

Setting up VPN access at TH Köln

20.09.2024



th-koeln.de/campus-it

Content

1. Introduction	1
2. What is VPN?	2
3. Requirements for the use of VPN	3
4. VPN access on Windows	4
4.1. VPN access on Windows - automatic installation	4
4.2. VPN access on Windows - manual installation	6
4.3. Start Before Login for domain users	9
4.3.1. Start Cisco Secure Client later	11
5. VPN access on macOS	13
6. VPN access on Ubuntu Linux	18
7. VPN access for iPhone/iPad	20
8. VPN access for smartphones/tablets with Android	22
9. LAN access	24
10. Contact	26

1. Introduction

This manual explains in short steps how you, as a member of TH Köln, can establish a secure connection to the network of the university.

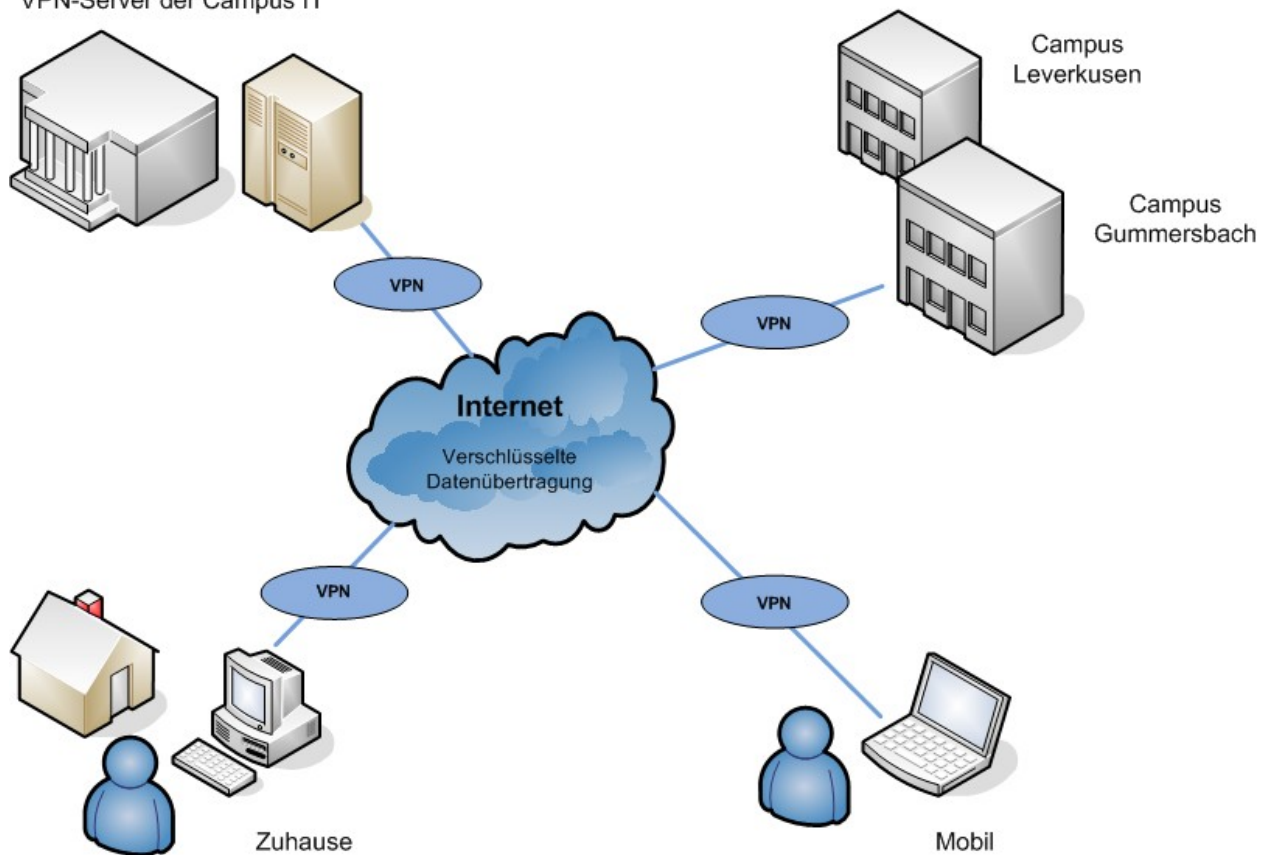
Data connections via the public network (internet) are not secure. It is recommended to secure your personal data, especially in public wifi networks such as internet cafés, at train stations and airports, and in shared accommodation with shared internet access.

In order for you to have secure access to the network of TH Köln with your mobile devices or your PC from home, Campus IT offers you what is called a VPN connection.

VPN is to be understood as a secure personal line in your active Internet connection. This VPN connection is started in addition to your Internet connection and requires authentication.

Please be aware that the VPN client has been renamed from "Cisco AnyConnect" to "Cisco Secure Client". In addition, some minor adjustments have been made to the design.

VPN-Server der Campus IT



2. What is VPN?

A Virtual Private Network (VPN) is a computer network that uses a public network, for example the Internet, to transport private data. The connection via the public network is usually encrypted. It thus enables secure transmission over an insecure network. Participants in a VPN can exchange data in the same way as in a LAN (local network). The individual participants themselves do not have to be directly connected to each other for this. The networks are connected via a tunnel between the VPN client and the VPN server.

The VPN client is software that establishes an encrypted and authenticated connection to the VPN server. The user receives an IP address from the network of Technische Hochschule Köln – University of Applied Sciences, which enables them to access services within the University.

3. Requirements for the use of VPN

To set up and use a secure Internet connection (VPN), you need:

- A WLAN-enabled device, e.g. notebook/PC with the operating system Microsoft Windows, MAC OSX, Linux or a smartphone or tablet with an active Internet connection
- A campusID. All University members receive a personal user account – called a campusID. This user account allows access to various Campus IT services
- A Cisco VPN client. The use of this client is mandatory in order to use the offered services.
- A current version of Java. We recommend Java in its current version for the easy automatic installation of the Cisco VPN client. You can download Java free of charge here:

<https://www.java.com/en/download/>

We have summarized the common VPN installation routines for you below.

You can find further information on the Campus IT website:

www.th-koeln.de/campus-it

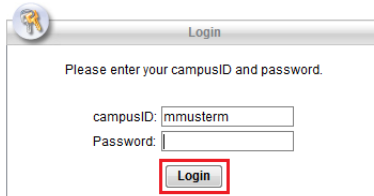
4. VPN access on Windows

1. To set up VPN access, please enter the following address in your browser:

vpn.th-koeln.de

vpn-gm.th-koeln.de (if you are at the Gummersbach site)

2. Please enter the login details for your campusID on the website and then click on "Login".



3. After a short verification phase, either the automatic installation will start or you will be asked to install manually. Please make sure that you have administrator rights on your computer, i.e. that you are authorized to install programs.

