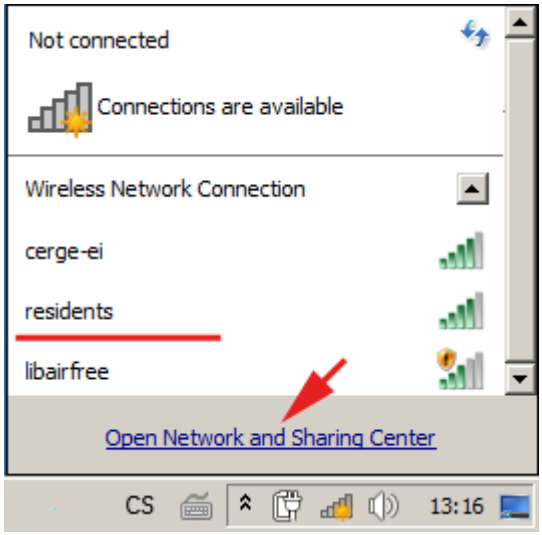
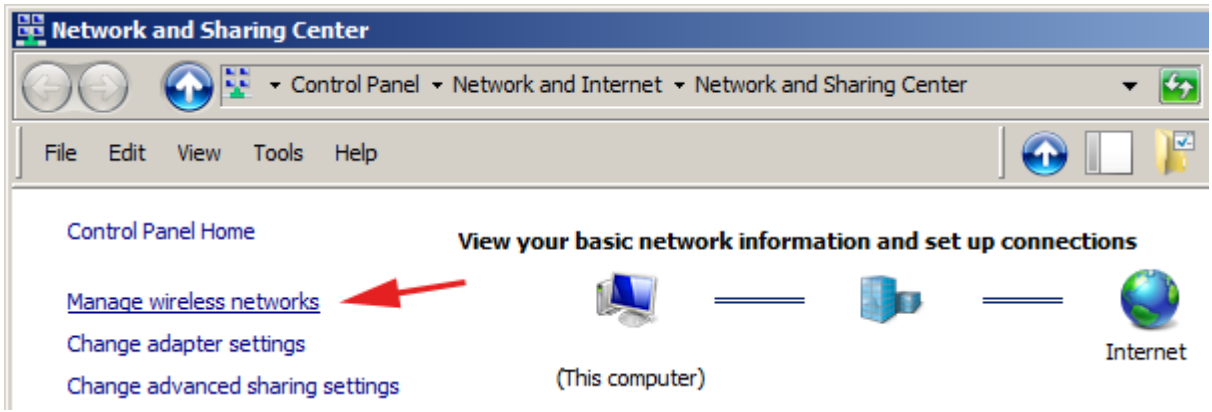
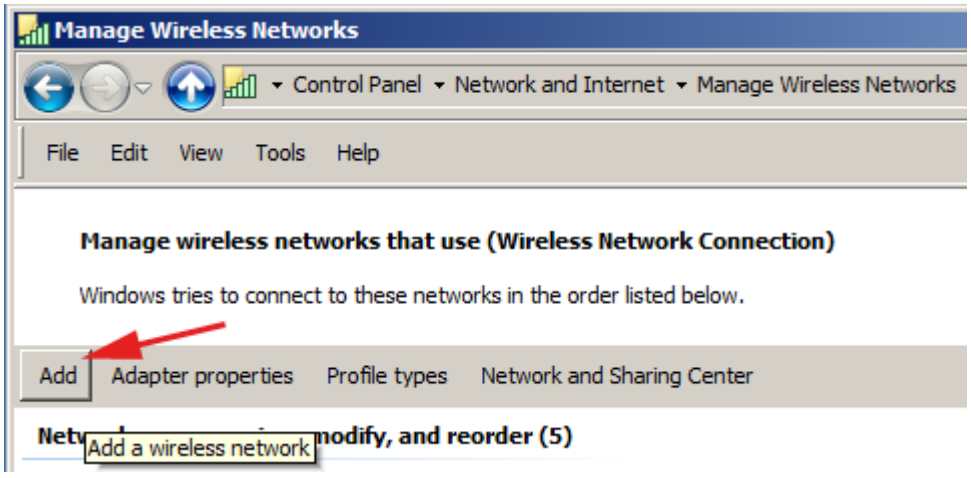
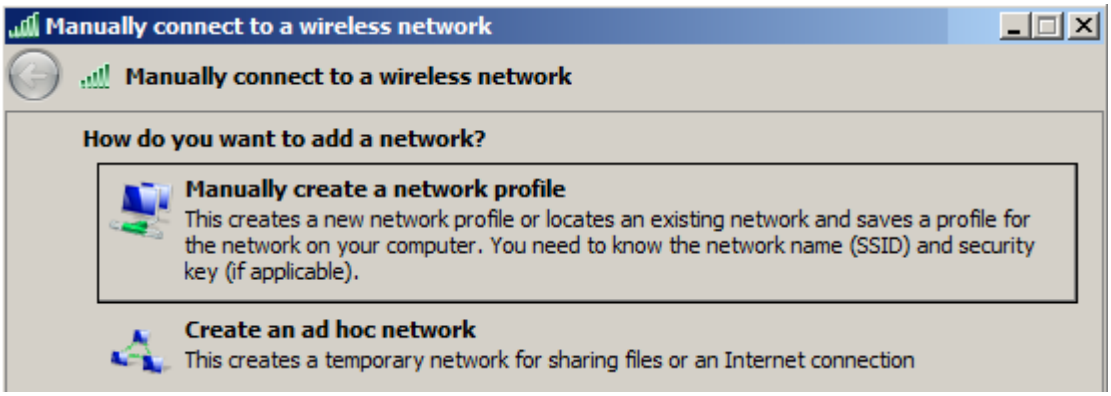
Wi-Fi 'residents' - Windows 7 Howto Guide

