Sys-Aid

strumenti per il telelavoro al tempo del #coronavirus

Indice generale

Premessa

di seguito le prime semplici indicazioni affinché sia possibile lavorare da casa in assenza di una adeguata infrastruttura tecnologica sicura.

Utilizzeremo i classici strumenti di telecontrollo (utilizzati anche dalle software house) configurando adeguatamente il server ed il client affinché non si verifichino blocchi o spegnimenti del computer controllato (es. stand-by).
Utilizzeremo solo software certificato o open surce, e mai non gratuito.

Usciremo successivamente con un documento maggiormente esaustivo sulle alternative on-premise di connessione, backup e installazioni su server remoti anche in cloud system.

Questo è un Si raccomanda di fare attenzione anche alla normativa relativa all'utilizzo di strumenti aziendali per il dipendente, GDPR e Statuto dei Lavoratori per non incorrere in spiacevoli situazioni.

Definizioni

- Server: il Computer (solitamente in studio) che deve essere controllato da remoto e che solitamente è quello che usiamo ogni giorno e che ha accesso a tutte le risorse di studio (testi e gestionale in primis)
- Client: il PC che utilizzate da remoto per collegarvi e per lavorare.

Prerequisiti

- Linea internet attiva da entrambi i lati
- Controllo dei computer per malware in generale
- Antivirus attivo
- Adeguate impostazioni del PC sul controllo dell'energia

Accessori consigliati posto di lavoro

- Schermo almeno 21''
- tastiera e mouse
- sedia regolabile
- posto comodo e ampio

Installazione del software

Sul mercato ci sono numerosi software di telecontrollo facciamo un esempio non esaustivo:

- Teamviewer
- Anydesk
- Logmein e GoTOMyPC
- SupRemo
- Splashtop
- Chrome Remote Desktop
- Iperius remote Desktop

a questi si aggiungono una serie di prodotti anche open source il cui significato ci teniamo a precisare, non è sinonimo di "gratuito", che hanno la peculiarità di lavorare solo dietro una VPN e che sono da utilizzare in un ambiente di rete strutturata.

Per chi volesse approfondire, a questa pagina trovate un elenco comparativo dei principali software di remotizzazione del desktop https://en.wikipedia.org/wiki/Comparison_of_remote_desktop_software .
Per chi è appassionato di informatica saprà invece che Linux teoricamente non necessita di tali software in quanto il "server grafico" (X Server) si posizione su di un layer superiore al sistema operativo ed è remotizzabile su qualsiasi display per sua natura.

Non sarebbe utile una guida per tutti i sistemi software, ed abbiamo pertanto deciso di focalizzare l'attenzione su due prodotti che abbiamo ritenuti validi per un buon compromesso tra sicurezza, serietà del produttore, costi, facilità d'utilizzo.
Successivamente amplieremo per i prodotti "dietro VPN" che rappresentano la situazione ideale per lavorare su ambiente client server remoti.

Si raccomanda, sempre per mantenere la sicurezza al primo posto, di non scaricare mai software pirata, craccati software di dubbia provenienza o da siti internet non ufficiali, in quanto potrebbero non essere versioni originali e contenere malware. Se disponibili fare il check del pacchetto con MD5Sum e confrontare l'hash prodotto con quello messo a disposizione del produttore, se l'impronta non corrisponde vuol dire che il file scaricato non è sicuro.

Questo documento è solo un compendio, che lascia ovviamente libero chiunque di scegliere il prodotto che ritiene più valido per le sue esigenze, consigliamo sempre di leggere la licenza d'uso che lo accompagna e di tenere aggiornato il sistema operativo e controllare sempre che il tutto sia privo di malware. La licenza è fondamentale in quanto spesso i software proprietari hanno una licenza d'uso "gratuita" per il solo utilizzo commerciale e non aziendale, pertanto non sono utilizzabili per il nostro scopo se non dietro regolare pagamento della licenza. Diversamente altri software potrebbero semplicemente offrire delle versioni "trial" (di prova) che poi smetterebbero di funzionare dopo un certo periodo di tempo di utilizzo.
I software open source invece non hanno questo problema in quanto il software è sempre utilizzabile per qualsiasi scopo.

Fase iniziale di controllo

Antimalware

Questa fase non è obbligatoria, ovviamente potreste già essere strutturati ed aver già installato tutti gli strumenti di protezione necessari, noi la inseriamo comunque a favore di chi non fosse attrezzato, sottolineando che non si tratta di un obbligo ai fini del "controllo remoto" ma una precauzione dettata dal buon senso e da poter inserire a livello di GDPR quali "misure intraprese".
Non è necessario invece per chi utilizza Linux o Mac. Trattandosi di controllo remoto

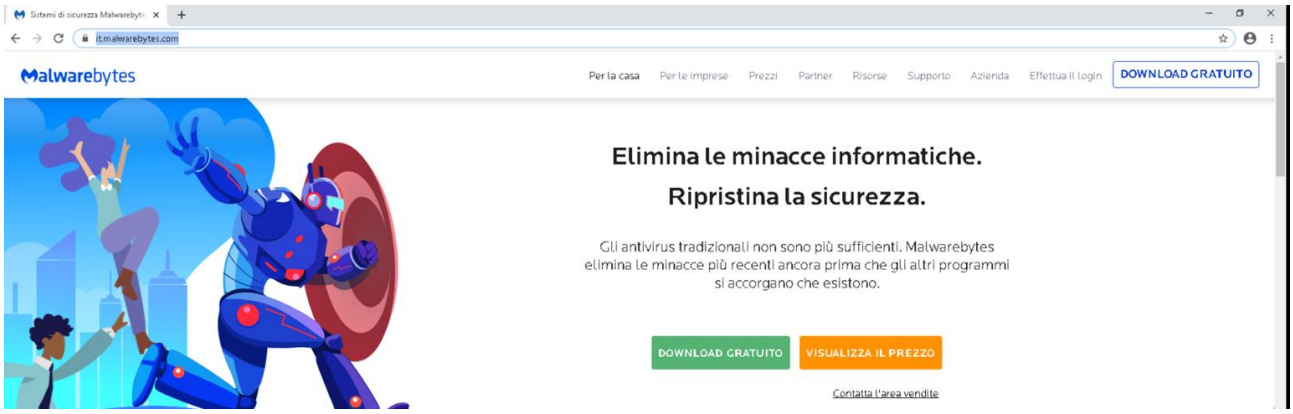
Controllare il proprio PC con i seguenti software:

- procedere ad un preventivo controllo con il proprio antivirus
- scaricare ed installare il programma Malwarebyte o in alternativa superantispyware entrambi nella versione free

Malwarebyte

Scaricare il software da qui e procedere alla sua installazione https://www.malwarebytes.com/mwb-download/thankyou/

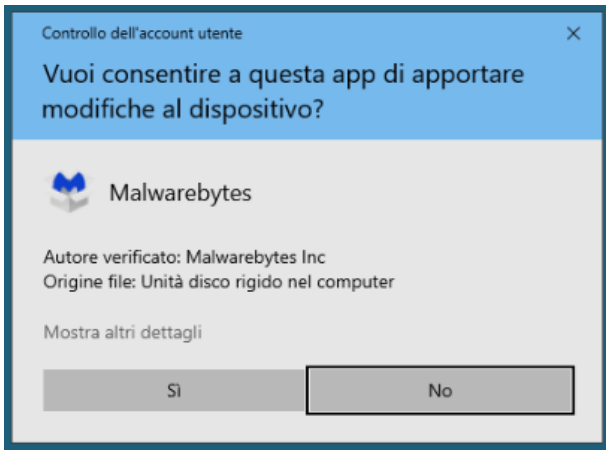
quindi premere su "Download Gratuito"



Salvare e/o eseguire il file. A seconda del browser utilizzato e delle sue impostazioni vi verrà richiesto il salvataggio oppure verrà salvato nella cartella di Download di default.

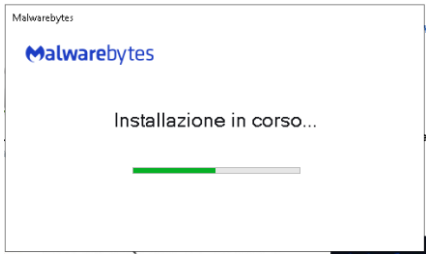
- In Chrome potete trovarlo in basso a sinistra della barra dei download
- In Firefox in alto a destra nei download evidenziati con un freccia verso il basso

Lanciate l'installer e confermate l'eventuale richiesta di "super user" (anche in questo caso le indicazioni possono cambiare in base alla versione di sistema operativo Windows utilizzato e alle sue impostazioni a livello di utente e permessi.

