

Setting up VPN access at TH Köln

Contents

1	Introduction	2
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
5	VPN access on MAC OS X from 10.6	9
5.1	VPN access on MAC OS X – automatic installation	9
5.2	VPN access on MAC OS X – manual installation	13
6	VPN access via integrated Mac VPN client	17
7	VPN access on Ubuntu Linux – manual installation	20
8	VPN access for the iPhone/iPad	23
9	VPN access for smartphones/tablets with Android	24
10	LAN access	26
11	Support	28

1 Introduction

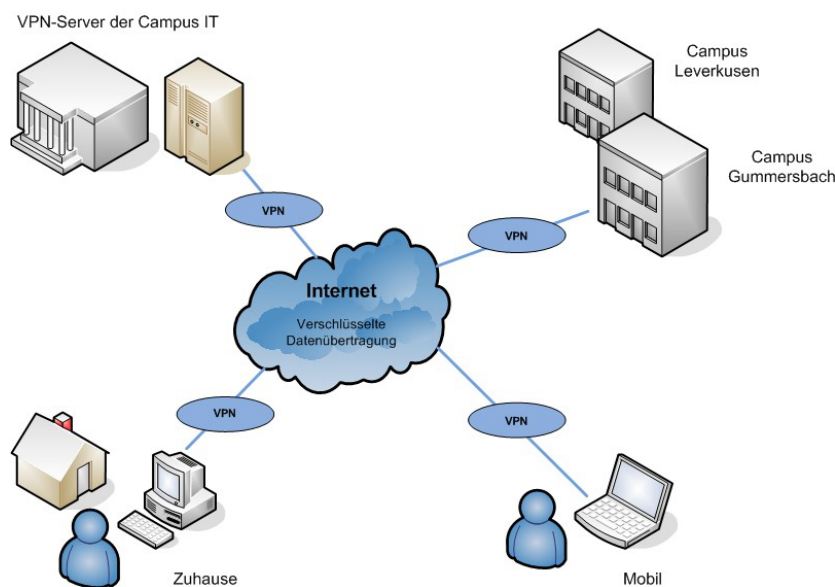
This manual explains in short steps how you, as a member of the University, can establish a secure connection to the network of Technische Hochschule Köln – University of Applied Sciences.

Data connections via the public network (Internet) are not secure. It is useful to secure your personal data, especially in public WLAN 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 Technische Hochschule Köln – University of Applied Sciences 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.



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:

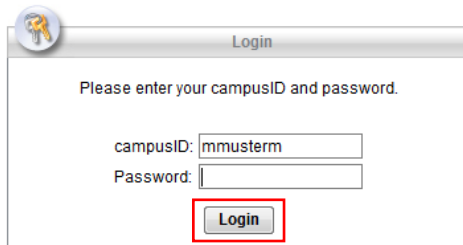
- A WLAN-enabled device, e.g. notebook/PC with the operating system Microsoft Windows, MAC OSX, Linux or a smartphone or tablet with an active Internet connection
- A campusID. All University members receive a personal user account – called a campusID. This user account allows access to various Campus 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.

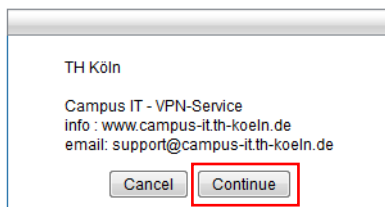
You can find further information on the Campus IT website: www.th-koeln.de/campus-it

4 VPN access on Windows

1. To set up VPN access, please enter the following address in your browser:
<https://vpn.th-koeln.de>
<https://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. Please click on “Continue” in the following window.



4. 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

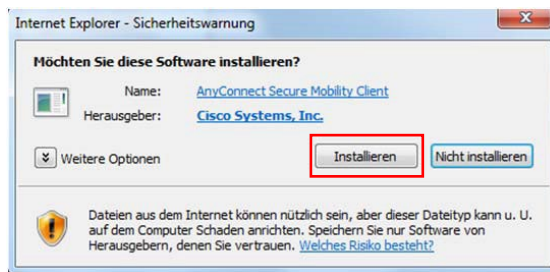
1. The automatic installation starts automatically if all requirements are met.

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.

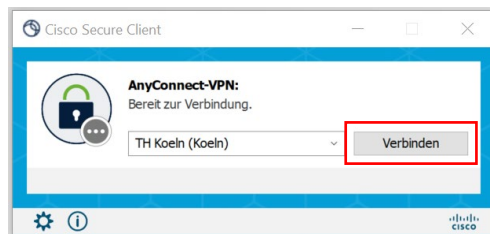
2. You may receive security warnings.
In each case, check the box *“I accept the risk and want to run the application”* and click *“Run”*.



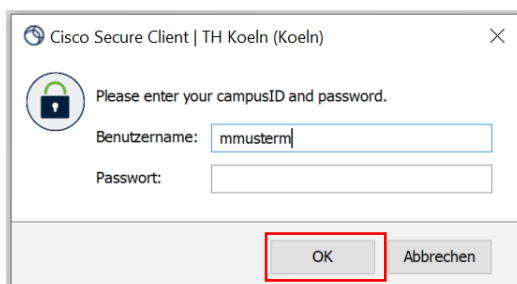
3. Please confirm the message *“Do you want to install this software?”* by clicking on *“Install”*.



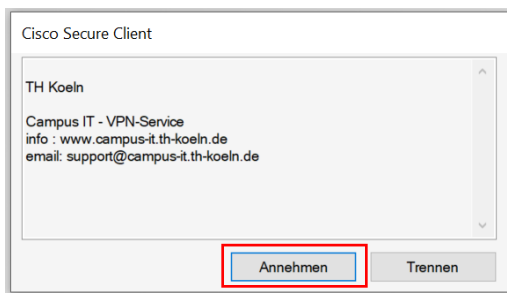
4. To use the Secure Client now, open the program and click on *“Connect”*.



