Enterprise

BusinessLog

Ver. 2.24.2.X

BUSINESSLOG

VERSIONE 2.24.2.X

BLog2022 è un software per la registrazione centralizzata dei log-access, idonea per le registrazioni obbligatorie degli accessi degli Amministratori di Sistema (G.U. 300 / 2008) ed è uno strumento idoneo come misura di sicurezza ai fini del regolamento europeo (GDPR) e per la copertura alle misure per la NIS2.

SOMMARIO

Sommario

Installazione completa

DOWNLOAD DEL PACCHETTO D'INSTALLAZIONE:

Il pacchetto di installazione è per sistemi a 64 bit,

https://www.businesslog.it/download/BusinessLog2022.exe

REQUISITI MINIMI:

CPU Intel o AMD di classe i7 o superiore (almeno 6 vCore per VM)

*** CONSIGLIATA MACCHINA FISICA ***

> 8 Gb di Ram (consigliata 16)

Almeno 100 Gb di spazio libero per database ed archivi

È consigliabile l'utilizzo di dischi SSD o M2 o, in caso di Macchina virtuale, l'utilizzo del controller disco Paravirtual (per VMware) o con Hyper-V Generation 2 (per Hyper-V)

.net Framework 4.8 (compreso, comunque, nel setup) Sistemi operativi:

- Windows 10 pro
- Windows 11 pro
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Tutto il sistema BusinessLog funziona, esclusivamente, su piattaforma a 64 bit!

NB: La macchina deve trovarsi nel dominio principale.

ATTENZIONE

Alcuni antivirus, tramite il processo euristico, potrebbero bloccare l'esecuzione del setup e della corretta esecuzione degli eseguibili

È importante mettere in esclusione la cartella di installazione di BusinessLog per permettere ai processi di eseguire correttamente le proprie azioni.

Cartelle da escludere:

- C:\Program Files (x86)\Enterprise\BusinessLog
- C:\Users\[UTENTE]\AppData\Local\Temp\AppLifeLauncher\
- C:\Users\[UTENTE]\AppData\Local\Kjs.AppLife.Update

Sostituire [UTENTE] con il nome utente utilizzato per accedere alla macchina con BusinessLog

Comunicazioni con l'esterno

BusinessLog, ha bisogno di comunicare con la rete e con alcune risorse esterne, verificate che il Firewall non blocchi una o più porte per il corretto funzionamento; qui il riepilogo:

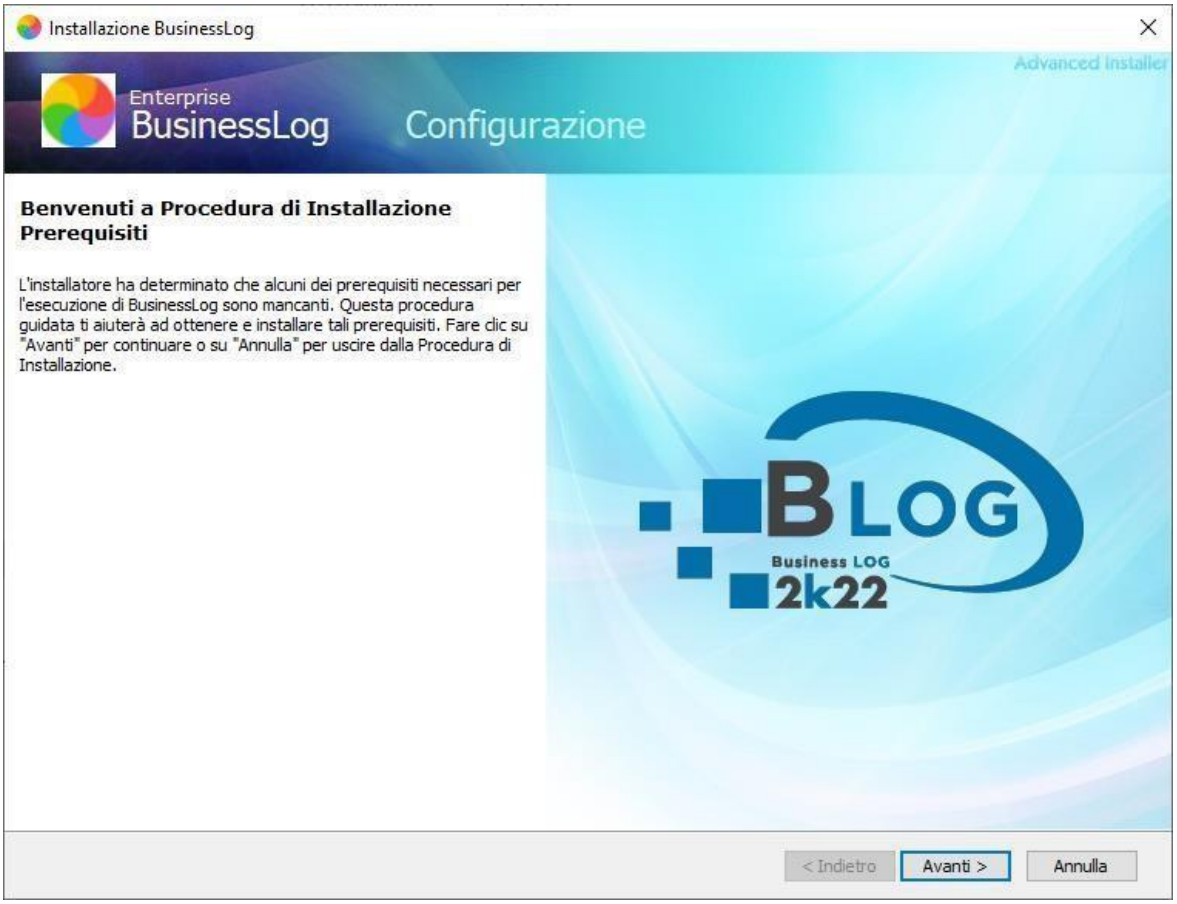
SISTEMA	<>	PORTA	DESTINAZIONE	MOTIVO
NIST	OUT	TCP 13	time-c.nist.gov	Verifica di coerenza dell'orario
SERVER LICENZE	OUT	TCP 443	Https://api.businesslog.it	Comunicazioni e sincronizzazione licenza
AGGIORNAMENTI	OUT	TCP 443	https://www.applifeupdate.com/	Verifica e aggiornamenti interni
ACCESSO WINDOWS	INT	Dinamica / TCP 445, 139	Macchine Windows	Utilizzo del servizio Remote Registry per scansione e raccolta log
DCOM	INT	TCP 135	Macchine Windows	Raccolta di informazioni integrative dalle macchine
ACCESSO SYSLOG	INT	UDP 514	Macchine e Dispositivi Syslog	Utilizzo dello stream syslog per la raccolta degli eventi mandati dai dispositivi SysLog
NETBIOS	INT	UDP 137	Scansione inventario NetBios	Utilizzato per eseguire la risoluzione dei nomi durante l'inventario macchine
DNS	INT	TCP 53	Server DNS di rete (Reverse Zone)	Utilizzato per eseguire la risoluzione dei nomi durante l'inventario macchine
MAIL	OUT	TCP 465	mail.businesslog.cloud	Invio comunicazioni e notifiche verso il sistema di mail
TELEGRAM	OUT	TCP 443	https://api.telegram.org	Invio comunicazioni e notifiche verso il bot Telegram
CLOUD	OUT	TCP 1433	i5a4baz3lv.database.windows.net	Comunicazioni con il server cloud per la registrazione dei log nel datacenter
RT	INT	TCP 22422	Client RT	Comunicazione con i client con installato BlogRT
IA	OUT	TCP 443	https://api.openai.com/v1/	Comunicazione con l'Intelligenza Artificiale di OpenAI

Installazione

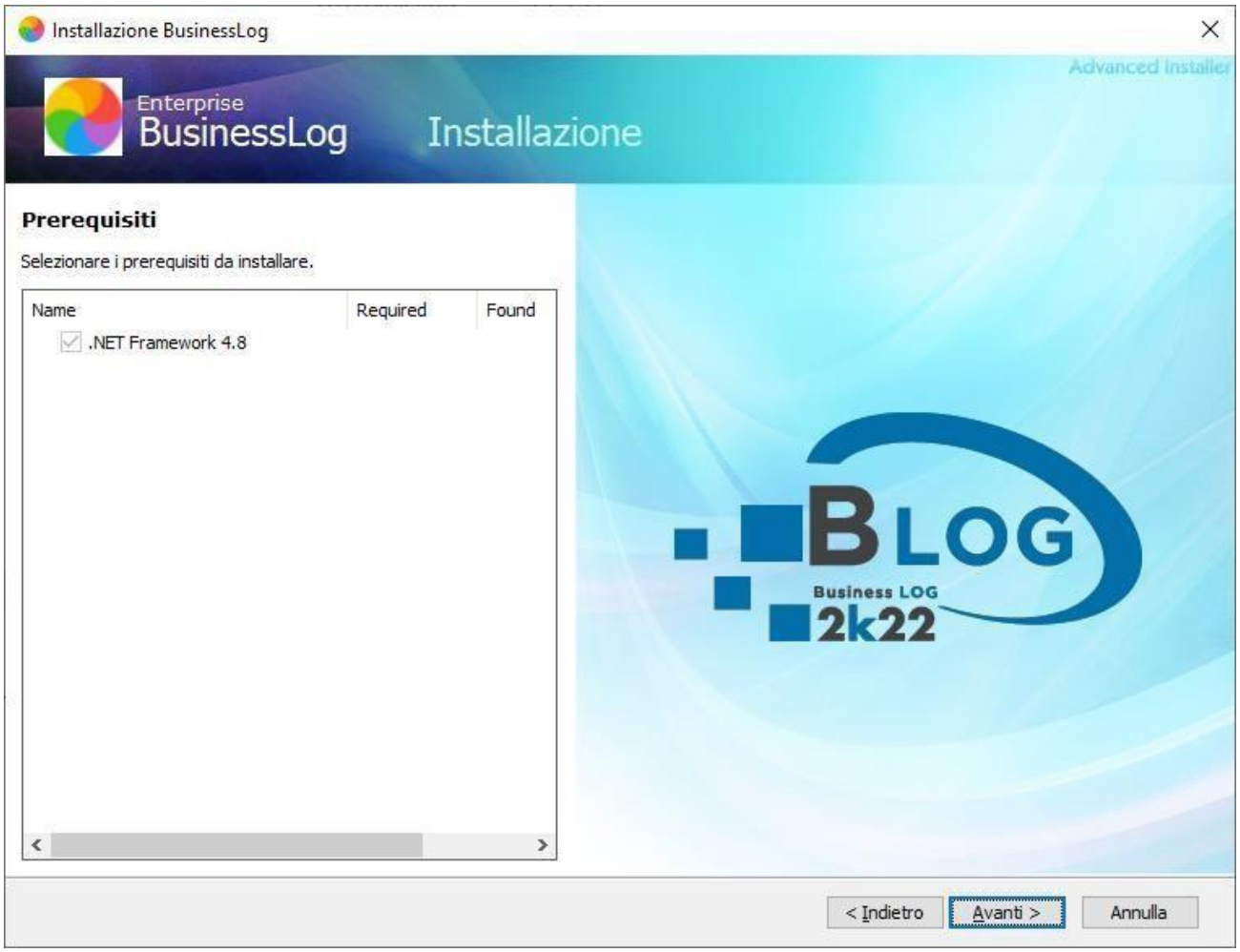
ESECUZIONE SETUP

Per avviare il processo di setup è necessario essere Amministratori della macchina, avviare il setup con clic destro > “Esegui come amministratore”

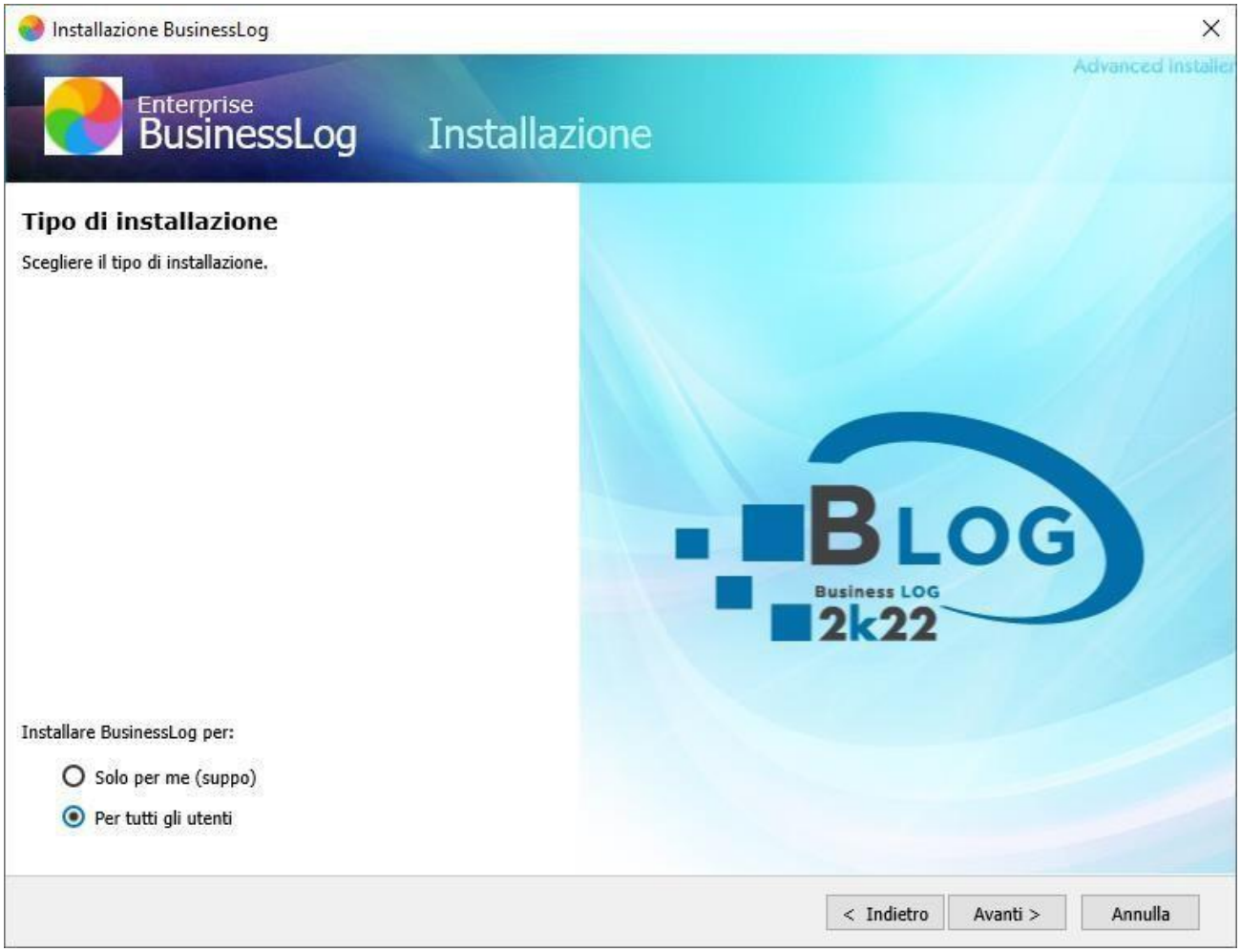
Partirà il processo di installazione del programma.



All’avvio verranno verificati i requisiti per l’installazione, ed eventualmente installati prima di procedere.

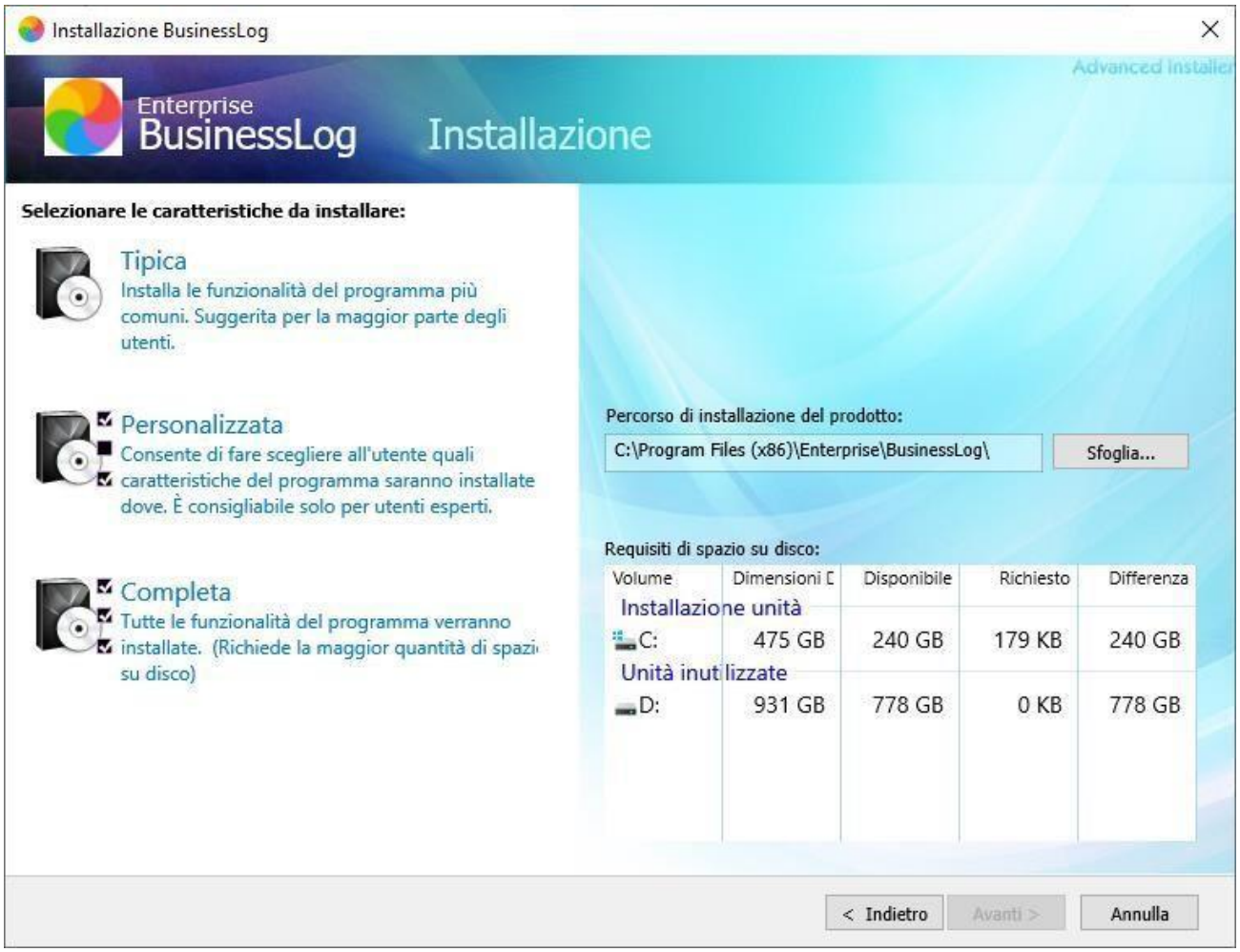


ATTENZIONE: in alcuni casi, dopo l’installazione del .net Framework 4.8 sarà necessario un riavvio della macchina.

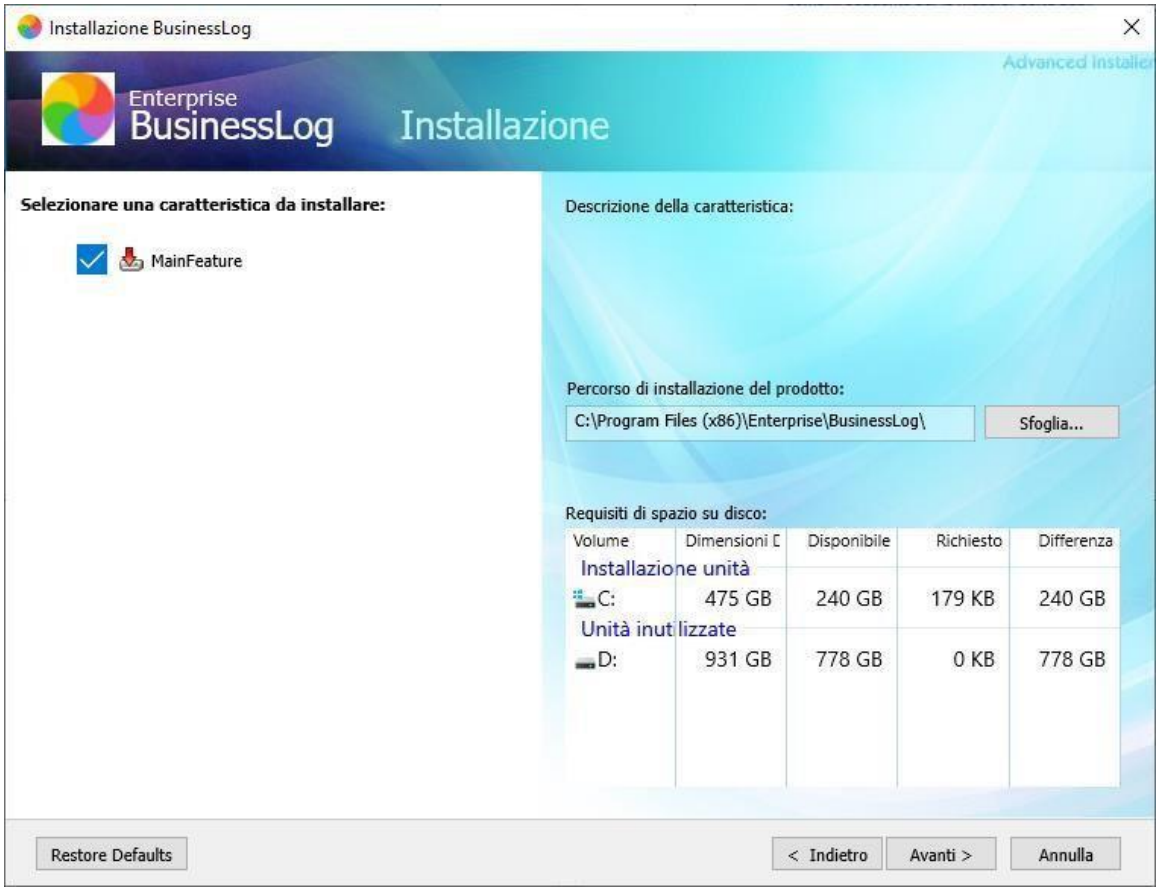


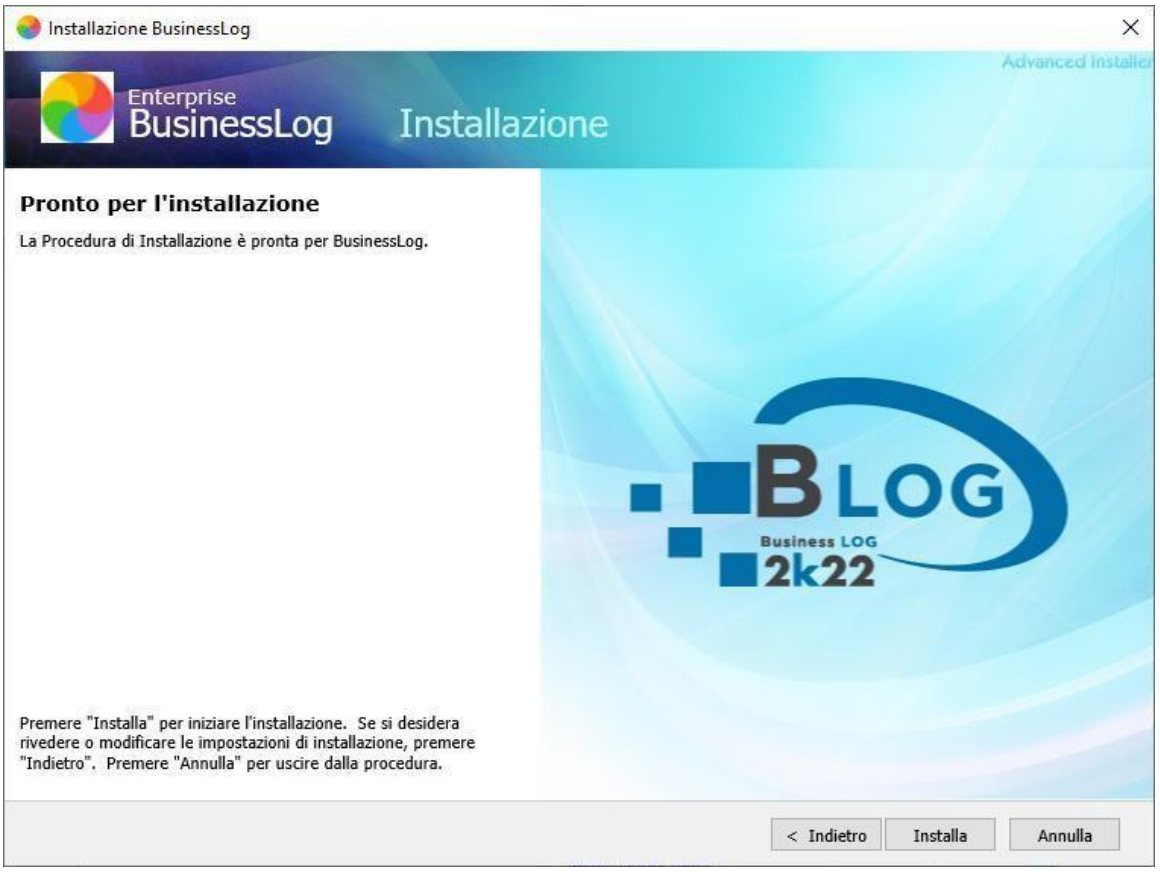
Scegliere “Per tutti gli utenti”

È consigliato di utilizzare le impostazioni predefinite per le cartelle di destinazione



In alternativa, è possibile specificare un percorso diverso


Installazione BusinessLog
Enterprise
BusinessLog
Installazione
Selezionare una caratteristica da installare:
MainFeature
Descrizione della caratteristica:
Percorso di installazione del prodotto:
C:\Program Files (x86)\Enterprise\BusinessLog\
Sfoglia...
Requisiti di spazio su disco:
Volume
Dimensioni d
Disponibile
Richiesto
Differenza
Installazione unità
C:
475 GB
240 GB
179 KB
240 GB
Unità inutilizzate
D:
931 GB
778 GB
0 KB
778 GB
Restore Defaults
< Indietro
Avanti >
Annulla


Installazione BusinessLog
Enterprise
BusinessLog
Installazione
Pronto per l'installazione
La Procedura di Installazione è pronta per BusinessLog.
BLOG
Business LOG
2k22
Premere "Installa" per iniziare l'installazione. Se si desidera rivedere o modificare le impostazioni di installazione, premere "Indietro". Premere "Annulla" per uscire dalla procedura.
< Indietro
Installa
Annulla

Migrazione dalla versione 2021

Nel caso abbiate, in funzione, una versione 2021 o precedente, occorre migrare i database al nuovo formato.

Le versioni precedenti utilizzando Microsoft SQL Compact come base dati, ma questa versione non è più compliance ed aveva importanti limiti:

- Utilizzo della memoria condivisa
- Limite massimo database a 4 Gb
- Accesso protetto da password

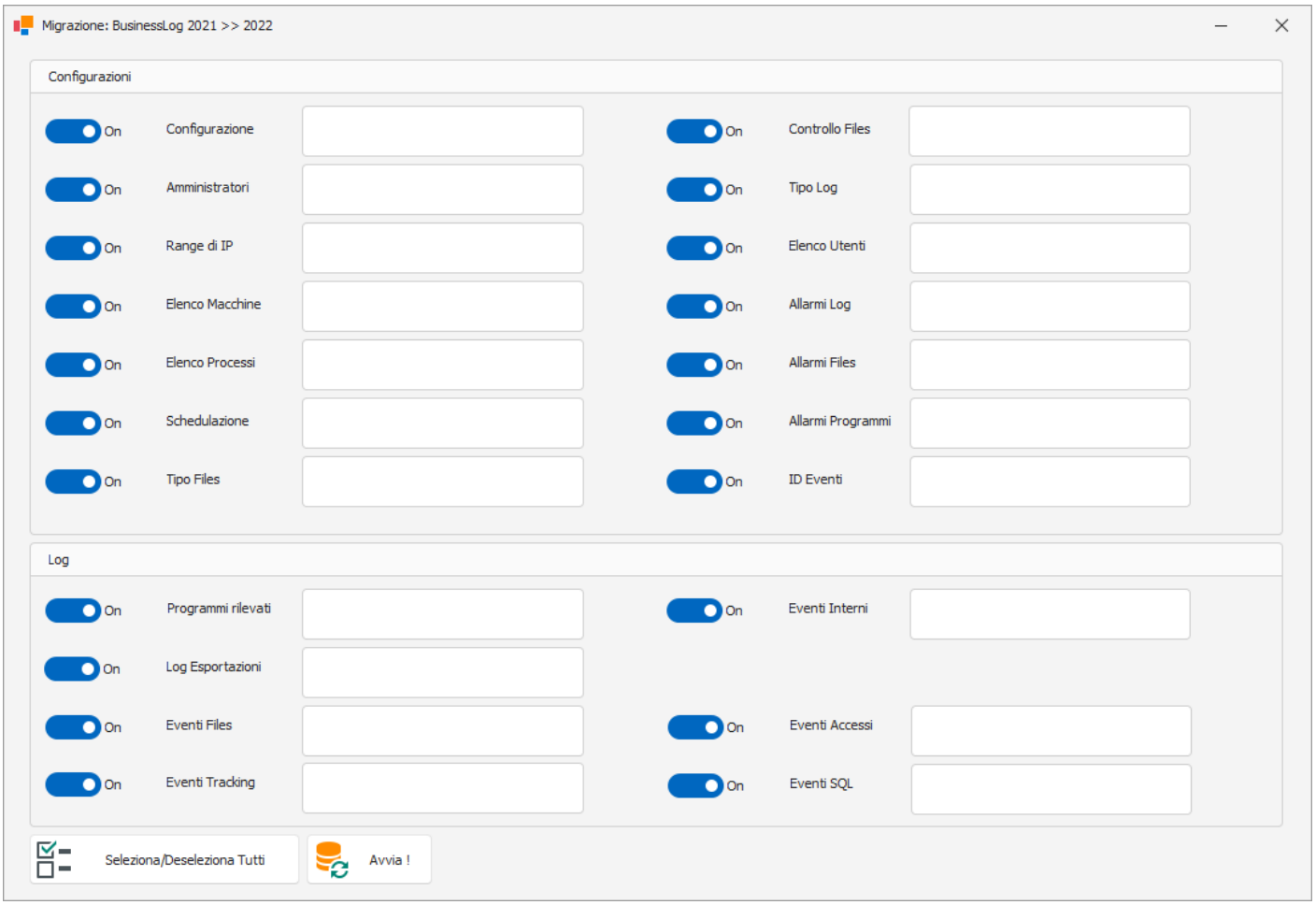
Il nuovo formato utilizza VistaDB che, oltre ad essere compliance ha nuove funzionalità:

- il database non ha limiti di utilizzo di memoria (512 Mb sono sufficienti per mappare 2 Tb di spazio)
- Il limite massimo del database è ora di 4 Tb
- Tutto il database è crittografato (AES 256 bit con BlowFish)
- Supporta il caricamento disconnesso ORM

Per effettuare la migrazione, occorre scaricare il seguente setup: www.businesslog.it/download/BusinessLog2022Update-From2021.exe

Avviate il setup scaricato come “Esegui come amministratore”

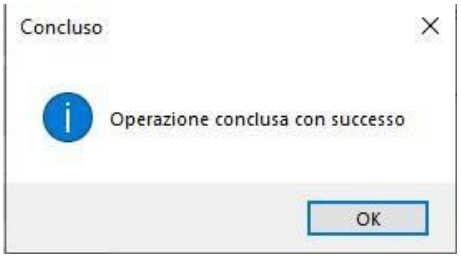
Al termine dell'installazione, comparirà la seguente schermata:



È possibile selezionare le voci desiderate cliccando sullo switch blu oppure è possibile selezionare / deselezionare tutte le voci contemporaneamente cliccando sul pulsante presente in basso a sinistra Selezione/Deseleziona Tutti.

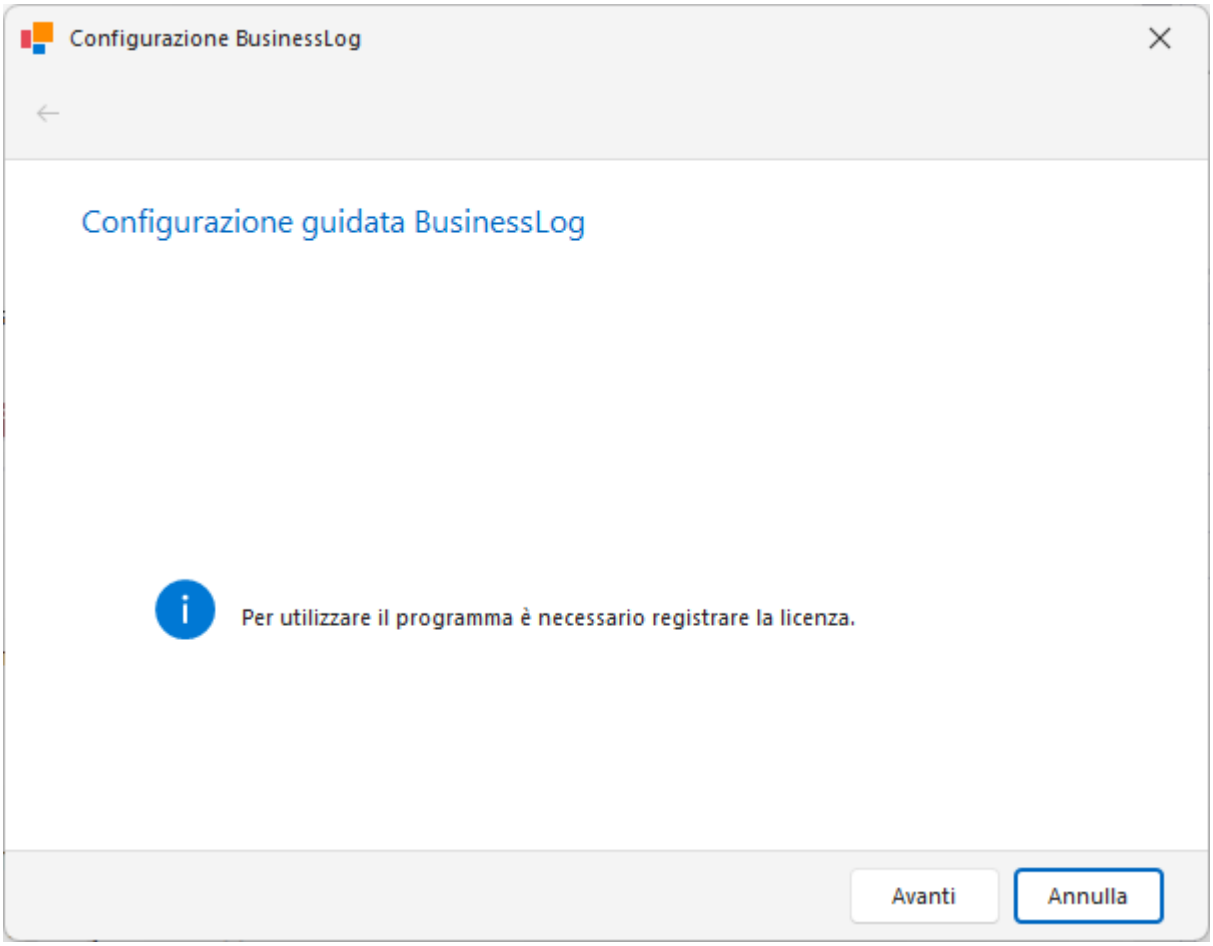
Successivamente, cliccate su Avvia!

Al termine della procedura, se eseguita nel modo corretto, comparirà la seguente schermata:



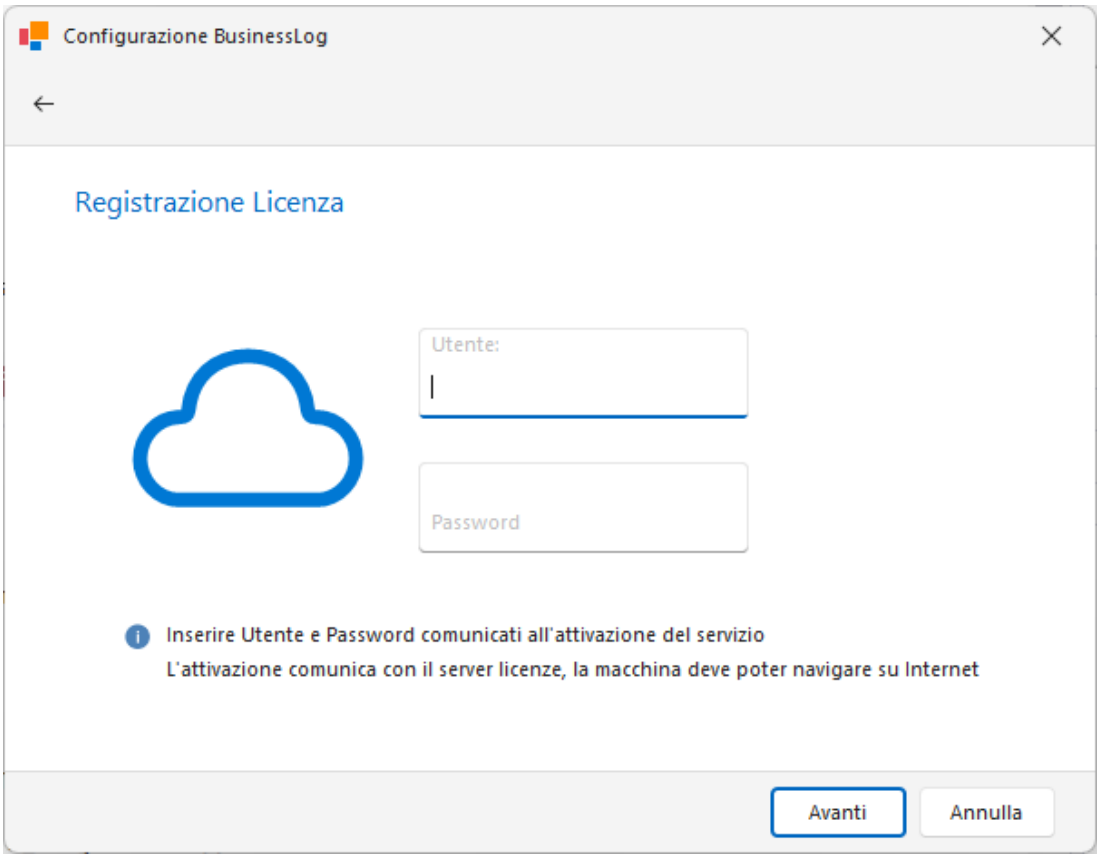
Il Wizard iniziale (setup completo)

Alla fine del setup partirà la procedura iniziale per la preimpostazione e la registrazione della licenza:

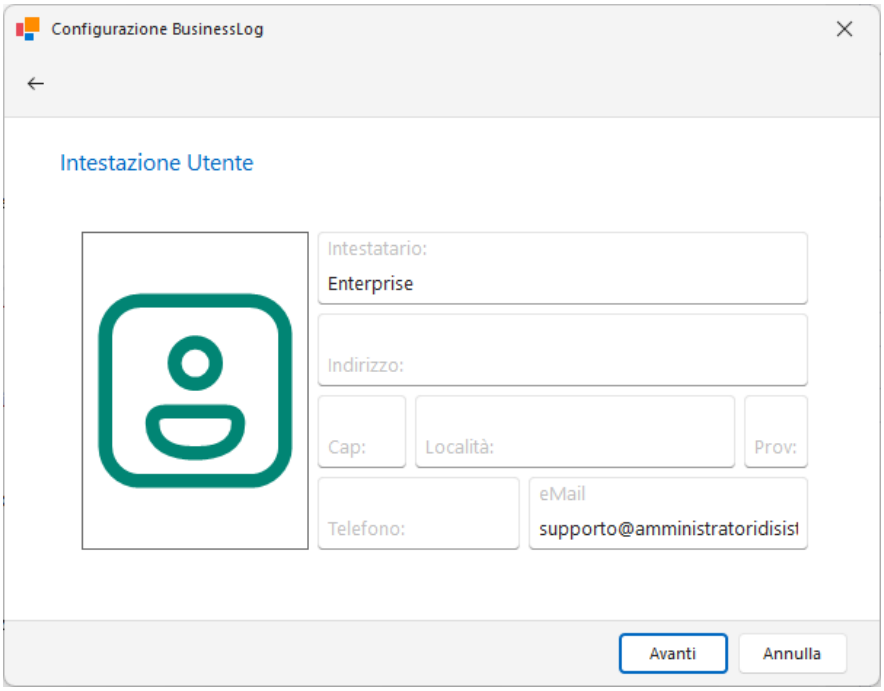


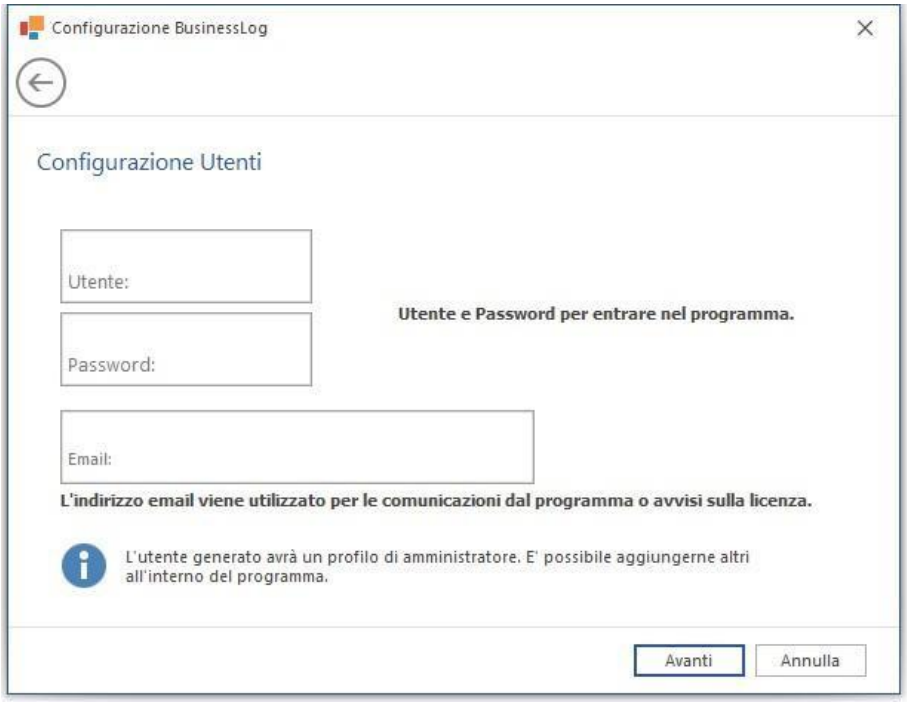
NB: Per registrare la licenza è necessario che la macchina possa navigare in Internet, il dominio per la registrazione della licenza è http://api.businesslog.it fate riferimento alla tabella a pag. 2 per le porte necessarie al programma.

Per effettuare la registrazione è necessario inserire l'Utente e la Password che avrete ricevuto come attivazione del prodotto.

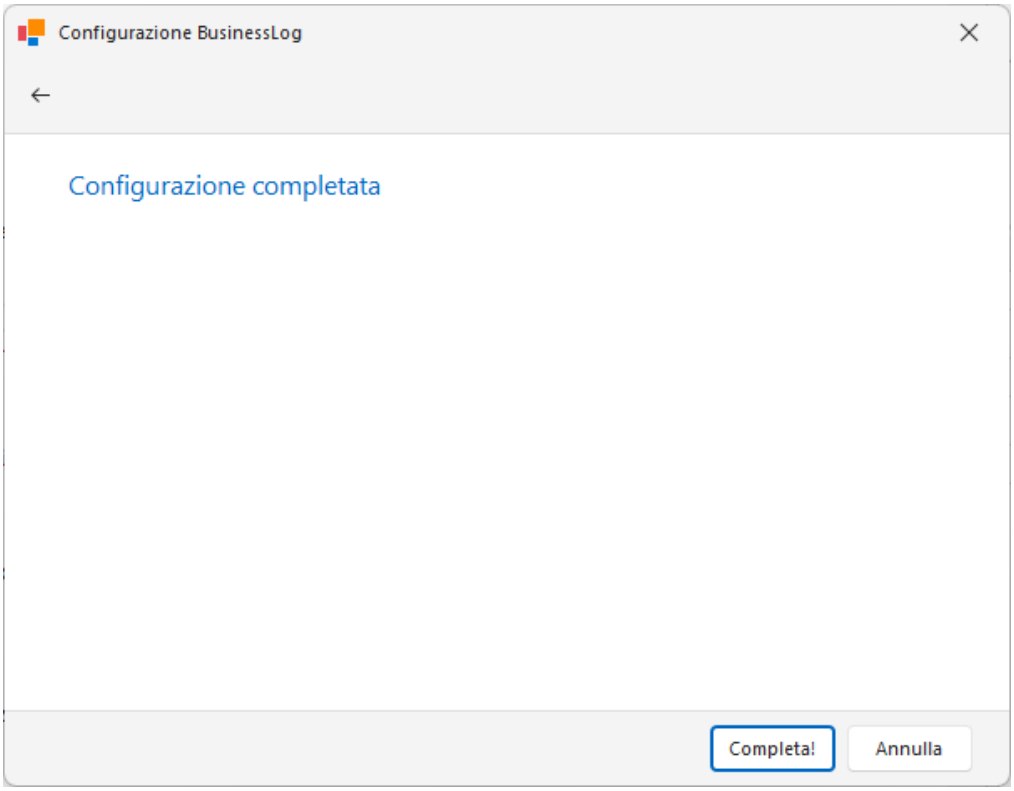


Completare i dati mancanti. Questa è l'intestazione della licenza:





Inserire le credenziali per **l'accesso al programma** di visualizzazione e un indirizzo mail valido per le comunicazioni riguardanti la **licenza.**



Se la procedura è corretta si ottiene una finestra di conferma.

Preparazione del server

Blog 2022 sfrutta le registrazioni di sistema per acquisire i log-access e il sistema integrato di accesso remoto al registro per le scansioni remote, per cui è necessario:

Abilitare gli audit di registrazione degli accessi utente

Avvio servizio Registro di sistema remoto (o Remote Registry)

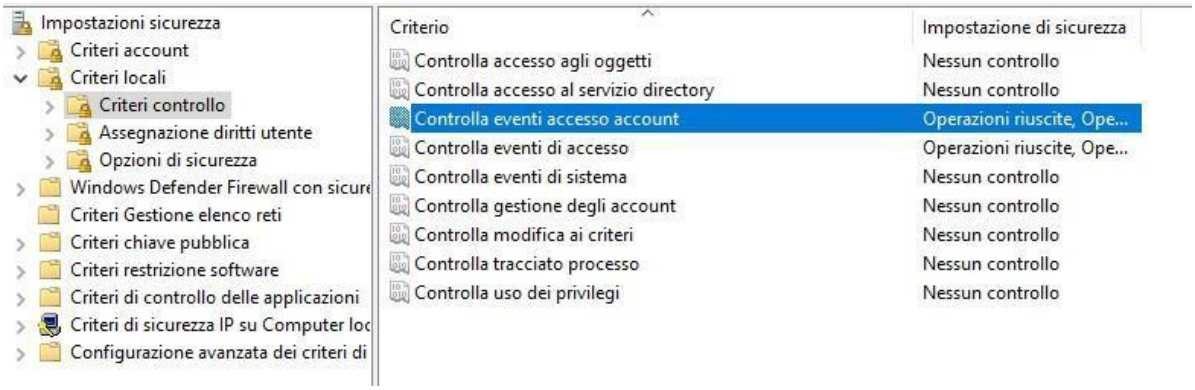
RPC Locator (per le installazioni "legacy")

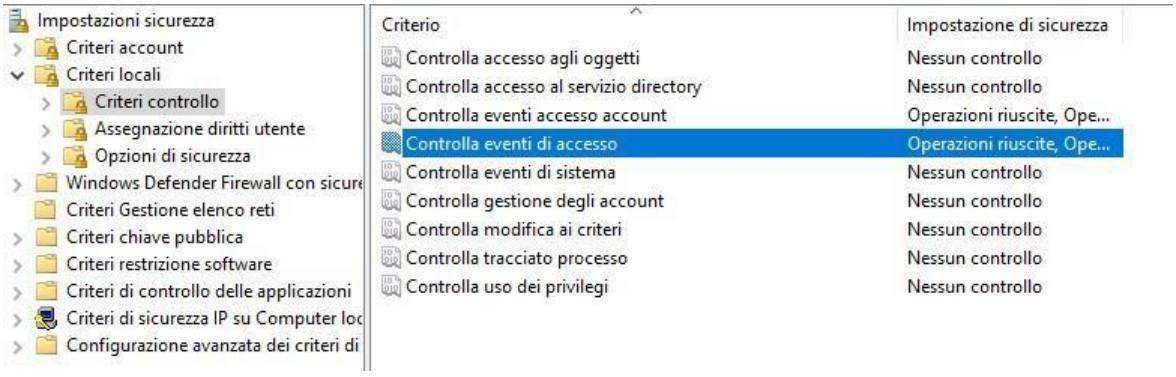
WMI (Windows Management Instrumentation)

Chiamata di procedura remota (RPC)

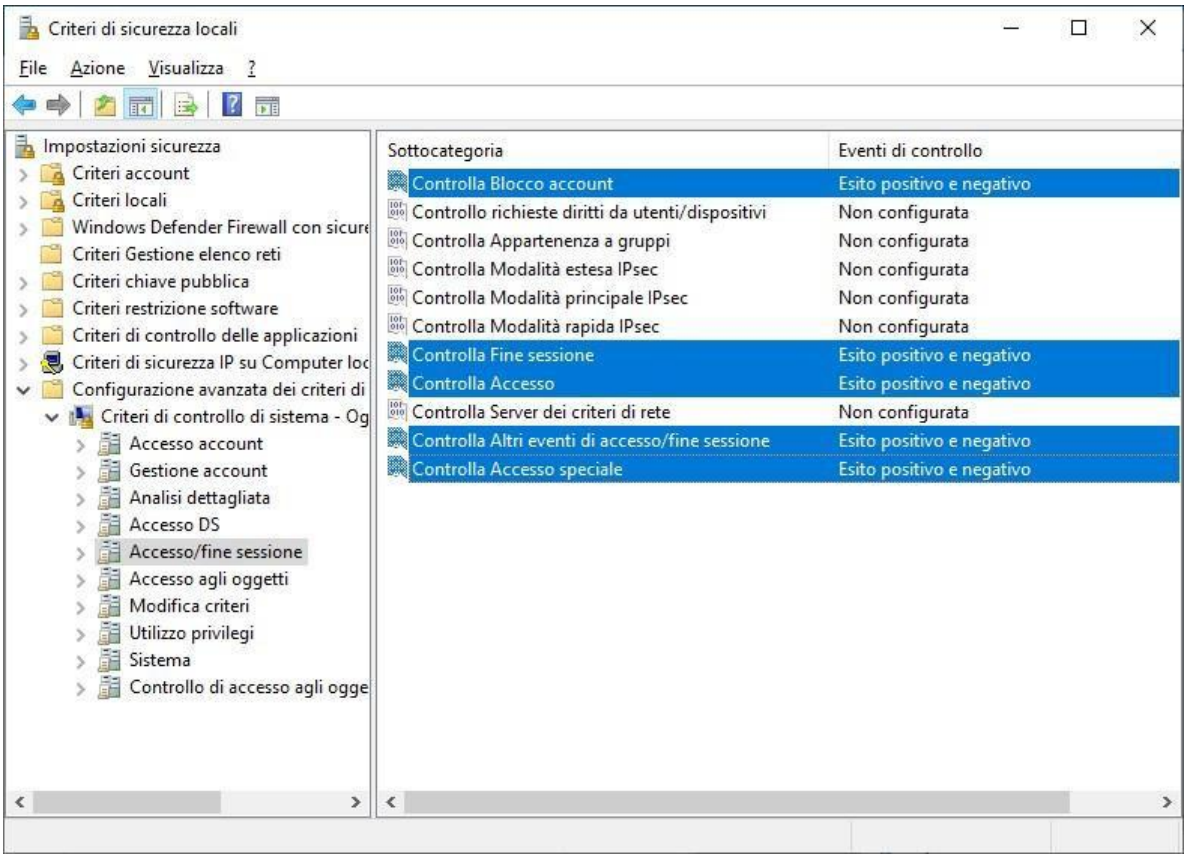
In **tutti** i client, meglio abilitare una Group Policy in grado di propagare l'attivazione a tutte le macchine

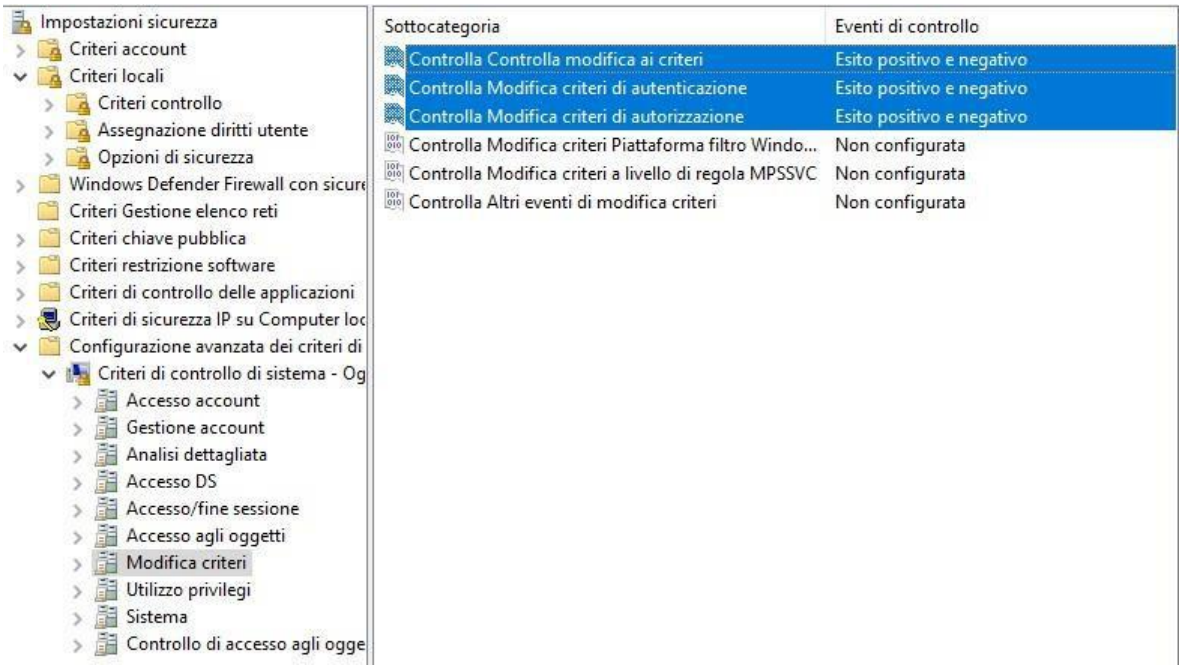
Sara necessario modificare le Group Policy per la registrazione degli accessi utente (se non già abilitato)

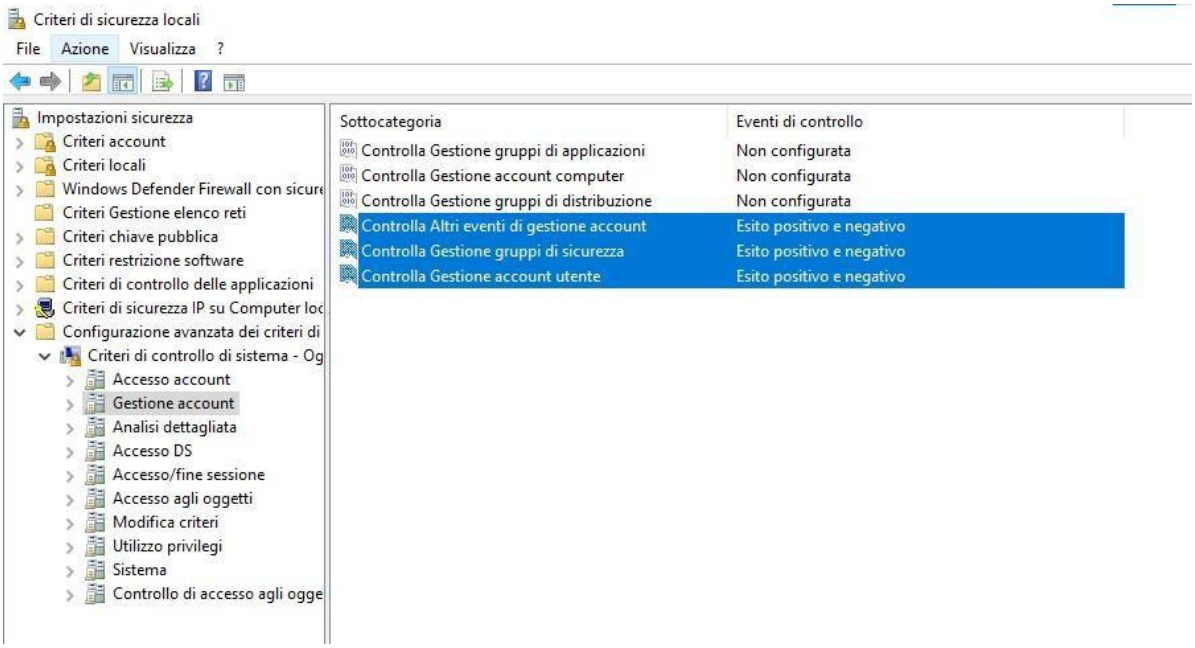




Inoltre, per avere un controllo completo sugli access-log, è necessario agire anche nella “Configurazione Avanzata”:



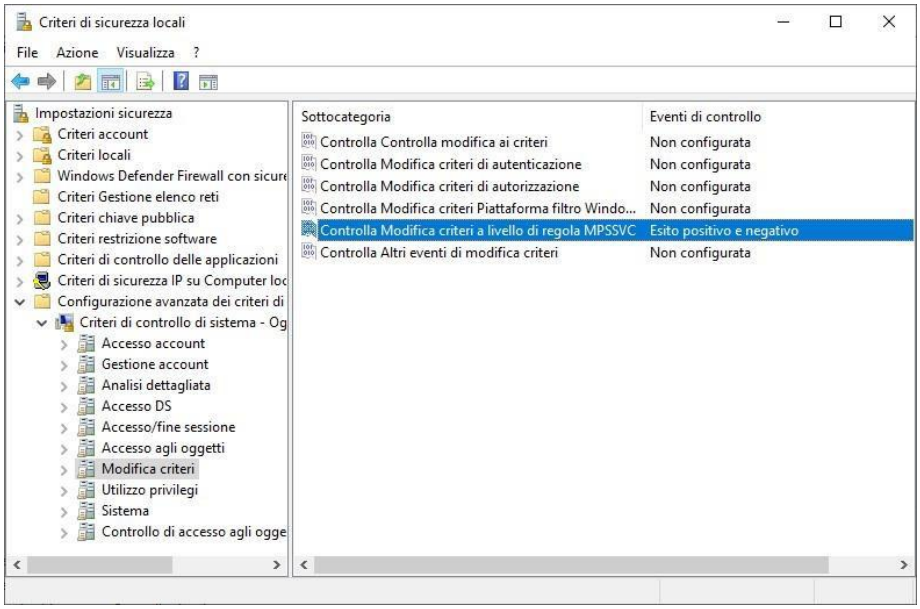




Queste sono le voci che abbiamo individuato come “audit predefinito”, ovviamente sarà possibile integrare anche altre policy, secondo le indicazioni del Vostro sistemista.

