



Università
di Brescia

Configuring Authenticated Wired Networks

This document walks through installing the certificate used to verify the trustworthiness of the wired network on Windows 11.

STEP 1 · DOWNLOAD THE CERTIFICATE

Find the certificate on the university website

- Before installing the certificate, you need to download it from the University's official website.
- Since the website layout may change over time, this tutorial only shows generally where the download links are located.
- Look for the Windows certificate link, highlighted below.

CERTIFICATE



[Windows Certificate - unibs-ca.der](#)



[Mac-Android Certificate - unibs-ca.crt](#)



STEP 1 · DOWNLOAD THE CERTIFICATE

Extract the downloaded archive

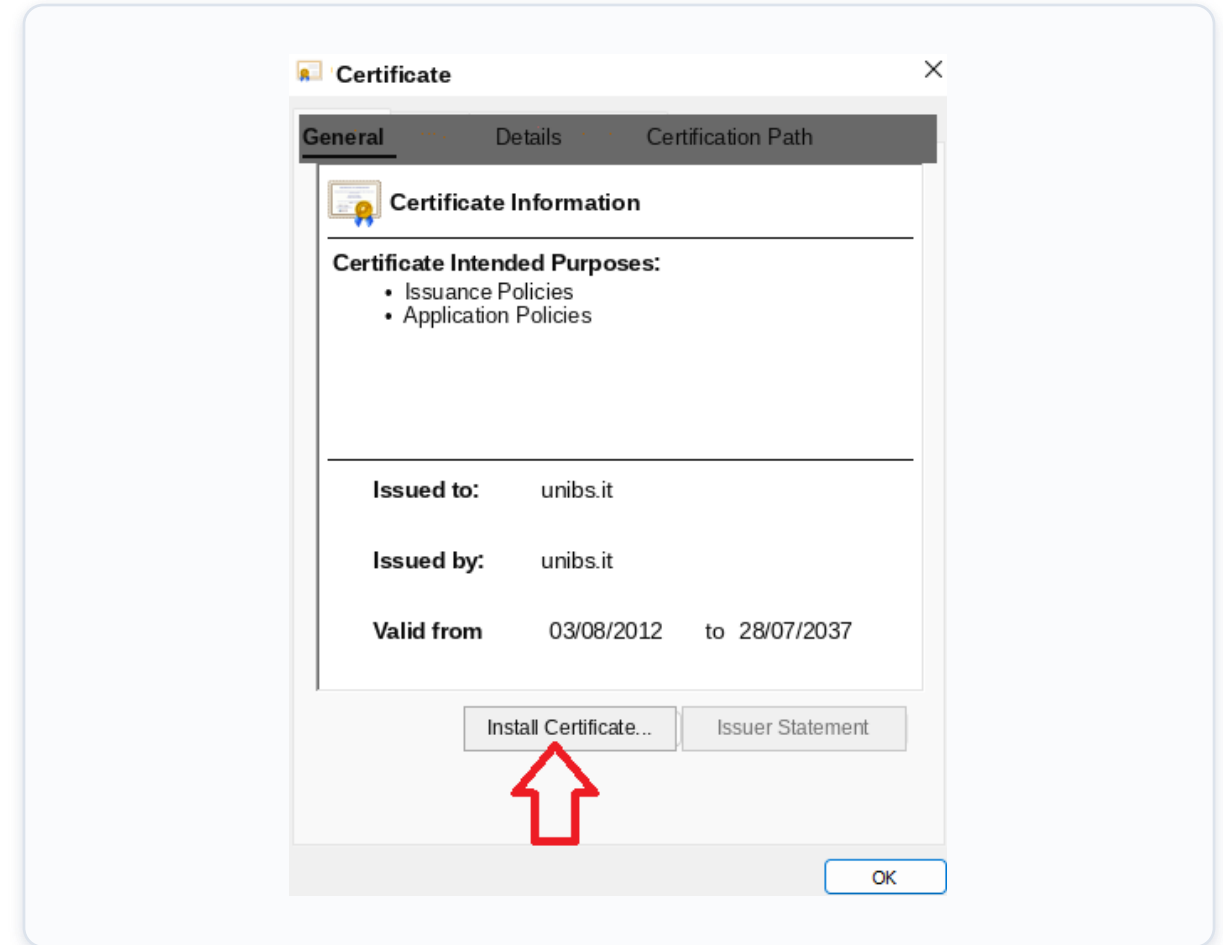
- After downloading the certificate, extract it using the tool provided by Microsoft.
- Generally, clicking on the zip file should automatically extract its contents.
- Once the process is complete, the file unibs-ca.der should appear.



