Algo SIP Endpoints and Cisco Webex Calling Registration Guide

Need Help?

(604) 454-3792 or support@algosolutions.com

Table of Contents

Introduction

Algo SIP Endpoints can register to Cisco Webex Calling as a third-party SIP endpoint for voice paging, loud ringing, and emergency alerting.

This document provides instructions to set up the Algo IP Endpoints on the Cisco Webex Calling Control Hub (CH) administration portal. All tests were conducted with the Algo 8301 SIP Paging Adapter & Scheduler, 8186 SIP Horn, 8180 SIP Audio Alerter (G2), 8128 G2 SIP Strobe Light and 8201 SIP PoE Intercom. These are representative of all Algo IP speakers, paging adapters, visual alerters and door phones and similar registration steps would apply.

The firmware version tested on the Algo devices is 3.3.3. The devices with firmware 3.3.3 and above will register to Webex Calling.

Please note the following Algo devices that are supported with Webex Calling:

1. **IP SPEAKERS & HORNS**
   - 8180 (G2)
   - 8186
   - 8188
   - 8189
   - 8190 & 8190S
   - 8196
   - 8198
2. **IP PAGING ADAPTER**
   - 8301
   - 8373
3. **IP STROBE LIGHTS**
   - 8128 (G2)
   - 8138
4. **IP DOORPHONES/INTERCOMS**
   - 8028 (G2)
   - 8063
   - 8201
   - 8300
5. **IP CONTROLLERS**
   - 8300

Please see certain exceptions regarding unsupported devices below:

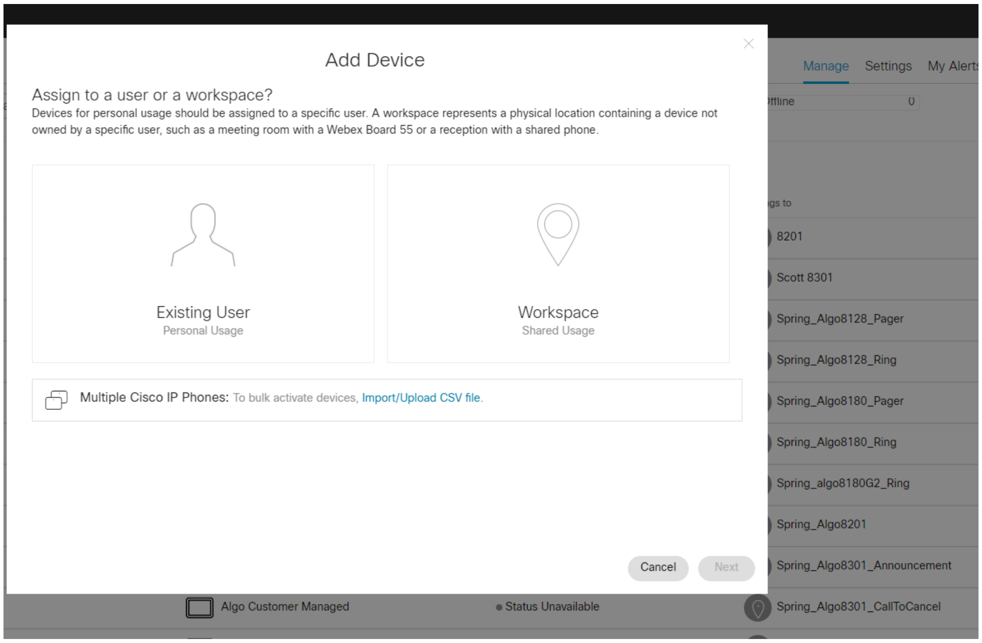
Note 1: The following endpoints are exceptions and cannot be registered to Cisco Webex Calling, as TLS/SRTP support is not available: 8180 SIP Audio Alerter(G1), 8028 SIP Doorphone(G1), 8128 Strobe Light(G1) and 8061 SIP Relay Controller. For more information, please contact Algo support.

