

## **INDICE:**

Creazione e impostazione Indirizzo ip statico - pag.2

Creazione degli Utenti e gestione permessi - pag.3

Creazione Gruppi e assegnazione - pag.5

Creazione dei file e permessi ai gruppi - pag.7

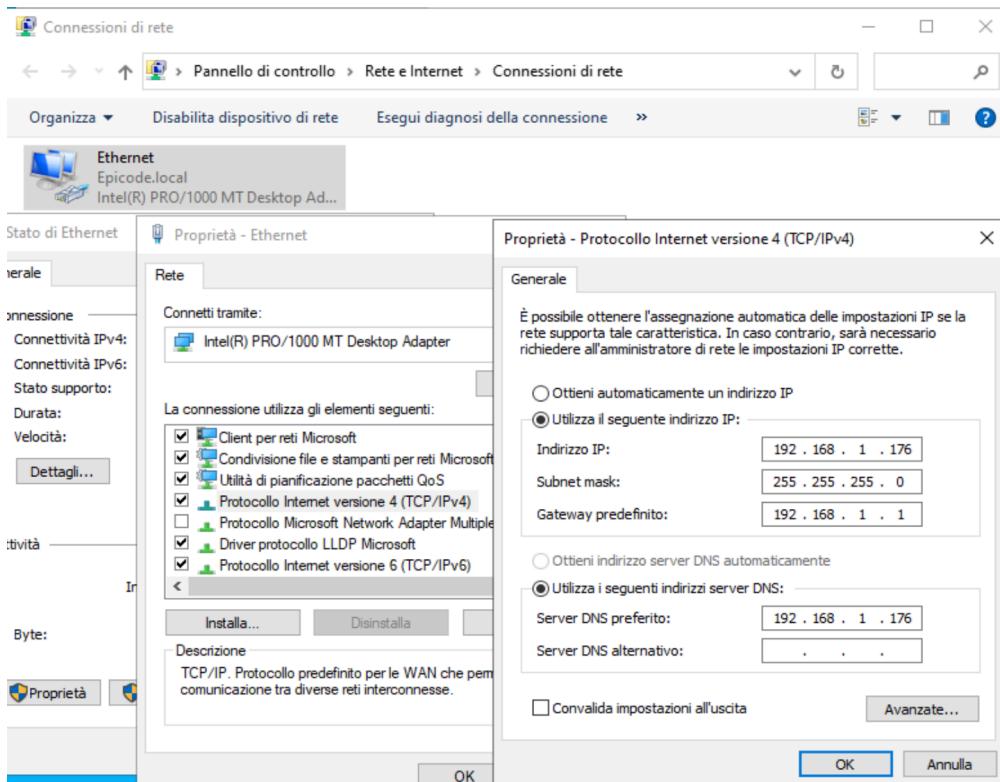
Cambio Password primo accesso - pag.9

Accesso da altro dispositivo collegato - pag.11

## Creazione di Utenti e Gruppi su Windows Server e collegamento tramite Domini.

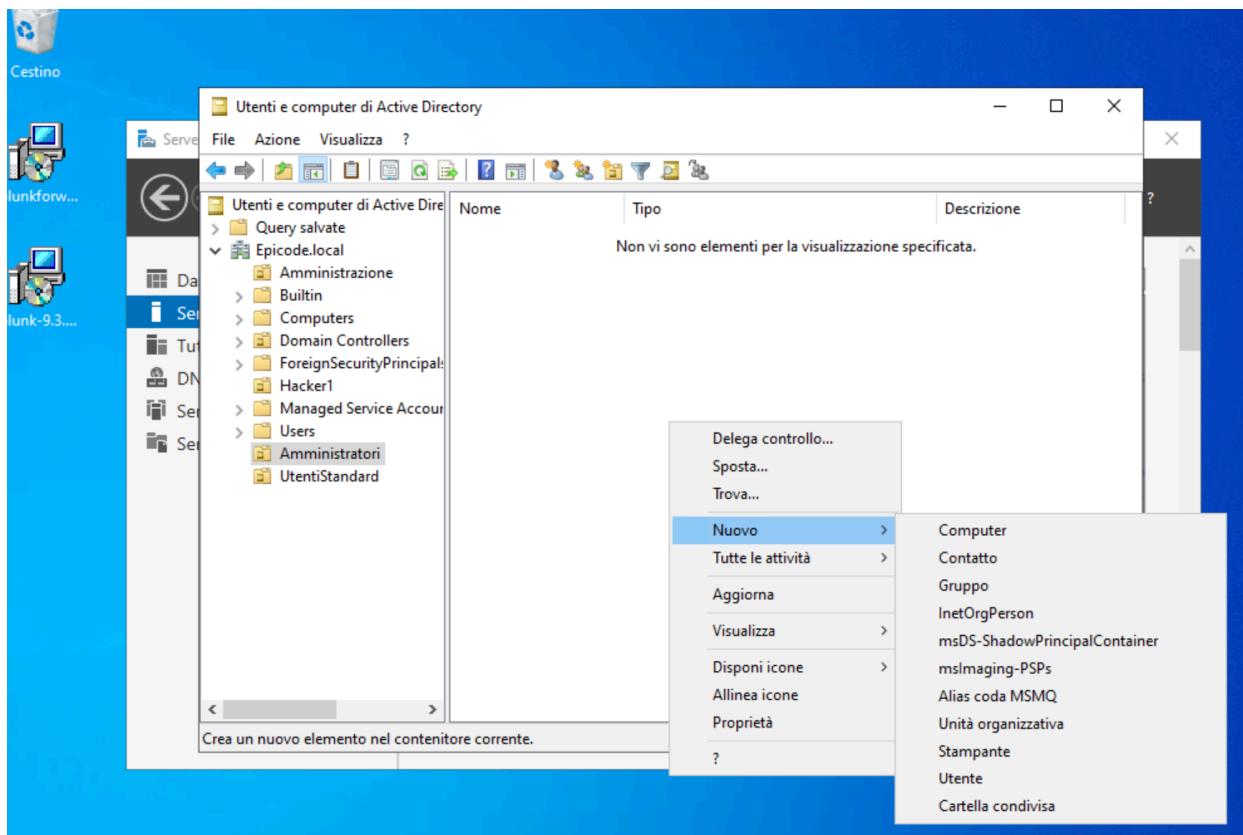
Impostiamo windows server in maniera che abbia il suo server personale attivo come in questo caso, quindi facciamo questi procedimenti:

- Click destro sulla connessione in basso a destra della home
- Apri impostazioni rete e internet
- Ethernet
- Proprietà
- Protocollo internet versione 4
- Impostiamo indirizzo ip statico, subnet mask, gateway e server DNS che sarà uguale al nostro indirizzo ip



Considerando un Server già creato andiamo a distribuire e creare permessi e utenti quindi andiamo su Server Manager e seguiamo i seguenti passaggi:

- Strumenti
- Utenti e computer di Active Directory
- Creiamo nel nostro server le cartelle di contenuto (i settori della nostra rete)
- Dentro poi ci metteremo Utenti e Gruppi che conterranno i singoli Utenti



### Creazione di un nuovo Utente:

- Inserisci dati e password

Nuovo oggetto Utente X

 Crea in: Epicode.local/CyberSecurity

---

Password:

Conferma password:

Cambiamento obbligatorio password all'accesso successivo  
 Cambiamento password non consentito  
 Nessuna scadenza password  
 Account disabilitato

---

[< Indietro](#) Avanti > [Annulla](#)

Nuovo oggetto Utente X

 Crea in: Epicode.local/CyberSecurity

---

Dopo aver scelto Fine, verrà creato il seguente oggetto:

Nome completo: Diego

Nome di accesso dell'utente: Diego@Eicode.local

Cambiamento obbligatorio password all'accesso successivo

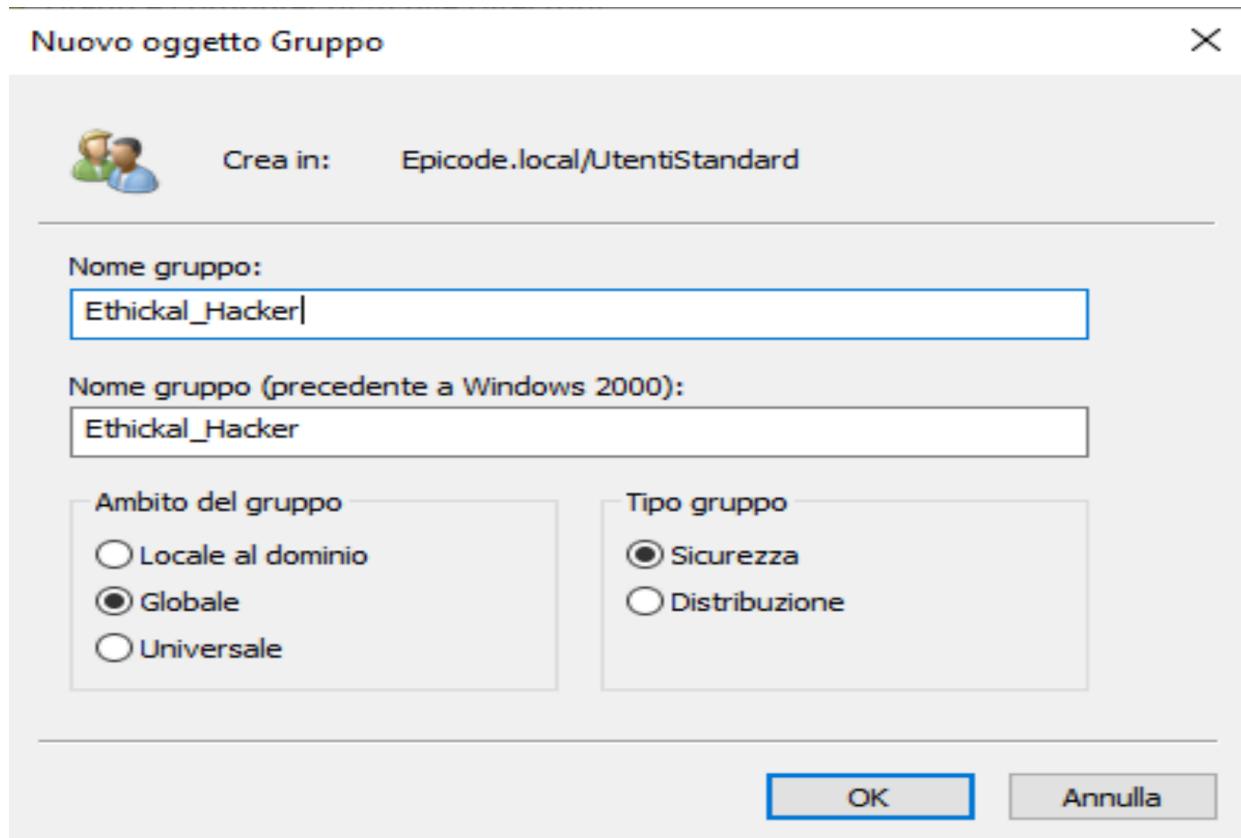
---

[< Indietro](#) Fine [Annulla](#)

### Creazione di un Gruppo e popolamento di esso:

- Crea Gruppo
- Metti il nome
- Clicca sul gruppo creato
- Aggiungi i nomi

- Applica



Utenti e computer di Active Directory

File    Azione    Visualizza    ?

Utenti e computer di Active Dire

- > Query salvate
- > Epicode.local
  - Amministrazione
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipal:
  - Hacker1
  - Managed Service Account
  - Users
    - CyberSecurity
    - UtentiStandard

Nome	Tipo	Descrizione
Beatrice	Utente	
Christian	Utente	
Diego	Utente	
Ethical_Hacker	Gruppo di sicurezza - Globale	
Mirko	Utente	
Sonia	Utente	

Proprietà - Ethical\_Hacker

Generale    Membri    Membro di    Gestito da

Membri:

Nome	Cartella di Servizi di dominio Active Directory
Beatrice	Epicode.local/CyberSecurity
Christian	Epicode.local/CyberSecurity
Diego	Epicode.local/CyberSecurity
Mirko	Epicode.local/CyberSecurity
Sonia	Epicode.local/CyberSecurity

The screenshot shows the Windows Active Directory Users and Computers snap-in. On the left, the navigation pane displays the structure of the Active Directory, including the domain 'Eicode.local' and its subfolders like 'Amministrazione', 'BuiltIn', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipal', 'Hacker1', 'Managed Service Account', 'Users', 'CyberSecurity', and 'UtentiStandard'. The main pane lists a security group named 'Assistenza\_Clienti' with the following details:

Nome	Tipo	Descrizione
Assistenza_Clienti	Gruppo di sicurezza - Globale	
Carlo Verdi	Utente	
Giorgio Bianchi	Utente	
Mario Rossi	Utente	

A modal dialog titled 'Proprietà - Assistenza\_Clienti' is open, showing the 'Membri' tab which lists the three users as members of the group. Below the list are 'Aggiungi...' and 'Rimuovi' buttons, and at the bottom are 'OK', 'Annulla', and 'Applica' buttons.

Creiamo una cartella che sarà pubblica “Email”

The screenshot shows a Windows File Explorer window with a blue theme. The left sidebar shows a 'File' icon and a list of quick access locations: Desktop, Download, Documenti, Immagini, Dati Sensibili, Questo PC, Unità CD (D:), and Rete. The main pane displays a folder named 'Email' containing two sub-folders: 'Email\_Sicure' and 'Email\_Sospette'. The file list shows the following details:

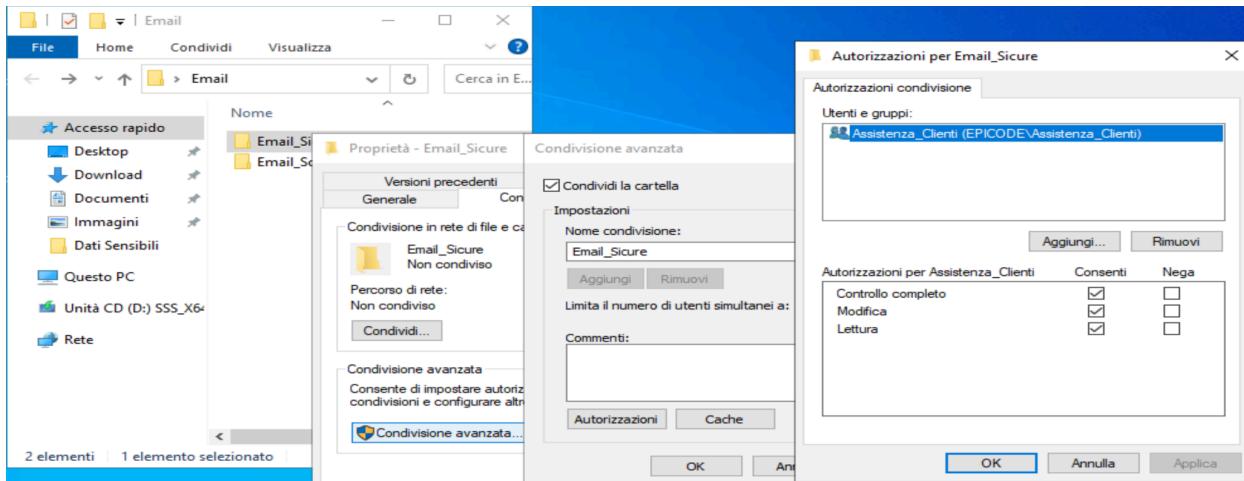
Nome	Ultima modifica	Tipo
Email_Sicure	06/12/2024 11:16	Cartella di file
Email_Sospette	06/12/2024 11:16	Cartella di file

At the bottom of the window, it says '2 elementi'.

