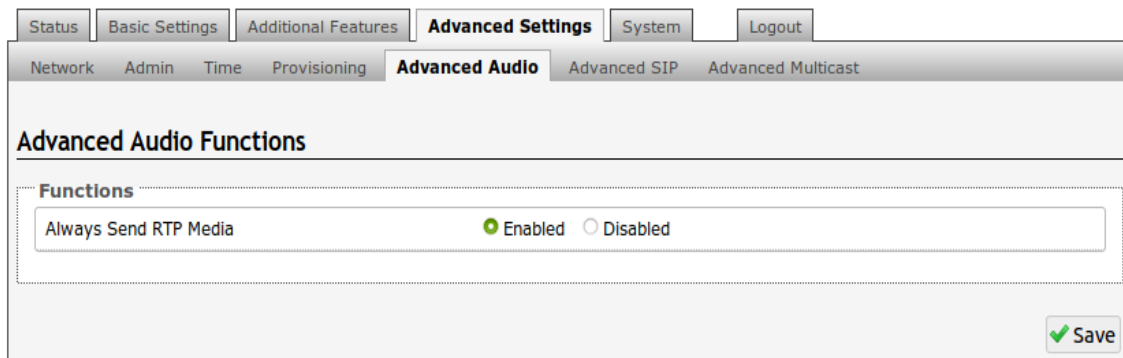
1. Follow steps 1 to 6 as listed in the section “Generating a generic configuration file”.
2. Rename file settings.txt to algom[MAC address].conf (e.g. algom0022EE020009.conf)
3. File algom[MAC address].conf can now be uploaded on the Provisioning server.

The specific configuration file will only be downloaded by the 8138 with the MAC address specified in the configuration file name. Since all the necessary settings can be included in this file, the 8138 will be ready to work immediately after the configuration file is downloaded. The MAC address of each 8138 Strobe can be found on the back label of the unit.

For more Algo SIP endpoint provisioning information, see:

[www.algosolutions.com/provision](http://www.algosolutions.com/provision)

## Advanced Settings Tab – Advanced Audio



### Always Send RTP Media

If enabled, audio packets will be sent at all times while a call is active. This option is needed in cases when the server expects to see audio packets at all times.

## Advanced Settings Tab – Advanced SIP

Status
Basic Settings
Additional Features
Advanced Settings
System
Logout

Network
Admin
Time
Provisioning
Advanced Audio
Advanced SIP
Advanced Multicast

### Advanced SIP Settings

**General**

SIP Transportation	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Auto</div> <p><small>④ Select Auto to check DNS NAPTR record, then try UDP/TCP. ④ 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 &gt; File Manager" tab to upload a certificate file renamed to 'sipclient.pem' in the 'certs' folder.</small></p>
SIPS Scheme	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Validate Server Certificate	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <p><small>④ Validate the SIP server against common certificate authorities. To validate against additional certificates, use the "System &gt; File Manager" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder.</small></p>
Force Secure TLS Version	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <p><small>④ Enable this option to require TLS connections to use TLSv1.2.</small></p>
SDP SRTP Offer	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Disabled</div>
SIP Outbound Support (RFC 5626)	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <p><small>④ 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.</small></p>
Outbound Proxy	<input style="width: 100%;" type="text"/>
Register Period (seconds)	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">3600</div>

**NAT**

Media NAT  None  ICE  STUN

**Server Redundancy**

Server Redundancy Feature (Multiple SIP Server Support)  Enabled  Disabled

**Interoperability**

Keep-Alive Method	<input checked="" type="radio"/> None <input type="radio"/> Double CRLF <p><small>④ This setting will enable sending periodic CRLF messages for both UDP and TCP connections.</small></p>
Use Outgoing TLS port in SIP headers	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled <p><small>④ Use ephemeral port number from outgoing SIP TLS connection instead of listening port number in SIP Contact and Via headers. This is useful to connect the device to some local SIP servers, like Asterisk or FreeSWITCH.</small></p>
Do Not Reuse Authorization Headers	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <p><small>④ When enabled, all SIP authorization information from the last successful request will not be reused in the next request.</small></p>
Allow Missing Subscription-State Headers	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <p><small>④ When enabled, allow SIP NOTIFY messages that do not contain a "Subscription-State" header.</small></p>

✔ Save

### 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.

## 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.

## 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 8138 SIP Strobe Light will re-register with the SIP server. Default setting is 3600 seconds (1 hour). Only change if instructed otherwise.

