802	1 x	Windows	7

If this is the first time that the computer is connected via 802.1x authentication must enable the service.

Enabling the service

- click the Start button in the Search box, type services.msc and then press ENTER,
- on the Services tab that opens, look for the service named Wired AutoConfig right-click and select Properties,
- change the item Startup type from Manual to Automatic,
- if the service status is *Stopped*, click on the **Start** button.

Wired AutoConfig	Properties (Local Computer)	×
General Log On	Recovery Dependencies	
Service name:	dot3evc	
Display name:	Wired AutoConfig	
Description:	The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X	*
Path to executab C:\Windows\syst	le: em32\swchost.eve.ik.LocalSystemNetworkRestricted	
Startup type:	Automatic	$\overline{}$
Help me configur	e service startup options,	_
Service status:	Stopped	
Start	Stop <u>P</u> ause <u>R</u> esume	
You can specify t from here.	he start parameters that apply when you start the servi	ce
Start parameters:		
	OK Cancel A	ply

Settings Supplicant 802.1x

- Open the settings for the network adapter: DX-click on the icon of the LAN connection (lower right) then select *Open Network and Sharing Center*, click on *Change adapter setting*,
- DX-click on the connection for which you want to enable 802.1x authentication then select **Properties**,
- click on tab **Authentication** and then select the check boxes:
 - $\circ\,$ Enable IEEE 802.1X authentication,
 - Remember my credentials...,
 - Fallback to unauthorized....

Last update: 2013/10/22 13:06

pub:win-7-en



- Click on the button Settings and on the Protected EAP Properties window that appears check that:
 - is checked Validate server certificate choosing from the Trusted Root Certification Authorities the voice AddTrust External CA Root,
 - is checked Connect to these servers stating the following (separated by ;) nps1.unitn.it;nps2.unitn.it;nps3.unitn.it,
 - the authentication method selected is Secured password (EAP-MSCHAP v2).

Uben conner	ting	-	
when connect	tang:		
<u>V</u> alidate	server certificate		
	t to these servers:		
nps1	.unitn.it;nps2.unitn.it;	nps3.unitn.it	
Trusted Ro	ot Certification Author	ities:	
AddTr	ust External CA Root		*
E Baltimo	re CyberTrust Root	•	
Class 3	Public Primary Certific	ation Authority	
Class :	Public Primary Certific	ation Authority	
DigiCe	rt High Assurance EV P	toot CA	
Entrus	t.net Secure Server O	ertification Authority	
Equifa	x Secure Certificate Ar	uthority	-
4			
certifica	tion authorities.		
Select Auther			
elect Auther	sword (EAP-MSCHAP v	2) - 🗸	Configure
Secured pas	sword (EAP-MSCHAP v st Reconnect	(2)	Configure
elect Auther Secured pas Enable Ea	sword (EAP-MSCHAP) st Reconnect etwork Access Protect	(2) 🔹 📢	<u>C</u> onfigure
Secured pas	sword (EAP-MSCHAP) st Reconnect etwork Access Protect t if server does not pr	(2)	Configure
elect Auther Secured pas Enable Ea Enforce N Disconnec Enable Ide	sword (EAP-MSCHAP) st Reconnect etwork Access Protect t if server does not pr entity Privacy	(2) vion esent cryptobinding TLV	Configure
Secured pas	sword (EAP-MSCHAP) st Reconnect etwork Access Protect t if server does not pr entity Privacy	(2) vion esent cryptobinding TLV	<u>C</u> onfigure
Secured pas	sword (EAP-MSCHAP) st Reconnect etwork Access Protect t if server does not pr entity Privacy	(2)	Configure

The following configuration is required only for PC **NOT** in the UNITN domain (for PC in the UNITN domain skip this step)

• Click the **Configure** button, then from the Properties window that appears EAP MASCHAPv2 **de**select the item *Automatically use....* as shown below:

EAP MSCHA	Pv2 Properties	5	x
When con	necting:		
	natically use my word (and domai	Windows logon na n if any).	ame and
	ОК	Cancel]

- Click the button Additional Settings... for the tab *Properties Local Area Connection* (*LAN*) and on the tab *Advanced setting* that will appear check:
 - that the item *Specify authentication mode* is checked, choosing among:
 - User authentication (For computer NOT in UNITN domain),
 - User or computer authentication (For computer in UNITN domain),
 - click on the button **Save Credetials**.

. IX settings	
Construction model	
User authentication	 Replace gredentials
Delete credentials for all use	rs
Enable gingle sign on for this ne	twork
Perform immediately before	user logon
Perform immediately after us	ser logon
Maximum delay (seconds):	10 *
Allow additional dialogs to be sign on	e displayed during single
This network uses separate and user authentication	virtual LANs for machine

• After connecting the network cable when prompted, enter your unitn credentials

pub:win-7-en



In the event that the credentials are not recognized you will be automatically redirected to a Captive Portal authentication.

Problems

Force the reauthentication:

• Unselect *Remember my credentials...* then deactivate/activate the network card:



