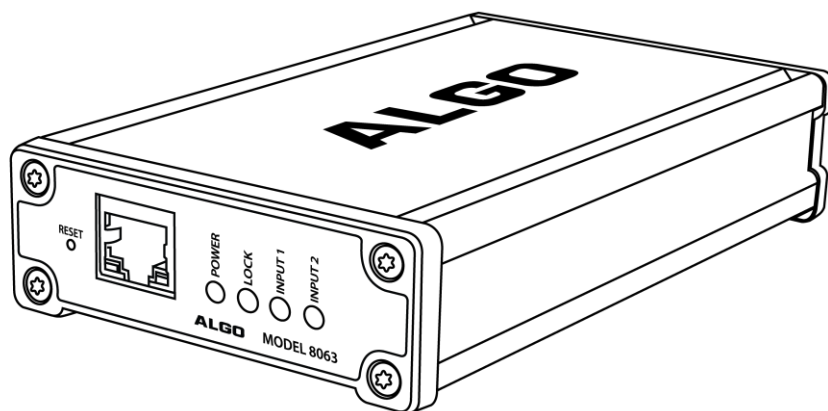


8063

IP Door Controller User Guide



Powered by **ALGO**

Table of Contents

Important Safety Information	3
Overview	5
Introduction.....	5
Setup and Installation	6
Getting Started - Quick Install & Test	6
Installation	7
Programming and Configuration	7
Wiring Connections	8
Reset	9
TLS for SIP Signalling and Provisioning	10
Web Interface Status and Login	13
Web Interface login	13
Status	14
Web Interface Basic Settings	15
Basic Settings Tab – Door Control & I/O.....	15
Basic Settings Tab – Stand-Alone Mode	16
Web Interface Advanced Settings	19
Advanced Settings Tab - Network	19
Advanced Settings Tab – Admin.....	21
Advanced Settings Tab – Time	23
Advanced Settings Tab – Provisioning.....	24
Advanced Settings Tab – Advanced Audio	26
Advanced Settings Tab – Advanced SIP.....	27
Web Interface System.....	30
System Tab – Maintenance	30
System Tab – Firmware.....	31
System Tab – File Manager	32
System Tab – System Log	33
Specifications	34
FCC Compliance Statement	35

Important Safety Information

Important Safety Information

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

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

Consignes de Sécurité Importantes

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

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

Información de Seguridad Importante

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

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

Wichtige Sicherheitsinformationen

Dieses Produkt wird durch eine zertifizierte Stromquelle mit begrenzter Leistung (LPS – Limited Power Source) betrieben. Die Stromversorgung erfolgt über Ethernet (PoE – Power over Ethernet). Dies geschieht durch eine Cat-5-Verbindung oder eine Cat-6-Verbindung zu einer IEEE 802.3at PoE+ or 802.3af-konformen Ethernet-

Netzwerkweiche. Das Produkt wurde konzipiert für die Installation innerhalb eines Gebäudes. Alle Kabelverbindungen zum Produkt müssen im selben Gebäude bestehen. Wenn das Produkt jenseits des Gebäudes oder für mehrere Gebäude genutzt wird, müssen die Kabelverbindungen vor Überspannung und Spannungssprüngen geschützt werden. Algo empfiehlt das Produkt von einem qualifizierten Elektriker installieren zu lassen.

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 802.3at PoE+ or 802.3af 兼容的 PoE 网络交换机供电。本产品适用于室内或建筑物周边安装。所有联接本产品的线路必须源自同一建筑物。本产品如需用于超出建筑物周边范围或跨建筑物的安装，线路联接部分必须有过压和瞬态保护。Algo 建议本产品由专业电工安装。

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

EMERGENCY COMMUNICATION

If used in an emergency communication application, the 8063 should be routinely tested. SNMP supervision is recommended for assurance of proper operation.

DRY INDOOR LOCATION ONLY

The 8063 IP Door Controller is intended for dry indoor locations only.

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 8063 IP Door Controller may leave the building perimeter without adequate lightning protection.

Overview

Introduction

The 8063 IP Door Controller provides a dry contact relay closure for the activation of electronic door strikes. It is typically used in conjunction with an Algo Intercom, including the 8201, 8036 & 8039, allowing the door wiring to be kept securely inside the building to prevent unauthorized tampering. In this case, the 8063 does not require a SIP registration, and communicates only with the Algo Intercom via a secure communication path over the LAN.

In applications where voice communication is not required, the 8063 can also be used in standalone mode, and activated directly via a SIP call.

The 8063 also has two relay inputs, and one relay output, allowing it to interface with external sensors and switches, including magnetic door sensors for tracking the state of the door to prevent tailgating, or trigger an alarm if the door is held open.

