



Avaya Solution & Interoperability Test Lab

Application Notes for Algo 8036 SIP Multimedia Intercom Version 1.7.1 with Avaya IP Office Release 11 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Algo 8036 SIP Multimedia Intercom with Avaya IP Office. Algo 8036 SIP Multimedia Intercom is device that integrates into the Avaya IP Office and enables conversations and remote entry using door release features.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for Algo 8036 SIP Multimedia Intercom to interoperate with Avaya IP Office. Algo 8036 SIP Multimedia Intercom (hereafter referred as 8036) is SIP-based device that can register with Avaya IP Office as SIP endpoint using UDP protocol.

The 8036 is a SIP compliant Power over Ethernet (PoE) outdoor intercom combining the functionality of an IP phone, security camera and interactive kiosk via a touch screen interface. The intercom is designed for public access locations and secure entrances/gates, to provide enhanced communication and support for guests and visitors.

In the compliance testing, Avaya IP Office Server Edition system (IP Office) consists of Avaya IP Office Primary Linux running on Virtualized Environment and a 500V2 Expansion.

2. General Test Approach and Test Results

The feature test cases were performed manually. The focus of this interoperability compliance testing was to verify if the 8036 can register as a SIP endpoint on the IP Office and able to make a call to and from a telephone on the IP Office and able to open the door when the key is pressed on the phone.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products only (private network side). Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the 8036 did not include use of any specific encryption features as requested by Algo.

2.1. Interoperability Compliance Testing

Compliance testing verified that the 8036 was able to interoperate with the telephones residing on the IP Office system. The following interoperability areas were covered:

- The 8036 can register to the IP Office as a SIP endpoint.
- The 8036 can make a call to an endpoint on the IP Office and establish a clear speech path.
- An endpoint on the IP Office can call the extension assigned to the 8036 and establish speech path.
- Endpoints on the IP Office can send required DTMF tones and therefore ensure the remote door release features work successfully.

The serviceability testing focused on verifying the ability of the 8036 to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to the device.

2.2. Test Results

The objectives outlined in **Section 2.1** were verified. All test cases passed, the following observations were made during the compliance testing:

- A call between the 8036 and Avaya endpoint (H.323, SIP, and digital) cannot be transferred by Avaya endpoint to Avaya SIP endpoint. This feature is currently not supported on the 8036.

2.3. Support

Technical support on Algo 8036 SIP Multimedia can be obtained through the following:

- Phone: + 1 604 454 3792
- Web: <http://www.algosolutions.com/support/support.html>
- Email: support@algosolutions.com

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance testing between Avaya IP Office and Algo 8036 SIP Multimedia Intercom. The 8036 communicated with IP Office through Avaya switch with Power over Ethernet (PoE) and registered with Avaya IP Office as SIP endpoint. The PRI T1 trunk was also configured to connect from IP Office to PSTN for test cases off-net via PRI T1 trunk.