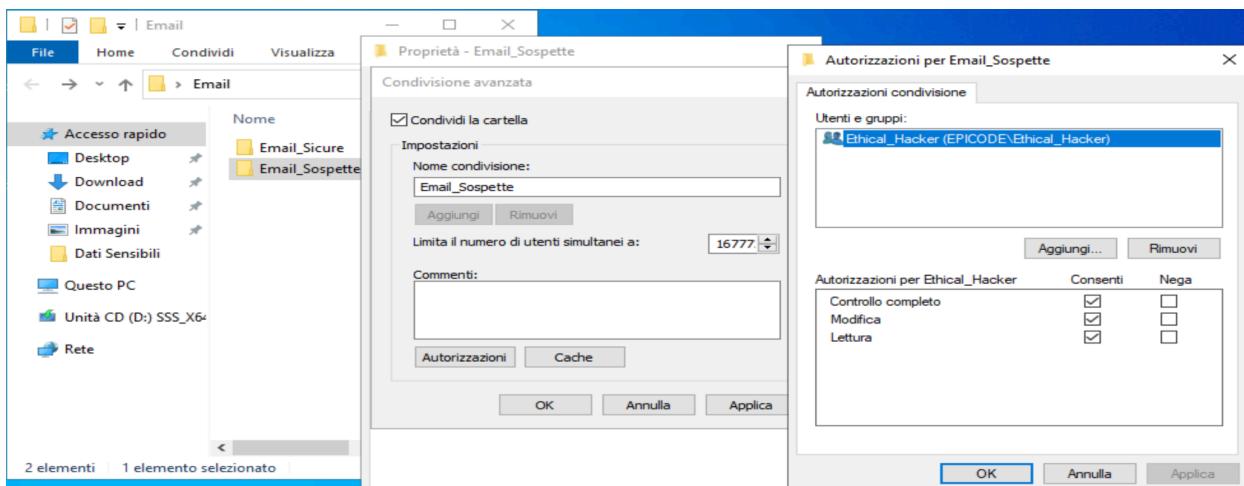
Creiamo 2 Cartelle che avranno permessi diversi

Impostiamo i permessi:

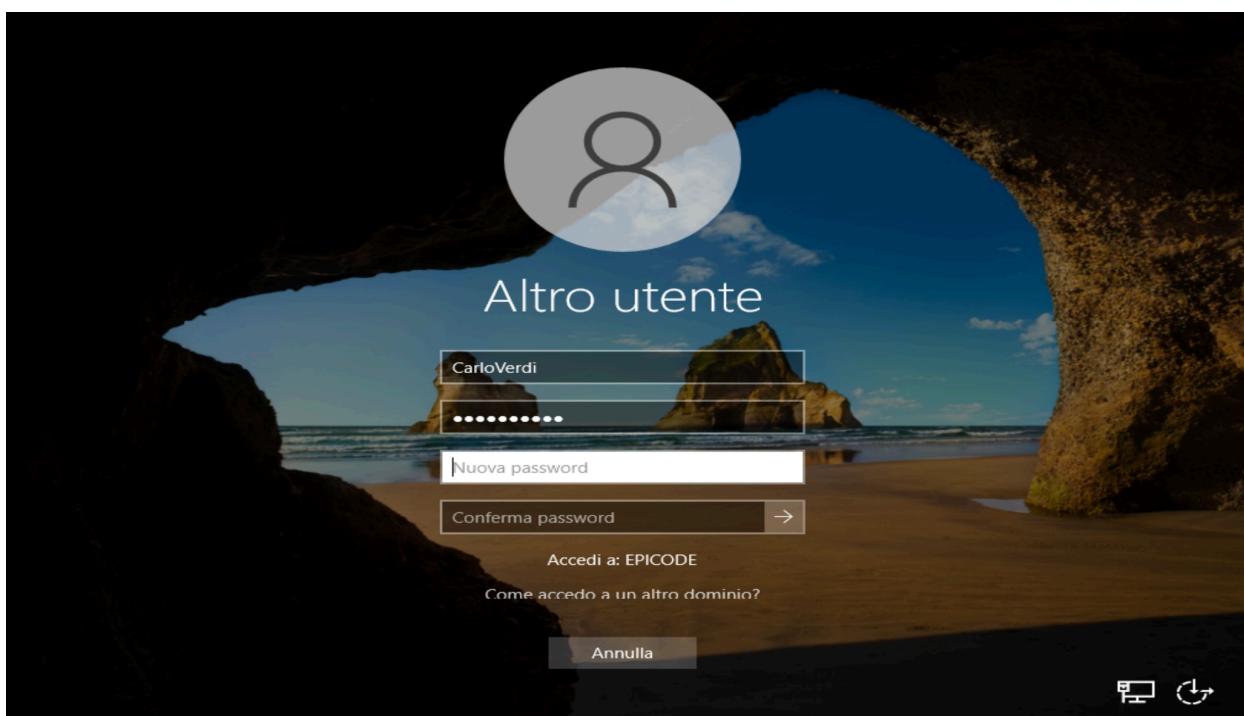
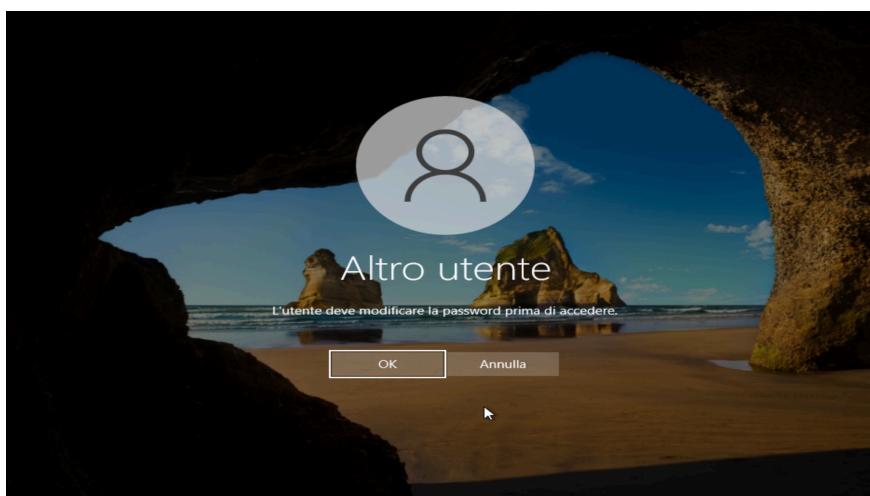
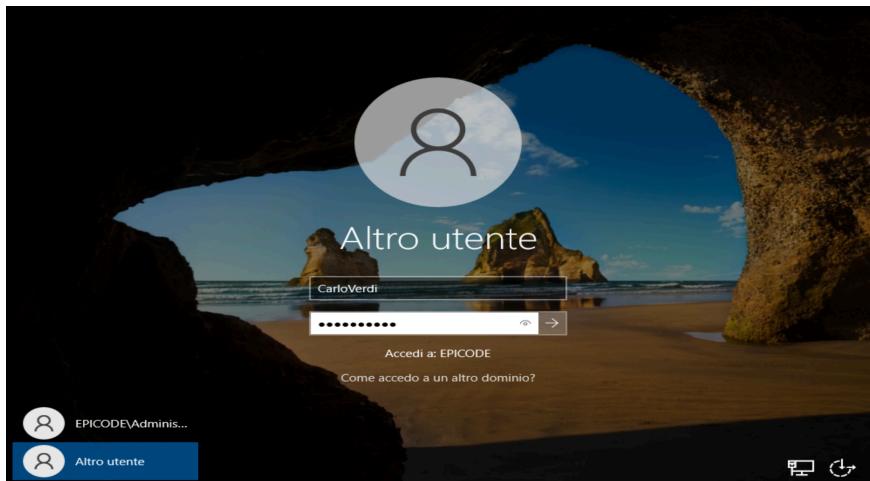
Andiamo in “Proprietà” della cartella e clicchiamo su “Condivisione” e aggiungiamo “Assistenza\_Clienti” tra gli utenti che possono accedere alla cartella.



