



# Configurazione reti cablate autenticate Windows 11

In questo documento sarà esposta la procedura di installazione del certificato per la verifica dell'attendibilità della rete cablata per il sistema operativo Windows 11.

# Fase 1: Download del certificato

- Prima di procedere all'installazione del certificato è necessario scaricare il certificato dal sito web ufficiale dell'Ateneo.
- Dal momento che il sito potrebbe cambiare, in questo tutorial viene esposto generalmente dove si trova.

---

## CERTIFICATO

 [Certificato Windows - unibs-ca.der](#)



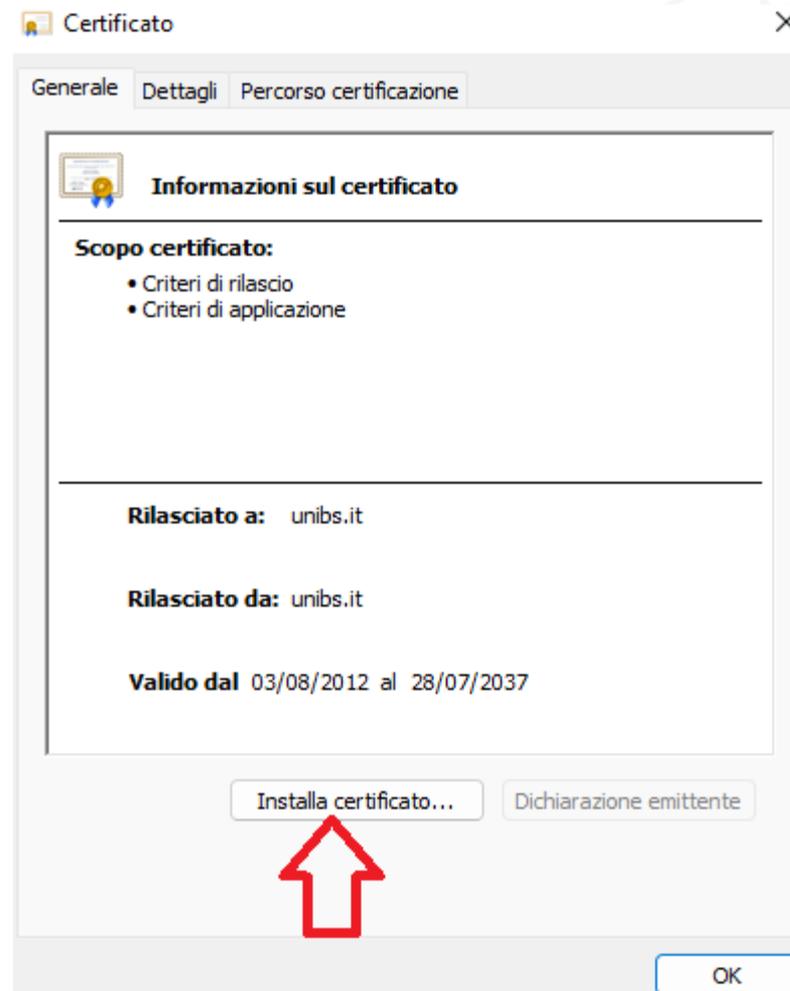
 [Certificato Mac-Android - unibs-ca.crt](#)

# Fase 1: Download del certificato

- Dopo aver scaricato il certificato si può procedere alla sua decompressione usando lo strumento messo a disposizione dalla Microsoft.
- Generalmente cliccando sul file zip dovrebbe procedere automaticamente alla decompressione del file zip.
- Dopo aver completato la procedura dovrebbe apparire il file **unibs-ca.der**

# Fase 2: Installazione del certificato

- Per installare il certificato è necessario fare doppio click sul file.
- Apparirà la schermata visibile sulla destra.
- Per installare il certificato è necessario cliccare sul pulsante Installa certificato



# Fase 2: Installazione del certificato

- Si aprirà una nuova schermata dove bisogna selezionare Computer locale
- Completata questa procedura cliccare su Avanti.
- Se viene chiesto «Consentire a questa app di apportare modifiche», cliccare Sì.

← Importazione guidata certificati

## Importazione guidata certificati

Questa procedura guidata permette di copiare certificati, elenchi di scopi consentiti ed elenchi di revoche di certificati dal disco all'archivio certificati.

Un certificato rilasciato da un'Autorità di certificazione conferma l'identità dell'utente e contiene informazioni utilizzate per proteggere i dati o per stabilire connessioni di rete sicure. L'archivio certificati è l'area del sistema dove i certificati sono archiviati.

Percorso archivio

Utente corrente

Computer locale



Per continuare, fare clic su Avanti.

