## 802.1x Windows Vista Spk2

Se non è la prima volta che il computer viene collegato mediante autenticazione 802.1x occorre abilitare il servizio.

## Abilitazione del servizio

- Click sul pulsante Start, nella casella Cerca digitare **services.msc** e quindi premere INVIO.
- Sulla scheda Servizi che si è aperta, cercare il servizio con nome **Configurazione automatica reti cablate** fare click destro e selezionare **Proprietà**.
- Cambiare la voce Tipo di avvio da Manuale ad Automatico.
- Se lo stato del servizio è Arrestato, cliccare sul pulsante Avvia.

Proprietà (Computer locale) - Configurazione automatica reti cabl			
Generale Connessione Ripristino Relazioni di dipendenza			
Nome del servizio: dot3svc			
Nome visualizzato: Configurazione automatica reti cablate			
Descrizione: Questo servizio esegue l'autenticazione IEEE * *			
Percorso file eseguibile: C:\Windows\system32\svchost.exe +k LocalSystemNetworkRestricted			
Ipo di avvio: Automatico			
Informazioni sulla configurazione delle opzioni di avvio del servizio,			
Stato del servizio: Arrestato			
Agvia Arresta Sospendi Riprendi			
È possibile specificare i parametri iniziali da applicare quando il servizio viene avviato da qui.			
Parametri di avvio:			
OK Annulia Applica			

## Impostazioni del Supplicant 802.1x

- Aprire le impostazioni della scheda di rete cliccando su Start selezionare *Pannello di Controllo Rete e Internet* e quindi su **Centro di connessioni di rete e condivisione**, a questo punto selezionare dalla lista in alto a sinistra la voce **Gestisci connessioni di rete**.
- Fare click con il pulsante destro del mouse sulla connessione per cui si desidera abilitare l'autenticazione 802.1x e quindi scegliere **Proprietà**.
- Fare click sulla scheda **Autenticazione** e quindi selezionare le caselle di controllo Abilita autenticazione IEEE 802.1X e Memorizza informazioni utente per....

×

Fare click sul pulsante *Impostazioni* e sulla finestra di Proprietà PEAP che apparirà controllare:

 che sia spuntata la voce *Convalida certificato del server* scegliendo tra le *Autorità di certificazione principale attendibili* la voce *AddTrust External CA Root*,

• che il metodo di autenticazione selezionato sia *Password protetta (EAP-MSCHAP v2)* 

Proprietà PEAP
Per la connessione: Convalda certificato server Conne <u>t</u> ti ai server seguenti:
Autorità di certificazione principale attendibili:
Selezionare il metodo di autenticazione:  Password protetta (EAP-MSCHAP v2)  Abilita riconnessione rapida  Attiva controli quarantena  Disconnetti se il server non presenta TLV di cryptobinding  OK Annulia

La seguente configurazione è necessaria solo per PC **NON nel dominio unitn** (per PC nel dominio unitn saltare questo passaggio)

\* Cliccare sul tasto configura, quindi dalla finestra Proprietà EAP MASCHAPv2 che appare deselezionare la voce *Utilizza automaticamente....* come di seguito illustrato:

Proprietà EAP MSCHAP	12 💌
Per la connessione:	
Distribution of the second sec	mente il nome utente, la ponibile, il dominio di accesso
ОК	Annulla

\* Dopo aver collegato il cavo di rete, alla richiesta, inserire le proprie credenziali unitn



Nel caso in cui le credenziali non vengano riconosciute si verrà ridirezionati automaticamente ad una autenticazione Captive Portal.

## Troubleshooting

Forzare la riautenticazione:

• Deselezionare il flag Memorizza credenziali per... quindi deattivare/riattivare la scheda di rete:

Proprietà - Connessione alla rete locale (LAN)
Rete Autenticazione Condivisione
Selezionare questa opzione per fomire accesso di rete autenticato a questa scheda Ethemet. ✓ Abilita autenticazione IEEE 802.1X Scogliere un metodo di autenticazione di rete: Microsoft: PEAP (Protected EAF  _ Impostazioni Memorizza informazioni utente per connessioni auccessive a questa rete
OK Annula

×

From: https://wiki.unitn.it/ - Wiki UniTn

Permanent link: https://wiki.unitn.it/pub:win-vista-sp2?rev=1336655971

Last update: 2012/05/10 13:19