

Radiator Auth.fi Wi-Fi configuration for roam.fi network

27.5.2024

Note

These instructions are for making a proper WPA Enterprise Wi-Fi configuration for organisations and users using roam.fi network and Radiator Auth.fi authentication service. The instructions can be used as a guideline for configuring other WPA Enterprise Wi-Fi network, but it should be noted that for example Wi-Fi network names, CA and certificates as well as their fingerprints, RADIUS server names and available authentication methods (e.g. PEAP, EAP-TTLS) may be different for each network and home organisation.

Windows 10

Connecting manually to the roam.fi Wi-Fi network

**Choose roam.fi
from Windows
network menu.**



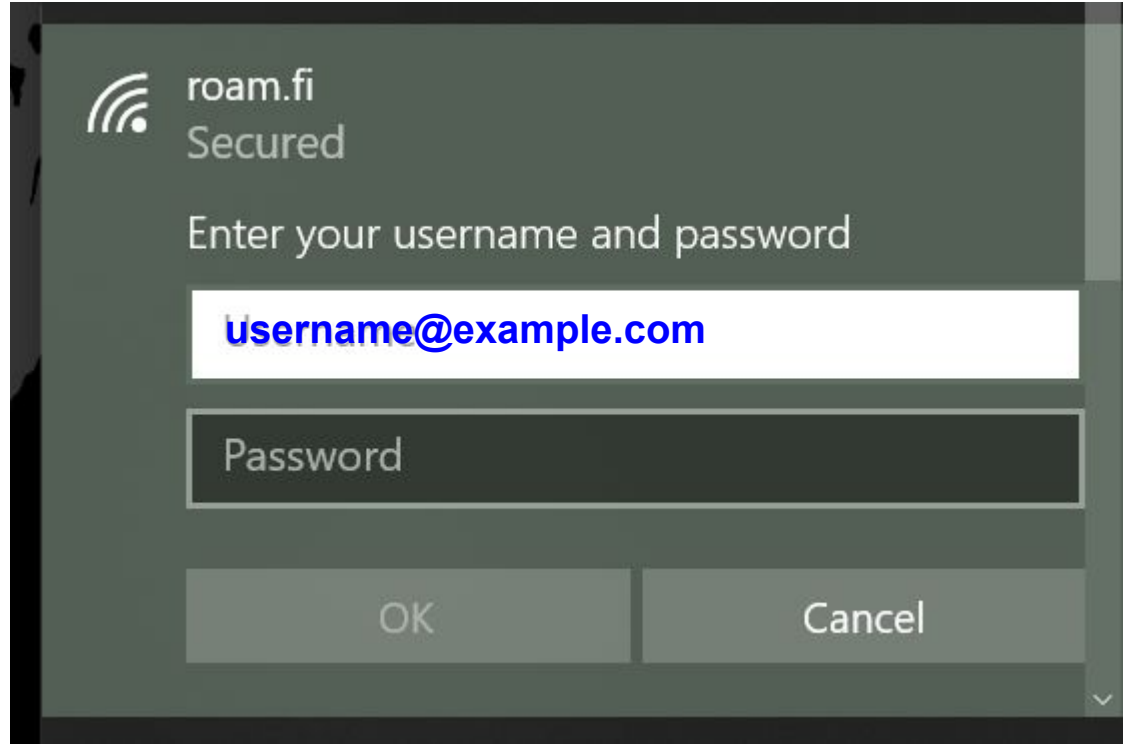
**Accept
'Connect
automatically'
and click
Connect.**



Fill in your organisation username and password.

Remember to include also the domain part of the username.

If you use automatic text fill, please check that there is no space after your username or email address.



roam.fi
Secured

Enter your username and password

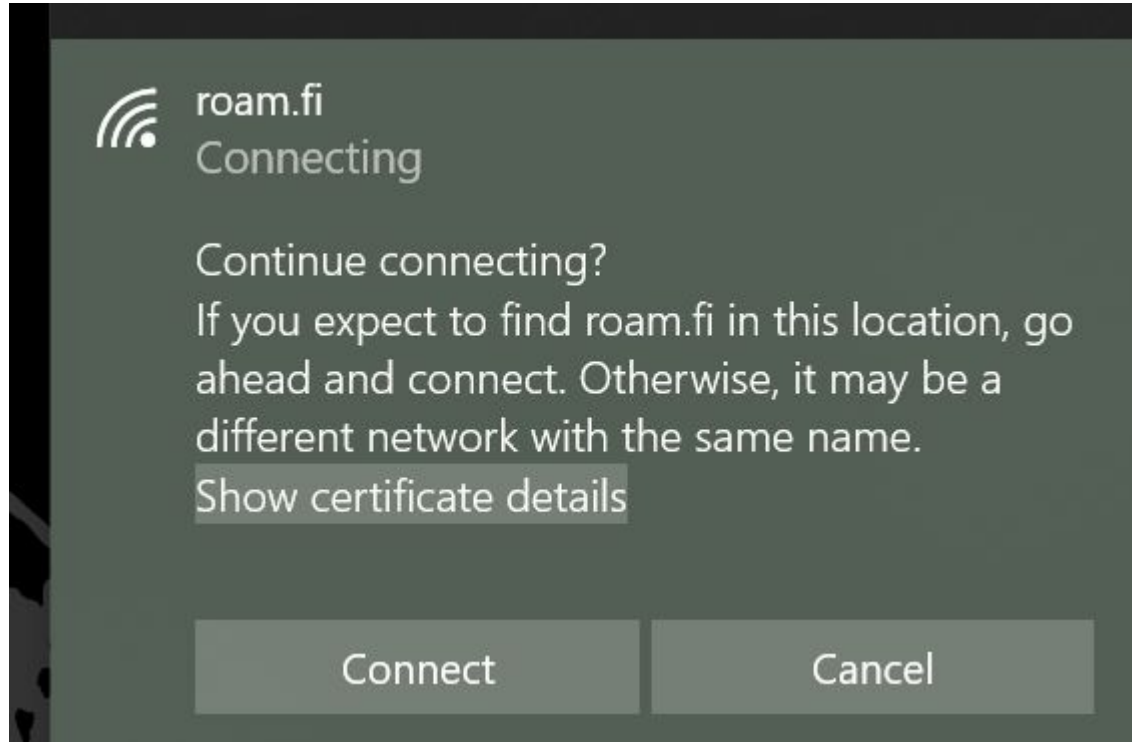
Username@example.com

Password

OK Cancel

If you connect to roam.fi network for the first time or if the RADIUS server certificate of your home organisation has been changed, Windows may ask you to accept new certificate.

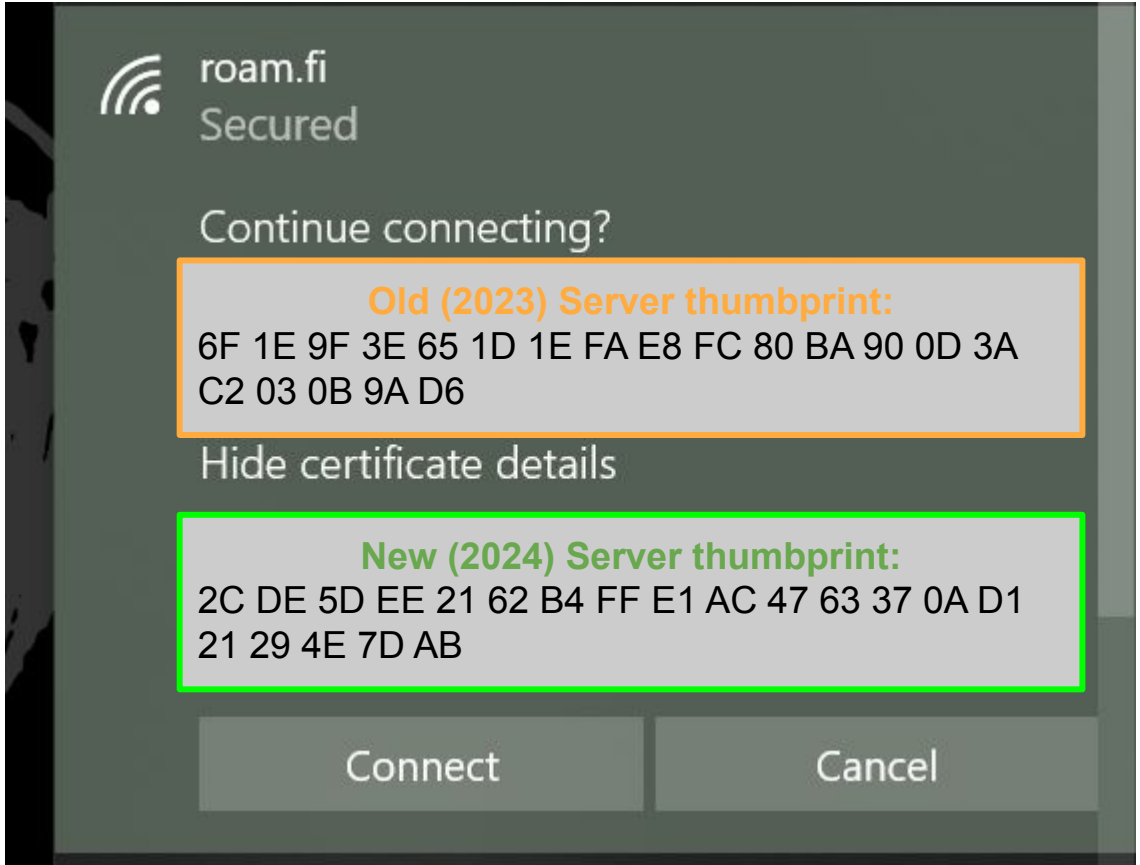
By clicking 'Show certificate details' you get more information about the server certificate so that you can verify the certificate.



The server thumbprint is different for each RADIUS server certificate. On the right are the old (2022) and new (2023) certificate thumbprint.

Please check with your home organisation, whose username and password you are using, what should be the thumbprint of their RADIUS server certificate.

By comparing the thumbprint to your home organisation's server certificate, you can verify that you are sending your username and password to home organisation and not to an eavesdropper.

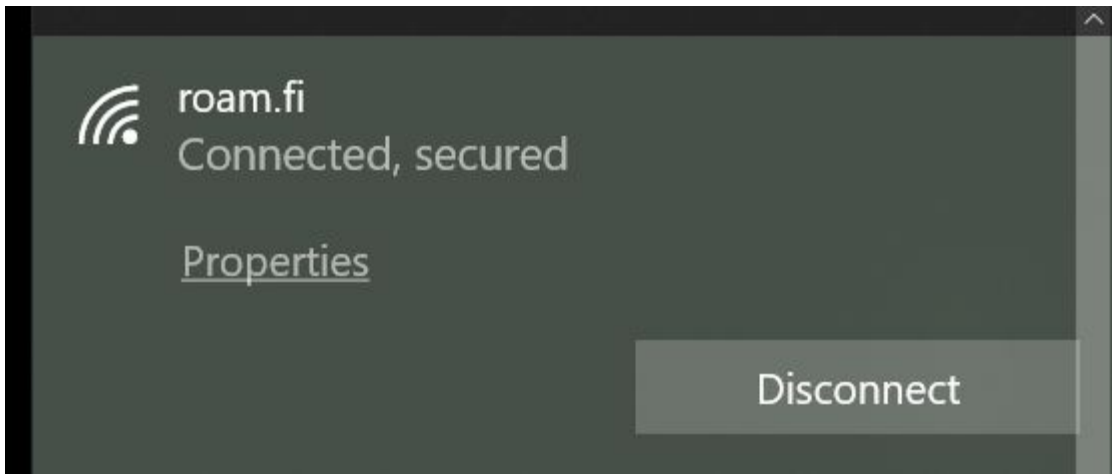


Note for system administrators: you can get thumbprint with openssl for certificate with: `openssl x509 -noout -fingerprint -sha1 -in cert.pem`

After clicking 'Connect', you should be able to connect automatically to roam.fi network and the state of the connection would change to "Connected, secured".

Sometimes when it takes time to write the username and password or accepting the certificate, the RADIUS server may decide that the authentication has taken too much time and connection fails.

By repeating the previous test quicker, you should be able to connect to the network.



The weakness of this way of manual join to network is that you may have to verify the home organisation RADIUS server certificate or create the network configuration every time the home organisation RADIUS server updates. This may happen every year.

By configuring a network profile for Windows 10 may take more time from initial configuration but will set you free from verifying certificate thumbprints or doing manual joins to network each year.

Windows 10

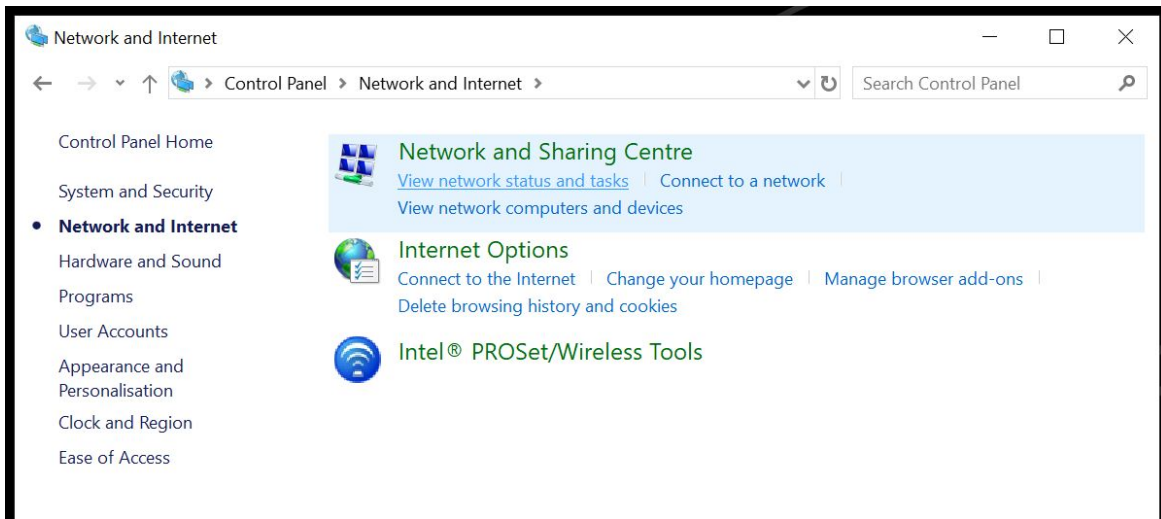
Configuring a network profile for roam.fi
(may require local administrator privileges)

Before creating a network profile, please ensure from Windows Wi-Fi settings that you do not have existing roam.fi network profile.

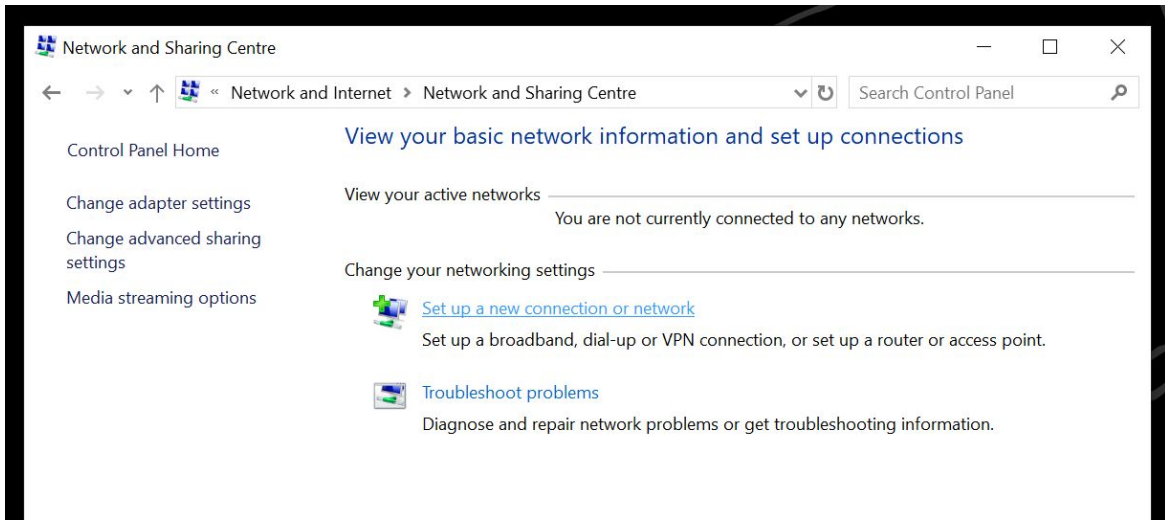
If you have one, please remove it before proceeding.

Use Windows search to find *Control Panel*.

Find next *Network and Internet*. Select *Network and Sharing Centre* and from there *View network status and tasks*



From *Network Sharing Centre* choose *Set up a new connection or network* and after that *Manually connect a wireless network*.



The picture on the left shows the correct configuration settings for roam.fi network.

If after filling these details and clicking Next, Windows informs that there is already a configuration for network, you may have old roam.fi network configuration profile somewhere and you have to instruct the device to forget that network.

←  Manually connect to a wireless network

Enter information for the wireless network that you want to add

Network name:

Security type:

WPA2-Enterprise

Encryption type:

AES

Security Key: ☐ Hide characters

☒ Start this connection automatically

☐ Connect even if the network is not broadcasting

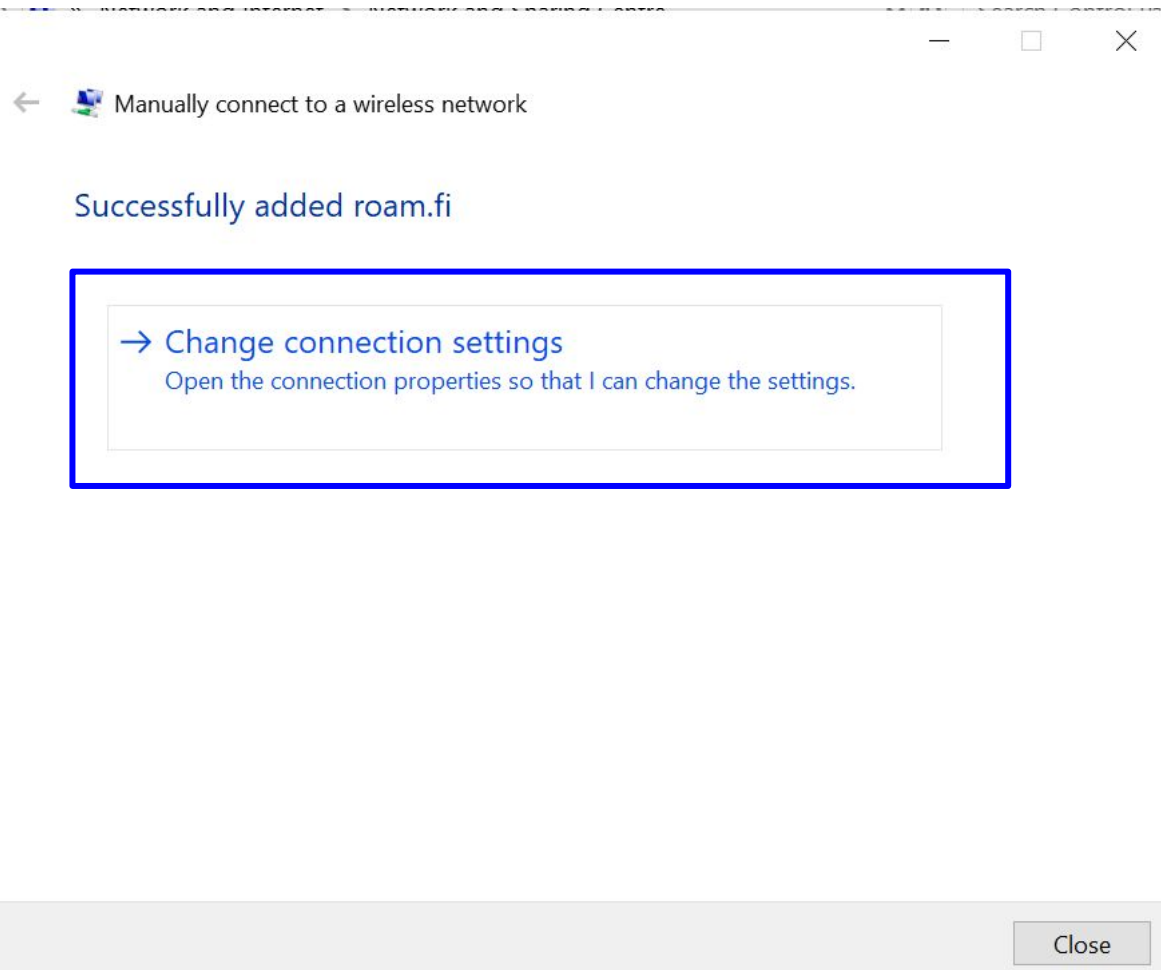
Warning: If you select this option, your computer's privacy might be at risk.

Next

Cancel

If there is no conflicting old profile, Windows informs that it has successfully added roam.fi profile.

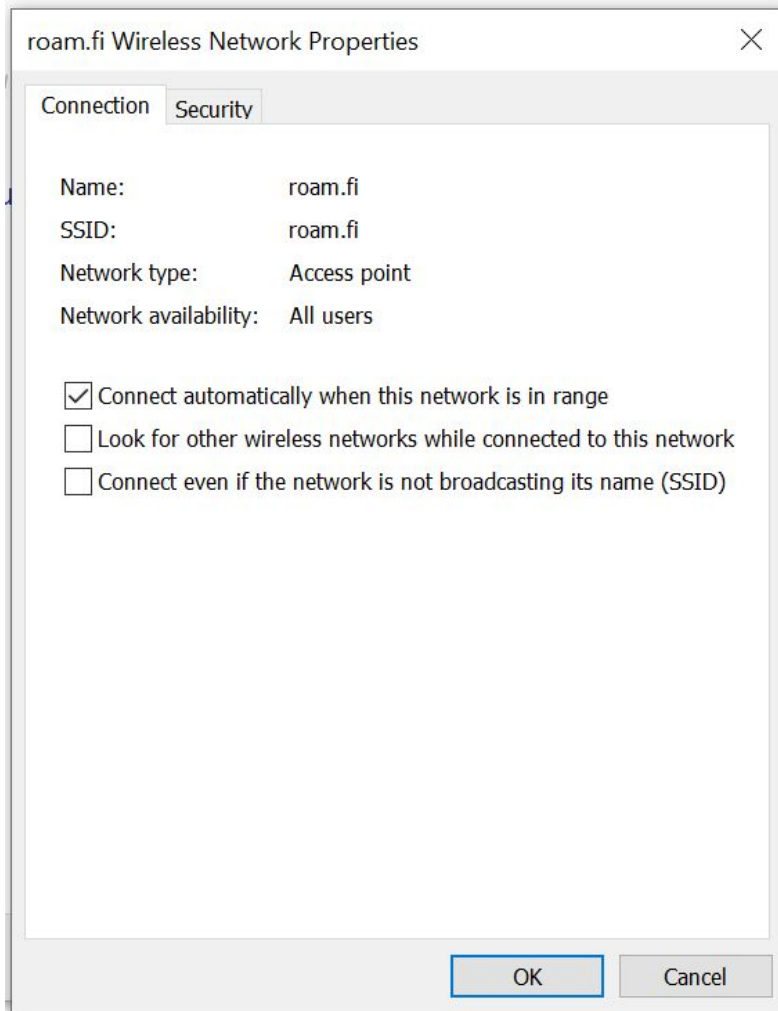
Don't click *Close* just yet, but select instead *Change connection settings*.



You should now see more detailed configuration settings for roam.fi.

Check the correct settings for Connection from the picture on the right.

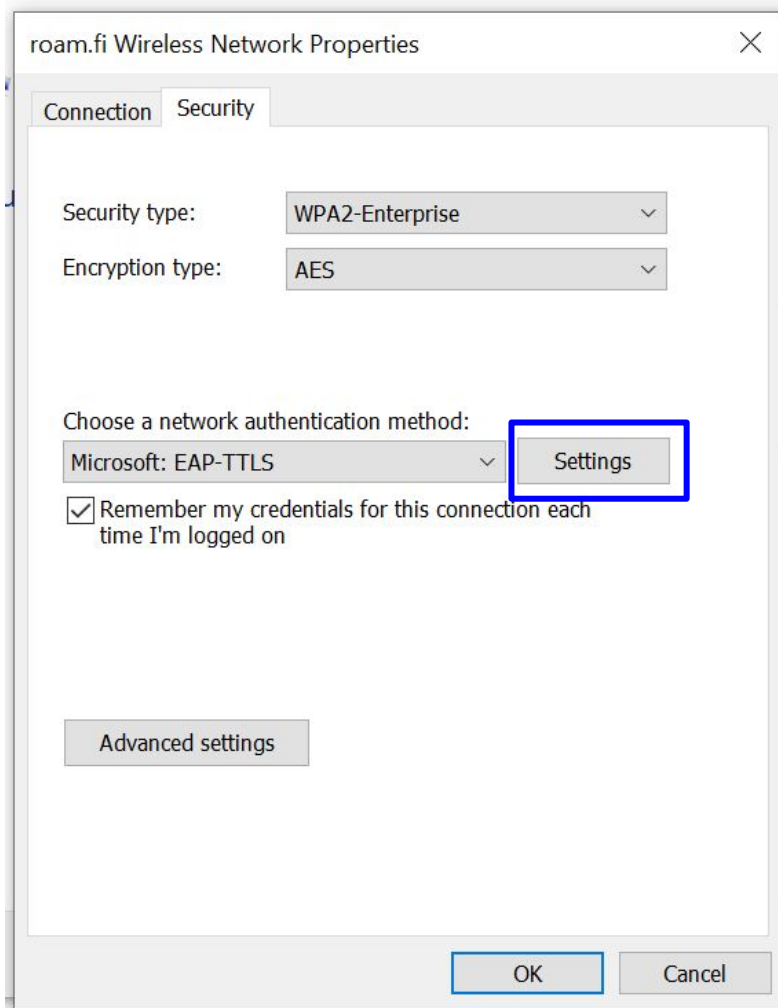
After setting these do not click OK, but select Security tab.



The correct settings for roam.fi and Radiator Auth.fi service are shown on the right.

Please note that your settings may be different unless your home organisation is a Radiator Auth.fi user.

Choose next *Settings* close to *Choose a network authentication method*.



Selecting **Settings** should open you TTLS properties dialog such as in the picture on the right.

Replace anonymous in the place of anonymous@example.com with **anonymous@your_home_organisation's_domain**. This enhances your privacy while roaming in other organisation's roam.fi networks.

Fill in the home organisation RADIUS server's name to *Connect to these servers*. Use **wifi.auth.fi** and select DigiCert Global Root G2 if your home organisation is using Radiator Auth.fi service. Select also Microsoft: Secured password (EAP-MSCHAPv2).

If your organisation is not using Radiator Auth.fi service, please follow your organisation's recommended settings for the above.

Select **Configure** to configure EAP-MSCHAPv2 settings.

TTLS Properties

☒ Enable identity privacy

anonymous@example.com

Server certificate validation

Connect to these servers:

wifi.auth.fi

Trusted Root Certification Authorities:

- ☐ COMODO RSA Certification Authority
- ☐ DigiCert Assured ID Root CA
- ☒ DigiCert Global Root CA
- ☒ DigiCert Global Root G2
- ☐ DigiCert High Assurance EV Root CA

Select only: DigiCert Global Root G2

☒ Don't prompt user if unable to authorise server

Client authentication

☐ Select a non-EAP method for authentication

Unencrypted password (PAP)

☐ Automatically use my Windows account name and password (and domain, if any)

☒ Select an EAP method for authentication

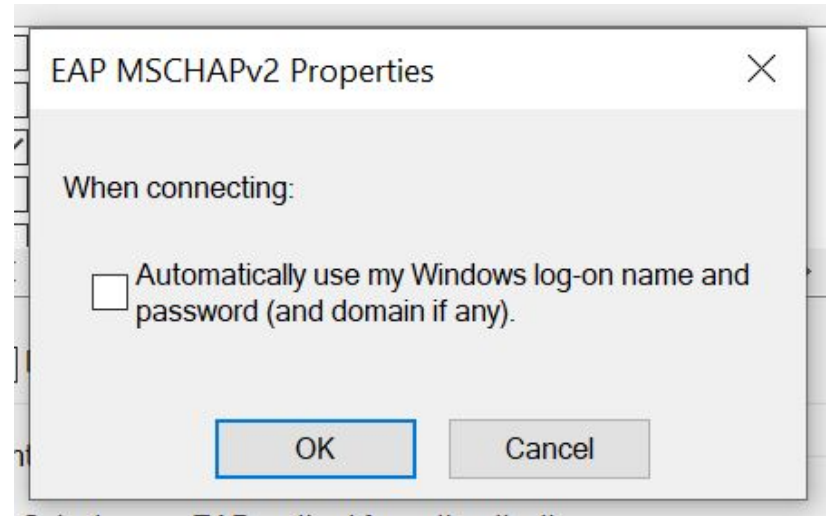
Microsoft: Secured password (EAP-MSCHAP v2)

Configure

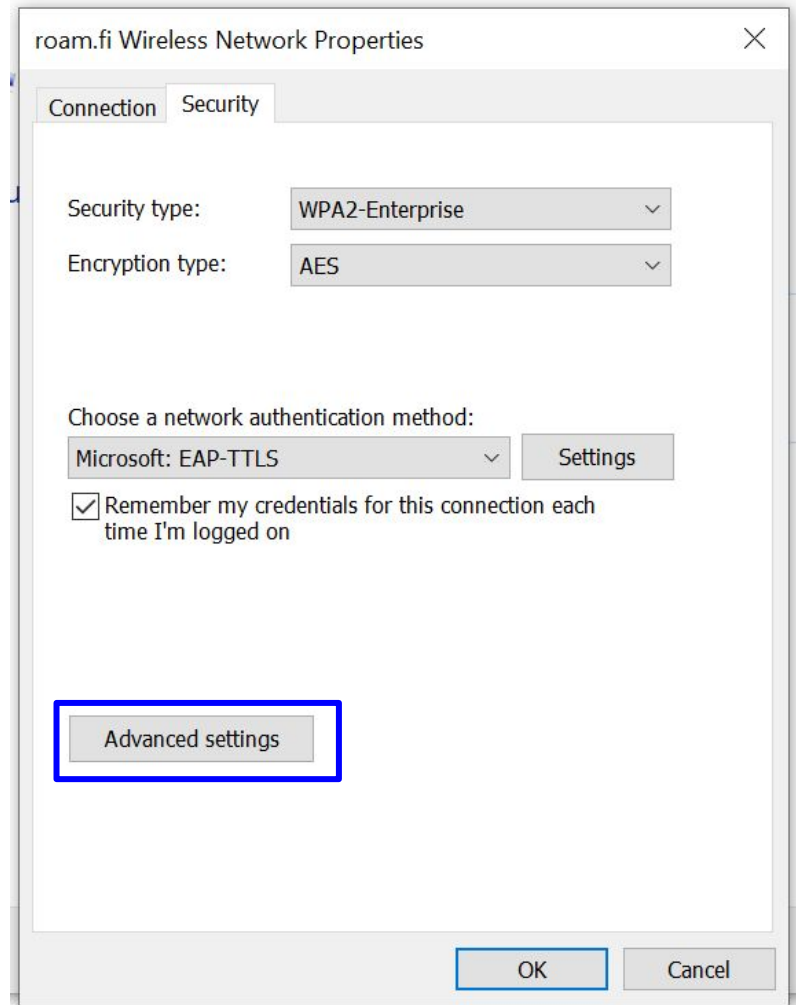
OK Cancel

Ensure from these EAP MSCHAPv2 Properties that Windows does not try to use Windows log-on name and password.

After this you can close this dialog and TTLS settings dialog below by clicking ok on both windows.

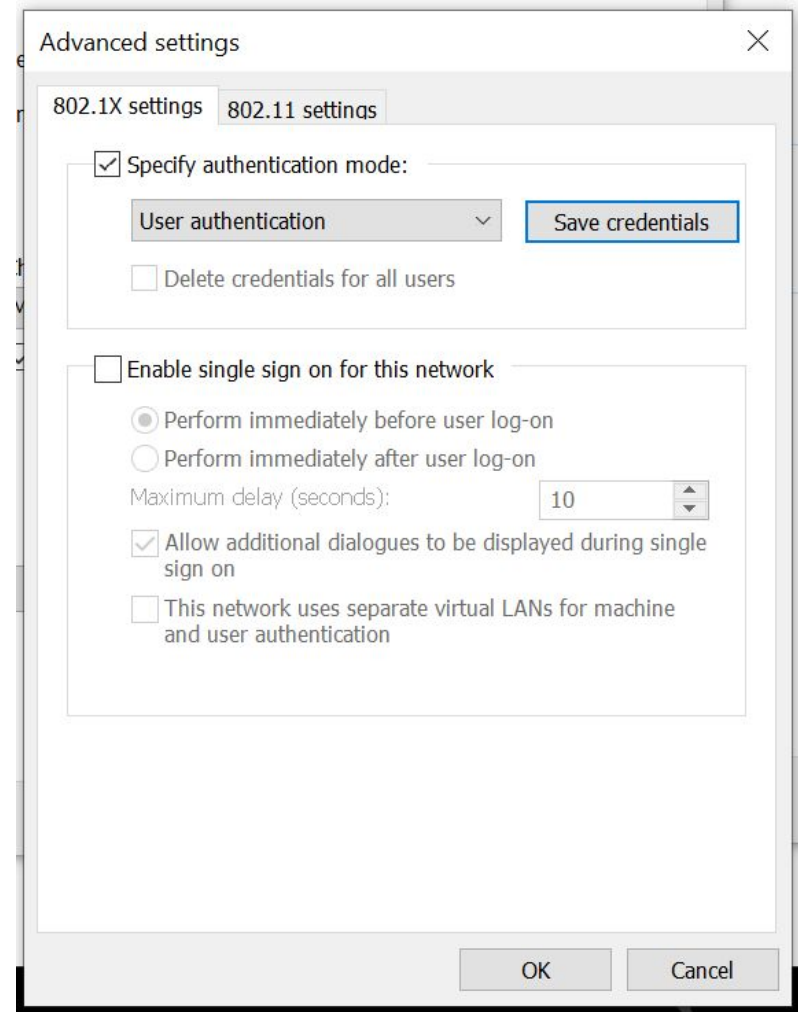


Do not select OK from roam.fi Wireless Network Properties but instead click open Advanced settings.



Set 802.1X settings from Advanced settings as described on the right.

Choose then to *Save credentials* if you have your Radiator Auth.fi or home organisations credentials (username and password) close by.



The image shows a screenshot of a Windows-style dialog box titled "Advanced settings". It has a close button (X) in the top right corner. Inside the dialog, there are two tabs: "802.1X settings" (which is selected) and "802.11 settings".

Under the "802.1X settings" tab, there are two main sections:

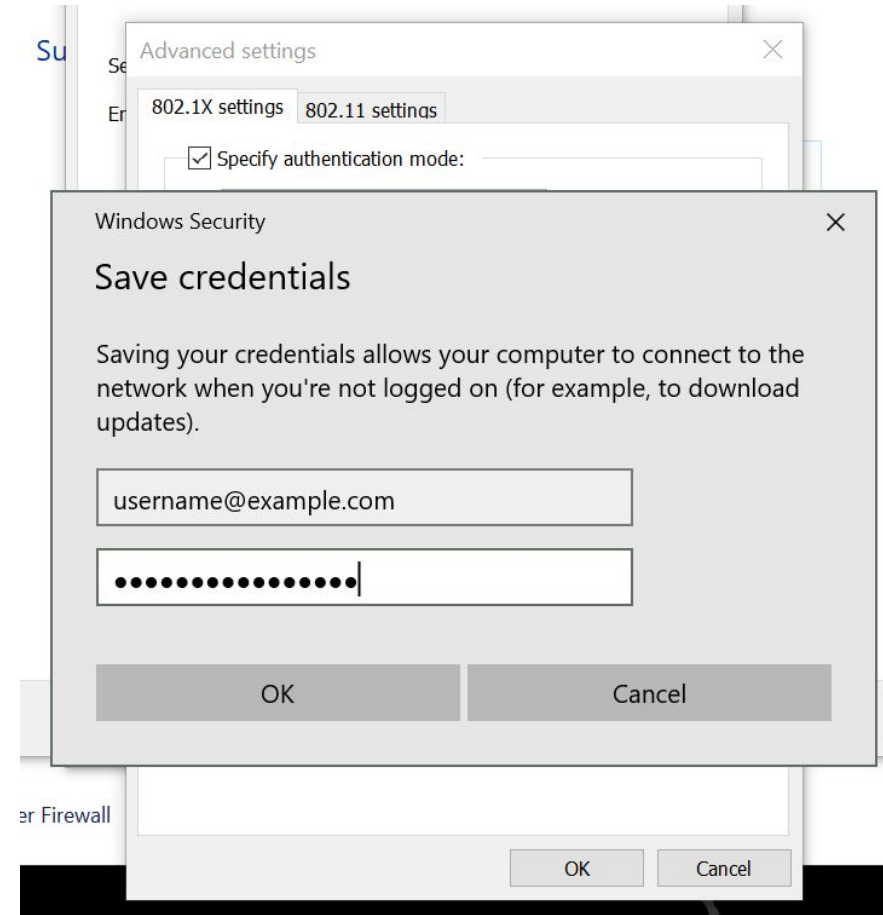
- The first section is titled "Specify authentication mode:" and is preceded by a checked checkbox. It contains a dropdown menu currently set to "User authentication" and a "Save credentials" button to its right. Below this, there is an unchecked checkbox labeled "Delete credentials for all users".
- The second section is titled "Enable single sign on for this network" and is preceded by an unchecked checkbox. It contains two radio buttons: "Perform immediately before user log-on" (which is selected) and "Perform immediately after user log-on". Below these is a label "Maximum delay (seconds):" followed by a numeric input field containing the value "10" and a small up/down arrow control. At the bottom of this section, there are two more checkboxes: "Allow additional dialogues to be displayed during single sign on" (checked) and "This network uses separate virtual LANs for machine and user authentication" (unchecked).

At the bottom of the dialog box, there are two buttons: "OK" and "Cancel".

Fill in the opening *Windows Security* dialog your actual home organisation username and password without forgetting your home organisation (in the example example.com).

By clicking OK Windows saves your username and password for network configuration profile so that you should not need to enter them again.

After clicking OK you will return to the *Advanced Settings* where you can select the *802.11 settings* tab.



The default settings on this **802.11 settings** tab are fine, but you can check from the left that the settings are the same.

When you have verified these settings you can click OK and your roam.fi network configuration profile is ready.

With this profile you do not have to worry about checking server certificate thumbprint or that your device would try to connect a malicious network as the profile does not allow from malicious RADIUS servers or ask you to accept new RADIUS server certificates.

Advanced settings

802.1X settings 802.11 settings

Fast roaming

- ☒ Enable Pairwise Master Key (PMK) caching
 - PMK time to live (minutes): 720
 - Number of entries in PMK cache: 128
- ☐ This network uses pre-authentication
 - Maximum pre-authentication attempts: 3
- ☐ Enable Federal Information Processing Standards (FIPS) compliance for this network

OK Cancel

EXTRA: Additional commands for managing network profiles from command line

Exports existing Wi-Fi profile to an XML file:

**netsh wlan export profile
roam.fi**

```
C:\Users\Karri Huhtanen>netsh wlan export profile roam.fi  
  
Interface profile "roam.fi" is saved in file ".\WiFi-roam.fi.xml" successfully.
```

Deletes a Wi-Fi profile:

**netsh wlan delete profile
roam.fi**

```
C:\Users\Karri Huhtanen>netsh wlan delete profile roam.fi  
Profile "roam.fi" is deleted from interface "WiFi".
```

Imports Wi-Fi profile from XML file to the system and to a current user's use only:

**netsh wlan add profile
filename="WiFi-roam.fi.xml"
user=current**

```
C:\Users\Karri Huhtanen>netsh wlan add profile filename="WiFi-roam.fi.xml" user=current  
Profile roam.fi is added on interface WiFi.
```

These profiles and XML configuration files can also be used with Active Directory domain policies or Intune mobile device management to provision roam.fi and Radiator Auth.fi compatible Wi-Fi configuration profiles to end user devices.

Android

roam.fi network configuration
for Radiator Auth.fi service

By default Android does not support getting the network configuration profile to the device without joining it under some mobile device management. This means that you may need to configure the network settings manually.

On the right there's a screenshot of Android One device correct Wi-Fi network settings for roam.fi network and Radiator Auth.fi authentication service. If your home organisation uses different authentication service, please check the settings from your home organisation.

Domain means the RADIUS server certificate hostname. *Identity* is the actual identity (username) of the user, while *Anonymous Identity* is the anonymous outer identity. Please verify that if you use automatic text fill, it does not add space after the identities. If you are using a roaming network, remember to keep domain as part of your identity and same with both identities

Some Androids do not let user to set CA certificate check at all. These Android devices cannot be configured securely to verify the RADIUS server certificate, which means they are possibly open to man-in-the-middle attacks.

The screenshot shows the Wi-Fi settings of an Android One device. At the top, the status bar displays the time 16:38, battery level at 65%, and icons for alarm, VoWiFi, and cellular signal. The main screen shows a list of Wi-Fi networks. The first network is 'roam.fi' with the EAP method set to 'TTLS' and Phase-2 authentication set to 'MSCHAPV2'. The CA certificate is set to 'Use system certificates'. The domain is 'wifi.auth.fi'. Below this, the 'Identity' field is set to 'username@example.com' and the 'Anonymous identity' field is set to 'anonymous@example.com'. The 'Password' field is set to '(unchanged)'. At the bottom right, there are 'CANCEL' and 'SAVE' buttons. The background shows a blurred view of the device's home screen with some text visible at the bottom: '(fe:ec:da:14:03:5e=2462-503s)(?)' and '12/03/2024'.

16:38 65%
roam.fi
EAP method
TTLS
Phase-2 authentication
MSCHAPV2
CA certificate
Use system certificates
Domain
wifi.auth.fi
Identity
username@example.com
Anonymous identity
anonymous@example.com
Password
(unchanged)
CANCEL SAVE

Apple iPadOS/iOS

Connecting manually to the roam.fi Wi-Fi network

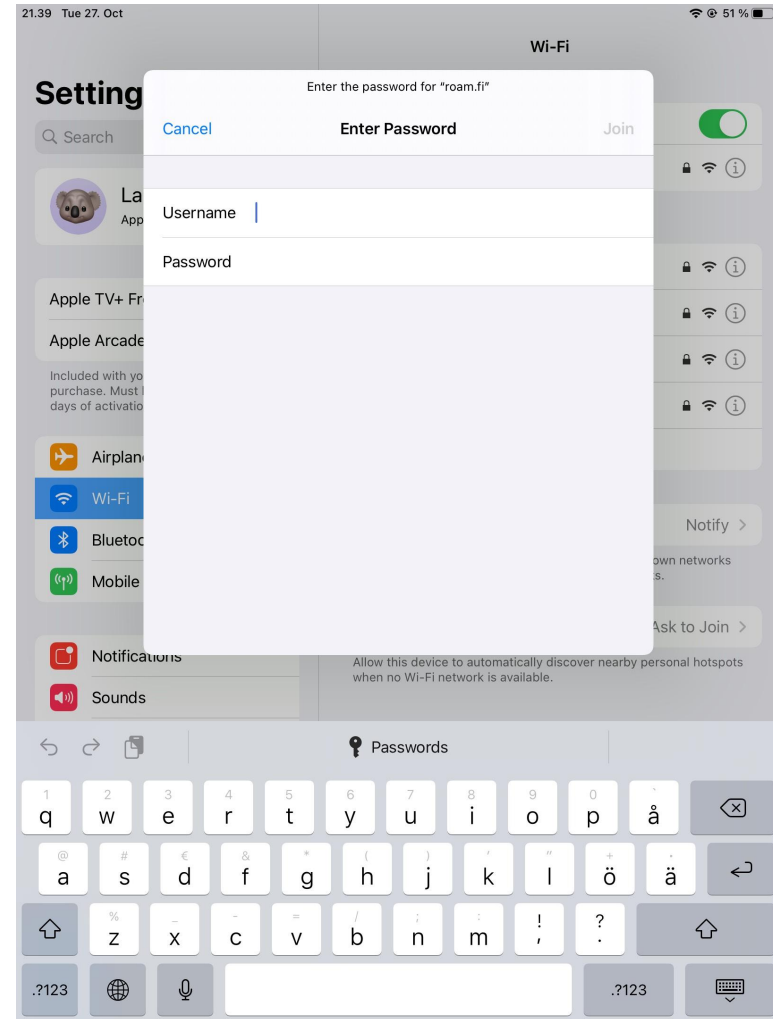
Start by selecting roam.fi network from the list of the Wi-Fi networks.

Next iOS/iPadOS asks for username and password.

When using roaming networks, please remember to fill also domain part of the username.

If you use automatic text fill for username, please check that it does not add spaces after the username.

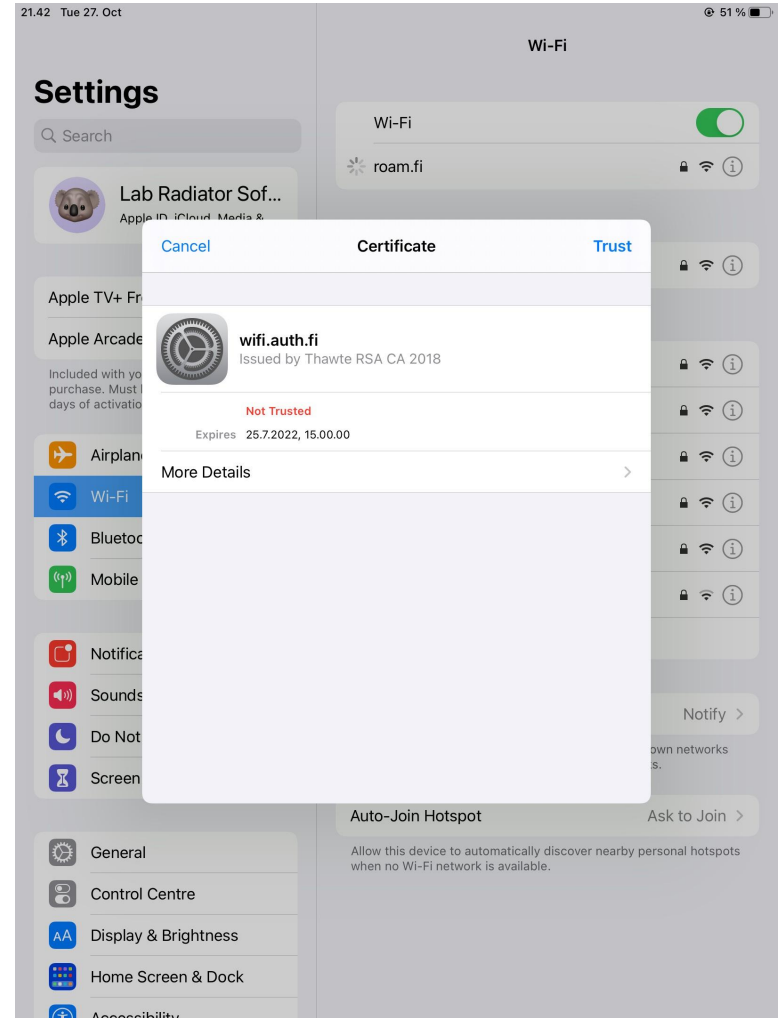
When you have finished entering username and password, click *Join*.



Next iOS/iPadOS asks you to verify the RADIUS server certificate.

For Radiator Auth.fi service the name in the certificate is wifi.auth.fi and iPadOS/iOS informs that it has been issued by Thawte TLS RSA CA G1.

By selecting More Details you can get more information about the certificate to compare it to the details on the next page or with the details provided by your home organisation.



To verify the certificate you can compare the details below to the details your device displays to you.

The certificate *Common Name* wifi.auth.fi.

The issuing organisation is DigiCert Inc. The issuer's *Common Name* is Thawte TLS RSA CA G1.

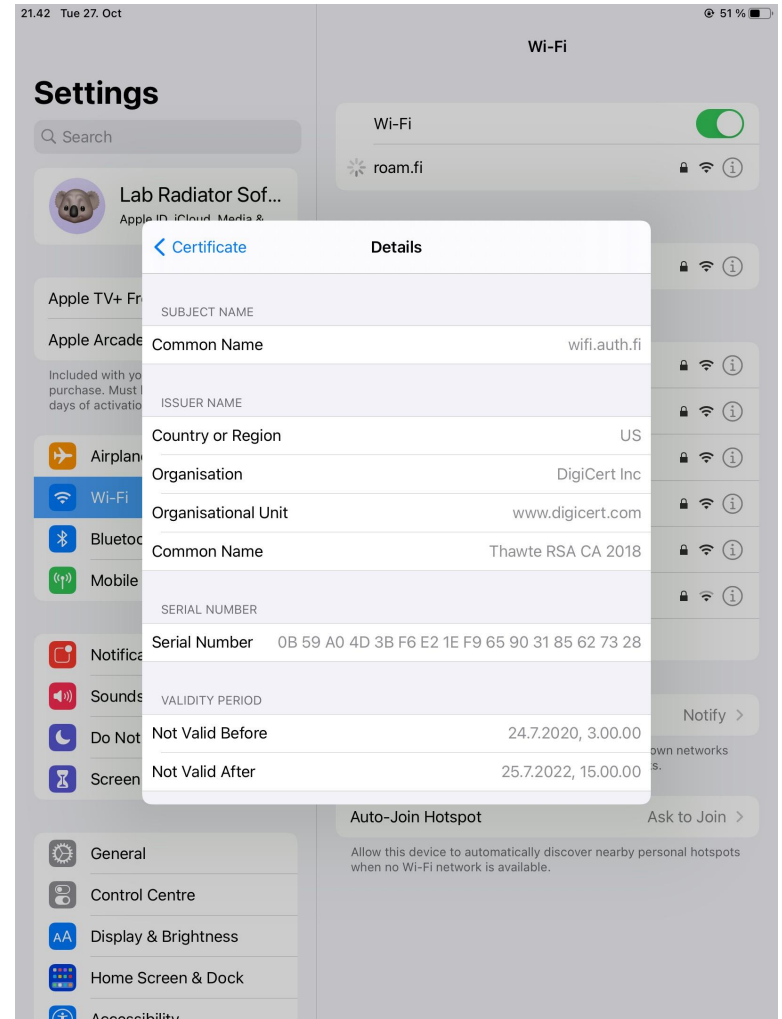
The renewed (2024) certificate's *Serial Number* is:
09 49 28 3F B2 CC 01 16 8F 9B 1B F3 1B 95 42

Validity period (please note that iOS/iPadOS presents this in local time and not in GMT):

Not Valid Before: May 27 00:00:00 2024 GMT

Not Valid After: Jun 27 23:59:59 2025 GMT

If the certificate details look ok, you can return to the previous dialog by clicking Certificate link in the top part of the dialog.



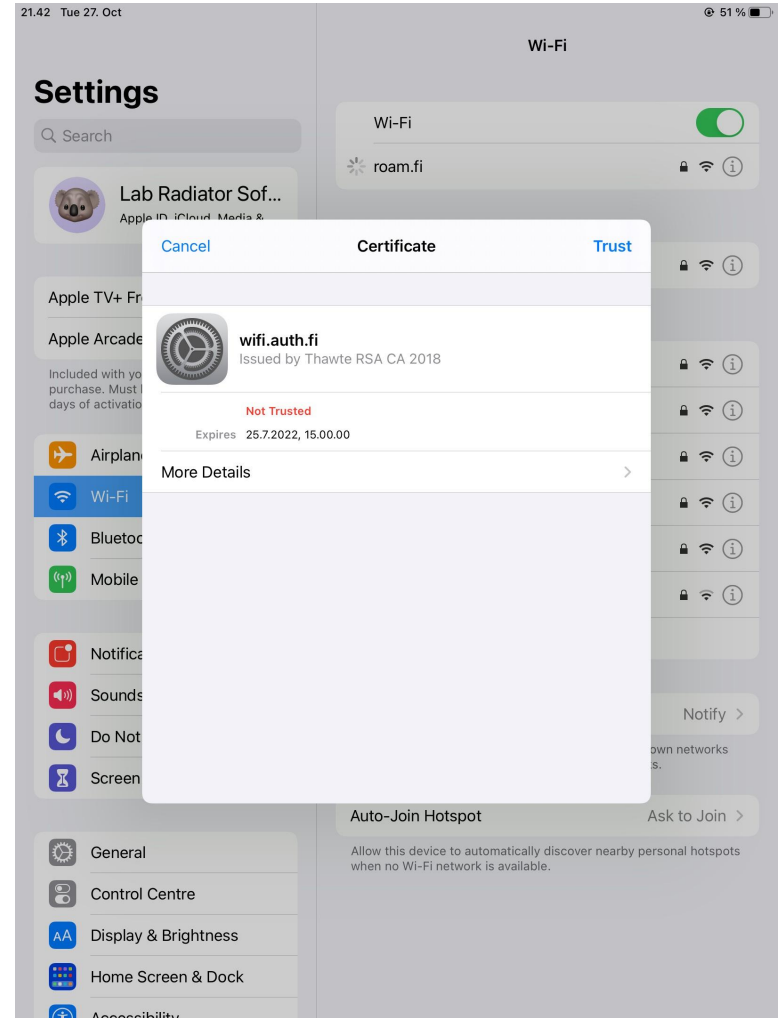
After verifying certificate details or ensuring otherwise the possibility for man-in-the-middle attack is small, you can trust the certificate by clicking trust.

The device should now connect to roam.fi network.

Sometimes entering username and password, verifying certificate details may take too long and authentication expires. The solution is to go through the setup more quickly.

iOS/iPadOs may offer a new certificate to be accepted if the certificate is updated or if someone is trying to capture your username and password. Please check in this case that the certificate has valid details for Radiator Auth.fi service or for your home organisation.

To make an automatic, more secure connection profile for Apple devices, you can use Apple Configurator 2 application to define the Wi-Fi network connection. This kind of profile can be shared via WWW page to users.



Apple MacOS

Connecting manually to the roam.fi Wi-Fi network

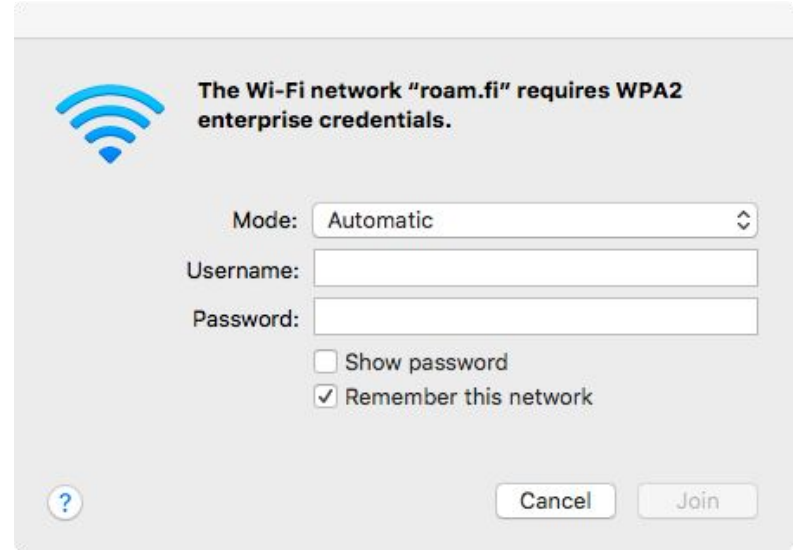
Start by selecting roam.fi network from the list of the Wi-Fi networks.

Next MacOS asks for username and password.

When using roaming networks, please remember to fill also domain part of the username.

If you use automatic text fill for username, please check that it does not add spaces after the username.

When you have finished entering username and password, click Join.



The image shows a MacOS system dialog box for configuring a Wi-Fi network. At the top left is a blue Wi-Fi signal icon. To its right, the text reads: "The Wi-Fi network "roam.fi" requires WPA2 enterprise credentials." Below this, there are three input fields: "Mode:" with a dropdown menu showing "Automatic", "Username:" with an empty text box, and "Password:" with an empty text box. To the right of the password field are two checkboxes: "Show password" (unchecked) and "Remember this network" (checked). At the bottom left is a small circular help icon with a question mark. At the bottom right are two buttons: "Cancel" and "Join".

Next MacOS asks user to *Verify Certificate*.

By clicking *Show Certificate* the certificate details are displayed for better verification.

Checking the certificate details may take so long that the connection is interrupted. The second dialog on the right may be displayed then.

The solution is to enter the username and password more quickly for example by using copy-paste. Also the certificate can be verified more quickly or trusted if in a safe location.



To verify the certificate you can compare the details below to the details your device displays to you.

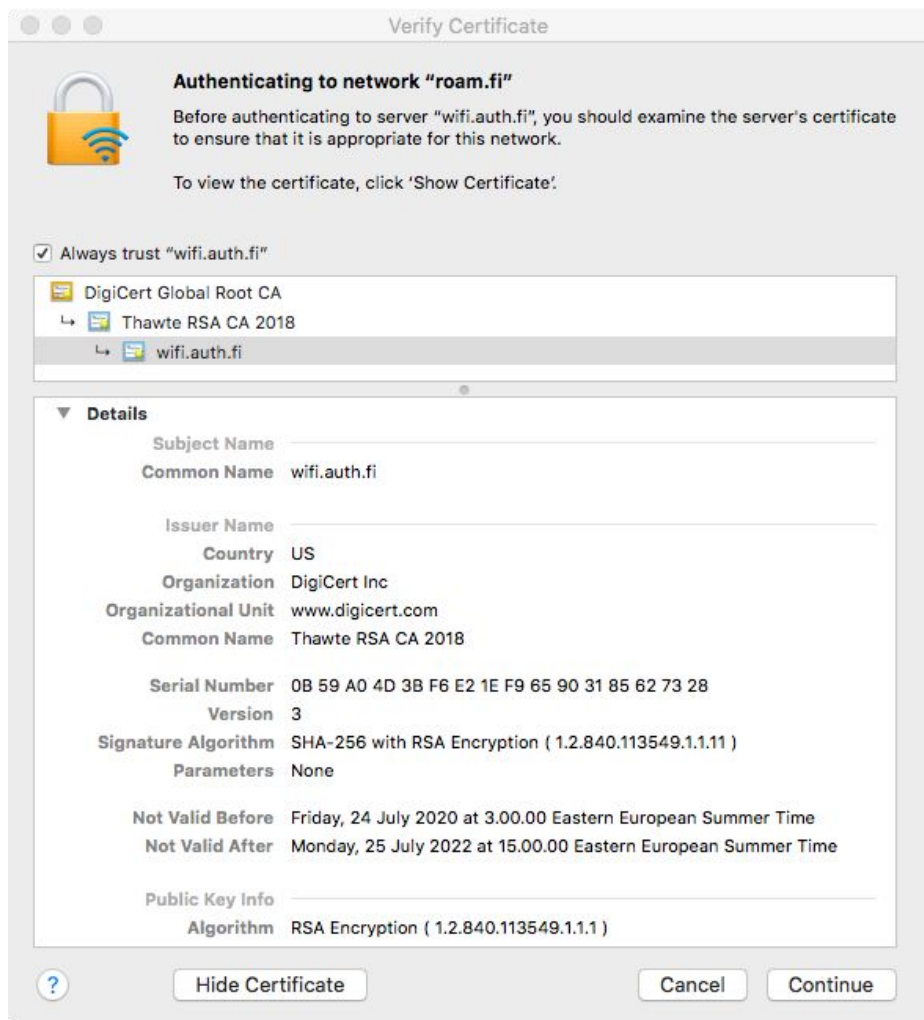
The certificate *Common Name* wifi.auth.fi.

The issuing organisation is DigiCert Inc. The issuer's *Common Name* is Thawte TLS RSA CA G1.

The certificate *Serial Number* is (2024):
09 49 28 3F B2 CC 01 16 8F 9B 1B F3 1B 95 42

Validity period (please note that iOS/iPadOS presents this in local time and not in GMT):
Not Valid Before: May 27 00:00:00 2024 GMT
Not Valid After: Jun 27 23:59:59 2025 GMT

If the certificate details look ok, you can click *Continue*.



If this is a first time connecting into the network, the MacOS may ask user to accept changes to Certificate Trust Settings by entering the current User Name and Password. This is the User Name and Password used in logging into the device. Click Update Settings and the device should join the Wi-Fi network.

Sometimes entering username and password, verifying certificate details may take too long and authentication expires. The solution is to go through the setup more quickly.

MacOS may offer a new certificate to be accepted if the certificate is updated or if someone is trying to capture your username and password. Please check in this case that the certificate has valid details for Radiator Auth.fi service or for your home organisation RADIUS server certificate.

To make an automatic, more secure connection profile for Apple devices, you can use Apple Configurator 2 application to define the Wi-Fi network connection. This kind of profile can be shared via WWW page to users.



The image shows a MacOS dialog box titled "You are making changes to your Certificate Trust Settings." It features a yellow padlock icon with a document and a pencil. The text "Enter your password to allow this." is displayed. Below this, there are two input fields: "User Name:" with the text "Apple User" and "Password:" which is currently empty. At the bottom right, there are two buttons: "Cancel" and "Update Settings".

You are making changes to your Certificate Trust Settings.

Enter your password to allow this.

User Name:

Password:

General Wi-Fi configuration settings

For connecting to roam.fi network
using Radiator Auth.fi service

roam.fi network settings for Radiator Auth.fi using organisations

Setting	Recommended choice	Other supported choices
EAP method / network authentication method	TTLS	PEAP, EAP-PWD*
Phase-2 authentication	MSCHAP-V2	EAP-MSCHAP v2
CA Certificate	If DigiCert Global Root G2 is choosable, then it, otherwise Use System Certificates	If device does not support certificate verification one may have to choose Do not validate (**) or other similar setting, which makes the user/device vulnerable.
CA / Root CA / Trusted Root Certification Authority	DigiCert Global Root G2	
Domain / server name	wifi.auth.fi	
Identity / inner identity / username	username@example.com	
Anonymous Identity / outer identity	anonymous@example.com	username@example.com

*) EAP-PWD does not need certificates and its use is safer than TTLS and PEAP if the device does not support certificate verification. It is however available only as an experimental level protocol in the Radiator Auth.fi service and the operating system support is limited.

**) Android 11 QPR1 security update in December 2020 is supposed to remove the option of not validating the server certificate in Android