



IP access and authorization

Many messaging connections only accept traffic from approved public IP addresses. This guide explains how to find the right address and how to request access.

Educational guide. There is no online IP check, self-service allow-list or OTP verification on this website. IP access for existing connections is arranged by email with our support team.

Online version: <https://wisenetwork.co/support/ip-access/> · Content updated 28 October 2026

Why providers restrict IP addresses

An IP allow-list (also called a whitelist) is a list of public addresses permitted to connect. It adds a second barrier: stolen credentials alone are not enough, because the attacker must also connect from an approved address. It does not replace credentials, and it must be kept up to date when your network changes.

Public and private addresses

Computers inside an office or data centre usually have private addresses, such as 10.x.x.x, 172.16.x.x to 172.31.x.x or 192.168.x.x. These are not visible on the internet. When they connect out, a router or firewall translates them to a public address (network address translation, NAT). The provider only ever sees the public address, so that is the one to register.

Where your public address comes from

Where your system runs	Public address seen by the provider
Office network	The office router or firewall's public address.
Dedicated or virtual server	The server's public address, unless traffic leaves through another gateway.
Cloud platform	The NAT gateway or static outbound address configured for the service. Auto-assigned addresses can change.
Containers or serverless functions	Usually a shared gateway address. Configure a fixed outbound address first.
Mobile or home internet	Often shared and changing (carrier-grade NAT). Not suitable for allow-listing.

Find the address your system really uses

Check from the machine that will send the traffic, not from your own laptop. Opening an "what is my IP" web page in your browser shows the address of the network you are browsing from, which is often different from your server's.

- Ask your network administrator, hosting or cloud provider for the outbound public addresses, including failover and disaster-recovery sites.
- Or run a query from the server itself. For example, a widely used DNS query returns the public address of the machine that runs it:

Example commands for Linux (first line) and Windows (second line). They use a third-party DNS service, not Wise Network.

```
dig +short myip.opendns.com @resolver1.opendns.com  
nslookup myip.opendns.com resolver1.opendns.com
```

Write addresses in standard notation. A single IPv4 address looks like 203.0.113.10; a range uses CIDR notation, such as 203.0.113.0/28 for 16 addresses. IPv6 addresses look like 2001:db8::10. These examples use ranges reserved for documentation ([RFC 5737](#), [RFC 3849](#)). Confirm with the provider whether IPv6 is accepted.

Request access from Wise Network

For an existing or planned connection, email support@wisenetwork.co with:

- Your company name and the service or account concerned.
- Each public IP address or range, and whether it is primary, failover or for testing.
- The date the addresses should be added, and any old addresses to remove.
- A technical contact for confirmation.

We may confirm the request with your registered contact before changing access. Never include passwords or keys in the email.

Self-service IP check and OTP verification

Some providers offer a page that shows the visitor's address and adds it to an allow-list after a one-time passcode (OTP) check. Wise Network does not offer this. A safe version needs a messaging backend, verified account ownership, OTP delivery, rate limits, audit logs and approval rules, because simply showing an address is not proof of authorization. Until such a service exists, use the email process above.

Questions? Email support@wisenetwork.co. This PDF is generated from the web page above; the online version is the reference.