STEP 2 · INSTALL THE CERTIFICATE

Open the certificate file

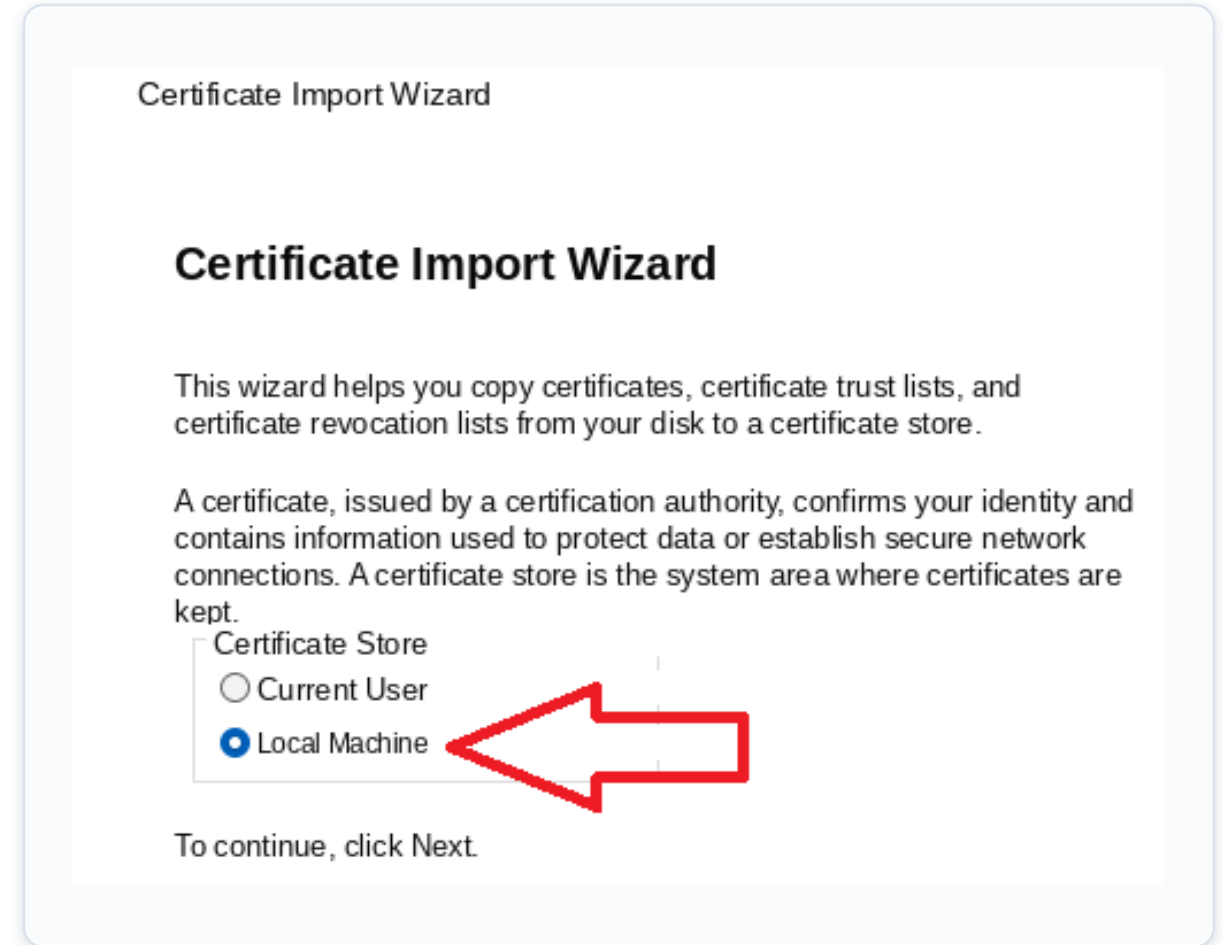
- To install the certificate, double-click on the file.
- The screen shown on the right will appear.
- Click the “Install Certificate...” button to begin.



STEP 2 · INSTALL THE CERTIFICATE

Choose the certificate store location

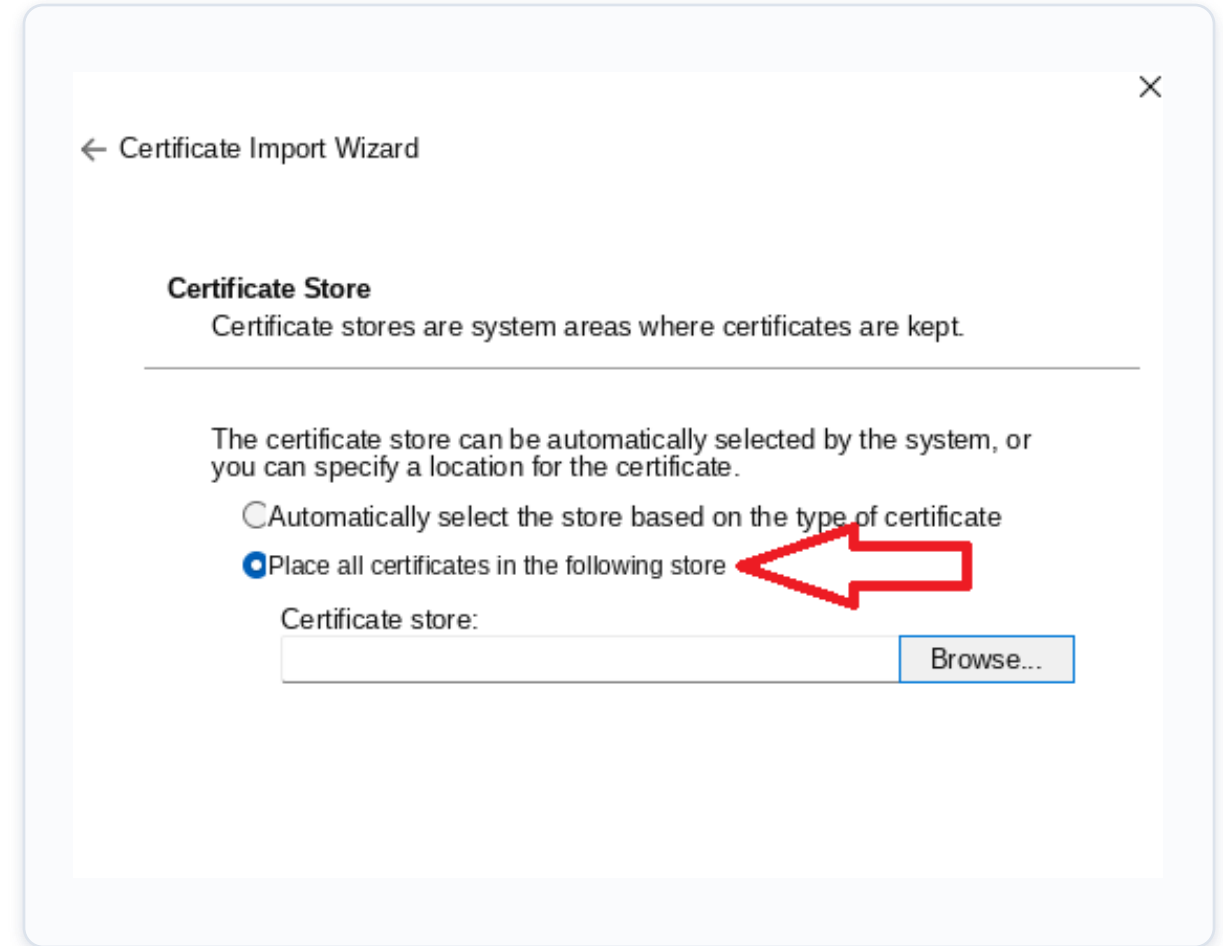
- A new window will open — select “Local Machine”.
- Once selected, click “Next”.
- If asked “Do you want to allow this app to make changes to your device?”, click “Yes”.



