8450 IP Console User Guide

Updated on Jun 10, 2025 • Published on Jun 9, 2025

51 minute(s) read

The 8450 IP Console optimizes user experience and communication effectiveness for announcement broadcasting and emergency alerting. With a customizable GUI and 10.1" LCD touchscreen, the 8450 is used as an input device to activate paging or emergency alerts.

A gooseneck microphone allows for daily announcements, while touchscreen buttons can activate pre-recorded messages or alerts. The tactile, backlit action button can also be configured for push-to-talk, screen activation, or screen lock. Ideal for education, health, and other facilities with unique paging needs, the 8450 integrates easily into IP paging ecosystems through SIP, multicast, and API. Configurable via web interface and mountable to a desk, wall, or rack in landscape orientation, the 8450 adds flexibility and ease to IP paging environments.

Included

- 8450 IP Console

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.

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

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

Important
This guide contains safety information which should be read thoroughly before permanently installing the product.

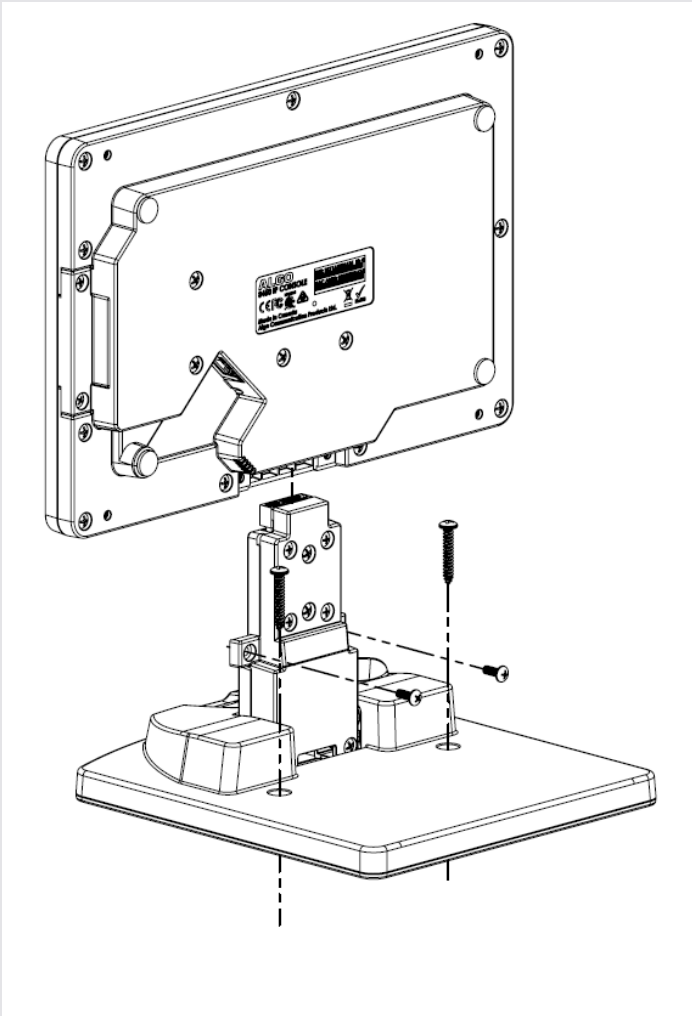
Dry Indoor Location Only
The 8450 IP Console is intended for dry indoor locations only with ambient temperatures of 32 °F - 104 °F (0 °C - 40 °C).
CAT5 or CAT6 connection wiring to an IEEE 802.3af compliant network PoE switch must not leave the building perimeter without adequate lightning protection. No wiring connected to the 8450 may leave the building perimeter without adequate lightning protection.

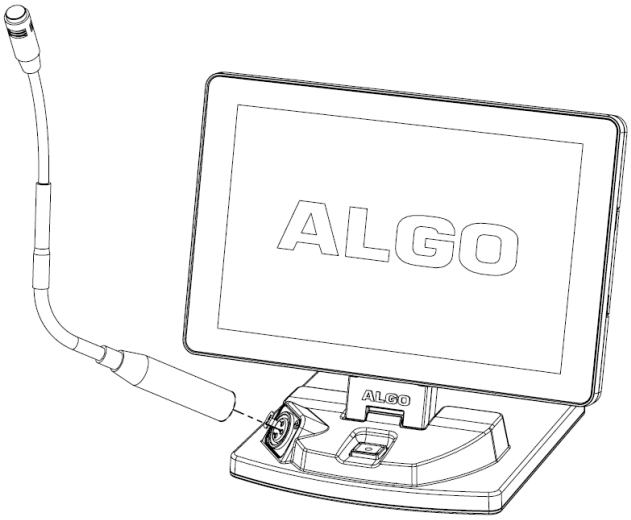
Setup & Installation

Mounting

Use the following instructions to install the stand for desktop use:

1. Install the 8450 IP Console in landscape orientation onto the stand. Remove the docking station cover along the long edge of the console by removing the two Philips head screws.
2. Slide the stand tongue into the docking station gently until fully seated. The retaining screw holes should align with the console threaded inserts to re-install the two Philips head screws.
3. Adjust the friction hinge on the stand as needed by applying firm pressure to the console while holding the stand firmly in place.
4. Although the stand is weighted and equipped with high friction feet to minimize movement, two holes are provided in the stand for securing the console stand to a work surface. Use fasteners appropriate to your work surface material (not included).
5. Connect a network cable from a PoE switch into the RJ45 jack on the rear of the console.
6. If desired, a goose-neck microphone can be connected to the stand for live voice paging.





8450 landscape orientation with desktop mount.	A gooseneck microphone can be connected to the front of the desk mount stand.

Accessing the Web Interface

To configure your device, you must enter the IP address for your device into your browser (see below).

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

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

Web Interface Setup

1. Connect the 8450 to an IEEE 802.3af PoE network switch. The Algo logo will appear on the screen until boot-up is completed (about 30 seconds).
2. Once complete, the IP address of your device should appear on the display momentarily. Once the device fully boots to the Home Screen the IP is accessible via the settings gear in the bottom right corner of the screen. You can also find your device IP address by downloading the Algo locator tool: www.algosolutions.com/locator. The tool is only available for Windows computers.
3. Type the device IP address into a web browser to access the web interface and configure your device for testing. Note that these devices may be configured using centralized provisioning or the Algo Device Management Platform (ADMP).

Check Device Status

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

The Status page contains information such as:

• Device Name • SIP Registration • Call Status • Proxy Status • Provisioning Status • MAC	• IPv4 • IPv6 • Date/Time • Multicast Mode • Volume • Relay Input Status

Register Your Product

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

Reset

A small, round button located next to the ethernet jack at the back of the device can be used to reset the 8450. To return all the settings in the 8450 to the factory default, reboot or power cycle the 8450. To do this, wait until the blue LED on the back of the device flashes (visible in the product label), then press and hold the reset button until the LED begins a double flash pattern. Release the reset button and allow the unit to complete its boot process.

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

Once booting is complete, the IP address should appear on the screen if the device is in the factory reset state.

Security

Algo devices use TLS for provisioning and SIP signaling to mitigate cyberattacks by those trying to intercept, replicate, or alter Algo products. Algo devices also come pre-loaded with certificates from a list of trusted certificate authorities (CA) to ensure secure

communication with reputable sources. Pre-installed trusted certificates are not visible to users and are separate from those in the ‘certs’ folder.

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

Display Configuration

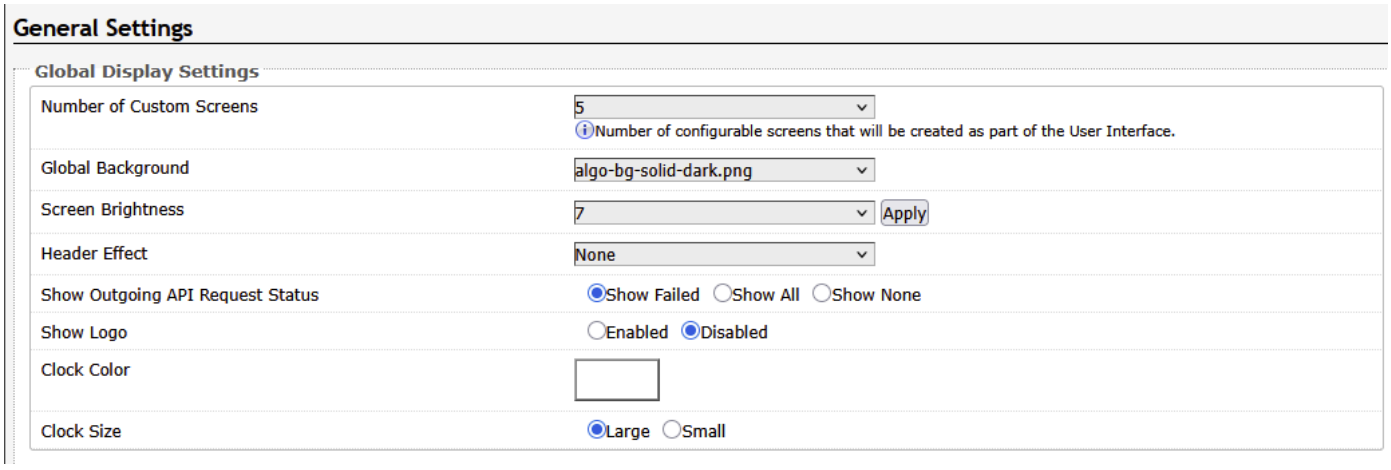
The 8450 was designed to allow users to create a visual menu of paging and emergency alerting actions. Groups of commands can be configured on screens by applying and configuring buttons to perform specific actions.

When configuring an 8450, it is important to consider the following:

1. What general display settings are needed?
2. What screens are needed beyond the defaults?
3. What should the home screen be? The lock screen?
4. What actions need to be available on each screen?
5. What additional requirements does the device need? Passcode? Timeout?

Essential Device Settings

Configure the general visual device settings that will apply to all screens through **Basic Settings > Display**.



Global Settings	

Number of Custom Screens	Select the number of configurable screens required for the user interface.
Global Background	Select a background image to use for the device. Images can be uploaded in the File Manager. The ideal dimensions of a background image are 1280×800.
Screen Brightness	Select screen brightness on a scale of **1** to **7**.
Header Effect	Appears at the top of the device screen. Select **None**, **Light**, **Dark**, or **Solid Color** when contrast is needed at the top of the screen for the clock placement.
Show Outgoing API Request Status	Controls whether API success or failure messages appear on the screen. Choose from **Show Failed**, **Show All**, and **Show None**.
Show Logo	Select a logo. Upload custom logos to be listed in the File Manager under the **logos** folder.
Clock Color	Select a clock font color.
Clock Size	Choose a **Large** or **Small** clock size.

Apply Theme

Themes allow you to quickly change the visual appearance of the device.

Apply Theme	
Theme	Selecting a theme changes the visual settings under Basic Settings > Display to a pre-configured value based on the selected theme. To preview the theme select “Load”. After loading select Save to apply the theme.

Navigation Bar

The Navigation Bar helps you easily access screens. Only default screens can be accessed via the nav bar. Other custom screens must be “linked” via a button. Alternatively, a custom screen with custom buttons can be assigned as the Home Page to access other custom screens.

Nav Bar Settings	
Background Color	Select a background color for the navigation bar.
Icon Color	Select a color for the icons that appear on the navigation bar.
Main Button	When Enabled, the Main Button will appear on the left side of the navigation bar. The screen it is assigned to will have it's icon removed from the right side of the navigation bar. The main button can be used to access the Emergency screen or Paging screen. Alternatively, the clock can be displayed in the bar. The clock can be configured using the **Clock Settings** parameters. 
Back Icon	Will take a user to the previous screen the device had displayed.
Home Icon	Will take a user to the assigned Home Screen.
Directory Icon	Will take a user to the default Directory screen.
Paging Icon	Will take a user to the default Paging screen.
Emergency Icon	Will take a user to the default Emergency screen.
Settings Icon	View the device's **Screen Brightness**, **MAC address**, and **IP Address**. The screen brightness can be adjusted directly on the device.

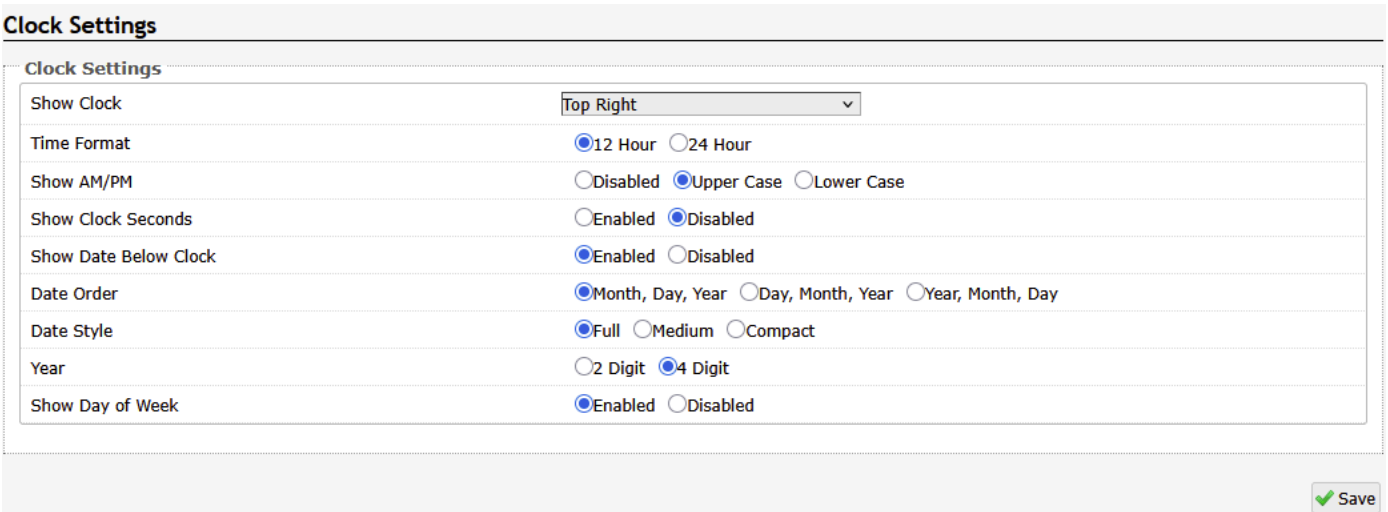
Global Default Button Settings

The global default button settings are used when a new screen with buttons is created. Buttons on a new screen can be configured to use screen-specific settings that are different from the default global button settings.

Button Spacing	Select **Small** or **Large** button spacing. **Small** spacing will result in larger buttons with narrow space between each button while **Large** spacing will result in smaller buttons with wider space between each button.
Button Color	Select a color to fill the button space.
Button Border Color	Select a color to use as the border for the button.
Button Border Thickness	Select **None, Small, Medium, or Large** button border thickness.
Image Position	Select where an image appears on the button if an image is uploaded for a specific button.
Image Size	Select how large an uploaded image should be on a button.
Text Position	Select where button text should be displayed on a button.
Text Color	Select the button text color.