# Fase 2: Installazione del certificato

- Nella schermata seguente cliccare su «Colloca tutti i certificati nel seguente archivio»
- Successivamente cliccare sul pulsante Sfoglia.

← Importazione guidata certificati ×

**Archivio certificati**  
Gli archivi certificati sono le aree del sistema dove i certificati sono archiviati.

---

L'archivio certificati può essere selezionato automaticamente dal sistema oppure è possibile specificare il percorso per il certificato.

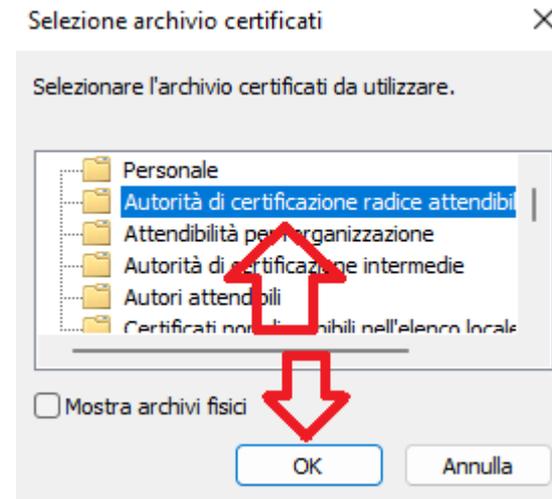
Seleziona automaticamente l'archivio certificati secondo il tipo di certificato

Colloca tutti i certificati nel seguente archivio

Archivio certificati:

# Fase 2: Installazione del certificato

- Come mostrato nella schermata alla destra, è necessario selezionare l'opzione «Autorità di certificazione radice attendibile»
- Per completare la procedura cliccare su OK.



# Fase 2: Installazione del certificato

- Se l'operazione è stata eseguita con successo dovrebbe apparire una schermata del genere.

←  Importazione guidata certificati

## Archivio certificati

Gli archivi certificati sono le aree del sistema dove i certificati sono archiviati.

L'archivio certificati può essere selezionato automaticamente dal sistema oppure è possibile specificare il percorso per il certificato.

- Seleziona automaticamente l'archivio certificati secondo il tipo di certificato
- Colloca tutti i certificati nel seguente archivio

Archivio certificati:

Autorità di certificazione radice attendibili

Sfoglia...

# Fase 2: Installazione del certificato

- Per completare il processo di installazione è necessario cliccare su Fine

-  Importazione guidata certificati

## Completamento dell'Importazione guidata certificati

Scegliendo Fine, il certificato verrà importato.

Impostazioni selezionate:

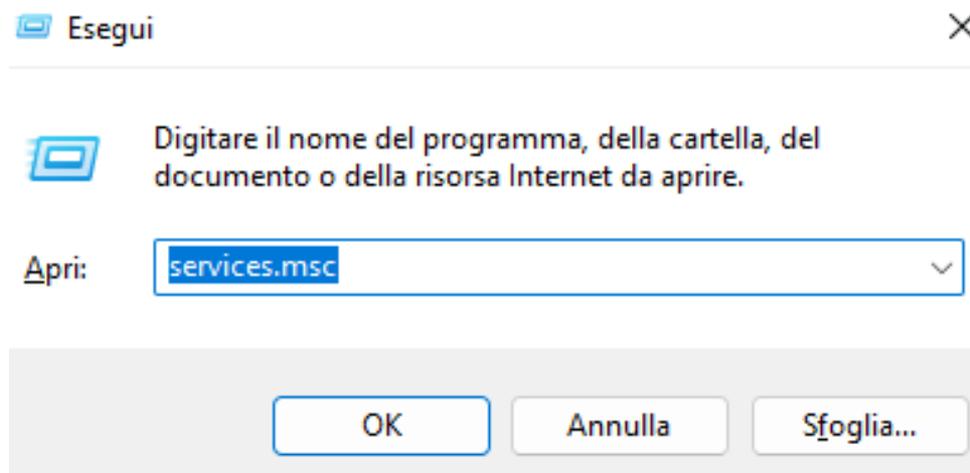
Archivio certificati selezionato dall'utente	Autorità di certificazione radice attendibili
Contenuto	Certificato

