biamp.™

CROWD MICS™

# Network Administrator's Guide

**Crowd Mics** is an audience engagement system comprised of mobile applications and a form-factor computer known as an ATOM. The application allows attendees of an event, such as a lecture, conference or company meeting to use their phones as a wireless microphone. It also allows text commenting to the moderator(s) as well as live polling. Events may be hosted online and locally.

This document is intended to guide network administrators and IT teams in successfully integrating a Crowd Mics system into a network environment.

## ATOM Network Characteristics

The ATOM has the following external connections for networking and A/V:

- Dual 100/1000Base-T Ethernet ports
- 2x HDMI connections (mirrored)
- Dual USB 3.0 ports (Type A)
- 1/8" unbalanced audio out
- Euroblock connector (balanced audio out)

## Network Prerequisites

For local events, the ATOM and all mobile devices (moderator and participants) must be connected to the same WLAN, and must be in the same subnet address range* in order to receive multicast inter-device discovery data.

**does not apply to manual device discovery*

- Each device must have an IP address provided by the WLAN, assigned via DHCP by default or via Crowd Mics configuration software or API.
- IP addresses are based on IPv4 (IPv6 not supported).

## Online Events

Events hosted online require purchase of a license. See licensing.biamp.com for details.

- Online participants need only be connected to the internet but will require a 'Join Code' to access the event. The event would also need to be broadcast via a conferencing application for live video/audio.

## Network Connection and Performance

Due to the potential that dozens of users will connect to the same WLAN to participate in a local event, Crowd Mics should be deployed on a professional, enterprise-grade wireless network to ensure optimal reliability/connectivity during an event.

## Deployment

An open WLAN between participants and the presenter is the recommended method to deploy Crowd Mics. This entails the participants' and moderator(s) being on the same wireless network/subnet and uninhibited communication on any port.

### Configuration Details

- IPv4 WLAN for moderator and participants
- Bonjour/mDNS allowed in the WLAN
- Client isolation/peer-to-peer blocking disabled (allow 'any-to-any' communication among devices on the WLAN.)

This configuration allows direct communication between the participants and the moderator.

## Deployment (continued)

### Manual Device Discovery Methods

Participants may connect to an ATOM by scanning a QR code shown in the Display application. This directs the user's Crowd Mic application to the ATOM's IP address.

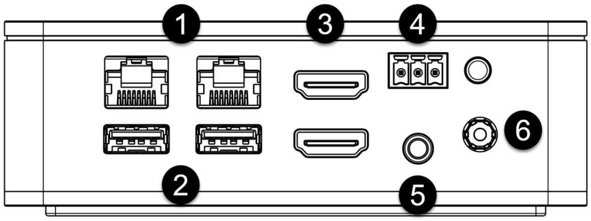
Connecting via QR code is convenient in a network where mDNS communication is not desired and restricted/blocked by the network administration.

If both the ATOM and the mobile device are in the same network yet the event is not automatically discovered by the Crowd Mics application, try using the QR code method or enter the ATOM's IP address manually.

Click this link or enter the following URL (**bia.mp/DisplayApp**) for information on enabling QRs/showing the IP address on the Display application.

## Physical Connections

1. Ethernet Ports - Control and User Networks
2. USB 3.0 (Type A)
3. HDMI
4. Euroblock Audio Connector
5. 1/8" (3mm) unbalanced Audio Out
6. Power



## Physical Connections (continued)

Connect the ATOM's power supply.

Connect HDMI, 1/8" balanced audio ports, USB and/or the Euroblock connector to the venue's A/V system. These connections may be used simultaneously in any combination.

Connect the user Ethernet network port to the venue's Wifi system. On the user side, the protocols are a combination of mdns-sd, webrtc, and http. Mobile devices will find the ATOM via mdns over wifi. atom.local broadcasts on the user port.

The second Ethernet network port is optionally used for control via SageVue and may be connected to the corporate LAN. The protocols on the control side are https and http.

Either port may be configured for network or control, but for consistency it is recommended that Port 1 be used for management (control) and Port 2 be used for connecting to the wireless network.

Both ports are on independent NICS, they are not switched, and the ATOM has been penetration tested to ensure isolation of the two ports. Once all connections are made, power up the ATOM.

Diagrams shown later in this document give typical network connection examples.

