Privacy statement eduVPN

This privacy statement applies to the service eduVPN that is being provided by DeiC, the National Research and Education Network of Denmark. References to 'we', 'our' and 'us' refer to eduVPN, while 'you' and 'your' refer to the user of eduVPN.

1. Principles and values

We believe (the opportunity to have) privacy in a secure way is fundamental but unfortunately also increasingly scarce. eduVPN strengthens the user's security by enabling institutions, students, teachers, employees and researchers to connect securely to the internet and their institution network wherever they are. eduVPN has been developed with privacy and security in mind since the very beginning of the project because we think privacy and security are inseparable within eduVPN.

That being said, eduVPN collects, stores and logs information. We use this information with the purpose of providing the service eduVPN, for auditing and analysis in order to maintain, protect and improve eduVPN. Our principles regarding data collection are:

- We don't collect personal information or data when it is not necessary.
- We will never use personal data for other purposes than those for which the personal data were initially collected.
- We will never sell or market the obtained personal data to third parties.
- We will never store or view the content of the traffic on the VPN network.
- We will be transparent about all aspects of processing personal data and logging.

The legal ground of processing personal information is legitimate interest to provide the service eduVPN and to prevent abuse on the research network Forskningsnet. As a user you have the right to inspect all the user data we collect from you. In some cases you also have the right to rectify or delete the data and or restrict the processing of the data. You may always object to the processing of your user data. Such requests may be sent to the email address below. DeiC will give a response to the request within four weeks.

In order to be transparent, this Privacy Statement is quite comprehensive and thus a quite long read. Therefore we also included a shorter summary that is more easily readable.
Don't hesitate to contact us via eduvpn@deic.dk if you have any questions or concerns.

2. Short summary

From a user's perspective, eduVPN consists of a user portal (web server) where configuration files can be downloaded and a VPN server that can be used to establish a connection with eduVPN. These components log and store the following information for one month:

2.1 User portal

The unique user ID of the user.
A list of certificates created by the user.
When two factor authentication is used, the OTP secret.

2.2 Connection

The unique user ID of the user.
The time the connection was established.
The time the connection was closed.
The IP addresses assigned to the user's VPN client.
The amount of data that was transferred by the VPN client.

3. Elaborate version

3.1 The information you provide

When you start using eduVPN and log in for the first time, WAYF will ask if you agree with the release of personal data. There are two types of profiles within eduVPN, each requiring different personal data (explained below). You will also be asked to read and accept this eduVPN Privacy Statement.

Secure Internet

If you choose this type of profile, all traffic will be going through eduVPN. eduVPN only uses the attribute ‘eduPersonTargetedID' (example: b466f1047193791ga9aop7224a98fd24a1ce4551) from the user. This identifier is randomly generated by WAYF and pseudonymous. The mapping of the eduPersonTargetedID to the associated user can be made when DeiC is required to do so pursuant to the law, a judicial decision or abuse.

Institute Access

If you choose this type of profile, only traffic to the institution's network or all traffic will go through eduVPN, depending on the institution’s choice. This is the profile you want when you need access to your institution's network. eduPersonTargetedID is in general not used for this profile since users need to be identifiable for authorization. This means that the chosen attribute for this profile can differ between institutions.

3.2 The information we collect

eduVPN collects more information and data than the aforementioned WAYF attributes you provide. This is mostly because of error logging so we can troubleshoot more easily when something is not working as intended. We made a list of all the logging components within eduVPN.

Statistics

eduVPN servers provide us with general and anonymous statistics. The following is part of these statistics:

Total amount of bytes transferred per session
Total number of unique users
Highest number of concurrent connections

These statistics are being created daily and will also be available in consolidated form for other periods of time like weekly and monthly. These data are available to the institution's application managers and the eduVPN team. There is no user data and / or personal data being processed in these statistics and there is no time limit applied.

Logging for application managers

An application manager can request specific logs from within the admin-portal. For the Secure Internet profile logs can only be accessed by the eduVPN team while only the institution's application managers have access to the logs of the Secure Access profile. The application manager needs the point of time in combination with the issued IP address to request logging. When the combination is available in the logs, the following will be provided:

Used profile *(i.e. 'Secure Access').*
The UserID *(i.e. 'b466f1047193791ga9aop7224a98fd24a1ce4551').*
The name of the configuration file *(i.e. 'Android_1478521025').*
The issued IP addresses (VPN) *(i.e. '145.101.113.74 and 2001:610:188:71::1008')*.
Timestamp start of connection *(i.e. '2016-11-07 13:17:19').*
Timestamp end of connection *(i.e. '2016-11-07 13:23:40').*

These data are being stored for one month.

Server logging OpenVPN

eduVPN uses OpenVPN software for the underlying VPN server. All logging of OpenVPN has been disabled so nothing will be logged at this level.

Access log

The web server's access log logs all requests from clients. This log is turned off but can be temporary enabled when there is need of additional logging when troubleshooting problems that can not be fixed in other ways. When access log is enabled, the following data is being stored for one month:

The (real) IP address from the visitor.
The username as determined by HTTP authentication.
The time of the request.
The request line of the client *(i.e. 'GET / HTTP/1.0).*
The status code that the server sends to the client *(i.e. 200, 404 etc.).*
The size of the server's answer to the client (in bytes).
The requested page / URL.

Error logging

Under normal circumstances, there will be no errors. But of course not everything is normal and things can go wrong in for example the user's browser of the web server. The web server sends this diagnostic information and detected errors to the error log. This is the first place where we will look when there is something wrong with the web server. This logging is turned on, stored for one month and consists of the following information:

The timestamp of the error.
The category of the error (low - severe).
The IP address from the client.
The error code or the message with the error.

Example:

```
[Wed Nov 21 07:45:23.681239 2021] [:error] [pid 18283] [client 10.42.101.100:59892] No known parameters passed to the logout handler. Query string was "(null)". To initiate a logout, you need to pass a "ReturnTo" parameter with a url to the web page the user should be redirected to after a successful logout.
```

Logging between nodes

The internal logging from communication between different eduVPN components is being tracked in a log file. Think of: "User creates a new certificate through the user-portal". The logging is being stored for one month and consists of the following:

Timestamp of the action.
The request *(i.e. GET /api.php/).*
The UserID.
The request line from the client.
The status code.

Example:

```
[14/Nov/2021:10:51:27 +0000] "GET /api.php/is_disabled_user?user_id=b117d1efaadc006f243fefb722b28430754ka2dq HTTP/1.1" 200 35
```

php-fpm logging

php-fpm is a process manager for PHP and is being used to initiate and stop PHP scripts in the server. php-fpm only logs errors and contains no user data. This logging is turned on, is stored for one month and looks as follows:

```
[20-Oct-2021 14:00:45] NOTICE: fpm is running, pid 7692
[20-Oct-2021 14:00:45] NOTICE: ready to handle connections
[20-Oct-2021 14:00:45] NOTICE: systemd monitor interval set to 10000ms
[21-Oct-2021 16:23:19] NOTICE: Terminating ...
[21-Oct-2021 16:23:19] NOTICE: exiting, bye-bye!
```