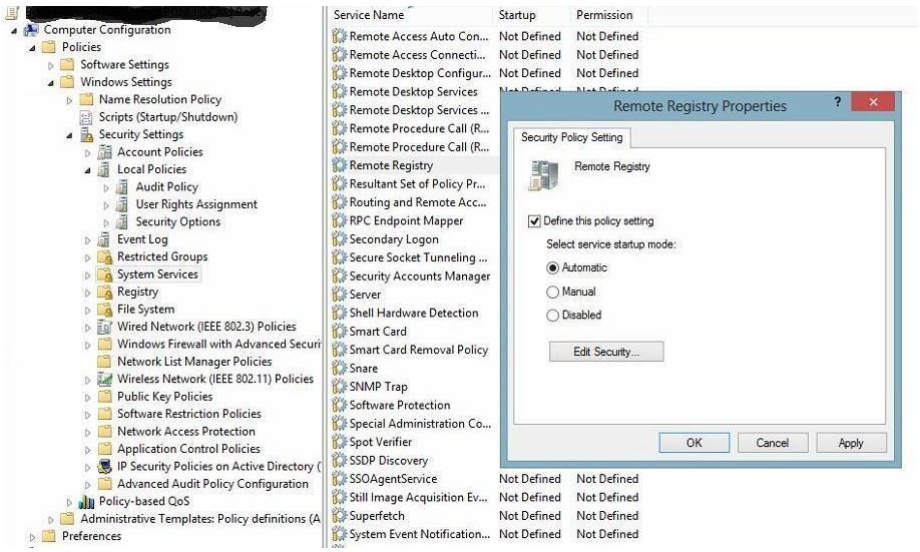
* Facoltativo:

Per monitorare, **eventualmente**, le modifiche a **Windows Firewall**, occorre attivare:



L’attivazione degli audit Firewall comporta una notevole produzione di log nei client, causati dalle numerose modifiche effettuate dai software installati. Un audit di questo tipo è consigliabile solo per i server.

Per l'avvio automatico del servizio Remote Registry in tutte le macchine:



Il servizio REMOTE REGISTRY è **fondamentale** per le comunicazioni tra la macchina host di BusinessLog e le altre rilevate in rete e messe sotto scansione, nel caso questo servizio risulti disabilitato, la scansione remota NON sarà possibile e sarà restituito un errore di rete.

Su alcuni sistemi, per impostazione predefinita, il servizio REMOTE REGISTRY viene interrotto automaticamente quando non viene utilizzato per 10 minuti.

Per disabilitare questo comportamento potete provare ad impostare in questa chiave di registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RemoteRegistry

il valore "DisableIdleStop" (DWORD) a 1. Dopo l'impostazione non è richiesto il riavvio del computer, il servizio non dovrebbe più interrompersi.

Eventualmente, controllare che il servizio WMI (Strumentazione Gestione Windows) sia già avviato nei client o che non esistono policy per disabilitare questo servizio.

Il WMI viene utilizzato per acquisire informazioni "extra" per le macchine windows in rete.

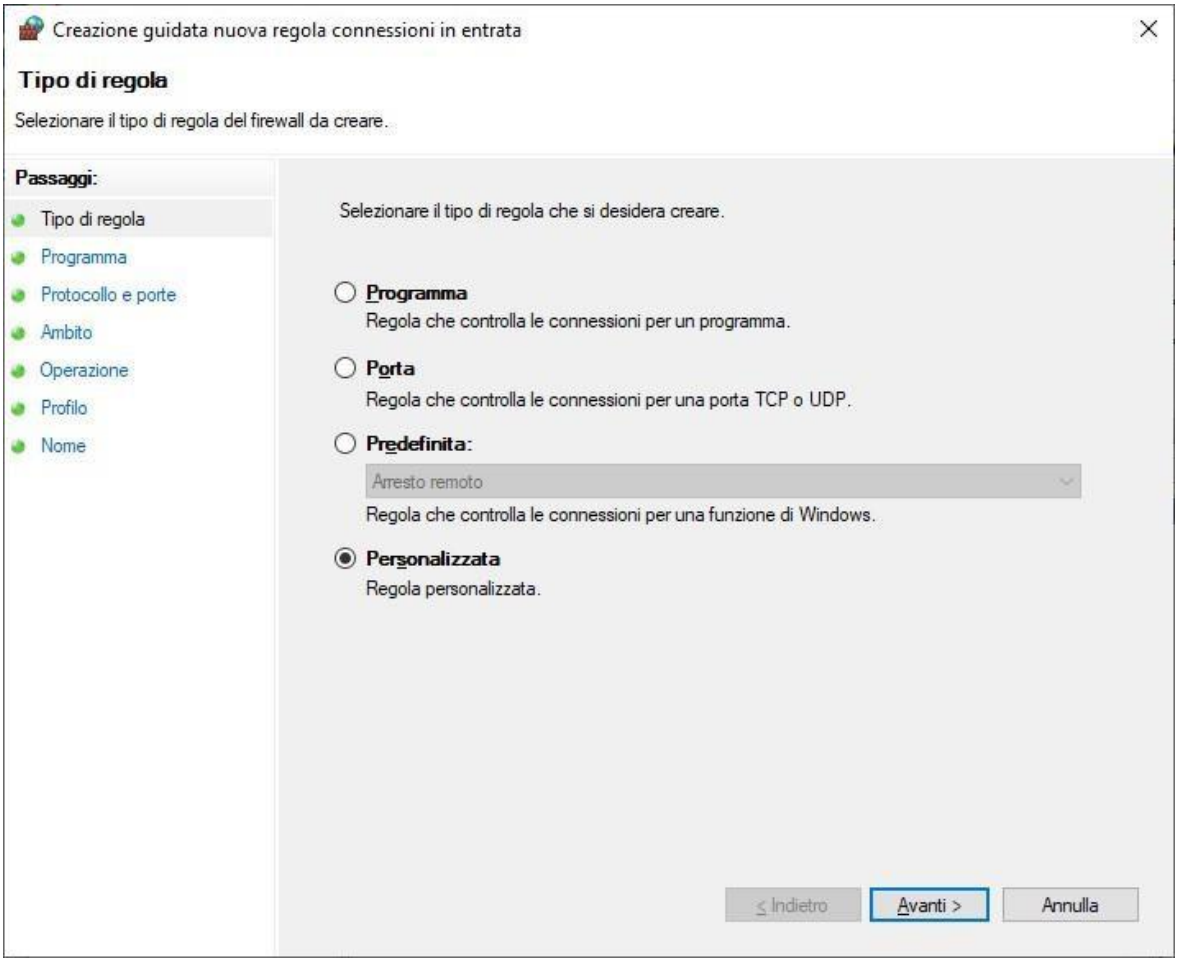
Stessa cosa per il servizio Chiamata di procedura remota (RPC) o (Remote Procedure Call (RPC) che va avviato automaticamente su tutte le macchine.

Allo stesso modo verificare il servizio GESTIONE REMOTA WINDOWS (WS-MANAGEMENT) se si intende utilizzare le funzionalità di invio comandi PowerShell dal programma BusinessLog

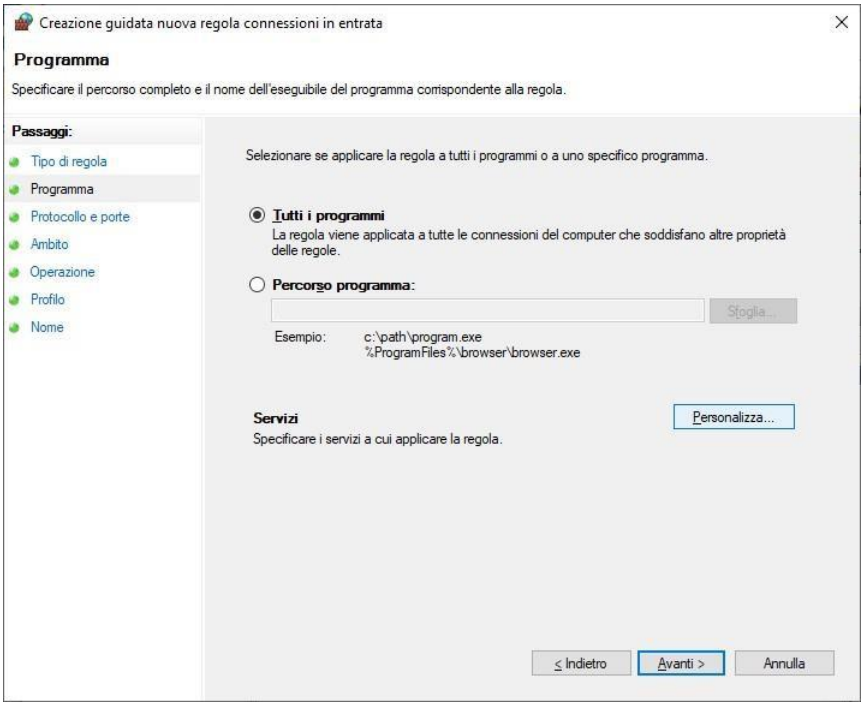
Firewall

Nella maggior parte dei casi, non sarà necessario applicare alcuna regola, tuttavia, se vengono specificate regole restrittive sul server o nei client della rete, sarà necessario autorizzare il servizio appena configurato:

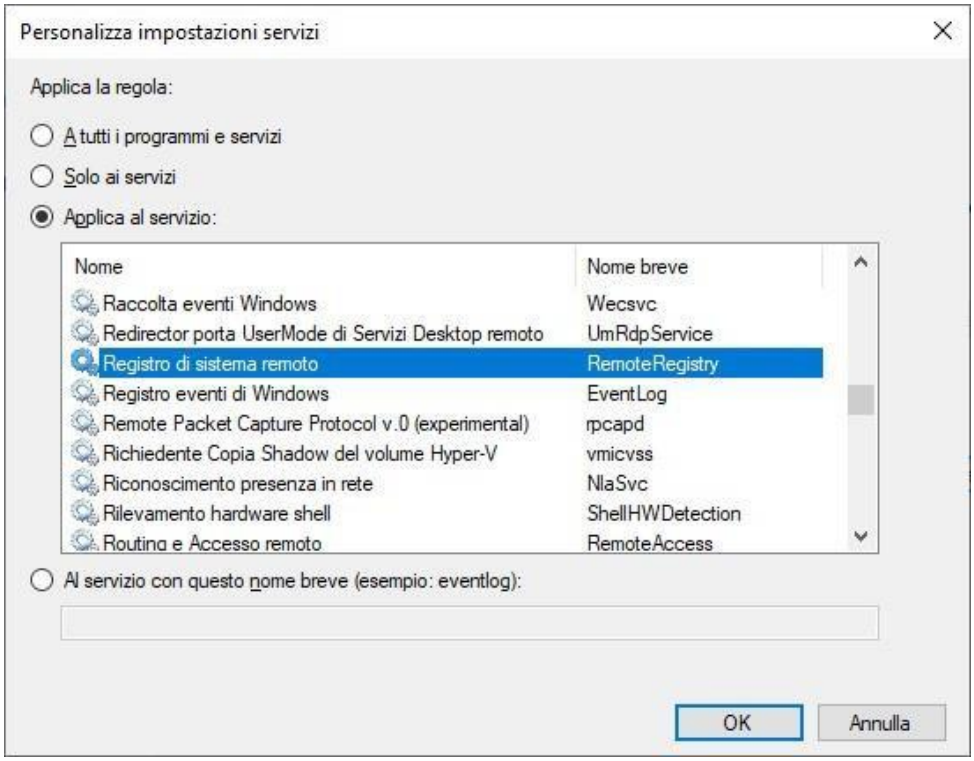
Dal Firewall di Windows > Configurazione avanzata > Regole in entrata > Nuova > Personalizzata

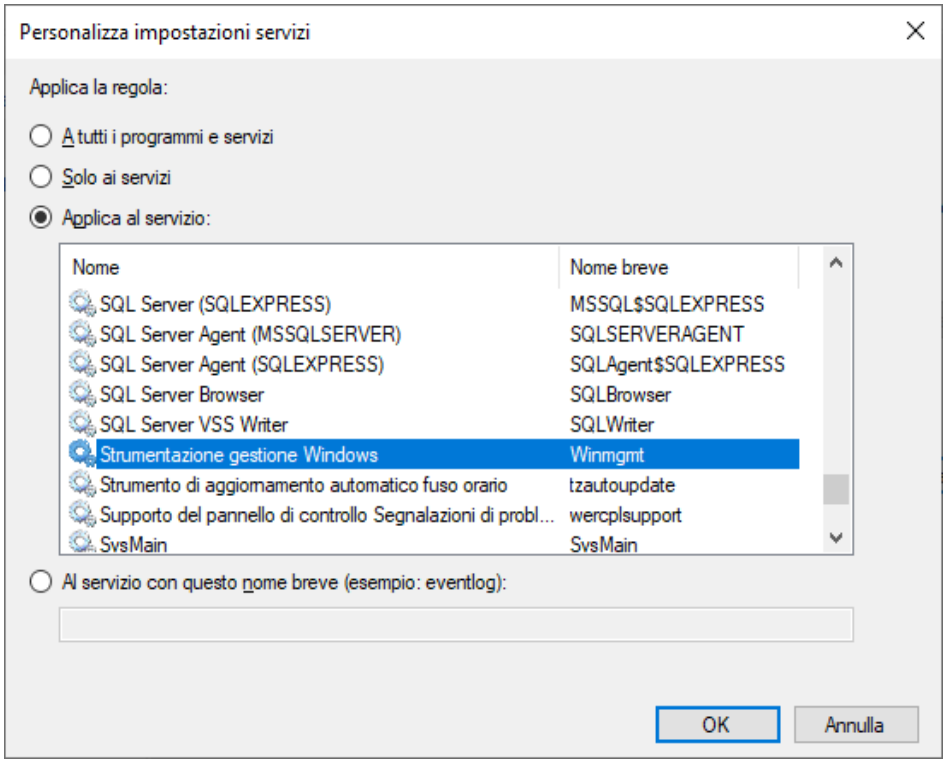


Scegliamo Servizi > [Personalizza]

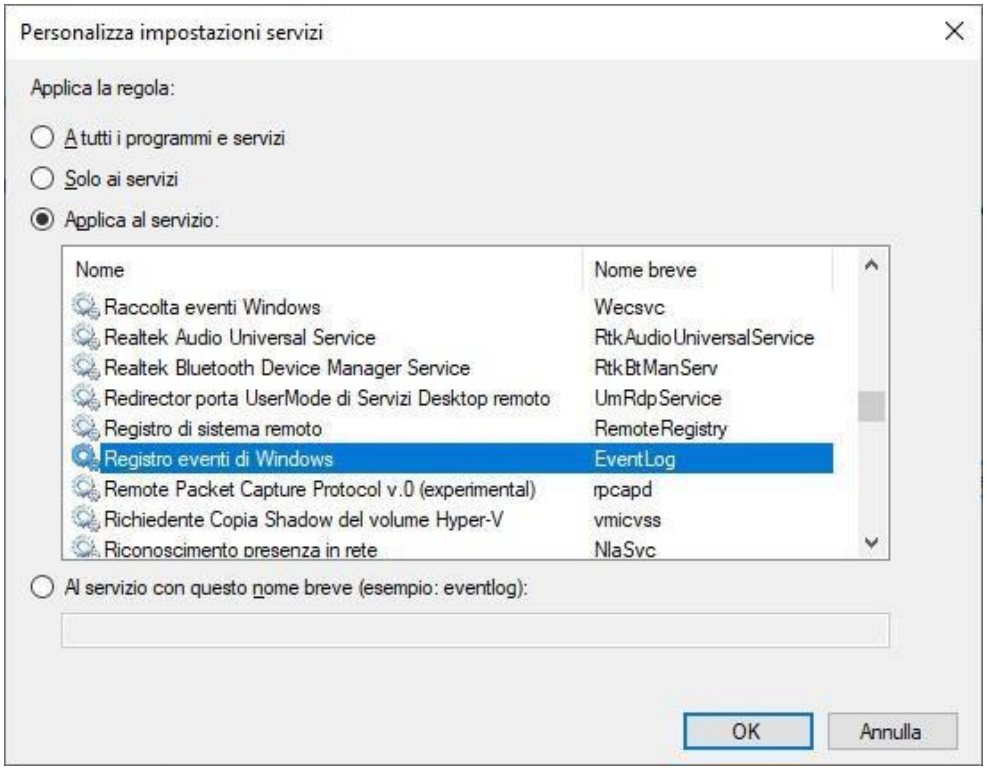


Scegliere “Applica al servizio” > Registro di sistema Remoto



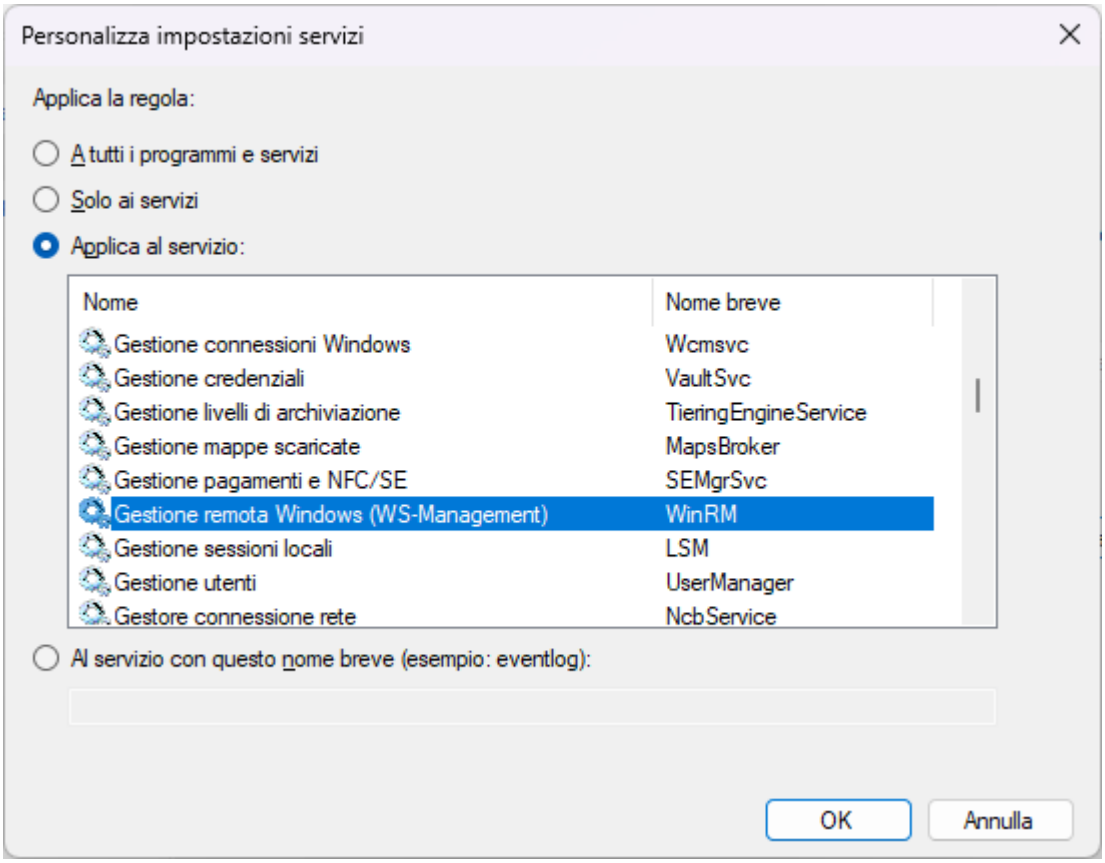


Ripetere la procedura con "**Registro di sistema eventi**" (EventLog)



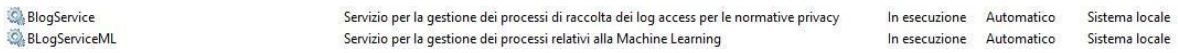
Inoltre, per permettere l'accesso ai dati relativi a WMI, occorre autorizzare anche:

Autorizzare la "Gestione remota Windows" per consentire l'invio di comandi PowerShell personalizzati dal programma.



Controllare anche eventuali porte da autorizzare, in base alla tabella riportata nelle prime pagine

Alla fine del wizard sarà installato un servizio Windows “BLogService” e un “BLogServiceML”



Il processo di installazione deve avere i permessi di amministrazione per poter inserire il servizio, in caso di errori, è possibile generare, manualmente, il servizio, da un prompt dei comandi (sempre come amministratore)

Sc create BLogService binpath=”C:\Program Files (x86)\Enterprise\BusinessLog\BlogService.exe”

NB: Il percorso potrebbe essere differente se lo avete modificato in fase di installazione

In alternativa potete utilizzare:

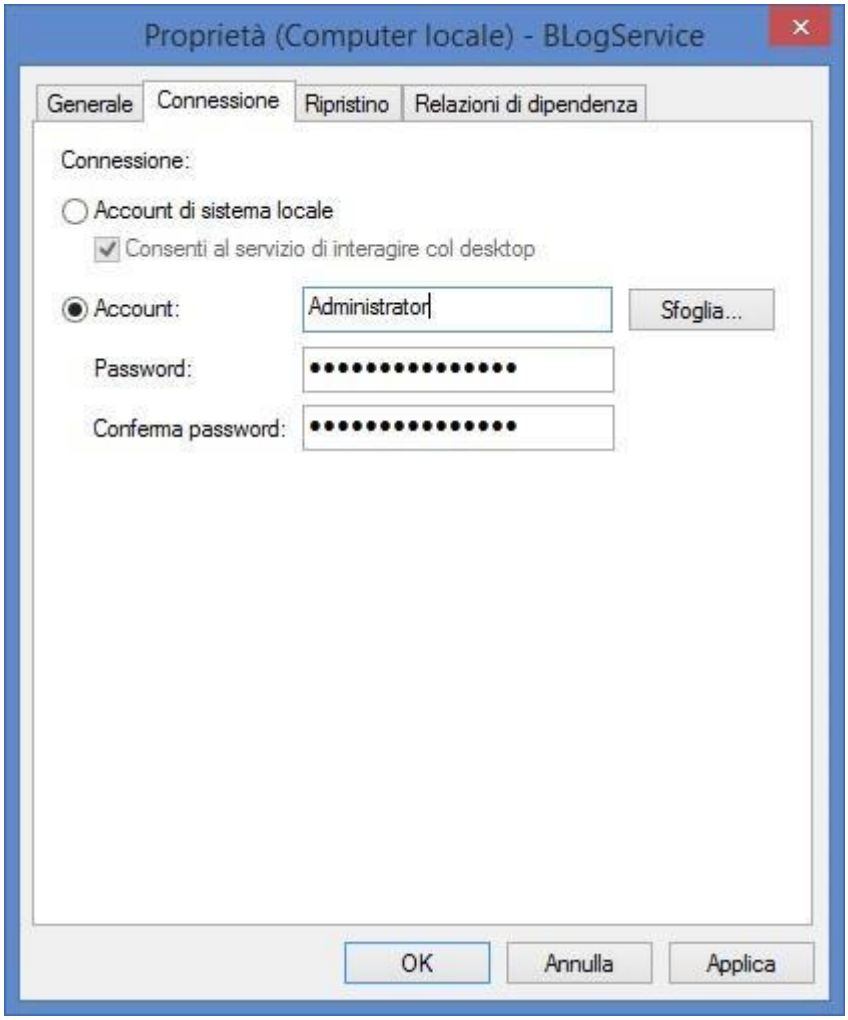
c:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe "C:\Program Files (x86)\Enterprise\BusinessLog\BLogService.exe"

Allo stesso modo, in caso di necessità, è possibile anche disinstallarlo con il comando:

Sc delete BlogService

Inoltre, è necessario **preparare il servizio appena installato** perché si possa avviare, in modo autonomo, con un utente "domain admin" in quanto deve possedere le credenziali per accedere al registro di sistema in tutte le macchine.

Occorre togliere l'accesso locale (potrebbe raccogliere solo i log dalla macchina locale) ed attivare:



Inserite utente e password di un account "domain-admin", ne potete creare anche uno "ad hoc" che abbia solo questa funzionalità:

- Accesso al Registro Eventi
- Accesso al servizio WMI e DCom
- Accesso al Registry
- Accesso alle share nascoste

Primo avvio

Il visualizzatore si dovrebbe avviare subito dopo il wizard, potrete sempre riavviarlo dal menu Start > BusinessLog

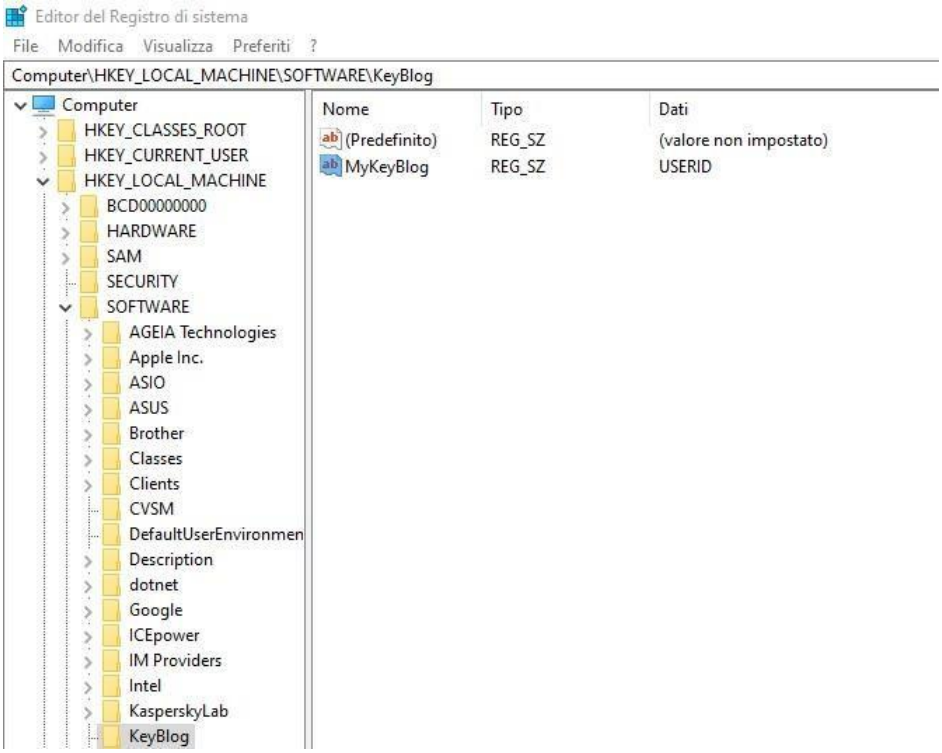
Il login chiede utente e password (l'avete già inserita nel wizard) per accedere al programma.

NB: se l'apertura della finestra del login impiega oltre 30 secondi è probabile che abbiate la porta TCP 13 verso in server NIST, non abilitata.

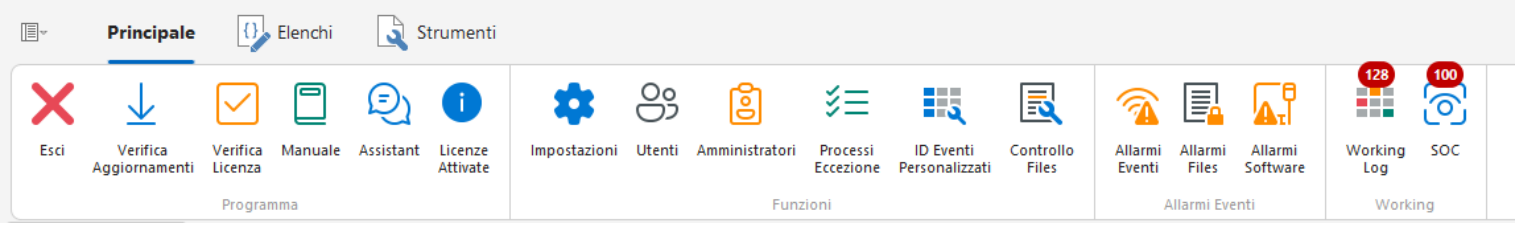
NB: **SE** in questa fase il sistema espone un errore di “Licenza Corrotta o Mancante” e propone, continuamente, il wizard iniziale, è segnale che la macchina non ha permesso di scrivere una chiave di registro:

[HKEY_LOCAL_MACHINE\SOFTWARE\KeyBlog]

"MyKeyBlog"="VOSTRO ID ASSEGNATO" (dovrete inserire lo UserID assegnato alla licenza)

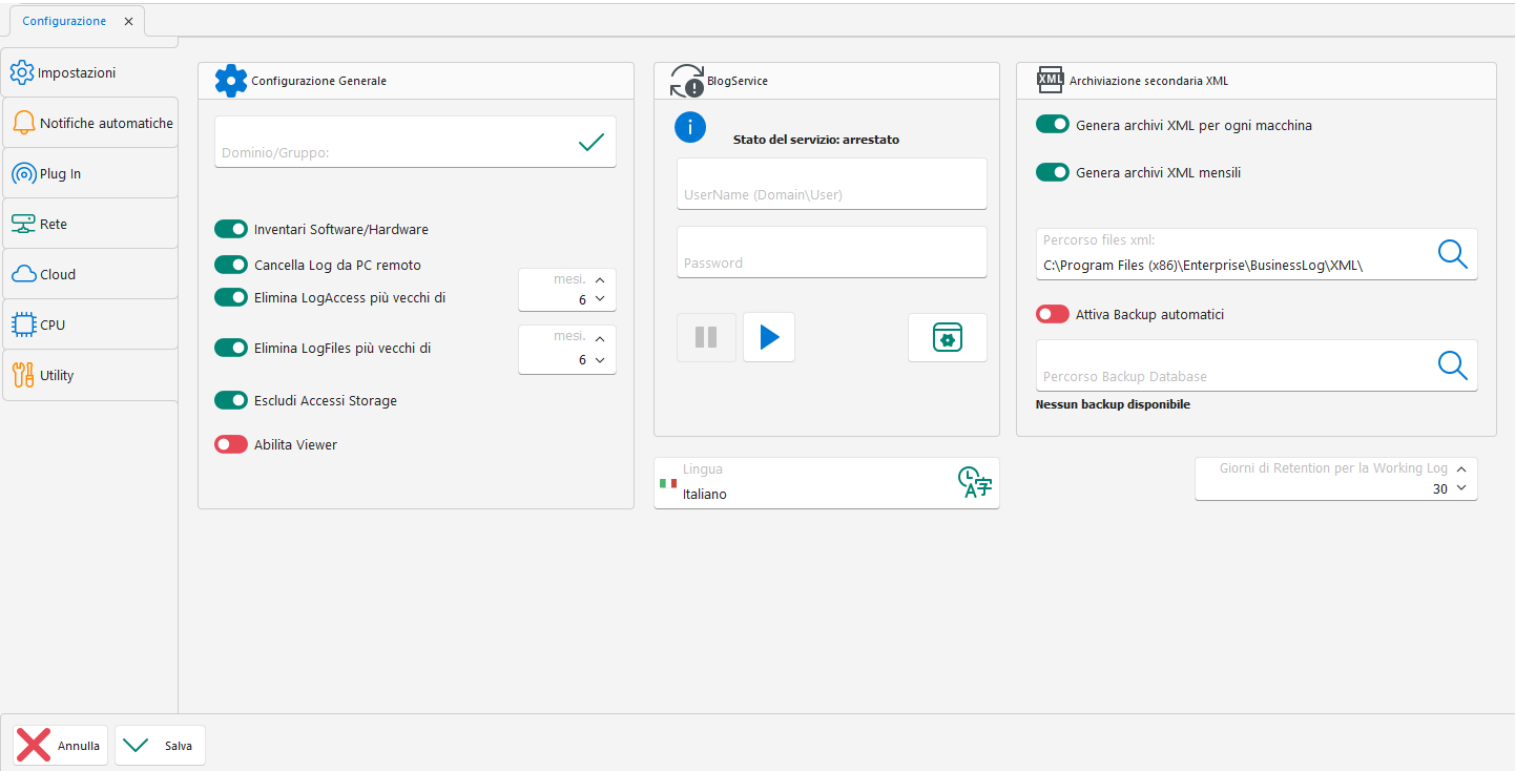


La prima schermata sarà simile a questa:



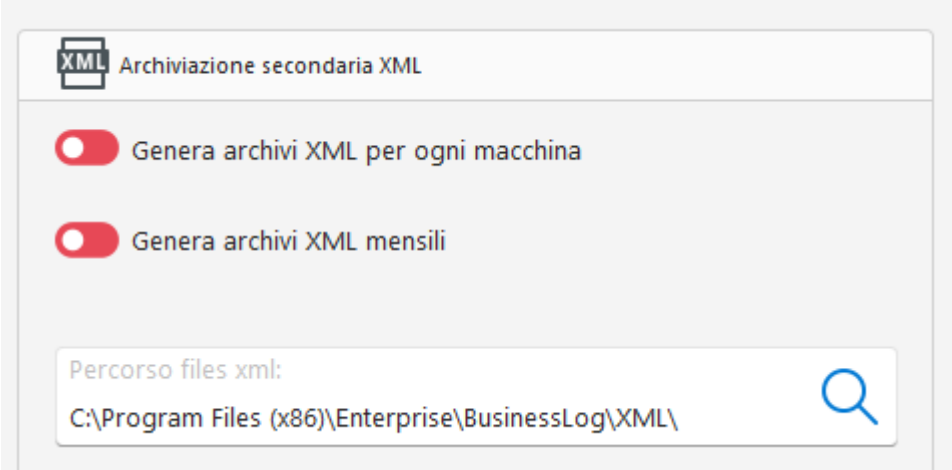
Niente paura, mancano solo pochi passi:

PER LA PRIMA APERTURA DEL PROGRAMMA fate clic su Impostazioni La finestra di configurazione appare così:



Lasciate le caselle predefinite così (potrete modificarle in seguito)

Andate poi nella sezione “Archiviazione secondaria XML”

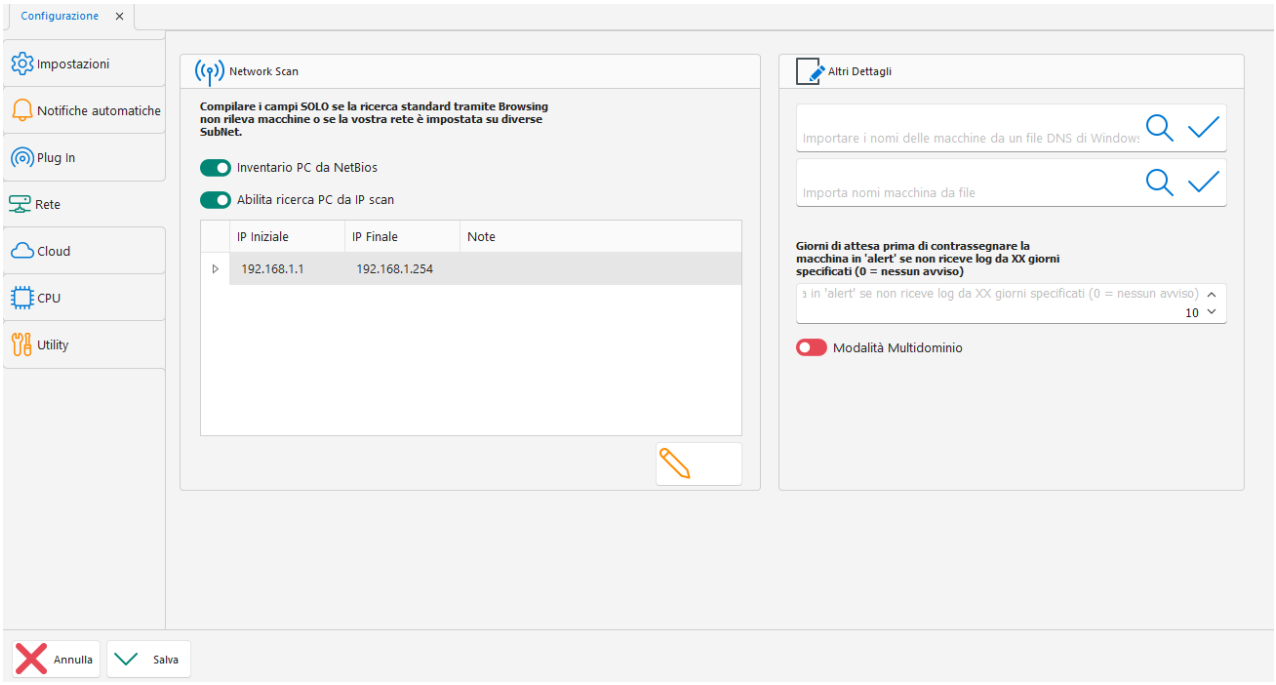


La finestra permette di generare dei files xml (crittografati) nella cartella specificata, in modo da avere una copia di sicurezza dei log registrati

Qui potete abilitare l’archiviazione crittografata (per macchina e/o mensile) e selezionare una cartella valida (attenzione ai permessi di scrittura), cliccando sull’icona.

Potete selezionare anche solo un’opzione: nel primo caso verranno un file per ciascuna macchina (divisi per anno), es: PC-MARIO-2022.xml, nel secondo caso un file per ciascun mese (es. 12-2022) con, all’interno, tutte le macchine di quello specifico mese.

Nella sezione “rete”

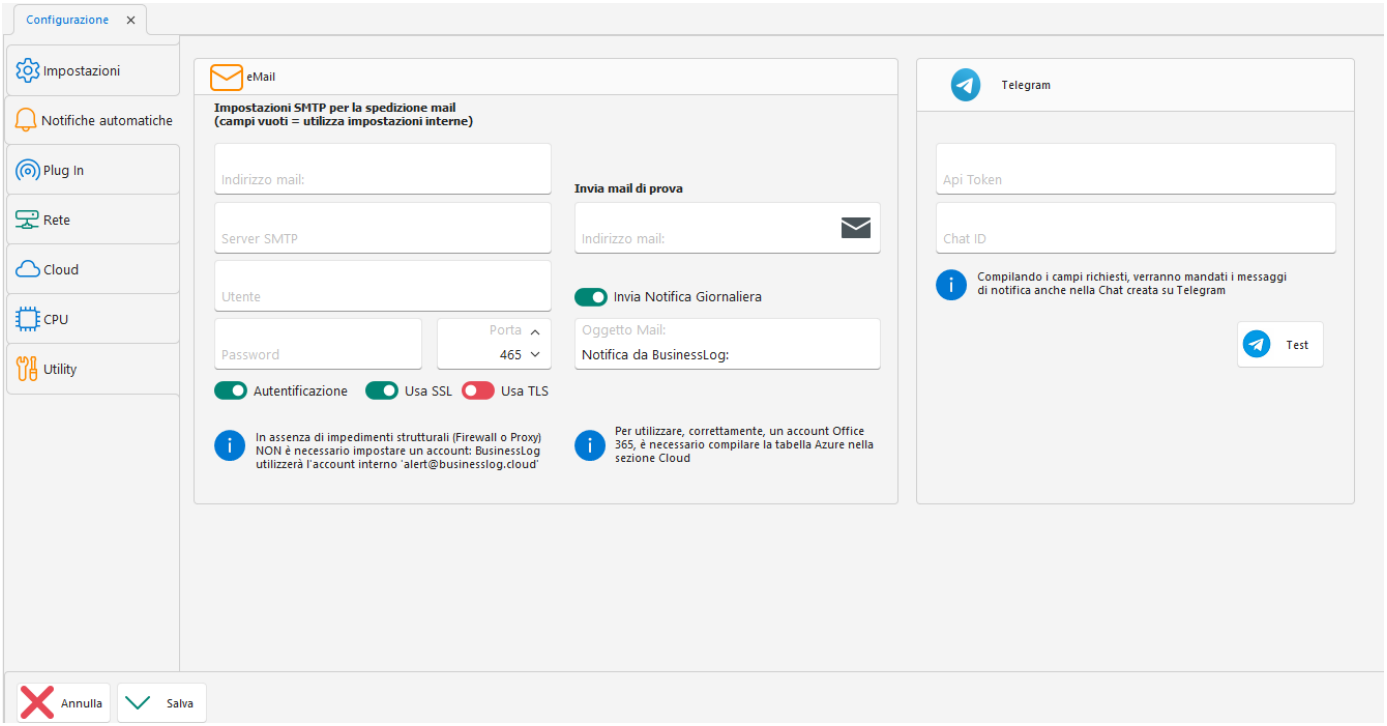


Specificate il tipo di ricerca delle macchine (eventualmente scrivete i range di IP di tutte le vostre subnet) premendo il pulsante [Ab]

Il box “Giorni di attesa” notifica, nell’elenco macchine e, con un riepilogo, nella mail di notifica serale, le macchine che, pur avendo ricevuto log nei giorni precedenti, non registrano log da X giorni (default = 10).

Modalità Multidominio: va attivata **SOLO** in caso di presenza di 2 o più domini (verranno inventariati i nomi PC con il suffisso dominio, es. PC-Mario.dominio1.local e PC-Mario.dominio2.local)

Nella sezione “Notifiche automatiche”



Le impostazioni mail attivano la notifica automatica serale in cui il programma spedisce una mail con:

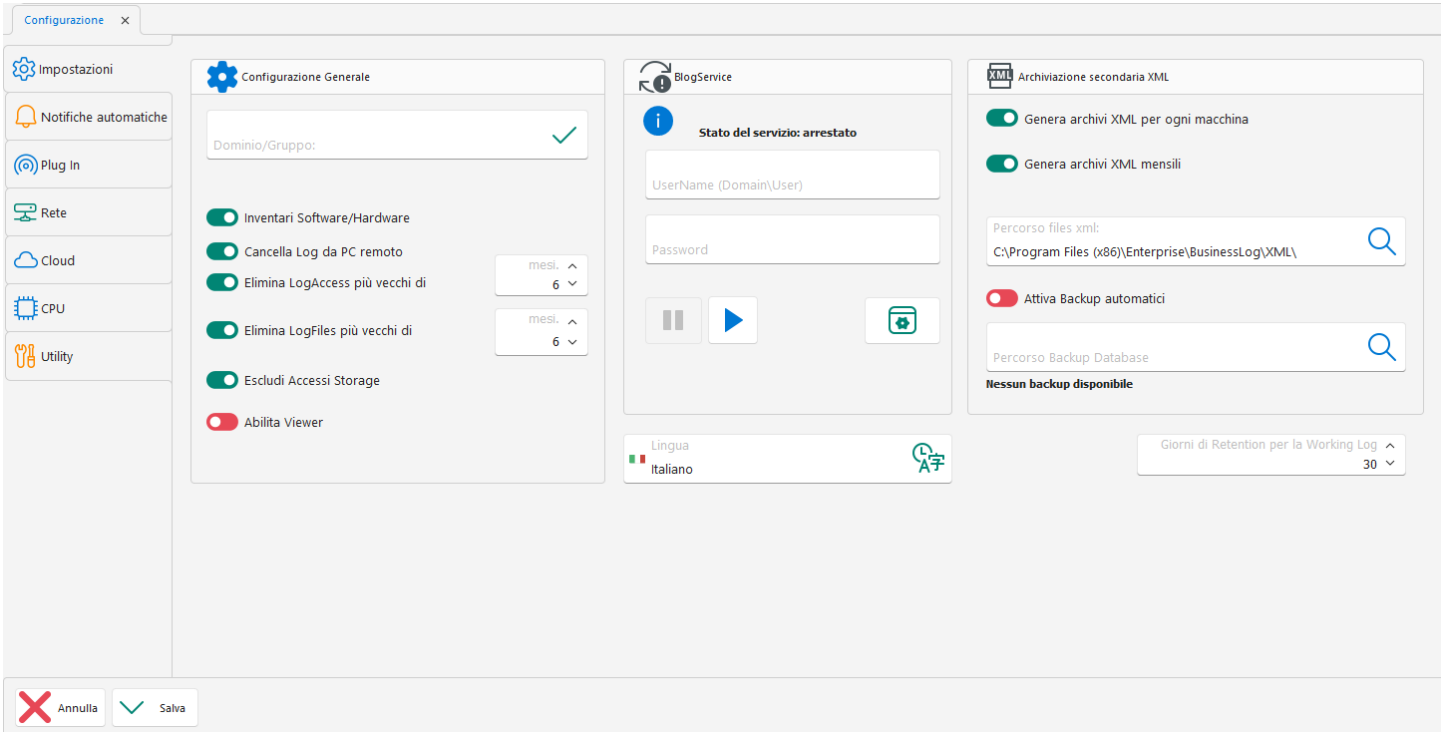
- Numero di log registrati e numero di log di Amministratori di Sistema
- Numero di tentativi d’accesso falliti
- Dimensione del database
- Variazioni significative di Registrazioni per ogni macchine
- Indicazioni sulle macchine che hanno smesso di registrare log da più di 10 giorni

Qui è possibile impostare, oltre ad un oggetto personalizzato, anche i parametri smtp con cui spedire la mail,

NB: BusinessLog ha un account interno con cui spedire le mail, specificate i parametri smtp **SOLO** se volete personalizzarli o se state utilizzando un proxy server per cui è necessario inserire le credenziali corrette.

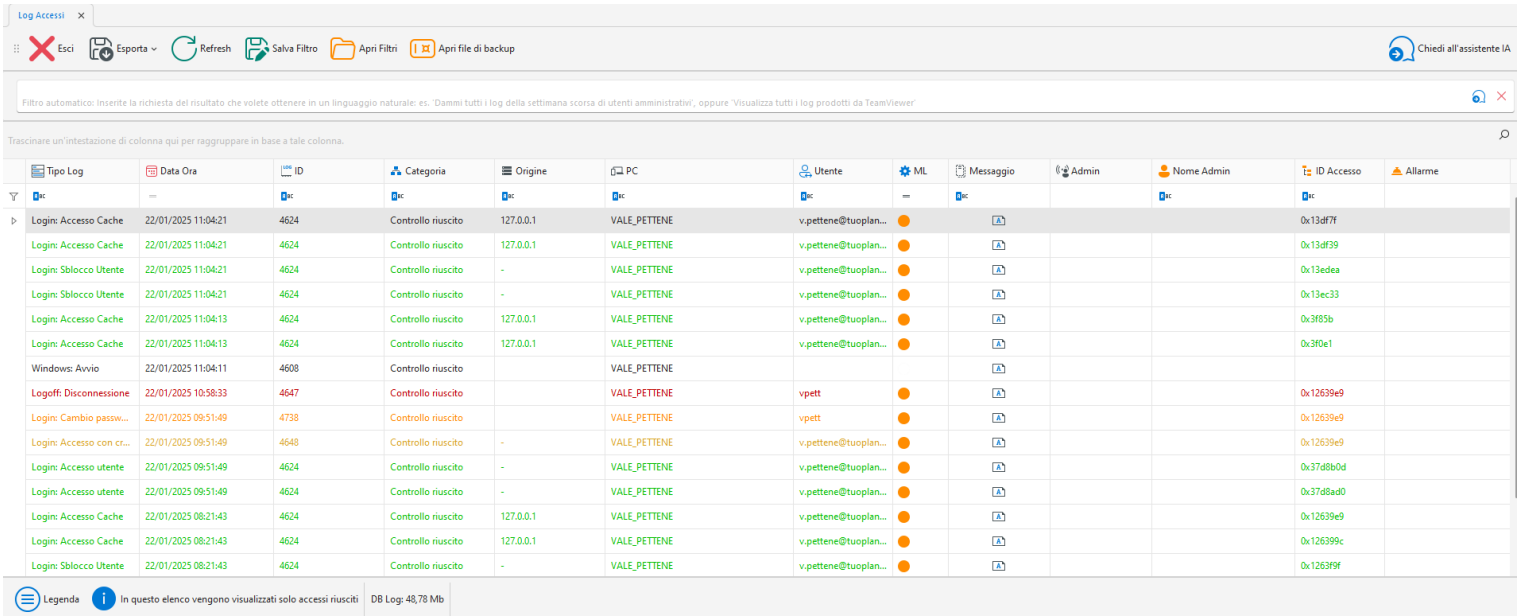
Nel caso, assicurarsi che la porta 465 sia autorizzata verso il server **mail.businesslog.cloud**

Tornate quindi nella sezione “Impostazioni” e fate partire il servizio (assicuratevi di aver seguito le istruzioni sulla preparazione del servizio)



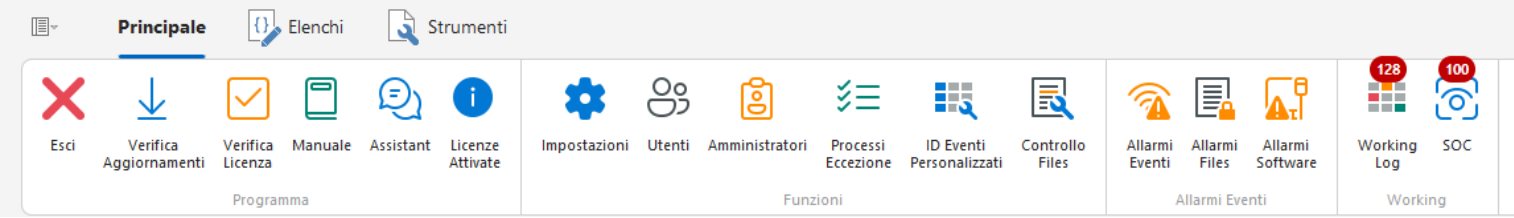
Dopo che il servizio sarà avviato i log cominceranno ad arrivare ed essere visibili nel visualizzatore.

Cliccando su [Log Accessi]

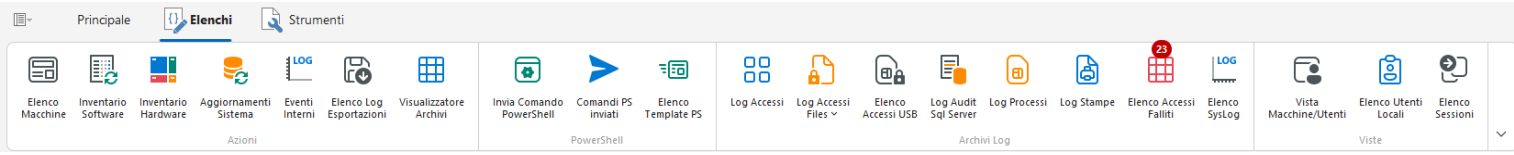


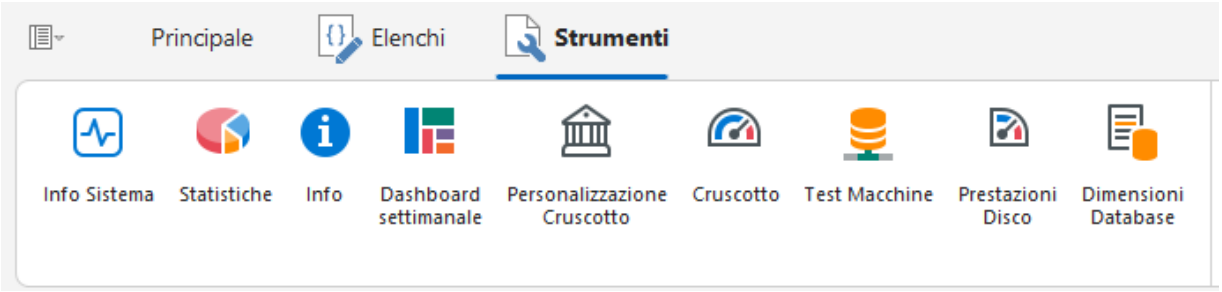
L’interfaccia

Il menu si presenta molto semplice e con un layout simile a quello di “Office”



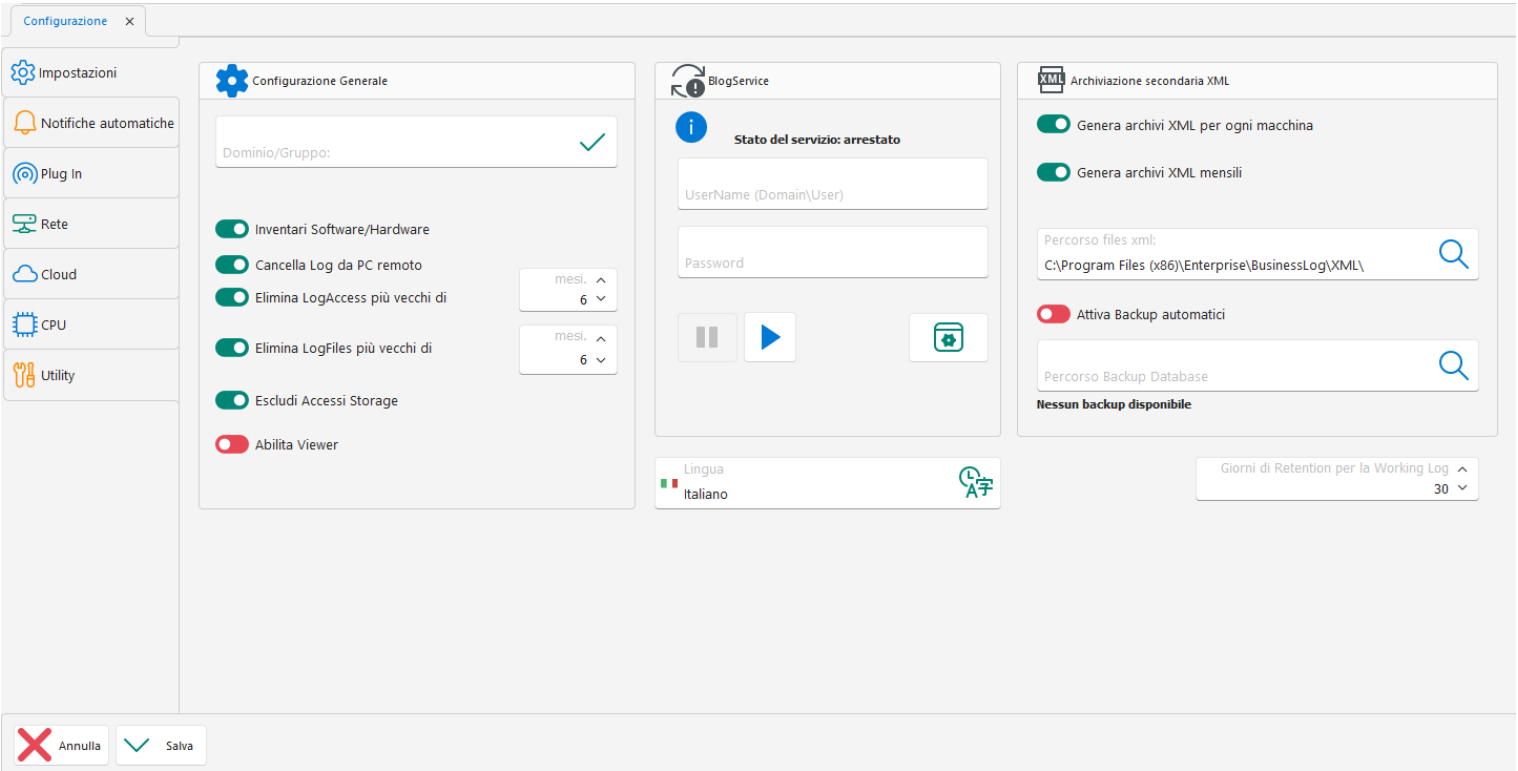
Cliccando nelle linguette vicino alla “Principale” appariranno le seguenti categorie:





Impostazioni e configurazione

Cliccando nelle sezioni si apriranno le relative finestre o funzioni:



Dominio/Gruppo: Il vostro dominio o gruppo (è automatico, non è obbligatorio specificarlo)

Inventari Software/Hardware: il programma andrà a rilevare le informazioni extra delle macchine (programmi, aggiornamenti, cpu, sistema operativo, ecc…)

Cancella Log da PC remoto: consente di cancellare il registro “Applicazioni” e “Sicurezza” nei PC client in modo da velocizzare le prossime scansioni.

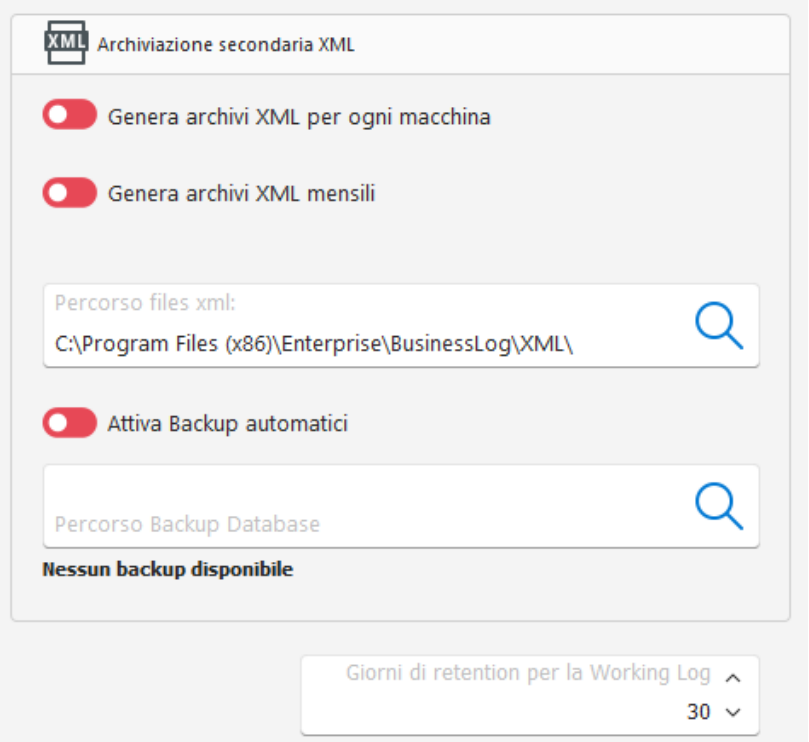
Elimina LogAccess più vecchi di XX mesi: Al termine di ogni scansione il programma andrà ad eliminare i log access più vecchi di XX mesi, come impostato (ovviamente il numero minimo e 6)

Elimina LogFiles più vecchi di XX mesi: Al termine di ogni scansione il programma andrà ad eliminare i log access dei files più vecchi di XX mesi, come impostato (ovviamente il numero minimo e 6)

Abilita Viewer: Se selezionato consente l’avvio del server Name Pipes e la connessione della versione Viewer da installare in rete.

Escludi Accessi Storage: evita la registrazione dei “login speciali” effettuati dai software di backup.

Archiviazione Secondaria



L'archiviazione secondaria registra gli stessi log su files xml crittografati, gli archivi possono essere utilizzati sia per un backup di sicurezza, sia per confronto ai log registrati nel database principale.

Genera archivi per ogni macchina: attiva la registrazione secondaria su files xml crittografati.

Esegue archiviazione mensile: se selezionata verrà prodotto un ulteriore archivio del mese precedente.

Percorso files xml: la cartella in cui verranno archiviati i files xml

Giorni di retention per la Working Log: Giorni in cui vengono conservati i log per la griglia WorkingLog (consigliati 30 giorni, NON impostate una retention inferiore ai 14 giorni per consentire un efficace controllo della Machine Learning)

Attiva Backup automatici: Attiva la procedura automatica (notturna) per le operazioni di Manutenzione, Compattazione ed Archiviazione dei db

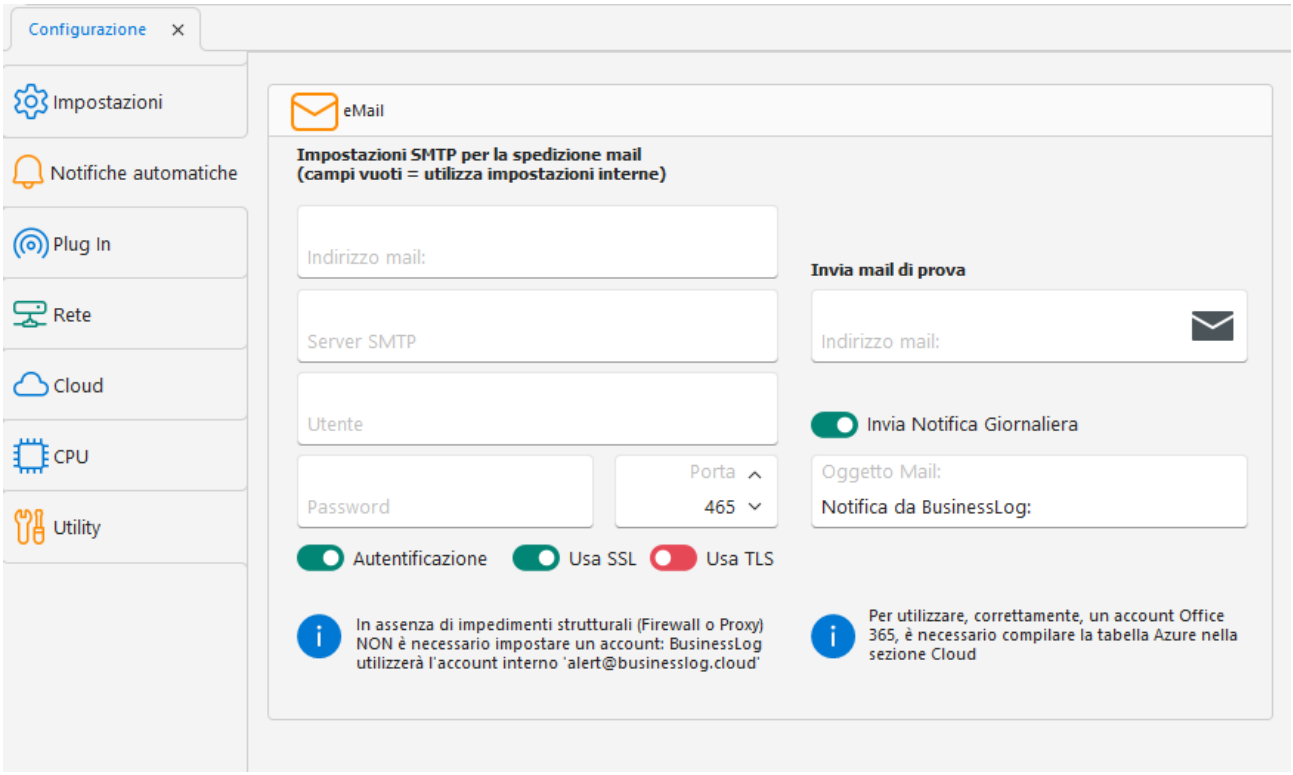
Attivando l'opzione, ogni notte il sistema CHIUDE tutte le procedure (anche l'interfaccia di BusinessLog, se operativa) ed esegue le seguenti operazioni per tutti i db:

- Riparazione preventiva (ripara un db con righe corrotte)
- Compattazione (libera lo spazio non assegnato nel db)
- Backup (esegue un backup e sposta i files. BackupCopy nella cartella specificata)

Al termine delle operazioni, i servizi vengono fatti ripartire automaticamente, queste operazioni potrebbero impiegare molto tempo, fate riferimento al file regBack.log per valutarne le tempistiche.

NB: I processi Syslog e RTServer NON vengono interrotti per assicurare la continuità delle ricezioni.

Notifiche automatiche



BLog2022 ha già un utente interno per le spedizioni, se volete personalizzarlo o la vostra azienda permette di spedire SOLO da determinati account è necessario compilare tutti i campi

È possibile testare il funzionamento scrivendo una casella esistente e cliccando sul pulsante a fianco nel box “Invia mail di prova”.

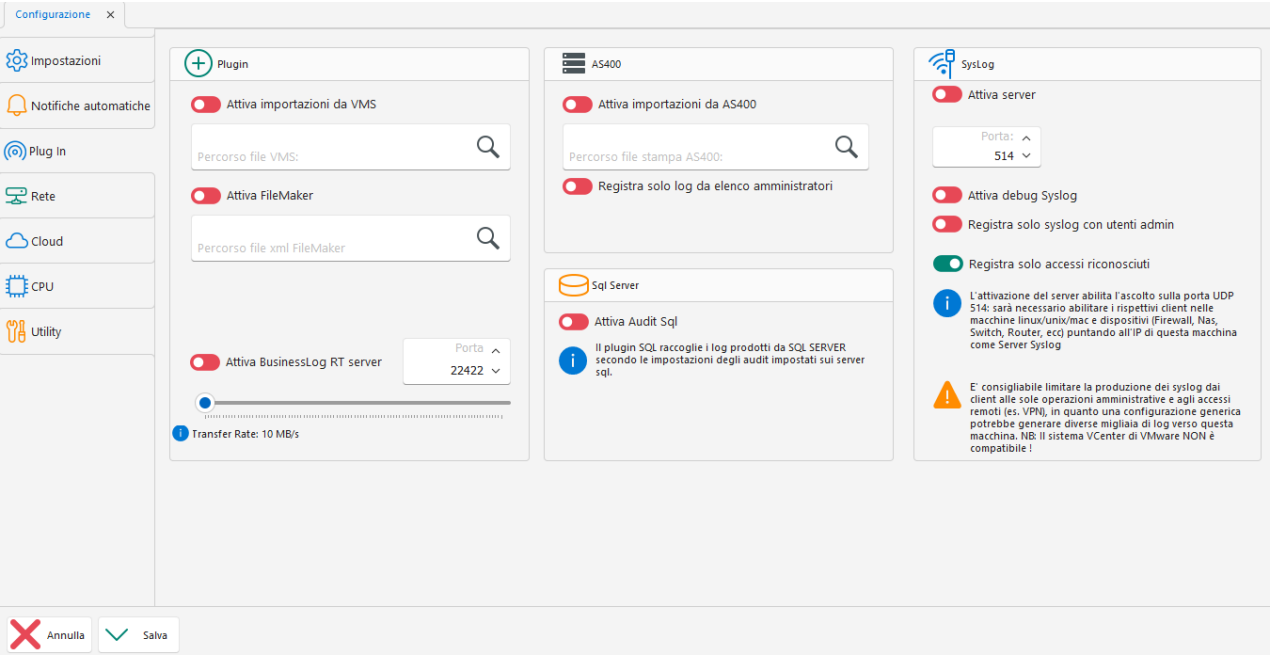
- Invia Notifica Giornaliera:

Attivando l’opzione, viene mandata una mail quotidiana con un piccolo riepilogo dei log raccolti (e quanti come amministratore) e la dimensione del db raggiunta.

Verranno aggiunti gli eventuali “tentativi d’accesso falliti” causati da login di sistema o su SQL server è possibile personalizzare l’oggetto della mail con un testo specifico.

NB: Nel caso sia necessario l’utilizzo di un account Office365, è indispensabile compilare la tabella “Azure”nella sezione Cloud !

Plugin



Attiva importazioni da VMS: Attivazione/Disattivazione da client VMS

Percorso file VMS: Le macchine HP VMS generano i propri log su files preformattati, nelle macchine sarà necessario orientare questi files su un'apposita cartella, qui indicheremo la cartella al programma che

servirà a prendersi i files ed interpretarli all'interno del programma.

Attiva importazioni da AS400: Attivazione/Disattivazione importazione AS400

Percorso file stampa AS400: L'acquisizione dei log da sistemi AS400 avviene tramite una schedulazione del comando DSPLOG che manda in stampa i log di sistema interni su una PRT configurata in modo che possa stampare su un file di testo. Il percorso deve puntare ad una cartella in cui vengano depositati questi files. (è bene farsi seguire da un sistemista AS400)

Attiva BusinessLog RT Server: Attiva o disattiva l'acquisizione da BusinessLog RT

Porta RT: La porta TCP utilizzata dai client RT (predefinita 22422)

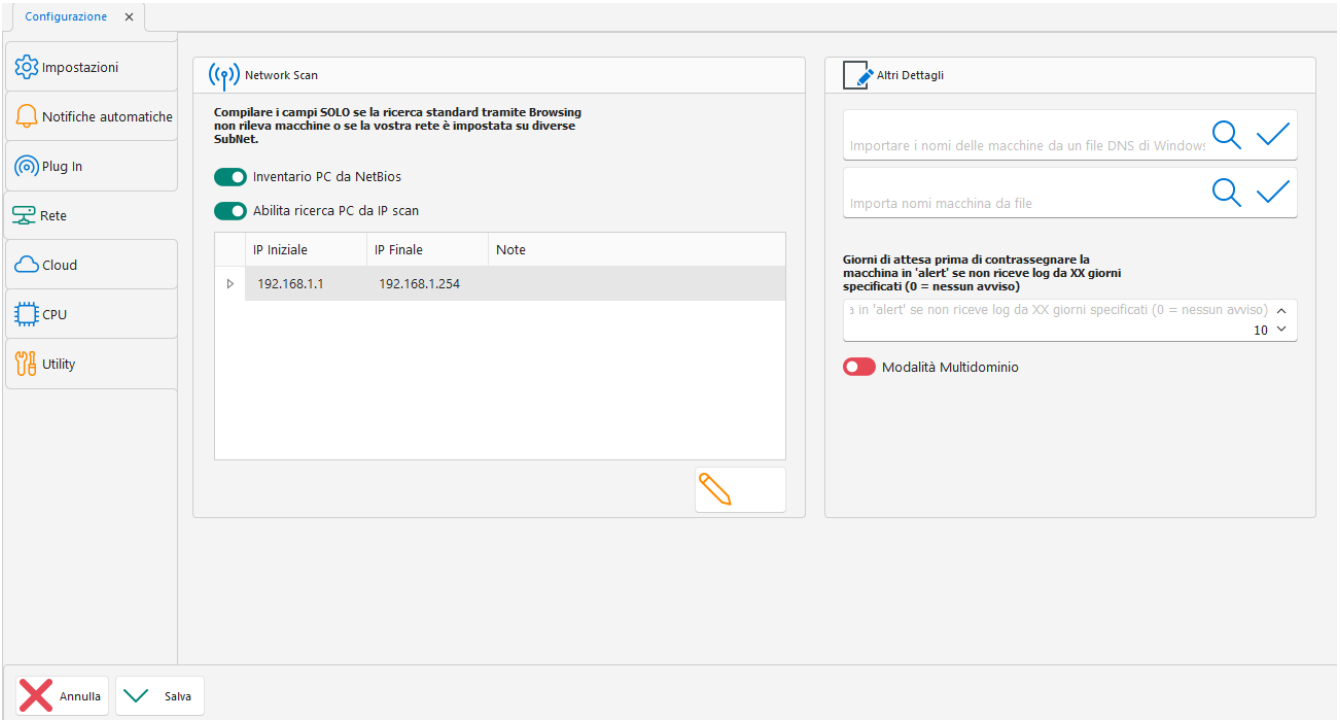
Transfer Rate RT: La banda utilizzata per il transfer rate dei files RT attraverso TCP

Percorso FileMaker: Attivando l'opzione e specificando un percorso verranno acquisiti i log prodotti da FileMaker.

Attiva Audit SQL: Attiva l'acquisizione dai files esportati dal sistema di audit di Sql Server

Attiva Server: L'attivazione del server attiva l'ascolto sulla porta UDP 514. Sarà necessario abilitare i rispettivi client nelle macchine e nei dispositivi interessati, puntando all'IP di questa macchina come Server Syslog

Rete



Inventario PC automatico: al termine di ogni scansione, il programma aggiornerà l'inventario PC delle macchine rilevate in rete utilizzando NetBios (verificare che sia attivato nella macchina server)

Abilita ricerca PC da IP scan: Attiva l'autoriconoscimento da scansione "passo-passo" per ogni IP, occorre impostare un IP iniziale e un IP finale, e utile soprattutto se si utilizzano subnet diverse.

MultiDominio: In caso sia necessario importare il nome completo (NOMEPC.DOMINIO.COM) se disattivato importa il nome semplice (NOMEPC). ATTENZIONE: Da utilizzare SOLO in presenza di una rete MULTI- DOMINIO, attivandolo in un secondo momento potreste trovare molte macchine doppie nell'elenco macchine (con e senza suffisso)

Importa nomi macchina da file esportato Windows DNS: Permette di importare una lista di host dall'esportazione standard di Windows DNS (dal server DC).

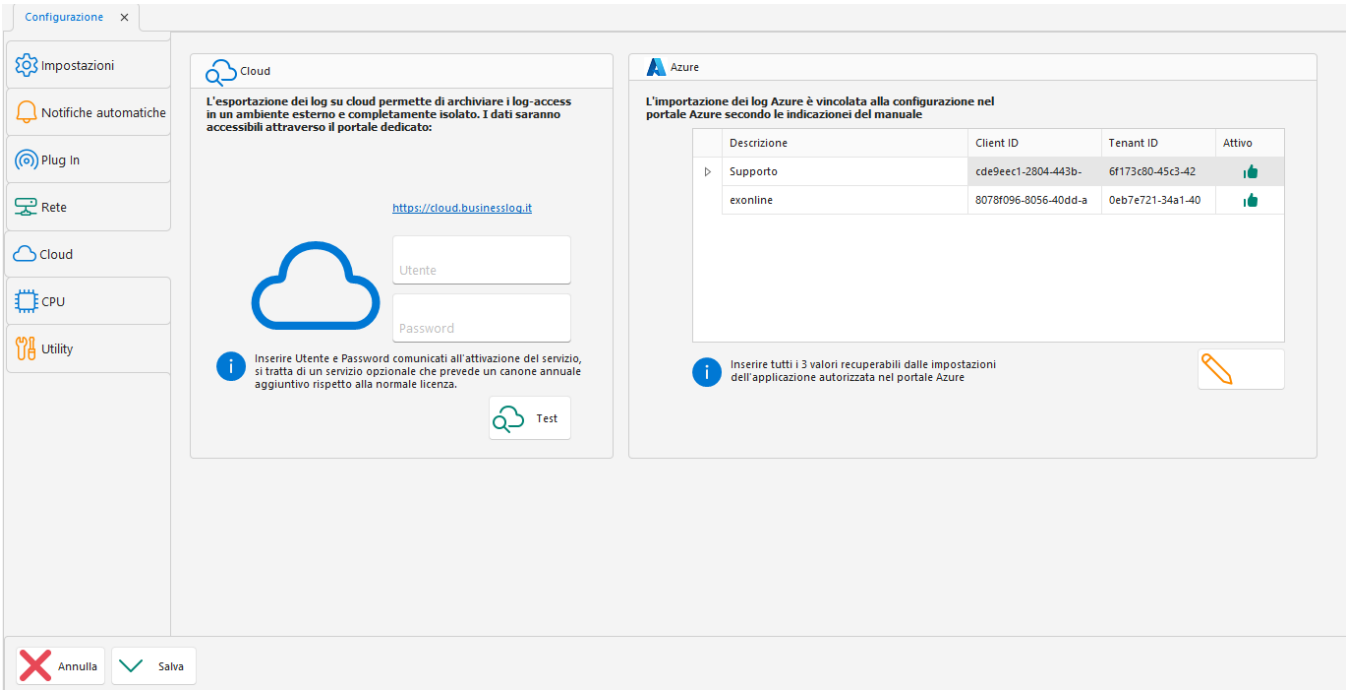
Importa nomi macchina da file: È simile alla funziona DNS ma permette di importare i nomi macchina da una lista "libera" utilizzando anche altri tool, il formato del file dove essere a singola colonna, es:

PC1
PC2

Se si intende far eseguire la scansione delle macchine con uno o più range di IP, cliccare sul pulsante di modifica:

In alert se non riceve log da XX giorni: consente di contrassegnare la macchina in alert se per XX giorni scelti, non si ricevono log

Cloud



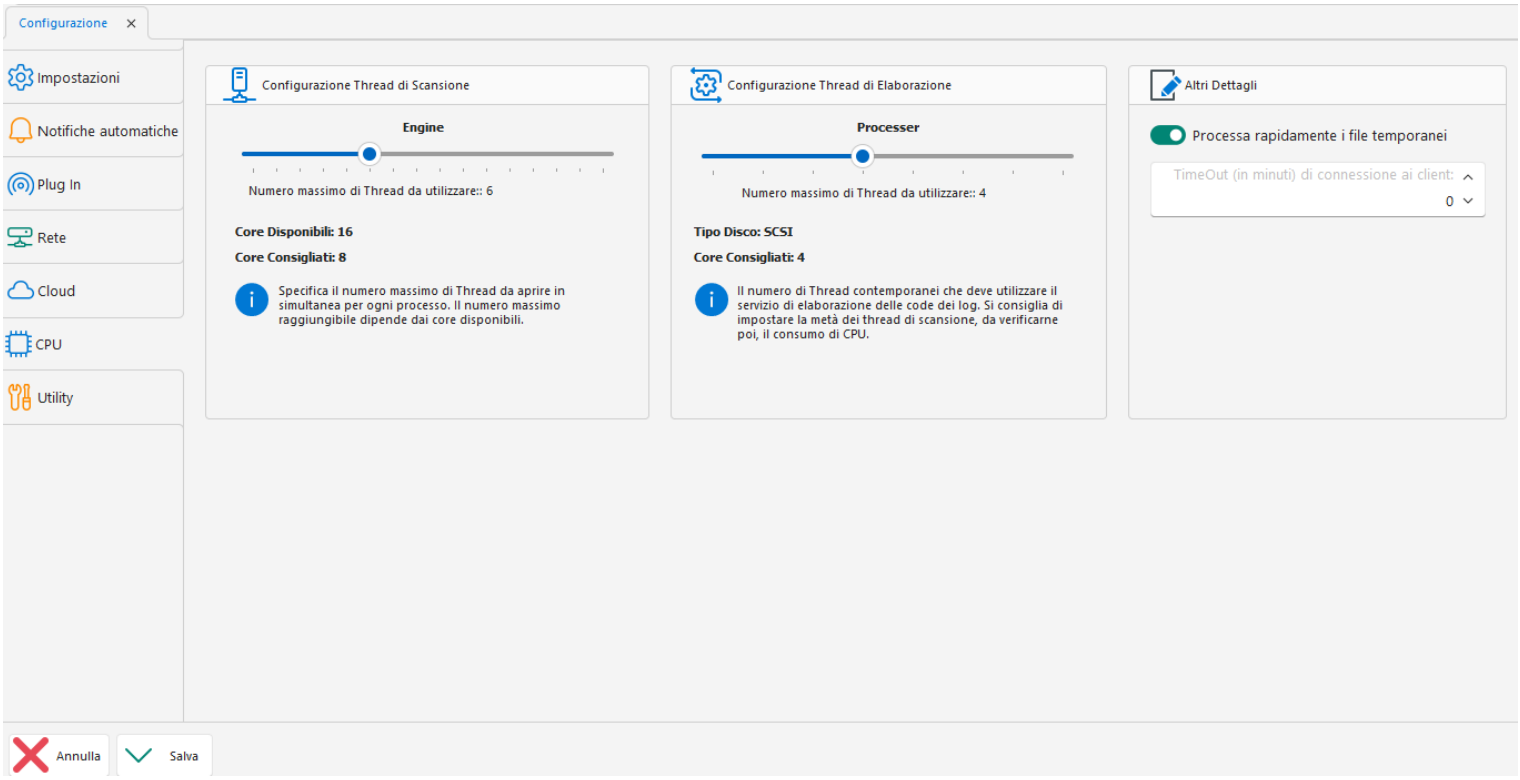
Se avete attivato l'opzione "Cloud" il programma sarà in grado di copiare una copia dei log rilevati in un database cloud esterno al sistema ed accessibile da un portale web (http://cloud.businesslog.it) anche dall'esterno.

È possibile testare la connessione utilizzando il pulsante "Test"

NB: per poter utilizzare l'archiviazione cloud è necessario aprire la porta TCP 1433 nell'eventuale firewall.

Inoltre, è possibile attivare l'importazione dei log Azure, che sarà vincolata alla configurazione nel portale Azure secondo le indicazioni del manuale

Impostazioni Cpu



Numero massimo di thread da utilizzare (ENGINE): il numero massimo è impostato in base ai processori disponibili, praticamente è il numero di macchine (windows) in scansione contemporaneamente, ad ogni ciclo

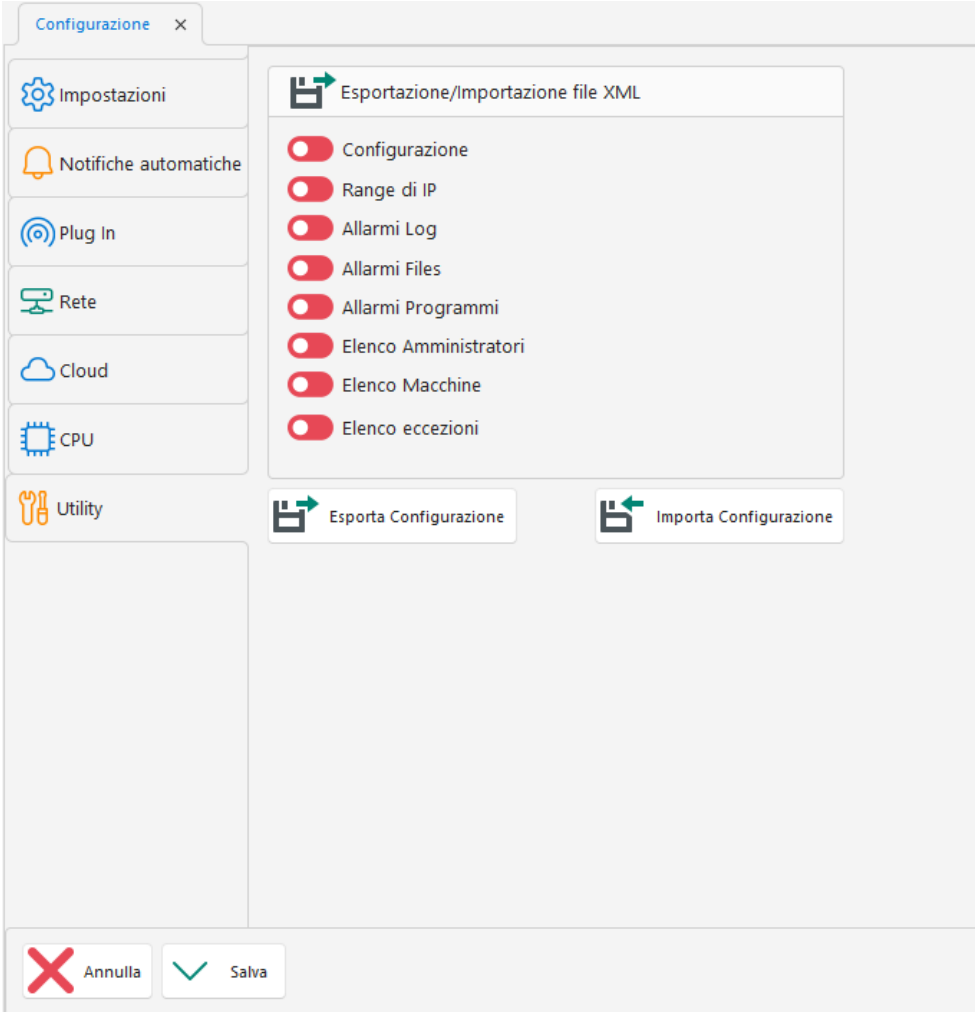
Numero massimo di thread da utilizzare (PROCESSER): il numero massimo di thread da utilizzare per il processamento dei files temporanei, può influire molto sulla velocità di registrazione ma occorre valutare attentamente l'impatto con la macchina per evitare errori di scrittura nel db (da evitare assolutamente),

Solitamente si consiglia un numero 2 volte inferiore all'ENGINE, ma dipende molto dalle prestazioni del disco fisso.
(Sata e Sas avranno prestazioni molto più basse di un SSD/M2)

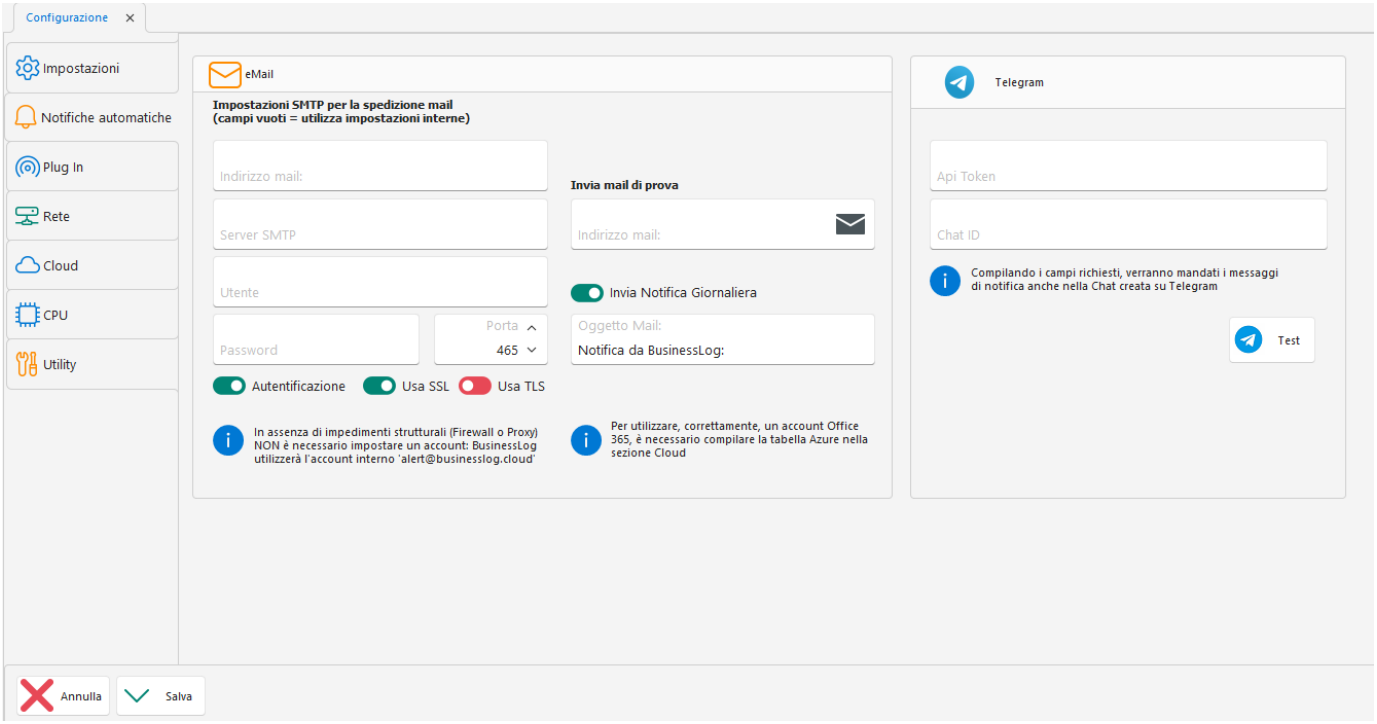
Processa rapidamente i file temporanei: Il sistema processa i file temporanei ogni 100 scritture, accelerando la visualizzazione nel visualizzatore.

Timeout: Imposta un timeout (in minuti) che forza la disconnessione dal client dopo il tempo impostato. 0 = Nessun Timeout.

Questa sezione permette di esportare o importare le configurazioni in caso di migrazione o backup



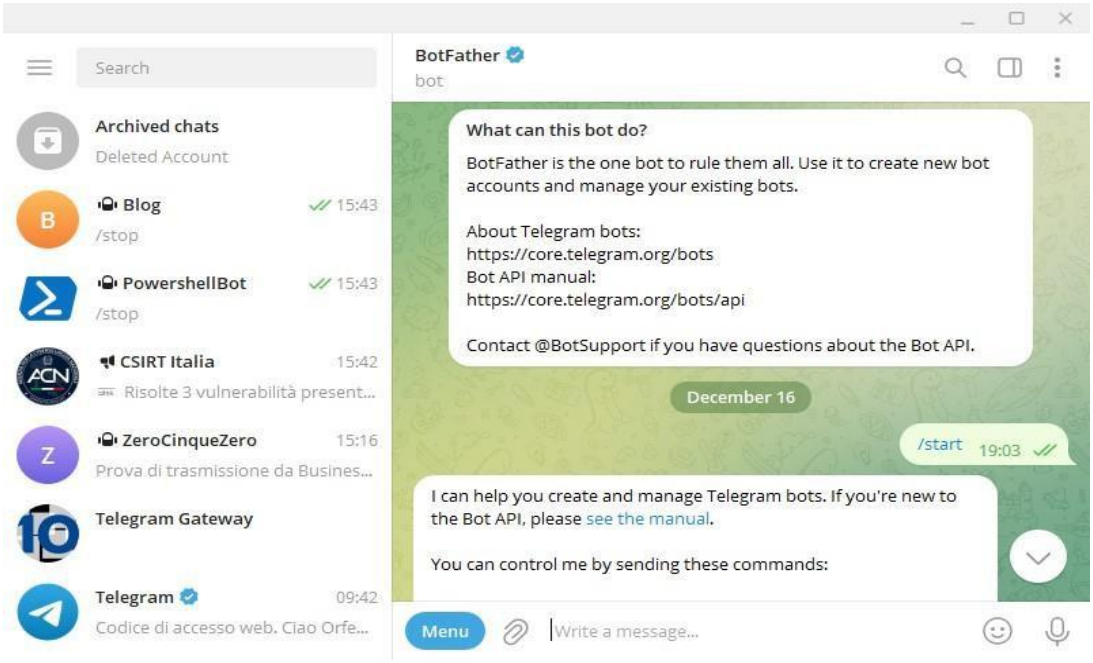
Notifiche automatiche Telegram



BusinessLog è in grado di comunicare con Telegram attraverso una ChatBot che potete configurarvi in pochi minuti

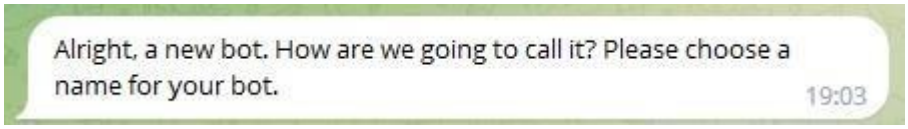
Aprite l'app Telegram (dal vostro telefono o dalla versione desktop) Cercate

"BotFather" e aprite la chat:



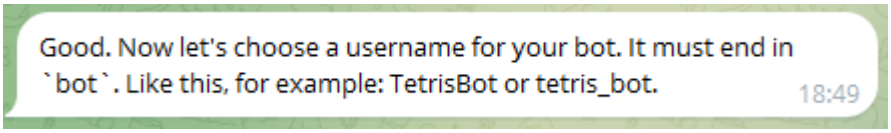
Con **BotFather** di Telegram Create un nuovo ChatBot, una volta entrati scri-

vete **/newbot**



Scrivete un nome per il vostro bot (ad esempio “aziendabot”) se già utilizzato, verrete invitati ad inserirne uno nuovo.

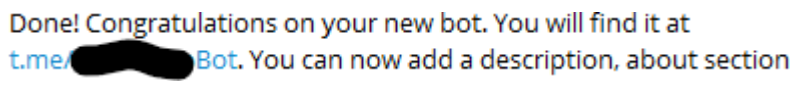
Ora otterrete:



Inserite un NomeUtente per il vostro Bot, ad esempio “UtenteAziendaBot” (deve terminare con “Bot”)

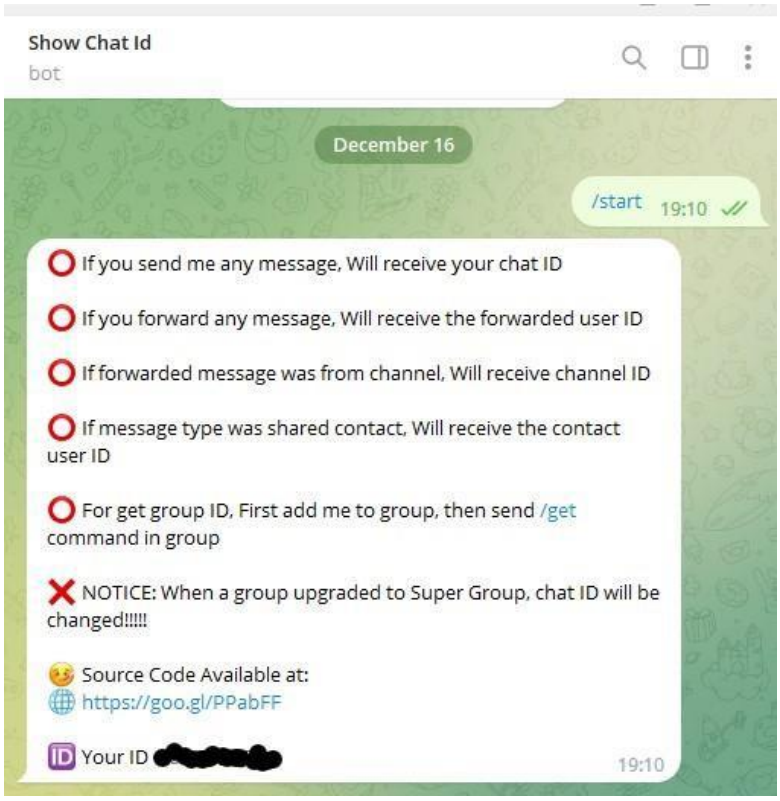
Otterrete:

Annotatevi la chiave che sarà la vostra **API TOKEN**



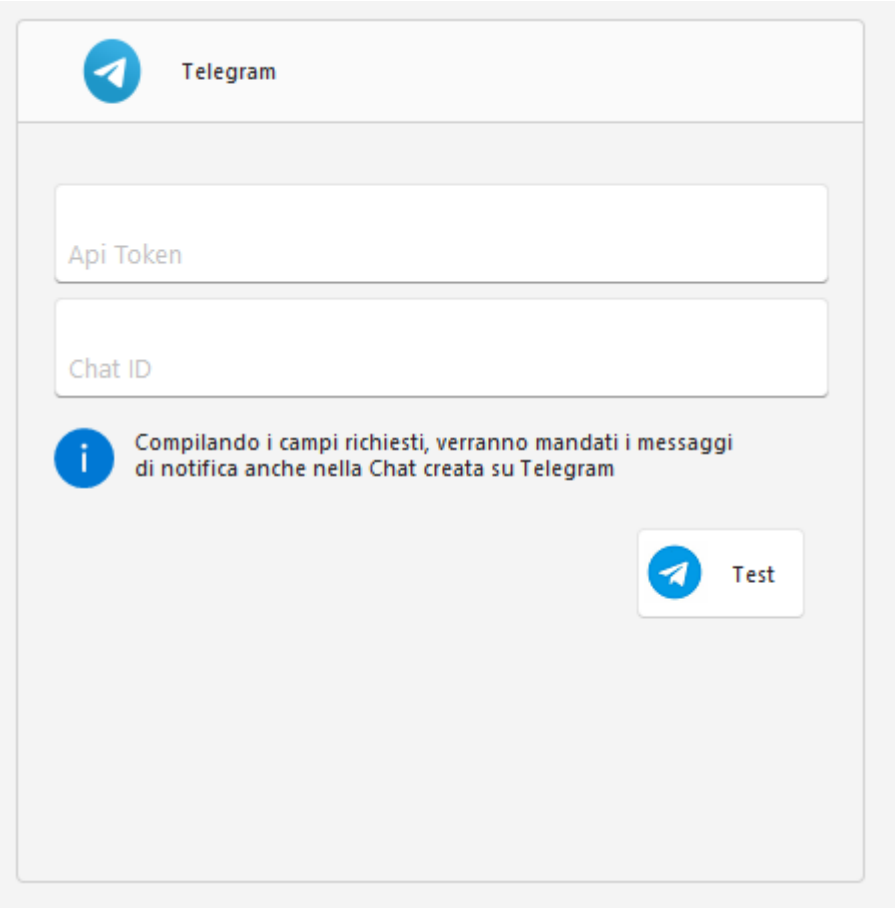
Seguite il link che vedete nella parte superiore (tipo t.me/CHATBOT) e cliccate su “Avvia”, nel caso scrivete /start per avviare il bot.

Adesso, cercate, sempre in Telegram “Show Chat Id”



Annotate, qui il “vostro ID” in calce che sarà il vostro **CHAT ID**

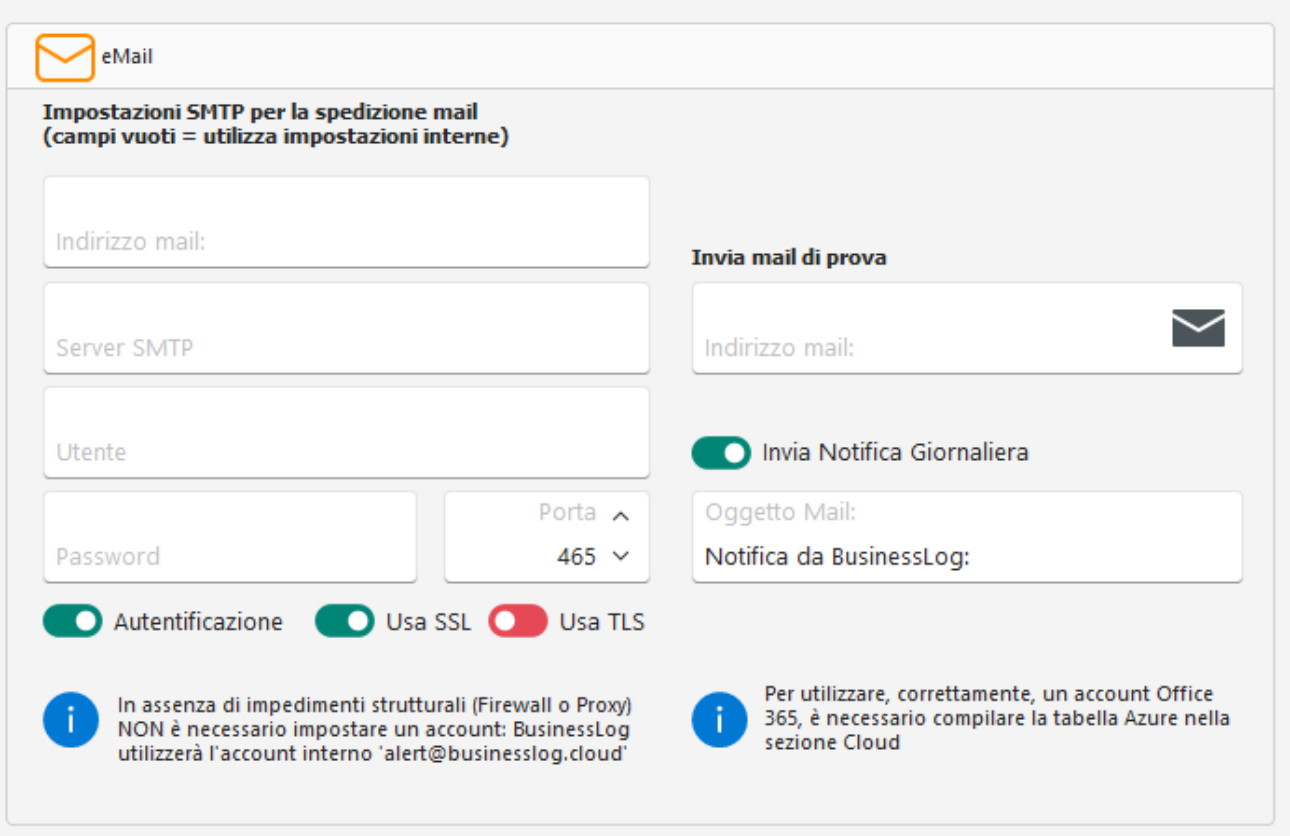
Ora in BusinessLog > Impostazioni > Notifiche automatiche > Telegram potete inserire i dati necessari:



Inserite i 2 parametri appena ottenuti, Salvate, tornate nella schermata e fate clic su “Test” Dovreste ricevere un messaggio con tanto di notifica, nel caso di errore, rivedete la prima parte. Queste informazioni, se compilate, saranno utilizzate per mandare le notifiche via Telegram Verificate che, nella macchina, sia possibile raggiungere l’url https://api.telegram.org/bot

Invio Mail con caselle Office 365

Nel caso sia necessario l'utilizzo di un account Office 365 nelle impostazioni di invio mail, è necessario operare in più punti, in quanto Microsoft non permette più l'utilizzo di smtp SENZA autorizzazione nel tenant Azure.