What is Included

- 8063 IP Door Controller
- Network Cable
- Wall Mount Bracket

What is not Included

- This Installation Guide (www.algosolutions.com/8063/guide)
- Door Strike
- Door Strike Power Supply
- Intercom (compatible with Algo 8201, 8036 & 8039)

Setup and Installation

Getting Started - Quick Install & Test



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

1. Connect the wiring from your door strike (not included), to the Door Control relay output terminal block on the 8063 (either “Normally Open” [‘NO’] and “Common” [‘C’], or “Normally Closed” [‘NC’] and “Common” [‘C’], as appropriate for the door strike). See the [Door Strike Wiring Guide](#) for further information.
2. Connect the 8063 IP Door Controller to a PoE or PoE+ network switch. The blue lights on the front will remain on until boot up is completed – about 30 seconds.
3. After the blue lights turn off, the IP address may be discovered by downloading the Algo locator tool to find Algo devices on your network:
www.algosolutions.com/locator
4. Access the 8063 IP Door Controller web page by entering the IP address into a browser (Chrome, Firefox etc) and login using the default password **algo**.
5. Use the test buttons in the web interface (**Basic Settings > Door Control & I/O**) to confirm the operation of the door strike. Press the Unlock button to test that the door unlocks, and then press Lock again to confirm that it locks.

After confirming that the hardware installation with the door strike is successful, the 8063 can now be configured for use with either an Algo Intercom (typical application), or in Stand-Alone Mode (without an Algo Intercom and thus no voice path). Please choose the appropriate section below based on your application.

For Use with an Algo Intercom (Typical Application)

6. Open the web interface for the Algo Intercom (8201, 8036 or 8039) that is to communicate with the 8063, using the IP address for this device.

In the web interface for the Intercom, select the **Network Door Controller** options and enter the IP address of the 8063 here (and password), so that the Intercom can contact the 8063 in order to unlock the door. These settings are in **Basic Settings > Door Control** in the Intercom web interface – see the documentation of your specific Algo Intercom model (8201, 8036 or 8039) for further details.

7. Make a call to the Algo Intercom, and press ‘6’ (or appropriate DTMF code as configured on the Intercom) to unlock the door using the 8063 IP Door Controller.

For Stand-Alone Mode

8. In the 8063 web interface, enter the IP address or the name for the SIP server into the SIP Domain field under the **Basic Settings > Stand-Alone Mode** tab.
9. Enter the credentials (SIP Extension, Authentication ID, and Password) for the SIP extension.

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.

10. Make a call to the controller by dialling the SIP extension of the adapter from a telephone.

Installation

The 8063 is wall mountable in a horizontal orientation using the supplied bracket.



Example installation on ½" drywall:

Use appropriate drywall anchors for #8 screws, and pre-drill per anchor manufacturer's instructions. Insert 4 anchors into the wall, and then attach bracket to wall anchors using #8 screws. Snap the 8063 into the bracket.

Connect the 8063 to a PoE network switch.

Programming and Configuration

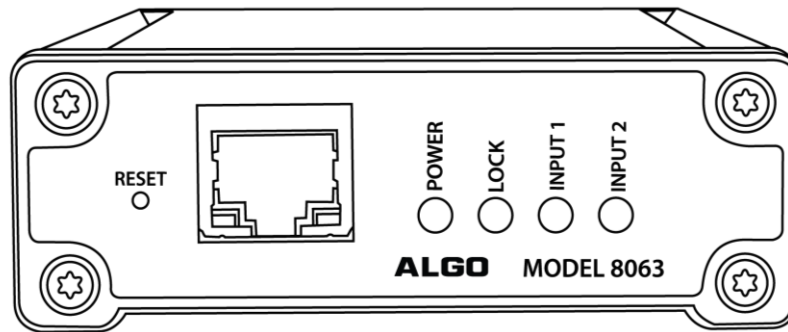
The 8063 IP Door Controller is configurable using the web interface or provisioning features.

After boot up the blue lights on the front will turn off (except for the power light) and the adapter will have obtained an IP address. If there is no DHCP server the 8063 IP Door Controller will default to the static IP address **192.168.1.111**.

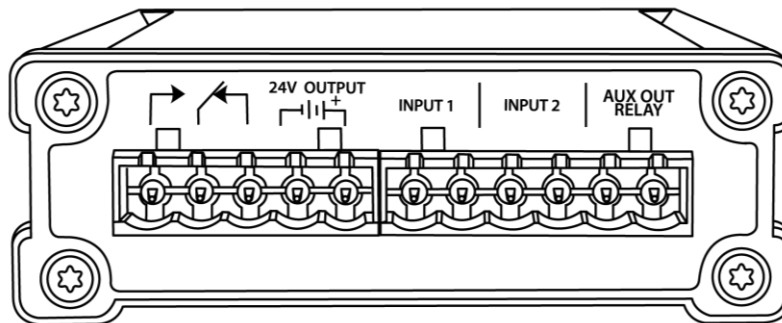
The IP address may be discovered by downloading the Algo locator tool to find Algo devices on your network: www.algosolutions.com/locator

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

Wiring Connections



8063: Front View



8063: Back View

Network Connection (Front)

The 8063 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 can be used for most applications, whether provided by the network switch or injector. If using the 24V output to drive a high power door strike directly (as opposed to just using the relay in conjunction with the door strike's existing power supply), then PoE+ may be used to allow more power. See the Specifications section for details on the current limits in each case.

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.

Reset

A recessed reset button (RST) next to the Ethernet Jack can only be used to reset the 8063 at time of power up. To return all settings to a factory default, wait until the SIP LED flashes and then press and hold the reset button until the POWER LED begins a double flash pattern. Release the reset button and allow the unit to complete its boot process.

Do not press the reset button until the POWER LED begins flashing.

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

TLS for SIP Signalling and Provisioning

Algo devices that support firmware 1.6.4 or later support Transport Layer Security (TLS). This feature adds security by ensuring that Algo products can trust the hosted SIP server. This is useful for when third-party devices or attackers may try to intercept, replicate, or alter Algo products, and try to connect to the server. TLS protocol will ensure that third parties cannot read/modify any actual data. Previously security was less of a concern because phone systems were on isolated networks, but hosted services are becoming increasingly more common. Using a hosted SIP service requires traffic to be sent over the public internet and thus much more susceptible to attacks. Signed certificates are an important piece in the Algo device's operation, to ensure the security, integrity, and privacy of its communication. Algo components that use TLS are **Provisioning** and **SIP Signaling**.

These Algo devices each come pre-loaded with certificates from a list of trusted certificate authorities (CA), which are installed in the hardware at the time of manufacture. Note these pre-installed trusted certificates are not visible to users and are separate from the 'certs' folder.

The TLS handshake happens to make sure that the client and server can trust each other, and once that trust is established, the two parties can freely send encrypted data and decrypt any data that they receive. After the TLS handshake process is complete, a TLS session is established, and the server and client can then exchange messages that are symmetrically encrypted with shared (pre-master) secret key.

For further details reference the [Algo TLS guide for SIP Signalling and HTTPS Provisionings](#).

Uploading Public CA Certificates to Algo SIP Endpoints

To install the public CA certificate on the Algo 8063, follow the steps below:

1. Obtain a public certificate from you Certificate Authority.
2. Rename the public certificate 'siptrusted' with any of supported formats (.pem, .cert, or .cer).
3. In the web interface of the 8063, navigate to the **System > File Manager** tab.
4. Upload the certificate files into the 'certs' directory. Click the Upload button in the top left corner of the file manager and browser to the certificate.

HTTPS Provisioning

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

[Status](#)
[Basic Settings](#)
[Additional Features](#)
[Scheduler](#)
[Advanced Settings](#)
[System](#)
[Logout](#)

[Network](#)
[Admin](#)
[Users](#)
[Time](#)
[Provisioning](#)
[Advanced Audio](#)
[Advanced SIP](#)
[Advanced Multicast](#)

Provisioning Settings

Mode

Provisioning Mode ☒ Enabled ☐ Disabled

Settings

Server Method

☐ Auto (DHCP Option 66/160/150)
☐ DHCP Option 66 only
☐ DHCP Option 160 only
☐ DHCP Option 150 only
☒ Static

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

Static Server

Download Method ☐ TFTP ☐ FTP ☐ HTTP ☒ HTTPS

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.

Force Secure TLS Version ☐ Enabled ☒ Disabled

Enable this option to require HTTPS connections to use TLSv1.2.

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.

☒ Save



Important: To verify the server you must 'Enable' the 'Validate Server Certificate' option. This then checks if the certificate that is provided by the server is signed by any of the CAs included in the list of trusted CAs (used by the Debian infrastructure and Mozilla browsers). If we receive a certificate signed by any of these CAs, then that server will be trusted. Certificates can also be manually uploaded using the 'File Manager'.

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

prov.download.cert = 1

SIP Signalling (and RTP Audio)

SIP signaling is secured by setting 'SIP Transportation' to 'TLS' (under the **Advanced Settings > Advanced SIP** tab). Setting it to 'TLS' ensures that the SIP traffic will be encrypted. The SIP signalling is responsible for establishing the call (the control signal to start and end the call with the other party), but it does not contain the audio.

Status	Basic Settings	Additional Features	Scheduler	Advanced Settings	System	Logout
Network	Admin	Users	Time	Provisioning	Advanced SIP	Advanced Multicast

Advanced SIP Settings

General

SIP Transportation	TLS <i>i</i> Select Auto to check DNS NAPTR record, then try UDP/TCP. <i>i</i> In TLS mode, if the SIP Server requires endpoints to be authenticated, a PEM file containing both a device certificate and a private key needs to be installed on the Algo device. Use the "System > File Manager" tab to upload a certificate file renamed to 'sipclient.pem' in the 'certs' folder.
SIPS Scheme	☐ Enabled ☒ Disabled
Validate Server Certificate	☐ Enabled ☒ Disabled <i>i</i> Validate the SIP server against common certificate authorities. To validate against additional certificates, use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder.
Force Secure TLS Version	☐ Enabled ☒ Disabled <i>i</i> Enable this option to require TLS connections to use TLSv1.2.
SIP Outbound Support (RFC 5626)	☐ Enabled ☒ Disabled <i>i</i> 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

Interoperability

Keep-Alive Method	☒ None ☐ Double CRLF <i>i</i> This setting will enable sending periodic CRLF messages for both UDP and TCP connections.
Use Outgoing TLS port in SIP headers	☒ Enabled ☐ Disabled <i>i</i> 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 <i>i</i> 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 <i>i</i> When enabled, allow SIP NOTIFY messages that do not contain a "Subscription-State" header.

