WPanel

Manuale configurazione Chromebook per VPS OpenVPN

Versione 1.0

11 dicembre 2023

Indice

1. Creazione del certificato client 3

1.1 Inserimento del certificato client all'interno del Chromebook 7

1.2 Download dei file per verificare il funzionamento della VPN in Windows 12

1.3 Chiusura della finestra di emissione del certificato client 13

2. Acquisto del VPS 14

3. Ricezione delle credenziali e dei parametri di configurazione 16

3.1 Pannello servizi del VPS 17

4. Configurazione della connessione VPN 18

4.1 Verifica della connessione VPN su un PC Windows 21

5. Accesso al desktop remoto via web 25

5.1 Visualizzazione a tutto schermo 27

5.2 Tasti funzione F1-F12 sulla tastiera del Chromebook 30

5.3 Connessione al desktop remoto trame app nativa 32

5.4 Inserimento dell'icona del desktop remoto sulla barra delle applicazioni 33

6. Configurazione accesso alle condivisioni di rete 36

7. Cifratura della partizione dati con BitLocker 41

7.1 Blocco dell'accesso alla partizione cifrata con BitLocker 48

7.2 Nuovo accesso alla partizione cifrata con BitLocker 50

8. Accesso a WPanel tramite smart card o token USB da un Chromebook 51

9 Recupero o modifica delle credenziali e accesso multiutente 57

9.1 Modifica delle credenziali dell'utente Administrator 57

9.2 Modifica delle credenziali dell'utente associato alla VPN 59

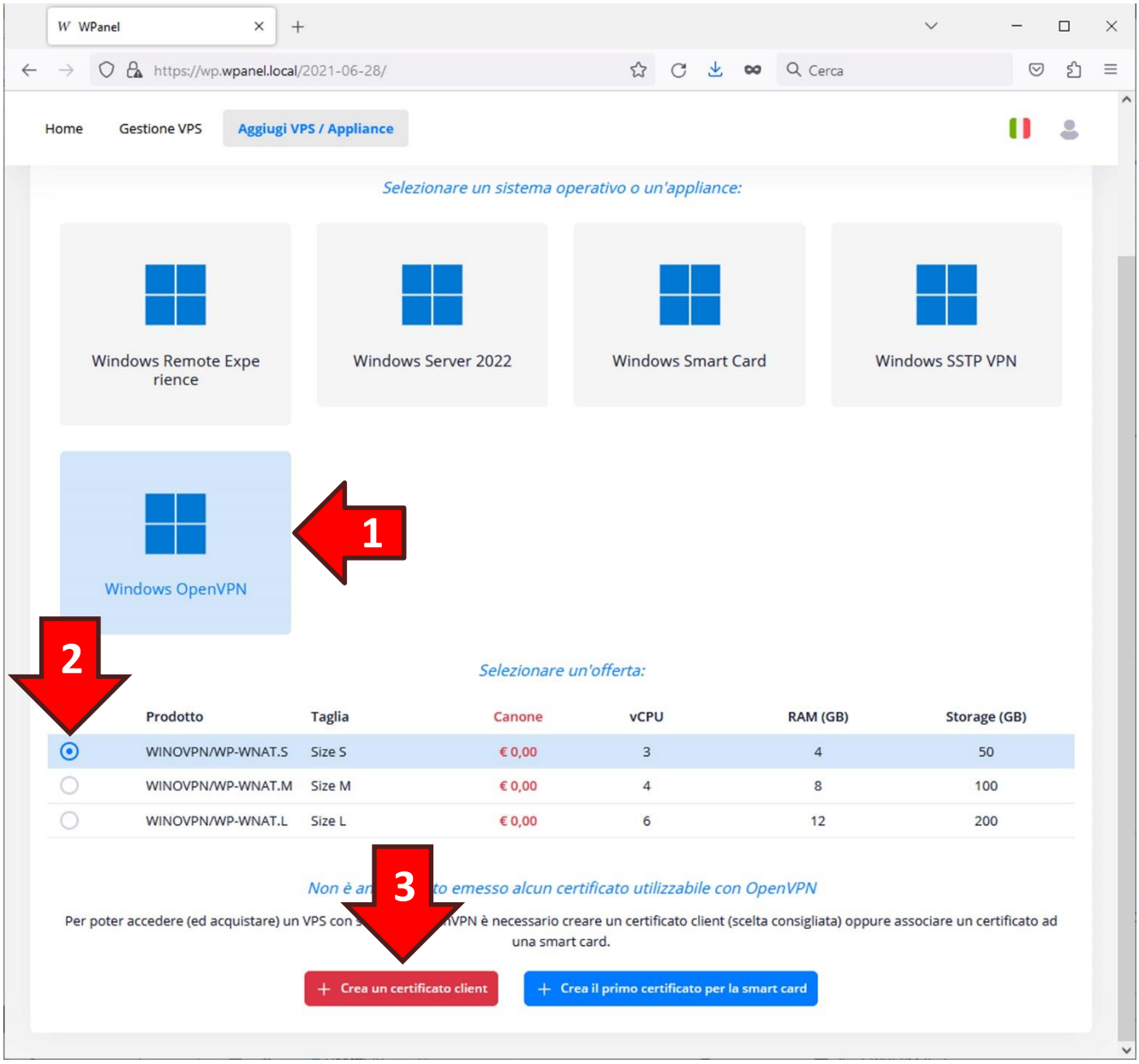
9.3 Accesso VPN con più certificati client (UPN multipli) 63

9.4 Accesso VPN da parte di più utenti 65

1. Creazione del certificato client

I VPS della linea OpenVPN sono accessibili dall'esterno esclusivamente con un client OpenVPN. Per questo motivo il nostro sistema richiede che l'utente sia in possesso di almeno un certificato da inserire nel proprio client OpenVPN.

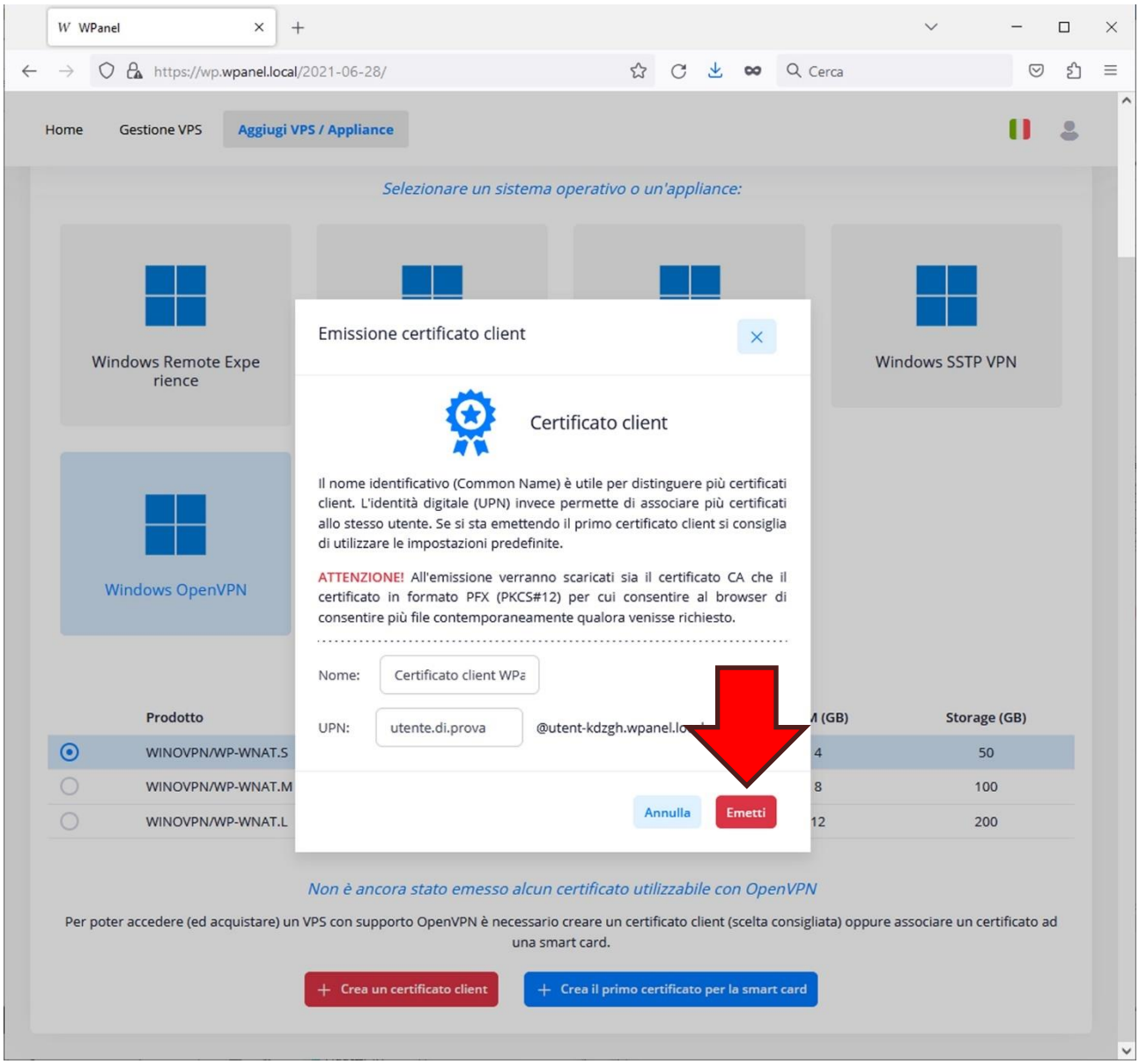
Per questo, motivo una volta selezionato il **tipo (1)** ed il **taglio (2)** in fase di acquisto, prima di procedere al pagamento il sistema richiederà di generare il primo certificato client. Cliccare quindi sul tasto rosso **Crea un certificato client (3)**.



Verrà visualizzata la finestra di emissione del certificato client. Se si è l'unico utente ad accedere al VPS si consiglia di utilizzare i valori predefiniti.

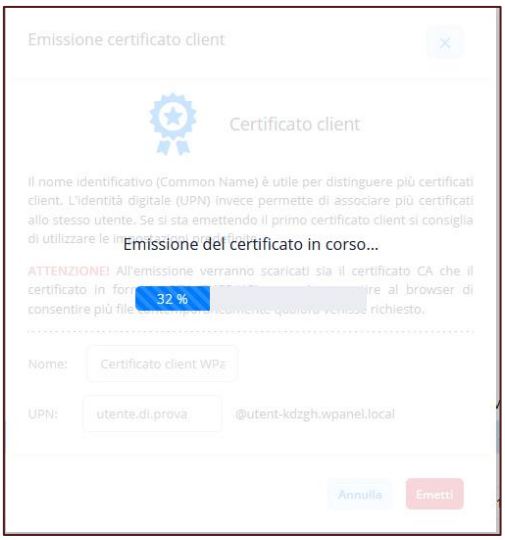
Se invece si ha intenzione di creare un pool di VPS accessibili da specifici gruppi di Chromebook aziendali è necessario sapere che il server VPN, una volta riconosciuta la validità del certificato client, filtra l'accesso sulla base di un elenco di **identità digitali (User Principal Name)**. La prima identità digitale (UPN) viene selezionata in fase di acquisto del VPS. Le successive identità digitali (UPN) possono essere inserite nell'elenco seguendo le indicazioni del paragrafo ***9.3 Accesso VPN con più certificati client***.

Per ottenere il certificato client cliccare il tasto **Emetti**.

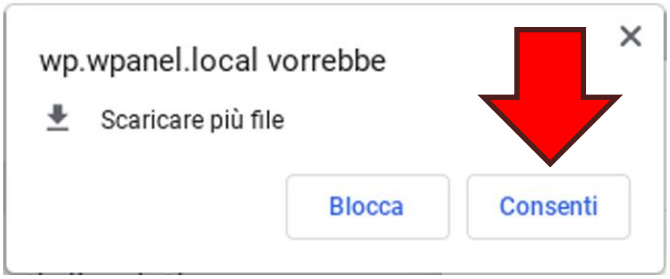


Attualmente, per agevolare l'utente nella configurazione della propria VPN su un Chromebook, non è possibile inviare un *File richiesta di emissione del certificato (CSR)* mantenendo riservata la chiave privata. Il nostro reparto di ricerca e sviluppo è al lavoro per fornire in futuro tale opportunità.

Il sistema emetterà il certificato client nell'arco di alcuni secondi:

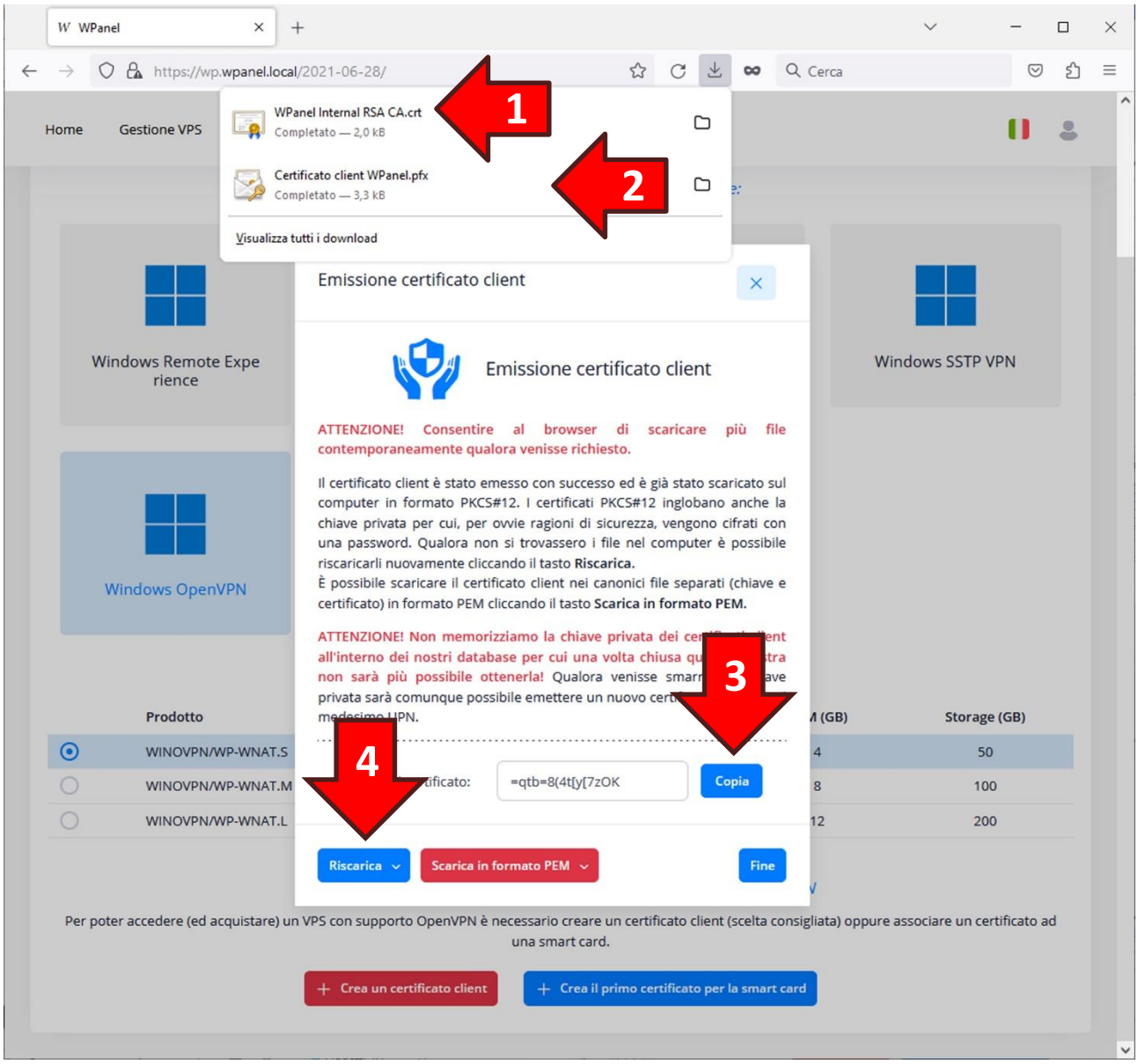


Al termine dell'elaborazione verrà automaticamente scaricato sia il *Certificato client in formato PKCS#12* che il *Certificato CA* necessario a dare validità al certificato client. Autorizzare quindi il browser Chrome al download di più file contemporaneamente cliccando il tasto **Consenti** dall'avviso che apparirà in alto della finestra:



Per ragioni di sicurezza i certificati contenenti la chiave privata vengono crittografati con una password. Quindi cliccare il tasto **Copia (3)** per acquisire tale password nella clipboard.

Se sul proprio Chromebook non si dovessero trovare **i due file indicati (1) (2)** è possibile ri scaricarli, anche singolarmente, utilizzando il tasto **Riscarica (4)**.

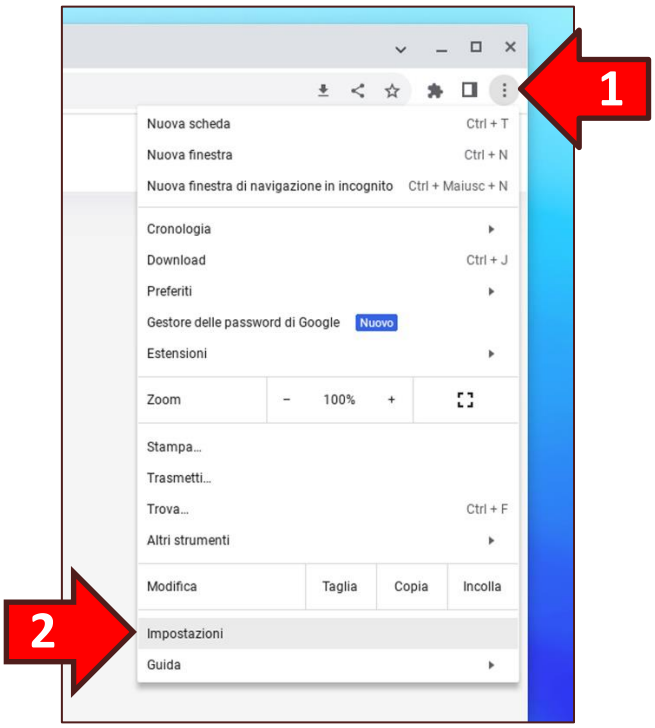


Si ricorda che il nome del **Certificato CA (1)** varia in base al fornitore del VPS.

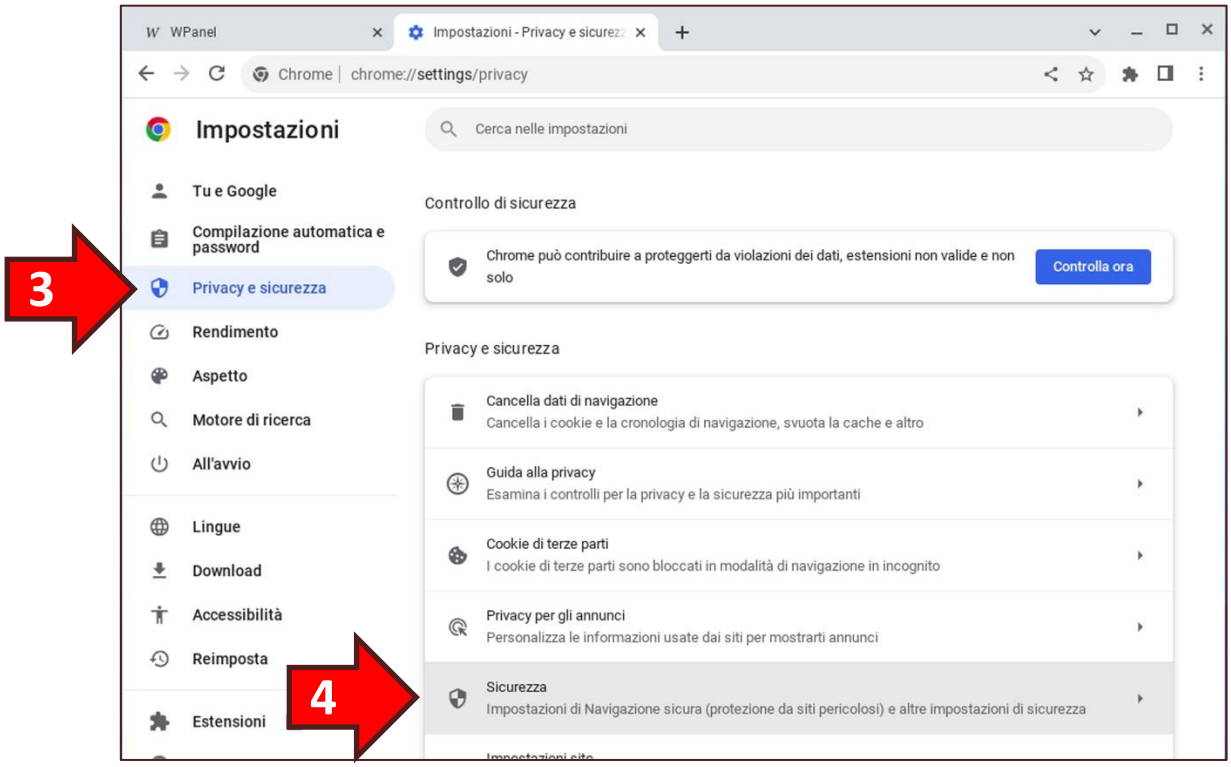
ATTENZIONE! Non chiudere la finestra Emissione del certificato client finché non si è completata la procedura di cui al successivo **paragrafo 1.1 Inserimento del certificato client all'interno del Chromebook**.

1.1 Inserimento del certificato client all'interno del Chromebook

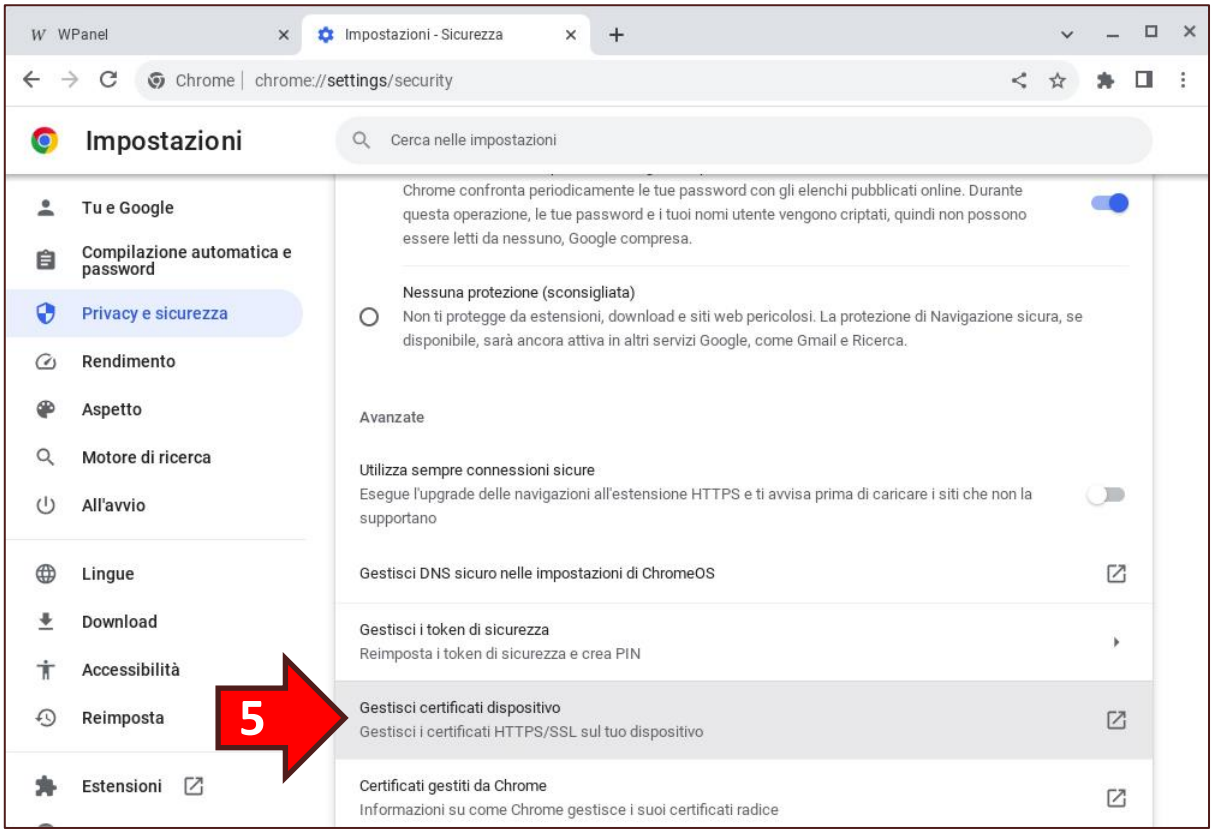
Dal browser Chrome del Chromebook cliccare sui **tre puntini (1)** in alto a destra. Poi dal menù selezionare l'opzione **Impostazioni (2)**:



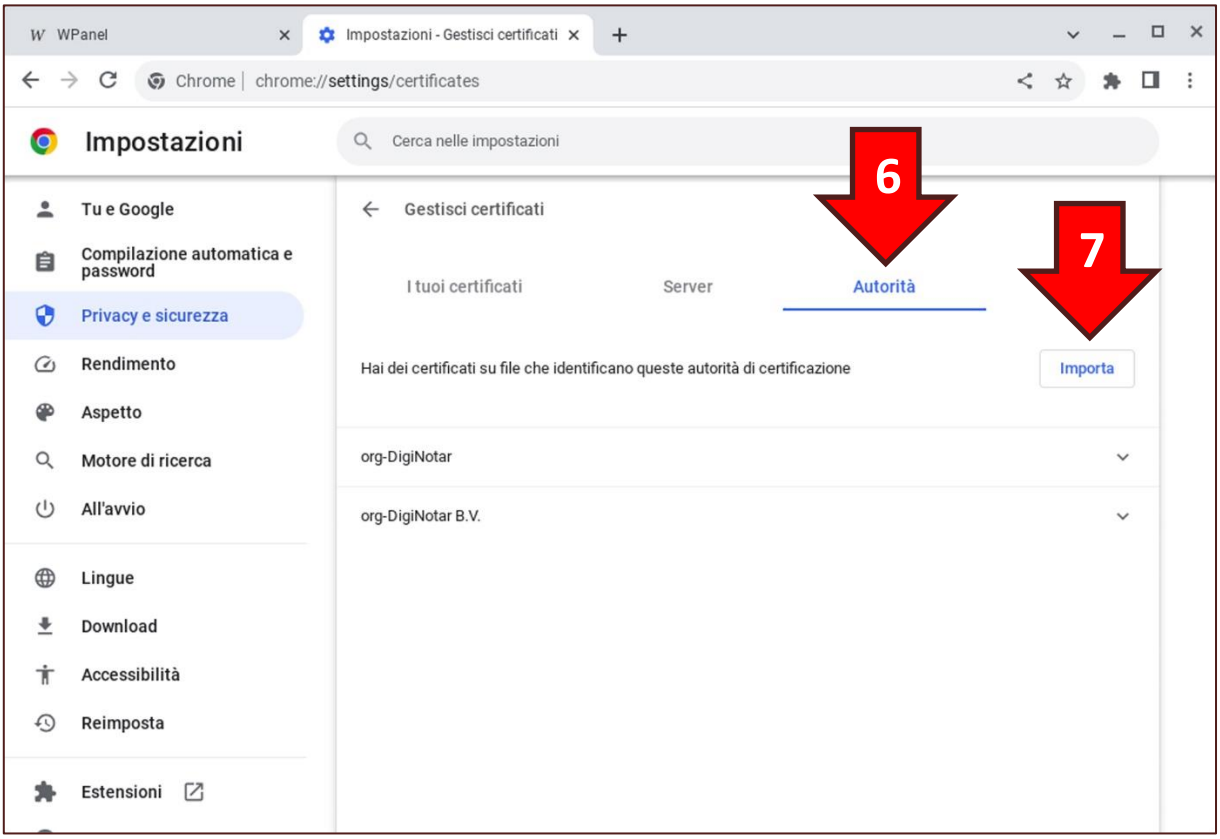
Nella sezione di sinistra selezionare l'opzione **Privacy e sicurezza (3)** e successivamente nella sezione di destra cliccare sull'opzione **Sicurezza (4)**:



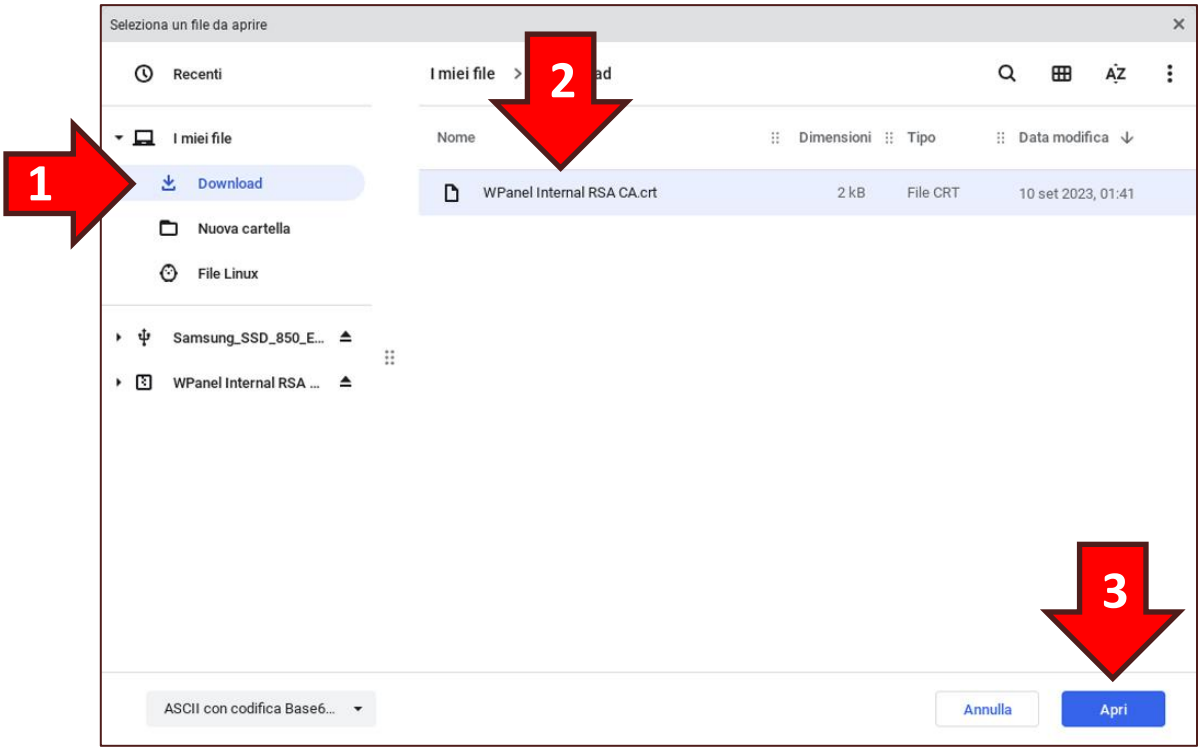
Scorrere poi la sezione di destra fino a trovare l'opzione **Gestisci certificati dispositivo (5)**:



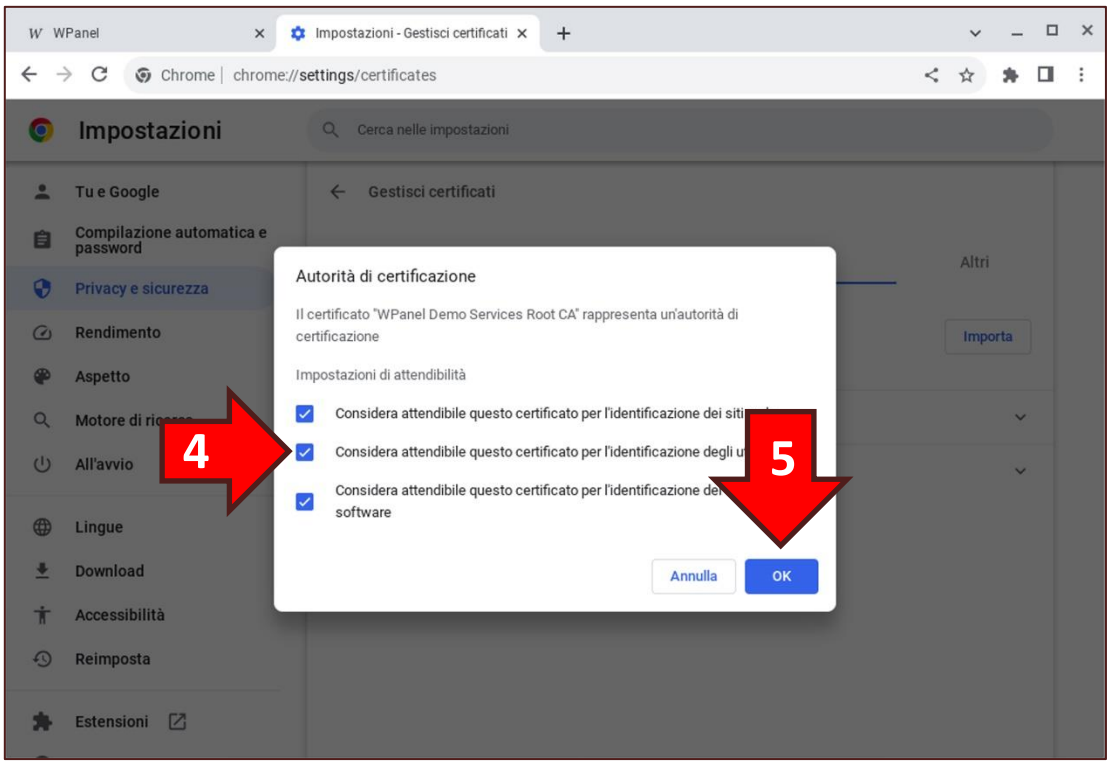
Poi nella sezione di destra cliccare prima sulla dicitura **Autorità (6)** e poi sul tasto **Importa (7)**:



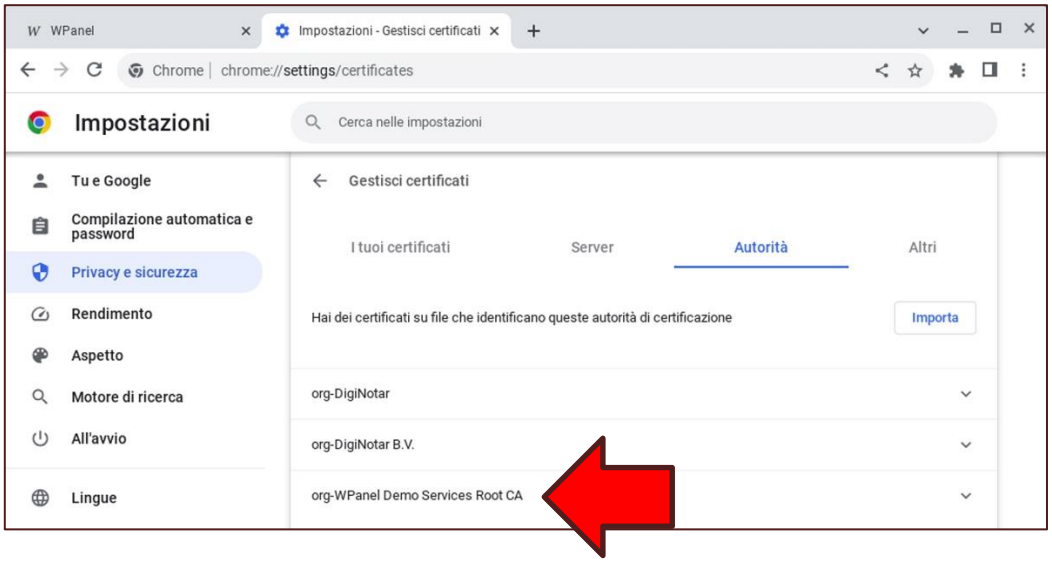
Dalla finestra *Seleziona un file da aprire* accertarsi di visualizzare i file della cartella **Download (1)**, poi selezionare **il file CA del proprio fornitore di VPS (2)** (il nome file dovrebbe terminare con *…Internal RSA CA.crt*). Quindi cliccare il tasto **Apri (3)**:



Nellla finestra *Autorità di certificazione* abilitare **tutte le spunte disponibili (4)** e poi cliccare sul tasto **OK (5)**:

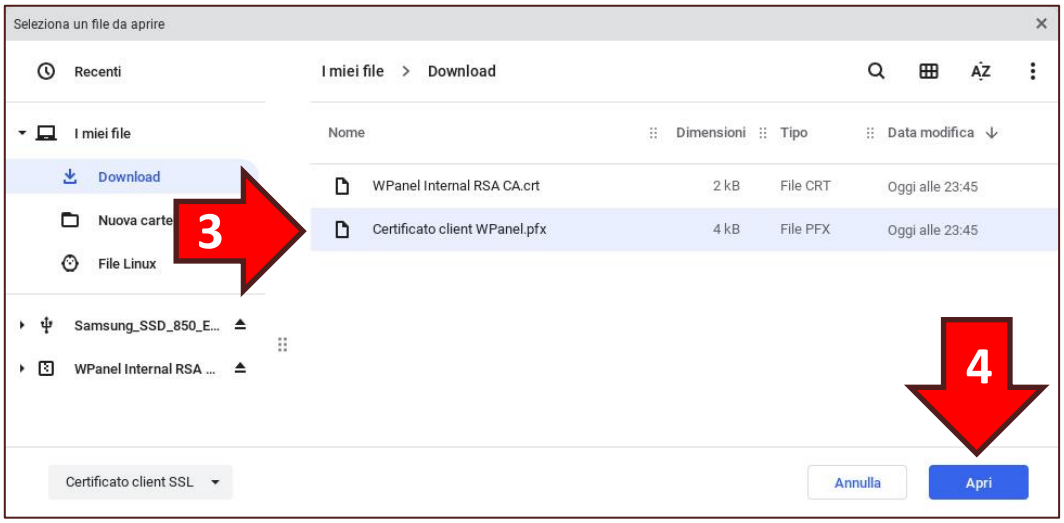


Trascorso qualche secondo l'**Autorità di certificazione** del vostro fornitore di VPS dovrebbe apparire in fondo all'elenco:

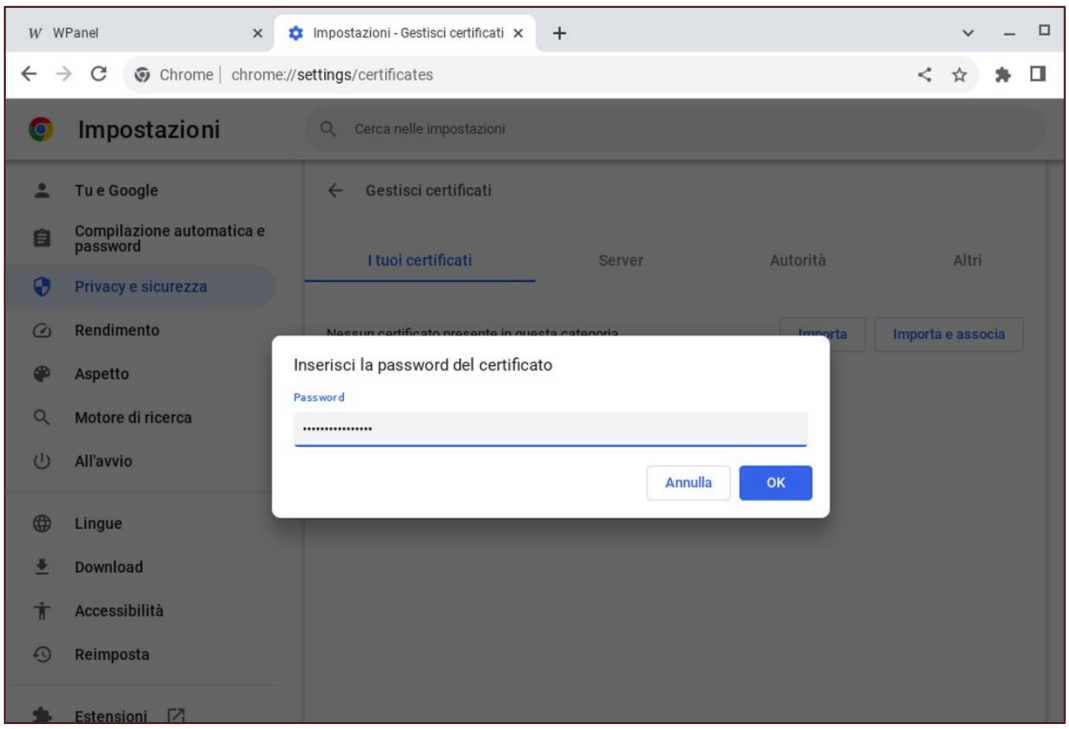


Ora nella sezione di destra cliccare sulla dicitura **I tuoi certificati (1)** e successivamente sul tasto **Importa e associa (2):**

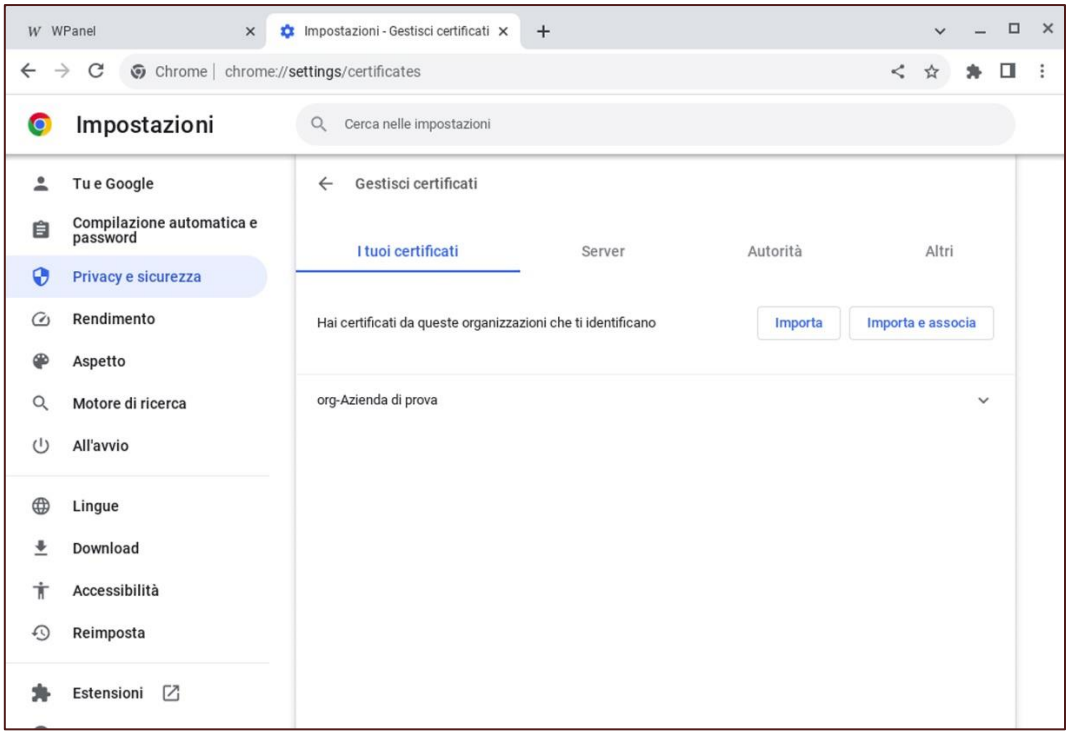
Poi dalla finestra *Seleziona un file da aprire* selezionare il nome del **certificato con estensione PFX (3)** e cliccare il tasto **Apri (4)**:



Nella finestra *Inserisci la password del certificato* premere la combinazione di tasti **CTRL+V** oppure digitare la password di cui all'ultima figura di **pagina 6**. Quindi cliccare il **tasto OK**:



Trascorso qualche secondo **il certificato client con il vostro nominativo** dovrebbe apparire in fondo all'elenco:

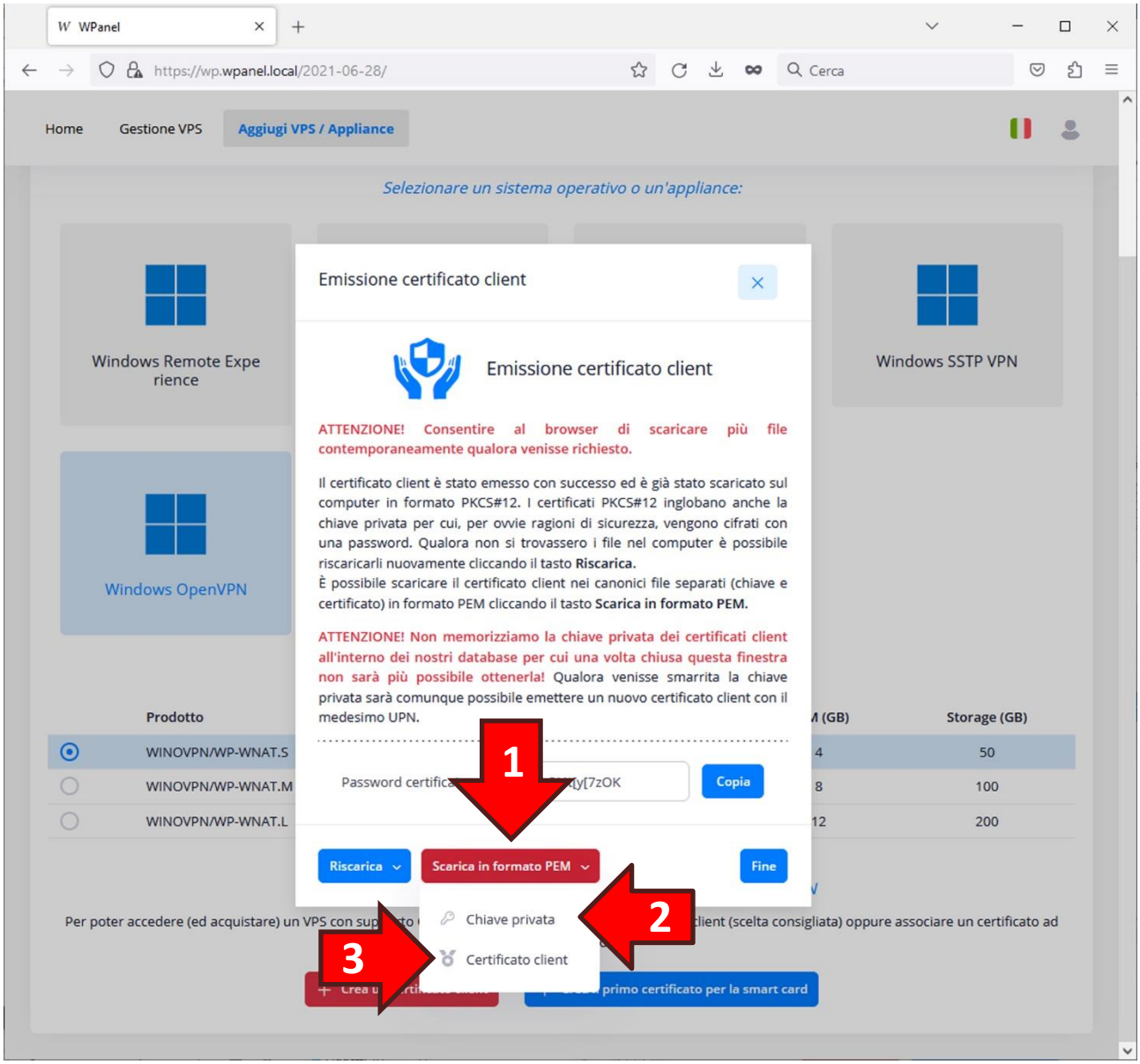


Ora è possibile chiudere la scheda delle Impostazioni e ritornare sulla scheda del sito WPanel del vostro fornitore.

1.2 Download dei file per verificare il funzionamento della VPN in Windows

WPanel permette il download del certificato client in due file separati (chiave privata e certificato client) in formato PEM per permettere a chi non ha confidenza con le VPN di tipo OpenVPN di effettuare i test di connessione attraverso il client OpenVPN per sistemi operativi Windows.

Cliccare quindi il tasto rosso **Scarica in formato PEM (1)** per selezionare il download della **chiave privata (2)** o del **certificato client (3)**:



ATTENZIONE! A titolo informativo si precisa che il file in formato PEM contenente la **chiave privata (2)** non è protetto da alcuna password.

1.3 Chiusura della finestra di emissione del certificato client

ATTENZIONE! Il sistema WPanel non memorizza per nessun motivo e in alcun caso le chiave private dei certificati generati quindi prima di chiudere la finestra di emissione del certificato accertarsi della presenza dei file nel proprio computer.

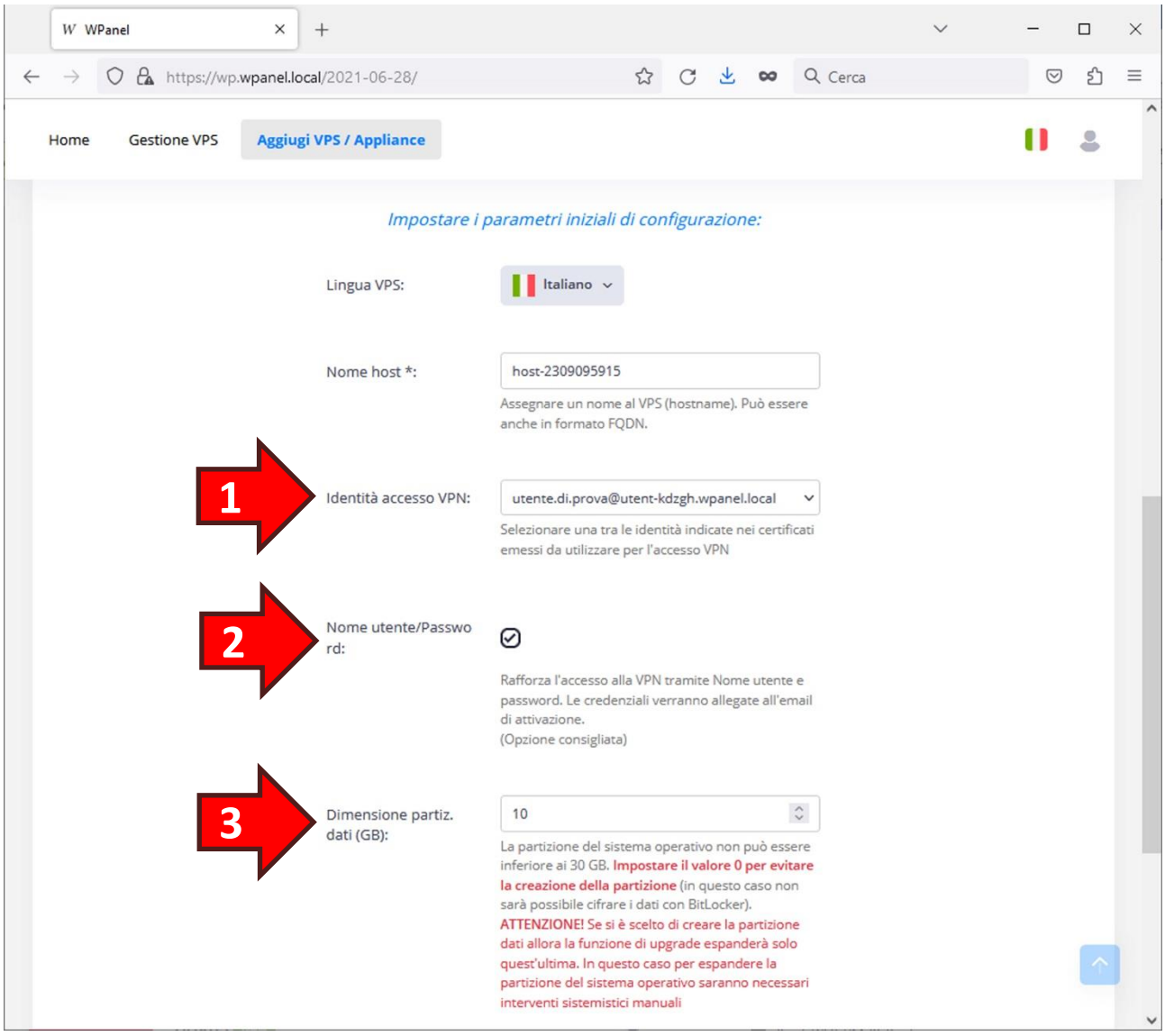
In caso di errore sarà comunque possibile generare un nuovo certificato client con il medesimo UPN utilizzando la **funzione Certificati** all'interno del menù del **profilo utente**.

2. Acquisto del VPS

Una volta generato il certificato client è possibile procedere con l'acquisto del VPS.

Il server OpenVPN verrà già configurato per accettare l'**identità digitale predefinita (UPN) (1)**. Qualora fossero stati generati più certificati client con differenti UPN, è possibile scegliere l'UPN desiderato da menù a tendina. Per aggiungere ulteriori UPN al server OpenVPN attendere la generazione del VPS e seguire le istruzioni indicate al paragrafo ***9.3 Accesso VPN con più certificati client***.

In fase di acquisto è possibile aumentare la sicurezza del tunnel OpenVPN attraverso le credenziali aggiuntive **nome utente/password (2)**. In questo modo è possibile proteggere l'accesso al VPS anche in caso di furto del Chromebook (perché la protezione risulti efficace è necessario disattivare il salvataggio delle credenziali nella configurazione della connessione OpenVPN all'interno del Chromebook).



In fase di acquisto è possibile creare una **seconda partizione (3)** destinata al salvataggio dei dati sensibili. La dimensione della partizione è espressa in GB. È possibile cifrare i dati della partizione attraverso il software *Microsoft BitLocker* già preinstallato nel VPS. A tal proposito si rimanda al **capitolo 7. Cifratura della partizione dati con BitLocker**.

Se non si desidera avere la partizione dati inserire il valore 0.

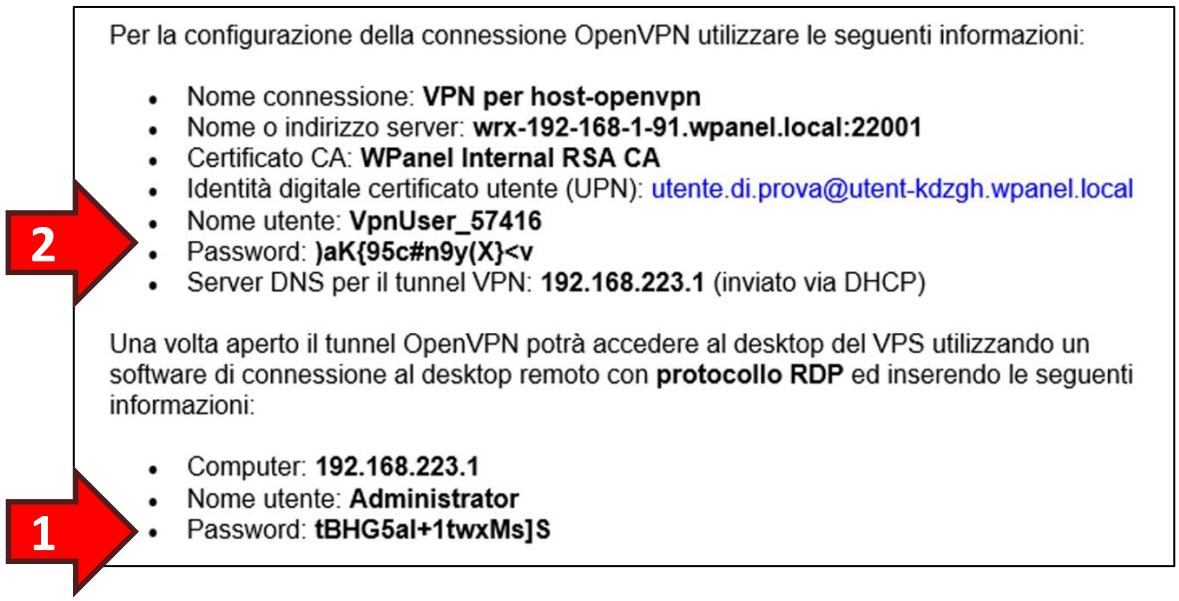
ATTENZIONE! La partizione dati verrà creata all'interno dello storage del VPS sottraendo spazio alla partizione del sistema operativo! Per consentire al sistema operativo di effettuare i dovuti aggiornamenti non è possibile restringere questa partizione al di sotto dei 30 GB.

3. Ricezione delle credenziali e dei parametri di configurazione

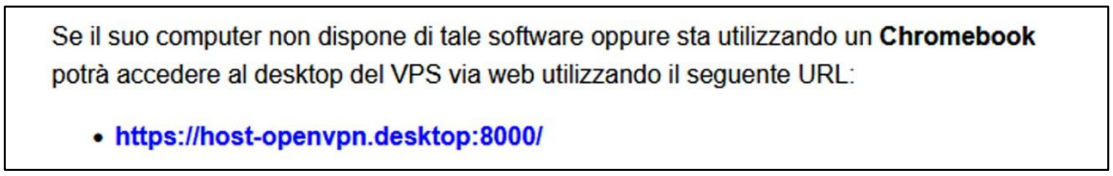
Una volta generato il VPS verranno inviate le credenziali di accesso via email. **Si consiglia di conservare tale email per eventuali riconfigurazioni!** Le credenziali al suo interno comprendono:

- la password dell'**utente Administrator (1)** del VPS;
- l'eventuale **nome utente (2)** associato alla connessione OpenVPN;
- l'eventuale **password (2)** associata al nome utente della connessione OpenVPN.

L'email conterrà i parametri di configurazione del tunnel VPN da inserire nel Chromebook come indicato nel **capitolo 4. Configurazione della connessione VPN**.

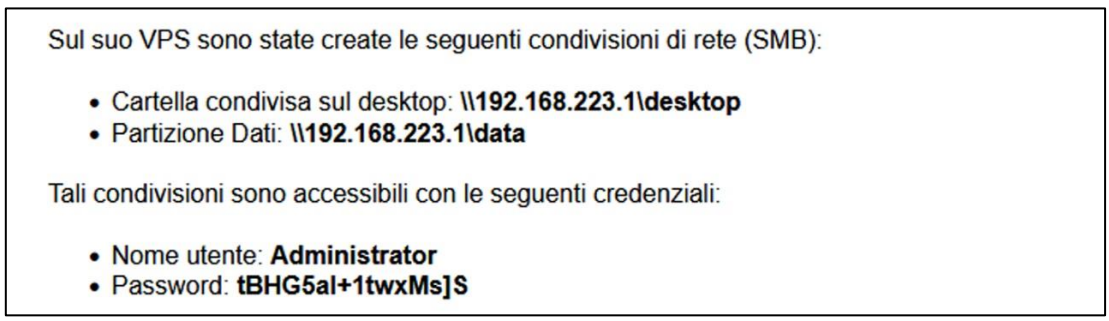


Nell'email sarà presente un URL per accedere al desktop remoto del VPS utilizzando il browser Chrome.



A tal proposito si rimanda al **capitolo 5. Accesso al desktop remoto via web**.

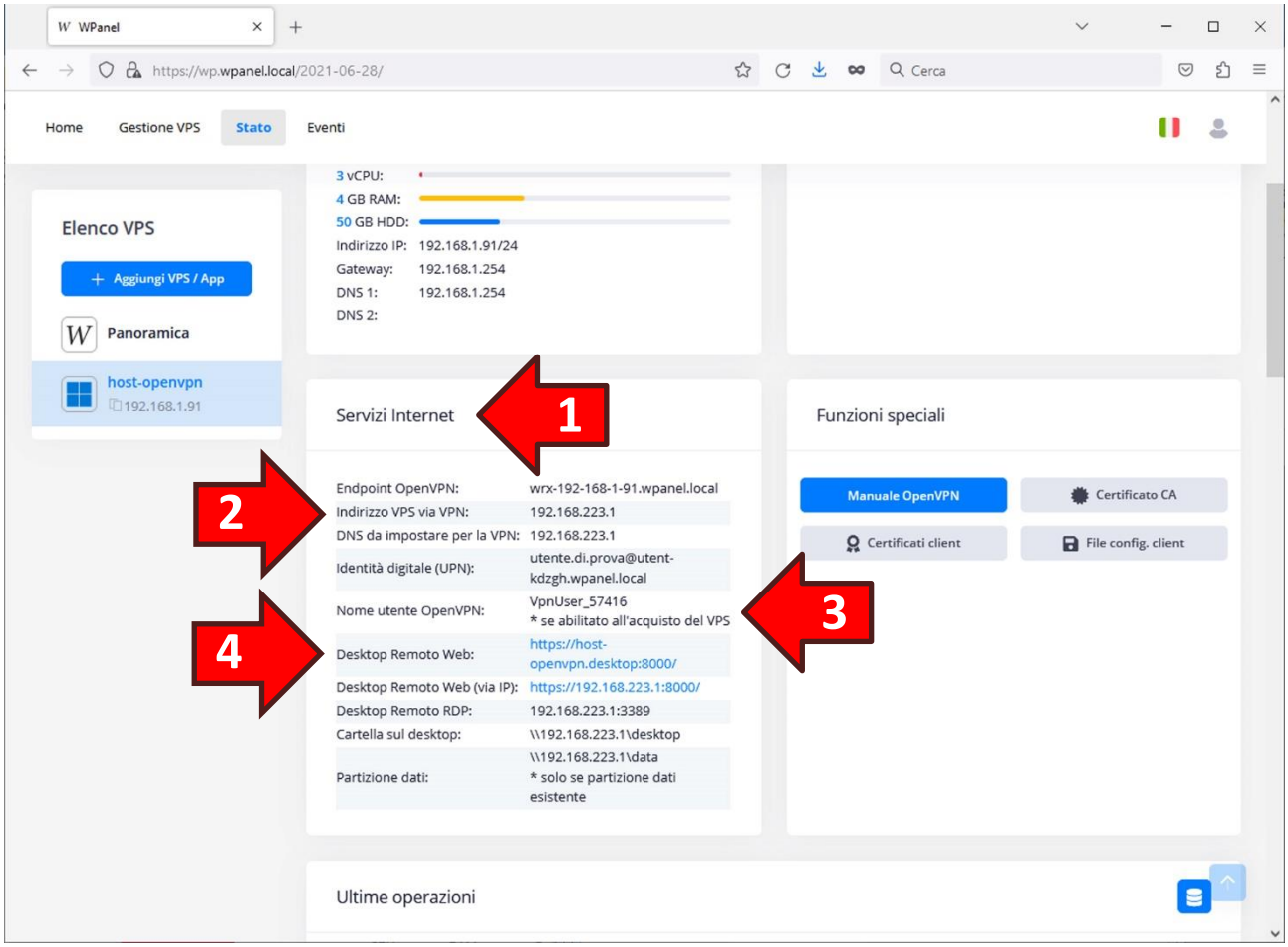
Infine l'email conterrà anche i parametri di configurazione delle condivisioni di rete attivate sul VPS:



3.1 Pannello servizi del VPS

Nel dettaglio del VPS, all'interno del sito WPanel del vostro fornitore, è presente un riquadro denominato **Servizi Internet (1)**. Da notare all'interno del riquadro **l'indirizzo del server VPN (2)**, **l'eventuale nome utente (3)** e l'indirizzo cliccabile per l'accesso al **Desktop Remoto del VPS via web (4)**.

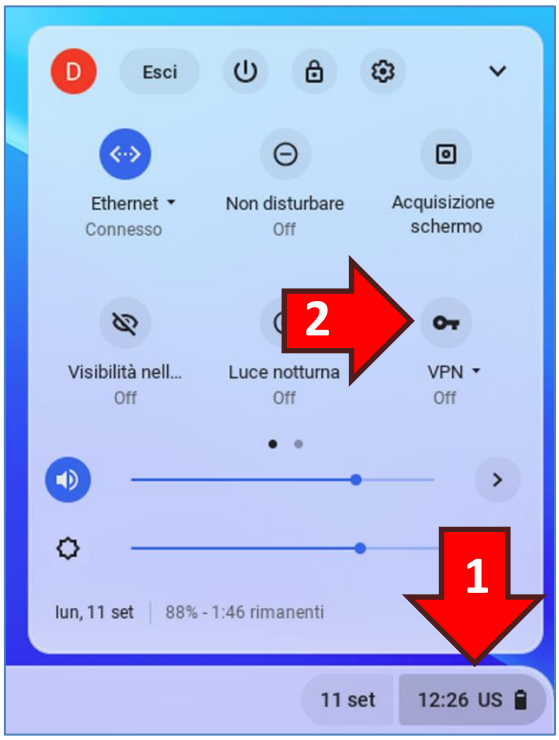
ATTENZIONE! WPanel non conserva le credenziali di sicurezza inserite nel VPS. **L'unico documento contenente dette credenziali è l'email inviata in fase di attivazione.**



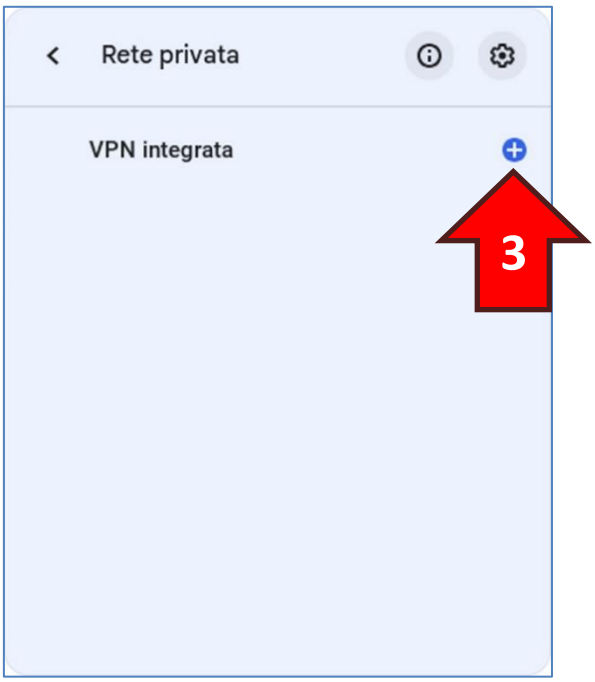
4. Configurazione della connessione VPN

Durante questa procedura recuperare i parametri di configurazione e le credenziali di cui al **capitolo 3. Ricezione delle credenziali e dei parametri di configurazione**.

Nel proprio Chromebook cliccare l'**orologio (1)** in basso a destra dello schermo. Dalla finestra pop-up che si aprirà cliccare sull'**icona della chiave VPN (2)**:

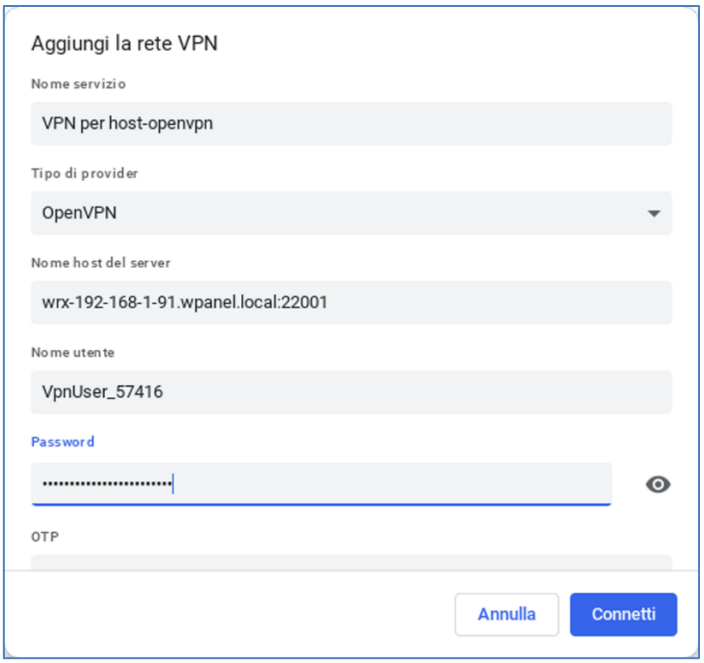


Verrà visualizzata la scheda *Rete privata*. Cliccare quindi il **simbolo + (3)**:

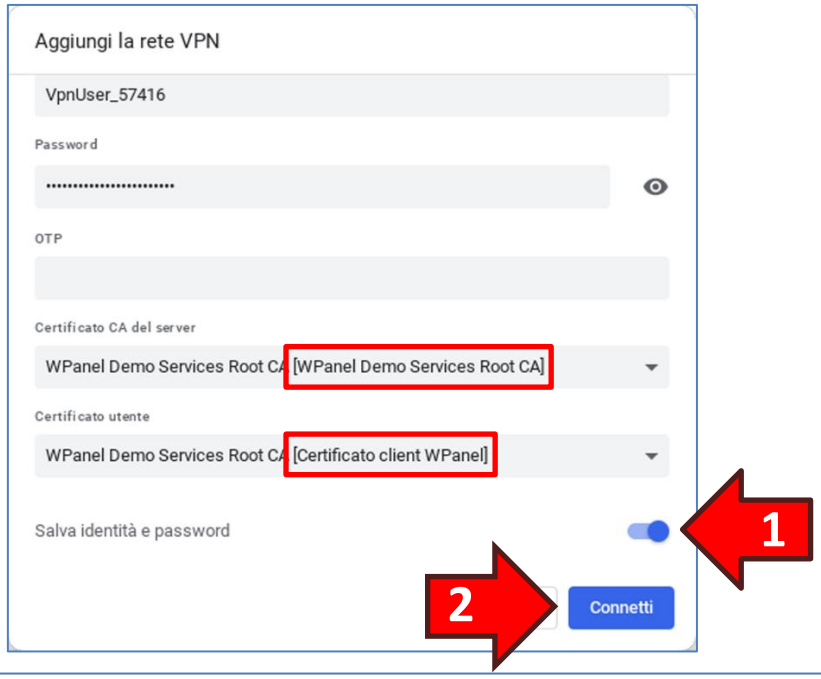


Si aprirà la finestra Aggiungi la rete VPN. Dopo essersi accertati che il **Tipo di provider** sia impostato su **OpenVPN** ricopiare i parametri di configurazione nei rispettivi spazi.

ATTENZIONE! Se in fase di acquisto del VPS non si è impostata la spunta Nome utente/Password inserire dei valori a caso negli spazi riservati a **Nome utente** e **Password**. In ogni caso questi due spazi **non** devono essere lasciati vuoti.