5. Then please enter your campusID login details.



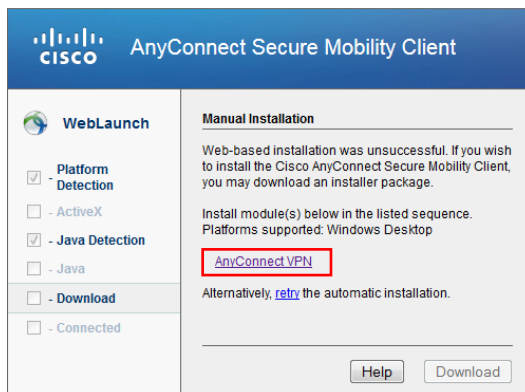
6. There is now an active VPN connection. Confirm the connection notification with “Accept”.



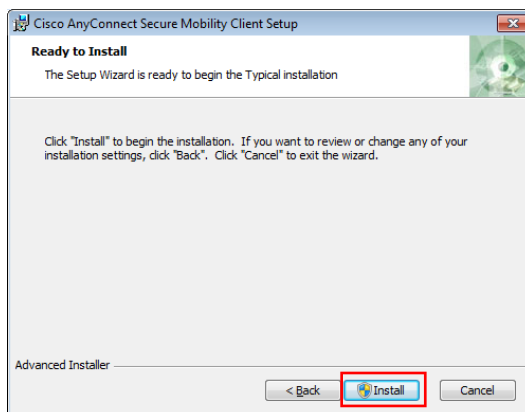
Please note: You can launch the Secure Client manually at any time to connect with it or disconnect the existing connection. You can find the program in the Windows Start menu.

4.2 VPN access on Windows - manual installation

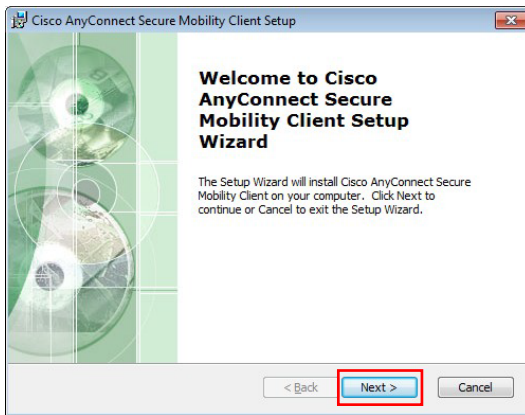
1. If the automatic installation fails, please click on the suggested link in the window below.



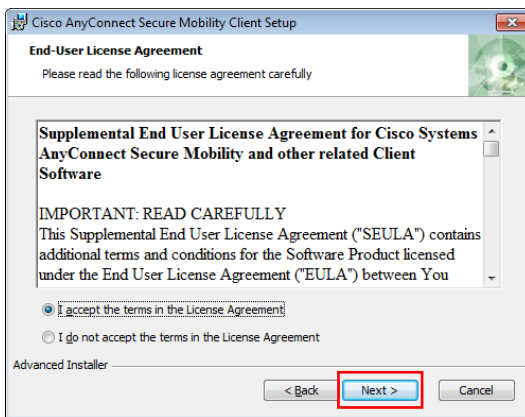
2. In the following window, confirm the start of the installation by clicking on “Install”.



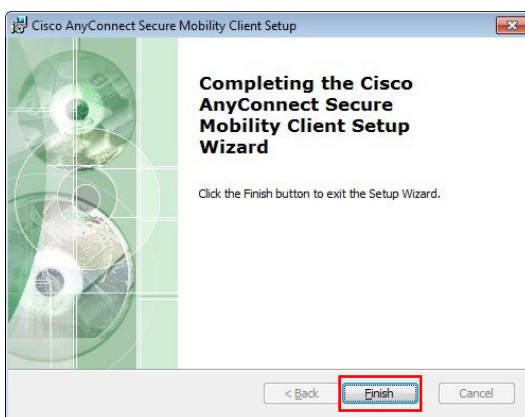
- Please click on “Next” in the following window.



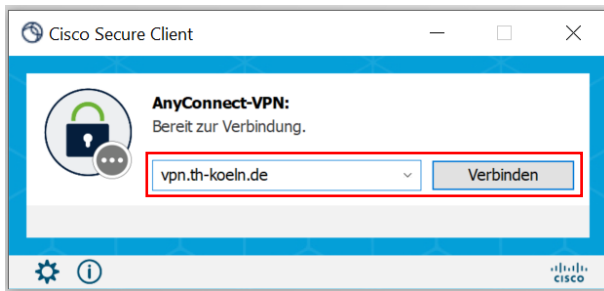
- Please read the Software License Agreement and select “I accept the terms in the License Agreement” and then click on “Next”:



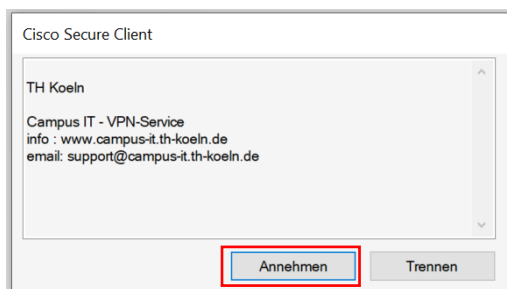
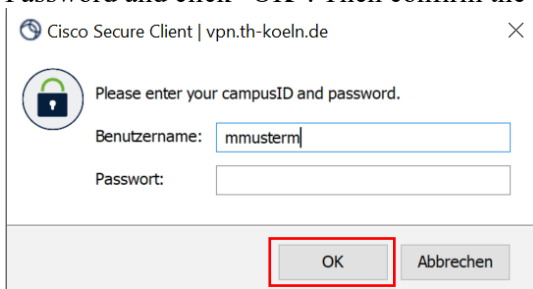
- In the following window, please click on “Install” to confirm the start of the installation.
- After successful installation, please click on “Finish” in the following window.



