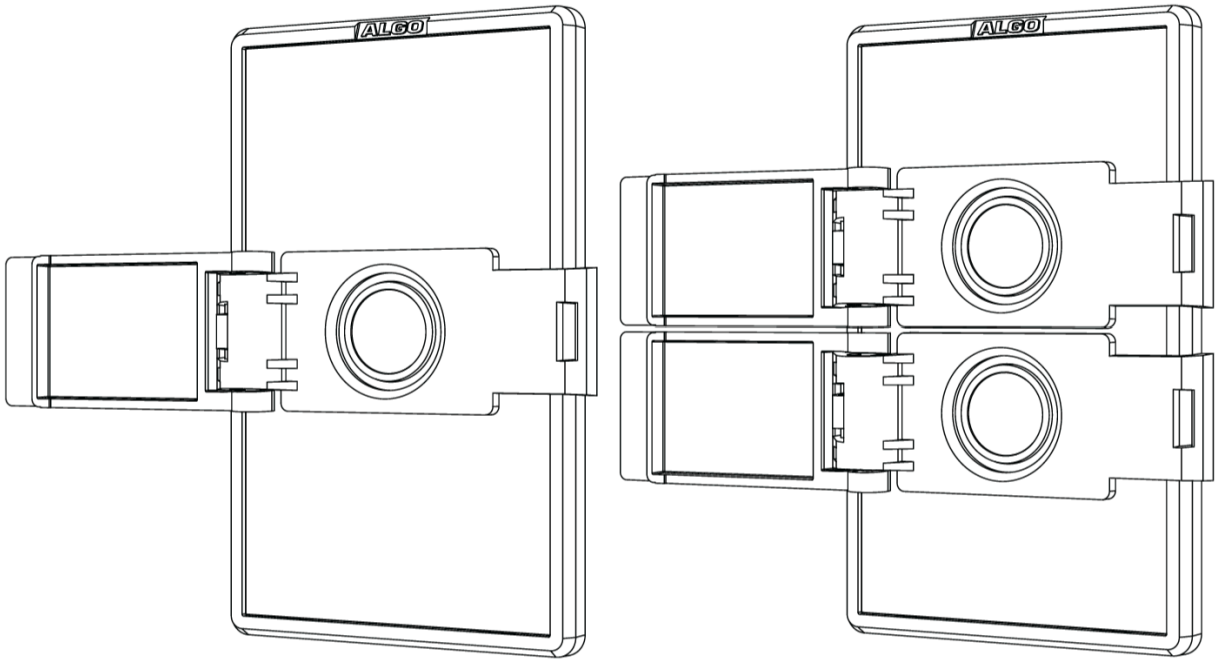
Algo 8211 IP Single Button and 8212 IP Dual Button User Guide

Updated on Oct 8, 2026 • Published on Aug 12, 2026

67 minute(s) read

Focus

Article summary



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:
1-604-454-3792
support@algosolutions.com

About

The Algo 8211 IP Single Button and Algo 8212 IP Dual Button are standalone IP buttons that connect directly to the network and initiate configurable actions. The 8211 IP Single Button contains one button and the 8212 contains two buttons. Each button supports two separate configurable actions—press and long press—giving the 8211 a total of two configurable actions and the 8212 a total of four.

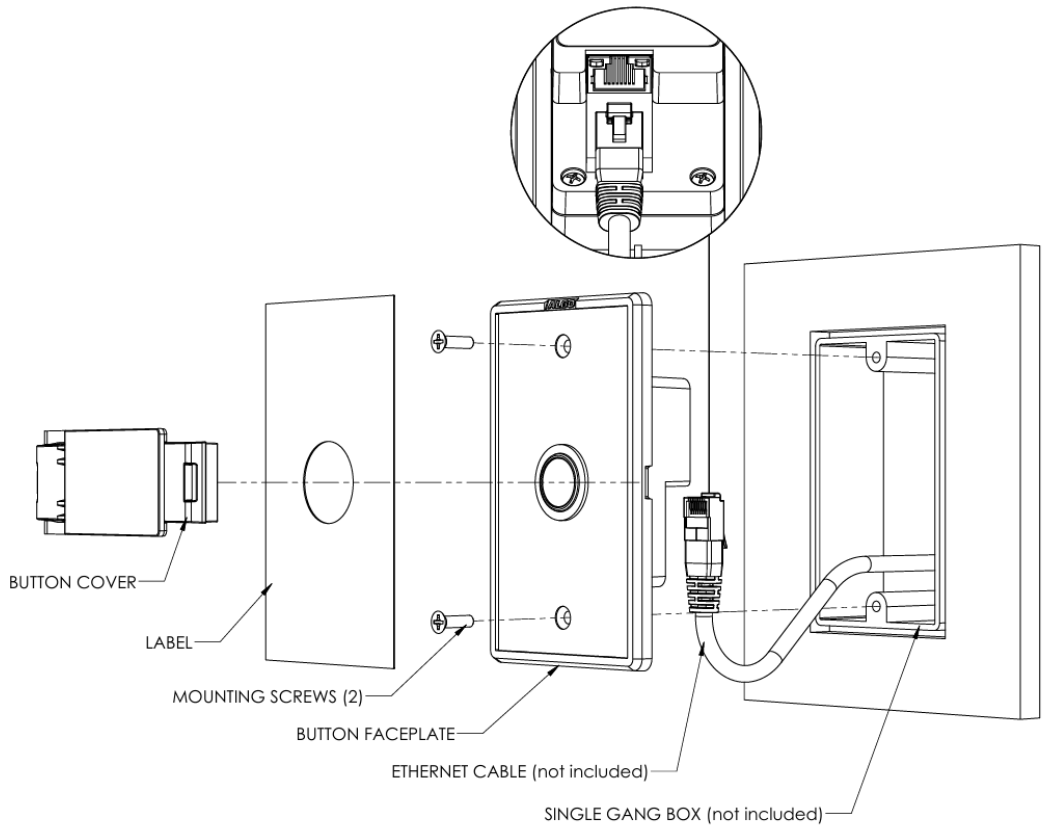
The 8211 and 8212 buttons are designed to be customized for each deployment's specific needs, featuring configurable multi-color illuminated button(s), selectable faceplate labels for unique colors and text, and optional protective cover(s) to prevent unintentional button presses.

As standalone IP endpoints, the 8211 and 8212 buttons can be deployed wherever a network connection is available, providing independent device management, direct SIP registration, and device-level monitoring. The buttons can be configured as operational buttons or fully supervised panic buttons to initiate a defined communication or alert workflow. If configured as a panic button, the Algo Device Management Platform (ADMP) can provide centralized visibility into device status, connectivity, and operational readiness.

What is Included

8211 IP Single Button	8212 IP Dual Button
• Algo 8211 IP Single Button • Optional button cover • Labels (x5) • Mounting screws (x2)	• Algo 8212 IP Dual Button • Optional button covers (x2) • Labels (x3) • Mounting screws (x2)

Installation



Note

- Install the 8211/8212 and test functionality before applying the faceplate label. This label covers the mounting screws and is difficult to remove once applied.
- This product is designed for indoor dry environments only.

1. Connect the 8211/8212 to an IEEE 802.3af-compliant PoE network switch. The button illuminates steady blue until boot-up is completed (about 1 minute). When startup is complete, the button illumination turns off.
2. Attach the 8211/8212 to a single-gang box or low-voltage bracket using the provided flat-head screws.

   Ensure the end with the **Algo** logo is at the top.

   Note

   Do not attach the faceplate label until functional testing is complete. Refer to the **Getting Started** section for more details.

3. Select the preferred faceplate label. Peel off the adhesive backing from the faceplate label and apply it to the 8211/8212 button. Ensure the label is aligned to the edge of the label indent to ensure a proper fit. After positioning the label, apply firm, even pressure across the entire surface, including the edges and corners, to ensure proper adhesion and a long-lasting bond.
   If customized product labels are required, please contact Algo Support (support@algosolutions.com).
4. (Optional) Install the button cover by aligning it with the slots on the outside edges of the faceplate, then press down firmly along the left and right edges until the button cover snaps into place.

   > **Note**
   >
   > If the button cover(s) need to be removed, insert a small screwdriver into the slot on the hinge side of the button cover to pry the cover snap away from the faceplate.

Assembling the Button Cover

The button cover consists of two pieces (Button Frame and Button Cover) and is pre-assembled. In case you need to assemble it yourself, follow this procedure.

To assemble the button cover:

1. Place the Button Frame (the piece with the circular hole) with the curved ends facing upward. Position the Button Cover so the recessed side faces downward.
2. Insert the hinge-channel end of the Button Frame into the opening of the Button Cover, then align the axle with the two short guide channels.
3. Hold the two pieces at approximately 90 degrees to each other, then press both ends of the axle on the Button Cover piece until it snaps fully into the guide channels on the Button Frame.
4. Open and close the Button Cover to verify smooth movement and proper alignment.

Getting Started

This section walks you through the basic steps to get started with the device, including locating its IP address, accessing the web interface, securing the login password, and

configuring a basic button action. Complete these steps before configuring additional device features and integrations.

Obtaining the Device IP Address

You will need the device IP address to access its web interface. You can find the device IP address using one of the following methods:

- Use Algo Network Device Locator Tool.
- Use other network discovery methods.

Alternative Methods to Obtain Device IP

Alternatively, use one of the following methods to find devices on your local network and identify their IP and MAC addresses. All Algo devices have a MAC address starting with 00:22:ee. Use this prefix to quickly identify your Algo devices.

- Log in to your router or DHCP server and check the DHCP client list.
- Use a network scanning tool.
- Use a network management software to view DHCP-assigned IPs.
- Open a terminal or command prompt and check your ARP table:
  - **Windows:** `arp -a`
  - **Linux/macOS:** `arp -a` or `ip neigh`

Accessing the Web Interface

You can configure the device through its web interface. All settings, integrations, and file uploads can be accessed via the web interface.

To access the device web interface:

1. Enter the device IP address into your web browser.
2. Enter the login password and select **Login**.

The default login password is *algo*.

> **Note**
>
> This password can be changed in **Advanced Settings** → **Admin** tab after you log in for the first time. It is highly recommended to change the default password if the device is directly connected to a public network.

Changing the Login Password

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

To change the login password:

1. Go to **Advanced Settings** → **Admin** → **Admin Password.**
2. Enter the **Old Password**.
3. Enter your new **Password**.
4. Repeat the new password in **Confirmation**.
5. Select **Save**.

   The device reboots to apply the new setting.

Login Password Requirements

The login password requirements depend on the **Force Strong Password** setting.

> **Note**

> Before you can enable the strong password, your current login password must meet the strong password requirements listed below. If it does not, change your login password first.

Force Strong Password Enabled	Force Strong Password Disabled
• Must contain at least 10 characters • Must contain at least 1 uppercase character • Must contain at least 1 lowercase character • Must contain at least 1 digit (0 – 9) • Must contain at least 1 special character	• Must contain at least 1 character

To enable strong password:

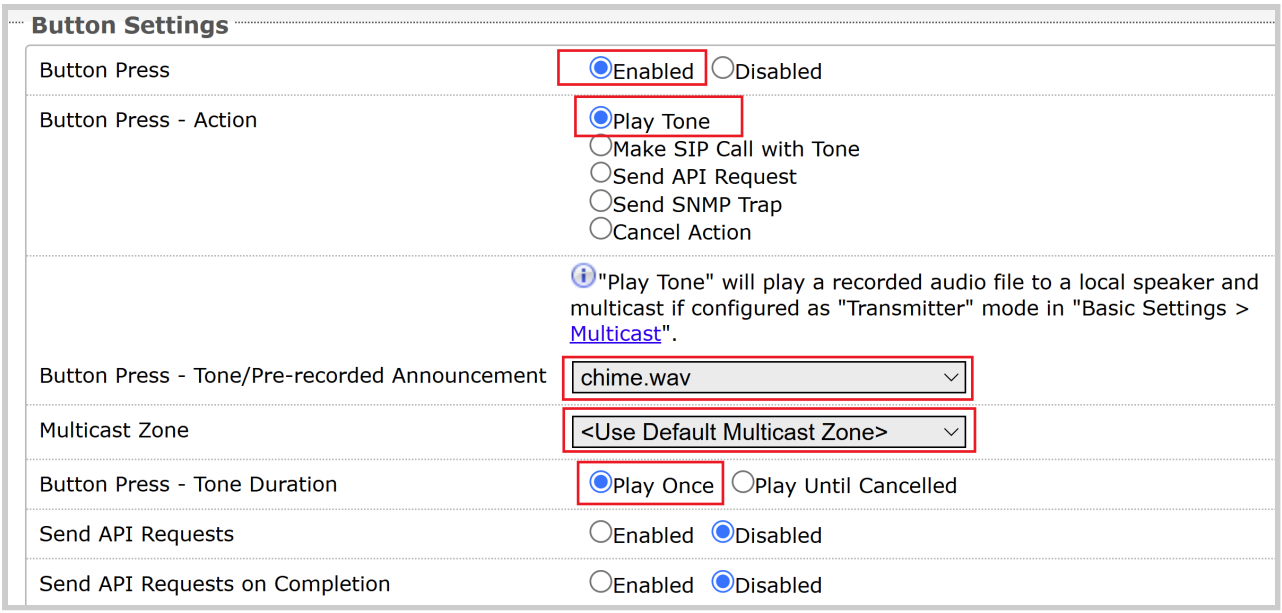
1. Go to **Advanced Settings** → **Admin** → **Management.**
2. Set **Force Strong Password** to **Enabled.**
3. Select **Save**.

Triggering Your First Button Action

This procedure demonstrates the minimum configuration required to configure a button action on the 8211.

To trigger your first button action:

1. Go to **Basic Settings** → **Button Settings** and configure the following:



- **Button Press**: Set to **Enabled**.
- **Action**: Set to **Play Tone**.
- **Tone/Pre-recorded Announcement**: Accept the default tone or select one.
- **Multicast Zone**: Accept the default zone or select one.
- **Tone Duration**: Set to **Play Once**.

2. Select **Save**.
3. Press the button.

   By default, the button ring illuminates steady red to indicate the active state.

   If there are IP speakers configured as multicast receivers in your deployment, the speakers play the tone.

Device Status

The web interface has a **Status** page which, by default, is available both before and after login.

Depending on your device configuration and firmware version, the **Status** page may display the following information:

• Device Name • SIP Registration • Call Status • Proxy Status • Provisioning Status	• Multicast Mode • Panic Button Status • OAuth Profile Status • ADMP Cloud Monitoring

• MAC • IPv4 • IPv6 • Switch Port ID • Date/Time	

Restricting the Status Page to Logged-In Users

The **Status** page can be restricted to logged-in users.

To restrict the Status page to logged-in users:

1. Go to **Advanced Settings** → **Admin** → **General**.
2. Set **Show Status Section on Status Page when Logged Out** to **Off**.
3. Select **Save**.

Customizing Your Status Page

You can customize the content of the **Status** page.

To customize your status page:

1. Go to **Advanced Settings** → **Admin**.
2. Configure the **General** section:
   - **Introduction Section on Status Page**: Select whether to show the introduction text on the **Status** page.
   - **Display Switch Port ID on Status Page**: Select whether to display the switch port ID on **Status** page.
3. Select **Save**.

Register Your Product

Register your product to receive the latest firmware and product updates, important service notifications, and a 3-year extended warranty for IP products.

To register your product:

- Do one of the following:
  - Go to https://www.algosolutions.com/product-registration/.
  - Scan this QR code:

Security

Algo devices use TLS for provisioning and SIP signaling to help protect against cyberattacks that attempt to intercept, replicate, or alter Algo products. Algo devices also come pre-loaded with certificates from a list of trusted certificate authorities (CA) to ensure secure communication with reputable sources. Pre-installed trusted certificates are not visible to users and are separate from those in the '**certs**' folder under **System** → **File Manager**.