Fine

Annulla

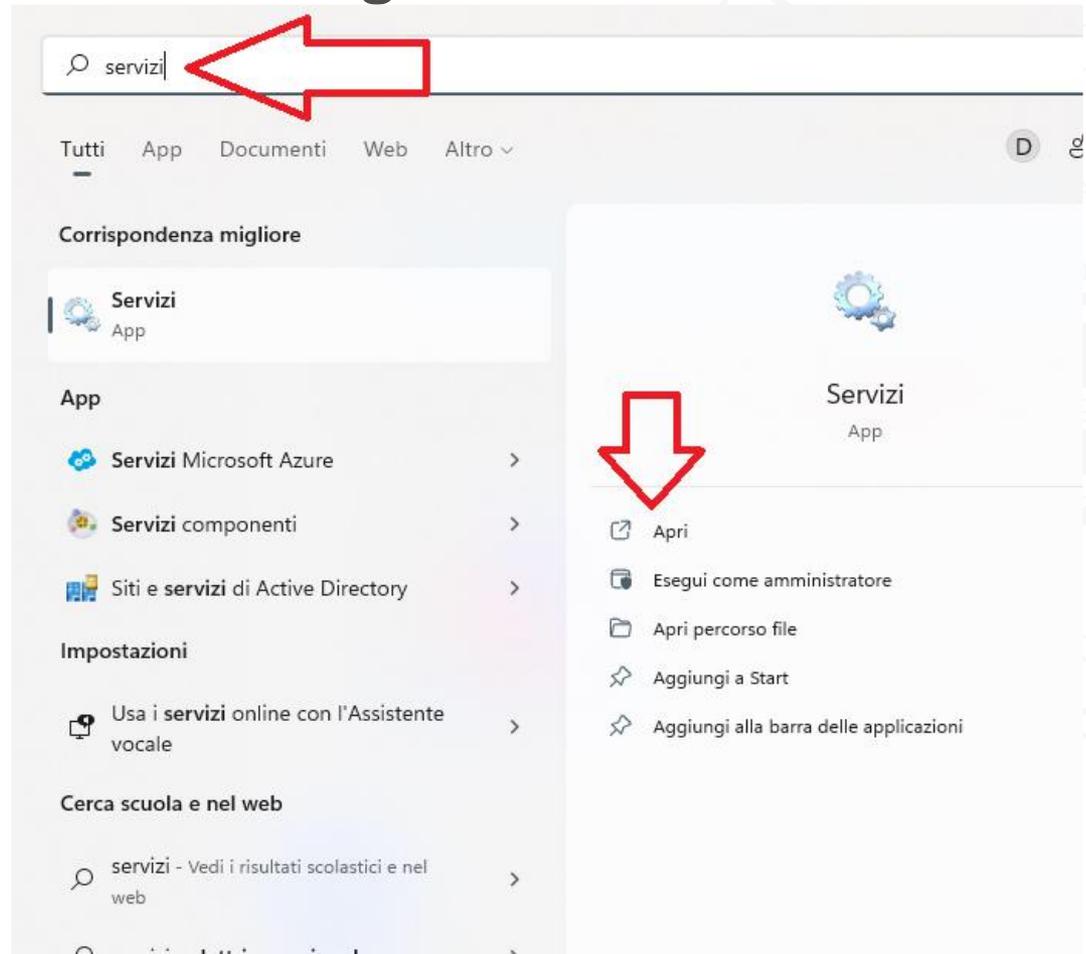
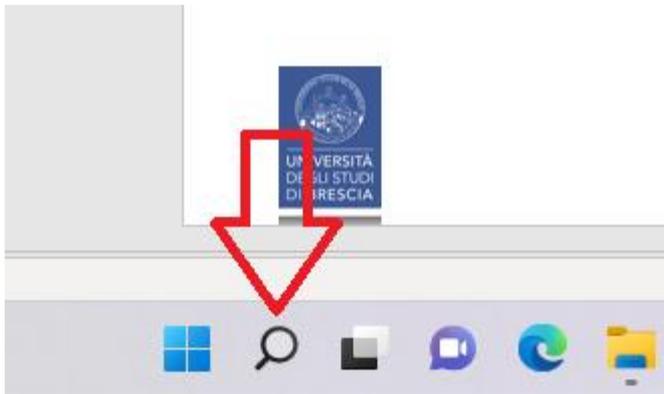
# Fase 3: Attivazione del servizio

- Per poter usufruire del certificato è necessario abilitare il servizio «Configurazione automatica reti cablate».
- Da Windows 11 basta premere la combinazione di tasti WIN(Bandiera di Windows) + R e poi scrivere «services.msc», infine, premere OK