Note 2: The video intercoms 8039 and 8036 are exceptions as they do not support SDP SRTP encryption at the moment. Accordingly, they cannot be registered to Cisco Webex Calling.

Note 3: Currently, only a single endpoint can be assigned to a workspace. Devices cannot have multiple extensions registered to a same workspace.

Configuration Steps – Webex Portal

1. Log in to the Webex Control Hub as the Organization's Administrator and select **Manage Devices**. Click on **Add Device** in the top right corner. The window shown below will open.



Add Device

Assign to a user or a workspace?

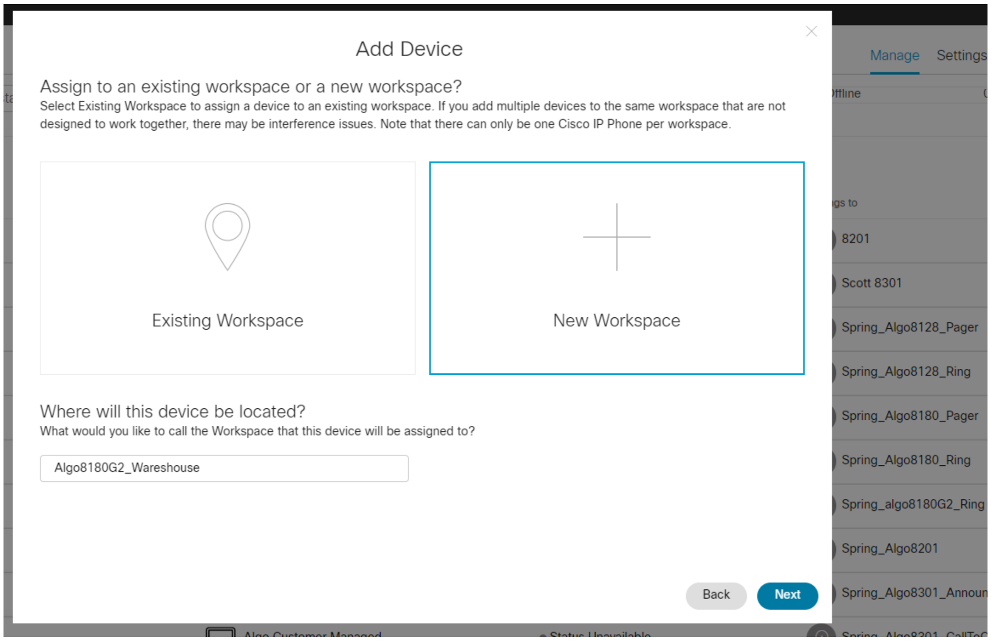
Devices for personal usage should be assigned to a specific user. A workspace represents a physical location containing a device not owned by a specific user, such as a meeting room with a Webex Board 55 or a reception with a shared phone.

Multiple Cisco IP Phones: To bulk activate devices, Import/Upload CSV file.

2. Assign a workspace to the device by selecting **Workspace**. Currently, only one workspace can be allocated to a device. Press **Next**.

3. If there is an existing workspace, that is not allocated yet, you may assign it by selecting **Existing Workspace** or create a new workspace by clicking the "**+ New Workspace**."

4. Enter a name or description for the Workspace that will be created (e.g., Algo8180G2_Warehouse), and press **Next**.



Add Device

Assign to an existing workspace or a new workspace?