Passo 1:

Impostate la casella O365 come "Indirizzo mail" e "Utente" Impostate nel "Server SMTP": smtp.office365.com Completate con la Password nella relativa casella

Porta: 587 Autentificazione = Sì

Usa SSL = No

Usa TLS = Sì

Passo 2:

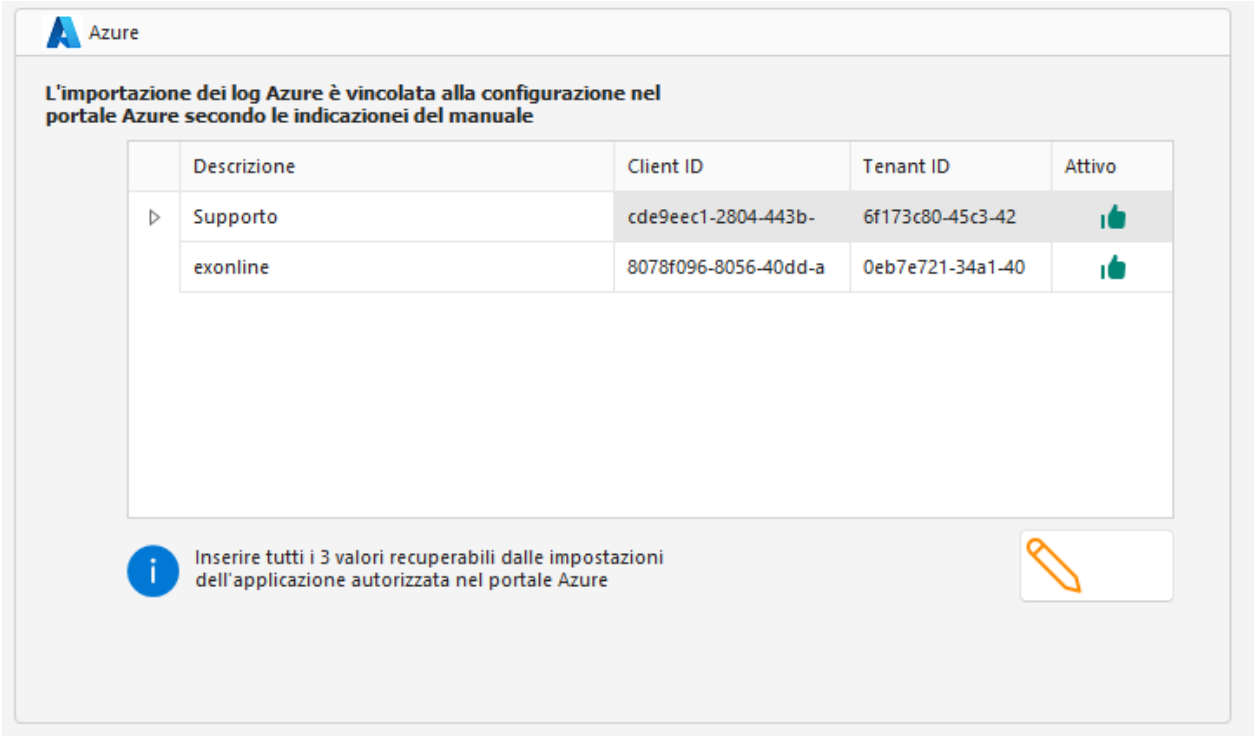
Come per la procedura Registrazione log Azure (pag 66)

È necessario autorizzare l'applicazione a livello di Tenant ed ottenere i permessi su Graph per:

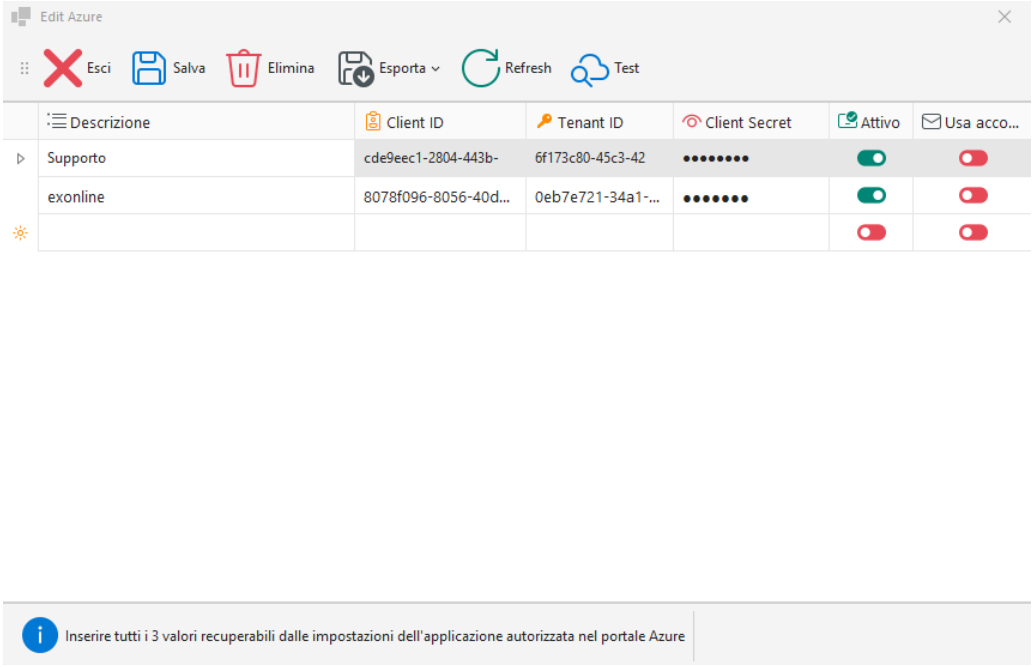
Mail.send

Passo 3:

Nelle impostazioni > Cloud > Azure cliccare sulla “penna” in basso



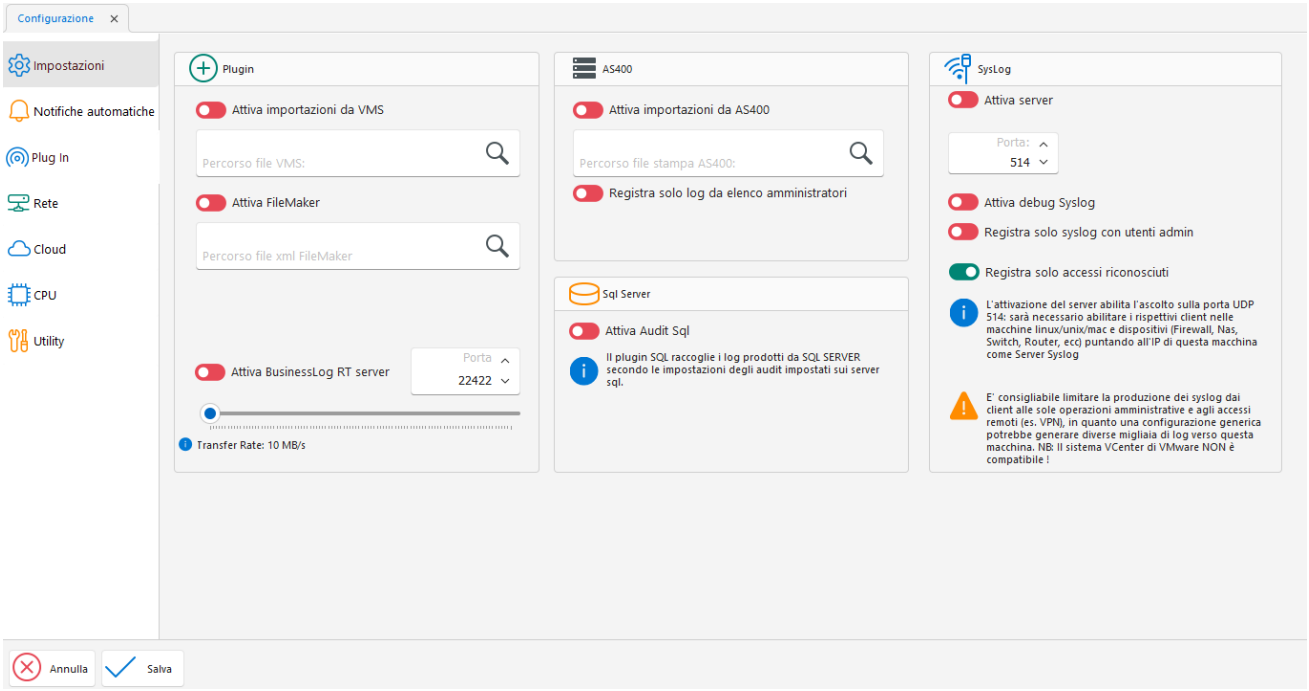
Si aprirà la finestra:



Inserire i 3 parametri specificati nel tenant azure e selezionare l’opzione “Usa account mail” nel rispettivo Tenant, la casella mittente DEVE far parte dell’AD (Entra ID) di Azure!

Syslog

Con il connettore Syslog è possibile acquisire log da qualsiasi macchina/dispositivo NON windows: Lato BusinessLog sarà sufficiente attivare il server



Attiva server: BusinessLog ha un suo SysLog server integrato (avviato sempre dal servizio) attivando l'opzione si potrà convogliare i syslog generati dai dispositivi verso l'IP di questa macchina.

Porta: viene già specificata la porta predefinita, è possibile, comunque, specificare una porta personalizzata (attenzione che dovrà essere la stessa anche per i client). La predefinita e UDP 514

Attiva debug syslog: se selezionato, attiva la scrittura, in modalità "raw" in un file specifico che troverete nella sottocartella "Reg": RegSysList.log

Registra solo syslog con utenti admin: i syslog potrebbero generare centinaia o migliaia di log al giorno e non tutti i dispositivi permettono di filtrarne i log in uscita. Attivando questa opzioni il programma riceverà tutti i log ma andrà a registrare solo quelli relativi alle utenze specificate nella tabella "Amministratori"

Dopo l'attivazione, riavviando il servizio, noterete l'avvio del processo BusinessSysLog.exe che è il listener in ascolto sulla porta.

ATTENZIONE: NON è possibile utilizzare più di un listener in ascolto sulla stessa porta, per cui se utilizzate altri software per la registrazione dei syslog sarà necessario disattivarli (o modificare la porta)

Una volta abilitato il syslog server, sarà necessario accedere alle macchine (linux/unix/mac) per attivare il CLIENT syslog (fate riferimento alla documentazione di ciascuna distribuzione per scoprire le funzionalità di attivazione)

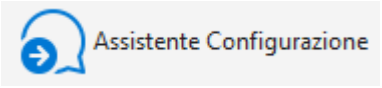
Per i dispositivi potete accedere all'interfaccia amministrativa, cercare la sezione syslog e configurare l'invio dei log VERSO l'IP della macchina che ospita BusinessLog (attenzione al protocollo, deve essere UDP)

CERCATE, ove possibile, di LIMITARE la produzione di questi log, in quanto potrebbero risultare diverse migliaia (al minuto!) se attivate massivamente:

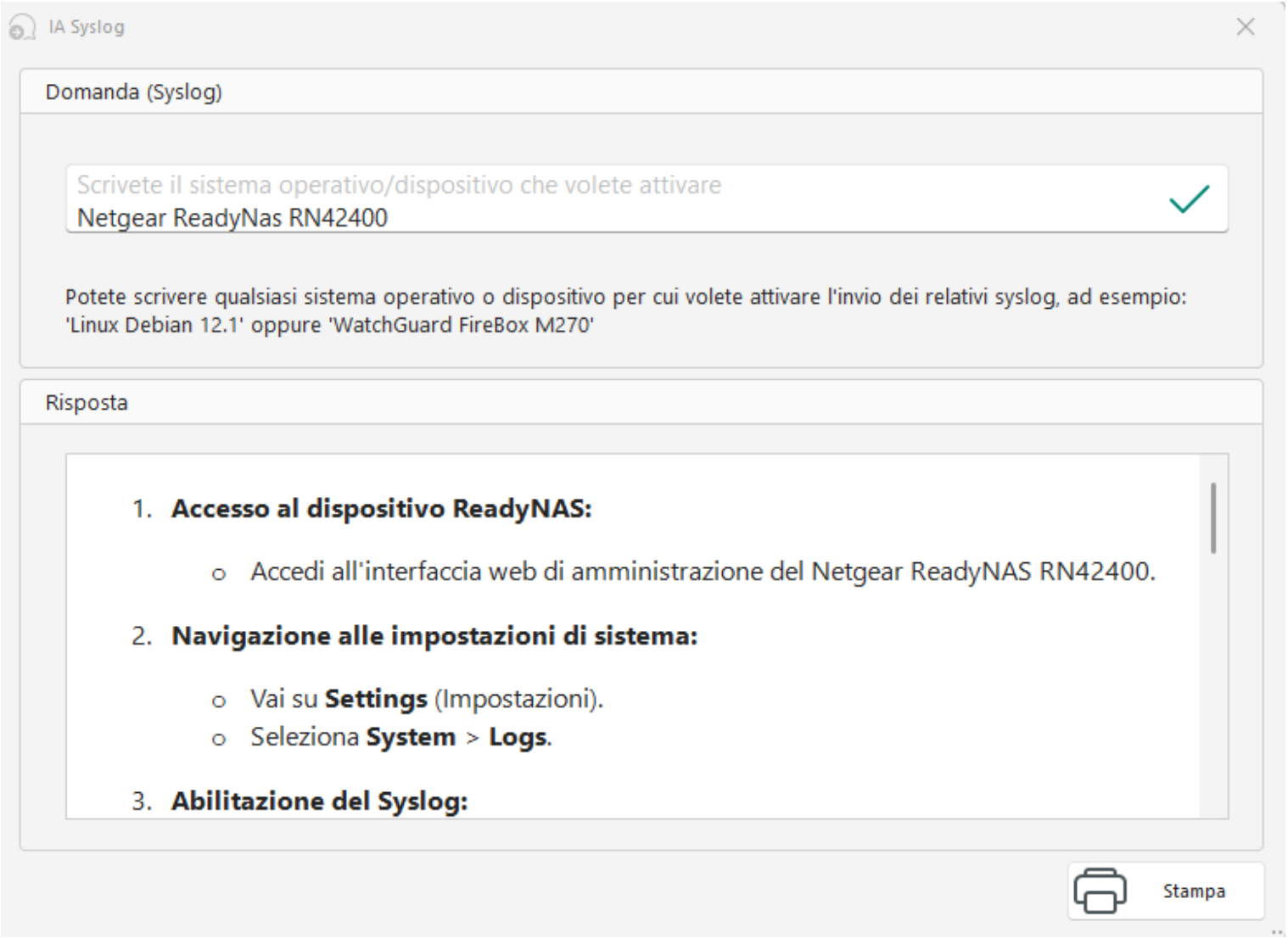
Macchine Linux/Unix/Mac: abilitare *.users e *.auth (le definizioni potrebbero essere diverse secondo la distribuzione) per produrre solo gli eventi degli utenti e autenticati.

Dispositivi: abilitare solo gli accessi all'interfaccia amministrativa e le vpn (per i firewall)

NB: Nella sezione Elenchi > Elenco Syslog compare l'elenco dei syslog acquisiti, qui trovate una funzione IA per le configurazioni dei dispositivi



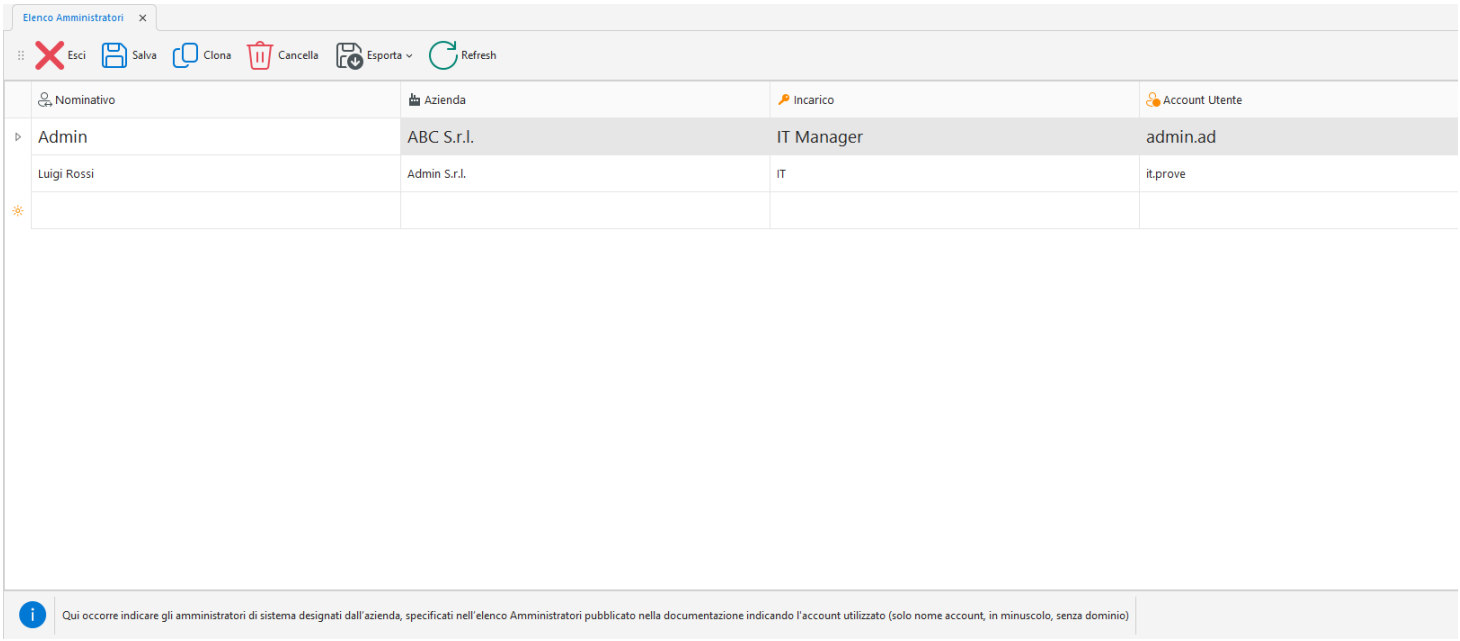
Qui e possibile inserire Marca modello e versione del dispositivo:



Per ottenere le istruzioni in merito all'attivazione dei syslog in quello specifico modello:

La risposta può essere stampata o esportata in PDF cliccando su "Stampa"

Tabella Amministratori

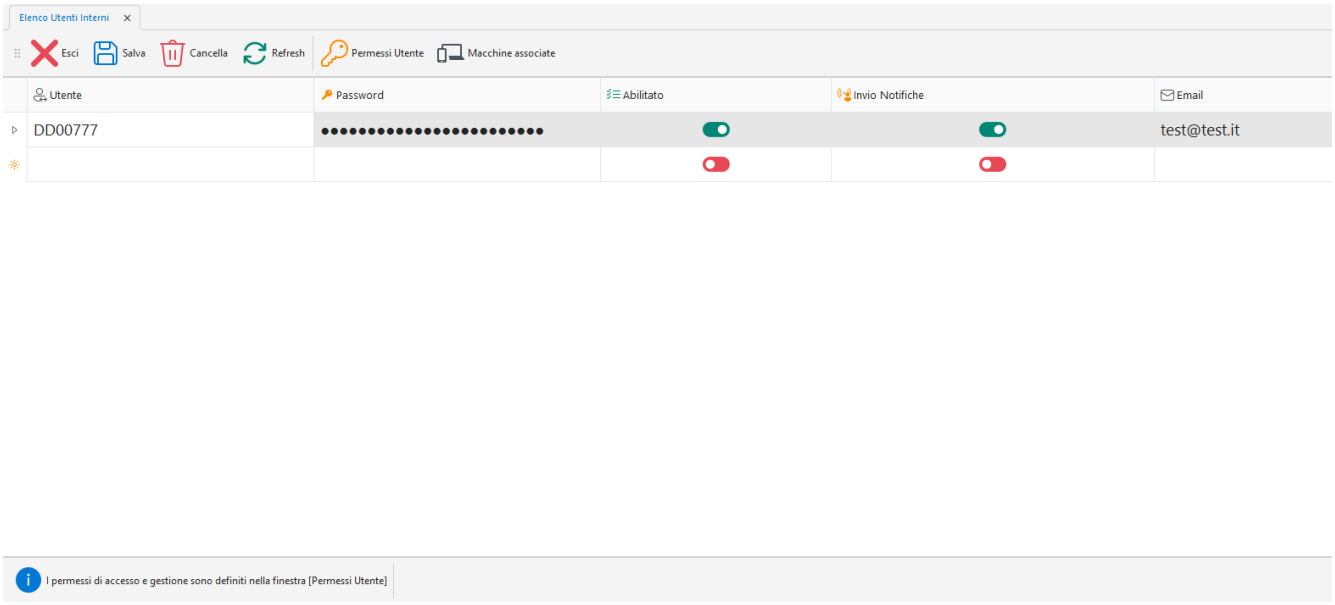


Qui occorre indicare gli amministratori di sistema designati dall'azienda, specificati nell'elenco

Amministratori pubblicato nella documentazione e che abbiano controfirmato la lettera di nomina.

NB: ogni amministratore può avere UN SOLO account, la condivisione dell'account "administrator", ad esempio, e' una "non conformita'" alla normativa per cui sono previste delle sanzioni.

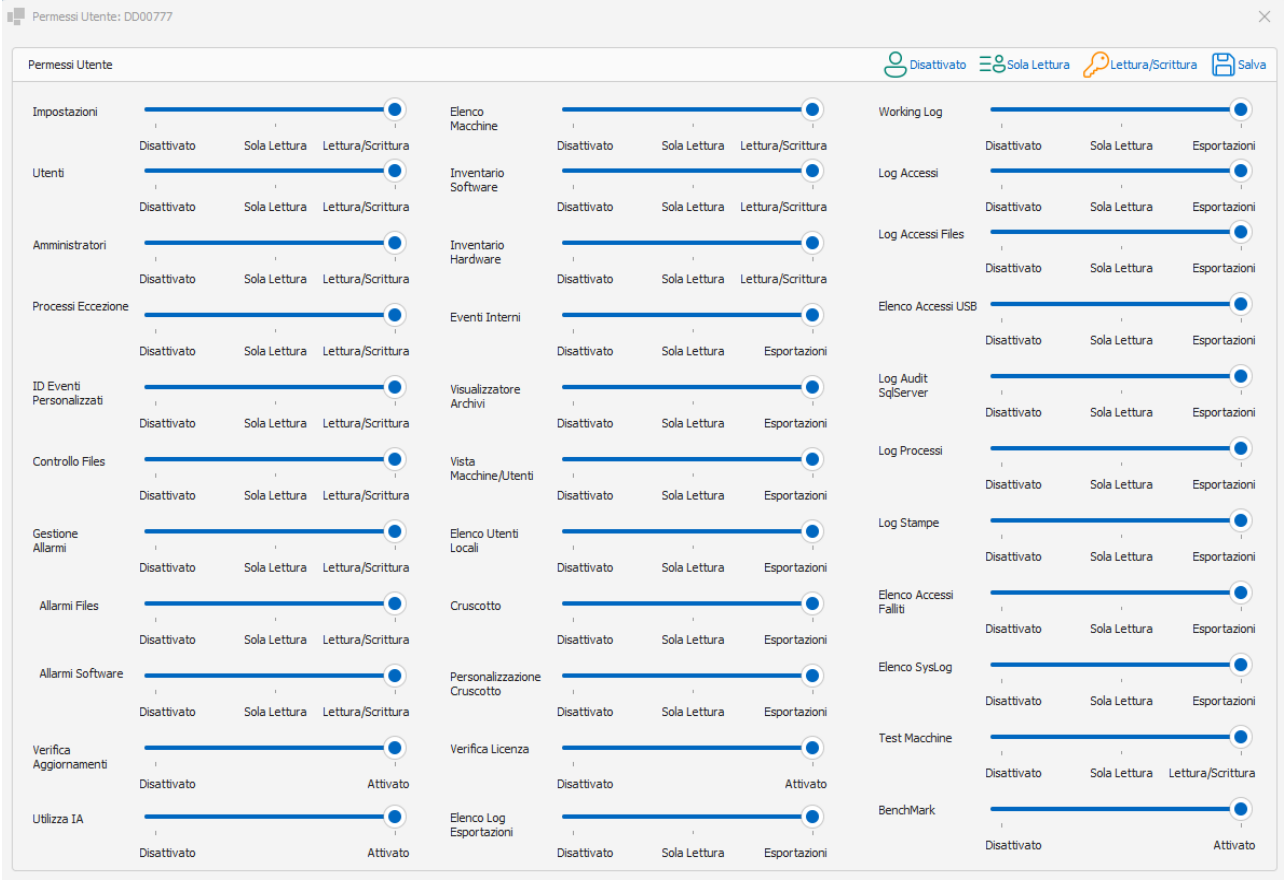
Tabella Utenti



Si possono generare infiniti utenti, abilitandoli al login.

Gli utenti NON amministratori non possono modificare le configurazioni. La mail indicata sarà utilizzata per le comunicazioni del programma.

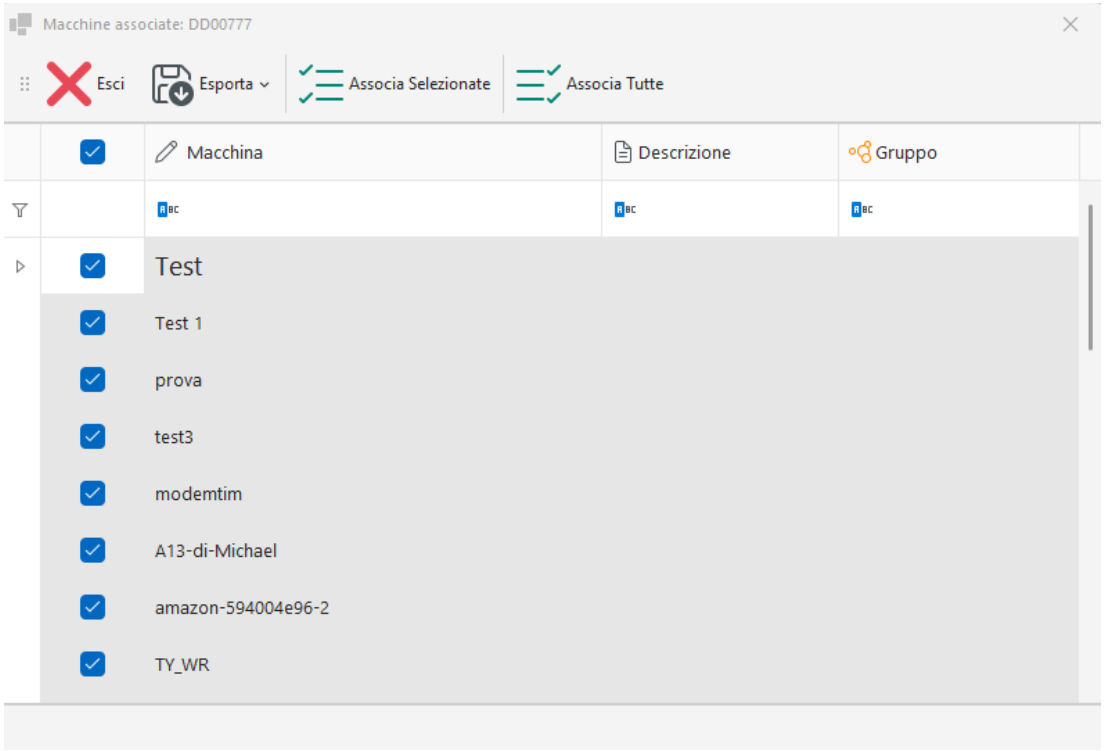
Cliccando su PERMESSI UTENTI, comparirà la seguente schermata:



È possibile gestire e abilitare i permessi degli utenti scegliendo tra tre diverse opzioni:

- Disattivato: L'utente vedrà la funzione completamente disabilitata e non potrà accedervi
- Sola Lettura: L'utente potrà accedere alla funzione ma NON effettuare modifiche
- Scrittura: L'utente ha accesso pieno anche per le modifiche
- Esportazioni: se non attiva, l'utente non potrà effettuare alcuna esportazione dei dati nei formati previsti

Cliccando su MACCHINE ASSOCIATE, comparirà la seguente schermata:



È possibile visualizzare l'elenco delle macchine associate, associando solo quelle selezionate oppure associandole tutte, cliccando su ASSOCIA TUTTE.

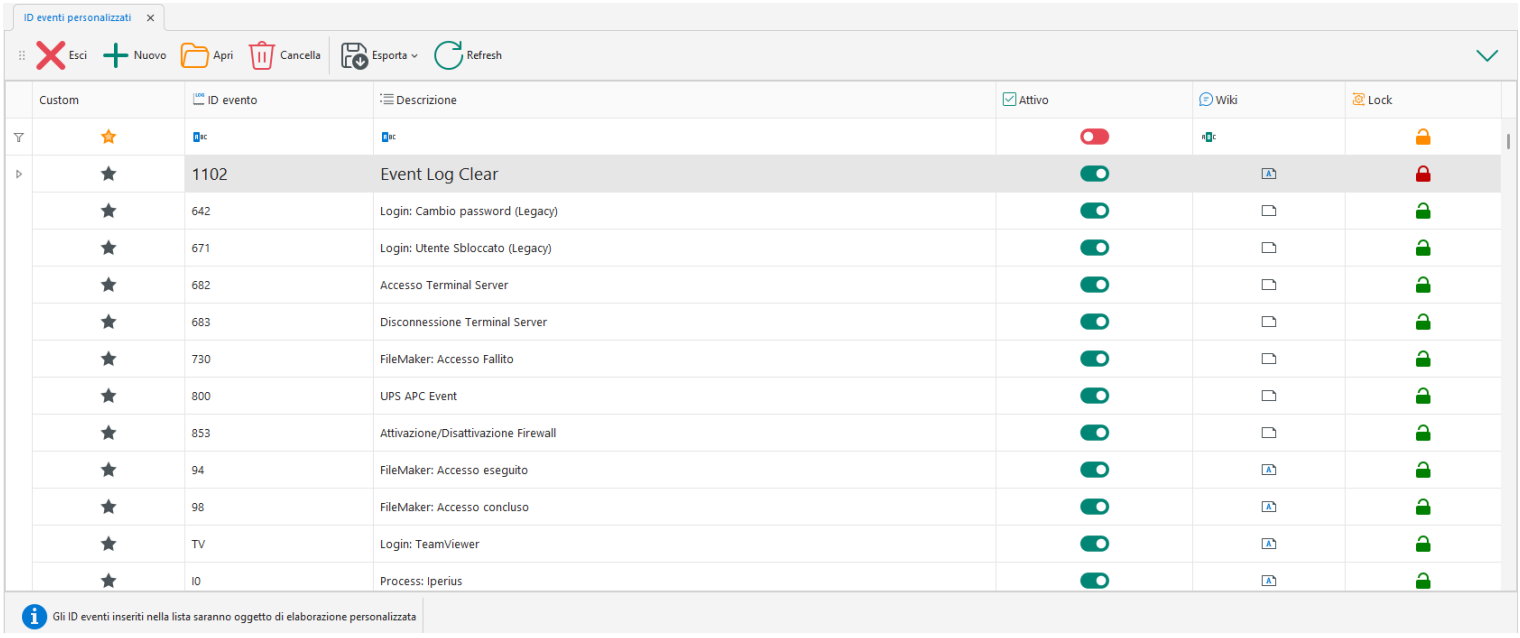
Questa associazione influenzerà la visualizzazione dei log che saranno limitati alle sole macchine associate, nascondendo tutte le altre.

TABELLA ELENCO PROCESSI

Alcuni programmi effettuano registrazioni di log-access nel registro, se alcuni di questi non sono da monitorare basta inserirli in questa tabella di “eccezione”.

Scrivere il nome dell’eseguibile e attivare l’opzione “Attivo”

ELENCO ID EVENTI MONITORATI

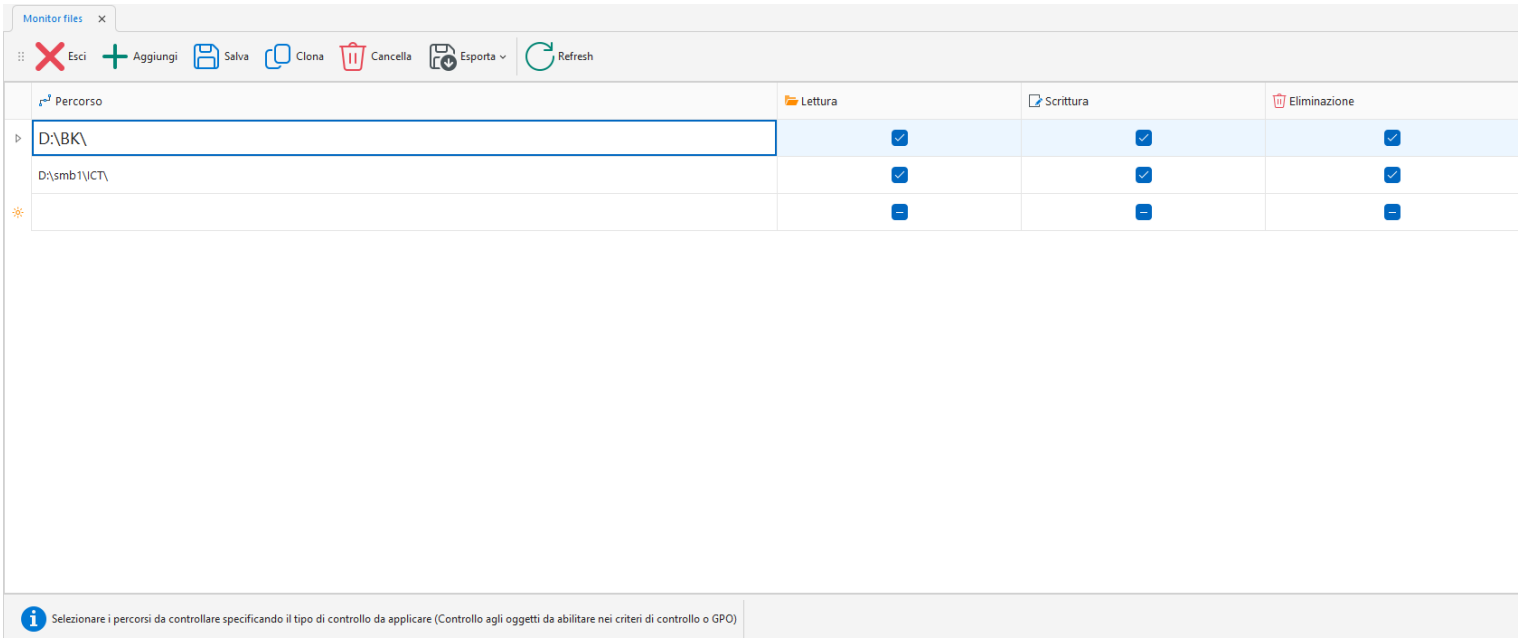


Qui e possibile visualizzare quali eventi sono oggetto di monitoraggio da parte del programma e quali sono esclusi.

È possibile aggiungere ID Eventi personalizzati (solo Windows) che devono essere scritti nella categoria Application o Security (le altre categorie vengono ignorate)

La colonna Lock indica che quell’evento non può essere Attivato/Disattivato

Tabella controllo Files (se abilitato)



Qui si possono specificare le cartella da monitorare per cui attendersi un log-access specifico (e possibile controllare lettura, scrittura ed eliminazione).

NB: attenzione che tutte le sotto-cartelle e i files contenuti saranno oggetto di controllo, NON abusare di questa funzione per non trovarsi **milioni** di log-access al giorno!

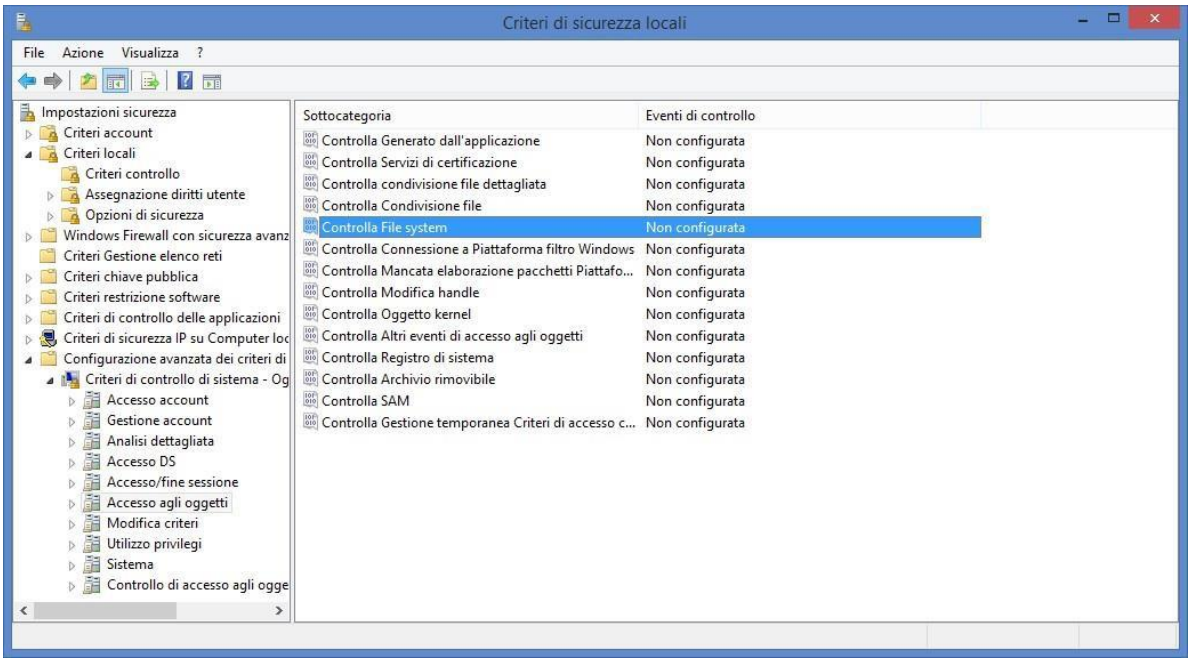
ATTENZIONE: questo controllo e subordinato all'attivazione del "Controlla File System" nella Configurazione avanzata dei criteri di controllo (cartella "Accesso agli oggetti")

NB: I controlli ai files sono attivabili SOLO per i file server WINDOWS, per gli altri sistemi o dispositivi occorre verificare la disponibilità di questi controlli e che siano esportabili attraverso syslog.

ATTIVAZIONE CONTROLLO FILES

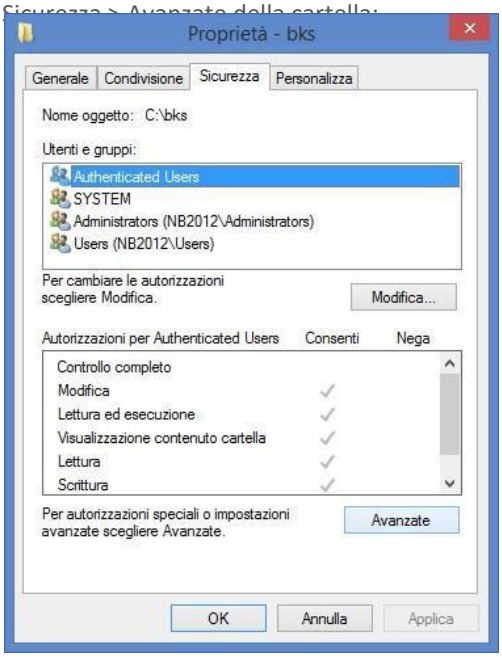
Nella Group Policy di dominio e possibile attivare questa opzione (filtrato per le sole macchine a cui occorre attivarlo) nella configurazione avanzata > Accesso agli oggetti > Controlla File system

***È possibile gestirlo anche direttamente nei criteri locali del/dei file server**

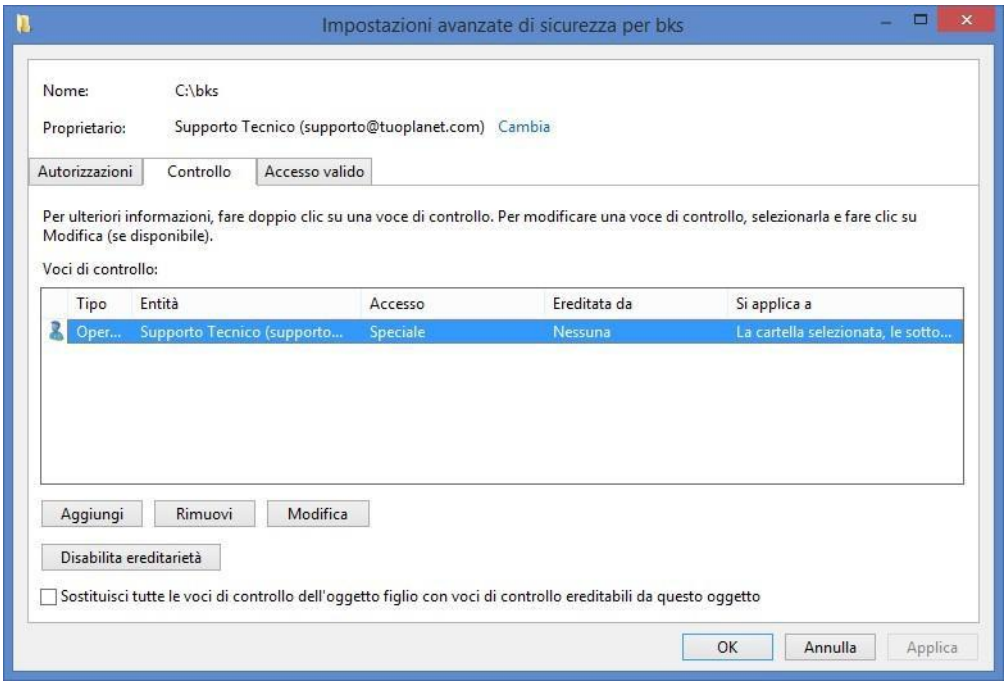


Successivamente sarà necessario estendere il controllo alla cartella da monitorare: Da

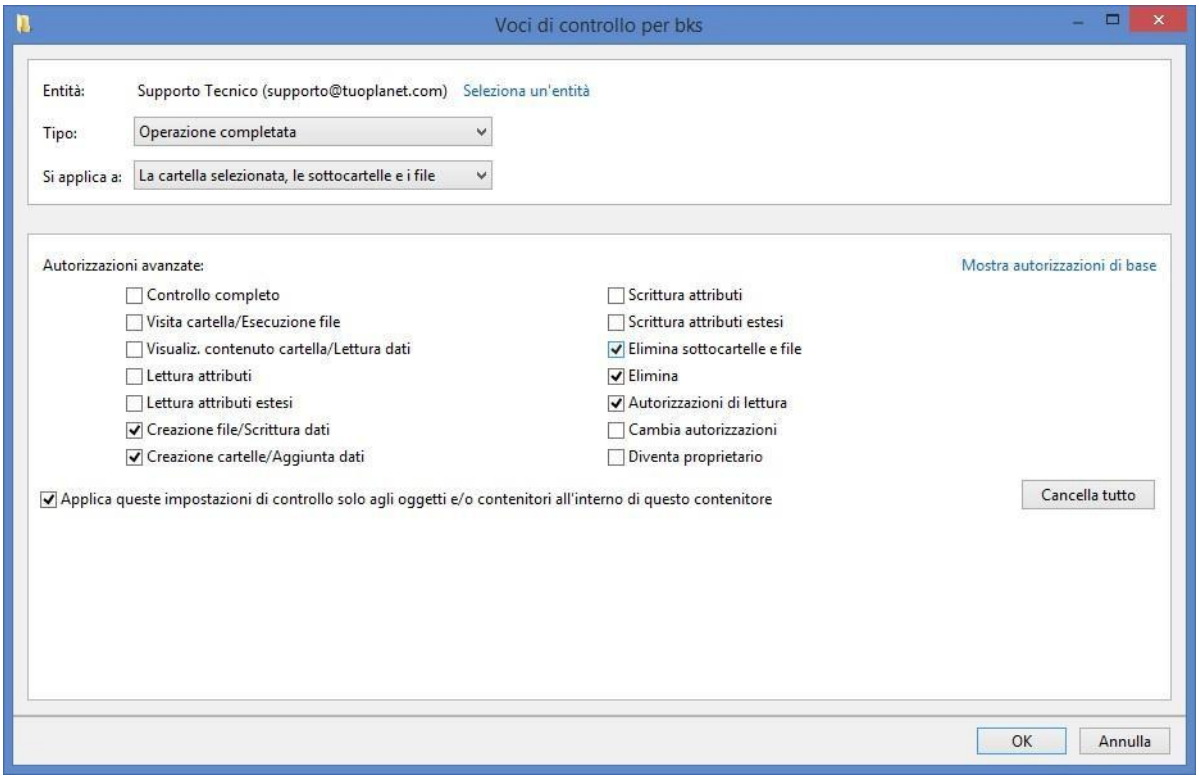
Sicurezza > Avanzate della cartella:



Qui è possibile specificare i controlli aggiuntivi alla cartella, si possono fare controlli diversi per utenti o gruppi:



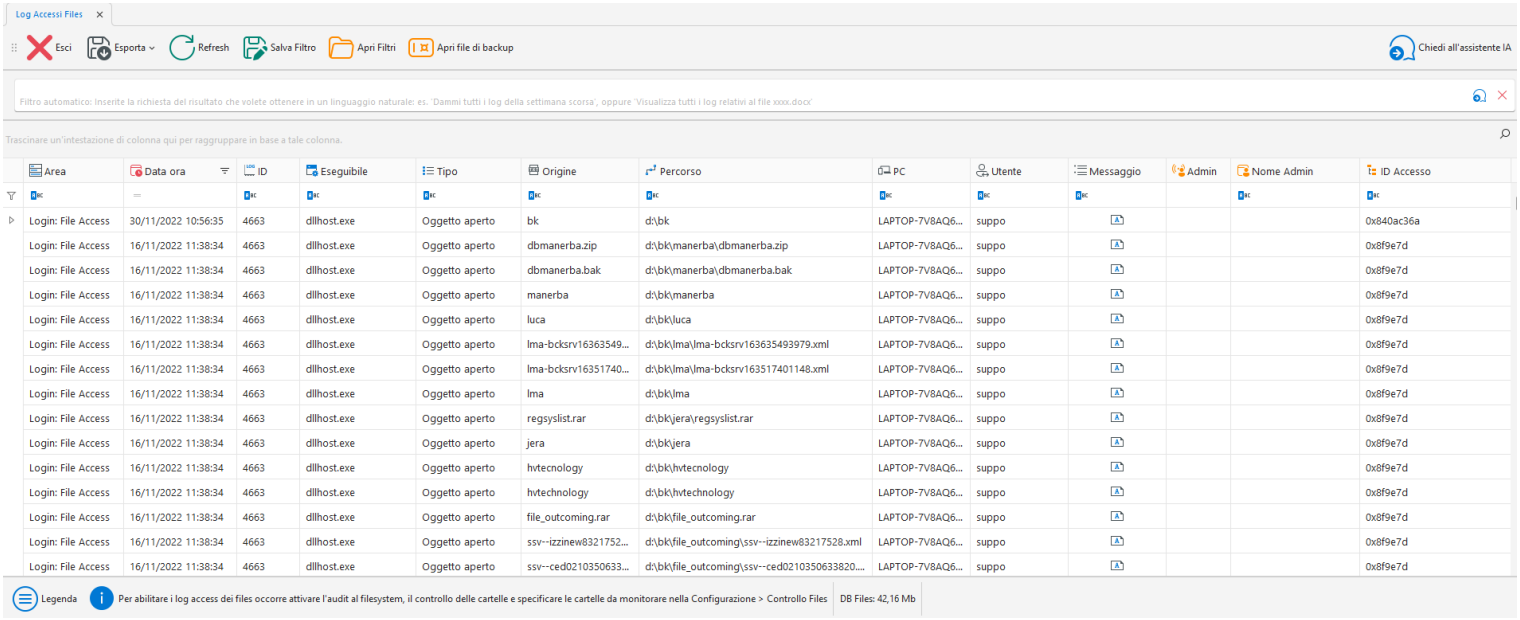
Nello specifico:



Questi sono i controlli suggeriti per il monitor completo di BusinessLog, ovviamente potete limitare o aumentare il livello di audit secondo le indicazioni aziendali.

NB: attenzione che tutte le macchine e utenti selezionati saranno oggetto di controllo, NON abusare di questa funzione per non trovarsi migliaia di log-access al giorno!

LOG ACCESSI AI FILES



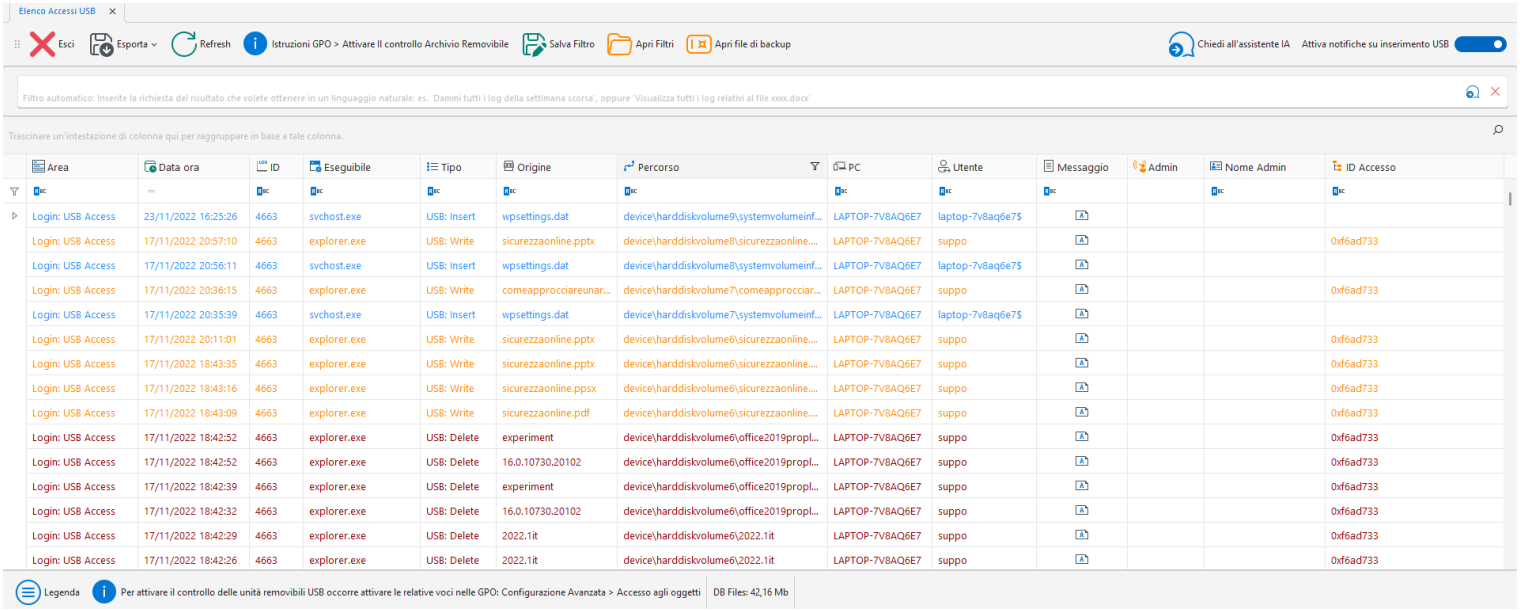
Dopo aver attivato il controllo files e i relativi controlli agli oggetti, verrà compilata la tabella relativa agli accessi ai files che si trova staccata dai normali log-access alle macchine.

Da Log > Log accessi files: verrà visualizzata una finestra contenente i log-access ai files con le stesse caratteristiche (filtri, ordinamenti, raggruppamenti, esportazioni) dei normali accessi.

Inoltre, in configurazione, si possono specificare criteri diversi di ritenzione di questi log rispetto ai normali log-access.

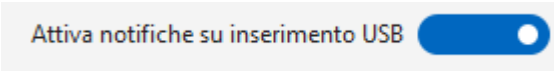
Controllo accessi di unità Removibili (opzionale)

ACCESSI USB



Se attivata l'opzione, è possibile ottenere gli accessi di dispositivi removibili (chiavette USB, Dischi esterni, SD o MicroSD) in tutte le macchine della rete.

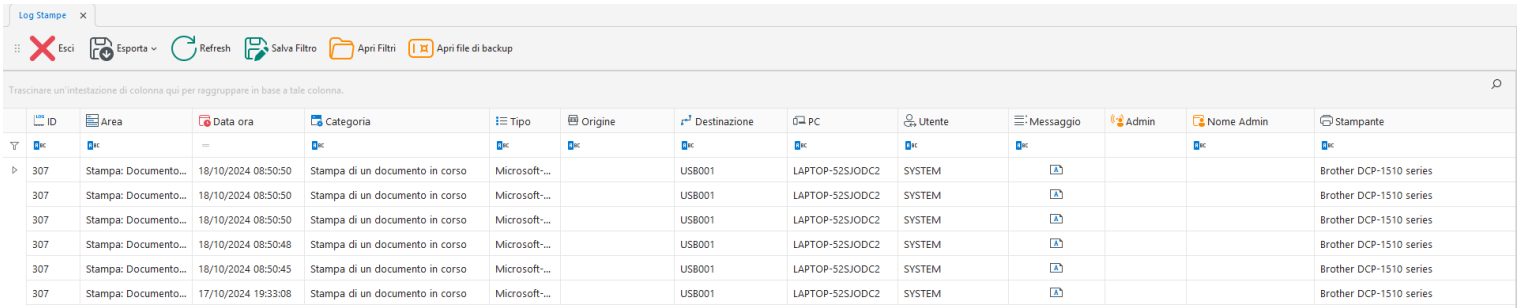
Per abilitare la scrittura di questi eventi, è disponibile una semplice guida cliccando sul pulsante (i)



Attivando l'opzione di notifica, si riceverà una notifica ogni volta che un utente inserisce un dispositivo removibile.

* ATTENZIONE: alcune piattaforme di Virtualizzazione possono far apparire le proprie unita virtuali come se fossero "unita removibile", in questo caso è Windows che viene "ingannato".

