## Connecting to eduroam on Windows 8 and 10 operating systems (manual)

1. Open the **Control Panel / Network and Sharing Center** from the Start menu, or right-click the network icon in the bottom right corner of the taskbar to select it in the pop-up window.



2. Select **Set up a new connection or network**, then select **Manually connect** to wireless network.



Next

Cancel

 After clicking Next, you can enter the details of the new wireless network. The Network name: eduroam, the Security type: WPA2-Enterprise and the Encryption type: AES. Once the data is filled in, click Next!

Enter informatio	n for the wireless netwo	ork you want to add	
Network name:	eduroam		
Security type:	WPA2-Enterprise	~	
Encryption type:	AES		
Security Key:		Hide characters	
Start this conne	ection automatically		
Connect even i	f the network is not broadcasti	ng	
Warning: If you	select this option, your compu	ter's privacy might be at risk.	

4. When the Network Profile is ready, click on Change Connection Settings.



5. In the eduroam network properties window, switch to the *Security tab* and click the *Settings* button next to *Network authentication method*.

connection Security	>	
Security type:	WPA2-Enterprise	~
Encryption type:	AES	$\sim$
Choose a network a Microsoft: Protecte	authentication method: ed EAP (PEAP) V	ettings
	and the second	
Remember my time I'm logged	credentials for this connection	escht -
✓ Remember my time I'm logged Advanced setting	credentials for this connection	

6. For the server, type: **wifi.bibl.u-szeged.hu** and in the list of CAs, click the checkbox in front of **USERTrust RSA Certification Authority**.

When connecting:  Verify the server's identity by validating the certificate  Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):  Wifi.bibl.u-szeged.hu  Trusted Root Certification Authorities: UCA Root UTN-USERFirst-Client Authentication and Email UTN-USERFirst-Alardware UTN-USERFirst-Network Applications USERTrust RSA Certification Authority USERTrust ECC Certification Authority USERTrust ECC Certification Authority USERTrust ECC Certification Authority USERFirst-Object  Textifications before connecting: Tell user if the server's identity can't be verified
<ul> <li>Verify the server's identity by validating the certificate</li> <li>Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):</li> <li>wifi.bibl.u-szeged.hu</li> <li>Trusted Root Certification Authorities:</li> <li>UCA Root</li> <li>UTN-USERFirst-Client Authentication and Email</li> <li>UTN-USERFirst-Network Applications</li> <li>USERTrust RSA Certification Authority</li> <li>SERTrust ECC Certification Authority</li> <li>SERTIFICE Content Authority</li> <li>SERTIFICE Content Authority</li> <li>SERTIFICE Content Authority</li> <li>Sertification Server's identity can't be verified</li> </ul>
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com): <pre>wifi.bibl.u-szeged.hu Trusted Root Certification Authorities: UCA Root UTN-USERFirst-Client Authentication and Email UTN-USERFirst-Hardware UTN-USERFirst-Network Applications USERTrust RSA Certification Authority USERTrust RSA Certification Authority USERTrust ECC Certification Authority USERFirst-Object Confications before connecting: Tell user if the server's identity can't be verified </pre>
Connect to these server's (examples: stv1; stv2;, - (.stv3,.com):  wifi.bibl.u-szeged.hu  Trusted Root Certification Authorities: UCA Root UTN-USERFirst-Client Authentication and Email UTN-USERFirst-Network Applications USERTrust RSA Certification Authority USERTrust ECC Certification Authority USERTrust ECC Certification Authority USERFirst-Object  Notifications before connecting: Tell user if the server's identity can't be verified
wifi.bibl.u-szeged.hu         Trusted Root Certification Authorities:         UCA Root         UTN-USERFirst-Client Authentication and Email         UTN-USERFirst-Network Applications         UTN-USERFirst-Network Applications         USERTrust RSA Certification Authority         USERTrust ECC Certification Authority         UTN-USERFirst-Object         VIN-USERFirst-Object         Notifications before connecting:         Tell user if the server's identity can't be verified
Trusted Root Certification Authorities: UCA Root UTN-USERFirst-Client Authentication and Email UTN-USERFirst-Hardware UTN-USERFirst-Network Applications USERTrust RSA Certification Authority USERTrust ECC Certification Aut
UCA Root UTN-USERFirst-Client Authentication and Email UTN-USERFirst-Hardware UTN-USERFirst-Network Applications USERTrust RSA Certification Authority USERTrust ECC Certification Authority USERFirst-Object  Notifications before connecting: Tell user if the server's identity can't be verified
UTN-USERFirst-Client Authentication and Email UTN-USERFirst-Hardware UTN-USERFirst-Network Applications USERTrust RSA Certification Authority USERTrust ECC Certification Authority UTN-USERFirst-Object
UTN-USERFIrst-Hardware         UTN-USERFirst-Network Applications         USERTrust RSA Certification Authority         SERTrust ECC Certification Authority         UTN-USERFirst-Object         Image: Series of the server's identity can't be verified         Tell user if the server's identity can't be verified
UTN-USERFirst-Network Applications USERTrust RSA Certification Authority SERTrust ECC Certification Authority UTN-USERFirst-Object  Notifications before connecting: Tell user if the server's identity can't be verified
VUSERI rust RSA Certification Authority VISERTrust ECC Certification Authority VISERTILUSERFIRST-Object  Notifications before connecting:  Tell user if the server's identity can't be verified
Automit ECC Certification Automity      Structure Certification Automity      Notifications before connecting:      Tell user if the server's identity can't be verified
A variable of the server's identity can't be verified
Notifications before connecting:  Tell user if the server's identity can't be verified
Notifications before connecting: Tell user if the server's identity can't be verified ~
Tell user if the server's identity can't be verified V
Colored Authorithmeticae Marthands
Select Authentication Method:
Secured password (EAP-MSCHAP v2)  V Configure
Enable East Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK Cancel

7. Next to Authentication Mode, click **Configure** and in the pop-up window, **uncheck the box** next to **Automatically use Windows login name and password** when connected if it is checked.

Protected EAP Properties	×
When connecting:	
EAP MSCHAPv2 Properties	×
When connecting: τ τ τ τ τ τ τ τ τ τ	e and
UTN-USERFirst-Network Applications USERTrust RSA Certification Authority SERTrust ECC Certification Authority UTN-USERFirst-Object	
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 Enable Identity Privacy	TLV

8. Click *OK* to go back to the eduroam network properties window and open the *Advanced settings*. In the Authentication Mode drop-down menu, select *User Authentication*.

Connection Security				
Security type:	WPA2-E	nterprise		~
Encryption type:	AES			$\sim$
	Adva	nced setting	gs	
Choose a network au	the 802.1	X settings	302.11 setting	js
Microsoft: Protected	FAI			
		Snocify au	thentication m	node:
Remember my cro	ede	Specify au	thentication m	node: enticatior ~
Remember my cro time I'm logged o	ede n	Specify au User or o User or o Computer	thentication m computer author computer author authentication	node: enticatior ~ entication
Remember my cro time I'm logged o	ede n	Specify au User or o User or o Computer User auth Guest aut	thentication m computer author computer author authentication contication hentication	node: enticatior ~ entication on
Remember my cru time I'm logged o	ede n	Specify au User or o User or o Computer User auth Guest aut	thentication m omputer author outputer author authentication hentication gle sign on fo	node: enticatior v entication on r this network
Remember my cro time I'm logged o	ede n	Specify au User or o User or o Computer User auth Guest aut	thentication m omputer author authentication entication hentication gle sign on for m immediately	entication v entication on r this network
Remember my cro time I'm logged o	ede n	Specify au User or o User or o Computer User auth Guest aut Enable sin Perfor	thentication n omputer authomputer authomputer authentication entication hentication gle sign on foo n immediately n immediately	node: entication v entication on r this network y before user log v after user log
Remember my creative settings	ede n	Specify au User or o User or o Computer User auff Guest aut Enable sin Perforr Perforr Maximum	thentication m omputer auth- outhentication entication gle sign on for m immediately n immediately delay (second	entication v entication v entication on r this network y before user log ds):
Remember my creative lime I'm logged o	ede n	Specify au User or o User or o Computer User auth Guest aut Enable sin Perforr Maximum Allow a sign or	thentication m omputer auth- muter auth- authentication entication gle sign on for m immediately delay (second additional dial-	entication v entication on r this network y before user log da): ogs to be displa

9. Click on the Save Credentials button and enter your username and password.



The *username* consists of two parts. The first half is the **number of your** *student card/library card/university staff card*, the second half is the same for everyone: @*bibl.u-szeged.hu* 



123456789@bibl.u-szeged.hu OLV99887766@bibl.u-szeged.hu

The default password (if you previously have not set a unique password in the online catalogue) is our *own date of birth* in the *form dd-MMM-yy*, e.g.: *04-SEP-94* (in the middle, the first three characters of the month all should be in capital letters).

10. If everything is set up and configured correctly, your device is connected to the network.

