IXG Series Network Security Summary

Stations and Devices

All IXG Series stations are PoE and require a wired connection, with the exception of the Aiphone IXG Mobile App. Each station has flexibility with the choice of hardware and media. IXG Series stations must reside on the same logical network.

Entrance Station:	IXG-DM7-HID
Tenant Station:	IXG-2C7
Master Stations:	IX-MV7-*
Door Stations:	IX-DA, IX-BA, IX-DV, IX-DVF-*, IX-SSA-*
Mobile App:	Aiphone IXG *(IXGW-GW Gateway Adaptor Required)*
Adaptors:	IXGW-GW, IXGW-LC

Support Tool Software Information

Preinstallation Information

The IXG Support Tool is designed to batch configure all stations simultaneously, by finding each station on the network by its MAC address. The IXG Series is designed to function on managed, however, the broadcast method used to find stations during the programming process may require advanced network configuration or routing to function properly in this environment.

It is possible **Windows Defender or other firewalls and antivirus software may prevent this broadcast** search for stations. Typically, temporarily disabling these for a short time during the programming process prevents interruption or failure. Also, disabling all other network connections and adaptors during this time will ensure the PC sends the broadcast to the right location. **This includes Wi-Fi, VPN, and Bluetooth connections**.

It is recommended, when possible, that stations and the programming PC are placed on the same unmanaged network for initial programming. Once completed, the stations may be removed from this environment and deployed where needed.

Download and install the IXG Support Tool programming software. The latest version of Support Tool and IXG Series station firmware can always be found here *https://www.aiphone.net/support/software-documents/ixg/*

Support Tool and Line Supervision Software System Requirements

OS: Windows 7 *(Professional, Enterprise, Ultimate)*, Windows 8 *(Pro, Enterprise)*, Windows 8.1 *(Pro, Enterprise)* Windows 10 *(Home, Pro, Enterprise)*
CPU: 32 bit *(x86)* or 64 bit *(x64)* of 1 GHz or more
RAM: 4GB or more
Screen Resolution: 1280 x 768 or greater

ID and Passwords

Administrator ID: admin *(max. 32 characters)*
Administrator Password: admin *(max. 32 characters)*
Property Management ID: admin *(max. 32 characters)*
Property Management Password: admin *(max. 32 characters)*

Security and Communication

Security

The IXG Series supports the use of HTTPS and SSL/TLS (v1.0, 1.1, and 1.2), providing the ability to upload signed certificates to encrypt and secure authentication. Support Tool allows centralized certificate management, with the ability to upload CA certificates.

SSH is used when uploading a setting file to stations using the IXG Support Tool, but not during typical operation. *This is a critical function, therefore SSH cannot be disabled.*

IEEE 802.1X authentication is supported.

Hash Algorithms: **MD5**, **SHA1**, **SHA256**

Communication

SIP Connection Port: **5060**

Audio codec: **G.711** (**μ-law**, A-law)
Video codec: **H.264**/AVC, Motion JPEG

Video Encoder 1 (*Intercom Communication*)

RTP Video: Start **30000** - End 31000
RTP Audio: Start **20000** - End 21000

Video Encoder 2 (*Secondary HD Streaming*)

RTP Video: Start **32000** *(1-65534)* - End 33000 *(1-65535)*
RTP Audio: Start **22000** - End 33000

Minimum / Maximum Frame Rate (FPS): **1** / **30**
Minimum / Maximum Bitrate: **32** / **2048**
Minimum / Maximum Resolution *(Encorder 2)*: **320x240** / **1280x960**

Multicast

By default, IXG stations use Unicast when placing outbound calls to other stations, but may utilize Multicast in network environments that would benefit from the method. When Paging to more than 50 stations Multicast is required, and a Multicast address must be set in Support Tool. If Multicast is used, either for calling or when required for large paging groups, any address in the 224.0.0.0 to 239.255.255.255 range may be used.

Security and Communication

The information below contains the most common and critical ports and protocols for the IXG Series. Some are used only during the initial programming process, others during general use and optional feature functions.

Port	Type	Service or Protocol	Notes
5060	UDP	SIP communication between devices	
8740	UDP	Keep-alive during door release	
8620	SSL	Door release command	
65011	TCP	Option Relay Output control	
65030	UDP	Lift Control Adaptor control	
123	UDP	NTP	Required for IXGW-GW Gateway Adaptor and IXG Mobile App
53	UDP	DNS	Required for IXGW-GW Gateway Adaptor and IXG Mobile App
25	TCP	SMTP - Email notifications	
443	TCP	HTTPS over SSL (TLS) - Secure Web Access for certification server control	Required for IXGW-GW Gateway Adaptor and IXG Mobile App
22	TCP	SFTP over an SSH session - Setting File Upload	From programing PC to Stations during initial system configuration
8883	TCP	Secure MQTT - Call control server connection	Required for IXGW-GW Gateway Adaptor and IXG Mobile App
8700	UDP	Broadcast for Station Search and Association functions	From programing PC to Stations during initial system configuration
UDP	55550	Paging Delivery	
TCP	59900	Message Page Delivery	
UDP	65000	Multicast Paging Delivery	50 stations or more receiving a page
UDP	55552 - 56552	RTP Range used when paging	
UDP	65001	Multicast range for External Input Paging Delivery	
UDP	20000 - 21000 30000 - 31000	RTP Audio and Video ranges for Encoder 1	
UDP	22000 - 23000 32000 - 33000	RTP Audio and Video ranges for Encoder 2	The 32000 - 33000 range can be adjusted
UDP	10000-20000	RTP Audio and Video Transmission for IXG Mobile App	Required for IXGW-GW Gateway Adaptor and IXG Mobile App