
Network Security Summary

Stations and Devices

IX|IXG Series stations require a PoE connection for communication and power.

| | |
|---------------------|--|
| Entrance Station: | IXG-DM7-HID(A) |
| Answering Stations: | IXG-2C7, IX-MV7-*, IX-RS-*, IXG-MK, IX-SOFT |
| Door Stations: | IX-EA, IX-DV, IX-DVF-*, IX-DVM, IX-SSA-*, IX-SS-2G |
| Adaptors: | IXGW-(T)GW, IXGW-LC, IXW-MA(A) |
| Mobile App: | “Aiphone IXG” |

Programming Information

There are two methods that can be used to configure IX|IXG equipment. One is IXG Support Tool, which is software that is installed on a local PC. Sites using the IXGW-(T)GW gateways can access AiphoneCloud, which allows for remote programming from any location.

Both of these methods are used to batch configure all stations simultaneously by finding each station on the network by its MAC address. The IX|IXG Series is designed to function on managed or enterprise-level networks. However, the broadcast method used to find stations during the programming process may require advanced network configuration to allow network-wide broadcasts.

It is possible **Windows Defender or other firewalls and anti-virus software may prevent this broadcast search for stations**. If this occurs, make a rule in the firewall for IXG Support Tool.

It is recommended that stations are set up on the same unmanaged switch for initial configuration. Once the IP addresses have been set, the stations may be removed from this environment and deployed to the network.

Remote Management can be accessed at: <https://aiphone.cloud>

Alternatively, download and install the IXG Support Tool programming software. The latest version of Support Tool and IX|IXG Series station firmware can be found at the links below.

IXG Support Tool: <https://www.aiphone.com/IXG-SupportTool>
Firmware Upgrades: <https://www.aiphone.com/kbtopic/firmware>

Support Tool and Line Supervision Software Minimum System Requirements

OS: Windows 7 (Professional, Enterprise, Ultimate), Windows 8 (Pro, Enterprise), Windows 8.1 (Pro, Enterprise), Windows 10 (Home, Pro, Enterprise), Windows 11 (Home, Pro, Enterprise)

CPU: 32 bit (x86) or 64 bit (x64) at 1 GHz or higher

RAM: 4GB or more

Screen Resolution: 1280 x 768

Support Tool and Line Supervision Software Default ID and Passwords

Administrator ID: admin (*up to 32 alphanumeric characters*)

Administrator Password: admin (*must be changed after first use, up to 32 alphanumeric characters*)

Property Management ID: admin (*up to 32 alphanumeric characters*)

Property Management Password: admin (*must be changed after first use, up to 32 alphanumeric characters*)

Security and Communication

The IX|IXG Series supports the use of **HTTPS** and **TLS (v1.2)**, providing the ability to upload signed certificates to encrypt and secure authentication. IXG Support Tool allows centralized certificate management with the ability to upload **CA certificates** to stations.

SSH (SFTP over SSH) is used when uploading a setting file to stations, but not during typical operation. This is a critical function, therefore SSH cannot be disabled.

HTTPS is used when uploading to the IXG Cloud server. This may require whitelisting the following URL:
***.ap-northeast-1.amazonaws.com** (this * is a wildcard representing multiple subdomains).

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 (Encoder 2): 320x240 / 1280x960

IXGW-GW Cloud Communication: TLS 1.2 is used to setup encrypted connections with allowed cipher suites ECDHE-ECDSA-AES128-GCM-SHA256 and ECDHE-RSA-AES128-GCM-SHA256. Certificates are set to automatically renew with AWS Certificate Manager.

By default, **IX|IXG Series 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 *(continued)*

Addressing

The IX|IXG Series offers batch IP addressing or can be manually set for each device using IXG Support Tool or Remote Management. Most IX|IXG Series stations are set to the same default static IP address, 192.168.1.160. The IXGW-TGW uses 192.168.1.161. These can be manually changed or set to DHCP during the programming process.

