kontakt.io

Portal Light network requirements

The Portal Light, available in three models, is Kontakt.io's Bluetooth® Low Energy (BLE) to Wi-Fi gateway. It receives and aggregates data from Kontakt.io BLE tags and infrastructure devices, transmitting this data to the Kio Cloud platform over a local Wi-Fi network. Additionally, Portal Lights deliver over-the-air (OTA) firmware and configuration updates.

To allow Portal Light connectivity to the local Wi-Fi network and the Kio Cloud platform, specific network requirements must be met. The following information outlines these requirements, including the supported network communication protocols, firewall configurations, and port settings.

Network communication protocols

To meet network security and protocol standards, the Portal Light supports an array of options for secure network connectivity.

- Wireless networking protocols: 802.11 b/g/n (802.11n up to 150 Mbps) | Portal Light: 2.4 ~ 2.5 GHz | Portal Light 2 models: 2.4 and 5 GHz
- Wireless security protocols: Open, WEP, WPA (TKIP & AES), WPA2 (TKIP & AES) - Personal and Enterprise modes
- Wireless authentication protocols: EAP-TLS, PEAPv0/EAP-MSCHAPv2, EAP-TTLS/MSCHAPv2
- Network communication protocols: Hypertext Transfer Protocol Secure (HTTPS)/TLS 1.2
- IP addressing: Dynamic Host Configuration Protocol (DHCP)
- Data Packet Size: typically less than 6 kilobytes (kB) per second
- Captive portal and web-based login pages requiring a username/password are not supported.

Network firewall requirements

The Kio Cloud platform runs on the Amazon Web Services (AWS) cloud infrastructure. Organizations with network firewalls in place must proactively allow outbound network communication and file downloads through specific Kio Cloud Domains and URLs.

IMPORTANT
Kio Cloud is a high-availability (HA) platform that may change IP addresses at anytime. Therefore, the use of firewall IP addressing filtering is not supported.

kontakt.io

If the firewall support wildcards:

	US (United States) environment	UK (United Kingdom) environment
Domain filters	*.api.kontakt.io *.event.cloud.us.kontakt.io *.software.kontakt.io *.gateway.cloud.us.kontakt.io *mqtt.cloud.us.kontakt.io:443	*.dm-api.cloud.uk.kontakt.io *.event.cloud.uk.kontakt.io *.software.kontakt.io *.gateway.cloud.uk.kontakt.io *mqtt.cloud.uk.kontakt.io:443
URL filters	https://*.kontakt.io	https://*.kontakt.io

If the firewall does not support wildcards:

	US (United States) environment	UK (United Kingdom) environment
Domain filters	api.kontakt.io event.cloud.us.kontakt.io software.kontakt.io gateway.cloud.us.kontakt.io mqtt.cloud.us.kontakt.io:443	dm-api.cloud.uk.kontakt.io event.cloud.uk.kontakt.io software.kontakt.io gateway.cloud.uk.kontakt.io mqtt.cloud.uk.kontakt.io:443
URL filters	https://api.kontakt.io https://event.cloud.us.kontakt.io https://software.kontakt.io https://gateway.cloud.us.kontakt.io mqtts://mqtt.cloud.us.kontakt.io:443	https://dm-api.cloud.uk.kontakt.io https://event.cloud.uk.kontakt.io https://software.kontakt.io https://gateway.cloud.uk.kontakt.io mqtts://mqtt.cloud.uk.kontakt.io:443

NOTE

api.kontakt.io | dm-api.cloud.kontakt.io | mqtt.cloud.[us or uk].kontakt.io:443 > Used by Kio Cloud APIs, SDKs, Stream integration, Kio Setup Manager

event.cloud.us.kontakt.io | event.cloud.uk.kontakt.io > Used for Portal Light data transmission

software.kontakt.io > Used for Portal Light firmware distribution updates

gateway.cloud.us.kontakt.io | gateway.cloud.uk.kontakt.io > Used as Proxy server for the apiHost and dataHost

kontakt.io

Network port requirements

Portal Lights communicate with Kio Cloud over the facility's network using the HTTPS protocol. All data is encrypted in transit and at rest. A Portal Light establishes an outbound HTTPS connection and releases its IP address once the connection is complete.

The following ports must be open to enable outbound communication from the facility network.

- **Port TCP 443:** Enables secure HTTPS communication with Kio Cloud over TLS/SSL.
- **Port UDP 123:** Allows Portal Lights to synchronize with external Network Time Protocol (NTP) servers (e.g., pool.ntp.org, time.google.com).

> **NOTE**
> An internal NTP server may also be used.

Portal Light deployment recommendations for use in enterprise networks

When deploying Kontakt.io Portal Lights within an enterprise network, Kontakt.io recommends the utilization of a Virtual Local Area Network (VLAN) to optimize security, streamline operations, and simplify management for your IoT ecosystem. Using VLANs for specific IoT (Internet of Things) devices in an enterprise environment, including not relying solely on MAC address filtering, offers several benefits that contribute to better security, performance, and management of the network.

By placing Kontakt.io Portal Light devices on a VLAN, there are several key advantages including:

- **Complete Network Isolation.** The setup ensures a clear demarcation between the standard corporate network and IoT devices. This guarantees that data traffic associated with employee or patient data remains entirely separate from IoT device data.
- **Prevention of Unauthorized Access.** The arrangement eliminates any possibility of IoT devices gaining access to network file servers, printers, code repositories, or other resources not specifically designated for IoT devices. This ensures that IoT devices can only see the other IoT devices.
- **Zero Additional Cost.** The implementation of this solution does not require the incorporation of extra network infrastructure. Modern networking equipment, including a single set of Wireless Access Points, can efficiently serve multiple VLANs created for distinct purposes, such as accommodating IoT devices.
- **Customized Configuration and Security**. The IoT VLAN can be tailored to the unique requirements of IoT devices. This configuration, encompassing SSIDs, passwords, firewall rules, etc., has no bearing on the corporate network. For instance, the IoT network can be restricted to communication with approved URLs, while the corporate network retains more lenient policies to facilitate unrestricted access for employees and other users.
- **No Need for Whitelisting.** While it's feasible to manually whitelist IoT devices using their MAC addresses and then configure corresponding firewall rules, this approach is both unwieldy and prone to errors. A more effective strategy involves segregating IoT devices on their own VLAN, thereby establishing a comprehensive security protocol for the entire IoT network. This avoids complications arising from incorrect MAC address configurations when devices are replaced or added over time.