

VPN Remote Connections



This page is outdated!

Cisco AnyConnect is discontinued in Metropolia. Please use the Palo Alto GlobalProtect VPN instead.

- [VPN Connection via GlobalProtect Service](#)

The VPN remote connection is available to all Metropolia users. It is needed to connect to Metropolia's internal services from outside. Internal services include Financial and Administrative Services, Koulutuskalenteri and instruction supporting project servers, educloud, and laboratory systems. VPN access to internal services is determined by user role and terminal device.

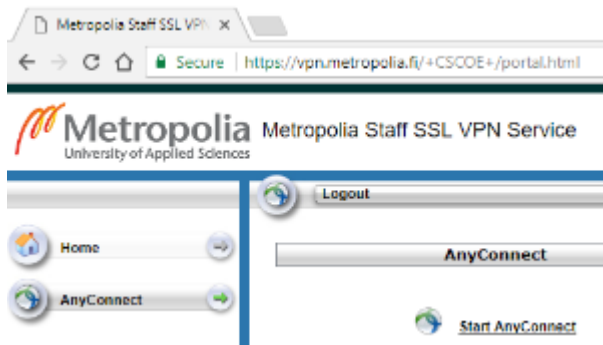
- [Install the VPN client on a home computer](#)
- [Install and use the VPN client on a mobile device](#)
- [Using VPN on Metropolia Windows computers](#)
- [Installation and use of the VPN client on macOS computers](#)
- [Services available via VPN](#)
 - [Devices in Metropolia maintenance](#)
 - [The users' own devices](#)
- [Other remote services](#)
 - [VPN restrictions](#)

Install the VPN client on a home computer

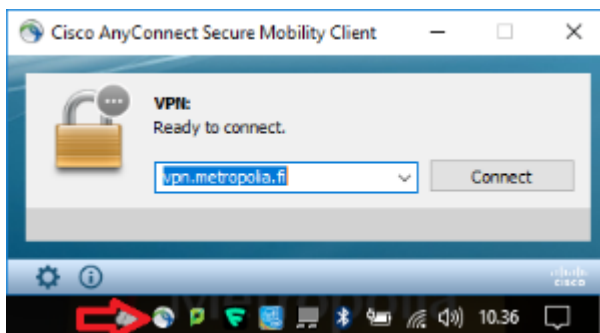
The use VPN you need AnyConnect client. It is preinstalled on all Metropolian laptops. Do not install or update the client yourself on Metropolia computers.

Users are allowed to install AnyConnect client on their own devices (Windows and Mac computers).

1. Log in at <https://vpn.metropolia.fi>
2. On the left, select AnyConnect.
3. Select Start AnyConnect.



4. Log in at vpn.metropolia.fi or at



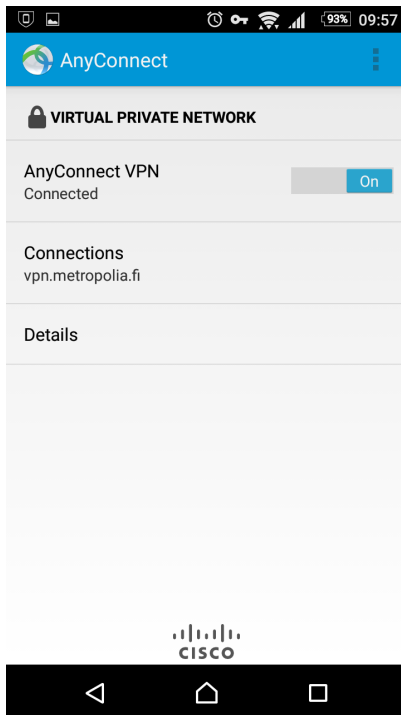
5. Read detailed instructions for Windows at: [Install and Use VPN Utility Program Installation on Your Own Computer](#)

Install and use the VPN client on a mobile device

1. Open your device's app store and search for "anyconnect" or "cisco anyconnect".



2. Install the app on your device.
3. Add a new VPN connection: Connections > Add New Connection.
4. In the Server Address field, enter vpn.metropolia.fi
5. Select Done.
7. Select AnyConnect VPN to open the connection.