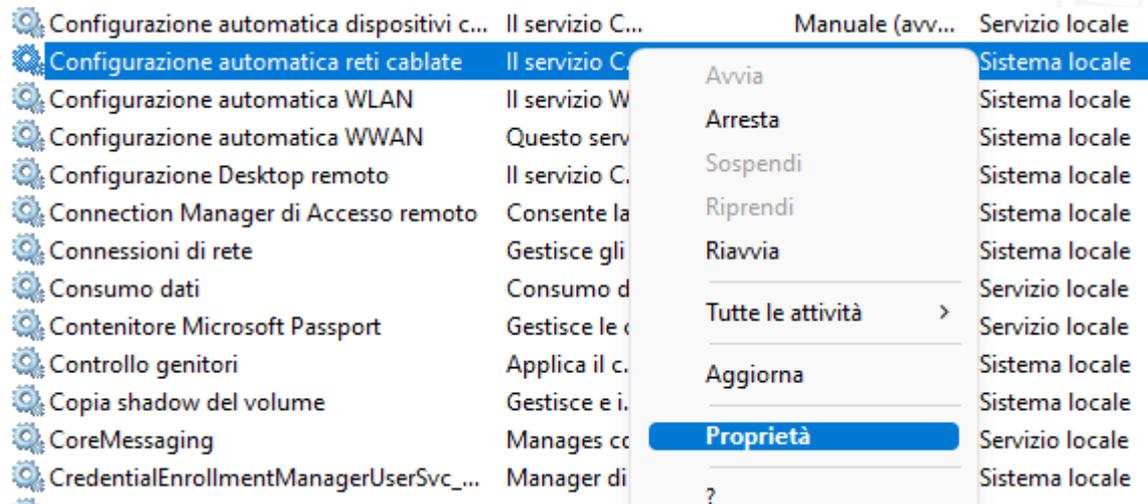
# Fase 3: Attivazione del servizio

- Alternativamente basta cercare «Servizi» cliccando sull'icona a forma di lente di ingrandimento, come mostrato nella seguente immagine.



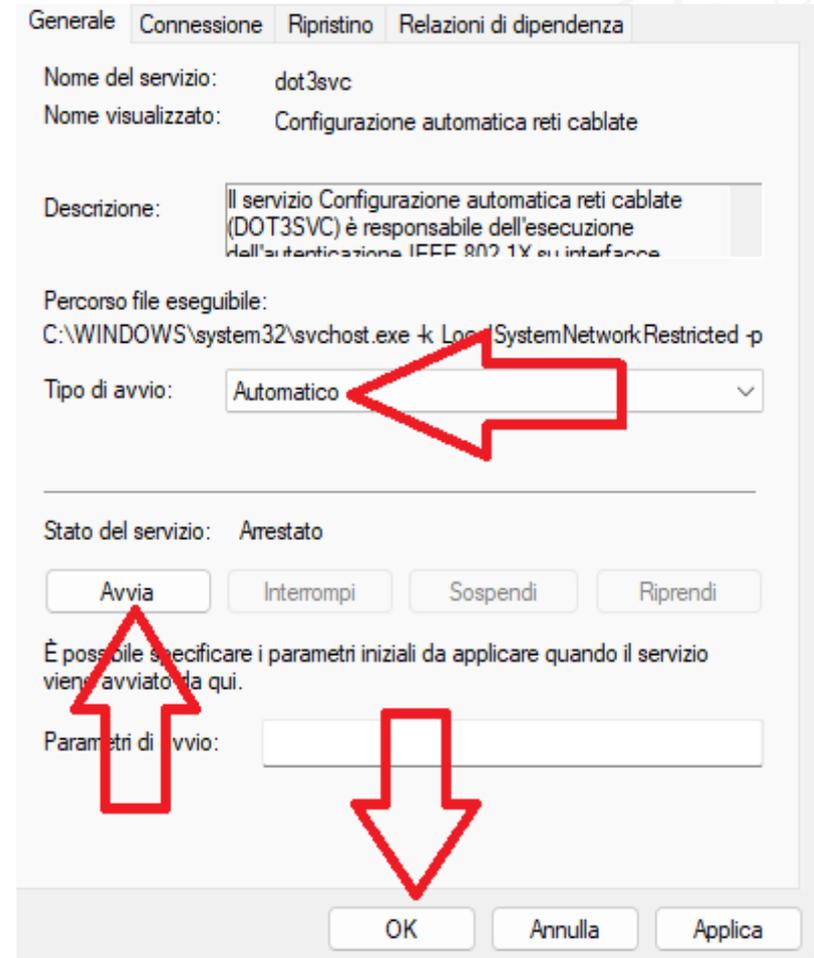
# Fase 3: Attivazione del servizio

- Dopo aver aperto la sezione Servizi, cercare all'interno della lista il servizio denominato «Configurazione automatica reti cablate».
- Fare click destro su di esso e selezionare Proprietà