4.1. VPN access on Windows - automatic installation

1. The automatic installation starts automatically if all requirements are met.

Note: If you do not have Java installed or you block the applet, follow the instructions for manual installation. You can already download the installer in this window.

2. You may receive security warnings.

In each case, click on "Run".

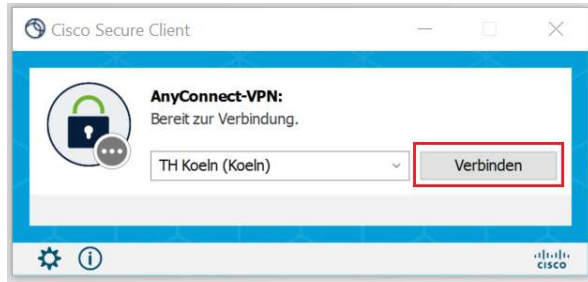


3. Please confirm the message "Do you want to install this software?" by clicking on "Install".

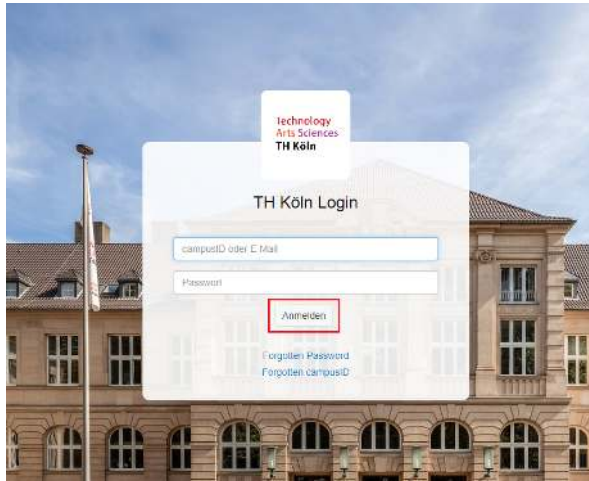


4.1. VPN access on Windows - automatic installation

4. To use the Cisco Secure Client now, open the program and click on "Connect".



5. A browser window will open and you will be asked to enter your campusID and password. Confirm by clicking the 'Login' button.



You may be asked to enter a second factor.

For further information about this can be found at: <https://www.th-koeln.de/mfa>

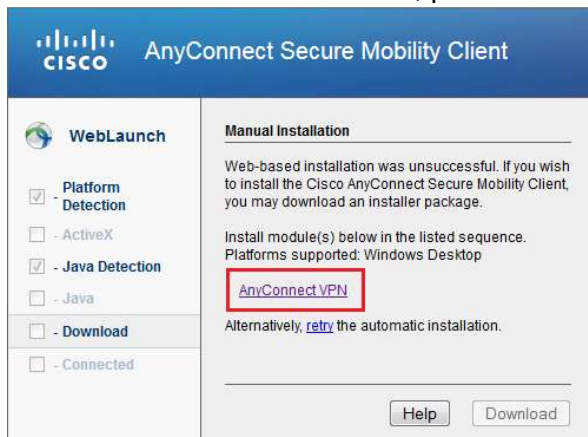
6. Once you have entered the correct information, this window will appear and you can close the browser tab.



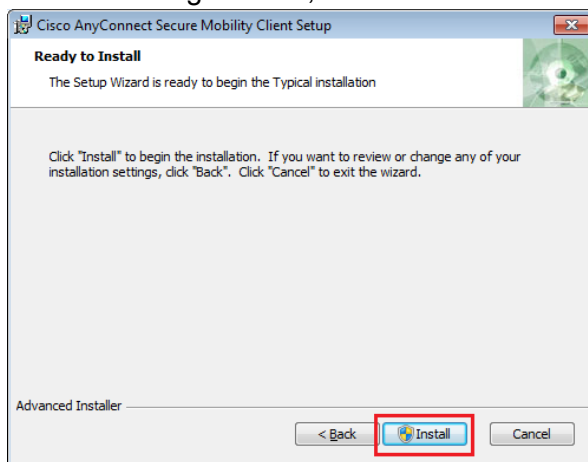
Please note: You can launch the Cisco Secure Client manually at any time to connect with it or disconnect the existing connection. You can find the program in the Windows Start menu.

4.2. VPN access on Windows - manual installation

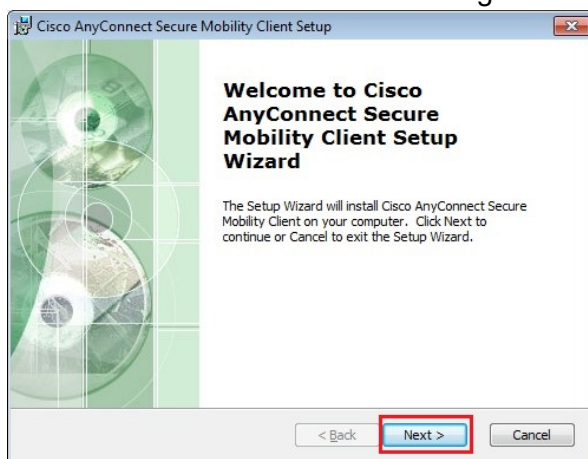
1. If the automatic installation fails, please click on the suggested link in the window below.



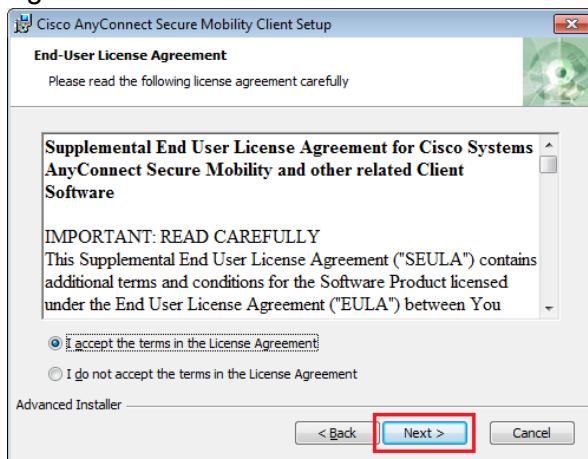
2. In the following window, confirm the start of the installation by clicking on "Install".