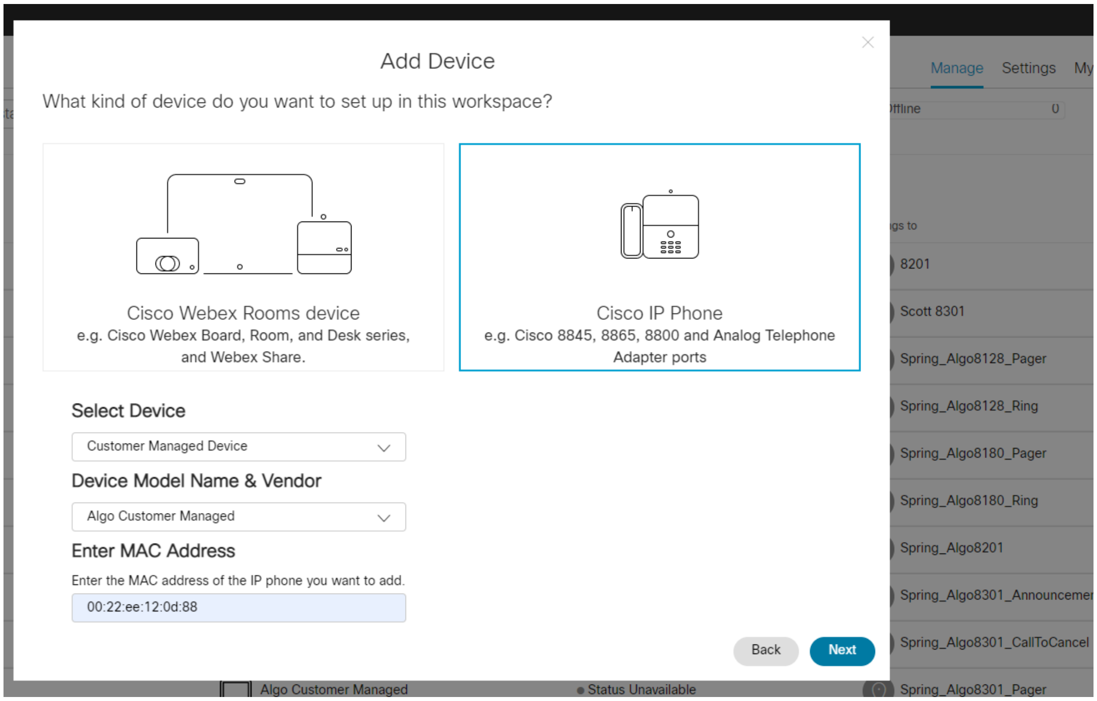
Select Existing Workspace to assign a device to an existing workspace. If you add multiple devices to the same workspace that are not designed to work together, there may be interference issues. Note that there can only be one Cisco IP Phone per workspace.

Where will this device be located?

What would you like to call the Workspace that this device will be assigned to?

Algo8180G2_Wareshouse

5. Select **Cisco IP Phone** to enter the device information. First, under the **Select Device** dropdown select **Customer Managed Device** as the device type. For the **Device Model Name & Vendo**r, select **Algo Customer Managed**. Lastly, enter the MAC address of the Algo endpoint (e.g. 00:22:ee:xx:xx:xx).



Add Device

What kind of device do you want to set up in this workspace?

Cisco Webex Rooms device
e.g. Cisco Webex Board, Room, and Desk series, and Webex Share.

Cisco IP Phone
e.g. Cisco 8845, 8865, 8800 and Analog Telephone Adapter ports

Select Device: Customer Managed Device

Device Model Name & Vendor: Algo Customer Managed

Enter MAC Address

Enter the MAC address of the IP phone you want to add.

00:22:ee:12:0d:88

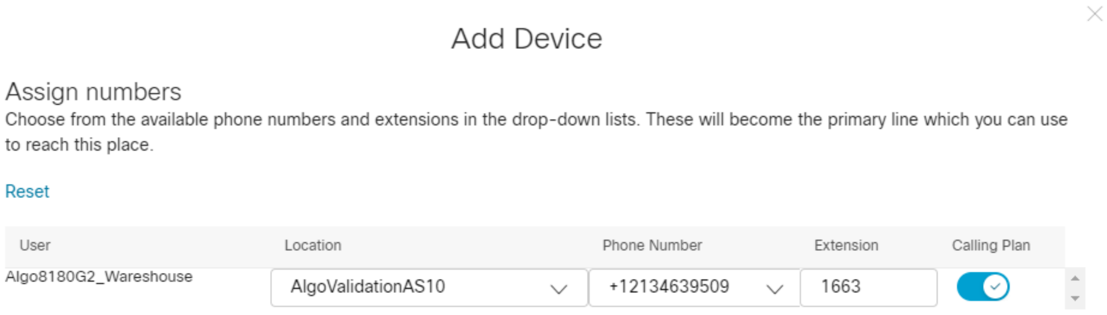
6. Click **Next** to proceed to the **Assign numbers** entry.