IPv4 (most stations): 192.168.1.160 (1.0.0.0-223.255.255.254)

IPv4 (IXGW-TGW): 192.168.1.161 (1.0.0.0-223.255.255.254)

Subnet Mask: 255.255.255.0 (128.0.0.0-255.255.255.254)

Default Gateway: - (1.0.0.0-223.255.255.254)

IPv6: - (2000::0-3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF or
FD0::0-FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFFE)

IPv6 Default Gateway: - (::FF:0-FE9F:FFFF:FFFF:FFFF:FFFF:FFFF:FFFFE)

DNS Primary Server IPv4: - (1.0.0.1-233.255.255.254)

IPv6: - (::FF:0-FE9F:FFFF:FFFF:FFFF:FFFF:FFFF:FFFFE)

Secondary Server IPv4: - (1.0.0.1-233.255.255.254)

IPv6: - (::FF:0-FE9F:FFFF:FFFF:FFFF:FFFF:FFFF:FFFFE)

NTP IPv4: ntp.jo.aiphone-app.net (1.0.0.0-223.255.255.255 or Hostname)

IPv6: - (::FF:0-FE9F:FFFF:FFFF:FFFF:FFFF:FFFF:FFFFE or Hostname)

LTE Connection

The IXGW-TGW Mobile App Gateway can be used to connect the IX|IXG system to a 4G LTE mobile network, using the included SIM card. This connection can be used as a primary network connection for the system, or as a backup to the ethernet connection. The SIM card also allows for calls to a single phone number on each call from an entrance station or door station.

Supported Networks: AT&T® (requires activation of included AT&T SIM card). Third-party SIM cards are not supported.

Additional IXG App and Remote Management Information

A reachable DNS and NTP server must be assigned to the IXGW-(T)GW Mobile App Gateway. A public DNS server, such as 8.8.8.8, may be used. Note that the IXG Support Tool has a preset NTP server for the IXGW(T)-GW Gateway. However, this NTP server is based in Japan, so using a local NTP server is recommended.

Outbound communication is required for the IXG Mobile app and/or Remote Management to function. Please whitelist the following outbound hostnames and ports:

*.ixg.aiphone-app.net : 443
iot.prod.aiphone.cloud : 8883
ixgw-gwapi.prod.aiphone.cloud/v1/gwprovisioning : 443
ixgw-gwapi.prod.aiphone.cloud/v1/gwresults : 443
*.compute-1.amazonaws.com : 10000-20000
If using an external DNS server: 53
If using an external NTP server: 123

*: wildcard representing multiple subdomains

Ports and Protocols

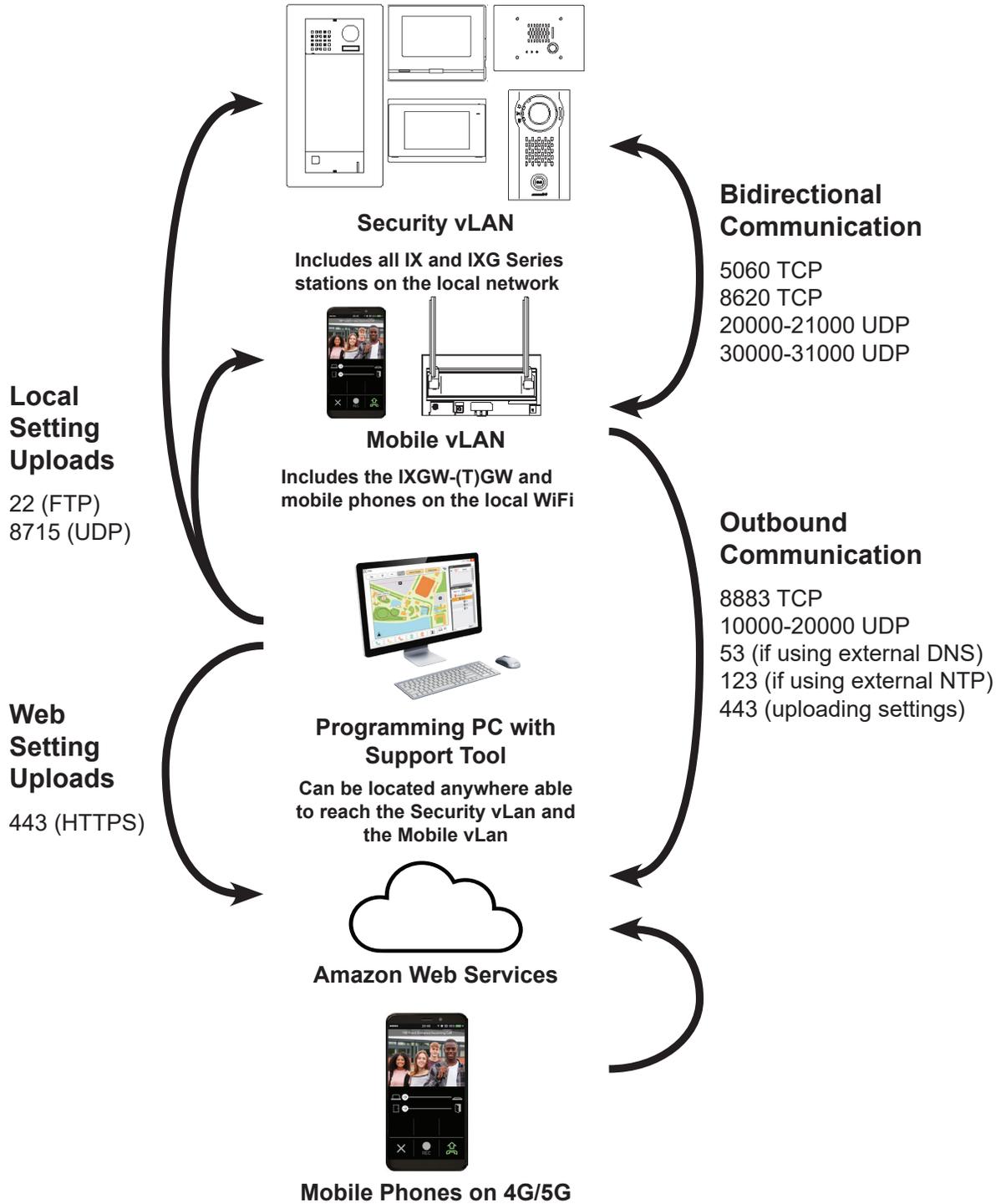
The information below contains the most common and critical ports and protocols for the IX|IXG Series. Some are used only during the initial programming process, others during general use and optional features.

