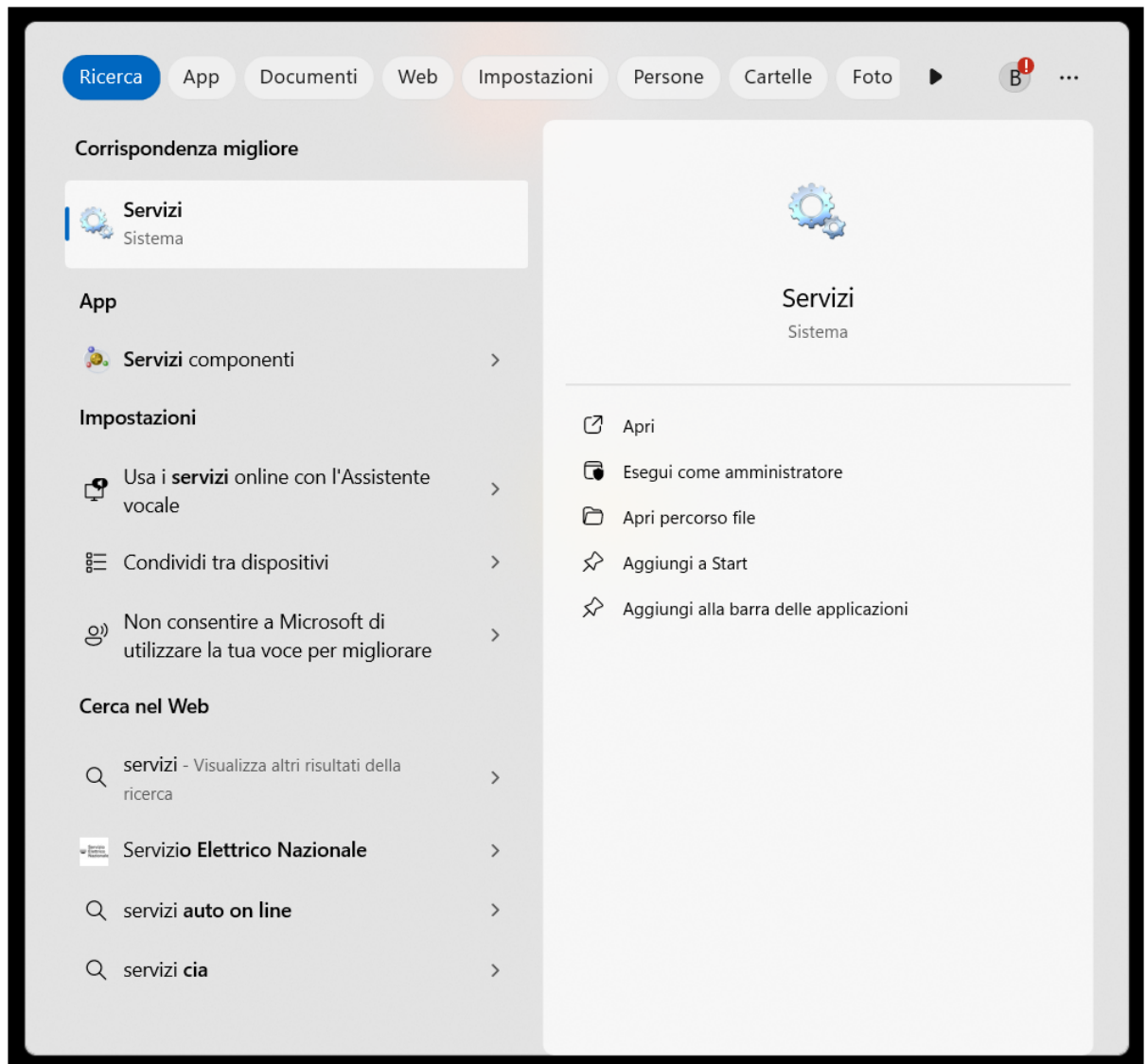