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

Configuring SIP Extension

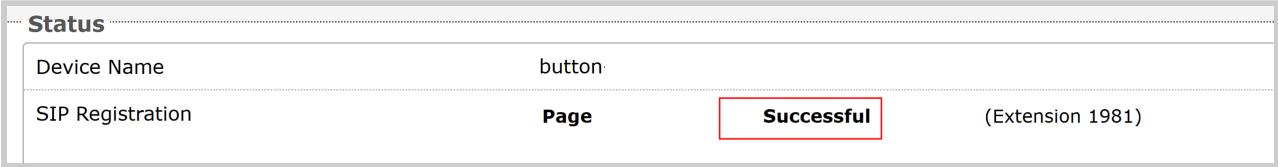
You can configure SIP registration to place SIP calls to other devices.

To configure SIP registration:

1. Go to **Basic Settings** → **SIP**.

2. Enter the SIP server IP address or domain name in **SIP Domain (Proxy Server)**.
3. Configure the following:
    - **SIP Extension**
    - **Authentication ID**

      Note that some SIP servers may use the term **Username** instead of **Authentication ID**.
    - **Authentication Password**
4. Select **Save**.
5. Go to the **Status** page and make sure that the SIP registration is successful.



Related Links:

- Configuring the Button to Make a SIP Call with a Tone

Configuring Button Actions

You can configure the 8211/8212 button to trigger an action when the button is pressed or long-pressed. The 8212 provides two independently configurable buttons.

The available button actions allow the 8211/8212 to initiate multicast (with preconfigured audio file), make outgoing SIP calls, Initiate InformaCast scenarios, send API requests or SNMP notifications, or cancel an active action.

> **Note**
>
> Button configuration procedures use the 8211 as an example. You can use them as a reference when configuring a button action on the 8212; however, the 8212 user interface differs slightly.

Understanding Button Press and Long Press Actions

Each button can respond differently depending on how you operate it:

- **Press**: Triggers the action when the button is pressed normally.
- **Long Press**: Triggers a separate action when the button is held for the configured **Button Hold Time (seconds)**.

On the 8211, you can configure one **Press** action and one **Long Press** action.

On the 8212, the top and bottom buttons are configured independently. Each button can have its own **Press** and **Long Press** actions. This allows a single 8212 to provide up to four different button actions.

For example, you could configure:

- Top button **Press** to play an alert tone.
- Top button **Long Press** to send an API request.
- Bottom button **Press** to make a SIP call with a tone.
- Bottom button **Long Press** to cancel an ongoing action.

Available Button Actions

Select an action according to what should happen when the button is activated.

Action	Description
Play Tone	Multicast a selected tone to a configured multicas
Make SIP Call with Tone	Play a tone or pre-recorded announcement to a c
Start InformaCast Scenario	Trigger an InformaCast notification scenario for m
Send API Request	Send one or more HTTP/HTTPS requests to anoth
Send SNMP Trap	Notify a configured network management system
Cancel Action	Cancel an ongoing action.

Configuring an Action for a Button Press

A **Press** triggers an action when the button is pressed.

To configure a button Press action:

1. Go to **Basic Settings** → **Button Settings**.

2. Set **Button Press** to **Enabled**.
3. For **Action**, select the action to trigger.
4. Configure the fields displayed for the selected action.
   Refer to the following examples for common configurations:
   - Configuring the button to play a tone
   - Configuring the button to make a SIP call with a tone
   - Configuring the Button to Trigger an InformaCast Scenario
   - Configuring the button to send an API request
   - Configuring the button to send an SNMP trap
5. To send an API request along with the action, enable **Send API Requests** for that action.
6. To send an API request after the action finishes, enable **Send API Requests on Completion**.
7. Select **Save**.
8. Press the button and verify that the configured action occurs.

Configuring an Action for a Button Long Press

A **Long Press** triggers an action after the button has been held for the configured amount of time.

To configure a button Long Press action:

1. Go to **Basic Settings** → **Button Settings**.
2. Set **Button Long Press** to **Enabled**.
3. Set **Configure Button Hold Time (seconds)** to the minimum amount of time the button must be held before the long-press action is triggered.
4. For **Button Long Press - Action**, select the action to trigger.
5. Configure the fields displayed for the selected action.
   Refer to the following examples for common configurations:
   - Configuring the button to play a tone
   - Configuring the button to make a SIP call with a tone
   - Configuring the Button to Trigger an InformaCast Scenario
   - Configuring the button to send an API request
   - Configuring the button to send an SNMP trap
6. To send an API request along with the action, enable **Send API Requests** for that action.

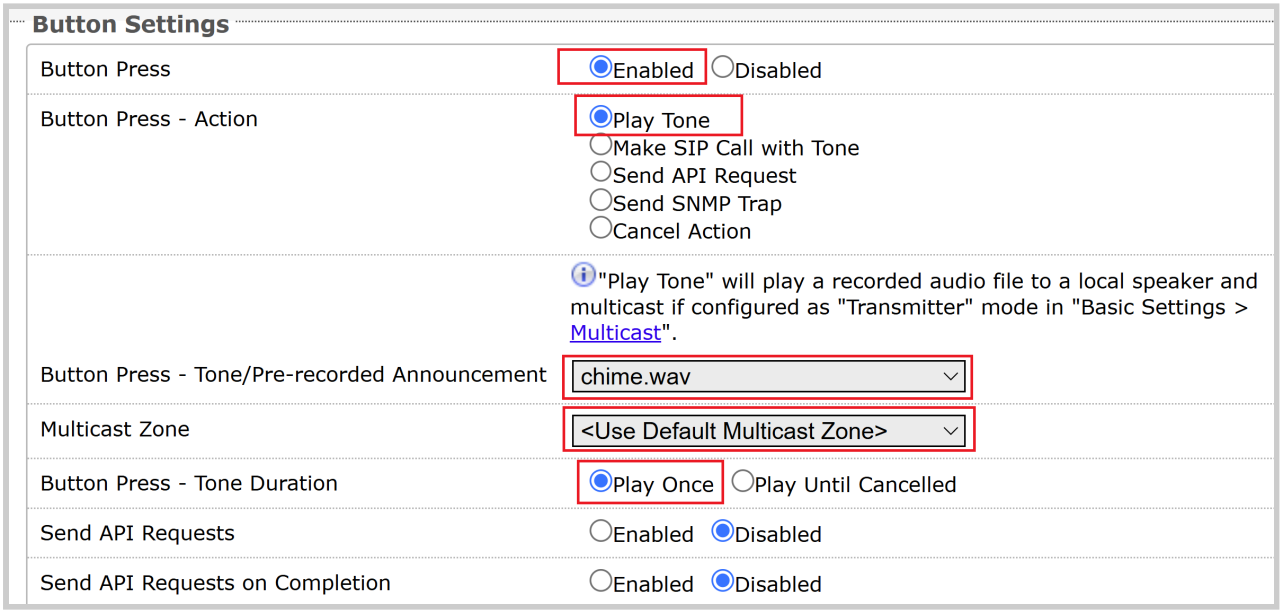
7. To send an API request after the action finishes, enable **Send API Requests on Completion**.
8. Select **Save**.
9. Press and hold the button for at least the configured long-press time.
   The configured **Long Press** action is triggered instead of the normal **Press** action.

Configuring the Button to Play a Tone

Use **Play Tone** to multicast a tone or pre-recorded announcement. This provides a simple way to use the button for notifications or alerts without requiring a SIP call.

To configure the button to play a tone:

1. Go to **Basic Settings** → **Button Settings**.
2. Enable the required **Button Press** or **Button Long Press.**
3. Set **Action** to **Play Tone**.
4. Configure the following.



Depending on the **Multicast Type** and **Allow Same Button Press to Cancel Active Action** setting, the available settings may include:

- **Tone/Pre-recorded Announcement**: Select an audio file.
- **Multicast Zone**: Select the target multicast zone.
- **Poly Group**: Select the target Poly group.
- **Tone Duration:** Specifies the playback times.
- **Interval Between Tones (seconds)**: Specifies the interval between tone playbacks, in seconds.
- **Maximum Tone Duration:** Specifies the maximum playback time.

5. To send an API request along with the action, enable **Send API Requests** for that action.
6. To send an API request after the action finishes, enable **Send API Requests on Completion**.
7. Select **Save**.
8. Press or long-press the button, depending on the configured trigger.
9. Verify that the expected tone is played.

> **Note**
>
> The 8211/8212 does not play the tone directly. Instead, it multicasts the tone to devices configured as multicast receivers.

Configuring the Button to Make a SIP Call with a Tone

Use **Make SIP Call with Tone** when the button should initiate a SIP call and play a pre-recorded announcement to the destination once the call is answered.

To configure the button to make a SIP call with a tone:

1. Go to **Basic Settings** → **Button Settings**.
2. Enable the required **Button Press** or **Button Long Press**.
3. Set **Action** to **Make SIP Call with Tone**.
4. Enter the target SIP extension in **Extension to Dial**.
5. Configure the following:
   - **Tone/Pre-recorded Announcement**: Select an audio file.
   - **Interval Between Tones (seconds)**: Specifies the interval between tone playbacks, in seconds.
   - **Maximum Tone Duration:** Specifies the maximum playback time.
6. To send an API request along with the action, enable **Send API Requests** for that action.
7. To send an API request after the action finishes, enable **Send API Requests on Completion**.
8. Select **Save**.
9. Press or long-press the button.

10. Verify that the SIP call is established and that the expected audio is played at the destination.

Related Links:

- Configuring SIP Extension

Configuring the Button to Trigger an InformaCast Scenario

Use **Start InformaCast Scenario** when you want to trigger a predefined scenario in Singlewire InformaCast.

Before configuring the button action, enable the **InformaCast Scenarios API Support** and configure the credentials required to communicate with InformaCast.

To enable the InformaCast Scenarios API:

1. Go to **Advanced Settings** → **Admin** → **InformaCast Scenarios API**.
2. Set **InformaCast Scenarios API Support** to **Enabled**.
3. Enter the **Security Token** for the InformaCast scenario.
4. To include the device location when triggering the scenario, set **Include Location** to **Enabled**, then configure the applicable:
   - **Site ID**
   - **Building ID**
   - **Floor ID**
   - **Zone ID**
5. Select **Save**.

To configure the button to trigger an InformaCast scenario:

1. Go to **Basic Settings** → **Button Settings**.
2. Enable the required **Button Press** or **Button Long Press**.
3. Select **Start InformaCast Scenario** for the corresponding action.
4. Enter the target **InformaCast Scenario ID**.

5. To send an API request along with the action, enable **Send API Requests** for that action.
6. To send an API request after the action finishes, enable **Send API Requests on Completion**.
7. Select **Save**.
8. Press or long-press the button.
   Verify in InformaCast that the expected scenario is triggered and that the configured notifications are delivered to the intended recipients.

Related Links:

- Singlewire InformaCast Integration Guide

Configuring the Button to Send an API Request

Use **Send API Request** to control another Algo endpoint or an external system when the button is activated.

For example, a button could send API requests to activate an alert, control another IP endpoint, or initiate an action in a third-party application.

> **Note**
>
> Make sure your API requests meet the following requirements:
> - **Custom Headers**: Maximum 300 characters
> - **Headers**: Maximum 1,000 characters
> - **Data Payload**: Maximum 1,500 characters
> - **Target(s)**:
>   - Maximum total target length: 500 characters
>   - Maximum number of targets: 30

To configure the button to send an API request:

1. Go to **Basic Settings** → **Button Settings**.
2. Enable the required **Button Press** or **Button Long Press**.
3. Select **Send API Request** for the corresponding action.

4. Configure the required API request.

   Depending on the command, the configuration can include:

   - **Number of API Requests**
   - **Command**
   - **Data Payload**
   - **Target**
   - **Method**
   - **Custom Path**
   - **Header**
5. Select **Save**.
6. Press or long-press the button.
7. Verify on the target device or application that the expected request was received and the required action occurred.

> **Note**
>
> When your device sends an API request to a device that requires authentication, make sure you enter the target device's API password in **Basic Settings → Features → Remote Device RESTful API Password**.
> The password must match the **RESTful API Password** configured on the target device under **Advanced Settings → Admin → API Support**.

Related Links:

- See **RESTful API Guide** for a complete list of API commands, parameters, and applicable devices.

REST API Commands for a Button

Your device comes with pre-configured REST API commands to allow you to perform actions such as playing a tone, or starting a strobe light.

You can also create custom REST API commands to send API requests to any third-party devices and services that accept API requests.

API Command	Description
Start Tone	Play a tone on the target device.

Stop Tone	Stop the tone.
Start Strobe	Turn on a strobe light.
Stop Strobe	Turn off the strobe light.
Start Screen	Display a screen with text, an image, or both.
Stop Screen	Hide the screen.
Other	Enter a custom REST API command. This allows you to send any Algo-supported REST API commands. You can also send API requests to non-Algo devices and services th

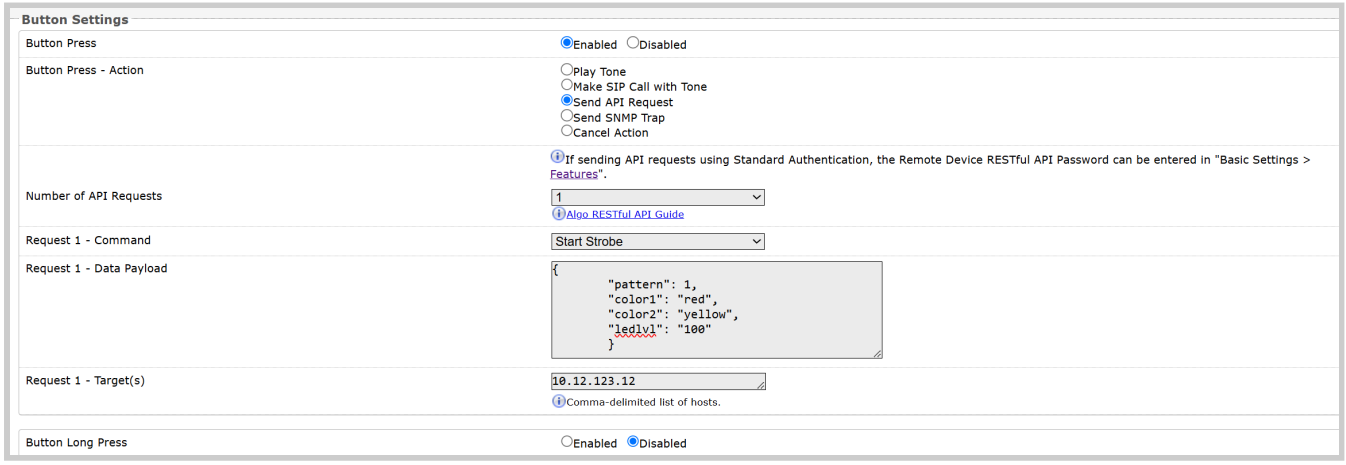
Related Links:

Examples of REST API Configurations

Here are some examples of REST API configuration.

Example 1: Start a strobe light

In this configuration, when the 8211/8212 is pressed, it sends a REST API command to an Algo IP strobe (IP: 10.12.123.12) to start the strobe light, flashing in red and yellow using pattern 1 at a brightness of 100.



