theremino

•the•real•modular•in-out•

Theremino **System**

VPN Help

Connections via Internet

Some theremino system applications (SlotsOverNet, IotHAL and NetHAL) that are normally used in the local network, can also communicate through Internet.

Connecting through Internet requires a fixed IP, and a port must be chosen and this port must not be blocked by firewalls.

Alternatively, you can use some types of VPN that provide a "Mesh with direct connection" type.

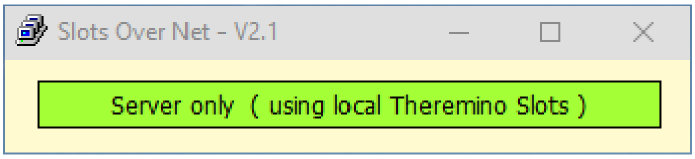
A convenient and free VPN (up to five simultaneous connections) could be Hamachi (from LogMeIn).

We have no interest in recommending it, we are not in contact with them and they do not pay us, if you want (and can) use another one.

Using the VPN with SlotsOverNet

To make SlotsOverNet communicate via the Internet, proceed as if you were working on a local network.

Only one server will have to be started, on any one of the PCs.

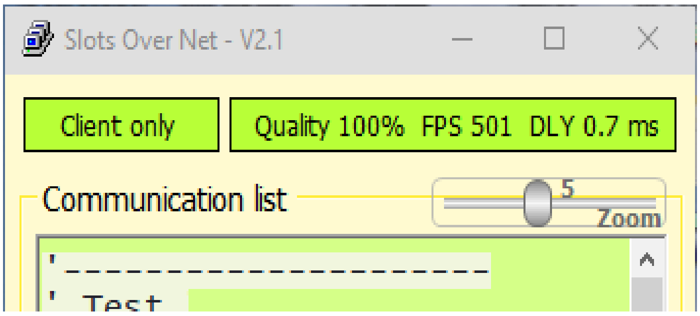


Slots Over Net - V2.1

Server only (using local Theremino Slots)

All the other SlotsOverNet applications, one for each PC, must be configured as "Client only".

You will not have to do anything else because the VPN will take care of showing all the PCs as if they were in the same local network.



Slots Over Net - V2.1

Client only

Quality 100% FPS 501 DLY 0.7 ms

Communication list

```
'-----------------------
' Test
```

Using the VPN with IotHAL and NetHAL

Read the application documentation and proceed as if you were working on a local network, the VPN will take care of the rest.

VPN installing

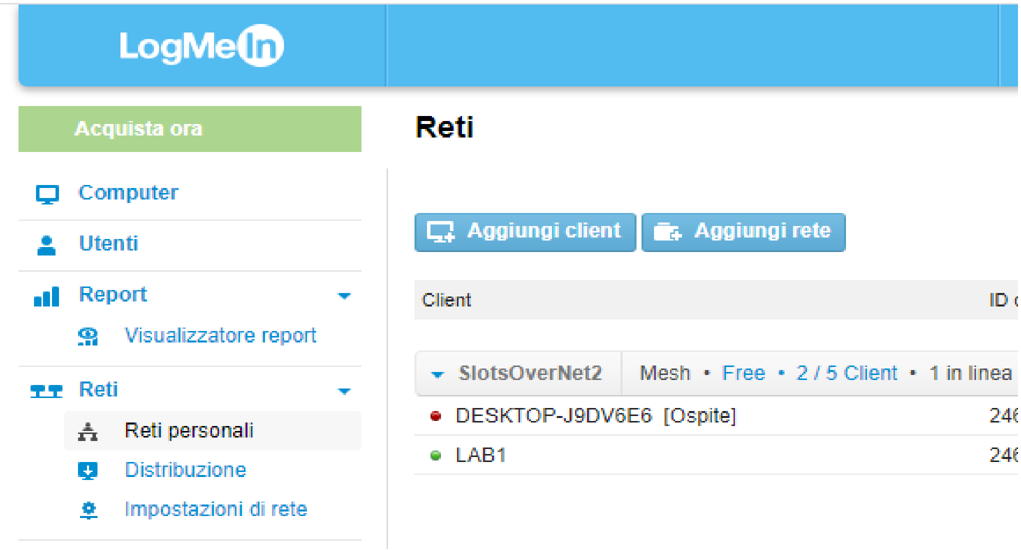
Download and install the Hamachi VPN

- Download from here: ***https://www.vpn.net*** and launch hamachi.msi
- Choose the language and press "Next"
- Accept the license agreement and press "Next"
- Create shortcut on Desktop and press "Next"
- Be careful not to install LastPass or other programs and press "Install"
- If Windows asks for permission, grant it for "Private network"

When Hamachi asks "Create network" or "Join" **do not create the network and do not participate**. To create the network and for the details of the VPN configuration we use ***this page***.

First time

- Register your account on ***this page***.
- When registering, enter a valid email and password and press "Create Account".
- If Windows asks for permission, grant it for "Private network".

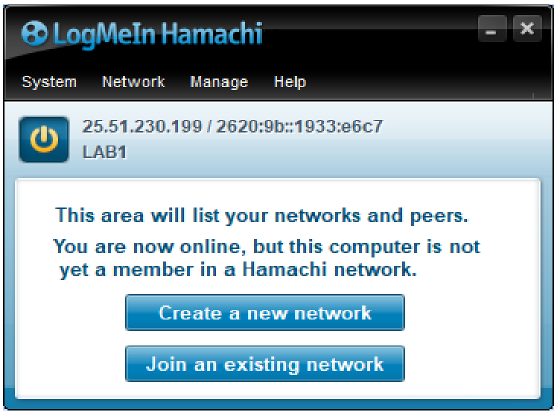


SlotsOverNet2 Mesh • Free • 2 / 5 Client • 1 in linea

Client	ID
DESKTOP-J9DV6E6 [Ospite]	246
LAB1	246

Connect PCs through the Hamachi VPN

After installing the VPN and creating the LogMeIn account and a network, you will have to join to the existing network.



25.51.230.199 / 2620:9b::1933:e6c7
LAB1

This area will list your networks and peers.

You are now online, but this computer is not yet a member in a Hamachi network.

- Once the network has been created, go to the Amachi program and press "Join the network".
- If Windows asks for permission, grant it for "Private Network".
- Go to the configuration web page and give consent to participate (to avoid this, the network could be changed so as not to ask for consent).
- When the Hamachi program asks for "Network-ID" do not give the name of the network but its "ID" (otherwise a password rejected error occurs).
- The ID is in the configuration web page, menu on the left, networks / Personal networks / Click on the first "Modify" at the top / The first number in the top left is the network ID.
- After the ID, the password must also be written.

If the VPN becomes "Public Network"

If the Windows request is not answered, the VPN becomes "Public network" and the SlotsOverNet application cannot communicate. In this case it is difficult to modify the VPN and make it "Private Network", we have found no other way than to modify the Registry and restart Windows.

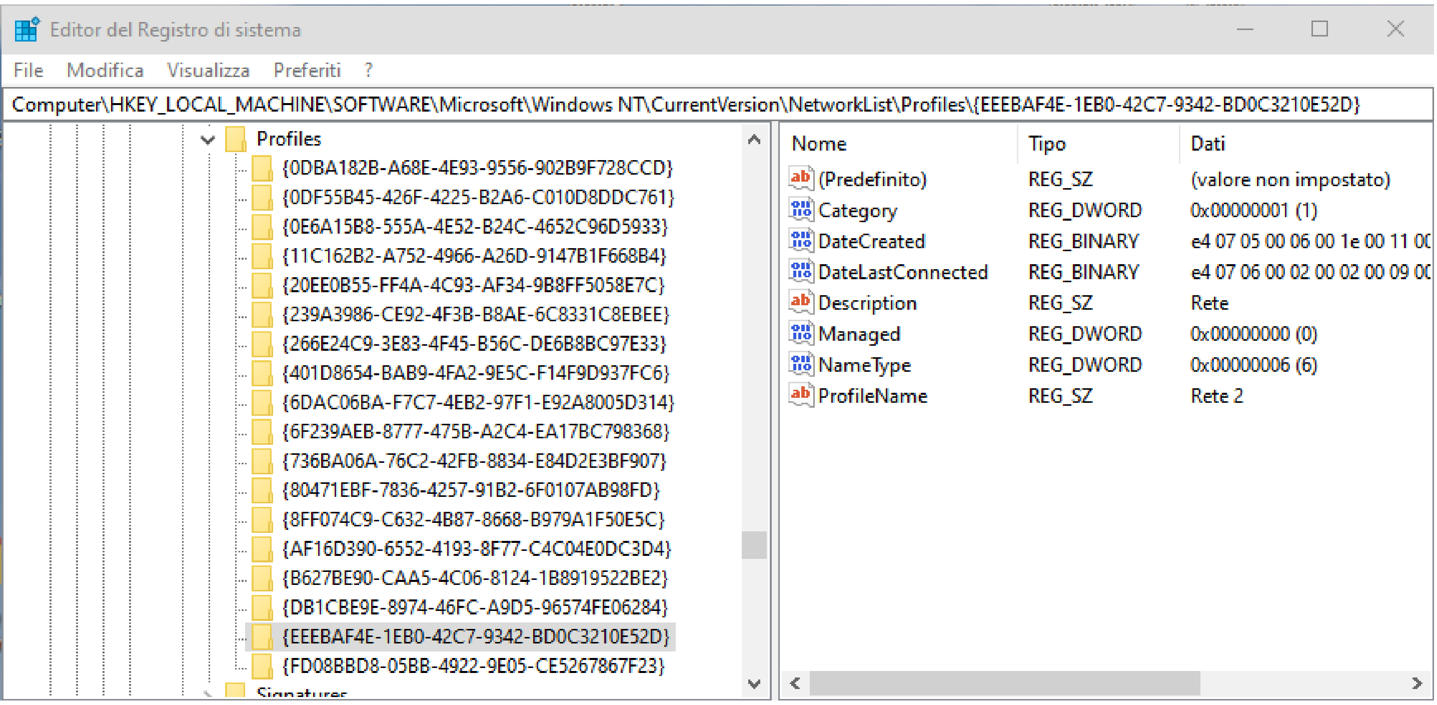
First of all you have to find the name of the network related to the VPN connection

- Click the Networks icon, in the lower right part of the desktop.
- Choose "Network and Internet Settings".
- Choose "Network Connection Center".
- Find the network name (left) of the Hamachi connection (right).

Then you start the system registry editor writing "RegEdit" in the Windows search box.

Once the RegEdit is open go to the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{EEEBAF4E-1EB0-42C7-9342-BD0C3210E52D}

- Profiles
  - {0DBA182B-A68E-4E93-9556-902B9F728CCD}
  - {0DF55B45-426F-4225-B2A6-C010D8DDC761}
  - {0E6A15B8-555A-4E52-B24C-4652C96D5933}
  - {11C162B2-A752-4966-A26D-9147B1F668B4}
  - {20EE0B55-FF4A-4C93-AF34-9B8FF5058E7C}
  - {239A3986-CE92-4F3B-B8AE-6C8331C8EBEE}
  - {266E24C9-3E83-4F45-B56C-DE6B8BC97E33}
  - {401D8654-BAB9-4FA2-9E5C-F14F9D937FC6}
  - {6DAC06BA-F7C7-4EB2-97F1-E92A8005D314}
  - {6F239AEB-8777-475B-A2C4-EA17BC798368}
  - {736BA06A-76C2-42FB-8834-E84D2E3BF907}
  - {80471EBF-7836-4257-91B2-6F0107AB98FD}
  - {8FF074C9-C632-4B87-8668-B979A1F50E5C}
  - {AF16D390-6552-4193-8F77-C4C04E0DC3D4}
  - {B627BE90-CAA5-4C06-8124-1B8919522BE2}
  - {DB1CBE9E-8974-46FC-A9D5-96574FE06284}
  - {EEEBAF4E-1EB0-42C7-9342-BD0C3210E52D}
  - {FD08BBD8-05BB-4922-9E05-CE5267867F23}
- Signatures

Nome	Tipo	Dati
(Predefinito)	REG_SZ	(valore non impostato)
Category	REG_DWORD	0x00000001 (1)
DateCreated	REG_BINARY	e4 07 05 00 06 00 1e 00 11 00
DateLastConnected	REG_BINARY	e4 07 06 00 02 00 02 00 09 00
Description	REG_SZ	Rete
Managed	REG_DWORD	0x00000000 (0)
NameType	REG_DWORD	0x00000006 (6)
ProfileName	REG_SZ	Rete 2

- A list of numbers similar to this appears: {0DBA182A-A68E-4E93-9556-703A9F728EEF}
- Select them until you find the one that has the name of the VPN as "Profile name".
- Double click on "Category" and change the "Value data" number from "0" to "1".
- Press OK and restart your PC.
- The VPN should have become "private" and SlotsOverNet should communicate.

Safety of UDP communications

Premise.

Never check critical or dangerous equipment.

Our system is not designed for this.

Local network or Internet

Internet is more vulnerable than the WiFi and wired local network. To increase security on the Internet we could use a VPN.

In any case, the greatest dangers are not from hackers, but gaps in speech, human error and hardware and software defects. So, as already written, never use our system to control dangerous or essential equipment.

Cyber attacks

Use this application to install viruses or spy on the data that is on your computer, it is quite impossible. The maximum that an attacker could get is to modify a numerical value. A value that will be promptly corrected within a few milliseconds.

In any case the maximum damage may be to ignite the irrigation for a brief moment, or to know the temperature or humidity orchard. No one is interested in knowing about or changing this kind of data, so normally you can be completely assured.

There would have to worry only if you control appliances that may break, explode, doing damage or be hazardous to the safety of persons.

In these cases, the risks would be many, from the PC that goes crazy to human error, the power failure, the software defects ... well most common dangers and likely of a cyber attack.

Packet loss and communication disruptions

To transfer data at the maximum speed possible to use the UDP protocol and this protocol does not guarantee that packets arrive.

TCP could respond with a confirmation, and in case of error could repeat the transmission. This in our case it would be quite useless, because we repeat the transmission every few milliseconds. And this time is less than the time it would take the TCP to give the confirmation, when added to the eventual re-transmission.

In case of interruptions in communication, even cease the TCP protocol to transfer data. It would also be slower to resume communication, it should come out of a state error, putting the lost packets and then resume communication at regular times.