Scorrere la finestra verso il basso per mostrare le altre opzioni. Lo spazio riservato all'OTP deve restare vuoto. In *Certificato CA del server* e *Certificato utente* devono essere impostati rispettivamente l'**Autorità di certificazione del vostro fornitore** e il **Certificato client** generato in fase di acquisto. **ATTENZIONE! Considerare sono i nomi racchiusi tra le parentesi quadre!**



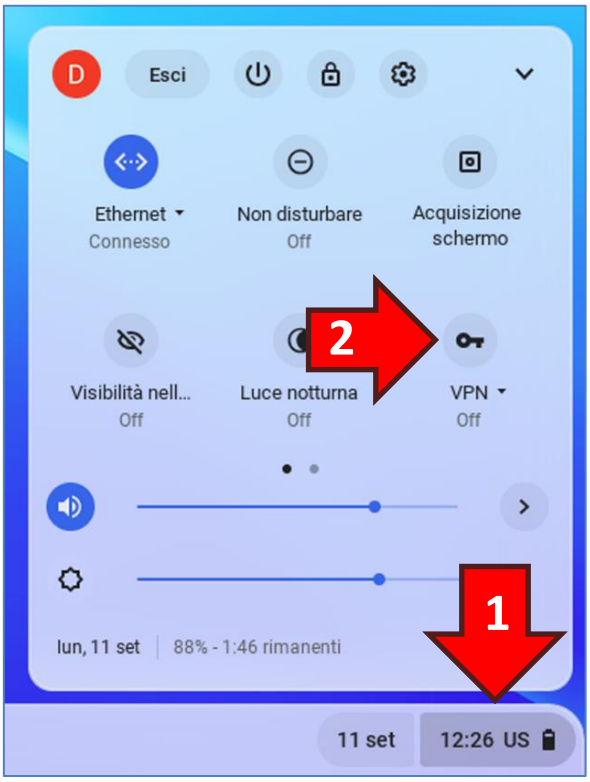
ATTENZIONE! Attivando l'opzione **Salva identità e password (1)** potrebbe creare un problema di sicurezza in caso di furto del Chromebook!

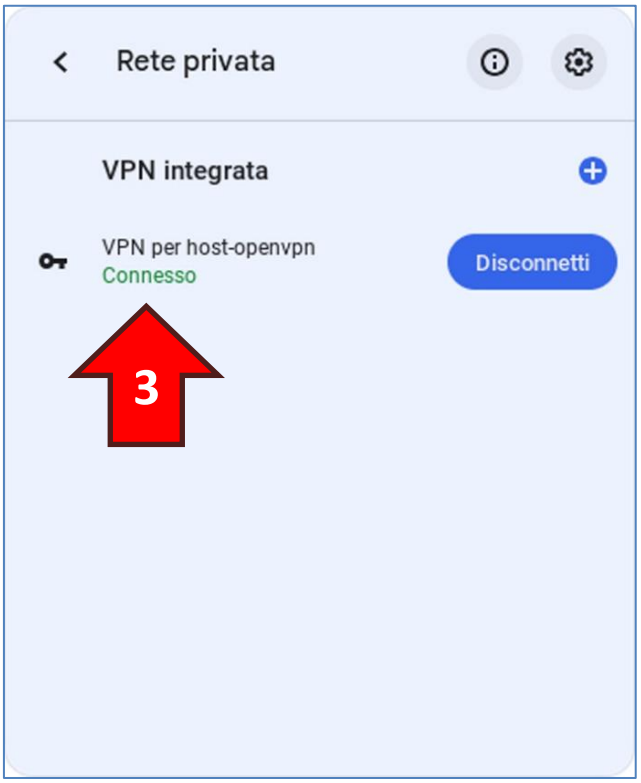
Si ricorda che è possibile modificare la password dell'utente assegnato alla VPN seguendo le indicazioni di cui al **capitolo 9.2 Modifica delle credenziali dell'utente associato alla VPN**.

Si consiglia di attivare l'opzione solo il Chromebook è utilizzato in ambiente domestico.

Cliccare poi il tasto **Connetti (2)** per salvare le impostazioni e aprire il tunnel VPN.

Infine verificare lo stato della connessione VPN cliccando nuovamente sull'**orologio (1)** e poi sull'**icona della chiave VPN (2)** nella finestra pop-up. Nella scheda *Rete privata* deve apparire la dicitura verde **Connesso (3)** sotto la connessione verso il VPS.





Ora sarà possibile accedere al Desktop Remoto del VPS all'indirizzo web formato dal prefisso **https://** seguito dal nome dell'host del VPS e dal suffisso **.desktop:8000/**
(ad esempio **https://host-openvpn.desktop:8000/**).
A tal proposito si rimanda al **capitolo 5. Accesso al desktop remoto via web**.

Si consiglia inoltre di prendere visione del **capitolo 6. Configurazione accesso alle condivisioni di rete** per accedere direttamente ai documenti del VPS dal vostro Chromebook.

4.1 Verifica della connessione VPN su un PC Windows

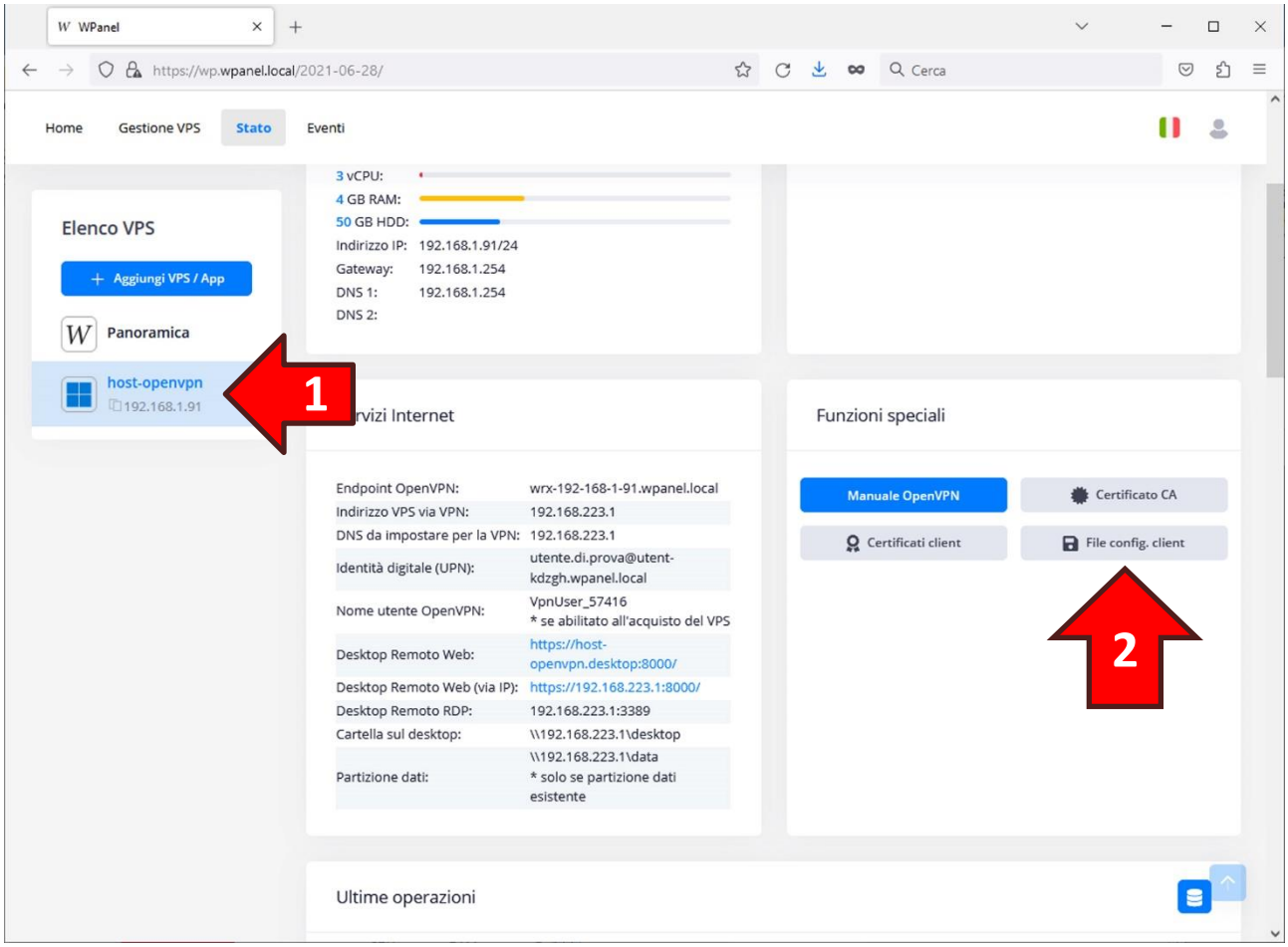
Per effettuare questa verifica è necessario aver scaricato il file della chiave privata e il file del certificato client in formato PEM come indicato al **paragrafo 1.2 Download dei file per verificare il funzionamento della VPN in Windows**.

Prima di avviare la verifica è necessario installare il software client OpenVPN in versione community. Tale software può essere prelevato dalla seguente pagina web:

https://openvpn.net/community-downloads/

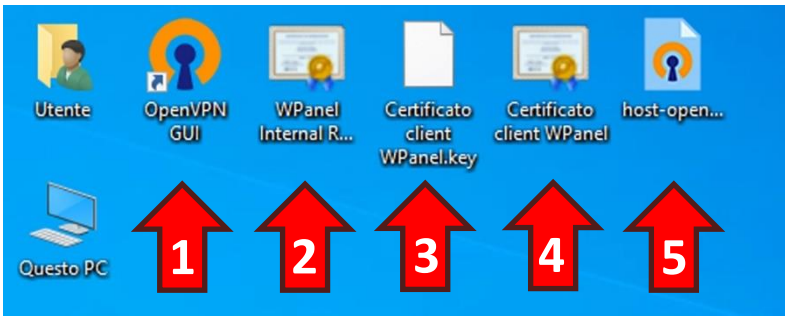
Dalla pagina web scaricare **Windows 64-bit MSI installer** oppure **Windows 32-bit MSI installer** in base alla versione del proprio sistema operativo Windows (nella quasi totalità dei casi i sistemi operativi Windows sono a 64-bit).

Per la verifica è inoltre necessario scaricare il file di configurazione OpenVPN dal sito WPanel del vostro fornitore di VPS. Nello specifico entrare nello **stato del VPS (1)** e nel riquadro delle Funzioni speciali cliccare il tasto **File config. Client (2)**:

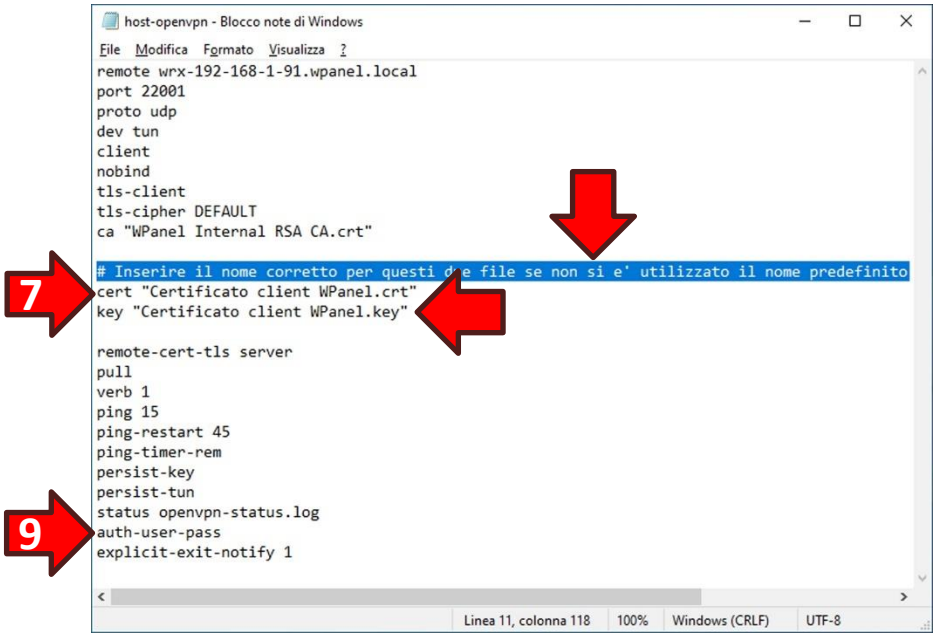


A questo punto si assume che sul proprio desktop siano presenti i seguenti file:

1. L'applicazione GUI di OpenVPN;
2. Il certificato CA del fornitore del VPS;
3. La chiave privata del certificato client in formato PEM;
4. Il certificato client in formato PEM;
5. Il file di configurazione OpenVPN associato al VPS.



Aprire il **Blocco note** e trascinare il **file di configurazione OpenVPN (5)** all'interno della finestra del **Blocco note**:



Come indicato dal **commento (6)** accertarsi che il nome del file indicato nel parametro **cert (7)** corrisponda al nome del file del **Certificato client (4)** e che il nome del file indicato nel parametro **key (8)** corrisponda al nome del file contenente la **chiave privata (3)**. In caso di mancate corrispondenze apportare le dovute modifiche e salvare il file con la funzione del menù **File** -> **Salva**.

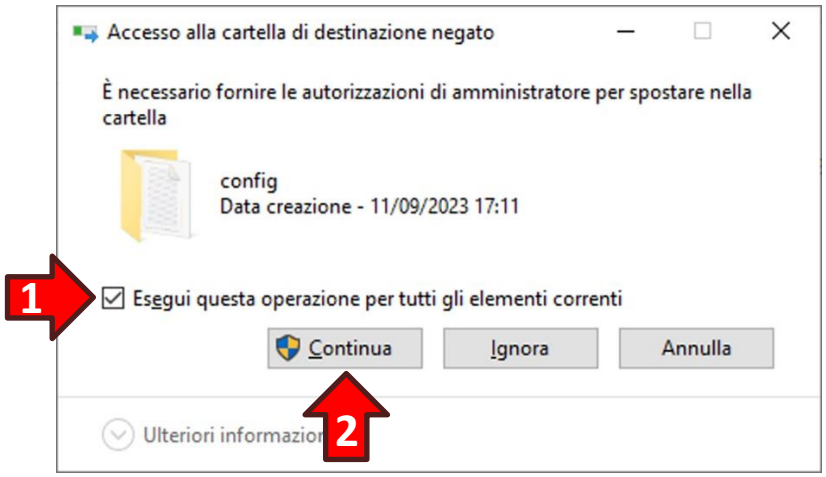
ATTENZIONE! Molto probabilmente il nome del **Certificato client (4)** sul vostro desktop non riporterà l'estensione **.crt** ma nel parametro **cert (8) questa non deve essere omessa!**

ATTENZIONE! Eliminare la riga **auth-user-pass (9)** se in fase di acquisto del VPS si è tolta la spunta sull'opzione **Nome utente/Password**.

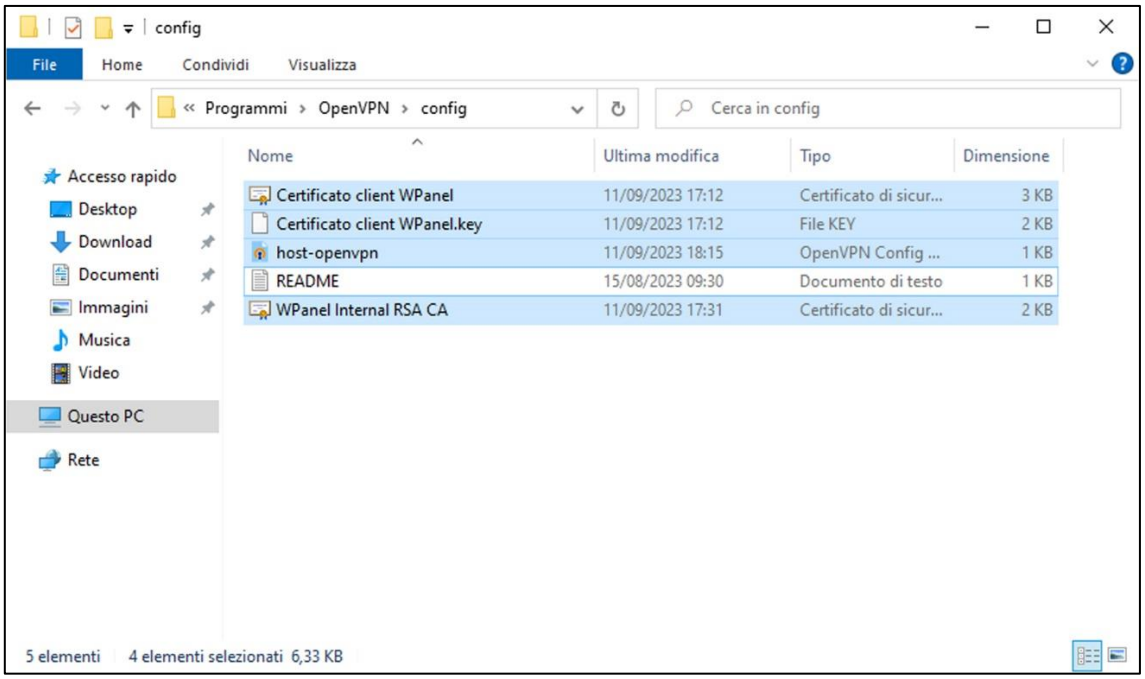
Ora copiare i seguenti file nella cartella **C:\Program Files\OpenVPN\config**:

- Il certificato CA del fornitore del VPS (2);
- La chiave privata del certificato client in formato PEM (3);
- Il certificato client in formato PEM (4);
- Il file di configurazione OpenVPN associato al VPS (5).

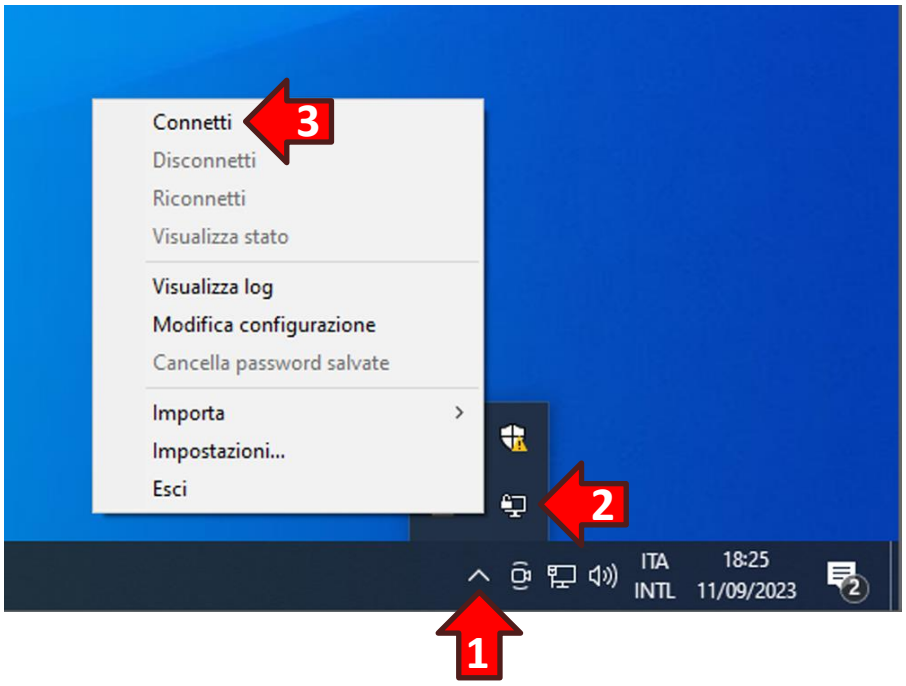
Potrebbe essere necessario fornire le autorizzazioni di amministratore per spostare i file. In tal caso spuntare l'opzione **Esegui questa operazione per tutti gli elementi correnti (1)** e poi cliccare il tasto **Continua (2)**:



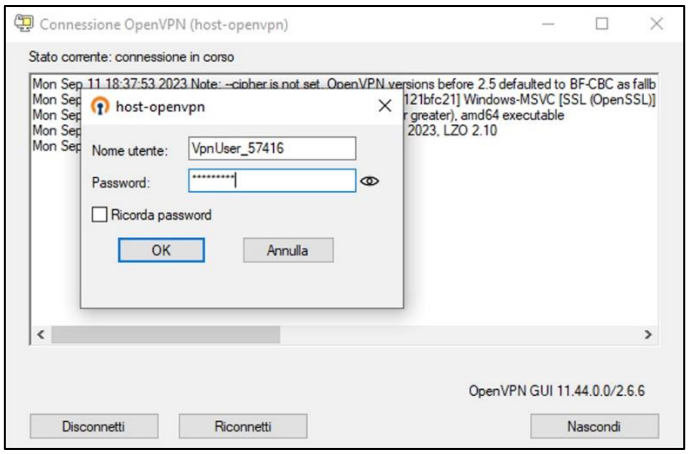
A questo punto il contenuto della cartella **C:\Program Files\OpenVPN\config** dovrebbe essere il seguente:



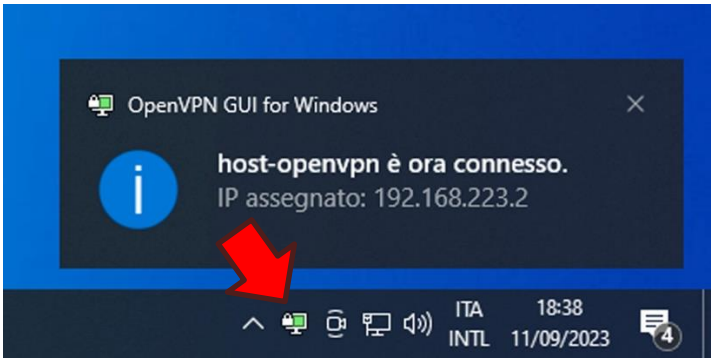
Dall'area di notifica di Windows, in basso a sinistra dello schermo, cliccare la **freccia verso l'alto (1)** per mostrare le icone di notifica nascoste, quindi cliccare con il tasto destro del mouse sull'**icona OpenVPN GUI a forma di schermo (2)**. Poi dal menù pop-up cliccare sull'opzione **Connetti (3)**:



Se richiesto, inserire le credenziali dell'utente OpenVPN e cliccare il tasto OK:



Se il tunnel VPN viene aperto correttamente l'icona di OpenVPN GUI si colora di verde:



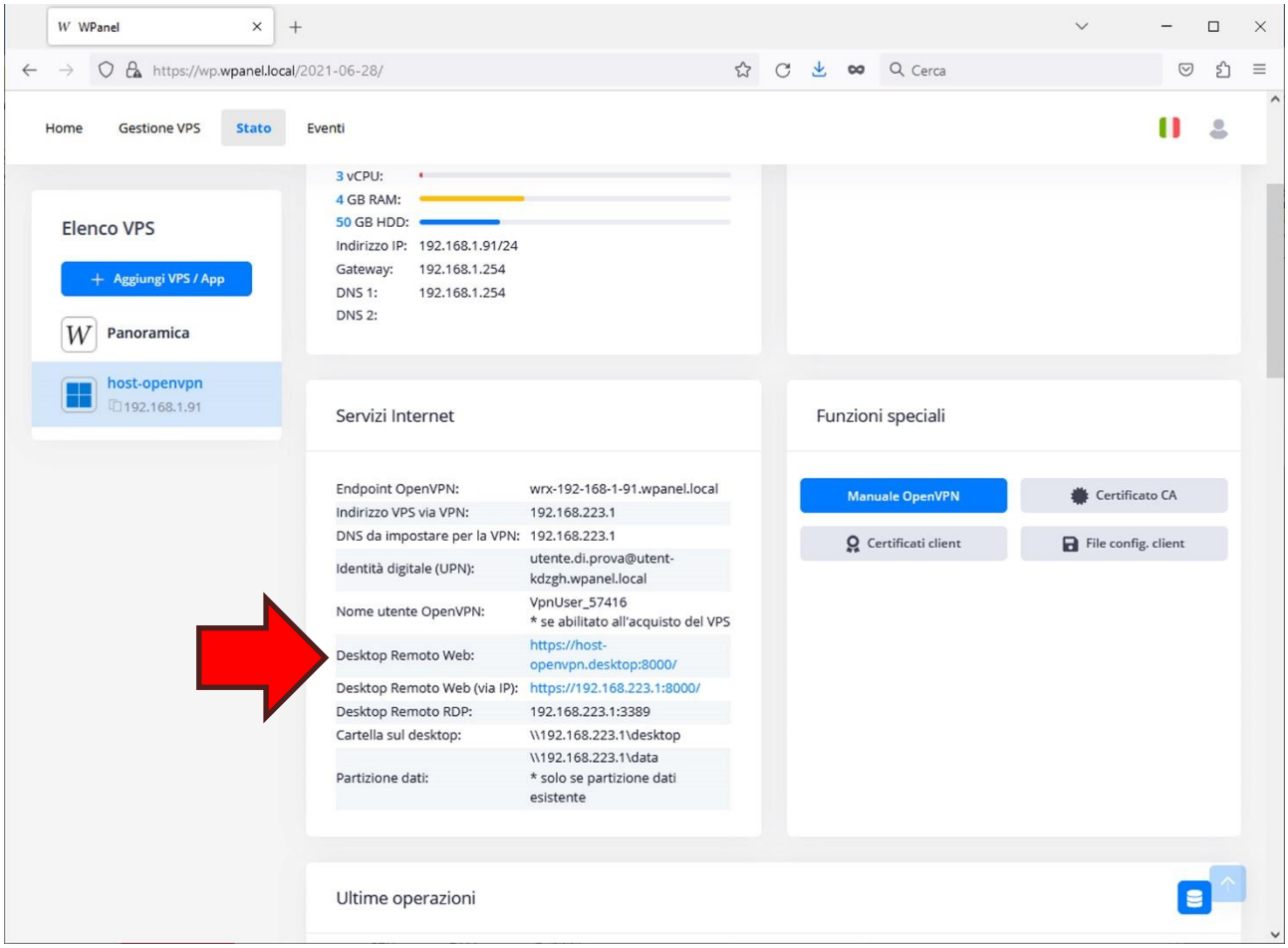
5. Accesso al desktop remoto via web

L'URL per l'accesso al desktop del VPS è formato dal prefisso **https://** seguito dal nome dell'host del VPS e dal suffisso **.desktop:8000/**

L'URL esatto è riportato sia nell'email contenente le credenziali del VPS:

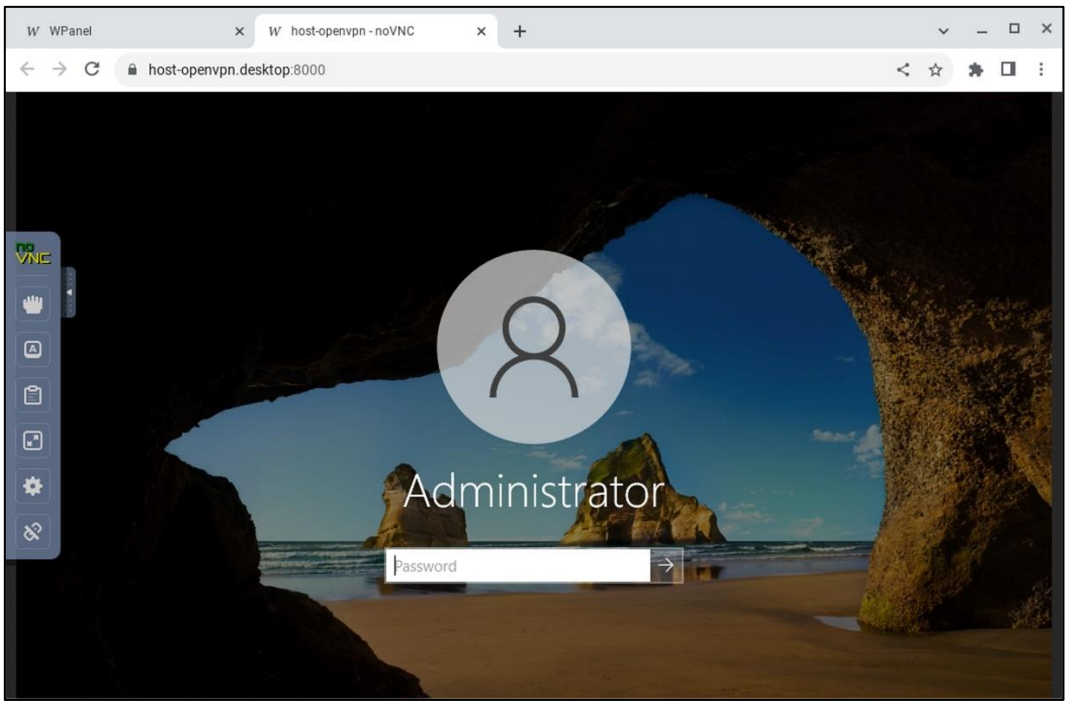
> Se il suo computer non dispone di tale software oppure sta utilizzando un **Chromebook** potrà accedere al desktop del VPS via web utilizzando il seguente URL:
>
> - **https://host-openvpn.desktop:8000/**

che nel riquadro Servizi Internet del dettaglio VPS all'interno del sito WPanel del vostro fornitore:



È possibile accedere al desktop remoto anche digitando l'indirizzo IP del VPS alla fine del tunnel VPN seguito dalla porta 8000 ma in tal caso sarà necessario confermare nel browser l'eccezione sulla validità del certificato.

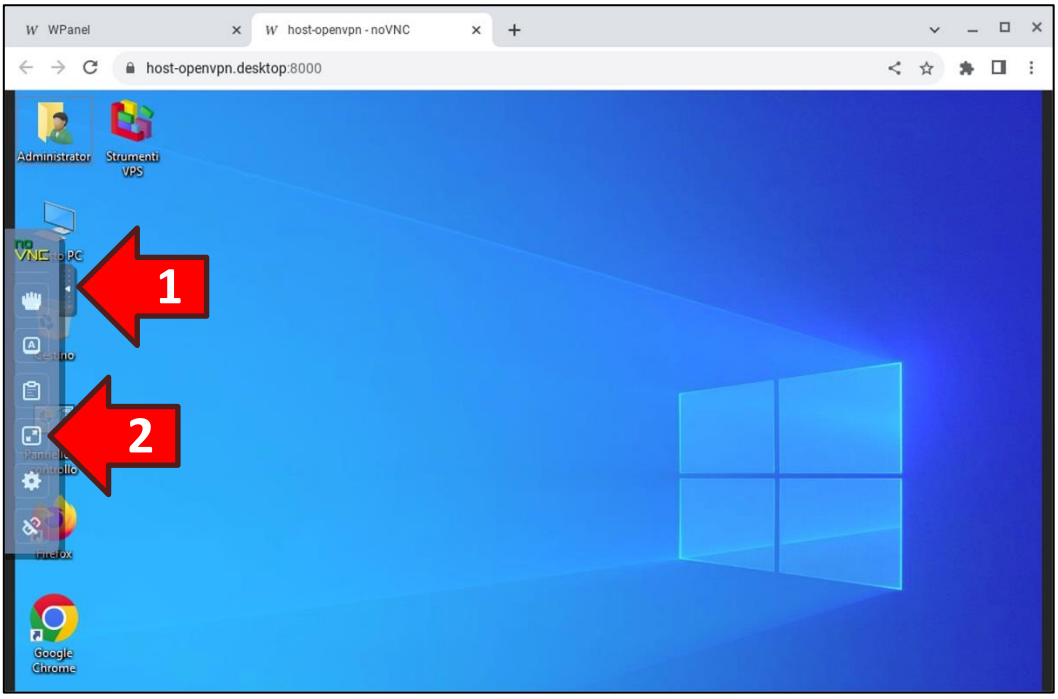
Aprendo l'URL verrà visualizzato direttamente lo schermo del VPS con la richiesta della password dell'utente Administrator:



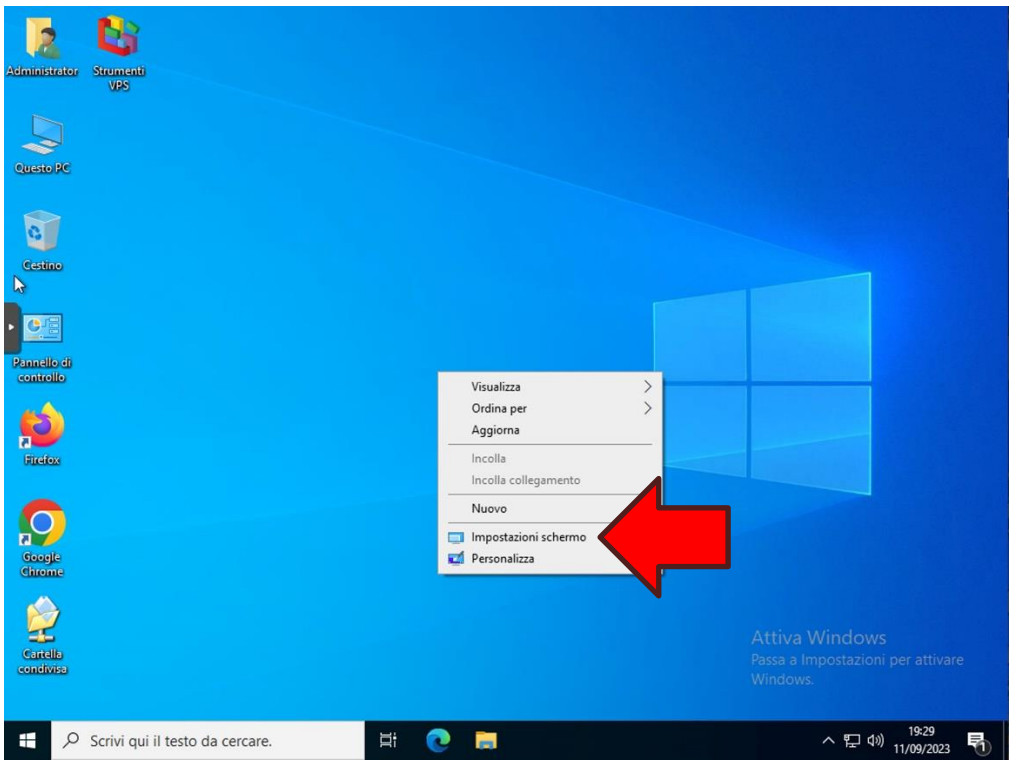
ATTENZIONE! Per ragioni di sicurezza la password dell'utente Administrator verrà richiesta ad ogni accesso. È comunque possibile rimuovere questo vincolo rivolgendosi al supporto.