| Port | Type | Service or Protocol | Notes |
|--------------------------------|------|--|---|
| 5060 | UDP | SIP | For establishing a call |
| 8740 | UDP | Keep-alive during door release | |
| 8620 | TLS | Door release command | Encrypted Door Release with TLS 1.2 |
| 65011 | TCP | Option Relay Output control | |
| 65014 | UDP | SIF | IXW-MA(A) Destination Port |
| 65030 | UDP | Lift Control Adaptor control | |
| 65060 | UDP | SIF | Acquire IX-SOFT License from IXW-MA(A)-SOFT |
| 123** | UDP | NTP | IXGW-(T)GW Gateway must have an assigned NTP server address to function |
| 53** | UDP | DNS | IXGW-(T)GW Gateway must have an assigned DNS server address to function |
| 25 | TCP | SMTP | Email notifications |
| 443 | TCP | HTTPS (TLS 1.2) | Secure Web Access for certification server control |
| 22* | TCP | SFTP over an SSH session | Setting File Upload to intercom stations from IXG Support Tool or IXGW-TGW via AiphoneCloud |
| 8883** | TCP | Secure MQTT | Call control server connection to Cloud Server |
| 8700* | UDP | Broadcast | Station Search and Association functions with Support Tool |
| 8715 | UDP | Aiphone Proprietary | Command functions to intercom stations from IXG Support Tool or IXGW-TGW via AiphoneCloud |
| 55550 | UDP | Paging Delivery | |
| 59900 | TCP | Message Page Delivery | |
| 65000 | UDP | Multicast Paging Delivery | |
| 55552 - 56552 | UDP | RTP Range used when paging | |
| 10000-20000** | UDP | SRTP/SRTCP, DTLS, ICE(STUN) | IXGW-(T)GW and IXG Mobile App cloud server communication |
| 20000 - 21000 30000 - 31000 | UDP | RTP Audio and Video ranges for Encoder 1 | Intercom to Intercom communication |
| 22000 - 23000 32000 - 33000 | UDP | RTP Audio and Video ranges for Encoder 2 | Intercom to 3rd Party Streaming |