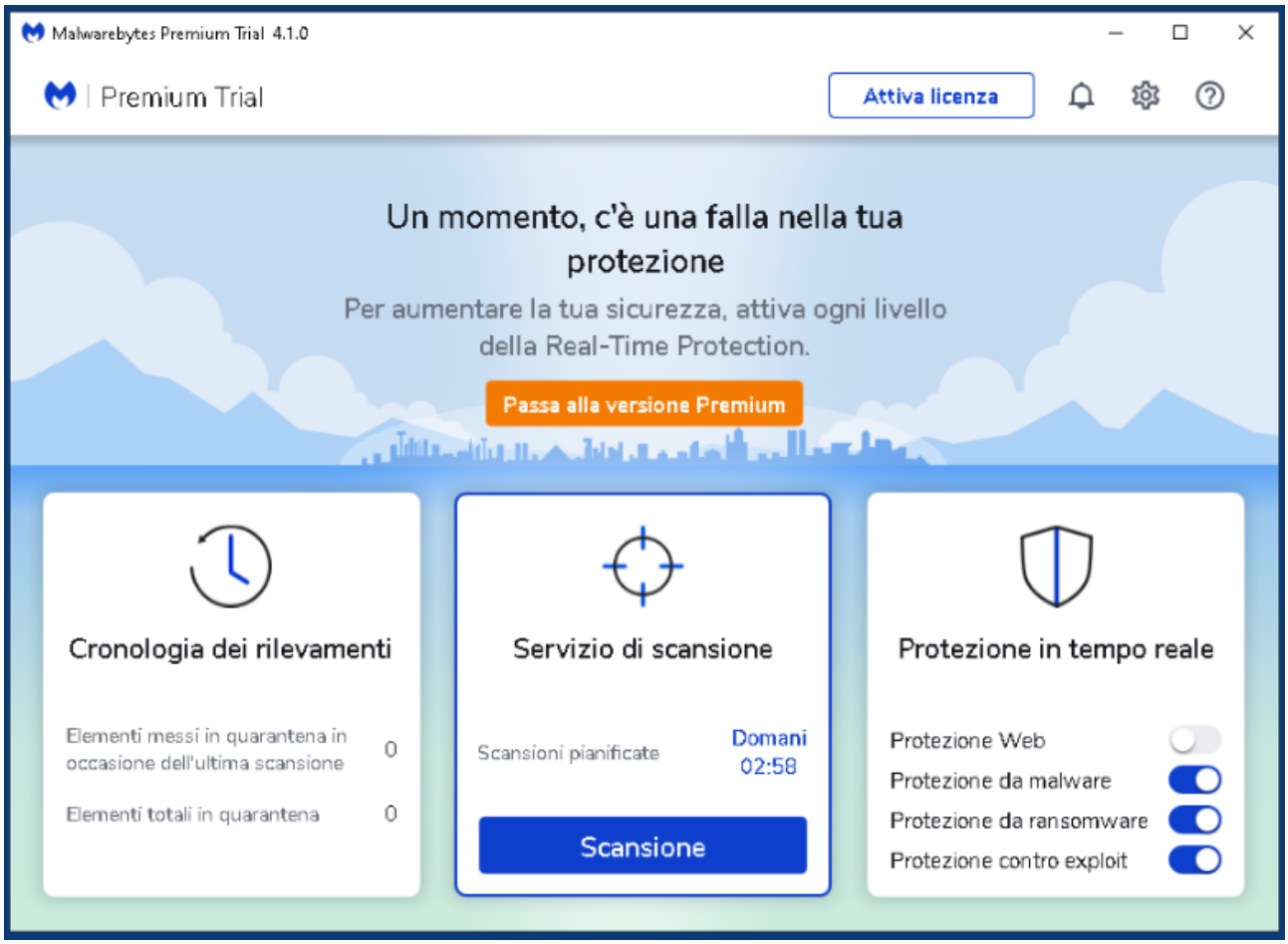


Confermate quindi che volete effettuare una installazione su “computer Personale”

e confermate con il pulsante installare

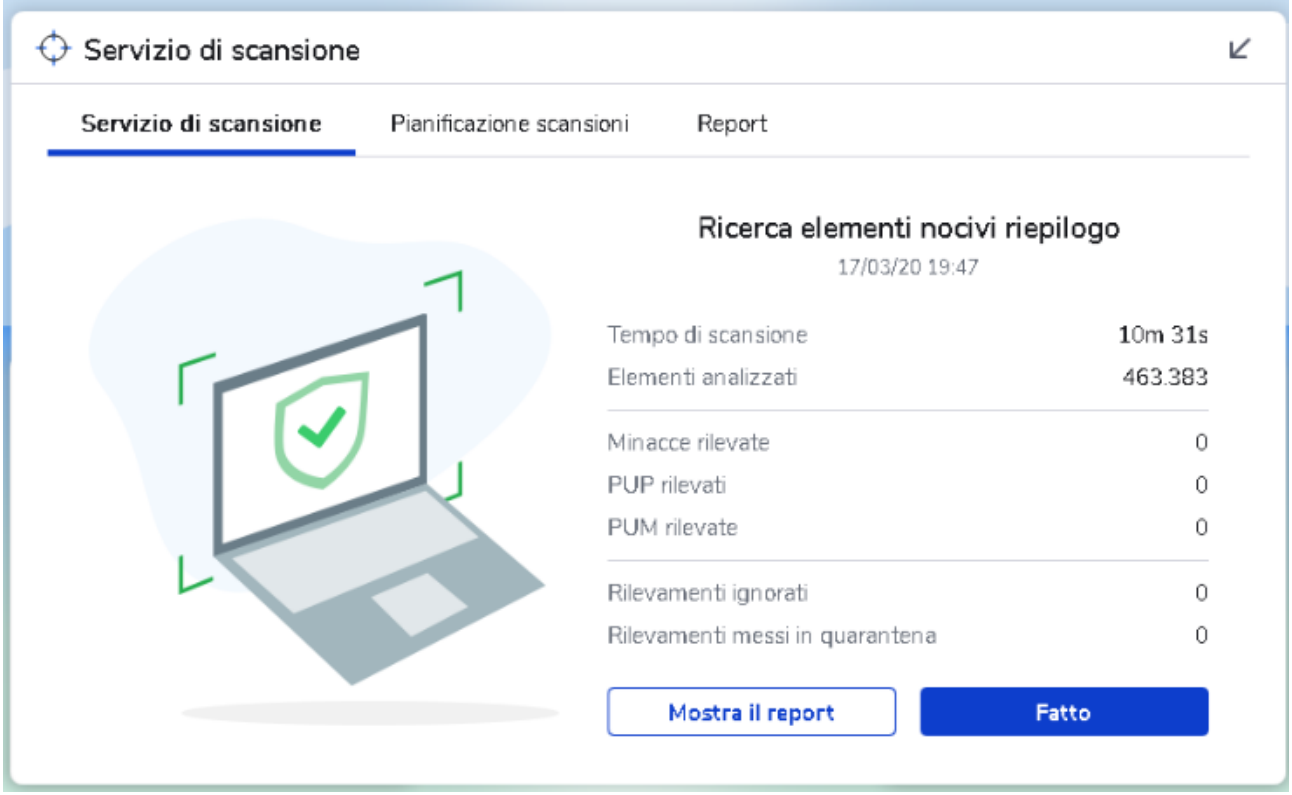


al termine dell’installazione, se non avete acquistato la versione “pro” e non sono di vostro interesse potete disattivare la funzione di “Protezione Web” e quindi procedere alla scansione



Se al termine della stessa non vi sono problemi potete anche disistallare il prodotto.

Al termine dell'operazione, la cui durata dipende sostanzialmente da quanti dati sono salvati sul disco fisso, verrà prodotto un reporter che ovviamente dovrà risultare negativo



Superantispyware

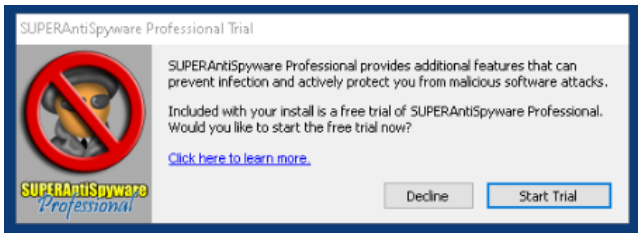
Si tratta di una versione simile, ma evoluta, rispetto al precedente. Nella versione gratuita non permette la scansione in tempo reale, ma per il nostro scopo può non essere utile. L'interfaccia è molto spartana e può sembrare un software "vecchio" in realtà è funzionale pur utilizzabile solo in versione trial per 14gg è anche dotato di una versione "live" cioè da utilizzare senza installarlo, magari su supporto usb.