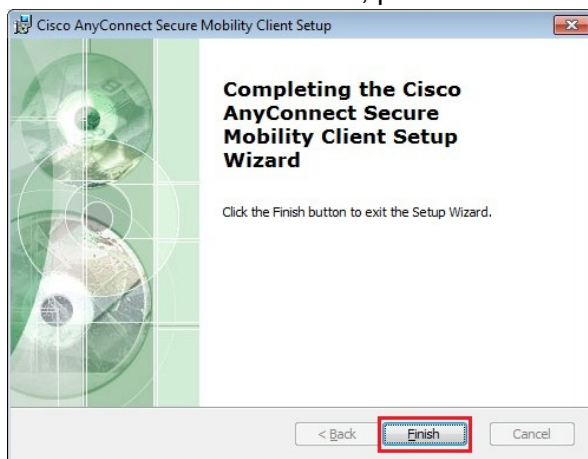
3. Please click on "Next" in the following window.



4. Please read the Software License Agreement and select "I accept the terms in the License Agreement" and then click on "Next":



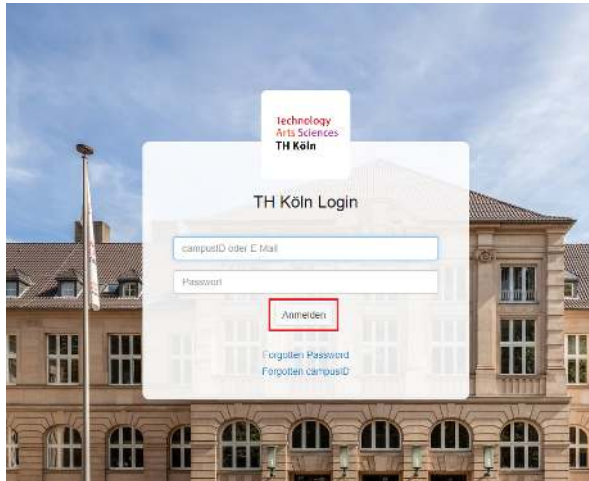
5. In the following window, please click on "Install" to confirm the start of the installation.
6. After successful installation, please click on "Finish" in the following window.



7. To use the Cisco Secure Client now, open the program and enter vpn.th-koeln.de in the empty address field. Then click on Connect.



8. A browser window will open and you will be asked to enter your campusID and password.



You may also be asked to enter a second factor.

For more information, please see: <https://www.th-koeln.de/mfa>

The Cisco Secure Client is now set up and you are connected. You can start the Cisco Secure Client manually at any time to connect or disconnect.

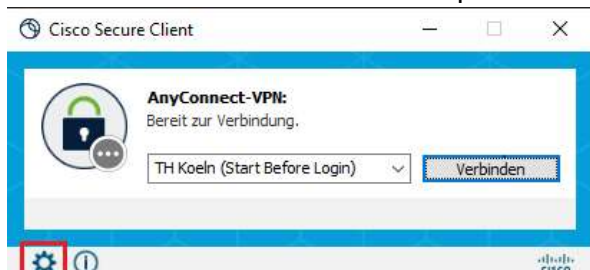
4.3. Start Before Login for domain users

4.3. Start Before Login for domain users

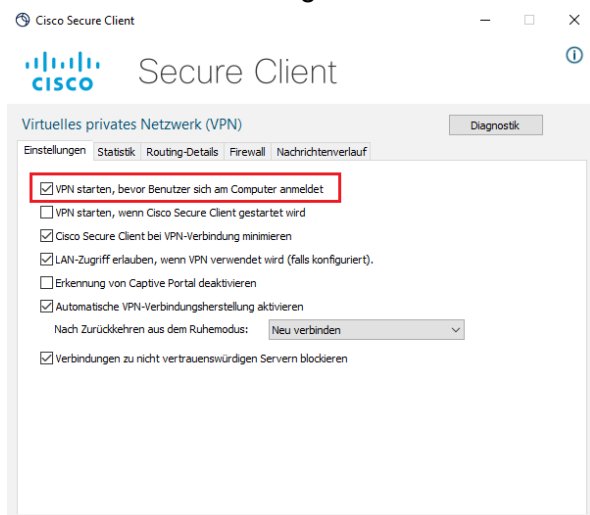
To automatically connect to network shares for example, you might need to start the vpn connection before you login into Windows.

Please verify the setting "Start VPN before user logon to computer" is set in order to be able to open the Cisco Secure Client on the Windows login screen.

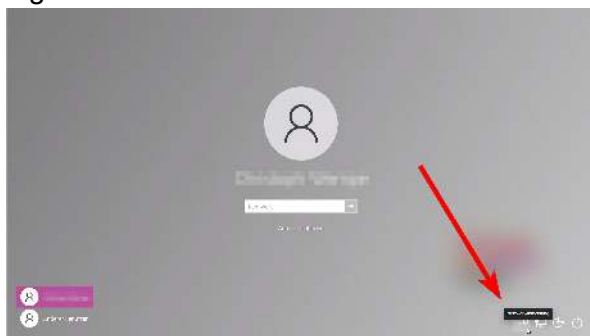
1. Start the Cisco Secure Client and open the settings by clicking on the gear symbol.



2. Now check if the setting "Start VPN before user logon to computer" is set



3. The next time you start your computer you will see a new symbol with two monitors on the login screen.

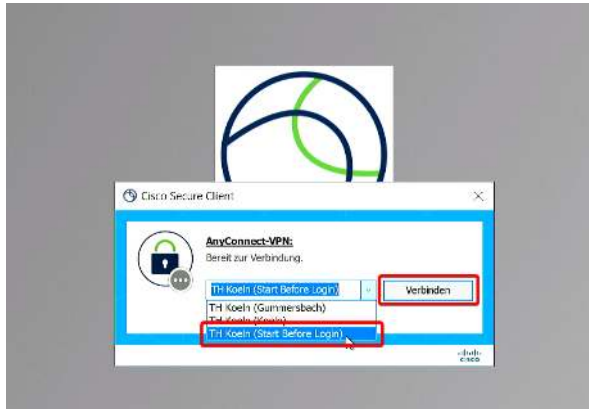


Click it to open Cisco Secure Client.

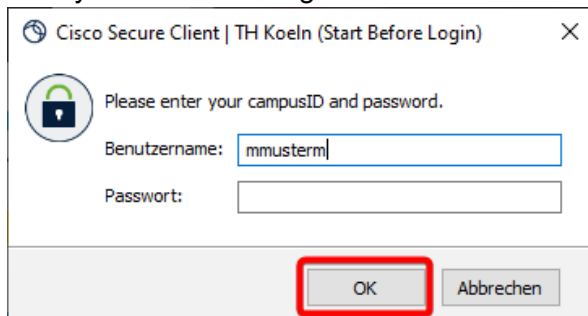


4.3. Start Before Login for domain users

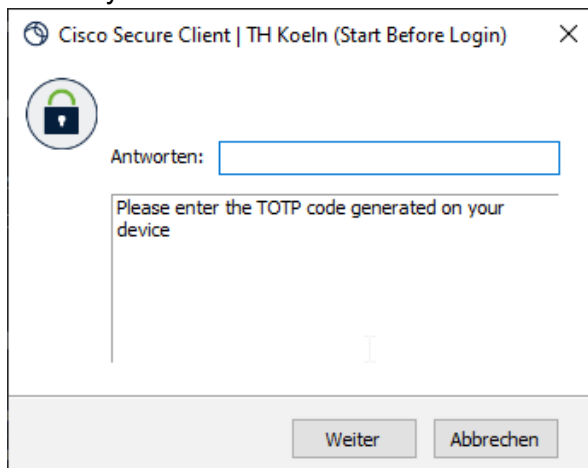
4. After the client is started, select the profile "TH Koeln (Start Before Login)".