5.1 Visualizzazione a tutto schermo

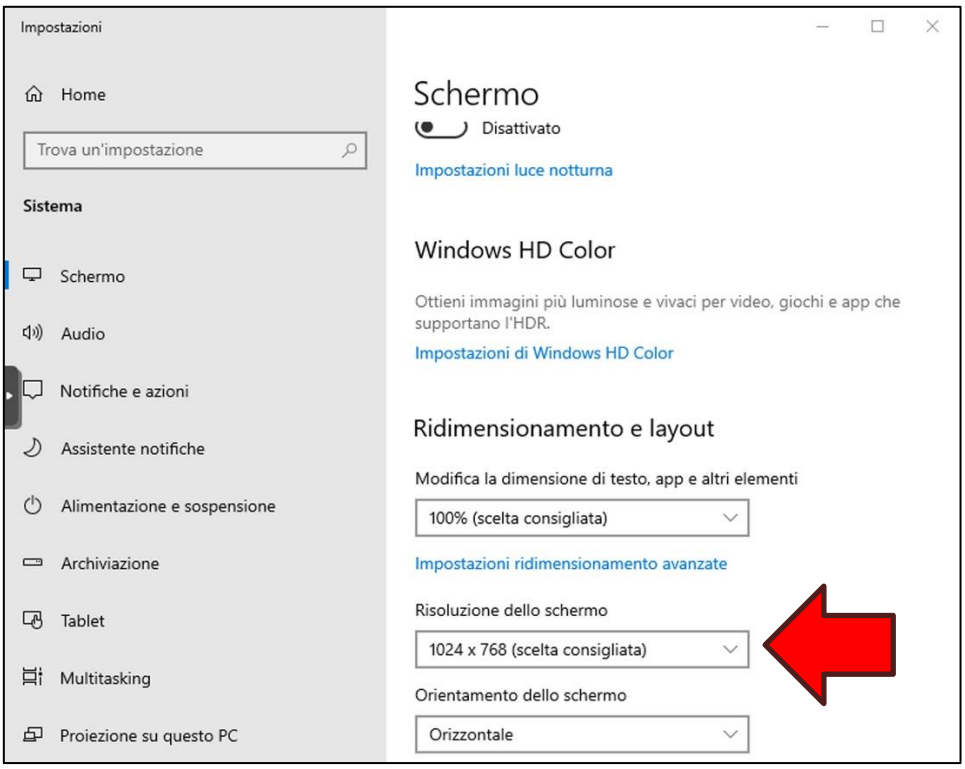
Una volta effettuato il login cliccare sulla **linguetta (1)** nell'estremità sinistra della finestra del browser per mostrare i controlli del software web NoVNC. Quindi cliccare sull'**icona del quadrato con due frecce diagonali opposte (2)** per mostrare il desktop del VPS a tutto schermo:



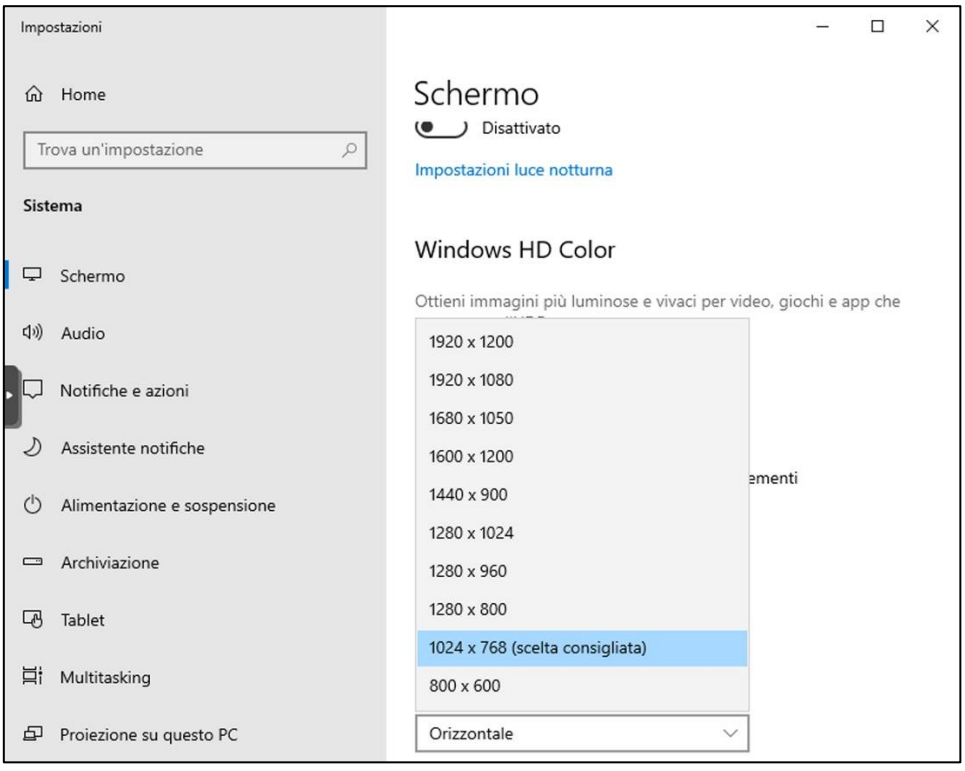
Ora impostare la risoluzione dello schermo del VPS cliccando il tasto destro del mouse in una posizione vuota del desktop e selezionando dal menù pop-up l'opzione Impostazioni schermo:



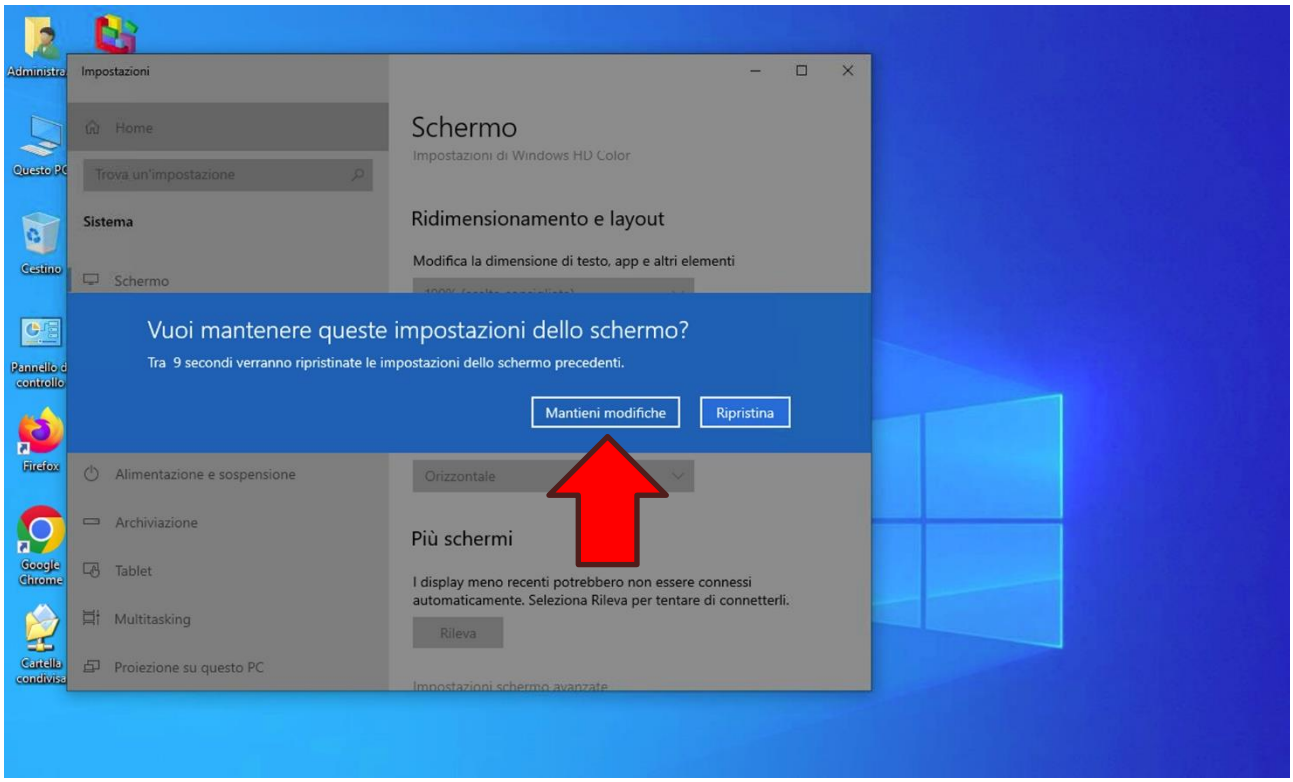
Se necessario scorrere verso il basso la sezione di destra delle impostazioni fino a visualizzare l'opzione Risoluzione dello schermo. Quindi cliccare sul riquadro a tendina per visualizzare tutte le combinazioni di risoluzione disponibili:



A questo punto selezionare la risoluzione dello schermo del Chromebook. Nella maggior parte dei casi dovrebbe corrispondere a 1920 x 1080:



Se la dimensione desktop del VPS corrisponde alla dimensione dello schermo del Chromebook confermare la risoluzione selezionata cliccando il tasto **Mantieni modifiche**:

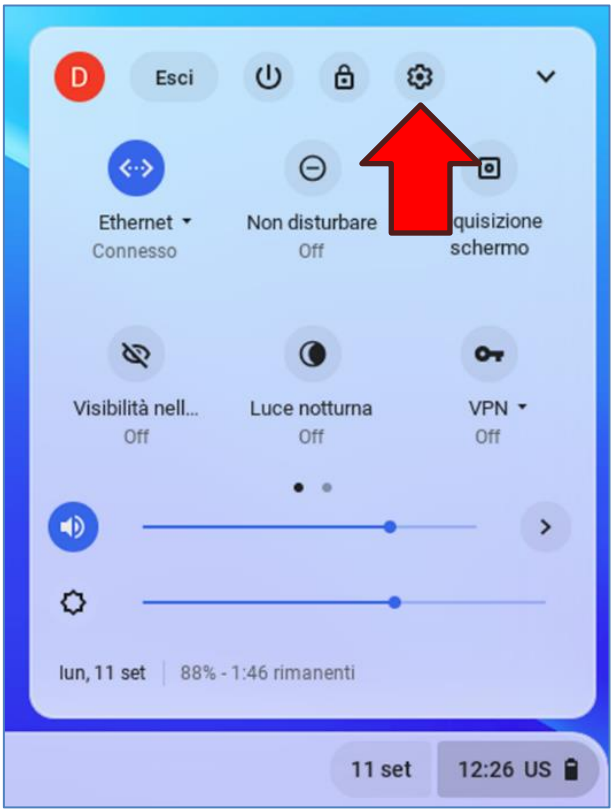


5.2 Tasti funzione F1-F12 sulla tastiera del Chromebook

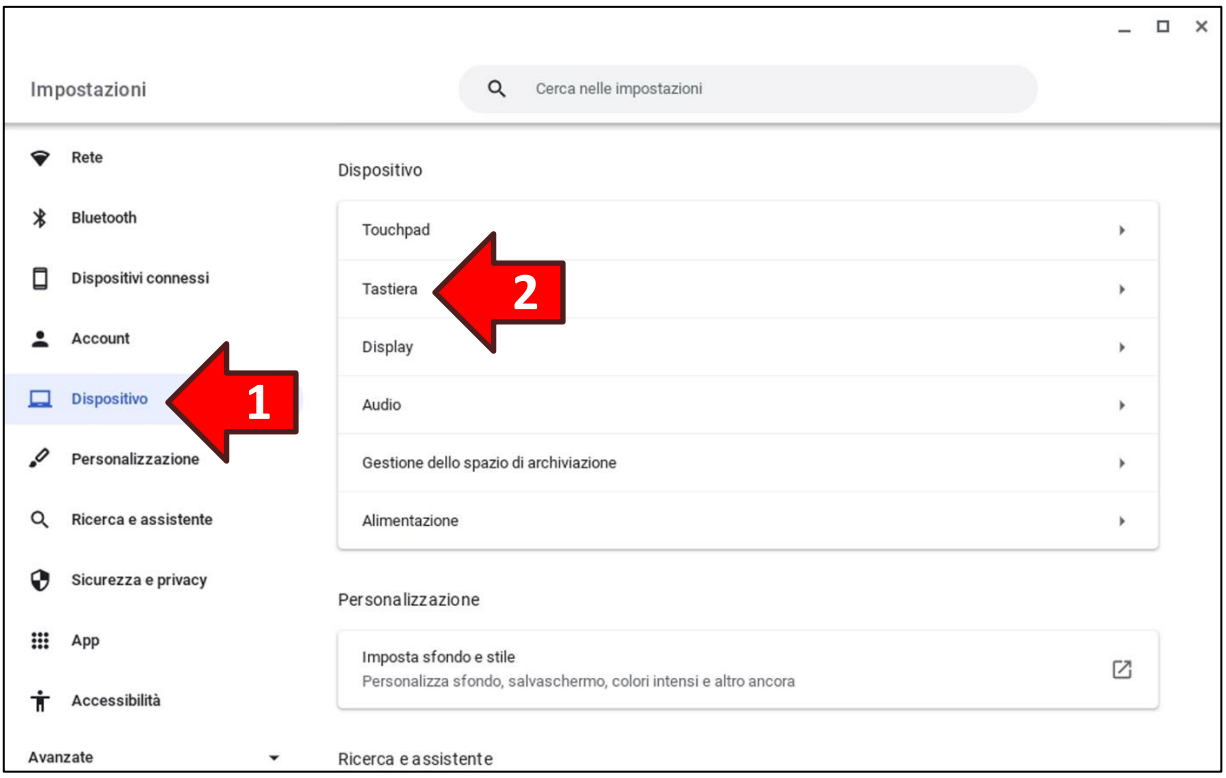
La tastiera del Chromebook non dispone dei tasti funzione F1-F12. Qualora si avesse questa esigenza è possibile simulare tali tasti sulla prima fila della tastiera.

ATTENZIONE! In ogni caso il browser Chrome non è in grado di inoltrare al Desktop Remoto del VPS via web la pressione del tasto **ESC** e la pressione del tasto **F11**. Se gli applicativi che si utilizzano sul VPS richiedono l'uso di questi tasti specifici fare riferimento al **paragrafo seguente 5.3 Connessione al desktop remoto trame app nativa**.

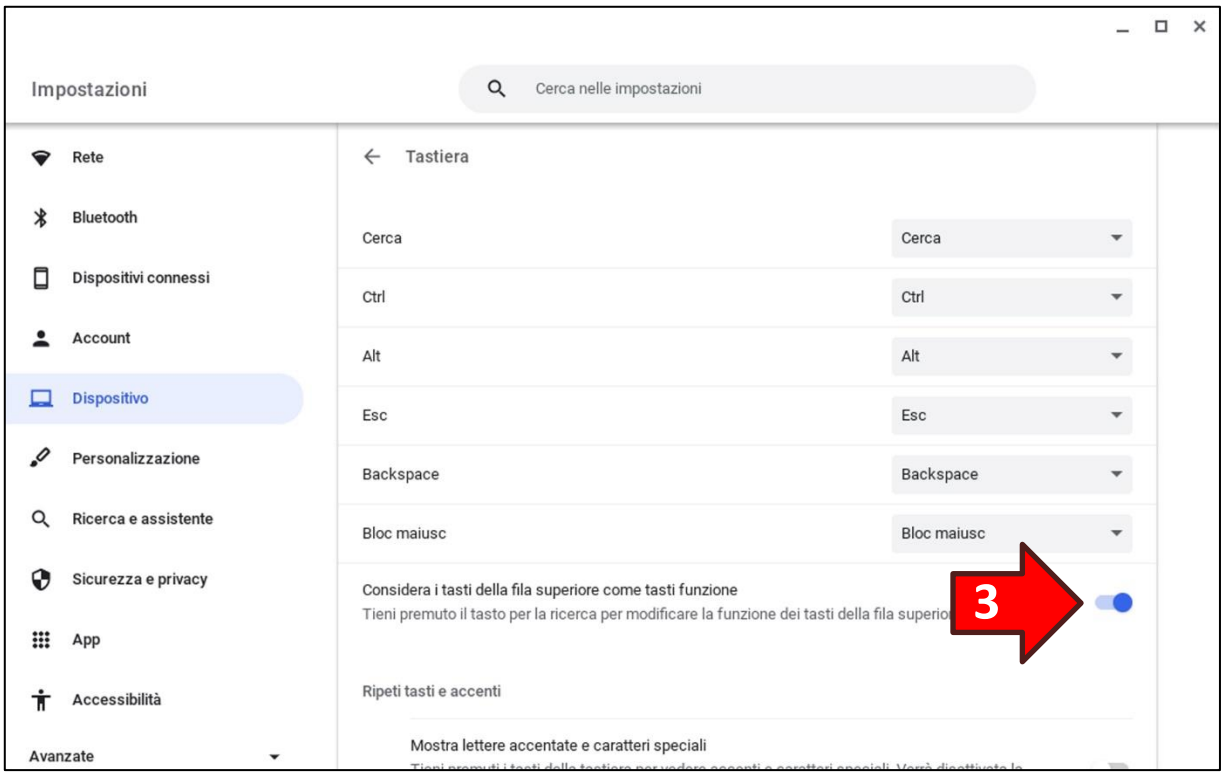
Nel proprio Chromebook cliccare l'**orologio (1)** in basso a destra dello schermo. Dalla finestra pop-up che si aprirà cliccare sull'**icona dell'ingranaggio (2)** per la modifica delle impostazioni:



Nella finestra che si aprirà selezionare prima l'opzione **Dispositivo (1)** dalla sezione di sinistra e poi l'opzione **Tastiera (2)** dalla sezione di destra:



Ora abilitare l'opzione **Considera i tasti della fila superiore come tasti funzione (3)** e chiudere la finestra Impostazioni:



5.3 Connessione al desktop remoto trame app nativa

Come si evince dai precedenti paragrafi, l'esperienza utente del desktop del VPS via browser web presenta alcune limitazioni.

In ogni caso sul tunnel VPN è disponibile anche la connessione nativa Desktop Remoto tramite protocollo RDP sulla porta TCP predefinita 3389.

Per sfruttare la connessione nativa del Desktop Remoto è necessario installare sul proprio Chromebook un'applicazione che funga da client RDP nativo.

Se il proprio Chromebook è basato su architettura ARM è possibile installare l'app **Remote Desktop** della Microsoft Corporation tramite il **Play Store**.

Se il proprio Chromebook è basato su architettura x86 è possibile acquistare, ad esempio, l'app **Xtralogic Remote Desktop Client for Chrome** tramite il **Web Store**.

Il nome del computer da specificare in tali applicazioni deve essere formato dal nome dell'host del VPS seguito dal suffisso **.desktop** come ad esempio **host-ovpn.desktop**.

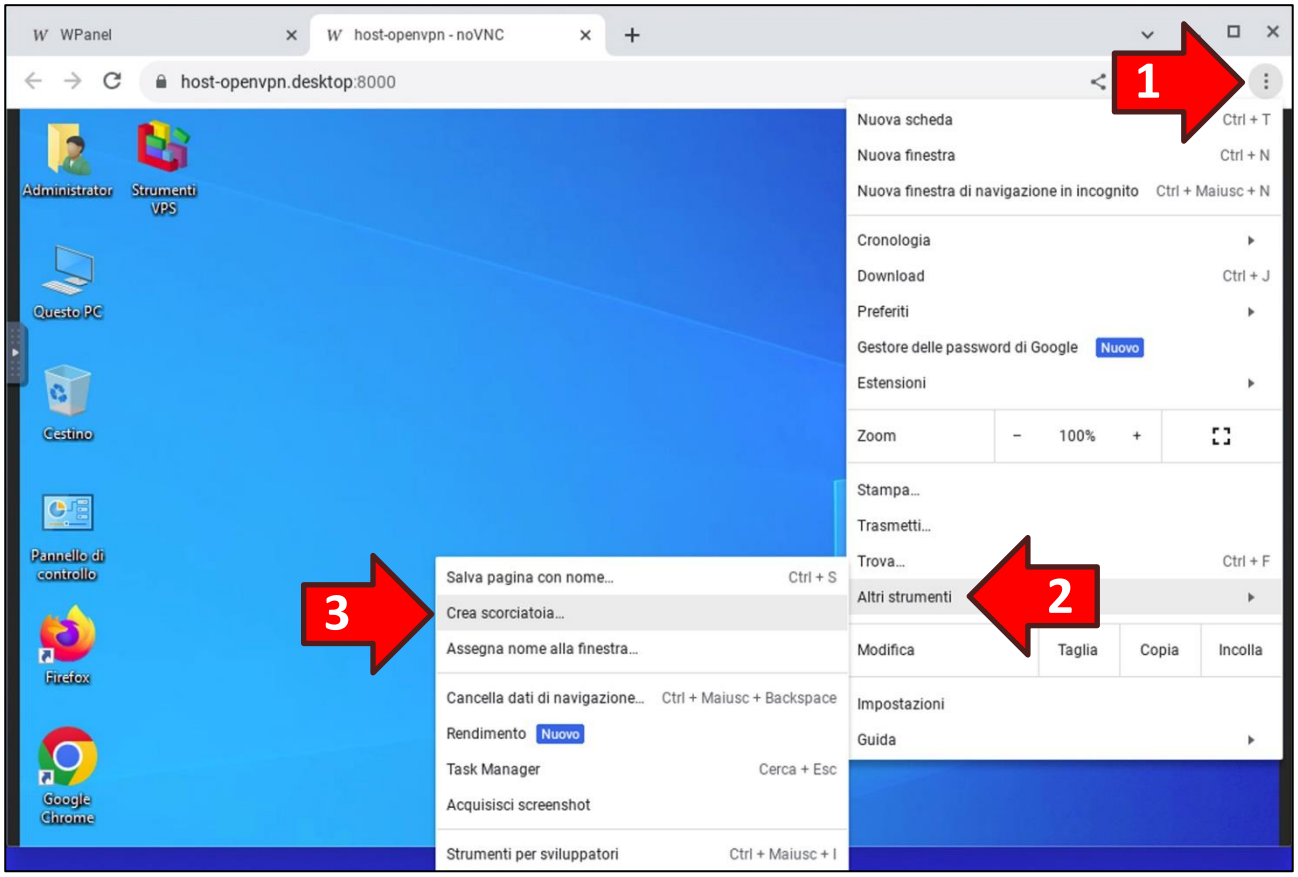
5.4 Inserimento dell'icona del desktop remoto sulla barra delle applicazioni

ChomeOS consente di inserire sulla barra delle applicazioni un'icona per l'apertura veloce di un indirizzo web. Ciò potrebbe rivelarsi particolarmente utile per aprire l'indirizzo web del desktop del VPS una volta aperto il tunnel VPN.

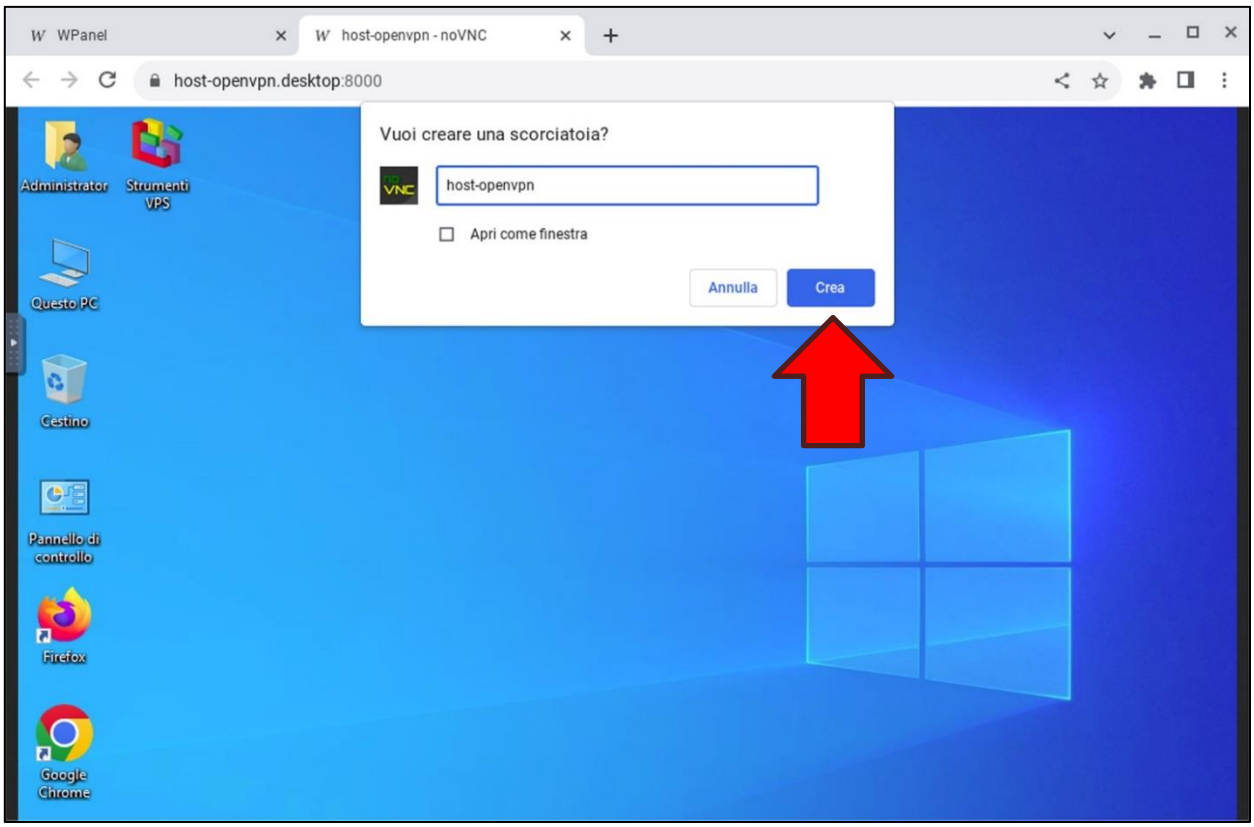
Per effettuare questa operazione aprire la pagina web del desktop del VPS utilizzando l'indirizzo ricevuto tramite email:

> Se il suo computer non dispone di tale software oppure sta utilizzando un **Chromebook** potrà accedere al desktop del VPS via web utilizzando il seguente URL:
>
> - **https://host-openvpn.desktop:8000/**

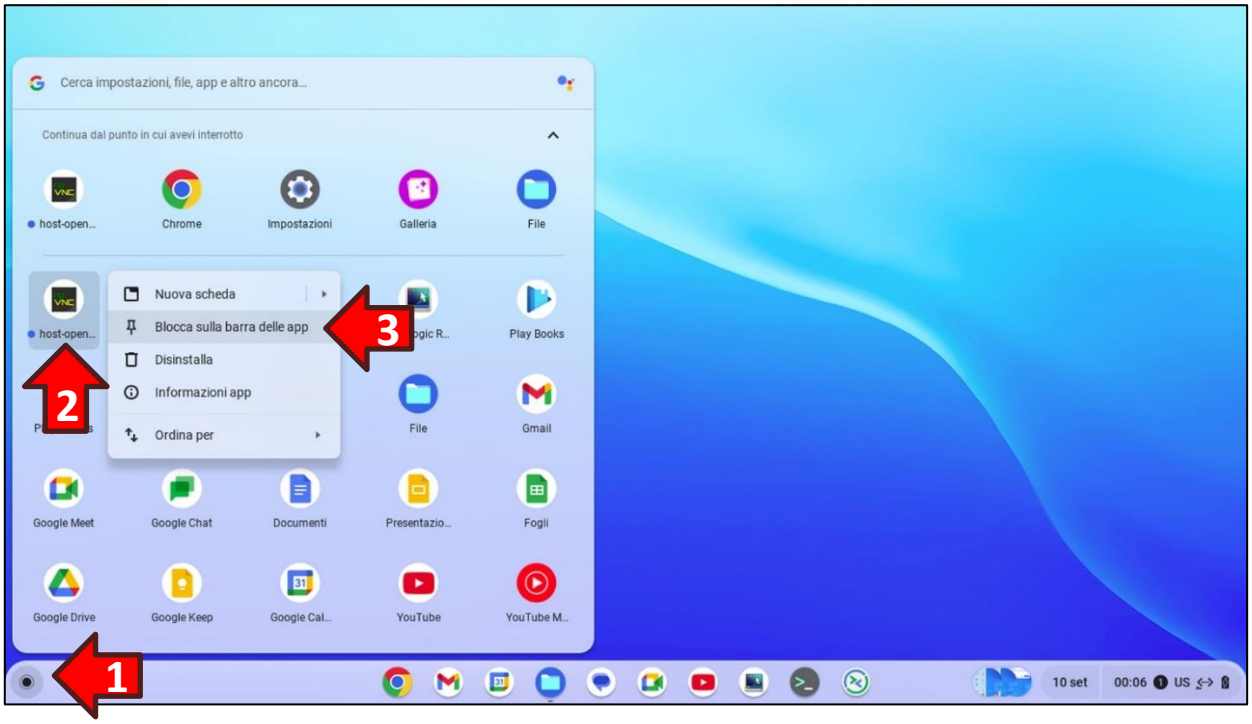
Quindi cliccare sui **tre puntini (1)** in alto a destra della finestra di Chrome per visualizzare il menù pop-up per poi cliccare prima sull'opzione **Altri strumenti (2)** e successivamente sull'opzione **Crea scorciatoia (3)**:



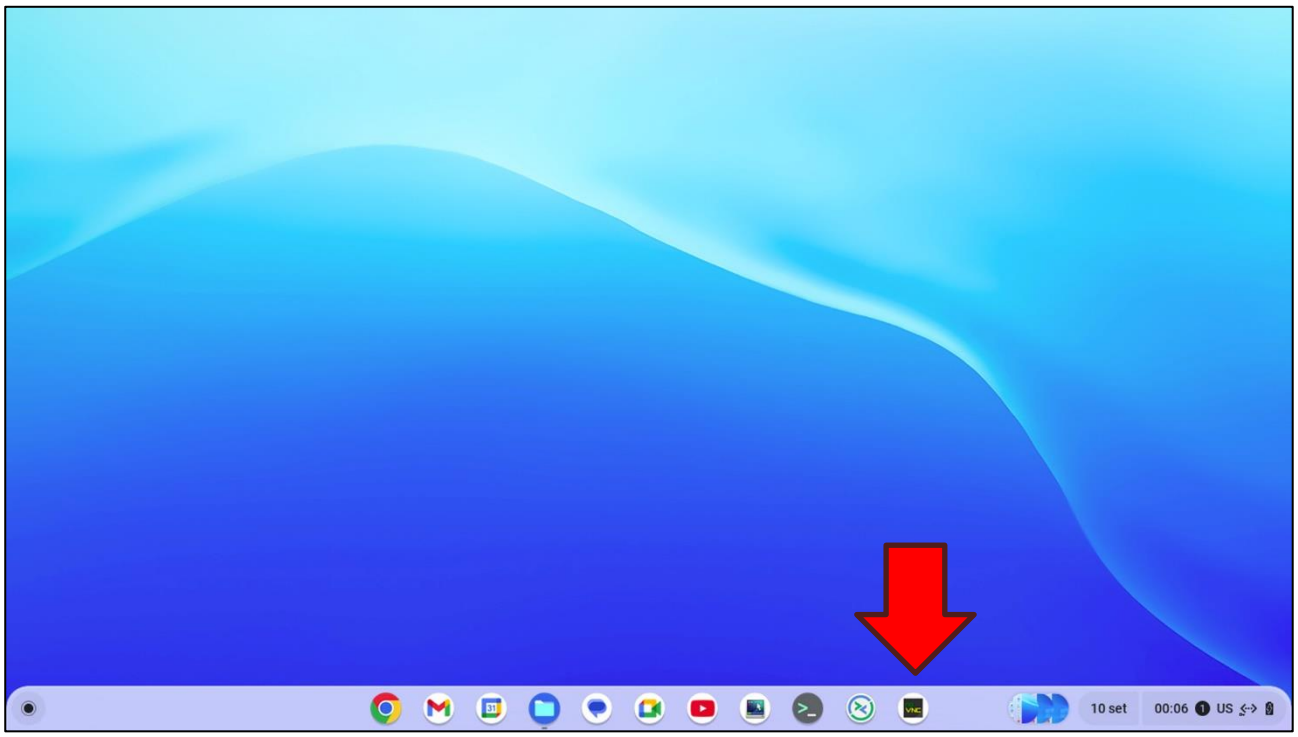
Verificare che il nome della scorciatoia corrisponda con il nome host del VPS e poi cliccare il tasto **Crea**.



Ora cliccare il tasto di avvio delle app (1) in basso a sinistra e cercare l'icona con il nome host del VPS (2). Cliccare sopra l'icona con il tasto destro del mouse e dal menù pop-up selezionare l'opzione Blocca sulla barra delle app (3):



Ora, cliccando sull'icona appena aggiunta sulla barra delle app, sarà possibile aprire direttamente la pagina web del desktop del VPS senza dover digitare l'indirizzo ogni volta che si intende effettuare l'accesso:



6. Configurazione accesso alle condivisioni di rete

Dal vostro Chromebook è possibile accedere alle condivisioni di rete del vostro VPS come se fossero cartelle create all'interno del Chromebook.

ATTENZIONE! La condivisione delle cartelle è attivata solo sul tunnel VPN quindi non sussistono rischi di intrusione da Internet!

L'utilizzo delle condivisioni di rete rende maggiormente agevole il tipico lavoro d'ufficio poiché ChomeOS ha già preinstallata una suite di app per la creazione e la modifica dei tipici documenti di Microsoft Office.

L'utilizzo di queste app evita l'accesso al desktop del VPS.

La **Cartella condivisa** presente sul desktop del VPS è condivisa in rete con il nome **desktop**.

Se al momento dell'acquisto del VPS si è scelto di creare la **partizione dati** questa è condivisa in rete con il nome **data**. La condivisione resta attiva anche se la partizione dati è stata cifrata con BitLocker. Ovviamente per accedervi è necessario che la partizione risulti sbloccata. A tal proposito si rimanda al prossimo **capitolo 7. Cifratura della partizione dati con BitLocker**.

