Open Cascade VPN

Installation and activation manual

April 2023

Open Cascade VPN description and conditions

VPN is designed to access the Open Cascade (here and after OCC) internal resources from outside OCC intranet.

VPN provides the secure connection between the client computer and OCC VPN entry point (firewall at the OCC Cloud)

OCC employee/contractor can use OCC VPN from his corporate or personal device with conditions:

- OCC employees/contractors having CG Corp or OCC domain device are provided with full-functioning VPN, it is prohibited installing and using it on the own device.
- OCC employees/contractors which do not have CG or OCC device are provided with limited VPN connection, allowing to access OCC cloud workspace and OTP portal for own OTP tokens' management.
- The policy towards OCC VPN credentials is the same as for normal CG account (**please got acquainted with and follow its rules** on the CG Talent portal, Acceptable Use Policy).

Open Cascade VPN installation

During the onboarding process the employee/contractor receives the email with OCC account activation instructions and information about some OCC services, including OCC file sharing service: https://drive.opencascade.com (OCC Drive), which contains company-wide shared folder with useful manuals like this one.

The temporary password to the OCC account and OTP token's activation keys are sent with separate SMSs to the new employee.

The VPN installation and activation process consists of 3 simple steps (please see "OpenCascade VPN" folder for files, you can skip 2 first steps in case of OCC domain laptop):

1. VPN client installation (OpenVPN client). Links to download the app for: Windows | Mac
2. Copying the VPN profile files. Shared and available on OCC Drive, please see "_OCC_infra_guides\OpenCascade VPN" folder for details.
3. Installing Authenticator app on the user's device and activating the token (We recommend using the Google or Microsoft Authenticator app for Android or iOS (links are on the next slide).

Useful links for VPN client installation

(please install the one, which is suitable in your case)

The OpenVPN Windows client download page

OpenVPN Connect for macOS

Google Authenticator for Android

Google Authenticator for iOS

or

Microsoft Authenticator for Android

Microsoft Authenticator for iOS

Authenticator for Google Chrome browser (extension)

Notice: it is allowed to use 2 activated tokens on 2 devices (e.g. smartphone + laptop), you can manage it on OTP portal (please use “Internet over VPN” profile and OCC account to login).

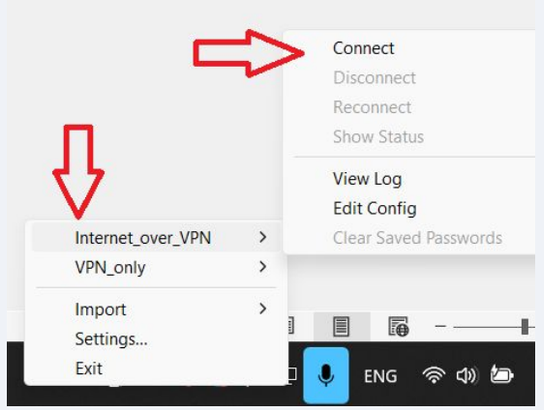
How to use VPN

After installing of Authenticator please activate OTP token (just scan the QR code with the app or insert the activation key)

Important: do not forget changing default PIN code (**1234**) on the OTP portal just after OCC VPN first activation.

How to use OpenVPN client:

1. **Right click on the OpenVPN icon in the system tray select the VPN profile and click "connect"** ("Internet over VPN" profile will route all the HTTP(s) traffic through VPN, useful for accessing internal HTTP resources, e.g. OTP portal)
2. **Use your OCC account nickname as login** (without "ocn\" prefix)
3. **Use OTP PIN + OTP password generated by app as password** (in other words, please combine a word out of 2 parts: PIN and OTP password). OTP password changes every 30 sec, so you need to apply it before it is expired.



Connection usually takes ~20 sec. After successful connection, the OpenVPN icon becomes green.

If so, congratulations, you've got the VPN set ☺