Clock

The device's clock settings can be configured through **Basic Settings > Clock**. A clock can be displayed on any configured screen or on the left side of the navigation bar.



Clock Settings	

Show Clock	Display the time in one of the following positions on a screen: • Top Left • Top Center • Top Right • Center
Time Format	Select a clock format of **12 Hou**r or **24 Hour**.
Show AM/PM	If shown, select if AM/PM is shown in **Upper Case** or **Lower Case**.
Show Clock Seconds	Enable or disable showing clock seconds.
Show Date Below Clock	Enable or disable showing the current date below the clock.
Date Order	Select the date format. Options include: • Month, Day, Year • Day, Month, Year • Year, Month, Day
Date Style	Select the date style. Options include: • Full (ex. Wednesday, March 19, 2025) • Medium (ex. Wed, Mar 19, 2025) • Compact (ex. Wed/03/19/2025)
Separator	If a compact date style is chosen, select the separator to use.
Year	Choose to display the year as **2 digits** or **4 digits**.
Show Day of Week	Enable or disable showing the day of the week.

Lock & Timeout Settings

For security and energy savings, the 8450 can be configured to activate a screensaver or turn off when the device is inactive or locked.

Timeout Settings	

User Interface Timeout	Set an amount of inactivity that will cause the device to perform a set action.
Timeout Action	Set the device to **Go to Home Screen**, **Show Image**, or **Turn Off Screen**, **None**, or **Lock Screen** after the device has been inactive for a set amount of time.
Timeout Image	If the device timeout action is set to **Show Image**, set an image to display.
LCD Brightness after Timeout	If the device timeout action is set to **Go to Homepage** or **Show Image**, or **None** use this parameter to dim the display if desired.

Lock Settings	
Lock Icon in Nav Bar	Control whether a lock icon will appear in the navigation bar. If enabled, the device can be locked by tapping this icon.
Lock on Startup	If set, the device will enter the locked state upon starting.
Lock Action	Set the device to **Go to Homepage**, **Show Image**, or **Turn Off Screen**, or **None** after the device has been inactive for a set amount of time.
Lock Image	If the device timeout action is set to **Show Image**, set an image to display.
LCD Brightness after Lock	If the device timeout action is set to **Go to Homepage**, **Show Image**, or **None** use this parameter to dim the display if desired.
Valid Passcodes	Select which Passcode levels can unlock the device when locked. Passcodes can be configured in **Basic Settings > Passcodes**.

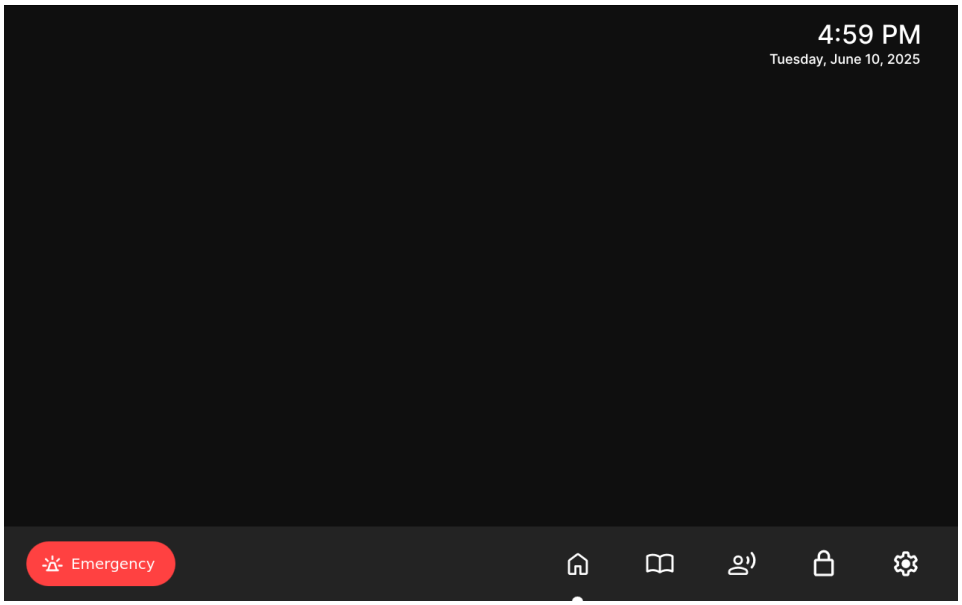
Passcode Protection

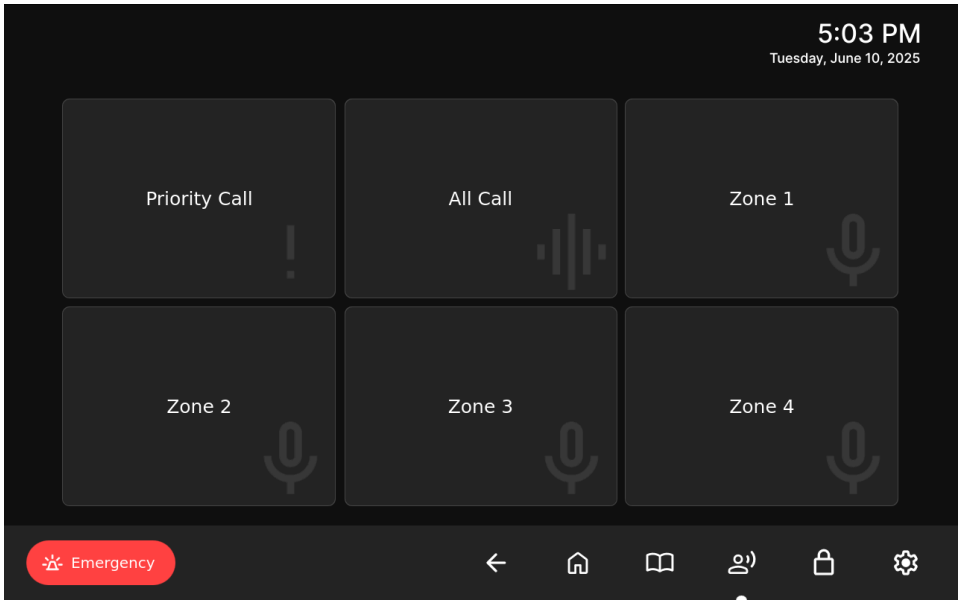
Up to five distinct passcodes can be configured to limit device users to specific functions or controls. After passcode levels are set, they can be enabled for accessing the device in general and to activate a button action. Passcodes can be configured in **Basic Settings > Passcodes**.

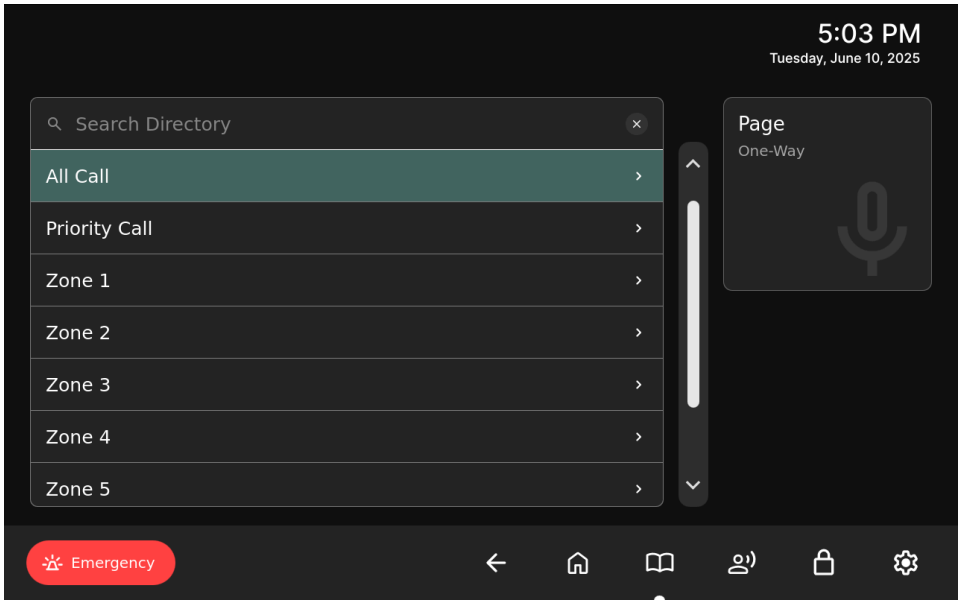
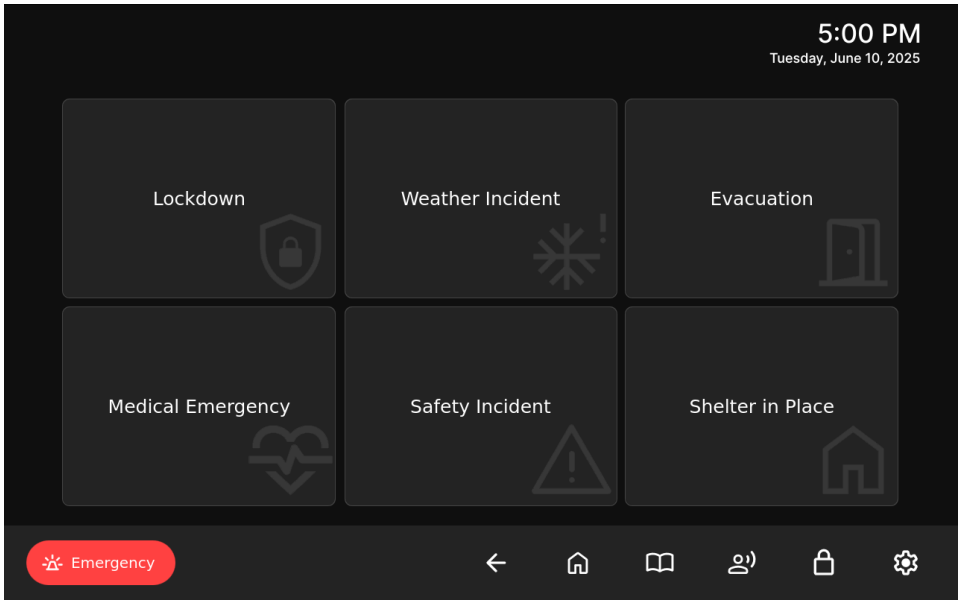
Passcode Settings	
Level 1-5	Rename the passcode if desired (for example, “Access All”, “Limited Access”, or “Emergency Access Only”). Enter the passcode. Share the passcode(s) with others who should have access at the configured level. Passcodes can be assigned to unlock the device via **Basic Settings > Lock & Timeout** or for individual button actions via the **Screens** tab. For more details on how to manage passcodes and button action access, see the Button section.

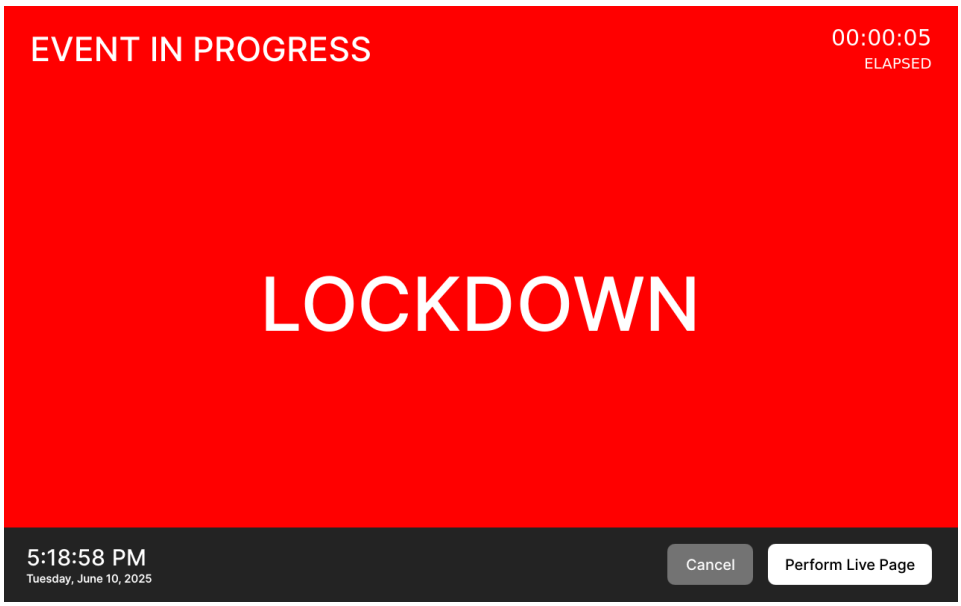
Default Screens

There are four screens available by default. Users can add up to 20 more. The defaults are:

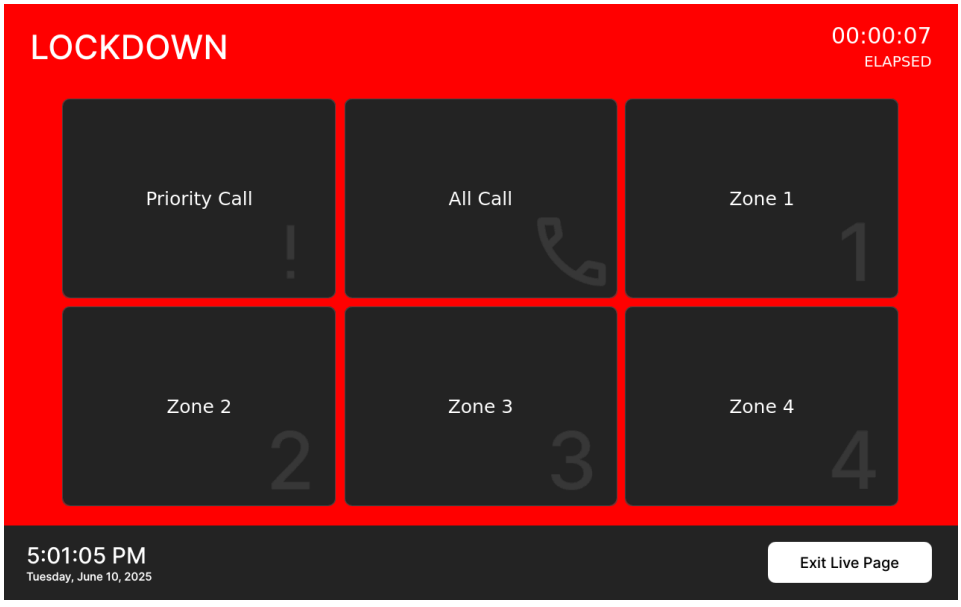
Home	The Home screen is the first screen shown when the device starts. Up to 16 buttons can be added to the home screen to perform actions or link to other screens. 
Paging	The default Paging screen can be accessed from the navigation bar if the Paging icon is enabled. By default, there

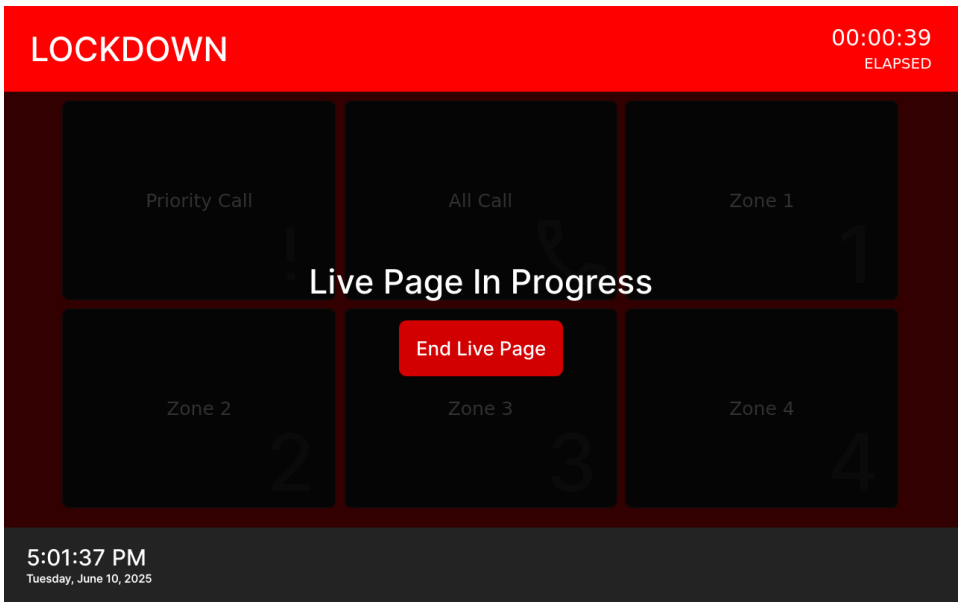
	will be six buttons with all buttons having their action set to **One-way Mic Multicast**. 
Directory	The default Directory screen can be accessed from the navigation bar if the Directory icon is enabled. The Directory screen will display an assigned Address Book File. An Address Book File can be uploaded in the File Manager to addressbook. To create a tab-delimited text file using Microsoft Excel: 1. Open your spreadsheet and go to File → Save As. 2. Change Save as type or Format to Text (Tab delimited). 3. Enter a name for the document and click Save.

