test IO

test IO's Commitment to Security

Data security is at the core of test IO's services. Founded and based in Berlin since 2011, test IO has deep roots in the stringent data protection frameworks in Germany and the European Union. With hundreds of thousands of successful tests on proprietary software for our clients, our six years of experience and execution shows our commitment to keeping customer data safe.

We take several steps to ensure data security on the test IO platform. This begins with requiring all crowdtesters to complete a rigorous selection and onboarding process. This training ensures testers adhere to best practices in quality assurance and operate within our established testing framework. Before testers begin testing for us, they agree not to disclose any proprietary information under penalty of expulsion from the platform and fines, ensuring they maintain confidentiality with regard to the scope and results of our clients' tests.

We have additional technical measures at our disposal for clients with highly sensitive data, such as those in fintech or insurance. The best solution depends on several factors: whether your product is already available publicly, the type of software (SaaS, mobile app, native desktop or web), as well as what existing security measures, server infrastructure, and processes are already in place.

Below are specifics of maintaining data security with test IO:

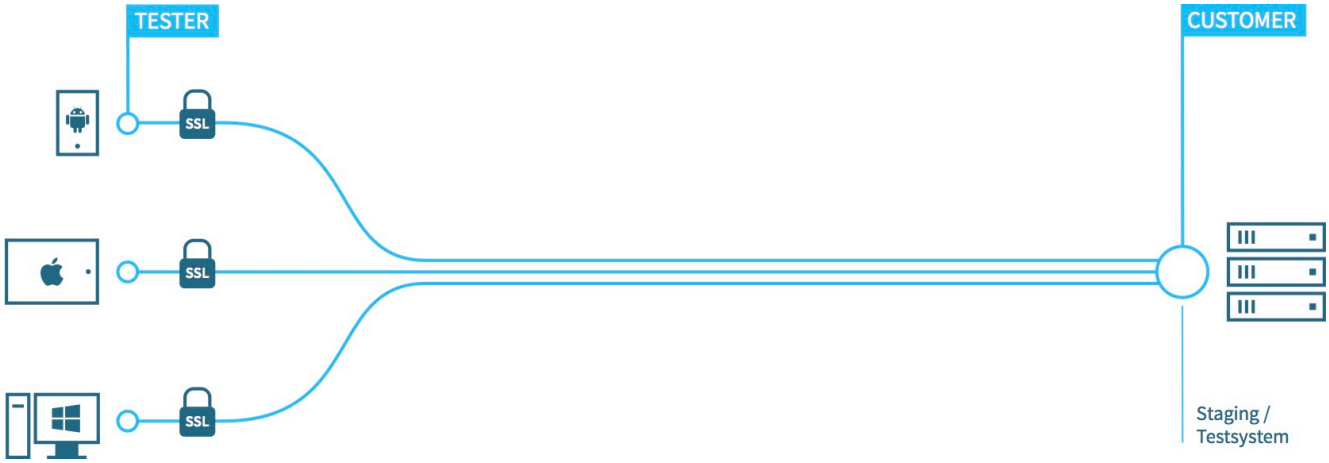
Raw .IPA & .APK File Distribution (iOS & Android Developer Files)

Some testing vendors simply don't work with iOS apps, or they require TestFlight accounts for all testers, limiting the number of testers and complicating the process on the client side.

With our Apple enterprise certificate, test IO securely code signs your pre-production app, using SSL for transport security. We give the installation link (which allows an over-the-air direct install) only to authenticated testers. We use this same process for distributing .APK files on Android.

Basic Access Authentication

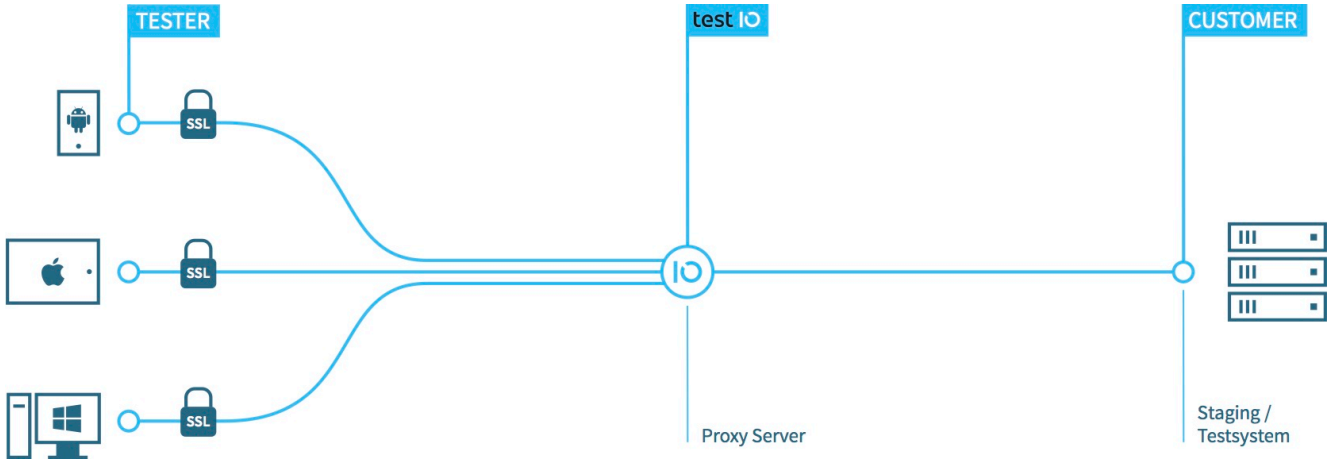
You can set up basic access authentication to provide testers with access to staging or testing servers. When you set up this test environment on the test IO platform, simply provide the credentials within designated fields. We'll provide them to the testers selected for your test cycle.