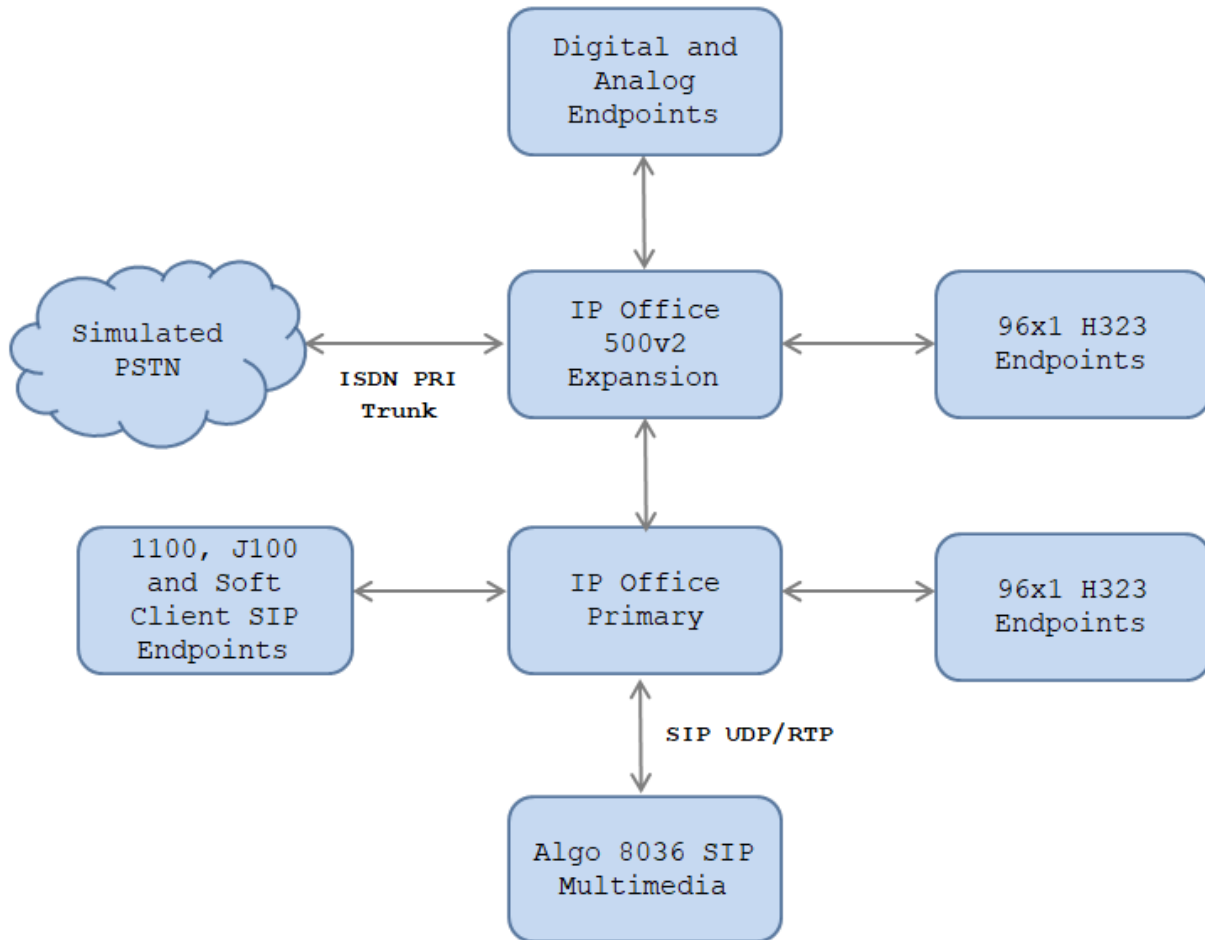


Figure 1: Test Configuration Diagram

The following table indicates the IP addresses that were assigned to the systems in the test configuration diagram:

Description	IP Address
IP Office Primary Server Edition	10.10.97.110
IP Office 500V2 Expansion	10.10.97.230
Avaya SIP and H323 Endpoint	10.33.5.30-10.33.5.36
Algo 8036 Multimedia Intercom	10.33.5.50

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya IP Office Primary Server Edition running on Virtual Environment	11.0.0.2.0 Build 23
Avaya IP Office 500v2 Expansion	11.0.0.2.0 Build 23
Avaya IP Office DIG DCPx16 V2	11.0.0.2.0 Build 23
Avaya IP Office Manager	11.0.0.2.0 Build 23
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.6604
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya J129 SIP Deskphone	3.0.0.16
Avaya Equinox™ for Windows	3.4.4.45.14
Algo 8036 SIP Multimedia Intercom Firmware Version	1.7.1_rc
Base Version	1.7

Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500v2 and also when deployed with all configurations of IP Office Server Edition.

5. Configure Avaya IP Office

This section provides the procedures for configuring Avaya IP Office. The procedures include the following areas:

- Verify IP Office license
- Obtain LAN IP address
- Administer SIP registrar
- Administer SIP extensions
- Administer SIP users

5.1. Verify IP Office License

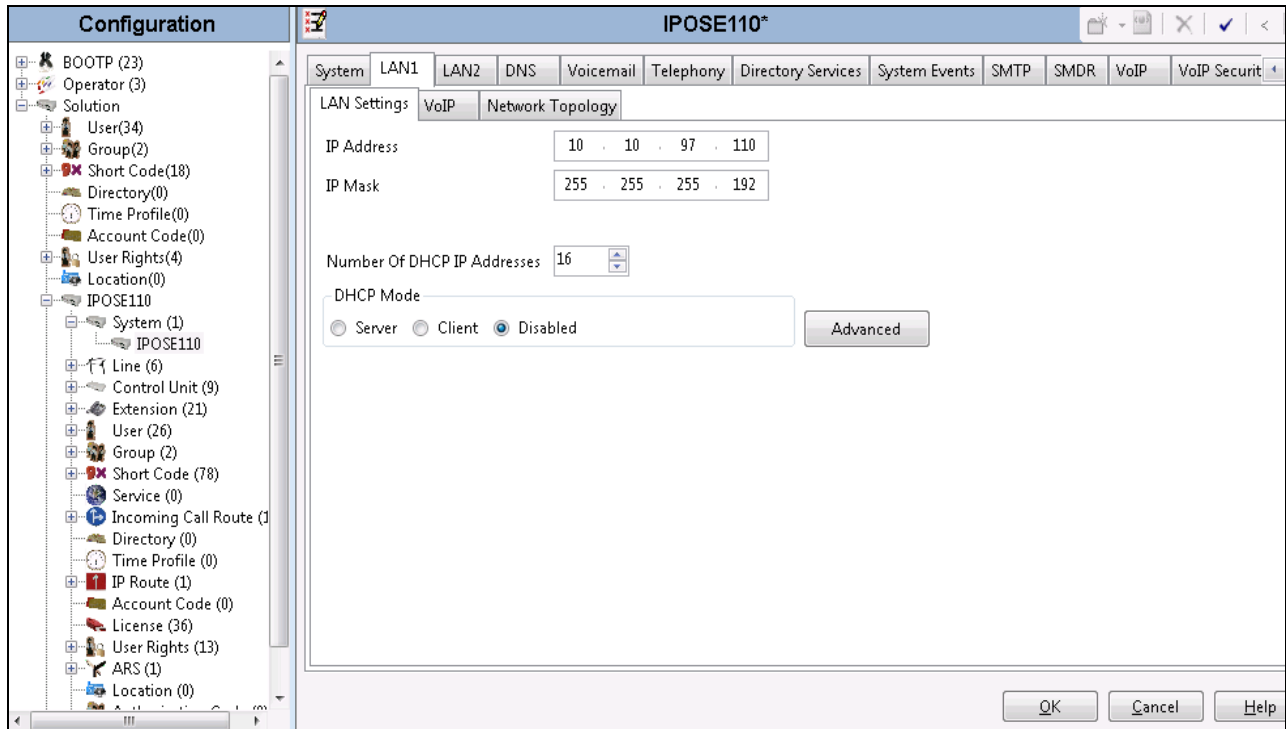
From a PC running the Avaya IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the Manager application. Select the proper IP Office system, and log in using the appropriate credentials.