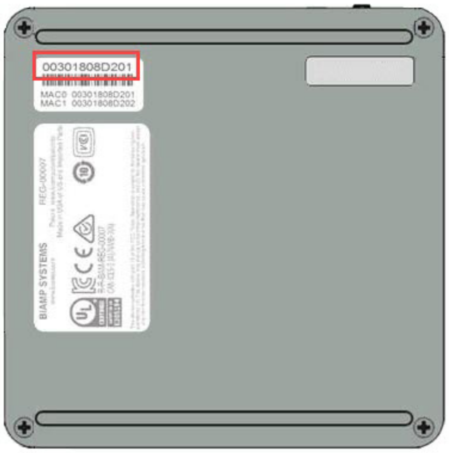
## ATOM Configuration

The ATOM is designed to deploy ‘out of the box,’ with no configuration needed, but is equipped with an advanced setup feature which allows users to access more advanced configuration options via a dashboard interface.

Make all physical connections as described previously. Connect to the ATOM configuration dashboard via a PC on the same subnet with the following URL:

**https://atom-XXXXXXXXXXXX.local**

X’s represents the MAC address of the ATOM and may be found on a label on the underside of the ATOM:



Alternatively, a user may navigate to the dashboard page via the IP address if it is known. A log in screen requires the following case-sensitive default credentials:

Username: **admin**

Password: **first four and last four characters of the device serial number.**

**IMPORTANT**: Any letters in the device serial number *must be entered in lowercase*.

From the dashboard, users have numerous options such as adjusting audio levels, changing language preferences, modify network preferences, etc.

Users may also connect to the ATOM via SSH while on the same subnet.

Alternatively, users may log into a terminal session directly on the ATOM. This requires direct connection of a keyboard and monitor to the ATOM.

Only one ATOM may be routed to a particular SSID.

## Network Ports

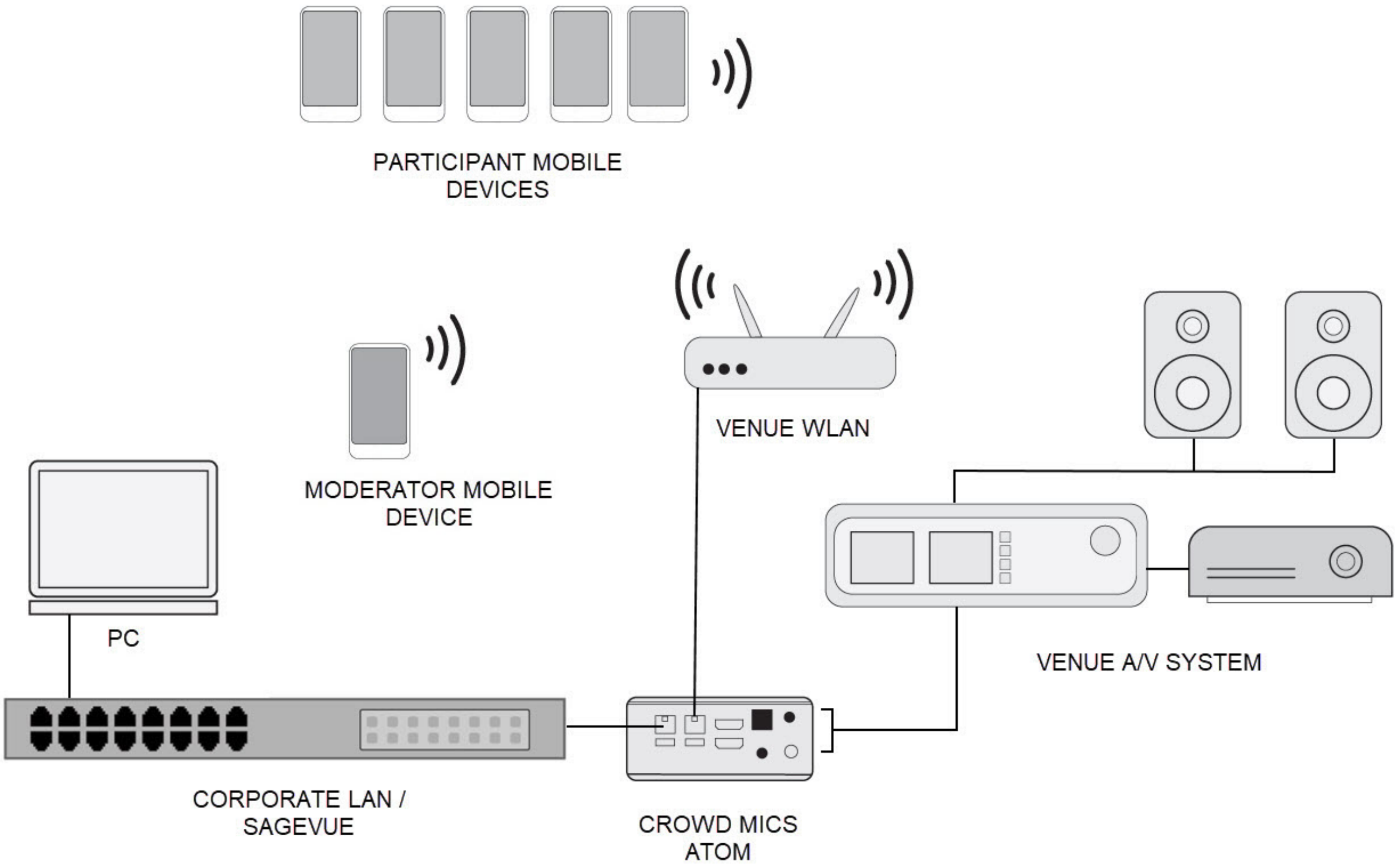
Some communication ports might be locked by default, typically for security reasons in routed or restricted network segments such as public wireless access for guests. For optimal operation of Crowd Mics, ports in the table that follows should be open and without restriction for the duration of the Crowd Mics event.