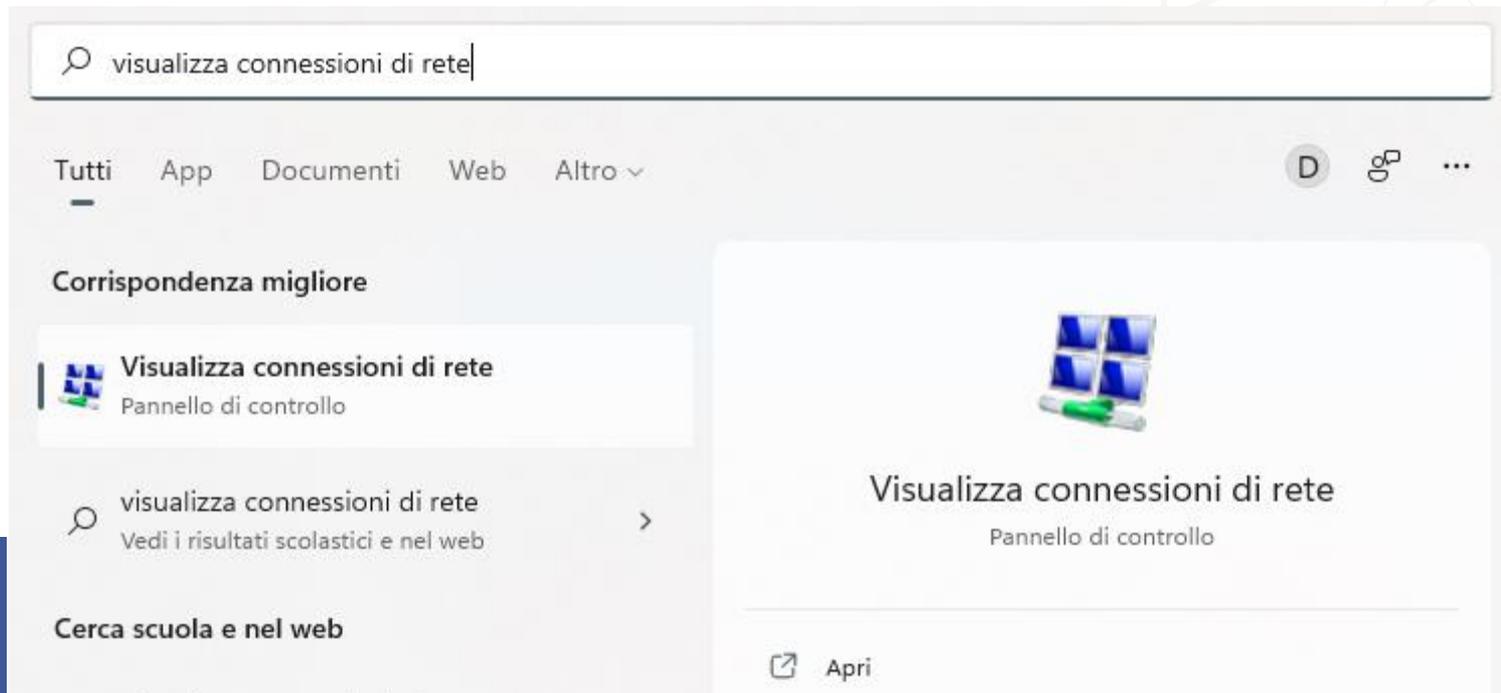
# Fase 3: Attivazione del servizio

- Dopo aver selezionato proprietà come spiegato nella slide precedente si aprirà una nuova finestra.
- In questa finestra bisogna impostare «Tipo di avvio» in Automatico.
- Successivamente cliccare su «Avvia» e infine premere il pulsante OK.



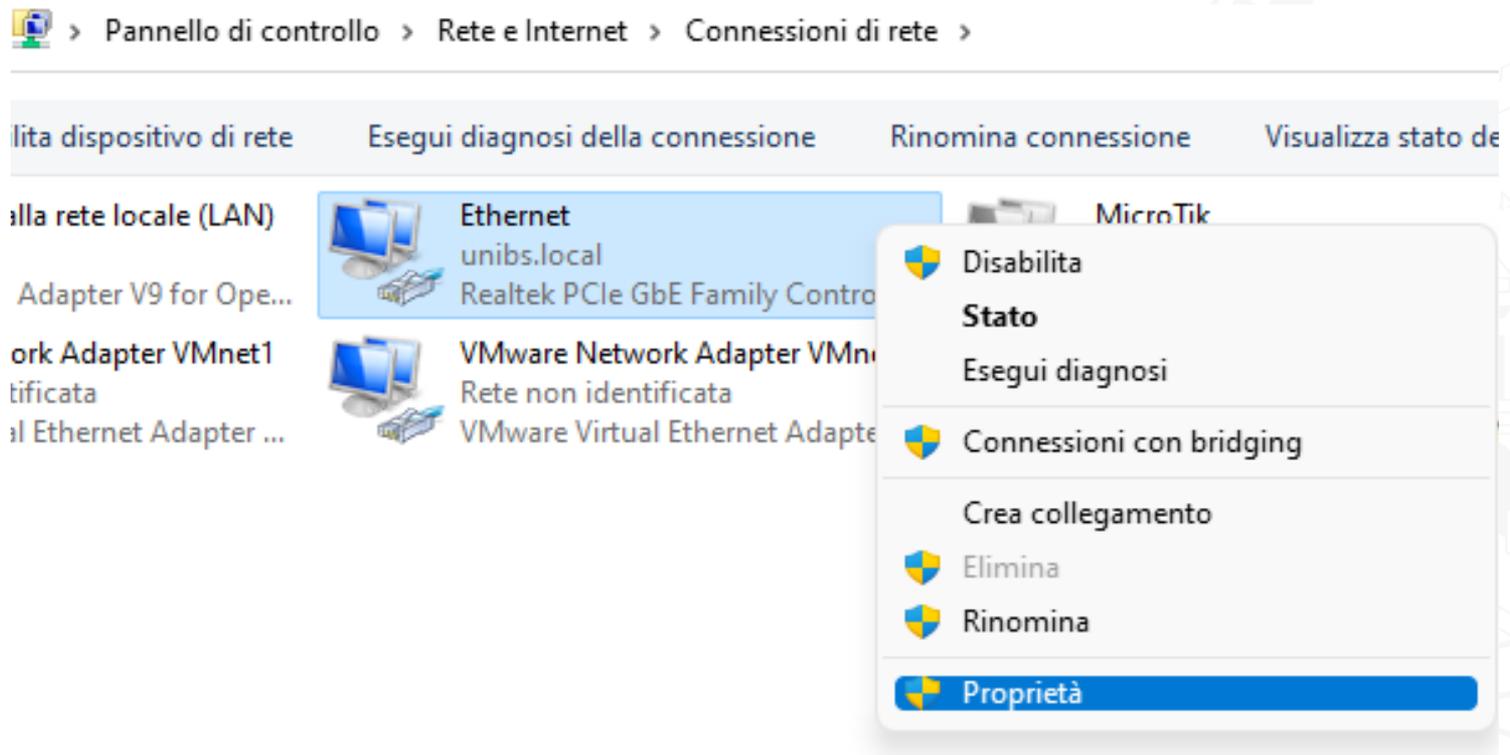
# Fase 4: Attivazione del certificato

- Adesso è tutto pronto per attivare la verifica del certificato sulla rete cablata.
- E' necessario cliccare sulla lente di ingrandimento come mostrato nell'immagine e cercare «Visualizza connessioni di rete»



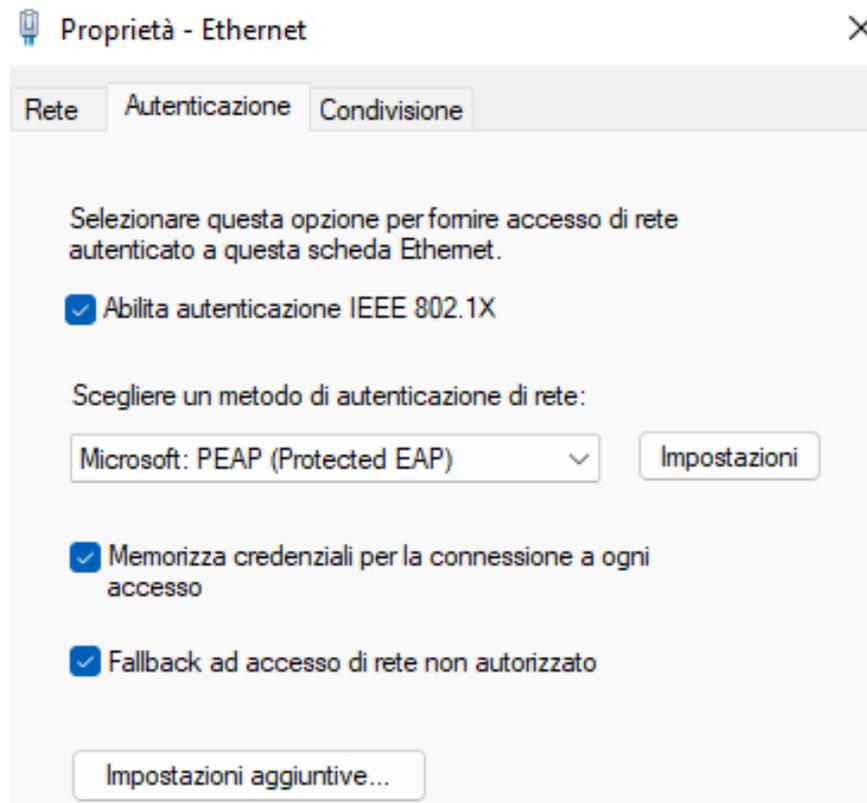
# Fase 4: Attivazione del certificato

- Selezionare la rete «Ethernet», cliccare con il tasto destro e selezionare proprietà.



# Fase 4: Attivazione del certificato

- Nella sezione proprietà accedere alla sezione «Autenticazione».
- Questa sezione sarà visibile solo se sono stati completati i passi precedenti.
- Assicurarsi che le impostazioni siano equivalenti a quelle visibili in figura sulla destra.
- Cliccare su «[Impostazioni](#)»



# Fase 4: Attivazione del certificato

- Dopo aver cliccato su Impostazioni apparirà la seguente schermata.
- Selezionare unibs.it dalla lista come mostrato in immagine.

Per la connessione:

Verifica l'identità del server mediante convalida del certificato

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

Autorità di certificazione radice attendibili:

- Symantec Enterprise Mobile Root for Microsoft
- T-TeleSec GlobalRoot Class 2
- unibs.it
- USERTrust RSA Certification Authority
- Veeam Backup Server Certificate
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G5

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...](#)

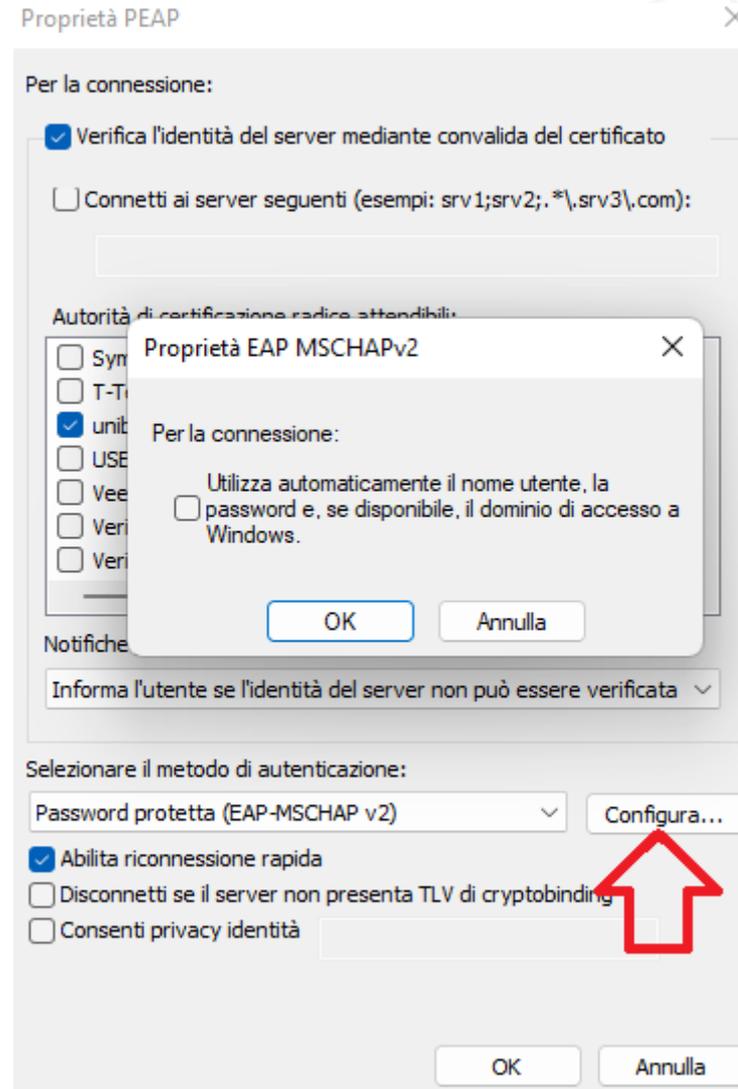
Abilita riconnessione rapida

Disconnetti se il server non presenta TLV di cryptobinding

Consenti privacy identità

# Fase 4: Attivazione del certificato

- Assicurarsi, cliccando sul tasto «Configura» che l'opzione «utilizza automaticamente il nome utente, la password e, se disponibile, il dominio di accesso a Windows sia disabilitato come da immagine.
- Infine, cliccare su OK.



# Fase 4: Attivazione del certificato

- Completati tutti i passi precedenti cliccare su OK.