	
Emergency	The default Emergency screen can be accessed from the navigation bar if the emergency icon is enabled. By default, there will be six buttons with all buttons having their action set to **Start Emergency Alert**. 



Emergency Paging	The Emergency Paging screen can only be accessed via the default Emergency screen by pressing Perform Live Page. When an emergency alert is activated, there will be an option to broadcast a live page over top of the alert. This screen is available through **Advanced Settings > Emergency Paging**.



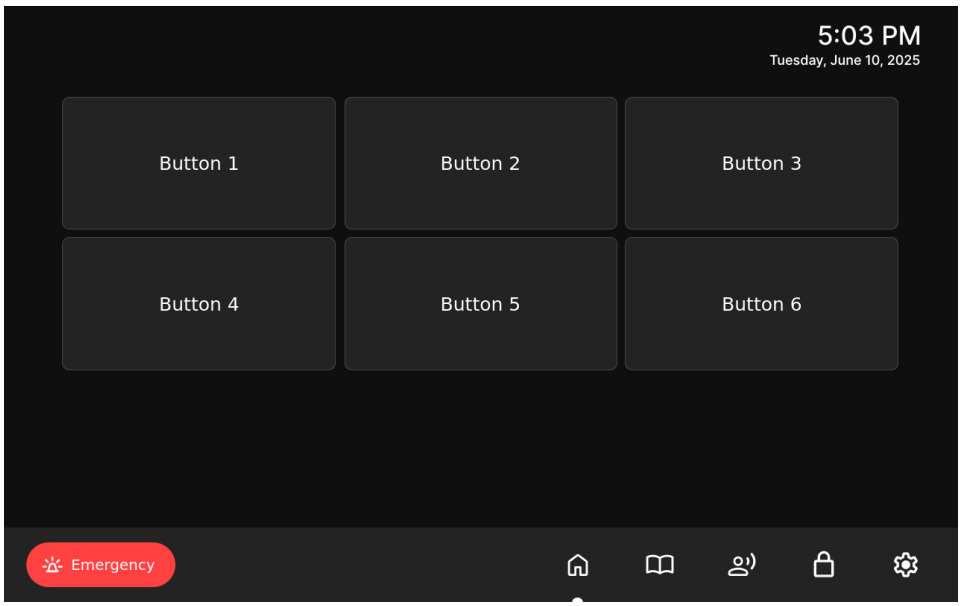
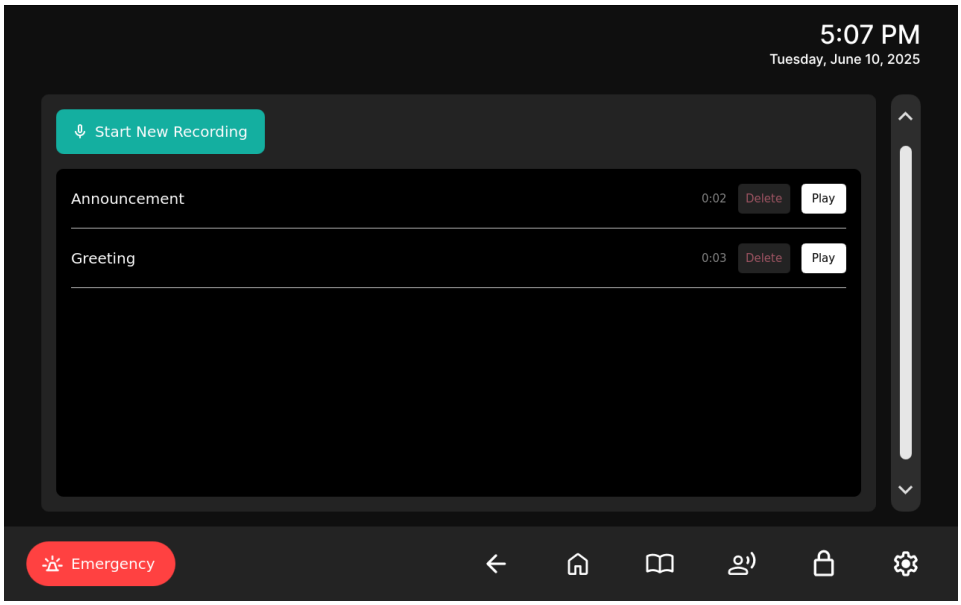
	
Screen #	The 8450 supports up to 20 custom screens. Additional Custom Screens are available via **Basic Settings > Display > Global Display Settings > Number of Custom Screens**.

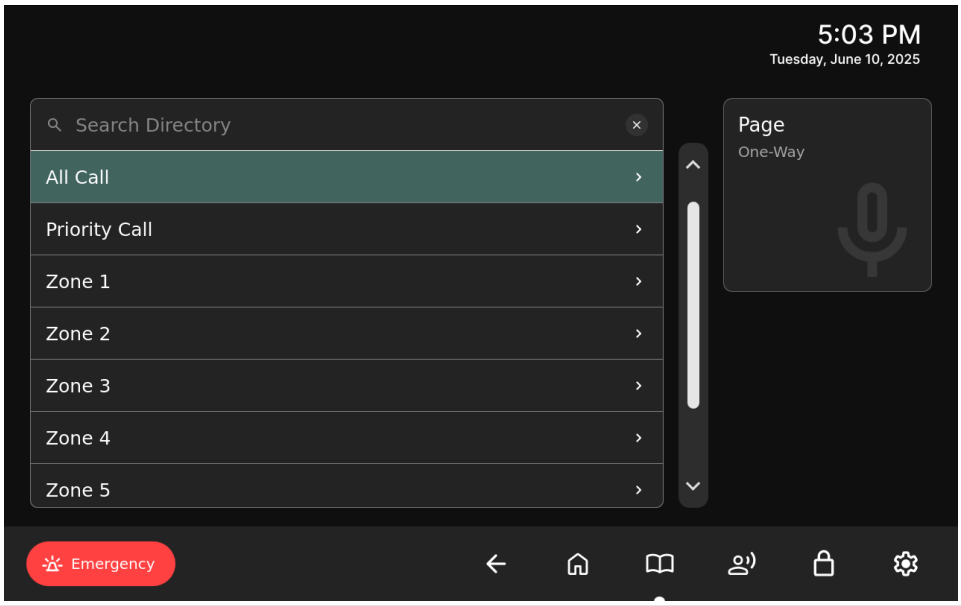
Custom Screens (Screen Types)

In addition to the out-of-box screen configurations, custom screens can be added and customized. When creating a new screen, the first step is to select a screen type.

Screen types include:

Button	Use to create a screen similar to the Emergency and Paging screens with buttons that perform specified actions. See the button section below for more details.

	
Recordings	A recordings screen can be created to record audio via the connected gooseneck microphone. 
Directory	Use to create a screen similar to the default Directory screen. The Directory screen will display an assigned Address Book File. An Address Book File can be uploaded in the File Manager to addressbook. To create a tab-delimited text file using Microsoft Excel:

	1. Open your spreadsheet and go to File → Save As. 2. Change Save as type or Format to Text (Tab delimited). 3. Enter a name for the document and click Save. 

Templates

Algo includes a number of pre-configured screens called templates. A template is a configuration that controls every button and setting on a screen. Applying a template will overwrite all general and button settings for that screen.

Template	Instead of creating a custom screen from scratch, a template can be used. When a template is selected and applied, the web interface will refresh to show the template parameters. Templates include: • Emergency • Paging • Directory (Paging) – 6 • Directory (Paging) – 50

General Screen Settings

Default and custom screens all have the same general settings for the screen. They include:

Description	Set the description or name of the screen. This will change the name displayed on the screen tab in the web interface.
Background	Choose a screen background.
Show Clock on Page	Enable a clock to be displayed on the screen. Clock settings are configured under **Display → General**.

Buttons

Button Appearance Settings

Under **Display → General → Button Settings**, adjust the default button settings to be used when a new screen with buttons is created. Buttons on a new screen can be configured to use screen-specific settings that are different from the default global button settings.

Button Layout	Select a layout based on the number of buttons required on a screen. 1, 2, 3, 4, 6, 9, 12, or 16 buttons can be displayed on a screen.
Button Appearance	Select **Global** for buttons on the screen to default to global button appearance settings or **Custom** to open and configure button appearance settings for the screen.
Button Spacing	Select **Small** or **Large** button spacing. **Small** spacing will result in larger buttons with narrow space between each button while **Large** spacing will result in smaller buttons with wider space between each button.
Button Color	Select a color to fill the button space.
Button Border Color	Select a color to use as the border for the button.
Button Border Thickness	Select **None, Small, Medium, or Large** button border thickness.
Image Position	Select where an image appears on the button if an image is uploaded for a specific button.
Image Size	Select how large an uploaded image should be on a button.

Text Position	Select where button text should be displayed on a button.
Text Color	Select the button text color.

Basic Button Settings

Button #	**Enable** or **Disable** a button in the layout.
Text	Type in the text to be displayed on the button.
Action	Select an action for the button to perform.

Screen Button Actions

Most button extensions require a SIP page extension to be registered. This should be added before testing button functionality.

Button Actions	
Call with Dialpad	Display a dial pad on the screen to call an extension. Use the mic to communicate a message.
Call Pre-Configured Extension	Call a pre-configured extension number. Use the mic to communicate a message. Use the following configurations when this button action is set: • Call Destination
Make SIP Call with Tone	Call a pre-configured extension number and play a tone or recording on a loop. Use the following configurations when this button action is set: • Call Destination • Tone/Pre-recorded Announcement • Interval Between Tones (seconds) • Maximum Tone Duration

Multicast with Tone	Plays a tone over multicast. If **Remote Mode** is enabled, this will also notify the other 8450 devices in the **Console Group** that this alert is starting. Use the following configurations when this button action is set: • Alert Name • Tone/Pre-recorded Announcement • Alert Duration • Multicast Zone • Send API Requests
Start Emergency Alert	Play a pre-recorded announcement and set additional parameters for emergency alert control, such as requiring a password to cancel or to display a clock of elapsed alerting time. Use the following configurations when this button action is set: • Alert Name • Tone/Pre-recorded Announcement • Secondary Text • Background Color • Text Color • Passcode Required to Cancel • Clock • Elapsed Time • Paging During Emergency • Action Button During Emergency • Interval Between Tones (seconds) • Multicast Zone • Send API Requests
Send API Request	Send an API request to another device or system to activate a specific function or behavior (ex. An API request to an 8063 could unlock a door). Use the following configurations when this button action is set: • Number of API Requests

	• Command • Data Payload • Target Device(s)
One-way Mic Multicast	Broadcast live audio using the attached gooseneck microphone to the configured multicast zone. Use the following configurations when this button action is set: • Multicast Zone • Tone/Pre-recorded Announcement
Go to Screen	Select a page for the button to open. For example, to bring up a page with a dialpad or a page with buttons for playing alerts. Use the following configurations when this button action is set: • Target Screen

Screen Button Action Settings

Specific buttons can be configured on the tab of the screen where the button exists.

Call Destination	Input the call extension for the button to call.
Alert Name	Add text that appears on the screen when the alert is triggered.
Tone/Pre-recorded Announcement	Select a tone to broadcast when the button is pressed.
Alert Duration	Select an option to Play Once, Play Until Stopped, or Play Until Stopped Remotely.
Secondary Text	Enter additional text to display on the screen when an alert is activated. The text will appear on the top left of the screen
Background Color	Select a background color for the screen that will appear when an alert is activated.
Text Color	Select a text color to use for the text on the screen that will appear when an alert is activated.

Passcode Required to Cancel	Set a passcode that must be entered before canceling an event. This setting is ideal for situations that require evacuation to prevent an unauthorized individual from wrongly canceling the active alert.
Clock	Enable a clock to be displayed on the bottom left corner of the screen.
Elapsed Time	Enable a timer to be displayed in the top right corner of the screen to show how long the emergency alert has been active for.
Paging During Emergency	Enable the option to start a live voice paging announcement during the alert. When this happens, the recorded alert will be paused during the live paging announcement and will continue after the live page ends. When the **Perform Live Page** button is pressed, the user will be taken to the screen set up under the default **Emergency Paging** tab in the web interface to select the zone to page to.
Action button During Emergency	Enable the physical button on the stand to be possible to use during an emergency alert.
Interval Between Tones (seconds)	Enter the number of seconds of delay to have before replaying the tone
Multicast Zone	Select the multicast zone for the emergency alert to broadcast to.
Number of API Requests	Supports up to 3 requests (one button press can activate 3 actions/behaviors ex. Strobe light and door unlock and tone play).
Command (API)	Select an API command. See the RESTful API Guide for more information.
Data Payload (API)	Enter the data payload. See the RESTful API Guide for more information.
Target Device(s) (API)	Enter a comma-separated list of devices to receive the API command.