 Save



*Important: In order for a SIP server to validate the Algo device, an additional certificate may be installed on the Algo device manually. To add the user certificate file use a '.pem', '.crt', or '.cer' filetype extension and have the file named 'sipclient'. This is done by manually adding a file named 'sipclient', which contains a device certificate and private key, to the 'certs' folder (under the **System > File Manager** tab).*

Web Interface Status and Login

Web Interface login

Status
Basic Settings
Advanced Settings
System
Logout

Device Status

Welcome to the Algo 8063 Door Controller Control Panel

Setting up your Door Controller:

Step 1: Configure your Door Controller
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 Door Controller (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 Door Controller (Optional)
Please register your product using the link below:
<http://www.algosolutions.com/register>
Registration ensures your access to the latest upgrades to this product and important service notices.

Status

Device Name	doorcontroller-00a056	
SIP Registration	Page	No Account
Call Status	Idle	
Proxy Status	Single proxy mode	
Security	TLS	Disabled
	SRTP	Disabled
Provisioning Status	None Found	
MAC	00:22:ee:00:a0:56	
IPv4	10.30.30.230/8, Gateway: 10.0.1.1	
IPv6	Invalid	
Date / Time	Wed Jul 8 04:24:49 GMT 2020	
Door Sensor	Disabled	
Door Relay	Door Locked	
PoE Detection	PoE 802.3af (Max 12.95W) Warning: Some functionality will be reduced due to the present power connection.	

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

	Web Interface is accessed by entering the 8063's IP Address into a web browser.
	Important: It is highly recommended to change the default password if the device is directly connected to a public network.

Status

The device's Status page will be available before and after log on. The section can be used to check 8063's SIP Registration, Call Status, Relay Status (Door Sensor and Door Relay), Proxy Status, and general MAC, IP, Netmask, Date/Time, and Timezone information.



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

Web Interface Basic Settings

Basic Settings Tab – Door Control & I/O

The screenshot shows the 'Basic Settings' tab for 'Door Control & I/O'. The interface is divided into several sections:

- Door Control Link:** Radio buttons for 'Enabled' and 'Disabled' (selected).
- Input #1:** Radio buttons for 'Disabled' (selected) and 'Door Sensor'.
- Input #2:** Radio buttons for 'Disabled' (selected), 'Manual Door Release', and 'Door Control Lockout'.
- Aux Out Relay:** A dropdown menu set to 'Disabled'.
- Auxiliary 24V Output:**
 - 24V Output:** Radio buttons for 'Disabled' (selected), 'Always On', and 'Follow Door Control'.
 - Display Auxiliary Power State on Status Page:** Radio buttons for 'Enabled' and 'Disabled' (selected).
 - Current Limit:** Radio buttons for 'Low (200mA)' (selected) and 'High (500mA)'. A note below states: 'PoE+ power is required to use the high current limit.'
- Test Controls:**
 - Test Door Control Relay:** 'Unlock' and 'Lock' buttons.
 - Test 24V Output:** 'Enable' and 'Disable' buttons.

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

Door Control Link

To use the 8063 as a Network Door Controller, you may enable this function and set the password to securely connect from the Algo Doorphone.

Input #1

Select the Door Sensor (not included) to use the '**Door Open Alarm**' or '**Cancel if Door Opened**' function. The Door Sensor can be set to be normally open or normally closed.

Input #2

Another input can be set to Manual Door Release or Door Control Lockout

Aux Out Relay

Aux Out Relay can be set to one of the followings:

- Follow Door Control
- Follow Input #1
- Follow Input #2
- Door Alarm

24V Output

Set the Auxiliary 24V output to be disabled, always on, or to follow door control. If set to follow door control, then this terminal can be wired directly to the door strike (if compatible), without needing to be also wired through the relay.

Display Auxiliary Power State on Status Page

If enabled, status of Auxiliary Power State will be shown on the status page.

Current Limit

Set current limit to low or high. PoE+ power is required to use the high current limit.

Basic Settings Tab – Stand-Alone Mode

These settings are not needed if the 8063 is used with an Algo Intercom. Only use this section if operating the 8063 directly from a SIP call without voice communication.

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.

Status
Basic Settings
Advanced Settings
System
Logout

Door Control & I/O

Stand-Alone Mode

Stand-Alone Mode

These settings are not needed if the 8063 is used with an Algo doorphone. Use these settings only in stand-alone operation to unlock a door directly without an intercom. Select "Disabled" if using this product in conjunction with an Algo doorphone (eg. 8201, 8039, 8036).

Stand-Alone Settings

Unlock Door with Inbound Call (Stand-alone Mode)

☐ Disabled
☒ Unlock after DTMF Input
☐ Unlock Immediately Upon Ring (Do not answer call)
☐ Unlock Immediately and Answer Call

SIP

Inbound SIP calls are only for direct door control, not audio. The 8063 does not have a speaker nor microphone.

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)

Door Unlock via Inbound Call

Answer Prompt

Door Unlock Tone

Momentary Open Code

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

The amount of time for which the door will be unlocked.