5. Now you are able to login to the VPN client with your campusID and password.



6. You may also be asked to enter a second factor.



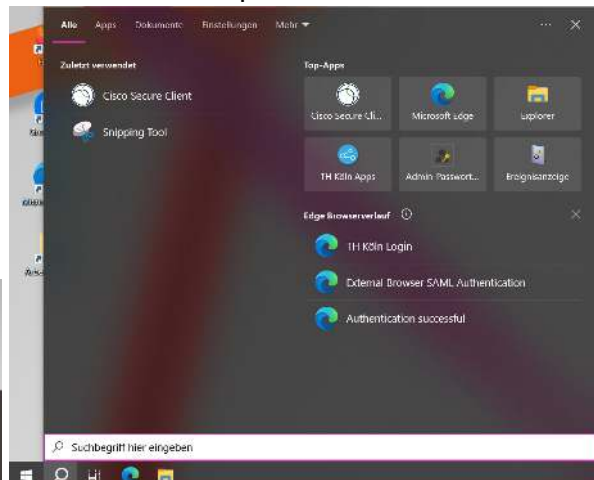
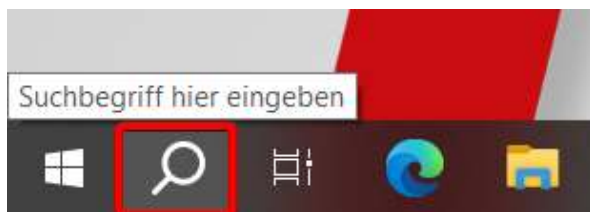
For more information, please see: <https://www.th-koeln.de/mfa>

4.3. Start Before Login for domain users

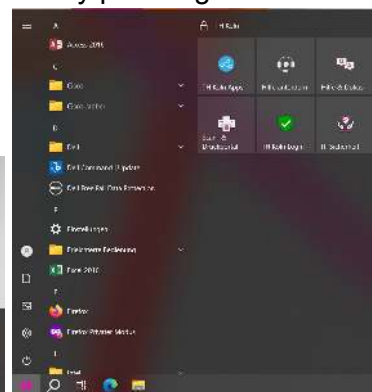
4.3.1. Start Cisco Secure Client later

You can also start the Cisco Secure Client later.
For example, if you forgot to do this when booting up.

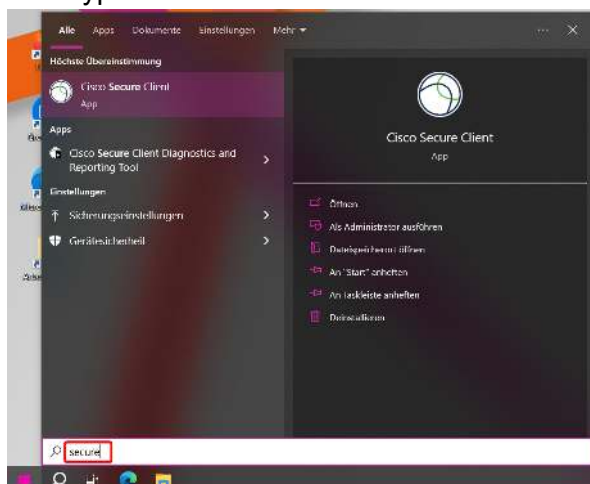
1. To do this, click on the magnifying glass icon in the task bar to open the Windows search.



- a. Alternatively, you can also open the Start menu by pressing the Windows key.



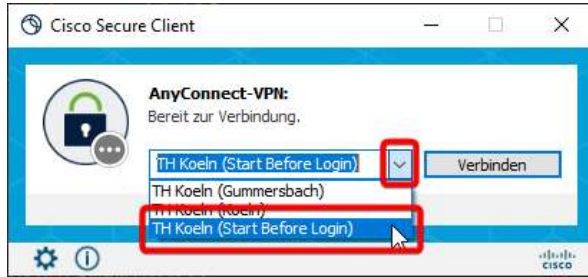
2. Now type "secure" to search for the Cisco Secure Client in the list of programs.



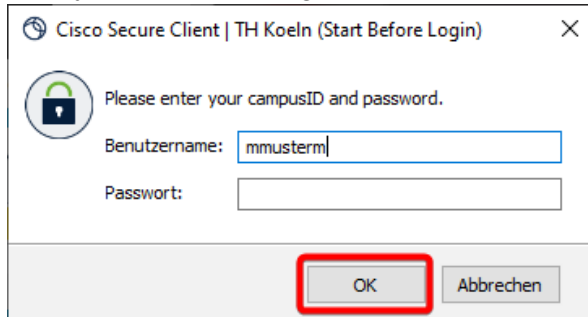
3. Press the Enter key or click with the mouse on the entry "Cisco Secure Client" to start the program.

4.3. Start Before Login for domain users

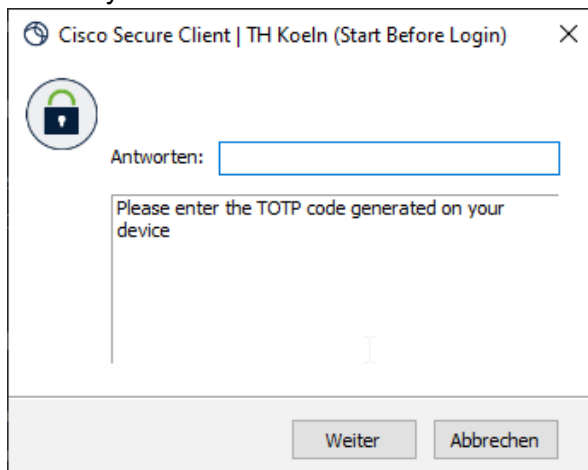
4. After the client is started, select the profile "TH Koeln (Start Before Login)".