STEP 2 · INSTALL THE CERTIFICATE

Place the certificate manually

- On the next screen, select “Place all certificates in the following store”.
- Then click the “Browse...” button to pick the store.

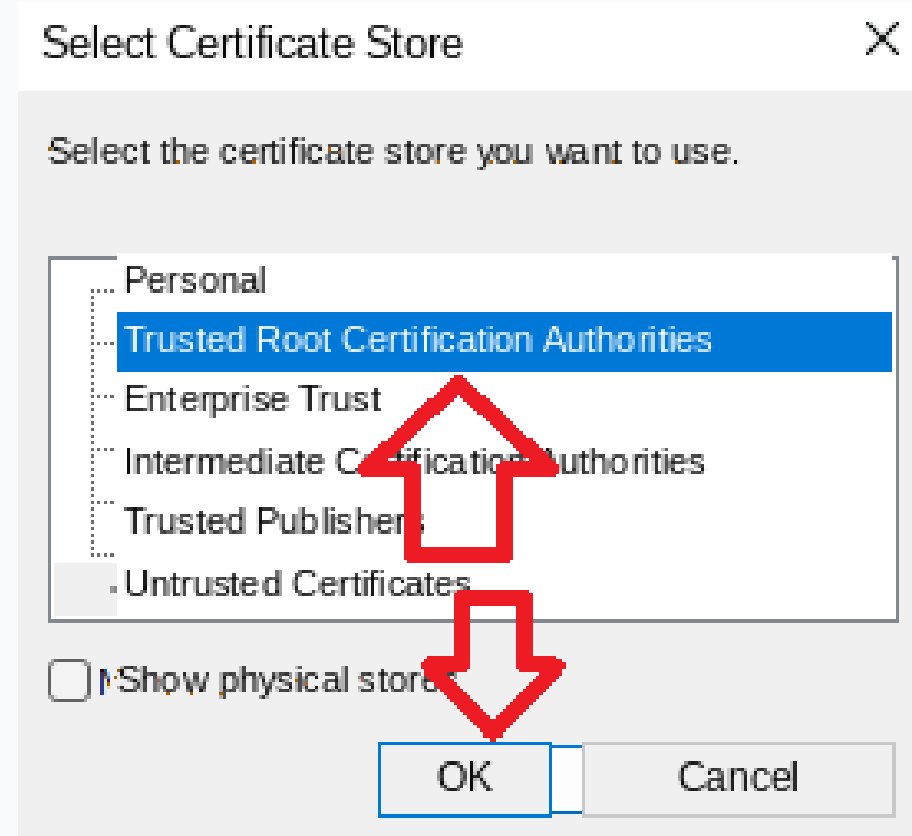


STEP 2 · INSTALL THE CERTIFICATE

Select the Trusted Root store

- 1 Select “Trusted Root Certification Authorities” in the list.
- 2 Click “OK” to confirm.
- 3 Return to the previous window and click “Next”.

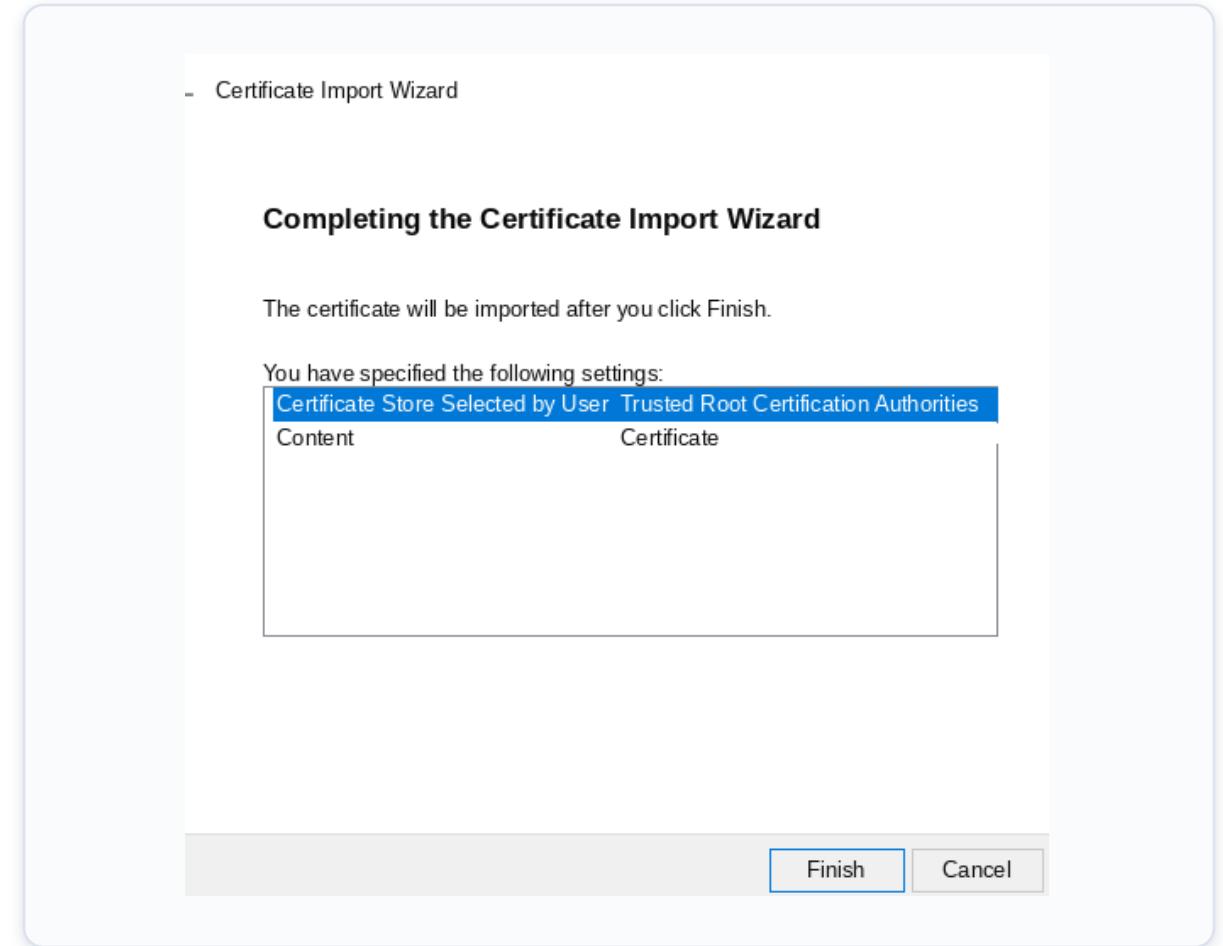
Important: select the Trusted Root Certification Authorities store. This is where the UniBS root CA certificate must be installed.



