

## IQIP24 INFORMATION FOR

# IT Managers and Network Administrators

## DESCRIPTION

IQIP24 is the secure, dual path alarm signaling and CCTV monitoring service designed for modern IP networks. IQIP24 ensures an 'always on' connection between the AGW (AlarmGateWay) and the 24 hour response centre – ensuring that all alarms always get through. For double protection the AGW uses two means of communication: it connects into the customer's existing broadband/IP network for the primary and wired communication path, it also connects to the best available GPRS network for the wireless, secondary path, using global roaming for optimum coverage from multi providers.

## CONNECTIVITY

The AGW uses **outbound TCP/IP connections only**, in the IP destination port range 18000 through to 18049, via the landline IP (Ethernet) and the GPRS IP networks. The AGW does not accept inbound connections and does not require any inbound IP ports to be opened on a customer firewall / router. GPRS connectivity is established via a private network connection (APN), and no internet connectivity is possible via GPRS in the AGW. No connectivity exists between the GPRS IP and landline IP networks in the AGW and no IP bridging is therefore possible and permitted between the networks in the AGW. The AGW also contains an internal firewall to isolate the AGW from any unauthorized inbound connections or IP traffic.

## SPECIFICATIONS

<b>Data traffic</b>	140 Bytes per poll • 10 Mbytes or less per month (grade 2)
<b>Firewalls</b>	The AGW does not interfere with network firewall operation or settings.
<b>IP Address</b>	As supplied the AGW is DHCP enabled. The AGW can also operate using a static IP address. Where a static IP address is required, this can be registered in the AGW using the GPRS path (remotely). No LAN connect needed to change the LAN IP address. (Network admin friendly and reusable for relocation)
<b>Ports</b>	Ports 18000 to 18049 open to <u>outbound</u> TCP/IP connections. • The AGW does not require any inbound IP ports to be opened/forwarded.
<b>Security</b>	The AGW does not interfere with the customer's security settings or operations. (MAC Address filtering could however need additional LAN settings to the LAN port)
<b>Power consumption</b>	Power Supply Requirements 12 VDC (ripple < 200mV) • Current typical 320ma and 350ma max. To be provided by existing Alarm Panel.
<b>Network performance</b>	The AGW does not interfere with broadband or network performance. No QoS settings needed.
<b>GPRS</b>	Non bridging private GPRS using global roaming SIM, data-usage included in service. No additional cost, activation, administration or management needed. Remote diagnostics on signal-strength.

## ADDITIONAL INFORMATION

The AGW complies to EN-50136 and 50131, suitable for alarm signaling up to grade 4. The Dual-Path principle relieves installers from placing additional back-up power to the active network components and the shielding of primary network-cabling, leaving infrastructure physically untouched and preventing liability issues. The full-outbound principle further reduces the need for support from IT staff to installer, concerning routing and firewall settings etc. The AGW is defaulted to communicate to the IQIP24 Platform only, this cannot be configured by installer. It uses the available route in the network, whether this is public internet or any other (private) connection to the IQIP24 platform.

The AGW is preferably placed in the alarm panel enclosure itself or adjacent to it in the cabinet. Again no interference with ICT network infrastructure or management. The AWG needs one LAN port (10/100 auto) only with outbound internet access on given ports.

The AGW is remotely manageable by Private GPRS to adjust network LAN settings on infrastructural changes by network/ICT management.

Alarm panel is non-TCP/IP Connected to the AGW. All TCP/IP traffic is physically limited to the non-bridging AGW only. Remote management to the panel is possible using a virtual modem by the installer. Access control however is done on double outbound (AWG and Installer) connections to the IQIP24 Platform. No need for ICT management to deliver special access privileges for remote management of panel and/or AGW.

For specific network situations, direct (private)connections can be made to the IQIP24 Platform using PPoE, Proxies and/or VPN connectivity directly between managed (private) network en IQIP24 Alarm Platform.

All platform communication is highly AES128 encrypted and further done within a proprietary IQIP24 protocol. Package sniffers could detect this as “unknown” and reject/alert traffic from the AGW to the IQIP24 Platform. If needed IQIP24 can provide IP Address series to the IQIP24 Platform to create appropriate rules within the “package sniffer/filter” appliance. Destination addresses can however vary in time. Preferred is a rule based on local-outbound traffic/addresses.

## PLATFORM MAP