5. Now you are able to login to the VPN client with your campusID and password.



6. You may also be asked to enter a second factor.



For more information, please see: <https://www.th-koeln.de/mfa>

5. VPN access on macOS

1. To install the VPN client, please establish an Internet connection, e.g. via WLAN, and enter the following address in the Internet browser:

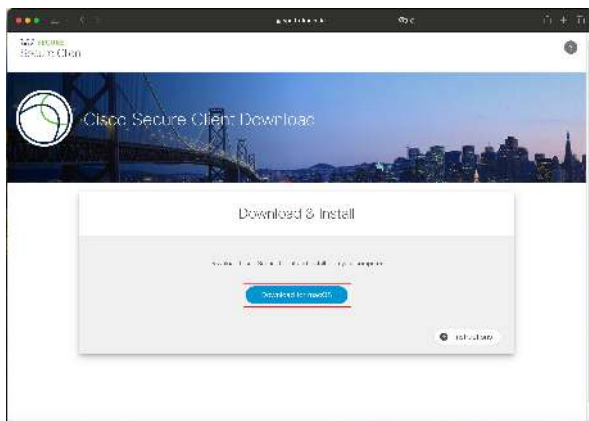
vpn.th-koeln.de

vpn-gm.th-koeln.de (if you are at the Gummersbach site)

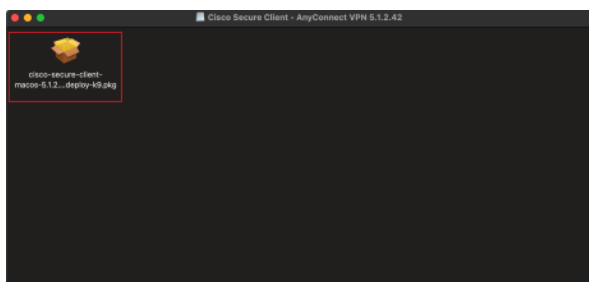
2. Please enter the login details for your campusID on the website and then click on "Login".



3. Click Download to download the installation file..

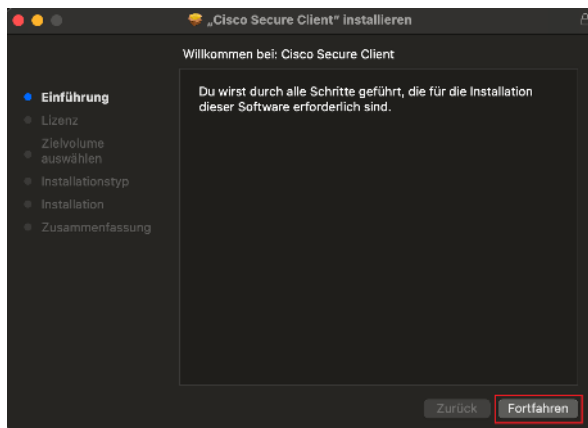


4. Then launch the installer by double clicking on it.

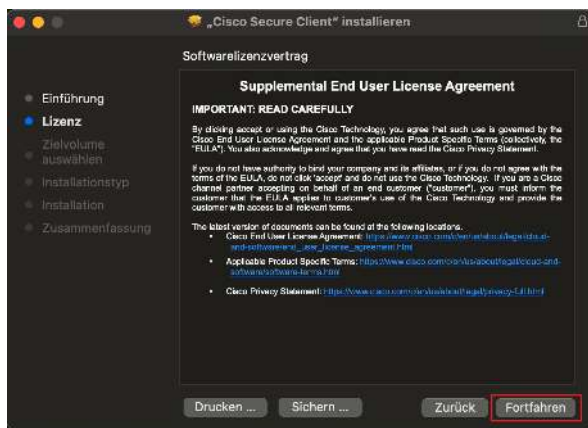


5. VPN access on macOS

5. Click on "Continue" in the welcome window.



6. Please read the Software License Agreement and then also click on "Continue" and accept the software license agreement by clicking on "Accept".

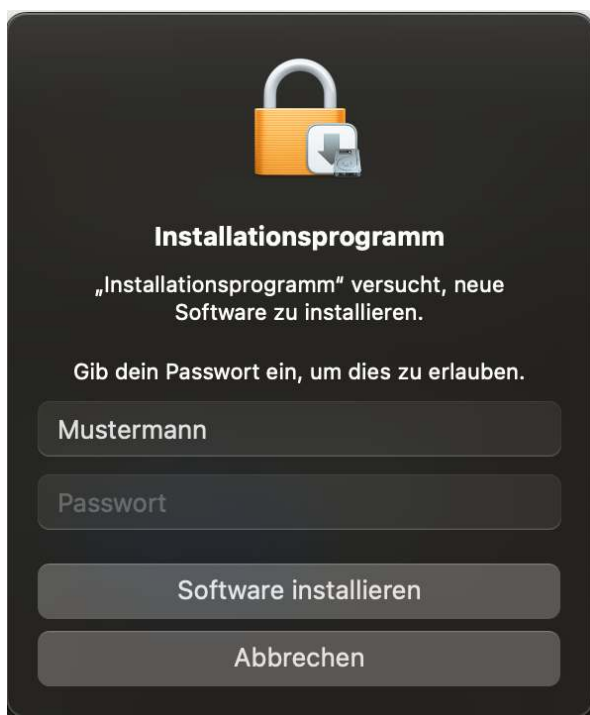


7. To perform the standard installation, click on "Install".



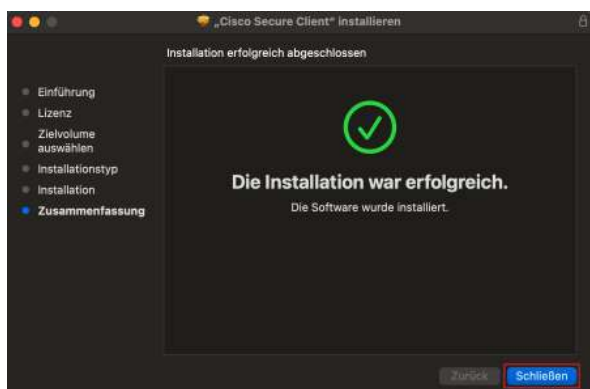
5. VPN access on macOS

Please note: You may be asked for your password

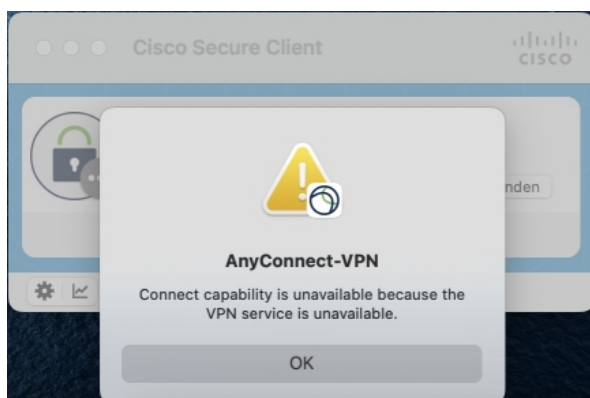


8. The installation routine is executed and completed with the notification of successful installation.

Now click on "Close" to end the manual installation.