| Port | TCP/UDP | Protocol | Notes |
|---|---|---|---|
| *443 | TCP | HTTPS | Communication with the License Server and CrowdMics Media Services (using TLS 1.2) |
| 8888 | TCP | HTTP/Web Sockets | |
| †5353 | UDP | mDNS | |
| *3478/3479 | UDP/TCP | STUN/TURN | Communication with the STUN/TURN server for WebRTC ICE Exchange |
| *5349 | TCP | STUN/TURN | Communication with the STUN/TURN server for WebRTC ICE Exchange (using DTLS) |
| *19302 | UDP | STUN | Google Public STUN Server |
| *1024-65535 | UDP | SRTP | WebRTC Media Ports |

** In order to run Crowd Mics Online, the ATOM must have permissions for the ports and protocols noted with an asterisk in the table above.*

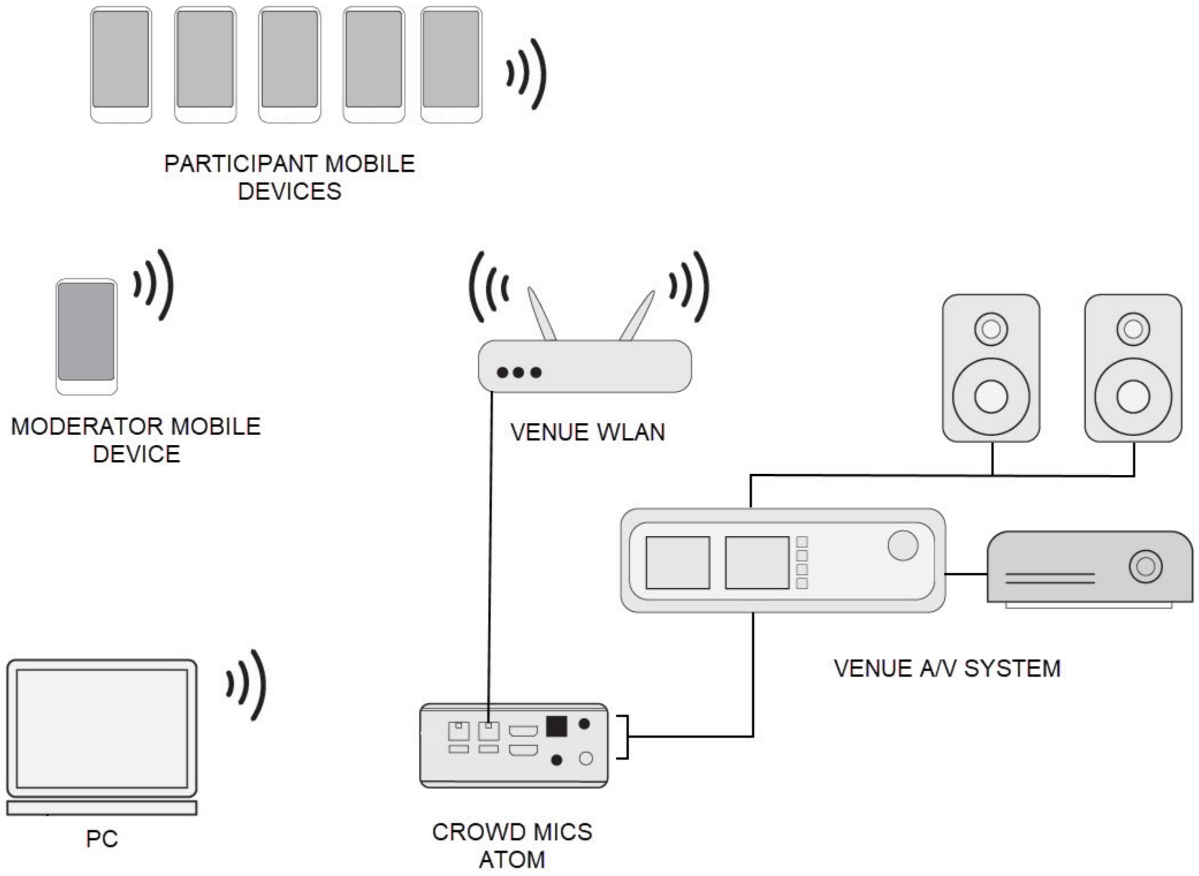
*† Port 5353 not required for manual device discovery methods.*