Prima di iniziare la procedura si consiglia di recuperare le credenziali delle condivisioni di rete dall'email inviata dopo la creazione del VPS:

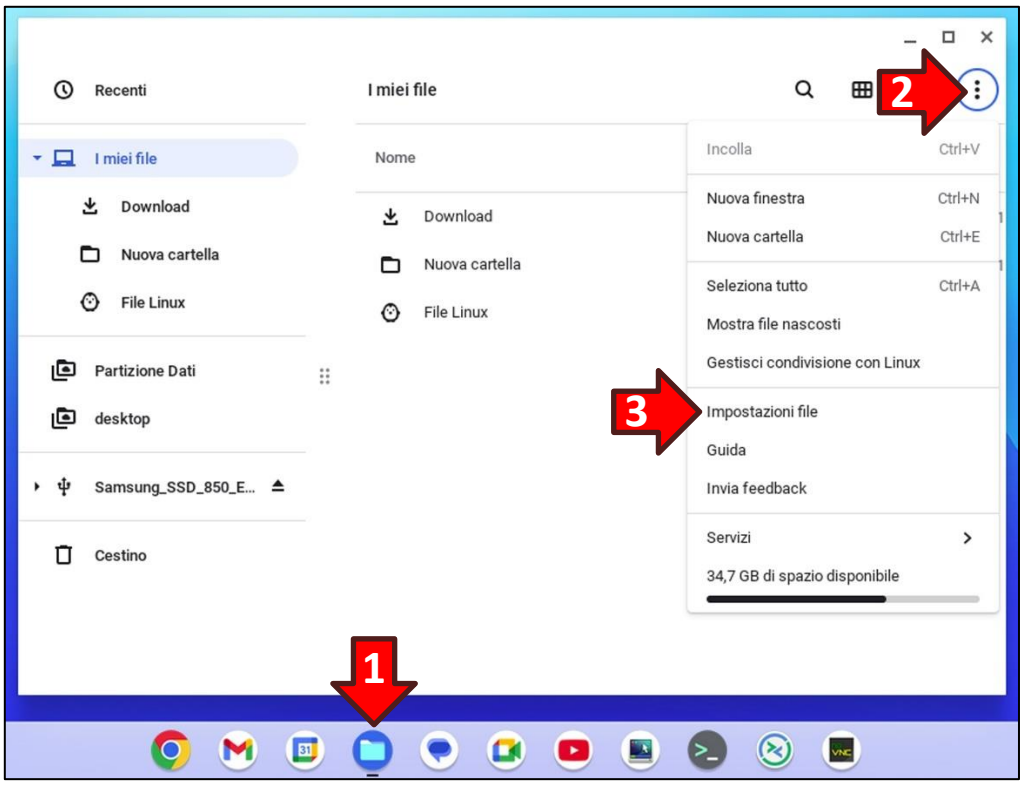
Sul suo VPS sono state create le seguenti condivisioni di rete (SMB):

- Cartella condivisa sul desktop: **\\192.168.223.1\desktop**
- Partizione Dati: **\\192.168.223.1\data**

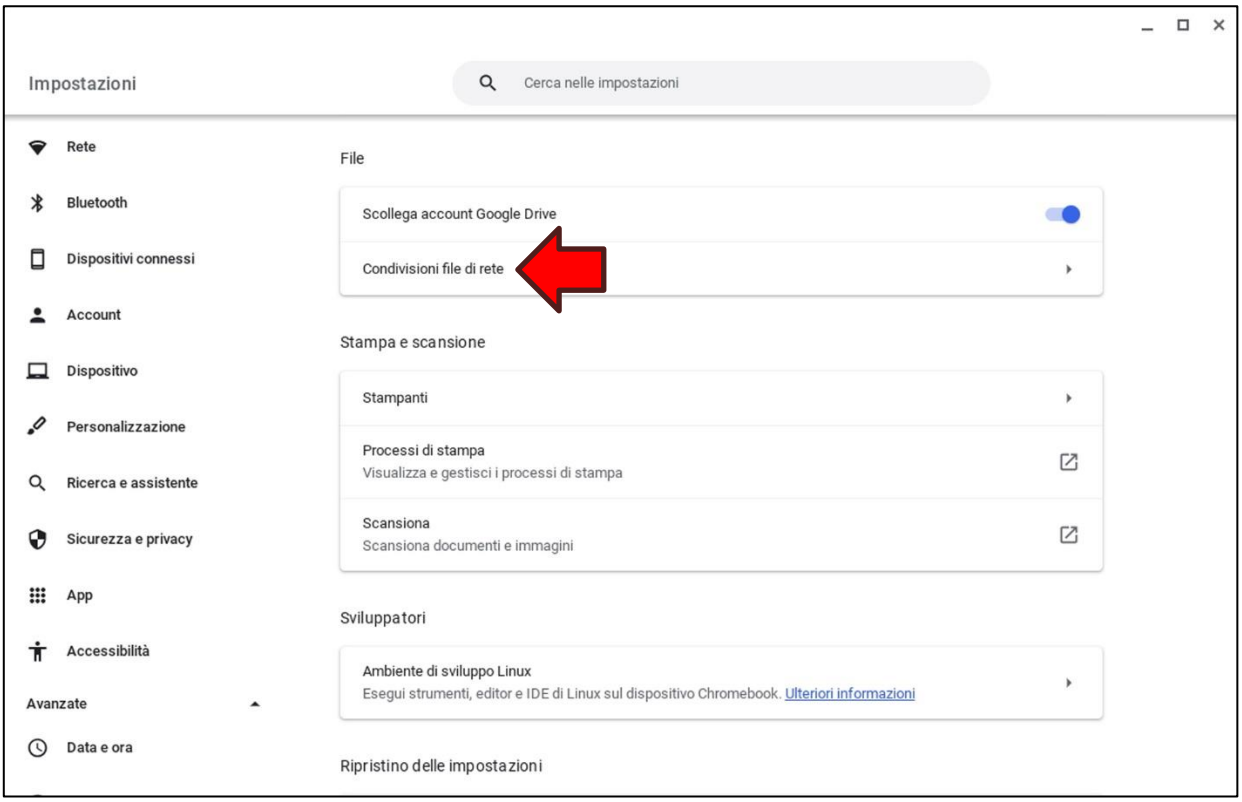
Tali condivisioni sono accessibili con le seguenti credenziali:

- Nome utente: **Administrator**
- Password: **tBHG5al+1twxMs]S**

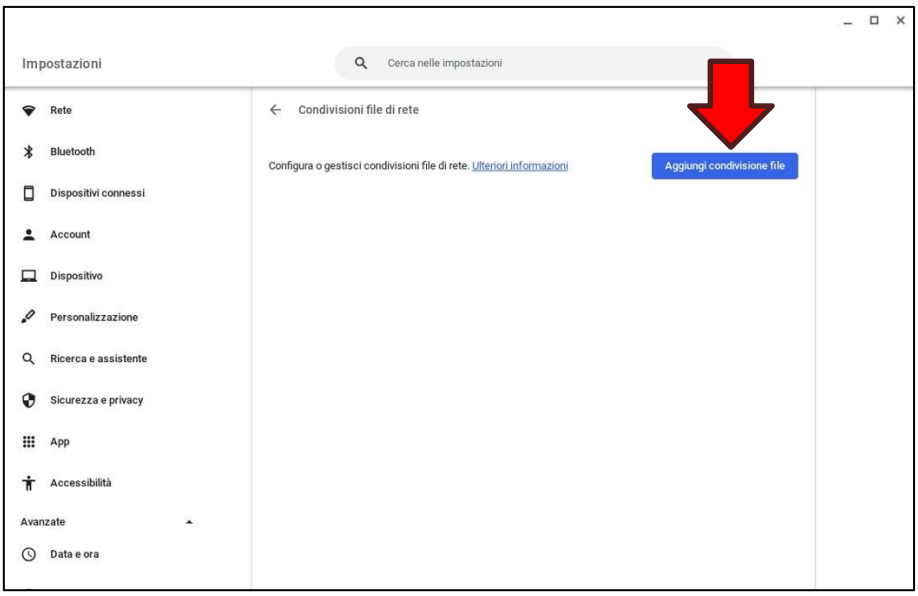
Per accedere alle condivisioni di rete del VPS prima accertarsi che la connessione VPN sia attiva poi sulla barra delle app cliccare prima l'**icona a forma di cartella (1)**, poi sui **tre puntini (2)** in alto a destra della finestra *I miei file* ed infine sull'opzione **Impostazioni file (3)** del menù:



Nella sezione di destra della finestra *Impostazioni* cliccare sull'opzione **Condivisioni file di rete**:



Poi nella scheda *Condivisioni file di rete* cliccare il tasto **Aggiungi condivisione file**:



Si aprirà la finestra *Aggiungi condivisione file*.

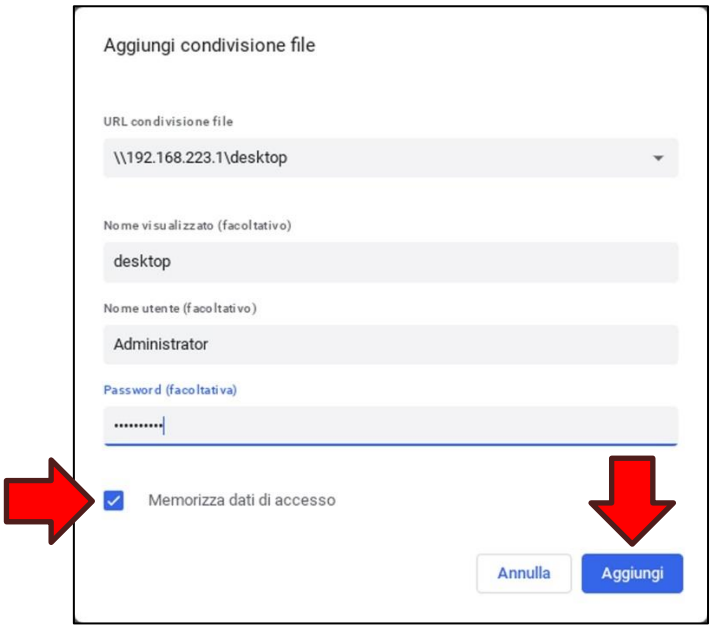
In **URL condivisione file** digitare l'indirizzo della cartella condivisa sul desktop (es. **\\192.168.223.1\desktop**).

In nome visualizzato digitare **desktop**.

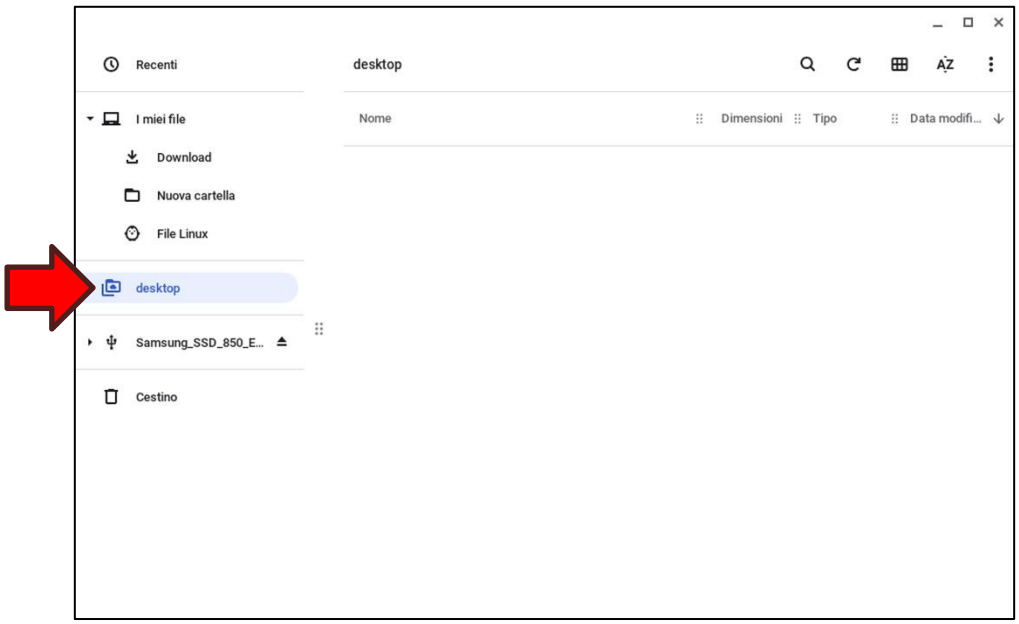
In **Nome utente** e **Password** specificare le credenziali indicate nell'email.

Infine, onde evitare l'inserimento della password ad ogni avvio del Chromebook, verificare che la spunta sull'opzione **Memorizza dati di accesso** sia impostata.

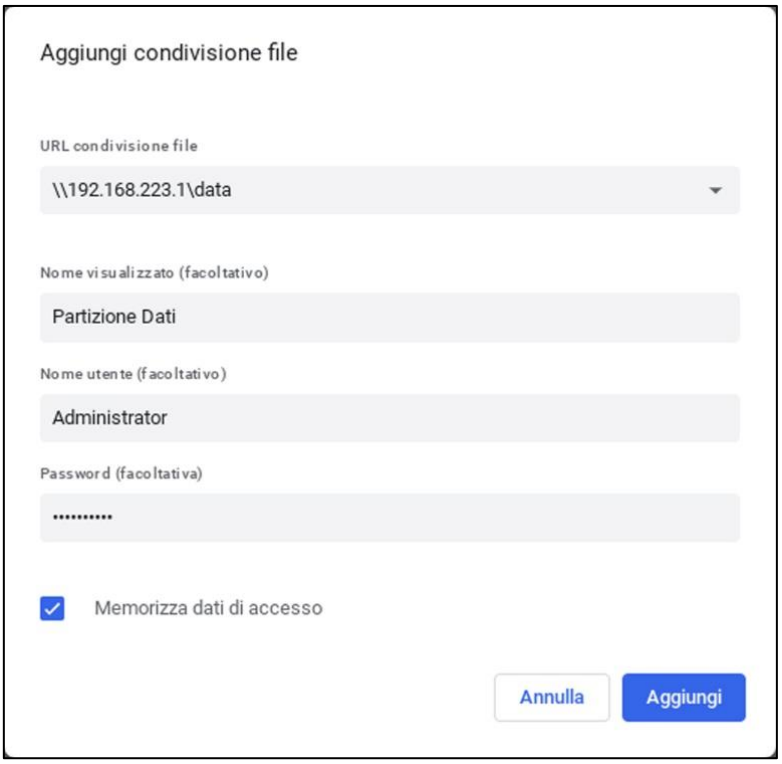
Infine cliccare il tasto **Aggiungi**:



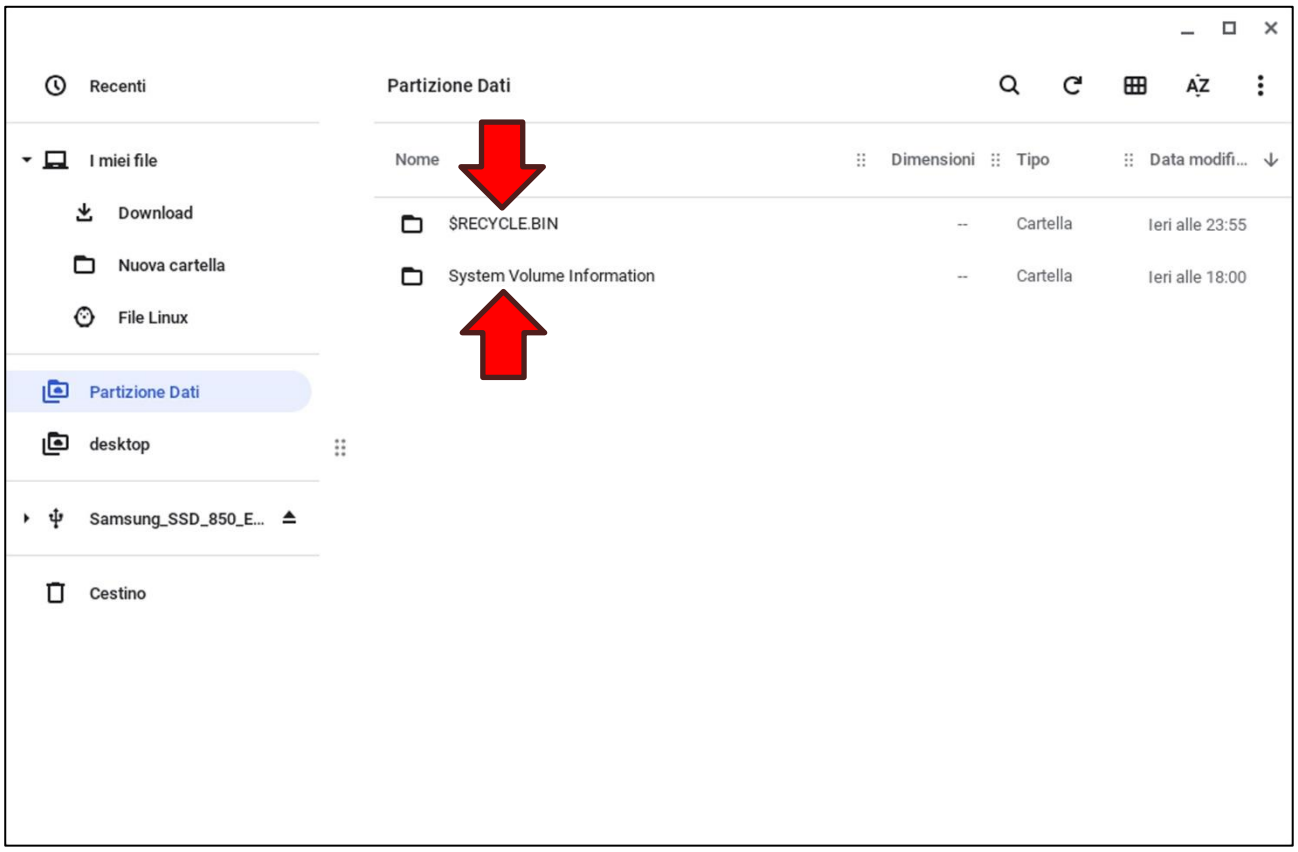
Se l'operazione è andata a buon fine verrà aggiunta la cartella speciale desktop nella sezione di sinistra dell'app per la gestione dei file. Cliccando sulla cartella dovrebbe apparire l'elenco dei file contenuti.



Ora, se impostata in fase di acquisto del VPS, ripetere la procedura descritta per l'aggiunta della condivisione della partizione dati. Una volta arrivati all'apertura della finestra *Aggiungi condivisione file* procedere come nel caso precedente salvo inserire l'indirizzo di rete della partizione dati (es. **\\192.168.223.1\data**) in **URL condivisione file** e la dicitura **Partizione Dati** in **Nome visualizzato**:



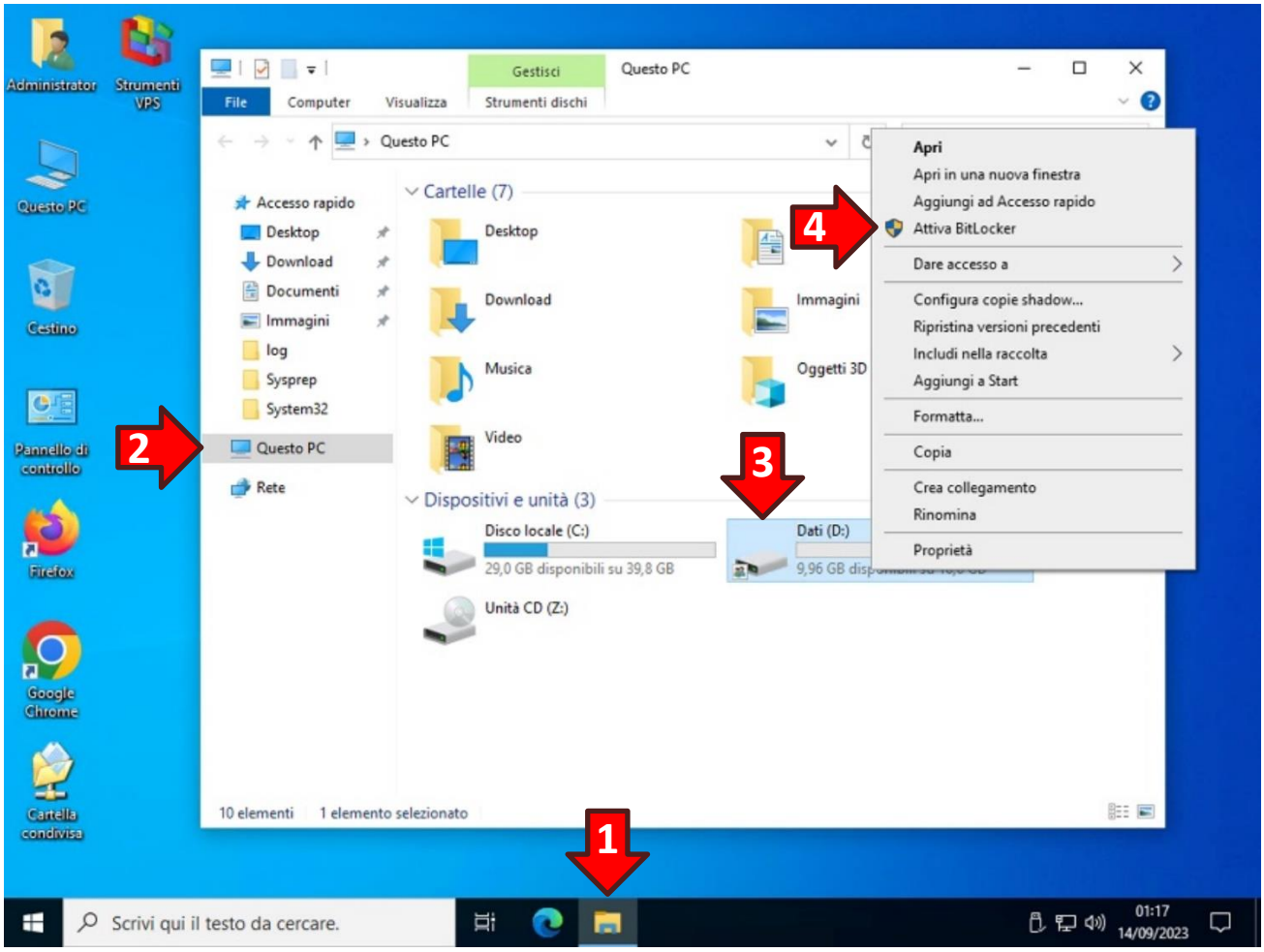
ATTENZIONE! Dalla condivisione della partizione dati non cancellare le cartelle $RECYCLE.BIN e System Volume Information. Tali cartelle sono utilizzate da Windows per il corretto funzionamento della partizione.



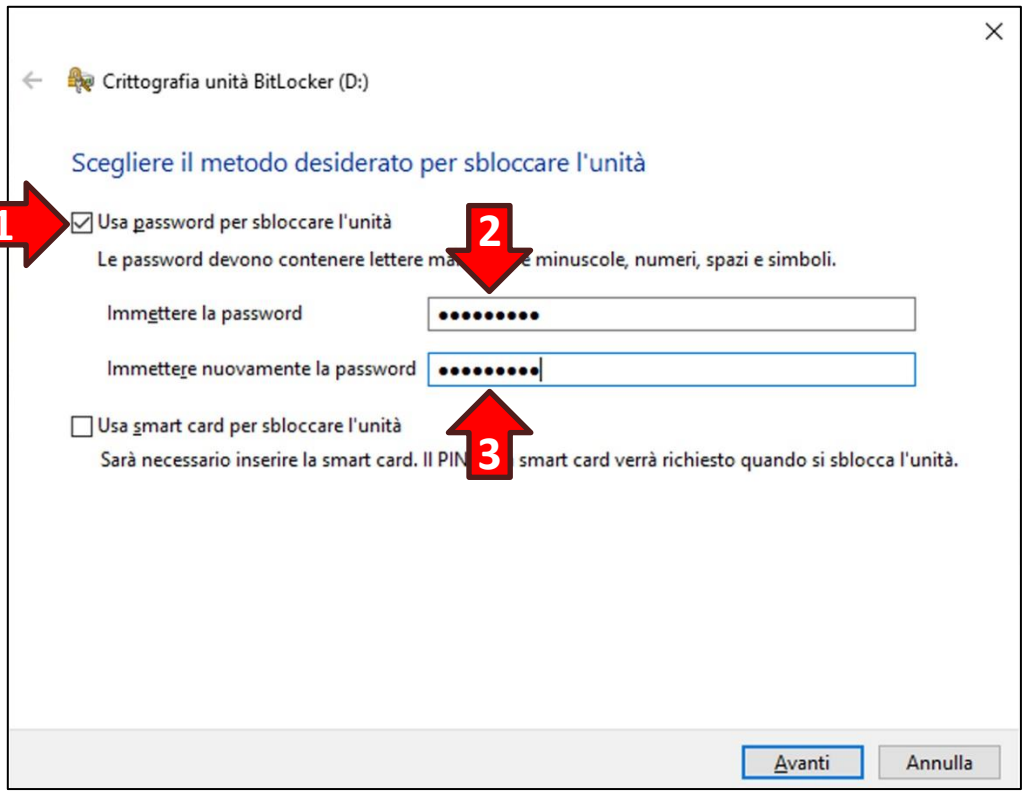
7. Cifratura della partizione dati con BitLocker

Se in fase di acquisto si è scelto di creare una partizione dati questa può essere cifrata con BitLocker.

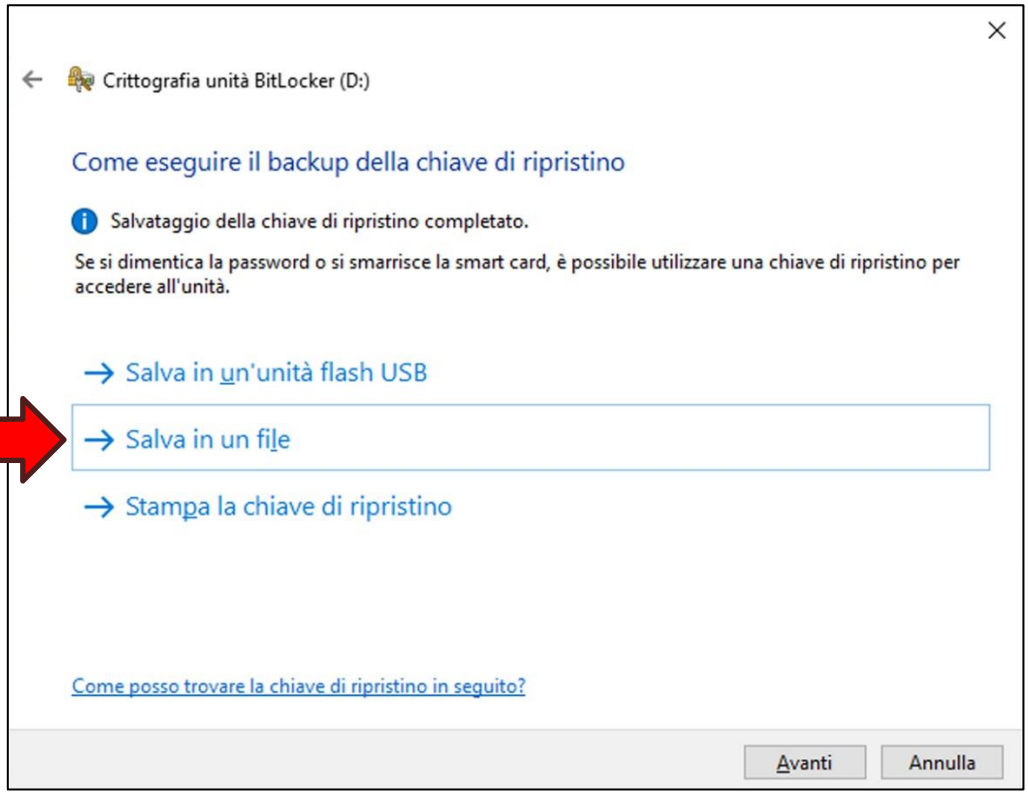
Per cifrare la partizione dati entrare nel desktop del VPS e cliccare sull'icona **Esplora Risorse (1)**. Quindi selezionare l'opzione **Questo PC (2)** dalla lista a destra e cliccare con il tasto destro del mouse sull'**icona della partizione dati (3)**. Infine dal menù pop-up scegliere l'opzione **Attiva BitLocker (4)**:



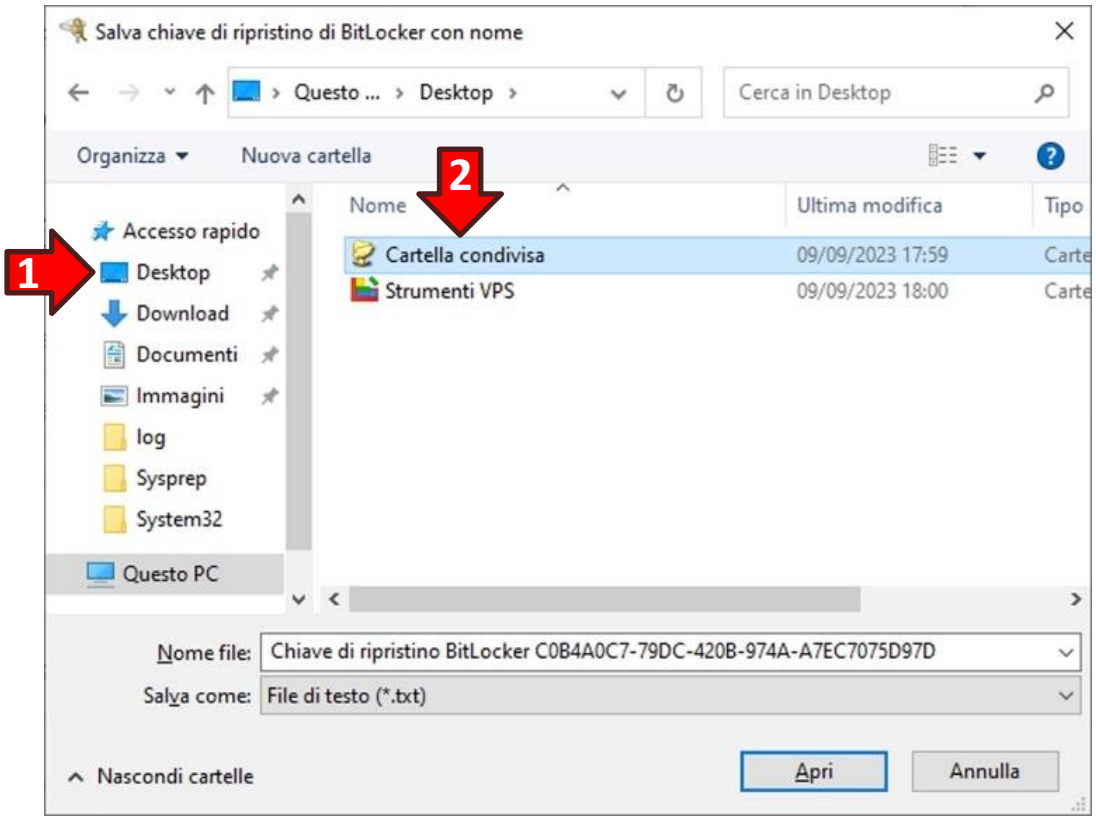
Nella finestra *Scegliere il metodo desiderato per sbloccare l'unità* spuntare l'opzione **Usa password per sbloccare l'unità (1)**. Poi **creare una nuova password (2)** nello spazio indicato e **confermarla (3)** nello spazio sottostante:



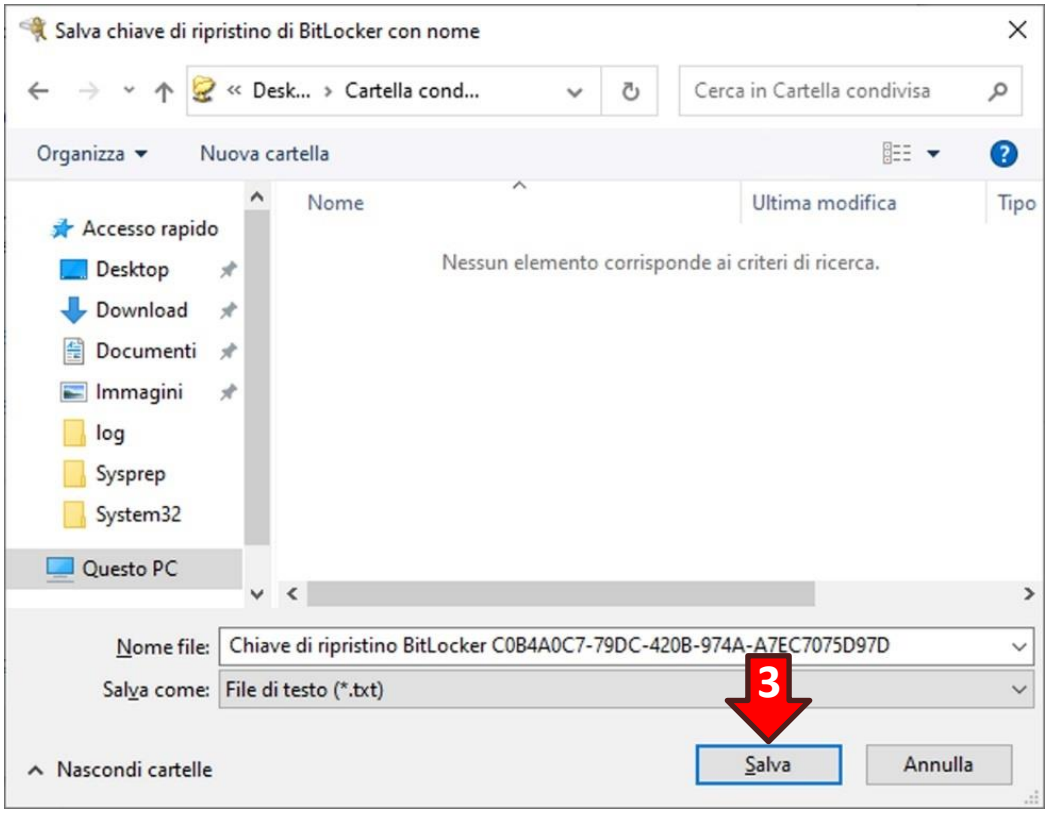
Dalla finestra *Come eseguire il backup della chiave di ripristino* cliccare sull'opzione **Salva in un file**:



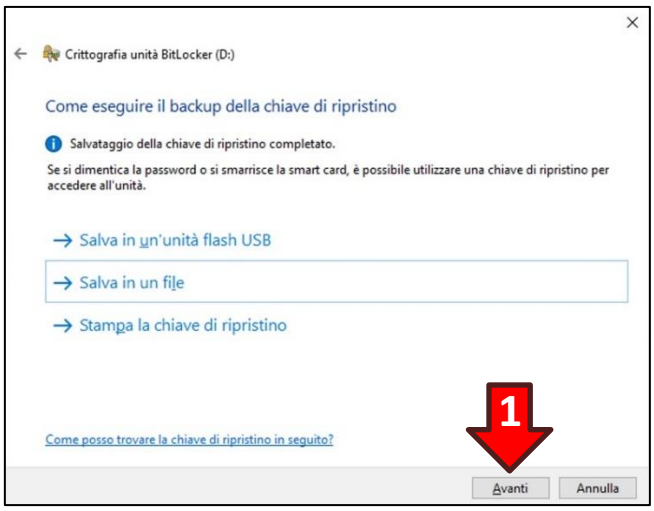
Si aprirà la finestra *Salva chiave di ripristino di BitLocker con nome*. Nell'albero di sinistra cliccare sulla voce **Desktop (1)** e nella sezione di destra fare doppio click sulla voce **Cartella condivisa (2)**:



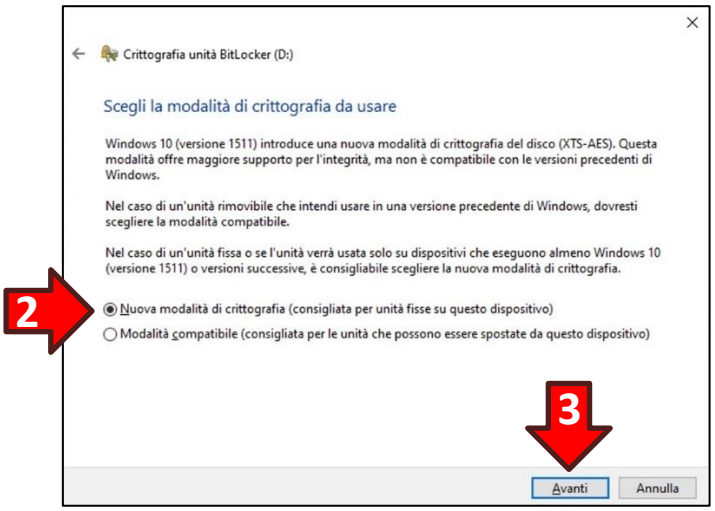
Quindi una volta impostato il salvataggio nella **Cartella condivisa** cliccare il tasto **Salva (3)**:



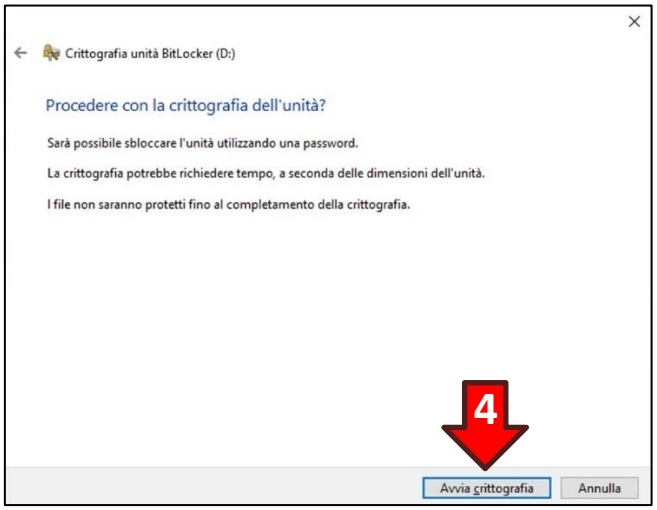
Dopo aver salvato la chiave di ripristino cliccare il tasto **Avanti (1)**:



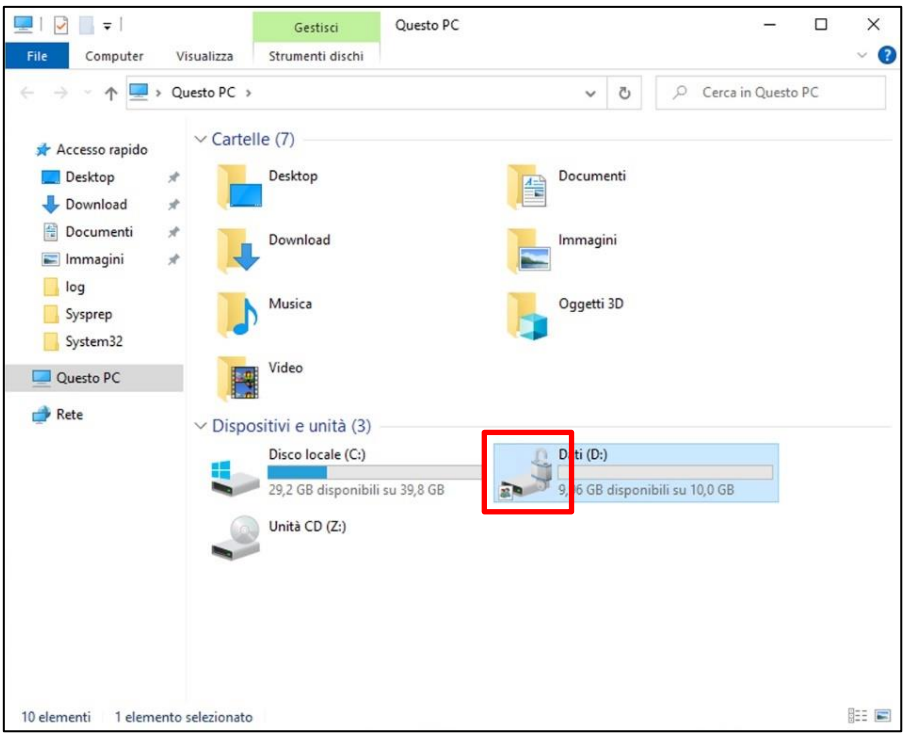
Nella finestra successiva accertarsi che sia spuntata l'opzione **Nuova modalità di crittografia… (2)** quindi cliccare sul tasto **Avanti (3)**:



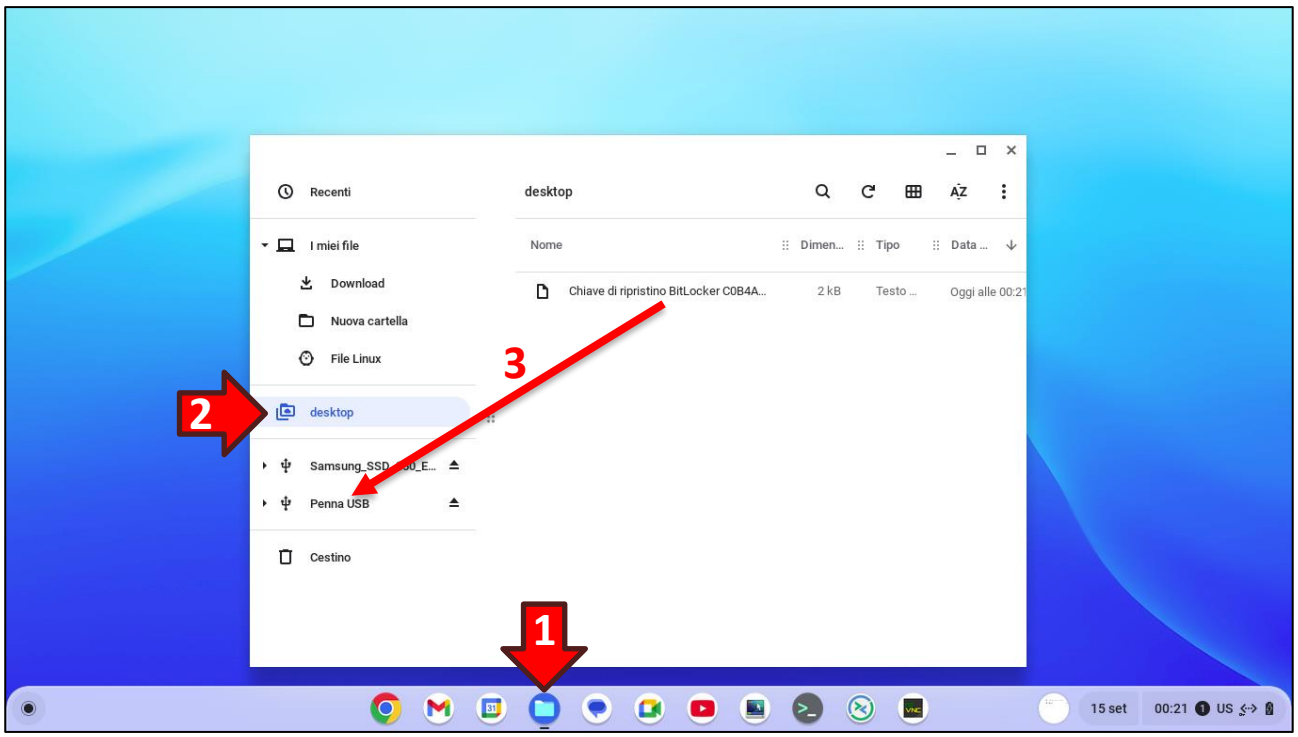
Infine nell'ultima finestra cliccare il tasto **Avvia crittografia (4)**:



Trascorso qualche istante sull'icona della partizione Dati apparirà un lucchetto grigio in posizione aperta:



Ora ritornare sul desktop del proprio Chromebook inserire una chiavetta USB in cui si intende memorizzare la Chiave di ripristino BitLocker. Quindi aprire **l'app di gestione dei file (1)** e dalla sezione di sinistra cliccare sulla condivisione **desktop (2)** del VPS. Poi **trascinare (3)** il file **Chiave di ripristino BitLocker…** sul nome della **chiavetta USB** nell'elenco di destra:



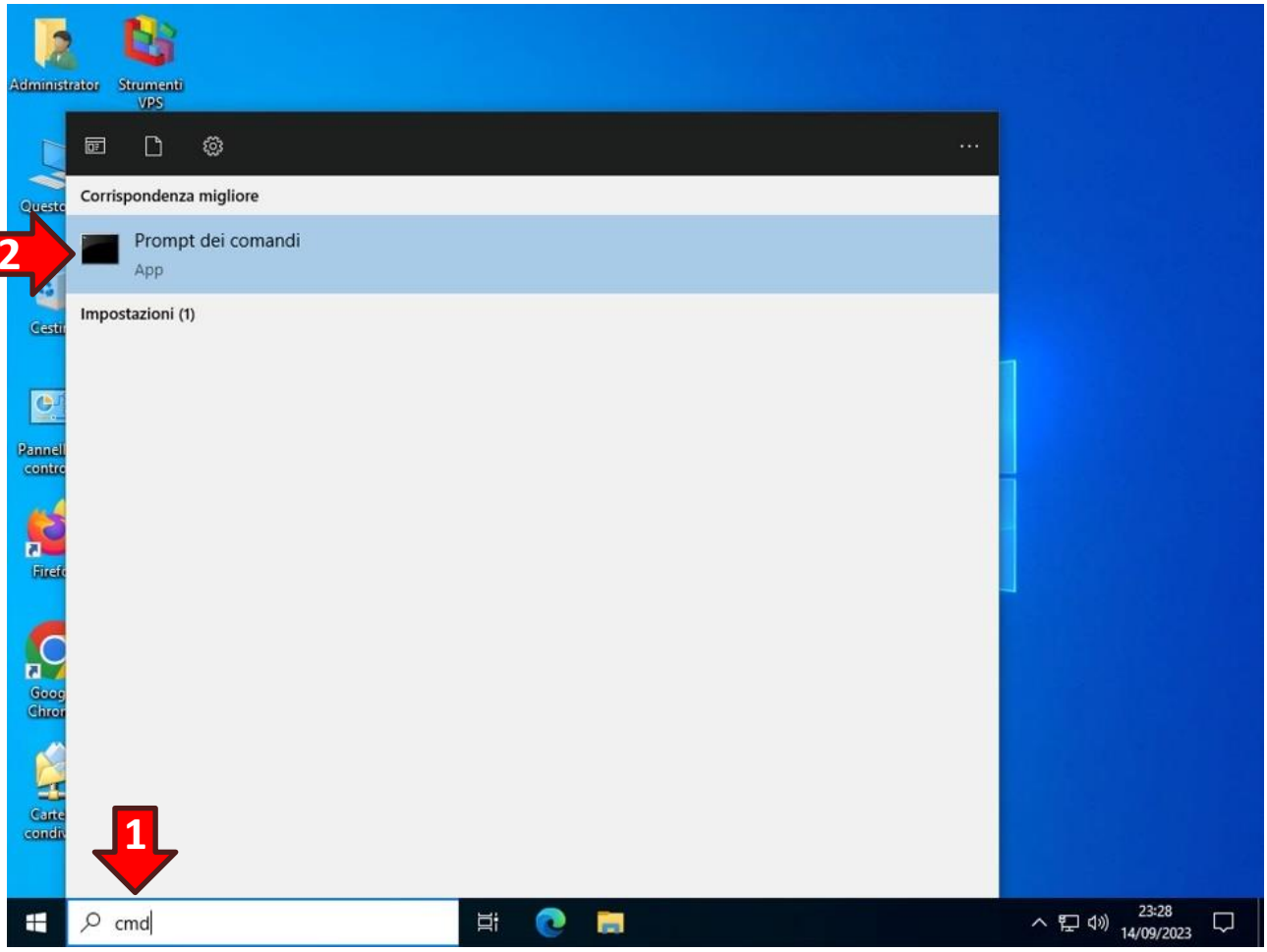
ATTENZIONE! Se si dispone di una stampante è preferibile conservare la *Chiave di ripristino BitLocker* su carta invece che su un dispositivo digitale.

ATTENZIONE! La *Chiave di ripristino BitLocker* è indispensabile in caso di smarrimento della password di accesso all'unità BitLocker quindi conservarla in un luogo sicuro.

ATTENZIONE! In caso di smarrimento sia della password di accesso all'unità BitLocker che della *Chiave di ripristino BitLocker* neppure il fornitore del vostro VPS non sarà in grado di recuperare i dati contenuti nella partizione cifrata e questi dovranno essere considerati definitivamente perduti.

Una volta effettuata la copia (o la stampa) della Chiave di ripristino BitLocker, ai fini della sicurezza è indispensabile rimuovere in modo sicuro il file contenente la chiave.

Quindi ritornare sul desktop del VPS e nella barra di ricerca digitare la dicitura **cmd** (1). Poi cliccare sull'icona nera della voce **Prompt dei comandi (2)** che apparirà nell'elenco:



Si aprirà la finestra Prompt dei comandi. All'interno della finestra digitare:

cd "Desktop\Cartella condivisa"

e poi premere il tasto **Invio** sulla tastiera.

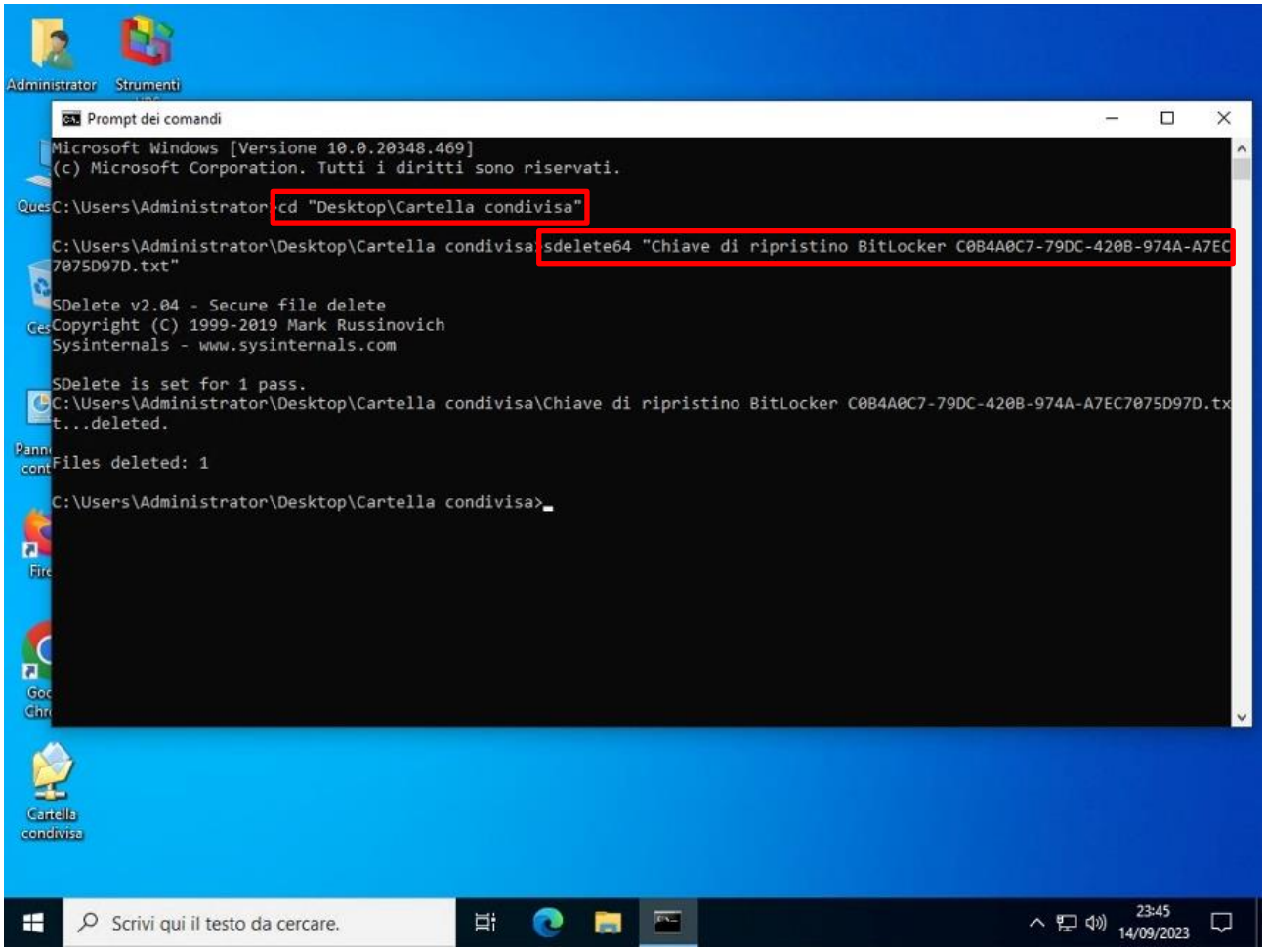
Poi digitare:

sdelete64 "Chiave di ripristino

e premere il tasto **Tab** della tastiera. Alla pressione del tasto **Tab** il nome del file verrà completato automaticamente, come ad esempio:

sdelete64 "Chiave di ripristino BitLocker C0B4A0C7-79DC-420B-974A-A7EC7075D97D.txt"

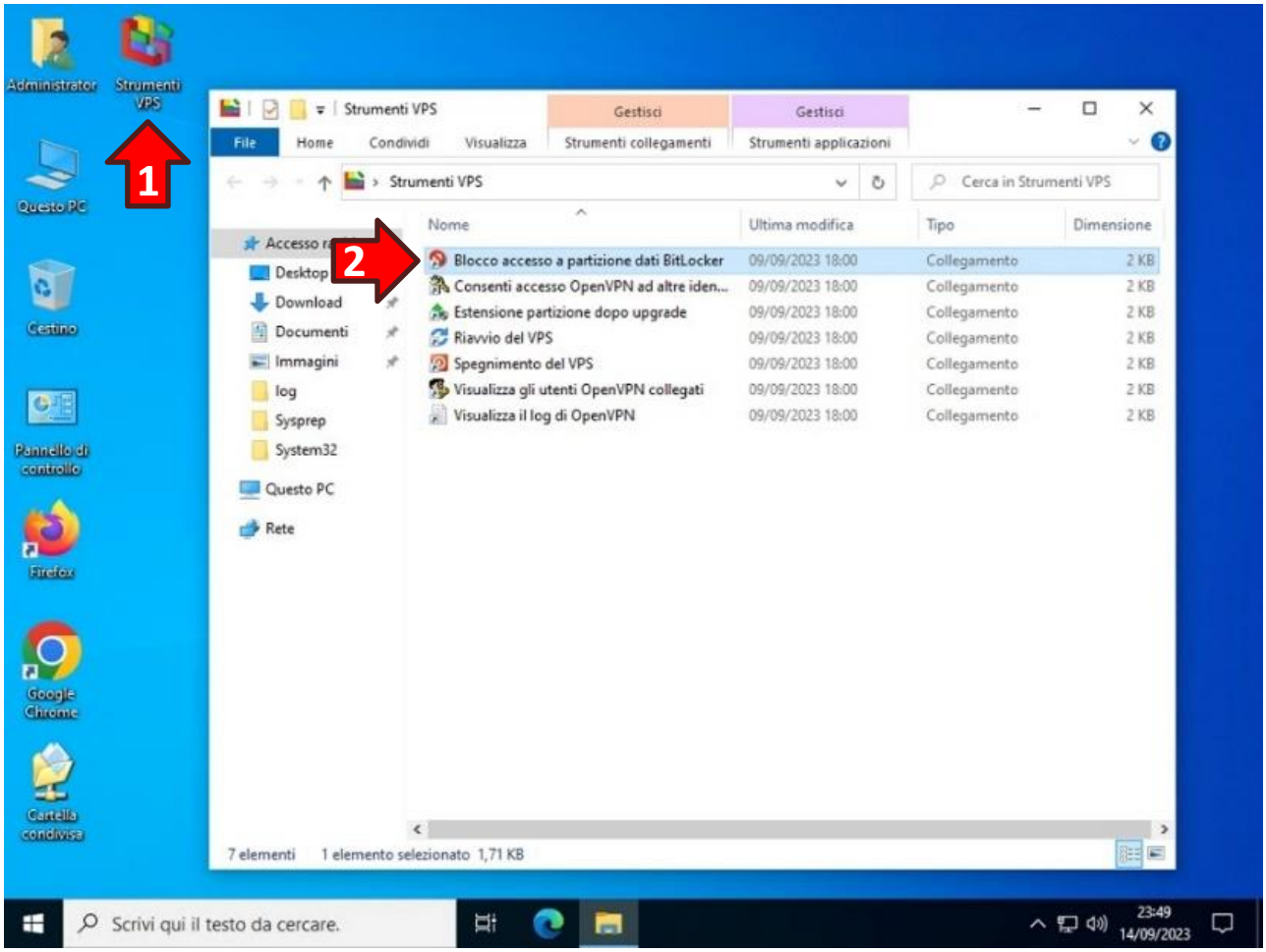
Ora premere il tasto **Invio** per effettuare la cancellazione sicura della chiave.



7.1 Blocco dell'accesso alla partizione cifrata con BitLocker

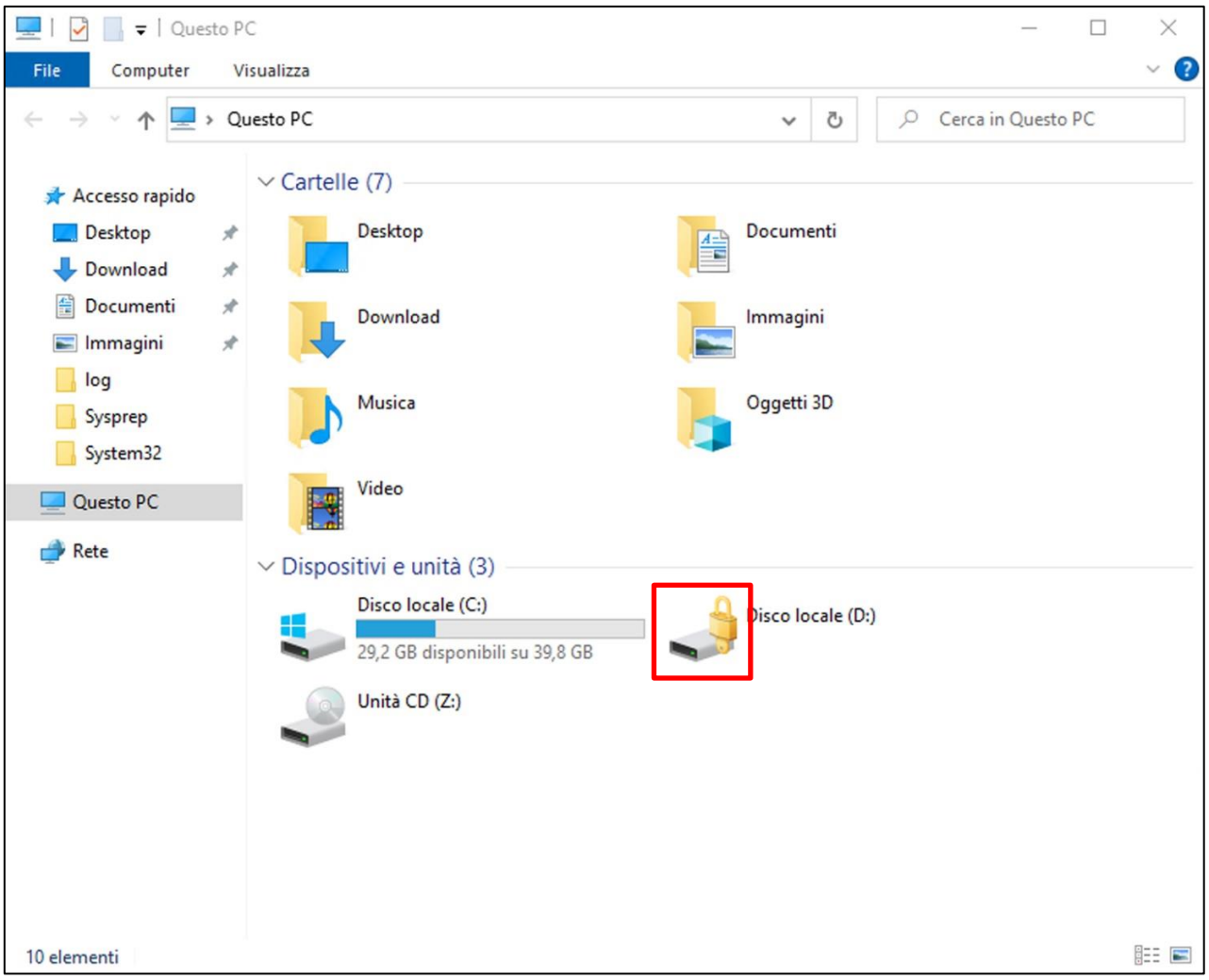
Una volta effettuata la copia sicura dei dati sensibili è consigliabile bloccare l'accesso alla partizione cifrata finché non sarà necessario accedere nuovamente a tali dati.

Per effettuare il blocco fare doppio click sull'icona **Strumenti VPS (1)** presente sul desktop del VPS. Si aprirà una nuova finestra con un elenco di strumenti, quindi fare doppio click sulla voce **Blocco accesso a partizione dati BitLocker (2)**:



Confermare la richiesta di apportare modifiche al dispositivo cliccando il tasto **Sì (3)**:

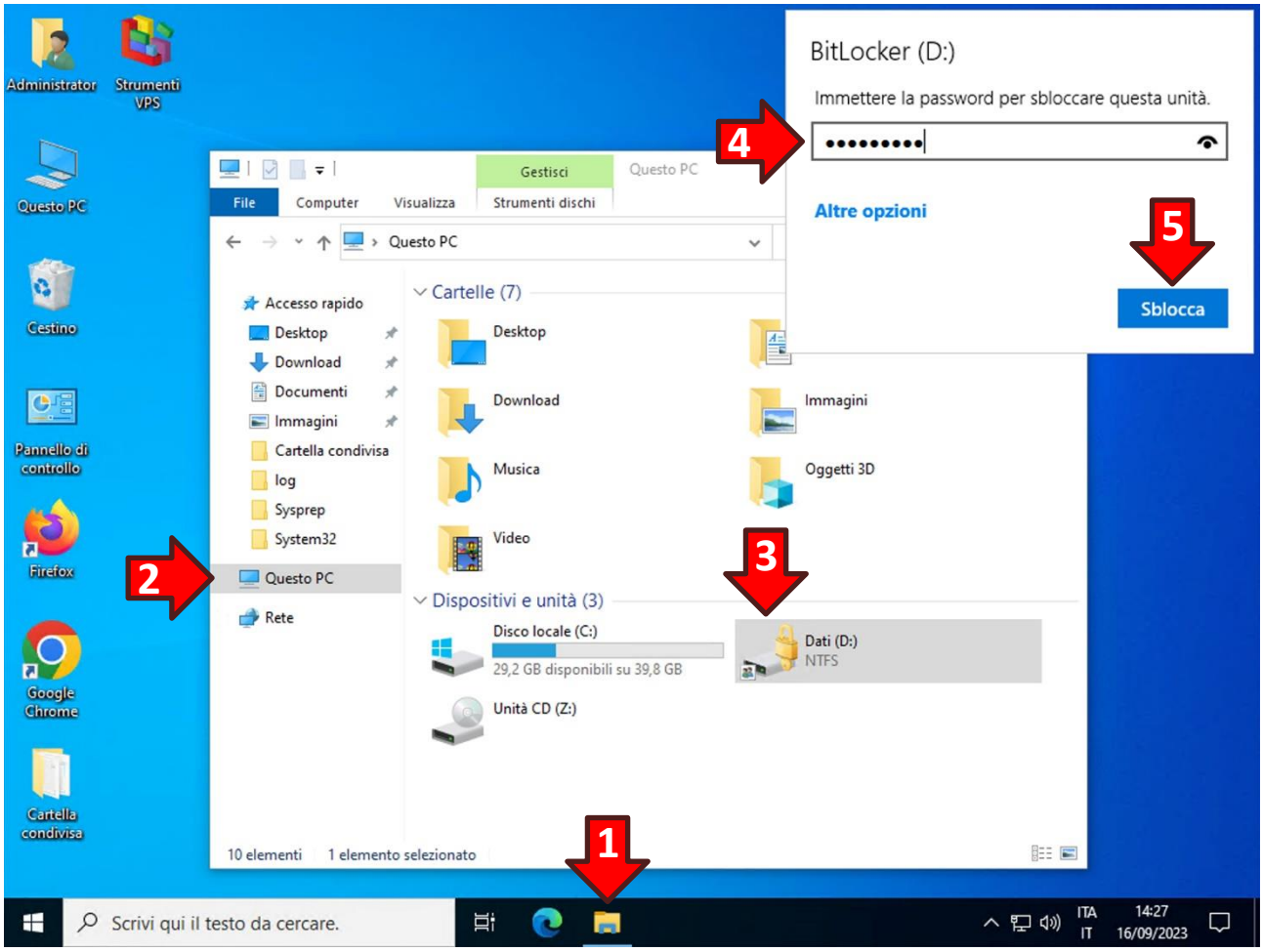
Ora nella finestra **Esplora Risorse** nell'icona dell'unità della partizione dati sarà presente un lucchetto dorato in posizione chiusa:



7.2 Nuovo accesso alla partizione cifrata con BitLocker

Per accedere nuovamente alla partizione cifrata BitLocker è necessario aprire **Esplora Risorse (1)** dalla barra delle applicazioni, poi cliccare sull'opzione **Questo PC (2)** nella sezione di destra e fare doppio click sull'**icona della partizione dati (3)**.

A questo punto inserire la **password (4)** creata per cifrare la partizione e cliccare il tasto **Sblocca (5)** per accedere alla partizione.



ATTENZIONE! In caso di smarrimento della password è possibile utilizzare la *Chiave di ripristino BitLocker* cliccando sulla dicitura blu **Altre opzioni** e successivamente sulla dicitura **Immettere la chiave**.

8. Accesso a WPanel tramite smart card o token USB da un Chromebook

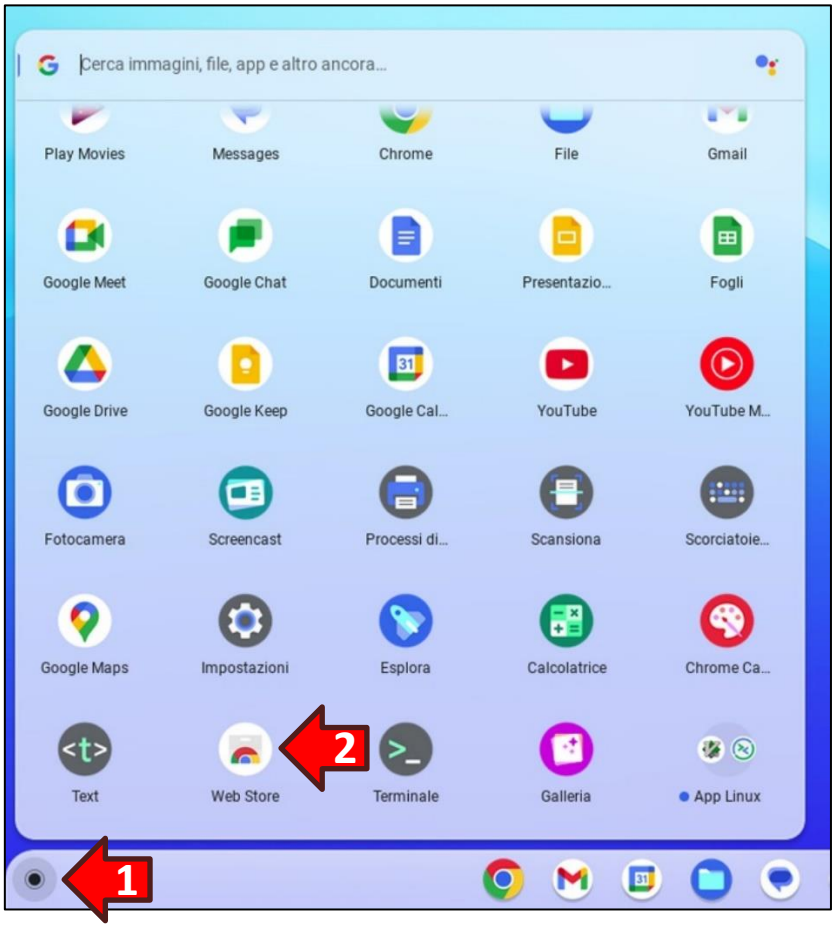
Al momento ChromeOS non supporta l'apertura di connessioni OpenVPN con un certificato memorizzato su una smart card o su un token USB.

Ciò nonostante è possibile accedere al sito WPanel del vostro fornitore attraverso un certificato di autenticazione WPanel memorizzato su smart card o token USB (Es. dispositivi Yubikey serie 5).

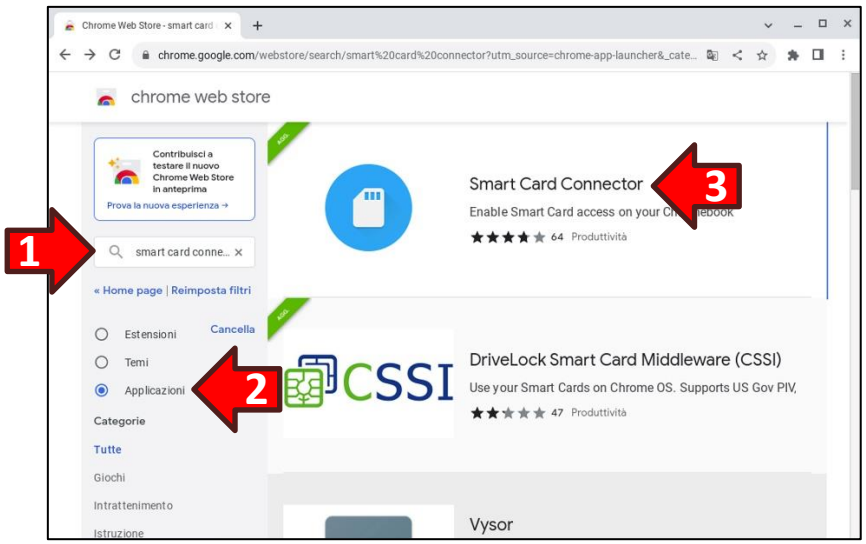
Se si sta già utilizzando una smart card per accedere al sito WPanel del vostro fornitore è possibile passare alla configurazione del Chromebook, diversamente per generare ed inserire un certificato di autenticazione WPanel in una smart card fare riferimento al **Manuale PKI per VPS della linea Smart Card**. Se non si ha a disposizione un computer con Microsoft Windows è necessario conoscere i fondamenti dei software OpenSSL e OpenSC per la creazione del keypair, la creazione della richiesta di emissione del certificato (CSR) ed il caricamento del certificato emesso all'interno della smart card.

Una volta completata la procedura di generazione del certificato di identificazione collegare il lettore di smart card (o il token USB) al Chromebook.