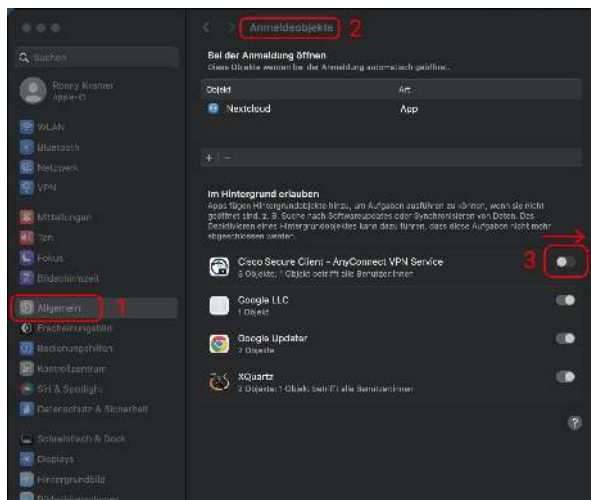
9. When setting up the VPN client, you may receive the error message "Connectability is unavailable because the VPN service is unavailable".



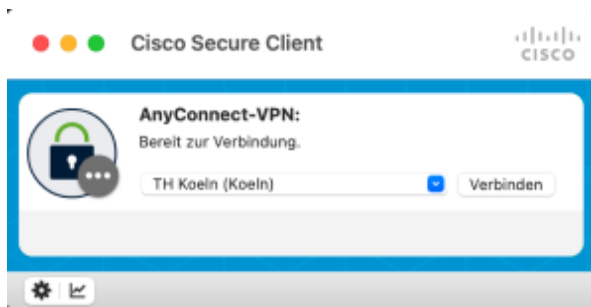
To resolve this, you must allow background services for the Cisco Client.

5. VPN access on macOS

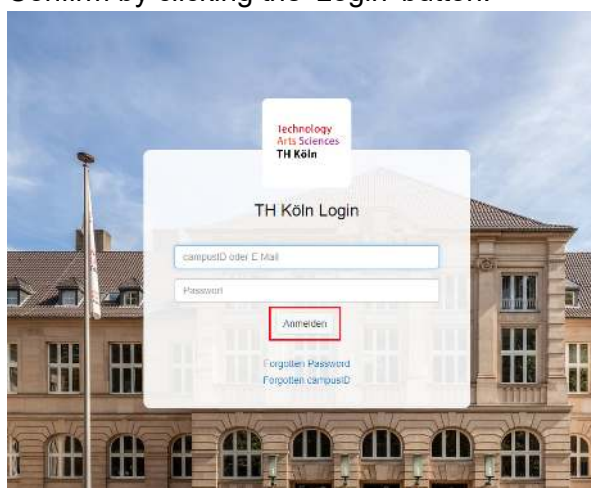
To do this, open system settings and navigate to General. Then open the "Ligon objects" submenu on the right. In the "Allow in background" section, enable the "Cisco Secure Client" slider.



10. To connect, select "Connect VPN".



11. A browser window will open and you will be asked to enter your campusID and password. Confirm by clicking the 'Login' button.



You may be asked to enter a second factor.

For further information about this can be found at: <https://www.th-koeln.de/mfa>

5. VPN access on macOS

- Once you have entered the correct information, this window will appear and you can close the browser tab.



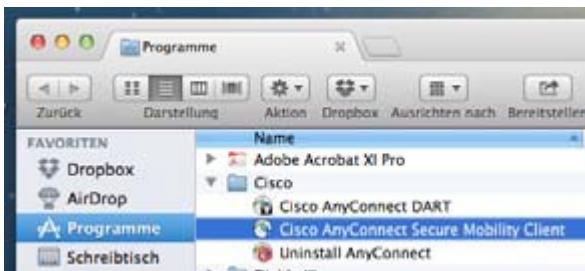
- If you want to disconnect an existing VPN connection, select "Disconnect VPN".
- You can launch the Cisco Secure Client manually at any time to establish the VPN connection or to disconnect the existing connection. Select the corresponding program icon on the taskbar, in the dock or the finder (under Programs/Cisco).



Taskbar



Dock

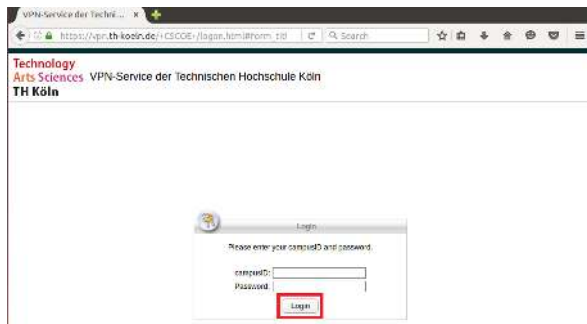


Finder

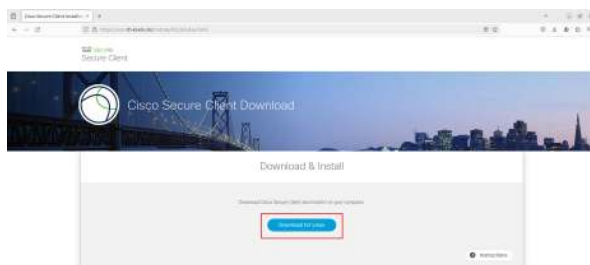
6. VPN access on Ubuntu Linux

1. Please enter the following address in your browser:

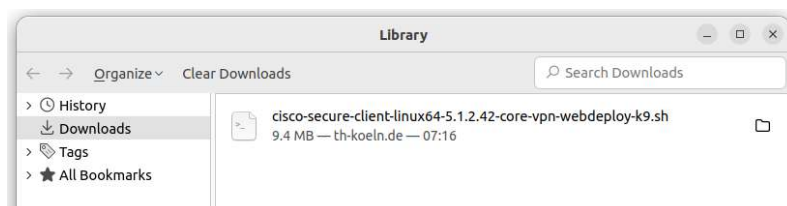
vpn.th-koeln.de



2. Now you can download the installer by clicking on the AnyConnect VPN link.



3. The following file will be downloaded.



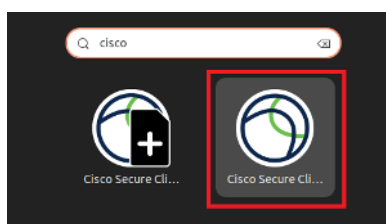
4. First execute the following command:

```
sudo apt-get update
```