# Network Connection Diagrams



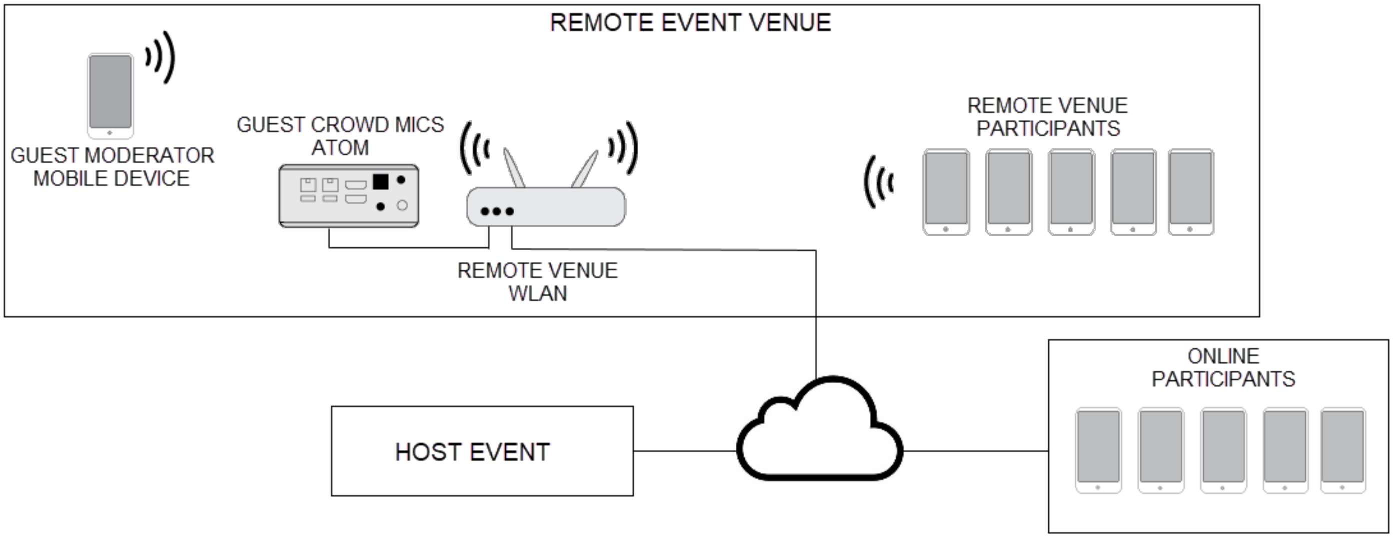
Typical Enterprise Network Connection Diagram

# Network Connection Diagrams



Typical Standalone Network Connection Diagram

# Network Connection Diagrams



Typical Online Event Connection Diagram

## Mobile Applications

There are two Crowd Mics mobile applications: one for the moderator and one for the participants. Participants should be informed in advance of the event in order to download the application. The moderator should set up any polling questions prior to the event.

Use the following QR codes to download the mobile applications.

Download on the App Store

Participant

Moderator

GET IT ON Google Play

Participant

## Support Websites

Visit sagevue-help.biamp.com or support.biamp.com for more information on configuring the ATOM via SageVue.

Visit crowd-mics-help.biamp.com for more information on set-up and configuration of Crowd Mics for local and online events.

**Contact:**

Email
support@biamp.com

Telephone
877-242-6796
+1-503-718-9257

www.biamp.com

biamp.
CROWD MICS