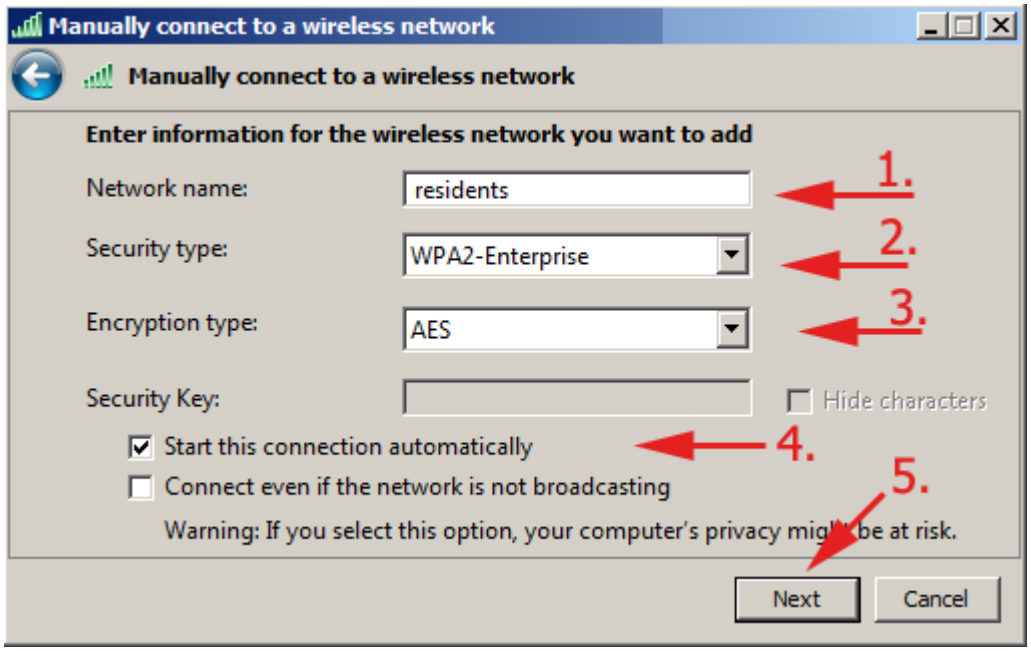
Following screenshots will guide you through the Wi-Fi setting in Windows 7. Other versions of Windows should work almost the same, pictures may vary...