Registro delle Stampe (Print Log)



ID	Area	Data ora	Categoria	Tipo	Origine	Destinazione	PC	Utente	Messaggio	Admin	Nome Admin	Stampante
307	Stampa: Documento...	18/10/2024 08:50:50	Stampa di un documento in corso	Microsoft-...		USB001	LAPTOP-52SJODC2	SYSTEM				Brother DCP-1510 series
307	Stampa: Documento...	18/10/2024 08:50:50	Stampa di un documento in corso	Microsoft-...		USB001	LAPTOP-52SJODC2	SYSTEM				Brother DCP-1510 series
307	Stampa: Documento...	18/10/2024 08:50:50	Stampa di un documento in corso	Microsoft-...		USB001	LAPTOP-52SJODC2	SYSTEM				Brother DCP-1510 series
307	Stampa: Documento...	18/10/2024 08:50:48	Stampa di un documento in corso	Microsoft-...		USB001	LAPTOP-52SJODC2	SYSTEM				Brother DCP-1510 series
307	Stampa: Documento...	18/10/2024 08:50:45	Stampa di un documento in corso	Microsoft-...		USB001	LAPTOP-52SJODC2	SYSTEM				Brother DCP-1510 series
307	Stampa: Documento...	17/10/2024 19:33:08	Stampa di un documento in corso	Microsoft-...		USB001	LAPTOP-52SJODC2	SYSTEM				Brother DCP-1510 series

Nelle versioni “Enterprise” è disponibile la registrazione dei log di stampa, praticamente qualsiasi stampa mandata a qualunque stampante (anche virtuale) può essere registrata:

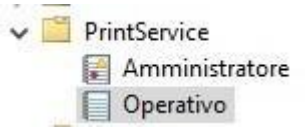
Nel log è possibile ottenere:

- PC di origine
- Utente che ha generato la stampa
- File di origine (solo il titolo di file)
- Porta di destinazione (file di destinazione se stampante virtuale, es. PDF)

La registrazione delle stampe NON è attivata in nessun client, ma vanno eseguite le seguenti operazioni REGI-

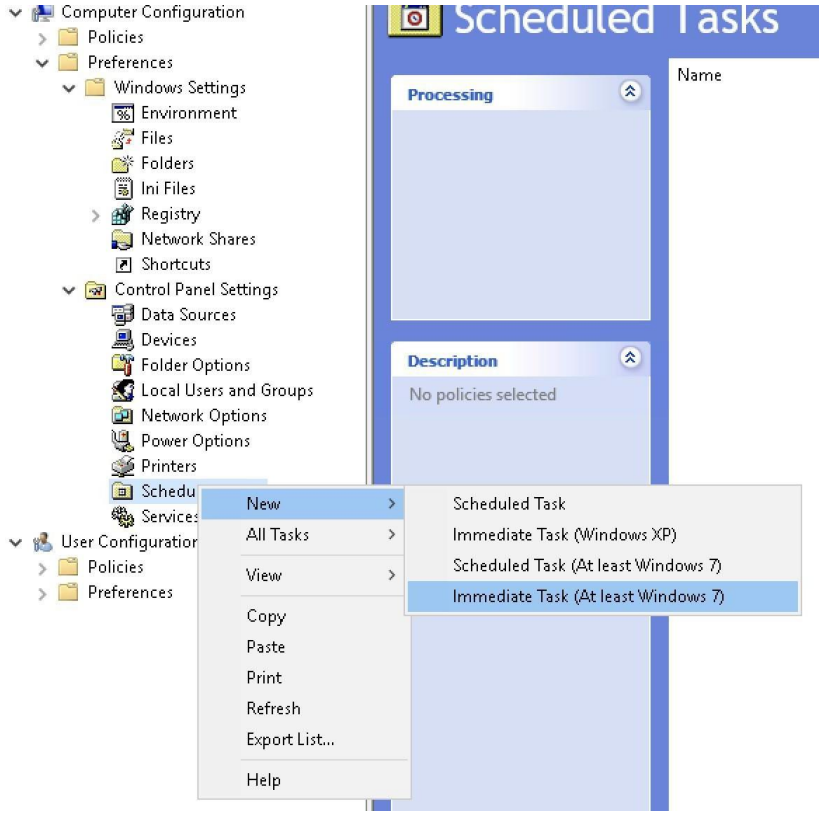
STRO EVENTI

Nel menu a sinistra: Registri applicazioni e servizi > Microsoft >Windows > Print Service > Operativo

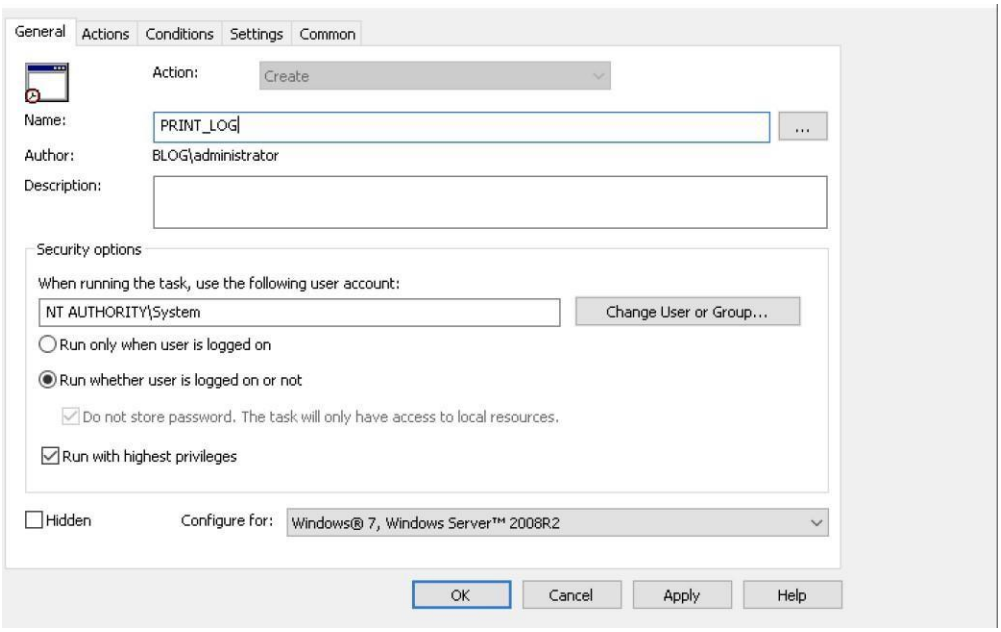


Fare clic destro > Attiva Registro

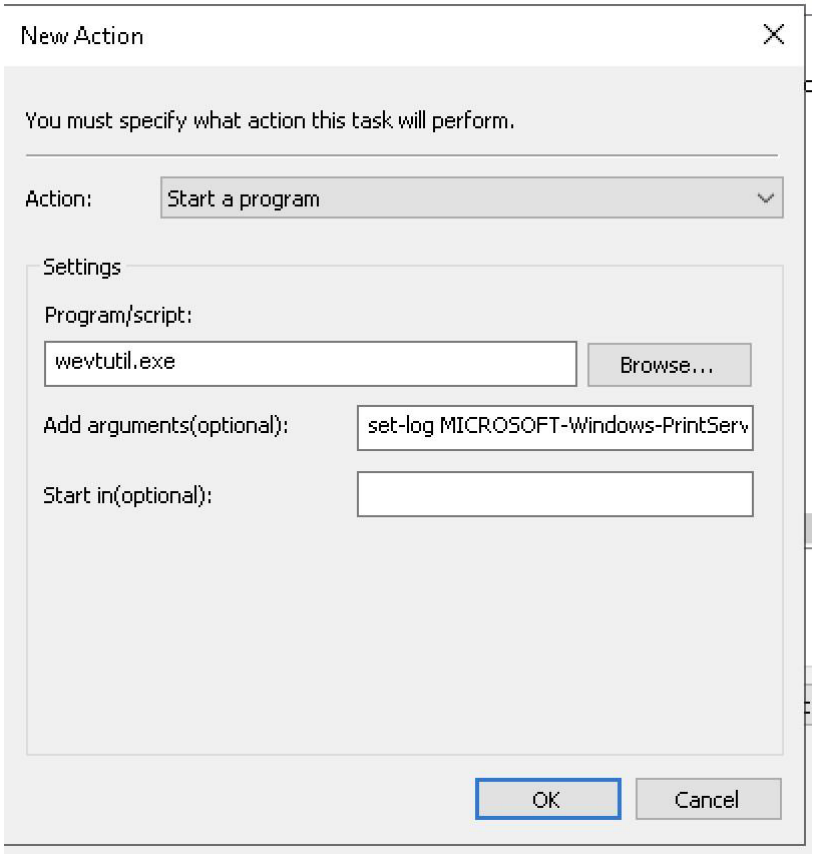
E' possibile gestire questa operazione mediante GPO:.



Creando un Task Immediato:



Creare una nuova azione:

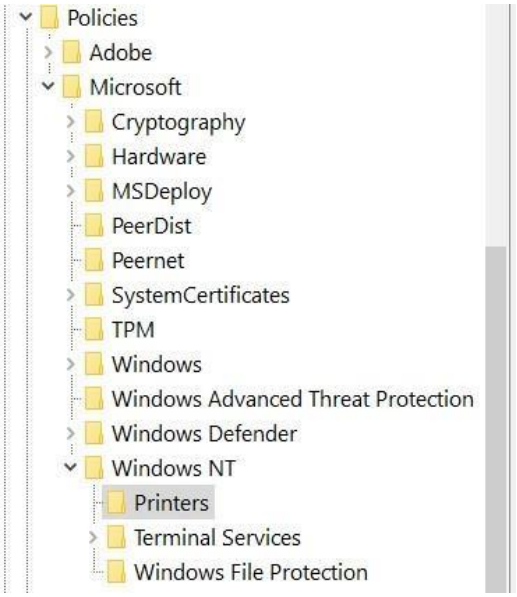


La stringa per “add arguments” è:

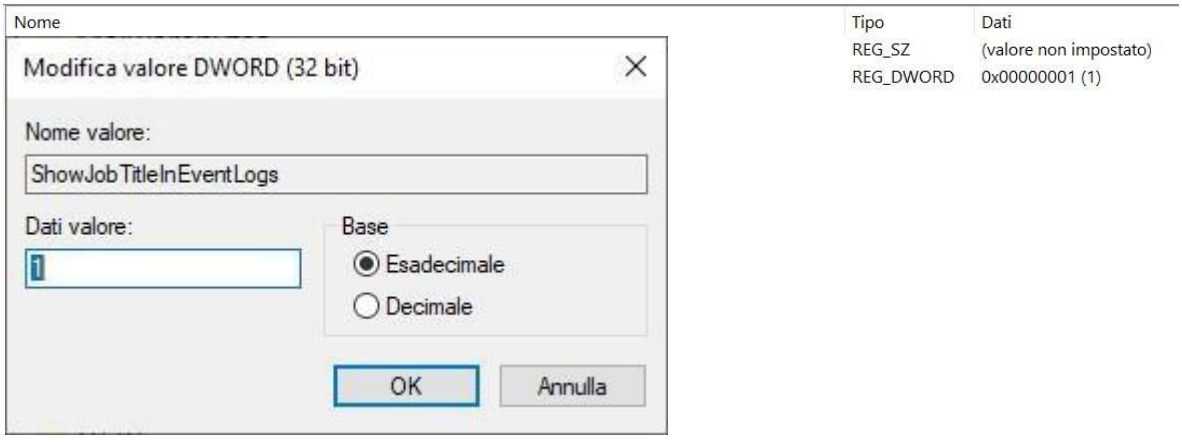
set-log MICROSOFT-Windows-PrintService/Operational /e:true /q:true REGISTRY (Registro di sistema)

Andare alla cartella Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT

CREARE la Chiave “Printers”



Quindi creare la voce ShowJobTitleInEventLogs (Nuovo > Valore DWORD 32 bit)

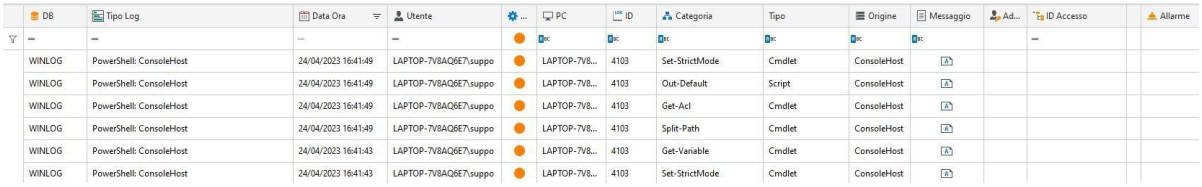


Questa chiave serve per ottenere il titolo del documento mandato in stampa (altrimenti risulterà vuoto)

È consigliabile impostare questa chiave nelle GPO per poterle distribuire nelle macchine in modo massivo.

Registro dei comandi PowerShell (PowerShell Log)

Nella Working Log e nei Log Accessi possono venire registrati i comandi Powershell emessi da uno script, da un applicativo o da un utente:



DB	Tipo Log	Data Ora	Utente	PC	ID	Categoria	Tipo	Origine	Messaggio	Ad...	ID Accesso	Allarme
WINLOG	PowerShell: ConsoleHost	24/04/2023 16:41:49	LAPTOP-7V8AQ6E7\suppo	LAPTOP-7V8...	4103	Set-StrictMode	Cmdlet	ConsoleHost				
WINLOG	PowerShell: ConsoleHost	24/04/2023 16:41:49	LAPTOP-7V8AQ6E7\suppo	LAPTOP-7V8...	4103	Out-Default	Script	ConsoleHost				
WINLOG	PowerShell: ConsoleHost	24/04/2023 16:41:49	LAPTOP-7V8AQ6E7\suppo	LAPTOP-7V8...	4103	Get-Acl	Cmdlet	ConsoleHost				
WINLOG	PowerShell: ConsoleHost	24/04/2023 16:41:49	LAPTOP-7V8AQ6E7\suppo	LAPTOP-7V8...	4103	Split-Path	Cmdlet	ConsoleHost				
WINLOG	PowerShell: ConsoleHost	24/04/2023 16:41:43	LAPTOP-7V8AQ6E7\suppo	LAPTOP-7V8...	4103	Get-Variable	Cmdlet	ConsoleHost				
WINLOG	PowerShell: ConsoleHost	24/04/2023 16:41:43	LAPTOP-7V8AQ6E7\suppo	LAPTOP-7V8...	4103	Set-StrictMode	Cmdlet	ConsoleHost				

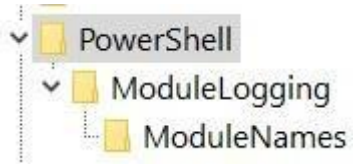
Per attivare la registrazione nelle macchine sono necessarie alcune chiavi nel Registy (Regedit) In

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\

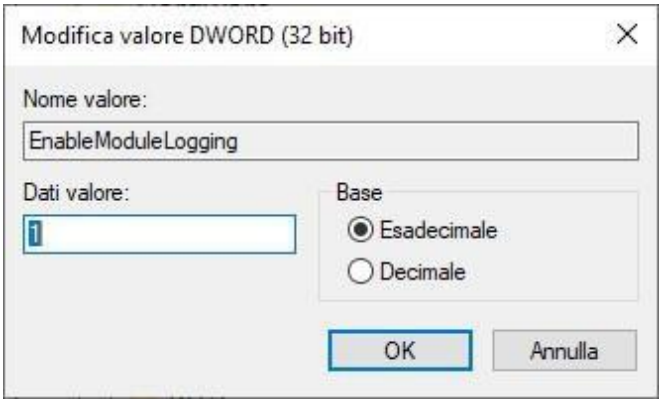
Create la chiave “PowerShell” e subito sotto, altre 2 chiavi: Module-

Logging

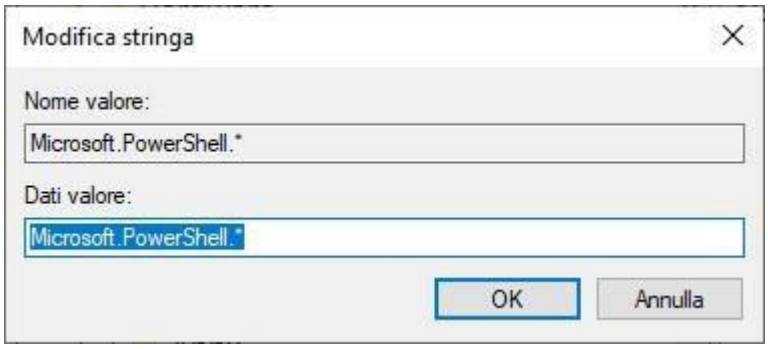
ModuleNames



Dentro a ModuleLogging create una DWORD “EnableModuleLogging” con valore 1



Mentre nella ModuleNames create una STRINGA con etichetta e valore:



Microsoft.PowerShell.*

Queste chiavi vanno generate da GPO, in modo da “spalmarle” in tutte le macchine

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell]

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging] "EnableModuleL-ogging"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging\Modu leNames] "Microsoft.PowerShell.*"="Microsoft.PowerShell.*"

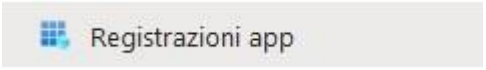
Registrazione log Azure

(Plugin Opzionale o per l'utilizzo di account O365 per l'invio delle mail)

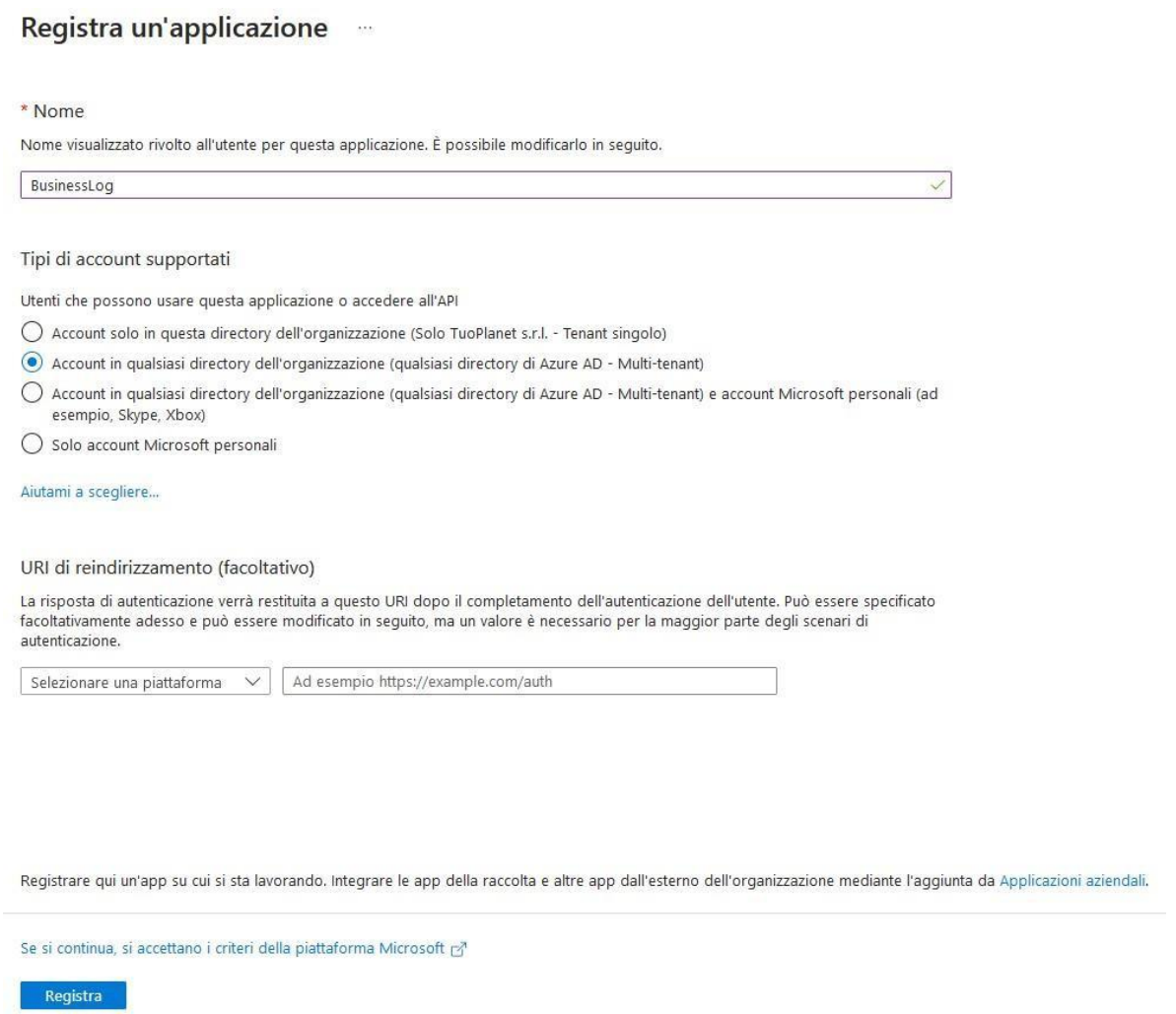
Mediante il plugin "Azure" è possibile registrare i log access degli account **azure**, per abilitarne la registrazione lato piattaforma è necessario registrare l'applicazione e autorizzarne l'accesso:

Accedere al portale Azure (da portal.azure.com) e cliccare su "Azure Active Directory)

Nel menu a sinistra cliccare su



E poi, nel menu in alto

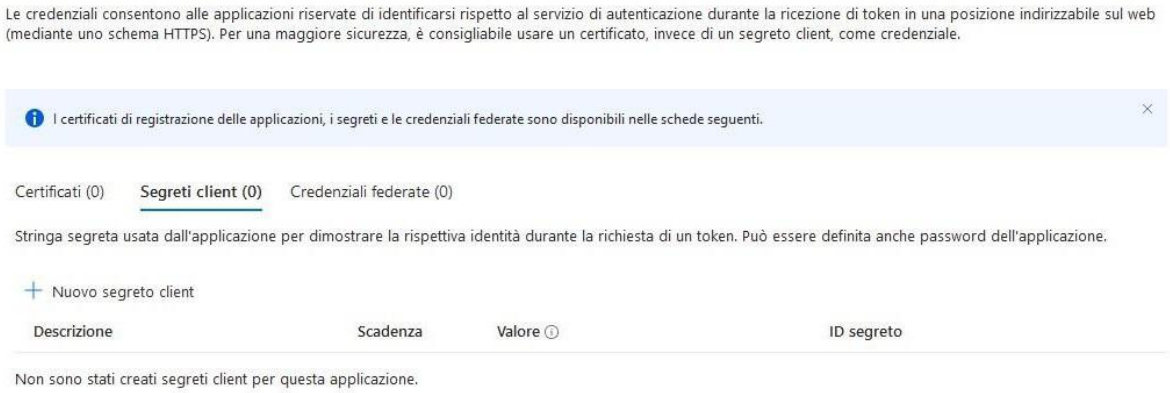


Quando pronti, cliccate su Registra

Arriverete alla pagina di configurazione dell'applicazione appena creata: Nel

menu a sinistra cliccate su:

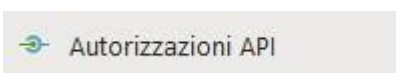
Otterrete:



Cliccando su Nuovo segreto client, otterrete (a destra)

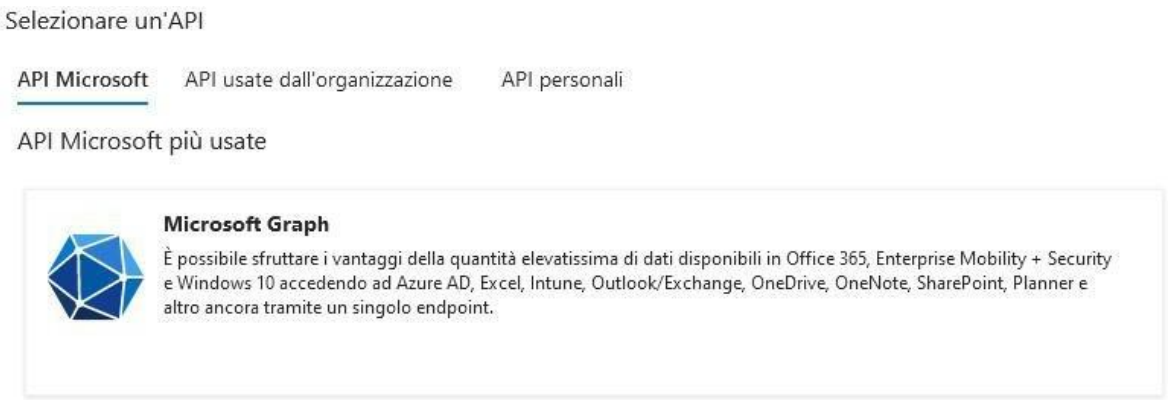
Specificare un nome e salvare.

Sempre nel menu a sinistra, ora, cliccate su



Otterrete:

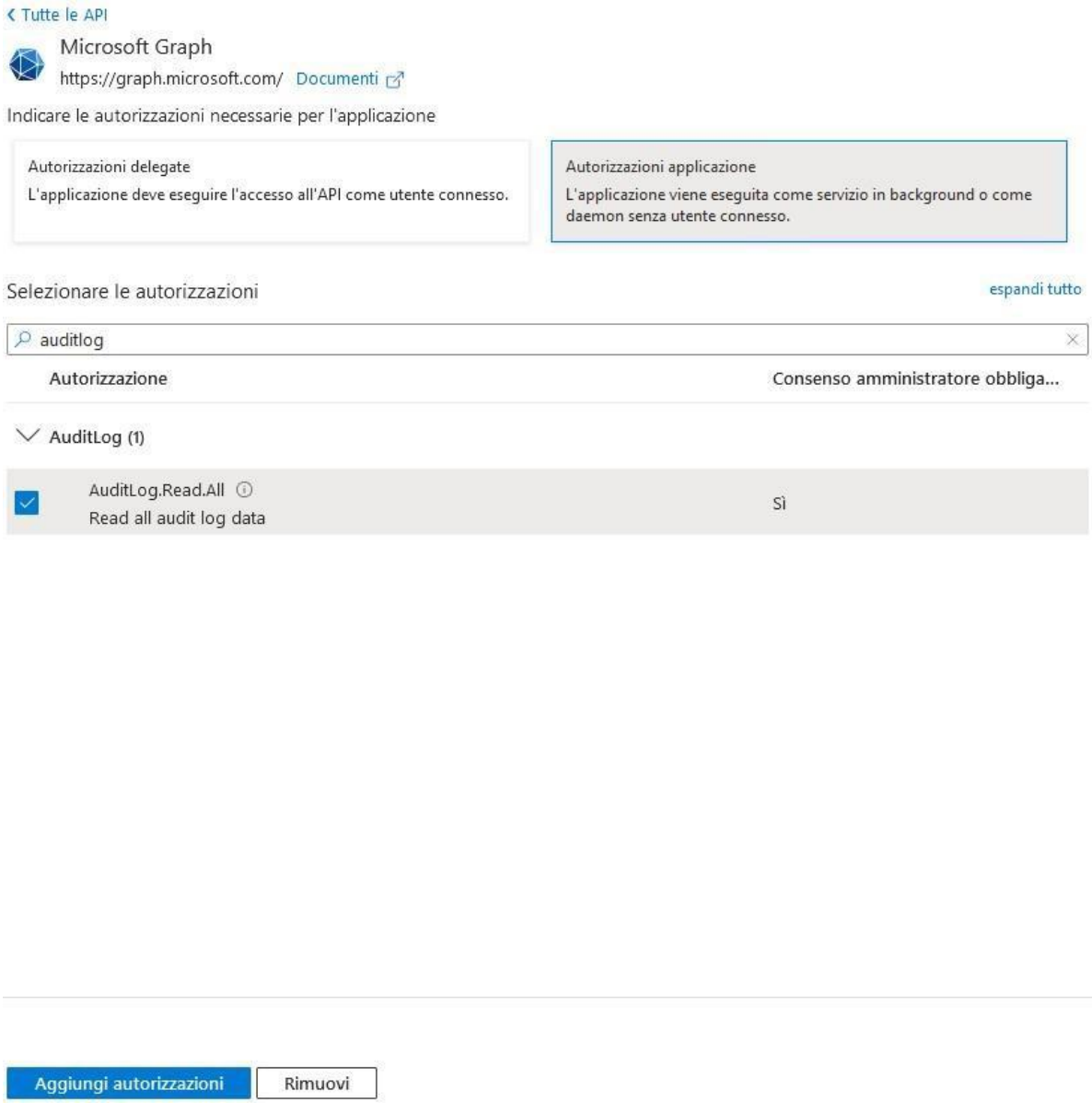
Aggiungi un'autorizzazione, otterrete, a destra:



Cliccate su Microsoft Graph

Scegliete "Autorizzazioni applicazione"

Cercate, nel box di ricerca “auditlog”, otterrete:



Infine, cliccate su “Aggiungi autorizzazioni”

ATTENZIONE: per abilitare l’invio delle mail, attraverso un account Office 365, è necessario aggiungere anche l’autorizzazione

Mail.Send

Se non utilizzate il plugin Azure, potete limitarvi alla sola autorizzazione delle mail!

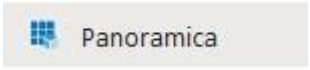
Ora le autorizzazioni dovrebbero comparire così:

Ora cliccate su “Concedi consenso amministratore per …”

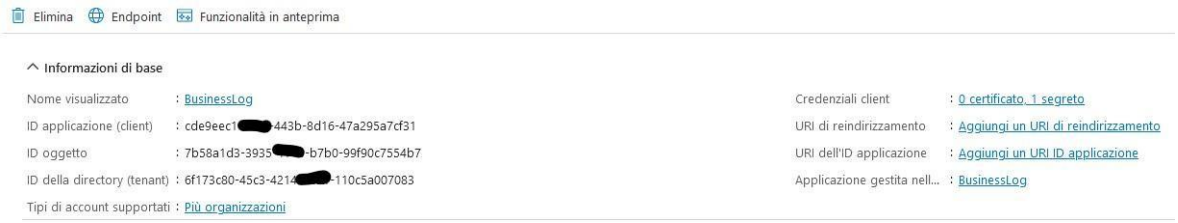
Ovviamente dovrete essere amministratori per poter concedere l’autorizzazione!

Ora avrete bisogno di 3 dati:

Nella sezione “Panoramica” (menu a sinistra)



Otterrete:



Prendete nota di:

ID applicazione (client)

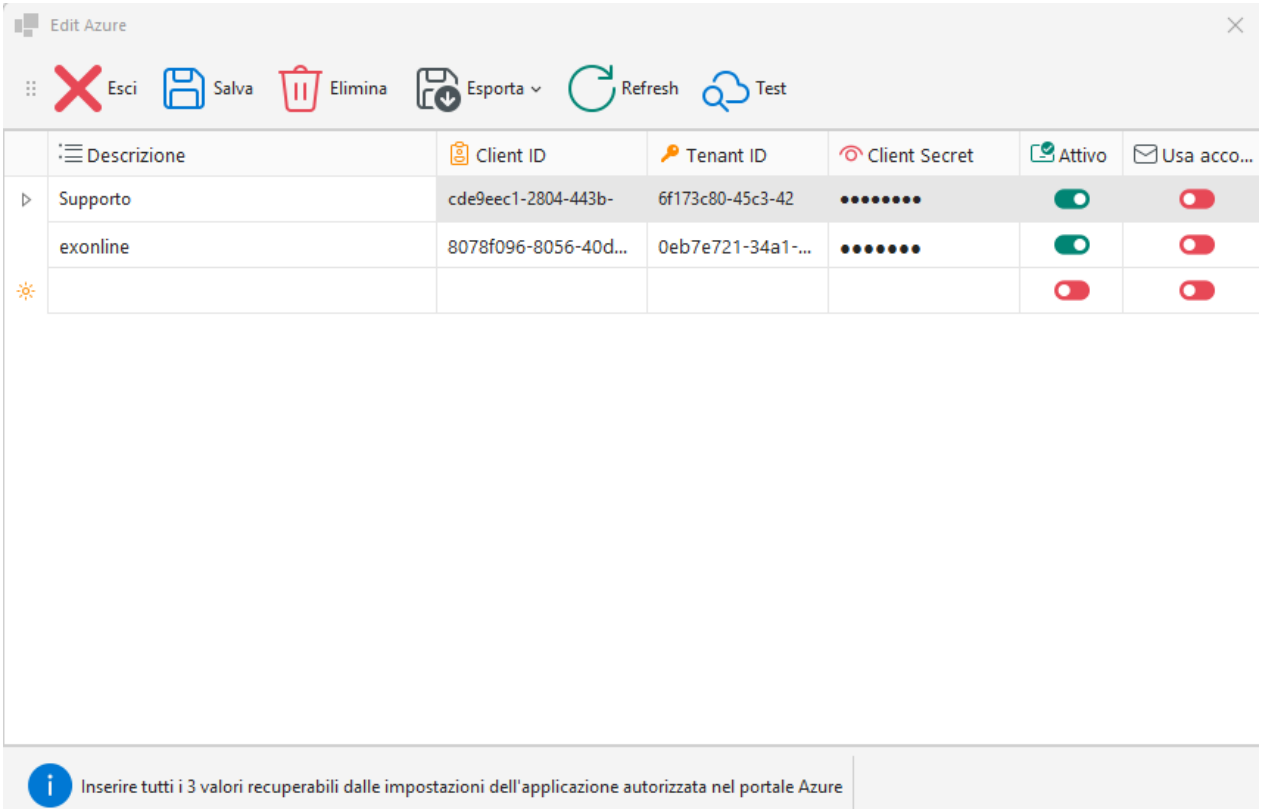
ID della directory (tenant)

Nella sezione “Certificati e segreti” potete accedere al valore ClientSecret

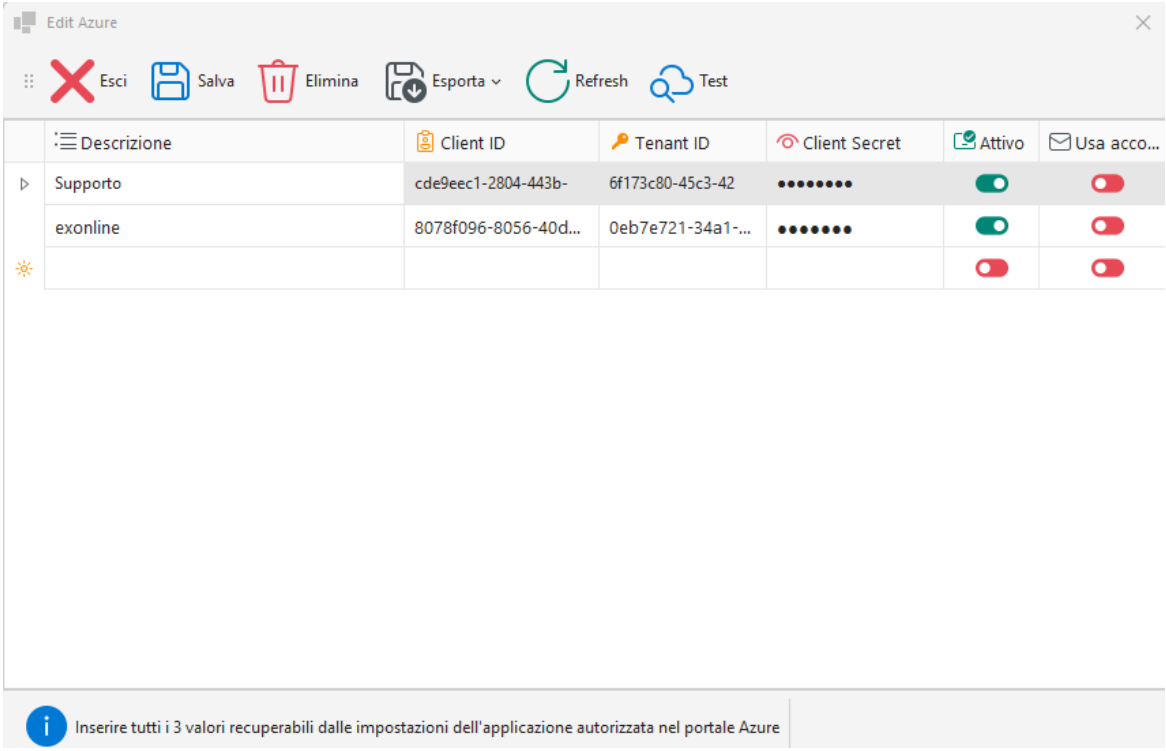
Copiate il valore della colonna “Valore” (c’è un’apposita icona)

ATTENZIONE: La copia del Valore del Client Secret e possibile SOLO subito dopo la creazione, per cui effettuate le impostazioni e il test PRIMA di chiudere questa finestra, altrimenti sarà necessario ripetere la generazione del certificato

Nella configurazione > Cloud (se abilitato) troverete:



In questa tabella è possibile specificare uno o più tenant di Microsoft Azure a cui accedere Premendo [Ab] potete editare le righe:



In questa tabella potete gestire i 3 campi necessari al funzionamento, cliccando su [Test] potete verificarne il funzionamento.

NB: Ricordate che l'autorizzazione all'accesso del tenant scade ogni X mesi e sarà necessario intervenire, manualmente, nel portale Azure per rinnovarlo! (la scadenza viene decisa al momento della generazione del certificato)

Il flag Usa account Mail serve per indicare questo Tenant come account MITTENTE della casella mail specificata.

SHAREPOINT / ONEDRIVE

Nel caso di acquisizioni di log da Sharepoint/Onedrive occorre attivare anche questi punti:

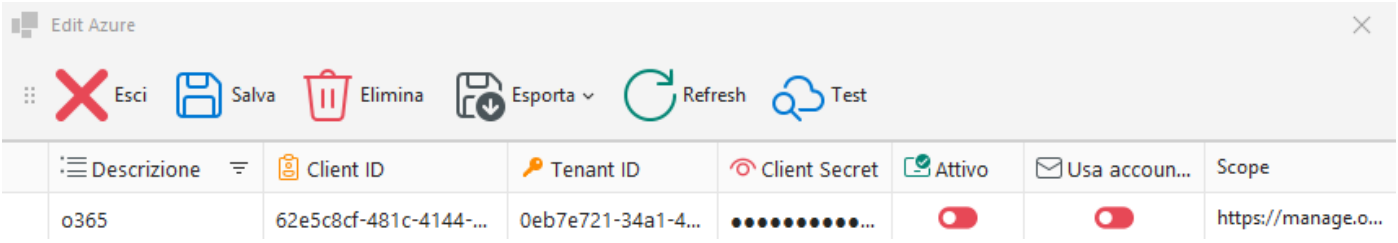
ServiceActivity-OneDrive.Read.All	Applicazio...	Read all One Drive service activity
SharePointTenantSettings.Read.All	Applicazio...	Read SharePoint and OneDrive tenant settings
Sites.Read.All	Applicazio...	Read items in all site collections

Inoltre, Vi consigliamo di creare una nuova autorizzazione (con conseguente nuovo Client ID e Secret) con le seguenti voci da attivare per le API di Microsoft O365:

Office 365 Management APIs (3)

ActivityFeed.Read	Applicazio...	Read activity data for your organization
ActivityFeed.ReadDlp	Applicazio...	Read DLP policy events including detected sensitive data
ServiceHealth.Read	Applicazio...	Read service health information for your organization

Nella tabella Azure aggiungete:



Lo scope (solo per O365) sarà:

https://manage.office.com/.default

SQL Audit

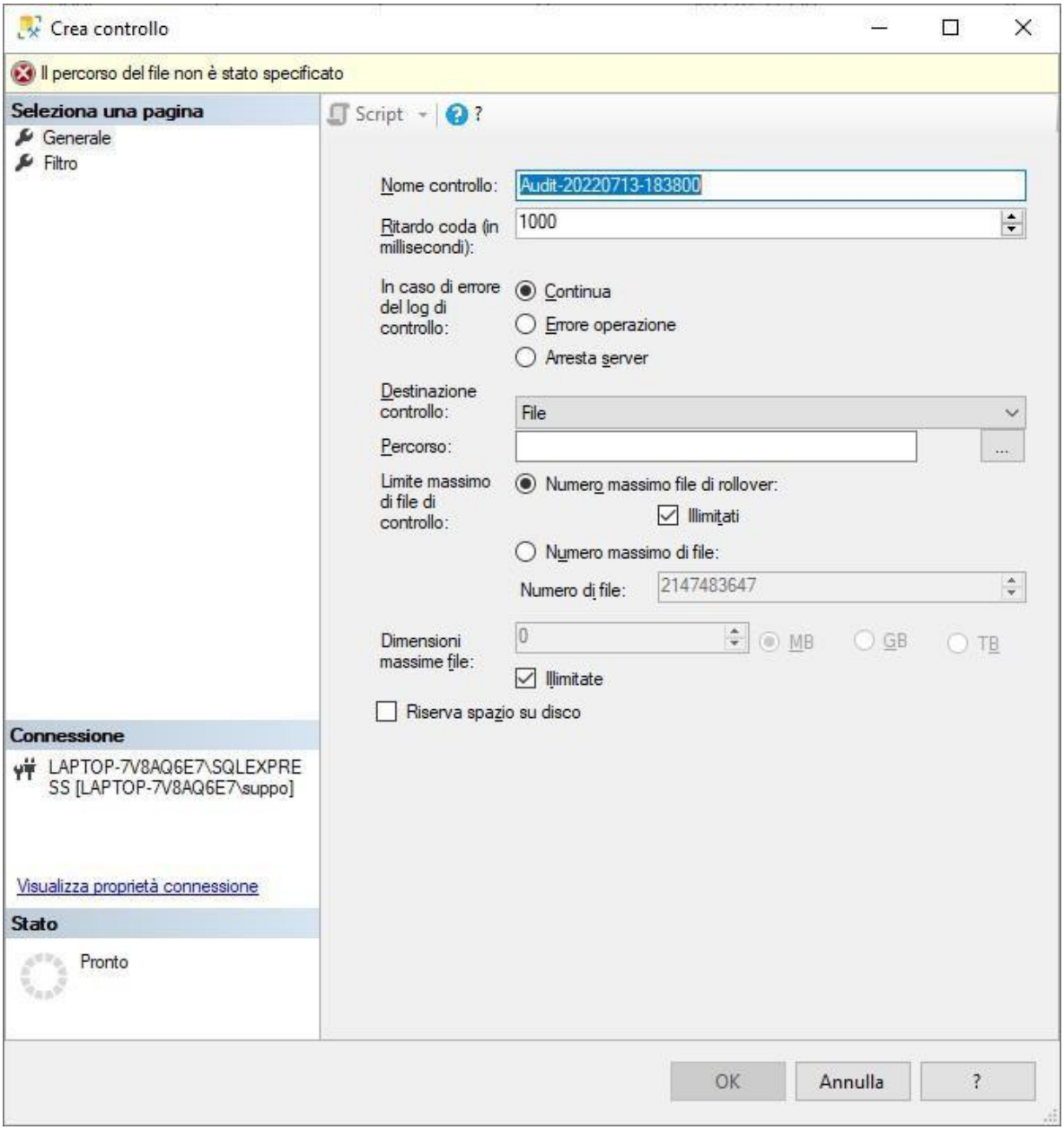
Con questo plugin opzionale è possibile acquisire i log prodotti dai server MS SQL SERVER (per gli altri database, sarà necessario utilizzare syslog)

Per attivare il plugin (una volta attivata la relativa licenza), nella configurazione > PlugIn

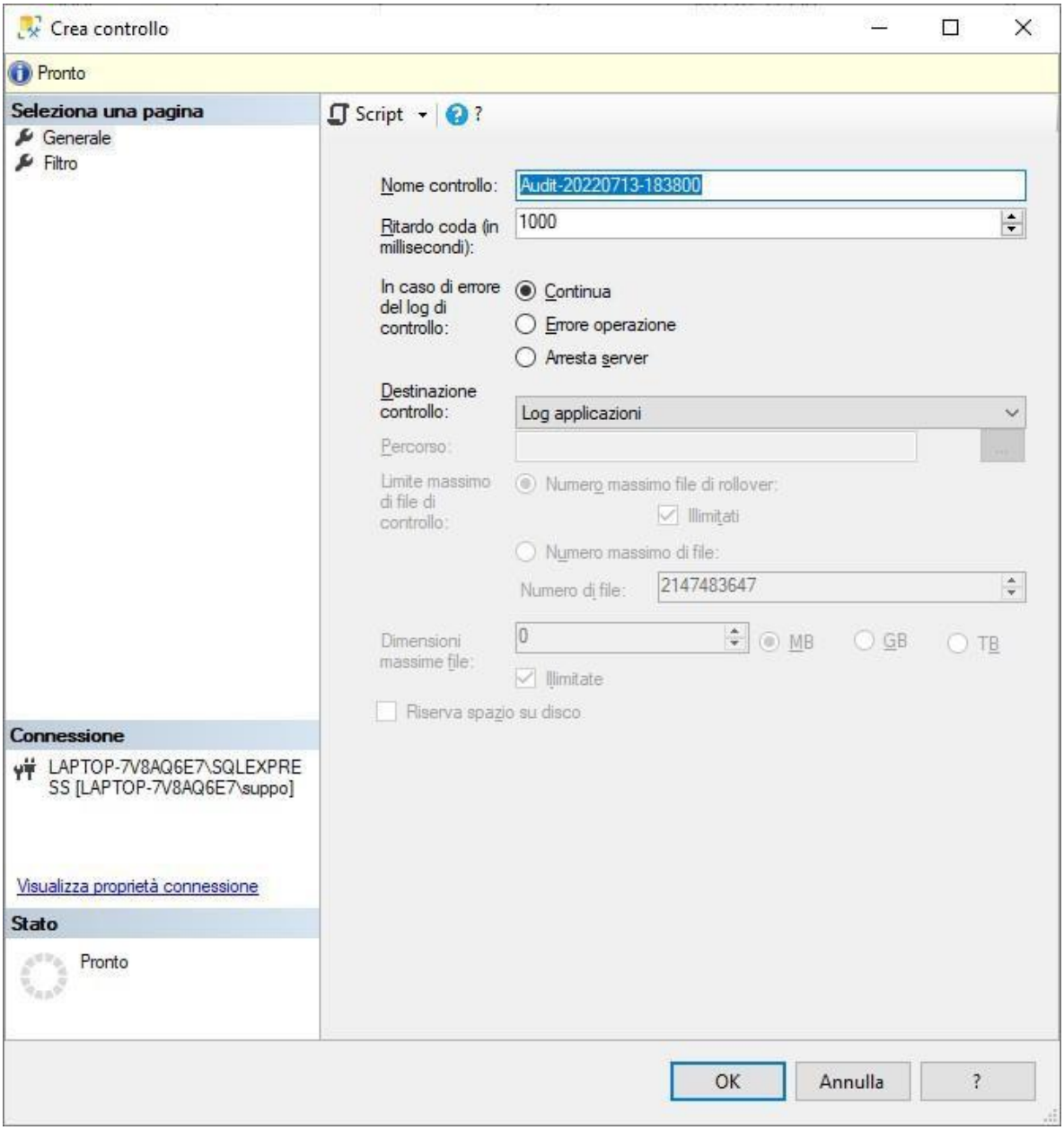
Successivamente sarà necessario intervenire in SQL Server utilizzando una StudioManagement

Una volta connessi (come amministratore di SQL), espandere l'albero a sinistra e selezionare Sicurezza > Controlli

Fare clic destro su Controlli > Nuovo Controllo:



Dare, eventualmente un titolo diverso al controllo (audit) e selezionare come Destinazione controllo: Log Applicazioni

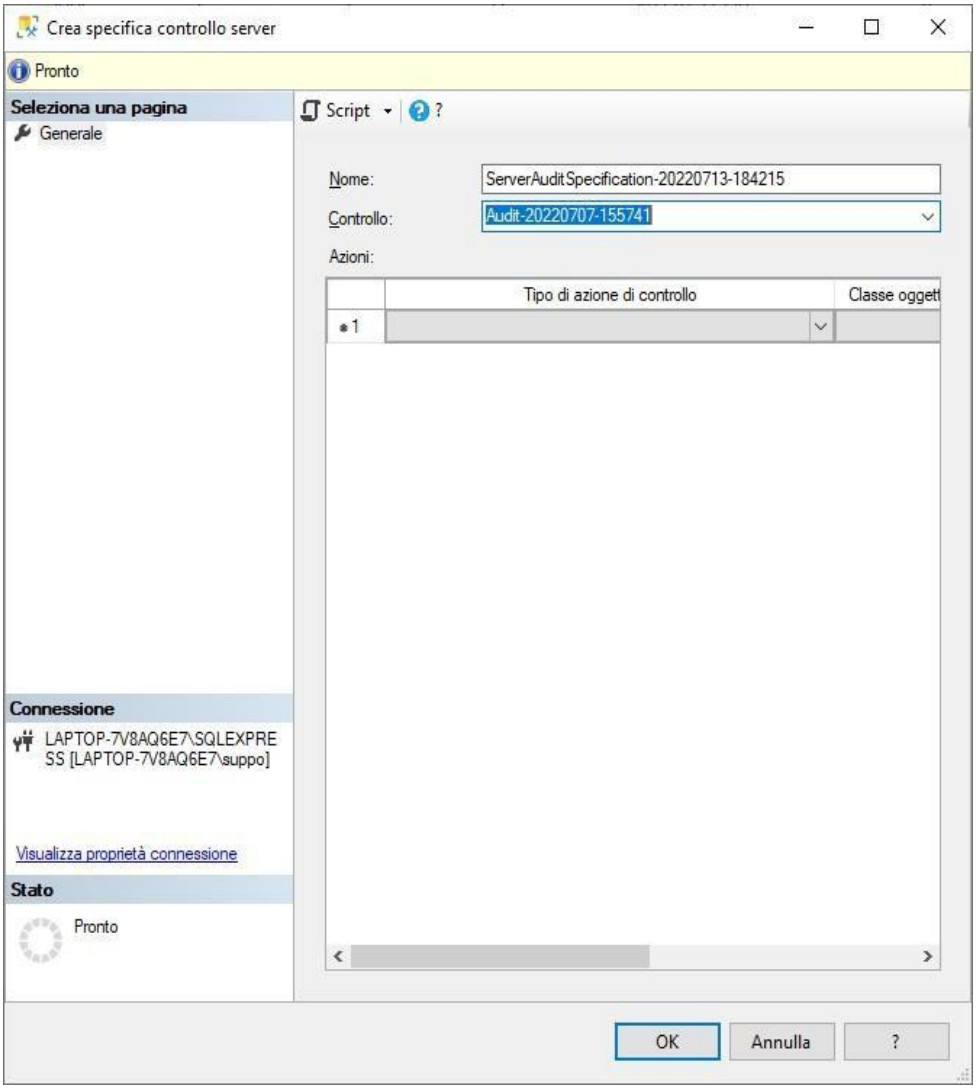


Dare OK e chiudere la finestra.

A questo punto è possibile programmare eventi a livello server o livello database

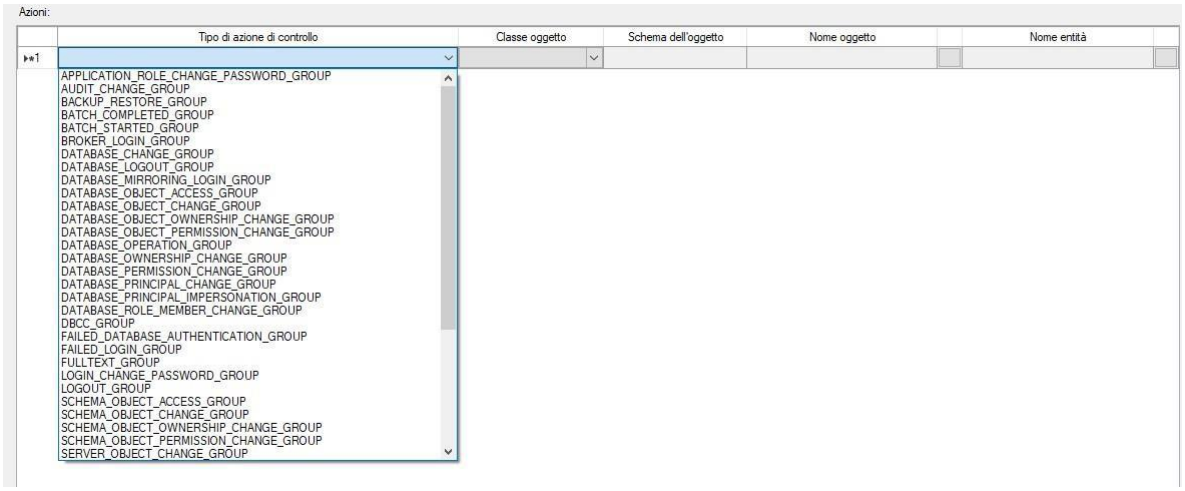
LIVELLO SERVER

Seleziona, poco più in basso, Specifiche controllo server, clic destro > Nuova specifica controllo server

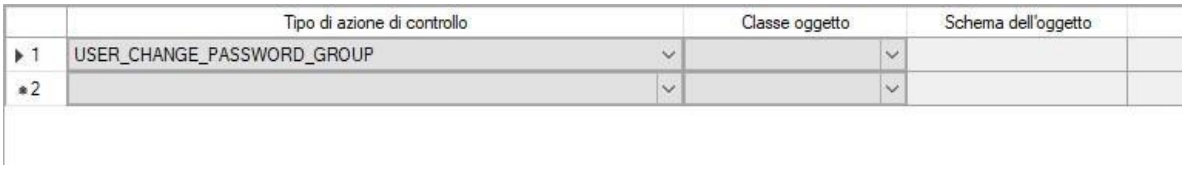


Selezionare, come Controllo, l'Audit appena creato (dovrebbe comparire nel menu a tendina).

