ExpressVPN's statement

We have prepared the accompanying description about how we operate our ExpressVPN service. We confirm, to the best of our knowledge and belief, that:

a. the accompanying description fairly presents the ExpressVPN service in relation to our privacy policy. The criteria used in making this statement were that the accompanying description:

    i. presents how ExpressVPN's systems in relation to our privacy policy are designed and implemented,

    ii. presents ExpressVPN's organization, the operated processes, and controls to ensure it remains compliant with its privacy policy

    iii. does not omit or distort information relevant to these claims

b. the ExpressVPN service is suitably designed and implemented in relation to our privacy policy at the date of this statement. The criteria used in making this statement were that

    i. the ExpressVPN service is implemented as described in the description at the date of this statement,

    ii. the processes to operate and monitor the ExpressVPN service are implemented, and

    iii. the controls within the operating and monitoring processes of the ExpressVPN service are defined and implemented.

Kind regards
Express VPN International Ltd.

ExpressVPN's description

The following section describes:

1. ExpressVPN's privacy policy as it relates to its VPN service
2. ExpressVPN TrustedServer technology
3. How ExpressVPN ensures that it operates in compliance with its privacy policy

Privacy policy

Excerpting relevant sections from the ExpressVPN privacy policy located at https://www.expressvpn.com/privacy-policy:

> ExpressVPN is committed to protecting your privacy. We want you to understand what information we collect, what we don't collect, and how we collect, use, and store information. **We do not collect logs of your activity, including no logging of browsing history, traffic destination, data content, or DNS queries. We also never store connection logs, meaning no logs of your IP address, your outgoing VPN IP address, connection timestamp, or session duration.**
>
> Our guiding principle toward data collection is to collect only the minimal data required to operate a world-class VPN service at scale. We designed our systems to not have sensitive data about our customers; even when compelled, we cannot provide data that we do not possess.
>
> This privacy policy will help you understand how Express VPN International Ltd. ("**ExpressVPN**," "**we**," "**our**," or "**us**") collects, uses, and stores information.
>
> We ensure that we never log browsing history, traffic destination, data content, IP addresses, or DNS queries. Therefore:
>
> - We do not know which user ever accessed a particular website or service.
> - We do not know which user was connected to the VPN at a specific time or which VPN server IP addresses they used.
> - We do not know the set of original IP addresses of a user's computer.
>
> Should anyone try to compel ExpressVPN to release user information based on any of the above, **we cannot supply this information because the data don't exist**.
> In order to maintain excellent customer support and quality of service, ExpressVPN collects the following information related to your VPN usage:
>
> ### Apps and Apps versions
>
> We collect information related to which Apps and Apps version(s) you have activated. Knowing your current version of the Apps allows our Support Team to troubleshoot technical issues with you.

ExpressVPN

Successful connection

We collect information about whether you have successfully established a VPN connection on a particular day (but not a specific time of the day), to which VPN location (but not your assigned outgoing IP address), and from which country/ISP (but not your source IP address). This minimal information assists us in providing technical support, such as identifying connection problems, providing country-specific advice about how to best use our Service, and to enable ExpressVPN engineers to identify and fix network issues.

Aggregate sum of data transferred (in MB)

We collect information regarding the total sum of data transferred by a given user. Although we provide unlimited data transfer, if we notice that a single user pushes more traffic than thousands of others combined, thereby affecting the quality of service for other ExpressVPN users, we may contact that user for an explanation.