* IXG Support Tool function / ** IXG App functionality

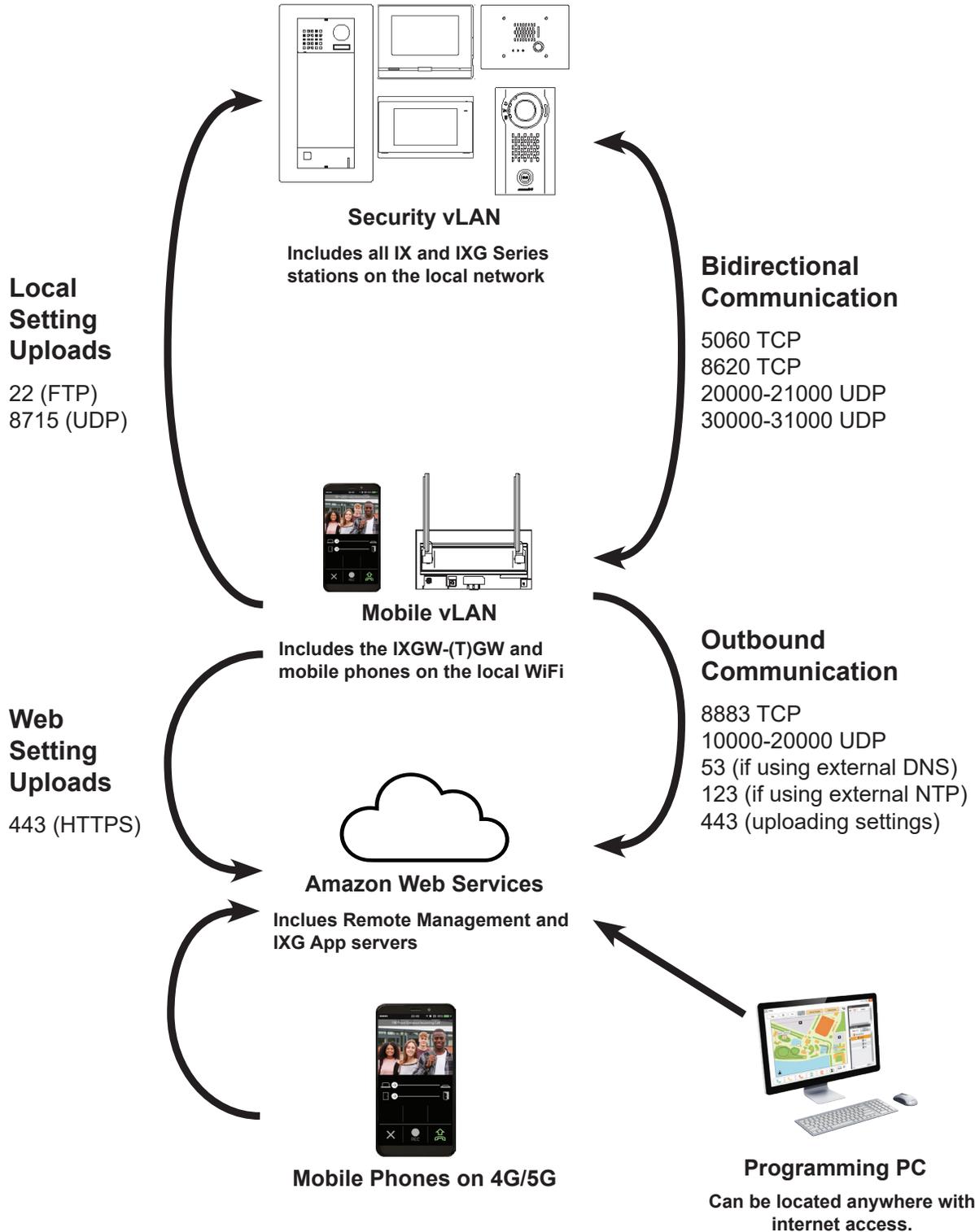
IXGW-(T)GW Network Flow Chart (IXG Support Tool)

This Flow Chart shows the expected communication for an IXGW-(T)GW when calling from a door or entrance station to an off-site mobile app, as well as the network connections used by local programming PC running IXG Support Tool. The Amazon Web Services servers used to make this connection can vary based on physical location, time of day, and server load.



IXGW-(T)GW Network Flow Chart (Remote Management)

This Flow Chart shows the expected communication for an IXGW-(T)GW when calling from a door or entrance station to an off-site mobile app, as well as how a remote PC can access Remote Management to program the system. The Amazon Web Services servers used to make this connection can vary based on physical location, time of day, and server load.



For more details about the features and information above, please contact Technical Support.