Monitoraggio degli Eventi di Accesso

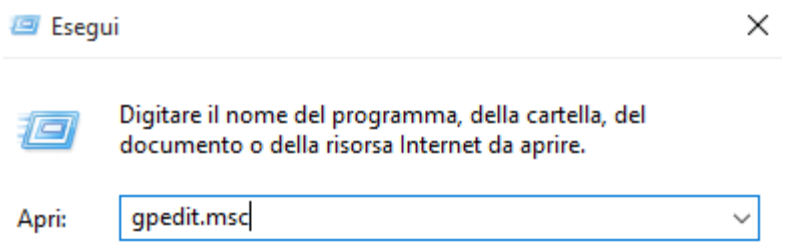
Il processo si divide in due fasi principali:

1. **Abilitazione delle policy di controllo:** Dire a Windows *quali* eventi deve registrare.
2. **Visualizzazione e filtraggio dei log:** Leggere e interpretare le informazioni registrate.

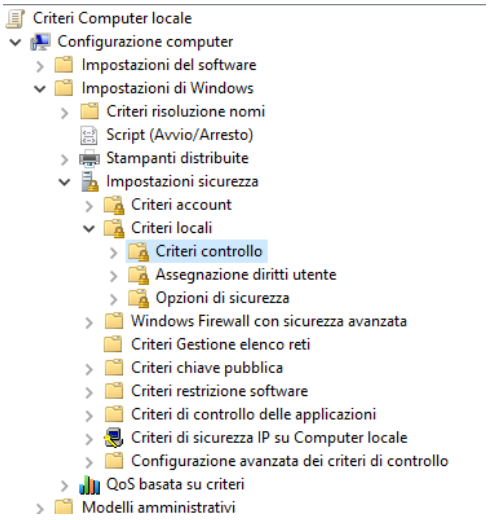
Parte 1: Abilitare la Registrazione degli Eventi di Accesso

Per impostazione predefinita, Windows non registra ogni singolo evento di accesso per non appesantire i log. Dobbiamo prima attivare questa funzione tramite i Criteri di Gruppo.

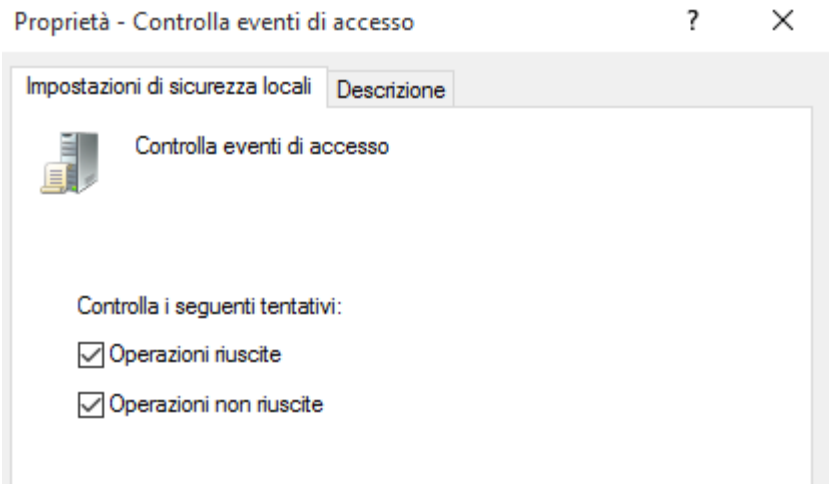
1. **Aprire l'Editor Criteri di Gruppo Locali:**
   - Premi i tasti Win + R per aprire la finestra "Esegui".
   - Digita gpedit.msc e premi Invio.



2. **Navigare alla Sezione Corretta:**
   - Nel pannello di sinistra, segui questo percorso:
     Configurazione computer -> Impostazioni di Windows -> Impostazioni di protezione -> Criteri locali -> Criteri di controllo.



3. **Configurare il Controllo degli Accessi:**
    - Nel pannello di destra, cerca e fai doppio clic sulla voce **"Controlla eventi di accesso"**.
    - Nella finestra che si apre, spunta entrambe le caselle:
        - **Operazioni riuscite:** Per registrare quando un utente accede correttamente.
        - **Operazioni non riuscite:** Per registrare i tentativi di accesso con password errata.
    - Clicca su "Applica" e poi su "OK" per salvare la modifica.

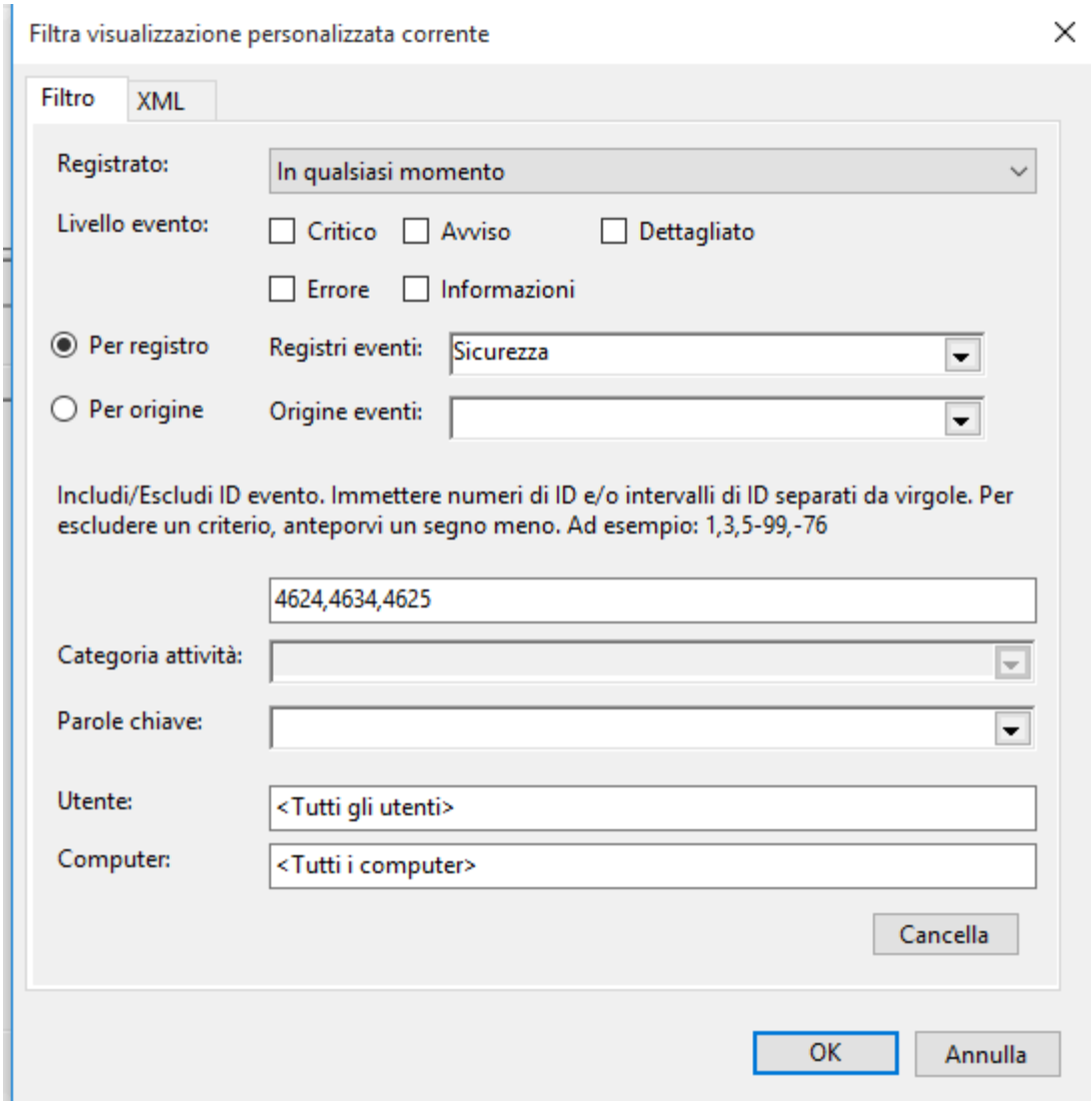


Parte 2: Verificare il Funzionamento e Visualizzare i Log

Una volta attivate le policy, possiamo verificare che il sistema stia registrando gli eventi correttamente.

1. **Aprire il Visualizzatore Eventi:**
    - Premi Win + R, digita eventvwr.msc e premi Invio.
    - Naviga in Registri di Windows -> Sicurezza.
2. **Filtrare il Registro per Trovare gli Eventi:**
    - Nel pannello di destra, clicca su **"Filtra registro corrente..."**.
    - Nel campo <Tutti gli ID evento>, inserisci i seguenti codici, separati da una virgola: 4624,4634,4625
    - Clicca su **OK**.

    Ora vedrai solo gli eventi relativi a:
    - **ID 4624:** Accesso riuscito (Logon).
    - **ID 4634:** Disconnessione (Logoff).
    - **ID 4625:** Tentativo di accesso fallito.



Ora possiamo visualizzare tutti gli eventi di accesso e disconnessione dal nostro utente Windows.

Informazioni	11/09/2025 15:03:30	Microsoft Windows security auditing.	4634	Disconnessione
Informazioni	11/09/2025 15:03:30	Microsoft Windows security auditing.	4634	Disconnessione
Informazioni	11/09/2025 15:03:24	Microsoft Windows security auditing.	4624	Accesso
Informazioni	11/09/2025 15:03:24	Microsoft Windows security auditing.	4624	Accesso