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

Cancel if Door Opened ☐ Enabled ☒ Disabled

This option is available only when a physical sensor is installed on the door and "Input #1" is set to "Door Sensor" in "Basic Settings > Door Control & I/O".

Door Open Alarm

The Door Open Alarm requires a door sensor to be configured on the relay input.

Save



Important: Any time changes are made to settings in the Web Interface the 'Save' key 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

This is the SIP extension for the 8063 IP Door Controller.

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.

Display Name

Enter a "Display Name" that will be sent when the SIP call is made. The PBX and phone(s) will have to be configured to display this message as the Caller ID.

Answer Prompt

The prompt tone upon answering of the inbound call to create awareness.

Door Unlock Tone

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

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.

DTMF Detection Type

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

Cancel if Door Opened

If enabled, cancels an inbound call if the door already has opened.

Max Door Open

Alarm will be triggered if the door remains open for longer than the selected duration.

Extension to Dial

Set an extension to be dialed when alarm is triggered.

Alarm Tone/Pre-recorded Announcement

Pre-loaded tones or custom loaded tones/recorded announcement can be used as an alarm tone.

Interval Between Tones (seconds)

Set interval between the alarm tones.

Maximum Alarm Duration

Set maximum alarm duration.

Web Interface Advanced Settings

Advanced Settings Tab - Network

The screenshot displays the 'Advanced Settings' tab for the 'Network' section of the 8063 IP Door Controller web interface. The top navigation bar includes 'Status', 'Basic Settings', 'Advanced Settings' (selected), 'System', and 'Logout'. Below this, a sub-navigation bar shows 'Network' (selected), 'Admin', 'Time', 'Provisioning', 'Advanced Audio', and 'Advanced SIP'.

The main content area is titled 'Network Settings' and contains several configuration sections:

- Common:** Includes a dropdown for 'Internet Protocol' set to 'IPv4 only' and a text field for 'DNS Servers'.
- IPv4:** Includes a radio button for 'IPv4 Method' set to 'Static' (with 'DHCP' as an option), a text field for 'IPv4 Address' with a hint 'Address (dot delimited)/Netmask (CIDR), e.g. 192.168.1.23/24', and a text field for 'IPv4 Gateway'.
- 802.1Q Virtual LAN:** Includes a radio button for 'VLAN Mode' set to 'Auto' (with 'None' and 'Manual' as options).
- 802.1X Port-based Network Access Control:** Includes a radio button for '802.1X Authentication' set to 'Enabled' (with 'Disabled' as an option), a text field for 'ID', and a text field for 'Password' with a toggle icon.
- Differentiated Services:** Includes three text fields for 'SIP (6-bit DSCP value)', 'RTP (6-bit DSCP value)', and 'RTCP (6-bit DSCP value)', each with a hint 'Valid values range from 0 to 63'.
- DNS:** Includes a radio button for 'DNS Caching Mode' set to 'Disabled' (with 'SIP' and 'All' as options). A note states: 'In "SIP" mode, only the results of DNS queries for SIP requests will be cached. In "All" mode, the results of all DNS queries will be cached.'

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

Internet Protocol

The 8063 can be set to have IPv4 only or both IPv4 and IPv6 method as its internet protocol.

IPv4/IPv6 Method

The 8063 can be set to a DHCP or a static IP address. When DHCP is selected, DHCP will automatically configure IP addresses for each 8063 IP Door Controller on the network.

IPv4/IPv6 Address

Enter the static IP address for the 8063.

IPv4/IPv6 Address

Enter the gateway 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 0xFFFF 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

StatusBasic SettingsAdvanced SettingsSystemLogout

NetworkAdminTimeProvisioningAdvanced AudioAdvanced SIP

Admin Settings

Admin Password

Password

Confirmation

General

Device Name (Hostname)

doorcontroller-\$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.

Log Settings

Log Level

☐ Error (Lowest) ☐ Notice ("Event") ☒ Info ("SIP") ☐ Debug (Highest)

Log Method

☒ Local ☐ Network ☐ Both

Management

Web Interface Protocol

☒ Both HTTP and HTTPS ☐ HTTPS Only

Force Strong Password

☐ Enabled ☒ Disabled

Allow Secure SIP Passwords

☐ Enabled ☒ Disabled

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

Simple Network Management Protocol

SNMP Support

☐ Enabled ☒ Disabled

Download MIB file [here](#).

API Support

RESTful API

☐ Enabled ☒ Disabled

Secure API for remote access & control via HTTP. Contact Algo Support for more information

System Integrity

System Integrity Checking

☐ Enabled ☒ Disabled

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

InformaCast

InformaCast Support

☐ Enabled ☒ Disabled

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

Save

Password

Password to log into the 8063 IP Door Controller 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

Allow 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 8063 Door Controller to write to external Syslog server if the option for external (or both) is selected.

Log Server

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

Web Interface Protocol

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

Force Strong Password

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

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

Allow Secure SIP Password

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

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

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

SNMP Support

Additional SNMP support is anticipated for future, but the 8063 IP Door Controller will respond to a simple status query for automated supervision. Contact Algo technical support for more information.

