Privex Inc.
13039 Cable Beach,
Nassau, Bahamas
(Company registered in Belize City)
+1-404S-PRIVEX (1-404-777-4839)

Tor Relay / Exit Registration Form

This form is intended to be filled out by customers who would like to run a Tor Exit Node in Sweden, or a Tor Relay/Bridge in regions with metered bandwidth such as Sweden, Japan, Netherlands, and the USA.

Tor exits found in any of our regions which were not officially registered with us, will be terminated with no refund.

How to order

To **order a Tor Exit/Relay Node in Sweden (SE), Japan (JP), or the Netherlands (NL),** please fill out this PDF form using a PDF application that supports form fields, and then email it to sales@privex.io - or via our support system: https://support.privex.io

Tor exits are prohibited in Germany (DE) and Finland (DE), however non-exit Tor relays may be operated in DE/FI without our permission, as networking in DE/FI is 100% unmetered by default.

Table of Contents

Tor Exit / Relay Registration Form

Your name (can be an alias / psuedonym):

Your Email Address:

Server Region:

○ Sweden (SE)

○ Japan (JP)

○ United States (US)

○ Netherlands (NL)

Type of Server:

○ Dedicated

○ Virtual (VPS)

Server package code (e.g. V2-SE, WEBBOX-SE-V4), or simply RAM/CPU/Disk specifications if you want a custom server:

Unmetered Networking (sometimes called Bandwidth)

○ 100mbps ○ 50mbps ○ 1gbps (1000mbps)

○ 200mbps ○ 300mbps ○ 400mbps

○ 500mbps ○ 800mbps ○ 2gbps (2000mbps)

○ 3gbps ○ 5gbps ○ 10gbps

○ Other (please specify in the notes at the end of this form)

Type of Tor Node:

○ Relay (middle/guard) ○ Exit Node

Planned nickname for Tor Relay / Exit:

If you have a domain available, please give us a domain or sub-domain that we can set as the reverse DNS (rDNS) for your relay/exit's IPv4 and IPv6 addresses:

If you already have a VPS or dedicated server from us, and would like to run an exit node on it (or relay if you don't have fully unmetered from us), then please fill out the below field with the IPv4 and/or IPv6 address(es) of the server:

Anything else we need to know about your order? (special notes)

I have read Privex's Tor Exit/Relay policy, and I agree to follow all requirements listed in the policy, and understand that breaching the policy may result in immediate termination of my server WITHOUT REFUND.

Sign below to confirm you agree to the policy

If your PDF app **doesn't support signature fields (above)**, please simply type your name in the box below to confirm you agree with our Tor policy:

Tor Exit Policy (as of January 2021)

For the latest version of our Tor Exit policy, please read https://www.privex.io/tor-exit-policy/

As of January 2021, the policy is as follows:

IMPORTANT INFORMATION - READ BEFORE RUNNING AN EXIT!

While Tor Exit nodes are permitted in *some of our regions*, exit nodes **may only be ran after contacting us and requesting permission to do so.**

If you run a Tor Exit node in **ANY OF OUR REGIONS without permission**, your server will be terminated as soon as we detect it, and refunds are not permitted for servers that were terminated due to abuse reasons (such as running a Tor Exit node without permission).

NOTE: While customers are forbidden from running Tor Exits without permission - customers may however run standard non-exit Tor Relays (entry (guard) / middle nodes) without asking for permission, as long as they have a dedicated server with unmetered networking.

If you have a VPS (virtual server), you should contact us before setting up the non-exit relay, so that we can clarify the bandwidth usage policy for that specific VPS package, and possibly offer an upgrade to truly unmetered (unlimited) networking for your VPS - so that you may run your Tor Relay without running into bandwidth caps, or unexpected suspension due to breaking our Fair Use Bandwidth Policy.

What is a Tor Exit Node

A Tor Exit Node is a type of Tor node which is configured to allow public access to the internet via it's external IPv4 / IPv6 address.

They act as an **open proxy** - but have no way of knowing who the original request came from.