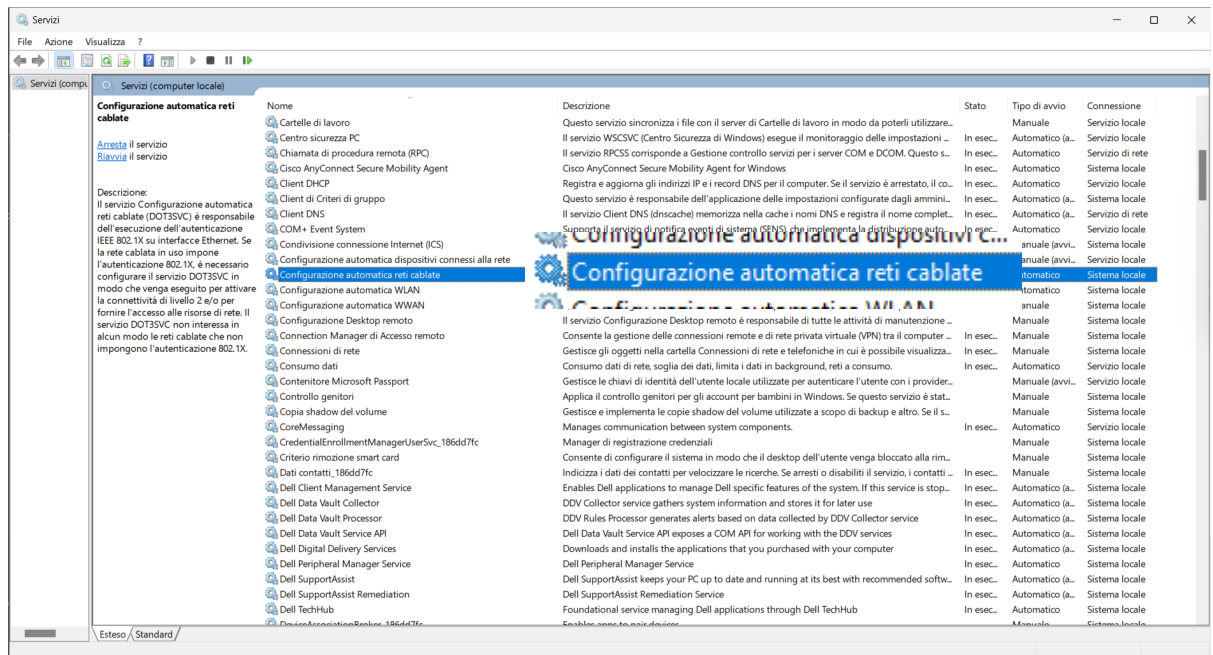


Linee Guida per l'autenticazione alla rete cablata da Windows

1. Apri l'applicazione "**Servizi**";



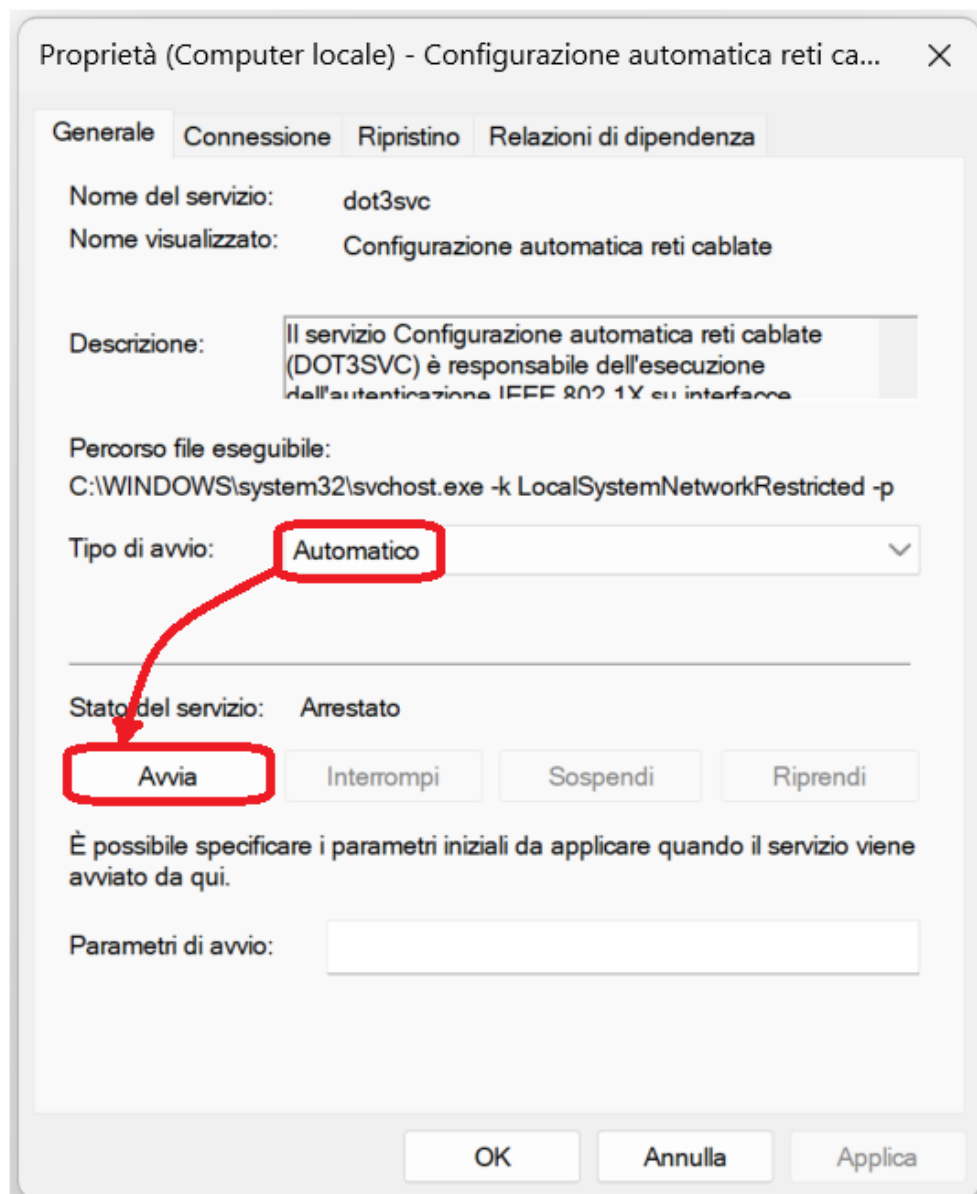
2. Cerca il servizio "**Configurazione automatica reti cablate**" e fai doppio click;



PS. Potrebbe essere più facile trovare il servizio se li ordini per Nome. Per fare questo clicca sull'intestazione della colonna del Nome.