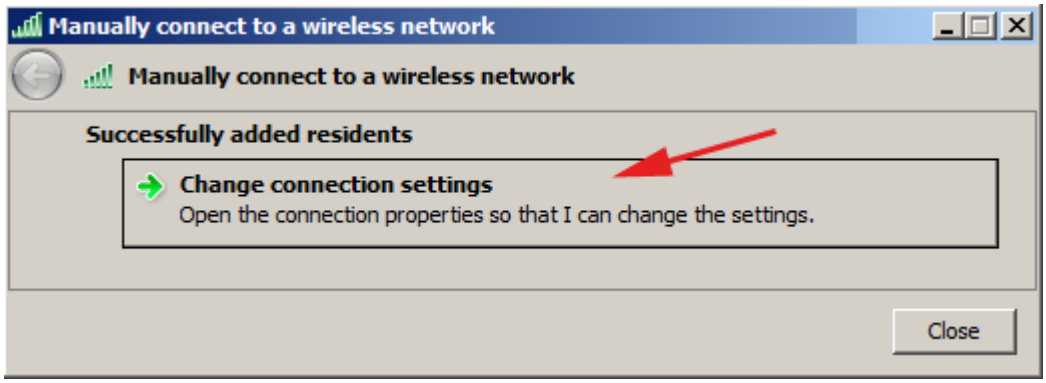


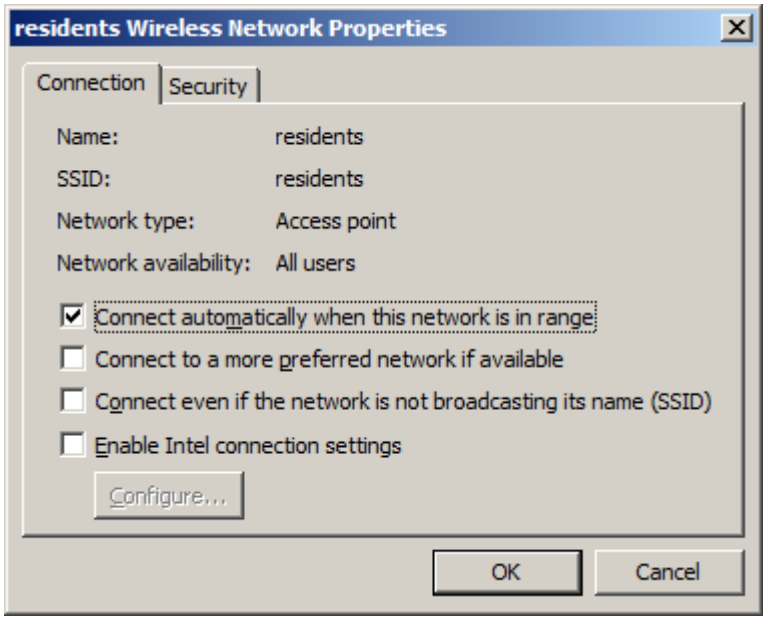


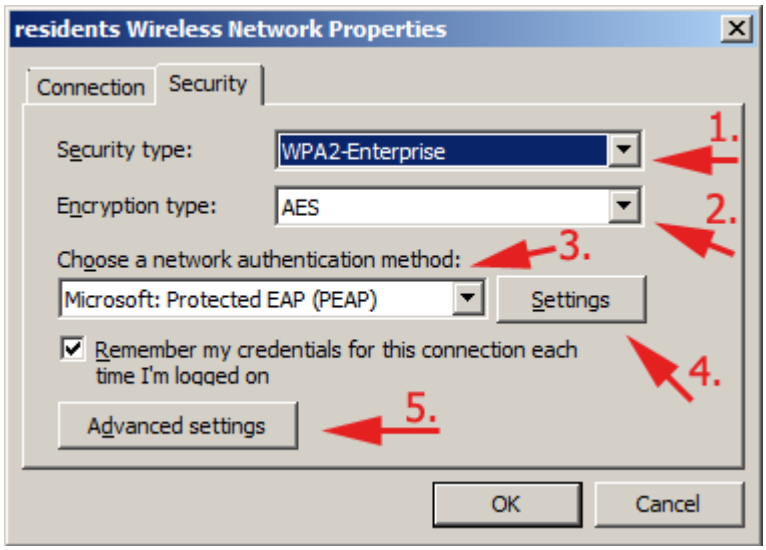


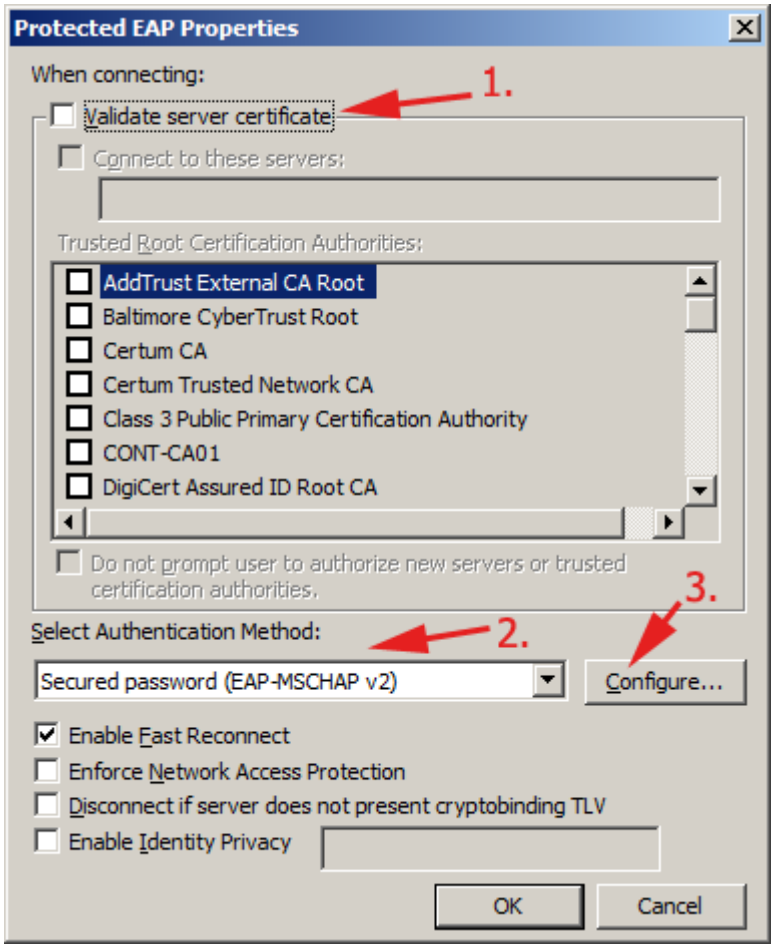

Manually connect to a wireless network
Manually connect to a wireless network
How do you want to add a network?
Manually create a network profile
This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).
Create an ad hoc network
This creates a temporary network for sharing files or an Internet connection

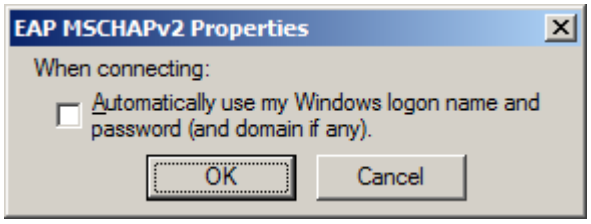

Manually connect to a wireless network
Manually connect to a wireless network
Enter information for the wireless network you want to add
Network name:
residents
1.
Security type:
WPA2-Enterprise
2.
Encryption type:
AES
3.
Security Key:
Hide characters
Start this connection automatically
4.
Connect even if the network is not broadcasting
5.
Warning: If you select this option, your computer's privacy might be at risk.
Next
Cancel