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



- A new login window will open. Enter your campusID login details in the fields Username and Password and click "OK". Then confirm the message from the VPN server with "Accept".



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

5 VPN access on MAC OS X from 10.6

To use the secured VPN connection, you need a Mac with the operating system MAC OS X Snow Leopard or later and a valid campusID.

With a Mac with OS X version 10.6 or higher, you have two options for setting up a secure VPN connection:

Installation of the Cisco Secure Client (automatic or manual).

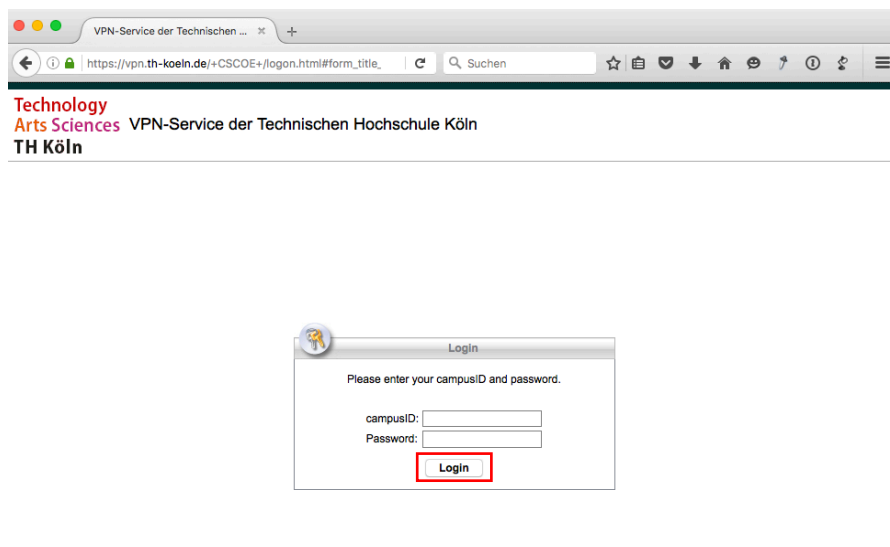
Or setting up an OS X VPN connection (Cisco IP-Sec). No additional software needs to be installed for this. This connection offers the additional advantage that you still have network access at home to devices in the home network (NAS, PCs, network printers, etc.). Data transmission outside your home network or to the Internet is carried out via the secure and encrypted IP-Sec VPN connection.

5.1 VPN access on MAC OS X – automatic installation

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

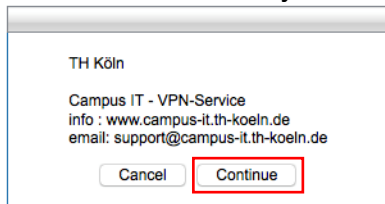
<https://vpn.th-koeln.de>

<https://vpn-gm.th-koeln.de> (if you are at the Gummersbach site)

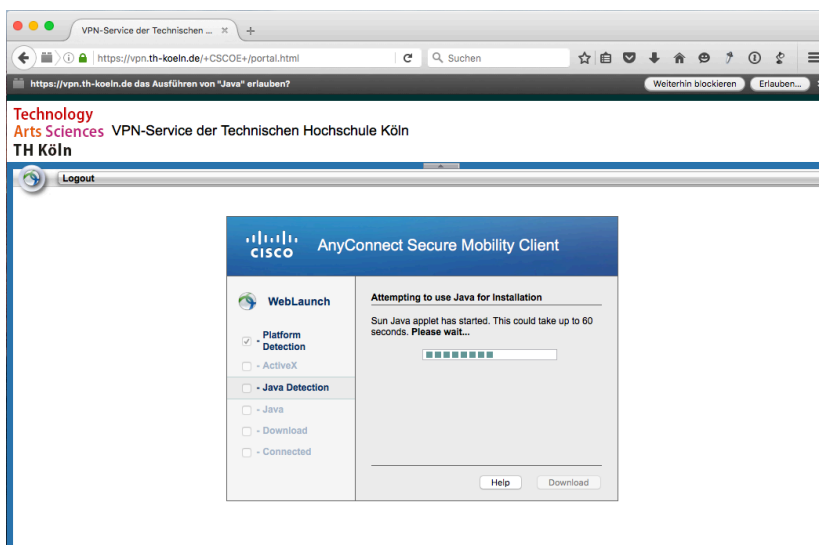


2. Please enter the login details for your campusID on the website and then click on “Login”.

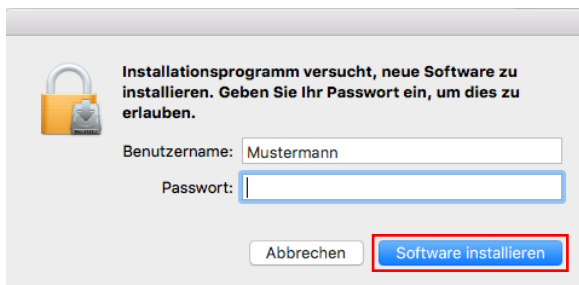
3. Please click on “Continue” in the following window:
After a short verification phase, either the automatic installation will start or you will be asked to install manually.