STEP 2 · INSTALL THE CERTIFICATE

Finish the import wizard

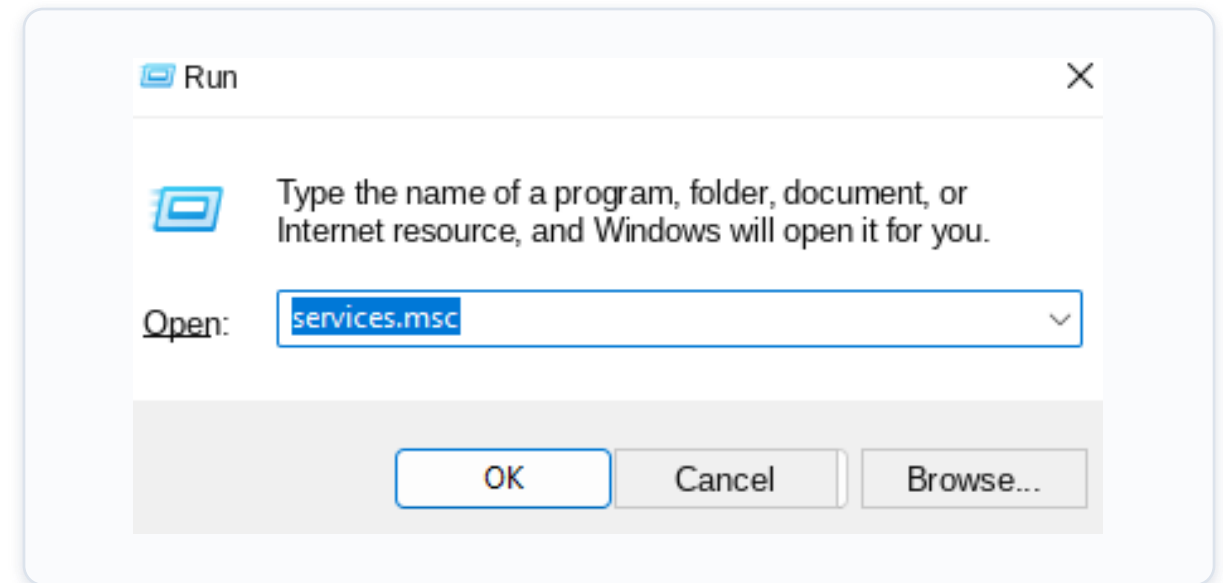
- To complete the installation process, click “Finish”.
- Windows will confirm once the certificate has been imported successfully.



STEP 3 · ACTIVATE THE SERVICE

Open the Services console

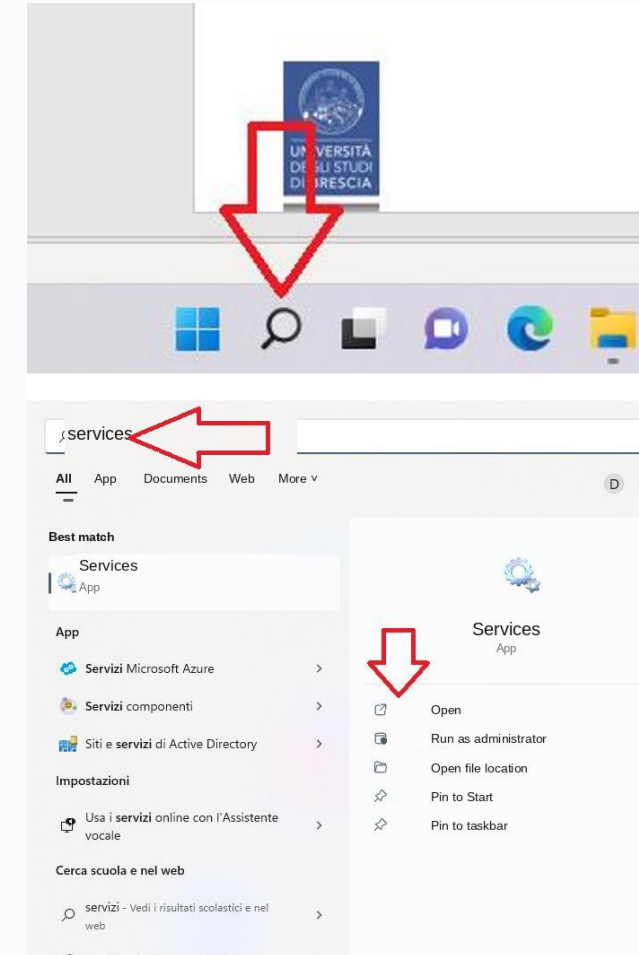
- To use the certificate, you need to enable the “Wired AutoConfig” service.
- On Windows 11, press WIN (Windows key) + R, type “services.msc”, then press OK.



STEP 3 · ACTIVATE THE SERVICE

...or search for it directly

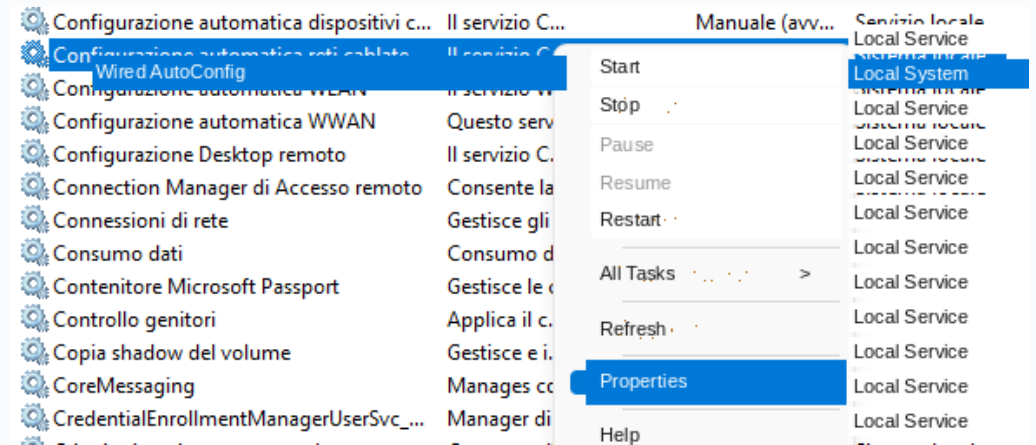
- Alternatively, click the magnifying glass icon on the taskbar and search for “Services”.
- Open the app from the search results, as shown on the right.



STEP 3 · ACTIVATE THE SERVICE

Locate the Wired AutoConfig service

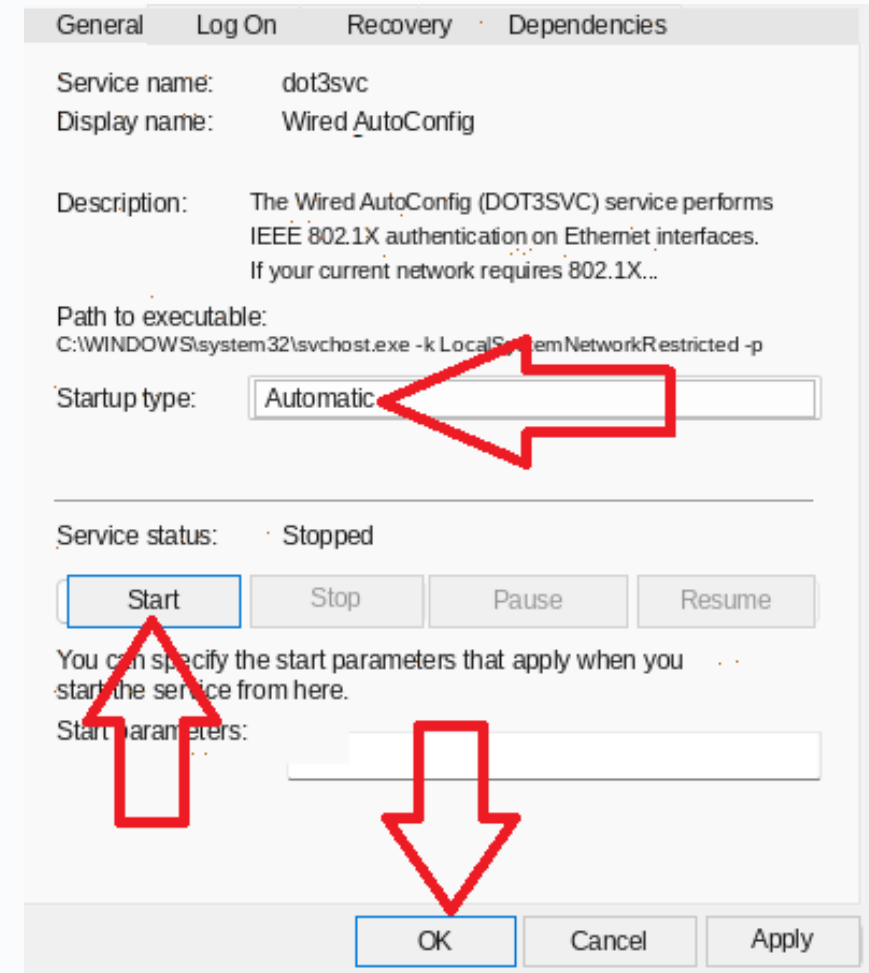
- After opening the Services window, find the service named “Wired AutoConfig” in the list.
- Right-click on it and select “Properties”.



STEP 3 · ACTIVATE THE SERVICE

Set the service to start automatically

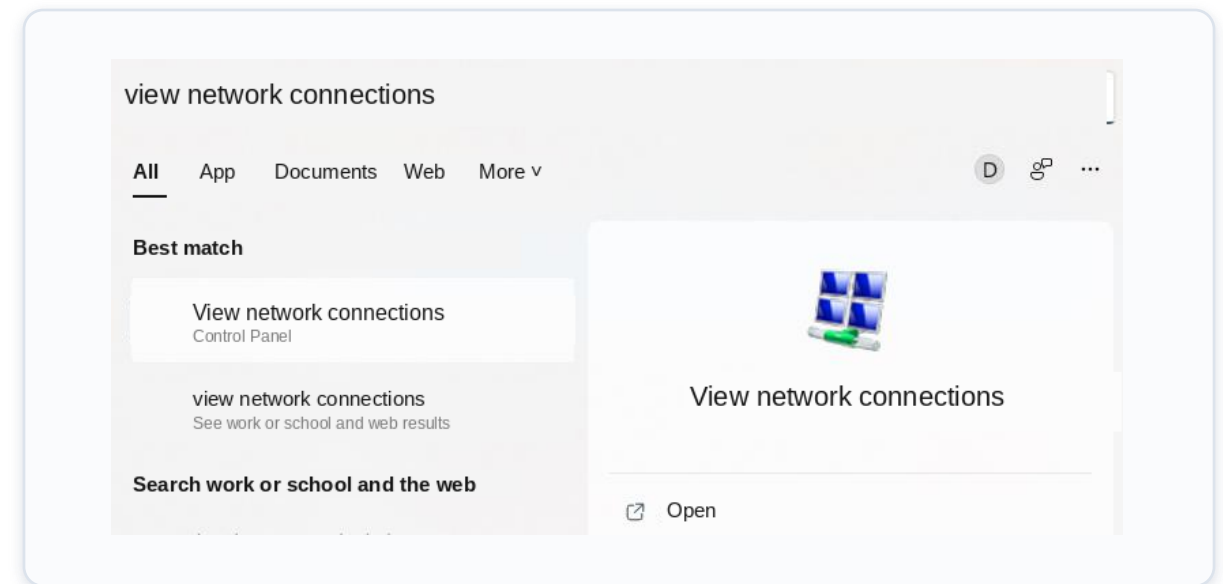
- In the Properties window, set “Startup type” to Automatic.
- Click “Start”, then press “OK” to confirm.



STEP 4 · ACTIVATE THE CERTIFICATE

Open your network connections

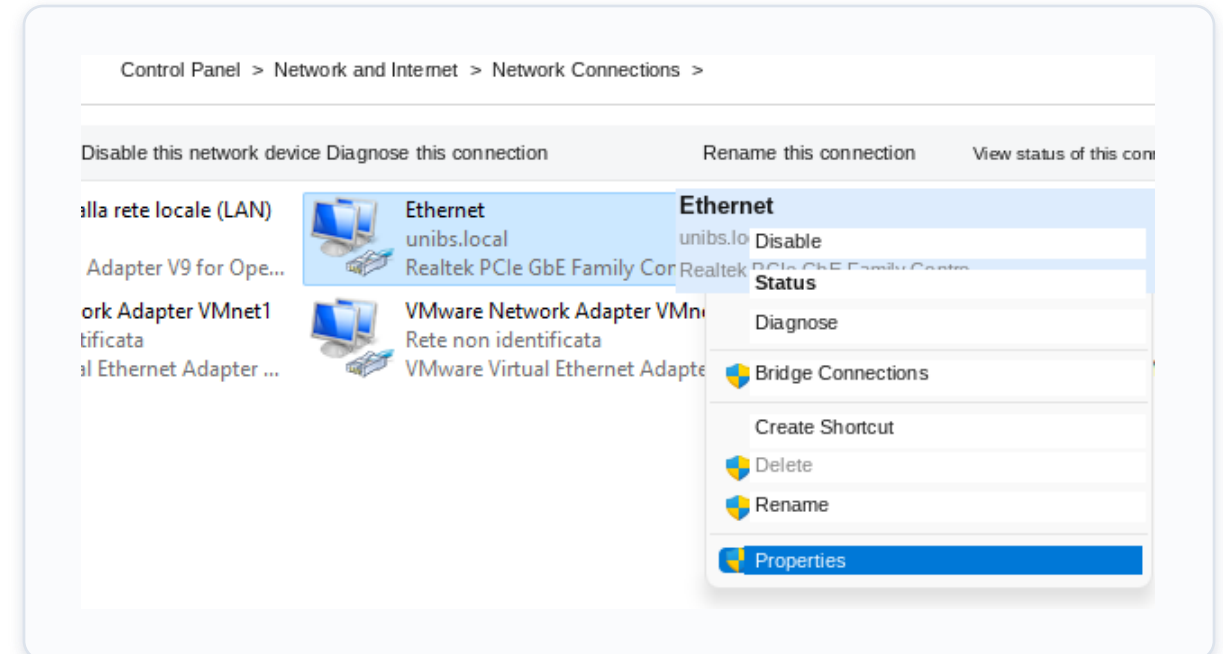
- Everything is now ready to enable certificate verification on the wired network.
- Click the magnifying glass icon and search for “View network connections”.



STEP 4 · ACTIVATE THE CERTIFICATE

Open the Ethernet properties

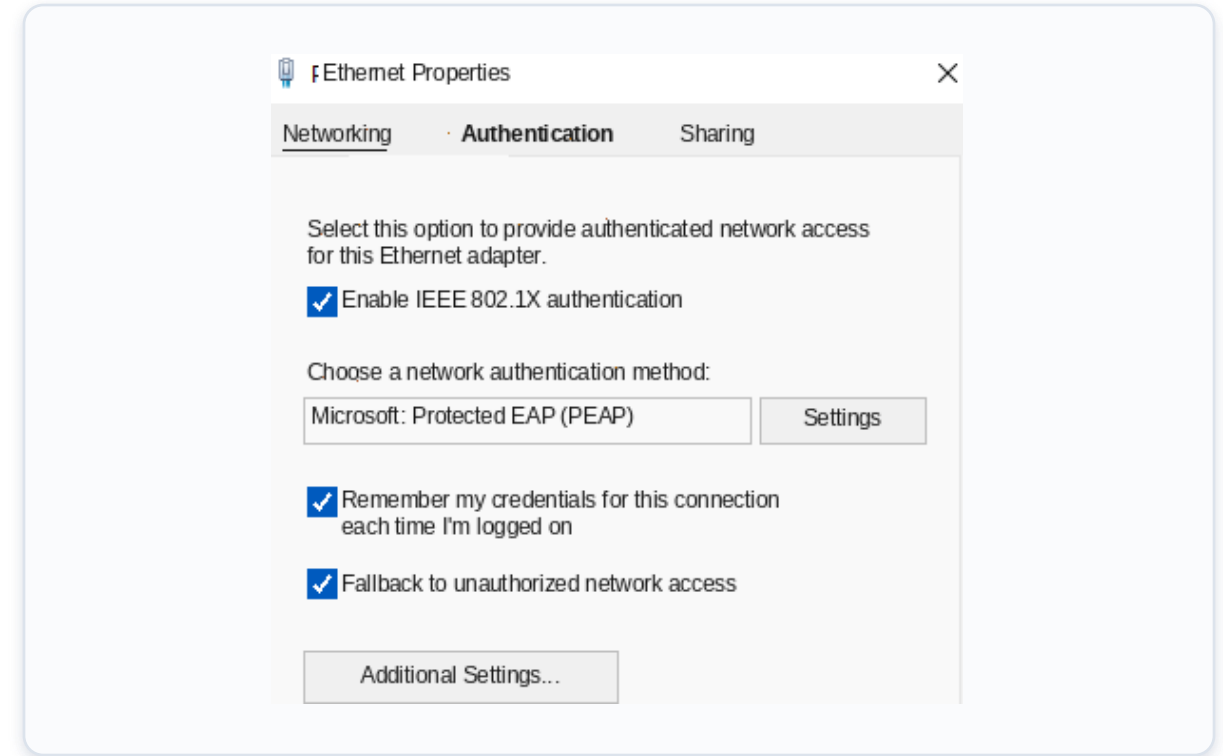
- Select the “Ethernet” network, right-click it, and choose “Properties”.



STEP 4 · ACTIVATE THE CERTIFICATE

Open the Authentication tab

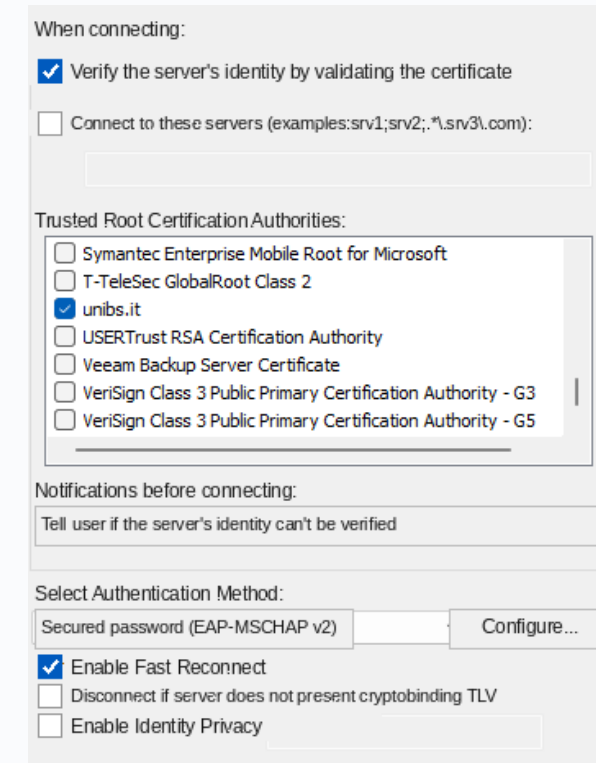
- In the Properties window, go to the “Authentication” tab.
- This tab only appears once the previous steps are complete.
- Make sure your settings match those shown on the right, then click “Settings”.



STEP 4 · ACTIVATE THE CERTIFICATE

Select the university's certificate authority

- After clicking “Settings”, the screen on the right will appear.
- Select unibs.it from the list of trusted root certification authorities.



When connecting:

☒ Verify the server's identity by validating the certificate

☐ Connect to these servers (examples: srv1;srv2;*.srv3\com):

Trusted Root Certification Authorities:

- ☐ Symantec Enterprise Mobile Root for Microsoft
- ☐ T-TeleSec GlobalRoot Class 2
- ☒ unibs.it
- ☐ USERTrust RSA Certification Authority
- ☐ Veeam Backup Server Certificate
- ☐ VeriSign Class 3 Public Primary Certification Authority - G3
- ☐ VeriSign Class 3 Public Primary Certification Authority - G5

Notifications before connecting:

☐ Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2) Configure...

☒ Enable Fast Reconnect

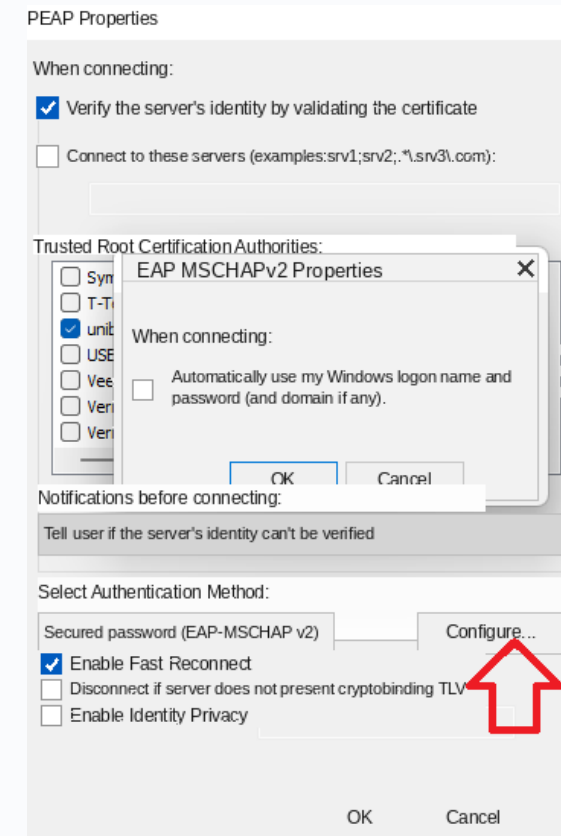
☐ Disconnect if server does not present cryptobinding TLV

☐ Enable Identity Privacy

STEP 4 · ACTIVATE THE CERTIFICATE

Disable automatic Windows credentials

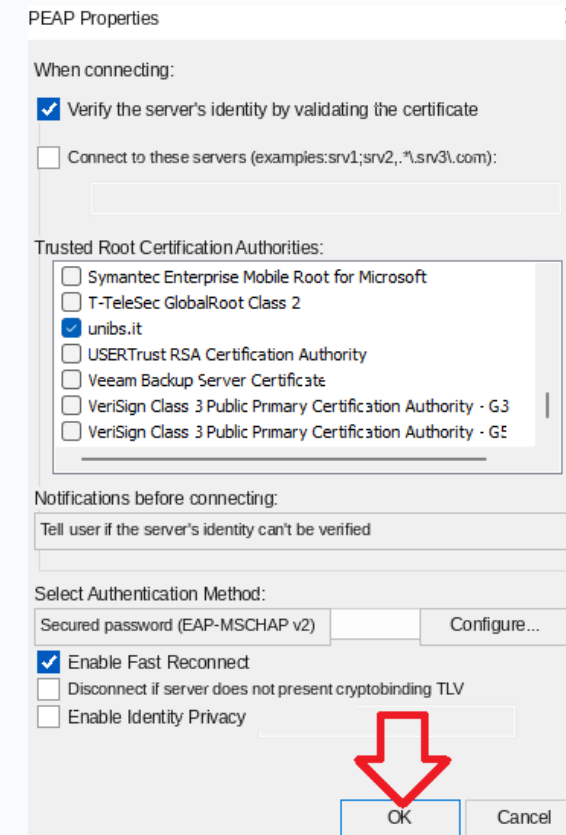
- Click “Configure...” and make sure “Automatically use my Windows logon name and password (and domain if any)” is unchecked.
- Then click “OK”.



STEP 4 · ACTIVATE THE CERTIFICATE

Confirm the authentication settings

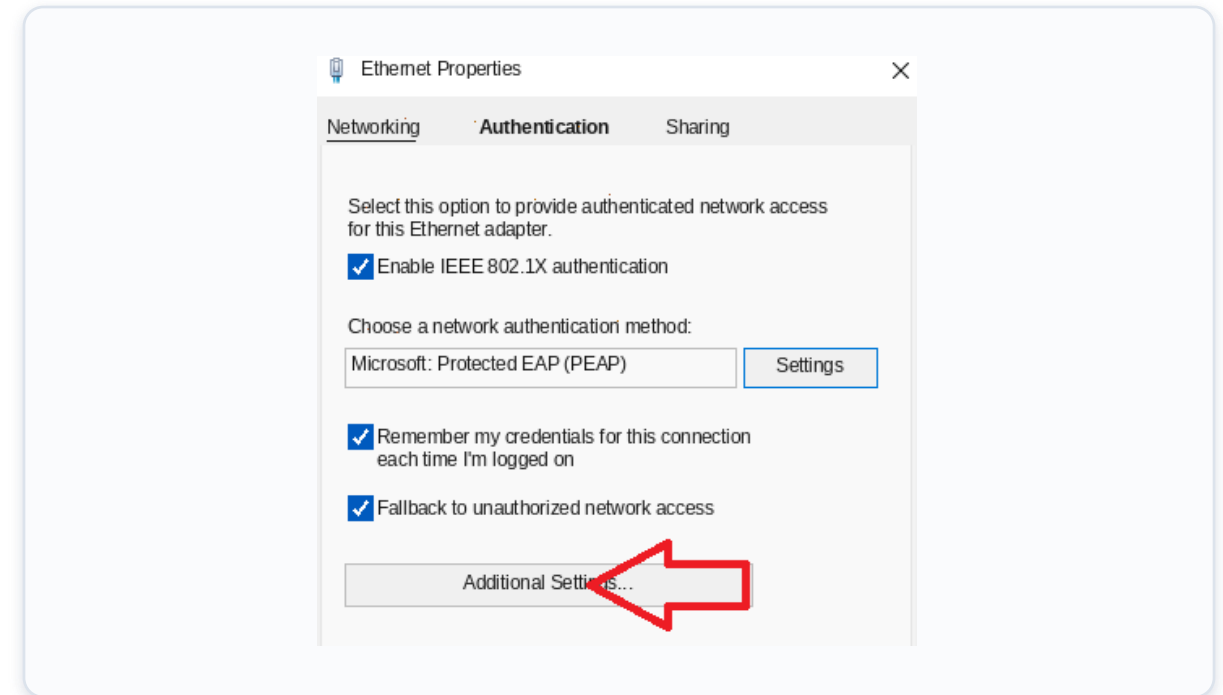
- Once all the previous steps are complete, click “OK”.



STEP 4 · ACTIVATE THE CERTIFICATE

Open the additional settings

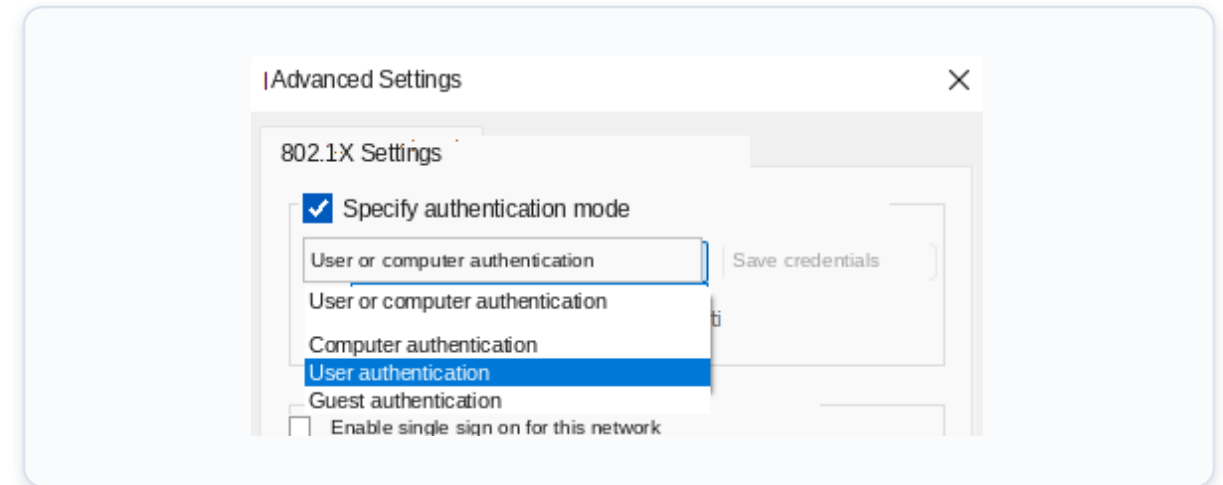
- You'll be taken back to the initial Ethernet properties screen.
- Click “Additional settings”.



STEP 4 · ACTIVATE THE CERTIFICATE

Specify the authentication mode

- Check “Specify authentication mode”.
- From the dropdown, select “User authentication”.
- Click “OK” to save.



STEP 4 · ACTIVATE THE CERTIFICATE

Configuration complete

- The configuration is now complete.
- If you are prompted for credentials when connecting, simply enter your own university username and password.