Proprietà PEAP

Per la connessione:

Verifica l'identità del server mediante convalida del certificato

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

Autorità di certificazione radice attendibili:

- Symantec Enterprise Mobile Root for Microsoft
- T-TeleSec GlobalRoot Class 2
- unibs.it
- USERTrust RSA Certification Authority
- Veeam Backup Server Certificate
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G5

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

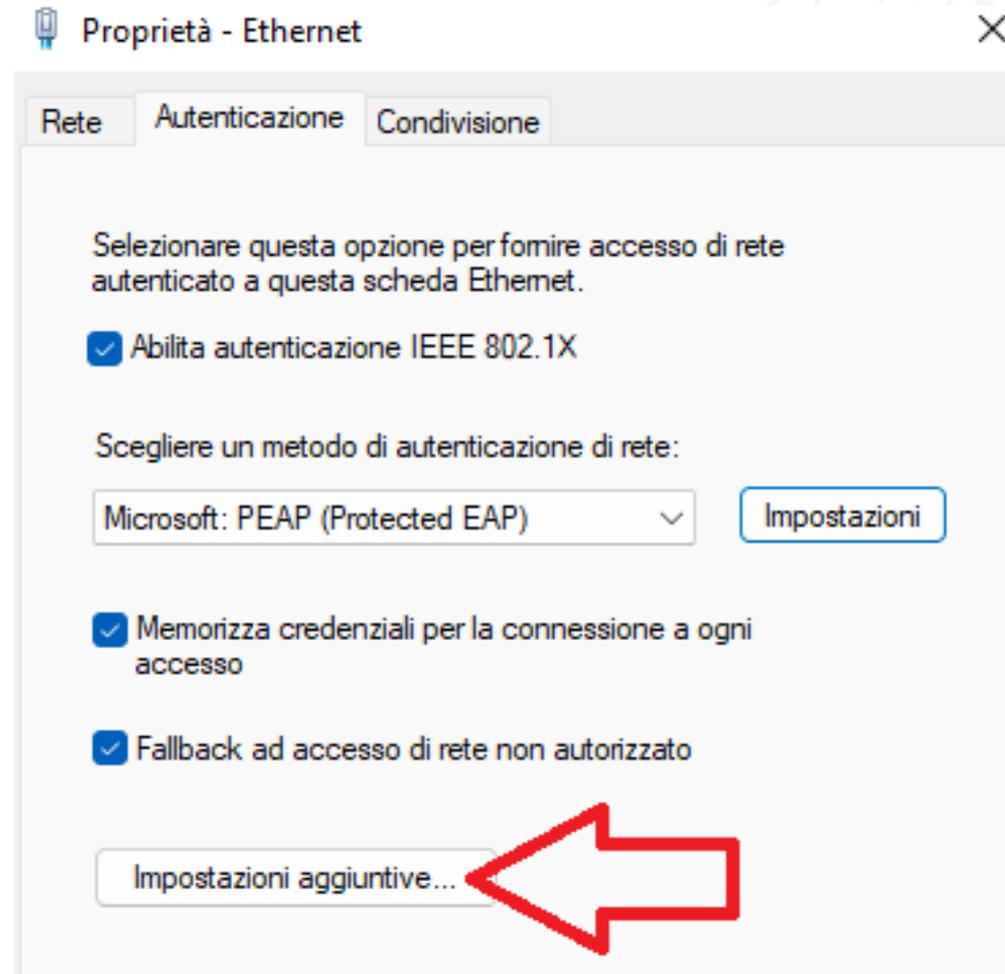
Consenti privacy identità



OK Annulla

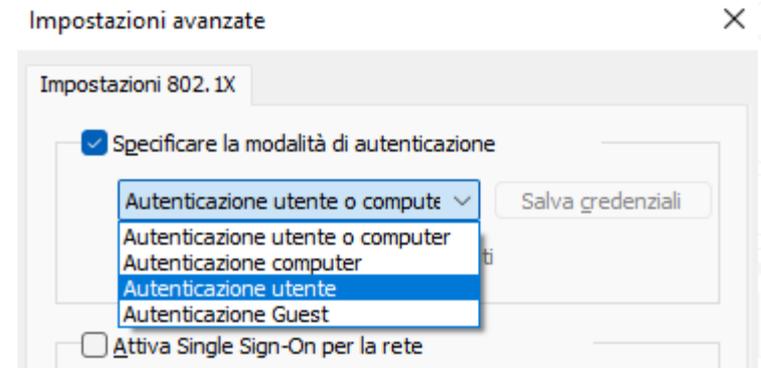
# Fase 4: Attivazione del certificato

- Sarete riportati nella schermata iniziale.
- Cliccare su impostazioni aggiuntive



# Fase 4: Attivazione del certificato

- Selezionare «Specificare la modalità di autenticazione»
- Dal menù a tendina selezionare «Autenticazione utente».
- Cliccare OK



# Fase 4: Attivazione del certificato

- La configurazione è completata, nel caso in cui vengano richiesta le credenziali, inserire le proprie.