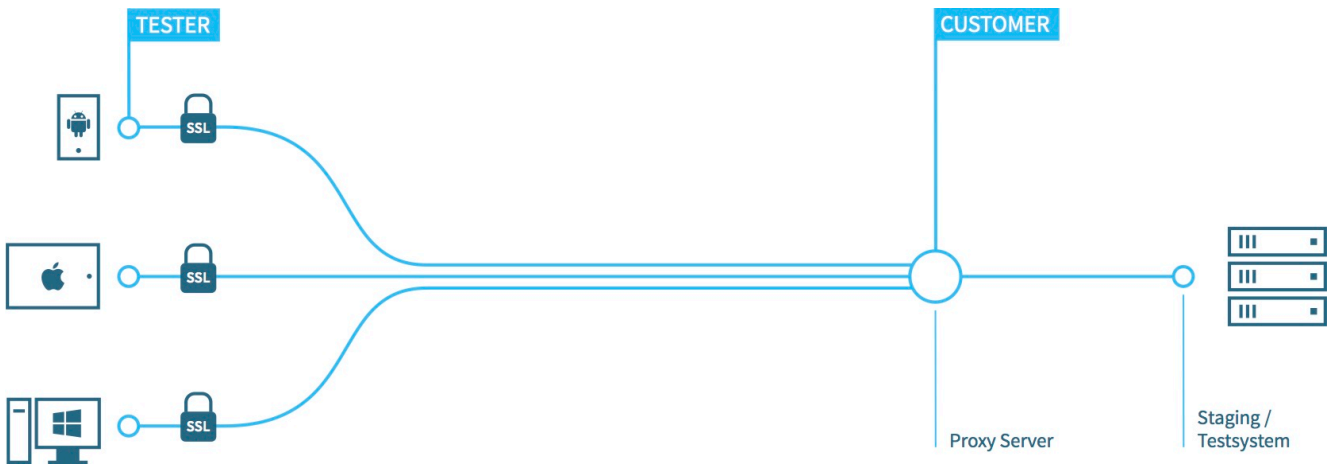
Proxy Server

By setting up a proxy server (you can provide your own or you can use test IO's), you can separate the connections of the software testers to the testing or staging system. Testers can then only access your software using the proxy server. There are two ways to implement this method:

1. test IO provides the proxy server, which you allow access to your system. The testers access the testing or staging system through this proxy server. To access the proxy server, testers authenticate using credentials test IO provides. **This is the recommended secure access method.**



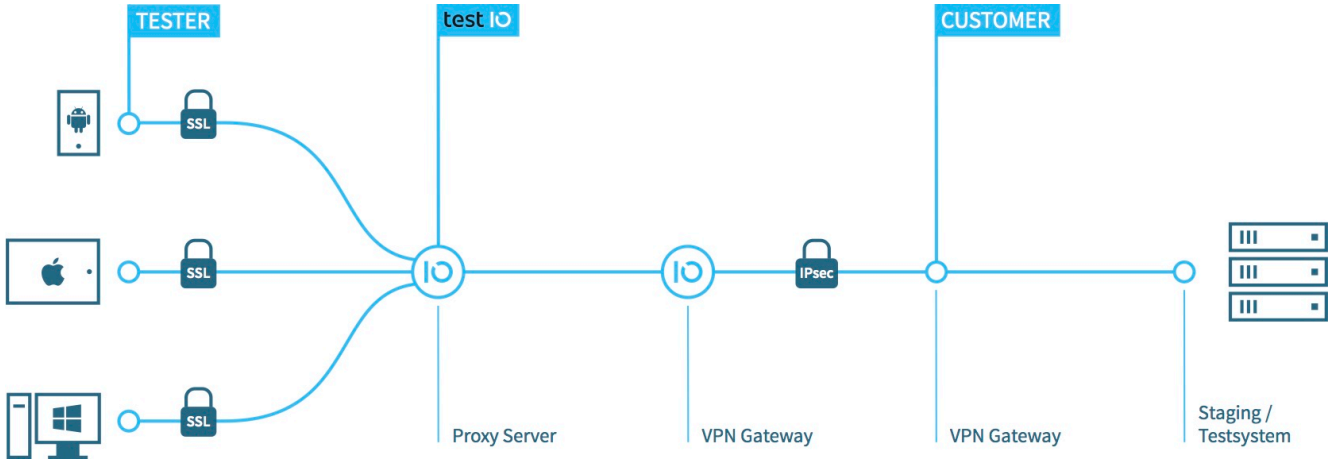
2. Testers use a proxy server you provide, using credentials that you provide.



