AIPHONE® **APPLICATION NOTE**

IX Series 2 Network and Security Summary

Stations

IX Series 2 Master Stations: IX-MV7*, "IX Mobile" Mobile App.
IX Series 2 Video Door Stations: IX-DV, IX-DVF, IX-DVF-P, IX-DVF-4, IX-DVF-2RA, and IX-DVF-RA.
IX Series 2 Audio Only Door/Sub Stations: IX-SS-2G, IX-SSA, IX-RS IX-SSA-2RA, and IX-SSA-RA.

IX Series stations require a wired network connection (with the exception of IX Mobile), with some flexibility on choice of hardware and media. As the IX Series 2 stations are **peer-to-peer**, all station must reside on the same logical network.

Pre-installation IX Series 2 Network Information

The IX Series 2 utilizes the following IP address and port ranges by default. If a specific network requirement is not called out, then by default it is blank. All information may be customized unless otherwise stated.

Passwords

IX Support Tool ID: **admin** (maximum 32 characters)
IX Support Tool Password: **admin** (maximum 32 characters)
IX Stations ID: **admin** (maximum 32 characters)
IX Stations Password: **admin** (maximum 32 characters)

Note that the ID and Password for each IX station can be set using 'IX Support Tool' or by logging into the station via browser.

Network Addressing

The IX Series 2 offers Batch IP addressing or can be manually set for each device using the 'IX Support Tool'.

IPv4 address: **192.168.1.160** *(1.0.0.0-223.255.255.254)*
IPv4 Subnet Mask: **255.255.255.0** *(128.0.0.0-255.255.255.254)*
IPv4 Default Gateway: - *(1.0.0.0-223.255.255.254)*

IPv6: - *(2000::0-3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF or FD00::0-FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFFE*
IPv6 Default Gateway: - *(::FF:0-FEFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFE)*

Multicast Addresses (for Paging)**:**
Multicast IPv4: - *(224.0.0.0-239.255.255.254)*
IPv6: - *(FF10::0-FF1F:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF)*

DNS
Primary Server IPv4: - *(1.0.0.1-233.255.255.254)*
IPv6: - *(::FF:0-FEFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFE)*
Secondary Server IPv4: - *(1.0.0.1-233.255.255.254)*
IPv6: - *(::FF:0-FEFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFE)*

NTP IPv4: - *(1.0.0.0-223.255.255.255 or Hostname)*
IPv6: - *(::FF:0-FEFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFE or Hostname)*

Pre-installation IX Series 2 Network Information (Continued)

Supported Audio and Video Codecs

SIP Connection Port: **5060** *(1-65535)*

Video Encoder 1 (Intercom Communication)
RTP Video: Start **30000** *(1-65534)* End 31000 *(1-65535)*
RTP Audio 1: Start **20000** *(1-65534)* End 21000 *(1-65535)*

Video Encoder 2 (Secondary HD Streaming)
RTP Video: Start **32000** *(1-65534)* End 33000 *(1-65535)*
RTP Audio 2: Start **22000** *(1-65534)* End 33000 *(1-65535)*

Encoding

Audio codec: **G.711** (**μ-law**, A-law), G.722
Video codec: **H.264**/AVC, Motion JPEG

Packet Delivery: Unicast and Multicast

The IX Series 2 utilizes either unicast (default) or multicast to efficiently send video and paging announcements to group members. If multicast is selected as the method of transmission, ensure IGMP group creation and routing is available.

Note that multicast is required for "All Call" paging, regardless of the number of stations in the system.

Software System Requirements (IX Support Tool and IX Supervision Tool)

Operating System	Windows 7 Professional, Windows 7 Enterprise, Windows 7 Ultimate Windows 8, Windows 8 pro, Windows 8 Enterprise Windows 8.1, Windows 8.1 pro, Windows 8.1 Enterprise Windows 10 Home, Windows 10 pro, Windows 10 Enterprise Windows 10 Education
CPU	32 bit (x86) processor or 64 bit (x64) processor of 1GHz
Memory	4 GB RAM
Resolution	1280x768

Security

The IX Series 2 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.