The **Avaya IP Office Manager** screen is displayed. From the configuration tree in the left pane, select **License**, the list of license displayed in the right panel. Verify that the **3rd Party IP Endpoints** status is “Valid”.

Feature	Instances	Status	Expiration Date	Source
Power User	384	Valid	Never	PLDS Nodal
Avaya IP endpoints	384	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	32	Obsolete	Never	PLDS Nodal
SIP Trunk Channels	512	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal
CTI Link Pro	5	Valid	Never	PLDS Nodal
Wave User	16	Obsolete	Never	PLDS Nodal
3rd Party IP Endpoints	384	Valid	Never	PLDS Nodal
Centralized Endpoints	100	Obsolete	Never	PLDS Nodal
Essential Edition	5	Obsolete	Never	PLDS Nodal
R8+ Preferred Edition (VM Pro)	5	Obsolete	Never	PLDS Nodal
Server Edition	5	Valid	Never	PLDS Nodal
UMS Web Services	100	Valid	Never	PLDS Nodal
WebLM Model	1	Obsolete	Never	PLDS Nodal
WebLM Model 9.1	1	Obsolete	Never	PLDS Nodal
Avaya Mac Softphone	100	Valid	Never	PLDS Nodal
SM Trunk Channels	128	Valid	Never	PLDS Nodal
Web Collaboration	64	Valid	Never	PLDS Nodal
Avaya Contact Center Select	5	Valid	Never	PLDS Nodal