7. Select a Location for the Workspace.

8. Assign a phone number for the device if desired. It may be set as **None** if no phone number is required. Note that this can be added at a later time.

9. Enter the Extension to be assigned.

10. Click **Save** to proceed.



Add Device

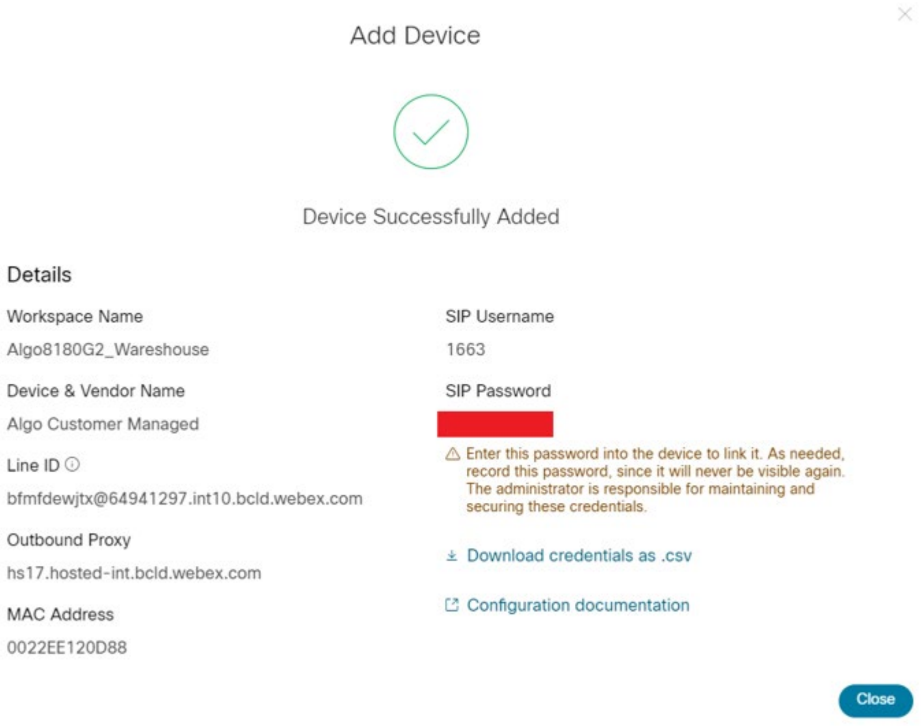
Assign numbers

Choose from the available phone numbers and extensions in the drop-down lists. These will become the primary line which you can use to reach this place.

Reset

User	Location	Phone Number	Extension	Calling Plan
Algo8180G2_Wareshouse	AlgoValidationAS10	+12134639509	1663	✓

11. The Webex Control Hub will then generate the SIP credentials for the Algo endpoint. It’s recommended to download the .csv file with the credentials and keep it in a secure location.



Add Device

Device Successfully Added

Details

Workspace Name
Algo8180G2_Wareshouse

Device & Vendor Name
Algo Customer Managed

Line ID
bfmfdewjtx@64941297.int10.bcld.webex.com

Outbound Proxy
hs17.hosted-int.bcld.webex.com

MAC Address
0022EE120D88

SIP Username
1663

SIP Password
[redacted]