RESTful API

Secure API for remote access & control via HTTP.

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

The screenshot displays the 'Advanced Settings' tab with the 'Time' sub-tab selected. The 'Time Settings' section is expanded, showing the following configuration options:

- Timezone:** A dropdown menu set to 'GMT'.
- NTP Time Server 1:** Text input field containing '0.debian.pool.ntp.org'.
- NTP Time Server 2:** Text input field containing '1.debian.pool.ntp.org'.
- NTP Time Server 3:** Text input field containing '2.debian.pool.ntp.org'.
- NTP Time Server 4:** Text input field containing '3.debian.pool.ntp.org'.
- Supersede NTP from DHCP:** Radio buttons for 'Enabled' and 'Disabled'. 'Disabled' is selected. A help icon and text state: "By default, if an NTP Server address is provided via DHCP Option 42, it will be used instead of the NTP servers listed below. Enable this option to ignore DHCP Option 42."
- Device Date/Time:** A text field showing 'Wed Jul 8 05:36:41 2020' and a 'Sync with browser' button.
- Manually Override Time:** A text field showing '05:36:30' and a 'Manually Set Time' button. A help icon and text state: "Manual time and date are intended for testing purpose only. Time will be lost upon power down if NTP server is reachable."

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

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

Time Zone

Select time zone.

NTP Time Servers 1/2/3/4

The adapter 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 for logging purposes.

Advanced Settings Tab – Provisioning



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 8063 IP Door Controller 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, the 8063 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 8063 IP Door Controller) algop8063.conf

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

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

MD5 Checksum

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

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

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

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

Generating a generic configuration file

1. Connect the 8063 to the network
2. Access the 8063 Web Interface Control Panel
3. Configure the 8063 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 algop8063.conf
8. File algop8063.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 8063 IP Door Controller 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 8063 IP Door Controller with the MAC address specified in the configuration file name. Since all the necessary settings can be included in this file, the 8063 will be ready to work immediately after the configuration file is downloaded. The MAC address of each 8063 IP Door Controller 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

The screenshot shows the web interface for the 8063 IP Door Controller. At the top, there are tabs for Status, Basic Settings, Advanced Settings (which is selected), System, and Logout. Below these, there are sub-tabs for Network, Admin, Time, Provisioning, Advanced Audio (which is selected), and Advanced SIP. The main content area is titled 'Advanced Audio Functions'. Under the 'Functions' section, there is a single setting: 'Always Send RTP Media'. This setting has a radio button that is currently selected for 'Enabled' and an unselected radio button for 'Disabled'. At the bottom right of the configuration area, there is a green checkmark icon and a 'Save' button.

Always Send RTP Media

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

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 "System > [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 "System > [File Manager](#)" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder.

Force Secure TLS Version: ☐ 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

SRTP

SDP SRTP Offer: Disabled

NAT

Media NAT: ☐ None ☒ ICE ☐ STUN

TURN Server:

TURN User:

TURN Password:

SIP Transportation

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

SIPS Scheme

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

SDP SRTP Offer

Setting 'SDP SRTP Offer' to 'Optional', means the SIP call's RTP data will be left unencrypted if the other party does not support SRTP. Setting 'SDP SRTP Offer' to 'Standard', encrypts RTP voice data, meaning the normal audio RTP packets will now be secure (SRTP). This means SIP calls will be rejected if other party does not support SRTP. The 'Standard' option secures the audio data between parties, by making sure that it's not left out in the open for third parties to later reconstruct and listen to.

SIP Outbound Support (RFC 5626)

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

Outbound Proxy

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

Register Period (seconds)

Maximum requested period of time where the 8063 IP Door Controller 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	
Server Redundancy Feature (Multiple SIP Server Support)	☒ Enabled ☐ Disabled
Backup Server #1	
Backup Server #2	
Polling Interval (seconds)	120 seconds (2 minutes) ⓘ Time to wait between sending monitoring packets to each server. Inactive servers are always polled and the active server may optionally be polled (see below).
Poll Active Server	☐ Enabled ☒ Disabled ⓘ Explicitly poll the current server to monitor its availability. Polling may also be handled automatically by other regular events, so this can be disabled to reduce network traffic.
Automatic Failback	☒ Enabled ☐ Disabled ⓘ Reconnect with a higher priority server once available, even if the backup connection is still working.
Polling Method	☒ SIP NOTIFY ☐ SIP OPTIONS ⓘ SIP message used to poll servers in order to monitor their availability.

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

Server Redundancy Feature

Two secondary SIP servers may be configured. The 8063 IP Door Controller will attempt to register with the primary server but switch to a secondary server when necessary. The configuration allows re-registration to the primary server upon availability or to stay with a server until unresponsive.

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

Backup Server #1

If the primary server is unreachable the 8063 IP Door Controller will attempt to register with the backup servers. If enabled, the 8063 will always attempt to register with the highest priority server.

Backup Server #2

If backup server #1 is unreachable the 8063 IP Door Controller will attempt to register with the 2nd backup server. If enabled, the 8063 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 Failback

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.

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.

