



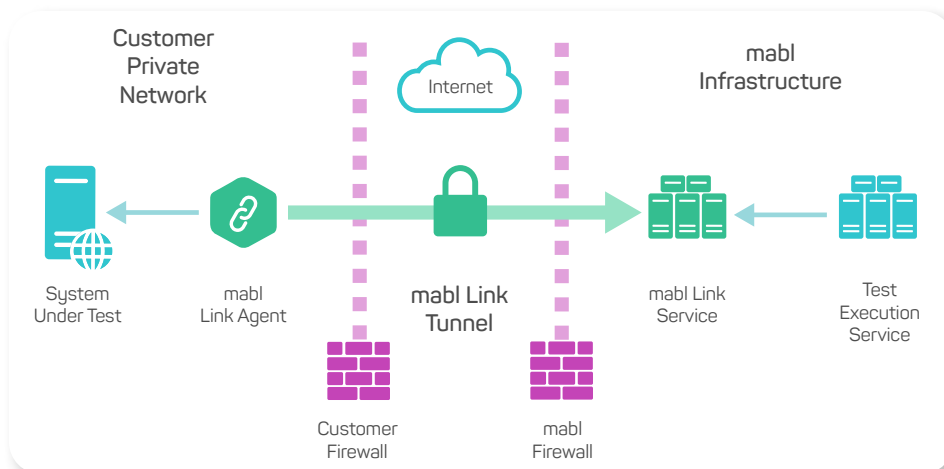
mabl Link Guide

Enabling mabl to securely connect to your web applications for automated testing

What is mabl Link?

mabl Link is a reverse proxy that makes it simple to establish a secure tunnel between your private network and mabl's servers in Google Cloud. This tunneling solution enables you to easily run tests against internal environments such as staging and localhosts.

To get started testing through mabl Link, simply install the Link agent on either a server or a computer within your network. Once the agent is up and running, mabl will be able to test against any web application the machine can access.



Who can help install mabl link?

Internal teams who oversee:

- Networking
- Proxies
- Firewalls
- Security
- Content
- IT

mabl Link Highlights:



Highly secure tunneling solution



No need to whitelist a broad range of IPs, just two domains



Automatic updates for mabl Link agent



High availability by design – just setup multiple agents with the same name



Support for https traffic and http forward proxies

Installing mabl Link

Get started by following our documentation on installing mabl Link. You can either use Docker (recommended), run the link agent as a service, or run it in a terminal on an appropriate machine. mabl Link includes logging to help you diagnose potential connection problems. If the Link agent is unable to connect to mabl's infrastructure, you may need to whitelist these domains: `api.mabl.com` and `*.link.mabl.com`.

You will be able to see if your Link agent is able to reach our infrastructure within the mabl web app. Log into `app.mabl.com`, and navigate to Settings -> Networking. If the link agent is able to reach `api.mabl.com` to authenticate, you will see a row in the mabl Link agent's section.

Restricting link-agent access to internal sites

Some companies may want to add additional guardrails around the Link agent server. We recommend using IP tables or other network restriction tools to limit what the Link agent can access. Make sure that the Link agent is able to reach "api.mabl.com" and "*.link.mabl.com", and any internal or external domains needed for your applications to function properly.

How it works (in detail)

Once the mabl Link agent is running on a machine within your network, it establishes a WebSockets connection to our Link servers. The WebSockets connection is a secure tunnel to our cloud infrastructure. Over that connection, we multiplex the HTTP web traffic of the UI tests we're running as securely encrypted SSL traffic. The mabl containers running browser tests are sent through the tunnel with their egress point inside the customer's network. All DNS resolution happens on the machine running the Link agent. That's how the cloud-based containers are able to connect to and resolve URI's of internal applications.

In some companies, traffic may be restricted based on behavior, especially if it looks like bot traffic. If you are unable to get the Link agent to connect to mabl, and you have already whitelisted the domains, we suggest talking to other internal teams (ie. people who oversee networking, proxies, firewalls, security, content or IT). This type of connection may need to be explicitly enabled to allow mabl traffic.

Support Documentation

What is mabl Link? How is it secured? How do I ensure that mabl can only access what I want it to?

- [Secure tunneling with mabl Link](#)
- [mabl Link FAQs](#)

How do I setup mabl Link on my computer or server? How do I tell mabl what tests I want to run with mabl Link? How do I know what link agents I have running?

- [Using mabl Link](#)
- [Link with Docker](#)
- [Link on Windows](#)