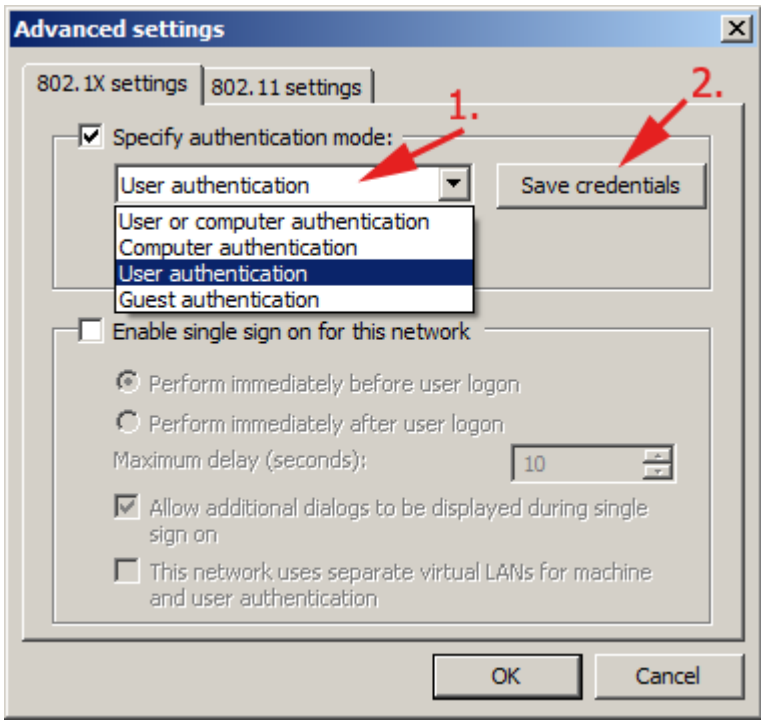

Manually connect to a wireless network
Manually connect to a wireless network
Successfully added residents
Change connection settings
Open the connection properties so that I can change the settings.
Close

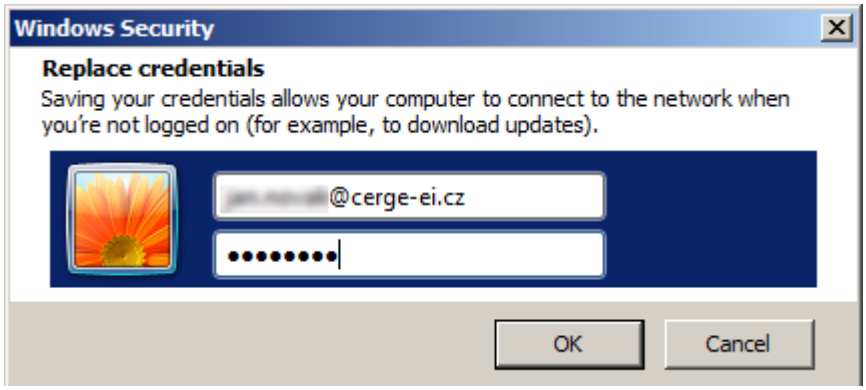

residents Wireless Network Properties
Connection
Security
Name: residents
SSID: residents
Network type: Access point
Network availability: All users
Connect automatically when this network is in range
Connect to a more preferred network if available
Connect even if the network is not broadcasting its name (SSID)
Enable Intel connection settings
Configure...
OK
Cancel

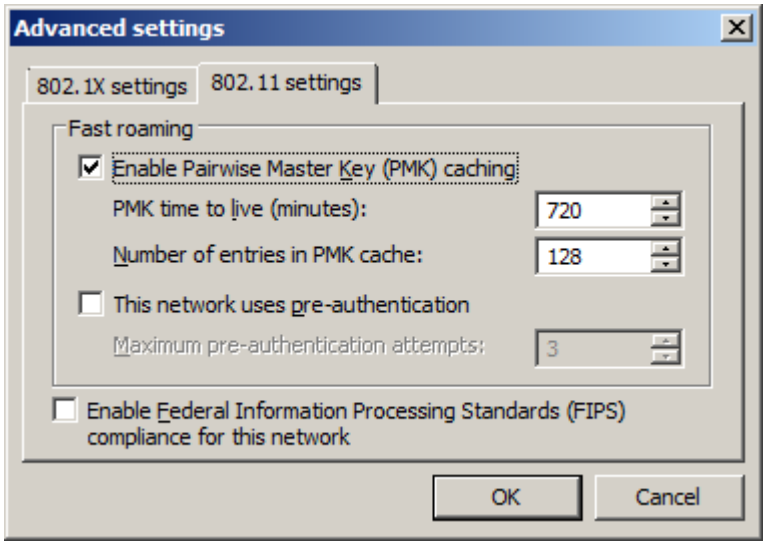

residents Wireless Network Properties
Connection
Security
Security type: WPA2-Enterprise
1.
Encryption type: AES
2.
Choose a network authentication method:
3.
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
4.
Advanced settings
5.
OK
Cancel

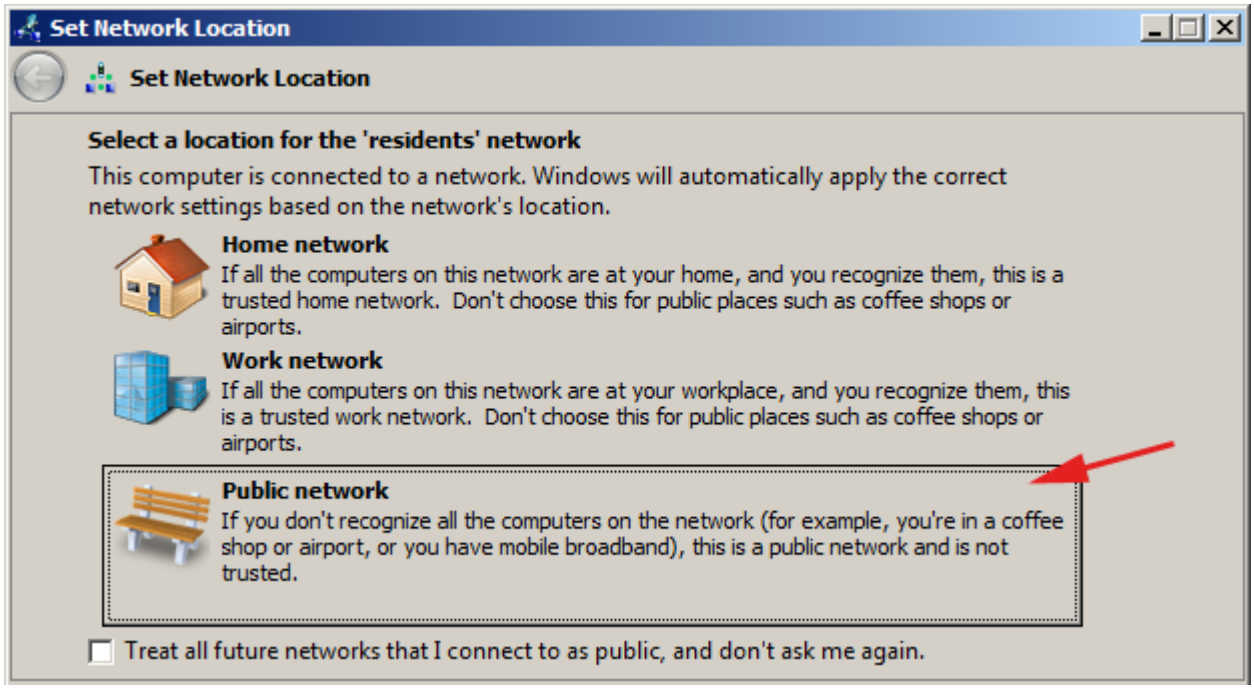

Protected EAP Properties
When connecting:
1.
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
AddTrust External CA Root
Baltimore CyberTrust Root
Certum CA
Certum Trusted Network CA
Class 3 Public Primary Certification Authority
CONT-CA01
DigiCert Assured ID Root CA
Do not prompt user to authorize new servers or trusted certification authorities.
3.
Select Authentication Method:
2.
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Enforce Network Access Protection
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