Facciamo lo stesso procedimento con la cartella delle "Email\_Sospette":

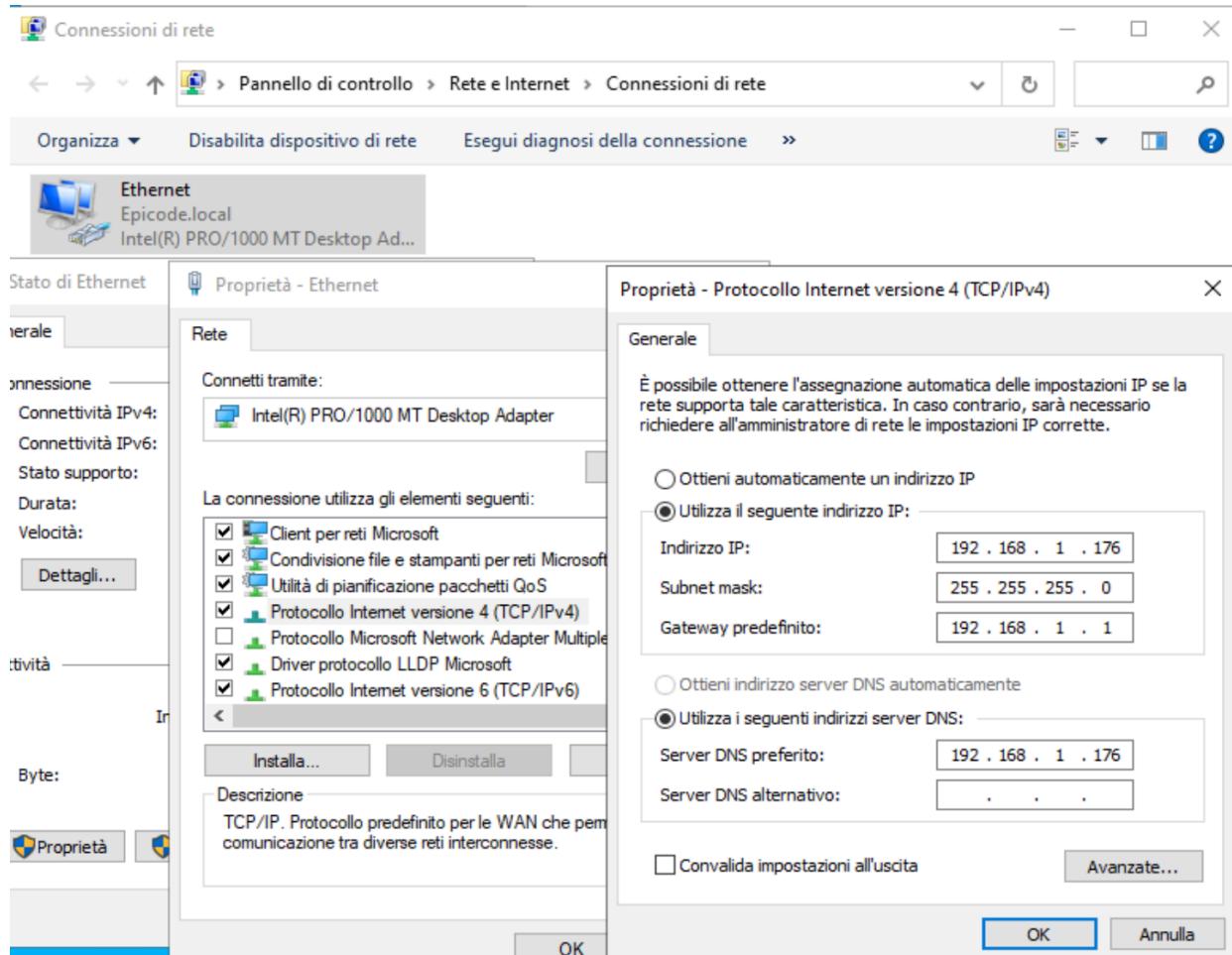


Per Concludere, andiamo su “windows”, “utente”, “disconnetti”, “altro utente”, e proviamo ad accedere con uno degli utenti registrati.