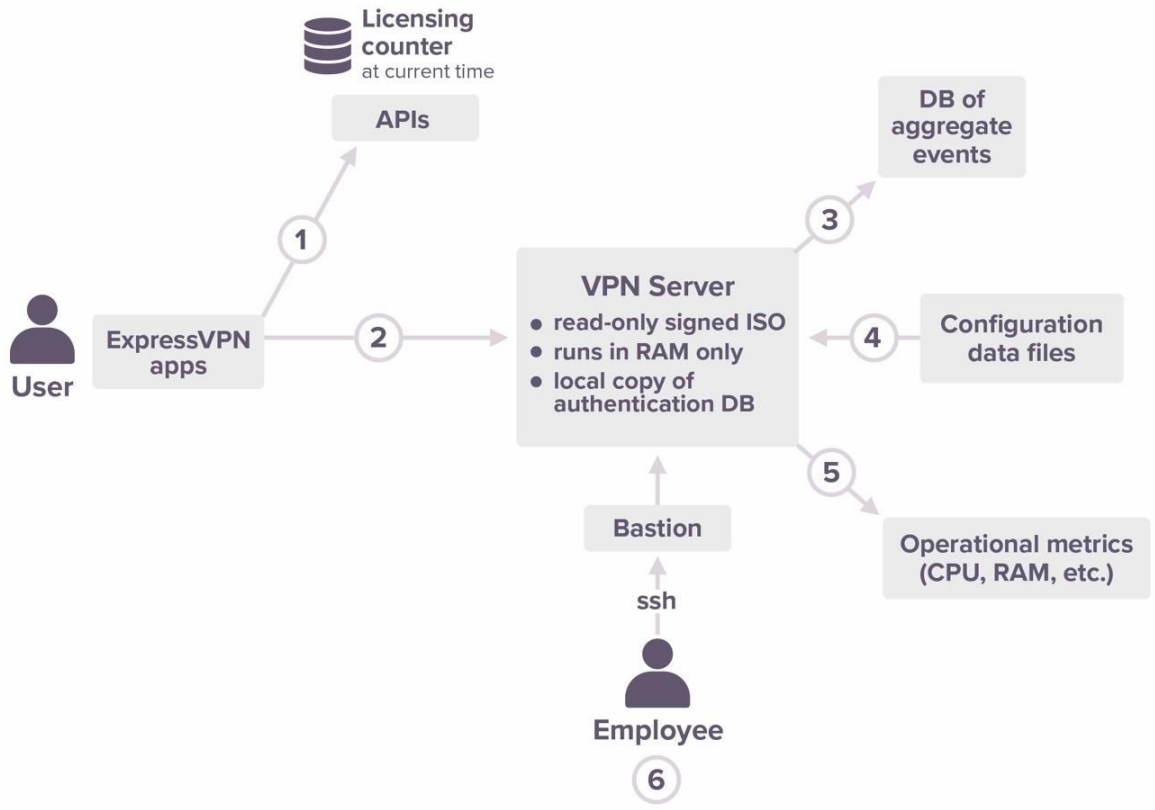
Summary

We collect minimal usage statistics to maintain our quality of service. We may know, for example, that our customer John had connected to our New York VPN location on Tuesday and had transferred an aggregate of 823 MB of data across a 24-hour period. John can't be uniquely identified as responsible for any specific behavior because his usage pattern overlaps with thousands of other ExpressVPN customers who also connected to the same location on the same day.

We've engineered our systems to categorically eliminate storage of sensitive data. **We may know THAT a customer has used ExpressVPN, but we never know HOW they have utilized our Service.** We stand by our firm commitment to our customers' privacy by not possessing any data related to a user's online activities.

How ExpressVPN ensures that it complies with its own privacy policy

System Architecture



Notes to explain the diagram above:

1. Only if the user chooses to use the ExpressVPN apps: **the apps call APIs operated by ExpressVPN**. If the user chooses to manually configure the VPN in their operating system, these API calls do not happen. The types of API calls are:
   a. Authenticate the user, retrieve credentials to connect to the VPN, and discover the set of available VPN infrastructure. This generates an event saved to a database with the OS and app version used.
   b. Check whether the user's license has reached its limit on the number of simultaneous connections. This system keeps **counters of simultaneous connections per license only at the current moment in time**. It does not keep historical records. Also, while an app is connected to the VPN, it sends a periodic heartbeat through the VPN to keep the simultaneous-connection counter accurate. Upon disconnect or absence of heartbeats, the counter resets within five minutes.

2. The user **connects to VPN servers** operated by ExpressVPN.
    a. **Authentication** is done with a username and password. Both credentials are generated randomly for each customer at the time of signup, and they are unrelated to the credentials used to login to the ExpressVPN website. Each VPN server has a local copy of the authentication database and authorizes the user without making additional network calls.
    b. The VPN servers are **designed and configured to prevent logging** of anything about what the user does with the VPN. **No connection logs, no activity logs (even of DNS lookups), or other types of logs that would contradict our privacy policy**.

3. The VPN server writes an event when the user disconnects the VPN connection. The VPN server uses the user's IP address to make a GeoIP lookup using a locally stored GeoIP database. The event is sent to a **database**. The **event does NOT include the user's IP address** or the outgoing IP address that the server used to route the user's traffic. The fields in the event are:
    a. The current date (not time).
    b. A salted and hashed version of the VPN username (which itself is randomly generated, unrelated to the user's email address or other personally identifiable information) that performed the event.
    c. The Country and ISP GeoIP attributes of the user who performed the event.
    d. The aggregate amount of data transferred in and out through the VPN tunnel, in megabytes, for the now completed session.
    e. An ID representing the VPN location. This does not identify the specific server used, but rather the group of servers corresponding to the location that the user selected.
    f. An ID representing the VPN protocol used.