## Media NAT

IP address for STUN server if present or IP address/credentials for a TURN server.

## Server Redundancy Feature

Two secondary SIP servers may be configured. The 8138 SIP Strobe Light will attempt to register with the primary server but switch to a secondary server if necessary. The configuration allows re-registration to the primary server upon availability or to stay with a server until unresponsive.

## Backup Server #1

Only visible if 'Server Redundancy Feature' is enabled. If primary server is unreachable the 8138 SIP Strobe Light will attempt to register with the backup servers. If enabled, the 8138 will always attempt to register with the highest priority server.

## Backup Server #2

Only visible if 'Server Redundancy Feature' is enabled. If backup server #1 is unreachable the 8138 SIP Strobe Light will attempt to register with the 2nd backup server. If enabled, the 8138 will always attempt to register with the highest priority server.

## **Polling Intervals (seconds)**

Only visible if 'Server Redundancy Feature' is enabled. 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**

Only visible if 'Server Redundancy Feature' is enabled. Explicitly poll current server to monitor availability. May also be handled automatically by other regular events, so can be disabled to reduce network traffic.

## **Automatic Failback**

Only visible if 'Server Redundancy Feature' is enabled. Reconnect with higher priority server once available, even if backup connection is still fine.

## **Polling Method**

Only visible if 'Server Redundancy Feature' is enabled. SIP message used to poll servers to monitor availability.

## **Keep-alive Method**

If Double CRLF is selected the 8138 will periodically send a CRLF message for both UDP and TCP connections to maintain connection with the SIP Server.

## **Keep-alive Interval**

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 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.

## Advanced Settings Tab – Advanced Multicast

**Advanced Multicast Settings**

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

**RTP Control Protocol (RTCP)**

RTCP Port Selection

Disabled  Next Higher Port  Multiplexed on Same Port

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

**Basic Zone Definition**

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

**Expanded Zone Definition**

Zone	IP Address and Port
Zone 10 (DTMF: *10)	224.0.2.110:50000
Zone 11 (DTMF: *11)	224.0.2.111:50000

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

### 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.

### Zone Definition

The "Expanded" Slave or Master zones can be enabled/disabled in Basic Settings > Multicast. Default IP addresses and ports may be revised for any given zone in the table.