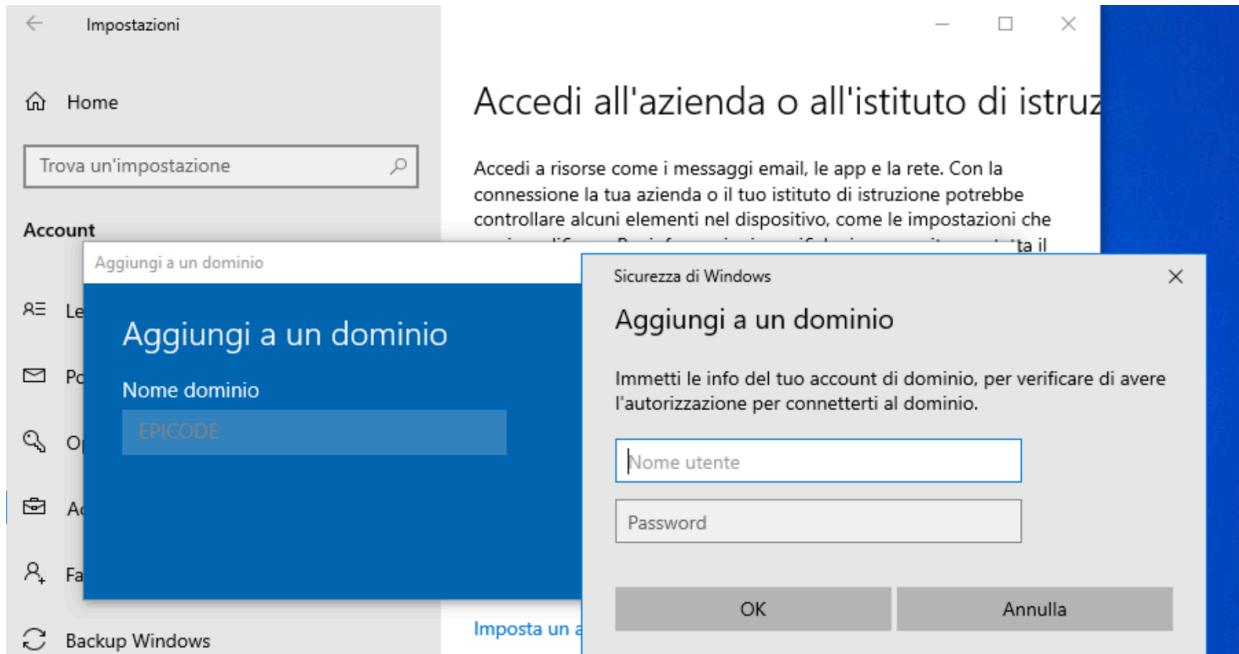
In questo caso la nuova password sarà “Changed1!”

ora trasferiamoci sulla macchina da cui ci interessa fare l’accesso, in questo caso windows 10 pro e andiamo a controllare le impostazioni di rete, in modo che le due macchine si trovino sulla stessa rete e possano comunicare:



In conclusione proviamo ad accedere tramite dominio:

- impostazioni
- Account
- Accedi all’azienda o all’istituto di istruzione
- Connelli
- Aggiungi un dominio locale di Active Directory
- Aggiungiamo il dominio “EPICODE”
- e scriviamo le credenziali



Una volta connessi dovremmo vedere nei documenti i file condivisi e potremo accedere solo a quelli con i permessi necessari.

#### Considerazione Finale:

Questa procedura è una procedura base di come viene gestito su server e come vengono assegnati i permessi, ovviamente in un'azienda ci sarebbe una Foresta molto più ramificata e ci sarebbero permessi differenti, però questo fa capire quanto sia importante questa procedura perchè non tutti dovrebbero poter fare le stesse cose ed è giusto diversificare i permessi di varie zone e cartelle per i lavoratori all'interno dell'azienda, in questo caso abbiamo lasciato la possibilità di maneggiare le email sospette con possibili script malevoli solo al team di specialisti che sa riconoscere i rischi in modo da non infettare altri dispositivi della rete.

La segmentazione di questi permessi è essenziale per migliorare la sicurezza dell'azienda e avere ordine nella gestione dei compiti.