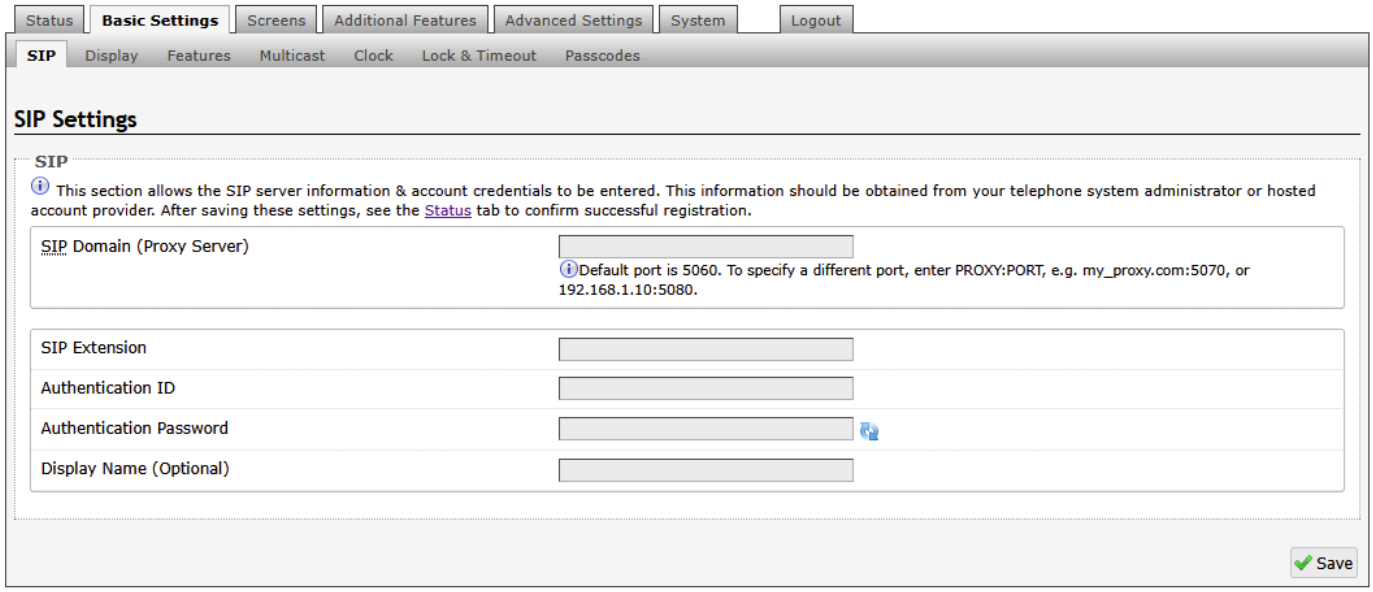
Image	Select an uploaded image or icon to display on the bottom right corner of the button.
Button Protection	Further protect users from starting an action accidentally by enabling a **Password** to activate the button action or a **Confirm** message and additional button.
Valid Passcodes	If **Password** is chosen for additional button protection, select which password can allow button access. Passcodes can be configured under **Display** → **General**.

SIP Configuration

Basic Settings

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

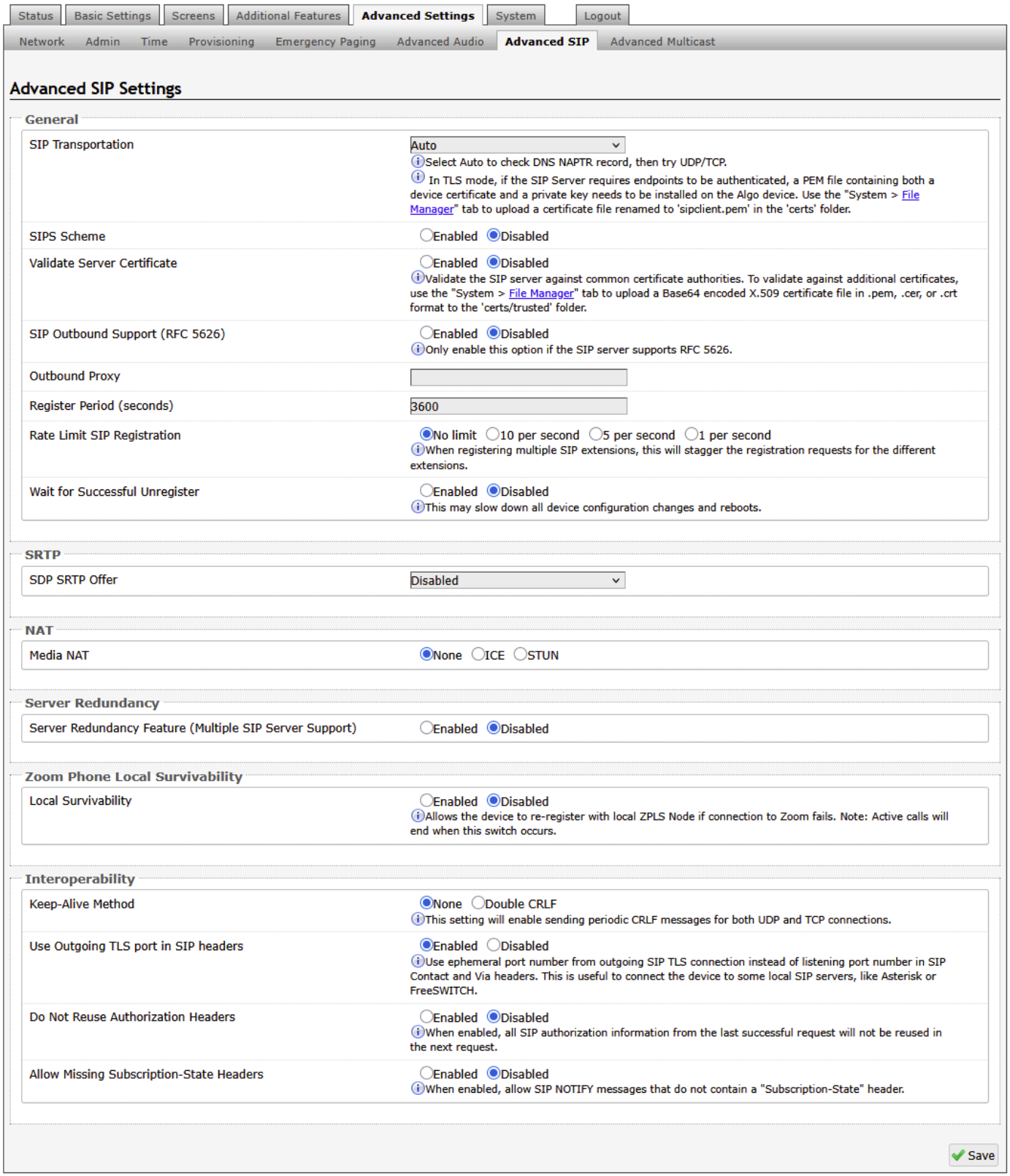
A SIP endpoint license associated with a UCaaS platform may be required to register the 8450. One license will be required per extension registered. If one device has multiple extensions registered, each registered extension will require a license. On a hosted or cloud platform, the required endpoint extension or seat may be treated the same as any other extension on the system and incur a monthly cost or similar fee.



SIP	
SIP Domain (Proxy Server)	The SIP Server's IP address (e.g., 192.168.1.111) or domain name (e.g., myserver.com).
Page Extension	Page extensions auto-answer and open a voice path, enabling live announcements. Enter the SIP page extension so the device will auto-answer any inbound call received on this extension and provide a voice paging path (and multicast if configured).
Authentication ID	The Authentication ID is a name that represents the page extension. It is also referred to as 'Username' for some SIP servers. This may be the same as the Ring or Page extension in some cases.
Authentication Password	This is the SIP password for the registered SIP account. Up to eight (63) characters can be used. The password can be used to authenticate SIP users. Contact your System Administrator for the password to obtain access.
Display Name (Optional)	Enter the name you want displayed when an SIP call is made. For the display name to be shown, the PBX and

	phone(s) must be configured to display this message as the Caller ID.

Advanced SIP



General

SIP Transportation	Select a transport layer protocol to use for SIP messages from the dropdown. These options include: • **Auto**: Will check the DNS NAPTR record, then try UDP/TCP. • **UDP** • **TCP** • **TLS**: Ensures the encryption of SIP traffic. In this mode, if the SIP Server requires endpoints to be authenticated, a PEM file containing both a device certificate and a private key must be installed on the device. Upload a certificate via **System → File Manager** and rename it to 'sipclient.pem' in the **certs** folder.
SIPS Scheme	Only visible when **SIP Transportation** is set to **TLS**. Enable to require the SIP connection from endpoint to endpoint to be secure.
Validate Server Certificate	Enable to validate the SIP server against common certificate authorities. To validate additional certificates, navigate to **System → File Manager** to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the **certs** folder.
SIP Outbound Support (RFC 5626)	Enable this option to support best networking practices according to RFC 5626. This option should be enabled if the device is registered with a hosted server or TLS is used for SIP Transportation. *Only enable this option if the SIP server supports RFC 5626.*
Outbound Proxy	Enter the IP address for an outbound proxy.
Register Period (seconds)	Enter the maximum requested period where the device will re-register with the SIP server. The default setting is 3600 seconds (1 hour).

	Note that if an Expires header is provided by the SIP response 200 (OK), this time will take precedence over the **Register Period** defined time here. Only change if instructed to do so.
Rate Limit SIP Registration	This option should be used in cases where many SIP extensions are registered (ex. one for each zone). Select a rate limit to stagger registration requests and prevent overloading the server by sending them all at the same time.
Wait for Successful Unregister	Enable to wait for the device to successfully unregister from the server. Enabling may cause a slight delay during configuration changes and reboots

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

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

ICE – TURN Password	Enter the password.
STUN - Server	Enter the IP address or domain of the STUN server.

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

Zoom Phone Local Survivability	
Local Survivability	Enable to re-register with local ZPLS Node if connection to Zoom fails. This allows sites to maintain a subset of Zoom Phone features even if connectivity to the Zoom Phone cloud is lost.
Survivability Proxy	The IP address or domain name of the local ZPLS node.

Interoperability

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

Multicast Configuration

The 8450 IP Console can only be programmed as a multicast transmitter to broadcast voice paging or alerts and trigger other devices. IP endpoints on the same local network as the 8450 can be grouped into up to 50 multicast zones and paged via multiple SIP extensions.

Multicast IP Addresses

Each 8450 has a unique IP address and shares a common multicast IP and port number (multicast zone) for multicast packets. The Transmitter units send to a configurable multicast zone, and the Receiver units listen to assigned multicast zones.

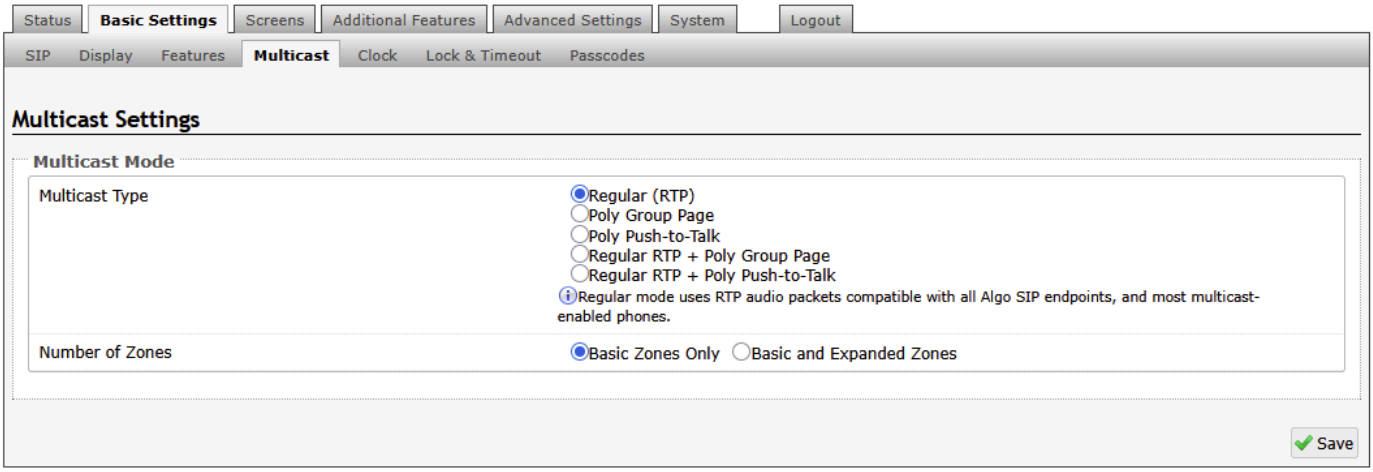
The network switches and router see the packet and deliver it to all the group members. The multicast IP and port number must be the same on each group's Transmitter and Receiver units. The user may define multiple zones by picking different multicast IP addresses and/or port numbers.

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

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

Basic Multicast Settings

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



Multicast Mode	
Multicast Type	The device may broadcast multicast paging compatible with Poly “on-premise group paging” protocol and most multicast-enabled phones that use RTP audio packets. Select **Regular (RTP)** if you are only multicasting to Algo IP endpoints or multicast-enabled phones. To multicast page announcements to Poly phones, select **Poly Group Page** or **Poly Push-to-Talk**. Select **Regular RTP + Poly Group Page** or **Regular RTP + Push-to-Talk** to multicast page audio to Poly phones, Algo IP endpoints, and multicast-enabled phones.

Number of Zones	Select **Basic Zones Only** if configuring nine or fewer multicast zones. Select **Basic and Expanded Zones** to configure up to 50 zones. The expanded zones have the same behavior as the basic Receiver zones but are hidden by default to simplify the interface.

Poly Group Paging/Push-to-Talk **(This section is used if the Multicast Type includes Poly Group Page or Poly Push-to-Talk.)**	
Poly Zone	Enter the same Multicast IP Address and Port number configured on the Poly phones.

Using Multicast Page Zones

The 8450 IP Console can broadcast to up to 50 paging. The multicast IP addresses define these zones.