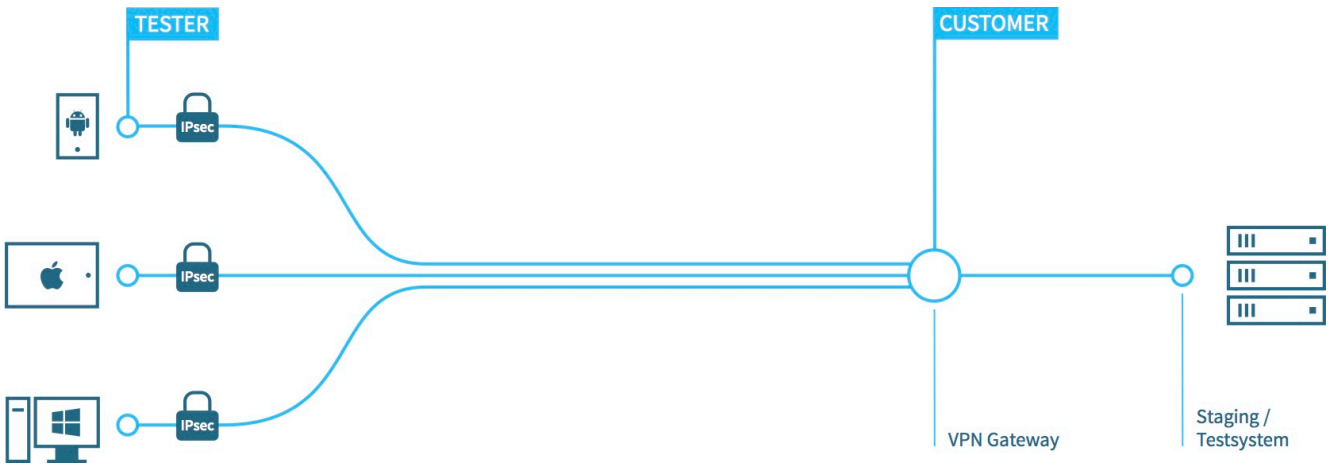
Virtual Private Network (VPN)

In some cases, you may wish to make connections to the testing or staging system only available through a VPN. There are two ways to set this up: by creating connection between the test IO VPN and your VPN, or you can provide each tester with access to your VPN.

1. The testers first connect to the test IO proxy. Their traffic is sent through the VPN tunnel from test IO's gateway through your gateway to the testing or staging system.



2. The testers connect to your VPN to access the testing or staging system behind it.



test IO

Encryption of Data at Rest

test IO encrypts your data using strong algorithms and have practices in place to protect your data both at rest and in transit. Sensitive data (like customer passwords) are encrypted using bcrypt. Information we need to be able to decrypt (like JIRA credentials) is encrypted using AES256.

All backups are encrypted with GPG. Multiple team members can initiate emergency restores, but their access can be revoked individually.

Will Testers Hack Us?

While we cannot control everything testers do while testing your application, testers understand that searching for vulnerabilities and exploiting them later puts them in extreme legal jeopardy.

The people who test with us know that this is a well-surveilled environment. We can proxy all of the traffic from the testers through test IO so that we have a log of all of the requests between each tester and the system under test. If, down the line, there were some sort of breach that you believe resulted from a tester's activities, test IO would have a complete log of those activities that is traceable to the tester himself.

In order to be paid, testers who work with us need to give test IO bank account and tax information, so we know their real names, where they live, and where they keep their money. So testers exploiting unreported vulnerabilities would not only violate the tester's legal agreement with us, it would 1) be illegal; and 2) be done in an environment that's highly conducive to identifying the criminal.

Learn More

Find out more about test IO and how we can enable your company to test smarter, code better, and ship faster.

Visit us online: test.io

test IO