OpenSSH is used when uploading a setting file to IX stations using the IX Series 2 Support Tool. This is a critical function, therefore OpenSSH cannot be disabled.

IEEE 802.1X authentication is supported.

Browser-based configuration is protected by username and password, secured by HTTPS.

Ports and Protocols

Protocol	Port	Adjustable	Function
HTTP	80	No	Accepts CGI commands
HTTPS	443	No	Web configuration interface + HTTPS CGI commands
SIP	5060 (UDP)	Yes	Station to station communication, SIP server communication.
RTP	20000 - 30000 ranges	Yes	Audio and Video
RTCP	20000 - 30000 ranges	Yes	
RTSP	10080	Yes	
IGMP		—	Join and leave requests based on SDP information
MLD		—	Join and leave requests based on SDP information
SFTP	22	No	Setting file upload. Only used during station programming process.
SMTP	25	Yes	Email (requires DNS)
DHCP	68	No	DHCP client
NTP	123	Yes	Network Time
DNS	53	No	DNS for email domain name lookup
Paging	55550 (UDP)	No	IX Series paging control messages
Paging	55552 and up (UDP)	No	IX Series paging audio
SIF	10000 (TCP)	Yes	Sends SIF event messages
Door Release	8620 (TCP)	No	Door release between two IX Series stations
App Server	5061	Yes	IX Mobile presence detection with IXW-MA (or RY-IP44)
Support Tool Search and Associate	8700 (UDP)	No	All subnet broadcast, only MAC address in message reacts to association, all respond to a station search. Only used during station programming process.
IXW-MA Destination Port	65014	No	

Best Practices

Using the IX Support Tool

Each intercom can have its own Admin ID and password as well as a User ID and password. These are typically managed via the IX Support Tool, but can be changed in the web interface. The IX Support Tool has its own ID and password, as well.

The IX Support Tool generates files that are sensitive from a security standpoint. The IX Support Tool should be located on a PC that normal users will not access. While these files are transported safely to their intended destinations, the storage of these files is not secure. Similar to a normal user is not having physical access to the file server, a normal user should not have physical access to the PC running the IX Support Tool.

IX Mobile relies on having an accurate configuration file generated by the IX Support Tool. If a user wants the configuration file, the best way to deliver it is through a secure method, such as putting the configuration file on a secured FTP server or a secure file server. These files contain specific passwords stored in plain text. An experienced user could read this configuration file and discover the admin password for the mobile app. Consider protecting mobile devices with encryption, pin codes, and remote wipe capabilities.

Interference with Other Network Devices

It is possible, although highly unlikely, that an IX Series station can interact with unregistered and unknown network devices, such as IP cameras, Video Management Systems, and Network Video Recorders. This typically occurs when a network device, such as those previously mentioned, attempt to communicate to an IX series station without being known to the station. In these rare cases, it is possible that the station may become unresponsive or reboot. Take necessary precautions when adding an IX series station to an existing network or security VLAN.

Using a Browser

When using a browser to make changes, be aware of the possibility of a Man in the Middle (MitM) attack if the browser makes a connection using anything other than TLS 1.2. The IX Series stations will accept incoming legacy SSL 3.0, TLS 1.0, and TLS 1.1 connections, however these are not secure against MitM attacks. Never enter your admin ID and password using a browser connected with these protocols.

Aiphone does not recommend configuring IX Series stations using their web interface. This option should only be used when necessary, with the exception of the IX-1/10AS, IX-PA, and the RY-IP44, which have some settings that must be configured using a browser.

IX Series Stations: Outside of a LAN, the best way to modify an IX Series system is to remotely access the PC running the IX Support Tool, then launch the IX Support Tool and make changes. Use a Remote Access system the administrator feels is secure. Launch a web browser on the remotely controlled PC running the IX Support Tool to change the configuration for any station, if required.

IX-1AS, IX-PA, RY-IP44: Do not modify the configuration of these adaptors outside of the LAN. Inside a LAN, passwords protect the configuration from local users. These devices do not use SSL or TLS, nor do they accept SSH configurations from the IX Support Tool. Ensure no one except the administrator will have access to the web configuration port (port 80). This is typically done using access control lists, isolated VLANs, or similar security measures.