**Important:** Ensure that the Address and Port settings are the same for all master and slave devices.

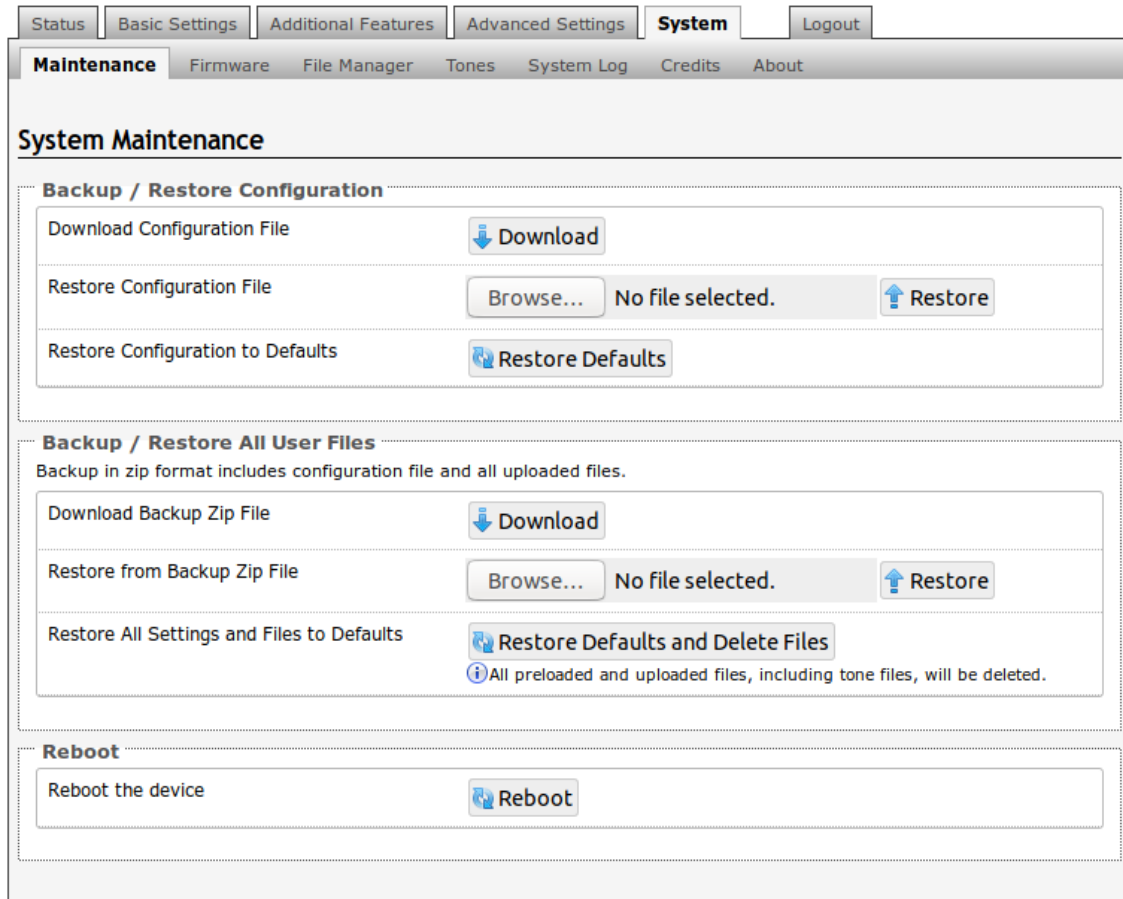
### Strobe Pattern

When the 8138 Strobe Light is the multicast Slave, a strobe pattern will flash each time a multicast stream is detected.

By default, the same flash pattern can be set for all Slave zones in the Basic Settings > Features tab. Unique flash patterns may be revised on a per-zone basis in the table above. For instance, emergency pages can be different on certain Slave strobes.

## Web Interface System

### System Tab – Maintenance



**System Maintenance**

**Backup / Restore Configuration**

Download Configuration File

Restore Configuration File  No file selected.

Restore Configuration to Defaults

**Backup / Restore All User Files**

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

Download Backup Zip File

Restore from Backup Zip File  No file selected.

Restore All Settings and Files to Defaults   
All preloaded and uploaded files, including tone files, will be deleted.

**Reboot**

Reboot the device

#### 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 8138 SIP Strobe Light device settings to factory default values.

#### Download Backup 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 the Device

Reboots the device.

## System Tab – Firmware

The screenshot shows the 'Firmware' page within the 'System' tab. The page has a navigation bar with tabs: Status, Basic Settings, Additional Features, Advanced Settings, System (selected), and Logout. Below the navigation bar are sub-tabs: Maintenance, Firmware (selected), File Manager, Tones, System Log, Credits, and About. The main content area is titled 'Firmware' and contains three sections: 'Installed Firmware', 'Online Upgrade', and 'Custom Upgrade'. The 'Installed Firmware' section lists three items: Product Firmware (algo-8138-3.1), Base Firmware (Linux Kernel and Boot Utilities) (algo-pb-base-3.1), and System Firmware (Debian System Packages) (algo-pb-sys-3.1). The 'Online Upgrade' section has a 'Check for Firmware Updates' button and a 'Check' button. The 'Custom Upgrade' section has a 'Method' section with radio buttons for 'From Local Files' (selected) and 'From URL'. Below this is a 'Signed Firmware File' section with a 'Browse...' button and the text 'No file selected.'. There is also an 'Allow Downgrade' section with radio buttons for 'Enabled' and 'Disabled' (selected). Below this are two informational messages: one with an 'i' icon stating 'Allow product or base firmware to be downgraded to an older version.' and one with a warning icon stating 'Enabling this option could cause upgrade issues. Please contact support if necessary.'. At the bottom of the 'Custom Upgrade' section is an 'Upgrade' button.