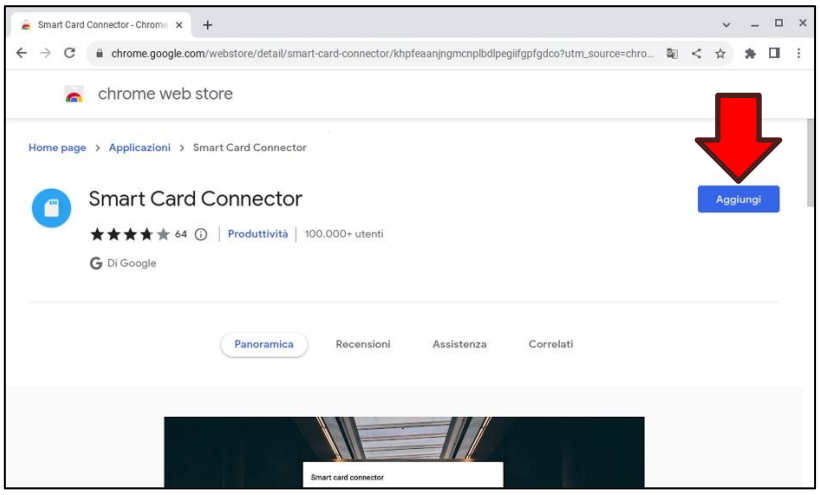
Poi cliccare sul **tasto di apertura del menù delle App (1)** e cliccare l'icona del **Web Store (2)**:



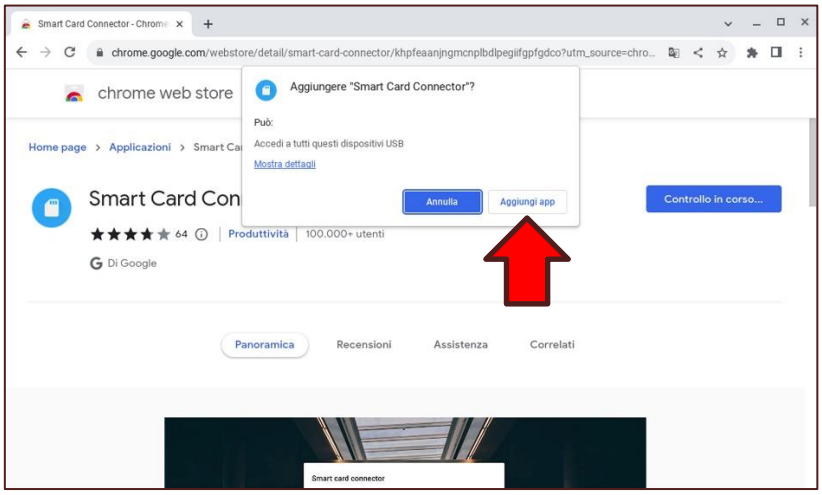
Nella sezione di sinistra ricercare l'app **Smart Card Connector (1)** poi impostare la ricerca sulla **categoria Applicazioni (2)** e nella sezione di sinistra cliccare sul **nome dell'app (3)**:



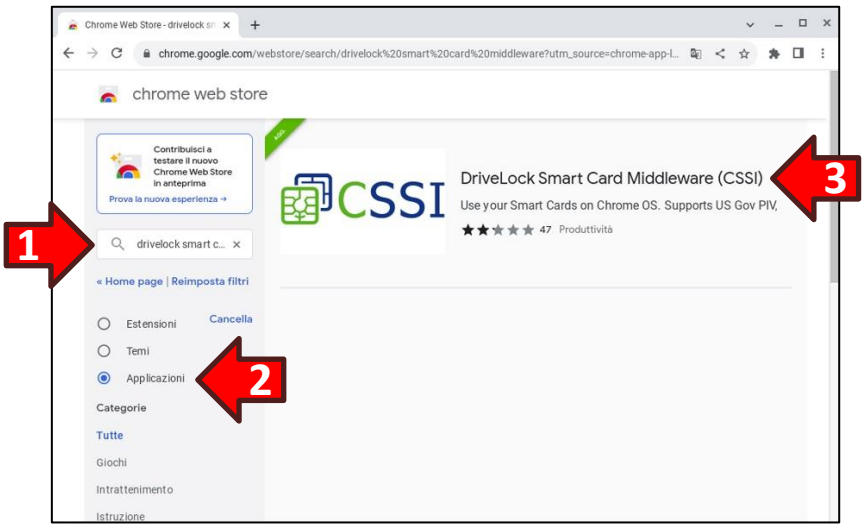
Una volta entrati nella pagina web dell'app cliccare il tasto **Aggiungi**:



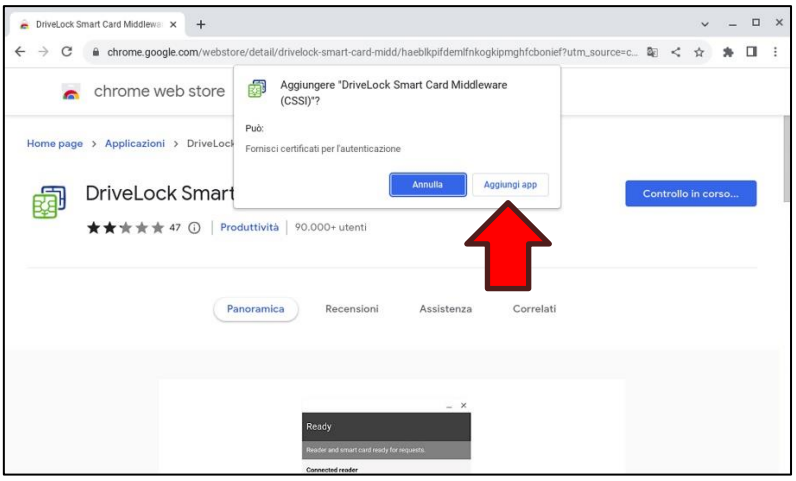
Apparirà un messaggio d'avviso per l'accesso ai dispositivi USB. Cliccare il tasto **Aggiungi App**:



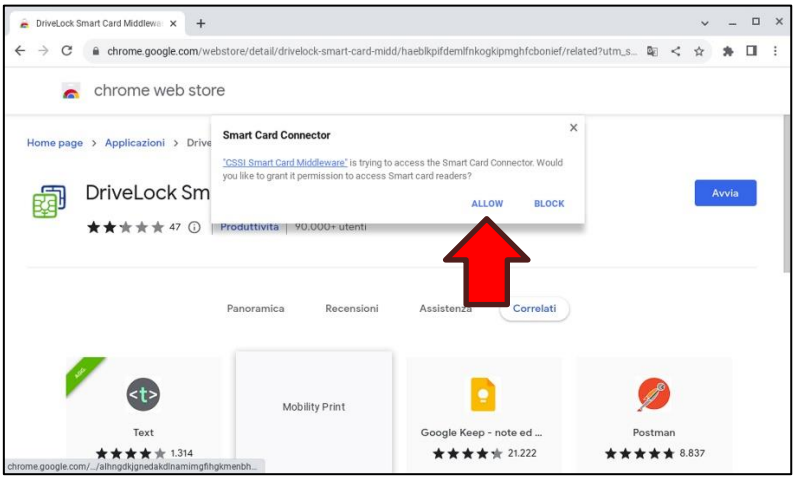
Rientrare nell'app Web Store e, nella sezione di sinistra, ricercare l'app **DriveLock Smart Card Middleware (CSSI) (1)** poi impostare la ricerca sulla **categoria Applicazioni (2)** e nella sezione di sinistra cliccare sul **nome dell'app (3)**:



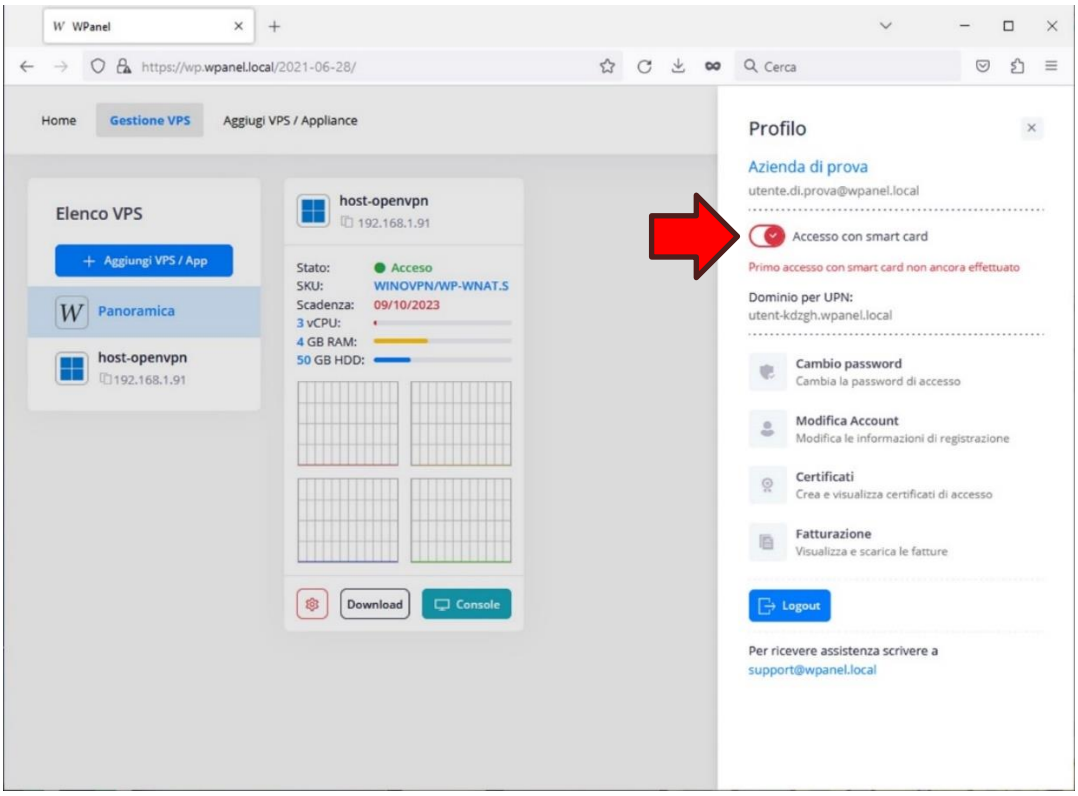
In fase di installazione cliccare il tasto **Aggiungi App** nel riquadro del messaggio di avviso:



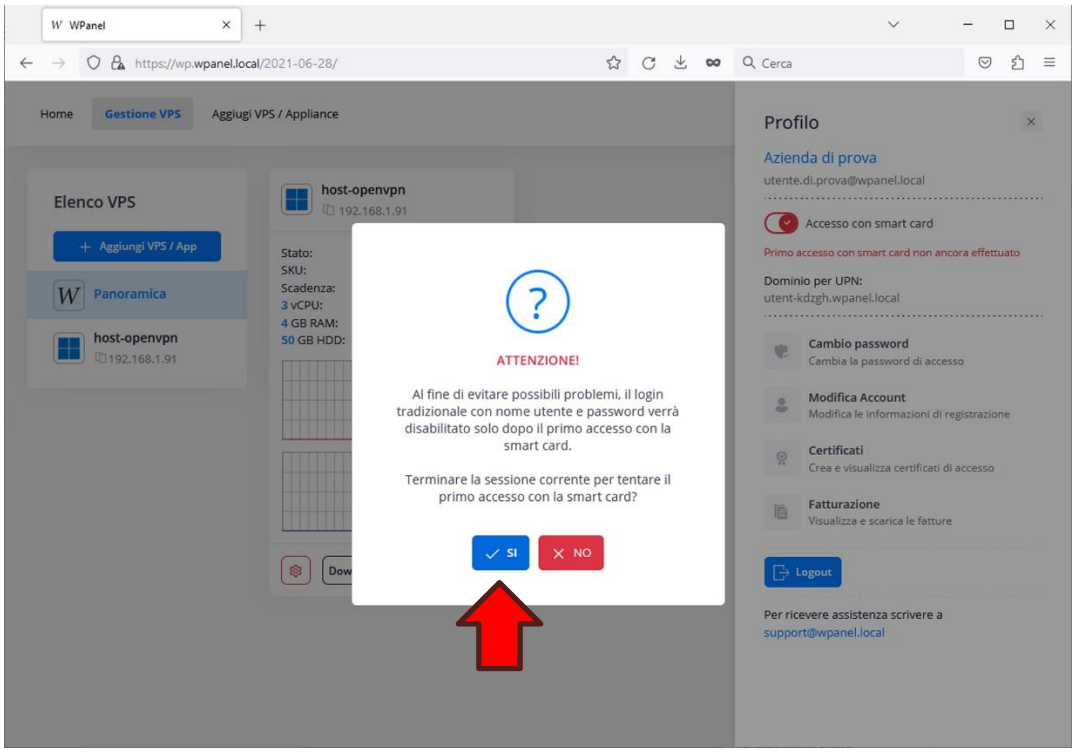
Infine cliccare sulla dicitura **ALLOW** nel messaggio in lingua inglese per l'accesso ai lettori smart card:



Se non si è già abilitato l'accesso con smart card nel sito WPanel del vostro fornitore, effettuare il login poi cliccare sull'icona del profilo in alto a destra per mostrare il menù laterale ed infine abilitare l'opzione **Accesso con smart card**:

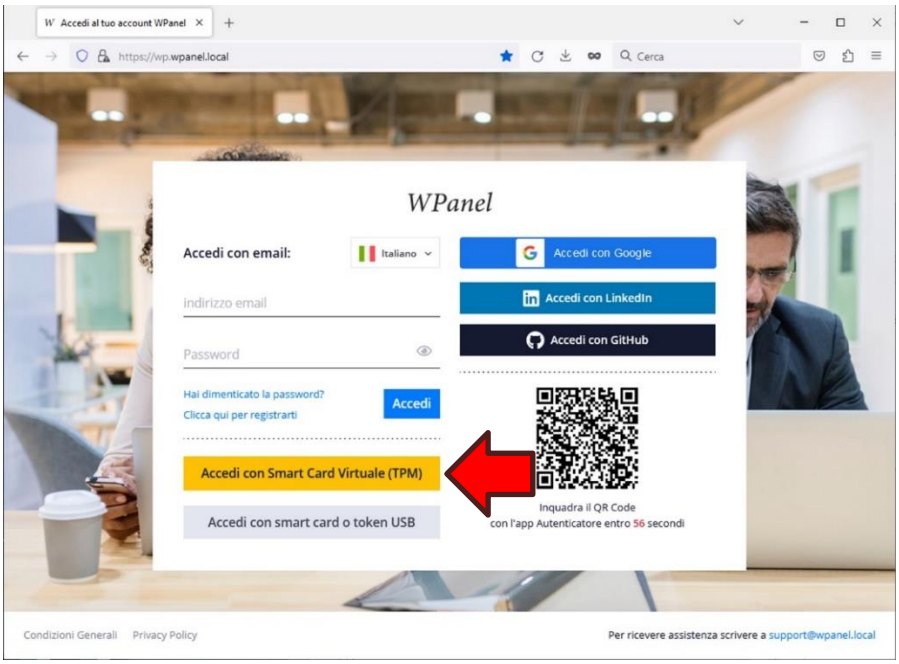


Una volta abilitata l'opzione apparirà la richiesta di disconnessione per verificare l'accesso con smart card. Procedere con il logout cliccando il tasto **Sì**:

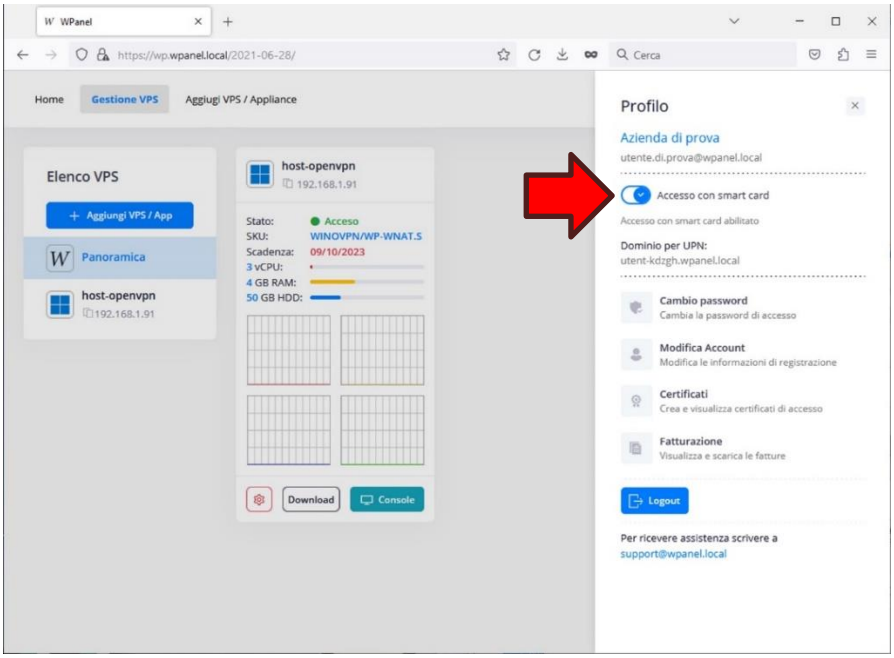


Ritornati alla pagina di login sarà possibile eseguire l'accesso con la smart card.

ATTENZIONE! L'insieme di software di gestione delle smart card in Chromebook non supportano i più recenti protocolli di crittografia (TLS 1.3), per cui è necessario utilizzare il protocollo TLS 1.2 cliccando il tasto Accedi con Smart Card Virtuale (TPM):



Se il certificato è valido e l'insieme di software per la gestione della smart card nel Chromebook funzionano correttamente verrà effettuato il login in WPanel l'opzione **Accesso con smart card** nel menù del profilo sarà diventata di colore blu:



A questo punto l'accesso con nome utente e password è stato disabilitato per cui sarà possibile accedere a WPanel esclusivamente tramite smart card.

Per disattivare l'accesso esclusivo con smart card:

- ritornare nel menù laterale del profilo e disattivare l'opzione Accesso con smart card (se non si sta utilizzando l'accesso OpenID Connect di un provider verrà richiesto di creare una nuova password di accesso);
- se è stata smarrita la smart card cliccare sulla dicitura **Hai dimenticato la password?** nella form di login e seguire le indicazioni.

9 Recupero o modifica delle credenziali e accesso multiutente

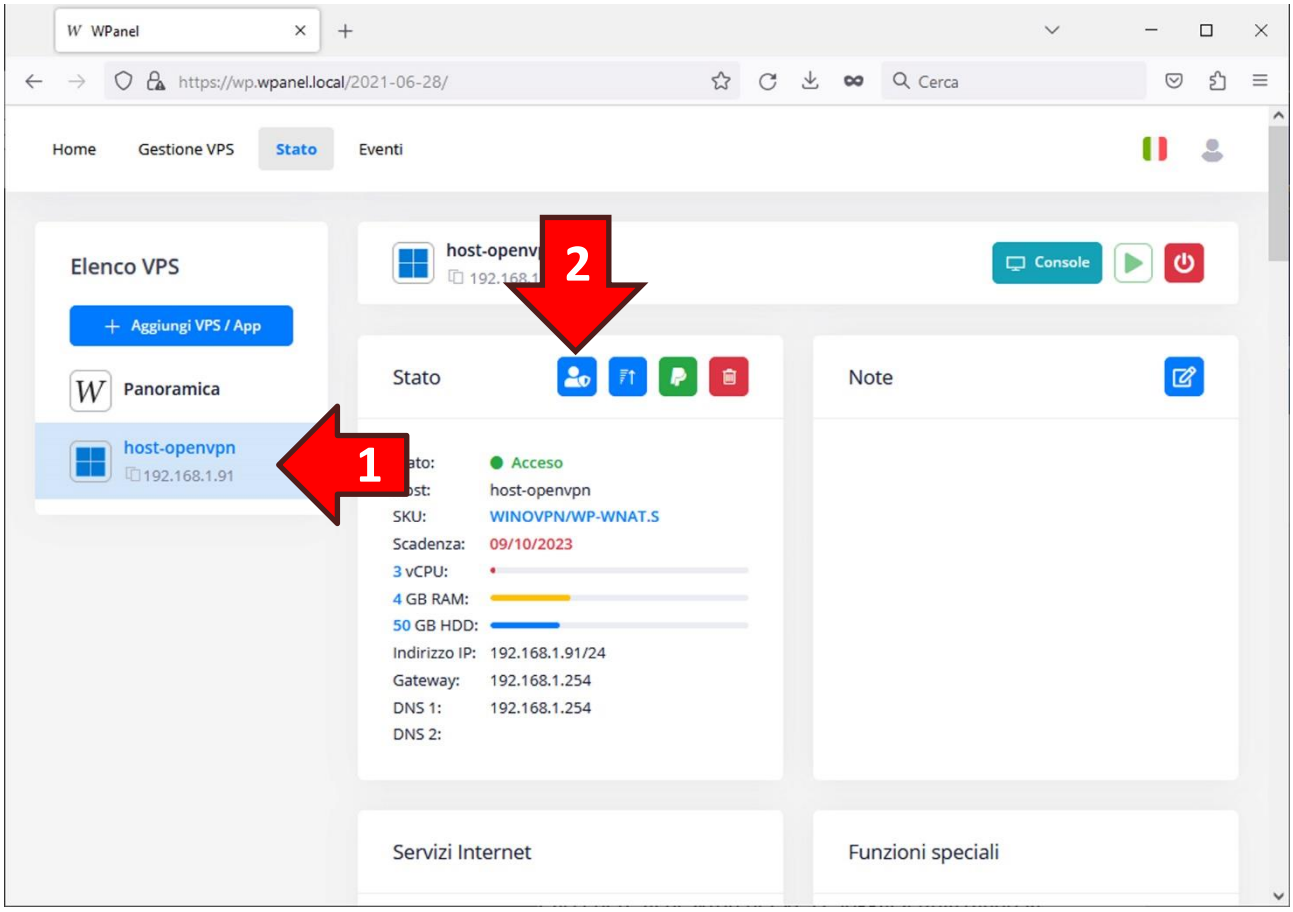
9.1 Modifica delle credenziali dell'utente Administrator

La procedura seguente può essere utilizzata anche in caso di smarrimento completo di tutte le credenziali del VPS.

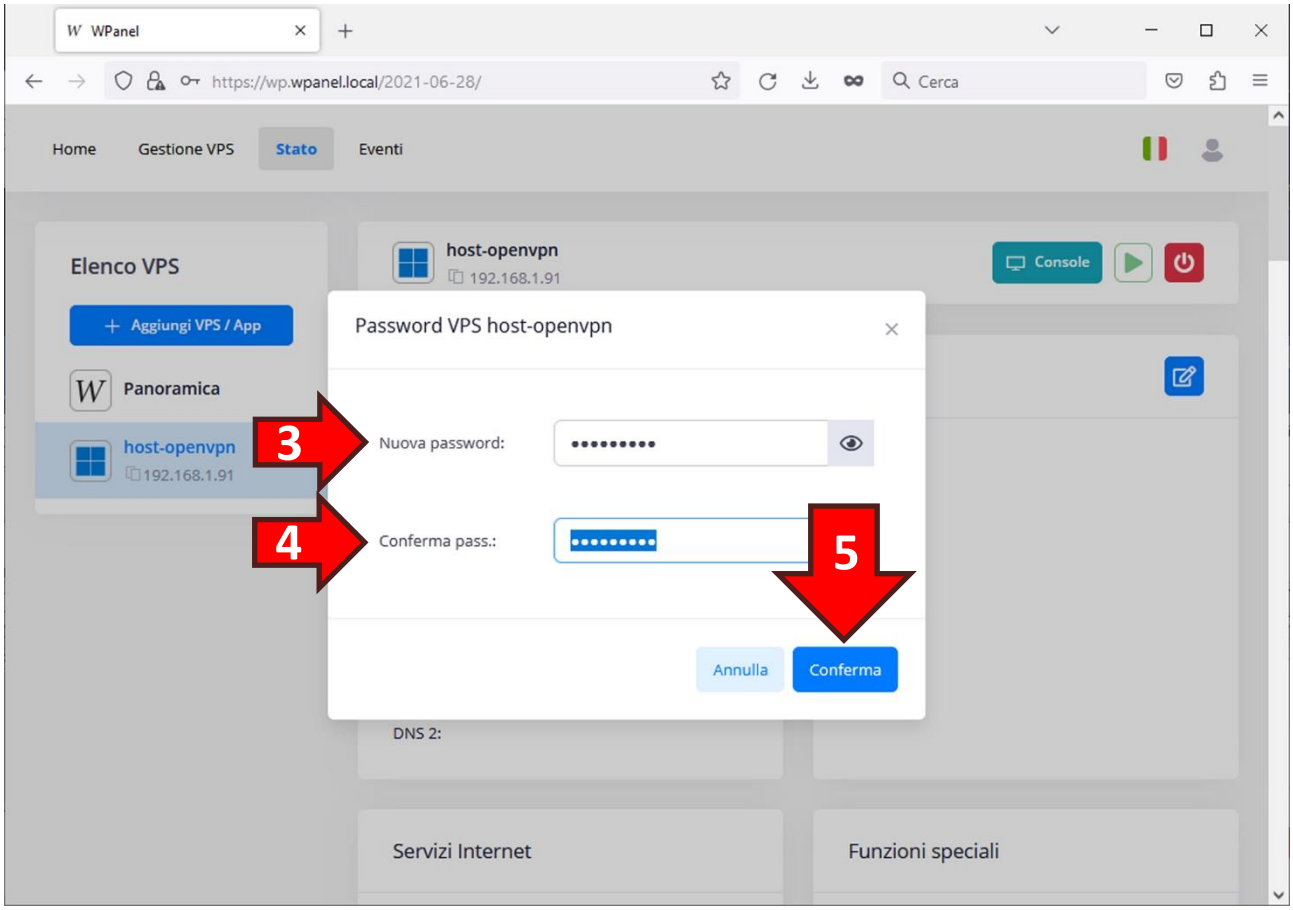
È possibile modificare le credenziali esistenti del VPS in totale autonomia attraverso il sito WPanel del vostro fornitore.

Il primo passo è la reimpostazione dell'utente Administrator. Per effettuare tale operazione il VPS deve essere acceso e deve avere i servizi Windows in esecuzione. Nel caso il VPS fosse stato spento è necessario sapere che i servizi Windows saranno operativi qualche minuto dopo l'accensione.

Per modificare la password dell'utente Administrator entrare nello **stato del VPS (1)** e cliccare sull'icona dell'**utente con lo scudo (2)**:



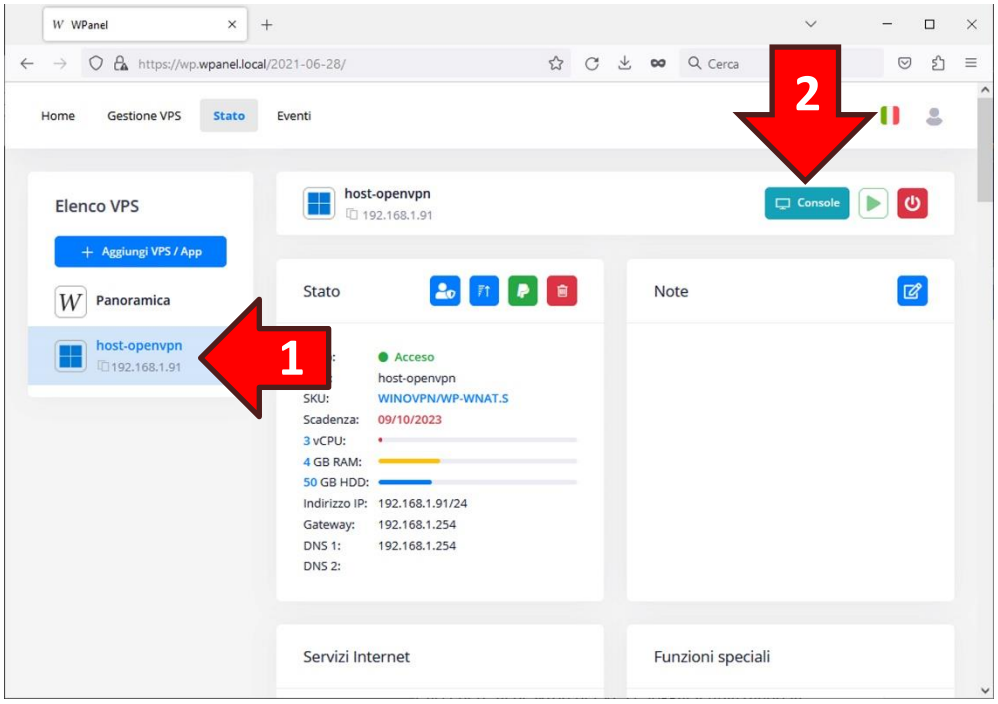
Nella nuova finestra **inserire (3)** e **confermare (4)** una nuova password facendo attenzione a digitare **almeno 8 caratteri tra cui almeno una lettera maiuscola, almeno un numero e almeno un simbolo**. Successivamente confermare il cambio password con il tasto **Conferma (5)**.



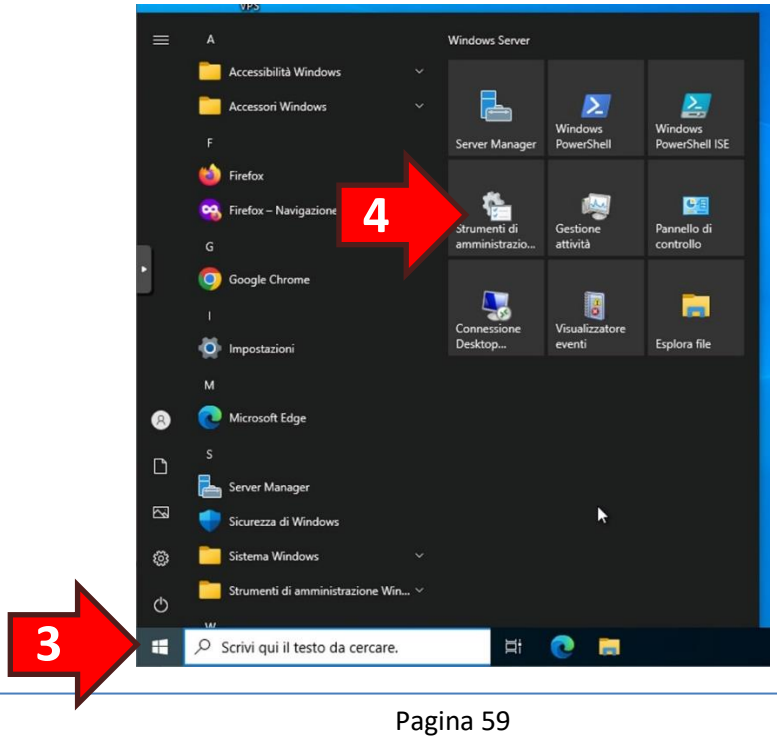
9.2 Modifica delle credenziali dell'utente associato alla VPN

Per modificare le credenziali dell'utente associato alla VPN è necessario accedere al desktop del VPS.

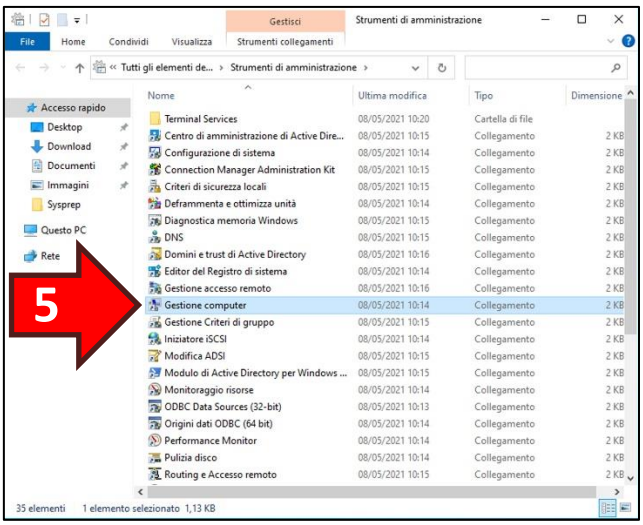
Se non è possibile attivare il tunnel OpenVPN basta accedere al sito WPanel del vostro fornitore, entrare nello **stato del VPS (1)** e successivamente cliccare il tasto **Console (2)**.