5. Then launch the previously downloaded file with the following command:

```
sudo bash /home/username/Downloads/cisco-secure-client-linux64-5.1.42-core-vpn-webdeploy-k9.sh_*
```

6. You will then see the installed Cisco Secure Client as a program



6. VPN access on Ubuntu Linux

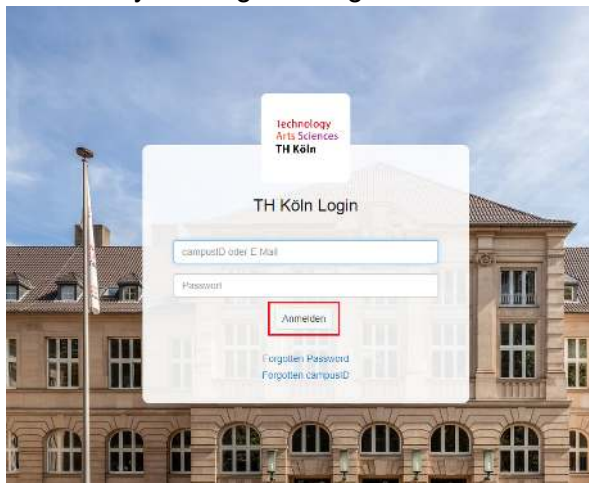
7. Launch the Cisco Secure Client and enter the address of the VPN server you want to connect to

vpn.th-koeln.de

vpn-gm.th-koeln.de (if you are at the Gummersbach site)



8. A browser window will open and you will be asked to enter your campusID and password. Confirm by clicking the 'Login' button.



You may be asked to enter a second factor.

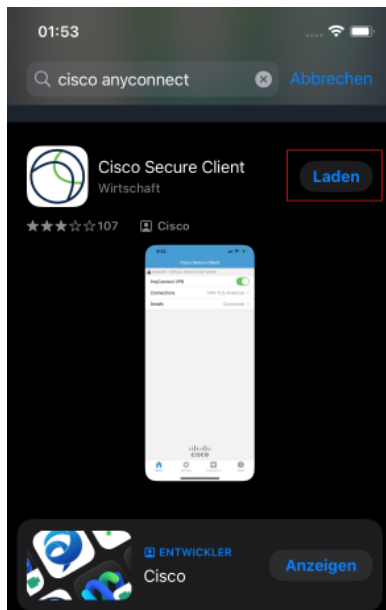
For further information about this can be found at: <https://www.th-koeln.de/mfa>

9. Once you have entered the correct information, this window will appear and you can close the browser tab.



7. VPN access for iPhone/iPad

1. Search the AppStore for Cisco Secure Client and install the app.



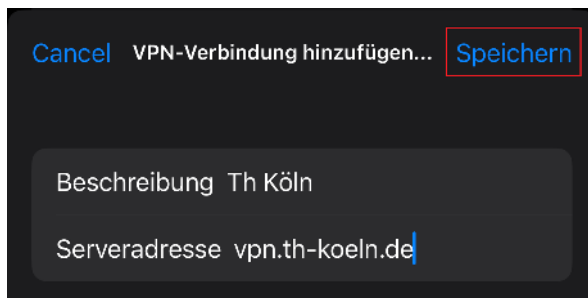
2. Configure VPN client: Settings → General
Select the menu item VPN and Add VPN configuration.

Description: TH VPN

Server address:

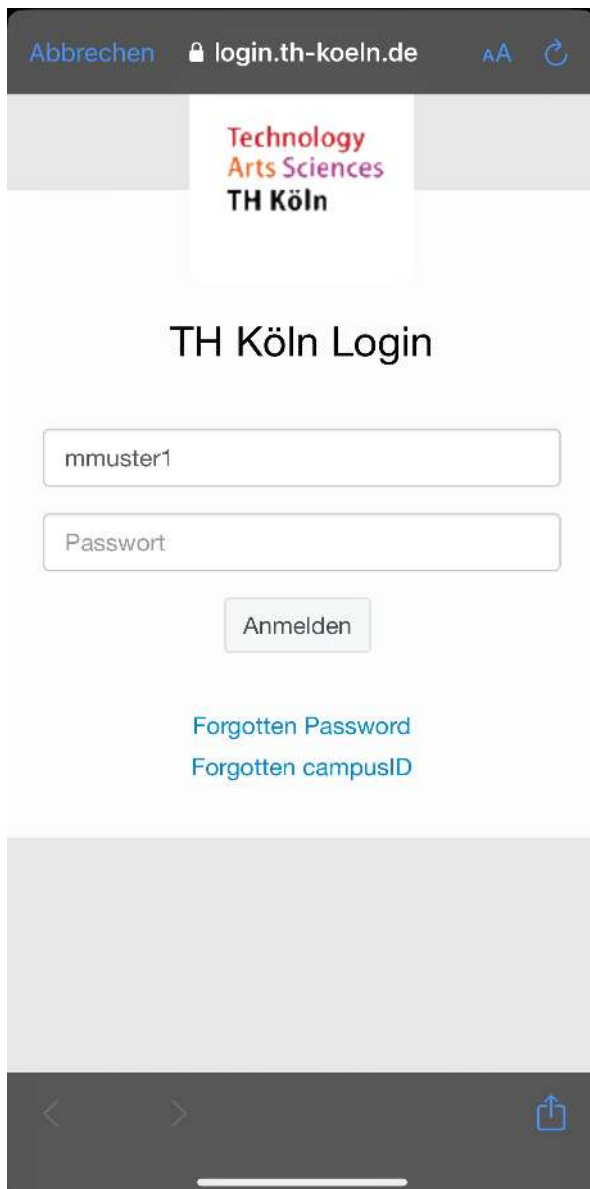
vpn.th-koeln.de

vpn-gm.th-koeln.de (if you are at the Gummersbach site)



7. VPN access for iPhone/iPad

3. . A browser window will open and you will be asked to enter your campusID and password. Confirm by clicking the 'Login' button.



The screenshot shows a mobile browser interface for the TH Köln login page. At the top, the address bar displays 'login.th-koeln.de' with a lock icon and a refresh button. Below the address bar is the TH Köln logo, which includes the text 'Technology Arts Sciences TH Köln'. The main heading is 'TH Köln Login'. There are two input fields: the first contains 'mmuster1' and the second is labeled 'Passwort'. Below the password field is a button labeled 'Anmelden'. Underneath the button are two links: 'Forgotten Password' and 'Forgotten campusID'. The bottom of the screen shows a dark navigation bar with back and forward arrows and a share icon.