4. On a recurring schedule, each VPN server downloads the latest **configuration data files**, including the **authentication database** and a specification of the server's expected configuration.

5. Once per minute, each VPN server saves **operational infrastructure metrics** to:
    a. A cloud-hosted **InfluxDB** database shared by all VPN servers. These data don't contain any personally identifiable information (PII). They are CPU, RAM, network utilization metrics, and the version-identifier of the ISO image running on this server.
    b. A cloud-hosted **Icinga** infrastructure-monitoring system shared by all VPN servers. These data don't contain any PII. They are uptime heartbeats commonly used in operating Linux servers.

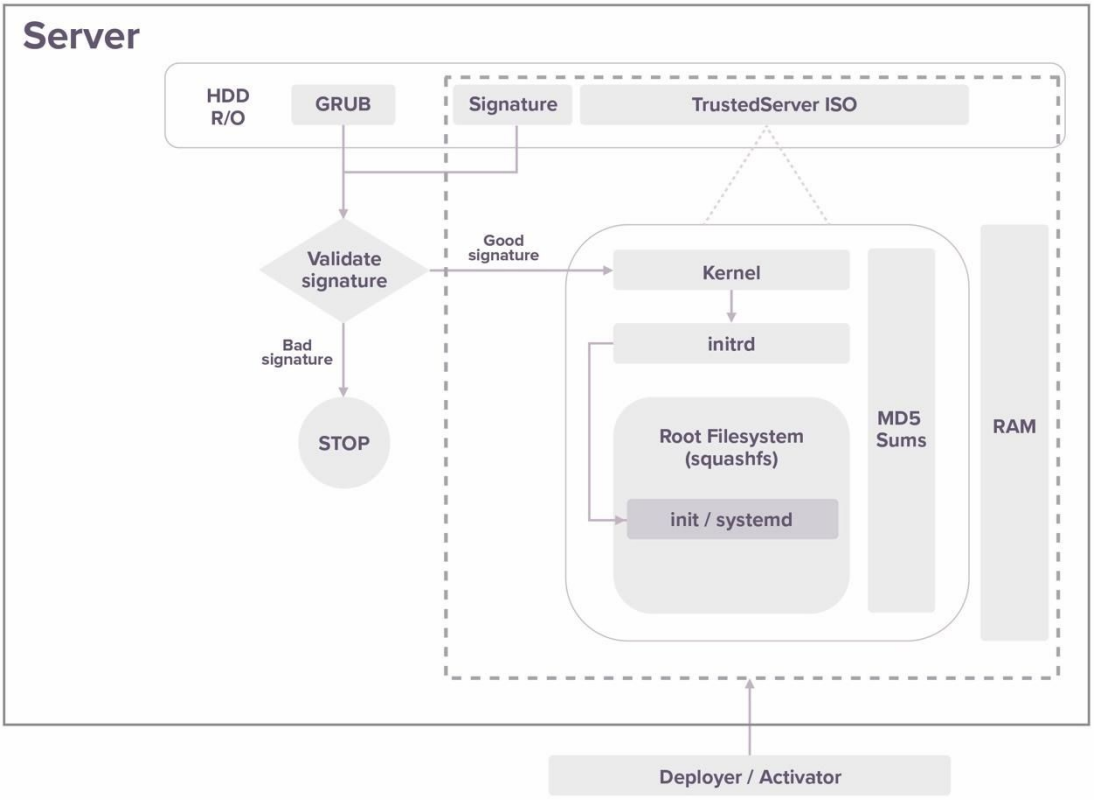
6. As needed, devops applications or authorized employees can, through a bastion-host, connect to a VPN server using SSH to upload new ISO images and trigger reboots.

ExpressVPN

TrustedServer Architecture

All ExpressVPN OpenVPN and IKEv2 servers are operated on the “ExpressVPN TrustedServer” RAM-only architecture as described below. This represents the vast majority of users and traffic, since all apps by default only use those two protocols.

The legacy protocols PPTP, L2TP and SSTP are operated on traditional server architectures still based on hard-drives. However, the ExpressVPN apps and website advise the user against using those protocols, and the ExpressVPN apps don’t use those protocols when in “Automatic” mode. The architecture of those legacy servers isn’t described in detail here, though we also consider them compliant with our privacy policy.