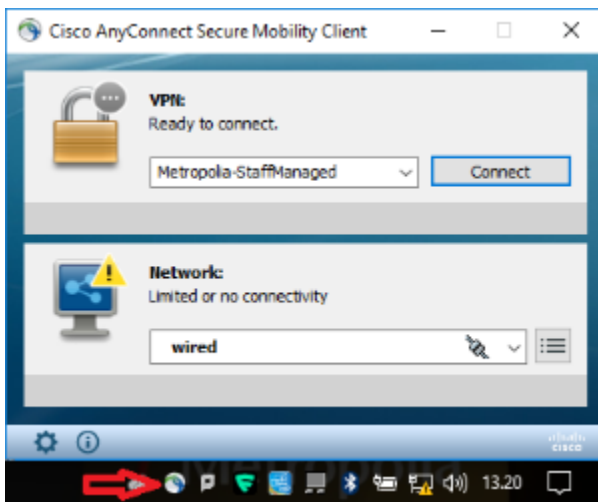


8. Enter your Metropolia username and password.
9. Log out by selecting Exit in the upper right, when you end the connection.

When the connection is secure, a lock icon is shown in the upper bar in Android. In iPhone there is a text VPN.

Using VPN on Metropolia Windows computers

1. Click on the Cisco AnyConnect icon in the lower right of the screen.
2. In the "Ready to connect" drop-down menu, select Metropolia-StaffManaged or, on student computers, Metropolia-StudentManaged.
3. In the Cisco AnyConnect Secure Mobility Client window's VPN box, click on Connect.
4. Log in to the service with your Metropolia username.



Installation and use of the VPN client on macOS computers

On Apple macOS computers, Cisco AnyConnect is automatically installed by Managed Software Center updates.

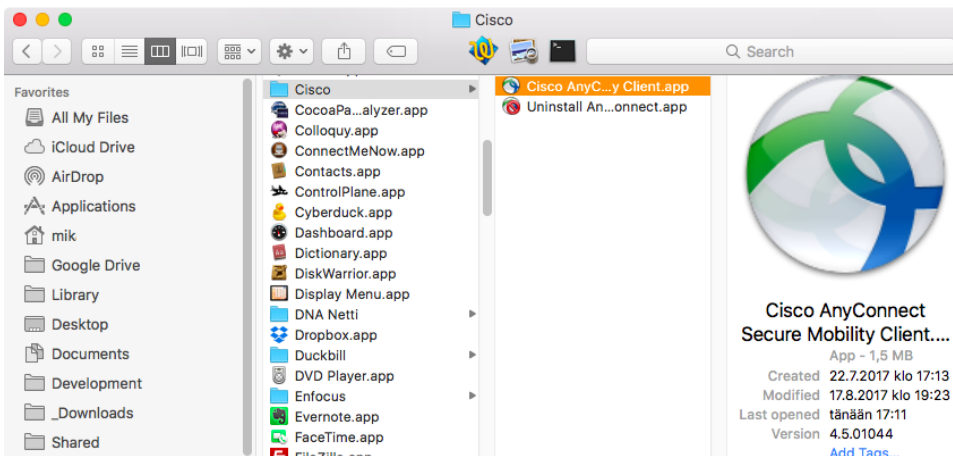
On you own a macOS computer, download and install the VPN client as follows:

1. Log in at <https://vpn.metropolia.fi>
2. On the left, select Anyconnect.
3. Select Start AnyConnect.

The program is installed in **/Applications/Cisco/Cisco AnyConnect Secure Mobility Client.app**.