Ingrandite la finestra e agite nella griglia centrale:



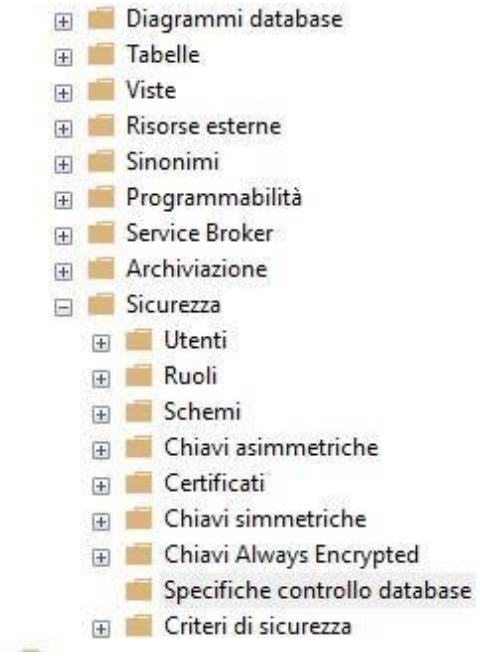
Ad esempio:



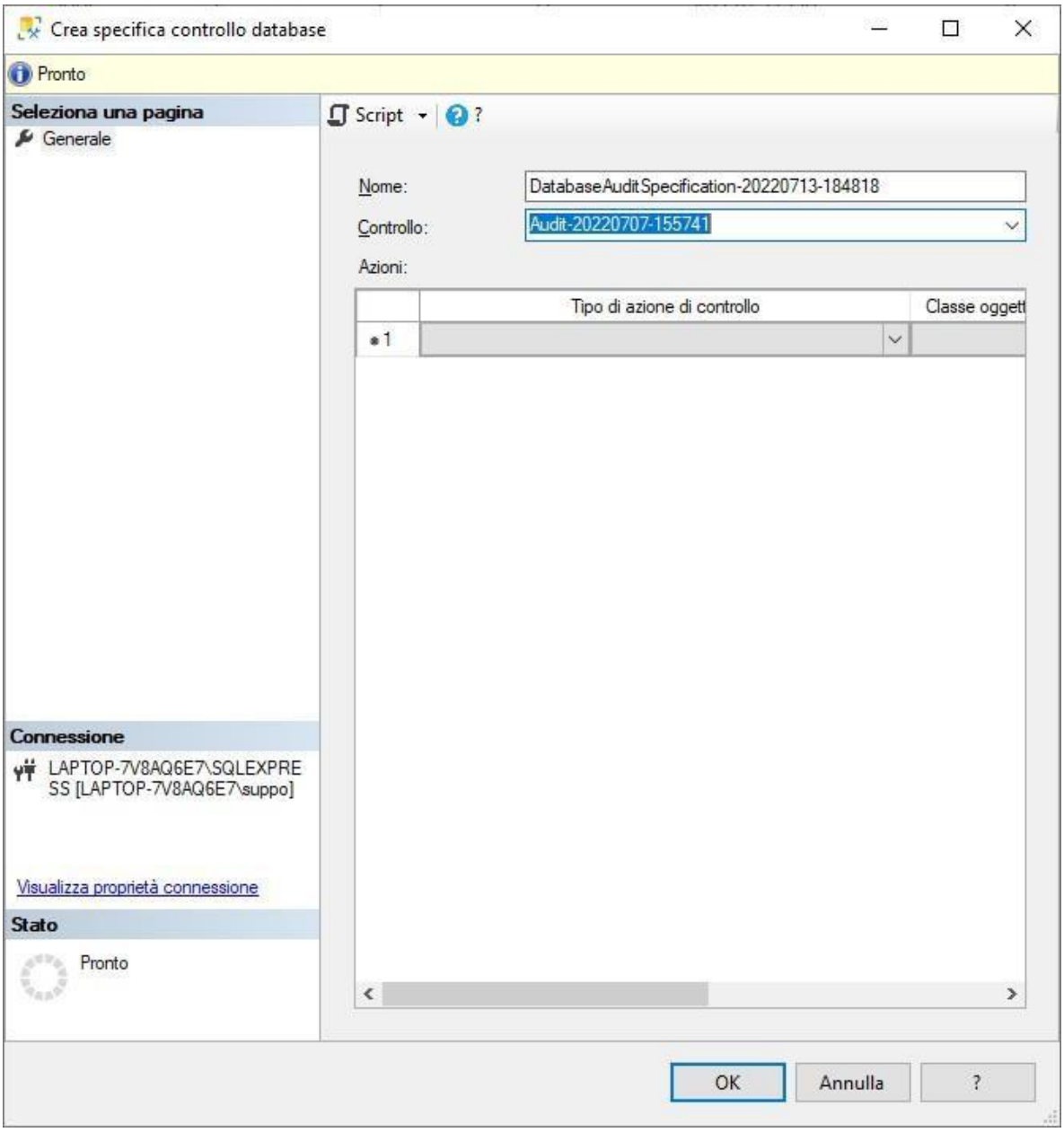
Consultatevi con il vostro esperto di SQL server per capire quali audit siano necessari a livello server

LIVELLO DATABASE

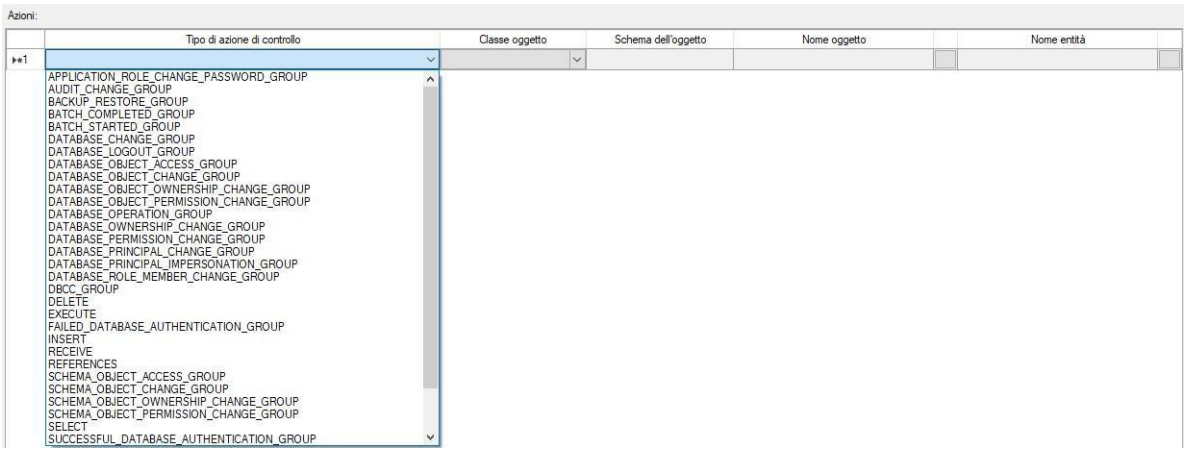
Espandete il DATABASE che intendete controllare e selezionate Sicurezza > Specifiche controllo database:



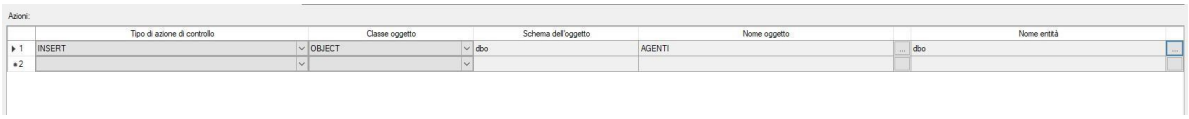
Analogamente agli audit server, create un nuovo controllo e associatelo al Controllo:



Espandete la finestra e agite sulla griglia centrale:



Qui potete inserire controlli a livello globale (database) o di una specifica tabella, ad es:



Questo controllo inserirà un log ogni volta che un utente (con schema dbo) eseguirà un insert in una specifica tabella (Agenti) del corrente DB

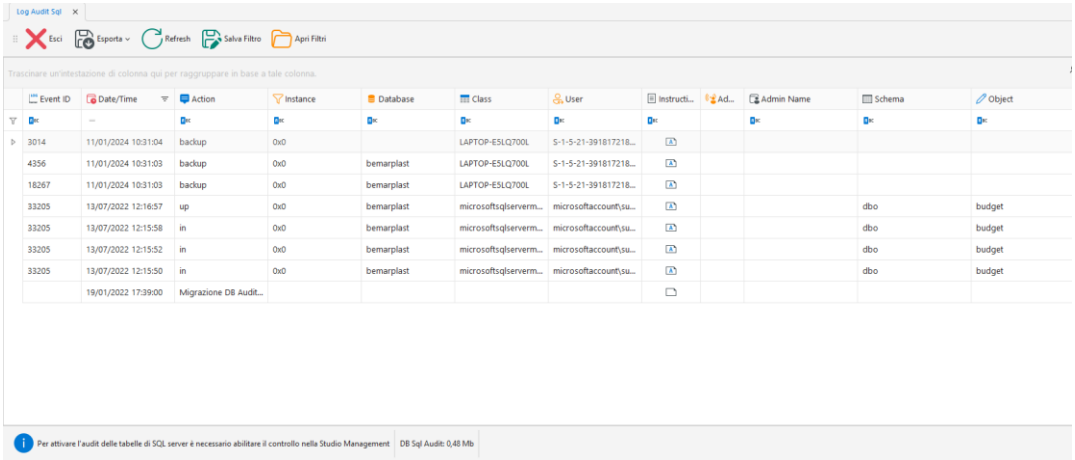
Ls classe oggetto determina il tipo di controllo (globale, di schema o di tabella) Il

nome oggetto rappresenta il db, uno schema o la tabella da specificare

Sono possibili diverse modalità di controllo, consultatevi sempre con il vostro esperto di sql server per capire quali controlli siano necessari per la vostra sicurezza.

NB: non scordatevi di ATTIVARE l'audit (è disabilitato di default). Qualsiasi modifica all'audit va effettuata con i controlli DISABILITATI

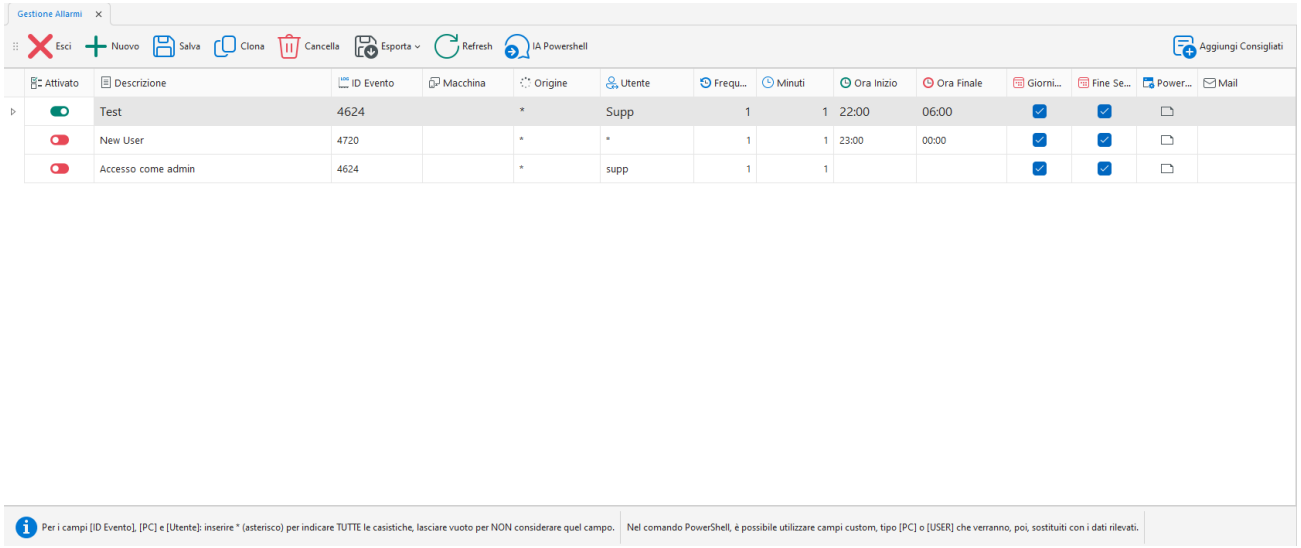
Dal momento che questi controlli saranno attivati, i log verranno scritti nell'apposita tabella (separata), nel menu principale > Log Audit SQL



Gestione Allarmi

Questa sezione imposta dei valori che, quando confrontati in fase di registrazione, manda una mail a TUTTI gli utenti contrassegnati come Amministratori con una mail IMPOSTATA. (Tabella Utenti) e al bot Telegram.

ALLARMI EVENTI

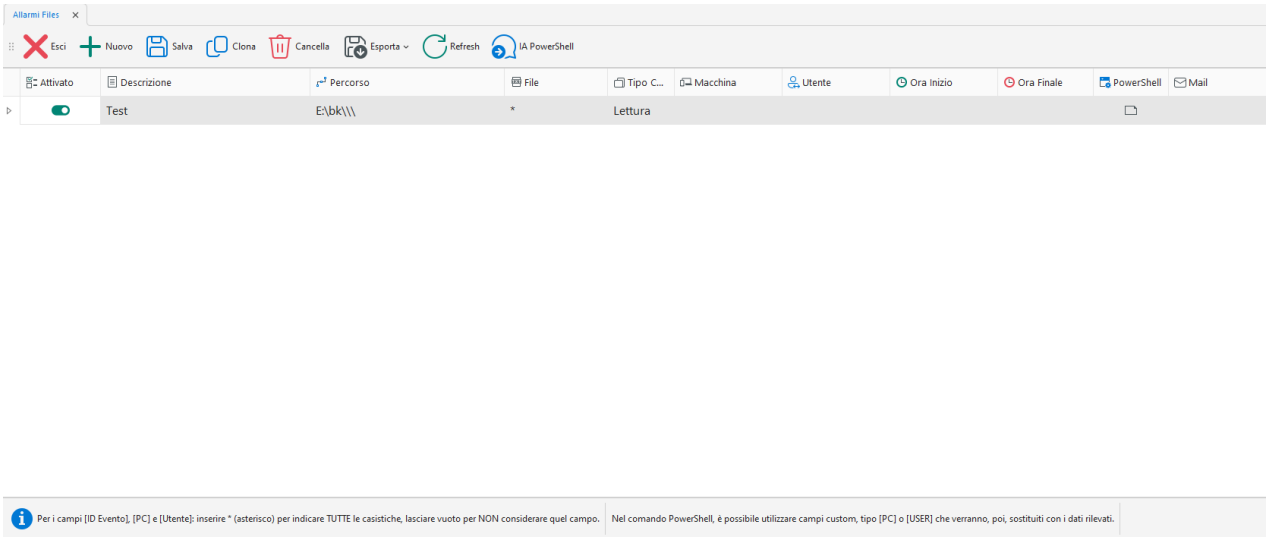


Qui si possono specificare i tipi di controllo che si vogliono applicare ad una specifica macchina/macchine e/ e ad uno specifico utente/utenti negli orari specifici stabiliti.

È possibile indicare anche un “frequenza”, cioè dopo QUANTI eventi registrati, il sistema spedisce la mail con l’allarme rilevato, questo lavora in combinata con la colonna “Minuti”, in questo modo sarà possibile gestire allarmi che si verificano con X frequenza in base ad un range di X Minuti

È disponibile un pulsante che inserisce automaticamente gli allarmi consigliati (saranno, inizialmente, disattivati)

ALLARMI FILES



Questa sezione e vincolata all'attivazione del controllo files

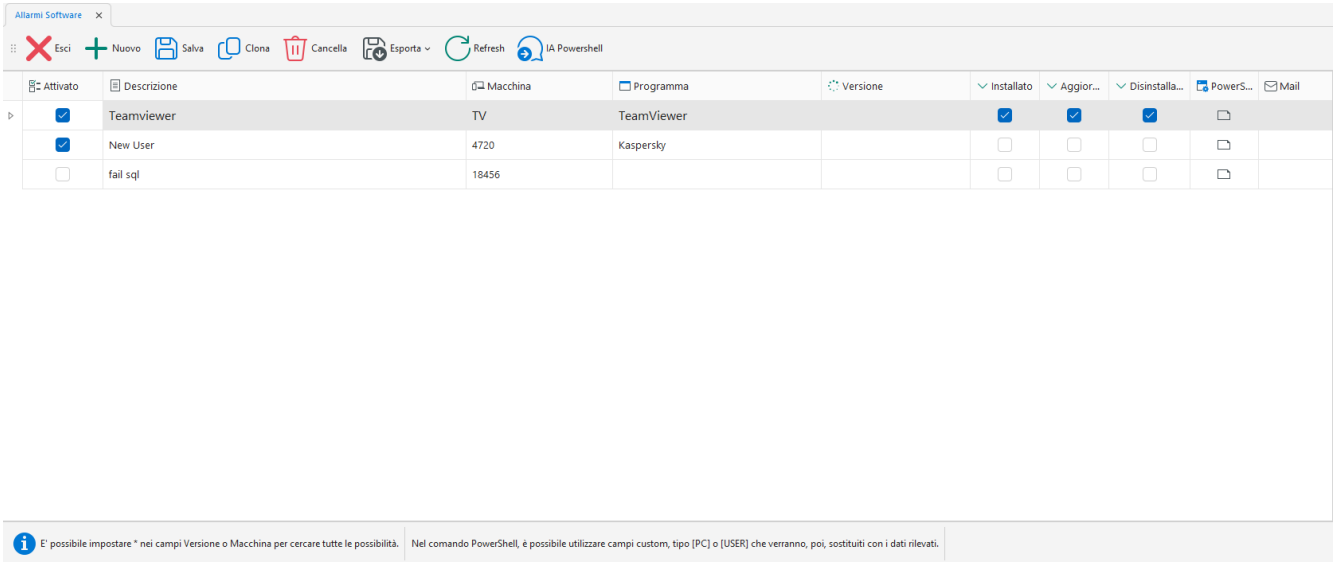
È possibile inserire allarmi che si attivano alla rilevazione di un evento associato all'allarme La

colonna percorso indica la path di riferimento

La colonna File indica se deve essere preso in considerazione uno specifico file oppure tutti i files contenuti nella cartella di riferimento

La colonna "Tipo di controllo" indica se l'allarme si deve attivare in caso di Lettura, Scrittura o Eliminazione (o tutti e 3 i casi)

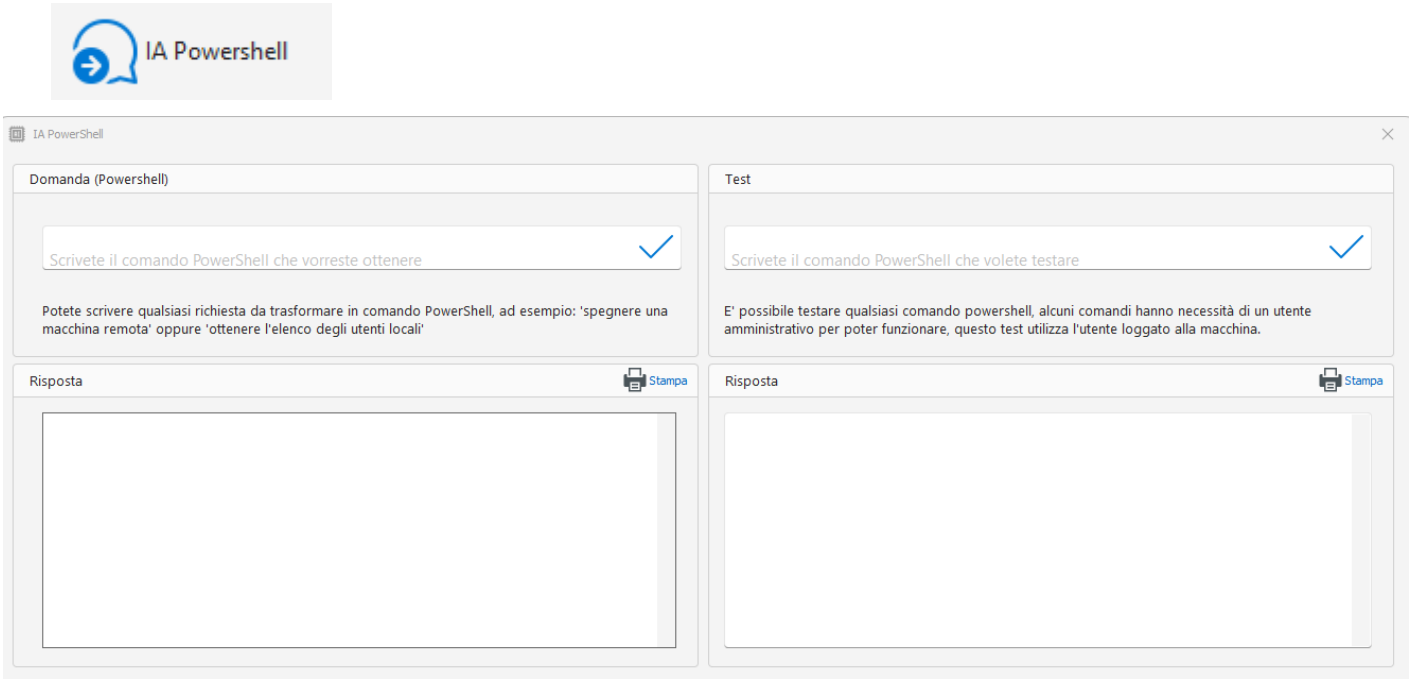
ALLARMI SOFTWARE



Questa sezione e vincolata all'attivazione dell'inventario software e hardware nelle impostazioni.

È possibile inserire allarmi che si attivano alla rilevazione del software specificato (in macchine specifiche oppure tutte) in caso venga rilevata un'installazione, aggiornamento o disinstallazione.

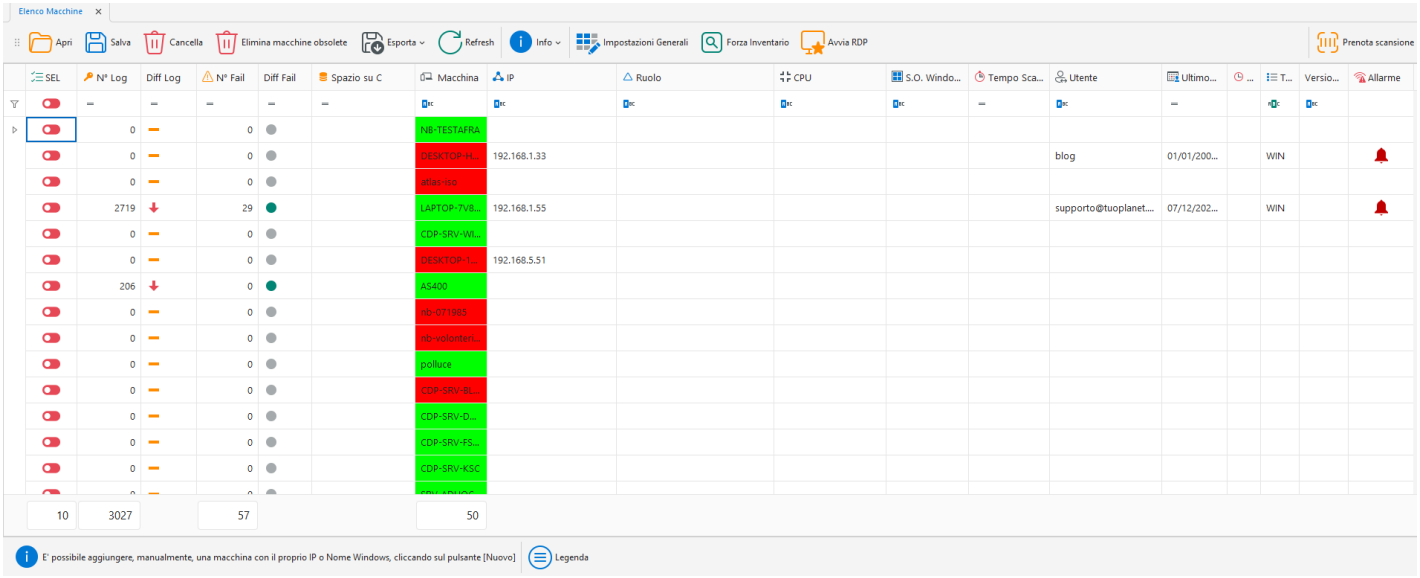
All’interno di ogni schermata relativa agli Allarmi, troverete IA Powershell



È possibile trasformare e testare una richiesta in un comando Powershell.

N.B. Alcuni comandi necessitano di un utente amministrativo per poter funzionare.

Elenco macchine



L'elenco macchine visualizza tutti i PC rilevati dalla procedura automatica In

VERDE le macchine per cui l'ULTIMA scansione è andata a buon fine

In ROSSO quelle con problemi durante l'ULTIMA scansione (vedere gli "Eventi interni" per capirne il motivo)

In GIALLO le macchine sotto scansione IN QUESTO MOMENTO Ven-

gono visualizzati:

Ultima Scansione: quando è stata effettuata la scansione per il recupero dei log

Ultimo accesso: data e ora dell'ultimo accesso interattivo

Spazio disponibile: Lo spazio, in Gb, disponibile in quella macchina nel disco C

Tempo Scansione: Tempo, in minuti, impiegati dal processo di scansione remoto

RT: La macchina e sotto controllo dal sistema BLogRT

Versione Client: La versione che dovrebbero avere i client RT, se diverso viene indicato in ROSSO.

La colonna IP indicherà, inizialmente, l'IP utilizzato per risolvere il nome macchine (viene utilizzata la Reverse Zone del DNS)

Utente visualizza l'ultimo utente che ha fatto accesso alla corrispondente macchina

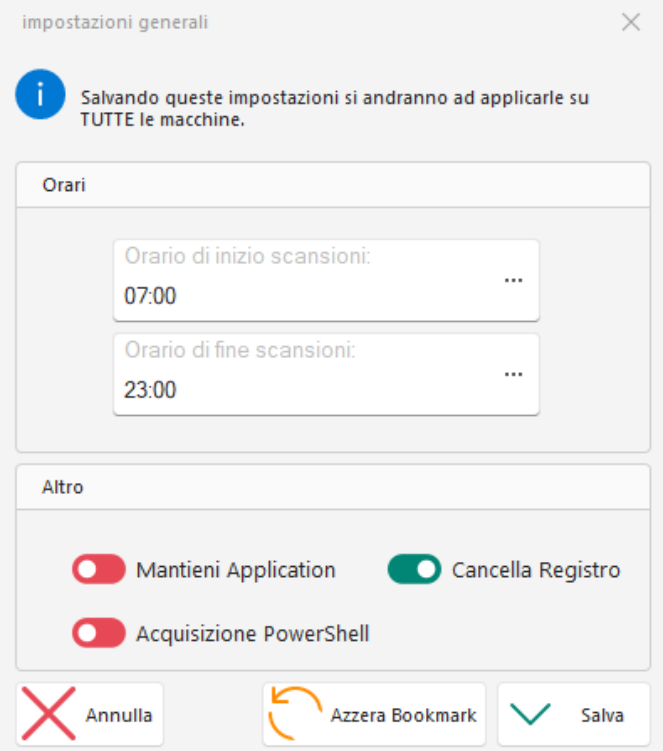
Tipo: La tipologia della macchina (WIN, SYS o RT)

[**Forza Inventario**]: fa partire (entro 1 minuto) la scansione macchine

[**Prenota Scansione**]: prenota la macchina selezionata alla prima scansione utile

Le Impostazioni Generali

Permettono di aggiornare contemporaneamente le impostazioni specificate per tutte le macchine; ideale per fare un'impostazione generica e poi lavorare sulle eccezioni.

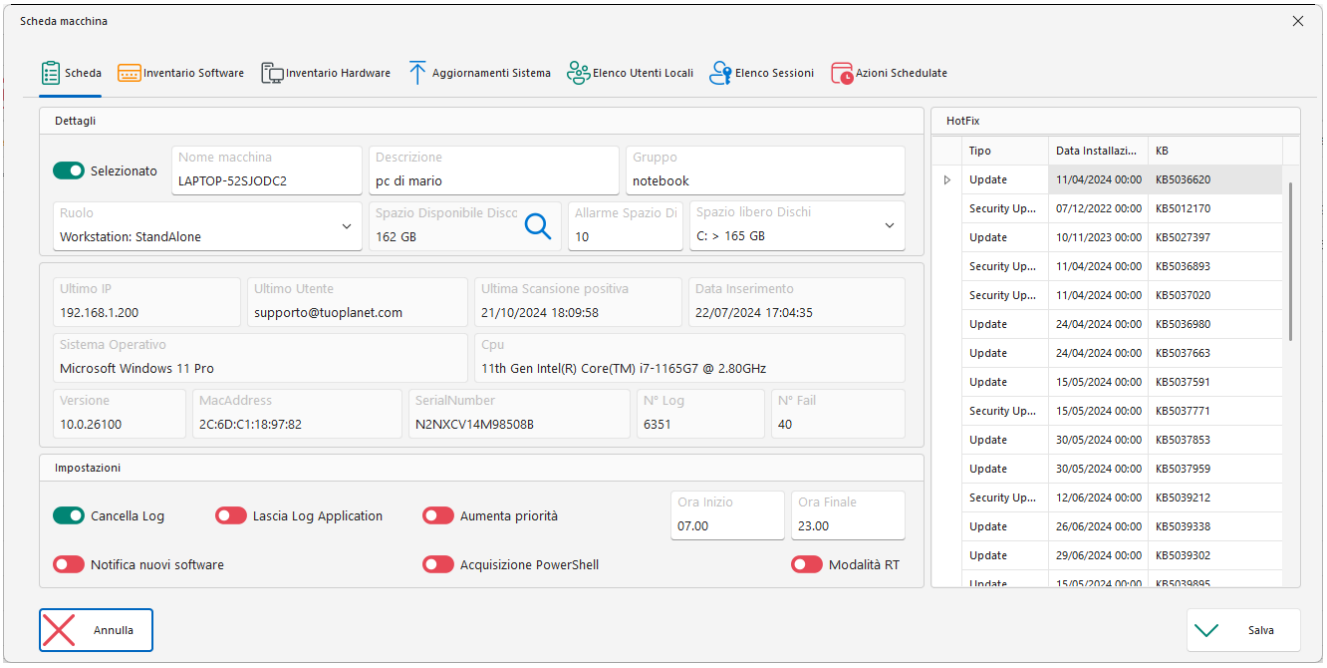


- Mantieni Application è utile nel caso in cui , in queste macchine, ci siano messaggi informativi o di errore prodotti da client gestionali, in questo caso la categoria Application NON viene mai azzerata

- Cancella Registro: le categorie Application e Security verranno azzerate ad ogni ciclo di scansione, è utile per mantenere pulito il registro ed evitare possibili corruzioni

- Acquisizione PoweShell: se si sono attivate le voci di registrazione dei comandi powershell, si possono abilitare le registrazioni nei log per una visione completa dei comandi PowerShell avviati in tutte le macchine.

Cliccando su [Apri] su ciascuna macchina si apre la relativa scheda tecnica:



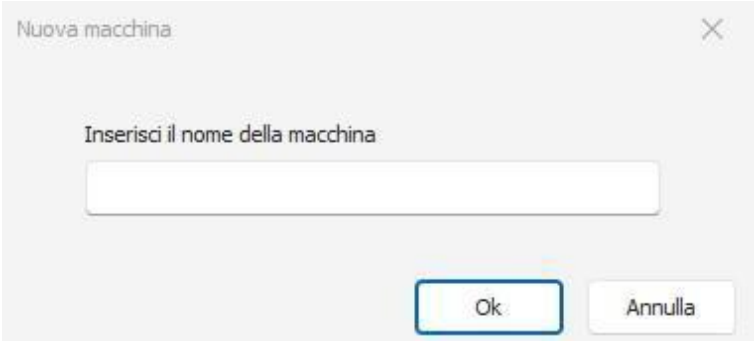
In questa scheda è possibile modificare alcune impostazioni relativa alla macchina selezionata.

Nell'elenco a destra saranno visualizzati tutti gli utenti che hanno fatto accesso alla macchina, Nei

relativi Box, compare lo spazio disponibile (disco C)

È possibile impostare un allarme di raggiungimento soglia, impostando un valore nel campo "Allarme Spazio"

È possibile anche cliccare su [Nuovo] per inserire il nome macchina (o IP) manualmente:

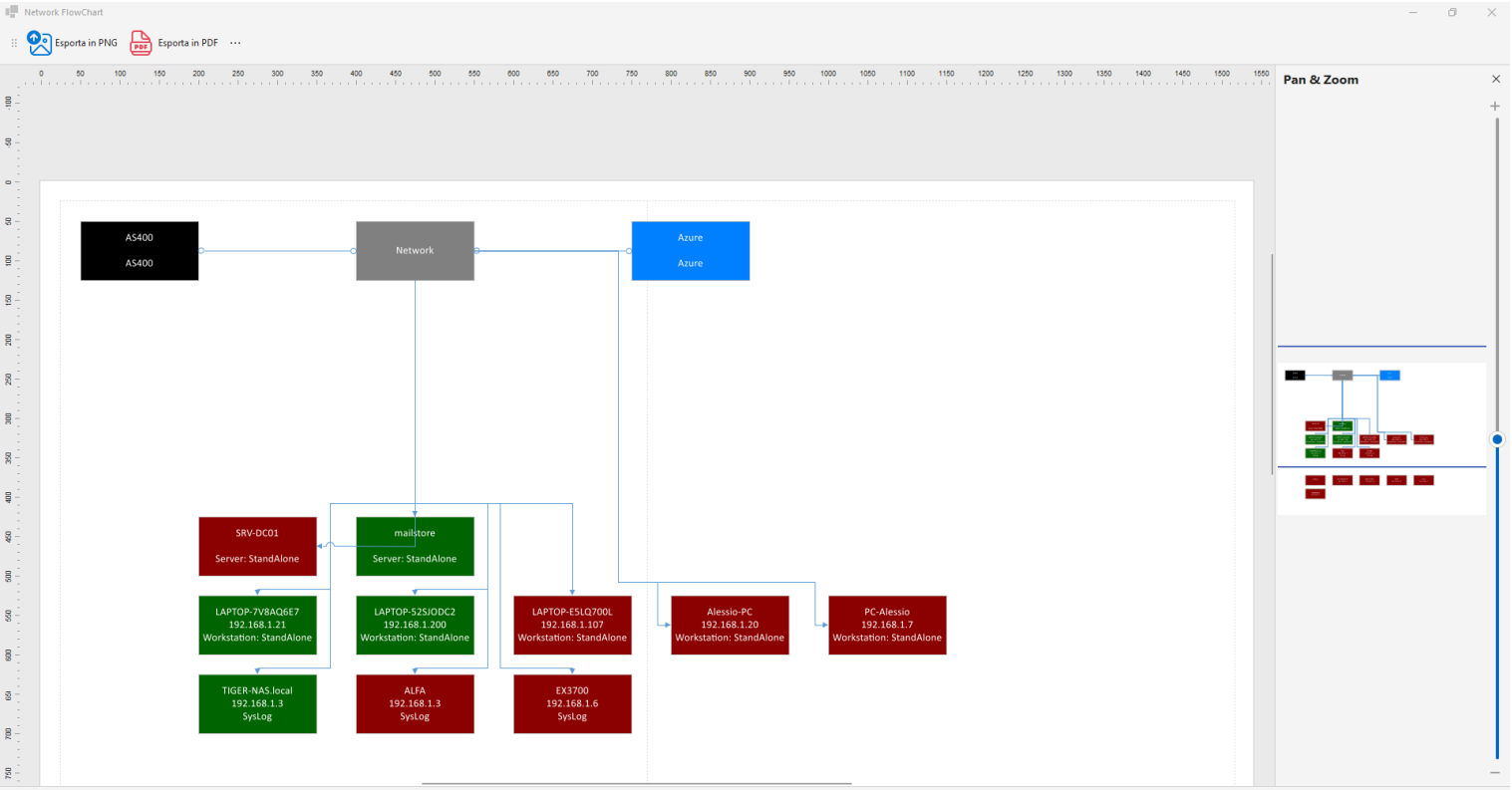


Network Flow Chart

Cliccando su Info > Network FlowChart si può ottenere una Chart con la rappresentazione grafica della rete, così come la identifica il programma.

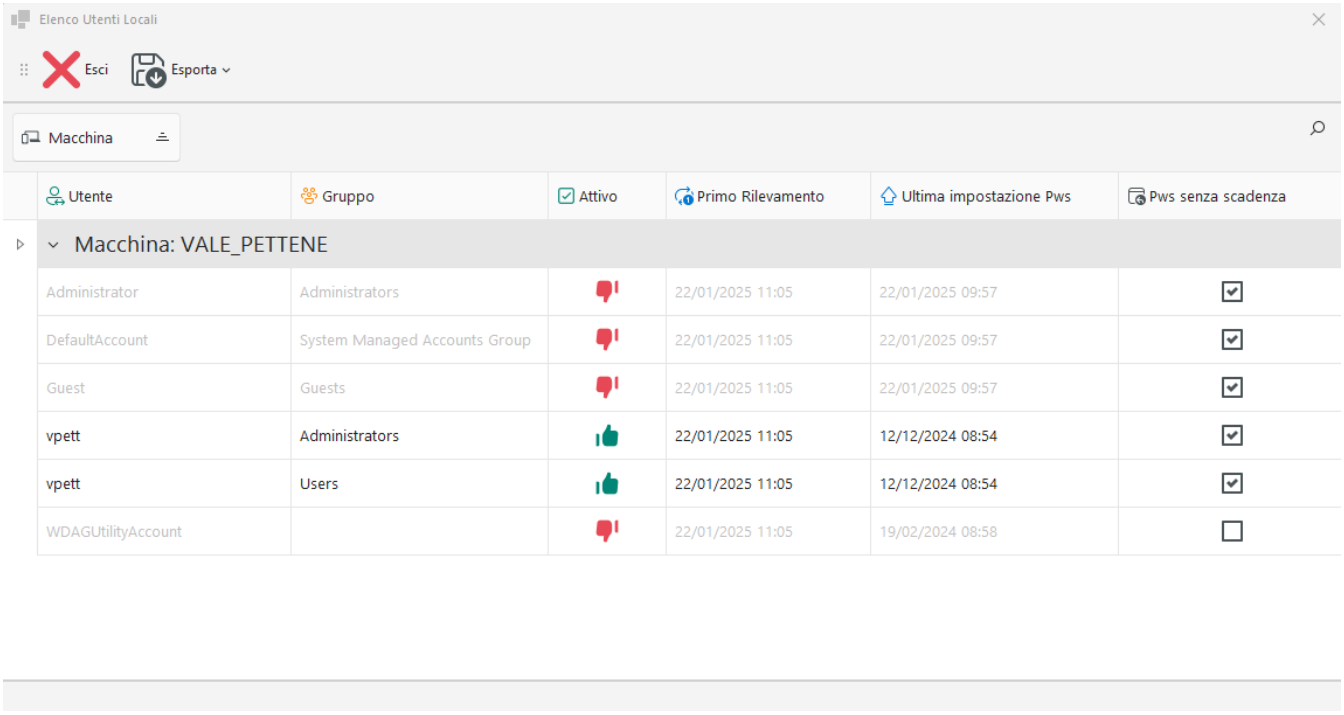
Per le macchine non ben identificate è possibile agire nelle corrispondenti Schede Macchine e specificando, manualmente, nella sezione [Ruolo[

Quindi si ottiene:



La Chart è esportabile in PDF o PNG

Elenco Utenti Locali



È possibile visualizzare gli utenti locali alle macchine.

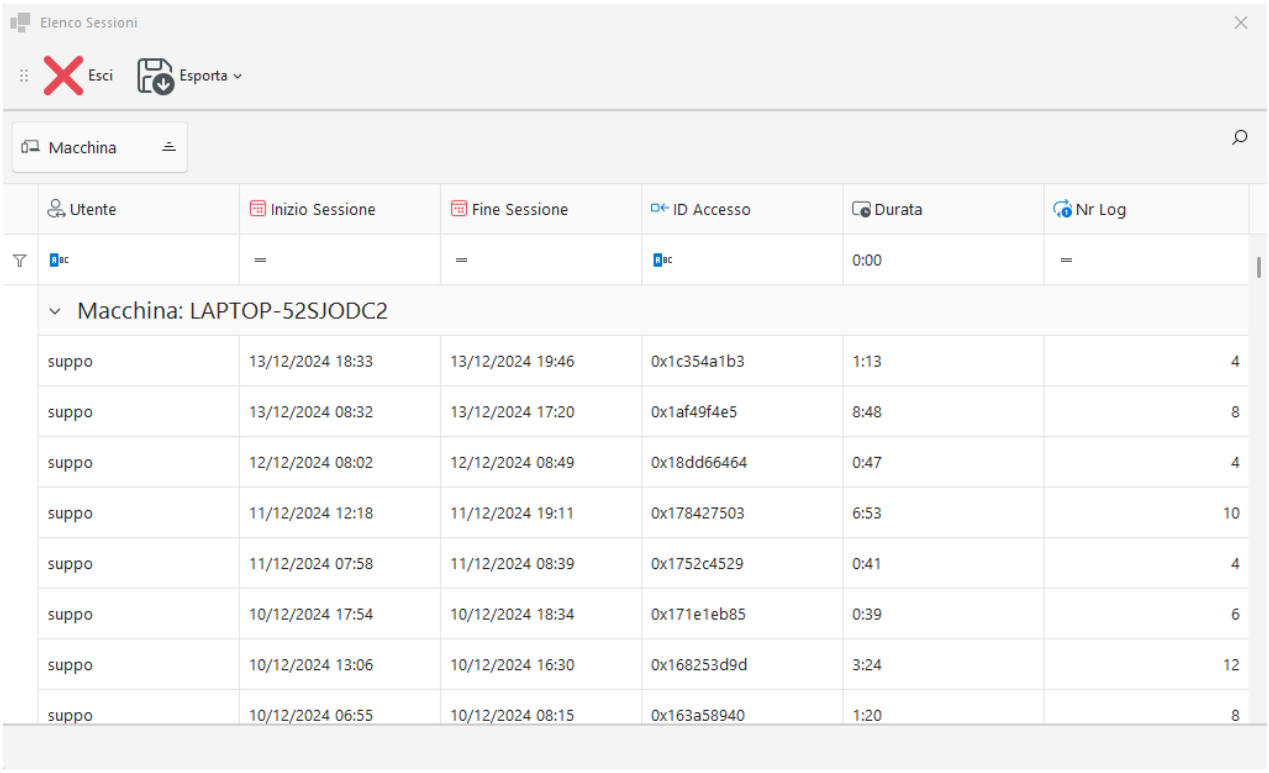
Nella sezione corrispondente al server AD verranno elencati tutti gli utenti generati in Active Directory

La colonna Ultima impostazione Pws è indicativa dell'ultima volta in cui l'utente ha modificato la propria password

La colonna "Pws senza scadenza" indica se l'account in questione ha il flag di "senza scasenza" per la password

Questo elenco può essere utilizzato per verificare gli account in essere e quelli obsoleti e tutti quegli utenti con un impostazione della password errata (fate riferimento alla normativa privacy vigente)

Elenco sessioni

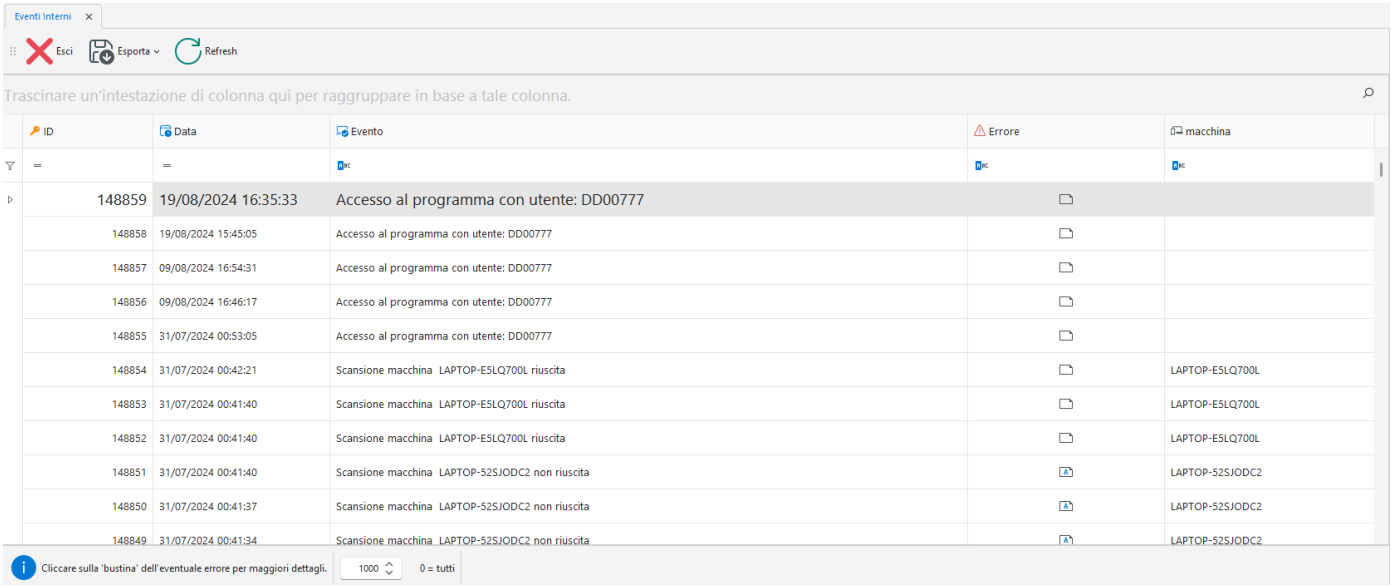


Questa finestra mostra, per ciascuna macchina WINDOWS le sessioni iniziate e concluse, rilevate dalla Working Log.

Per ogni macchina viene visualizzato l'inizio e la fine di ogni sessione, L' Accesso della sessione, la durata (in ore; minuti) e il numero di log coinvolti in quella sessione.

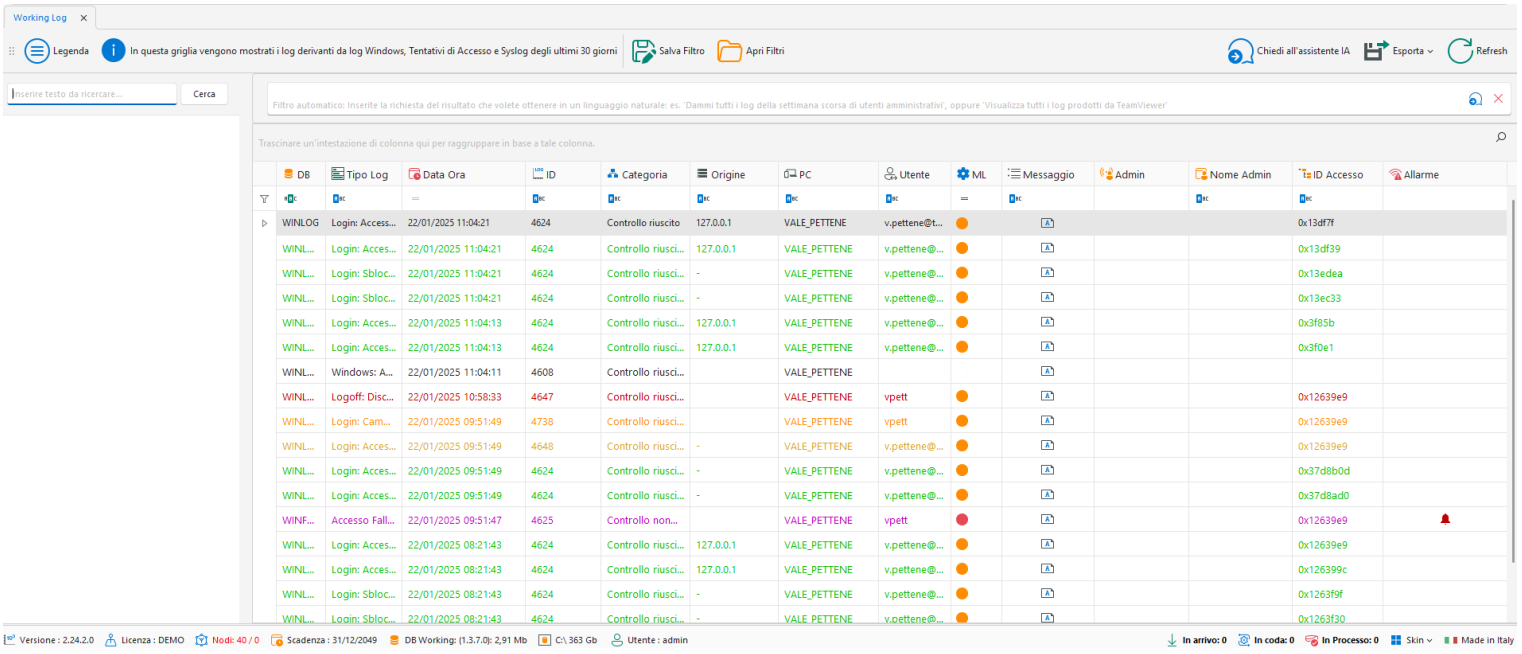
L'aggiornamento delle sessioni è UNA volta al giorno (in modalità notturna).

Eventi interni



L'elenco degli eventi interni eseguiti dal programma, gli eventuali errori sono contenuti nella "bustina" nell'ultima colonna.

Working Log



La griglia “Working Log” è uno strumento potente e versatile e permette di effettuare ricerche, filtri, ordinamenti e raggruppamenti in tempo reale su tutto l’archivio log degli ultimi 30 giorni.

Per effettuare una ricerca tra i log, ad esempio una determinata macchina, è sufficiente scrivere l’iniziale della macchina nella colonna PC nella PRIMA RIGA (riga filtro) oppure utilizzare la funzione “Filtro” cliccando nell’iconcina a forma di imbuto nell’intestazione colonna (stile Excel)

La colonna “Data Ora” permette, utilizzando la funzione “imbuto” di visualizzare un pratico calendario con le funzionalità integrate.

Descrizione Colonne:

Area: L'appartenenza del log, i login vengono evidenziati iniziando per "Login: …

- Accesso Utente: login fisico dell'utente
- Blocco/Sblocco: accesso dell'utente dopo un blocco utente desktop o da screen saver
- Accesso Remoto: accesso da desktop remoto
- Accesso Cache: Accesso dell'utente mediante verifica cache (es. su un notebook disconnesso dal dominio)
- TeamViewer: Accesso alla macchina tramite la connessione remota TeamViewer
- VNC: Accesso alla macchina tramite la connessione remota VNC
- NoMachine: Accesso alla macchina tramite la connessione remota NoMachine
- Dameware: Accesso alla macchina tramite la connessione remota Dameware
- SpaskTop: Accesso alla macchina tramite la connessione remota SpaskTop
- Iperius: Accesso alla macchina tramite la connessione remota Iperius

ID: L'event ID originale di windows

Data/Ora: data e orario di creazione dell'evento

Tipo: tipologia del log

Origine: applicazione o servizio di origine dell'evento

Categoria: categoria del log

PC: macchina in cui si è generato l'evento

Utente: utente legato alla generazione dell'evento

Messaggio: messaggio completo originale dell'evento

Login: se appare una "chiave" vuol dire che l'evento è stato generato da un accesso interattivo. (obsoleto)
Admin: l'utente rilevato è uno degli amministratori indicati nell'elenco amministratori

Nome Admin: il nome indicato nell'elenco amministratori

Inoltre, vengono evidenziate i login con colori diversi:

VERDE: Accesso di un utente secondo le diverse tipologie specificate nell'AREA

ROSSO: logout dell'utente

GIALLO: Accesso dell'utente con credenziali diverse dalle originarie

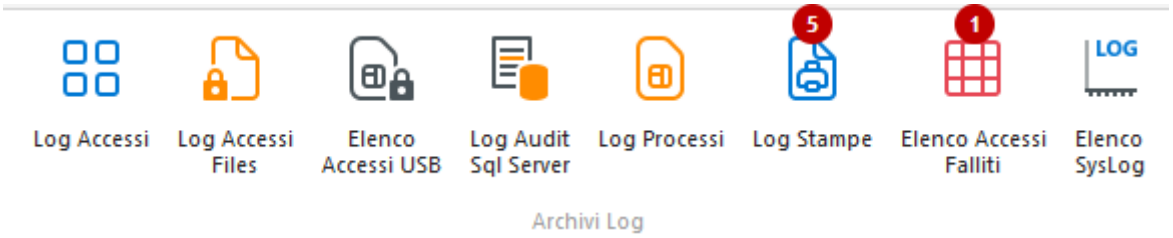
BLU: Accesso tramite Software di Desktop Remoto

ARANCIONE: Eventi legati alle password (cambiamenti, reset, ecc…)

BIANCO: Di minor importanza

Apertura files archiviati

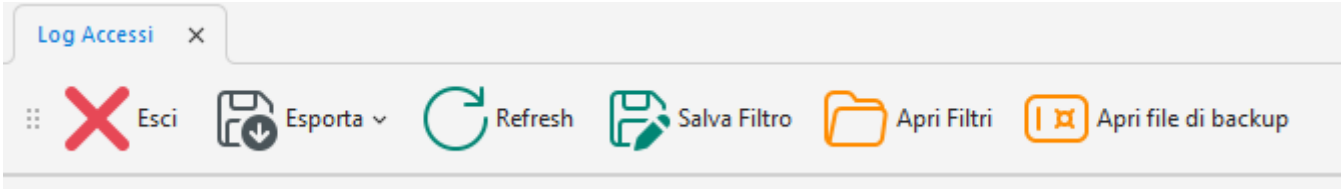
In tutte le griglie raggruppate in Archivi log



Troverete i record dei Log catalogati secondo la loro natura, in archivi separati, e conservati per il periodo indicato nella configurazione (retention) non inferiore ai 6 mesi.