Scarichiamolo da qui: https://www.superantispyware.com/

vanno bene entrambe le versioni Free o Pro con le differenze qui esposte

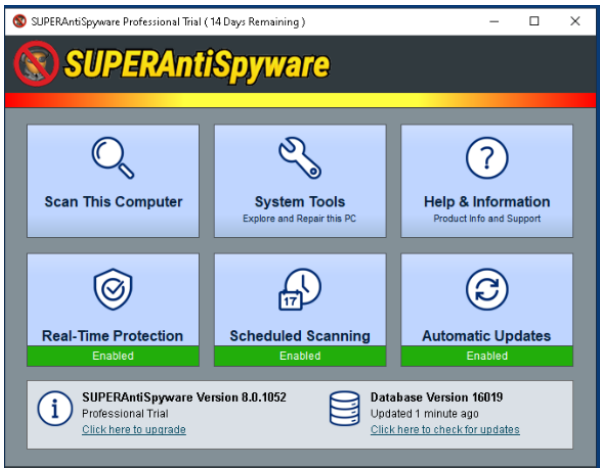
Features	SUPERAntiSpyware FREE	SUPERAntiSpyware PRO
Detect & Remove Malicious Threats from Malware, Spyware, Adware, Trojans, Dialers, Worms, Ransomware, Hijackers, Parasites, Rootkits, KeyLoggers, and many more.	●	●
Multi-Dimensional Scanning a next-generation scanning system that goes beyond the typical rules-based methods.	●	●
Process Interrogation Technology detects hard-to-find threats usually missed by standard anti-spyware applications.	●	●
Real-Time Threat Blocking stops malicious files from running as soon as they are detected.	*must run scans to block threats	●
Automatic Updates ensure the program is running with the latest database definitions.	*must update database manually	●
Multiple Scan Options schedule either quick, complete, or critical scans to fit your schedule.		●
Email Notifications get emails with scan results so you can monitor PCs remotely.		●

Al termine dell'installazione possiamo far partire i 14gg di prova, trascorsi i quali il software sarà disattivato

al termine la spartana 

finestra stile anni 90 attende la scansione del computer: clicchiamo quindi sul "Scan This Computer" ed attendiamo anche in questo caso il termine delle operazioni

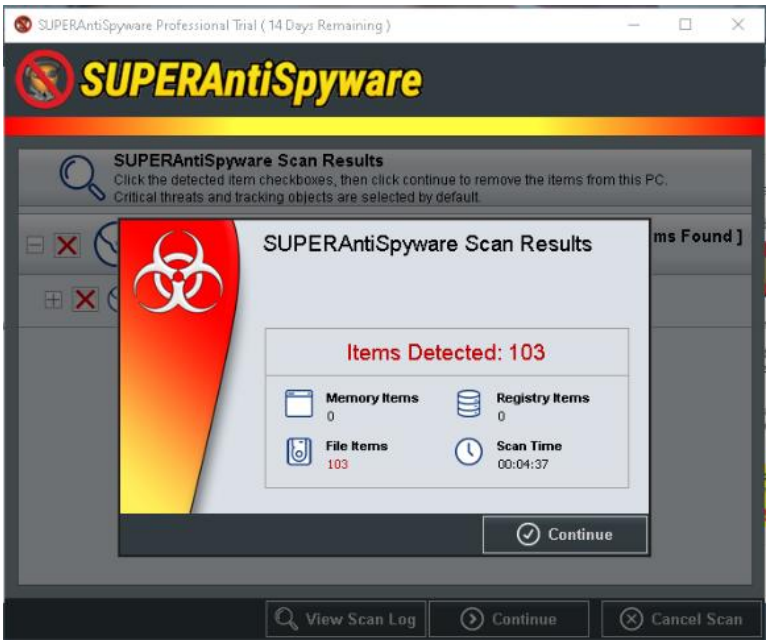
a noi la scelta tra la scansione profonda o rapida

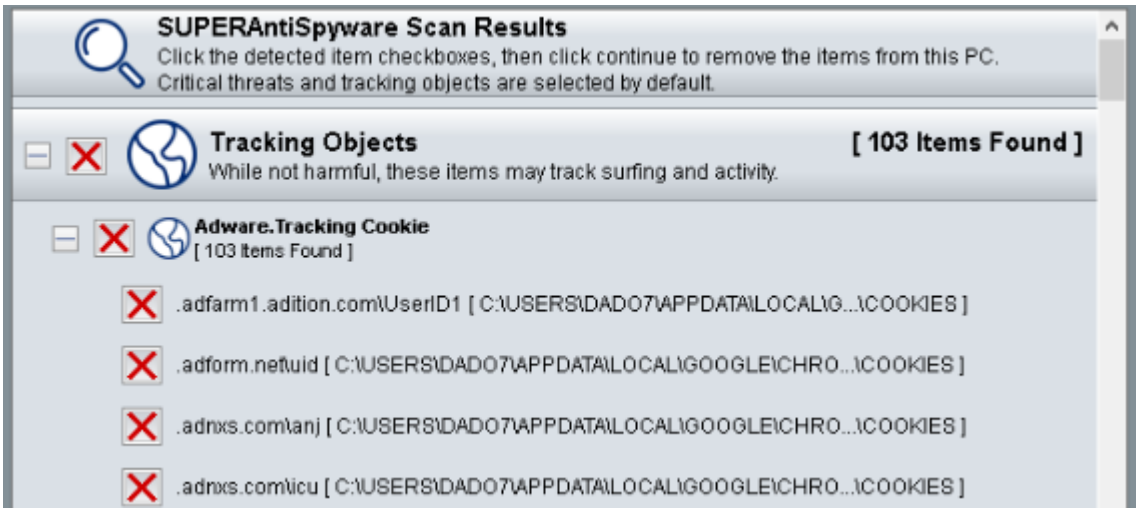


Al termine viene mostrato il relativo report

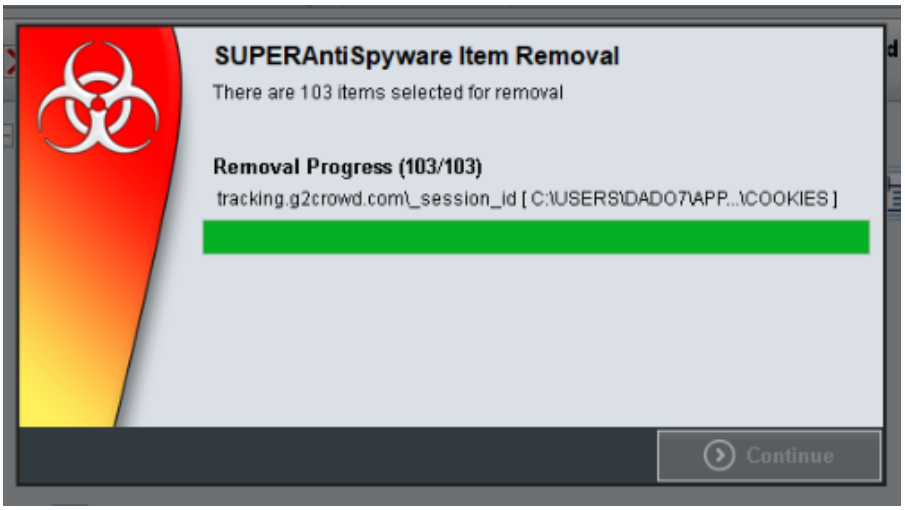
nel csaso specifico si nota che sono stati identificati ben 103 file potenzialmente pericolosi, rispetto al malwarebyte.

Cio perché sono stati evidenziati anche tutti i coockies di tracciametno prenseti nella cache del browser





possiamo cosi procedere anche alla loro cancellazione



Controllo Energia

Fondamentale che il computer non vada in standby (ibernazione o sospensione) altrimenti sarà impossibile collegarsi da remoto.

Anche per quanto riguarda gli aggiornamenti automatici di windows, che talvolta procedono al riavvio, oppure provocano problematiche (es. blocchi o errori) sarebbe opportuno procedere come segue:

- accertarsi che non vi siano problemi con gli ultii aggiornamenti rilasciati dal sito ufficiale di microsoft update
- Procedere ad aggiornare il sistema operativo (può essere una operazione che occupa parecchio tempo)
- disattivare la sospensione del pc (rocedura diversa da versione a versione

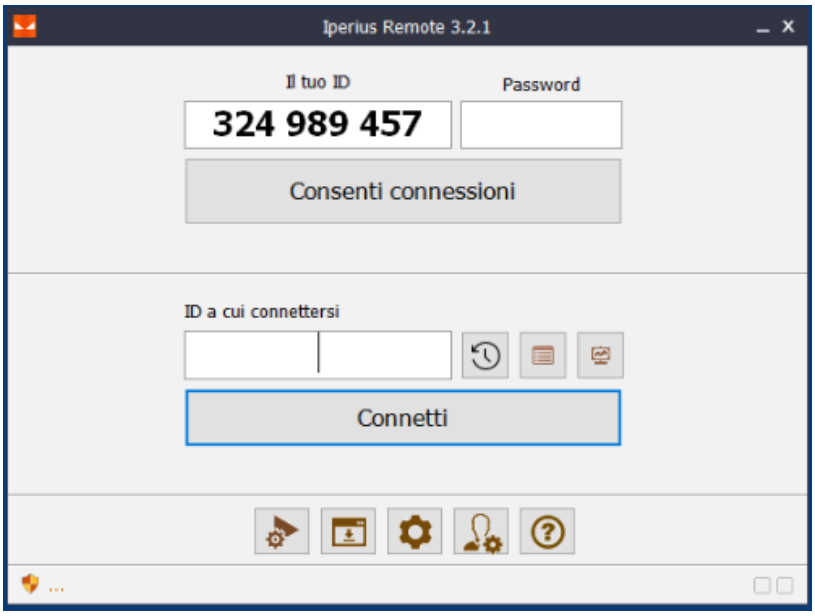
Fase di configurazione del software di controllo remoto

Ribadendo che la fase precedente precedente puo essere omessa ed è indicata per una maggior sicurezza, si passa adesso ad illustrare l'installazione del software che riteniamo il piu adatto alle nostre esigenze.

Ribadiamo che si trata di una scelta emergenziale ed orientata a piccoli studi o singoli professionisti, anche se, possedendo in ufficio una linea in fibra, non toglie che possa supportare numerose sessioni contemporanee in quanto il consumo di banda non è sicuramente idoneo.

Lato sicurezza abbiamo ovviametne scelto prodotti che garantiscono la sicurezza dei dati a livello di privacy, cryptazione e frequenza di aggiornamento e facilità di utilizzo con uno sguardo al prezzo

Iperius remote



Un prodotto poco conosciuto , prodotto da una software house italiana, strano a dirsi, ma questo è anche il momento di essere nazionalisti.

Non necessita di installazioni in quanto è utilizzato in modalità Live, disponibile solo per Windows e per i sistemi mobile iOS e Android

Procediamo al download , sempre dal sito ufficiale ed eseguiamo il file scaricato. L'interfaccia che ci viene mostrata è volutamente spartana e divisa in 3 parti orizzontalmente poste:

il nostro pc da contorllare sopra, i dati per controllare un pc remoto nel centro, e la barra delle configurazioni in basso

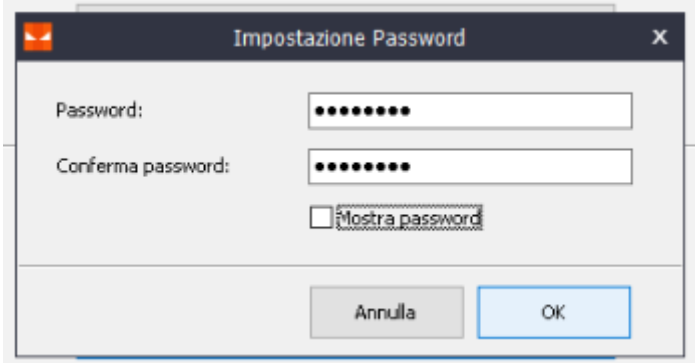
segnamoci "il tuo id" che ci servirà da remoto, assieme alla password, per collegarsi

per prima cosa va specificato che, nel caso si voglia impostare il software per un controllo "non vigilato" occorre procedere alla preventiva installazione, cosi che il box password possa essere attivato.

Dal pulsante delle impostazioni  andiamo a mettere il flag sulla voce " Impedisci al computere di andare in standby"

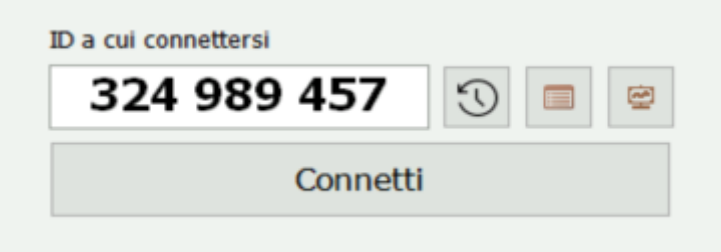
Clicchiamo poi sul primo pulsante da sinistra sulla barra in basso

Il sistema ci richiederà l'impostazione di una password per l'accesso da scegliere ovviamente con il solito criterio di "robustezza" (oltre 8 crt, maiuscole, minuscole, numeri, caratteri speciali e senza riferimenti specifici a cose o persone)



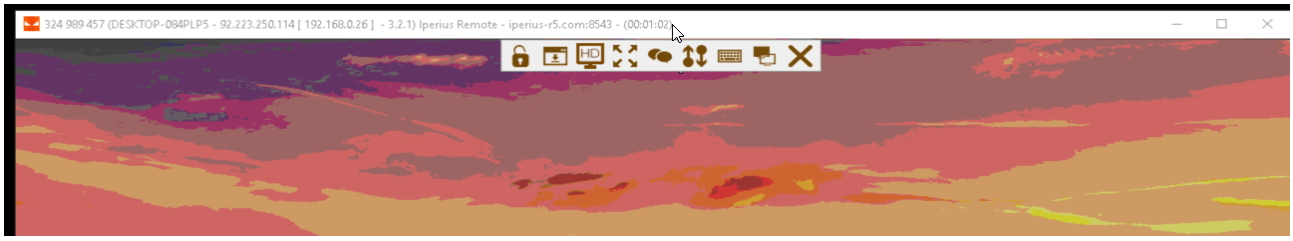
Spostandosi sul client dal quale effettuare la connessine (solitamente il portatile da casa, per fare un esempio) scarichiamo il medesimo software (oppure portarselo in un supporto usb) e lanciamolo

nella medesima mascherina inseriamo l'ID che ci siamo precedentemente appuntati e clicciamo su connetti



ci verrà richiesta la password da noi precedentemente impostata sul Server (pc in ufficio al quale collgarsi)

la login sul server sarà visualizzata e sarà prensete una barra dei comandi nella parte superiore contenente in sequenza



lancia CTRL ALT CANC sul computer remoto

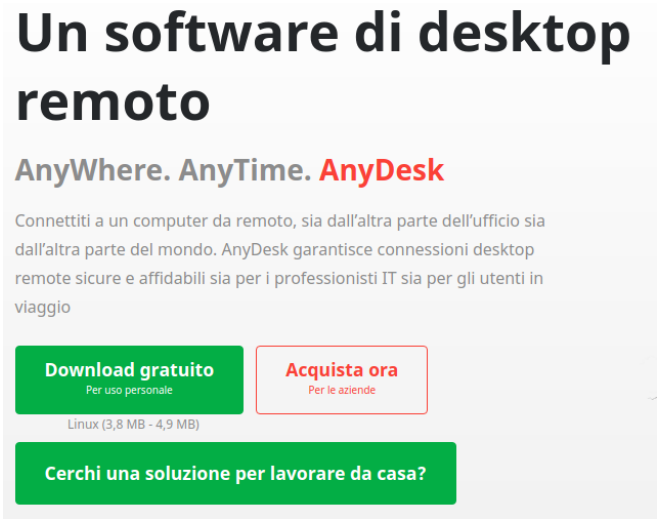
- aggiornamento del software
- impostazione della modalità frafica FullHD
- Impostazione a schermo intero (attiva/disattiva)
- Apertura di una chat
- Trasferimento file
- Mappatura della tastiera

Selezione del monitor (funzione quest'ultima utile se lato server fossero collegati piu di un monitor)

Il sotware non è compatibile con le sessini multiple RDP di microsoft e pertanto non è adatto ai server che hanno attivo tale servizio (es. Microsoft windows server + rdp server, o Thnstuff)

Anydesk

E' il secondo che ci consigliamo di segnalarvi; deriva da un fork di Teamviewer ed è gratuito per uso personale, pertanto necessità di essere acquistato per essere in regola. La versione free, limitata ma ottima è utilizzabile solo per utilizzo personale.



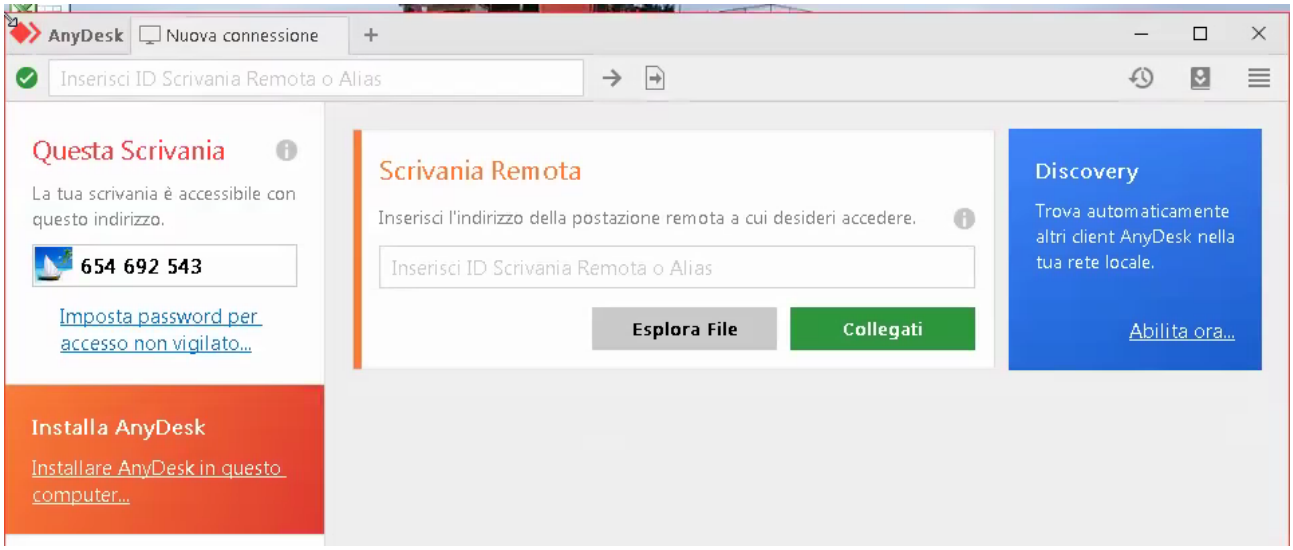
Da poche ore sul sito apparso un nuovo link riportante "Cerchi una soluzione per lavorare da casa?" segno che anche in Germania stanno organizzandosi per il telelavoro pensando al preggio.

Disponibile nativamente anche per Linux oltre che per windows mac, android e ios, è molto veloce e come Iperius permette accesso non vigilato mediante password.

Scarichiamolo da qui https://anydesk.com/it

nella versione che riteniamo idonea alle nostre esigenze e procediamo al classico doppio click (su windows) per il suo avvio in modalità live

l'interefaccia che si presenta è pulita e divisa verticalmente , non del tuto intuitiva



sulla sinistra i dati del PC server (da controllare nella parte centrale la "scrivania remota" da utilizzare sul client (controllore) ove andare ad indicare i dati del server remoto (pc di ufficio)

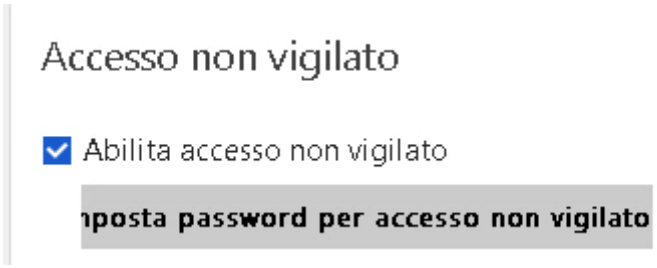
Anche in questo caso, come iperius, per abilitare la modalità di accesso non vigilato, occorre procedere all'installazione del software. Casella ben evidenziata in rosso

il software è molto leggero e l'installazione rapidissima anche su pc datati, dalla finestra post-installazione andiamo immediatamente ad impostare la password per l'accesso non vigilato.

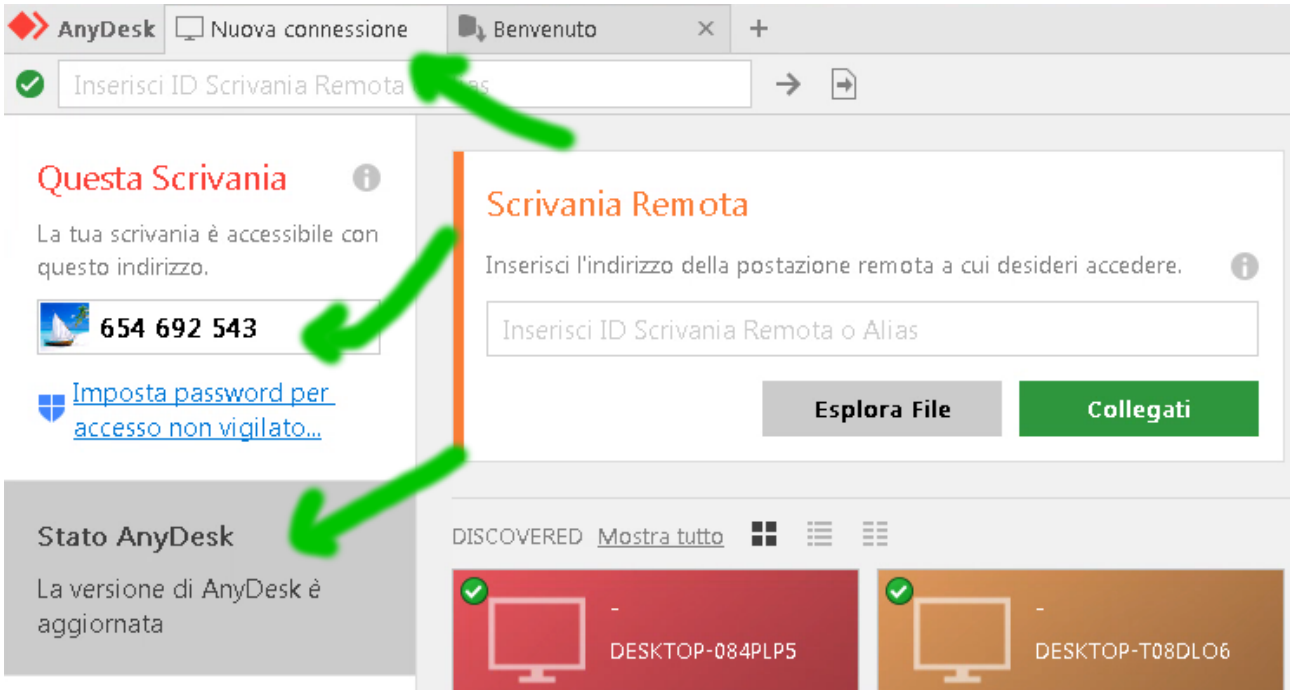
Premiamo quindi su “configura password”

Selezioniamo il flag su “Consenti sermpre”

quindi su Imposta password (valgono gli stessi criteri di sicurezza gia citati)



il software è pronto a ricevere connessioni da remoto



sul pc client procediamo ai medesimi passi (non occorre installarlo se non si vuol controllarlo) ed indicare nel box “Scrivania Remota” il numero presente in “questa scrivania” del server, che ci saremo annotati.

Anydesk non permette di disattivare il controllo energia che è quindi una operazione da fare a mano

Per Windows 10 occorre andare nel Pannello di controllo – gestione energia

ed impostare il profilo massime prestazioni. Quindi controllare che sia impostato con “non sospendere mai quando connesso alla rete elettrica”

non inseriamo screenshot perché le impostaizoni possono cambiare da versione a versione del sistema operativo

Altri software

Altri due software che citiamo in quanto di particolare interesse sono

- VNC (nelle varie versioni)
- NoMachine-NX

Entrambi sono multipiattaforma nativa e necessitano pertanto di una VPN per funzionare.

NoMachine è un software proprietario, altamente professionale e gratuito per uso personale casa/uffico (è specificato nelle FAQ) https://www.nomachine.com/it .

VNC è un software di controllo, sviluppato da olivetti e poi da Oracle, opensource ed è quindi utilizzato sotto svariati nomi non tutti rilasciati opensource.

Tra le varie versioni consigliamo TightVNC https://www.tightvnc.com/ di semplice installazione e opensource

Per l’installazione e l’utilizzo di tali software rimandiamo ai manuali e alla relativa documentazione ufficiale piu che esaudiente.

VPN

Diamo un cenno per quanto riguarda la VPN (Virtual Private Network https://it.wikipedia.org/wiki/Rete_virtuale_privata) in quanto se ne consiglia l’utilizzo aziendale come base per una infrastruttura piu solida.

La VPN è in pratica un servizio (software) che permette di creare una rete privata, attraverso la quale far viaggiare dati crittografati, appoggiandosi sull’infrastruttura di comunicazione internet.

Il Tunnel-VPN, come viene chiamato in gergo, in sostanza è l'equivalente del cavo di rete, virtualizzato.

Le VPN possono essere create sopra un firewall solitamente in azienda, oppure presso un fornitore di VPN remoto. Una volta creata la VPN, i client che vorranno far parte del nodo dovranno installare un piccolo software (client VPN) che metterà tutti i punti in collegamento. Apposite regole definite a livello di configurazione potranno gestire le regole di accesso a reti, sottoreti, indirizzi IP classi o sottoclassi, fornendo una infrastruttura modlulare e scalabile altamente sicura e robusta.

Tra i software piu utilizzati per creare VPN citiamo IPSec e OpenVPN entrambi opensource (come la maggior parte dei protocolli internet del resto) utilizzati in quasi tutti i firewall anche casalinghi ed in tutte le distribuzioni Linux.

Anche qui possiamo citare alcune distribuzioni specializzate in fireall quali:

- Pfsense
- IPCop
- ClearOS
- Smoothwall

Possono essere ovviamente installe sia presso l'azienda che su server in cloud reali o virtuali, l'unica necessità è un indirizzo publbico statico.

Per quanto a servizi di terze parti, queste vengono quasi sempre pubblicizzate come "sistemi per nascondersi" mentre la reale utilità è quella di unire punti remoti (pc, server, dispositivi) in sicurezza. Su internet si trovano facilmente servizi VPN ma, per sicurezza del nostro lavoro e dei nostri dati, consigliamo di rivolgersi ad un consulente (anche in CONEPRO ve ne sono) e di creare sempre una propria VPN.

A cura dell'associato Alessandro Scapuzzi, con il patrocinio della Commissione Informatica Co.Ne.Pro.

Roma, lì 18.03.2020