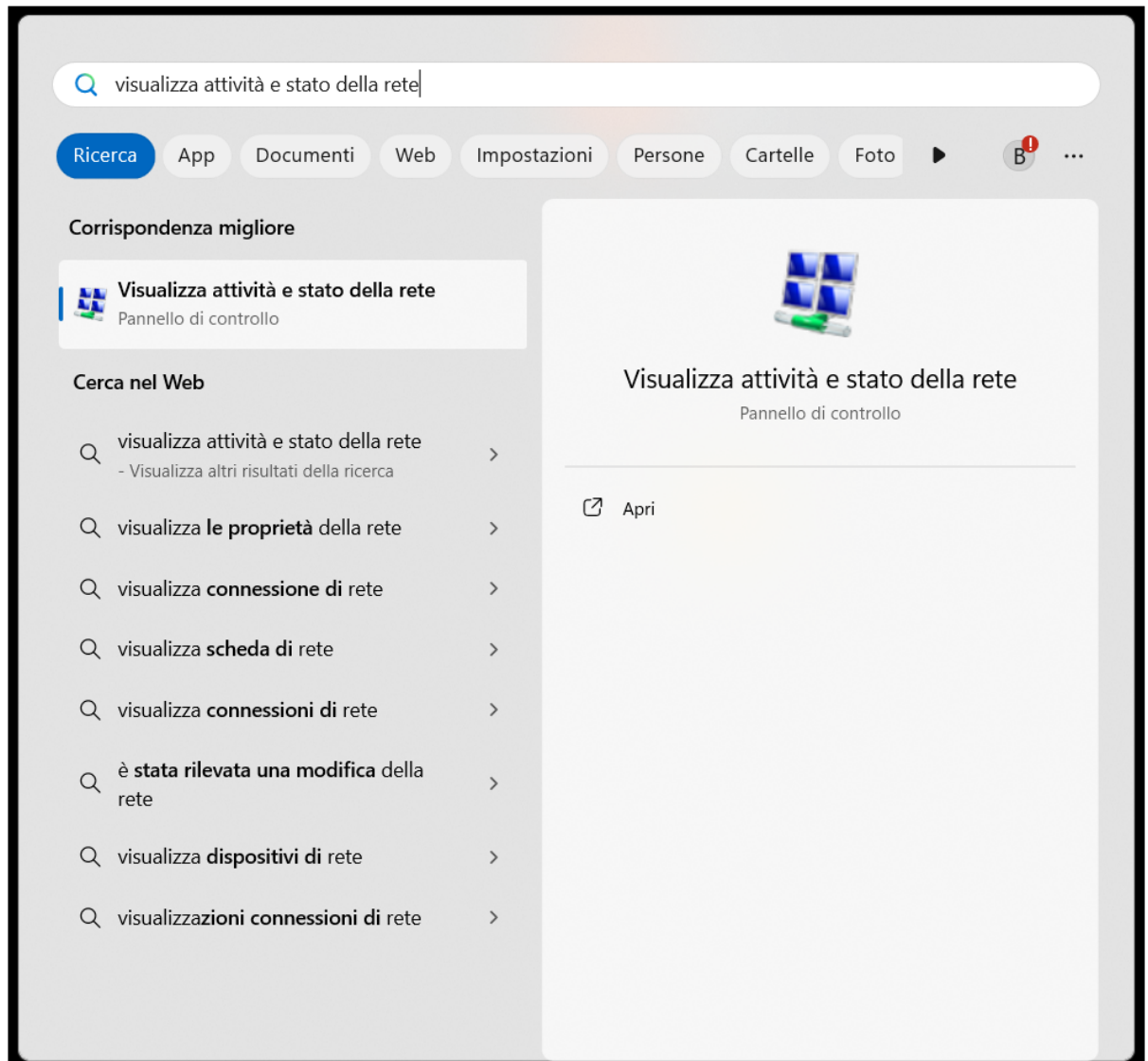
Nel caso il vostro pc è in lingua Inglese, dovete fare doppio click sulla voce "**Wired AutoConfig service**"