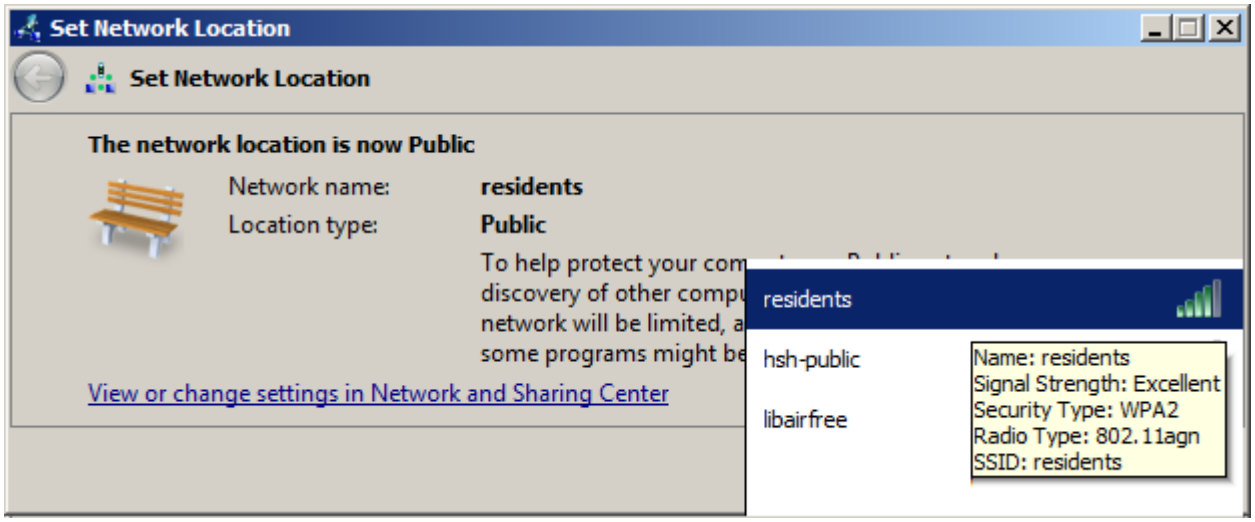

EAP MSCHAPv2 Properties
When connecting:
Automatically use my Windows logon name and password (and domain if any).
OK
Cancel


Advanced settings
802.1X settings
802.11 settings
1.
2.
Specify authentication mode:
User authentication
Save credentials
User or computer authentication
Computer authentication
User authentication
Guest authentication
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel


Windows Security
Replace credentials
Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).
@cerge-ei.cz
OK
Cancel


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


Set Network Location
Set Network Location
Select a location for the 'residents' network
This computer is connected to a network. Windows will automatically apply the correct network settings based on the network's location.
Home network
If all the computers on this network are at your home, and you recognize them, this is a trusted home network. Don't choose this for public places such as coffee shops or airports.
Work network
If all the computers on this network are at your workplace, and you recognize them, this is a trusted work network. Don't choose this for public places such as coffee shops or airports.
Public network
If you don't recognize all the computers on the network (for example, you're in a coffee shop or airport, or you have mobile broadband), this is a public network and is not trusted.
Treat all future networks that I connect to as public, and don't ask me again.



From:
https://wiki.cerge-ei.cz/ - **CERGE-EI Infrastructure Services**

Permanent link:
https://wiki.cerge-ei.cz/doku.php?id=public:wifiguide:resident-win7

Last update: **2017-03-30 08:34**