

Gli eventi con categoria attività "Logon" e "Special Logon" sono fondamentali per monitorare l'accesso e la gestione delle credenziali nel sistema.

Questi eventi vengono registrati quando un utente tenta di accedere a un sistema Windows, indipendentemente dal successo o dal fallimento. I più rilevanti sono:

| Event ID | Descrizione |
|----------|-----------------------------------|
| 4624 | Accesso riuscito |
| 4625 | Tentativo di accesso fallito |
| 4648 | Accesso con credenziali esplicite |
| 4672 | Accesso con privilegi elevati |

ID 4624

Significa che un utente o servizio è riuscito ad autenticarsi. Nei dettagli vengono specificati:

Account name: Nome utente autenticato

Logon Type: Determina il tipo di accesso in base a un numero (tabella sotto)

Source Network Address: indica l'indirizzo IP di origine

Process Name: indica il processo che ha gestito il logon

| | | | | |
|--------------------|---------------------|--------------------------------------|------|-------------------------|
| Controllo riuscito | 06/02/2025 13:06:08 | Microsoft Windows security auditing. | 5379 | User Account Management |
| Controllo riuscito | 06/02/2025 13:06:08 | Microsoft Windows security auditing. | 4672 | Special Logon |
| Controllo riuscito | 06/02/2025 13:06:08 | Microsoft Windows security auditing. | 4624 | Logon |
| Controllo riuscito | 06/02/2025 13:06:07 | Microsoft Windows security auditing. | 5061 | System Integrity |
| Controllo riuscito | 06/02/2025 13:06:06 | Microsoft Windows security auditing. | 4672 | Special Logon |
| Controllo riuscito | 06/02/2025 13:06:06 | Microsoft Windows security auditing. | 4624 | Logon |

Evento 4624, Microsoft Windows security auditing.

Generale Dettagli

Accesso di un account riuscito.

Soggetto:

ID sicurezza: SYSTEM

Nome account: DESKTOP-2111111111

Dominio account: WORKGROUP

ID accesso: 0x3E7

Informazioni di accesso:

Tipo di accesso: 5

Modalità amministrativa limitata: -

Account virtuale: No

Token elevato: Sì

Nome registro: Sicurezza

Origine: Microsoft Windows security Registrato: 06/02/2025 13:06:08

ID evento: 4624 Categoria attività: Logon

Livello: Informazioni Parole chiave: Controllo riuscito

Utente: N/D Computer: DESKTOP-2111111111

Opcodes: Informazioni

Altre informazioni: [Guida registro eventi](#)

Informazioni sul processo:

ID processo: 0x308

Nome processo: C:\Windows\System32\services.exe

Informazioni di rete:

Nome workstation: -

Indirizzo rete di origine: -

Porta di origine: -

ID 4625

Indica un tentativo di accesso non riuscito. Questo codice è molto importante per individuare possibili attacchi di brute force o accessi non autorizzati. Nei dettagli vengono specificati:

Failure Reason: motivo del fallimento

Source network Address: IP sorgente del tentativo di autenticazione

Account For Which Logon Failed: Nome utente bersagliato.

Per poter visualizzare questo processo, ho effettuato un logout dall'utente corrente premendo i tasti Win+L e messo delle credenziali errate.

| Parole chiave | Data e ora | Origine | ID evento | Categoria attività |
|------------------------|---------------------|-------------------------------------|-----------|--------------------|
| Controllo non riuscito | 06/02/2025 16:25:37 | Microsoft Windows security auditing | 4625 | Logon |
| Controllo non riuscito | 06/02/2025 16:25:36 | Microsoft Windows security auditing | 4625 | Logon |

Evento 4625, Microsoft Windows security auditing.

Generale | **Dettagli**

Accesso di un account non riuscito.

Soggetto:

ID sicurezza: SYSTEM
Nome account: **Controllo non riuscito**
 Dominio account: WORKGROUP
 ID accesso: 0x3E7

Tipo di accesso: **2**

Account il cui accesso non è riuscito:

ID sicurezza: NULL SID
 Nome account: -
 Dominio account: -

Nome registro: Sicurezza

Origine: Microsoft Windows security **Registrato:** 06/02/2025 16:25:36

ID evento: 4625 **Categoria attività:** Logon

Livello: Informazioni **Parole chiave:** Controllo non riuscito

Utente: N/D **Computer:** DESKTOP-XXXXXX

Opcode: Informazioni

Altre informazioni: [Guida registro eventi](#)

Informazioni sull'errore:

Motivo dell'errore: Errore durante l'accesso.
 Stato: 0xC000006D
 Stato secondario: 0xC0000380

Informazioni sul processo:

ID processo chiamante: 0x8e4
Nome processo chiamante: **C:\Windows\System32\svchost.exe**

Informazioni di rete:

Nome workstation: -
Indirizzo di rete di origine: **127.0.0.1**
 Porta di origine: 0

Il campo di **Logon Type** negli eventi di logon indica come è avvenuto l'accesso:

| Logon Type | Descrizione | Esempi D'uso |
|------------|-------------------|---|
| 2 | Interactive | Login con tastiera/mouse |
| 3 | Network | Accesso da rete |
| 4 | Batch | Script o processi automatizzati |
| 5 | Service | Account di servizio Windows |
| 7 | Unlock | Riattivazione da blocco schermo |
| 8 | NetworkClearText | Login via rete senza crittografia (!) |
| 9 | NewCredentials | Credenziali usate da un altro contesto |
| 10 | RemoteInteractive | Accesso da desktop remoto |
| 11 | CachedInteractive | Login con credenziali memorizzate (offline) |

ID 4672

Il special logon viene registrato quando un utente accede con privilegi elevati. Su windows, un evento 4672 viene prima di un evento 4624, se così non dovesse essere, potrebbe essere un sintomo di una manipolazione dei log di sistema.

Viene specificato:

Privileges Assigned: elenca i privilegi assegnati all'utente

Account Name: nome dell'account amministrativo

| Parole chiave | Data e ora | Origine | ID evento | Categoria attività |
|--------------------|---------------------|--------------------------------------|-----------|--------------------|
| Controllo riuscito | 06/02/2025 16:25:40 | Microsoft Windows security auditing. | 4672 | Special Logon |
| Controllo riuscito | 06/02/2025 16:25:40 | Microsoft Windows security auditing. | 4624 | Logon |
| Controllo riuscito | 06/02/2025 16:25:40 | Microsoft Windows security auditing. | 4624 | Logon |
| Controllo riuscito | 06/02/2025 16:25:40 | Microsoft Windows security auditing. | 4672 | Special Logon |

| | |
|-------------------|--|
| Privilegi: | SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege |
|-------------------|--|

ID 4648

viene registrato quando un processo utilizza credenziali esplicite per autenticarsi su un sistema.

| Parole chiave | Data e ora | Origine | ID evento | Categoria attività |
|--------------------|---------------------|--------------------------------------|-----------|--------------------|
| Controllo riuscito | 06/02/2025 16:25:40 | Microsoft Windows security auditing. | 4648 | Logon |
| Controllo riuscito | 06/02/2025 16:25:40 | Microsoft Windows security auditing. | 4648 | Logon |
| Controllo riuscito | 06/02/2025 16:25:40 | Microsoft Windows security auditing. | 4648 | Logon |

Account Name: L'account che ha avviato il processo che usa credenziali diverse.

Logon GUID: Identificativo univoco della sessione di logon.

Process Name: il processo che ha usato le credenziali (es. runas.exe, mstsc.exe, powershell.exe).

Account Whose Credentials Were Used: Il nome utente e il dominio delle credenziali inserite.

Target Server Name: Il nome del server o sistema di destinazione.

Source Network Address: L'IP da cui è stato effettuato il logon.

Logon Type: Il tipo di logon (vedi tabella pagina successiva).

Evento 4648, Microsoft Windows security auditing.

Generale | Dettagli

È stato tentato un accesso utilizzando credenziali esplicite.

Soggetto:

ID sicurezza: SYSTEM

Nome account: [redacted]

Dominio account: WORKGROUP

ID accesso: 0x3E7

GUID accesso: {00000000-0000-0000-0000-000000000000}

Account di cui sono state utilizzate le credenziali:

Nome account: [redacted]

Dominio account: MicrosoftAccount

GUID accesso: {00000000-0000-0000-0000-000000000000}

Server di destinazione:

Nome server di destinazione: localhost

Informazioni aggiuntive: localhost

Informazioni sul processo:

ID processo: 0x320

Nome processo: C:\Windows\System32\lsass.exe

Informazioni di rete:

Indirizzo di rete: -

Porta: -

| Logon Type | Descrizione | Esempi D'uso |
|------------|-------------------|---|
| 2 | Interactive | Login con tastiera/mouse |
| 3 | Network | Accesso a una risorsa di rete |
| 9 | NewCredentials | Login con credenziali diverse da quelle attuali |
| 10 | Remoteinteractive | Accesso Desktop Remoto (RDP) |