To open VPN remote connection:

1. Start **/Applications/Cisco/Cisco AnyConnect Secure Mobility Client.app**.

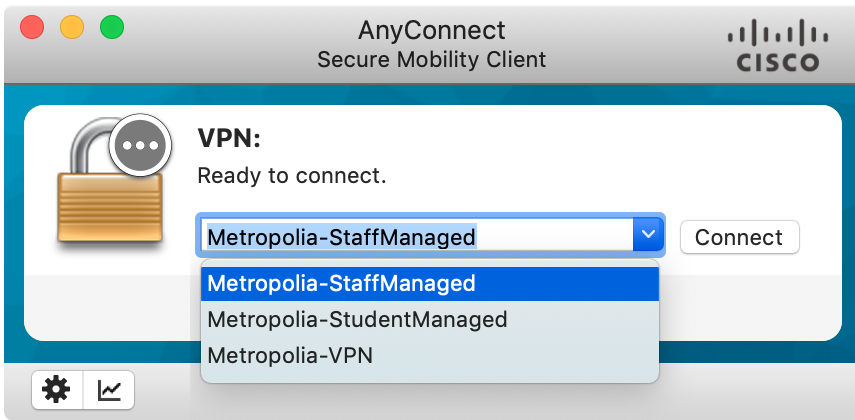


2. Select a VPN connection profile

a) Mac computer in Metropolia maintenance

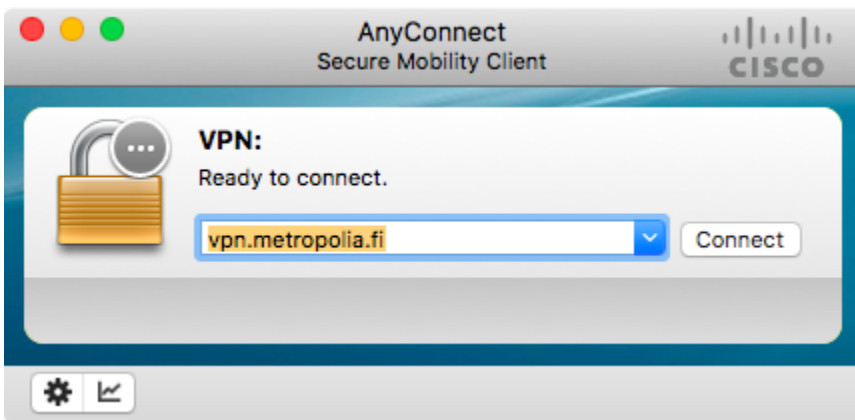
Under "Ready to connect" text, in the drop-down menu, select "Metropolia StaffManaged".

If the computer is used by students, select "Metropolia-StudentManaged".



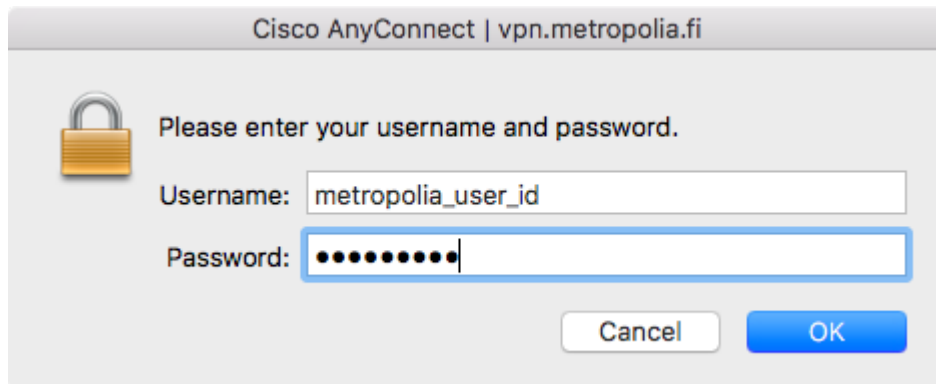
After selecting the address, click on **Connect**.

b) A Mac computer that is not maintained by Metropolia or if the address field is blank, type in the field the address: vpn.metropolia.fi.