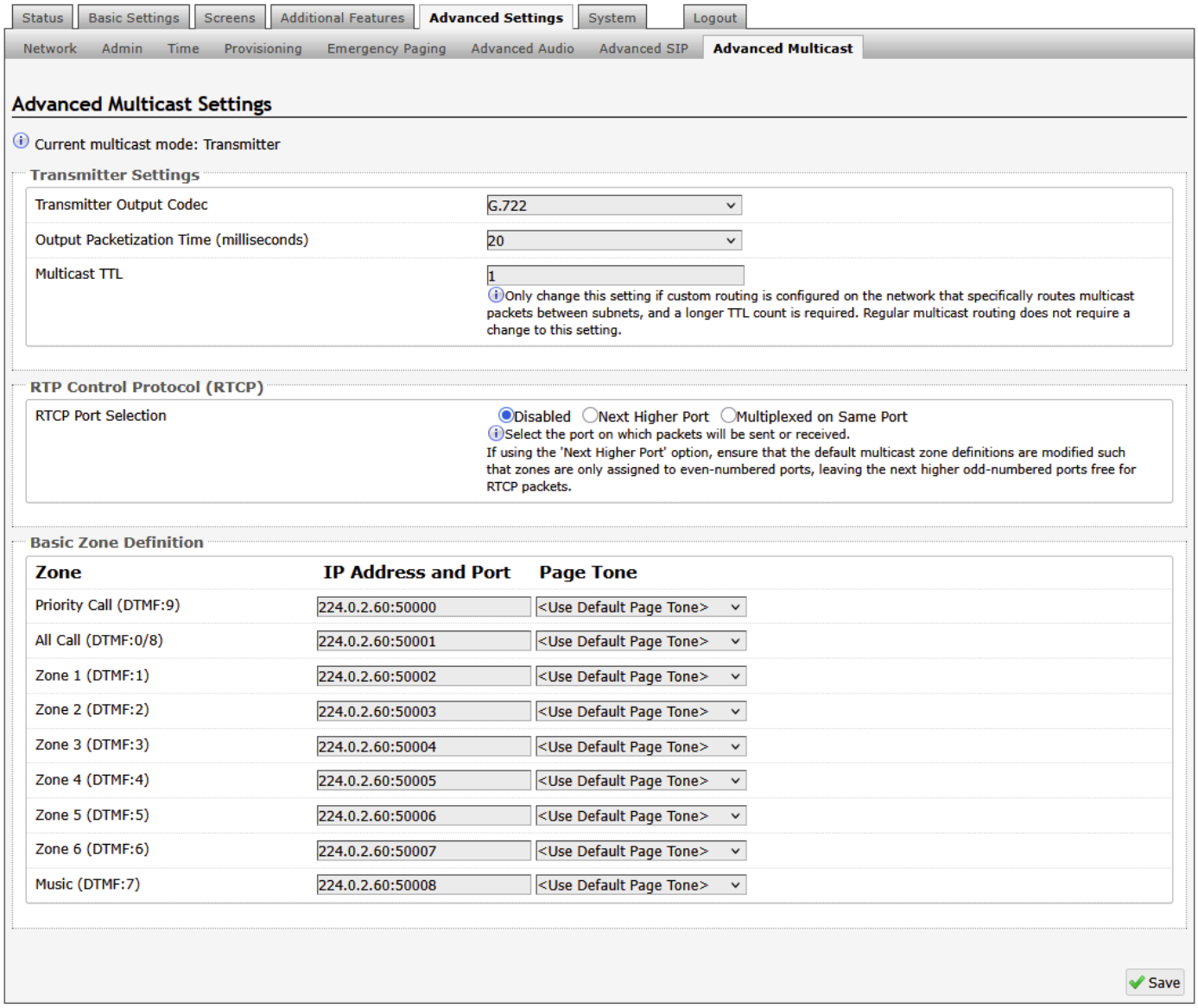
By default, these zones have the names below but can be used however you prefer.

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

As a multicast transmitter, event priority for the 8450 is based on the event type that initiated the multicast rather than the output multicast channel that will be active.

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

Advanced Multicast Settings



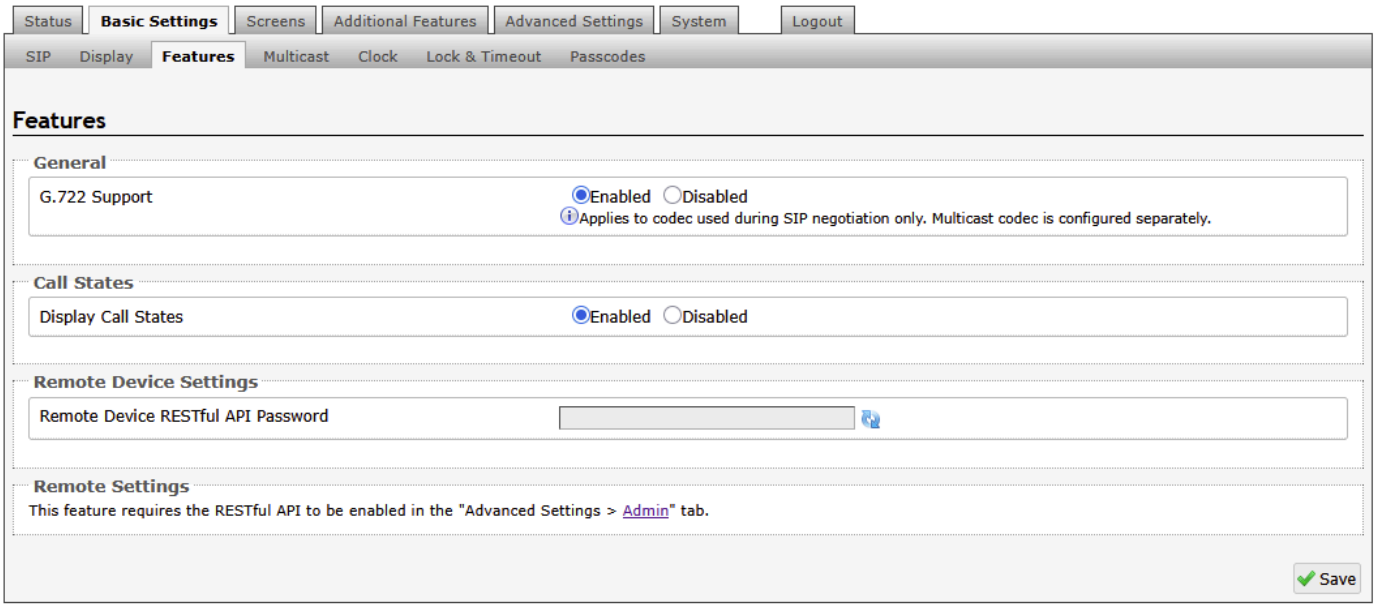
Transmitter Settings	
Transmitter Output Codec	Select an audio encoding format for the Transmitter device to use when sending output to the Receivers. Supported formats include: • G.711 ulaw • G.722 • Opus
Poly Output Codec	Select an audio encoding format when using Poly Group Page or Poly Push-to-Talk. Supported formats are G.711 ulaw and G.722 only.

Output Packetization Time (milliseconds)	Select the size of the audio packets the Transmitter sends to the Receivers from the dropdown menu. The default of 20 milliseconds is recommended unless a different value is specifically required for compatibility with other devices.
Multicast TTL	Only change the multicast time to live (TTL) setting if custom routing is configured on the network that specifically routes multicast packets between subnets and a longer TTL count is required. This ensures packets are not bounced back and forth in a network identity. When the TTL is reached, the router drops the packet.

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

Audio Configuration

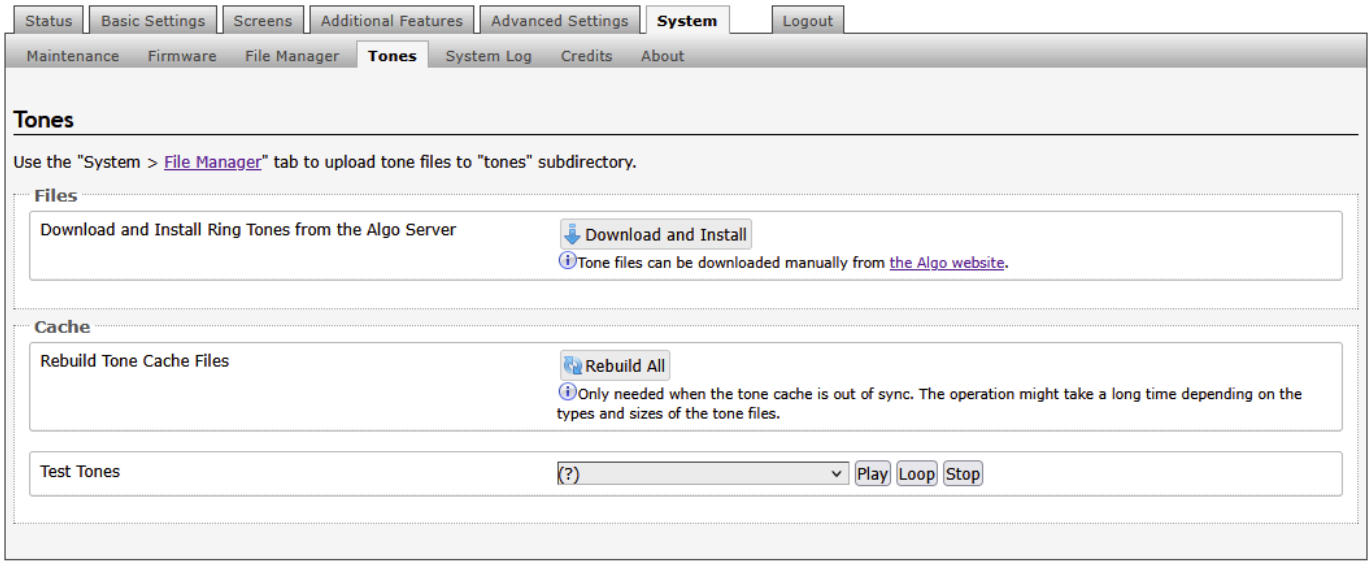
Basic Settings



Inbound Page Settings	
G.722 Support	Enable or disable the G.722 codec. G.722 enables wideband audio for optimum speech intelligibility.
Display Call States	Enable or disable specific information about the state of an active call (i.e. Dialing, Ringing, Answered).
Remote Device RESTful API Password	This password is used by the 8450 when sending API requests to Algo API Endpoints. This is used by buttons set to Send API Request.
Remote Mode	Used when the 8450 is part of a group of 8450 devices. a 'Multicast with Tone' or 'Start Emergency Alert' action started on one console will be shown on all consoles in the group.
Console Group	List of IP addresses of consoles in the console group to be notified of Multicast with Tone or Start Emergency Alert actions.
Allow Multicast with Tone Override	When a 'Multicast with Tone' event has been started within the console group, this config controls whether the console can override the event with another one. If enabled, the device will stop the current 'Multicast with Tone' event and start the new one. If disabled, the device will instead say 'Cannot override current alert'.
Allow Remote Multicast with Tone Cancel	When a 'Multicast with Tone' event has been started within the console group, this config controls whether the console can end it. If enabled, the top banner will contain the 'Stop Alert' button.

Tones

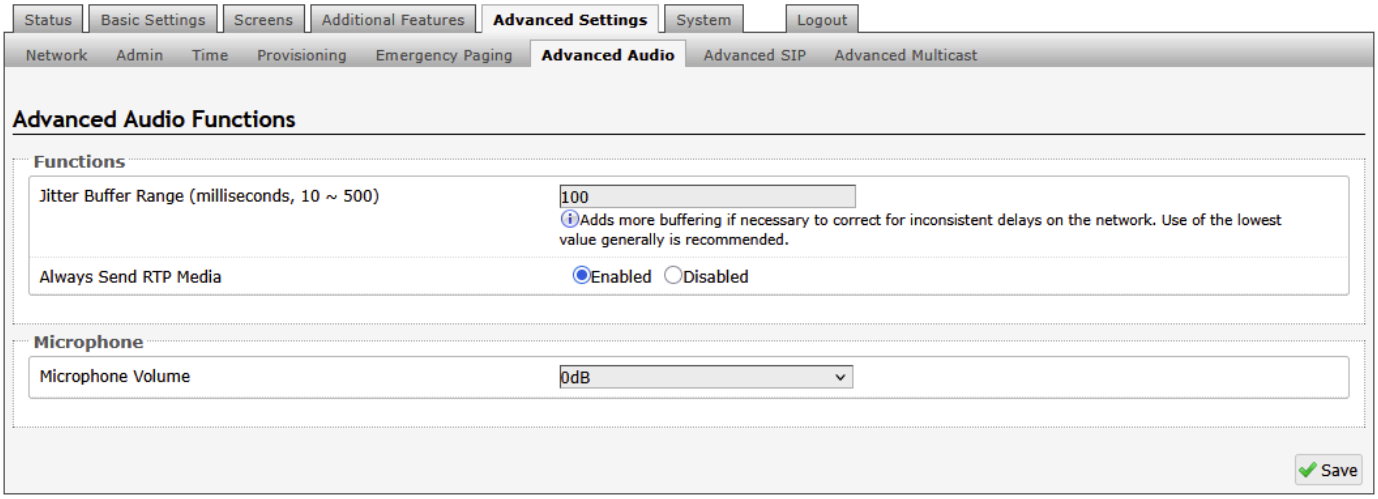
The 8450 includes several pre-loaded audio files that can be selected to play for various events. The web interface allows you to select a file and play it immediately over the speaker for testing, available in **Basic Settings** → **Features**. Files may also be added, deleted, or renamed. For more information see File Manager.



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

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

Advanced Audio



Functions	
Jitter Buffer Range (milliseconds, 10 ~ 500)	Enter a value between 10-500 to add more buffering if necessary to correct for inconsistent delays on the network. It is recommended to use the lowest value.
Always Send RTP Media	Enable to send audio packets at all times. This option is needed when the server expects to always see audio packets.
Microphone Volume	Lowers the volume of the gooseneck microphone in cases where feedback from nearby speaker occurs. Default value is 0dB and can be changed to -3dB or -6dB.

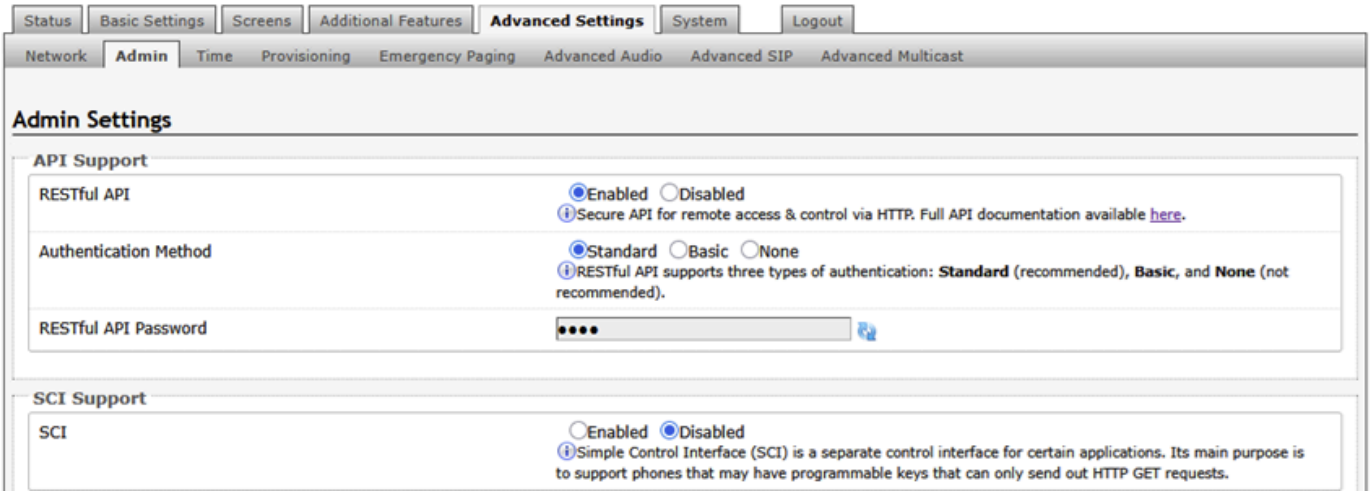
Integration

API

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

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

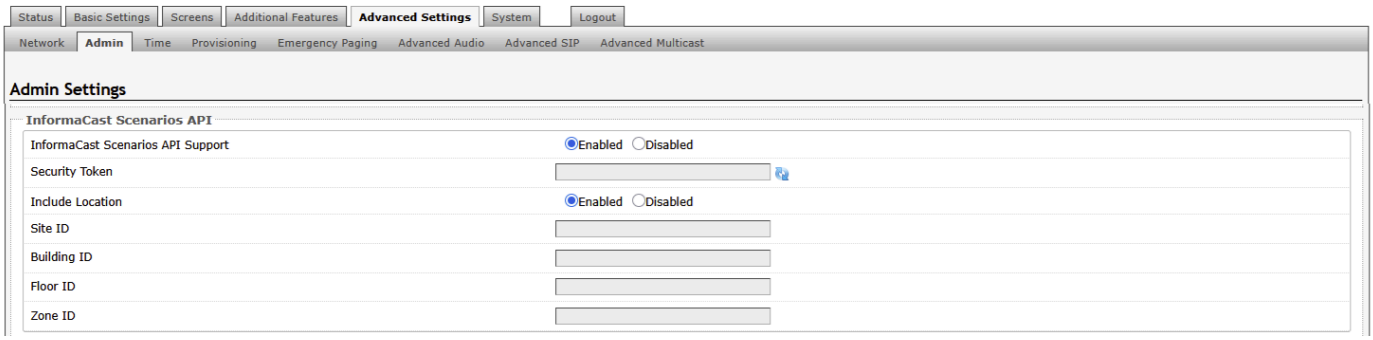
To configure API settings, use the web interface and navigate to **Advanced Settings** → **Admin** → **API Support**.



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

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

InformaCast



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

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

InformaCast Scenarios API	
InformaCast Scenario API Support	When enabled, a button can be configured to **Start InformaCast Scenario**. Input the Security Token and specify a location if applicable.

Device Management

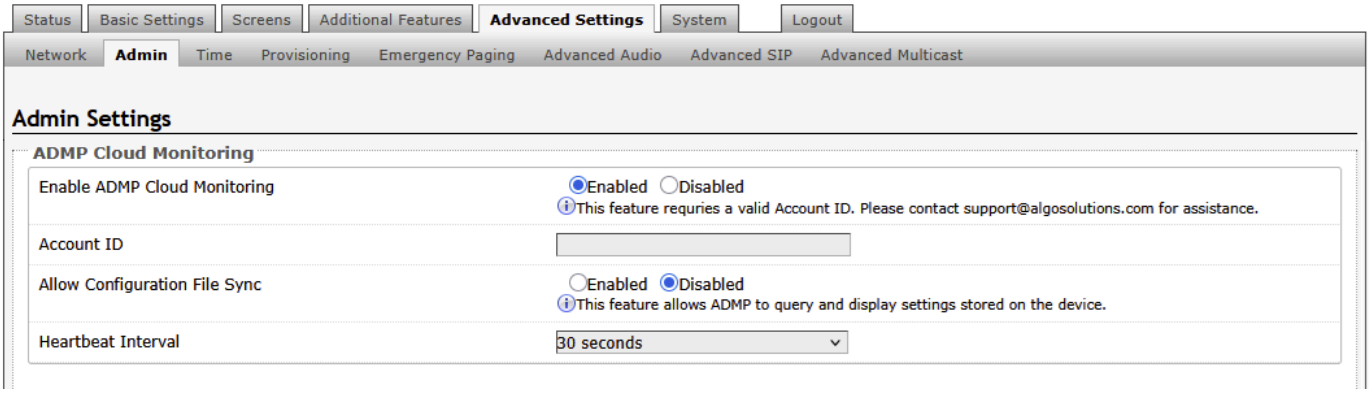
ADMP

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

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

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

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



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

Algo 8300 Controller

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

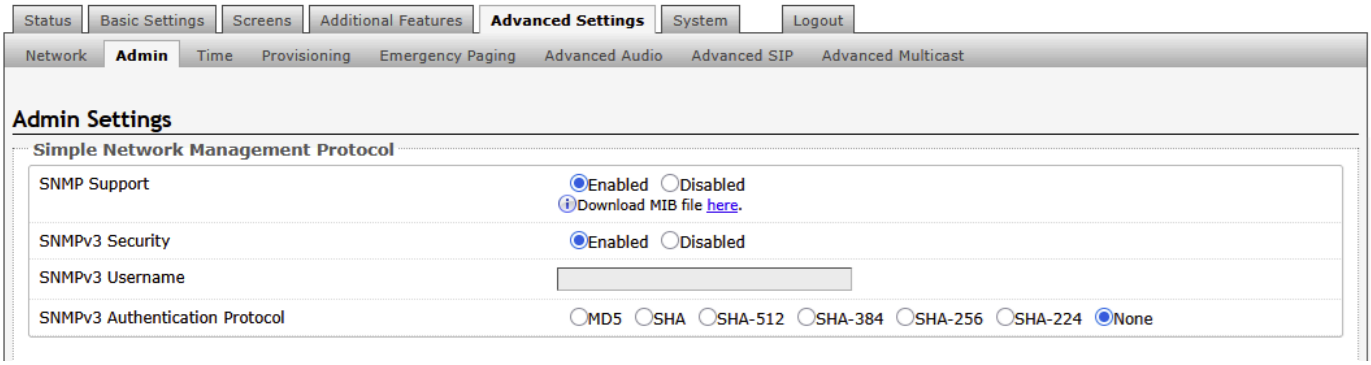
Note that if you choose to use the Algo 8300 IP Controller to manage your devices, ADMP cannot be used at the same time.

Learn more about the Algo 8300 IP Controller.

SNMP

Simple Network Management Protocol (SNMP) can be used to monitor and manage your device.

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

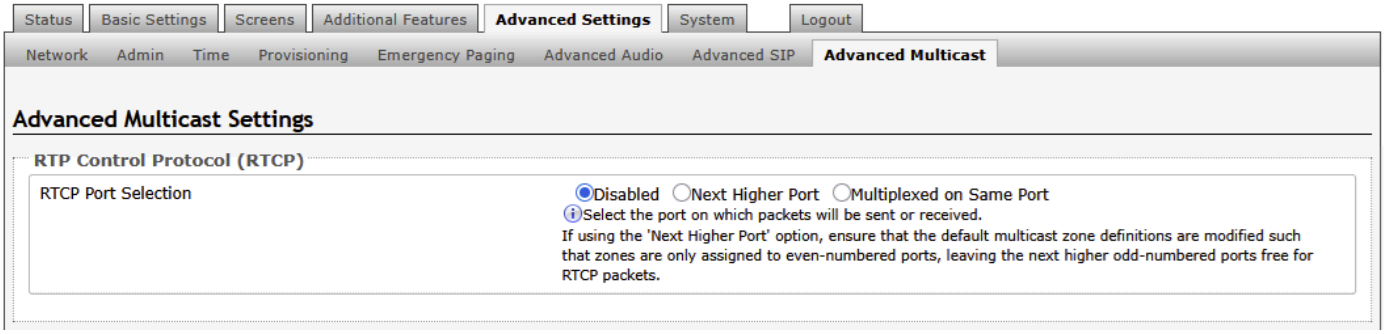


SNMP	
SNMP Support	Disabled by default. The existing setting will respond to a simple status query for automated supervision.
SNMP Community String	Speak to your IT Administrator for more information.
SNMPv3 Security	Speak to your IT Administrator for more information.

RTCP

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

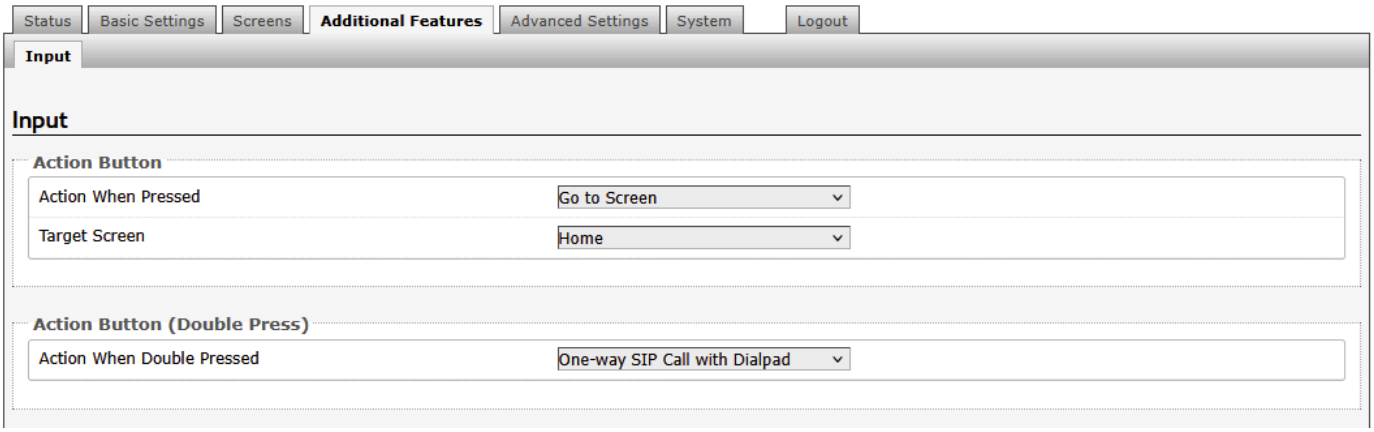
To configure your RTCP settings, use the web interface and navigate to **Advanced Settings → Advanced Multicast → RTP Control Protocol (RTCP)**.



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

System Configuration

Input



Action When Button Pressed	
Action	**Play Tone** When a button is pressed, a tone or a pre-recorded audio file will be broadcast. This function can be used to request support or assistance in service or retail environments, notify about an emergency at a specific location in medical or educational facilities, or sound an alarm during an intrusion. **Make Two-Way SIP Voice Call** When a button is pressed, a voice path will open for an intercom-like call via an external microphone connected to a pre-configured telephone extension. This option can be used when a call needs to be made from a public place where a telephone would not be practical to use. **Make SIP Call with Tone** When a button is pressed, a private call can be made to a pre-configured telephone extension with a pre-recorded message.

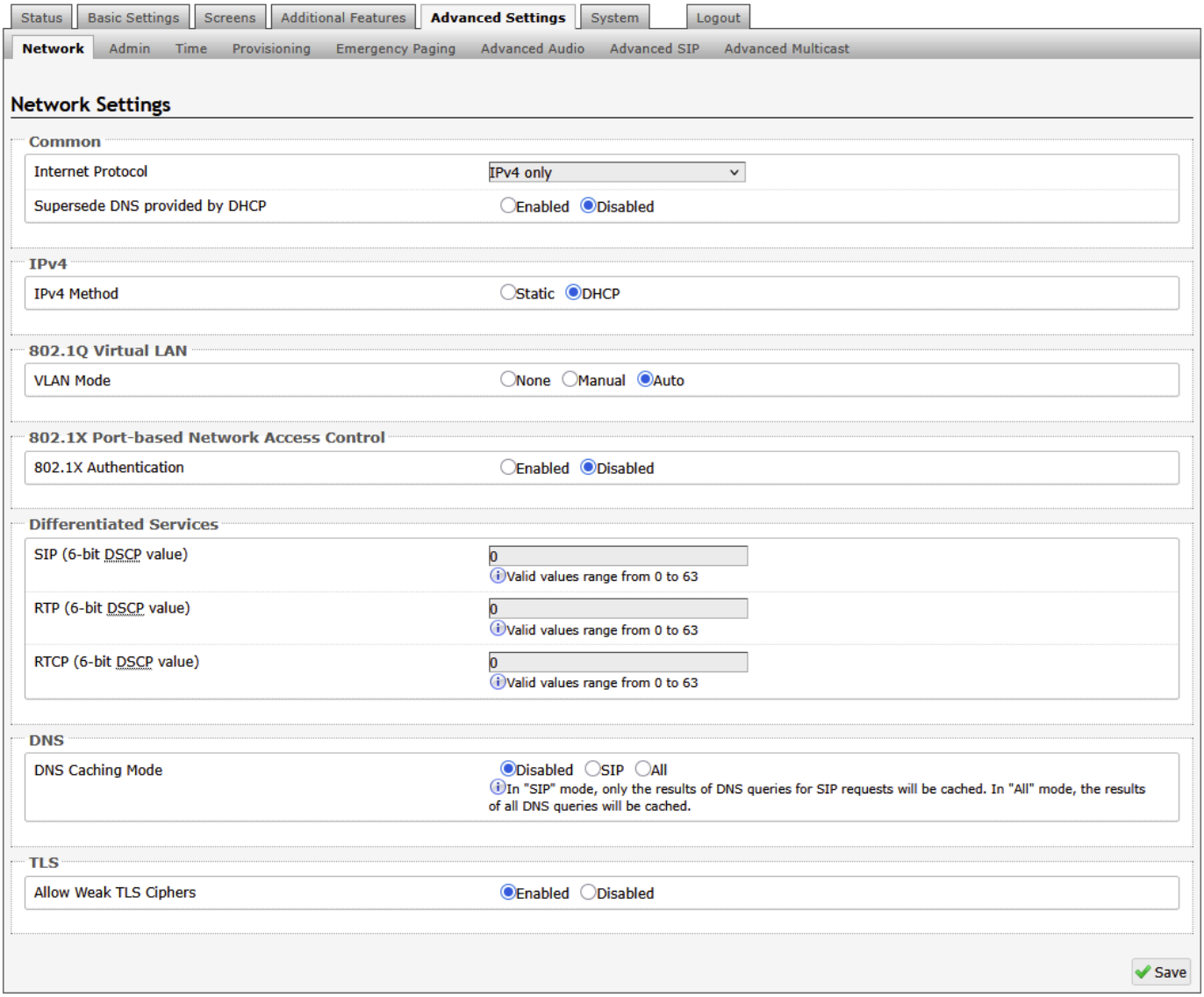
	For instance, a call to a supervisor's telephone notifying about an emergency or intrusion at some location. **Stream Mic Audio** When a button is pressed, audio from the attached microphone will be broadcast over multicast to the selected zone or group.
Tone/Pre-recorded Announcement	Available when **Action** is set to **Play Tone** or **Make SIP Call with Tone**. Select a recording or tone to use. Custom audio files may be used and uploaded through **System** → **File Manager**.
Tone Duration	Available when **Action** is set to **Play Tone**.
Multicast Zone	Available when **Action** is set to **Play Tone** or **Stream Mic Audio**. The RTP multicast zone where tones and microphone audio will be broadcast to.
Multicast Poly Group	Available when **Action** is set to **Play Tone** or **Stream Mic Audio**. The Poly Group where tones and microphone audio will be broadcast to.
Extension to Dial	Available when **Action** is set to **Make Two-Way SIP Voice Call** or **Make SIP Call with Tone**. A SIP account is required in **Page Extension** fields to make a call.
Allow 2nd Button Press	Available when **Action** is set to **Make Two-Way SIP Voice Call** or **Make SIP Call with Tone**. If enabled, the 2nd button press will End Call or End and Restart Call. Therefore, if an input is triggered a second time,

	the SIP call will be terminated and, in some cases, immediately called again.
Outbound Ring Limit	Available when **Action** is set to **Make Two-Way SIP Voice Call** or **Make SIP Call with Tone**. If enabled, the 2nd button press will End Call or End and Restart Call. Therefore, if an input is triggered a second time, the SIP call will be terminated and, in some cases, immediately called again.
Ringback Tone	Available when **Action** is set to **Make Two-Way SIP Voice Call** or **Make SIP Call with Tone**. The tone played during an outbound call while waiting for the call receiver to answer.
Maximum Call Duration	Available when **Action** is set to **Make Two-Way SIP Voice Call**. The maximum length a call can be.
Interval Between Tones (seconds)	Available when **Action** is set to **Make SIP Call with Tone**. Specify the time delay (seconds) between tones.
Maximum Tone Duration	Available when **Action** is set to **Make SIP Call with Tone**. Select the maximum tone duration. The tone will be terminated once the maximum time is reached.

Action Button (Double Press)

Additionally, a second action may be specified when the Action Button is pressed twice in rapid succession. The same settings apply to a Double Press Action Button.

Network Settings



Common	
Internet Protocol	Use the dropdown to select **IPv4 Only** or **IPv4 and IPv6**. If IPv6 is also configured, it will have to be set up via DHCP or statically, similarly to the IPv4.
Supersede DNS provided by DHCP	This setting will not appear if the selected Internet Protocol is set to **Static**.

IPv4	
IPv4 Method	The device can be set to a static or DHCP IP address. DHCP is an IP standard designed to simplify the administration of IP addresses. When selected, DHCP will automatically

	configure IP addresses for each device on the network. DHCP is selected by default. When **Static** is selected, the device will use the IP address entered in the fields below.
IPv4 Address/Netmask	Enter the static IP address and netmask (CIDR format) for the device (e.g., 192.168.1.23/24).
IPv4 Gateway	Enter the gateway address.

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

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

Rate Limit (packets per second)	Specify the packets per second allowed for Rate Limiting Outbound Messages.

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

802.1X Port-based Network Access Control	
802.1x Authentication	Enable to add credentials to access LAN or WLAN that have 802.1X network access control (NAC). You can ask your IT Administrator for this information
Authentication Mode	Select the desired authentication mode.
Anonymous ID	If configured, the device will send the anonymous ID to the authenticator instead of the 802.1X client username.

ID	The ID should contain a string identifying the IEEE 802.1X authenticator originating the request. Ask your IT administrator for details.
Password	Ask your IT administrator for details.
Validate Server Certificate	Enable to validate the authentication server against common authorities. To validate additional certificates, go to the System → File Manager to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the certs folder.

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

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

TLS	
Allow Weak TLS Ciphers	Enables compatibility with legacy systems that may not support the most current encryptions standards

Admin

Admin Settings

Admin Password

Old Password	
Password	
Confirmation	

General

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

Log Settings

Log Level	( ) Error (Lowest) ( ) Notice ("Event") (•) Info ("SIP") ( ) Debug (Highest)
Log Method	(•) Local ( ) Network ( ) Both
Log Additional Events	( ) Enabled (•) Disabled ⓘ Additional logs will be logged at the "Notice" level

Management

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

Simple Network Management Protocol

SNMP Support	( ) Enabled (•) Disabled ⓘ Download MIB file here.

API Support

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

SCI Support

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

System Integrity

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

InformaCast Scenarios API

InformaCast Scenarios API Support	( ) Enabled (•) Disabled

ADMP Cloud Monitoring

Enable ADMP Cloud Monitoring	( ) Enabled (•) Disabled ⓘ This feature requries a valid Account ID. Please contact support@algosolutions.com for assistance.

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

General	
Device Name (Hostname)	Add a name to identify the device in the Algo Network Device Locator Tool.
Introduction Section on Status Page	Turn On to show the introduction text on the login screen.
Show Status Section on Status Page when Logged Out	Turn On to allow others to view the status page without logging in. If turned Off, the settings and configurations on the status page will be hidden entirely unless a user is logged in to ensure only trusted users can view device information.
Display Switch Port ID on Status Page	Turn On to display the Switch Port ID on the Status Page. This option is only possible if the device is connected to a switch that supports LLDP or CDP.
Web Interface Session Timeout	Set the maximum duration of inactivity to log a user out of the web interface automatically.

Play Tone at Startup	The device can play a beep tone at startup. The device does not have a full speaker to play a custom audio file.

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

Management	
Web Interface Protocol	HTTPS is always enabled on the device. HTTP is enabled by default but may be disabled. To do so, select HTTPS Only mode so requests are automatically redirected to HTTPS. Note that no security certificate exists since the device can have any address on the local network. Therefore, most browsers will provide a warning when using HTTPS.
Force Strong Password	When Enabled, you can enforce a secure password for the device web interface for additional protection. The password requirements for a strong password are: • Must contain at least 10 characters • Must contain at least 1 uppercase character • Must contain at least 1 digit (0 – 9) • Must contain at least 1 special character
Allow Secure SIP Passwords	When **Enabled**, SIP passwords are stored in the configuration file in an encrypted format to prevent viewing and recovery. If enabled, navigate to **Basic Settings** → **SIP** and fill out the field Realm. To obtain your SIP Realm information, contact your SIP Server administrator or check the SIP log file for a

	registration attempt. The Realms may be the same or different for all the extensions used. All the configured Authentication Password(s) must be re-entered here as well as any other locations where SIP extensions have been configured to save the encrypted password(s). If the **Realm** is changed later, all passwords must be re-entered to save the passwords with the new encryption.

Simple Network Management Protocol	
SNMP Support	Disabled by default. The existing setting will respond to a simple status query for automated supervision.
SNMP Community String	Speak to your IT Administrator for more information.
SNMPv3 Security	Speak to your IT Administrator for more information.

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

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

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

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

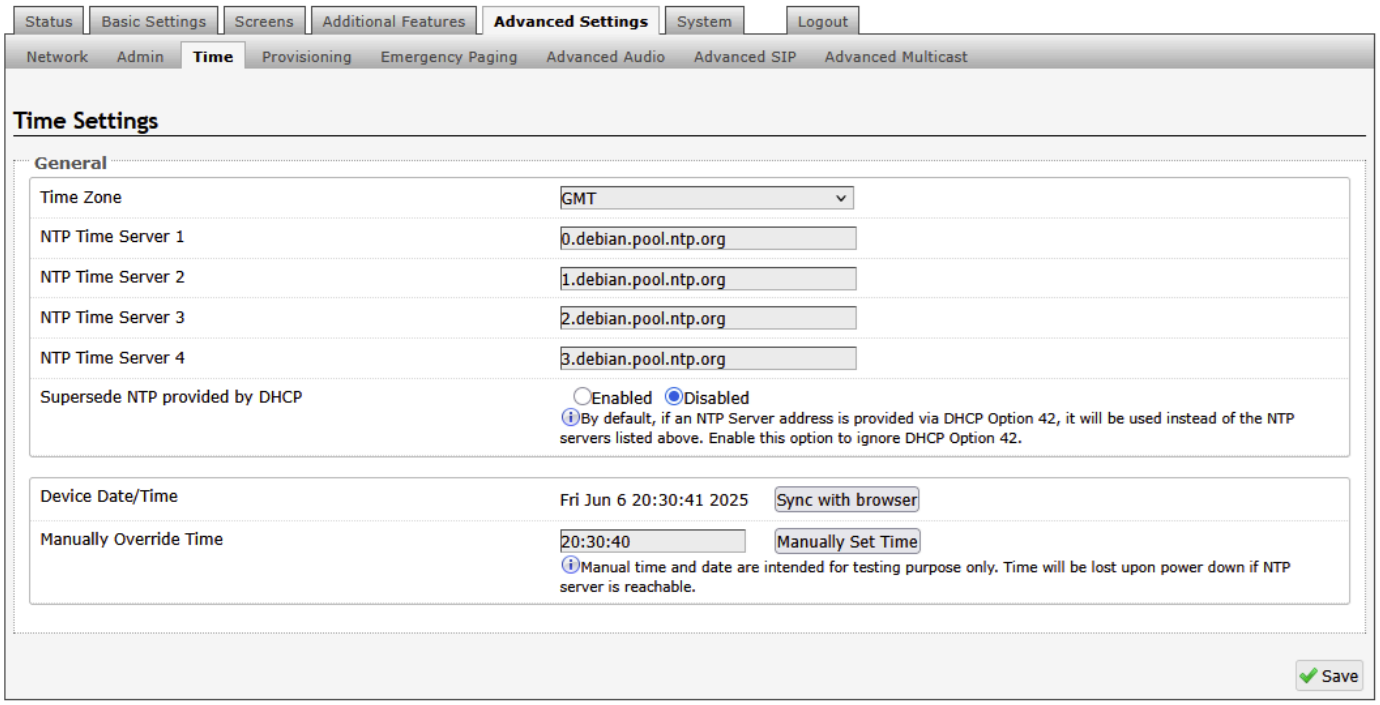
InformaCast Scenarios API	
InformaCast Scenario API Support	When enabled, a button can be configured to **Start InformaCast Scenario**. Input the Security Token and specify a location if applicable.

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

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

Sync	
Heartbeat Interval	Select how often ADMP should check the status of your device.

Time



Time Settings	
Time Zone	Use the dropdown to select the time zone required for your clock.
NTP Time Server	The interface will attempt to use Timer Server 1 and work down the list if one or more of the time servers become unresponsive. These settings are pre-populated with public NTP servers hosted on the internet. To use these, the device requires internet connection. Alternatively, this can be customized to point the device to any other NTP server hosted or premise-based.
Supersede NTP provided by DHCP	By default, if an NTP Server address is provided via DHCP Option 42, it will be used instead of the NTP servers listed above. Enable this option to ignore DHCP Option 42.

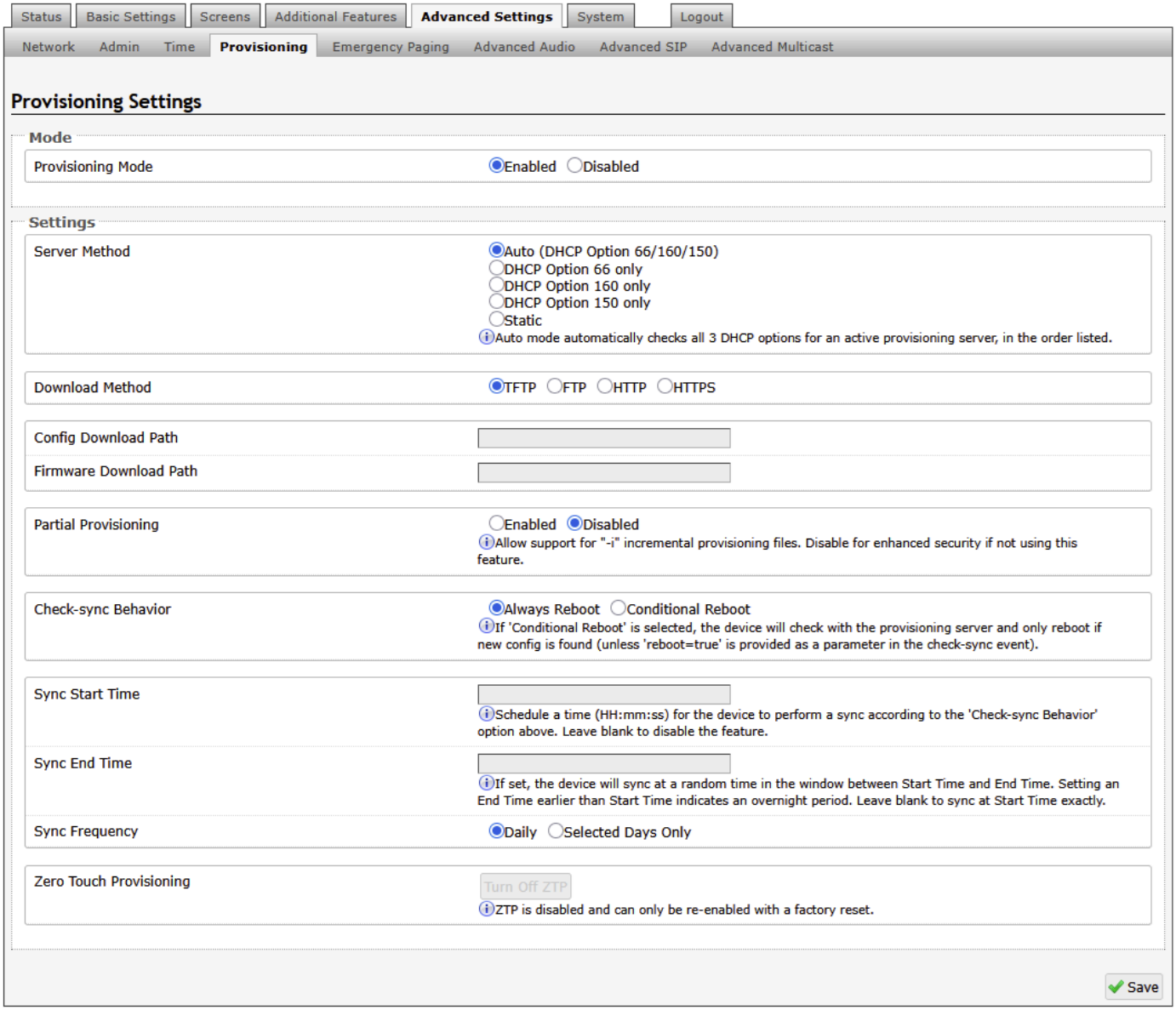
Device Date/Time	This field shows the current time and date set on the device. If you are testing the device on a lab network that does not have access to an external NTP server, click Sync with browser to temporarily set the time on the device. This time value will be lost at power down or overwritten if connection to the NTP server is available. Time and date are used for logging purposes and the scheduler feature.
Manually Override Time	Manual time and date are intended for testing purposes only. Time will be lost upon power down if the NTP server is reachable.

Provisioning

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

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

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



Mode

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

Settings

Server Method	Set to Auto by default. Select a Server Method. • **Auto**: All three DHCP options (66, 160, 150) will be automatically checked for an active provisioning server • **DHCP Option 66 Only**: Only DHCP Option 66 will be checked for a provisioning server • **DHCP Option 160 Only**: Only DHCP Option 160 will be checked for a provisioning server • **DHCP Option 150 Only**: Only DHCP Option 150 will be checked for a provisioning server • **Static**: Only the specified static server will be checked for a provisioning server For provisioning to work with a DHCP option, DHCP must be enabled under **Advanced Settings** → **Network** → **IPv4**.
Static Server	Enter the server address or domain.
Download Method	Select your preferred method for downloading provisioning files. The options are: • TFTP (Trivial File Transfer Protocol) — See MD5 Checksum below for more details • FTP • HTTP • HTTPS — This may help prevent configuration files from being read by an unwanted third party and having sensitive data stolen. The device configuration files can be automatically downloaded from a provisioning server using DHCP Option 66. This option code (when set) supplies a TFTP boot server address to the DHCP client to boot from. A file listed below can be uploaded on the provisioning server (for access via TFTP, FTP, HTTP, or HTTPS): • MAC specific (algom[MAC].conf) • MAC specific incremental (algom[MAC]-i.conf)

	• Generic (algop8450.conf) • Generic incremental (algop8450-i.conf) Both protocol and path are supported for Option 66, allowing for http://myserver.com/config-path to be used.
Config Download Path	Enter the path where the configuration file is located in the provisioning server (e.g., algo/config/8450).
Firmware Download Path	Enter the path where the configuration file is located in the provisioning server (e.g., algo/config/8450).
Partial Provisioning	Enable to allow support for “-i” incremental provisioning files. Disable for enhanced security if this is not required.
Check-sync Behavior	Select Always Reboot to set the device to always reboot despite other settings. Select Conditional Reboot to set the device and check the provisioning server. Only reboot if a new config is found (unless “reboot=true” is provided as a parameter in the check-sync event).
Sync Start Time	Set a time (HH:mm:ss) for the device to perform a sync according to the Check-sync Behavior setting. Leave this blank if not needed.
Sync End Time	If set, the device will sync randomly in the window between Sync Start Time and Sync End Time. Setting an End Time earlier than the Start Time indicates an overnight period. Leave blank to lank to sync exactly at the set start time.
Sync Frequency	Select the sync frequency. Frequency can be set to Daily or Selected Days Only.
Sync Days	Select the days of the week for syncs to occur.
Zero Touch Provisioning	ZTP is enabled by default but is disabled when any changes are made to the device configuration. This button can also be used to disable ZTP if no changes have yet been made to the device configuration.

MD5 Checksum

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

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

Generating a generic configuration file

This configuration file is device-generic in terms of MAC address and will be used by all connected 8450 devices.

If using a generic configuration file, extensions and credentials must be entered manually once the 8450 has automatically downloaded the configuration file.

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

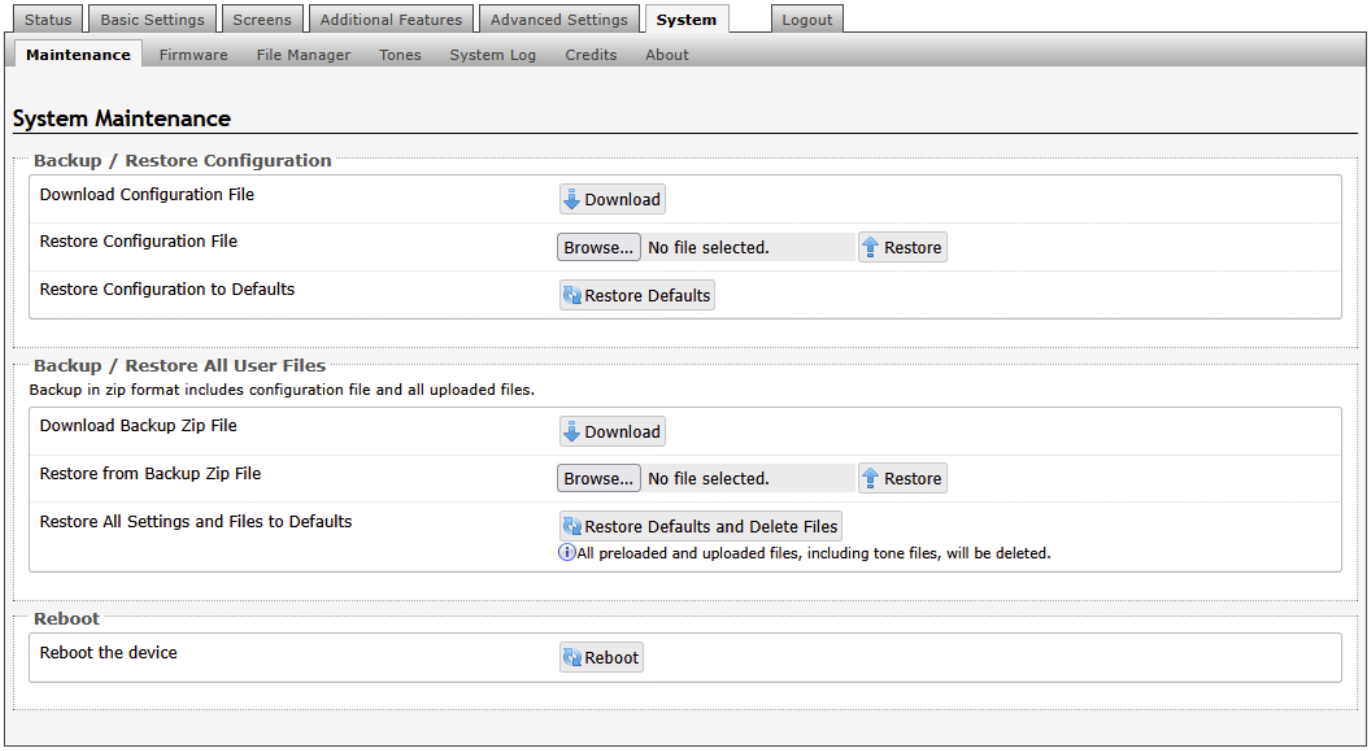
Generating a specific configuration file

The specific configuration file will only be downloaded by the 8450 with the MAC address specified in the configuration file name.

Since all necessary settings can be included in this file, the 8450 will be ready to work immediately after downloading the configuration file. The MAC address of each 8450 can be found on the back label of the unit.

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

System Maintenance

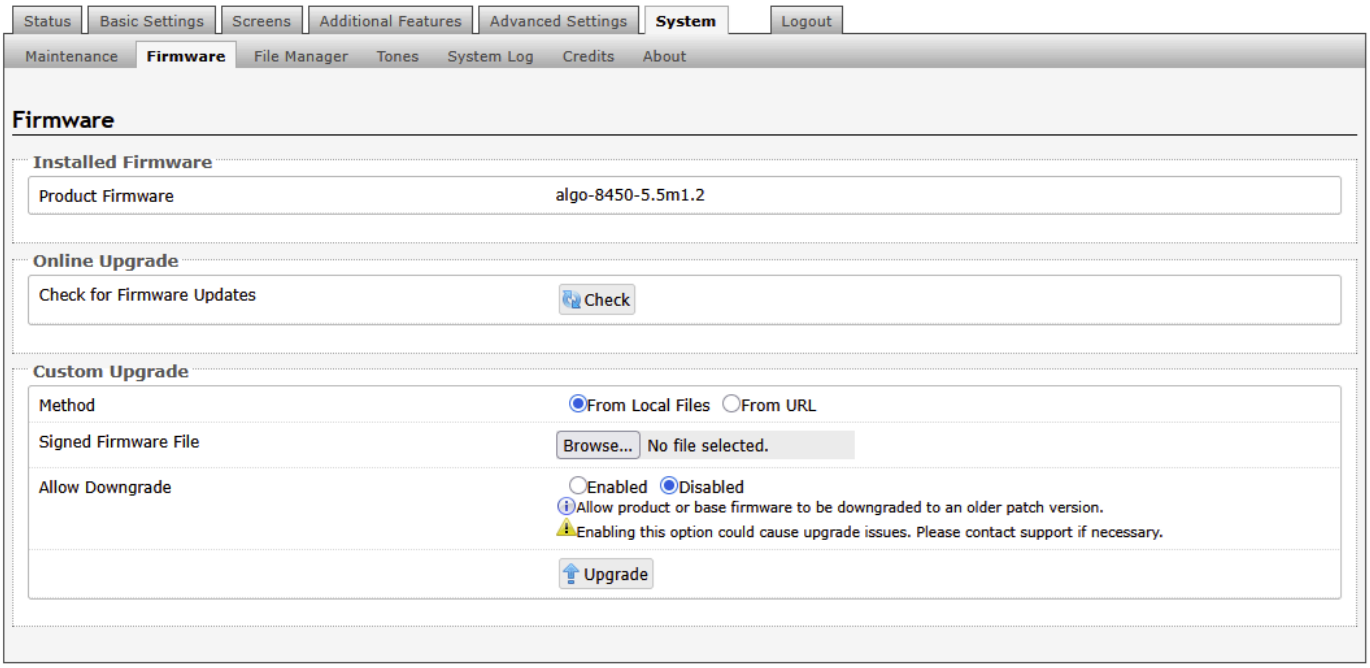


Backup/Restore Configuration	
Download Configuration File	Save configuration settings to a text file for backup or to set up a provisioning configuration file.
Restore Configuration File	Restore settings by uploading a backup file.
Restore Configuration to Defaults	This action will reset all device settings to factory defaults unless the device is registered with ZTP. If registered with ZTP, the device will reset to the defaults set by the conf ZTP file.

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

Reboot	
Reboot the Device	Reboots the device.

Firmware



Installed Firmware	
Product Firmware	Displays the current firmware on the device.

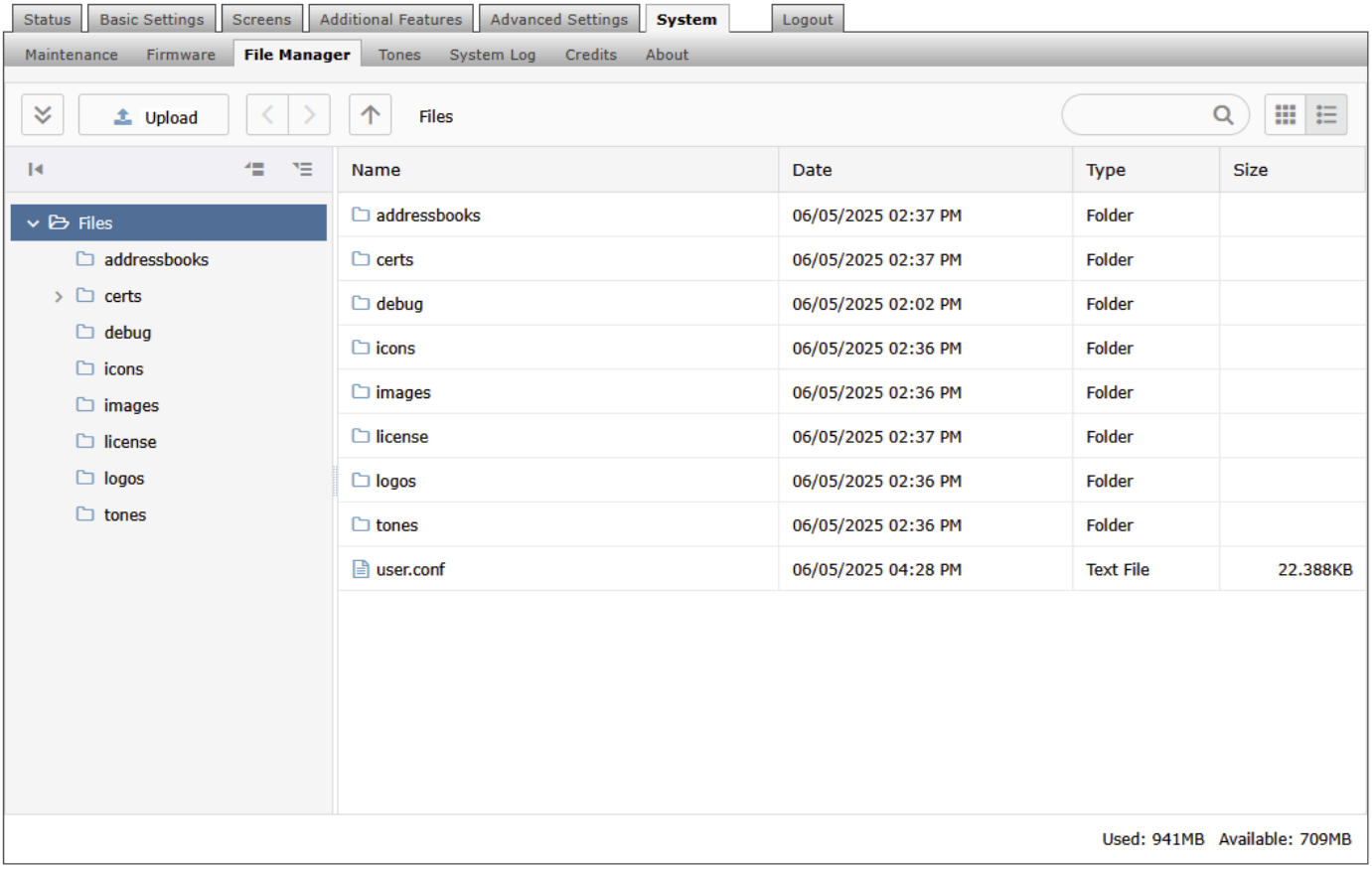
Online Upgrade	
Check for Firmware Updates	Click Check to check for the latest firmware. If the firmware is up to date, Latest Firmware will state Firmware up to date. If your firmware is outdated, the new firmware availability will be listed. Internet connection is required.

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

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

File Manager

The 8450 has 818MB of storage space for additional files.



addressbooks Folder

This folder contains address book files used by the Directory feature.

certs Folder

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

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

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

debug Folder

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

icons Folder

The icons folder is used for storing icons that appear within configurable screen buttons.

images Folder

Upload images to use as backgrounds for configured pages.

license Folder

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

logos Folder

Used by the logos feature to store logos that can be configured via Basic Settings > Display > Show Logo.

tones Folder

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

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

Audio files must be in the following format:

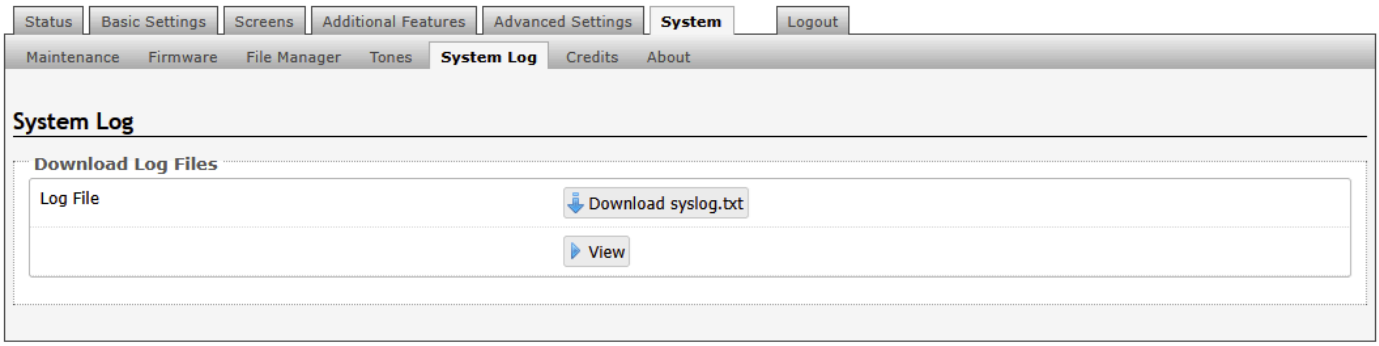
- WAV or MP3 format
- Smaller than 200 MB

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

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

System Log

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



Log Out

Log out of the web interface.

FCC Compliance Statement

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