LabraNet

Remote access guide

LabraNet

Remote access guide

INTRODUCTION

This is a guide for using LabraNet services remotely through a VPN connection. First part of the guide explains how to connect to LabraNet VPN with step-by-step instructions for the most common operating systems. Second part includes guides for accessing your home folder.

VPN Connection

You need a LabraNet user account for the connection.

Generic options for the connection are:

Connection type: SSTP
Authentication type: MS-CHAPv2 (Linux/Mac OS) EAP-MSCHAPv2 (Win)
VPN server address: vpn.labranet.jamk.fi (should resolve to 195.148.26.226)

Firewall:
If for some reason your firewall blocks web traffic, you need to allow outbound TLS/SSL connections (TCP port 443)

User information:
Domain: LABRANET
User name: Your LabraNet username
Password: Your LabraNet password

LabraNet

Remote access guide

Windows 11

The easiest way to create the VPN connection is to use the *Network & internet* –application. Open the start menu and type *settings* in the search window. Select the *Network & internet* from the navigation menu. Then select *VPN*.

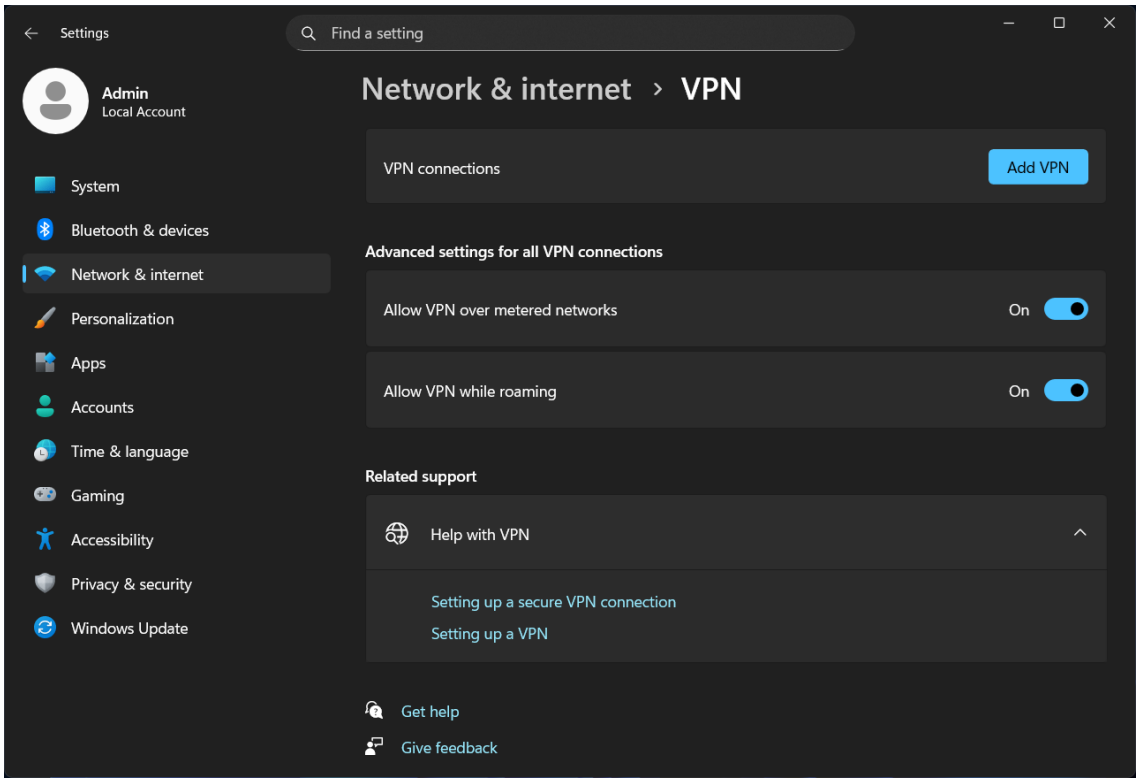

Figure 1. Network & internet - VPN

Click *Add VPN* in the application and fill in the connection information.

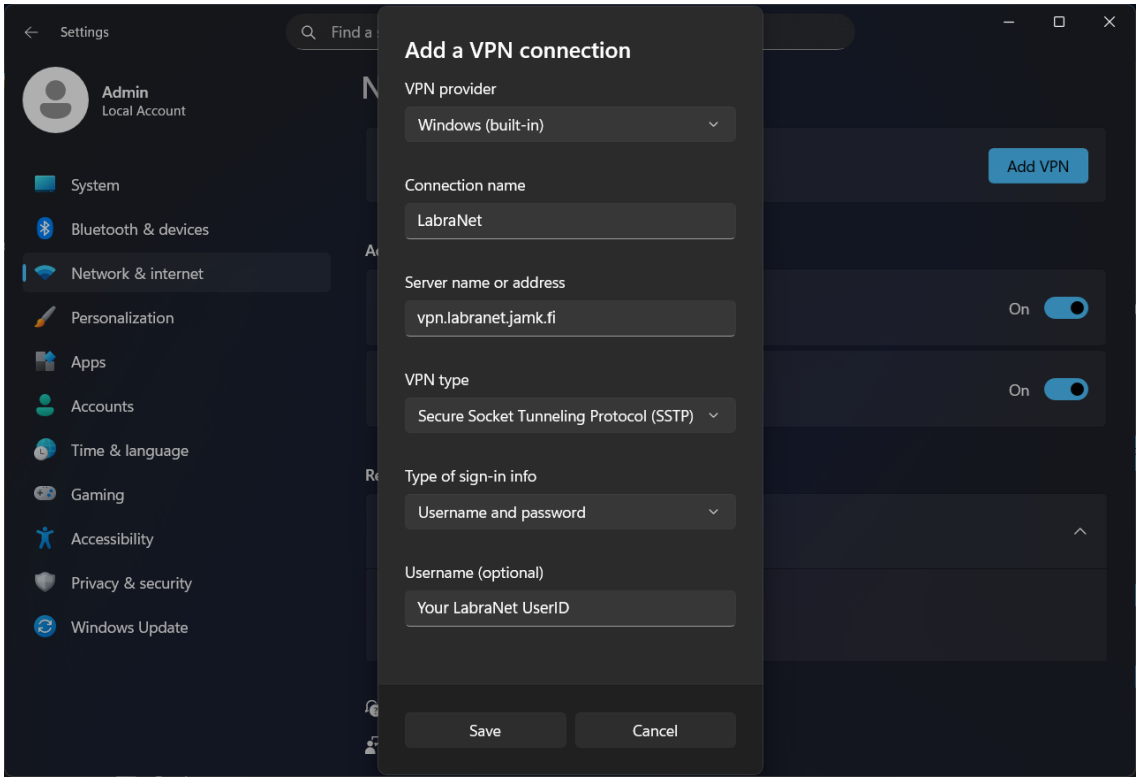

Figure 2. Add a VPN connection

Edit the connection settings by opening *Network and Sharing Centre* and choosing *Change adapter settings*. Right-click the VPN Connection and select *Properties*. Navigate to the *Security* tab and apply the following settings.