Data payload used:

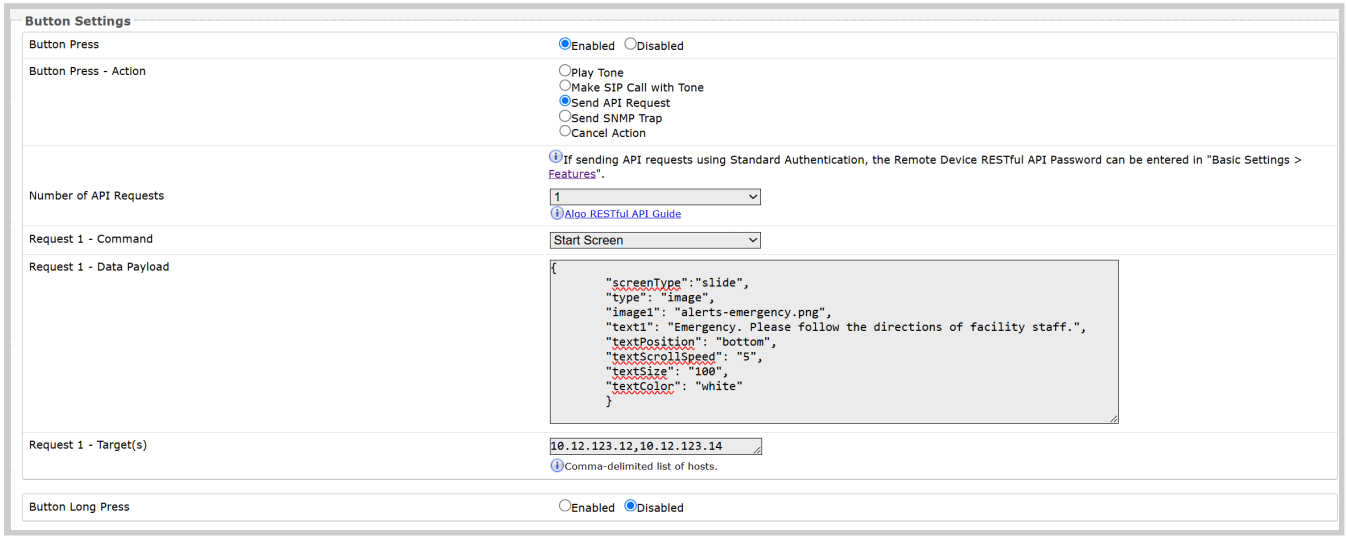
Bash COPY

```
{
        "pattern": 1,
```

```
"color1": "red",
"color2": "yellow",
"ledlvl": "100"
}
```

Example 2: Start a screen

In this configuration, when the 8211/8212 is pressed, it triggers a REST API request to Algo IP Displays (IP: 10.12.123.12 and 10.12.123.14) to display an emergency screen. The screen shows an emergency alert image with large, white scrolling text at the bottom instructing people to follow facility staff directions.



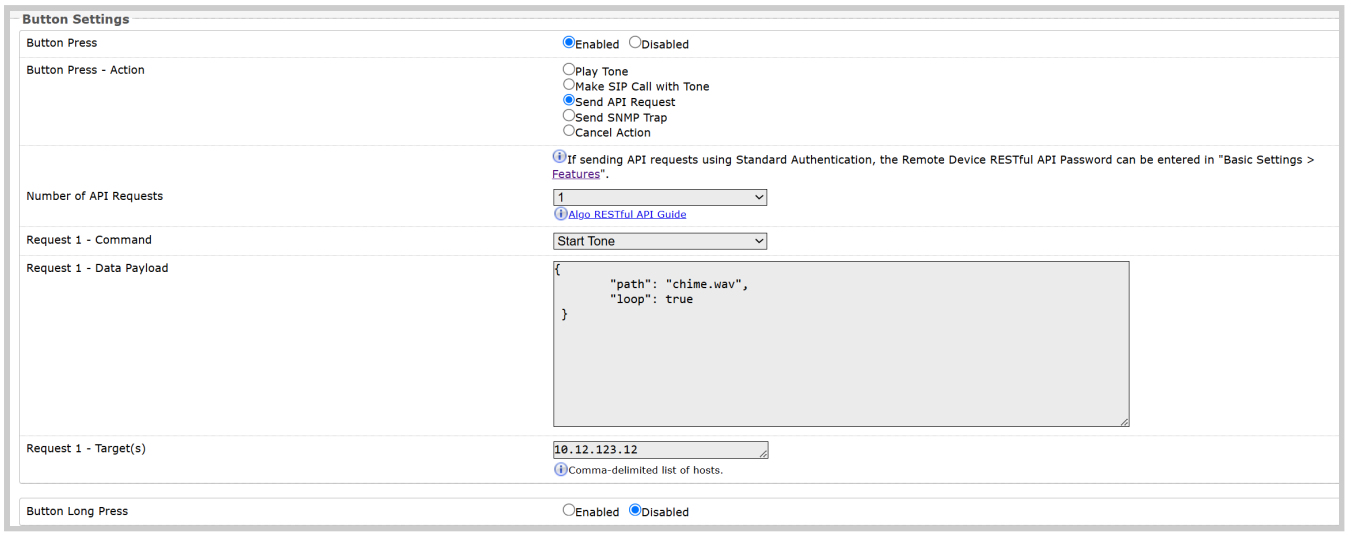
Data payload used:

Bash COPY

```
{
"screenType":"slide",
"type": "image",
"image1": "alerts-emergency.png",
"text1": "Emergency. Please follow the directions of facility staf
"textPosition": "bottom",
"textScrollSpeed": "5",
"textSize": "100",
"textColor": "white"
}
```

Example 3: Play a tone on devices

In this configuration, when the 8211/8212 is pressed, it triggers a REST API request to an Algo IP Speaker (IP: 10.12.123.12) to multicast the audio file `chime.wav` in a continuous loop.



Data payload used:

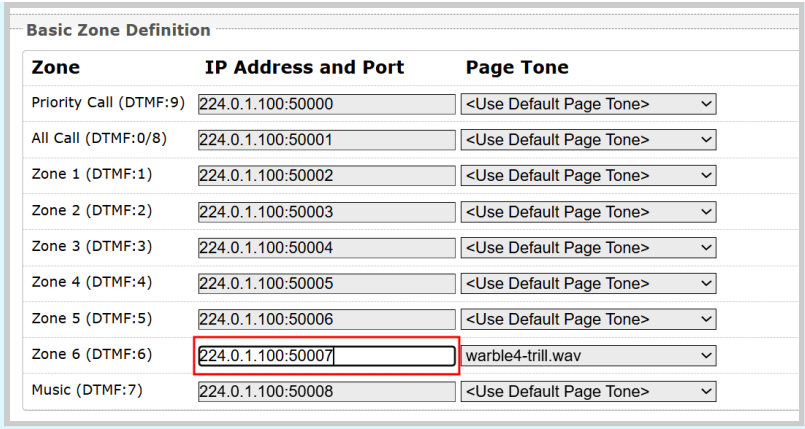
```bash
{
        "path": "chime.wav",
        "loop": true
        }
```

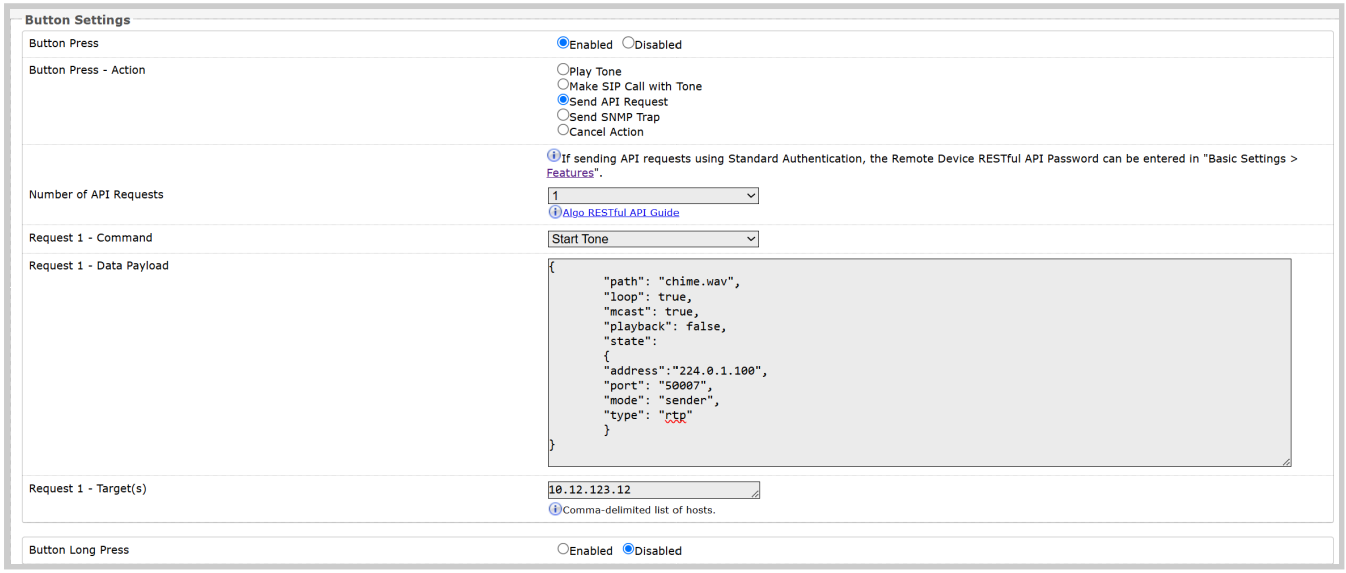
Example 4: Start a multicast with a tone

In this configuration, when the 8211/8212 is pressed, it triggers a REST API request to an Algo IP Speaker (IP: 10.12.123.12) to multicast the audio file `chime.wav` to zone 6, in a continuous loop, without playing it locally.

The IP Speaker is configured as a multicast transmitter, with the multicast zone defined as follows: IP address 224.0.1.100 and port 50007.

> **Note**
>
> The multicast zone definitions (`address` and `port`) must match those defined in the target device's web interface under **Advanced Settings → Advanced Multicast**. In this example, Zone 6 is used.





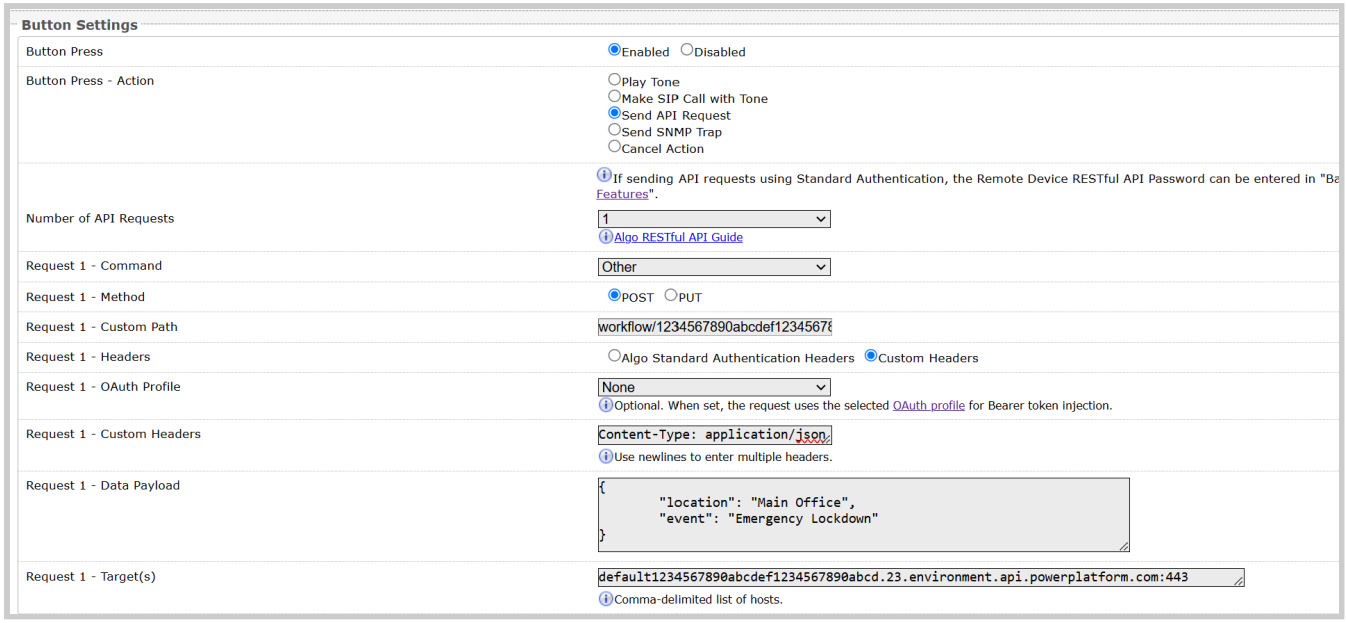
Data payload used:

Bash COPY

```
{
        "path": "chime.wav",
        "loop": true,
        "mcast": true,
        "playback": false,
        "state":
        {
        "address":"224.0.1.100",
        "port": "50007",
        "mode": "sender",
        "type": "rtp"
        }
}
```

Example 5: Trigger a third-party application workflow

In this configuration, when the 8211/8212 is pressed, it sends a POST request to trigger a Power Automate workflow, such as notifying a Microsoft Teams channel that an **Emergency Lockdown** event has been activated from the Main Office.



Configuring the Button to Send an SNMP Trap

Use **Send SNMP Trap** when a network management system should be notified that the button was activated.

SNMP must be configured on the device before this action can be used.

To configure the button to send an SNMP trap:

1. Go to **Basic Settings** → **Button Settings**.
2. Enable the required **Button Press** or **Button Long Press**.
3. Select **Send SNMP Trap** for the corresponding action.
4. Select **Save**.
5. Go to **Advanced Settings** → **Admin** → **Simple Network Management Protocol** and configure SNMP settings:
    - **SNMP Trap Remote IP**: Enter the IP address of the SNMP manager or trap receiver that will receive SNMP traps.
    - (Optional) **SNMP System Location**: Enter a description of the device's location. This information helps an SNMP management system identify and monitor the device.

6. To send an API request along with the action, enable **Send API Requests** for that action.
7. Select **Save**.
8. Press or long-press the button.
9. Verify that the configured SNMP manager receives the trap.

Cancelling, Replacing, or Overriding an Action

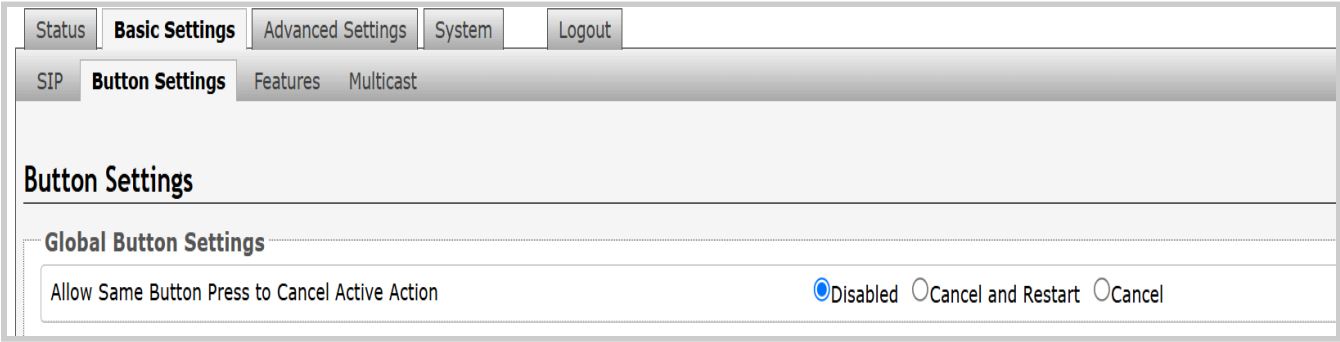
For actions that remain active after the initial button press, you can configure how additional button presses behave.

This is useful when you need to stop, restart, or replace an ongoing activity directly from the 8211/8212.

> **Note**
>
> - "Send API Request" and "Send SNMP Trap" actions cannot be canceled.
> - Cancel Action buttons will always override other button actions.

Using the Same Button to Cancel or Restart an Action

You can cancel or restart an action by pressing the same button again.



To configure the same button to control its active action:

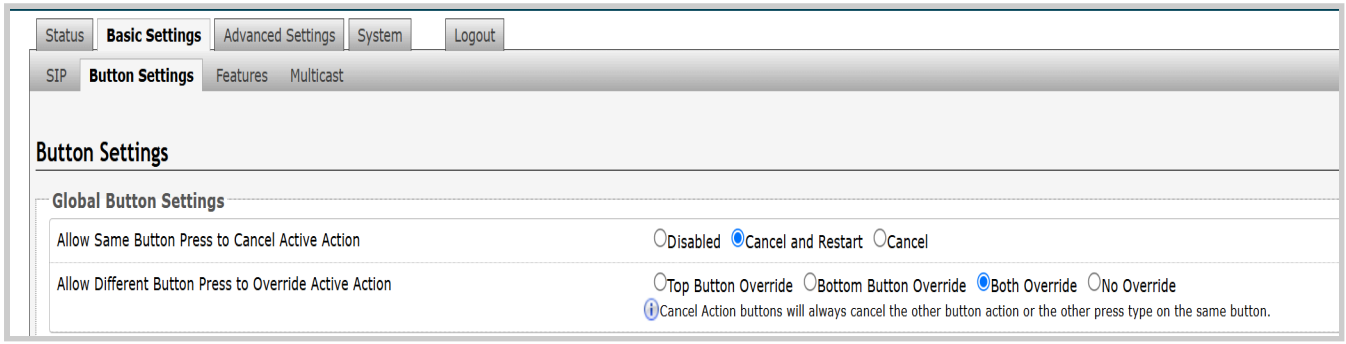
1. Go to **Basic Settings** → **Button Settings**.
2. Locate **Allow Same Button Press to Cancel Active Action**.
3. Select one of the following:
   - **Disabled**: Pressing the button again does not change the active action.
   - **Cancel and Restart**: Cancels the active action and immediately starts it again.