4. With the [automated installation](#) of the Cisco Secure Client, the download and installation is carried out automatically. Notification windows provide you with information on the installation status.

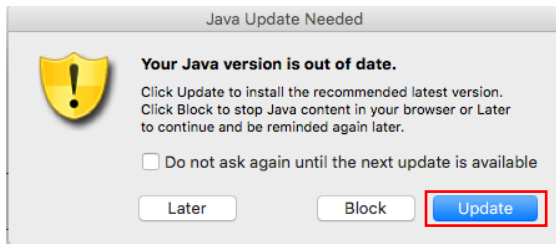


- Installation requires you to enter your Mac’s administrator ID.

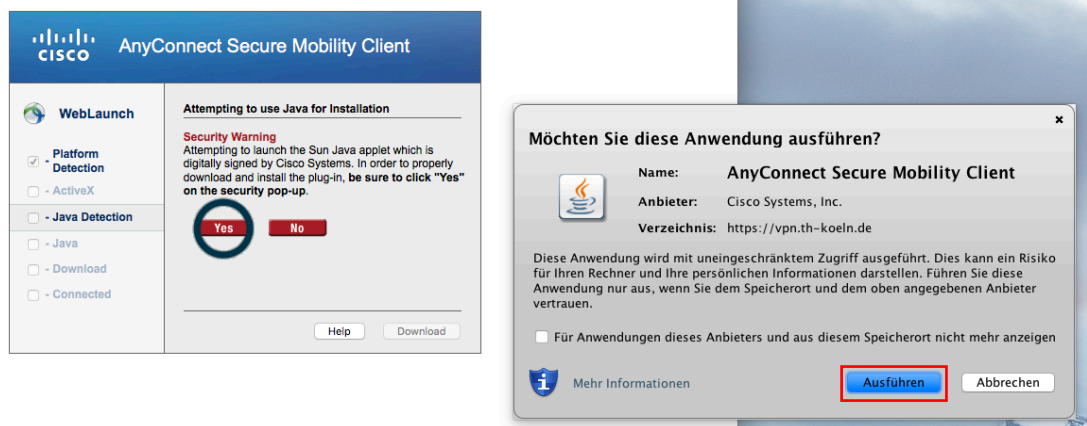


- You may be asked to confirm the trustworthiness of certificates. Click on “Next” here.

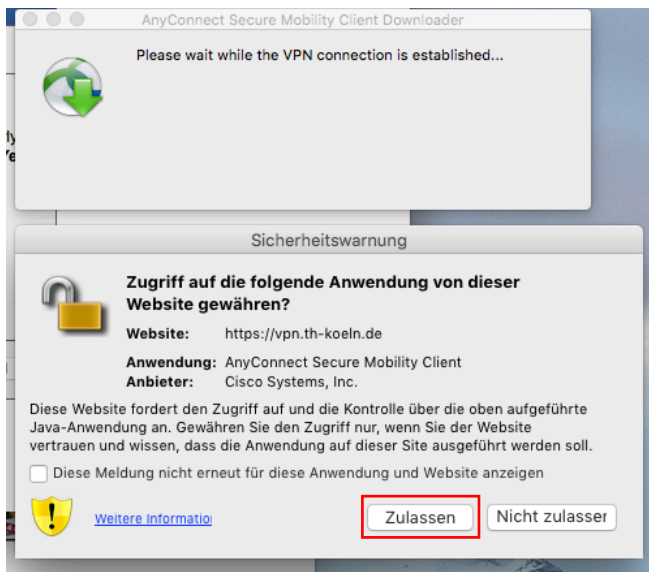
5. Your Java version may be out of date and you will need to update it.



6. Then confirm the launch of the client with “Run”.



7. The following security warning can be confirmed with “Allow”.

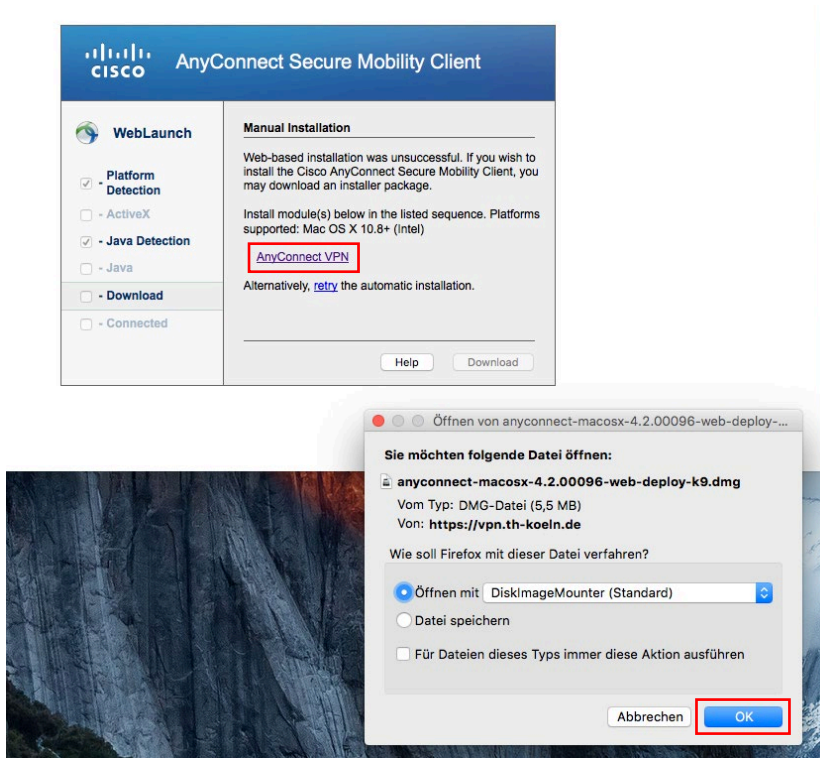




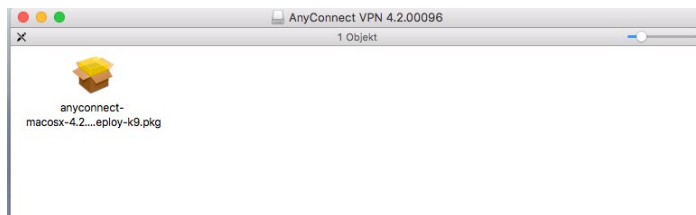
The Secure Client is now installed and launched.
A corresponding application icon is displayed on the taskbar and in the dock.