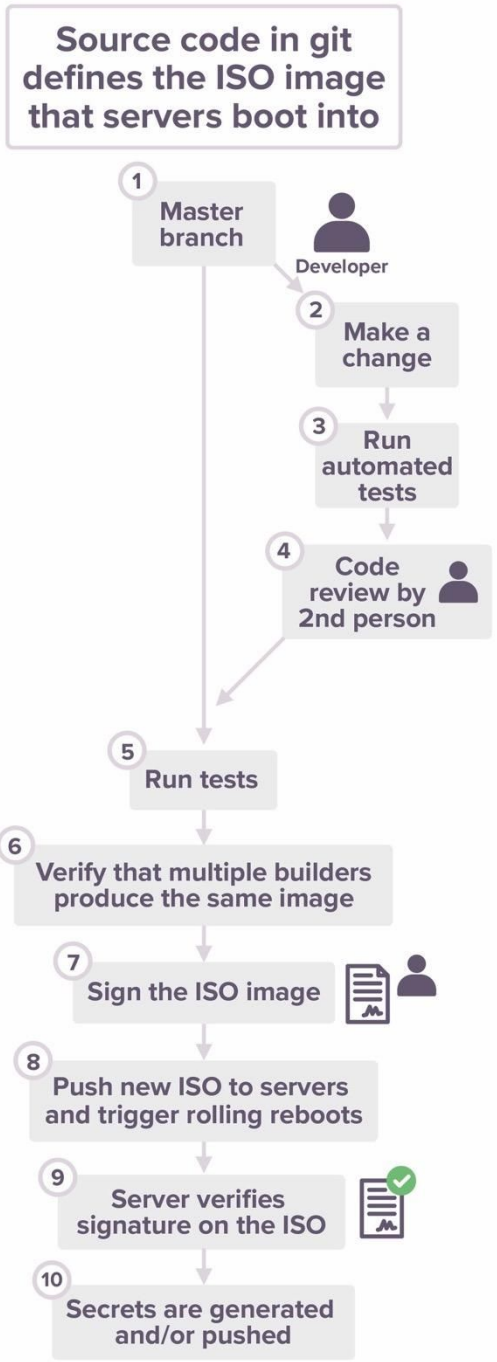


On an ExpressVPN TrustedServer:

1. The **servers run in RAM only**. The bootloader on the server hardware boots directly into a **read-only ISO image that is digitally signed by ExpressVPN**. The ISO contains **the entire Debian operating system compiled by ExpressVPN as well as all applications** in it. A server cannot boot without a valid signature on the ISO.
2. Files written to system locations are appended on an OverlayFS in memory only. None of the ISO contents can be modified.
3. With every reboot, the servers reset themselves to their standardized state based on the read-only ISO image, therefore any data that might have accumulated during operations are lost.
4. No secrets are shipped inside the ISO image. A separate “activator” validates the running OS before pushing or generating secrets.
5. No PII such as user IP address ever leaves the VPN server.

ExpressVPN

Workflows for changes and deployments



To ensure that our servers remain compliant with our privacy policy, we follow workflows to protect ourselves from accidental or malicious changes. The key points are:

1. Everything running on the TrustedServer, starting with the operating system on up, is defined in source code and stored in git. All source code is **compiled into a single ISO that defines all code** that will be on the TrustedServer.

2. No one can push source-code changes in the master branch directly. Instead, **changes must be made in a branch**.
3. **Automated unit tests** include checks that verify that configuration remains in a no-logging state. Tests fail if code-coverage is below 95%.
4. Branches **require review and approval from a second person**, as well as passing of all automated tests, before they can be merged into the master branch.
5. With every change to the master branch, automated tests are run again.
6. At least two independent machines tasked with compiling the ISO must produce the same identical results. TrustedServer is engineered to have **reproducible builds**. This ability raises our confidence that the ISO is in fact the exact result of compiling our source code.
7. Once approved for release to production, an **ISO is signed cryptographically** by an engineering manager using a private key stored on a pin-protected Yubikey.
8. The ISO is then uploaded to servers, and an automated scheduling system then coordinates rolling reboots to upgrade servers to the new ISO.
9. Servers will **only boot on ISOs with valid signatures** from the ExpressVPN key.
10. After boot, servers generate some secrets (such as Diffie Hellman parameters for OpenVPN), and others are pushed to the server (such as authentication credentials for downstream systems).