Web Interface System

System Tab – Maintenance

The screenshot shows the 'System' tab selected in the top navigation bar. Below it, the 'Maintenance' sub-tab is active. The main content area is titled 'System Maintenance' and contains three sections:

- Backup / Restore Configuration:**
 - 'Download Configuration File' with a 'Download' button.
 - 'Restore Configuration File' with a 'Browse...' button, 'No file selected.' text, and a 'Restore' button.
 - 'Restore Configuration to Defaults' with a 'Restore Defaults' button.
- Backup / Restore All User Files:**
 - 'Download Backup Zip File' with a 'Download' button.
 - 'Restore from Backup Zip File' with a 'Browse...' button, 'No file selected.' text, and a 'Restore' button.
 - 'Restore All Settings and Files to Defaults' with a 'Restore Defaults and Delete Files' button. Below this button is a warning icon and text: 'All preloaded and uploaded files, including tone files, will be deleted.'
- Reboot:**
 - 'Reboot the device' with a 'Reboot' button.

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 8063 IP Door Controller device settings to factory default values.

Download Backup File

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

Restore from Backup Zip File

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

Restore All Settings and Files to Defaults

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

Reboot the Device

Reboots the device.

System Tab – Firmware

The screenshot displays the 'Firmware' tab within the 'System' menu. It is divided into three main sections: 'Installed Firmware', 'Online Upgrade', and 'Custom Upgrade'. The 'Installed Firmware' section shows the current product firmware as 'algo-8063-3.3_alpha16'. The 'Online Upgrade' section includes a 'Check for Firmware Updates' button. The 'Custom Upgrade' section allows users to choose between upgrading 'From Local Files' (selected) or 'From URL'. It also features a 'Signed Firmware File' selection area with a 'Browse...' button and a 'No file selected.' status. Additionally, there is an 'Allow Downgrade' toggle set to 'Disabled', accompanied by a warning icon and text stating: 'Allow product or base firmware to be downgraded to an older version. Enabling this option could cause upgrade issues. Please contact support if necessary.' An 'Upgrade' button is located at the bottom of the custom upgrade section.

Method

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

Signed Firmware Image

Point to the signed firmware image provided by Algo.

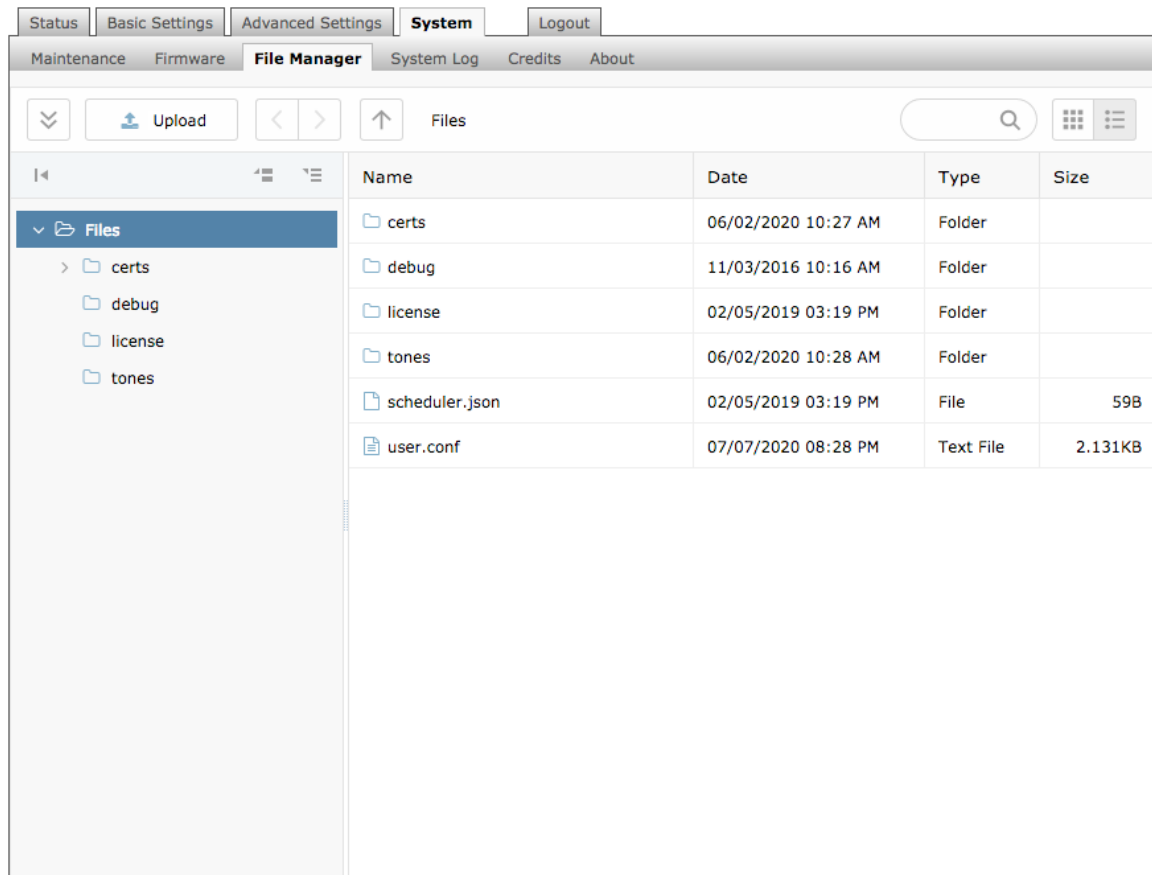
Allow Downgrade

Allow the 8063 to be downgraded to an older version. Please be advised that downgrades are supported only between same main version. For more information contact Algo Support.