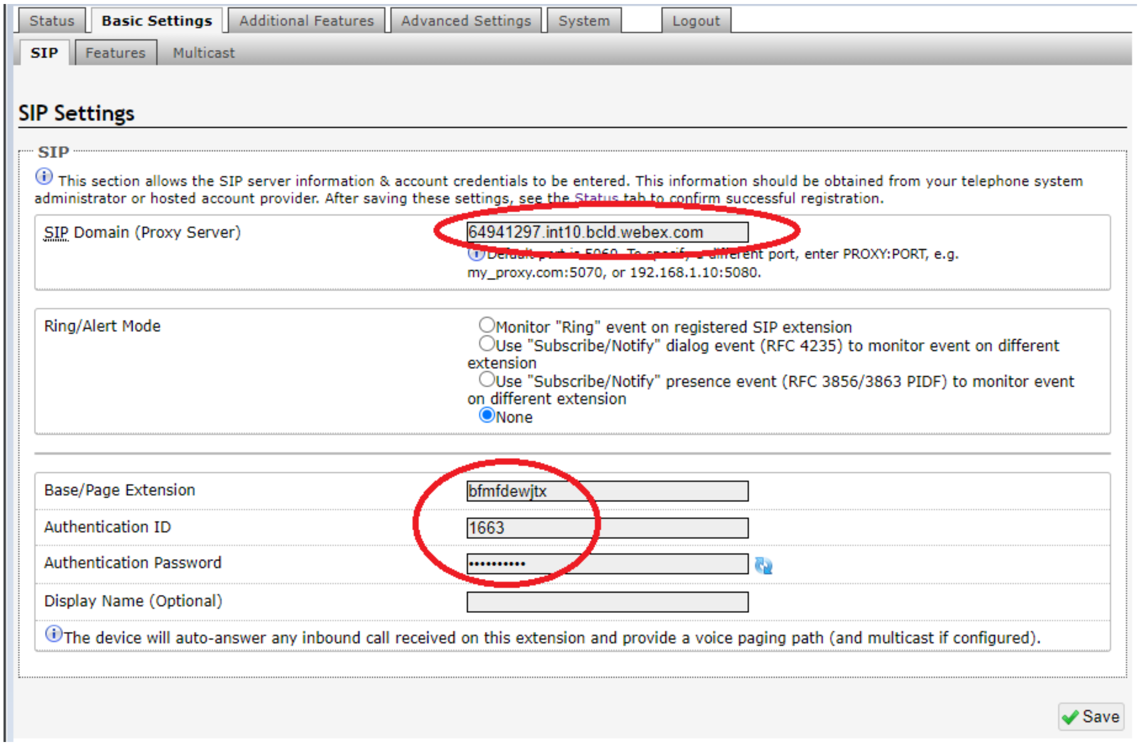
Enter this password into the device to link it. As needed, record this password, since it will never be visible again. The administrator is responsible for maintaining and securing these credentials.

Configuration Steps – Algo Endpoint

1. Open a web browser and log in to the Algo web interface, by entering the device's IP address. If you are not sure what is the IP address, check the Getting Started section in the User Guide.

2. Log in and navigate to Basic Settings -> SIP tab. Enter the SIP credentials provided from Webex as per the table below. Please note the credentials below are an example, use the credentials generated by your Webex portal.

Webex Parameter	Algo Parameter
Line ID (Use only the portion after the "@")	SIP Domain (Proxy Server)
Line ID (Use only the portion before the "@")	Extension
SIP Username	Authentication ID
SIP Password	Authentication Password



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): 64941297.int10.bcld.webex.com

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

Ring/Alert Mode:
○ Monitor "Ring" event on registered SIP extension
○ Use "Subscribe/Notify" dialog event (RFC 4235) to monitor event on different extension
○ Use "Subscribe/Notify" presence event (RFC 3856/3863 PIDF) to monitor event on different extension
● None

Base/Page Extension	bfmfdewjtx
Authentication ID	1663
Authentication Password	••••••••••
Display Name (Optional)	

ⓘ The device will auto-answer any inbound call received on this extension and provide a voice paging path (and multicast if configured).