5.2 VPN access on MAC OS X – manual installation

1. For the [manual installation](#), follow the steps above up to point 4 and then continue as follows:
2. Click on Download to open a confirmation dialog, which you confirm with OK.



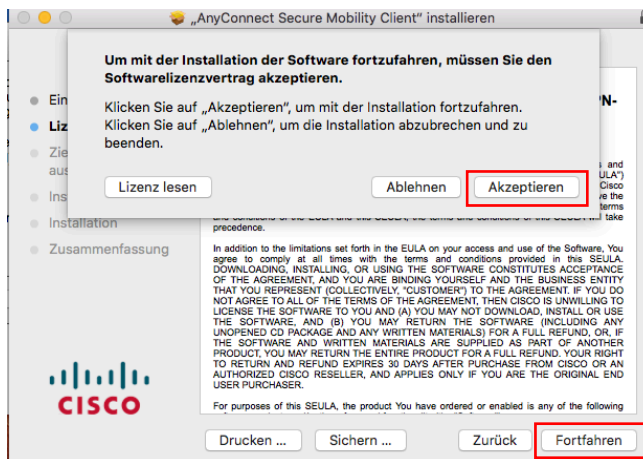
- Then launch the installer by double clicking on it.



- Click on "Continue" in the welcome window.



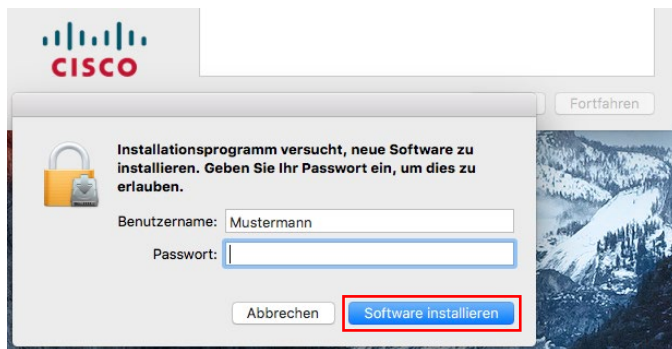
- Please read the Software License Agreement and then also click on "Continue" and accept the software license agreement by clicking on "Accept".



6. To perform the standard installation, click on “Install”.

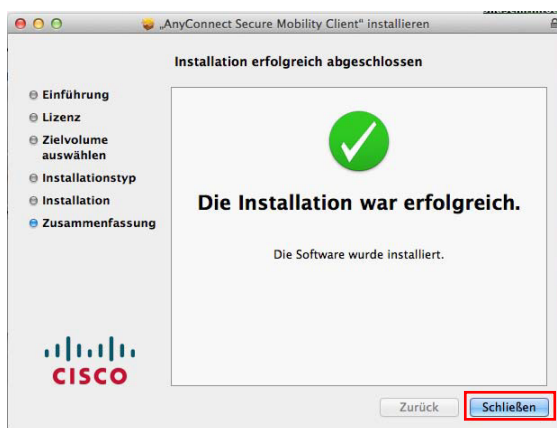


Please note: You may be asked for your password



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

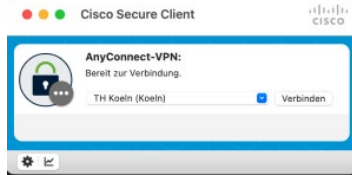
Now click on “Close” to end the manual installation.



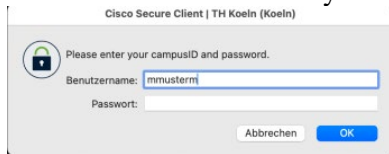
8. You can launch the Cisco Secure Client manually at any time to establish the VPN connection or to disconnect the existing connection.

Select the corresponding program icon on the taskbar, in the dock or the finder (under Programs/Cisco).

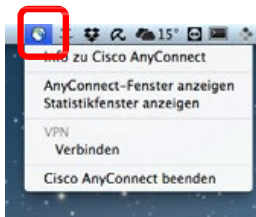
9. To reconnect, select “Connect VPN”.



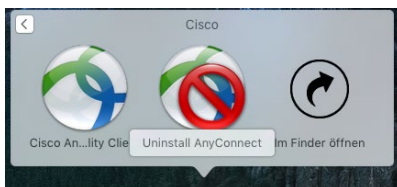
10. You will be asked to enter your campusID login details.



If you want to disconnect an existing VPN connection, select “Disconnect VPN”.