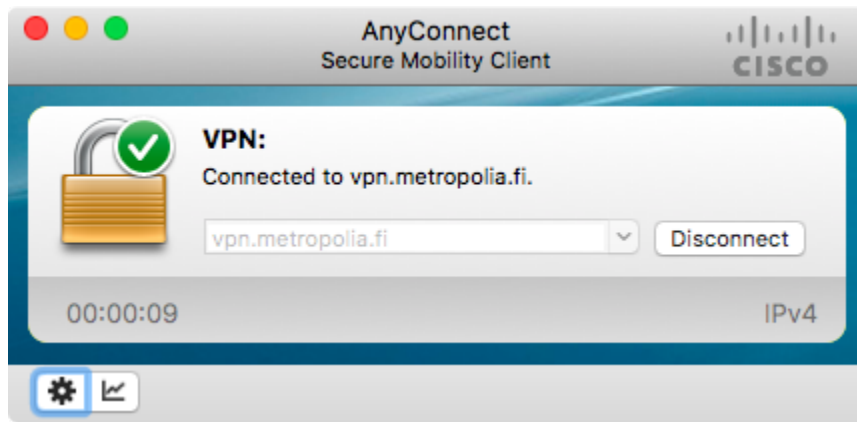


After selecting the address, click on **Connect**.

3. Enter your Metropolia username and password. Click on **OK**.



4. When the connection is established the connection window looks like this:



The AnyConnect VPN connection status is shown also in the AnyConnect icon in the upper menu bar.

When the connection works a lock is shown in the icon:



To close the VPN connection, stop the VPN client.

The VPN connection has a time limit after which an unused connection is closed.

The connection is also automatically closed then the computer shuts down or goes to sleep.

Services available via VPN

Which services are available via VPN connection depends on user role and the terminal devices used. Access to internal resources is limited because of information security considerations.

In VPN connection, the user's network traffic originates in Metropolia network, which makes it possible to use remotely such internet services that are restricted by the user's IP address or that require a Finnish source address.

Services that are available via VPN can be restricted temporarily or permanently if required by the information security situation.

Devices in Metropolia maintenance

In general, all the same services that are available on staff workstations and PC classroom workstations, are available also on devices that are in Metropolia maintenance. For information security reasons, network drives and many internal resources are available remotely only on devices that are owned by Metropolia and the information security of which is administered by Metropolia IT Services.

The users' own devices

Information security on users' own devices is not controlled in any way. Because of this, only restricted VPN services are available for all users on their own devices. Primarily users can access staff's and students' browser based services from their own devices. Access to services that requires database connections, licenses, and other internal resources are considered on a case-by-case basis because of the information security risk that poorly maintained devices might create.

Access to educloud virtual servers, project servers and laboratory environments is open from instruction's devices as appropriate. Remote access to systems used in instruction may be restricted also because of the license terms of the background systems and applications.

Other remote services

Other ways of using Metropolia IT services include

- Securedesktop for staff, [Securedesktop Remote Service](#)
- [SSH tunneling](#)
- Webdisk browser interface, <https://webdisk.metropolia.fi>
- Library databases, <http://ezproxy.metropolia.fi> and [instructions](#) (in Finnish)

VPN restrictions

Use a VPN connection only when necessary and prudent to ensure sufficient capacity!

Do not use a VPN connection while using online learning platforms, video conferencing services, or watching videos.

Services available remotely via VPN may be temporarily or permanently restricted when security or availability of critical services so require. Metropolia's VPN connection is not designed for crisis situations.

OMA, Moodle, Zoom, Teams, or Skype for Business don't need a VPN connection to work.

Notice: When traveling abroad, remember to always open VPN when using network connections, including fixed networks and password protected networks. VPN protects the connection with encryption which prevents outsiders from reading the network data. Make sure before your trip that VPN works.