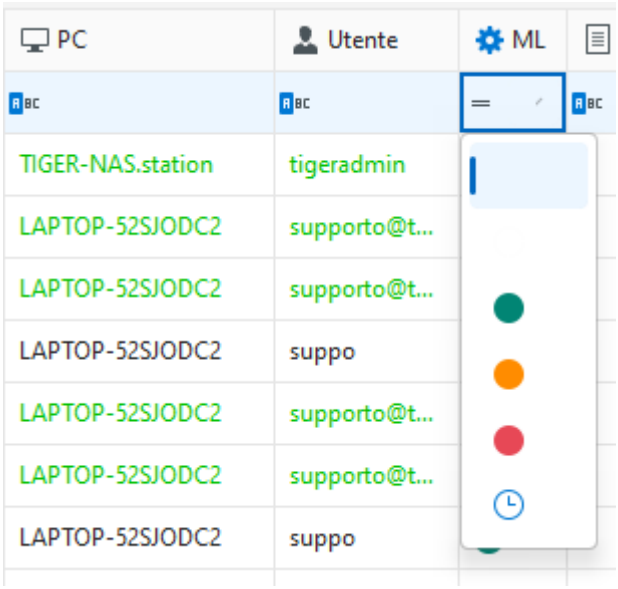
In ogni sezione troverete la possibilità di visualizzare, filtrare, raggruppare ed esportare l'archivio corrispondente.

In ultima troverete anche la funzione per riaprire file di archivio dei rispettivi database (estensione .vdb6)



Cliccando su "Apri file di backup" potrete cercare l'archivio conservato e riaprirlo temporaneamente, una volta caricato (i tempi dipendono dalla dimensione dell'archivio) la manipolazione dei dati è la stessa per il db corrente.

Machine Learning



BusinessLog ha integrata una Machine Learning che "impara" i log, man mano che vengono registrati ed è in grado di determinare l'utente che ha fatto accesso per stabilire se sia "atteso" o "non atteso" In particolare, trovate questa segnalazione nel working log o nei Log Accessi:

La colonna ML mostra la segnalazione della Machine Learning che ha 3 stati: VERDE:

L'utente rilevato corrisponde a quanto previsto dal modello

ARANCIONE: L'utente non corrisponde a quanto previsto ma, in ogni caso e riconosciuto come utente presente nei log

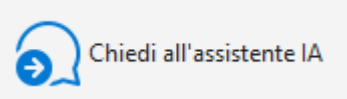
ROSSO: L'utente non corrisponde a quanto previsto e non è presente tra gli utenti registrati finora.

(OROLOGIO): L'utente è associato a quella macchina ma l'accesso rilevato NON è negli orari "consueti" fin qui rilevati

NORMALE che, inizialmente tutti le righe riportano ML arancioni o rossi, in quanto deve ancora imparare il registro archiviato, col tempo dovreste vedere le corrispondenze corrette.

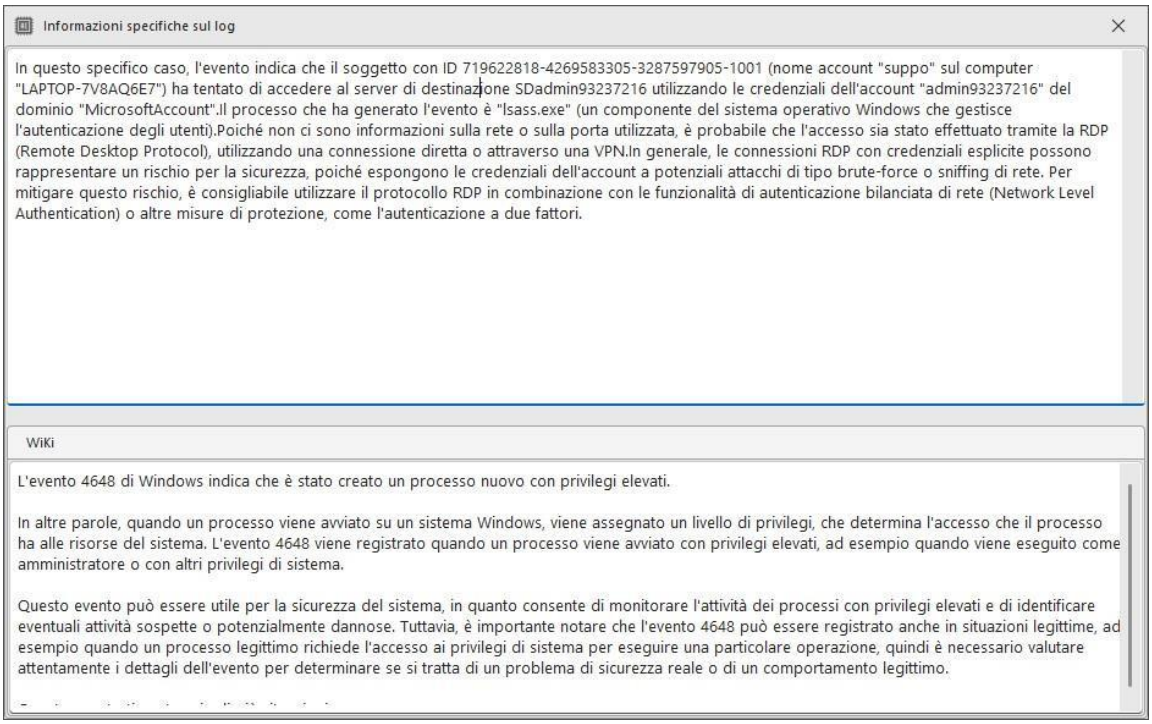
BusinessLog ha integrata la possibilità di “dialogare” con l’Intelligenza Artificiale per eseguire richieste mirate.

In particolare, è possibile chiedere chiarimenti, su uno specifico log, nella griglia dei Working Log Una volta selezionato il Log, è possibile cliccare sul pulsante (in alto a destra)



Oppure facendo doppio clic e selezionando:

In base al contenuto del log si otterranno maggiori informazioni dall’Intelligenza Artificiale:

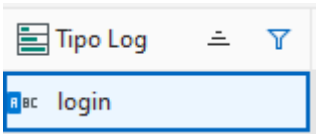


Nella parte bassa viene anche riportata la spiegazione dell’evento, in base alla Wiki integrata di BusinessLog.

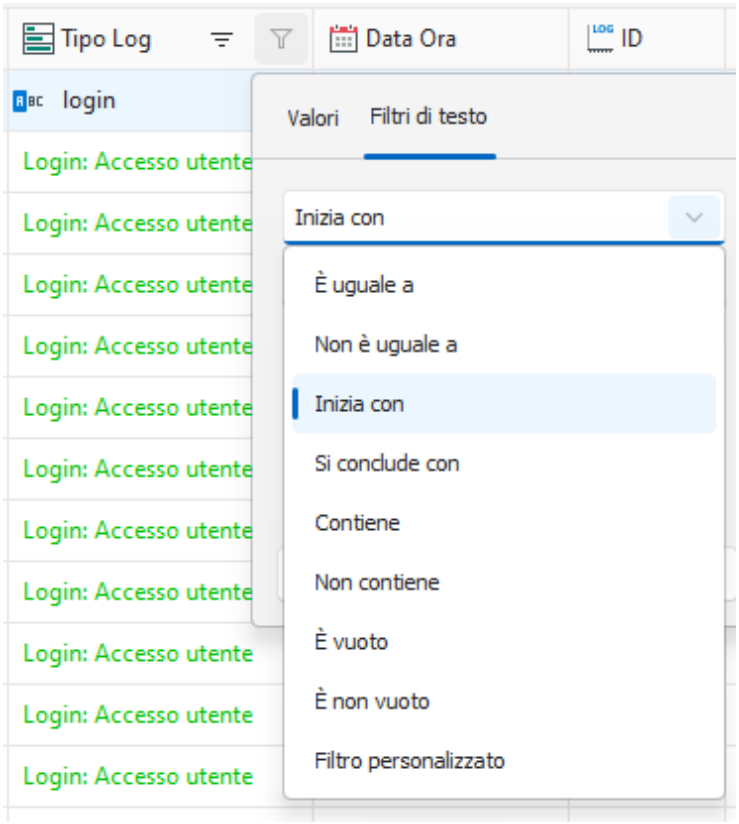
Salvataggio Filtri

Ogni volta che si esegue un filtro (per data, utente, macchina ecc…) si ottengono i dati filtrati con quella selezione (i tempi di visualizzazione dipendono dalla quantità di log e dai tempi di elaborazione della macchina)

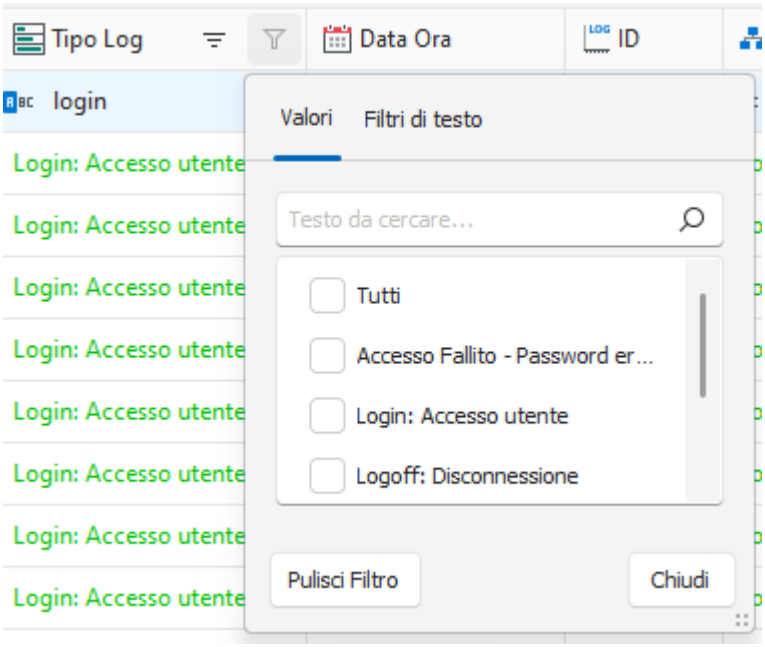
È possibile utilizzare la prima riga “filtro” per scrivere u filtro specifico:



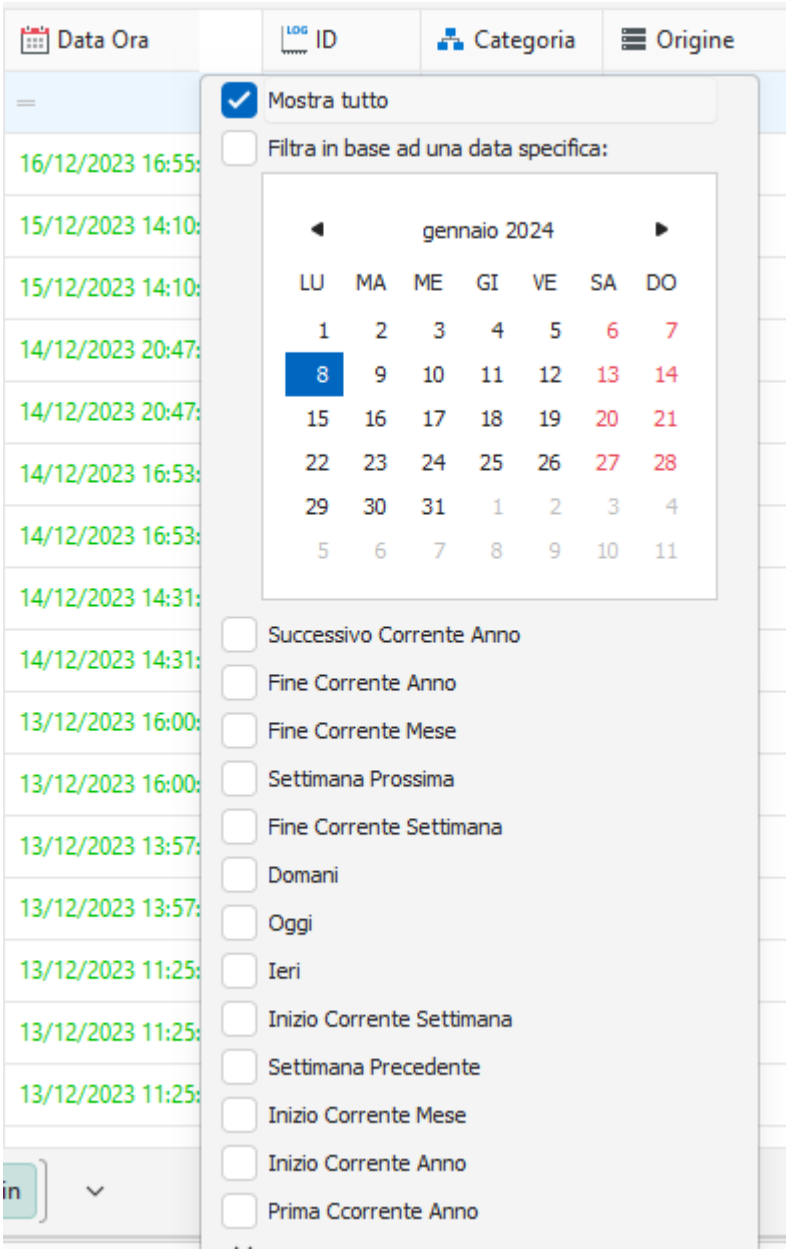
Oppure cambiare la modalità di filtro (cliccare su =, in questo caso)



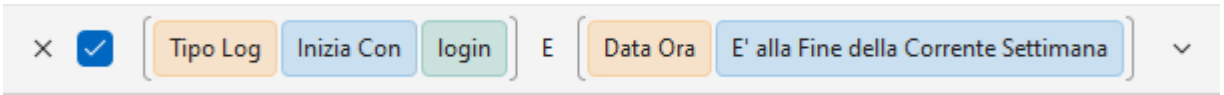
Oppure, cliccando sull'iconcina "imbuto" in alto a destra:



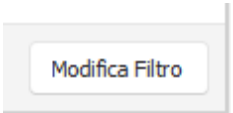
Il filtro automatico visualizzato si adatta al contesto, per cui, per filtrare una data, appare un calendario contestuale:

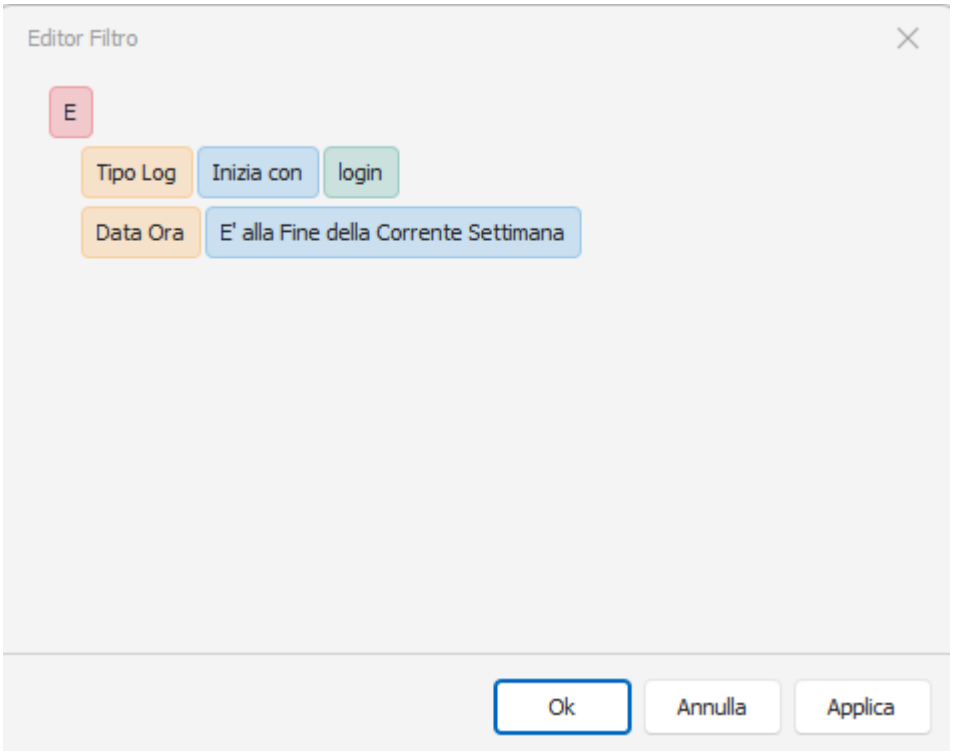


Il filtro viene riepilogato nella sezione inferiore:



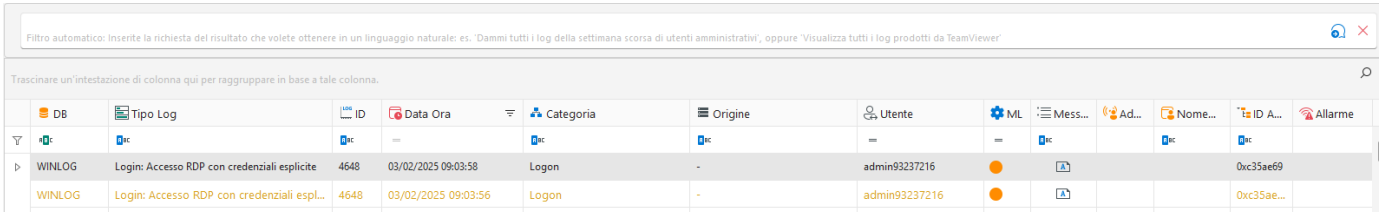
Qui è anche possibile modificare il filtro con una modalità manuale:





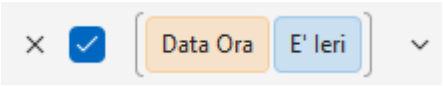
Ed introdurre filtri complessi anche in gruppo o in modalità and/or

Per facilitare la stesura di filtri in modo più semplice è possibile utilizzare il generatore basato su IA

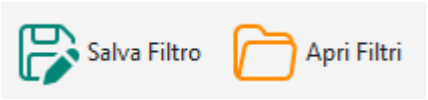


Sulle grigli di visualizzazione è stata integrata una riga per la compilazione automatica del fitro, utilizzando un linguaggio naturale ad esempio: “Mostrami i log di ieri”

In questo caso verrà generato il filtro:



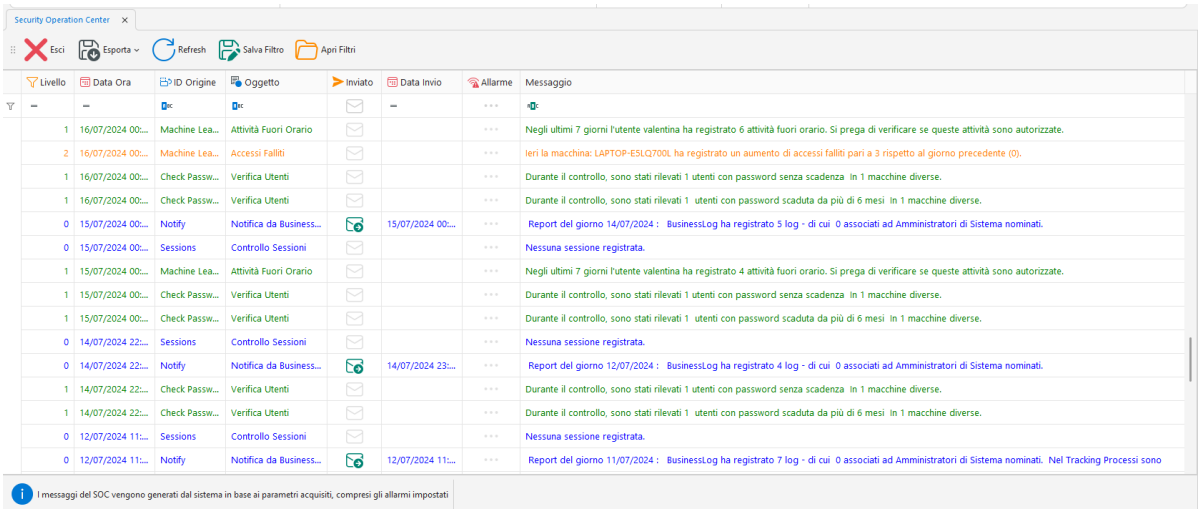
Questi filtri si possono salvare per un riutilizzo utilizzando i comandi:



Security Operation Center

Si tratta di una griglia di riepilogo che indica:

- Tutte le notifiche riepilogative spedite via mail/telegram
- Tutti gli allarmi rilevati e notificati
- Tutte le “considerazioni” rilevate dalla Machine Learning in base a quanto controllato nei dati



Livello = Livello di Attenzione della segnalazione (0 = Informazione, 1 Nota di rilievo, 2 Importante, 3 Critico)

ID Origine = Origine della notifica

Oggetto: Oggetto della notifica o della mail inviata

Inviata: Si evidenzia una “busta” se la notifica è stata inviata

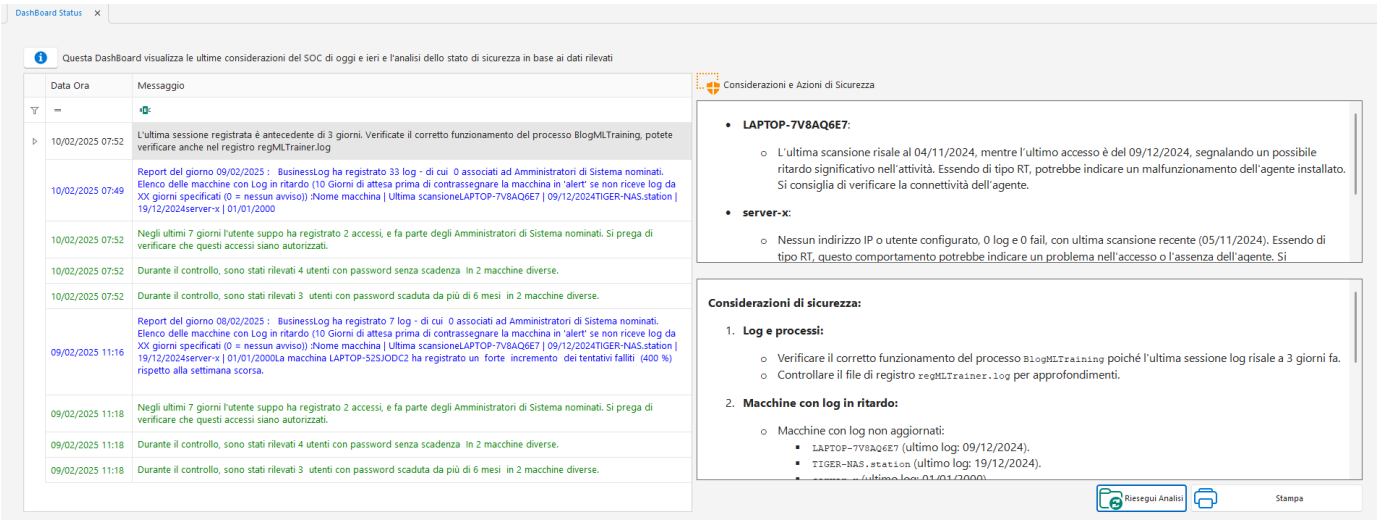
Data invio: Data dell’invio al sistema di mail/telegram

Allarme: Viene evidenziata una “campanella” se la notifica è scaturita da un allarme impostato

Messaggio: Il messaggio completo della notifica

DashBoard SOC

Nella DashBoard iniziale, vengono riepilogate le considerazioni SOC degli ultimi 2 giorni e, accanto, le riflessioni del sistema di analisi riguardo lo stato delle macchine e le segnalazioni del SOC (allarmi esclusi)



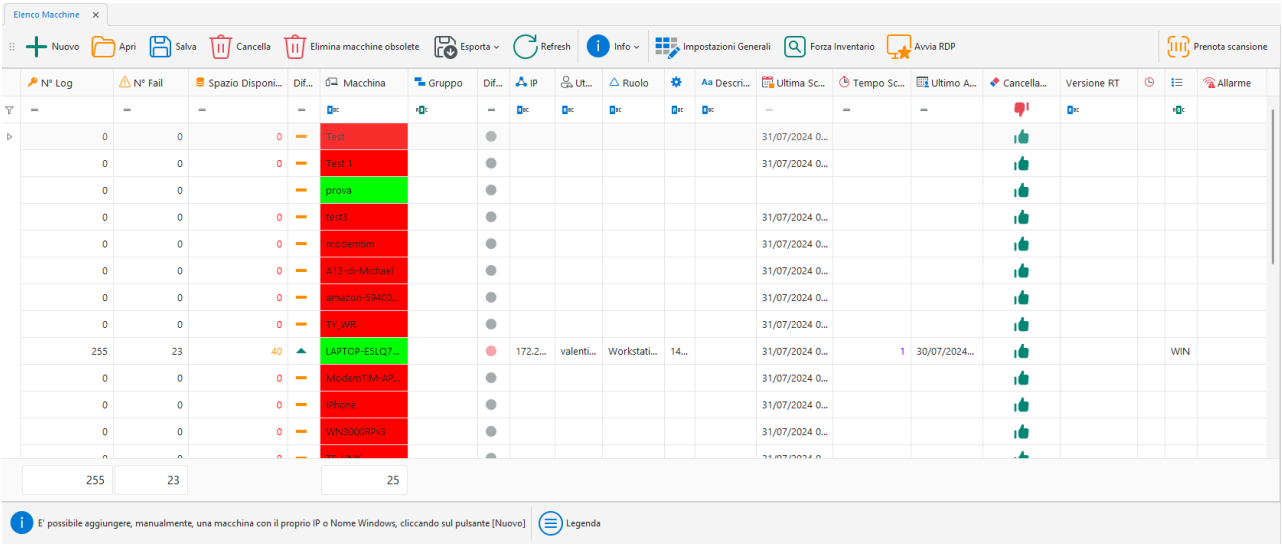
In questo modo è possibile ottenere indicazioni importanti sullo stato attuale e sulle eventuali azioni da effettuare.

Il testo completo è stampabile su un documento esportabile utilizzando il pulsante [Stampa]

Nel caso fosse necessario rieseguire l'analisi è possibile cliccare su [Riesegui Analisi]

PROBLEMATICHE DI SCANSIONE:

Aprendo Elenchi > Elenco macchine, potete visualizzarne lo “stato” di scansione:



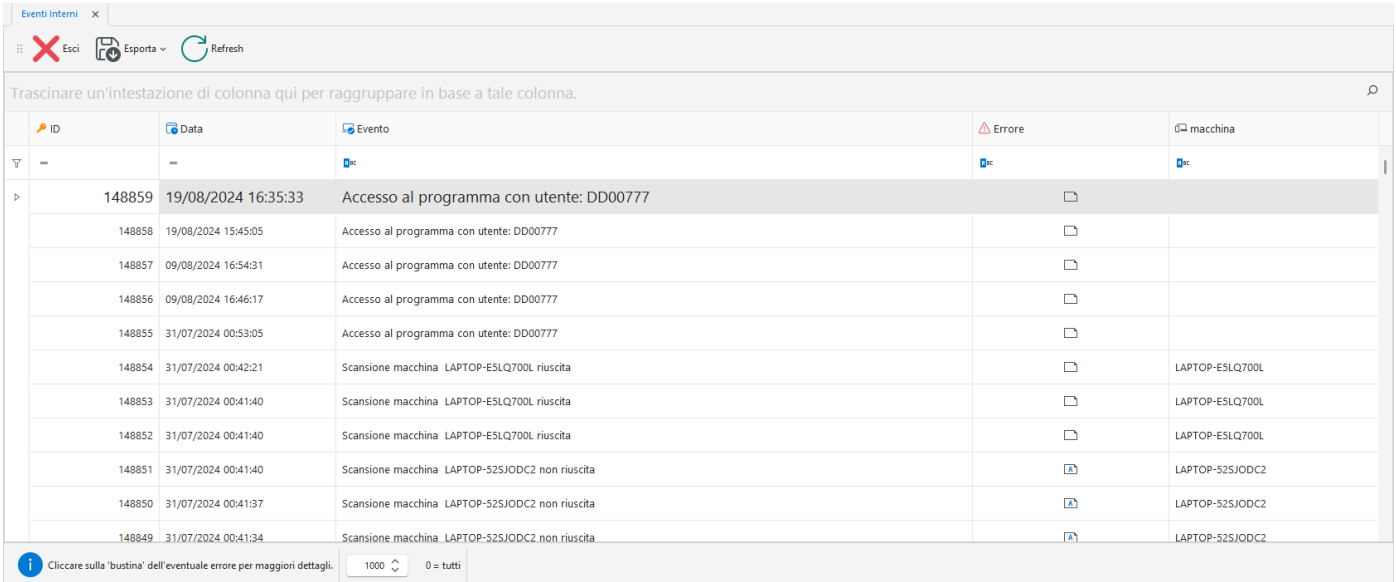
VERDE = Ultima scansione positiva

ROSSA = Ultima scansione negativa

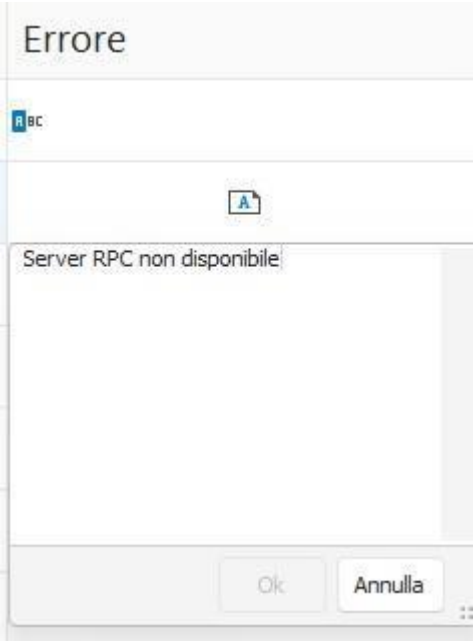
GIALLA = Scansione in corso

Fate attenzione alle macchine ROSSE con 0 log, queste macchine NON sono mai state oggetto di scansione e il sistema non riesce a prelevarne i log.

Aprendo Elenchi > Eventi Interni, troveremo anche un log interno sul possibile problema:



Eseguite una ricerca della macchina in questione (box ricerca in alto a destra) e visualizzate l’errore cliccando sulla “bustina” [A]

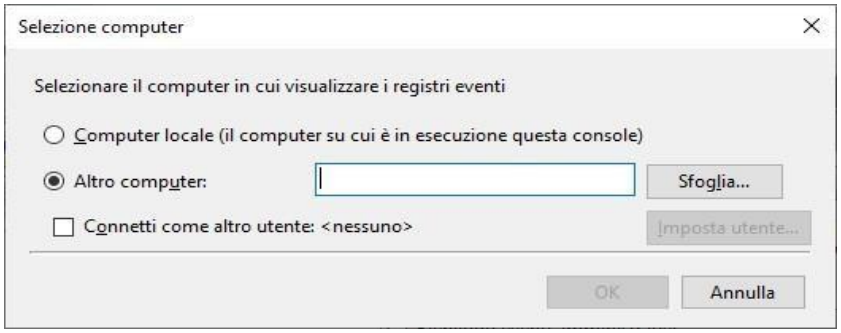


Questo errore si riferisce al fatto che la macchina remota NON risponde, i motivi potrebbero essere:

- La macchina è spenta
- La macchina non è raggiungibile
- Il servizio RemoteRegistry e fermo o disabilitato nella macchina target
- Un firewall sta bloccando la connessione tra server e client
- La macchina target non è aggiornata con la KB5003637 (aggiornamenti da giugno 2021)

A parte la verifica se la macchina sia accesa e raggiungibile (risolvibile con un banale ping), un buon metodo di verifica e utilizzare il banale EventViewer:

Aprite Event Viewer e cliccate sul menu in alto > Azione > Connetti a un altro computer:

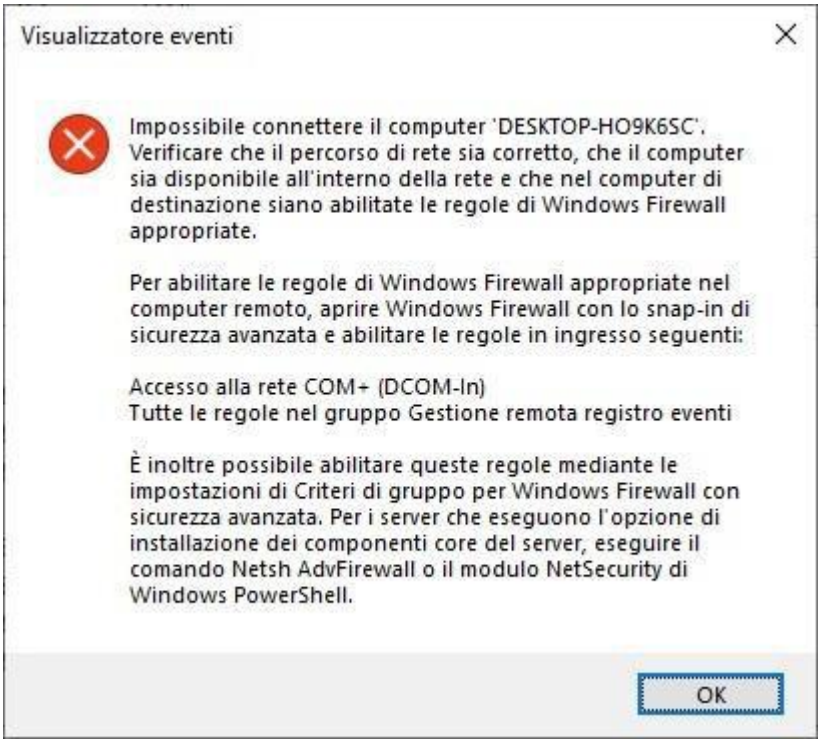


Qui sarà possibile specificare il nome macchine e, se necessario, impostare un utente “domain-admin” (per testare la stessa connessione, potete utilizzare lo stesso utente impostato nel servizio BlogService)

Otterrete, dopo un po’

In base alla problematica di connessione, otterrete un messaggio a video:

Esempio:



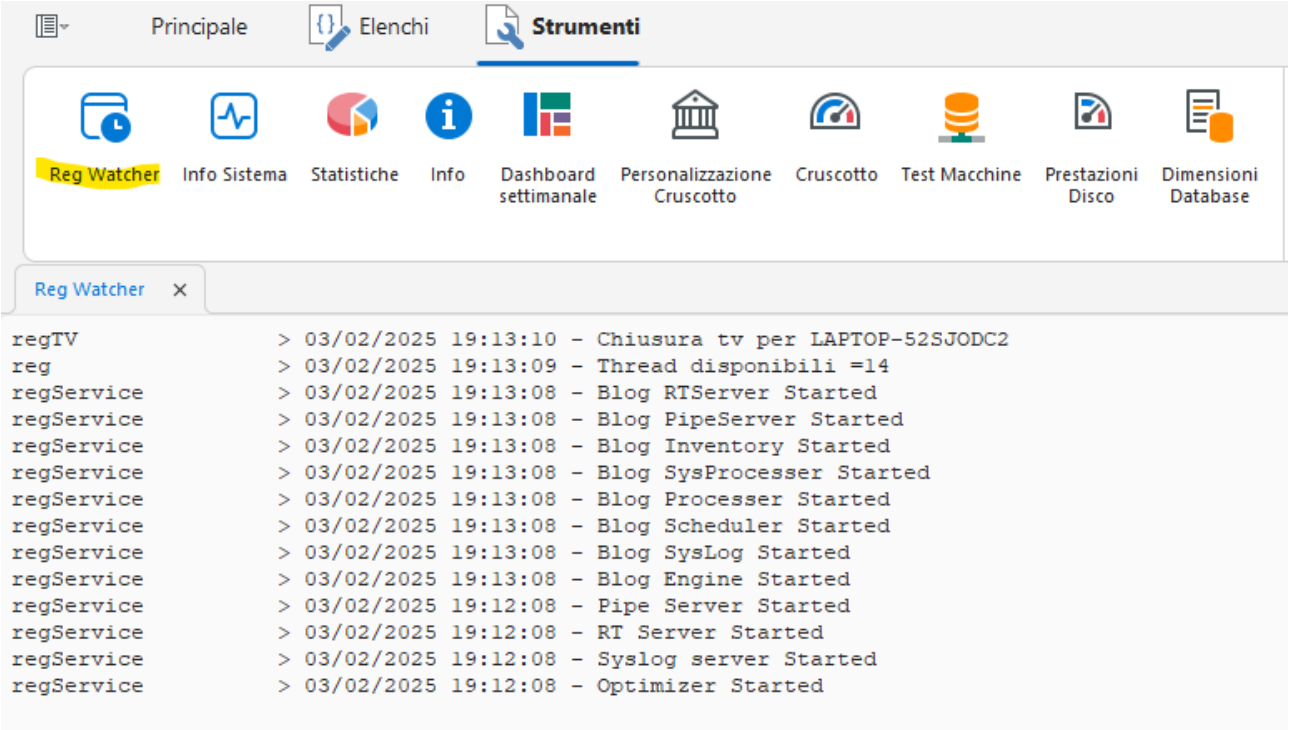
In questo caso e il firewall di windows che vi blocca la connessione alla macchina target.

Verificate che le GPO siano applicate e che la macchina target non abbia problemi di aggiornamento con le GPO di dominio.

Quando riuscirete a visualizzare, correttamente, i log della macchina remota, la connessione, anche con BusinessLog sarà possibile.

RegWatcher

Questa funzione consente di monitorare in tempo reale le modifiche ai file di registro di BusinessLog e permette di rilevare e registrare le modifiche effettuate ai log di sistema, fornendo un controllo dettagliato e immediato su tali eventi.



Tutte le registrazioni di funzionamento del software, comprese azioni ed errori, sono conservate nei files Regxxxx che trovate nella sotto-cartella \Reg

Per verifiche sul funzionamento o su possibili anomalie riscontrate, fate riferimento alla cartella e ai rispettivi files (vengono generati diversi files, secondo l'origine)

Modalità Offline

Si tratta di una modalità in cui è possibile acquisire files .evtx salvati dal registro eventi di macchine windows

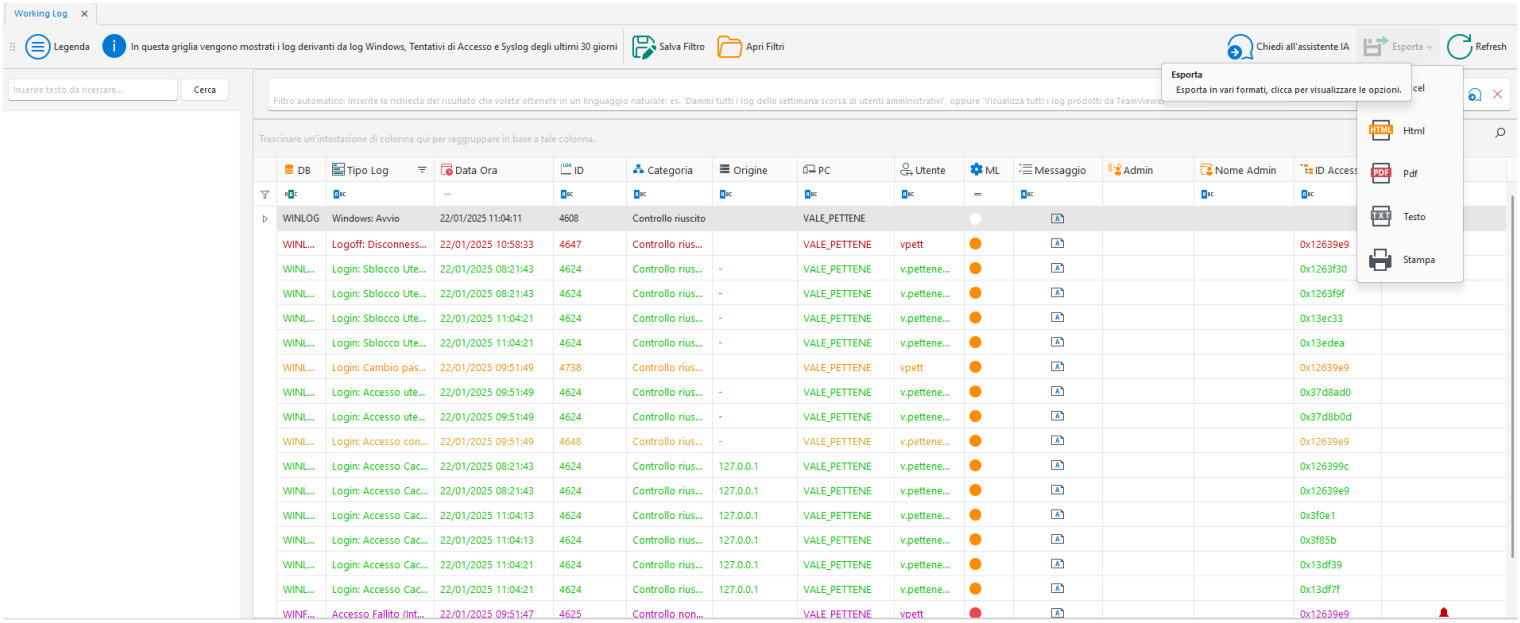
Nella cartella di installazione del programma, troverete una cartella “Offline”

In questa cartella potete copiare eventuali files .evtx salvati in precedenza.

Alla prima scansione del sistema rileverà i files contenuti e saranno oggetto di scansione offline.

NB: si tratta di una procedura NON standard e dedicata a misure straordinarie, per le normali scansioni fate sempre riferimento alla modalità online o con RT.

Esportazione dei dati

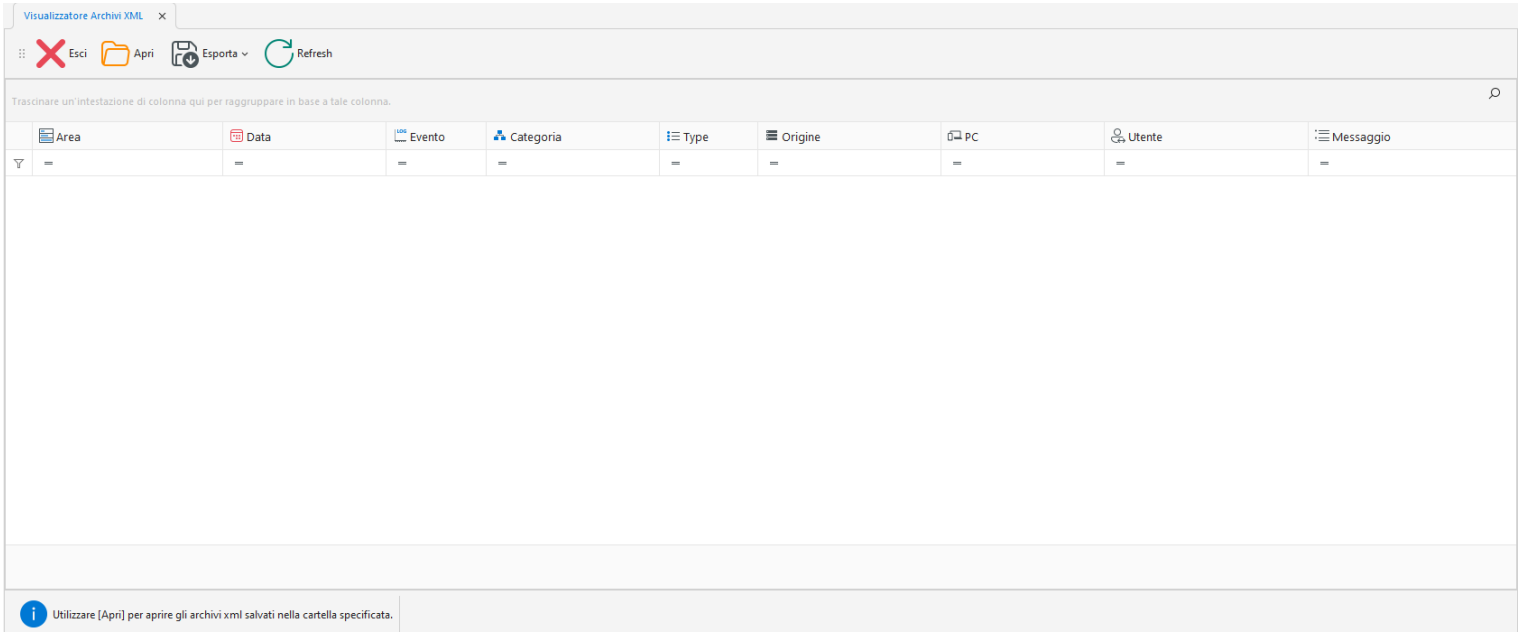


Nella griglia LOG (ma anche in TUTTE le altre griglie) è possibile esportare la visualizzazione corrente in 5 formati:

- Excel (xlsx)
- HTML
- PDF
- Testo
- Stampa

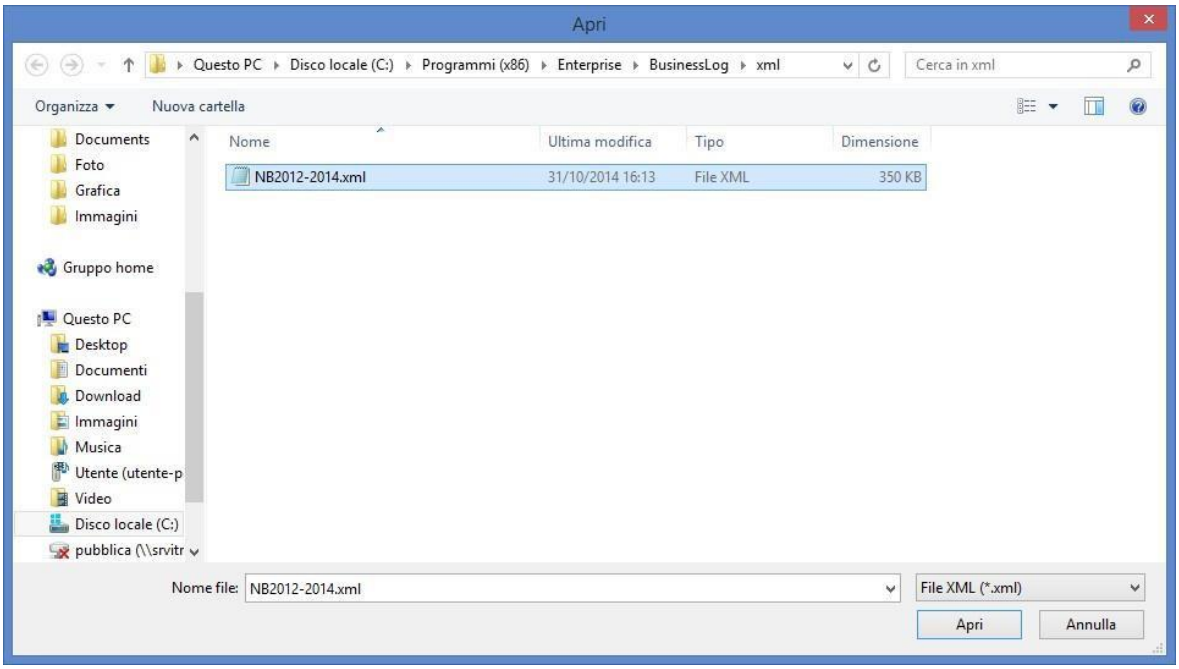
Nei formati Excel e PDF, verrà avviato un visualizzatore interno (pienamente compatibile) per cui NON È NECESSARIA l'installazione di licenze Office o di un altro visualizzatore nella macchina Host.

Visualizzatore archivi XML

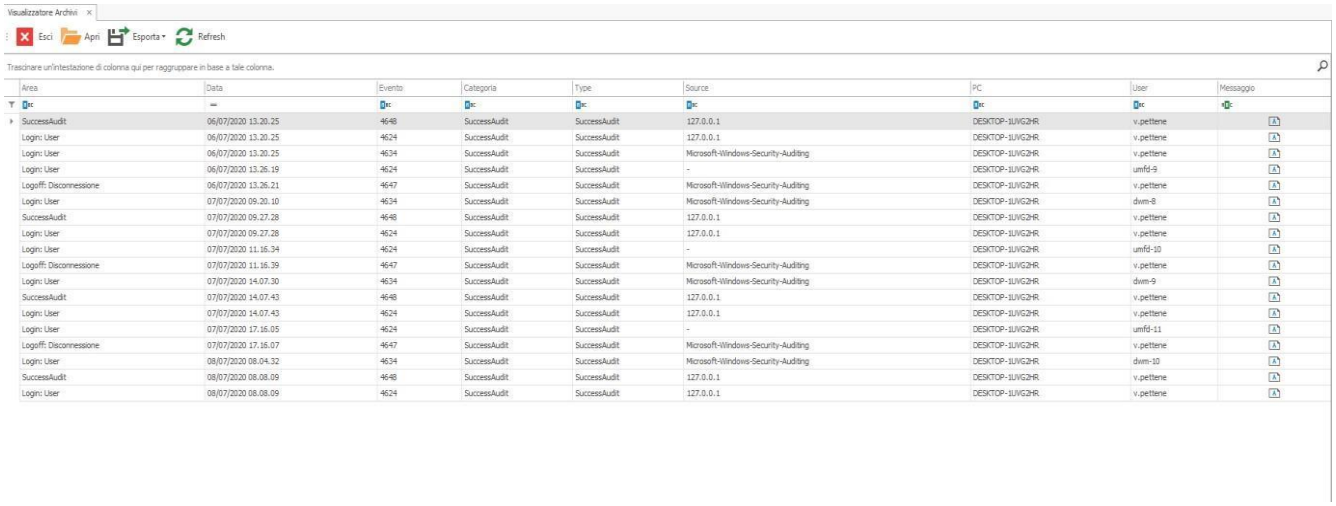


E lo strumento che consente di riaprire gli archivi in xml decriptandoli in real-time

Per aprire un archivio (troverete i files xml con un formato NOMEMACCHINA-ANNO.xml), cliccate su apri:



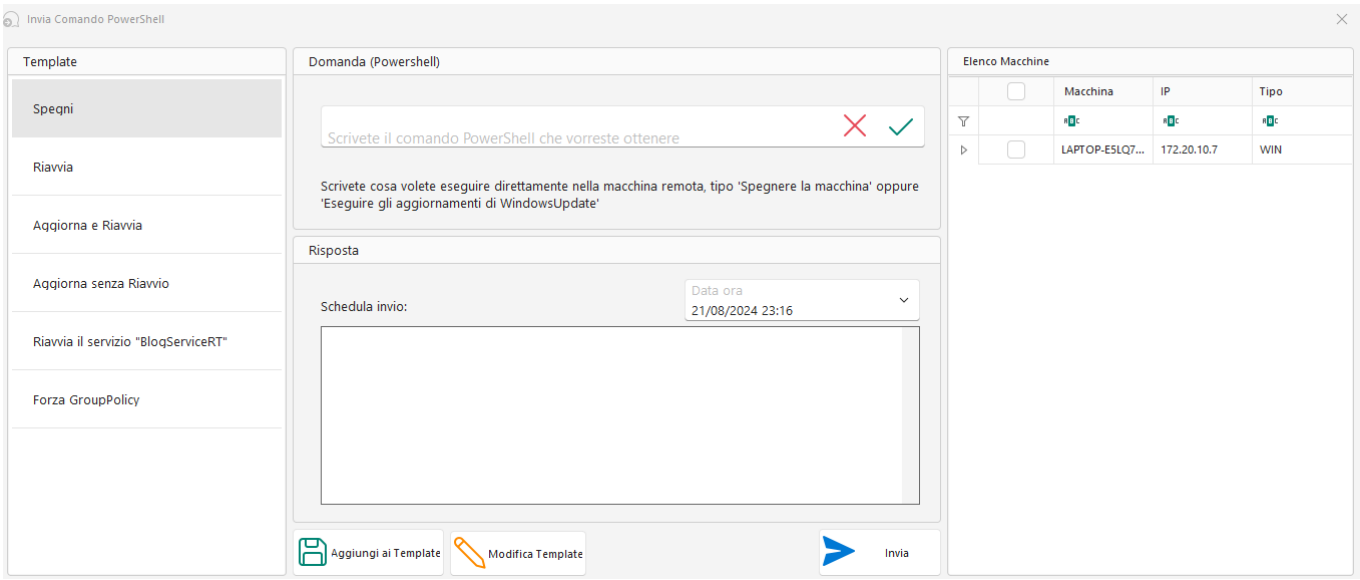
Otterrete:



Area	Data	Evento	Categoria	Type	Source	PC	User	Messaggio
SuccessAudit	06/07/2020 13.20.25	4648	SuccessAudit	SuccessAudit	127.0.0.1	DESKTOP-1UVG2HR	v.pettene	
Login: User	06/07/2020 13.20.25	4624	SuccessAudit	SuccessAudit	127.0.0.1	DESKTOP-1UVG2HR	v.pettene	
Login: User	06/07/2020 13.20.25	4634	SuccessAudit	SuccessAudit	Microsoft-Windows-Security-Auditing	DESKTOP-1UVG2HR	v.pettene	
Login: User	06/07/2020 13.26.19	4624	SuccessAudit	SuccessAudit	-	DESKTOP-1UVG2HR	umfd-9	
Logoff: Disconnessione	06/07/2020 13.26.21	4647	SuccessAudit	SuccessAudit	Microsoft-Windows-Security-Auditing	DESKTOP-1UVG2HR	v.pettene	
Login: User	07/07/2020 09.20.10	4634	SuccessAudit	SuccessAudit	Microsoft-Windows-Security-Auditing	DESKTOP-1UVG2HR	dwm-8	
SuccessAudit	07/07/2020 09.27.28	4648	SuccessAudit	SuccessAudit	127.0.0.1	DESKTOP-1UVG2HR	v.pettene	
Login: User	07/07/2020 09.27.28	4624	SuccessAudit	SuccessAudit	127.0.0.1	DESKTOP-1UVG2HR	v.pettene	
Login: User	07/07/2020 11.16.34	4624	SuccessAudit	SuccessAudit	-	DESKTOP-1UVG2HR	umfd-10	
Logoff: Disconnessione	07/07/2020 11.16.39	4647	SuccessAudit	SuccessAudit	Microsoft-Windows-Security-Auditing	DESKTOP-1UVG2HR	v.pettene	
Login: User	07/07/2020 14.07.30	4634	SuccessAudit	SuccessAudit	Microsoft-Windows-Security-Auditing	DESKTOP-1UVG2HR	dwm-9	
SuccessAudit	07/07/2020 14.07.43	4648	SuccessAudit	SuccessAudit	127.0.0.1	DESKTOP-1UVG2HR	v.pettene	
Login: User	07/07/2020 14.07.43	4624	SuccessAudit	SuccessAudit	127.0.0.1	DESKTOP-1UVG2HR	v.pettene	
Login: User	07/07/2020 17.16.05	4624	SuccessAudit	SuccessAudit	-	DESKTOP-1UVG2HR	umfd-11	
Logoff: Disconnessione	07/07/2020 17.16.07	4647	SuccessAudit	SuccessAudit	Microsoft-Windows-Security-Auditing	DESKTOP-1UVG2HR	v.pettene	
Login: User	08/07/2020 08.04.32	4634	SuccessAudit	SuccessAudit	Microsoft-Windows-Security-Auditing	DESKTOP-1UVG2HR	dwm-10	
SuccessAudit	08/07/2020 08.08.09	4648	SuccessAudit	SuccessAudit	127.0.0.1	DESKTOP-1UVG2HR	v.pettene	
Login: User	08/07/2020 08.08.09	4624	SuccessAudit	SuccessAudit	127.0.0.1	DESKTOP-1UVG2HR	v.pettene	

L'elenco è filtrabile, raggruppabile ed esportabile come nella griglia iniziale.