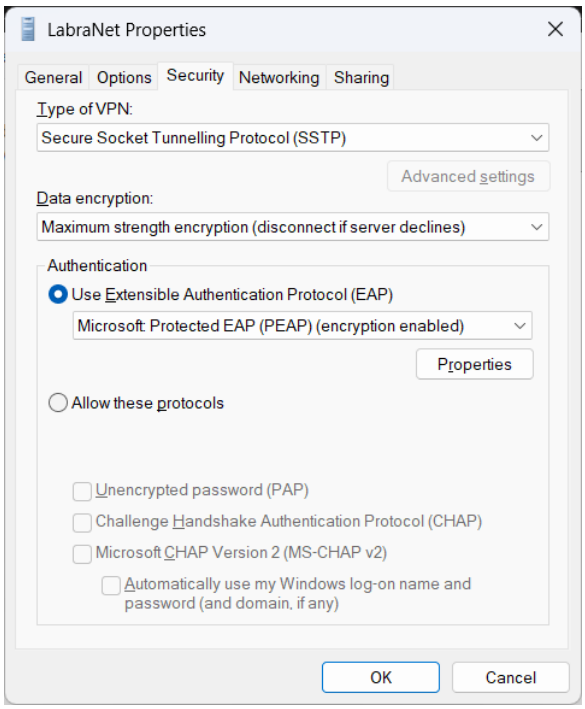

Figure 3. VPN connection security settings

Click *OK*.

To ensure functioning DNS, more configuration is recommended. Windows uses *smart multihomed name resolution* to optimize name resolution. This feature causes DNS to return incorrect IP addresses for some public LabraNet services when automatic interface metric assigns the LabraNet VPN connection lower *or* equal priority compared to the connecting devices physical network adapter.

For end users, this shows up as LabraNet services (including helpdesk and gitlab) not responding when the VPN tunnel is up. It is possible to correct this either by bumping the VPN connection up in priority or lowering the physical adapters priority. This guide focuses on altering the priority of the VPN connection.

Open *Network and Sharing Centre* and select *Change adapter settings*. This view shows all the network connections your device has.

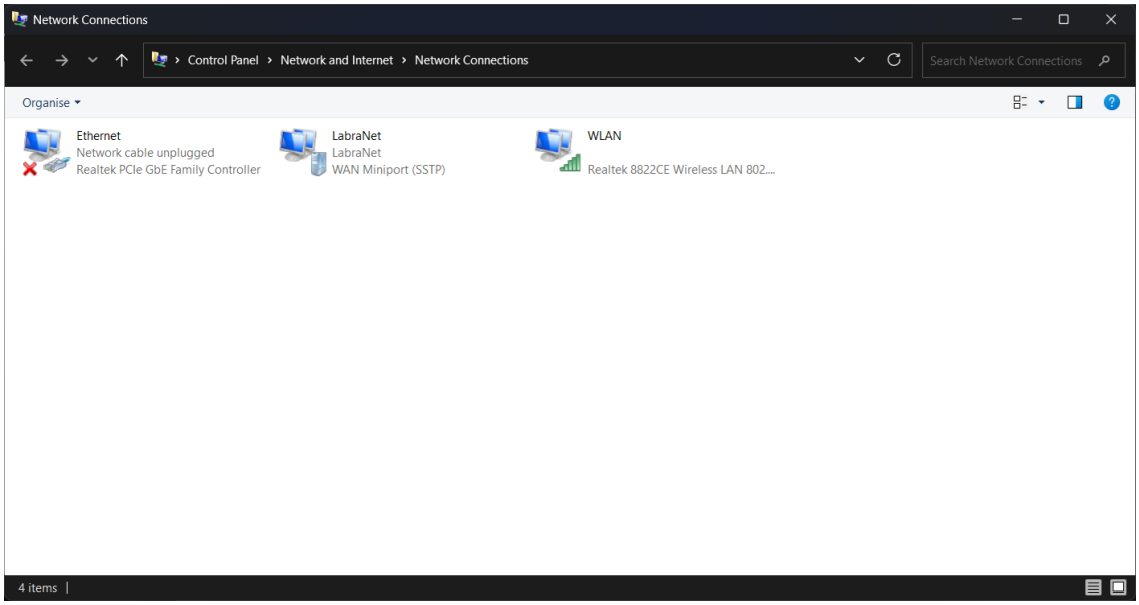

Figure 4. Network adapter settings

Note that the name of the active physical network connection is *WLAN*. This may vary depending on the number and type of physical adapters, and installed software.

Now issue the following PowerShell command by opening *Windows PowerShell* or *Terminal* and typing in:

Get-NetIPInterface | Select InterfaceAlias, InterfaceMetric | Sort InterfaceMetric

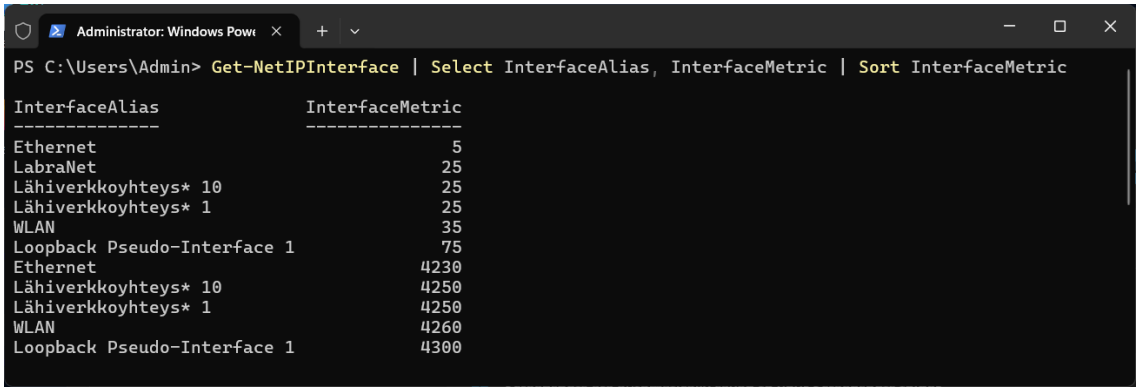

Figure 5. List network interface metrics

Note that the InterfaceMetric value assigned to the connection *WLAN* is 35 in this example. Please use the lowest number for your active connection as reference point. Whereas if connecting via the *Ethernet* interface we can note that the value assigned is 5.

Now select the newly created LabraNet VPN connection from *Network and Sharing Centre -> Network Connections* and select *Properties*. Choose the *Networking* tab and modify both the *Internet Protocol Version 6* and the *Internet Protocol Version 4* connection items (1).

Click open either one by selecting *Properties* (2). Then open the advanced settings by clicking *Advanced* (3). Clear the checkmark from *Automatic metric* and assign a value that is **less** than what the PowerShell command returned (4). This example sets the metric at 1 which is less than the 35 listed for the *WLAN* connection or the 5 listed for *Ethernet*.

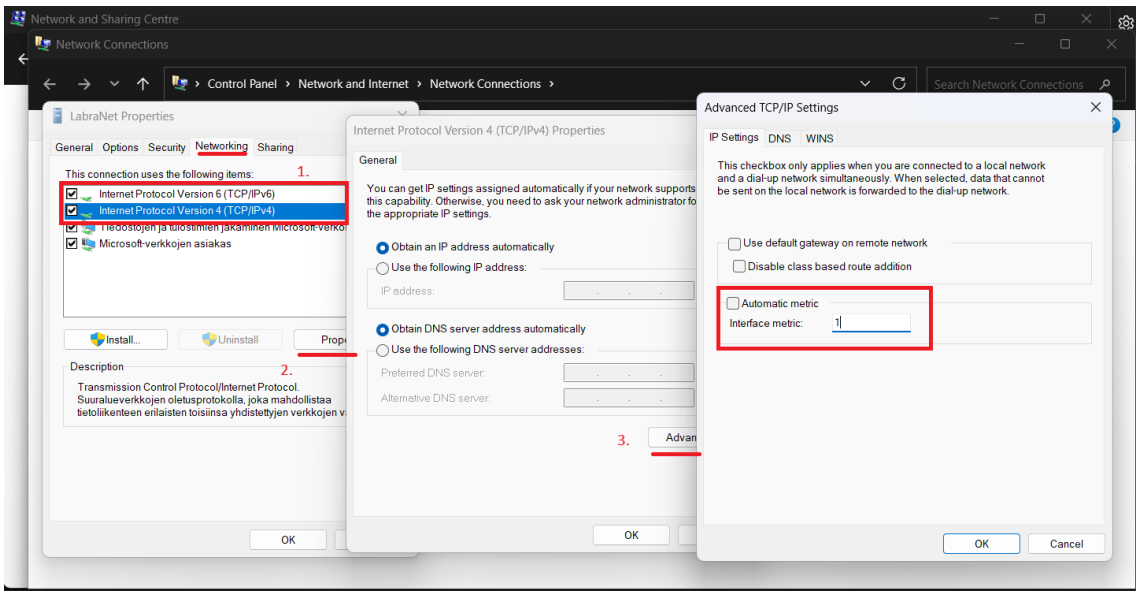

Figure 6. Modify the metric value

Modify both the IPv4 and IPv6 settings the same way and click *OK* at each setting window to save the settings.

Now connect to LabraNet via the VPN connection and issue the previous PowerShell command again to check that your settings were saved correctly.

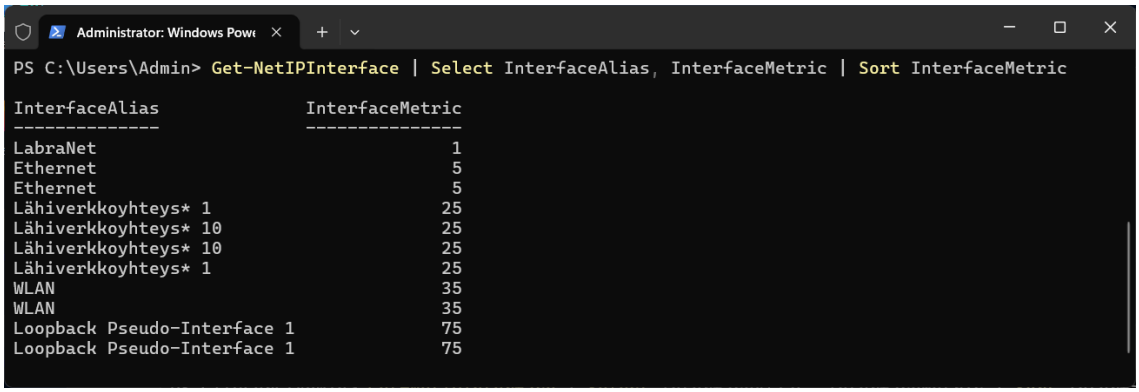

Figure 7. Check the values

LabraNet VPN should now be the first connection listed with the lowest *InterfaceMetric* value thus having the highest priority.

Note, if the Windows client is not able to parse the SSTP server certificate chain correctly you will get a warning at first connection attempt.

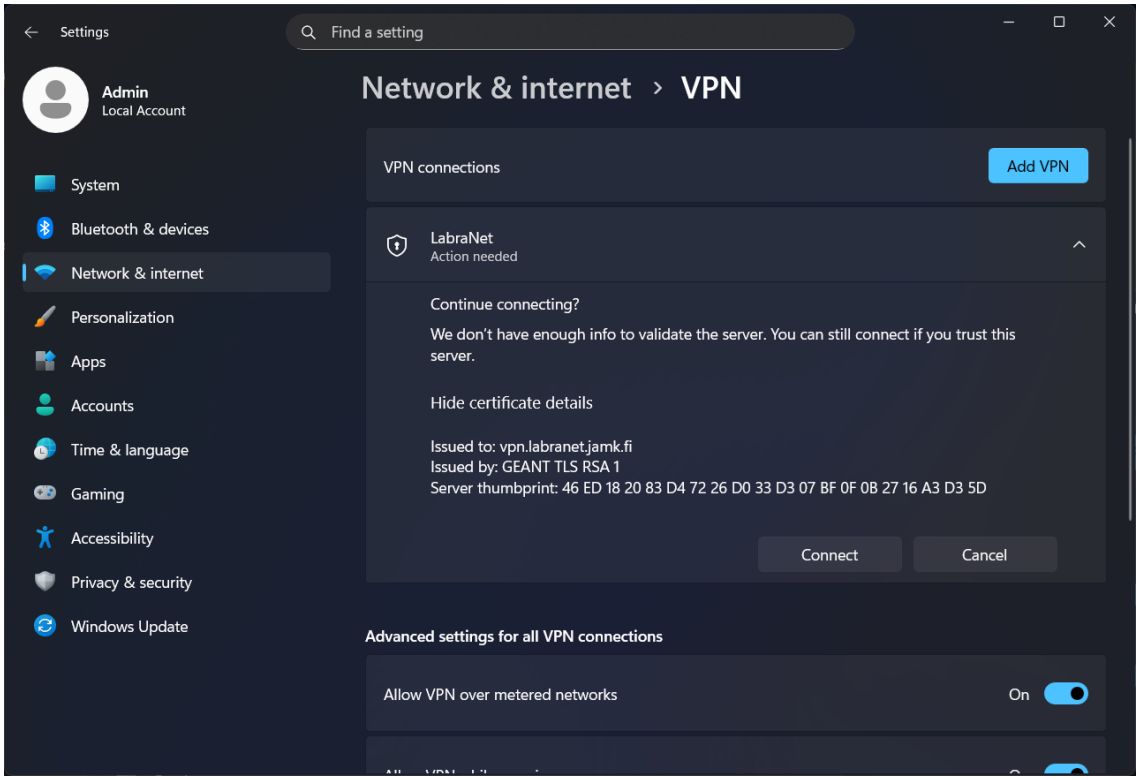

Figure 8. LabraNet SSTP connection certificate prompt

You can continue connecting to the VPN server by clicking *Connect* again. You can view the certificate by clicking *Show certificate details*. Figure 8 above shows the currently installed certificate. Contact Labranet helpdesk if this issue prevents you from working.

Mac OS X

These configurations have been tested up to version 26.3 (Tahoe).

IKEv2

LabraNet VPN server has been configured to also use Internet Key Exchange version 2. IKEv2 has a native client in Mac OS and it is easy to configure. IKEv2 is implemented with IPSec and user/password authentication.

The downsides to IKEv2 are problems with Network Address Translation and the lack of connection options (e.g. split tunneling is not possible by default). Generic options for the connection are:

Connection type: IKEv2
VPN server address: vpn.labranet.jamk.fi (should resolve to 195.148.26.226)

Firewall:
UDP Port 500 (IKE)
UDP Port 4500 (NAT-T)
IP protocol 50 (ESP)

User information:
Account Name: Your LabraNet username
Password: Your LabraNet password

Open *Network Preferences* from *System Preferences* to create the IKEv2 VPN. Select the … button under the available connections on the left side of the application window.

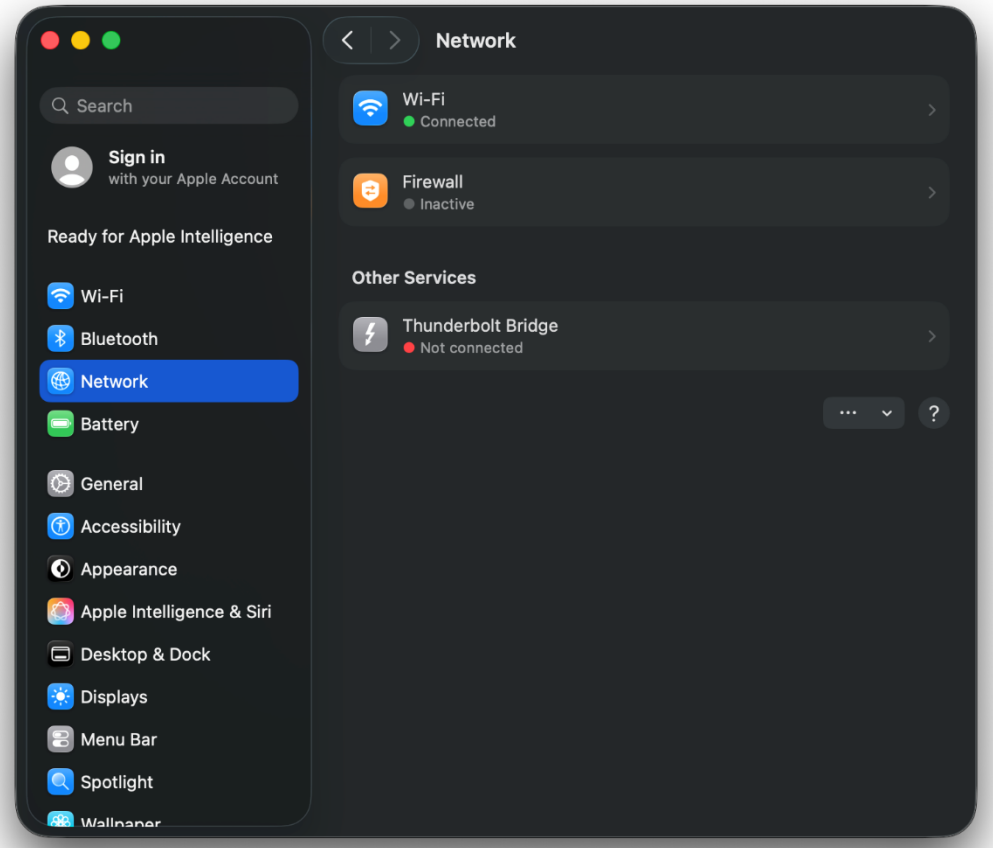

Figure 9. Network preferences

Select *Add VPN Configuration* and *IKEv2*.

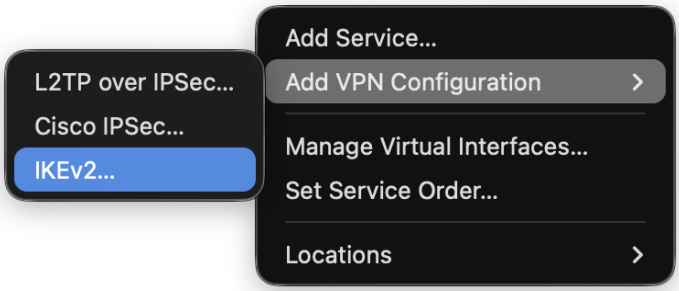

Figure 10. Connection type

Fill in the configuration for the IKEv2 connection as shown below.

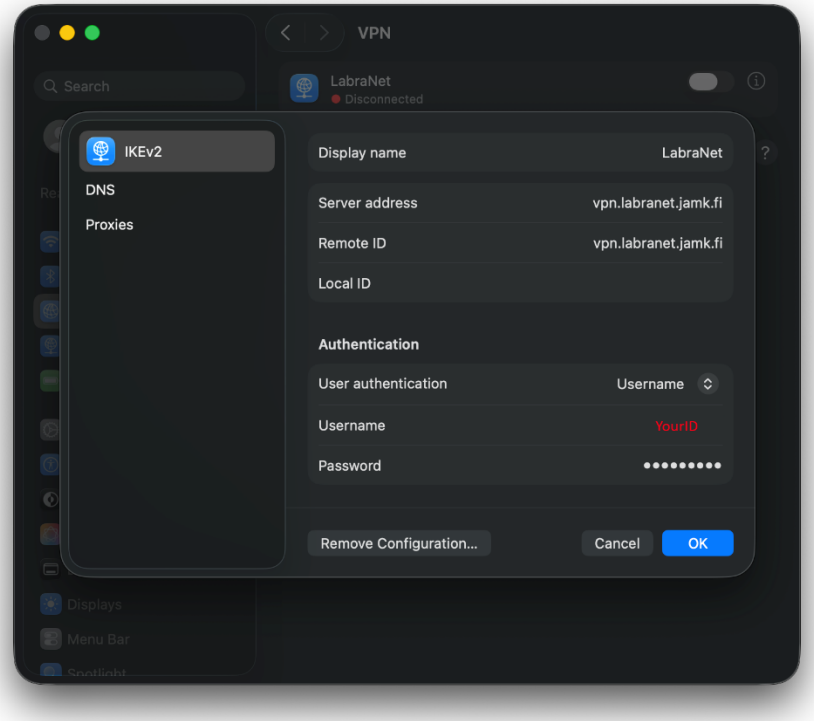

Figure 11. Add Configuration

Toggle the switch button to connect to LabraNet VPN.

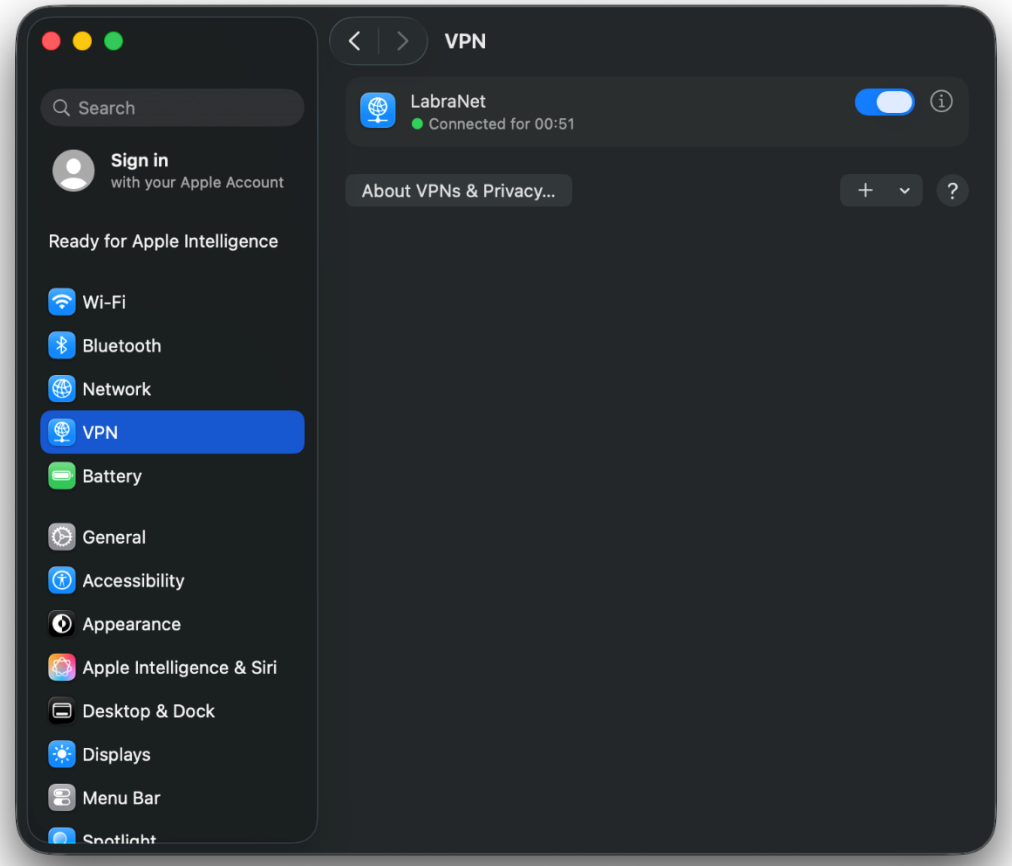

Figure 12. Connect to the VPN server

Linux (Graphical)

These apply to Linux-distributions which use Network-Manager. In the examples we use Ubuntu 24.04 LTS. Other distributions may use a different style in the UI for Network-Manager, but the basic steps are the same.

The first step is to install sstp-client. This can be done by adding the personal packet archive of the author of network-manager sstp-client.

sudo add-apt-repository ppa:eivnaes/network-manager-sstp
sudo apt update
sudo apt install network-manager-sstp network-manager-sstp-gnome sstp-client

Alternatively, you can find the packages here if you want to manually install them.

https://gitlab.com/sstp-project/sstp-client
https://gitlab.gnome.org/GNOME/network-manager-sstp

Open the Network settings and press the highlighted + button to set up the VPN connection.

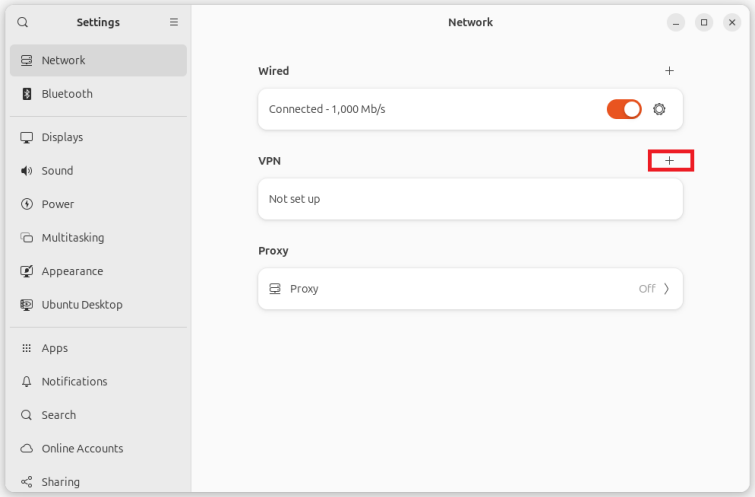

Figure 13. Network settings

Choose Point-to-Point Tunneling Protocol (SSTP).

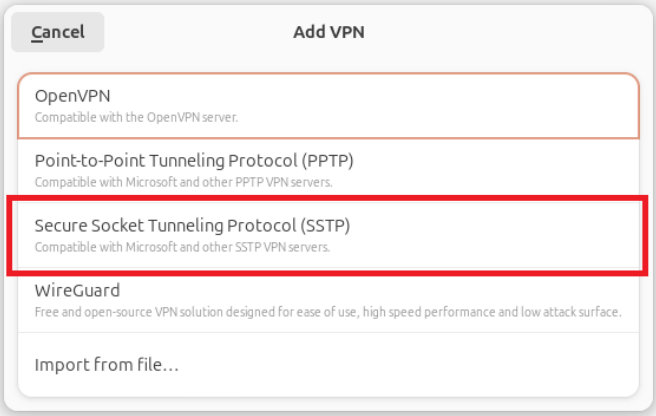

Figure 14. Connection type

On the next dialog, give the connection a name, fill in the gateway and your username and password.

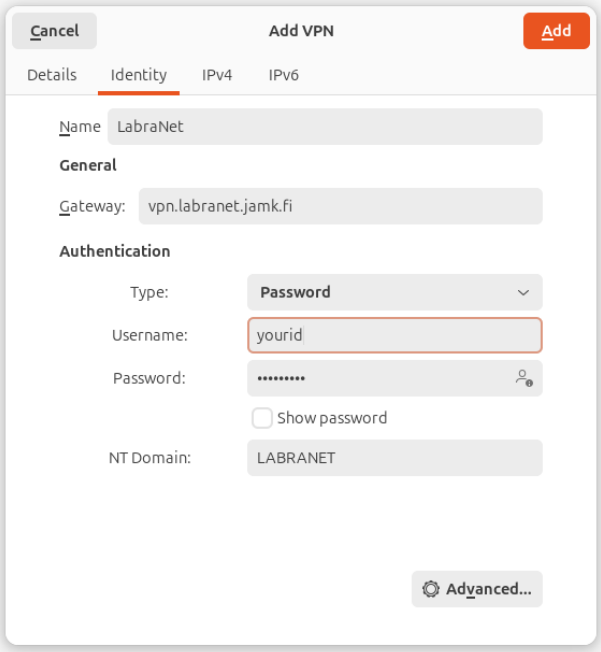

Figure 15. VPN Connection settings

Next click the *Advanced*-button. From the next dialog, select the following authentication method: *MS-CHAPv2*. You can leave other selections unchecked.

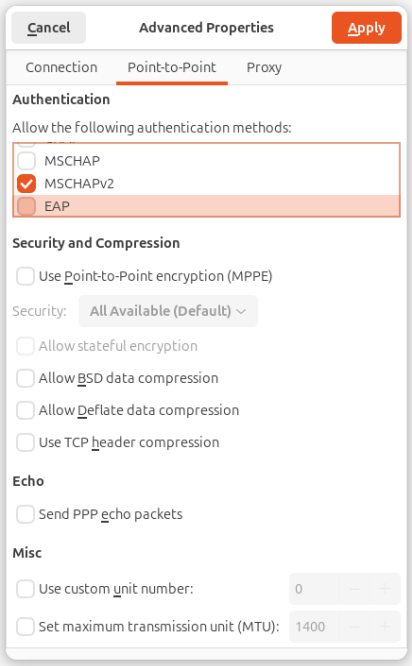

Figure 16. Advanced settings

Click *OK* and *Add*. You can now connect to LabraNet using this VPN connection from the tray applet.

Advanced routing

VPN tunnel can be used in full tunnel or split mode. With full tunneling, all traffic is routed through the VPN connection. In split mode, only traffic to resources in LabraNet networks are routed via the VPN connection.

This behavior can be changed by enabling or disabling the use of gateway on the VPN connection.

Windows

In Windows operating systems, the default mode is Full tunnel. To change the setting, go to VPN connection Properties and *Networking* tab. Select *Internet Protocol Version 4 (TCP/IPv4)* and click *Properties*. Click the *Advanced* button and on the next dialog, *Use default gateway on remote network*. When the setting is checked, Windows uses Full tunnel mode.

Mac OS

Currently, it is not possible to configure split tunneling on Mac OS IKEv2 client. All traffic will be routed through the VPN. You can manually create routes to change this behavior. Manual routing is beyond the scope of this guide. Additional notes and help are available through LabraNet helpdesk.

Linux (Graphical)

The VPN tunnel works best in Full tunnel mode. To change this, edit the *IPv4 Settings* of your VPN connection.

Check the *Use this connection only for resources on its network* checkbox. Per documentation of sstp-client, this is not recommended. When using split tunneling, ensure your distributions dhcp client supports *rfc3442-classless-static-routes option 121*. Otherwise routes to LabraNet services need to be added by hand.

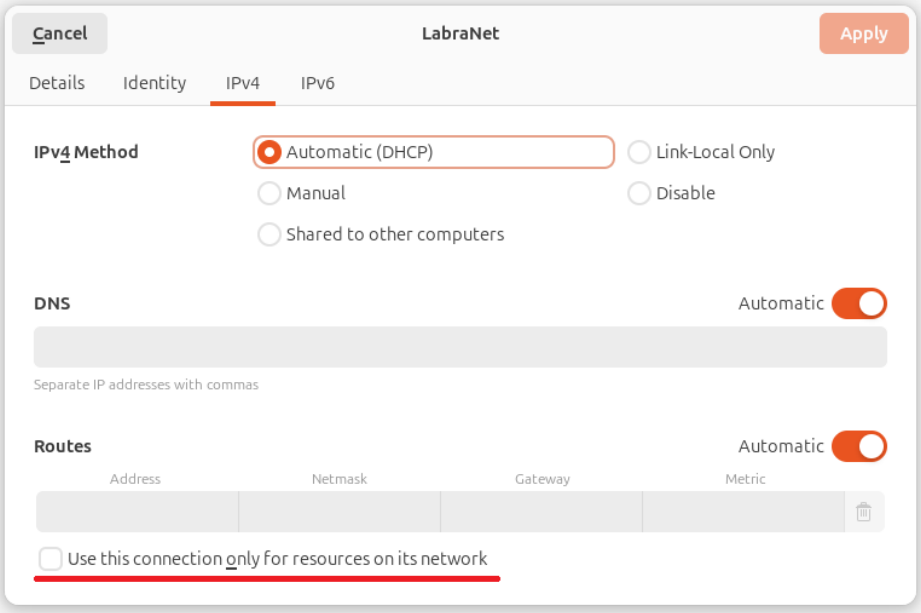

Figure 17. Advanced routing

Accessing Shares

After successfully connecting to VPN, you can now use shared files in a similar manner as from local LabraNet workstations. Here are guides for connecting to your home folder or any public share.

NOTE: In some cases, the VPN connection DNS servers will not be used immediately. In this case, wait for a few minutes and try again.

Your home folder can be found in the path
\\storage.labranet.jamk.fi\homes\userid

You can also use public shares, such as *\\ghost.labranet.jamk.fi\temp*.

You need to authenticate to the shares separately with your LabraNet account information. Provide the username either in format *LABRANET\userid* or *userid@LABRANET*.

Replace the *network-path* with desired network path in the following examples.

More information on accessing your LabraNet shares can be found in *http://student.labranet.jamk.fi/remote-using-your-home-folder/*

LabraNet

Remote access guide

Windows

Open *File explorer*. Write the path to the address bar on top of the window. Windows should ask you for your LabraNet username and password. Note! Username needs to be in the correct format e.g. A1234@labranet.jamk.fi or LABRANET\A1234.

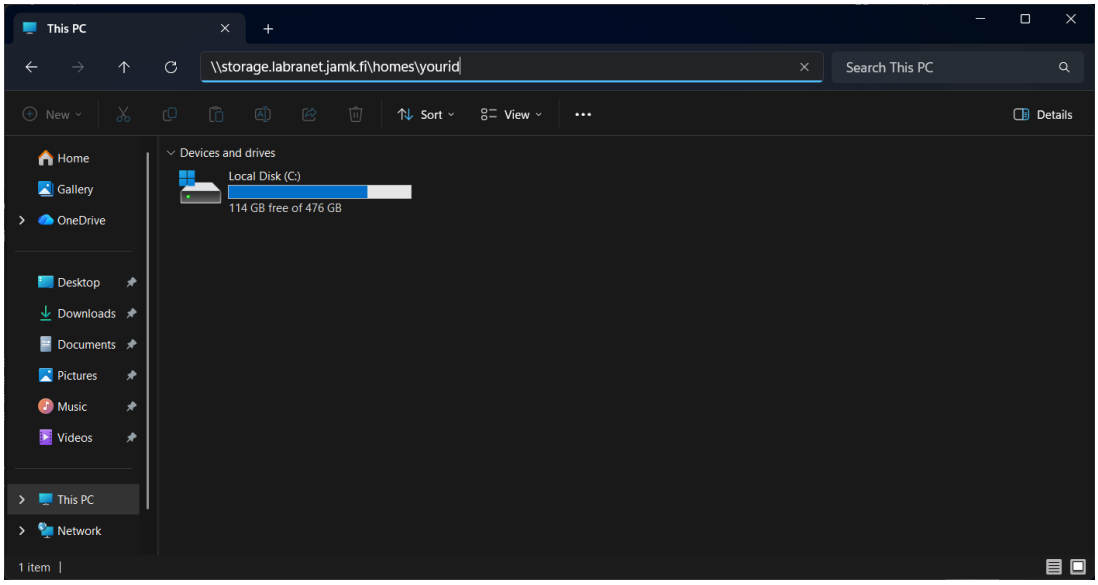

Figure 18. Enter the network path

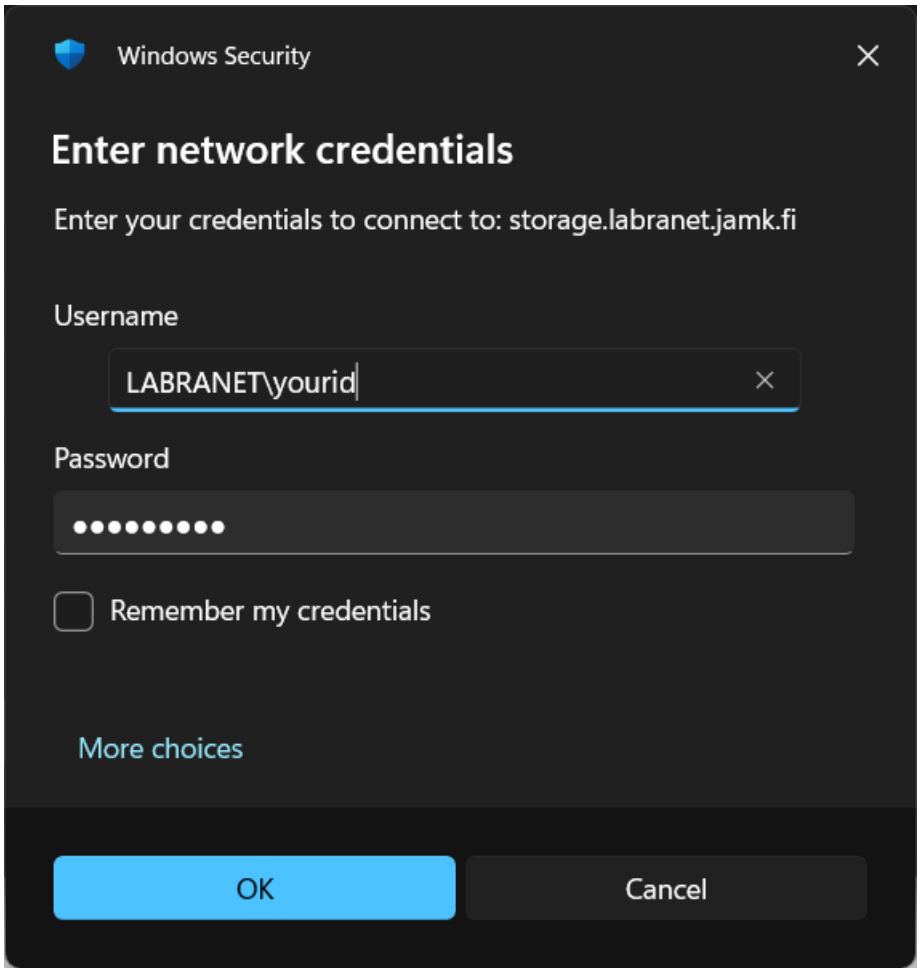

Figure 19. Enter your credentials

LabraNet

Remote access guide

Mac OS X

Go to Finder and press Cmd+K. Enter the path to the *Server Address* –field as follows *smb://network-path:*

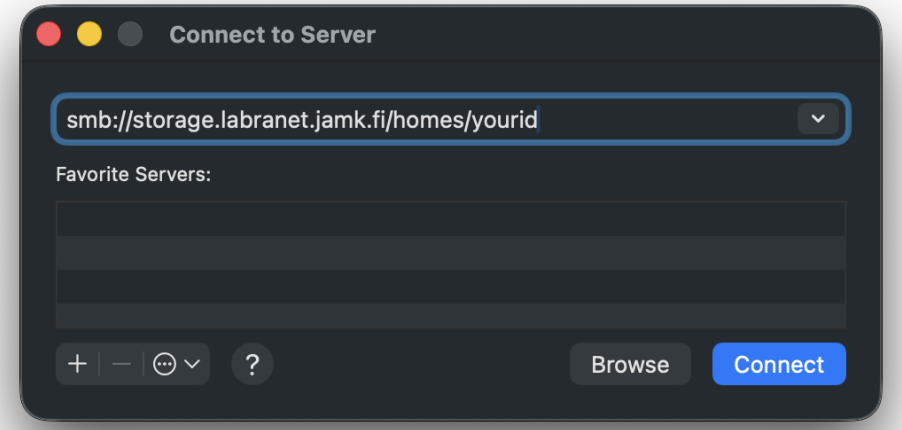

Figure 20. Connect to Server

Some versions of Mac OS X work better with cifs-protocol, path would then be *cifs://network-path*

Click *Connect*. You will be asked for your LabraNet credentials.

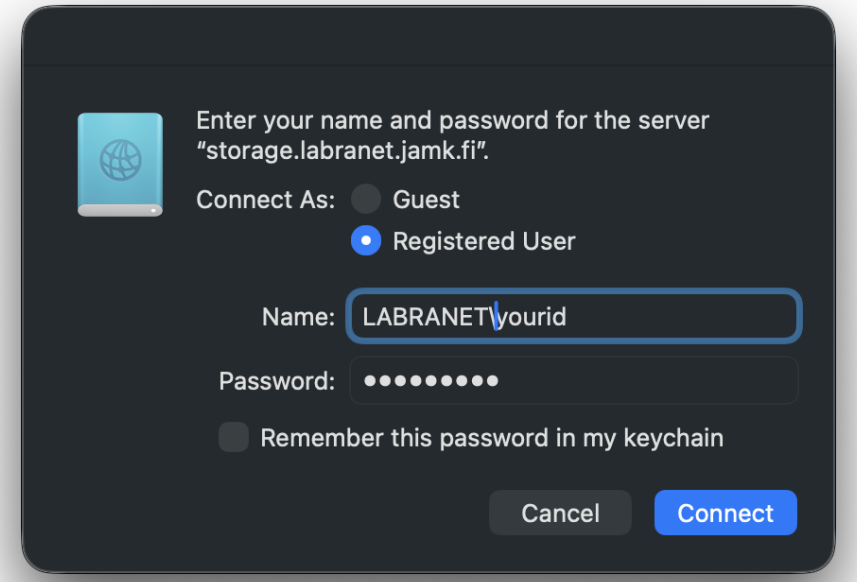

Figure 21. Credentials for user

LabraNet

Remote access guide

Linux (Graphical)

NOTE for older Linux distros: Due to being broken, SMBv1 has been disabled. This means you need to connect to shares with a newer version of the SMB protocol. This can be achieved by adding the following options to the *[global]* section of *smb.conf* in */etc/samba/smb.conf*.

client max protocol = SMB3
client min protocol = SMB2

Now you can connect to LabraNet network shares using your LabraNet account information. Type *smb://storage.labranet.jamk.fi/homes/yourid* and click *Connect*.

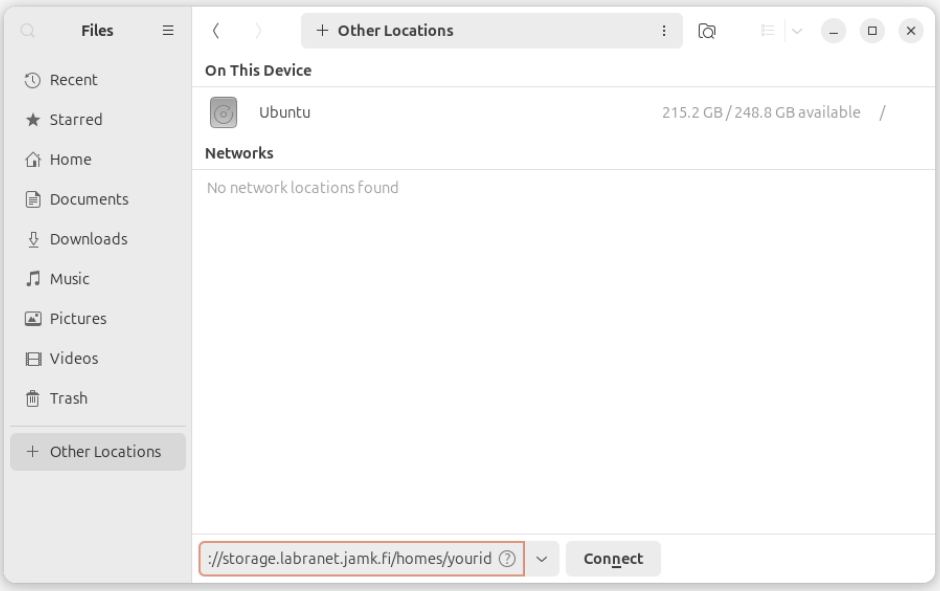

Figure 22. Connecting to server shares

You will then be asked to fill in your LabraNet account information.

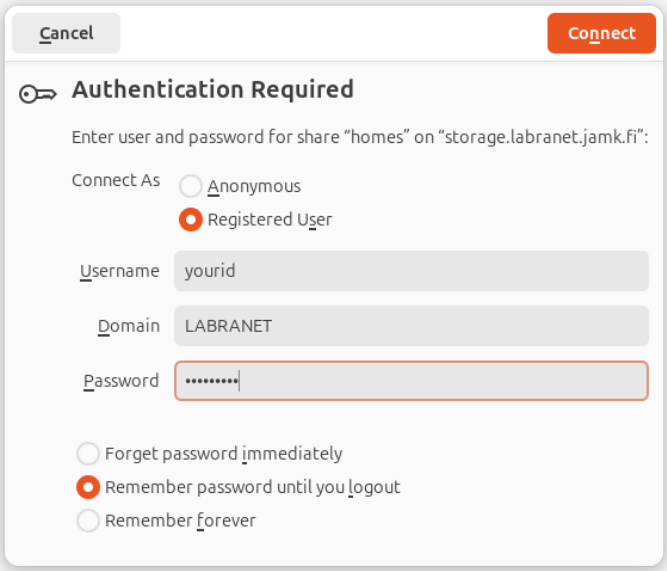

Figure 23. Creating the connection

LabraNet

Remote access guide

Linux (Command line)

Create a mountpoint and ensure *mount.cifs, cifs-utils* or equivalent package is installed depending on the distribution you're using.

Mount temporarily with:

sudo mount.cifs -o domain=LABRANET,username=<yourid>,vers=2.0 //network-path /mountpoint

Adding permanent mount to */etc/fstab*:

//network-path /mountpoint cifs domain=LABRANET,user=userid 0 0

You can also use *.smbcredentials* or *cifscreds* to store your credentials in a secure file or system keyring. Check your distributions documentation for more information.