- **Cancel**: Cancels the active action.

4. Select **Save**.
5. Trigger the button action and press the same button again to verify the configured behavior.

Using One 8212 Button to Override the Other Button

On the 8212, you can also define what happens when one button is pressed while an action started by the other button is active.



To configure button action override:

1. Go to **Basic Settings** → **Button Settings**.
2. Locate **Allow Different Button Press to Override Active Action**.
3. Select one of the following:
   - **Top Button Override**: Pressing the top button ends the ongoing activity triggered by the bottom button.
   - **Bottom Button Override**: Pressing the bottom button ends the ongoing activity triggered by the top button.
   - **Both Override**: Either button can end an activity triggered by the other button.
   - **No Override**: Pressing the other button does not change the ongoing activity.
4. Select **Save**.
5. Trigger an action from one button, and then press the other button to verify the configured override behavior.

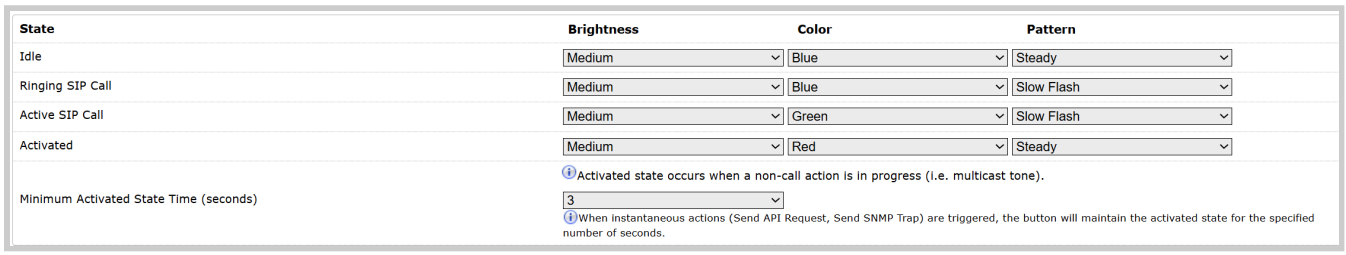
Configuring the Button Ring Illumination Behavior

The LED-illuminated button ring provides visual feedback about the current button state.

You can configure different illumination behavior for:

- **Idle**: No button activity is active.
- **Ringing SIP Call**: A SIP call is being established.
- **Active SIP Call**: A SIP call is active.
- **Activated**: A non-SIP action is active, such as tone playback, multicasting, an API operation, or an SNMP operation.

For each state, you can independently configure the brightness, color, and illumination pattern.



To configure the button ring illumination behavior:

1. Go to **Basic Settings** → **Button Settings**.
2. Go to the **Button Appearance** section.
3. For each button state, configure:
   - **Brightness**: **Off**, **Low**, **Medium**, or **High**.
   - **Color**: **Blue**, **Red**, **Green**, or **Amber**.
   - **Pattern**:
     - **Steady**: Illumination remains on.
     - **Slow Flash**: Illumination flashes slowly.
     - **Fast Flash**: Illumination flashes rapidly.
     - **Alarm**: Illumination flashes three times per cycle.
4. Set **Minimum Activated State Time (seconds)**.
   This setting defines the minimum amount of time the **Activated** illumination remains visible for non-SIP activities. It provides visible feedback even when an action, such as an API request, completes very quickly.
5. Select **Save**.
6. Trigger the configured button actions and verify that the ring indicates the expected states.

> **Note**
>
> If a SIP call cannot be established, for example because the destination is busy, the button ring uses the **Alarm** pattern to provide visual feedback that the call attempt

was unsuccessful.

Multicast

Your device can be used as a multicast transmitter and be grouped into up to 50 multicast zones. Multicast allows a single transmitting device to simultaneously send audio to multiple receiving devices over the network. Any number and combination of Algo Speakers, Paging Adapters, IP Displays, or Visual Alerters can be set as receiving devices. Receiving devices do not require a unique SIP extension and, therefore, do not need to be registered with the SIP server.

> **Note**
>
> The 8211/8212 is designed as a multicast transmitter, with multicast always enabled.

Key Configurations for Multicast

Ensure the following settings are correctly configured and consistent between the transmitter and receiver devices. These settings depend on your **Multicast Mode** setup:

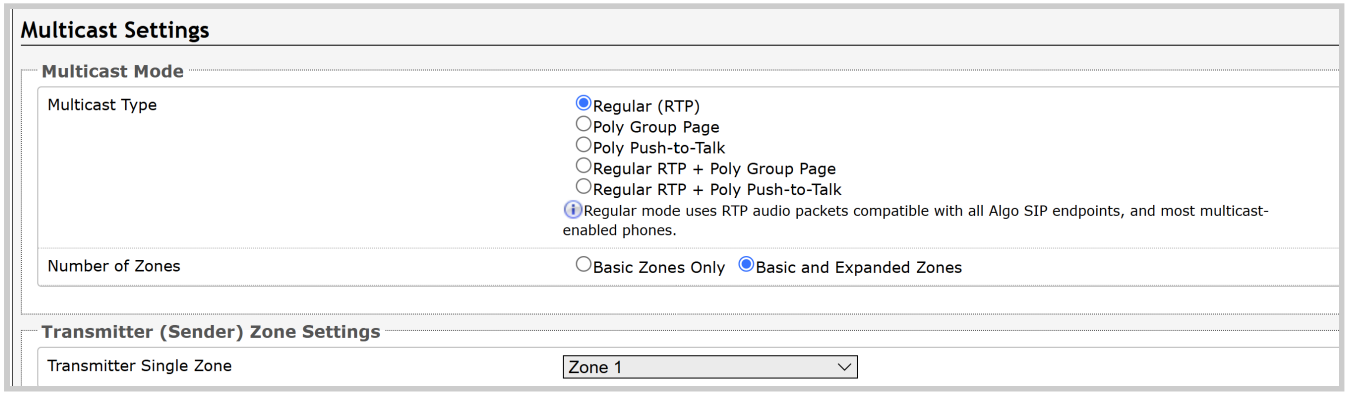
- Multicast Mode (under **Basic Settings** → **Multicast**)
  - Sender: Set to **Transmitter**
  - Receiver: Set to **Receiver**
- Multicast Type (under **Basic Settings** → **Multicast**)
  - Both sender and receiver should be set to the same **Multicast Type**. Normally, it's **Regular (RTP)** unless Poly devices are involved.
- Zone Number (under **Basic Settings** → **Multicast**)
  - Confirm the **Transmitter Single Zone** selected on the **Transmitter** is also enabled under the **Basic Receiver Zones** on the **Receiver**.
- Zone Definitions (under **Advanced Settings** → **Advanced Multicast**)
  - Verify that the **IP Address** and **Port Number** for the multicast zone match exactly on both the Transmitter and Receiver devices.

Configuring Multicast Settings

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

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

> **Note**
>
> Always ensure that the multicast settings on all receiver devices match those of the transmitter.



To configure Multicast settings:

1. Go to the **Basic Settings** → **Multicast**.
2. Configure **Multicast Mode** settings:
    - **Multicast Type**: Select an option.
        - **Regular (RTP)**: Multicasts only to Algo IP endpoints or multicast-enabled phones.
        - **Poly Group Page** or **Poly Push-to-Talk**: Multicasts to Poly phones.
        - **Regular RTP + Poly Group Page** or **Regular RTP + Push-to-Talk**: Multicasts to Poly phones, Algo IP endpoints, and multicast-enabled phones.

          > **Note**
          >
          > Make sure your multicast receivers are set to the same **Multicast Type**. Normally, it's **Regular (RTP)** unless Poly devices are involved.

    - **Number of Zones**:

    - **Basic Zones Only**: Uses nine or fewer multicast zones.
    - **Basic and Expanded Zones**: Uses 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.
3. For the **Transmitter Single Zone** option, select the default zone for the multicast audio to be sent to.
4. If your **Multicast Mode** includes **Poly Group Page** or **Poly Push-to-Talk**, configure also the following:
    - **Poly Zone**: Enter the same **Multicast IP Address** and **Port** number configured on the Poly phones.
    - **Poly Default Channel**: Selects the default group for the multicast audio to be sent to.

      The **Poly Default Channel** is the default channel used for multicast actions unless an option is available for a custom channel with specific parameters.
5. Select **Save**.

Configuring Multicast Zones

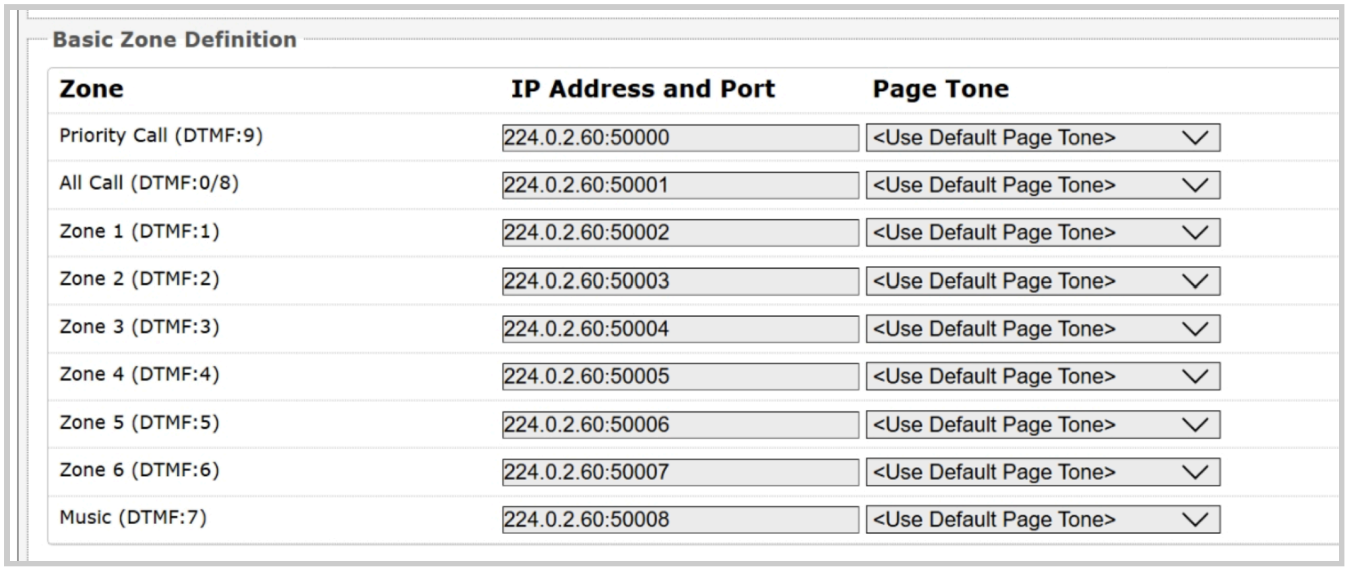
Each device has a unique IP address and shares a common multicast IP and port number (multicast zone) for multicast packets. The transmitter units send to a configurable multicast zone, and the Receiver units listen to assigned multicast zones.

The network switches and router see the packet and deliver it to all the zone members. The multicast IP and port number must be the same on all transmitter and receiver units of the same zone. You may define multiple zones by picking different multicast IP addresses and/or port numbers.

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

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

- Make sure that the **IP Address** and **Port Number** for the multicast zone match exactly on both the Transmitter and Receiver devices.



Notes

Ensure the IP Address and Port # match on both the **Transmitter (Sender)** and **Receiver (Listener)**, for the zone being used.

To configure Multicast zones:

1. Log in to the web interface of your multicast transmitter or receiver device.
2. Go to **Advanced Settings** → **Advanced Multicast**.
3. View the default zone **IP Address and Port**. Edit it if necessary.
4. To specify a different tone to play before the multicast starts, select an audio file from the **Page Tone** drop-down list.
   If you select **<Use Default Page Tone>**, the audio file specified under **Basic Settings** → **Features** → **Inbound Page Settings** → **Page Tone** plays.
5. Select **Save**.

Multicast Page Zones

By default, a multicast receiver can listen to nine basic multicast zones. Up to 50 zones are available when **Basic and Expanded Zones** is selected for **Number of Zones**. Each multicast zone is defined by a multicast IP address and port.

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

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

Multicast Page Zone Priority

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

Multicast Triggers

As a multicast transmitter, the multicast is triggered in the following events, with the audio content broadcast to receivers in the selected multicast zone. The type of content that is broadcast depends on what triggers the multicast.

Multicast Trigger	Audio Content Included in the Multicast
Button action: Play Tone	The specified tone audio.
Button action: Make SIP Call with Tone	The tone audio.

TLS for SIP Signaling and Provisioning

Algo devices 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. The 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 is therefore 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, see Algo TLS guide for SIP Signalling and HTTPS Provisioning.

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:

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 **System → File Manager** tab.
3. Upload the certificate files into the **certs/trusted** directory.
4. Click the **Upload** button in the top left corner of the file manager and browse to the certificate.

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

For SIP TLS, if the **Validate Server Certificate** option is enabled in **Advanced Settings → Advanced SIP** tab, then the device will validate the SIP server against common certificate authorities.

For Provisioning, if **HTTPS** is selected and the **Validate Server Certificate** option is enabled in the **Advanced Settings → Provisioning** tab, then the device will validate the server against common certificate authorities.

To validate against additional certificates:

1. Go to **System → File Manager.**
2. Upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the **certs** folder.

HTTPS Provisioning

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

> **Note**
>
> 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:

Plain text COPY

```
Prov.download.cert = 1
```

Using Configuration Files

When deploying your device, configuration files are used to provision the devices automatically. These configuration files define network settings, SIP credentials, and operational preferences, reducing the need for manual setup. There are two types of provisioning files available: generic and specific.

- **Generic configuration file**: The configuration file is not tied to a specific device. It does not include the MAC address in its filename, and any Algo device connected to the network can automatically download and use this file from the provisioning server. However, you must enter SIP extensions and credentials manually.
- **Specific configuration file**: The configuration file is intended for a single device and includes the device's MAC address in the filename. Only the Algo device with the matching MAC address can download and use this file.

For more information, see the Algo's SIP endpoint provisioning guide at www.algosolutions.com/provision.

MD5 Checksum

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

To create an `.md5` checksum file:

1. Download an MD5 tool. For example, http://www.fourmilab.ch/md5.
2. Extract the tool and open a command prompt in the same directory.
3. Run the `md5` command with the target filename to generate the `.md5` file.
4. To output the hash in lowercase, add the `-l` parameter:
   Custom

Plain text COPY

```
md5 -l yourfilename.ext
```

Plain text

The resulting `.md5` file will be saved in the same directory.

Securing SIP Signaling (and RTP Audio)

SIP signaling is secured by setting **SIP Transportation** to **TLS** (under the **Advanced Settings** → **Advanced SIP** tab). SIP transportation refers to the underlying protocol used for transmitting SIP messages between different entities in a network. Setting it to **TLS** ensures that the SIP traffic will be encrypted. SIP signaling 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.

Uploading Public CA Certificates

If the particular CA Certificate is not installed at factory, you can easily upload your own.

To install the public CA certificate:

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 **System** → **File Manager** tab.
3. Upload the certificate files into the **certs** directory.
4. Click the **Upload** button in the top-left corner of the file manager and browse to the certificate.

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

For SIP TLS, if the **Validate Server Certificate** option is enabled in **Advanced Settings** → **Advanced SIP** tab, then the device will validate the SIP server against common certificate authorities.

For Provisioning, if **HTTPS** is selected and the **Validate Server Certificate** option is enabled in the **Advanced Settings** → **Provisioning** tab, then the device will validate the server against common certificate authorities.

To validate against additional certificates:

1. Go to **System** → **File Manager**.
2. Upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the **certs** folder.

HTTPS Provisioning

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

> **Note**
>
> 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:

Plain text COPY

```
Prov.download.cert = 1
```

Using Configuration Files

When deploying your device, configuration files are used to provision the devices automatically. These configuration files define network settings, SIP credentials, and operational preferences, reducing the need for manual setup. There are two types of provisioning files available: generic and specific.

- **Generic configuration file**: The configuration file is not tied to a specific device. It does not include the MAC address in its filename, and any Algo 8211/8212 device connected to the network can automatically download and use this file from the provisioning server. However, you must enter SIP extensions and credentials manually.
- **Specific configuration file**: The configuration file is intended for a single device and includes the device's MAC address in the filename. Only the Algo 8211/8212 unit with the matching MAC address can download and use this file.

For more information, see Central Provisioning of Algo IP Endpoints.

MD5 Checksum

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

To create an `.md5` checksum file:

1. Download an MD5 tool. For example, http://www.fourmilab.ch/md5.
2. Extract the tool and open a command prompt in the same directory.
3. Run the `md5` command with the target filename to generate the `.md5` file.
4. To output the hash in lowercase, add the `-l` parameter:
   Custom

Bash COPY

```
md5 -l yourfilename.ext
```

The resulting `.md5` file will be saved in the same directory.

Securing SIP Signaling (and RTP Audio)

SIP signaling is secured by setting **SIP Transportation** to **TLS** (under the **Advanced Settings** → **Advanced SIP** tab). SIP transportation refers to the underlying protocol used for transmitting SIP messages between different entities in a network. Setting it to **TLS** ensures that the SIP traffic will be encrypted. SIP signaling 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.

Integrations

Your device supports integration with Microsoft Teams, InformaCast, and OAuth-enabled services.

These integrations allow the device to extend alerting and notification workflows across public address systems, SIP platforms, cloud services, and third-party notification systems.

Integration with Teams

Your device is certified for native compatibility with the Microsoft Teams SIP Gateway. Applications such as IP paging, emergency alerting, and hands-free visitor communication can be implemented using both Microsoft Teams and Algo IP endpoints.

You can configure Teams integration using one of the following ways:

- Microsoft Teams Configuration with Algo IP Devices Using ADMP
- Microsoft Teams Configuration with Algo IP Devices Using the Device Web Interface

Integration with InformaCast

Your device can trigger InformaCast Scenarios.

For more information, see Singlewire InformaCast Integration Guide.

Related Links:

- Configuring the Button to Trigger an InformaCast Scenario

Using OAuth for Authentication

OAuth (Open Authorization) is an industry-standard protocol that enables secure, delegated access to resources without requiring users to share credentials such as usernames and passwords.

Instead of storing static credentials on a device or application, OAuth allows a trusted third-party service (such as Google, Microsoft, or Slack) to issue time-limited access tokens. These tokens allow an Algo device to interact with the service on behalf of a user or system, without exposing sensitive login information.

For more information, see Using OAuth for Authentication.

System Maintenance

You can back up the current configuration, restore previously saved settings, reset the device to its factory defaults, and perform maintenance tasks to support troubleshooting, recovery, and device redeployment.

Monitoring your Device Status

You can check your device status using one of the following methods:

- From the **Status** page of the button's web interface

  This allows you to check the status of individual buttons.
- From ADMP

  Configure the 8211/8212 as a Panic Button so as to view its status in ADMP. ADMP allows a collective view for all panic buttons in your deployment. You can also download the event logs.

Configuring ADMP Cloud Monitoring

When **ADMP Cloud Monitoring** is enabled, your device can be identified as a panic button for cloud monitoring.

To enable ADMP Cloud Monitoring:

1. Go to **Advanced Settings** → **Admin**.
2. Go to the **ADMP Cloud Monitoring** section, and configure the following:
   - **Enable ADMP Cloud Monitoring**: Set to **Enabled**.
   - **Account ID**: Enter your ADMP account ID.
   - **Allow Configuration File Sync**: Set to **Enabled** to allow ADMP to query and display settings stored on the device.
   - **Heartbeat Interval**: Specify how often ADMP checks the device status.
   - **Enable Panic Button Monitoring**: Set to **Enabled**.
3. Select **Save**.

To configure your button as a Panic Button:

1. Go to **Basic Settings** → **Button Settings**.
2. Set **Panic Button** to **Enabled**.

> **Note**
>
> The **Panic Button** settings are available only when **ADMP Cloud Monitoring** is enabled.

3. Enter a **Panic Button Location** that identifies where the button is installed. For example, *Main Building*.
4. Enter a **Panic Button Description** that identifies the purpose of the button. For example, *Medical Emergency*.
5. Select **Save**.

To view Panic Button status in ADMP:

1. Log in to ADMP.
2. Go to **Panic Button** → **Status Overview**.
3. Locate your device by its IP or MAC address.

Backing Up and Restoring the Device Configuration

You can save the current device configuration to a `.txt` file and use it later to restore the device settings. Back up the configuration before making major configuration changes or upgrading the firmware so the settings can be restored if needed.

Backing Up the Device Configuration

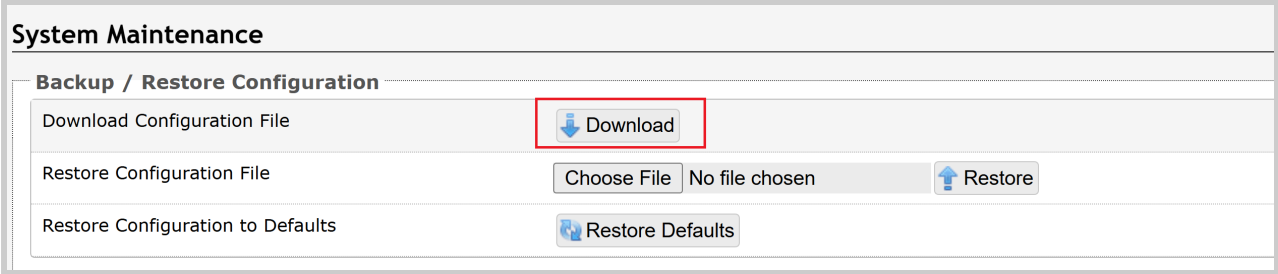
Download the current device settings as a configuration file and save it to your computer.

> **Note**
>
> The configuration backup contains the device settings only. To back up the configuration together with files stored on the device, such as certificates, licenses, and tones, use **Backup / Restore All User Files**.

To download the system configuration:

1. Go to **System** → **Maintenance** → **Backup / Restore Configuration.**

2. Select **Download**.



The configuration file is downloaded to your default downloads folder using the following file name format:

`settings-<product_model>-<product_MAC_ADDRESS>.txt`

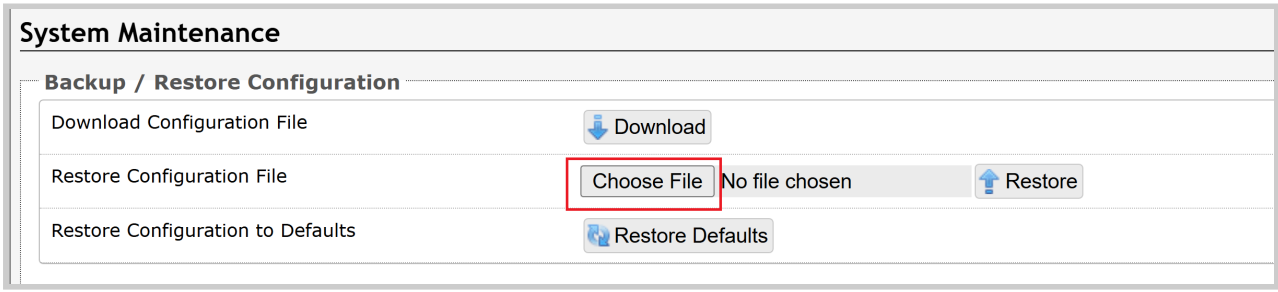
Restoring the Device Configuration

You can restore the device configurations from a backup configuration file, or restore to its factory default settings using either the button or its web interface.

You can also choose to restore the factory default settings and delete all preloaded and uploaded files.

To restore the device configuration:

1. Go to **System** → **Maintenance**.
2. Under **Backup / Restore Configuration**, select **Choose File**.



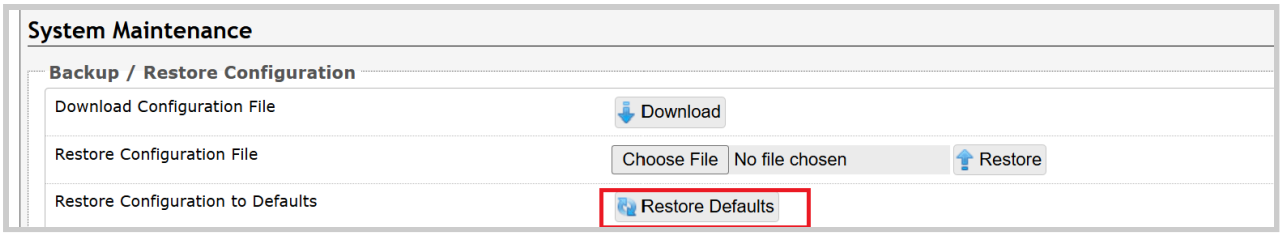
3. Select the configuration file, then select **Restore**.
   The system reboots to restore the settings.

Restoring the Configuration to Factory Defaults

Restore the device configuration settings to their factory default values while retaining the files stored on the device.

To restore the configuration to factory defaults:

1. Go to **System** → **Maintenance**.
2. Under **Backup / Restore Configuration**, select **Restore Defaults**.



3. When prompted to confirm the action, select **OK**.

   The device reboots and restores the configuration settings to their factory defaults.

Backing Up and Restoring All User Files

You can create a complete backup that includes the current device configuration and all user-uploaded files, such as certificates, licenses, and tone files. The backup is saved as a `.zip` file and can be used later to restore the configuration and files together.

Backing Up All User Files

To back up the device configuration and all user files:

1. Go to **System** → **Maintenance**.
2. Under **Backup / Restore All User Files**, locate **Download Backup Zip File**.
3. Select **Download**.
4. Save the downloaded `.zip` file to a secure location.

The backup `.zip` file contains the device configuration and all user-uploaded files.

Restoring All User Files from a Backup

Use a previously downloaded backup `.zip` file to restore the device configuration and user-uploaded files.

To restore the device from a backup:

1. Go to **System** → **Maintenance**.
2. Under **Backup / Restore All User Files**, locate **Restore from Backup Zip File**.
3. Select **Choose File** and select the backup `.zip` file.
4. Select **Restore**.
5. Wait for the restore process to complete.

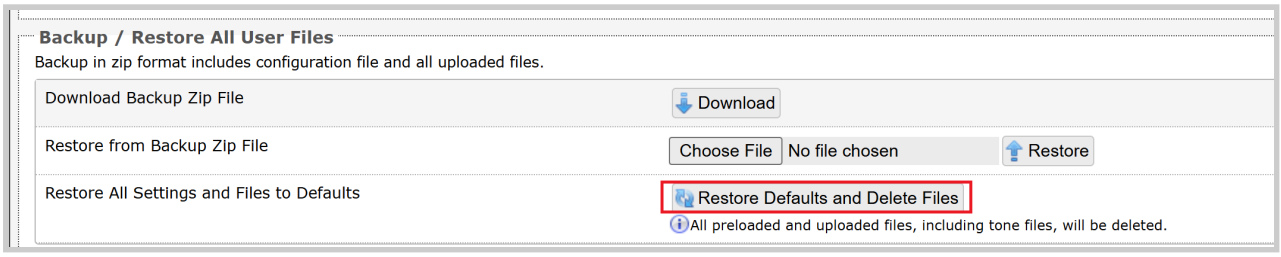
Restoring All Settings and Files to Defaults

Restore the device settings to their default values and delete the files stored on the device.

> **Note**
>
> This action deletes all preloaded and uploaded files, including tone files.

To restore all settings and files to defaults:

1. Go to **System** → **Maintenance**.
2. Under **Backup / Restore All User Files**, select **Restore Defaults and Delete Files**.



3. Select **OK** to confirm the action when prompted.

Managing Firmware

The **Online Upgrade** feature checks whether a newer firmware version is available from the Algo firmware server (firmware2.algosolutions.com). The device must have an active internet connection to perform this check.

> **Note**
>
> During the firmware update process, Algo devices communicate with two different hosts:
>
> - **firmware2.algosolutions.com**: Checks whether a newer firmware version is available.
> - **algofw.sfo3.cdn.digitaloceanspaces.com**: Downloads the firmware image when an update is available.

> If your network uses outbound firewall rules, web filtering, or proxy allowlists, ensure that HTTPS (TCP port 443) access to both hosts is permitted. Blocking either host may prevent firmware updates from completing successfully.

To check for firmware updates:

1. Go to **System** → **Firmware**.
2. Under **Online Upgrade**, click **Check**.
3. Wait while the device checks for the latest firmware.
   If the device is running the latest firmware, **Latest Firmware** displays **Firmware up to date**.
   If a newer firmware version is available, the available firmware version is displayed.

Upgrading or Downgrading Firmware

The Custom Upgrade section allows you to manually install firmware when internet access is unavailable or when instructed by Algo Technical Support.

You can install firmware from a signed firmware file stored on your computer or from a firmware download URL.

To install firmware from a local file:

1. Download the signed firmware file from the Algo firmware downloads page.
2. Go to **System** → **Firmware**.
3. Under **Method**, select **From Local Files**.
4. Click **Choose File**.
5. Browse to and select the signed firmware file.
6. Select **Upgrade**.
7. After the device restarts, verify that the firmware version has been updated.

To install firmware from a URL:

1. Copy the firmware download URL from the Algo firmware downloads page.
2. Go to **Firmware**.
3. Under **Method**, select **From URL**.
4. Enter the firmware download URL in **Upgrade URL**.

5. Start the firmware upgrade.
6. After the device restarts, verify that the firmware version has been updated.

Allowing Firmware Downgrade

The **Allow Downgrade** option controls whether the device can install an earlier firmware version.

> **Note**
>
> Downgrading firmware may affect future firmware upgrades. If you need to downgrade the firmware, contact Algo Technical Support for assistance.

To allow firmware downgrades:

- Enable **Allow Downgrade** only if instructed by Algo Technical Support.

Managing System Log

The **System Log** provides a record of device events and operational messages that can help monitor system activity and troubleshoot issues. You can view the log to verify device operation, identify errors or warnings, and gather diagnostic information when investigating configuration or network problems.

Configuring Log Settings

The **Log Settings** page allows you to configure how the device records and manages system log messages. You can adjust the logging level, enable or disable remote logging, and specify a remote syslog server to collect log information for centralized monitoring, diagnostics, and troubleshooting.

To configure the log settings:

1. Go to **Advanced Settings** → **Admin** → **Log Settings**.
2. Configure the following:
   - **Log Level:** Select the appropriate level for the information you want to capture.

     > **Note**

> Change the **Log Level** only under the guidance of Algo Technical Support. Higher log levels generate additional diagnostic information, which may clutter the logs and make routine monitoring and troubleshooting more difficult.

- **Log Method**:
  - **Local**: The log file is saved in RAM on the device.
  - **Network**: Send the log file to an external SysLog server so settings are not lost if the device is rebooted, or for ease of central access.
  - **Both**: Use both methods.
- **Network Log Protocol**: Select the transport protocol used to send Syslog messages to the configured log server.

  > **Note**
  >
  > The default port when using UDP/TCP is 514. The default port when using TLS is 6514. To specify a different port, enter ADDRESS:PORT. When using TLS, use the **System → File Manager** tab to upload the CA certificate renamed to ca.pem to the **certs/syslog** folder. If the server is using peer certificate authentication, also upload the certificate/key pair renamed to cert.pem and key.pem.

- **Log Server**: Enter the Syslog server address provided by your IT Administrator.
- **Log Additional Events**: To be used by support@algosolutions.com if necessary.
- **Select Additional Log Events**: To be used by support@algosolutions.com if necessary.

  > **Note**
  >
  > Configure additional log events only when requested by Algo Technical Support. These options are intended for advanced troubleshooting.

3. Select **Save**.

Downloading System Logs

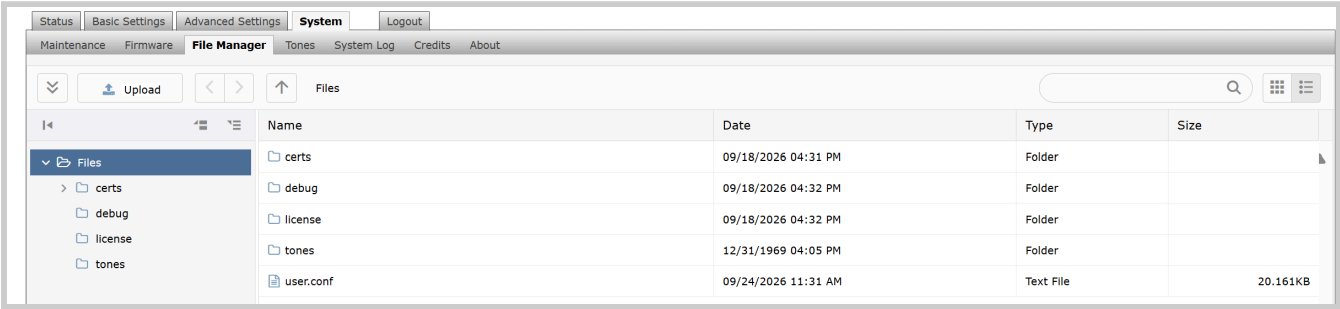
The **System Log** contains diagnostic information that can help identify and troubleshoot device issues.

To retrieve system logs:

1. Go to **System** → **System Log**.
2. Do one of the following:
   - **Download**: Save the log file to your local disk.
   - **View**: View the log information on-screen.

   Provide the file to Algo Technical Support if requested.

Managing Files Using File Manager



File Formats

When uploading files to the **File Manager**, refer to this table for supported file formats and requirements.

Folder	Supported Format
License	LIC
Tones	8SVX, AIF, AIFC, AIFF, AIFFC, AL, AMB, AMR-NB, AMR-WB, ANB, AU, AVR, AWB, CAF, CDDA, CDR, CVS, CVSD, CVU, DAT, DVMS, F32, F4, F64, F8, FAP, FLAC, FSSD, GSM, GSRT, HCOM, HTK, IMA, IRCAM, LA, LPC, LPC10, LU, MAT, MAT4, MAT5, MAUD, MP2, MP3, NIST, OGG, PAF, PRC, PVF, RAW, S1, S16, S2, S24, S3, S32, S4, S8, SB, SD2, SDS, SF, SL, SLN, SMP, SND, SNDFILE, SNDR, SNDT, SOU, SOX, SPH, SW, TXW, U1, U16, U2, U24, U3, U32, U4, U8, UB, UL, UW, VMS, VOC, VORBIS, VOX, W64, WAV, WAVPCM, WV, WVE, XA, XI

Certs Folder

The **certs** folder stores trusted Certificate Authority (CA) certificates used when validating server certificates.

Upload additional certificates only if **Validate Server Certificate** is enabled under **Advanced Settings → Advanced SIP**.

To install a public CA certificate:

1. Obtain a Base64-encoded X.509 certificate (.pem, .cer, or .crt) from your Certificate Authority.
2. Go to **System → File Manager**.
3. Open the **certs** folder.
4. Click **Upload**.
5. Select the certificate file.

The certificate is added to the trusted certificate store.

For a list of pre-installed trusted certificates, contact support@algosolutions.com.

Debug Folder

The **debug** folder stores diagnostic files generated by the device.

Diagnostic files are used by Algo Technical Support to troubleshoot device issues.

To retrieve diagnostic files:

1. Go to **System → File Manager**.
2. Open the **debug** folder.
3. Download the requested diagnostic files.
4. Provide the files to Algo Technical Support.

License Folder

The **license** folder stores license files required to enable licensed features.

To install a license:

1. Obtain the license file from Algo.
2. Go to **System → File Manager**.

3. Open the **license** folder.
4. Click **Upload**.
5. Select the license (.lic) file.
   The license is installed and becomes available after the upload completes.

Tones Folder

The **tones** folder stores custom audio files used for paging and notification applications.

To upload a custom audio file:

1. Go to **System** → **File Manager**.
2. Open the **tones** folder.
3. Click **Upload**.
4. Select the audio file from your computer.
5. Wait for the upload to complete.
   The uploaded audio file is available for notification applications.

To replace an existing audio file:

1. Download the existing audio file.
2. Modify the file as required.
3. Save the modified file using a different file name.
4. Upload the new file to the **tones** folder.

> **Note**
>
> Audio files must meet the supported format and file requirements listed in File Formats.

Managing Tones

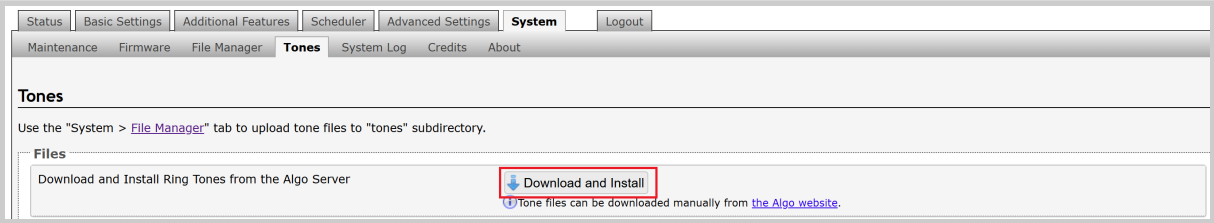
Tone files are used for ringing, alerts, and other audio notifications on the device. You can download the default Algo tone files, rebuild tone cache files if tones do not play correctly, and test tone files directly from the device interface.

Downloading Tone Files

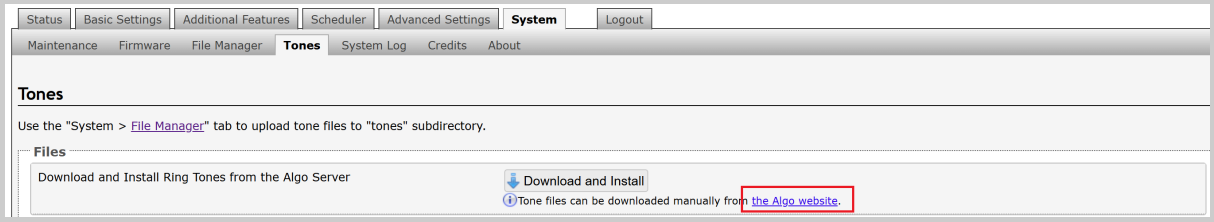
Your device includes a set of default ring tones, stored in **System → File Manager → Tones**. If you delete any of these files, you can download them again to restore the original ring tones.

To download Algo default tone files:

1. Go to **System → Tones**.
2. Do one of the following:
   - To download the tone files and install them into your **File Manager → Tones** folder, select **Download and Install**.

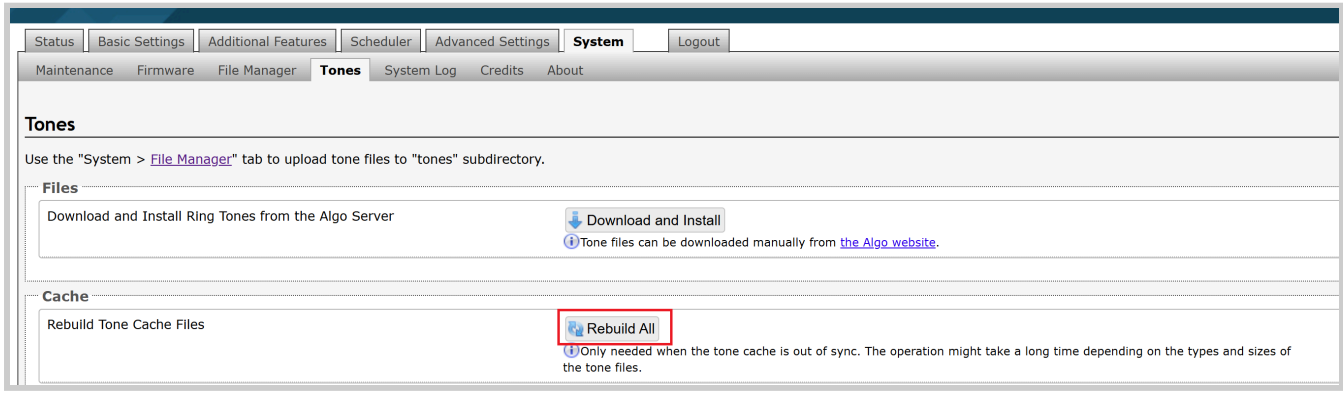


   - To download them to your local disk, select the **Algo website** link.



Rebuilding Tone Cache Files

Rebuild Tone Cache Files recreates the cached versions of all tone files on the device. Use this option only if the tone cache is out of sync with the tone files, such as when uploaded or modified tones do not play correctly. The operation does not change or delete the original tone files and may take several minutes depending on the number and size of the files.



To rebuild tone cache files:

1. Go to **System** → **Tones** → **Cache**.
2. Select **Rebuild All**.

Testing Tone Files

You can play uploaded audio files directly through the device to verify that they sound as expected.

To hear the sound, configure an IP Speaker in the deployment as the multicast receiver. When you test a tone, the speaker plays the tone.

To test tone files:

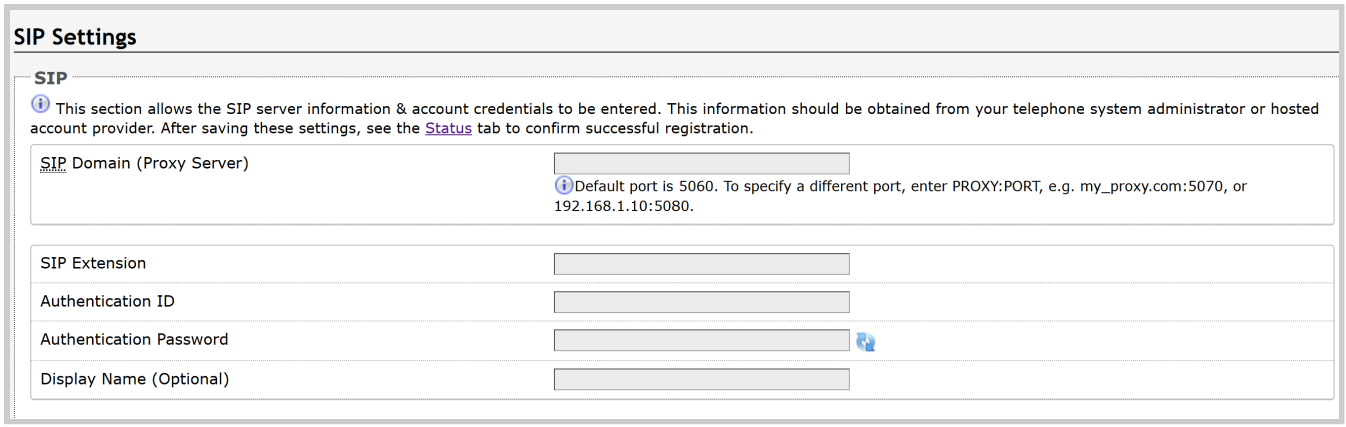
1. Go to **System** → **Tones**.
2. In the **Cache** section, select **Test Tones**.
3. In the **Test Tones** section, select an audio file and select **Play** or **Loop**.
4. To stop the playback, select **Stop**.

Appendix: Web Interface Reference

This section provides an overview of the pages and settings available in the 8211/8212 web interface. It describes the purpose of each configuration page to help you locate and configure the settings required for your deployment.

SIP Settings

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** page to confirm the registration was successful.



SIP	
SIP Domain (Proxy Server)	The SIP Server's IP address (e.g., 192.168.1.111) or don
SIP Extension	Enter the SIP extension of the 8211/8212.
Authentication ID	The Authentication ID is associated with the page ext servers.
Authentication Password	This is the SIP password for the registered SIP accou Contact your System Administrator for the password.
Display Name (Optional)	Enter the name you want to display on the receiving d shown, the PBX and phone(s) must be configured to

Features Settings

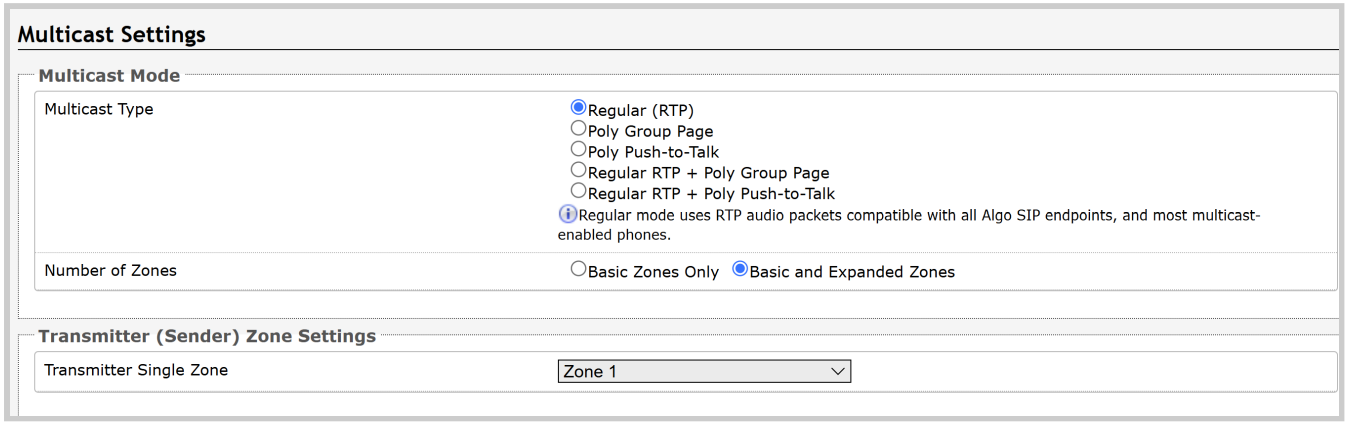
The **Features** tab under **Basic Settings** allows you to configure the API password used to authenticate API requests to the target device.

Remote Device Settings	
Remote Device RESTful API Password	When your device sends an API reque The password must match the RESTfu

Multicast Settings

The **Multicast** tab under **Basic Settings** allows you to configure your device to transmit multicast audio to compatible Algo IP endpoints, multicast-enabled IP phones, and supported Poly devices. You can configure the multicast type, zones, and Poly group paging settings.

> **Note**
>
> Always ensure that the multicast settings (such as zone numbers, the multicast IP address, and port definitions) on all receiver devices match those of the transmitter device.



Multicast Mode	
Multicast Type	The 8211/8212 may broadcast multicast paging co most multicast-enabled phones that use RTP audi • **Regular (RTP)**: Multicast only to Algo IP endp • **Poly Group Page** or **Poly Push-to-Talk**: Multic • **Regular RTP + Poly Group Page** or **Regular R** IP endpoints, and multicast-enabled phones.
Number of Zones	• **Basic Zones Only:** Configure nine or fewer mu • **Basic and Expanded Zones:** Configure up to 5 basic Receiver zones but are hidden by defau

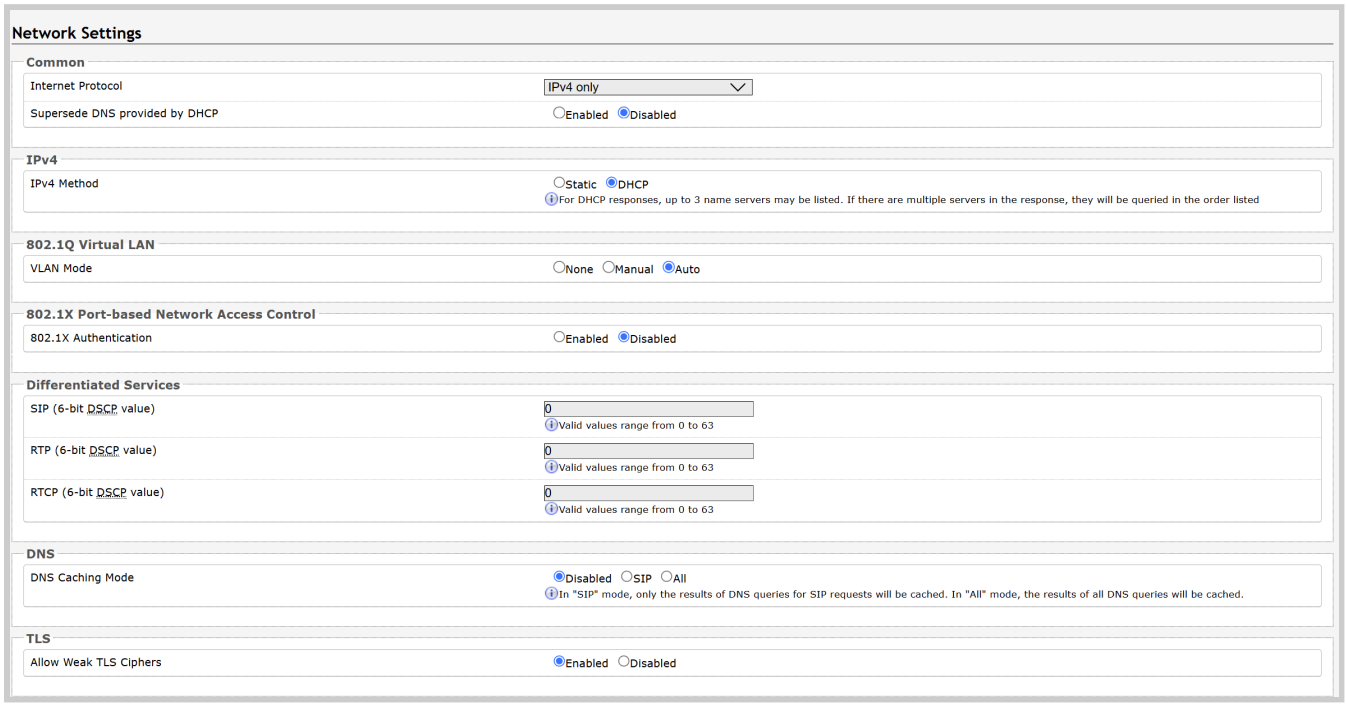
Poly Group Paging/Push-to-Talk This section is used if the Multicast Type includes Poly Group Page or Poly Push-to-Tall	
Poly Zone	Enter the same Multicast IP Address and Port numl
Poly Default Channel	Select the default group for the multicast stream tc

Network Settings

The **Network** tab under **Advanced Settings** allows you to configure how the device connects to your IP network, including IP addressing (DHCP or static), DNS, and

IPv4/IPv6 settings. These settings ensure the device can communicate with SIP servers, cloud services, and other network resources.

> **Note**
>
> Available settings may vary depending on your product model and firmware version.



Common	
Internet Protocol	Use the dropdown to select IPv4 Only or
Supersede DNS provided by DHCP	When enabled, this configuration allows been provided via DHCP.

IPv4	
IPv4 Method	• **Static**: The device will use the IP ad • **DHCP**: The specified DHCP server w DHCP is selected by default.
IPv4 Address/Netmask	Enter the static IP address and netmask equivalent to a netmask of 255.255.255.
IPv4 Gateway	Enter the gateway address.

IPv6	
IPv6 Method	The device can be set to a static or DHCI

	DHCP is an IP standard designed to simp automatically configure IP addresses for When **Static** is selected, the device will u
IPv6 Address/Netmask	Enter the static IP address and netmask (
IPv6 Gateway	Enter the gateway address.

ICMPv6 Options	
Destination Unreachable Messages	Enable to restrict traffic by filtering ICMP
Neighbor Discovery Redirect Messages	Enable to restrict traffic by filtering ICMP
Anycast Echo Replies	Enable to restrict traffic by filtering ICMP
Enable Rate Limiting Outbound Messages	Enable to limit the device to respond to o receiving multiple requests at the same ti
Rate Limit (packets per second)	Specify the packets per second allowed f

802.1Q Virtual LAN

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

VLAN Mode	None: Disable VLAN. Manual: Configure a VLAN by specifying Auto: Detect VLAN information automatic
VLAN ID	Specify the VLAN that the Ethernet frame All other values may be used as VLAN ide The reserved value 0x000 indicates that specifies only a priority and is referred to
VLAN Priority	Set the frame priority level. Otherwise kn refers to the IEEE 802.1p priority or frame

802.1X Port-based Network Access Control	
802.1x Authentication	Enable to add credentials to access LAN your IT Administrator for this information.
Authentication Mode	Select the desired authentication mode.
Anonymous ID	If configured, the device will send the an

ID	The ID should contain a string identifying Administrator for details.
Password	Ask your IT Administrator for details.
Validate Server Certificate	Enable to validate the authentication serv the **System** → **File Manager** to upload a I certs folder.

Differentiated Services	
SIP (6-bit DSCP value)	Enter the Differentiated Services Code Pc
RTP (6-bit DSCP value)	Enter the DSCP value for RTP packets.
RTCP (6-bit DSCP value)	Enter the DSCP value for RTCP packets.

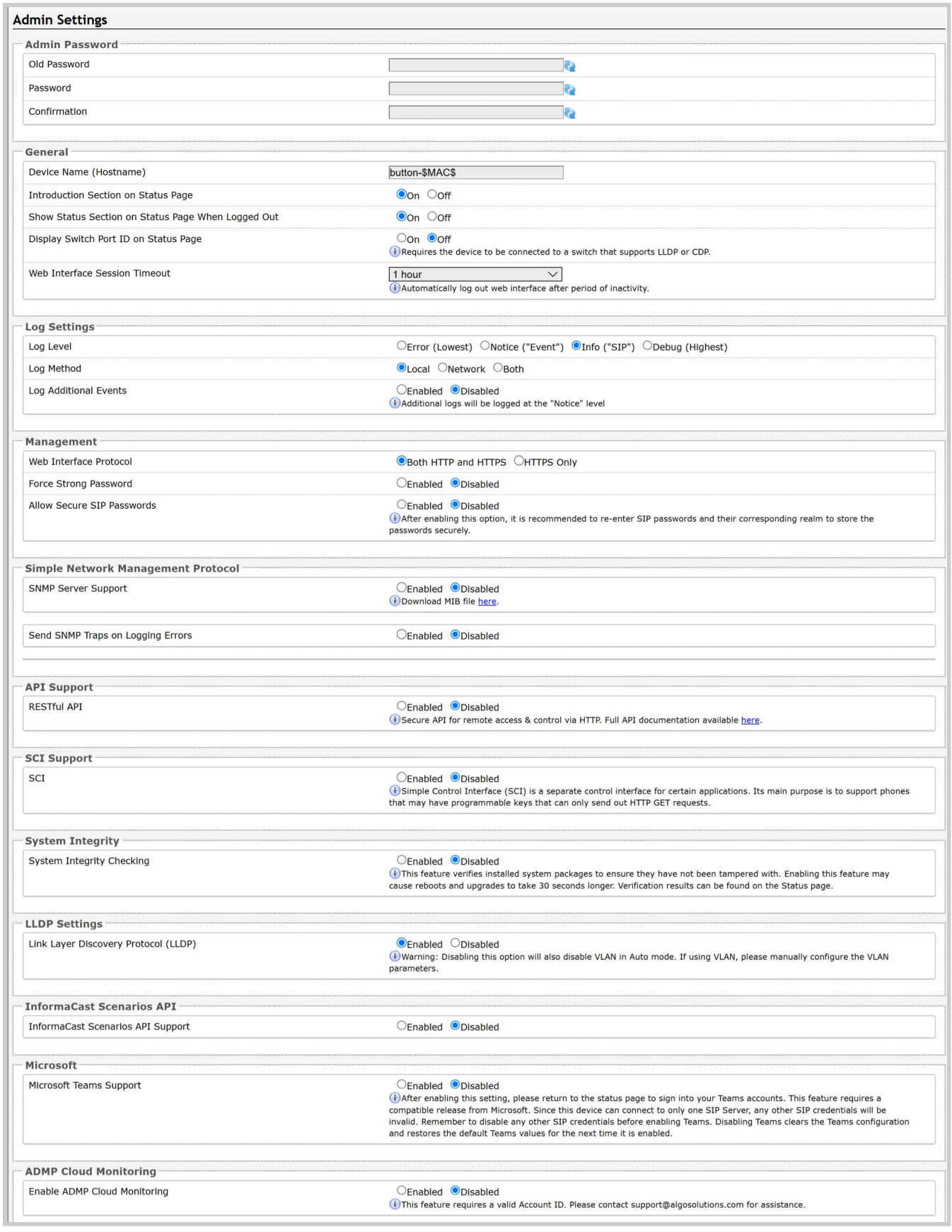
DNS	
DNS Caching Mode	There are three mode options: • **Disabled**: No DNS queries will be ca • **SIP**: Only the results of DNS queries • **All**: The results of all DNS queries w

TLS	
Allow Weak TLS Ciphers	Enables compatibility with legacy systems that m

Admin Settings

The **Admin** tab under **Advanced Settings** allows you to configure device access, security, management, monitoring, and integration features.

From this page, you can change administrator credentials, manage logging and network management settings, enable APIs and external services, and configure device maintenance options.



Admin Password

Old Password	Enter the old admin password. The default password
Password	Enter a new admin password to log into the device w If the password is forgotten, you must reset the devic will be reset to the original default settings as well.

	To enforce a strong password, see Login Password R To reset the device using the button, see Restoring F
Confirmation	Re-enter your new admin password.

General	
Device Name (Hostname)	Add a name to identify the device.
Introduction Section on Status Page	Select **On** to show the introduction text on the login s
Show Status Section on Status Page when Logged Out	Select **On** to allow others to view the status page with Select **Off** to hide the settings and configurations on t trusted users can view device information.
Display Switch Port ID on Status Page	Select **On** to display the Switch Port ID on the **Status** connected to a switch that supports LLDP or CDP.
Web Interface Session Timeout	Set the maximum duration of inactivity to log a user o

Log Settings	
Log Level	Select the types of information you want to include ir **Note** Change the **Log Level** only under the guidance of A additional diagnostic information, which may clutte troubleshooting more difficult.
Log Method	Select a log method: **Local**: The log file is saved in RAM on the device. **Network**: Send the log file to an external SysLog serv ease of central access. **Both**: Use both methods.

Network Log Protocol	Select the transport protocol used to send Syslog me
Log Server	Enter the Syslog server address provided by your IT a
Log Additional Log Events	To be used by support@algosolutions.com if necessa

Management	
Web Interface Protocol	HTTPS is always enabled on the device. HTTP is ena **HTTPS Only** mode so requests are automatically red **Note** No security certificate exists since the device can browsers will provide a warning when using HTTP
Force Strong Password	When **Enabled**, you can enforce a secure password password requirements for a strong password are: • Must contain at least 10 characters • Must contain at least 1 uppercase character • Must contain at least 1 lowercase character • Must contain at least 1 digit (0 – 9) • Must contain at least 1 special character
Allow Secure SIP Passwords	When **Enabled**, SIP passwords are stored in the conf recovery. If enabled, navigate to **Basic Settings** → **SIP** and fill c contact your SIP Server administrator or check the S same or different for all the extensions used. All the configured Authentication Password(s) must l extensions have been configured to save the encryp If the **Realm** is changed later, all passwords must be

Simple Network Management Protocol	
SNMP Support	Disabled by default. The existing setting will respond

Send SNMP Traps on Logging Errors	When enabled, the device sends unsolicited SNMP t
SNMP Community String	Speak to your IT Administrator for more information.
SNMPv3 Security	Speak to your IT Administrator for more information.

API Support	
RESTful API	Disabled by default. Enable a secure API for remote For more information, see Algo RESTful API Guide.
Authentication Method	**Select an option:** • **Standard**: A standard authentication payload wi the REST API password (secret key) and the HM string as digest using SHA-256. The HMAC dige formatted as: `[request_method]:[request_ur` • **Basic**: A basic authentication payload requires e encoded string is then included in the `Authoriz` should only be used over secure HTTPS connec • **None**: No authentication payload is required. For more information, see the Algo RESTful API
RESTful API Password	Authentication requires generating a valid HMAC sig device verifies this signature before processing you For more information, see the Algo RESTful API Guic

SCI Support	
SCI	Disabled by default. Simple Control Interface (SCI) i primary purpose is to support phones that may have requests and allow them to initiate events remotely
SCI Password	Enter your SCI password.

System Integrity	
System Integrity Checking	Enable this feature to verify that installed system pa Enabling this feature may cause reboots and upgra found on the Status page.

LLDP Settings	
Link Layer Discovery Protocol (LLDP)	Enables LLDP to exchange network configuration ir

> **Note**
>
> Disabling **Link Layer Discovery Protocol (LLDP)** prevents your device from exchanging network configuration information with the connected network switch. If you are using a VLAN, make sure **Link Layer Discovery Protocol (LLDP)** is enabled, or that the **VLAN Mode** (under **Advanced Settings** → **Network Settings**) is set to **Manual** so you can configuration VLAN settings manually.

InformaCast Scenarios API	
InformaCast Scenario API Support	Enable the device to start an InformaCast Scenario license, as only the output device requires a license
Security Token	Enter the Security Token used for authenticating AP
Include Location	Enable this option to include the device's location ir

Microsoft	
Microsoft Teams Support	Enable to allow the device to register with a Micros minutes to complete, as the device will communica requires a compatible release from Microsoft.

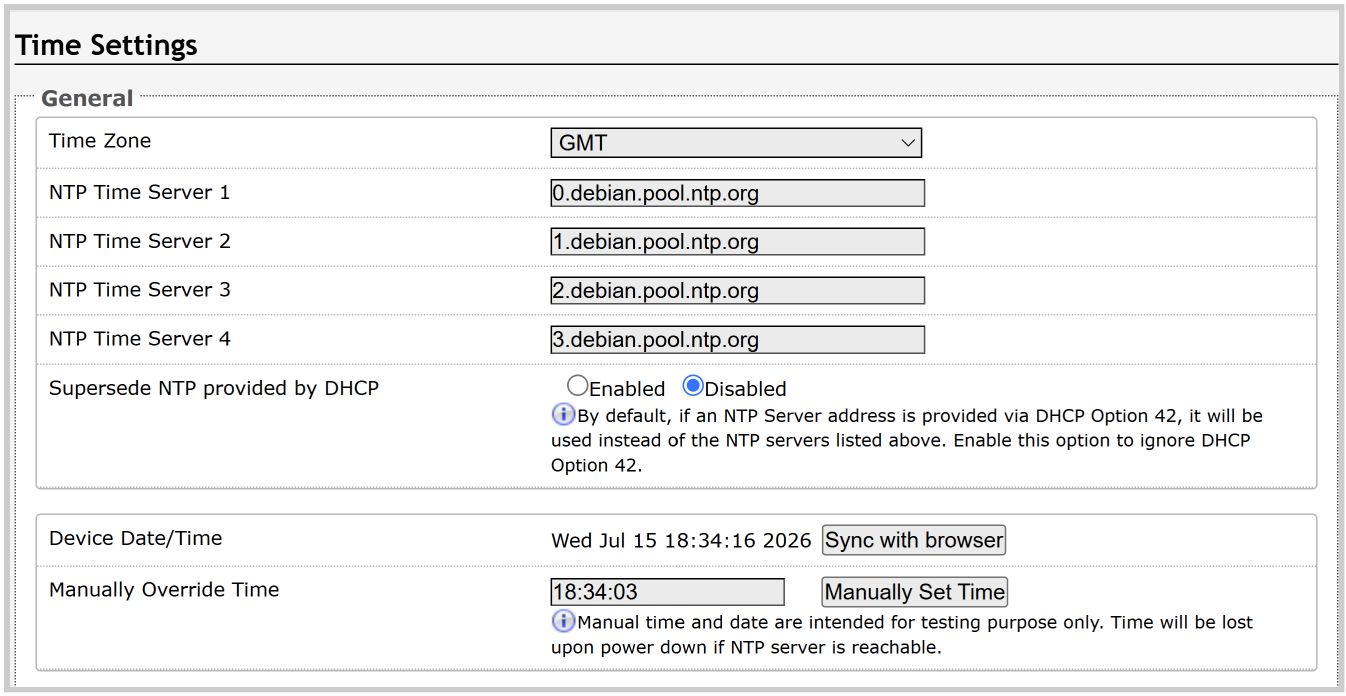
	After enabling this setting, please return to the **Stat** requires a compatible release from Microsoft. For more details, please see the Microsoft Teams C

ADMP Cloud Monitoring	
Enable ADMP Cloud Monitoring	The Algo Device Management Platform (ADMP) sir Algo devices from any location. This feature requir purchase a license, visit the ADMP webpage.
Account ID	Enter the account ID listed on the Settings page of
Allow Configuration File Sync	Enable ADMP to query and display settings stored
Heartbeat Interval	Select how often ADMP should check the status of
Enable Panic Button Monitoring	Enable to monitor Panic Button status in ADMP, inc • Device IP address, MAC address, and product • Panic Button status (online, offline, idle, activat • Event logs for the Panic Buttons

Time Settings

Time configures the device's date, time, time zone, and Network Time Protocol (NTP) settings to ensure accurate timekeeping and proper scheduling of time-based features.