Tor relays (middle/guard nodes, and bridges) are allowed in all of our regions. However, Tor exit nodes are only permitted in Sweden (currently open beta) with some specific requirements.

Our requirements for operating an exit node on our network

1. You **MUST** contact us for permission before attempting to run a Tor Exit node. Please do not purchase any of our standard packages on our order form with the intent for using them as a Tor Exit node. To run a Tor Exit, you need to use one of our special custom plans which includes unmetered networking, and any additional costs related to the high risk nature of a Tor Exit node.

2. Due to the amount of bandwidth + 24/7 network activity used by a Tor exit node, we require that you pay for an unmetered network connection. In Sweden we price this at $1 USD per month per megabit, e.g. 10mbps is $10/mo, 100mbps is $100/mo and so on. We can offer up to 5gbps for VPS's and 10gbps for dedicated servers. In the future, as we peer with more ISPs, we'll gradually reduce the cost per megabit.

3. As exit nodes result in our IP addresses ending up on blacklists, we require you to pay for at least the first 3 months of service in advance.

4. We request that you disallow at the very least port 25 on your exit node, as email spam is one of the biggest triggers for abuse emails and IP blacklisting.

5. If you use the official Reduced Exit Policy from TorProject (and remove port 22 from the allowed ports), then we will happily handle all abuse emails automatically and inform them that it's a Tor Exit Node - no action will be taken against your server as long as we can verify the IP we gave you is listed as a functional exit node on TorProject's Relay Search.

    1. If you wish to have an unrestricted exit policy, then we would request that you give us an abuse contact email that we may list on the WHOIS for the IP, so that all abuse emails should be directed straight to you to handle. We don't require any personal information for the WHOIS, only an email for Abuse.

Verify this document is authentic

This document will be signed with GPG (PGP) after it's finalized and published to our website / CDN.

The signatures will be available at:

https://cdn.privex.io/documents/tor-register/chris-sig.asc

Signature by Privex CEO - Chris S.
Fingerprint: A4A1 0213 ECA1 B50E 32E6 9180 DDB3 6F2B 5528 4433
Key ID: 5528 4433
Long Key ID: DDB3 6F2B 5528 4433

https://cdn.privex.io/documents/tor-register/kale-sig.asc

Signature by Privex CTO - Kale S.
Fingerprint: 4274 DEF7 4745 3454 CDA6 AED5 BED8 EFF8 9F1F 7520
Key ID: 9F1F 7520
Long Key ID: BED8 EFF8 9F1F 7520

https://cdn.privex.io/documents/tor-register/support-sig.asc

Signature by Privex Support Key (valid Jan 2021 to Jan 2023)
Fingerprint: 17E8 77C3 5C3E 886A 5232 6C6A 288D D163 2F6E 8951
Key ID: 2F6E 8951
Long Key ID: 288D D163 2F6E 8951

To verify using GPG CLI:

```
    $ gpg --keyserver hkps://keys.openpgp.org --recv-keys DDB36F2B55284433 BED8EFF89F1F7520
288DD1632F6E8951
        gpg: /home/john/.gnupg/trustdb.gpg: trustdb created
        gpg: key 288DD1632F6E8951: public key "Privex Support (Shared key by Privex Inc. support team
for Jan 2021 to 2023) <support@privex.io>" imported
        gpg: key BED8EFF89F1F7520: public key "Kale S <kale@privex.io>" imported
        gpg: key DDB36F2B55284433: public key "Christopher S. (Privex CEO) <chris@privex.io>" imported
        gpg: Total number processed: 3
        gpg:               imported: 3

    $ gpg --verify chris.asc tor-register.pdf
       gpg:                using RSA key A4A10213ECA1B50E32E69180DDB36F2B55284433
       gpg:                issuer "chris@privex.io"
       gpg: Good signature from "Christopher S. (Privex CEO) <chris@privex.io>" [ultimate]
```

Repeat the --verify command for each .asc signature file, or just one of them, if you trust a certain staff member like our CEO :)