Taskbar



Dock



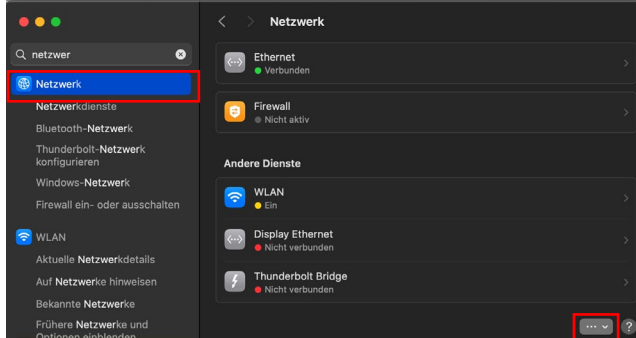
Finder

6 VPN access via integrated Mac VPN client

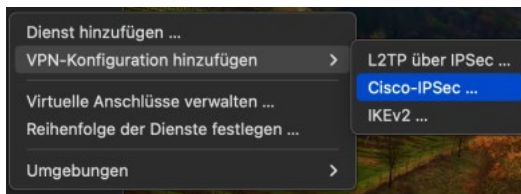
Instead of the Secure Client described above, it is also possible to use the Mac's own VPN client, Cisco IPSec, for the VPN connection. You will find the setup instructions below:

1. To do this, select the Network under System Preferences.

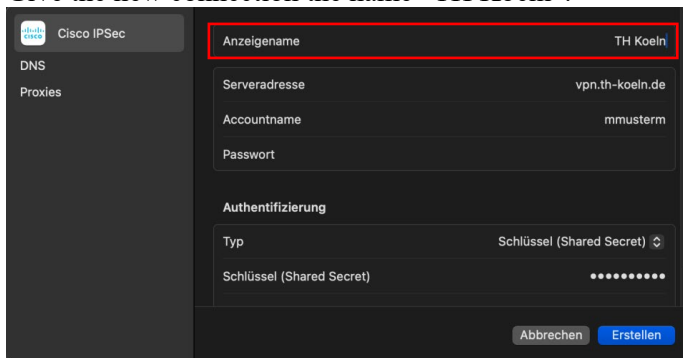
Click on the “...” sign to establish a new connection.



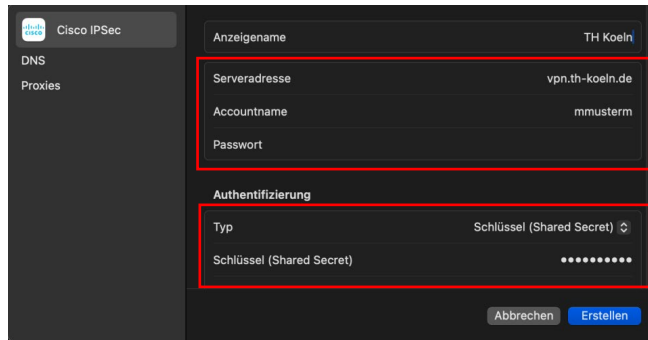
2. Select “Add VPN-Configuration” and then the sub item “Cisco-IPSec”.



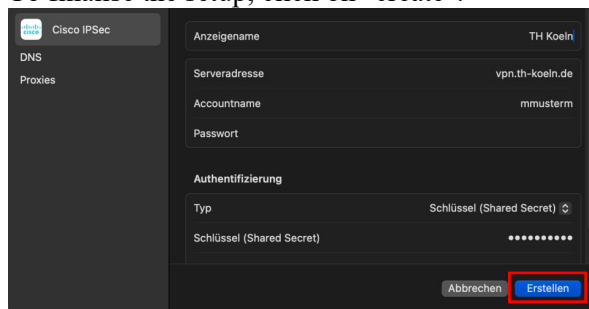
3. Give the new connection the name “TH Koeln”.



4. On the same screen, type in `vpn.th-koeln.de` as the server address, enter the campusID (account name) and the campusID password (password). Then enter "KoelnerDom" as the shared secret and FHK-VPN as the group name.

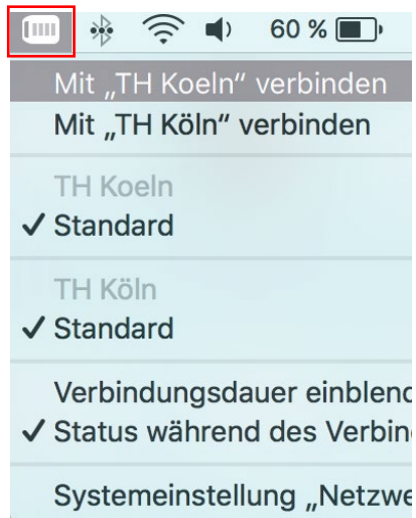


5. To finalise the setup, click on "create".



6. From now on, you can connect with VPN (Cisco IPSec) via Network in System Preferences. If the login is successful, a notification about the active VPN connection will appear and you can confirm it with "OK".
7. You can manually start the Mac IPSec VPN connection at any time to connect to the University VPN or to disconnect an existing connection.

8. Select the corresponding program icon on the task bar.
To reconnect, select:
Connect with “TH Koeln”.



In the following window, please enter your campusID login details as usual.

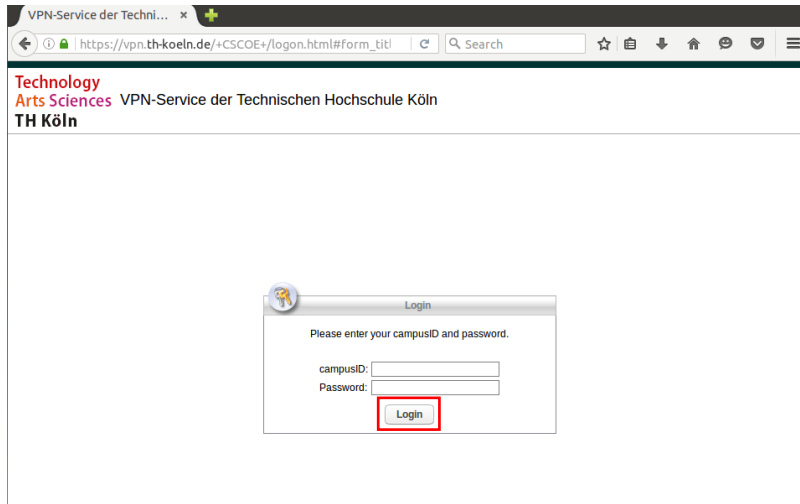
9. If you want to disconnect an existing VPN connection, select “Disconnect connection to “TH-Koeln”” via the program icon.

7 VPN access on Ubuntu Linux – manual installation

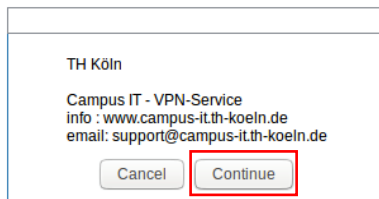
1. Please enter the following address in your browser:

<https://vpn.th-koeln.de>

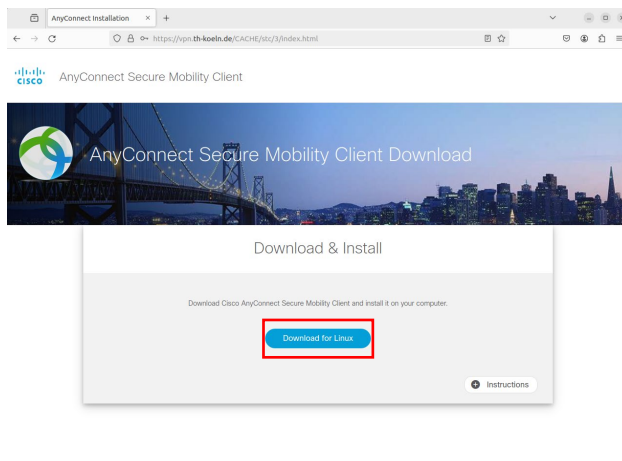
<https://vpn-gm.th-koeln.de> (if you are at the Gummersbach site)



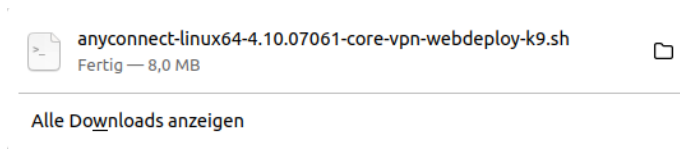
2. On the website, please enter the login details for your campusID account and click on “Continue”.



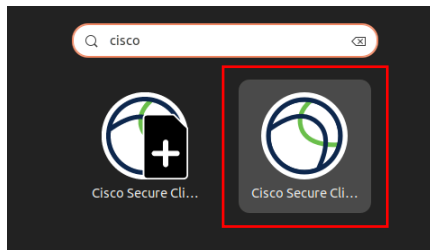
3. Now you can download the installer by clicking on the AnyConnect VPN link.



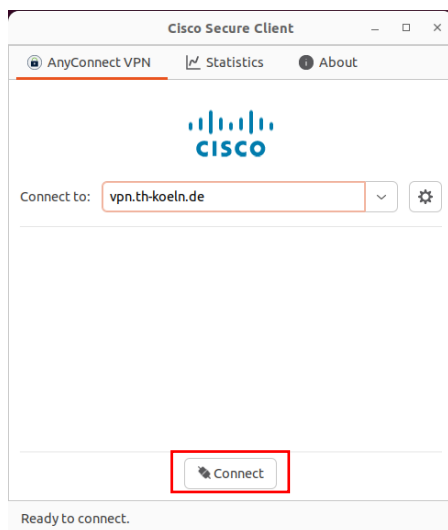
- The following file will be downloaded.



- First execute the following command:
`sudo apt-get update`
- Then launch the previously downloaded file with the following command:
`sudo sh /home/*username*/Downloads/ anyconnect-linux64-4.10.07061-core-vpn-webdeploy-k9.sh`
- You will then see the installed Cisco Secure Client as a program



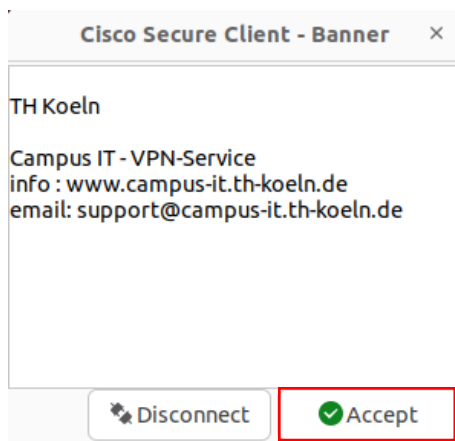
- Launch the Secure Client and enter the address of the VPN server you want to connect to vpn.th-koeln.de or vpn-gm.th-koeln.de (for the Gummersbach site)



9. Click on “Connect” and then enter your campusID login details.

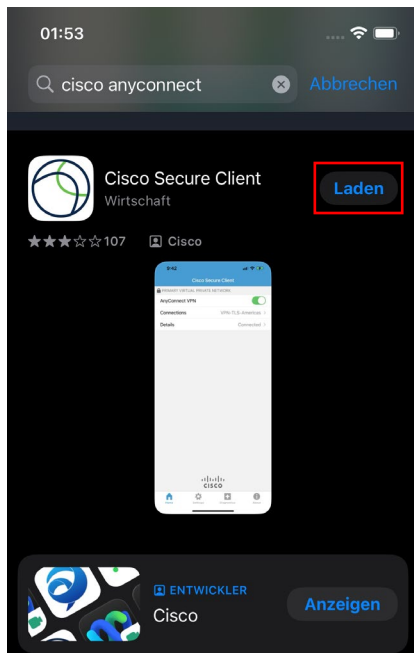


10. Finally, confirm the message of the VPN server by clicking on “Accept”.



8 VPN access for the iPhone/iPad

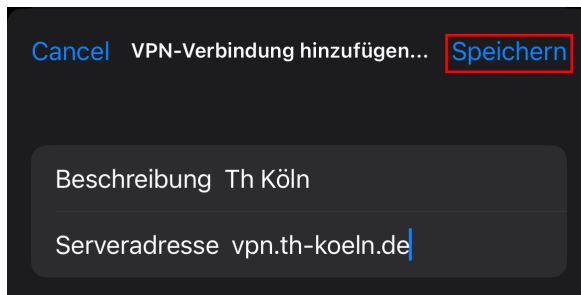
1. Search the AppStore for Cisco Secure Client and install the app.



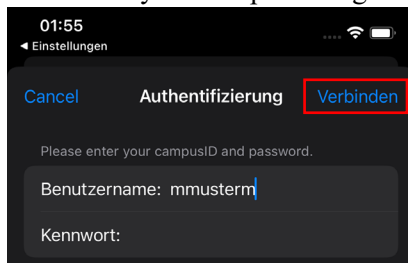
2. Configure VPN client: Settings -> General
Select the menu item VPN and Add VPN configuration.

Description: TH VPN

Server address: vpn.th-koeln.de



3. Then enter your campusID login details and click on "Connect"



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

9 VPN access for smartphones/tablets with Android

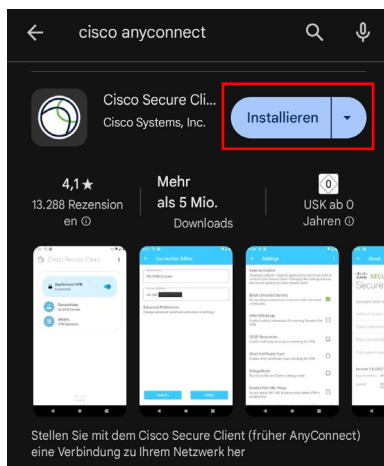
Supported devices for AnyConnect ICS (Ice Cream Sandwich):

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

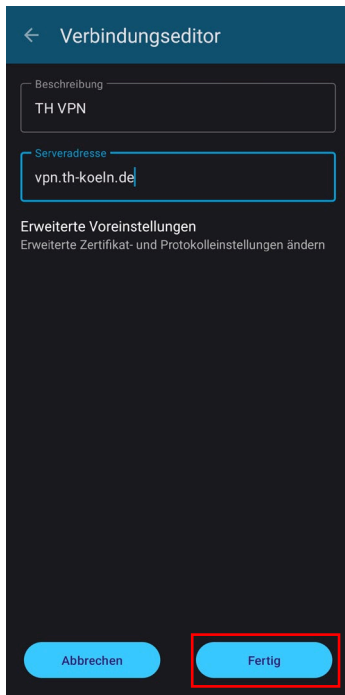
Note: To download the Cisco Secure Client-AnyConnect-app, you need Internet access on your device; this can be via WLAN or mobile communications. Another requirement is the Google Play app (AKA Play Store, formerly Market), which is installed on Android devices as standard. For more information, please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

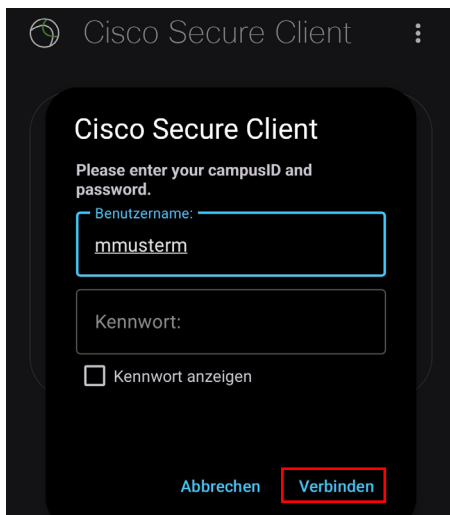


3. After you have selected and installed the appropriate version of the Cisco Secure Client-AnyConnect app, open the advanced settings in the app and select “Add new VPN connection”.

- As the description, choose the name: TH VPN.
Then enter the following server address:
vpn.th-koeln.de
vpn-gm.th-koeln.de (for the Gummersbach site)



- Enter your campusID login details in the following window and click on “Connect”.



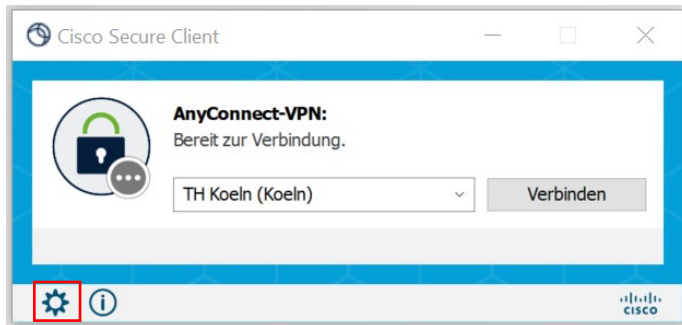
- Then confirm the connection notification and you are connected to the VPN client.

10 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 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 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.



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

11 Support

If you have any further questions, please contact Campus IT. You can reach us on +49 (0)221/8275-2323 during the following office hours:

http://www.campus-it.th-koeln.de/support/standort_service/index.html

You can also contact us by e-mail at support@campus-it.th-koeln.de.