Upgrade 8063 IP Door Controller Firmware

1. From the top menu, click on System, then Maintenance.
2. In the Upgrade section, click on Choose File and select the 8063 IP Door Controller 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 the Control Panel).

System Tab – File Manager



Files of different types must be uploaded to the appropriate folder, otherwise the 8063 will not recognize the file.

- For TLS provisioning and SIP signaling, a certificate file must be uploaded to the 'certs' folder.
- The 'tones' folder contains pre-loaded audio files. It is also the location where additional new audio files may be uploaded.

Uploading Custom Audio Files

Custom audio files (WAV or mp3) may be uploaded into memory (1 GB) to play for notification applications. Place your audio files into the **tones** directory.

An existing file may also be modified by downloading the original by right clicking the tone and selecting 'Download', making the desired changes, and then uploading the new version with a different name. Audio files must be in the following format:

- WAV or mp3 format
- Smaller than 200MB

Tone Files Included in Memory

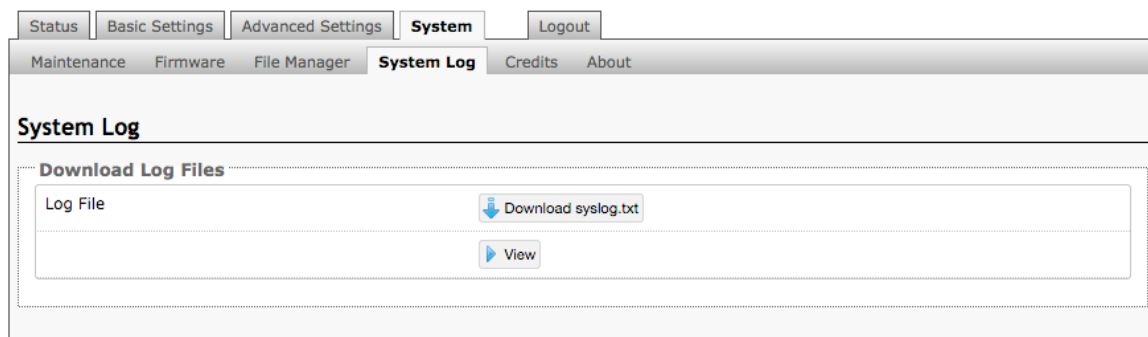
The 8063 IP Door Controller includes several pre-loaded audio files that can be selected to play for various events. Files may also be deleted or renamed.

Certificates

The user certificate for SIP over TLS and/or HTTPS Provisioning file must be named 'sipclient' with '.pem', '.crt', or '.cer' file type extension must be uploaded to 'certs' folder. For the trusted certificate, it should be named 'siptrusted' with '.pem', '.crt', or '.cer' file type extension must be uploaded to the 'trusted' folder inside the 'certs' folder.

System Tab – System Log

System log files are automatically created and assist with troubleshooting in the event the 8063 IP Door Controller does not behave as expected.



Specifications

Power Input:	48V PoE IEEE 802.3af Class 0 (Max 12.95 W) or Type 2 PoE+ IEEE 802.3at (Max 25.5 W) Idle nominal 2.5W
SIP:	Optional: Can be operated via a direct SIP call if not used in conjunction with an Algo Intercom product.
Processor:	Linux OS ARM Cortex-A8 32-Bit RISC Processor

Input/Output Terminals:

5 Position Terminal Block	Relay (30V 2A)	NO	Normally Open
		C	Common
		NC	Normally Closed
	24V Auxiliary Power Output (PoE+ or optional power supply needed)	PWR -	0.2A – PoE
		PWR +	0.5A – PoE+
6 Position Terminal Block	Input 1	Max 1kOhm	
	Input 2	Max 1kOhm	
	Aux Out Relay	Max 30V 1A	

Configuration:	Web interface (HTTP or HTTPS) or autoprovisioning server.
Provisioning:	TFTP, FTP, HTTP, HTTPS
Supervision:	SNMP
NAT:	STUN, CRLF Keep Alive
Environmental:	+32 to +122 deg F (0 to +50 deg C); Suitable for dry indoor environments only.
Dimensions:	3.25" W x 1.2" H x 5.4" D 8.3 cm W x 3.0 cm H x 13.7 cm D
Mounting:	Wall mountable or tabletop
Weight:	2.2 lb (1.0 kg)
Compliance:	EN60950:2001, IEEE 802.3-2008, RoHS, CE, FCC Class A, CISPR 22 Class A, CISPR 24, CSA/UL (USA & Canada)

FCC Compliance Statement

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

Document 90-00106
2020-09-02
Page 35

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

(604) 454-3792
support@algosolutions.com