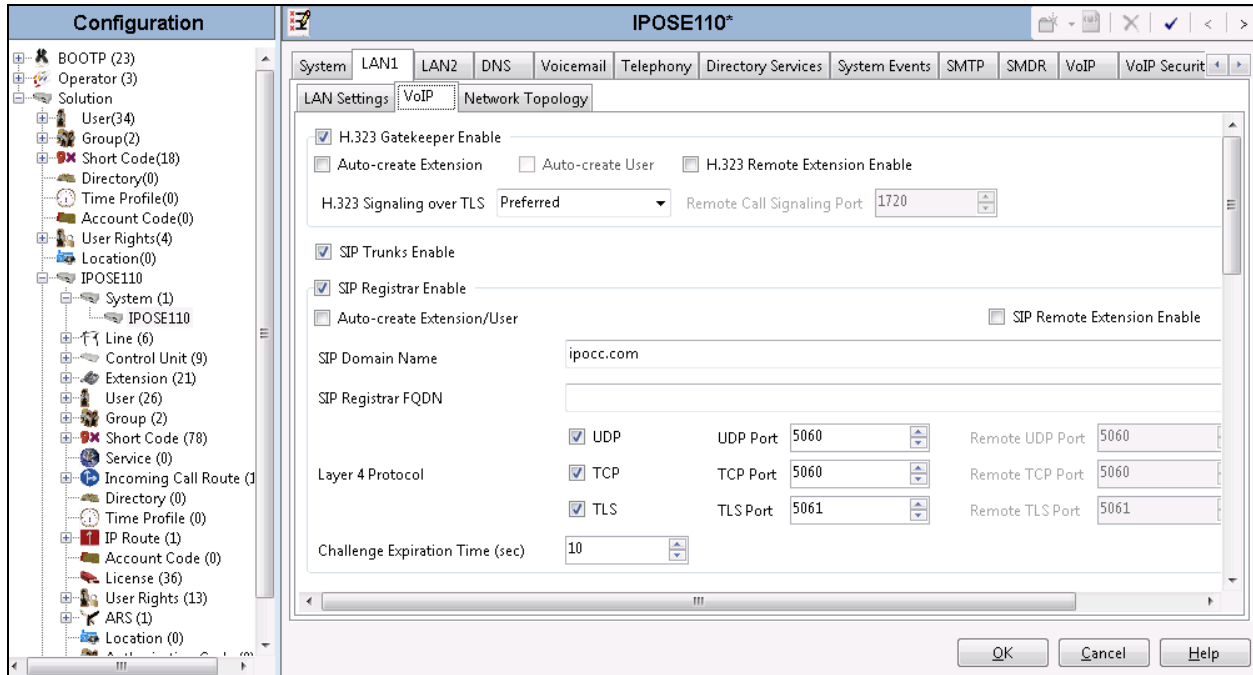
5.2. Obtain LAN IP Address

From the configuration tree in the left pane, select System to display the **IPOSE110** screen in the right pane. Select the LAN1 tab, followed by the LAN Settings sub-tab in the right pane. Make a note of the IP Address, which will be used later to configure Algo. Note that IP Office can support SIP extensions on the LAN1 and/or LAN2 interfaces, and the compliance testing used the LAN1 interface.



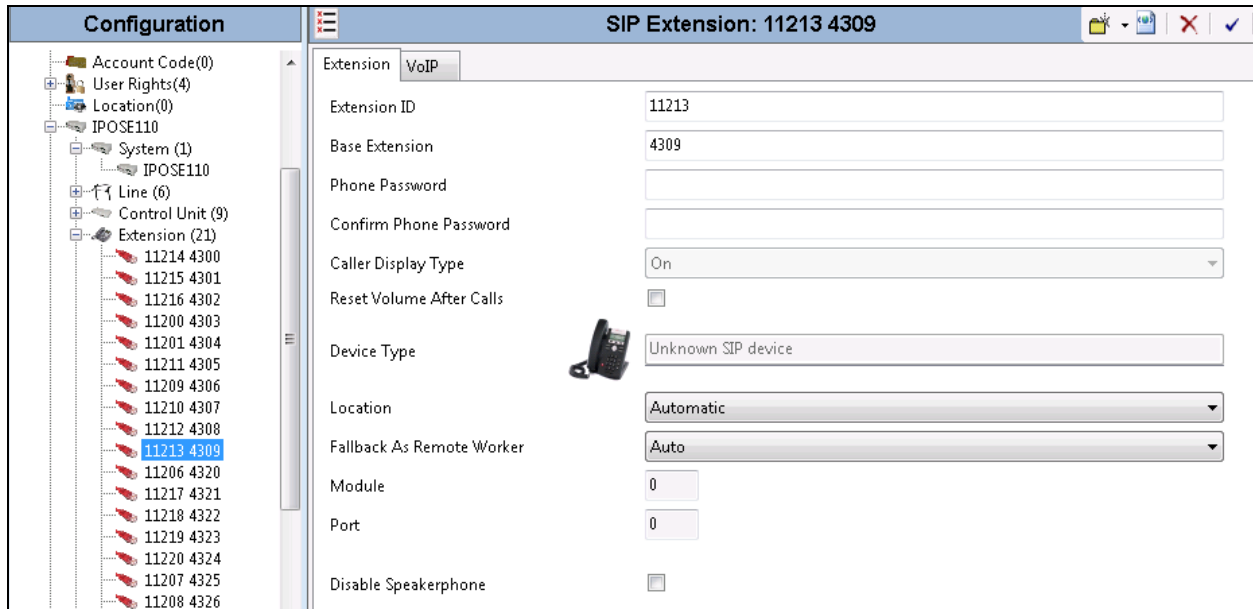
5.3. Administer SIP Registrar

Select the **VoIP** sub-tab. Make certain that **SIP Registrar Enable** is checked, as shown below. Enter a valid sip domain name for SIP endpoints to use for registration with IP Office. In the compliance testing, the sip domain name **ipocc.com** was used so the SIP endpoints used the sip domain name for registration.

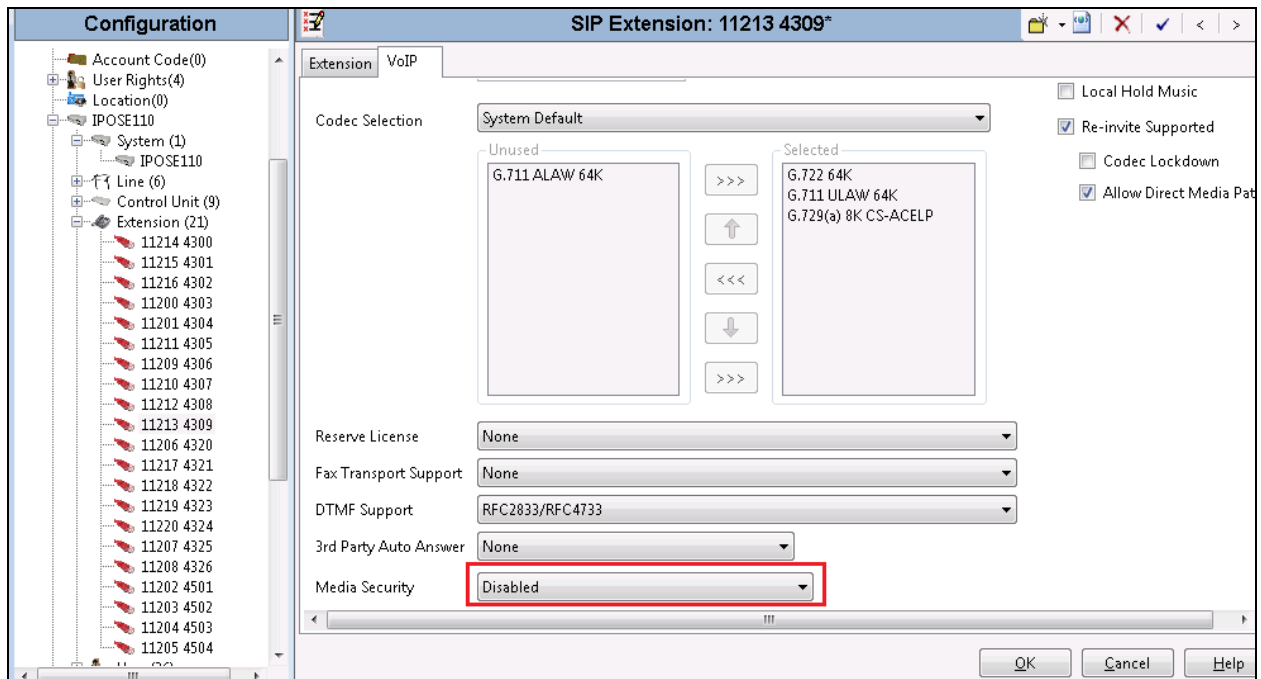


5.4. Administer SIP Extensions

From the configuration tree in the left pane, right-click on **Extension** and select **New → SIP Extension** from the pop-up list to add a new SIP extension. For **Base Extension**, enter the SIP door extension “**4309**”. Retain the default values in the remaining fields.



Select the **VoIP** tab, select **Disabled** in the **Media Security** field and retain other fields at default values. Repeat this section to add additional SIP extensions as desired.



5.5. Administer SIP User

From the configuration tree in the left pane; right-click on **User** tab and select **New** from the pop-up list. Enter desired values for **Name**. For **Extension**, enter the 8036 extension from **Section 5.4**. Remember these values as they will be needed to register the 8036 to IP Office. Enter desired values for **Password** and **Confirm Password**.

The screenshot shows the Avaya IP Office configuration interface. On the left is a configuration tree with 'User (26)' expanded. The main pane shows the configuration for extension 4309. The 'User' tab is active, and the 'Supervisor Settings' sub-tab is selected. The configuration fields are as follows:

Field	Value
Name	4309
Password	••••••
Confirm Password	••••••
Unique Identity	
Conference PIN	
Confirm Audio Conference PIN	
Account Status	Enabled
Full Name	SIP 3RD 4309
Extension	4309
Email Address	
Locale	
Priority	5
System Phone Rights	None
Profile	Basic User

Select the **Telephony** tab, followed by the **Supervisor Settings** sub-tab, and enter a desired **Login Code**. This **Login Code** is needed to register the 8036 to IP Office. Note: if the **Phone Password** in the **Extension** tab in **Section 5.4** is configured, the password in the Phone Password must be used for the registration, in case the **Phone Password** is left blank then the code in the **Login Code** is used for the registration. The difference between Phone Password and Login Code is that the Phone Password can combine letter and number while Login Code only allows number.

The screenshot shows the Avaya IP Office configuration interface for extension 4309, with the 'Telephony' tab and 'Supervisor Settings' sub-tab selected. The configuration fields are as follows:

Field	Value	Option
Login Code	••••••	<input type="checkbox"/> Force Login
Confirm Login Code	••••••	
Login Idle Period (sec)		<input type="checkbox"/> Force Account Code
Monitor Group	<None>	<input type="checkbox"/> Force Authorization Code
Coverage Group	<None>	<input type="checkbox"/> Incoming Call Bar
Status on No-Answer	Logged On (No change)	<input type="checkbox"/> Outgoing Call Bar
IPOCC Agent Type	<None>	<input type="checkbox"/> Inhibit Off-Switch Forward/Transfer
Privacy Override Group	<None>	<input type="checkbox"/> Can Intrude
Reset Longest Idle Time		<input checked="" type="checkbox"/> Cannot Be Intruded
	<input checked="" type="radio"/> All Calls	<input type="checkbox"/> Can Trace Calls
	<input type="radio"/> External Incoming	<input type="checkbox"/> Deny Auto Intercom Calls

6. Configure 8036 SIP Multimedia Intercom

This section provides the procedures for configuring the 8036. The procedures include the following areas.

6.1. Launch Web Interface

Access the 8036 web-based interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the 8036. The IP address can obtain initially from the call button on the 8036. The **Welcome to the Algo 8036 SIP Multimedia Intercom Control Panel** screen is displayed, as shown below. Log in using the appropriate credentials.

ALGO 8036 SIP Multimedia Intercom Control Panel Firmware: 1.7.1_rc1

Status

Status and Login Video

Welcome to the Algo 8036 SIP Multimedia Intercom Control Panel

Setting up your SIP Multimedia Intercom:

Step 1: Configure your SIP Multimedia 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 Multimedia 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 Multimedia 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

6.2. Administer Algo 8036

Select **Basic Settings** → **SIP** from the top menu, to display the screen below. Configure the **SIP Account** section toward the bottom of the screen as desired to match the configuration. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **SIP Domain (Proxy Server):** Enter the sip domain name of IP Office as configured in **Section 5.2**.
- **Extension:** Enter the SIP base extension as configured in **Section 5.4**.
- **Authentication ID:** Enter the SIP user name as configured in **Section 5.5**.

- **Authentication password:** The SIP extension password in **Section 5.4** or SIP user login code in **Section 5.5**.

The screenshot displays the ALGO 8036 SIP Multimedia Intercom Control Panel. The top navigation bar includes the ALGO logo, the title "8036 SIP Multimedia Intercom Control Panel", and the firmware version "Firmware: 1.7.1_rc1". Below the navigation bar are tabs for "Status", "Basic Settings", "User Interface", "Advanced Settings", "System", and "Logout". The "Basic Settings" tab is active, and within it, the "SIP" sub-tab is selected. The "SIP Settings" section contains a help message and several input fields: "SIP Domain (Proxy Server)" with the value "jpoc.com", "Extension" with "4309", "Authentication ID" with "4309", "Authentication Password" with masked characters "*****", and "Display Name (Optional)" which is empty. A "Save" button with a green checkmark is located at the bottom right of the settings area.

Field	Value
SIP Domain (Proxy Server)	jpoc.com
Extension	4309
Authentication ID	4309
Authentication Password	*****
Display Name (Optional)	

Navigate to **Advanced Settings** → **Advanced SIP**, the **Advanced SIP Settings** is displayed.
Enter the IP address of LAN1 IP Office in the **Outbound Proxy** and keep other values at default.

ALGO 8036 SIP Multimedia Intercom Control Panel Firmware: 1.7.1_rc1

Status Basic Settings User Interface **Advanced Settings** System Logout

Network Admin Users Time Provisioning File Manager **Advanced SIP**

Advanced SIP Settings

General

SIP Transportation:
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.
To force the Algo device to authenticate the SIP server, a certificate obtained from the SIP server needs to be installed. Use the "Advanced Settings > File Manager" tab to upload a certificate file renamed to 'siptrusted.pem' in the 'certs' folder.

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):

NAT

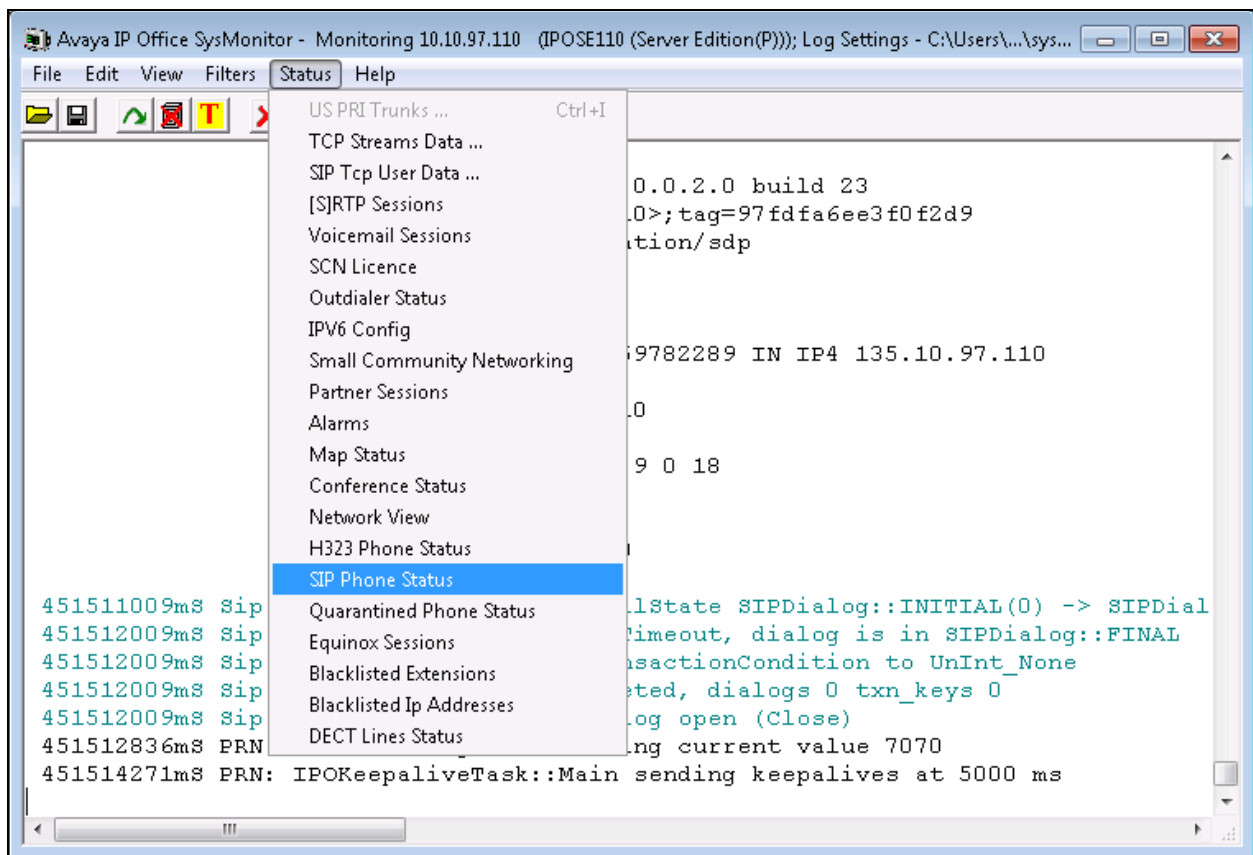
Media NAT: None ICE STUN

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of IP Office and the 8036.

7.1. Verify Avaya IP Office

From a PC running the Avaya IP Office Monitor application, select **Start → Programs → IP Office → System Monitor** to launch the application. The **Avaya IP Office SysMonitor** screen is displayed, as shown below. Select **Status → SIP Phone Status** from the top menu.



The **SIPPhoneStatus** screen is displayed and select the **Registered** radio button in the **Display Options** area it displays all SIP users currently register to IP Office. Verify that there is an entry for the **Algo-8036/1.7.1_rc1** in the list.

SIPPhoneStatus

Total Configured: 15 Waiting 3 secs for update

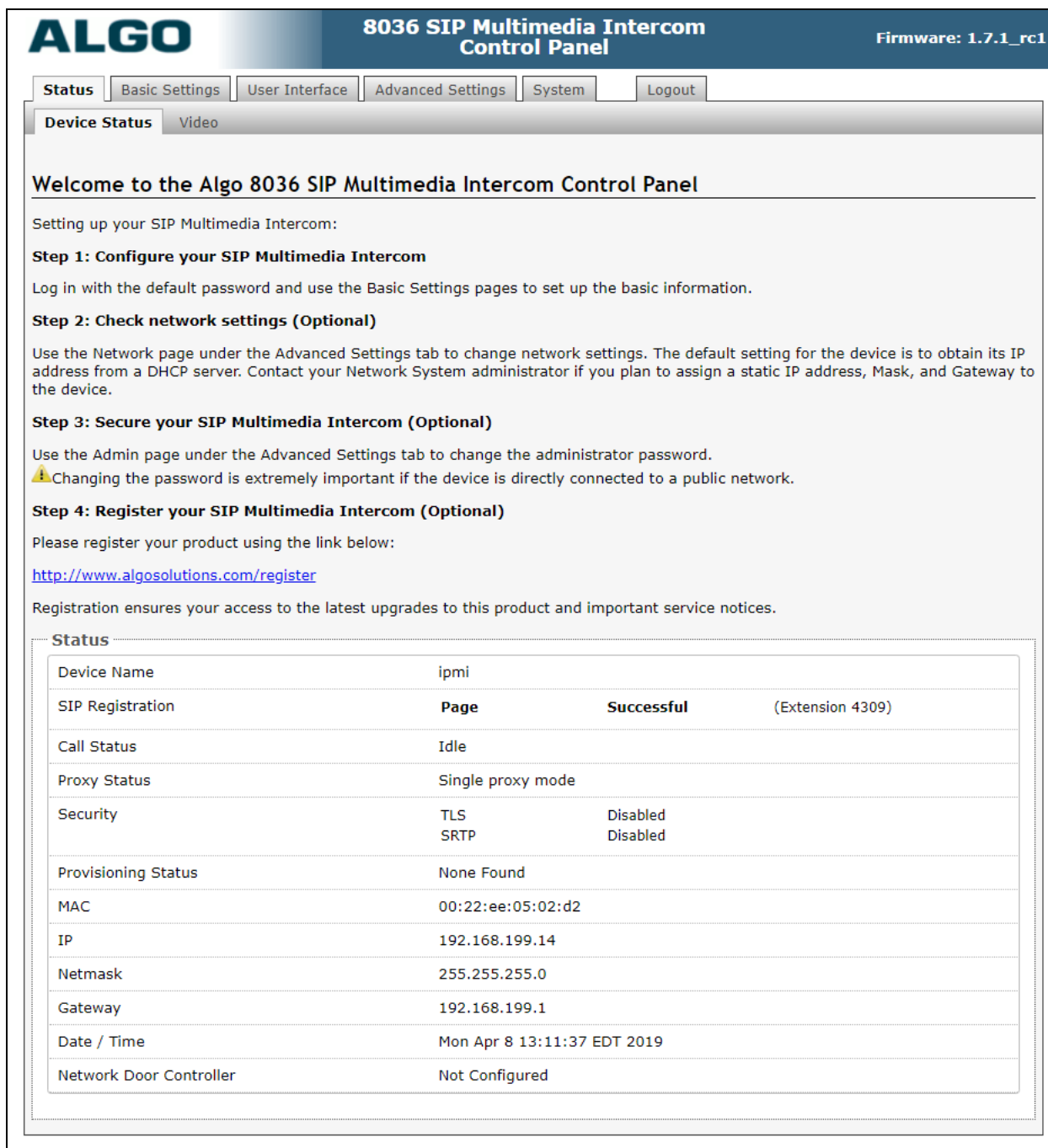
Total Registered: 3 Registered Status: [Progress Bar]

Extn Num	User Num	Phone Type	Security	Behind NAT	IP Address	Private Address	Transport	User Agent	Licensed
4306	4306	1140E_SIP	best effort		192.168.199.9		TCP	Avaya IP Phone 1140E (SIP1140e.04...	Avaya IP
4309	4309	SIP	disable		192.168.199.14		UDP	Algo-8036/1.7.1_rc1	3rd Party IP
SipRecExtn		Unknown	disable		0.0.0.0			UA?	Avaya IP

Display Options: Show All Registered UnRegistered Page 1 [Up/Down] Save Page Reset Phones Reregister Phones Cancel

7.2. Verify Algo 8036

From the 8036 web-based interface, select **Status** from the top menu. Verify that **SIP Registration** displays “Successful” in the **SIP Registration** as shown below.



The screenshot shows the web-based interface for the Algo 8036 SIP Multimedia Intercom. The top navigation bar includes the ALGO logo, the title "8036 SIP Multimedia Intercom Control Panel", and the firmware version "Firmware: 1.7.1_rc1". The main menu has tabs for Status, Basic Settings, User Interface, Advanced Settings, System, and Logout. The "Status" tab is selected, and the "Device Status" sub-tab is active. The page content includes a welcome message, a list of setup steps (Step 1: Configure your SIP Multimedia Intercom, Step 2: Check network settings (Optional), Step 3: Secure your SIP Multimedia Intercom (Optional), Step 4: Register your SIP Multimedia Intercom (Optional)), and a registration link. Below this is a "Status" section containing a table with various system parameters.

Status			
Device Name	ipmi		
SIP Registration	Page	Successful	(Extension 4309)
Call Status	Idle		
Proxy Status	Single proxy mode		
Security	TLS	Disabled	
	S RTP	Disabled	
Provisioning Status	None Found		
MAC	00:22:ee:05:02:d2		
IP	192.168.199.14		
Netmask	255.255.255.0		
Gateway	192.168.199.1		
Date / Time	Mon Apr 8 13:11:37 EDT 2019		
Network Door Controller	Not Configured		

The following tests were conducted to verify the solution between the 8036 and IP Office.

- Verify that when placing an outbound call from the 8036, an endpoint on the IP Office rings and a clear speech path is established.
- Verify that the solution works with different Avaya endpoint (e.g. digital, analog, IP etc) and that DTMF tones generated from these different endpoints are able to unlock the door release.
- Verify that the 8036 goes into an idle state when the call is completed.
- Verify that the 8036 can re-register without issues if the Ethernet cable is unplugged and plugged back in.

8. Conclusion

These Application Notes describe the procedures required to configure Algo 8036 SIP Multimedia Intercom to interoperate with Avaya IP Office Server Edition using as SIP 3rd endpoint. All the executed test cases passed and met the objectives outlined in **Section 2.1**, with some observations outlined in **Section 2.2**.

9. Additional References

This section references the documentation relevant to these Application Notes. Product documentation for Avaya IP Office, including the following, is available at:

<http://support.avaya.com/>

- [1] *Avaya IP Office Platform Solution Description*, Release 11.0, May 2018.
- [2] *Avaya IP Office Platform Feature Description*, Release 11.0, May 2018.
- [3] *IP Office Platform 11.0 Deploying Avaya IP Office Essential Edition*, Document Number 15-601042, Issue 33g, 20 May 2018.
- [4] *Administering Avaya IP Office Platform with Manager*, Release 11.0, May 2018.
- [5] *IP Office Platform 10.1 Using Avaya IP Office Platform System Status*, Document 15-601758, Issue 13a, 05 April, 2018.
- [6] *IP Office Platform 11.0 Using IP Office System Monitor*, Document 15-601019, Issue 09b, 10 May, 2018.

Additional Avaya IP Office documentation can be found at:

<http://marketingtools.avaya.com/knowledgebase/>

Product documentation for the Algo 8036 SIP Multimedia Intercom product may be found at:

<http://www.algosolutions.com/products/doorphones-security/8036/docs.html>

©2019 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.