Invia Comando PowerShell



Attraverso la seguente finestra, si possono selezionare dei comandi pre-impostati (o aggiungerne di personalizzati) oppure chiedere alla IA di generare il relativo comando, il comando apparirà nel box centrale.

Il comando sarà poi schedulabile, impostando la data/ora a fianco, e associabile alle macchine sulla destra.

Alcuni Template sono già inseriti, oppure si possono aggiungerne o modificarli.

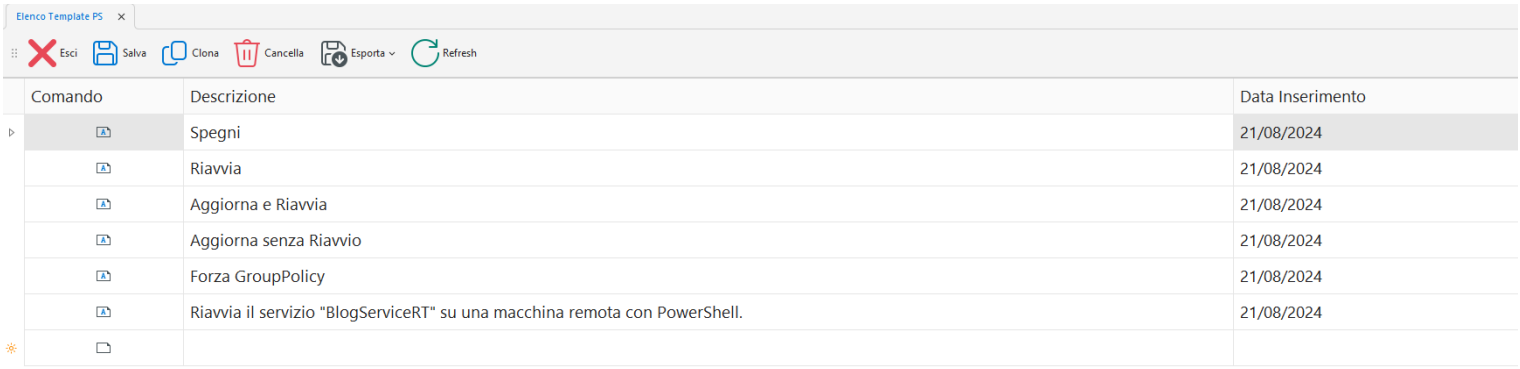
Una volta creato il comando, si può aggiungere, direttamente, ai Template cliccando su “Aggiungi ai Template”, la descrizione verrà aggiunta automaticamente dalla IA.

Comandi PS Inviati

Attraverso la seguente finestra, si possono visualizzare i comandi già inviati ed eventuali risposte associate.

In ROSSO i comandi che hanno restituito un errore (nella bustina della colonna RISPOSTA è disponibile l’errore dato da PowerShell)

Elenco Template PS



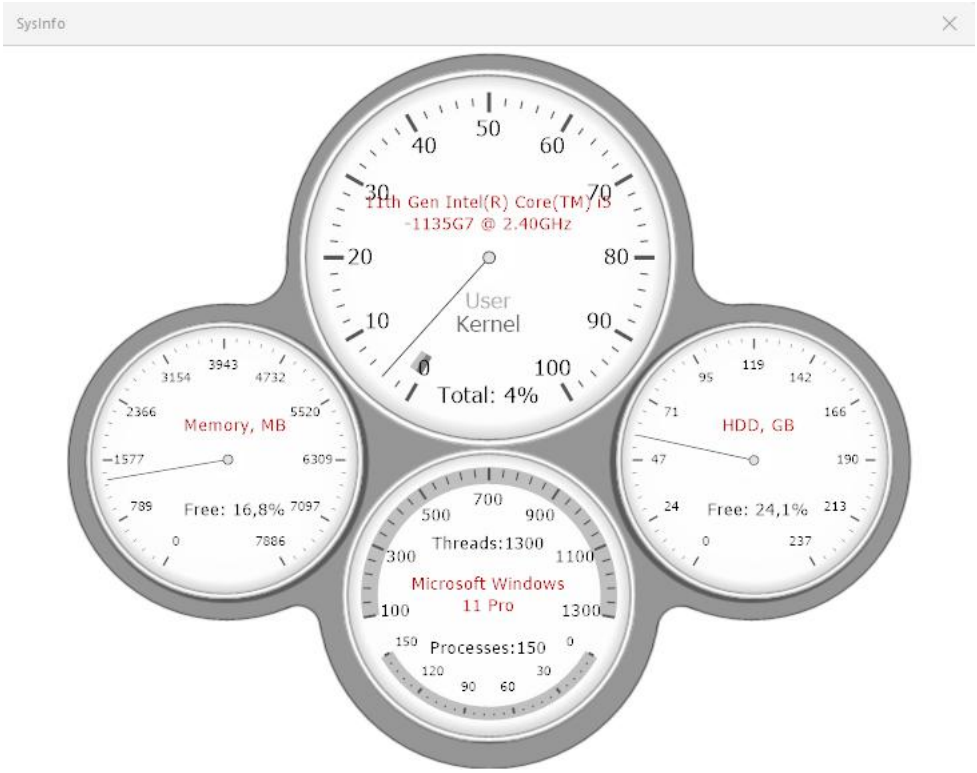
Comando	Descrizione	Data Inserimento
	Spegni	21/08/2024
	Riavvia	21/08/2024
	Aggiorna e Riavvia	21/08/2024
	Aggiorna senza Riavvio	21/08/2024
	Forza GroupPolicy	21/08/2024
	Riavvia il servizio "BlogServiceRT" su una macchina remota con PowerShell.	21/08/2024

Attraverso questa schermata, si possono aggiungere, modificare o eliminare dei template personalizzati.

Questi Template saranno disponibili nella sezione a sinistra nella finestra “Invia Comando Powershell”

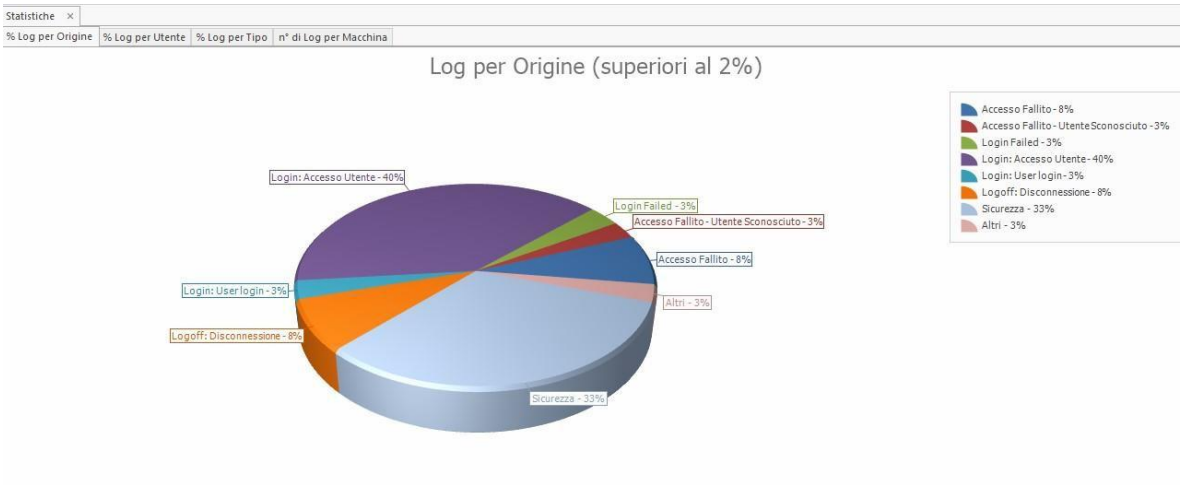
Altri Strumenti

INFO SISTEMA



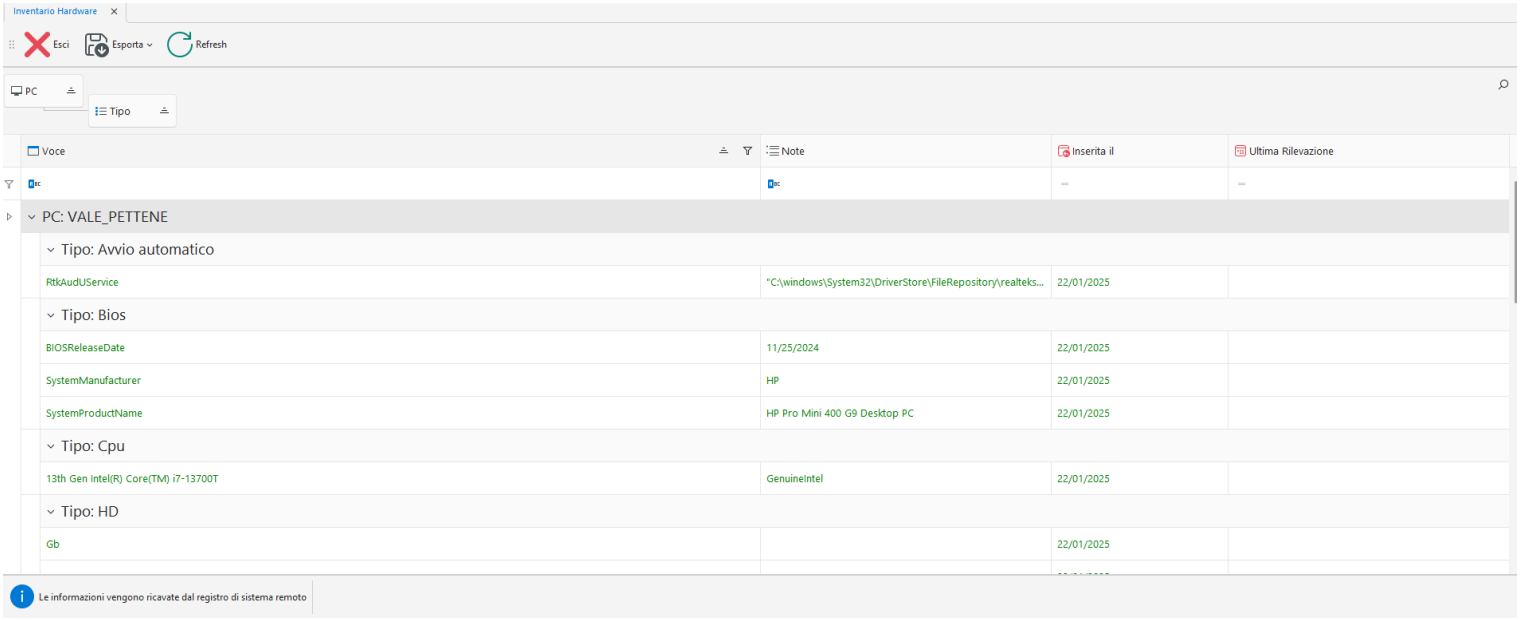
Avvia una connessione al servizio WMI per mostrare un pannello in realtime per il consumo delle risorse, può essere utile per controllare il consumo durante le scansioni.

Statistiche



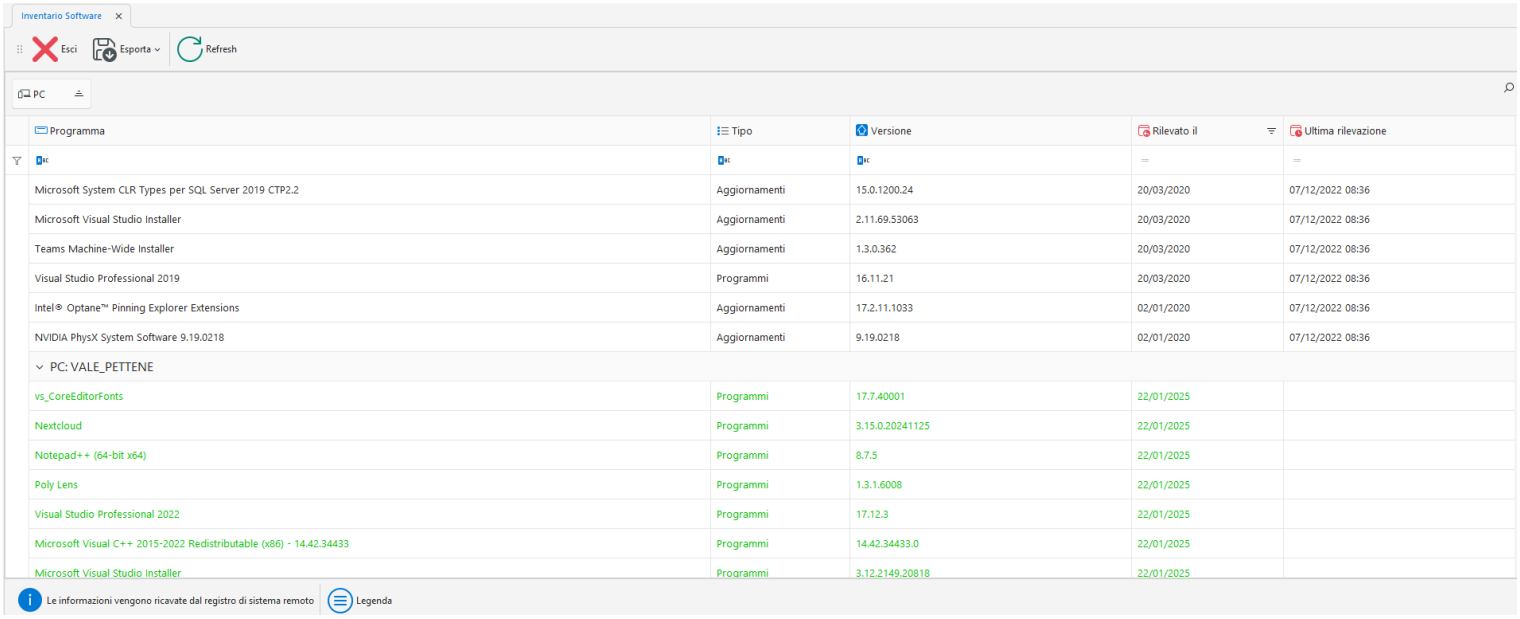
La finestra visualizza 4 tipi di grafici 3D per un'analisi statistica delle tipologie di log.

Inventario Hardware



Viene visualizzato un elenco di informazioni hardware raccolte dalle varie macchine (windows).

Inventario Software



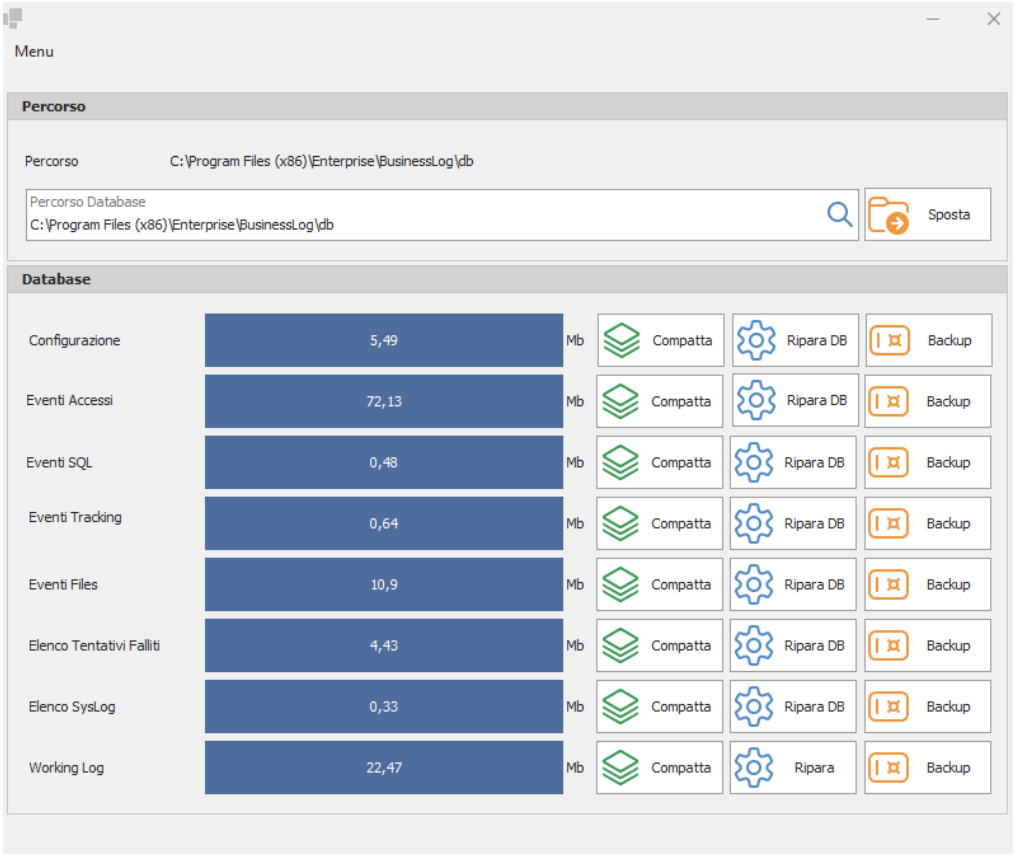
In questa tabella sono presenti tutti i programmi installati, i servizi e i driver presenti.

Per i programmi viene indicata la data di installazione e l'ultimo controllo, eventuali nuovi programmi vengono indicati in grassetto e i programmi disinstallati in italico.

BlogTools

Nella cartella di installazione del programma trovate un eseguibile denominato BlogTools.exe

ATTENZIONE: prima di avviare il programma e necessario **CHIUDERE** tutte le finestre BusinessLog, il servizio BlogService e verificare che non ci siano processi Blogxxxxx.exe o BusinessSysLog.exe attivi



La finestra permette di:

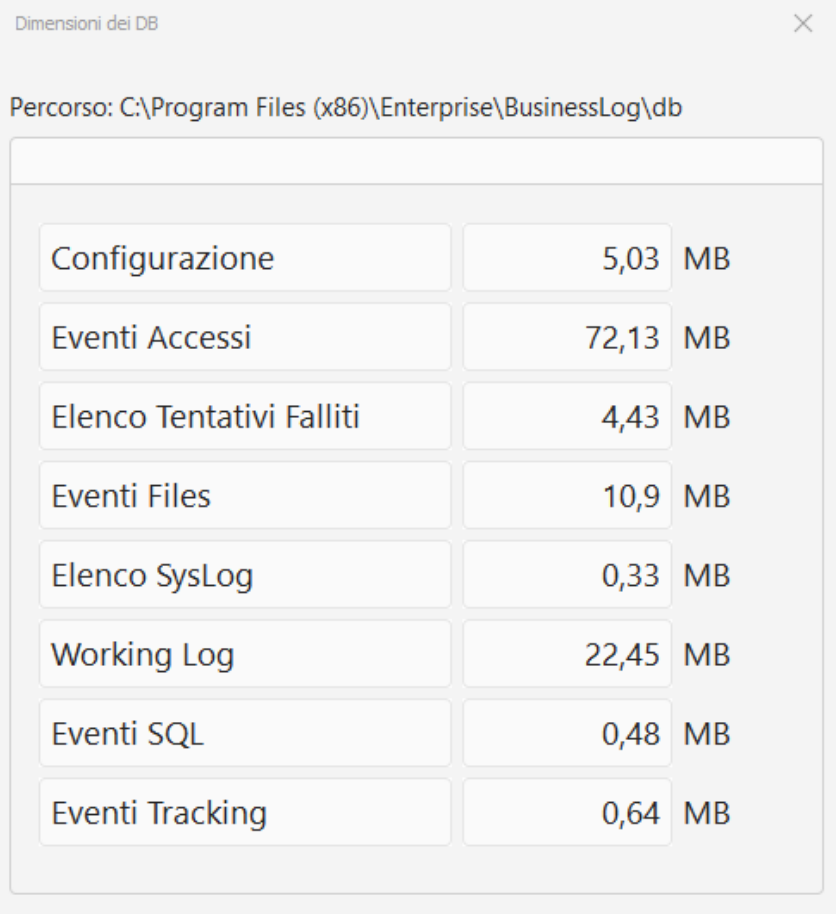
SPOSTARE i database: la versione 2022 permette di posizionare i database in una posizione diversa dalla pre-definita, per spostarli, occorre selezionare una nuova posizione (icona “lente”) e cliccare su [Sposta]

COMPATTARE i database: con il tempo è normale che i db raggiungano dimensioni considerevoli, potete compattare ogni database (verrà fatto un backup) e la barra indicherà quanto spazio è stato risparmiato.

BACKUP: esegue un backup del database corrispondente (stessa cartella) RIPARARE:

esegue una riparazione (anche preventiva) nel database specificato.

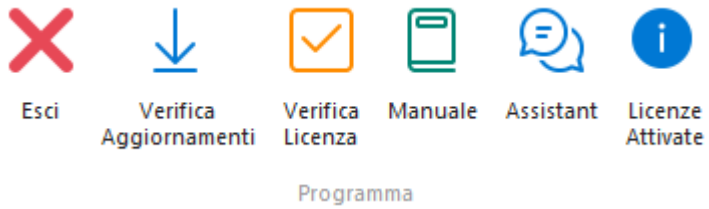
Dimensioni DB



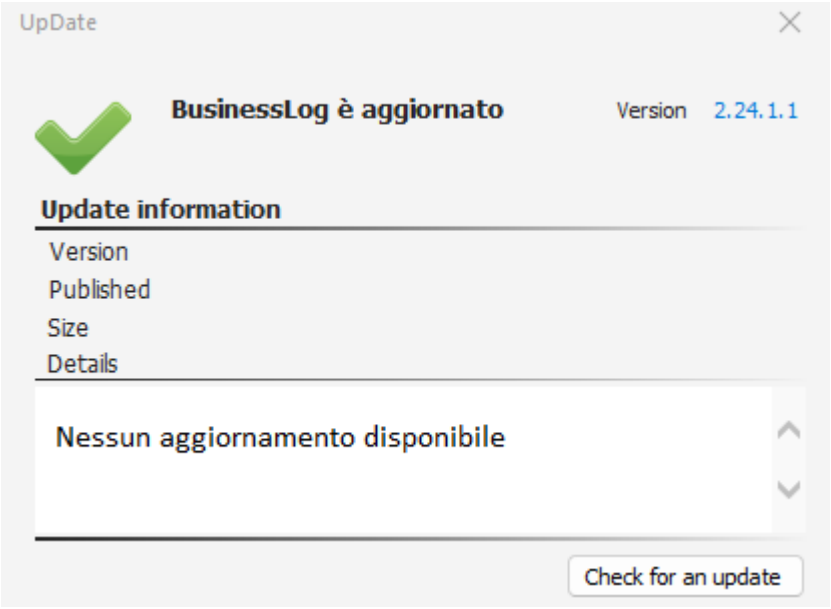
In questa finestra è possibile visualizzare le dimensioni del DB.

Aggiornamenti

BusinessLog viene costantemente aggiornato per aggiungere nuove funzionalità utili per l'amministratore, la via più semplice per aggiornare la propria installazione e:



Cliccare su "Verifica Aggiornamenti"



Se non ci sono aggiornamenti disponibili verrà notificato che il software è aggiornato, altrimenti inviterà a procedere con l'aggiornamento, la procedura ferma il servizio e chiude eventuali scansioni in sospeso.

Nel caso non sia possibile effettuare l'aggiornamento diretto (proxy o firewall che bloccano la procedura) è possibile scaricare l'aggiornamento diretto da:

http://www.businesslog.it/download/BusinessLog2022Upgrade.exe

La procedura diretta, tuttavia, richiede di fermare manualmente il servizio "BlogService" e di chiudere l'eventuale processo "BlogEngine.exe" e "BlogSysLog.exe" in esecuzione in background.

Al termine della procedura sarà sufficiente riavviare manualmente il servizio, i processi partiranno automaticamente.

VIEWER

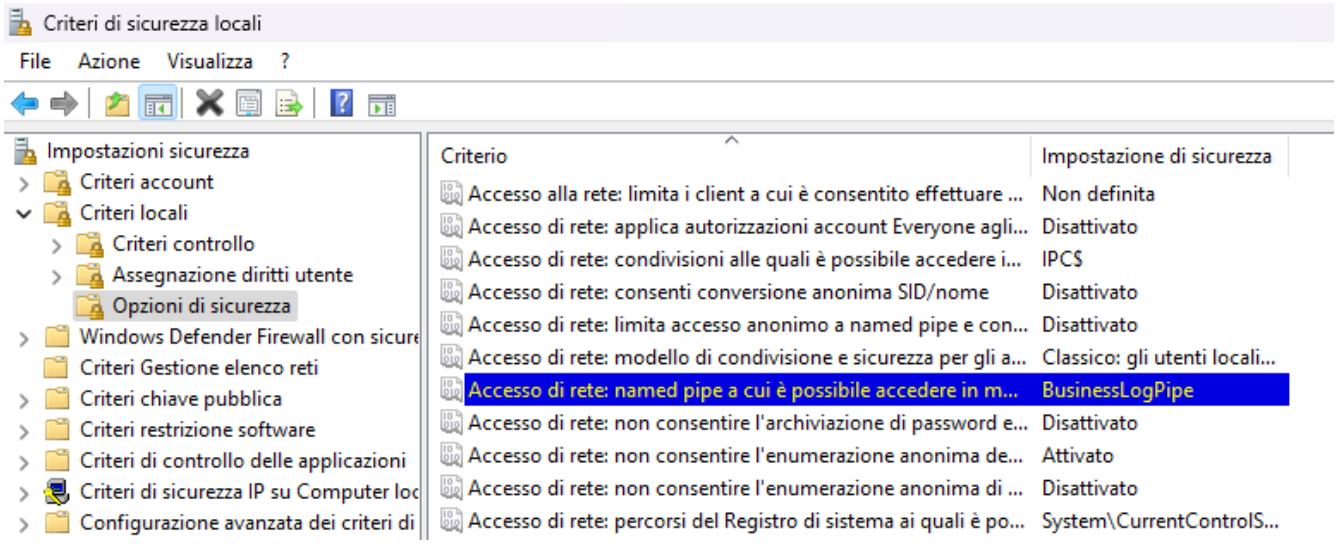
Il Visualizzatore “Stand Alone” permette di visualizzare i dati delle griglie dei log senza utilizzare il server e senza poter modificare le impostazioni di BusinessLog.

Inoltre, le autorizzazioni dell’utente ricalcano quanto impostato lato server.

Il sistema utilizza NAMED PIPE per la connessione, pertanto è necessario che, sia lato server che lato client abbiamo attivato:

- La porta TCP 445
- Il protocollo SMB (2 o superiore)

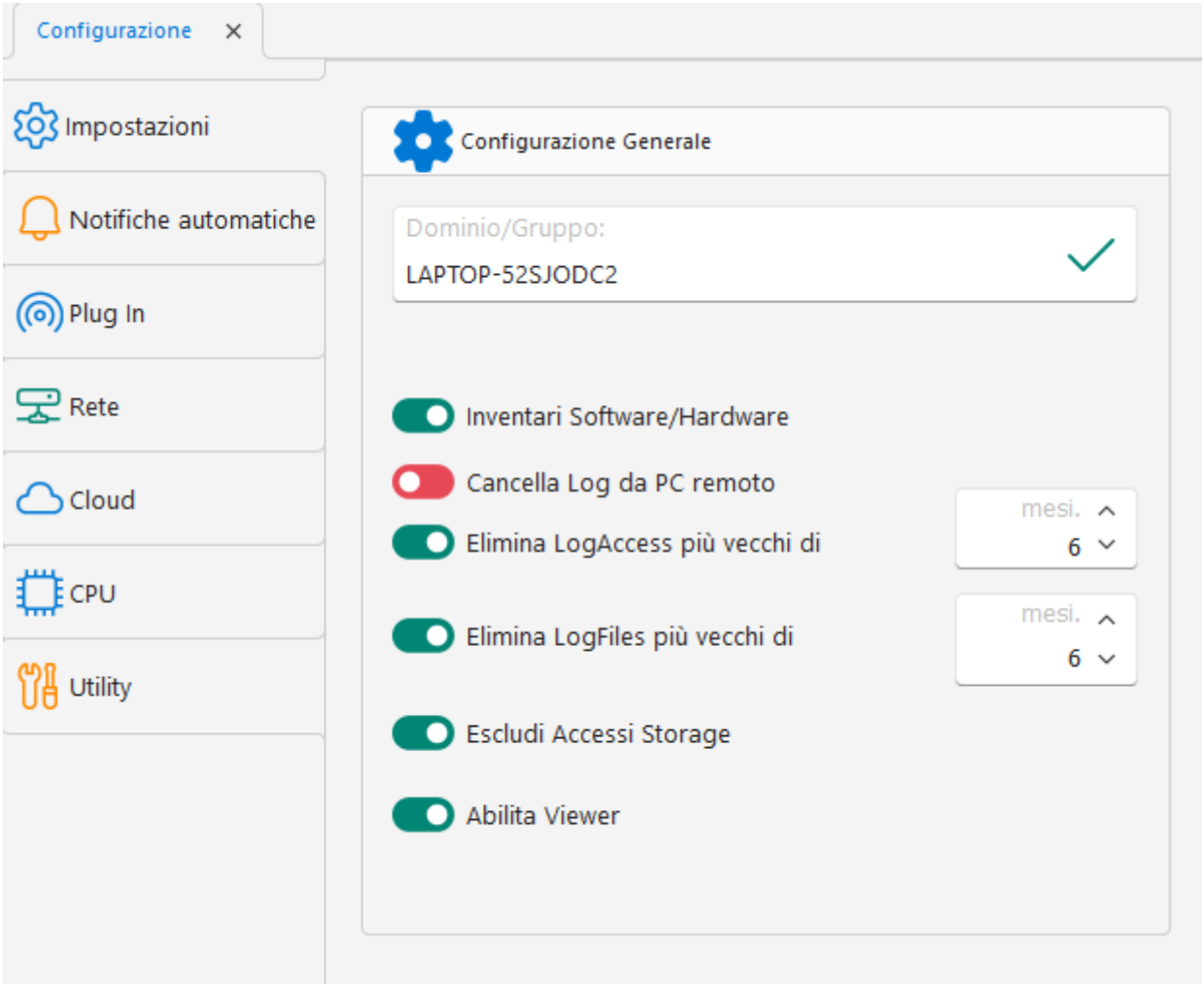
Il server deve avere la named pipe autorizzata, nei criteri locali:



Impostare il nome della Pipe da autorizzare alla voce indicata.

Lato server:

Attivare l’opzione “Abilita Viewer” nella Configurazione, Salvare e RIAVVIARE i servizi per abilitare il server Pipe.

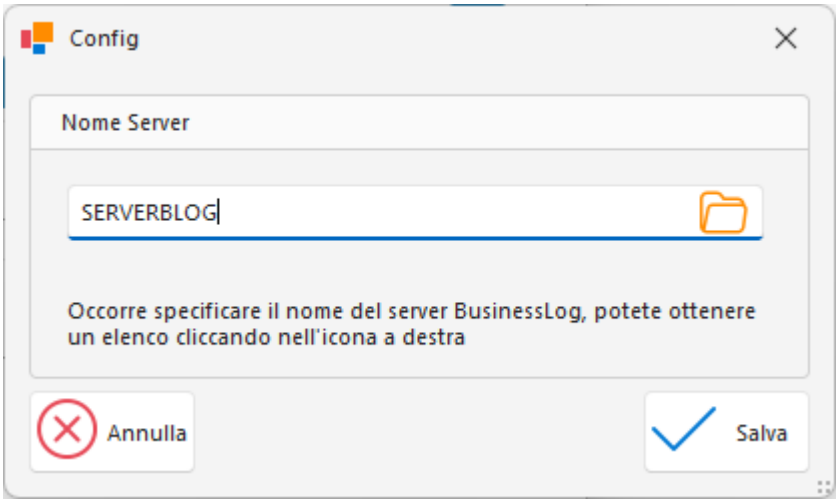


Il Viewer è scaricabile dal sito:

https://www.businesslog.it/download/BusinessLogViewer.exe

Il processo di installazione è minimale, al termine uscirà la finestra di login:

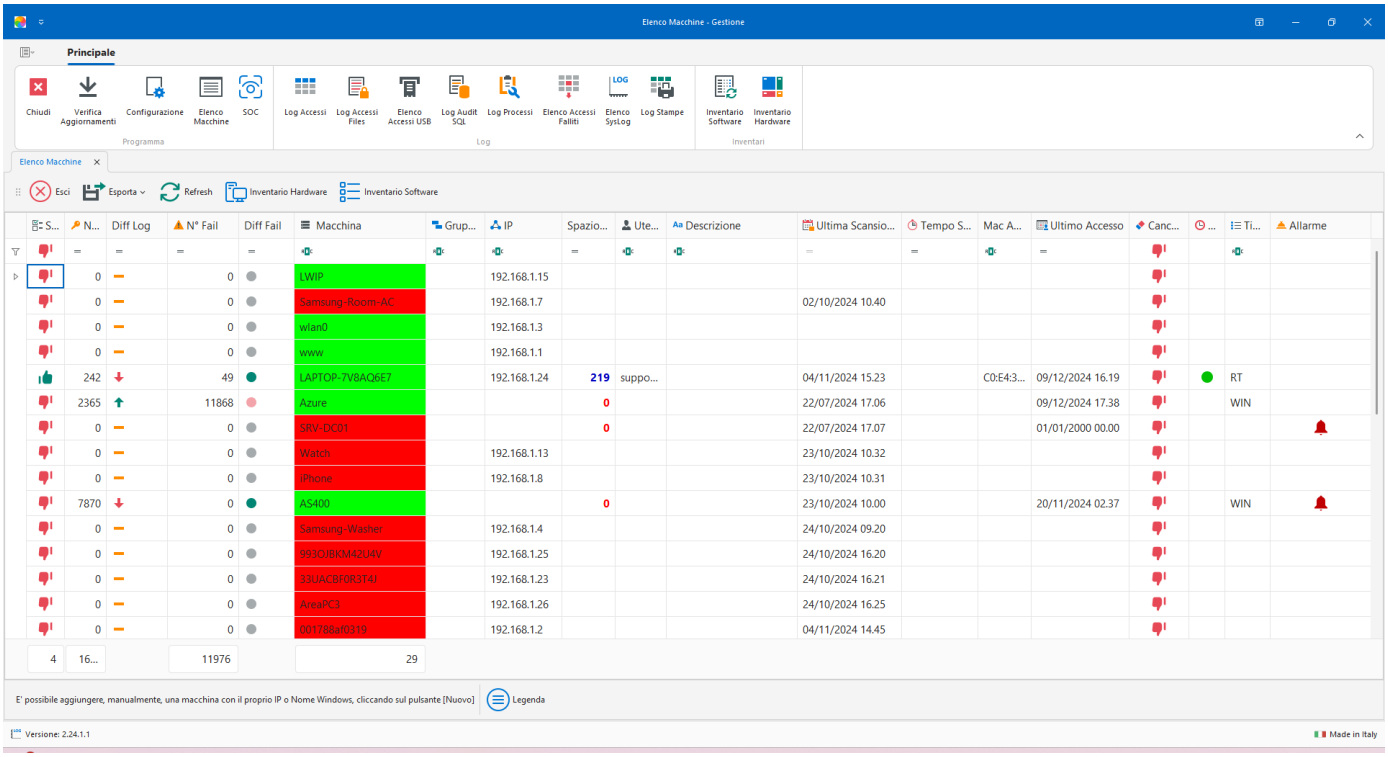
Se la Pipe non è stata ancora configurata, cliccare in basso a destra (iconcina con gli “strumenti”)



Una volta specificato il nome del server BusinessLog verificate che, nel messaggio inferiore esca:

“Connessione alla Named Pipe stabilita con successo.”

In questo modo sarà possibile accedere con Utente e Password



Le visualizzazioni sono le stesse del lato server, solo più semplificate !

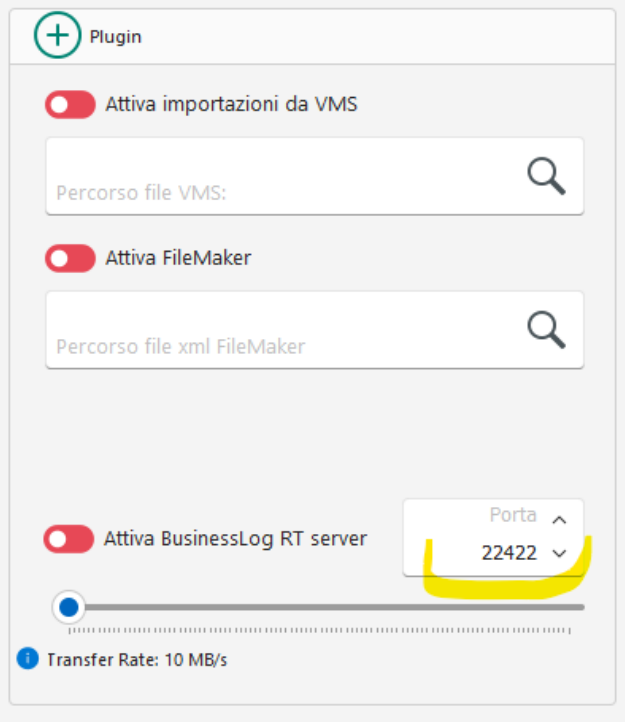
Il Visualizzatore può essere installato in qualsiasi postazione della rete interna, senza alcuna limitazione di licenza.

Modulo RT

Il modulo RT permette di acquisire i log di macchine Windows anche per le macchine fuori dominio o per quelle macchine per cui si rende necessario avere una registrazione in RealTime

Il client RT va installato nelle macchine da controllare mediante un setup dedicato molto semplice (unico pre-requisito il framework .net 4.8)

Requisito essenziale per il funzionamento e l'abilitazione della porta TCP configurata nella sezione plugin:



La porta predefinita e la (TCP) 22422

LATO SERVER

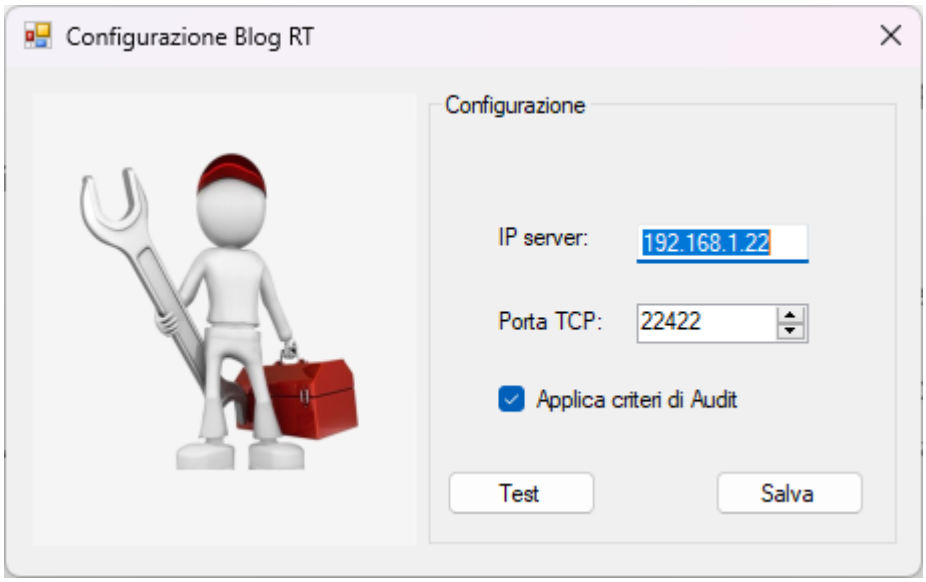
È sufficiente l'attivazione del server e l'impostazione della porta, dopo l'attivazione sarà necessario riavviare il servizio BlogService.

ATTENZIONE: occorre verificare che eventuali firewall (di windows o di terze parti) consentano la comunicazione utilizzando la porta specificata.

LATO CLIENT

Una volta attivata la licenza RT, e necessario scaricare il setup di installazione da: https://www.businesslog.it/download/BusinessLogRT.exe

L'installazione e simile a quella di BusinessLog, solo molto più rapida, al termine della procedura di installazione sarà necessario eseguire il file RTConfig.exe (configuratore)



Qui e necessario specificare:

- l'IP della macchina Host di BusinessLog
- La relativa porta impostata. (default = 22422)
- Se applicare, o meno, i criteri di audit automatici sulla macchina.

È possibile eseguire un test, alla fine cliccare su [Salva]

Al termine, verificare che il servizio BlogServiceRT sia avviato (nel caso avviarlo manualmente)

Il servizio lavora in background, il connettore partirà a collezionare i log presenti nella macchina (storico) e, da questo momento, ogni evento registrato in locale sarà spedito al server RT per la registrazione anche in BusinessLog.

Il modulo RT raccoglie anche l'inventario Software e Hardware della macchina locale.

Distribuzione MSI per BlogRT

È possibile utilizzare una versione .msi per la distribuzione via GPO (o altri strumenti) https://www.businesslog.it/download/BusinessLogRT.msi

Scaricato il setup potete aggiungerlo alle azioni di distribuzione.

Potete configurare, in remoto, le singole postazioni utilizzando il comando:

C:\Program Files (x86)\Enterprise\BusinessLogRT\rtconfig.exe /ip=[IP] /port=[PORTA] /script=[True/False]

Sostituendo, ovviamente, i parametri: ad esempio:

C:\Program Files (x86)\Enterprise\BusinessLogRT\rtconfig.exe /ip=192.168.1.1 /port=22422 /script=true

Verifica Licenza

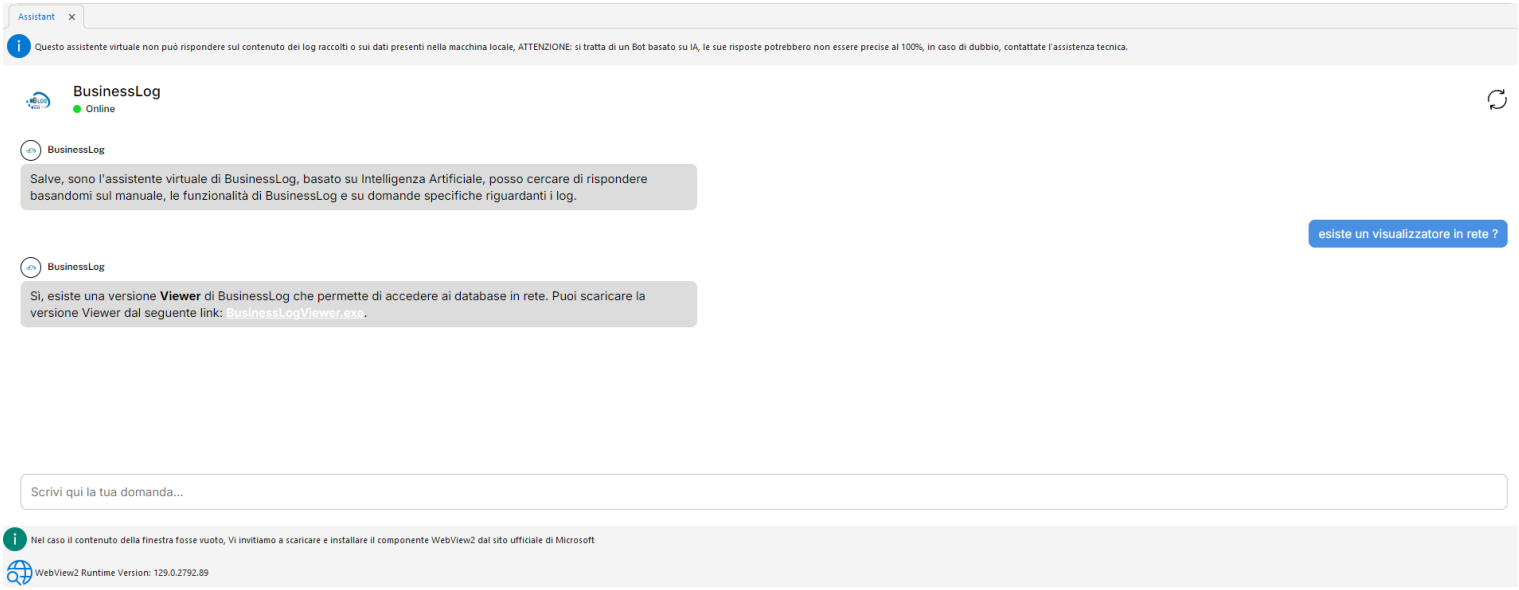
Il pulsante “Verifica Licenza”

Permette di effettuare un controllo diretto della licenza con l’aggiornamento della scadenza, effettuare upgrade di licenza o attivare funzionalità extra senza reinserire i dati di attivazione: il risultato viene immediatamente aggiornato.

Assistant

Nel menu Principale trovate il pulsante “Assistant”

Qui si avvierà una sessione Web con il nostro BusinessLog GPT (raggiungibile anche all’indirizzo https://online.businesslog.it) in questa Chat potrete porre domande al Bot riguardo ai log, alla documentazione in questo manuale e alle FAQ fin qui raccolte.



Il requisito essenziale per visualizzare l’assistant, all’interno di BusinessLog, è l’installazione del componente di Microsoft WebView2 Runtime scaricabile dal sito ufficiale a questo indirizzo:

Microsoft Edge WebView2 | Microsoft Edge Developer

Privacy Policy

BusinessLog raccoglie i seguenti dati dalla rete INTERNA in cui è installato:

- IP e Nome computer di ciascuna macchina connessa e all'interno del range IP configurato
- Nome Account degli utenti loggati nel registro eventi windows
- Nome Account degli utenti loggati nel registro syslog dei dispositivi compatibili
- Applicazioni installate nelle macchine WINDOWS (se abilitato)
- Nome e percorso dei files registrati dalla raccolta log files (se abilitato e configurato)
- Nome e percorso dei files registrati dalla raccolta log dispositivi esterni (se abilitato e configurato)
- Nominativo degli utenti specificati come "Amministratori di sistema" nominati e configurati nella tabella ELENCO AMMINISTRATORI
- Indirizzo mail configurato per le trasmissioni delle mail
- Chat ID Telegram configurata per la trasmissione al bot

Tutti i dati vengono registrati in LOCALE nei Database VistaDB (protetti e crittografati), attivando l'opzione "Backup Cloud" i log verranno ridondati anche nel nostro Datacenter, la trasmissione è crittografata con certificato Microsoft dedicato.

BusinessLog raccoglie e comunica all'ESTERNO solo i seguenti dati:

- UserID, Nome server, IP pubblico verso il server licenze
- Log completi, elenco amministratori, elenco macchine, software installati verso il datacenter cloud (SOLO se abilitato e configurato), la trasmissione è crittografata.
- Indirizzo IP pubblico, caselle mail e dettagli tecnici mail verso il server mail (se abilitato e configurato)
- Nome account, Chat ID, Bot ID per le comunicazioni verso Telegram
- Tenant Azure: per la raccolta dei log Azure o le richieste di autorizzazione per O365
- Log singolo Completo verso OpenAI, solo per le richieste di informazioni inoltrate alla IA, i log inoltrati vengono conservati da OpenAI per 30 giorni

Trasmissioni:

- I log vengono scritti in crittografia AES256 anche nei files temporanei
- Il traffico mail è crittografato, con certificato SSL (per l'account interno BusinessLog)
- Il traffico verso Telegram viene crittografato con TLS1.2
- Il traffico verso OpenAI viene crittografato con TLS1.2
- I log salvati nel datacenter vengono crittografati con TLS1.2 con certificato Microsoft Azure
- Le richieste di autorizzazione verso i tenant Azure sono crittografati con certificato SSL

Conservazione dei dati (Database Locali)

1. Sicurezza dei Dati

   Crittografia dei Dati: VistaDB utilizza la criptazione AES conforme agli standard FIPS (AES 256) per criptare l'intero database, inclusi schema e dati. Questo garantisce un alto livello di sicurezza per i dati archiviati.

   Gestione delle Chiavi di Crittografia: Le chiavi di crittografia sono gestite in modo sicuro, assicurando che solo gli utenti autorizzati possano decrittare e accedere ai dati.

2. Controllo degli Accessi

   Autenticazione e Autorizzazione: VistaDb supporta meccanismi di autenticazione robusti per garantire che solo gli utenti autorizzati possano accedere al database. Il controllo degli accessi può essere configurato per fornire livelli differenti di autorizzazione basati sui ruoli degli utenti.

3. Backup e Ripristino

   Backup Automatici: il software mette a disposizione un sistema di backup automatico dei db, tuttavia è discrezione del reparto IT sfruttare altre tipologie di backup e ripristino disponibili nei sistemi a disposizione della rete dell'utente finale.

4. Monitoraggio e Gestione

   Attraverso il modulo BlogTools è possibile monitorare, compattare, recuperare ed effettuare Backup specifici riguardante i database VistaDB utilizzati nel sistema Business Log

Conservazione dei dati (DB Cloud)

1. Ridondanza e Disponibilità

   Replica Geografica: SQL Azure utilizza la replica geografica per assicurare la disponibilità dei dati. Questo include la replica geografica attiva, che replica i database in diverse regioni per garantire la continuità operativa in caso di guasti regionali.

   Zone di Disponibilità: I database sono distribuiti su zone di disponibilità all'interno dell'area UE come ridondanza di disponibilità.

2. Sicurezza dei Dati

   Crittografia dei Dati: I dati vengono crittografati sia a riposo (con Transparent Data Encryption - TDE) sia in transito (utilizzando SSL/TLS). Questo assicura che i dati siano protetti da accessi non autorizzati.

   Controllo degli Accessi Basato su Ruoli (RBAC): La gestione degli accessi è centralizzata tramite Azure Active Directory (AAD) che consente il controllo dettagliato degli accessi ai dati.

3. Backup e Ripristino

   Backup Automatici: SQL Azure esegue automaticamente backup completi, differenziali e dei log delle transazioni. I backup completi vengono eseguiti settimanalmente, quelli differenziali ogni 12 ore e i log delle transazioni ogni 5-10 minuti.

   Ripristino Temporale: SQL Azure supporta il ripristino temporale, permettendo di ripristinare il database a un qualsiasi punto nel tempo all'interno del periodo di conservazione dei backup (fino a 35 giorni).

4. Resilienza e Recupero di Emergenza

   Piani di Recupero di Emergenza: Azure SQL Database include piani di recupero di emergenza che assicurano la disponibilità dei dati anche in caso di eventi catastrofici.

   Failover Automatico: In caso di guasto, il sistema esegue automaticamente il failover a un'istanza replica senza intervento manuale, minimizzando i tempi di inattività.

5. Monitoraggio e Gestione

   Monitoraggio Continuo: SQL Azure fornisce strumenti di monitoraggio continuo attraverso Azure Monitor, che permette di tracciare le prestazioni e rilevare eventuali anomalie.

   Avvisi e Automazione: Gli amministratori hanno avvisi per specifici eventi utilizzando Azure Automation e Azure Logic Apps.

6. Compliance e Certificazioni

   Certificazioni di Sicurezza: SQL Azure è conforme a vari standard di sicurezza e regolamentazioni, tra cui ISO/IEC 27001, ISO/IEC 27018, SOC 1, SOC 2, e SOC 3, HIPAA e il Regolamento Generale sulla Protezione dei Dati (GDPR).

Supporto Tecnico

Per poter contattare il reparto tecnico di Business LOG è disponibile il

BUSINESS LOG HELP CENTER

https://supporto.amministratoridisistema.it/hc/it

Da qui è possibile aprire un ticket per metterti in contatto con il nostro personale di assistenza, consultare guide e FAQ disponibili e costantemente aggiornate ed interagire col nuovissimo ChatBot di Business LOG.

Per essere in grado di inviare richieste di assistenza, è necessario richiedere le credenziali di accesso, disponibili solo ai nostri Clienti e Partner Certificati.

Se ancora non hai le credenziali, compila il form qui sotto per inviare la richiesta.

https://www.amministratoridisistema.it/richiedi-accesso-helpcenter

BusinessLog Cloud e BusinessLog 2022 sono prodotti di: