8039 SIP Video Intercom
FW Version 2.0.1

Installation & Configuration

Order Codes

8039	SIP Video Intercom

Algo Communication Products Ltd
4500 Beedie St Burnaby BC Canada V5J 5L2
www.algosolutions.com

(604) 454-3792
support@algosolutions.com

Table of Contents

Important Safety Information

⚠ Important Safety Information

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

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

⚠ Consignes de Sécurité Importantes

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

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

⚠ Información de Seguridad Importante

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

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

⚠ Wichtige Sicherheitsinformationen

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

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

⚠ 安全须知

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

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

⚠ EMERGENCY COMMUNICATION

If used in an emergency communication application, the 8039 SIP Video Intercom should be routinely tested. SNMP 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.

⚠ WET OR OUTDOOR ENVIRONMENTS

The 8039 SIP Video Intercom is intended for indoor or outdoor locations and may be subjected to spray or weather, provided the rear wiring cavity is properly sealed to prevent water ingress.

Gaskets included with the 8039 SIP Video Intercom may be effective against water ingress on some, but not all surfaces in which case additional protective measures must be taken such as a perimeter sealant.

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

When the Intercom is connected to wiring that exits the building, there is potential risk of lightning induced electrical surges or high voltages from fault conditions. To reduce risk, outdoor wiring should be protected by Earth grounded conduit whenever possible. Relay input and output connections must not leave the building perimeter without adequate lightning protection.

Overview

Introduction

The 8039 SIP Video Intercom is ideal for secure business entrances, emergency intercom, and gated entrances. The Algo 8039 provides hands-free intercom capability with video, entrance security with door unlock control, rugged weatherproof design, and superior audio performance.

Fully compatible with SIP industry standards, the 8039 SIP Video Intercom will work with most hosted or enterprise SIP-base servers supporting third-party SIP endpoints.

The 8039 SIP Video Intercom is configured using central provisioning features or by accessing a web interface using browsers such as Google Chrome, Firefox, or Internet Explorer.

What is Included

- 8039 SIP Video Intercom
- Mounting Plate

What is not Included

- Optional 8061 IP Relay Controller

Setup and Installation

Getting Started - Quick Install & Test

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

1. Connect the 8039 SIP Video Intercom to an IEEE 802.3af compliant PoE network switch. The backlight keypad will turn on. After about 30 seconds, a beep will signal the completion of the boot process.
2. After the boot is complete, press the call button on the 8039 to hear the IP address. (Once the SIP Server field is populated in the 8039 web interface, the call button will contact the preconfigured extension when pressed.) The IP address may also be discovered by downloading the Algo locator tool to find Algo devices on your network: www.algosolutions.com/locator
3. Access the 8039 SIP Video Intercom web page by entering the IP address into a browser (Chrome, IE, Firefox etc) and login using the default password ***algo.***
4. Enter the IP address for the SIP server into the SIP Domain field under the **BASIC SETTINGS > SIP** tab.
5. Enter the SIP Extension, Authentication ID, and Password. Also enter the target Dialing Extension that the Intercom will call.

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

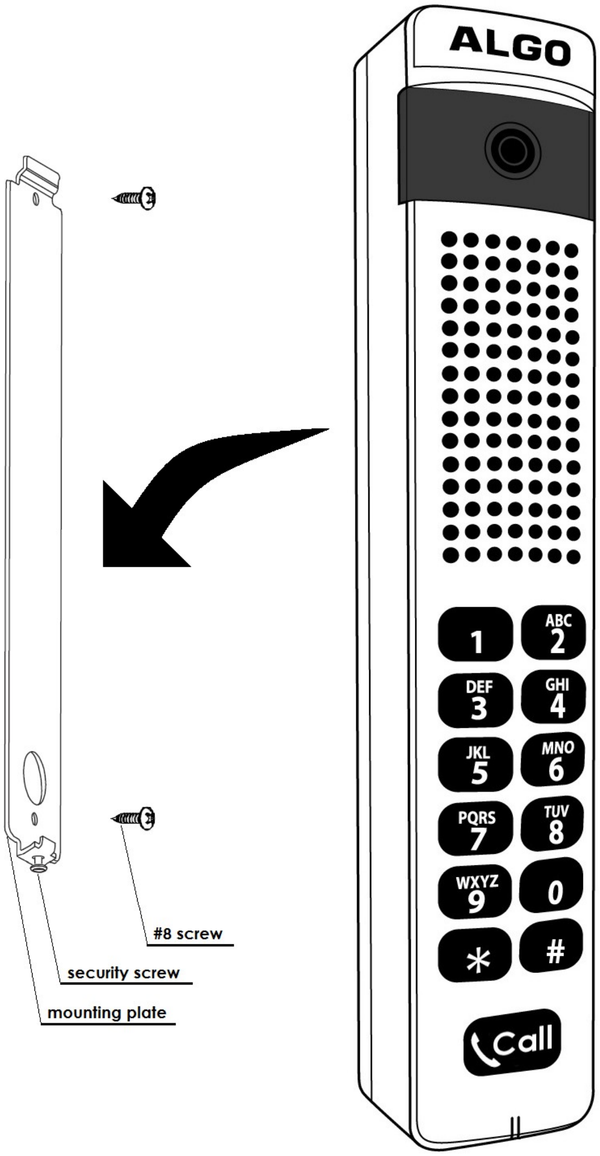
6. Press the Call Button on the 8039 Intercom, then answer the phone to communicate over the Intercom. Press the digit 6 on the phone keypad to activate the door control relay for three seconds (if applicable).

Installation

The 8039 SIP Video Intercom is weather protected for outdoor installation. However, if network cabling extends beyond the perimeter of the building, then adequate lightning protection is required to protect the cabling and network switch from lightning surges. No lightning protection is required by UL or CSA if the 8039 is located on the outside wall of a building and the wiring is inside the perimeter of the building.

The 8039 is wall and door frame (mullion) mountable via the supplied mounting plate:

Secure the mounting plate to the wall/ mullion door frame via two #8 screws. Attach the 8039 into the mounting plate and secure the device in place with the attached security screw at the bottom of the mounting plate using the provided Allen wrench.



Programming and Configuration

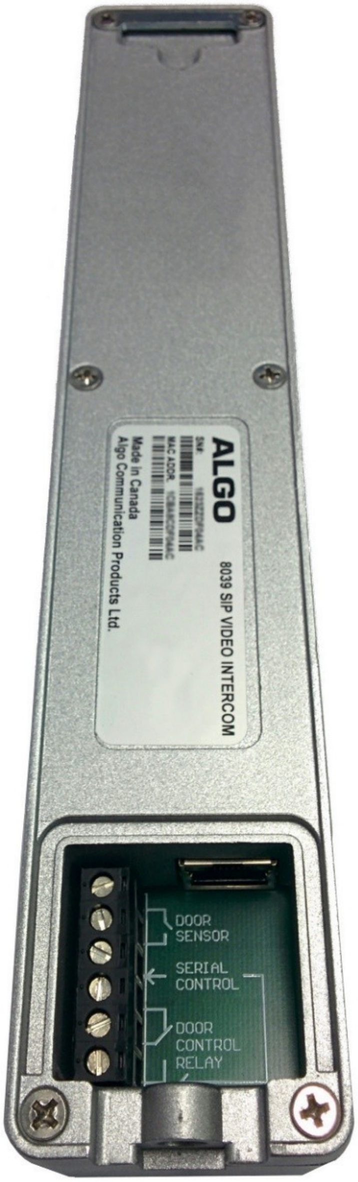
The 8039 SIP Video Intercom is configurable using the web interface or provisioning features.

After boot up, the speaker will beep and the intercom will have obtained an IP address. If there is no DHCP server the 8039 SIP Video Intercom will default to the static IP address **192.168.1.111**.

Before the 8039 is configured, the call button on the front can be pressed to play the IP address over the speaker. (Once the SIP Server field is populated on the 8039 web interface, the call button will contact the preconfigured extension when pressed.) The IP address may be discovered by downloading the Algo locator tool to find Algo devices on your network: www.algosolutions.com/locator

Enter the IP address (e.g 192.168.1.111) into a browser such as Google Chrome, Firefox, or Internet Explorer (other than IE9). The web interface should be visible and the default password will be ***algo*** in lower case letters.

Wiring Connections



Network Connection

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

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

There are two lights on the Ethernet jack:

Green light: On when Ethernet is working, flickers off to indicate activity on the port.

Amber light: Off when successful 100Mbps link is established. Typically on only briefly at power up.

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

Door Control Relay

Provides both normally open and normally closed relay contacts. *Note: The 8061 IP Relay Controller can be used as an alternative more secure option for door opening control, by using a separate relay from the public-facing intercom.*

Serial Control

Reserved for future use

Door Sensor (Dry Contact Input)

An external call button can be connected as a normally open switch. When the relay is triggered, this will dial the pre-configured “Extension to Dial”.

Backlit Keypad and Call Button

The backlit keypad and call button will be steady during power up and will flash during a reset.

If enabled, when making a call, the call button light will flash rapidly, while the call is ringing at the far-end phone. Once the call is answered, the flashing will slow down.

Reset

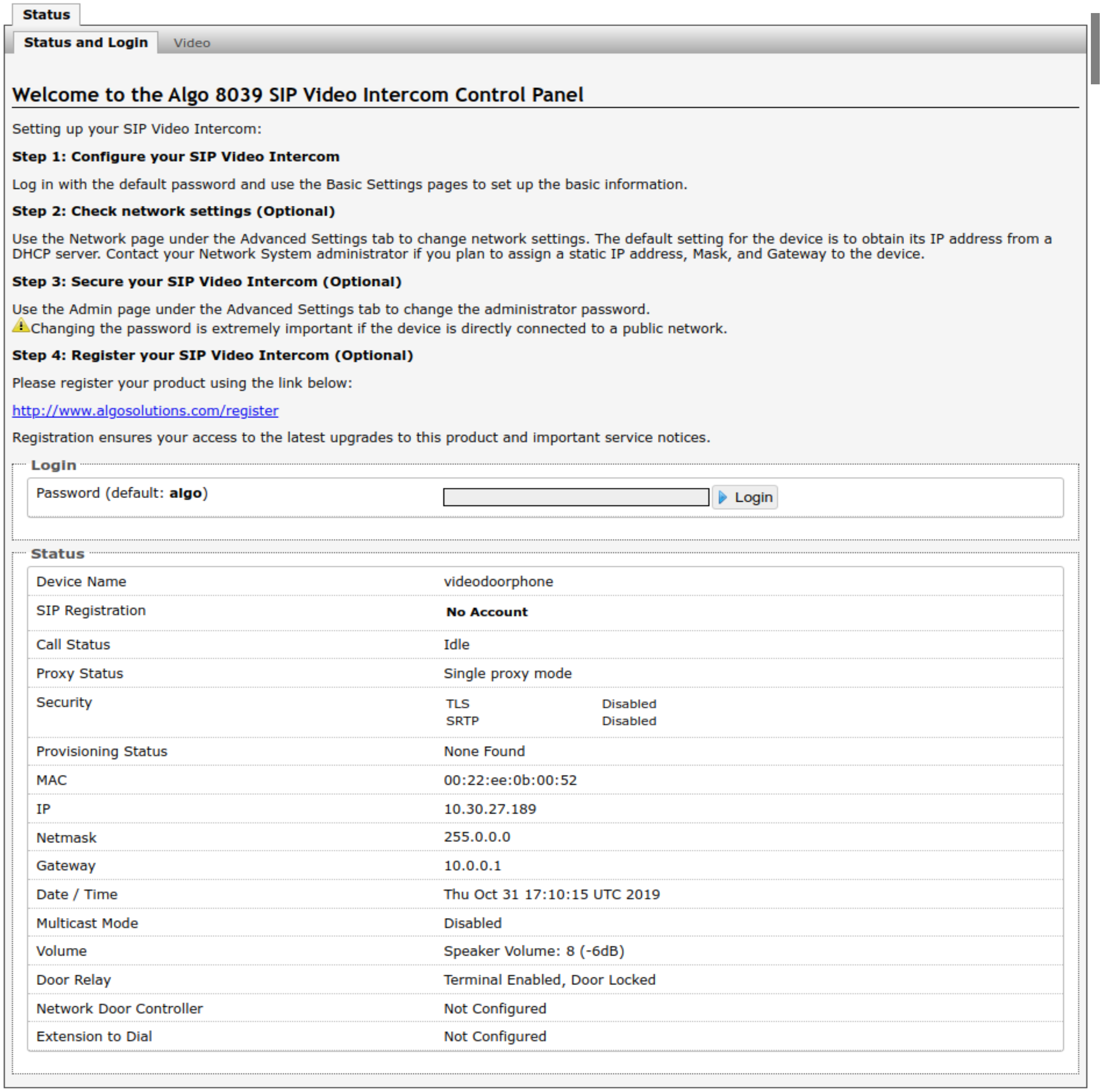
The 8039 SIP Video Intercom can only be reset during a power up. To return all the settings to the factory default for the 8039, wait until all the backlit keys start flashing. Then press and hold the call button until the call button backlight begins a double flash pattern. Release the call button and allow the unit to complete its boot process. **Do not press the call button until all the keys start flashing.**

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

Web Interface Status and Login

Web Interface Login

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



Welcome to the Algo 8039 SIP Video Intercom Control Panel

Setting up your SIP Video Intercom:

Step 1: Configure your SIP Video Intercom

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

Step 2: Check network settings (Optional)

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

Step 3: Secure your SIP Video Intercom (Optional)

Use the Admin page under the Advanced Settings tab to change the administrator password.
⚠Changing the password is extremely important if the device is directly connected to a public network.

Step 4: Register your SIP Video Intercom (Optional)

Please register your product using the link below:

http://www.algosolutions.com/register

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

Login

Password (default: **algo**) ▭ Login

Status

Device Name	videodoorphone
SIP Registration	**No Account**
Call Status	Idle
Proxy Status	Single proxy mode
Security	TLS Disabled SRTP Disabled
Provisioning Status	None Found
MAC	00:22:ee:0b:00:52
IP	10.30.27.189
Netmask	255.0.0.0
Gateway	10.0.0.1
Date / Time	Thu Oct 31 17:10:15 UTC 2019
Multicast Mode	Disabled
Volume	Speaker Volume: 8 (-6dB)
Door Relay	Terminal Enabled, Door Locked
Network Door Controller	Not Configured
Extension to Dial	Not Configured

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

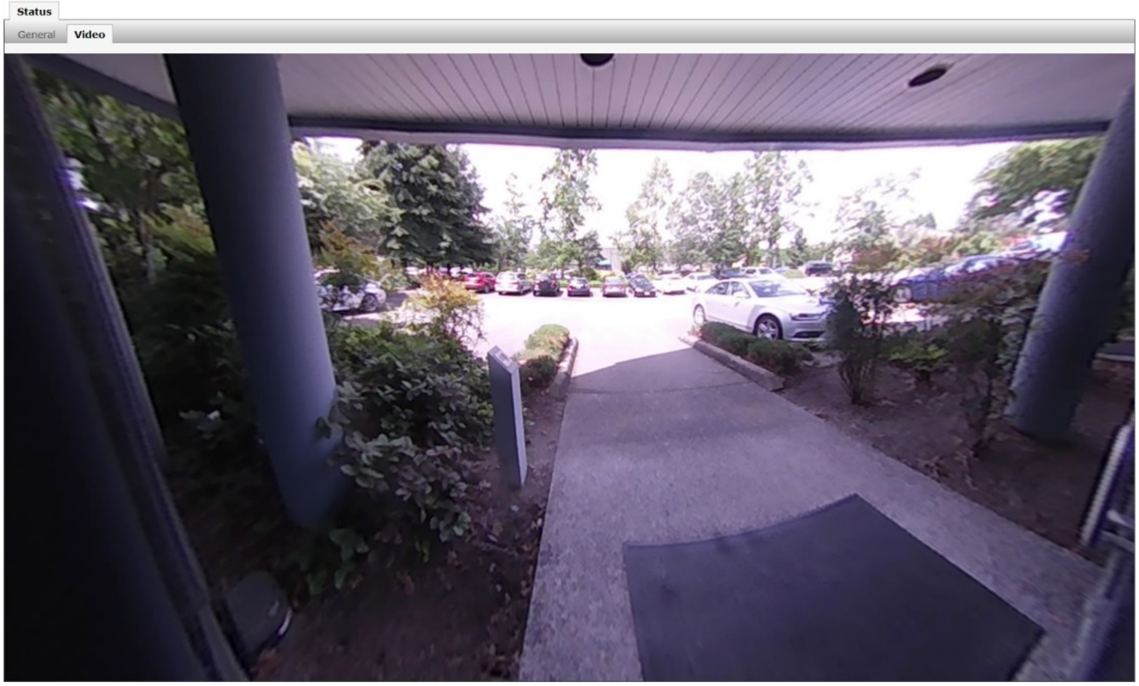
Status

The device's Status page will be available before and after log on. The section can be used to check 8039's SIP Registration status of the SIP extensions, Call Status, Proxy Status, Extension to Dial, Door Controller status, and general MAC, IP, Netmask, and Date/Time information.

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

Status Tab – Video

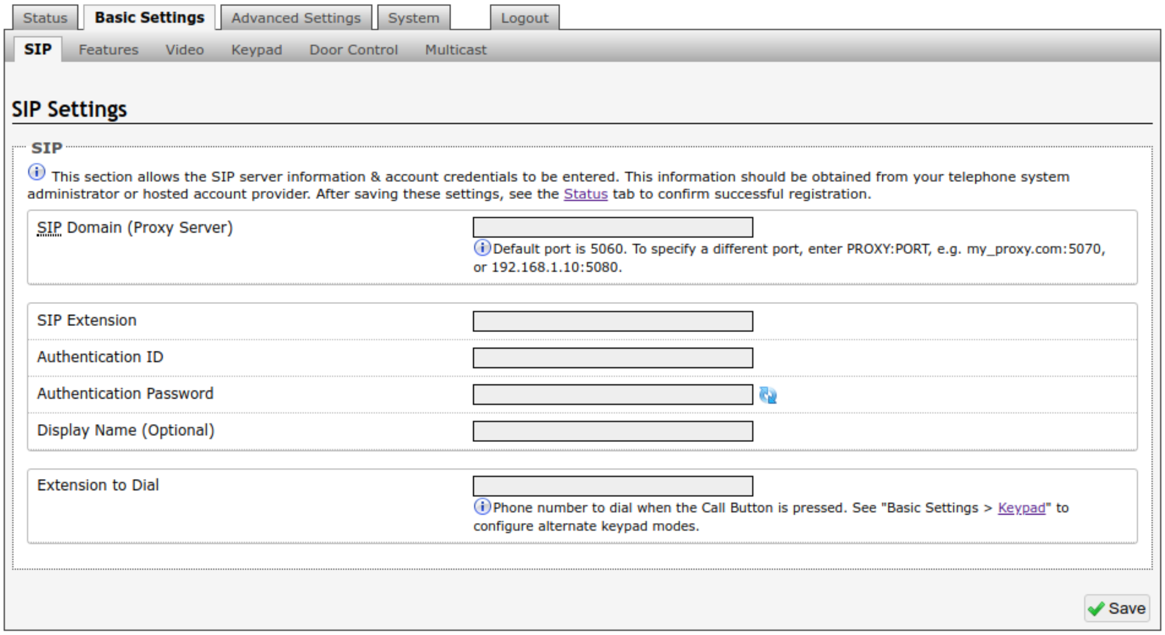
The video can be seen in the "Status > Video" tab when the user is not logged in. A separate video password can also be enabled, to allow users to access the video, but not the rest of the device settings. This password can be set in "Basic Settings > Video" tab, "Session Password" field. Video settings like brightness, contrast, view (Dewarped or Fisheye) are also available in the "Basic Settings > Video" tab.



Web Interface Basic Settings

Basic Settings Tab – SIP

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



SIP Settings

SIP

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

SIP Domain (Proxy Server)	ⓘ Default port is 5060. To specify a different port, enter PROXY:PORT, e.g. my_proxy.com:5070, or 192.168.1.10:5080.
SIP Extension	
Authentication ID	
Authentication Password	
Display Name (Optional)	
Extension to Dial	ⓘ Phone number to dial when the Call Button is pressed. See "Basic Settings > Keypad" to configure alternate keypad modes.

Important: Any time changes are made to settings in the web interface the ***'Save'*** *button must be clicked to save the changes.*

SIP Domain (Proxy Server)

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

SIP Extension

Used to register the 8039 on the SIP Server.

Authentication ID

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

Authentication Password

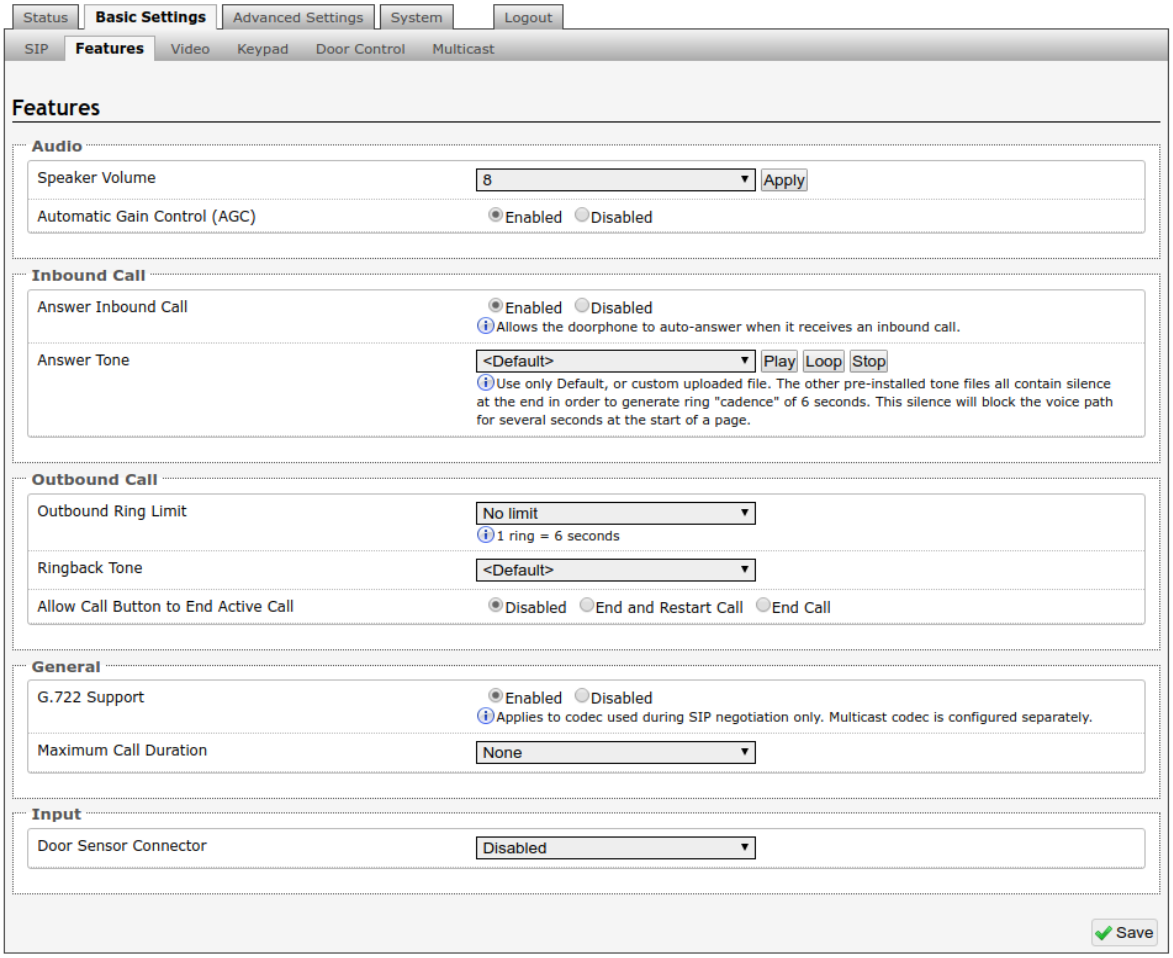
SIP password provided by the system administrator for the SIP account.

Extension to Dial

Enter the phone number that will be dialed when the call button is pressed. This can also be a Hunt Group number. Ensure that voice mail is not reached.

Note: The "Basic Settings > Keypad" tab offers additional keypad modes like playing a voice prompt when the call button is pressed and using the keypad to dial extensions or listed departments.

Basic Settings Tab – Features



Features

Audio

Speaker Volume	8
Automatic Gain Control (AGC)	● Enabled ○ Disabled

Inbound Call

Answer Inbound Call	● Enabled ○ Disabled Allows the doorphone to auto-answer when it receives an inbound call.
Answer Tone	<Default> Use only Default, or custom uploaded file. The other pre-installed tone files all contain silence at the end in order to generate ring "cadence" of 6 seconds. This silence will block the voice path for several seconds at the start of a page.

Outbound Call

Outbound Ring Limit	No limit 1 ring = 6 seconds
Ringback Tone	<Default>
Allow Call Button to End Active Call	● Disabled ○ End and Restart Call ○ End Call

General

G.722 Support	● Enabled ○ Disabled Applies to codec used during SIP negotiation only. Multicast codec is configured separately.
Maximum Call Duration	None

Input

Door Sensor Connector	Disabled

Speaker Volume

Select speaker audio level of the 8039 from 1 (lowest) to 10 (highest).

Automatic Gain Control (AGC)

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

Answer Inbound Call

Allow the 8039 to auto-answer an inbound call. By default, this functionality is activated.

Answer Tone

Select a tone to be played over the speaker when the intercom answers an inbound call. Use only Default, or custom uploaded file. The other pre-installed tone files all contain silence at the end in order to generate ring "cadence" of 6 seconds. This silence will block the voice path for several seconds at the start of a call.

Outbound Ring Limit

This feature can be used to set a limit on how long the intercom will ring before timing out. If the call is not answered within this time period, the 8039 will go back to an idle state.

Ringback Tone

Select an audible ringback tone to be played on the 8039 speaker until the call is answered.

Allow Call Button to End Active Call

If enabled, allows the visitor to end an active call by pressing the call button.

G.722 Support

Enable or disable the G.722 codec.

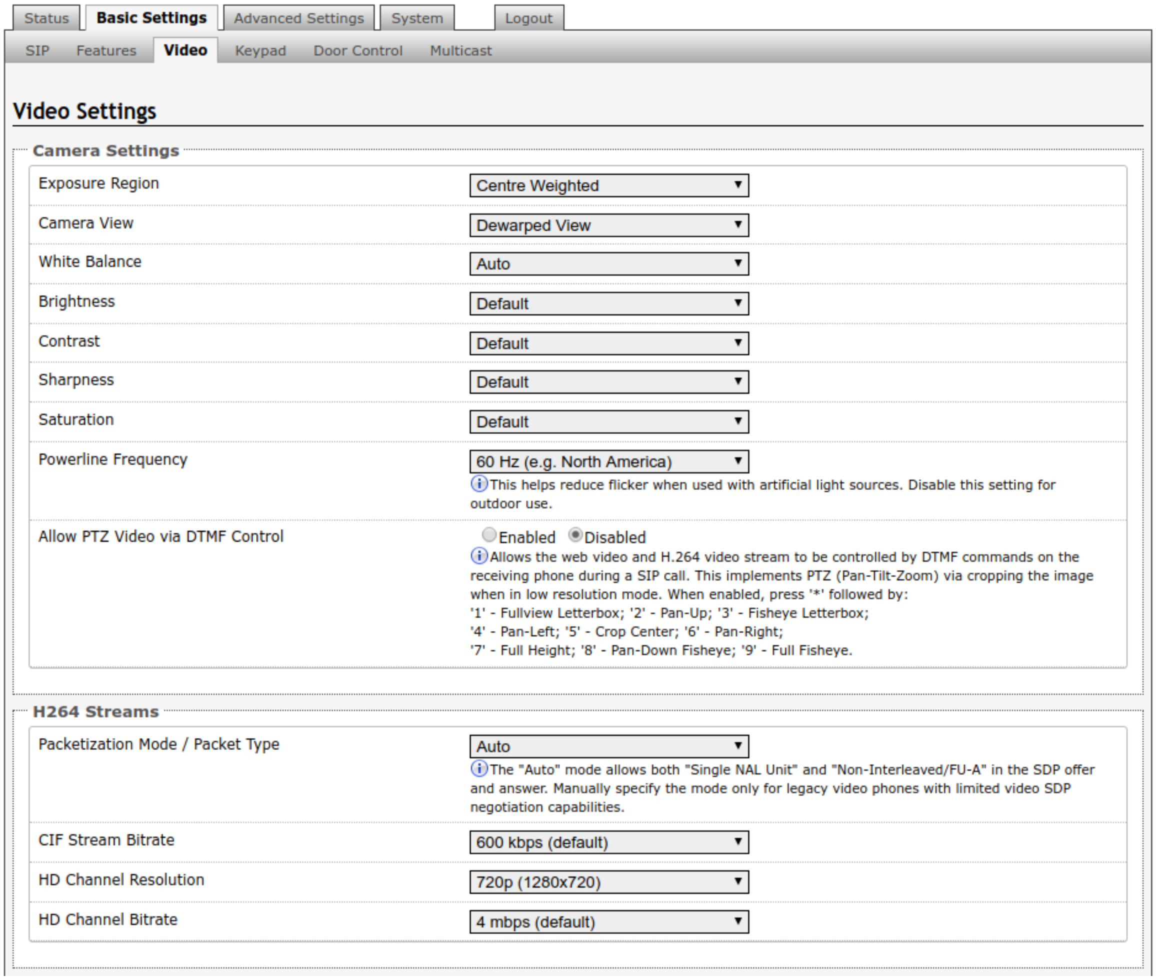
Maximum Call Duration

Select the maximum call length. The call will be terminated once the maximum time is reached. In the event that a call inadvertently reaches voicemail or gets accidentally left on hold, this setting ensures that the 8039 returns on-hook.

Door Sensor Connector

External call button can be used as an input to the door sensor connector. External call button will function like the call button on the device.

Basic Settings Tab – Video



Video Settings

Camera Settings

Exposure Region	Centre Weighted
Camera View	Dewarped View
White Balance	Auto
Brightness	Default
Contrast	Default
Sharpness	Default
Saturation	Default
Powerline Frequency	60 Hz (e.g. North America) ⓘThis helps reduce flicker when used with artificial light sources. Disable this setting for outdoor use.
Allow PTZ Video via DTMF Control	○ Enabled ● Disabled ⓘAllows the web video and H.264 video stream to be controlled by DTMF commands on the receiving phone during a SIP call. This implements PTZ (Pan-Tilt-Zoom) via cropping the image when in low resolution mode. When enabled, press '*' followed by: '1' - Fullview Letterbox; '2' - Pan-Up; '3' - Fisheye Letterbox; '4' - Pan-Left; '5' - Crop Center; '6' - Pan-Right; '7' - Full Height; '8' - Pan-Down Fisheye; '9' - Full Fisheye.

H264 Streams

Packetization Mode / Packet Type	Auto ⓘThe "Auto" mode allows both "Single NAL Unit" and "Non-Interleaved/FU-A" in the SDP offer and answer. Manually specify the mode only for legacy video phones with limited video SDP negotiation capabilities.
CIF Stream Bitrate	600 kbps (default)
HD Channel Resolution	720p (1280x720)
HD Channel Bitrate	4 mbps (default)

Exposure Region

Select an exposure calculation region for optimal image rendering. “Spot” method calculates exposure based on the center area of the image. “Full Frame” method uses the entire image to determine the exposure. “Centre Weighted” uses mainly the center area and a fraction of the remaining frame to compute the exposure.

Camera View

Camera view can be set to either a “Dewarped” full page view or a circular “Fisheye”.

White Balance

Select the white balance settings. “Auto” will auto-detect the light levels and auto-balance the video accordingly. Other balance choices include: Daylight 6500K and 5500K, Fluorescent, and Incandescent.

Brightness

Increase or decrease image brightness either above or below the default value.

Contrast

Increase or decrease image contrast either above or below the default value.

Sharpness

Increase or decrease image sharpness either above or below the default value.

Saturation

Increase or decrease image saturation either above or below the default value.

Powerline Frequency

Choose the local powerline frequency. For example, 60 Hz in North America and 50 Hz in Europe. This allows the device to reduce video flicker when used with indoor lighting.

Allow PTZ Video via DTMF Control

Use DTMF command to control the web video and H.264 video stream.

Packet Type

Refer to phone specifications to determine best supported packet type (“Single NAL Unit” or “Fragmentation Unit Type A (FU-A)”). Use ‘Auto’ mode except with legacy video phones with limited Video SDP negotiation capability.

CIF Stream Bitrate

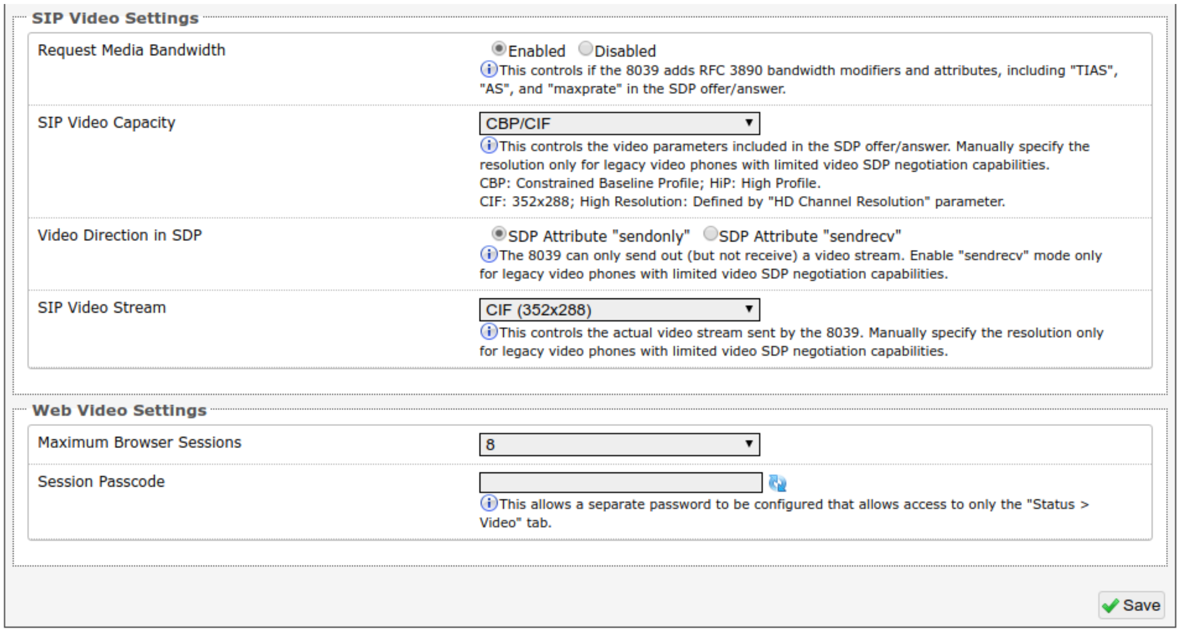
Select the amount of network traffic the device can use.

HD Channel Resolution

Select the video resolution as supported by the video phone that will answer the calls, 720p (1280x720) or VGA (640x480).

HD Channel Bitrate

Select the amount of network traffic the device can use.



SIP Video Settings

Request Media Bandwidth	● Enabled ○ Disabled ⓘ This controls if the 8039 adds RFC 3890 bandwidth modifiers and attributes, including "TIAS", "AS", and "maxprate" in the SDP offer/answer.
SIP Video Capacity	CBP/CIF ▾ ⓘ This controls the video parameters included in the SDP offer/answer. Manually specify the resolution only for legacy video phones with limited video SDP negotiation capabilities. CBP: Constrained Baseline Profile; HiP: High Profile. CIF: 352x288; High Resolution: Defined by "HD Channel Resolution" parameter.
Video Direction in SDP	● SDP Attribute "sendonly" ○ SDP Attribute "sendrecv" ⓘ The 8039 can only send out (but not receive) a video stream. Enable "sendrecv" mode only for legacy video phones with limited video SDP negotiation capabilities.
SIP Video Stream	CIF (352x288) ▾ ⓘ This controls the actual video stream sent by the 8039. Manually specify the resolution only for legacy video phones with limited video SDP negotiation capabilities.

Web Video Settings

Maximum Browser Sessions	8 ▾
Session Passcode	▭ ⓘ This allows a separate password to be configured that allows access to only the "Status > Video" tab.

Request Media Bandwidth

Adds bandwidth modifiers and attributes in the SDP offer/answer.

SIP Video Capacity

This controls the video parameters included in the SIP 'Offer' that is sent when the 8039 initiates a call. Select the video capacity as supported by the video phone that will answer the calls.

SIP Video Stream

This controls the actual video stream sent by the 8039. Use ‘Auto’ mode unless a manual override is required for compatibility with legacy video phones.

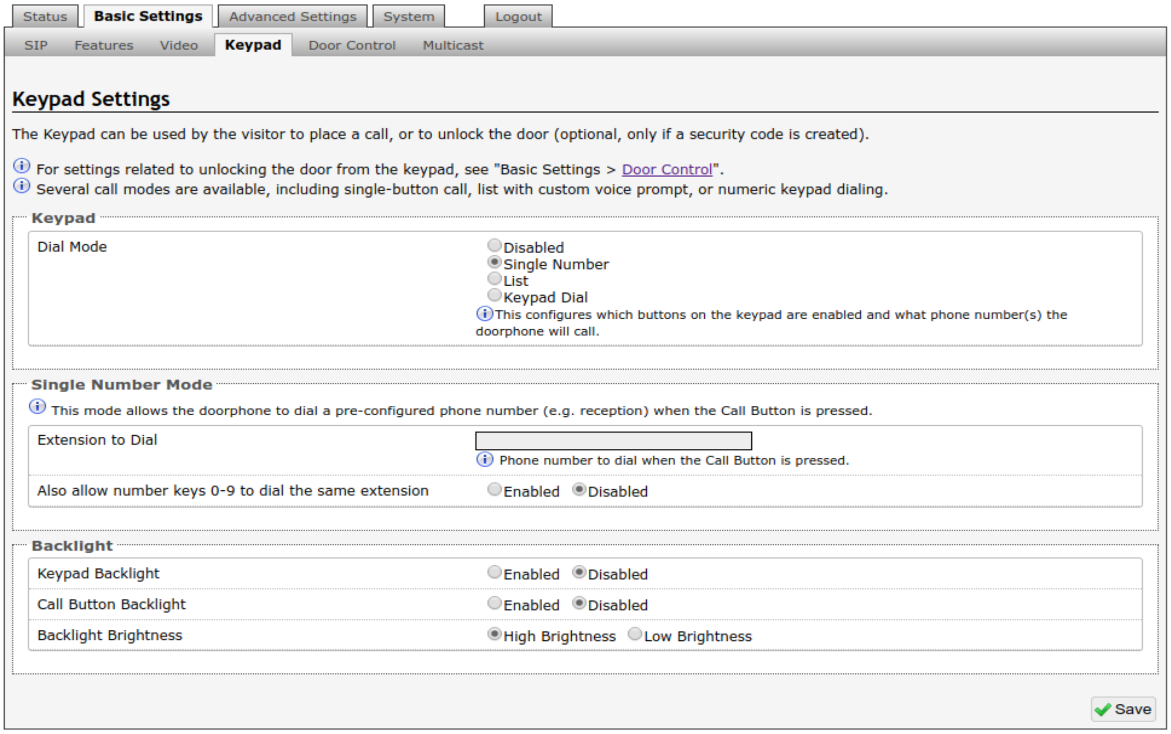
Maximum Browser Sessions

Allows for a limit to be set on the number of separate browser sessions that can be open simultaneously to show the video. The setting can be “Disabled” to turn off the web video capability.

Session Passcode

This allows a separate password to be configured that allows access to only the “Status > Video” tab.

Basic Settings Tab – Keypad



Keypad Settings

The Keypad can be used by the visitor to place a call, or to unlock the door (optional, only if a security code is created).

ⓘ For settings related to unlocking the door from the keypad, see "Basic Settings > Door Control".
ⓘ Several call modes are available, including single-button call, list with custom voice prompt, or numeric keypad dialing.

Keypad

Dial Mode	○ Disabled ● Single Number ○ List ○ Keypad Dial ⓘ This configures which buttons on the keypad are enabled and what phone number(s) the doorphone will call.

Single Number Mode

ⓘ This mode allows the doorphone to dial a pre-configured phone number (e.g. reception) when the Call Button is pressed.

Extension to Dial	ⓘ Phone number to dial when the Call Button is pressed.
Also allow number keys 0-9 to dial the same extension	○ Enabled ● Disabled

Backlight

Keypad Backlight	○ Enabled ● Disabled
Call Button Backlight	○ Enabled ● Disabled
Backlight Brightness	● High Brightness ○ Low Brightness

Dial Mode – Single Number

This mode allows the 8039's "Call" button to dial a pre-configured number, the "Extension to Dial". There is also an option to allow all the number keys on the keypad to dial this same extension.

Dial Mode – List

This mode allows each of the 10 "number" keys to dial a different preconfigured phone number. For example, 1 for Reception, 2 for Sales, 3 for Shipping, etc.

The Call button can be configured to play a voice prompt detailing the available options to the visitor. The voice prompt can be uploaded via a custom audio file in the "Advanced Settings > File Manager" tab.

Dial Mode – Keypad Dial

This mode allows the keypad to be used to dial extensions directly. If an incorrect number is dialed by mistake, the "#" key can be pressed to cancel, and the extension can be dialed again.

Set the "Length of Extension to Dial", correctly to match the extension length of your phone system.

The Call button can be set to "Dial Extension" (e.g. reception) or to "Play Voice Prompt" giving the visitor instructions and/or summary of main extensions to dial via the keypad.

Warning: Set appropriate permissions on the phone system to ensure that a malicious visitor cannot use the intercom to dial an external number. Also ensure that a visitor will not reach voicemail to prevent the call from getting "stuck"

Keypad Backlight

Enable or disable the Keypad's blue backlight.

Call Button Backlight

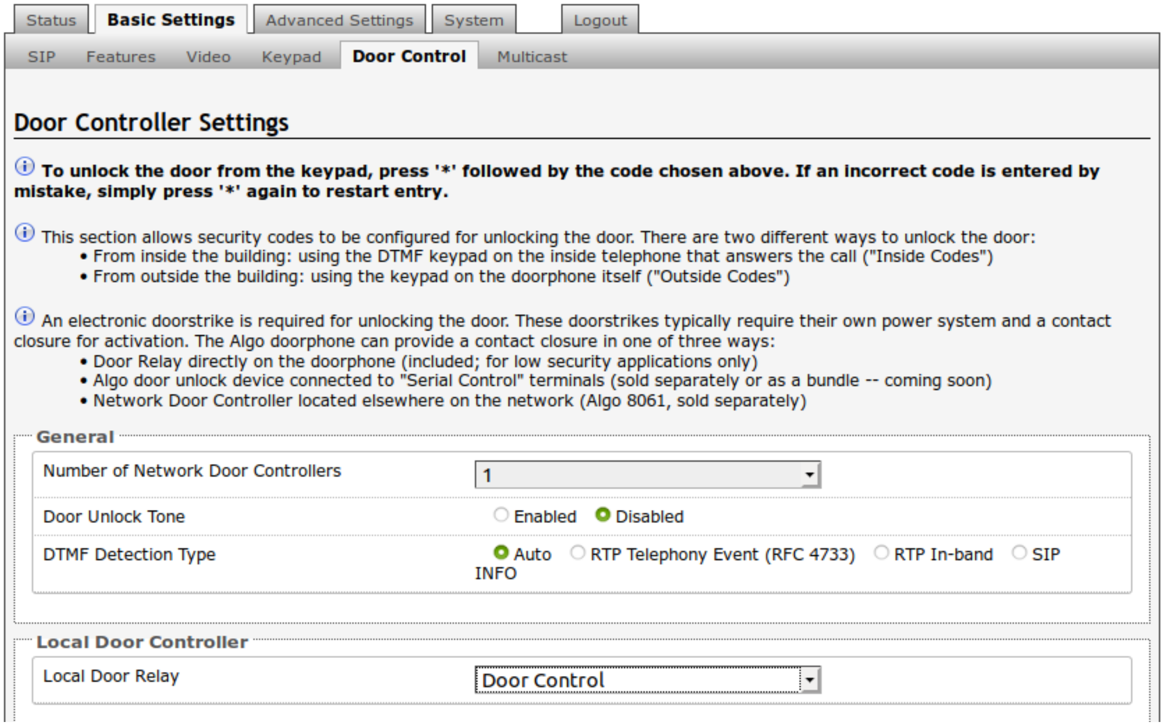
Enable or disable the Call Button's blue backlight.

Backlight Brightness

Configures the brightness of the Keypad and Call Button backlight if they are enabled.

Basic Settings Tab – Door Control

The 8039 contains a relay that can be used for Door Control, or it can be used with the optional 8061 IP Relay Controller (sold separately) for additional door security, as the 8061 can be located inside the building and separate from the public-facing intercom. This section allows you to configure the 8061 settings (if used), or the local door relay. For more information about the 8061, see "8061 IP Relay Controller" on page 48.



Door Controller Settings

To unlock the door from the keypad, press '*' followed by the code chosen above. If an incorrect code is entered by mistake, simply press '*' again to restart entry.

This section allows security codes to be configured for unlocking the door. There are two different ways to unlock the door:
- From inside the building: using the DTMF keypad on the inside telephone that answers the call ("Inside Codes")
- From outside the building: using the keypad on the doorphone itself ("Outside Codes")

An electronic doorstrike is required for unlocking the door. These doorstrikes typically require their own power system and a contact closure for activation. The Algo doorphone can provide a contact closure in one of three ways:
- Door Relay directly on the doorphone (included; for low security applications only)
- Algo door unlock device connected to "Serial Control" terminals (sold separately or as a bundle -- coming soon)
- Network Door Controller located elsewhere on the network (Algo 8061, sold separately)

General

Number of Network Door Controllers	1
Door Unlock Tone	○ Enabled ● Disabled
DTMF Detection Type	● Auto ○ RTP Telephony Event (RFC 4733) ○ RTP In-band ○ SIP INFO

Local Door Controller

Local Door Relay	Door Control

Number of Network Door Controllers

Set up to 4 network door controllers (8061s) to unlock/lock the doors.

Door Unlock Tone

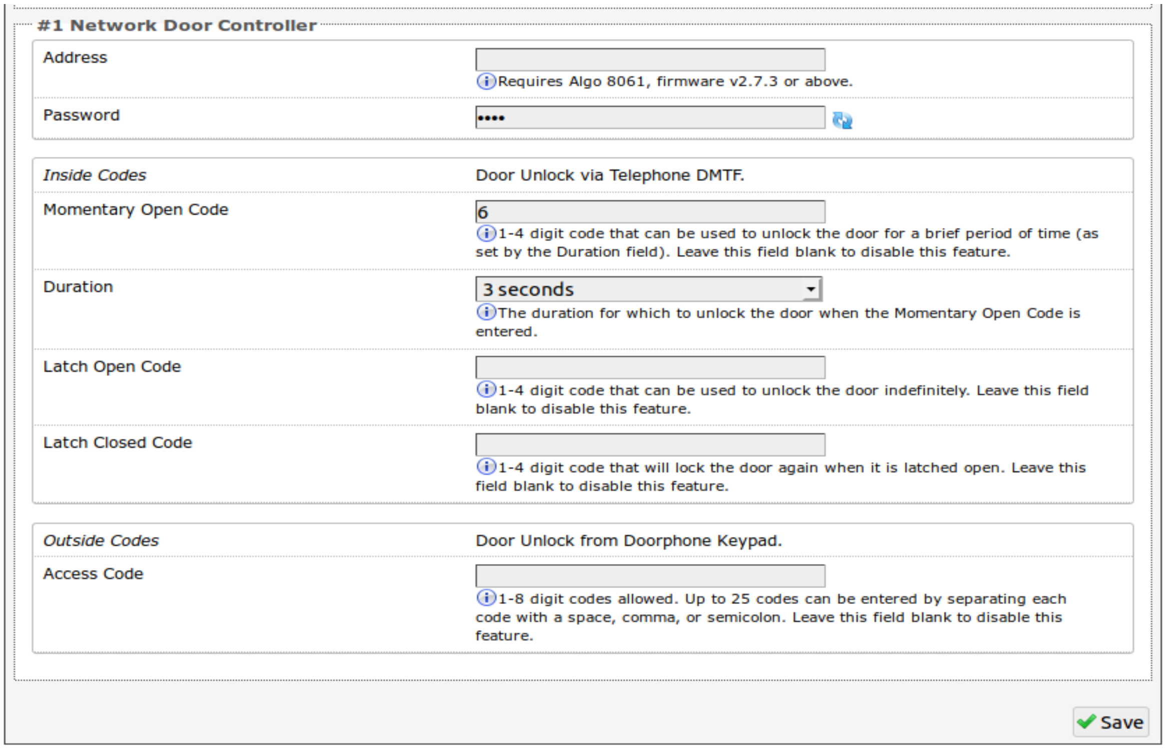
Allow a tone to be played when the door is unlocked to create awareness.

DTMF Detection Type

Different DTMF detection options are given. Use the default of ‘Auto’ unless advised by Algo technical support.

Local Door Relay

Enable or disable the door control relay on the 8039.



#1 Network Door Controller

Address	ⓘRequires Algo 8061, firmware v2.7.3 or above.
Password	••••

Inside Codes	Door Unlock via Telephone DMTF.
Momentary Open Code	6 ⓘ1-4 digit code that can be used to unlock the door for a brief period of time (as set by the Duration field). Leave this field blank to disable this feature.
Duration	3 seconds ⓘThe duration for which to unlock the door when the Momentary Open Code is entered.
Latch Open Code	ⓘ1-4 digit code that can be used to unlock the door indefinitely. Leave this field blank to disable this feature.
Latch Closed Code	ⓘ1-4 digit code that will lock the door again when it is latched open. Leave this field blank to disable this feature.

Outside Codes	Door Unlock from Doorphone Keypad.
Access Code	ⓘ1-8 digit codes allowed. Up to 25 codes can be entered by separating each code with a space, comma, or semicolon. Leave this field blank to disable this feature.

Network Door Controller Address

IP address of the optional 8061 IP Relay Controller. For 8061 configuration, see page 48.

Network Door Controller Password

Used to authenticate the link between the 8039 and the 8061. Ensure that the two devices have matching passwords. Default password is ***algo*.**

> *Note: The Relay Module Password is used solely to secure the link between the 8039 and the 8061. It is not the same as the Momentary Open Code.*

Momentary Open Code

1-4 digit DTMF code that can be used to unlock the door for a brief period of time. Leave this field blank to disable this feature.

(Default: 6)

Duration

The time period for which to unlock the door when the Momentary Open Code is entered. From ¼ to 30 seconds.

Latch Open Code

1-4 digit DTMF code that can be used to unlock the door indefinitely. Leave this field blank to disable this feature.

Latch Closed Code

1-4 digit DTMF code that will lock the door again when it is latched open. Leave this field blank to disable this feature.

Outside codes

This is a “secret” code that allows authorized visitors or employees to let themselves in without needing to call someone inside the building.

Access Code

1-8 digit codes allowed. Up to 25 codes can be entered by separating each code with a space, comma, or semicolon. Leave this field blank to disable this feature.

Basic Settings Tab – Multicast

Multicast IP Addresses

Each 8039 SIP Video Intercom has its own IP address, and shares a common multicast IP and port number (multicast zone) for multicast packets. The 8039 is able to act as a multicast Slave, allowing it to multicast messages from a Master device over the intercom speaker.

Note: The 8039 is not meant for voice paging in large areas. Instead we recommend using the 8186 SIP Horn Speaker for outdoor or wide-area applications, and the 8180 SIP Audio Alerter or 8188 SIP Ceiling Speaker for any other indoor paging requirements.

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

7. Multicast IP addresses range: 224.0.0.0/4 (from 224.0.0.0 to 239.255.255.255)
8. Port numbers range: 1 to 65535
9. By default, the 8039 Video Intercom is set to use the multicast IP address 224.0.2.60 and the port numbers 50000-50008

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

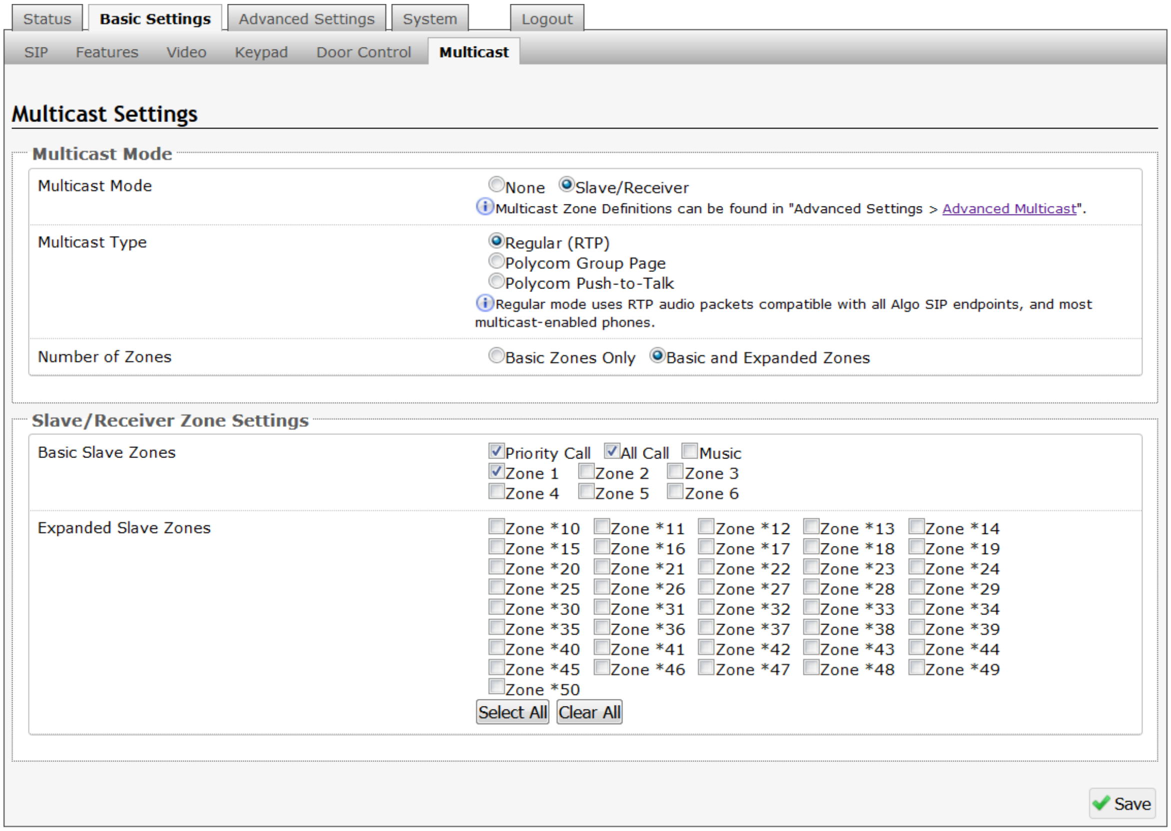
Multicast Page Zones

The 8039 Video Intercom supports nine “basic” multicast zones. These zones are defined by the multicast IP addresses.

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

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

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



Multicast Settings

Multicast Mode

Multicast Mode: ○ None ● Slave/Receiver

Multicast Zone Definitions can be found in "Advanced Settings > Advanced Multicast".

Multicast Type: ● Regular (RTP) ○ Polycom Group Page ○ Polycom Push-to-Talk

Regular mode uses RTP audio packets compatible with all Algo SIP endpoints, and most multicast-enabled phones.

Number of Zones: ○ Basic Zones Only ● Basic and Expanded Zones

Slave/Receiver Zone Settings

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

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

Multicast Mode (Slave Selected)

If Slave mode is enabled the 8039 intercom speaker will activate when receiving a multicast message.

Multicast Type - Regular

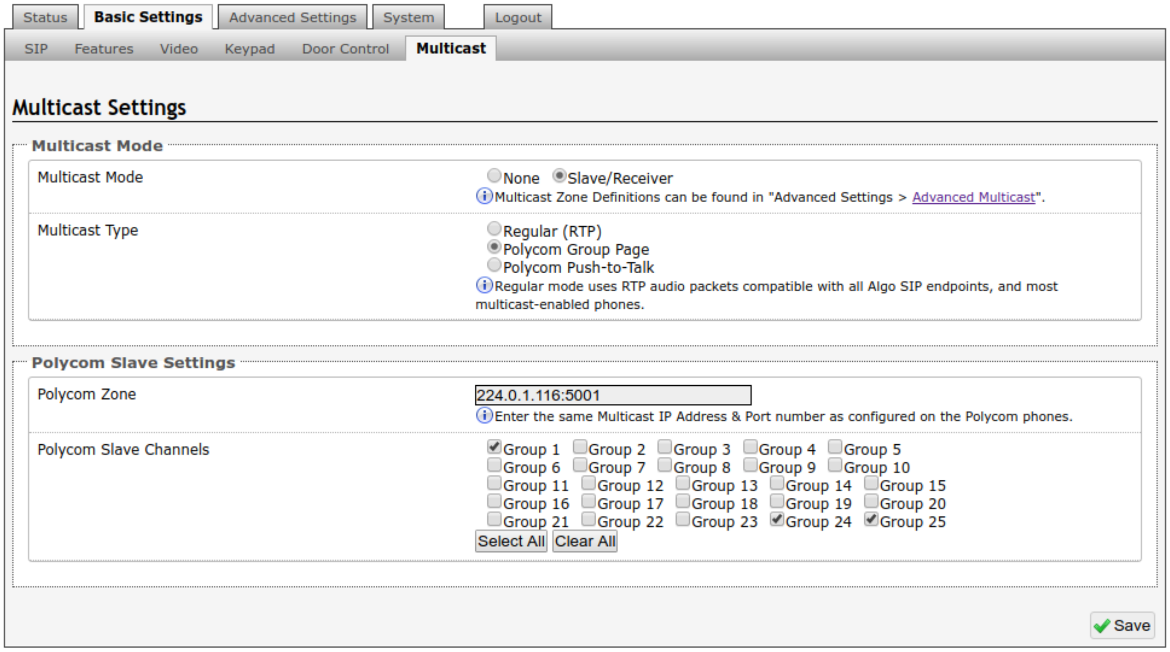
Select "Regular" if receiving multicast from other Algo SIP endpoint(s) and/or multicast-enabled phone(s) that use RTP audio packets.

Number of Zones

Select "basic" zones if configuring nine or fewer multicast zones or "expanded" to configure up to 50 zones. The expanded zones have the same behaviour as the basic slave zones, but are hidden by default to simplify the interface.

Slave Zones

Select one or more multicast zones for the 8039 SIP Video Intercom to monitor. Note that multicast zone priority is based on the zone definition list order (top to bottom).



Multicast Settings

Multicast Mode

Multicast Mode: ○ None ● Slave/Receiver
ⓘ Multicast Zone Definitions can be found in "Advanced Settings > Advanced Multicast".

Multicast Type: ○ Regular (RTP) ● Polycom Group Page ○ Polycom Push-to-Talk
ⓘ Regular mode uses RTP audio packets compatible with all Algo SIP endpoints, and most multicast-enabled phones.

Polycom Slave Settings

Polycom Zone: 224.0.1.116:5001
ⓘ Enter the same Multicast IP Address & Port number as configured on the Polycom phones.

Polycom Slave Channels:
☑ Group 1 □ Group 2 □ Group 3 □ Group 4 □ Group 5
□ Group 6 □ Group 7 □ Group 8 □ Group 9 □ Group 10
□ Group 11 □ Group 12 □ Group 13 □ Group 14 □ Group 15
□ Group 16 □ Group 17 □ Group 18 □ Group 19 □ Group 20
□ Group 21 □ Group 22 □ Group 23 ☑ Group 24 ☑ Group 25
Select All | Clear All

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

The 8039 SIP Video Intercom may receive multicast paging compatible with Polycom ***"on premise group paging"*** protocol.

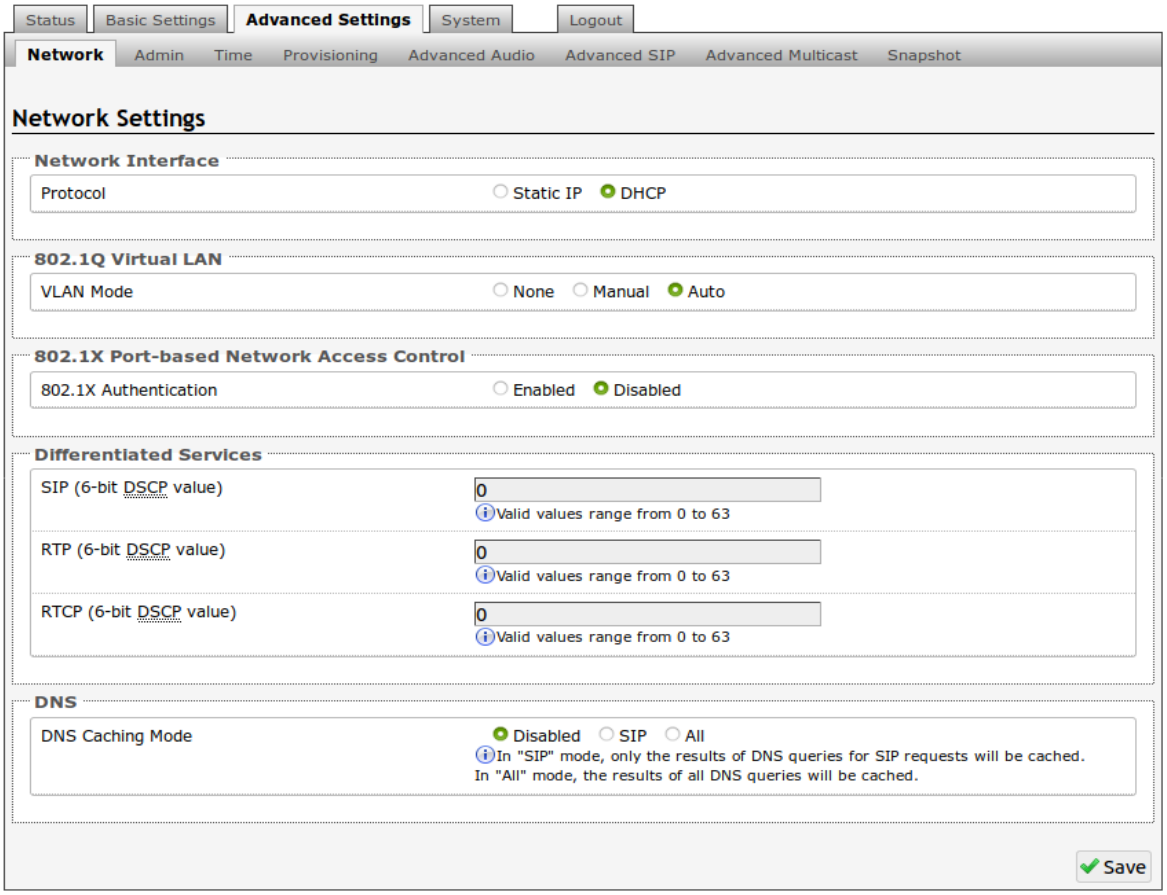
To configure the 8039 as a slave to play Polycom page announcements, select "Group Page" or "Push-to-Talk". Then enter the Polycom Zone (IP Address and Port) that matches the configuration of the Polycom phones and Channels. The "Default Channel" is the target group in a Polycom paging environment.

The Polycom phone used as page audio source for the 8039(s), must be configured to use either the G.711 or G.722 audio codec. **The Polycom phone(s) must also be configured with the "Compatibility" setting ("ptt.compatibilityMode")** **disabled** in order for this codec setting to be applied.

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

Web Interface Advanced Settings

Advanced Settings Tab - Network



Network Settings

Network Interface

Protocol ○ Static IP ● DHCP

802.1Q Virtual LAN

VLAN Mode ○ None ○ Manual ● Auto

802.1X Port-based Network Access Control

802.1X Authentication ○ Enabled ● Disabled

Differentiated Services

SIP (6-bit DSCP value) 0
ⓘValid values range from 0 to 63

RTP (6-bit DSCP value) 0
ⓘValid values range from 0 to 63

RTCP (6-bit DSCP value) 0
ⓘValid values range from 0 to 63

DNS

DNS Caching Mode ● Disabled ○ SIP ○ All
ⓘIn "SIP" mode, only the results of DNS queries for SIP requests will be cached.
In "All" mode, the results of all DNS queries will be cached.

Protocol

DHCP is an IP standard designed to make administration of IP addresses simpler. When selected, DHCP will automatically configure IP addresses for each 8039 on the network. Alternatively the 8039 can be set to a static IP address.

VLAN Mode

Enables or Disables VLAN Tagging. VLAN Tagging is the networking standard that supports Virtual LANs (VLANs) on an Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames. The standard also provides provisions for a quality of service prioritization scheme commonly known as IEEE 802.1p and defines the Generic Attribute Registration Protocol.

VLAN ID

Specifies the VLAN to which the Ethernet frame belongs. A 12-bit field specifying the VLAN to which the Ethernet frame belongs. The hexadecimal values of 0x000 and 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. On bridges, VLAN 1 (the default VLAN ID) is often reserved for a management VLAN; this is vendor specific.

VLAN Priority

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

802.1x Authentication

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

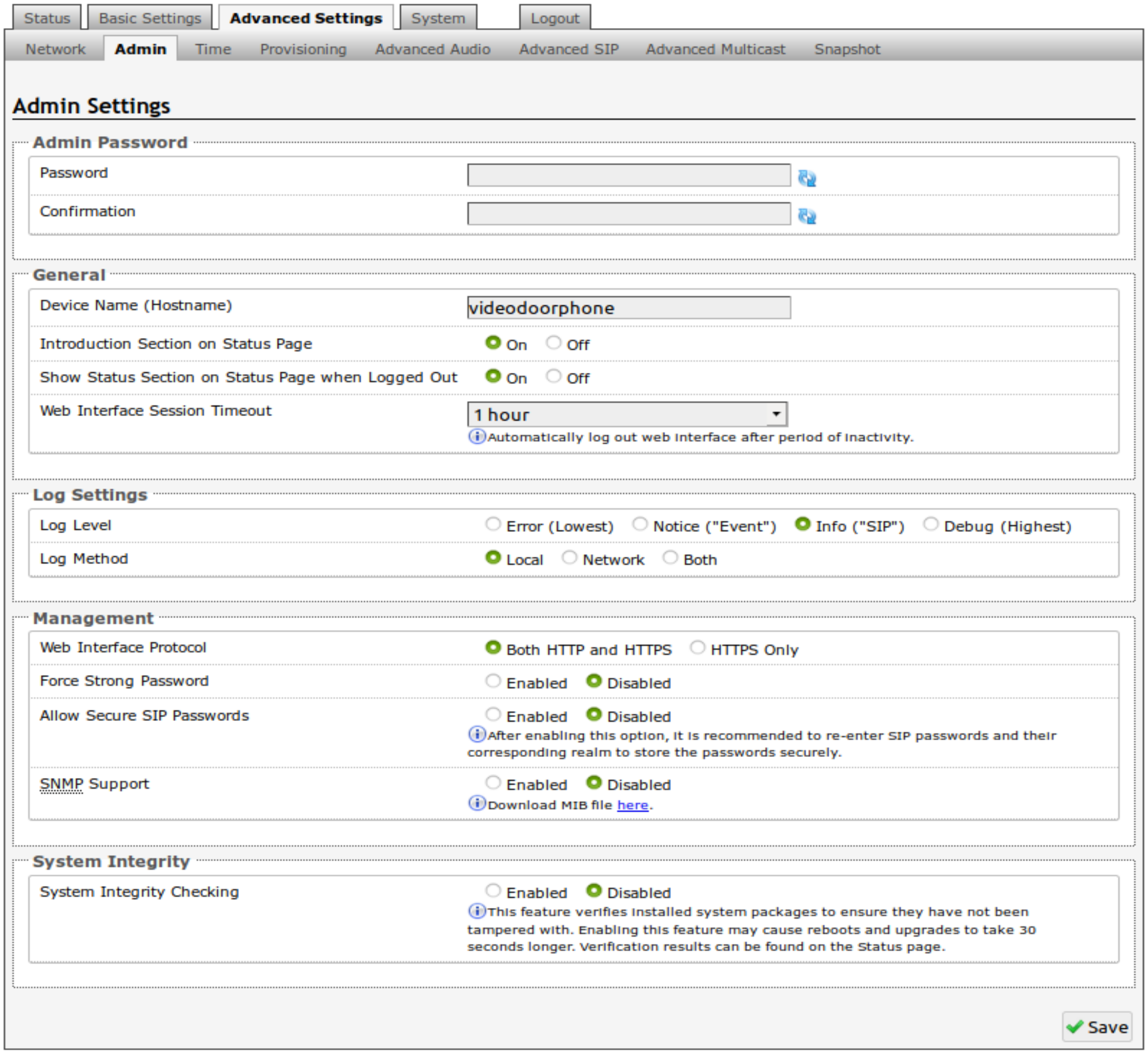
Differentiated Services (6-bit DSCP value)

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

DNS Caching Mode

In "SIP" mode, only the results of DNS queries for SIP requests will be cached. In "All" mode, the results of all DNS queries will be cached.

Advanced Settings Tab – Admin



Admin Settings

Admin Password

Password

Confirmation

General

Device Name (Hostname): videodoorphone

Introduction Section on Status Page: ● On ○ Off

Show Status Section on Status Page when Logged Out: ● On ○ Off

Web Interface Session Timeout: 1 hour

Automatically log out web interface after period of inactivity.

Log Settings

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

Log Method: ● Local ○ Network ○ Both

Management

Web Interface Protocol: ● Both HTTP and HTTPS ○ HTTPS Only

Force Strong Password: ○ Enabled ● Disabled

Allow Secure SIP Passwords: ○ Enabled ● Disabled

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

SNMP Support: ○ Enabled ● Disabled

Download MIB file here.

System Integrity

System Integrity Checking: ○ Enabled ● Disabled

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

Password

Password to log into the 8039 SIP Video Intercom web interface. You should change the default password ***algo*** in order to secure the device on the network. If you have forgotten your password, you will need to perform a reset using the Reset Button in order to restore the password (as well as all other settings) back to the original factory default conditions.

For additional password security see “Force Strong Password” below.

Confirmation

Re-enter network admin password.

Device Name (Hostname)

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

Introduction Section on Status Page

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

Show Status Section on Status Page when Logged Out

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

Web Interface Session Timeout

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

Log Level

Use on the advice of Algo technical support only.

Log Method

Allows the 8039 SIP Video Intercom to write to external Syslog server if the option for external (or both) is selected.

Log Server

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

Web Interface Protocol

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

Force Strong Password

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

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

Allow Secure SIP Password

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

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

To obtain your SIP Realm information, contact your SIP Server administrator (or check the SIP log file for a registration attempt). The Realms may be the same or different for all the extensions used.

SNMP Support

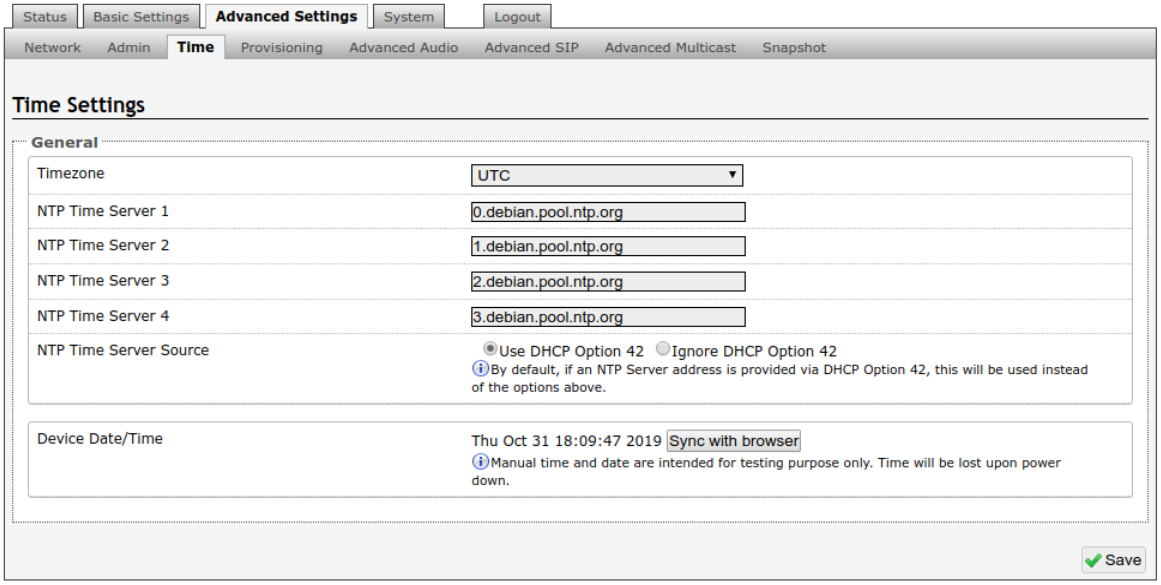
Additional SNMP support is anticipated for future, but the 8039 SIP Video Intercom will respond to a simple status query for automated supervision. Contact Algo technical support for more information.

System Integrity Checking

This feature verifies installed system packages to ensure they have not been tampered with by running ‘Perform Check’. Enabling this feature may cause reboots and upgrades to take 30 seconds longer. Verification results can be found on the Status page.

Advanced Settings Tab – Time

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



Time Settings

General

Timezone	UTC ▾
NTP Time Server 1	0.debian.pool.ntp.org
NTP Time Server 2	1.debian.pool.ntp.org
NTP Time Server 3	2.debian.pool.ntp.org
NTP Time Server 4	3.debian.pool.ntp.org
NTP Time Server Source	● Use DHCP Option 42 ○ Ignore DHCP Option 42 ⓘ By default, if an NTP Server address is provided via DHCP Option 42, this will be used instead of the options above.
Device Date/Time	Thu Oct 31 18:09:47 2019 Sync with browser ⓘ Manual time and date are intended for testing purpose only. Time will be lost upon power down.

Timezone

Select time zone.

NTP Time Servers 1/2/3/4

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

NTP Time Server Source

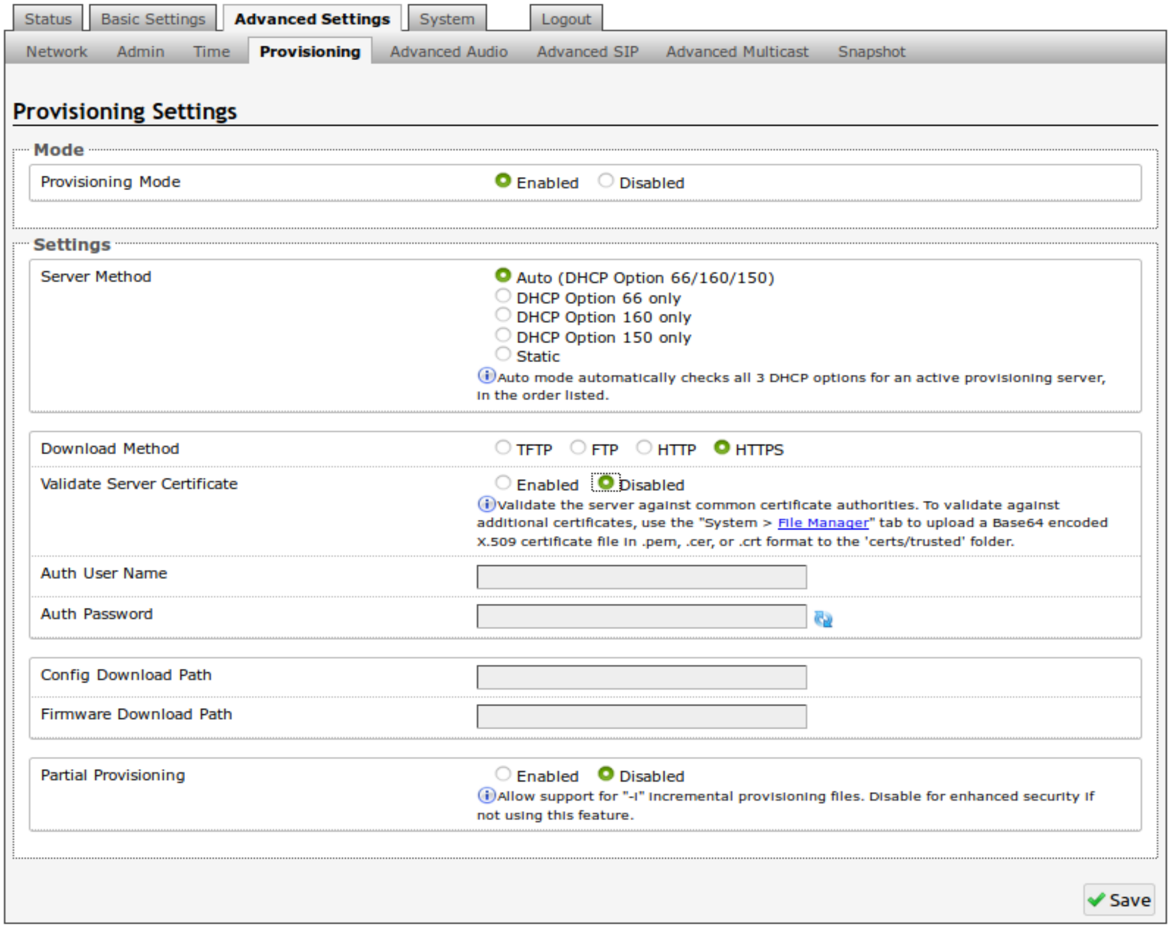
When “Use DHCP Option 42” is chosen, if an NTP Server address is provided via the DHCP Option 42, that NTP Server will be used instead of the 4 mentioned above. Alternatively, “Ignore DHCP Option 42” can be chosen to only use servers mentioned above.

Device Date/Time

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

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

Advanced Settings Tab – Provisioning



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

Validate Server Certificate: ○ Enabled ● Disabled
Validate the server against common certificate authorities. To validate against additional certificates, use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder.

Auth User Name:

Auth Password:

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.

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

Provisioning allows installers to pre-configure 8039 SIP Video Intercom units prior to installation on a network. It is typically used for large deployments to save time and ensure consistent setups.

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

For example, 8039 configuration files can be automatically downloaded from a TFTP server using DHCP Option 66. This option code (when set) supplies a TFTP boot server address to the DHCP client to boot from.

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

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

Generic (for all Algo 8039 Intercoms)	**algop8039.conf**
Specific (for a specific MAC address)	**algom[MAC].conf**

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

MD5 Checksum

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

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

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

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

Generating a generic configuration file

1. Connect 8039 to the network
2. Access the 8039 Web Interface Control Panel
3. Configure the 8039 with desired options
4. Click on the System tab and then Maintenance.
5. Click "Download" to download the current configuration file
6. Save the file settings.txt

7. Rename file settings.txt to algop8039.conf
8. File algop8039.conf can now be uploaded onto the Provisioning server

If using a generic configuration file, extensions and credentials have to be entered manually once the 8039 SIP Video Intercom has automatically downloaded the configuration file.

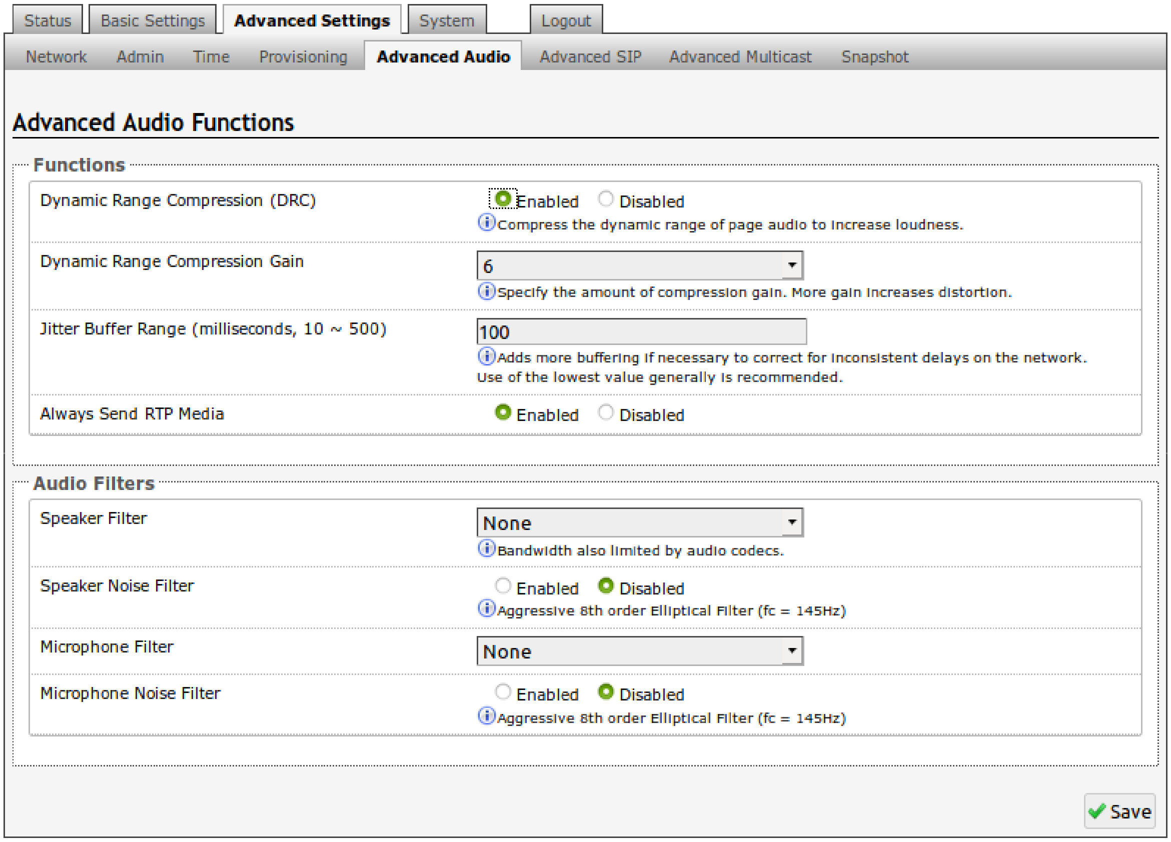
Generating a specific configuration file

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

The specific configuration file will only be downloaded by the 8039 SIP Video Intercom with the MAC address specified in the configuration file name. Since all the necessary settings can be included in this file, the 8039 will be ready to work immediately after the configuration file is downloaded. The MAC address of each 8039 SIP Video Intercom can be found on the back label of the unit.

For more Algo SIP endpoint provisioning information, see: www.algosolutions.com/provision

Advanced Settings Tab – Advanced Audio



Advanced Audio Functions

Functions

Dynamic Range Compression (DRC): ● Enabled ○ Disabled
Compress the dynamic range of page audio to increase loudness.

Dynamic Range Compression Gain: 6
Specify the amount of compression gain. More gain increases distortion.

Jitter Buffer Range (milliseconds, 10 ~ 500): 100
Adds more buffering if necessary to correct for inconsistent delays on the network. Use of the lowest value generally is recommended.

Always Send RTP Media: ● Enabled ○ Disabled

Audio Filters

Speaker Filter: None
Bandwidth also limited by audio codecs.

Speaker Noise Filter: ○ Enabled ● Disabled
Aggressive 8th order Elliptical Filter (fc = 145Hz)

Microphone Filter: None

Microphone Noise Filter: ○ Enabled ● Disabled
Aggressive 8th order Elliptical Filter (fc = 145Hz)

Dynamic Range Compression (DRC)

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

Dynamic Range Compression Gain

‘Dynamic Range Compression’ must be enabled to display this setting. Higher compression gain increases distortion.

Jitter Buffer Range

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

Always Send RTP Media

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

Speaker Filter

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

Speaker Noise Filter

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

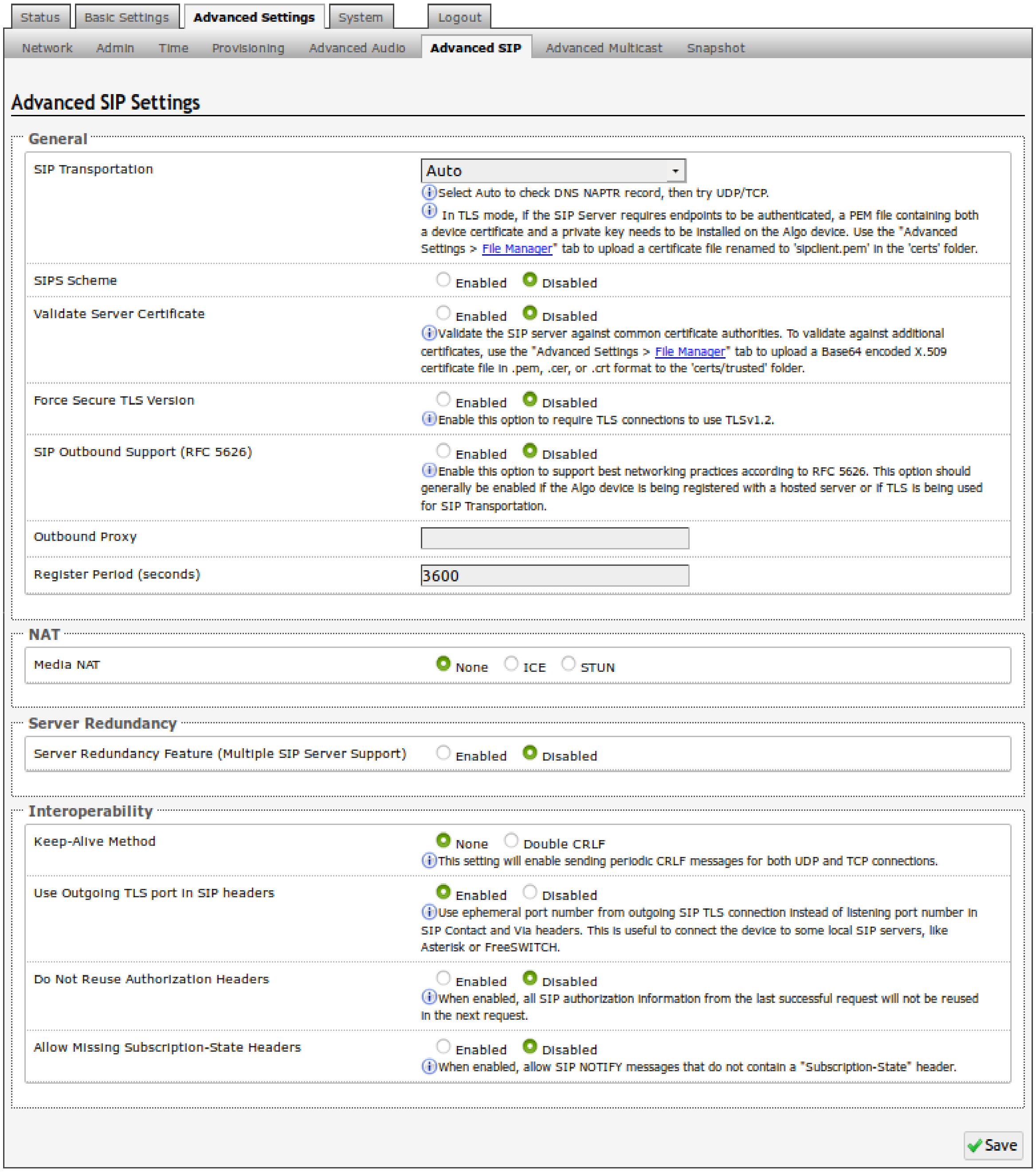
Microphone Filter

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

Microphone Noise Filter

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

Advanced Settings Tab – Advanced SIP



Advanced SIP Settings

General

SIP Transportation	Auto ⓘSelect Auto to check DNS NAPTR record, then try UDP/TCP. ⓘ In TLS mode, if the SIP Server requires endpoints to be authenticated, a PEM file containing both a device certificate and a private key needs to be installed on the Algo device. Use the "Advanced Settings > File Manager" tab to upload a certificate file renamed to 'sipclient.pem' in the 'certs' folder.
SIPS Scheme	○ Enabled ● Disabled
Validate Server Certificate	○ Enabled ● Disabled ⓘValidate the SIP server against common certificate authorities. To validate against additional certificates, use the "Advanced Settings > File Manager" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder.
Force Secure TLS Version	○ Enabled ● Disabled ⓘEnable this option to require TLS connections to use TLSv1.2.
SIP Outbound Support (RFC 5626)	○ Enabled ● Disabled ⓘEnable this option to support best networking practices according to RFC 5626. This option should generally be enabled if the Algo device is being registered with a hosted server or if TLS is being used for SIP Transportation.
Outbound Proxy	
Register Period (seconds)	3600

NAT

Media NAT	● None ○ ICE ○ STUN

Server Redundancy

Server Redundancy Feature (Multiple SIP Server Support)	○ Enabled ● Disabled

Interoperability

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

✓ Save

SIP Transportation

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

SIPS Scheme

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

SIP Outbound Support (RFC 5626)

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

Outbound Proxy

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

Register Period (seconds)

Maximum requested period of time where the 8128 SIP Strobe Light will re-register with the SIP server. Default setting is 3600 seconds (1 hour). Only change if instructed otherwise.

Media NAT

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

Server Redundancy Feature

Two secondary SIP servers may be configured. The 8039 SIP Video Intercom will attempt to register with the primary server but switch to a secondary server when necessary. The configuration allows re-registration to the primary server upon availability or to stay with a server until unresponsive.

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

Backup Server #1

If primary server is unreachable the 8039 SIP Video Intercom will attempt to register with the backup servers. If enabled, the 8039 SIP Video Intercom will always attempt to register with the highest priority server.

Backup Server #2

If backup server #1 is unreachable the 8039 SIP Video Intercom will attempt to register with the 2nd backup server. If enabled, the 8039 SIP Video Intercom will always attempt to register with the highest priority server.

Polling Intervals (seconds)

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

Poll Active Server

Explicitly poll current server to monitor availability. May also be handled automatically by other regular events, so can be disabled to reduce network traffic.

Automatic Fallback

Reconnect with higher priority server once available, even if backup connection is still fine.

Polling Method

SIP message used to poll servers to monitor availability.

Keep-alive Method

If Double CRLF is selected the 8039 SIP Video Intercom will send a packet every 30 seconds (unless changed) to maintain connection with the SIP Server if behind NAT.

Keep-alive Interval

Interval in seconds that the CRLF message should be sent.

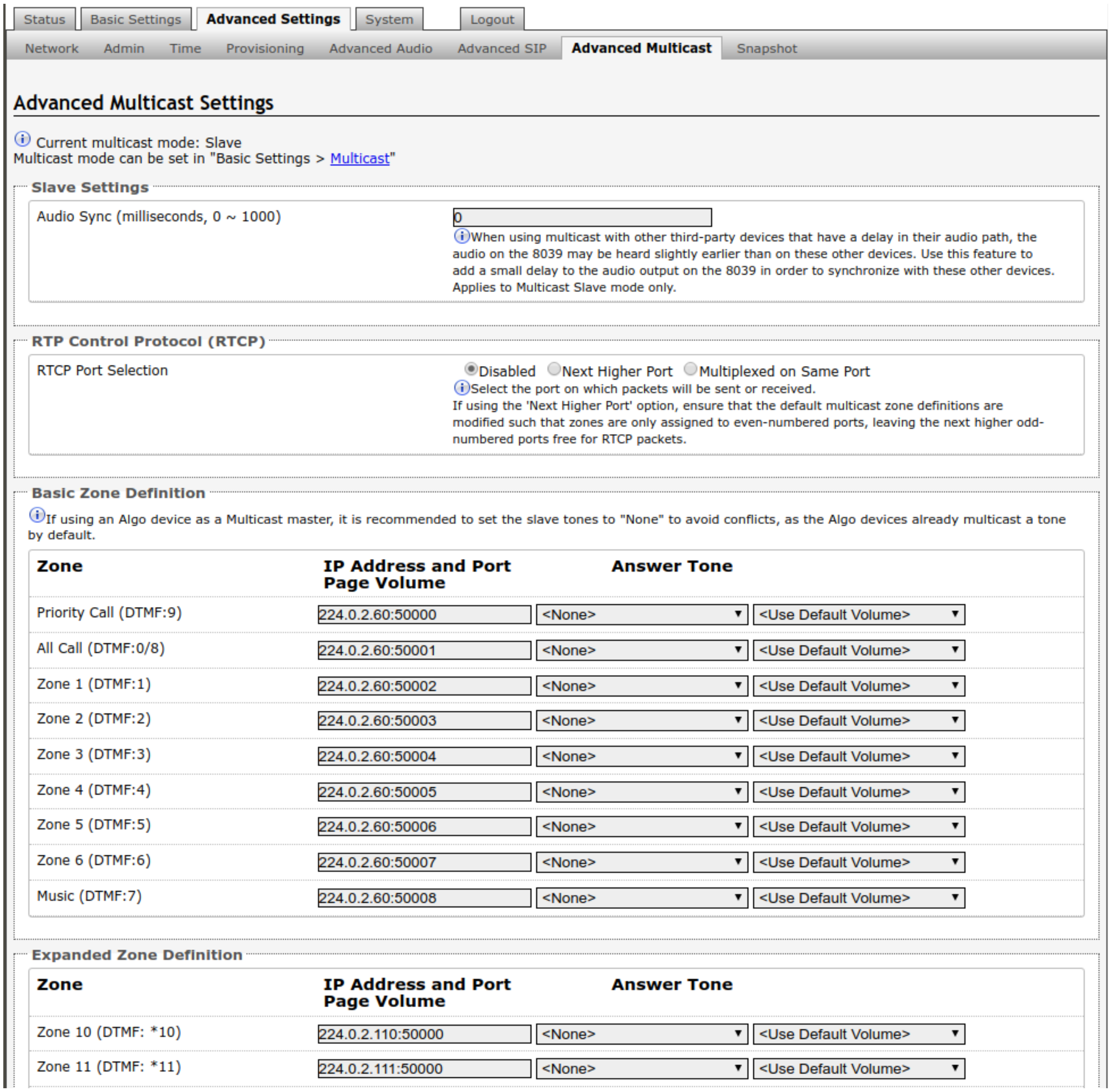
Use Outgoing TLS port in SIP headers

Use ephemeral port number from outgoing SIP TLS connection instead of listening port number in SIP Contact and Via headers. This is useful to connect the device to some local SIP servers, like Asterisk or FreeSWITCH.

Do Not Reuse Authorization Headers

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

Advanced Settings Tab – Advanced Multicast



Advanced Multicast Settings

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

Slave Settings

Audio Sync (milliseconds, 0 ~ 1000): 0

ⓘWhen using multicast with other third-party devices that have a delay in their audio path, the audio on the 8039 may be heard slightly earlier than on these other devices. Use this feature to add a small delay to the audio output on the 8039 in order to synchronize with these other devices. Applies to Multicast Slave mode only.

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

ⓘIf using an Algo device as a Multicast master, it is recommended to set the slave tones to "None" to avoid conflicts, as the Algo devices already multicast a tone by default.

Zone	IP Address and Port Page Volume	Answer Tone	
Priority Call (DTMF:9)	224.0.2.60:50000	<None>	<Use Default Volume>
All Call (DTMF:0/8)	224.0.2.60:50001	<None>	<Use Default Volume>
Zone 1 (DTMF:1)	224.0.2.60:50002	<None>	<Use Default Volume>
Zone 2 (DTMF:2)	224.0.2.60:50003	<None>	<Use Default Volume>
Zone 3 (DTMF:3)	224.0.2.60:50004	<None>	<Use Default Volume>
Zone 4 (DTMF:4)	224.0.2.60:50005	<None>	<Use Default Volume>
Zone 5 (DTMF:5)	224.0.2.60:50006	<None>	<Use Default Volume>
Zone 6 (DTMF:6)	224.0.2.60:50007	<None>	<Use Default Volume>
Music (DTMF:7)	224.0.2.60:50008	<None>	<Use Default Volume>

Expanded Zone Definition

Zone	IP Address and Port Page Volume	Answer Tone	
Zone 10 (DTMF: *10)	224.0.2.110:50000	<None>	<Use Default Volume>
Zone 11 (DTMF: *11)	224.0.2.111:50000	<None>	<Use Default Volume>

Note: The settings on this tab are only available when in multicast slave mode

RTCP Port Selection

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

Audio Sync

When paging to the 8039 SIP Video Intercom as well as other third party devices, the low latency of the 8039 may cause the audio to lead other devices. By adding audio delay up to one second, the 8039 may be synchronized with other endpoints or telephones that have greater latency.

Zone Definition

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

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

Page Tone and Page Volume

When an Algo device is the multicast Master, a page tone will play on the Slave device, so it is recommended to set the Slave tone to “None”. If a page is received from a non-Algo device that doesn’t send a tone, a tone can be inserted on the Slave device allowing for a page tone to be played prior to page audio starting.

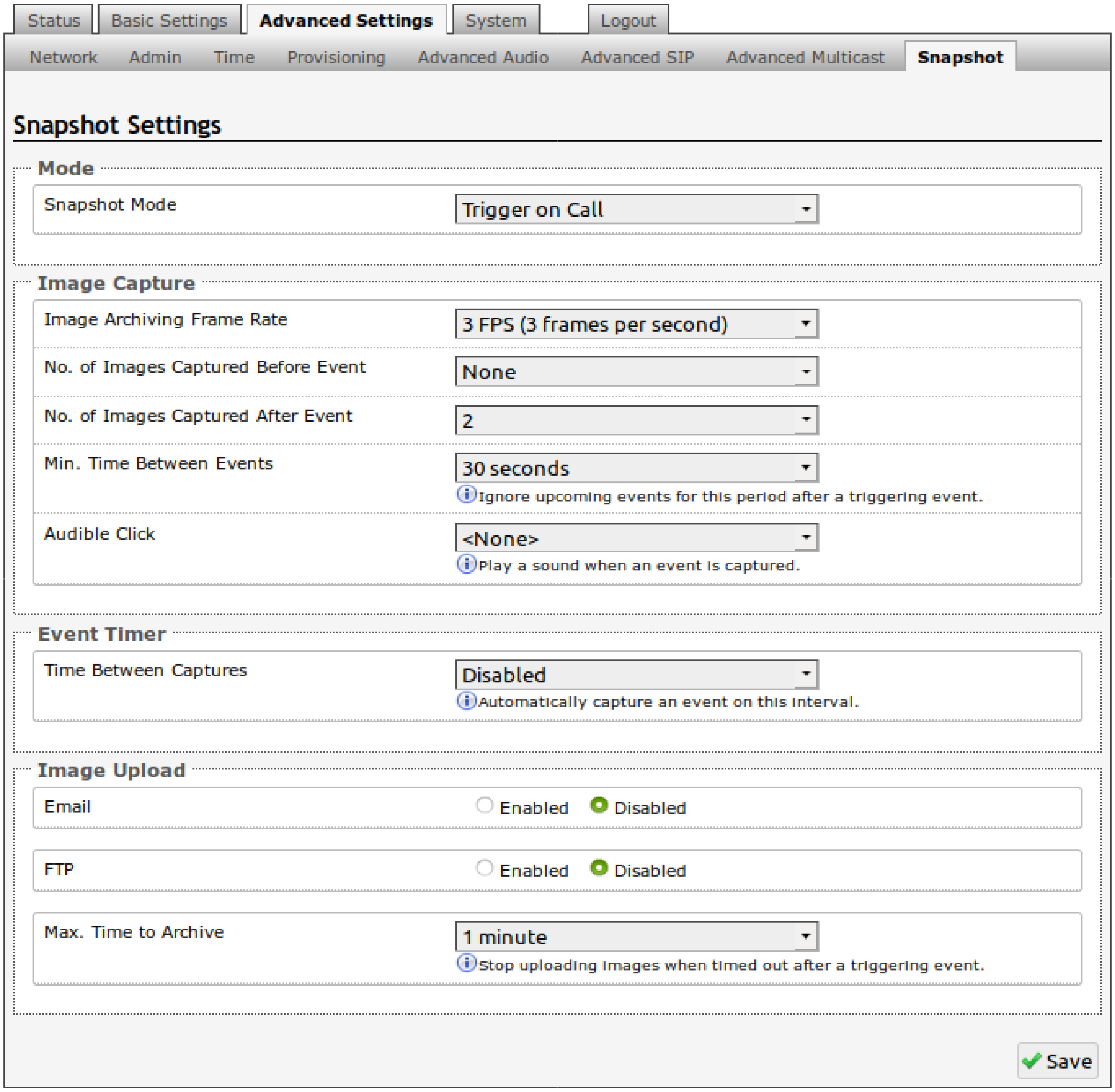
By default, the same page volume can be set for all Slave zones in the Basic Settings > Features tab. Unique page volumes may be revised on a per-zone basis in the table above. For instance, emergency pages can be louder on certain Slave endpoints.

Polycom Slave Tones

A tone may be set for any of the 25 Polycom Groups. If using an Algo device as a Multicast master, it is recommended to set the slave tones to “None” to avoid conflicts, as the Algo devices already multicast a tone by default.

These settings are available only if the 8039 is set as a Multicast Slave and “Polycom Group Page” or “Polycom Push-to-Talk” are selected in the Basic Settings > Multicast tab.

Advanced Settings Tab – Snapshot



Snapshot Settings

Mode

Snapshot Mode: Trigger on Call

Image Capture

Image Archiving Frame Rate: 3 FPS (3 frames per second)

No. of Images Captured Before Event: None

No. of Images Captured After Event: 2

Min. Time Between Events: 30 seconds
Ignore upcoming events for this period after a triggering event.

Audible Click: <None>
Play a sound when an event is captured.

Event Timer

Time Between Captures: Disabled
Automatically capture an event on this interval.

Image Upload

Email: ○ Enabled ● Disabled

FTP: ○ Enabled ● Disabled

Max. Time to Archive: 1 minute
Stop uploading images when timed out after a triggering event.

Snapshot Mode

Disable or enable the snapshot to be triggered when the call is made.

⚠ *Important: Enabling snapshot mode will disable low-power sleep mode.*

Image Archiving Frame Rate

Choose a frame rate from 1/5 FPS to 5 FPS.

No. of Images Captured Before Event

Number of images to be captured before the call is made.

No. of Images Captured After Event

Number of images to be captured after the call is made.

Min. Time Between Events

Ignore upcoming events for the chosen period after a triggering event.

Audible Click

Play a tone when image is captured.

Time Between Captures

Automatically capture an event on this interval.

Email

Set an email server for the images to be uploaded.

FTP

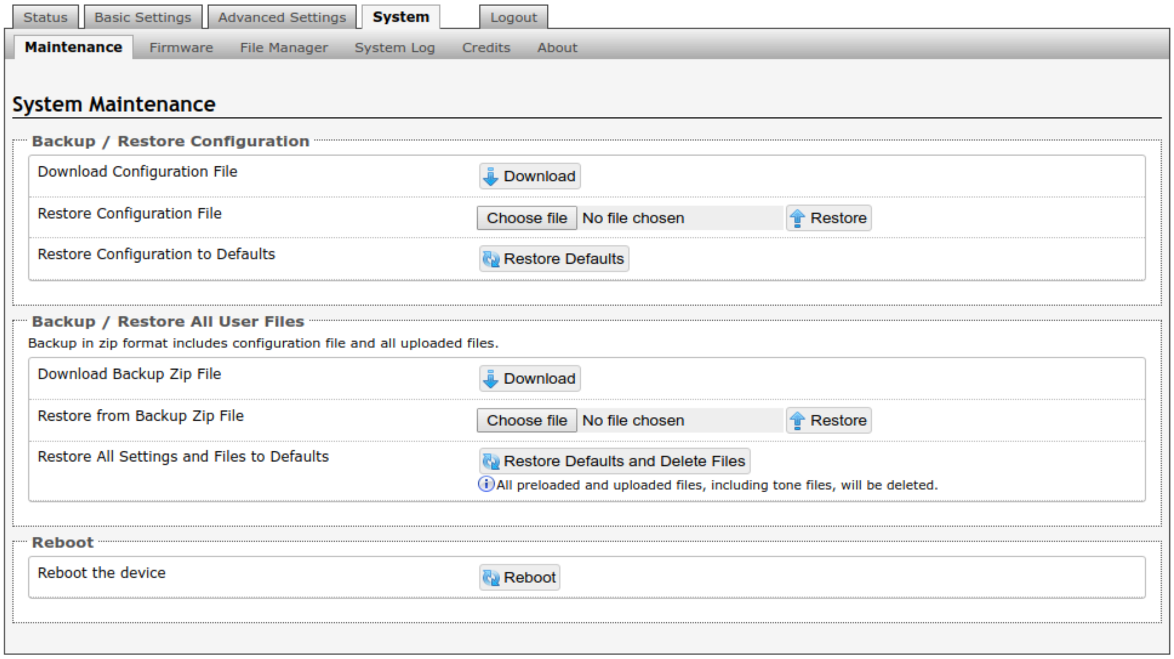
Set an FTP server for the images to be uploaded.

Max. Time to Archive

Stop uploading images when timed out after a triggering event.

Web Interface System

System Tab - Maintenance



System Maintenance

Backup / Restore Configuration

Download Configuration File	Download
Restore Configuration File	Choose file No file chosen Restore
Restore Configuration to Defaults	Restore Defaults

Backup / Restore All User Files

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

Download Backup Zip File	Download
Restore from Backup Zip File	Choose file No file chosen Restore
Restore All Settings and Files to Defaults	Restore Defaults and Delete Files ⓘ All preloaded and uploaded files, including tone files, will be deleted.

Reboot

Reboot the device	Reboot

Download Configuration File

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

Restore Configuration File

Restore settings from a backup file.

Restore Configuration to Defaults

Resets all 8039 SIP Video Intercom device settings to factory default values.

Download Backup File

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

Restore from Backup Zip File

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

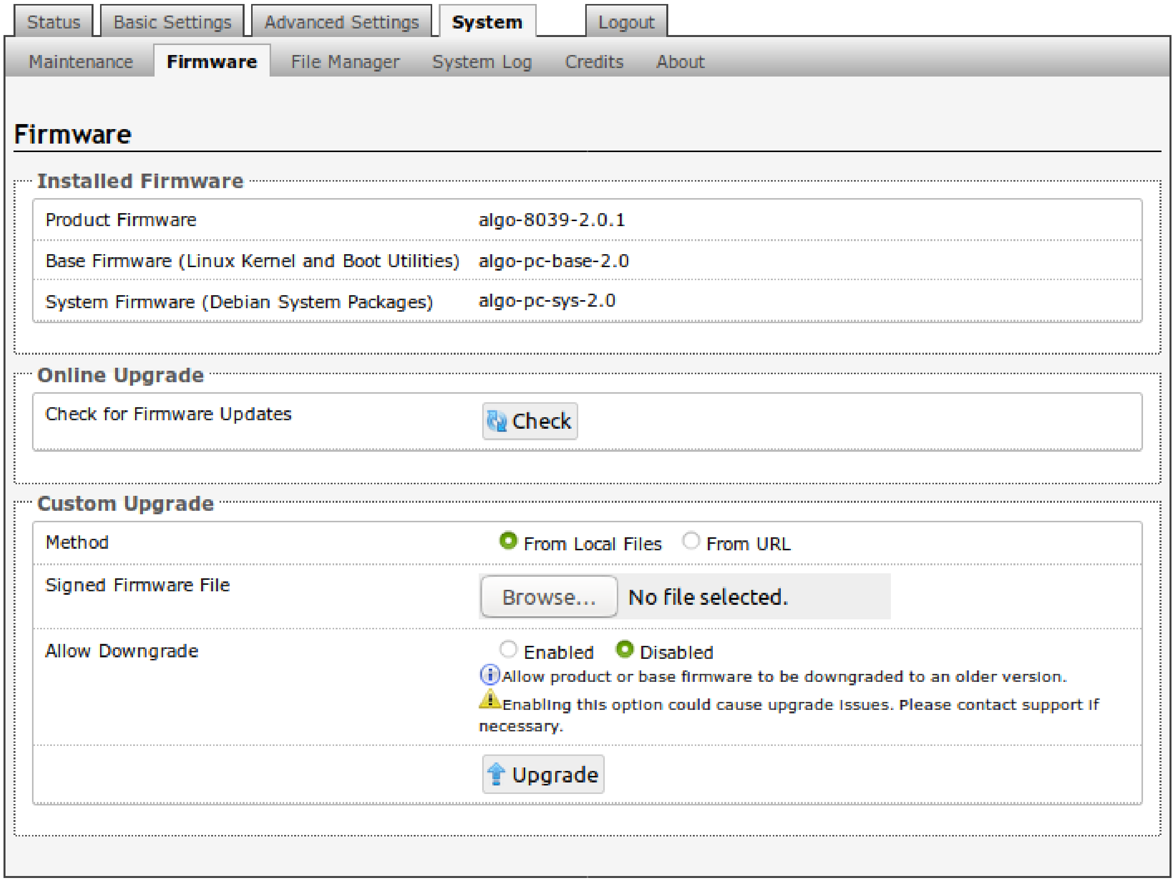
Restore All Settings and Files to Defaults

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

Reboot the Device

Reboots the device.

System Tab - Firmware



Firmware

Installed Firmware

Product Firmware	algo-8039-2.0.1
Base Firmware (Linux Kernel and Boot Utilities)	algo-pc-base-2.0
System Firmware (Debian System Packages)	algo-pc-sys-2.0

Online Upgrade

Check for Firmware Updates	Check

Custom Upgrade

Method	● From Local Files ○ From URL
Signed Firmware File	Browse... No file selected.
Allow Downgrade	○ Enabled ● Disabled Allow product or base firmware to be downgraded to an older version. Enabling this option could cause upgrade issues. Please contact support if necessary.
	Upgrade

Method

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

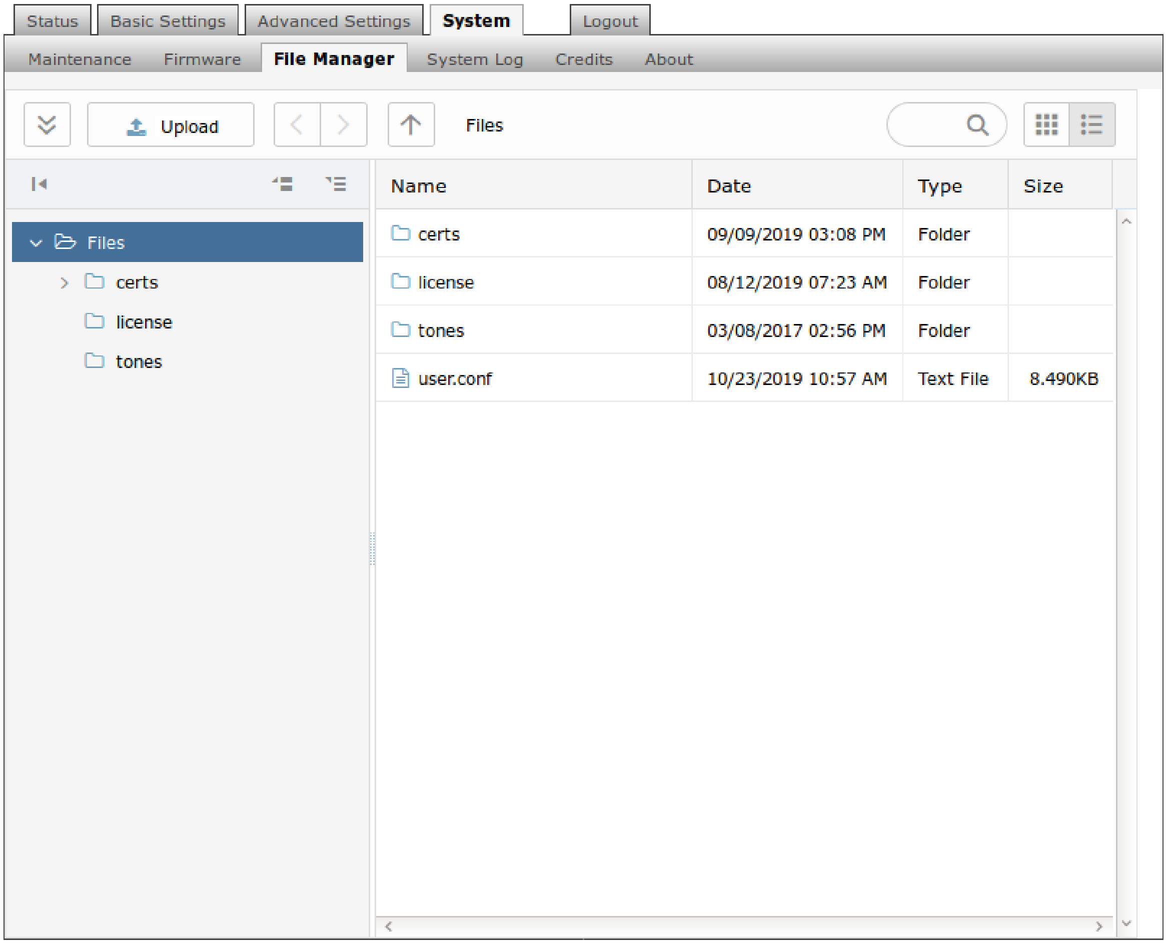
Signed Firmware File

Point to the SFW file provided by Algo

How to upgrade 8039 SIP Video Intercom Firmware

1. From the top menu, click on System, then Maintenance.
2. In the Upgrade section, click on Choose File and select the 8039 SIP Video Intercom firmware file to upload. Note that a SFW file must be loaded.
3. Click Upgrade
4. After the upgrade is complete, confirm that the firmware version has changed (refer to top right of Control Panel).

System Tab - File Manager



Name	Date	Type	Size
certs	09/09/2019 03:08 PM	Folder	
license	08/12/2019 07:23 AM	Folder	
tones	03/08/2017 02:56 PM	Folder	
user.conf	10/23/2019 10:57 AM	Text File	8.490KB

Uploading custom Ring Tones (WAV Files)

Custom WAV files may be uploaded into memory (1 GB) to play on the 8039 speaker.

An existing file may also be modified by downloading the original via the links in the web interface, making the desired changes, and then uploading the new version with a different name. Audio files must be in the following format:

- WAV format
- 8kHz or 16kHz sampling rate
- 16-bit PCM, or u-law
- Mono
- Smaller than 200MB

A zip files containing one or more audio files may also be uploaded. File names must be limited to 32 characters, with no spaces.

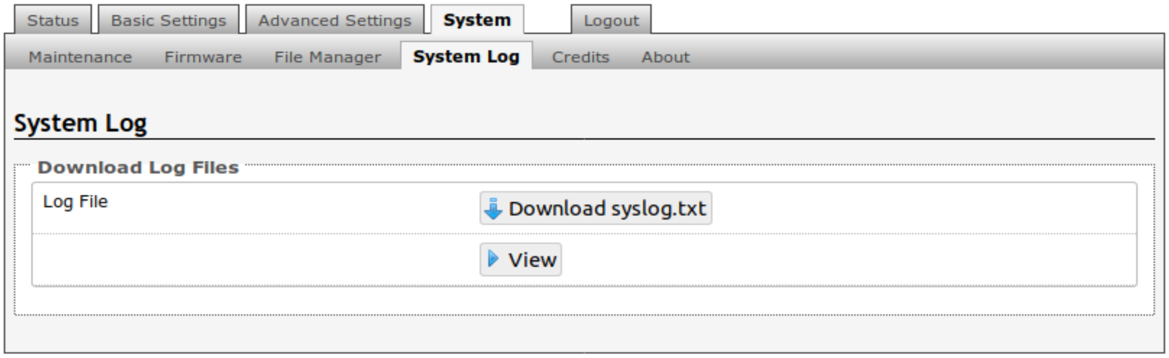
Uploading Certificate Files

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

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

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

System Tab – System Log



System log files are automatically created and assist with troubleshooting in the event the 8039 SIP Video Intercom does not behave as expected.

Specifications

Power Input: 48 V PoE IEEE 802.3af Class 0.

- Max 10 W when speaker active.
- 6 W when video in-use.
- 4 W idle when video not being viewed and backlight disabled.

Protocol: SIP (initiate or answer call).

Multicast: Receive.

Audio Codecs: G.711 A-law, G.711 u-law, G.722.

Video Codecs: H.264 Main or high profile.

Video Resolution: 720p, VGA, CIF up to 30fps.

Image Sensor: 187 Degree FOV horizontal and vertical. Fisheye image de-warped.

Server Redundancy: Primary, secondary, tertiary.

Processor: Linux OS; ARM Cortex-A8 Core with HD video processor and floating point DSP.

Enclosure: Metal.

Keypad Functions: Press any key to call; access control; dial number directly; directory annunciation.

Microphone: Single Wideband.

Memory: 1 GByte audio storage.

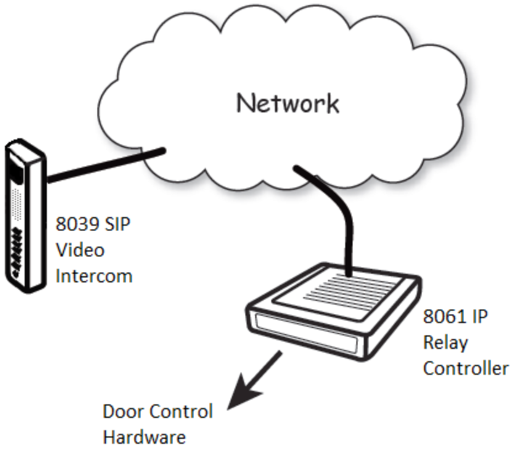
Door Control: Optional Algo 8061 IP Relay Controller or internal relay NO or NC rated 30V 1A.

Configuration: Web interface (HTTP or HTTPS) or auto provisioning server.

Provisioning: TFTP, FTP, HTTP, HTTPS

Supervision:	SNMP
NAT:	STUN, CRLF Keep Alive.
Environmental:	-40 to +122 deg F (-40 to +50 deg C); Rated for outdoor environments. Type 3R (IPX3)
Dimension:	1.95" W x 10.4" T x 1.64" D (4.95 cm x 26.3 cm x 4.17 cm).
Mounting:	Includes concealed mounting bracket and secure screw with matching security tool.
Weight:	2.65 lb (1.2 Kg).
Compliance:	EN60950:2001, IEEE 802.3-2008, RFC3261, RoHS, CE, FCC Class A, CISPR 22 Class A, CISPR 24, CSA/UL (USA & Canada).

8061 IP Relay Controller

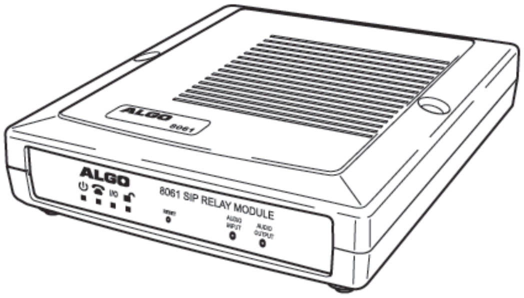


The 8039 can provide secure door control functionality when used with the optional Algo 8061 IP Relay Controller.

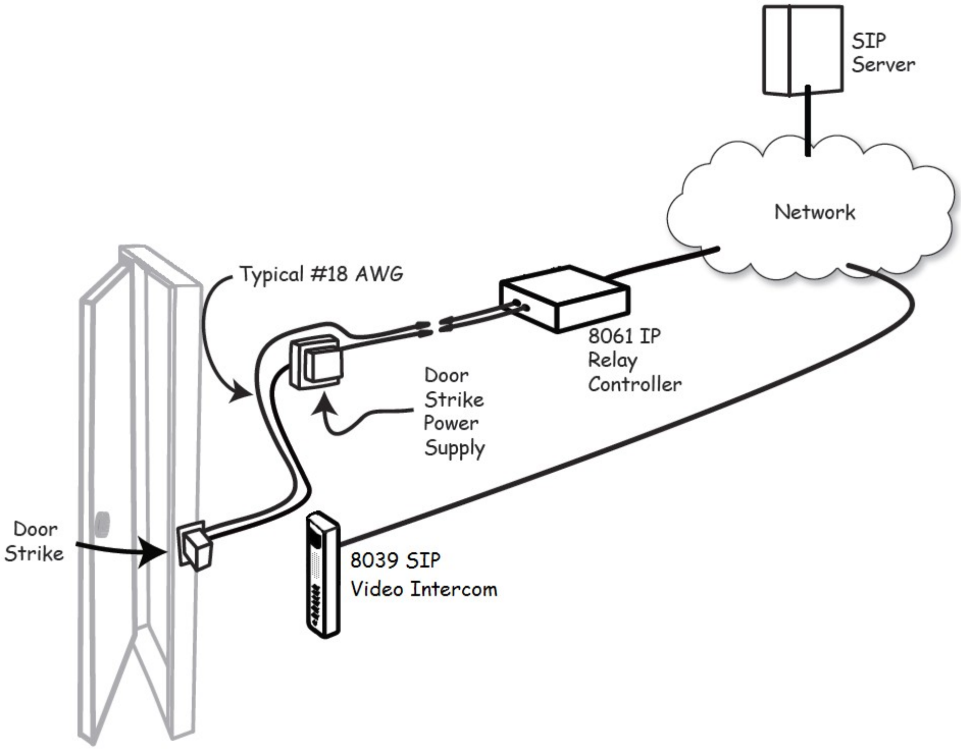
The 8061 serves as a bridge between the 8039 and peripheral hardware such as door strike.

As a door opening controller, the 8061 can be located in a secure environment to prevent tampering of the public-facing intercom, as compared to using the local Door control relay on the 8039 which would require the door strike wires to be run outside the building.

The door control feature is activated by a command from the answering telephone keypad, or entry of the door release code by a visitor via the 8039 itself.

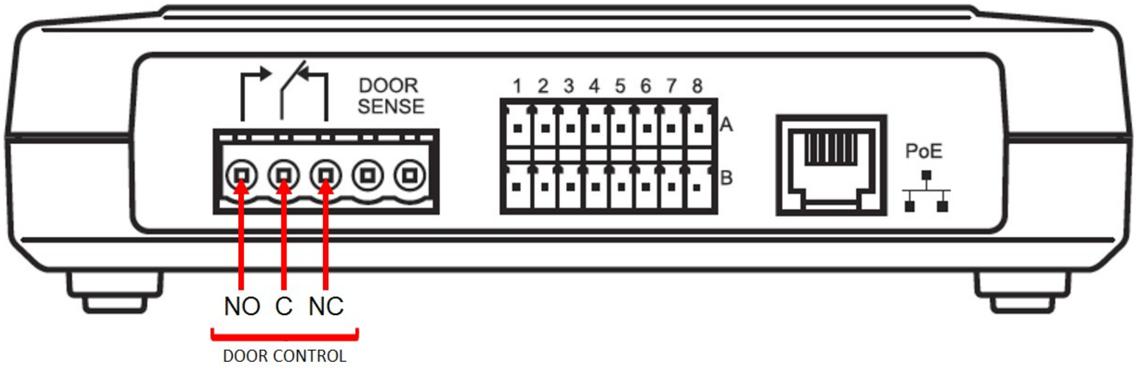


Typical 8039/8061 Setup



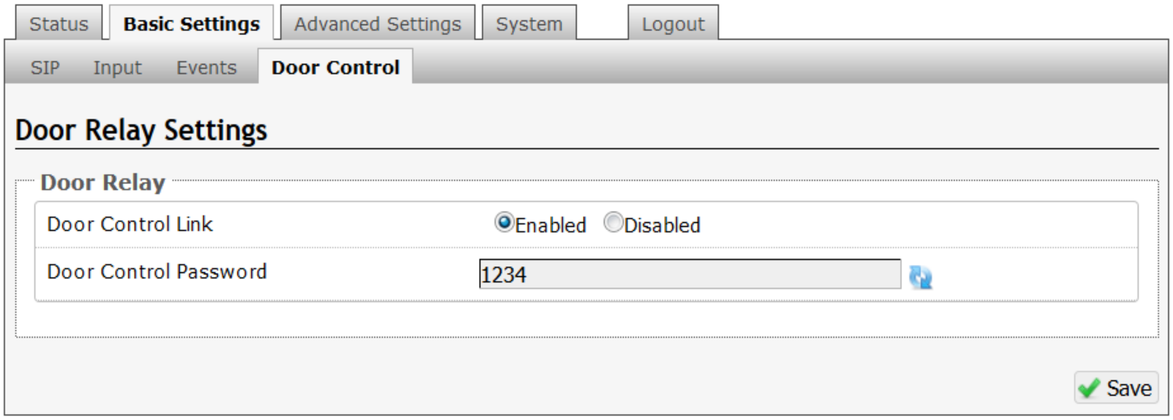
PoE and Relay Connections on back of 8061 IP Relay Controller:

1. Connect the 8061 to the network via an Ethernet cable at the back of the device. Ensure that a PoE port is used for power and that the 8061 is connected to the same subnet and VLAN as the target intercom.
2. Run two wires from the door strike to the Normally Open/Common (NO/C) input pair or Common/Normally Closer (C/NC) input pair on the 8061. For more wiring information please visit: www.algosolutions.com/doorstrike.



Configuring the 8061

1. Find the IP address of the Algo 8061 using the Algo locator tool available from the Algo website www.algosolutions.com/locator). This tool displays all of the Algo devices available on the network, and their corresponding IP addresses. Note this address down as you will need it when you configure the 8039 for use with this device.
2. Point your browser to the above IP address. The 8061 Control Panel will be displayed.
3. Log in. The default password is **algo**.
4. Go to the **Basic Settings** > **Door Control** tab.



Door Relay Settings

Door Relay

Door Control Link ● Enabled ○ Disabled

Door Control Password 1234

5. Set the “Door Control Link” to “Enabled”.
6. In the “Door Control Password” field set a password that will be used for configuring the intercom for door control. Note this password down as you will be reusing it when configuring the 8039 with this device.

See section “Basic Settings Tab – Door Control” page 20 for configuring the 8201 with the parameters from above.

FCC Compliance Statement

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