## Method

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

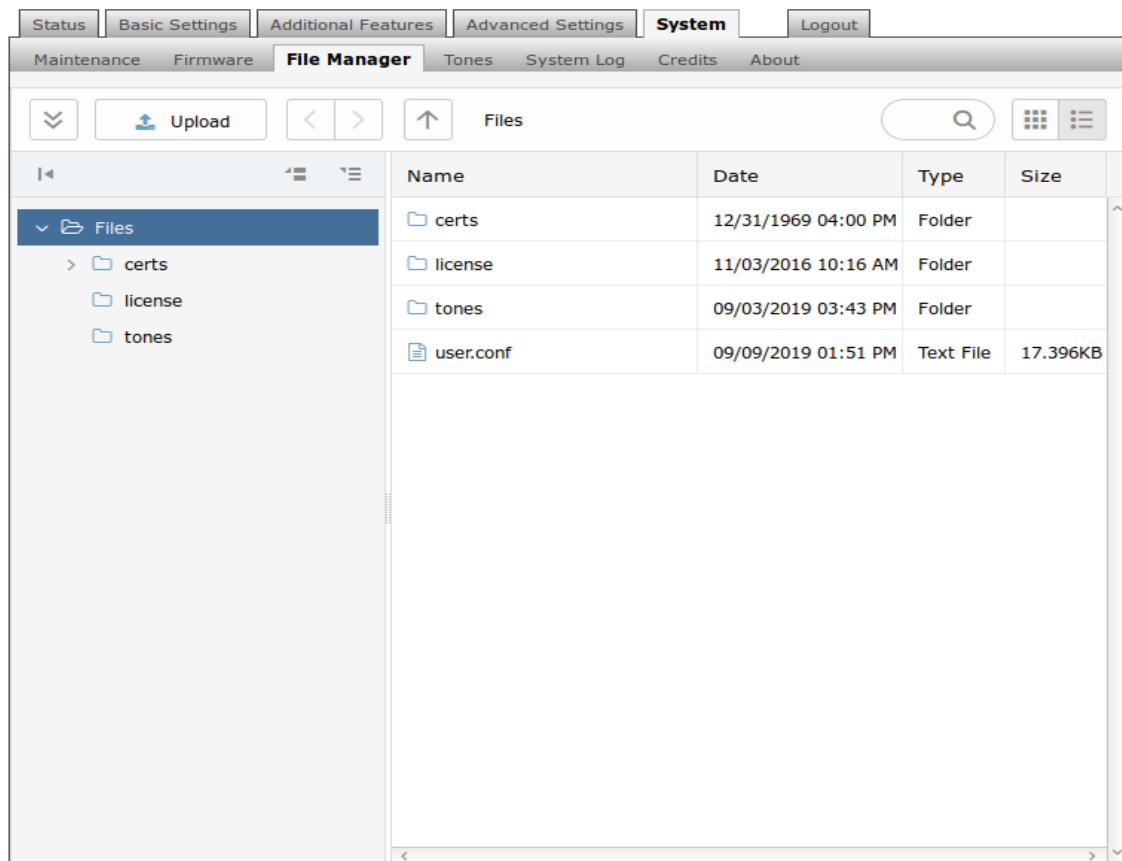
## Signed Firmware File

Point to the SFW file provided by Algo

## How To Upgrade 8138 SIP Strobe Light Firmware

1. From the top menu, click on System, then Firmware.
2. In the Upgrade section, click on Choose File and select the 8138 strobe firmware file to upload. Note that a SFW file must be loaded.
3. Click Upgrade
4. After the upgrade is complete, confirm that the firmware version has changed (refer to top right of Control Panel).