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



Time Settings	
Time Zone	Use the dropdown to select the time zone requ
NTP Time Server	The interface will attempt to use **Time Server 1** unresponsive. These settings are pre-populated with public N requires an internet connection. Alternatively, t hosted or premise-based.
Supersede NTP provided by DHCP	By default, if an NTP Server address is provide listed above. Enable this option to ignore DHCP
NTP Symmetric Key Authentication	To enable, create a new folder in the tab **Syste** symmetric key file and rename the file to *ntp.ke*
Device Date/Time	This field shows the current time and date set does not have access to an external NTP serve device. This time value will be lost at power down or ov date are used for logging purposes.
Manually Override Time	Manual time and date are intended for testing p server is reachable.

Provisioning Settings

Provisioning configures automatic device provisioning, allowing the device to retrieve configuration files and updates from a remote provisioning server.

For more information, see Central Provisioning of Algo IP Endpoints.

Provisioning Settings

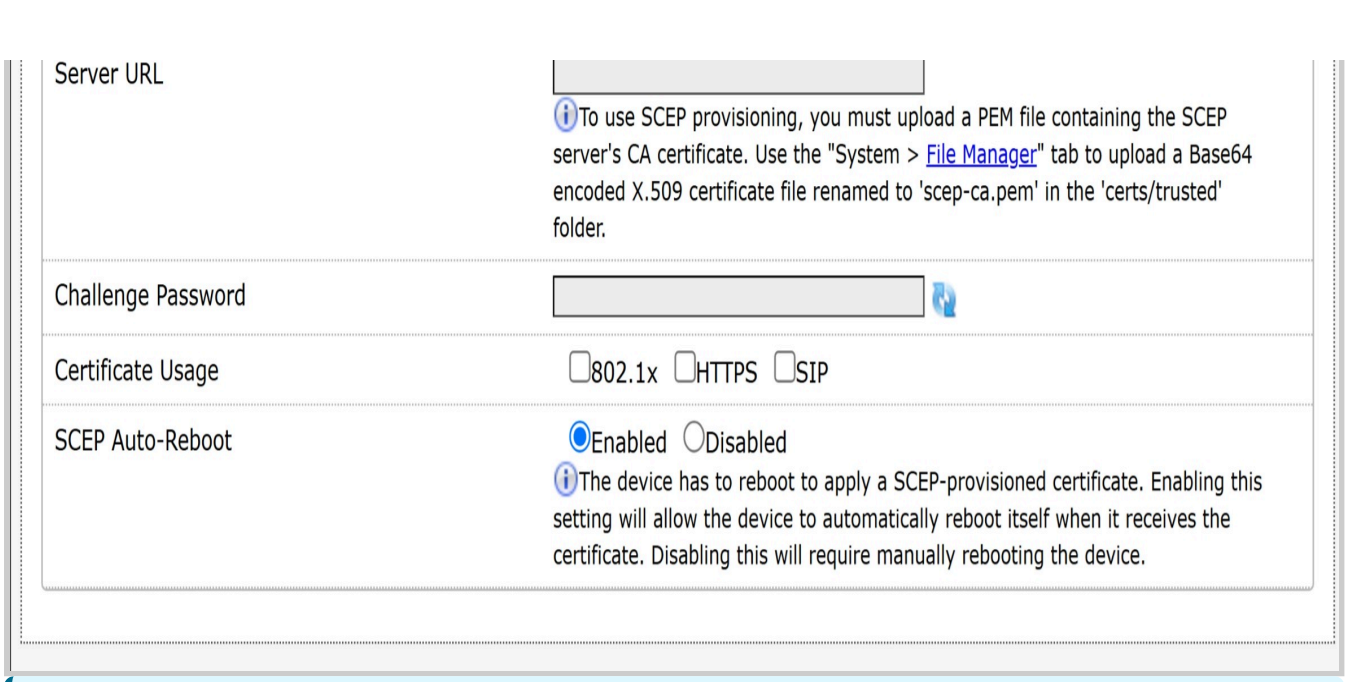
Mode

Provisioning Mode	(•) Enabled ( ) Disabled

Settings

Server Method	(•) Auto (DHCP Option 66/160/150) ( ) DHCP Option 66 only ( ) DHCP Option 160 only ( ) DHCP Option 150 only ( ) Static ⓘ Auto mode automatically checks all 3 DHCP options for an active provisioning server, in the order listed.
Download Method	(•) TFTP ( ) FTP ( ) HTTP ( ) HTTPS
Config Download Path	
Firmware Download Path	
Partial Provisioning	( ) Enabled (•) Disabled ⓘ Allow support for "-i" incremental provisioning files. Disable for enhanced security if not using this feature.
Check-sync Behavior	(•) Always Reboot ( ) Conditional Reboot ⓘ If 'Conditional Reboot' is selected, the device will check with the provisioning server and only reboot if new config is found (unless 'reboot=true' is provided as a parameter in the check-sync event).
Sync Start Time	ⓘ Schedule a time (HH:mm:ss) for the device to perform a sync according to the 'Check-sync Behavior' option above. Leave blank to disable the feature.
Sync End Time	ⓘ If set, the device will sync at a random time in the window between Start Time and End Time. Setting an End Time earlier than Start Time indicates an overnight period. Leave blank to sync at Start Time exactly.
Sync Frequency	(•) Daily ( ) Selected Days Only
Zero Touch Provisioning	Turn Off ZTP ⓘ ZTP is disabled and can only be re-enabled with a factory reset.

SCEP Settings



Note

It is recommended that **Provisioning Mode** be set to **Disabled** if this feature is not in use. This will prevent unauthorized re-configuration of the device if DHCP is used.

Mode	
Provisioning Mode	Enabling provisioning allows installers to pre-configure the d typically done for large deployments to save time and ensure It is recommended that **Provisioning Mode** be set to **Disable** unauthorized re-configuration of the device if DHCP is used.

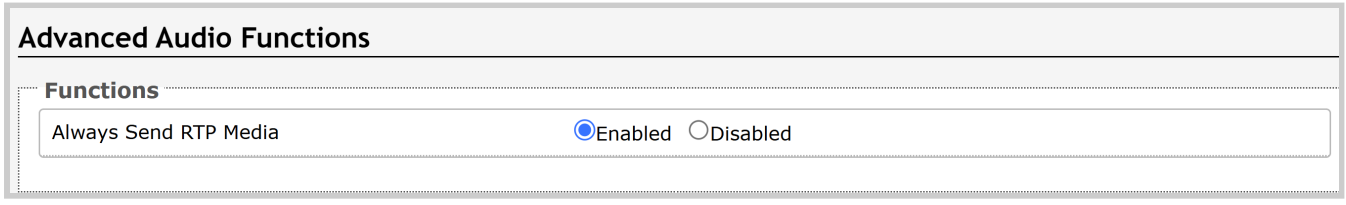
Settings	
Server Method	Set to **Auto** by default. Select a Server Method. • **Auto**: All three DHCP options (66, 160, 150) will be autor • **DHCP Option 66 Only**: Only DHCP Option 66 will be che • **DHCP Option 160 Only:** Only DHCP Option 160 will be c • **DHCP Option 150 Only**: Only DHCP Option 150 will be c • **Static**: Only the specified static server will be checked f For provisioning to work with a DHCP option, DHCP must be **IPv4**.
Static Server	Enter the server address or domain.
Download Method	Select your preferred method for downloading provisioning • TFTP (Trivial File Transfer Protocol) — See MD5 Checks • FTP

	• HTTP • HTTPS — This may help prevent configuration files fron sensitive data stolen. The device configuration files can be automatically downloa 66. This option code (when set) supplies a TFTP boot serve One of two files can be uploaded on the provisioning server • Generic (for all Algo 8211/8212) algop8211/8212.conf • Specific (for a specific MAC address) algom[MAC].conf Both protocol and path are supported for Option 66, allowin
Config Download Path	Enter the path where the configuration file is located in the p
Firmware Download Path	Enter the path where the firmware file is located in the provi
Partial Provisioning	Enable to allow support for "-i" incremental provisioning file required.
Check-sync Behavior	Select **Always Reboot** to set the device to always reboot de Select **Conditional Reboot** to set the device and check the p found (unless "reboot=true" is provided as a parameter in th
Sync Start Time	Set a time (HH:MM:SS) for the device to perform a sync acc this blank if not needed.
Sync End Time	If set, the device will sync randomly in the window between Time earlier than the Start Time indicates an overnight perio
Sync Frequency	Select the sync frequency. Frequency can be set to Daily or
Sync Days	Select the days of the week for syncs to occur.
Zero Touch Provisioning	ZTP is enabled by default, allowing the device to automatica provisioning server. However, to protect the device from unintended or malicious if any of the following occurs: • You make any changes to the device configuration. • You click the **Turn Off ZTP** button manually. **Note** Once ZTP is disabled, it can only be re-enabled by pe

SCEP Settings	
Server URL	Enter the URL of the Simple Certificate Enrollment Protocol (device. The SCEP server's CA certificate must be uploaded **Note** To use SCEP provisioning, you must upload a PEM file con **System** → **File Manager** tab to upload a Base64 encoded the 'certs/trusted' folder.
Challenge Password	Enter the challenge password used to authenticate the devic server.
Certificate Usage	Select where the SCEP-provisioned certificate will be used: services.
SCEP Auto-Reboot	Enable to automatically reboot the device after it receives a apply the certificate. If disabled, the device must be reboote

Advanced Audio Settings

Advanced Audio allows your device to send audio packets at all times.



Functions	
Always Send RTP Media	Enable to send audio packets at all times, ev server expects to always see audio packets.

Advanced SIP Settings

Advanced SIP configures advanced SIP communication settings, such as registration, session timers, transport, codecs, and other protocol options to optimize interoperability and call performance.

General	
SIP Transportation	Select a transport layer protocol to use for SI • **Auto**: Will check the DNS NAPTR record, • **UDP** • **TCP** • **TLS**: Ensures the encryption of SIP traffi authenticated, a PEM file containing both device. Upload a certificate via **System** -
SIPS Scheme	Only visible when **SIP Transportation** is set t endpoint to be secure.
Validate Server Certificate	Enable validation of the SIP server against cc navigate to **System** → **File Manager** to uploa format to the **certs** folder.
SIP Outbound Support (RFC 5626)	Enable this option to support best networking the device is registered with a hosted server **Note** Only enable this option if the SIP server su
Outbound Proxy	Enter the IP address for an outbound proxy.
Register Period (seconds)	Enter the maximum requested period that the 3600 seconds (1 hour). **Note** if the SIP response 200 (OK) provides an E Period defined time here. Only change if instructed to do so.
Rate Limit SIP Registration	This option should be used in cases where m Select a rate limit to stagger registration requ same time.

Wait for Successful Unregister	Enable to wait for the device to successfully configuration changes and reboots.

SRTP	
SDP SRTP Offer	Select an option from the dropdown menu: • **Disabled** • **Standard**: Encrypts RTP voice data to sec other party does not support SRTP. This c not left out for third parties to reconstruct • **Optional** (Non-standard AVP Profile): If th unencrypted.
SDP SRTP Offer Crypto Suite	The encryption and authentication algorithms

NAT	
Media NAT	**None:** Disable NAT. **ICE:** Enable advanced NAT support. **STUN:** Enable basic NAT support.
TURN Server	Enter the IP address or domain of the ICE ser
TURN User	Enter the username of the ICE server.
TURN Password	Enter the password of the ICE server.
STUN - Server	Enter the IP address or domain of the STUN

Server Redundancy	
Server Redundancy Feature	Enable to configure up to two secondary bac When enabled, the device will attempt to reg necessary. The configuration allows re-regis until unresponsive.
Backup Server #1, #2	Provided by your SIP provider or IT team.
Polling Intervals (seconds)	Select the time interval for sending monitorir are always polled and the active server may
Poll Active Server	Enable to explicitly poll the current server to automatically and can be disabled to reduce

Automatic Fallback	Enable to allow the device to reconnect with connection is still working.
Polling Method	Select a polling method based on what your

Zoom Phone Local Survivability	
Local Survivability	Enable re-registration with the local Zoom Phone Local Survivabi connection to Zoom fails. This allows sites to maintain a subset o even if connectivity to the Zoom Phone cloud is lost. **Note** Active calls will end when this switch occurs.
Survivability Proxy	Enter the IP address or domain name of the local Zoom Phone Lo node.

Interoperability	
Keep-Alive Method	Select a keep-alive method: • **None** • **Double CRLF**: The device will send NAT.
Keep-Alive Interval (seconds)	Set the interval in seconds that the CRI
Use Outgoing TLS port in SIP Headers	Enable to use of the ephemeral port nu number in SIP Contact and Via headers as Asterisk or FreeSWITCH.
Do Not Reuse Authorization Headers	Enable so all SIP authorization informat request.
Allow Missing Subscription-State Headers	Enable to allow SIP NOTIFY messages
Add MAC in SIP User Agent Header	Specifies whether to include the devic

Advanced Multicast Settings

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

Advanced Multicast Settings

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

Transmitter Settings

Transmitter Output Codec	G.722 When using Two-Way Paging mode, only G.711 and G.722 are supported.
Output Packetization Time (milliseconds)	20
Multicast TTL	1 Only change this setting if custom routing is configured on the network that specifically routes multicast packets between subnets, and a longer TTL count is required. Regular multicast routing does not require a change to this setting.

RTP Control Protocol (RTCP)

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

Basic Zone Definition

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

Transmitter Settings

Transmitter Output Codec	Select an audio encoding format for the Supported formats include: • G.711 ulaw • G.722 • Opus • L16
Output Packetization Time (milliseconds)	Select the size of the audio packets the default of 20 milliseconds is recommen other devices.
Multicast TTL	Only change the multicast time to live (T specifically routes multicast packets be are not bounced back and forth in a net

RTP Control Protocol (RTCP)	
RTCP Port Selection	Select how a port will be chosen to send **Note** If **Next Higher Port** is selected, ensure are only assigned to even-numbered p packets.

Appendix: Compliance and Safety

Product Warnings

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 802.3at- or

802.3af-compliant network PoE switch. The product is intended for installation indoors. 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**.

Emergency Communication
If used in an emergency communication application, the 8211/8212 should be routinely tested. SNMP or ADMP supervision is recommended for assurance of proper operation. Contact Algo for other methods of operational assurance including the use of the integrated microphone for automated “sound to air” acoustic testing.