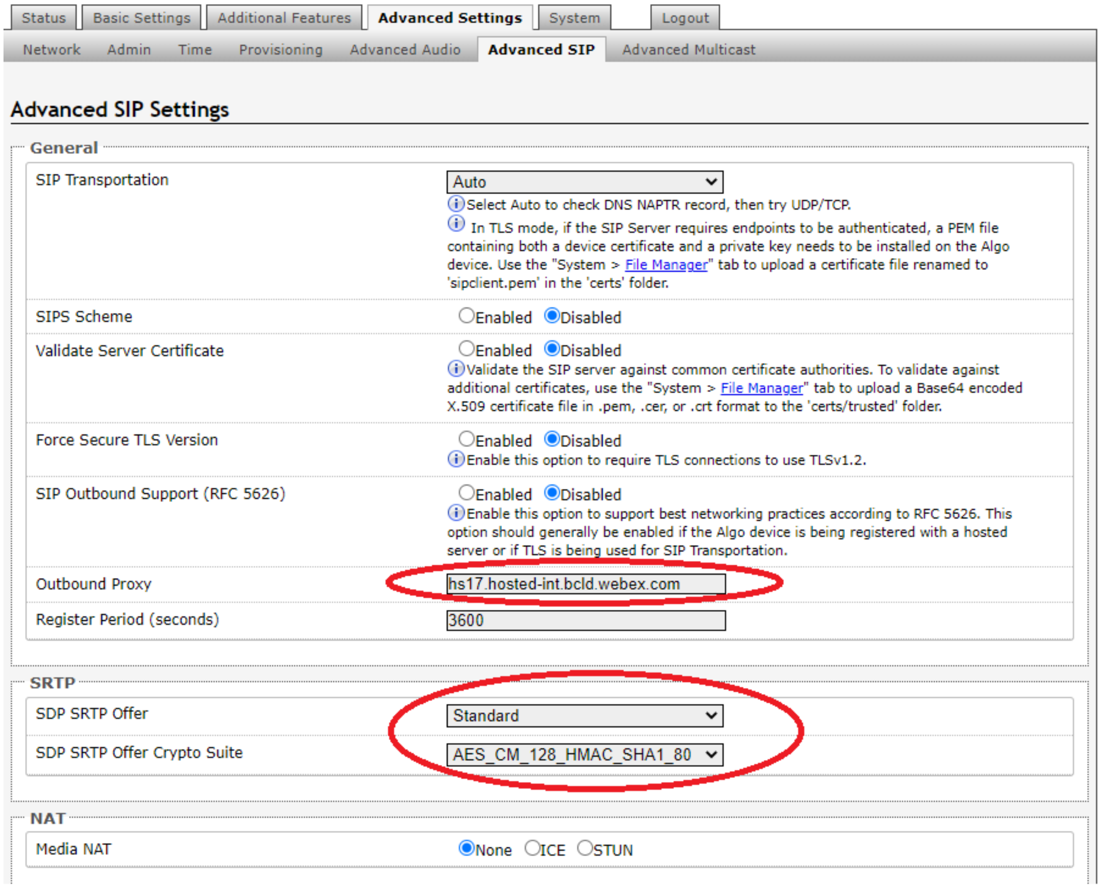
3. Go to Advanced Settings > Advanced SIP tab.

4. Enter Outbound Proxy address provided by Webex.

5. Set the SDP SRTP Offer to **Standard**.

6. Set SDP SRTP Offer Crypto Suite to **AES_CM_128_HMAC_SHA1_80**.

7. Save all the settings on this page.



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	hs17.hosted-int.bcld.webex.com
Register Period (seconds)	3600