## Advanced Settings Tab – File Manager



### Uploading Certificate Files

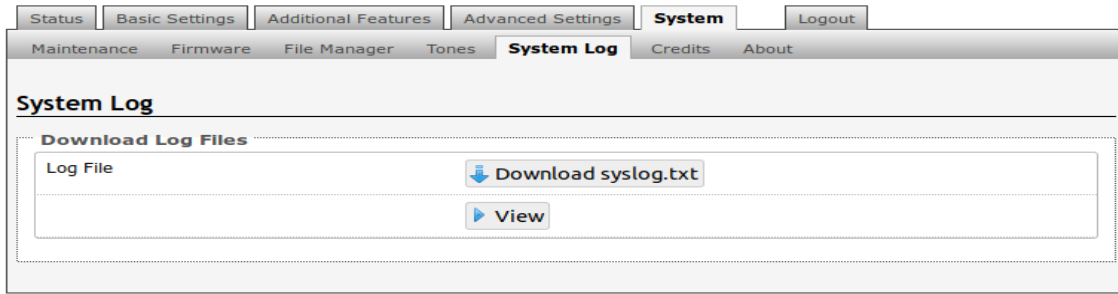
To use TLS SIP Signaling and provisioning, the certificate is required for a SIP server to validate the Algo device.

The TLS certificate can be uploaded to the certs folder. Rename the certificate to 'sipclient' using '.pem' filetype extension before uploading.

For the HTTPS provisioning, a certificate can also be manually uploaded into the certs folder through file manager.



## System Tab – System Log



System log files are automatically created and assist with troubleshooting in the event the 8138 SIP Strobe Light does not behave as expected.

## Wiring Connections

### Network Connection

The strobe 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 48V 350 mA IEEE 802.3at PoE+ or 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.

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.

### Connecting Input Devices

The dry contact relay on the 8138 SIP Strobe Light can be prompted by any normally open, normally closed switch, Algo 1202 Call Button and Algo 1203 Call Switch. The input switches can be connected to the back of the back of the 8138 via the "IN".

Connection options can be configured from normally open switch, to normally closed switch, to Algo 1202 Call Button with large blue button, to Algo 1203 single gang backlit Call Switch, or as an EOL resistor termination. The connection options can then be configured to complete an 'Action' when Relay Input is triggered.



*Note: See "Additional Features Tab – Input/Output" section of this user doc for additional information on input device configuration*

## Specifications

- Power Input:** 48V PoE IEEE 802.3af Class 0 (Max 12.95 W)  
Idle nominal 1W
- Strobe Triggers:** SIP extension ring, Subscribe/Notify, multicast, dry contact input
- SIP:** Multiple extensions for Page or Alerting
- Audio Memory:** 1 GByte available
- Relay Output:** Normally open, activated when 8138 is in use  
Max 30 V 50 mA
- Relay Input:** Normally open or normally closed dry contact,  
Algo 1202 Call Box, Algo 1203 Wall Switch, EOL termination
- Flash Patterns:** 15 Selectable Patterns

**Relay Input Current Draw Detection Thresholds:**

	Active	Idle	Tamper
<b>Normally Open</b>	>4mA	<4mA	N/A
<b>Normally Open with Supervision</b>	>20mA	4-20mA	<4mA
<b>Normally Closed</b>	<4mA	>4mA	N/A
<b>Normally Closed with supervision</b>	4-20mA	>20mA	<4mA

Nominal 12V source, current limited to 40mA  
Typical supervision resistor value = 1k ohm

- Configuration:** Web interface or provisioning
- Provisioning:** TFTP, FTP, HTTP, HTTPS
- Supervision:** SNMP
- NAT:** STUN, CRLF Keep Alive
- Processor:** Linux OS ARM Cortex-A8 32-Bit RISC Processor
- Environmental:** -20°C to +50°C; 10-95% RH non-condensing. Dry indoor location only unless wiring cavity protected from water ingress.
- Compliance:** EN60950:2001, IEEE 802.3-2008, RFC3261, RoHS, CE, FCC, CSA (USA & Canada)

## FCC Compliance Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation 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 own expense.