3. Nella voce "*Tipo di avvio*", selezionare "*Automatico*" e poi **Avvia**

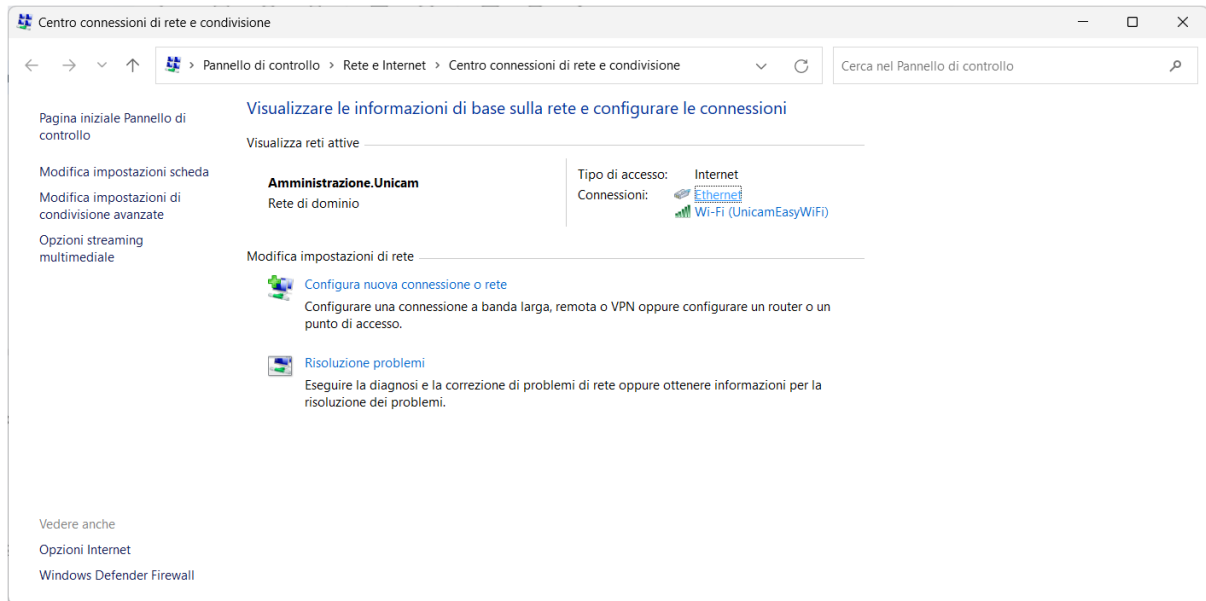


4. Successivamente clicca sul pulsante "*Applica*" in basso a destra e poi "OK";

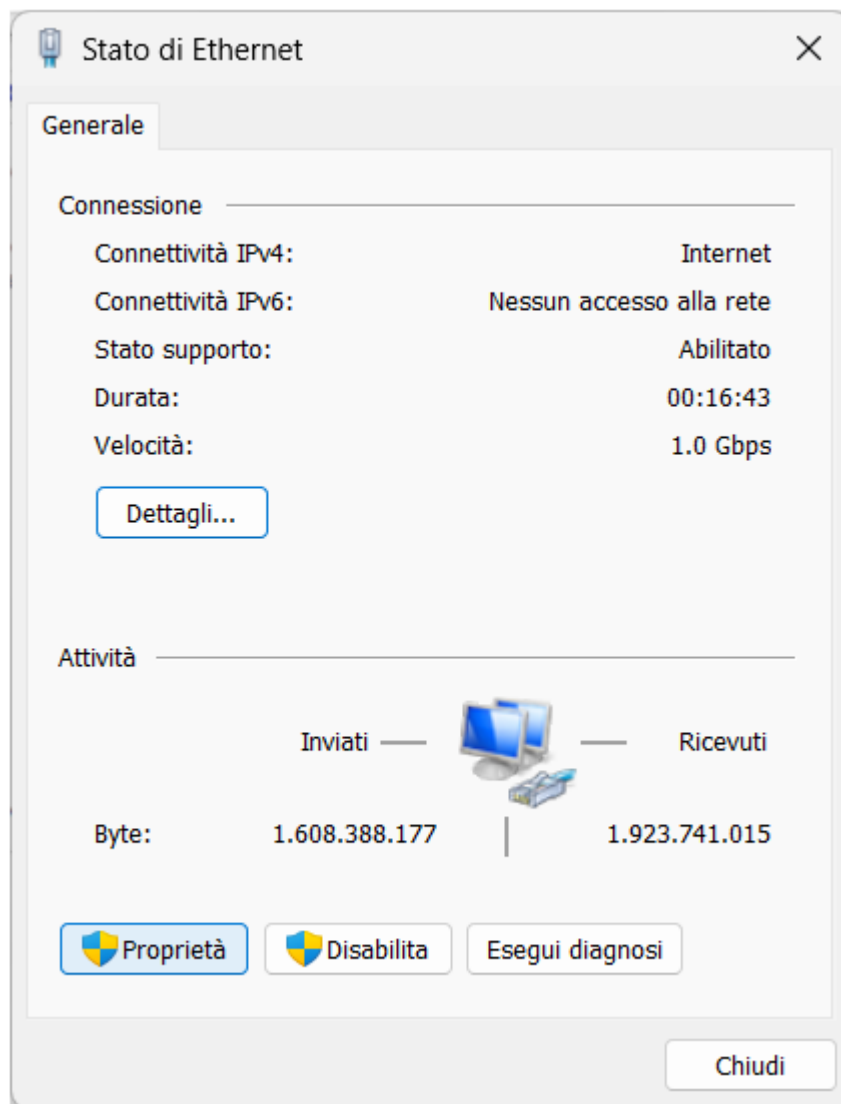
5. Ora apri "**Visualizza attività e stato della rete**";