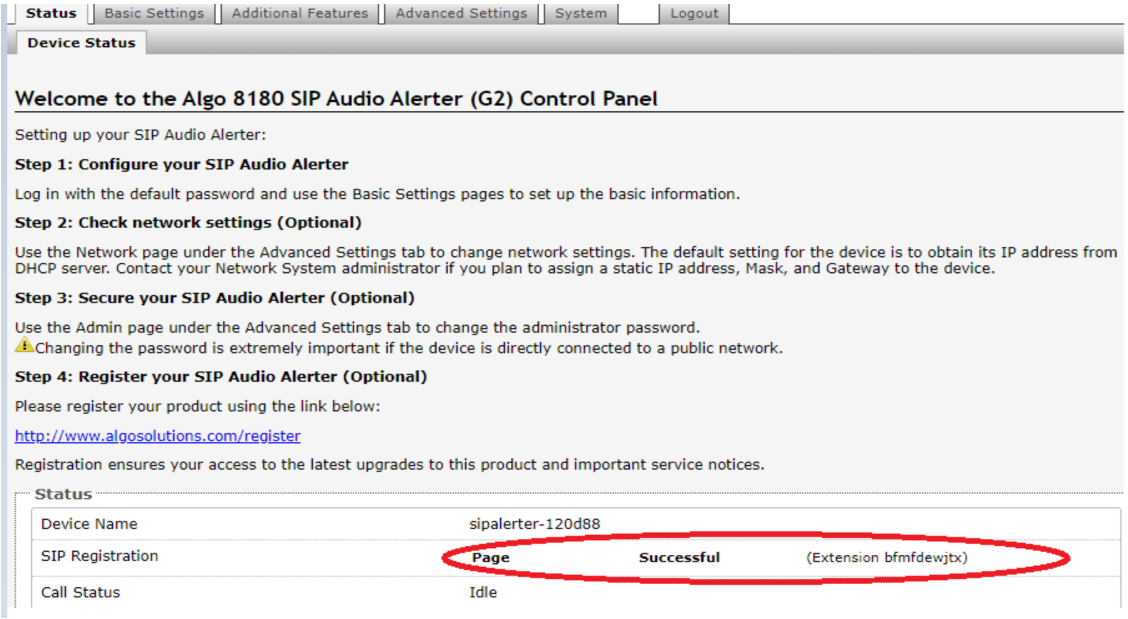
SRTP

SDP SRTP Offer	Standard
SDP SRTP Offer Crypto Suite	AES_CM_128_HMAC_SHA1_80

NAT

Media NAT	●None ○ICE ○STUN

8. Confirm the device is registered successfully in the Status tab.



Welcome to the Algo 8180 SIP Audio Alerter (G2) Control Panel

Setting up your SIP Audio Alerter:

Step 1: Configure your SIP Audio Alerter

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 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 Audio Alerter (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 Audio Alerter (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	sipalerter-120d88		
SIP Registration	**Page**	**Successful**	(Extension bfmfdewjtx)
Call Status	Idle		

9. Once the Algo endpoint is registered, call it by dialing the extension. In this particular example, 1663.

Troubleshooting

SIP Registration Status = “Rejected by Server” (in the Status tab)

Meaning: The Webex server receives SIP Register packets from the endpoint and responds with an unauthorized message.

- Ensure the credentials (extension, authentication ID, password) on the device match on the Server.
- Under Basic Settings -> SIP, click on the blue circular arrows to the right of the Password field. If the Password is not what it should be, the web browser is probably auto filling the password field. If so, any change on a page containing a password could be filled in with an undesired string.

SIP Registration Status = “No reply from server” (in the Status tab)

Meaning: the device is not able to communicate across the network to the phone server.

- Double check the "SIP Domain (Proxy Server)", under Basic Settings -> SIP tab field is filled out correctly with the address of your server and port number.
- Check if the Outbound Proxy is correct under Advanced Settings -> Advanced SIP.
- Try changing the SIP Transportation Method (Advanced Settings -> Advanced SIP) from “Auto” to “TLS”.
- Ensure the firewall (if present) is not blocking the incoming packets from the server.

Registration Drops Constantly

Enable the Keep-alive method. Navigate to Advanced Settings -> Advanced SIP, set Keep-alive to "Double CRLF" and set the period to 30 seconds.