4. Also confirm the VPN connection message with "OK". You are now connected to the University VPN.

8. VPN access for smartphones/tablets with Android

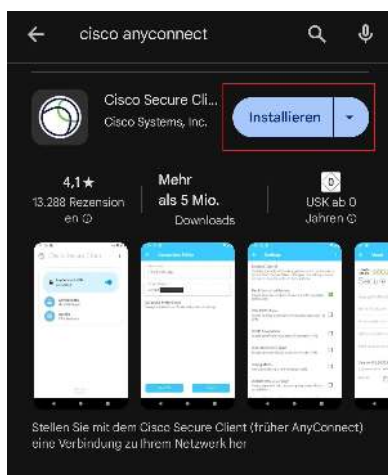
Supported devices for AnyConnect ICS (Ice Cream Sandwich):

According to information from Cisco, the AnyConnect app for Ice Cream Sandwich should work on all devices equipped with Android 4.0 and higher.

Requirement: Android 4.0 and above

Note: To download the Cisco Secure Client-AnyConnect-app, you need Internet access on your device; this can be via WLAN or mobile communications. Another requirement is the Google Play app (AKA Play Store, formerly Market), which is installed on Android devices as standard. For more information, please refer to the rest of this manual.

1. Download Cisco Secure Client-AnyConnect from the Play Store. To do this, go to the program menu on your device and select "Play Store" (or the "Market").
2. In the Play Store (or the Market), please search for "AnyConnect" and install the app.



3. After you have selected and installed the appropriate version of the Cisco Secure Client-AnyConnect app, open the advanced settings in the app and select "Add new VPN connection".

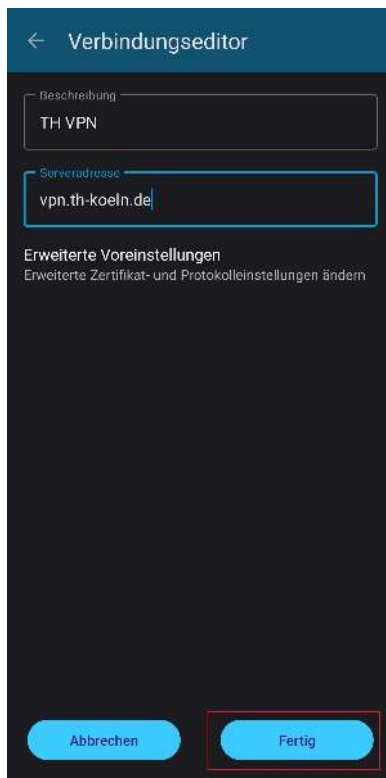
8. VPN access for smartphones/tablets with Android

4. As the description, choose the name: TH VPN.

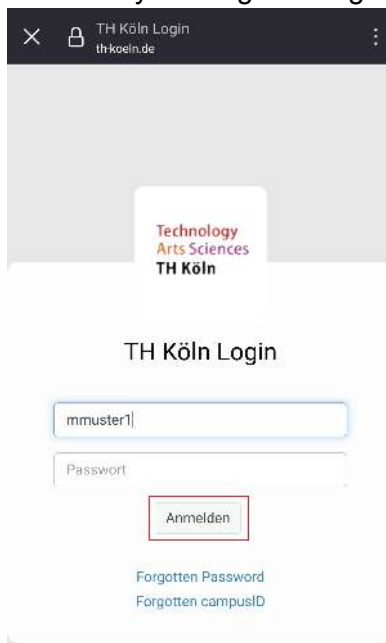
Then enter the following server address:

vpn.th-koeln.de

vpn-gm.th-koeln.de (if you are at the Gummersbach site)



5. A browser window will open and you will be asked to enter your campusID and password. Confirm by clicking the 'Login' button.



You may be asked to enter a second factor.

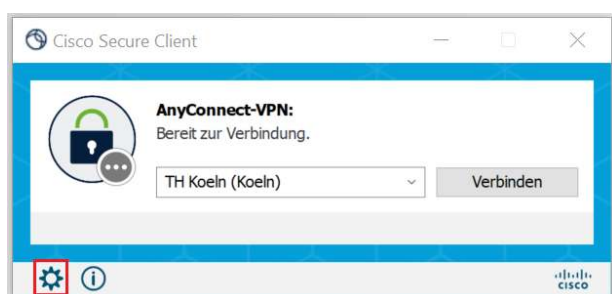
For further information about this can be found at: <https://www.th-koeln.de/mfa>

9. LAN access

If you also want to access devices in your local network (e.g. printers in your home office) in parallel to the VPN connection, you can activate the "LAN access" option.

Attention: For security reasons, this option should not be activated in public networks (e.g. hotel, train, airport, café, ...).

First, launch the Cisco Secure Client software on your computer (Windows, Linux, Mac) and click on the gear wheel in the bottom left.



On the Settings tab, now select "Allow LAN access, ...".

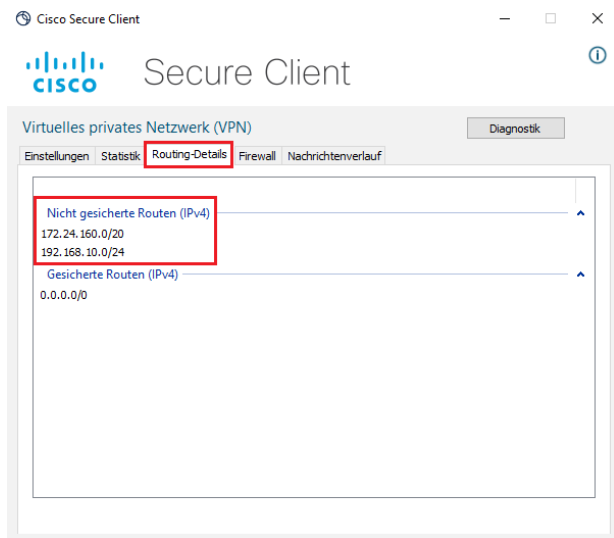


Close the window and connect to the VPN as usual.

You can check whether access to the local network is active as follows:

Open the main window of the Cisco Secure Client and click on the gear wheel again. On the "Routing Details" tab, you will now find the information that the IP address range of your local network is not routed over the secure VPN connection.

9. LAN access



Please note: You can only access your devices via the respective IP address.

10. Contact

Campus IT Service Desk

You can contact our Service-Desk

- on our telephone number [+49 221 8275-2323](tel:+4922182752323),
- at our SelfService-Portal <https://selfservice.th-koeln.de>
- or via our email address support@campus-it.th-koeln.de

during the following service hours:

Monday - Friday 8:00 am - 4:00 pm

On-site support

You can contact our On-site support at Campus Deutz, Campus Südstadt, Campus Gummersbach and Campus Leverkusen.

Further information about location and office hours can be found here:

https://www.th-koeln.de/hochschule/vor-ort-support_25368.php