6. Seleziona "*Ethernet*" tra le reti attive;



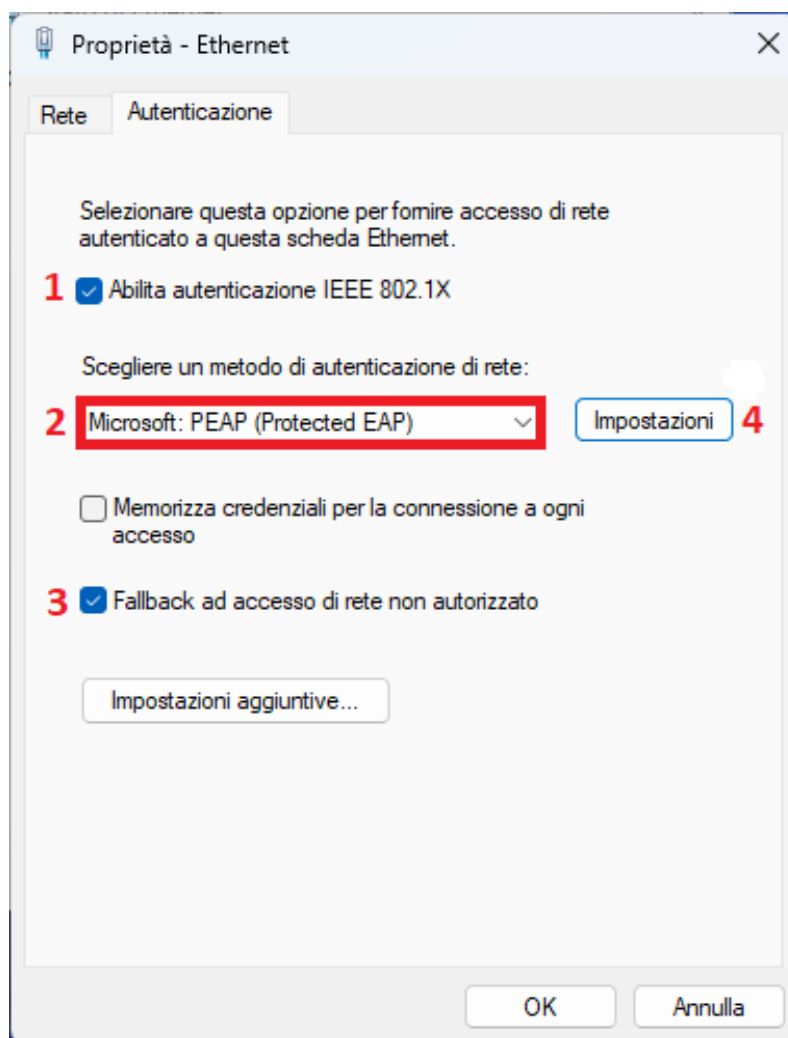
7. Clicca sul pulsante “*Proprietà*”;



8. Clicca sulla Tab “**Autenticazione**”.

Segui le seguenti istruzioni:

1. Seleziona la spunta “*Abilita autenticazione IEEE 802.1X*”;
2. Nel menù a tendina del metodo di autenticazione rete seleziona “*Microsoft: PEAP (Protected EAP)*”;
3. Seleziona la spunta “*Fallback ad accesso di rete non autorizzato*”
4. Clicca sul pulsante “**Impostazioni**” affianco al metodo di autenticazione;



P.S. la spunta “*Memorizza credenziali per la connessione a ogni accesso*”, serve a non richiedere l’inserimento delle credenziali ogni volta ci si connette alla rete cablata. Spuntatelo a vostra discrezione

9. Rimuovi la spunta su “*Verifica l’identità del server mediante convalida del certificato*”.

Seleziona dal menù a tendina in fondo il metodo di autenticazione “*Password protetta (EAP-MSCHAP v2)*”

Clicca OK

Proprietà PEAP

Per la connessione:

Rimuovi la spunta

☐ Verifica l'identità del server mediante convalida del certificato

☐ Connetti ai server seguenti (esempi: srv1;srv2;.*\,srv3\,com):

Autorità di certificazione radice attendibili:

- ☐ Class 3 Public Primary Certification Authority
- ☐ DigiCert Assured ID Root CA
- ☐ DigiCert Global Root CA
- ☐ DigiCert Global Root G2
- ☐ DigiCert Global Root G3
- ☐ DigiCert High Assurance EV Root CA
- ☐ DigiCert Trusted Root G4

Notifiche prima della connessione:

Informa l'utente se l'identità del server non può essere verificata

Selezionare il metodo di autenticazione:

Password protetta (EAP-MSCHAP v2)

Configura...

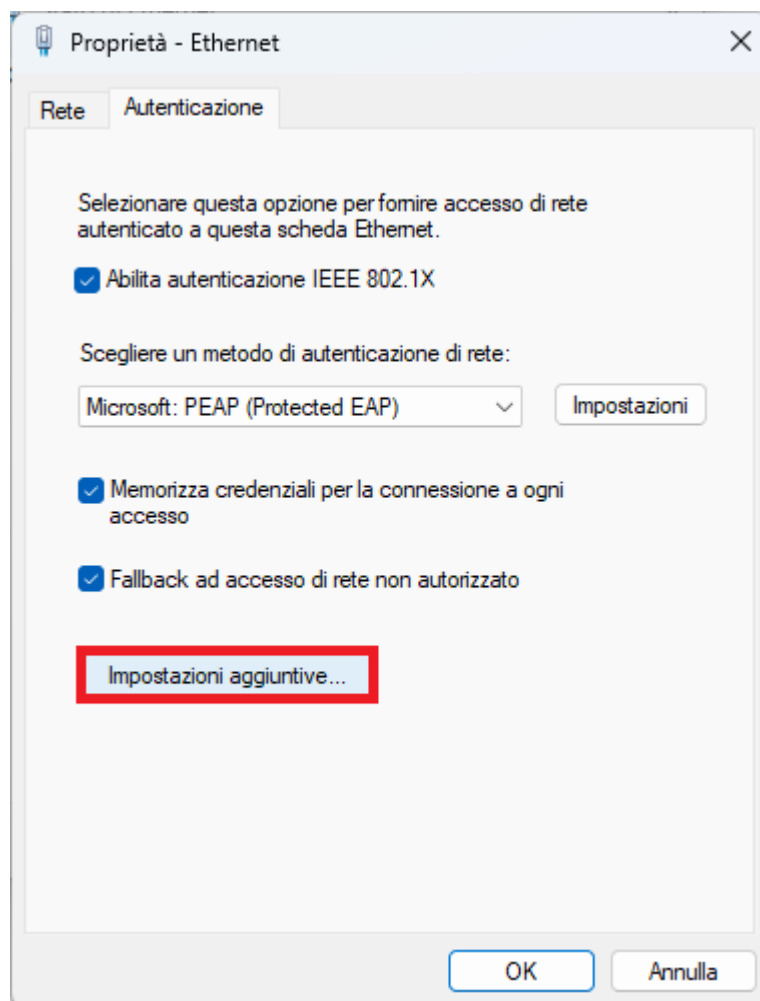
☒ Abilita riconnessione rapida

☐ Disconnetti se il server non presenta TLV di cryptobinding

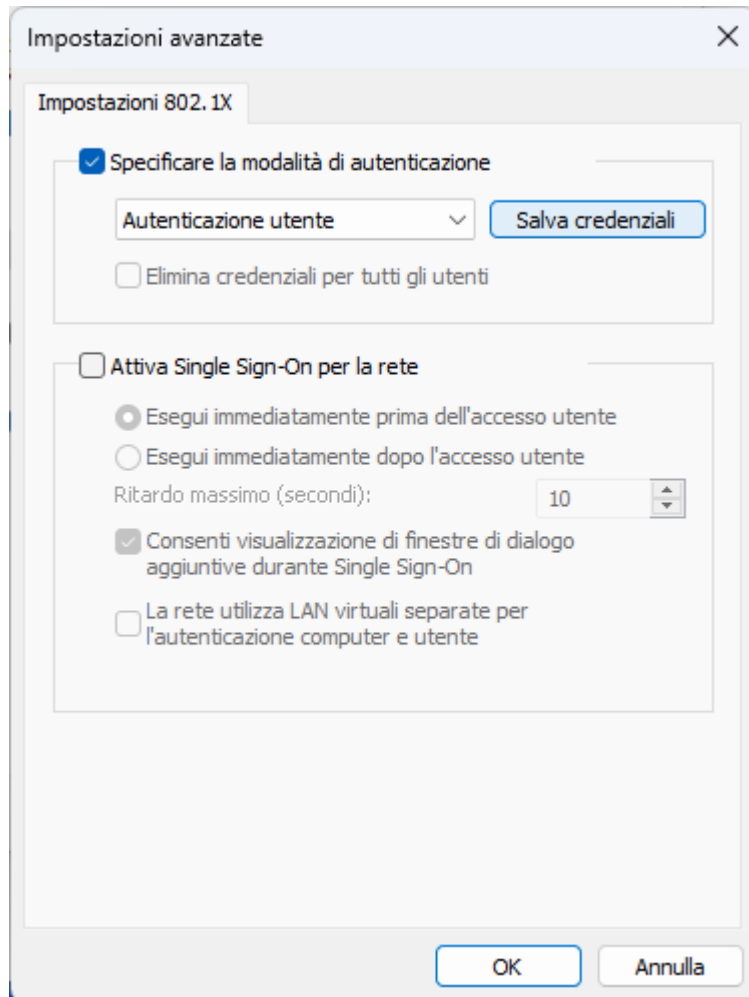
☐ Consenti privacy identità

OK Annulla

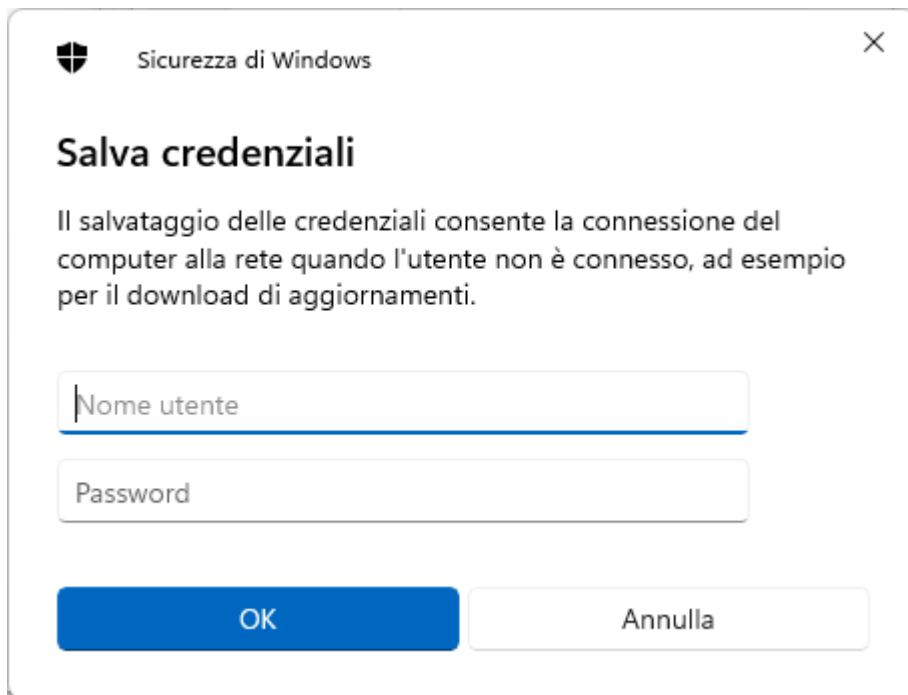
10. Clicca il pulsante “***Impostazioni aggiuntive...***” in basso



11. Metti la spunta su “*Specificare la modalità di autenticazione*” e scegli “*Autenticazione utente*” dal menù a tendina. Clicca il pulsante “**Salva credenziali**”



12. All'apertura della seguente finestra di accesso, inserisci le tue credenziali di Ateneo.



The image shows a Windows Security dialog box titled "Salva credenziali" (Save credentials). The window has a title bar with the Windows Security logo and the text "Sicurezza di Windows". The main text reads: "Il salvataggio delle credenziali consente la connessione del computer alla rete quando l'utente non è connesso, ad esempio per il download di aggiornamenti." Below this text are two input fields: "Nome utente" (Username) and "Password". At the bottom, there are two buttons: "OK" (highlighted in blue) and "Annulla" (Cancel).

13. Nel caso appare una finestra di confermare la connessione alla rete Ethernet dell'organizzazione ovviamente dovete confermare.

Queste impostazioni non inficiano il collegamento alle normali reti cablate senza autenticazione, quindi una volta effettuate queste abilitazioni nella vostra macchina, potrete collegarvi sia a reti cablate con o senza autenticazione, lasciando l'esperienza d'uso assolutamente inalterata.

Nel caso ci sia stato un qualche problema durante il processo di autenticazione, si può procedere a scollegare il cavo di rete dal computer e renservirlo così da poter effettuare nuovamente l'autenticazione di rete.