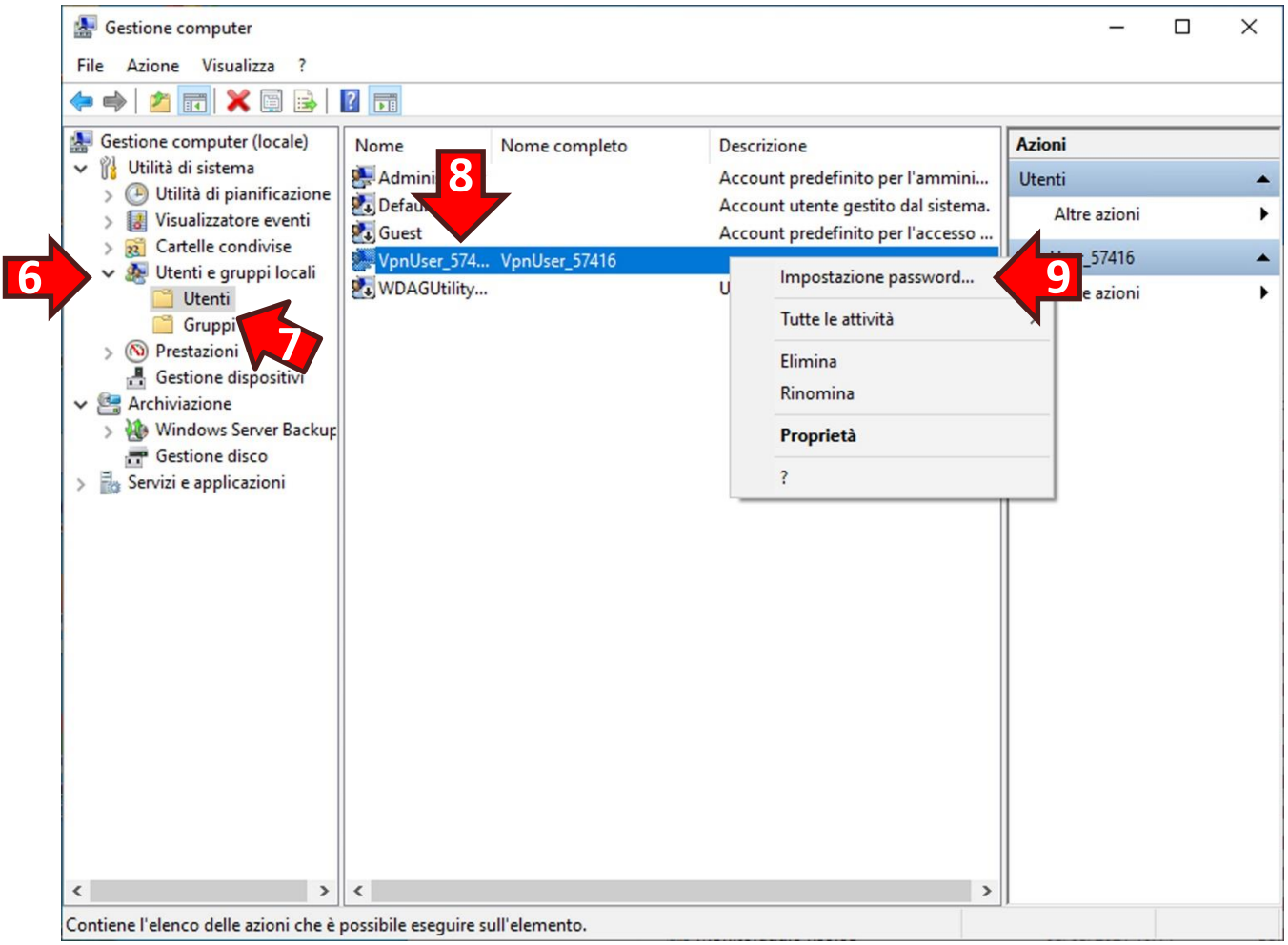
Una volta entrati nel desktop del VPS cliccare sul **Menù start (3)** e successivamente sull'icona **Strumenti di amministrazione (4)**:



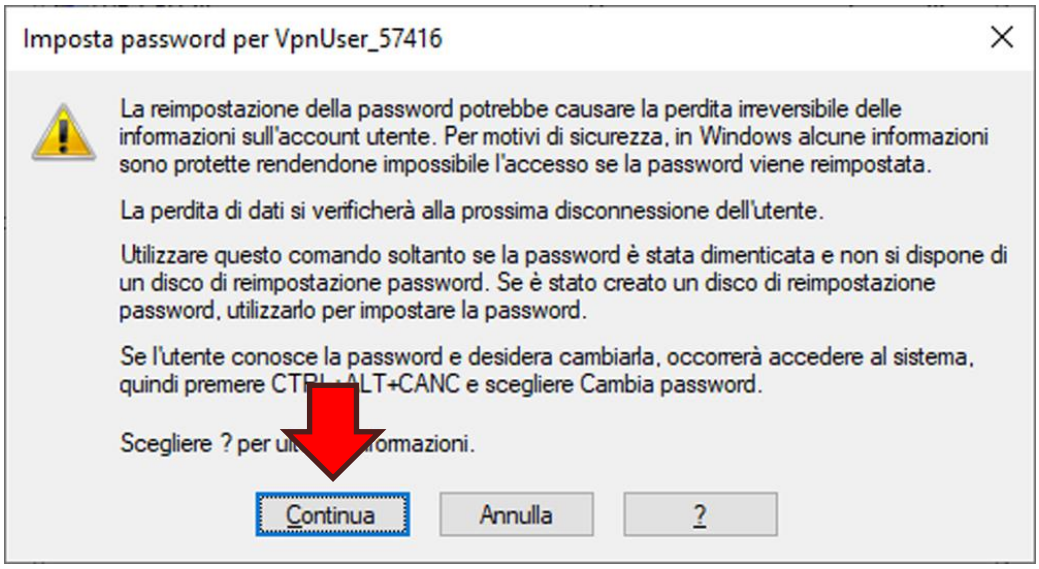
Dalla finestra *Strumenti di amministrazione* fare doppio click su **Gestione computer (5)**:



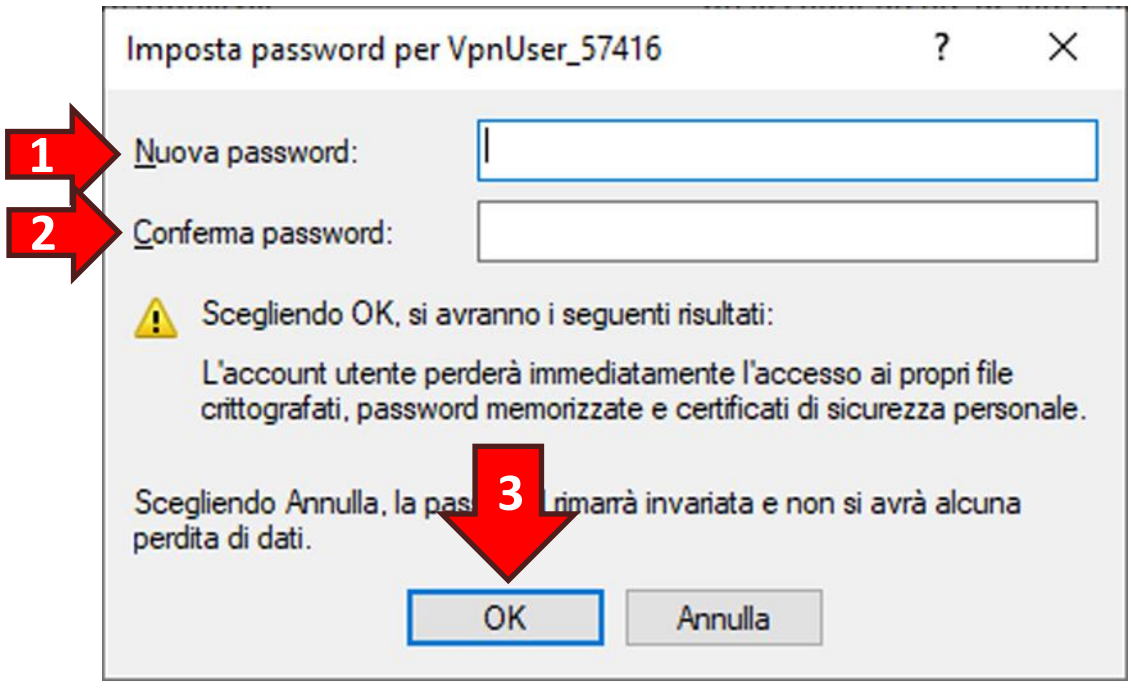
Dalla finestra *Gestione computer* fare doppio click sull'opzione **Utenti e gruppi locali (6)** e poi cliccare sul nodo **Utenti (7)**. Quindi nella sezione a destra selezionare l'**utente associato alla VPN (8)** con il prefisso VpnUser_ e successivamente cliccare il tasto destro del mouse per aprire il menù pop-up. Dal menù cliccare sull'opzione **Impostazione password… (9)**:



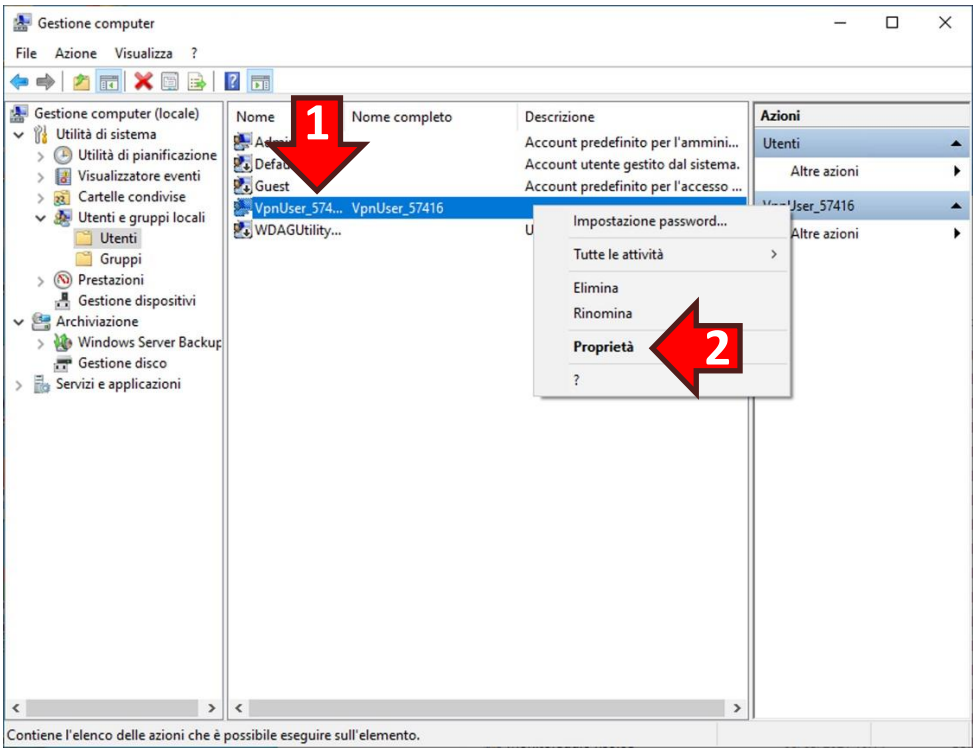
Nel messaggio di avviso di cambio password cliccare il tasto **Continua**:



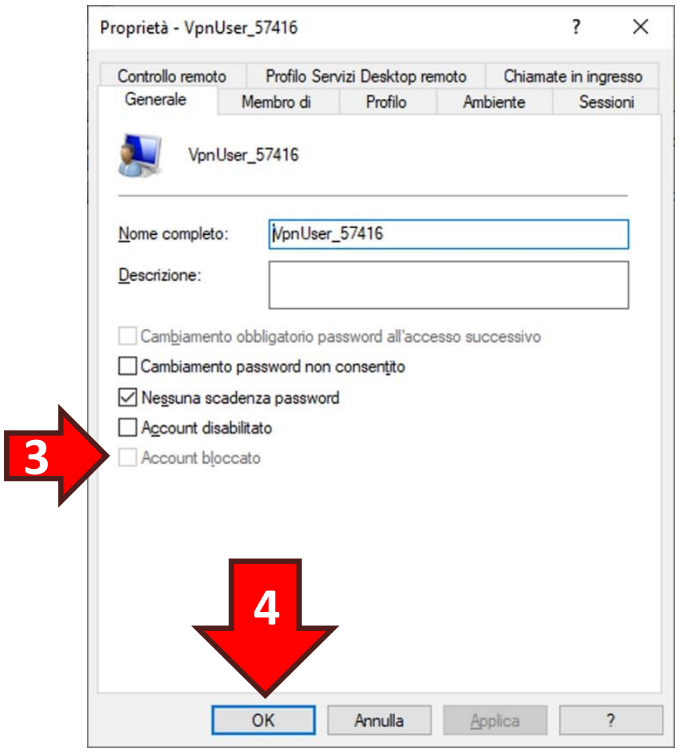
Digitare la **nuova password (1)** e confermarla nello **spazio sottostante (2)** poi cliccare il tasto **OK (3)**:



Dopo aver cambiato password è bene accertarsi che l'utente non risulti bloccato a seguito di svariati tentativi falliti di apertura del tunnel VPN. Quindi dalla finestra *Gestione computer* cliccare nuovamente con il tasto destro del mouse sull'**utente associato alla VPN (1)** e dal menù pop-up selezionare l'opzione **Proprietà (2)**:



Nella finestra delle proprietà accertarsi che non sia presente la spunta nell'opzione **Account bloccato (3)**. Qualora fosse presente rimuovere la spunta. Infine cliccare sul tasto **OK (4)**:

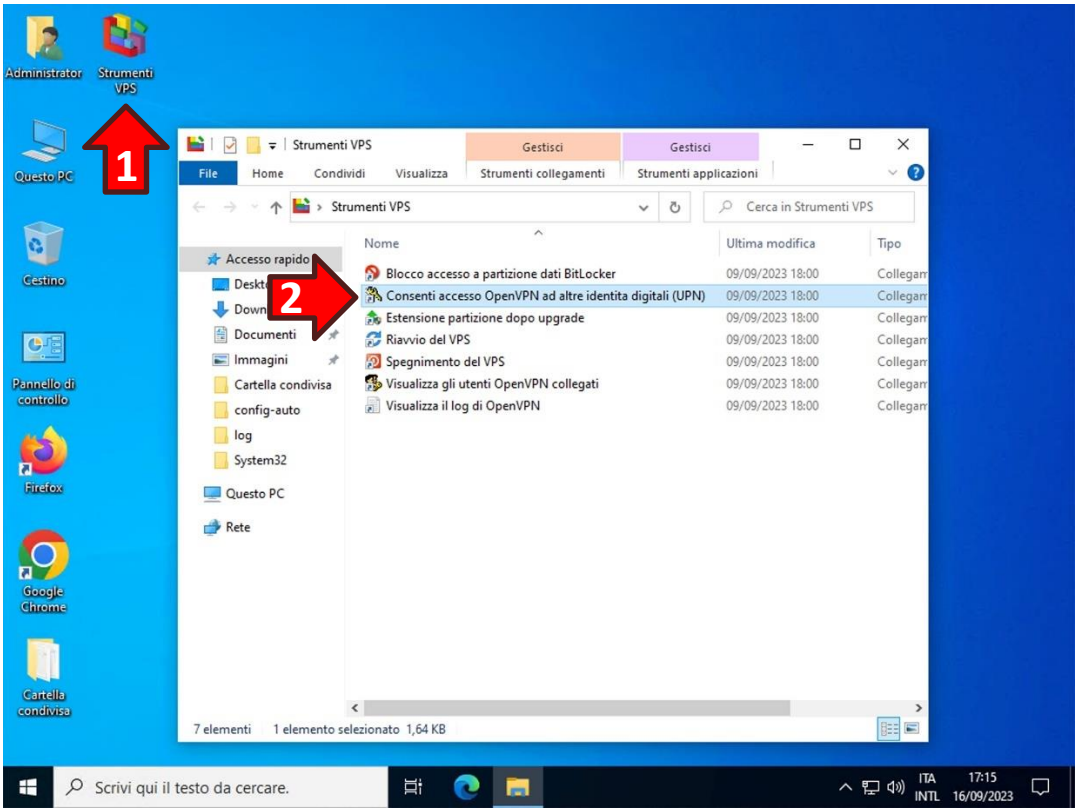


9.3 Accesso VPN con più certificati client (UPN multipli)

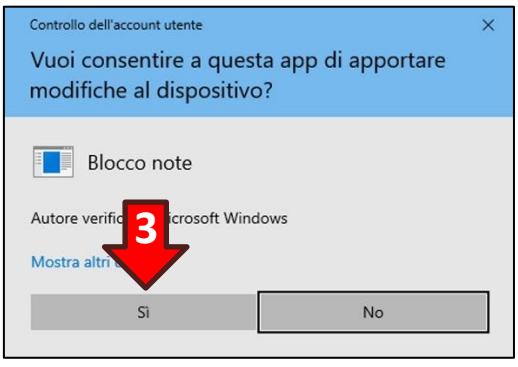
ATTENZIONE! Il server OpenVPN del vostro VPS accetta automaticamente differenti certificati client contenenti il medesimo UPN.

È possibile, per ragioni di carattere aziendale, configurare il server OpenVPN per accettare certificati client emessi sul sito WPanel del vostro fornitore con identità digitale (UPN) differente rispetto a quella selezionata in fase di acquisto del VPS.

Per consentire l'accesso ad un certificato client contenente un nuovo UPN fare doppio click sull'icona **Strumenti VPS (1)** presente sul desktop del VPS. Si aprirà una nuova finestra con un elenco di strumenti, quindi fare doppio click sulla voce **Consenti accesso OpenVPN ad altre identita digitali (UPN) (2)**:

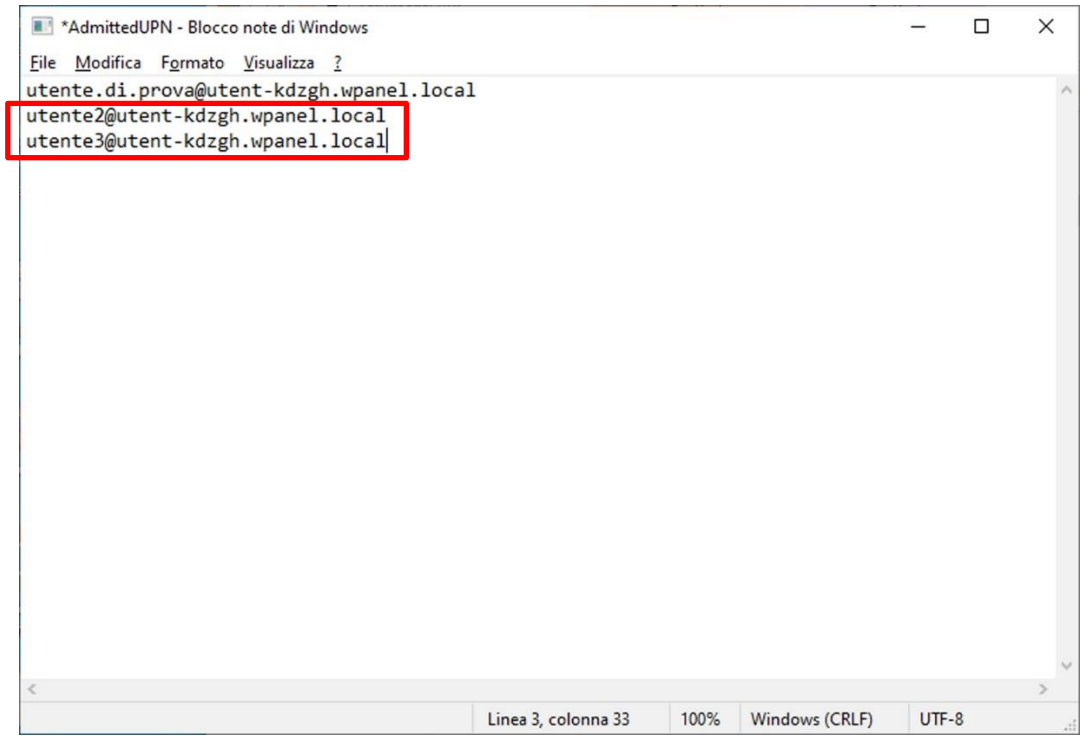


Confermare la richiesta di apportare modifiche al dispositivo cliccando il tasto **Sì (3)**:

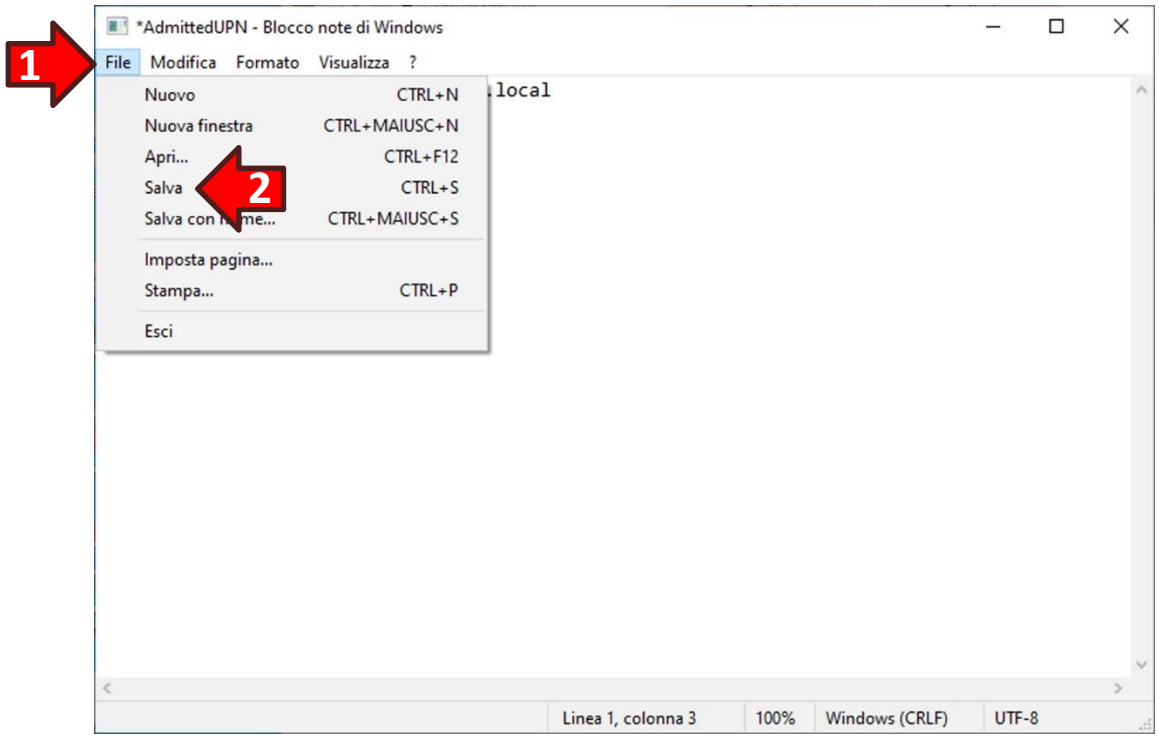


Si aprirà il Blocco Note con l'elenco delle identità digitali (UPN) abilitate all'accesso. Alla prima apertura l'elenco conterrà solamente l'UPN selezionato in fase di acquisto del VPS.

Aggiungere quindi gli UPN dei certificati client a cui si desidera consentire l'accesso (ogni nuovo UPN deve essere scritto su una riga distinta):



Per rendere subito effettivo il nuovo elenco cliccare sul menù **File (1)** in alto a sinistra della finestra e successivamente sull'opzione **Salva (2)**:



9.4 Accesso VPN da parte di più utenti

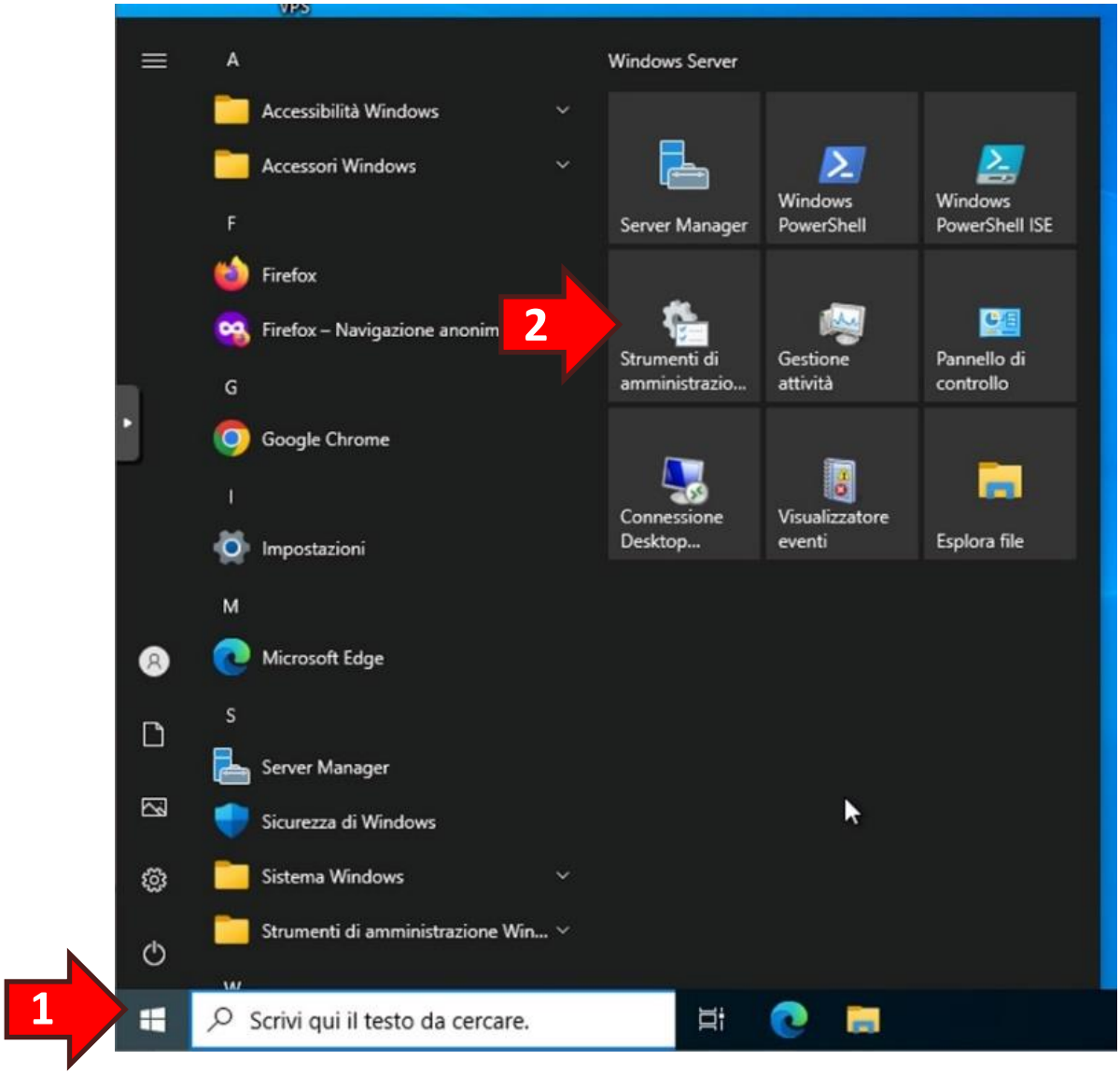
ATTENZIONE! Questa procedura può essere utilizzata solo se si è spuntata l'opzione Nome utente/Password in fase di acquisto del VPS.

Oltre a consentire l'accesso a più certificati client, come mostrato nel paragrafo precedente, è possibile consentire l'accesso a più utenti.

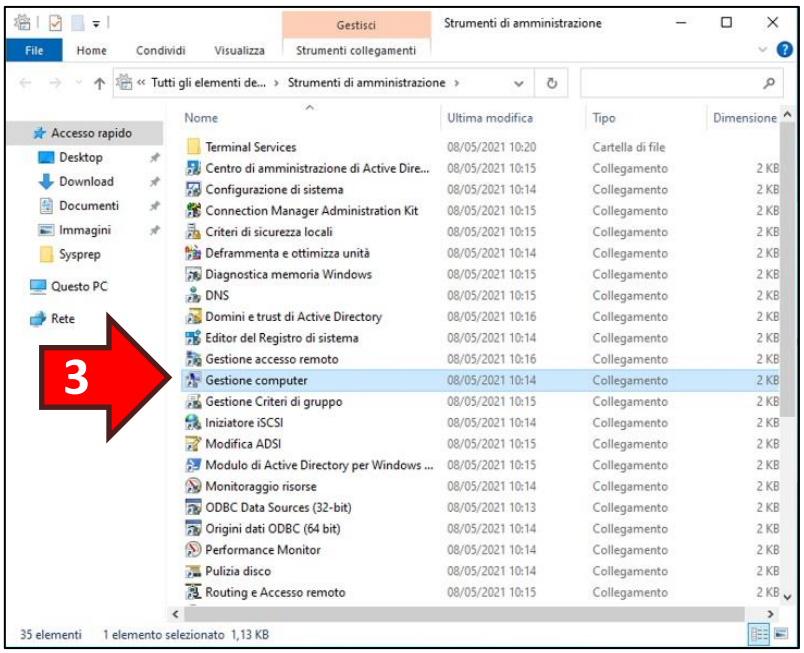
Il server OpenVPN utilizza la gestione degli utenti di Windows per discriminare o meno l'accesso.

ATTENZIONE! Perché un utente possa essere utilizzato dal server OpenVPN **è indispensabile** che nel nome sia presente il prefisso **VpnUser_** (es. VpnUser_Mattia).

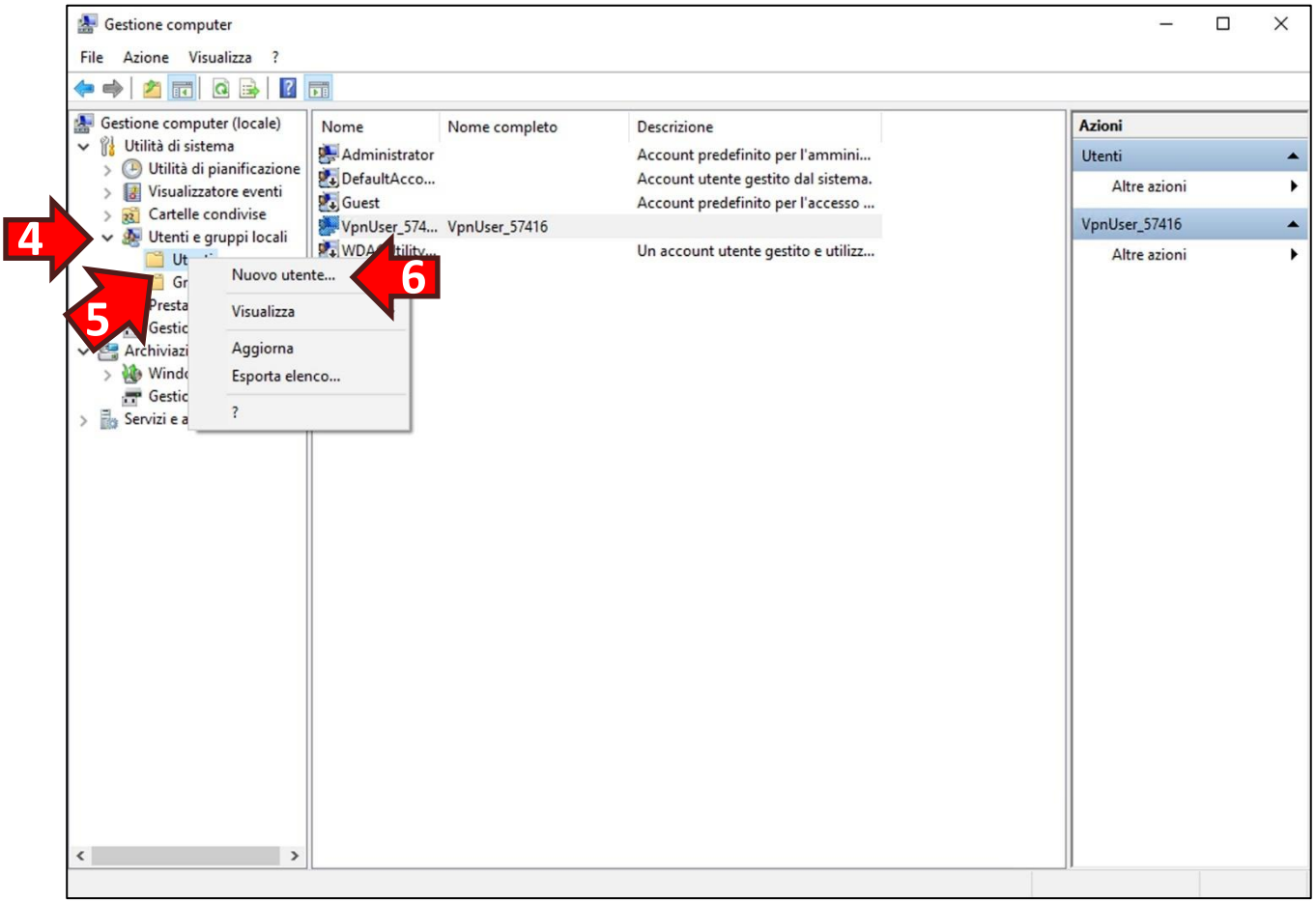
Per aggiungere un nuovo utente al server OpenVPN accedere al desktop del VPS, cliccare sul **Menù start (1)** e successivamente sull'icona **Strumenti di amministrazione (2)**:



Dalla finestra *Strumenti di amministrazione* fare doppio click su **Gestione computer (3)**:



Nella sezione a destra della finestra *Gestione computer* fare doppio click sull'opzione **Utenti e gruppi locali (4)** e poi cliccare con il tasto destro del mouse sul nodo **Utenti (5)**. Quindi dal menù pop-up selezionare l'opzione **Nuovo utente… (6)**:



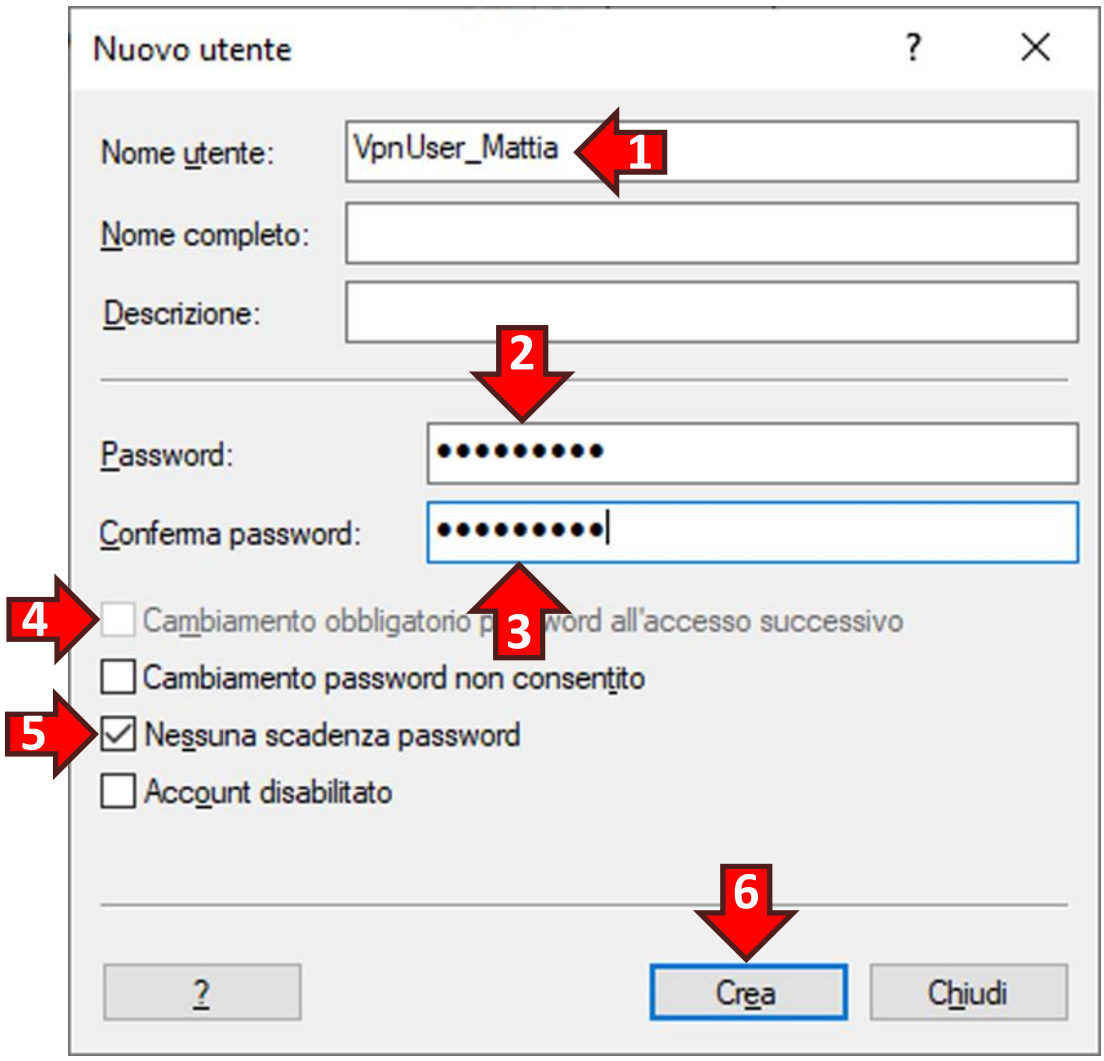
Nella finestra Nuovo utente digitare un **nome per l'utente (1)** ricordando di inserire il prefisso VpnUser_ (es. VpnUser_Mattia).

Creare una **password (2)** per l'utente facendo attenzione a digitare almeno una lettera maiuscola ed un numero (la password deve rispettare i criteri minimi di sicurezza imposti da Windows) e **confermarla nello spazio successivo (3)**.

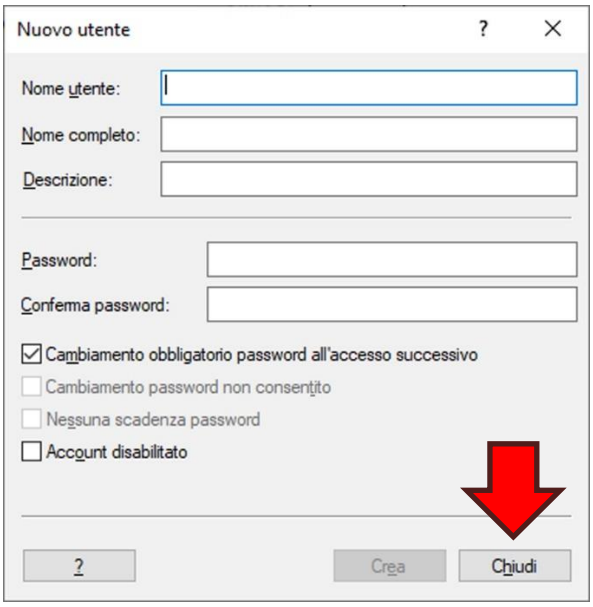
Rimuovere la spunta sull'opzione **Cambiamento obbligatorio password all'accesso successivo (4)**.

Inserire la spunta sull'opzione **Nessuna scadenza password (5)**.

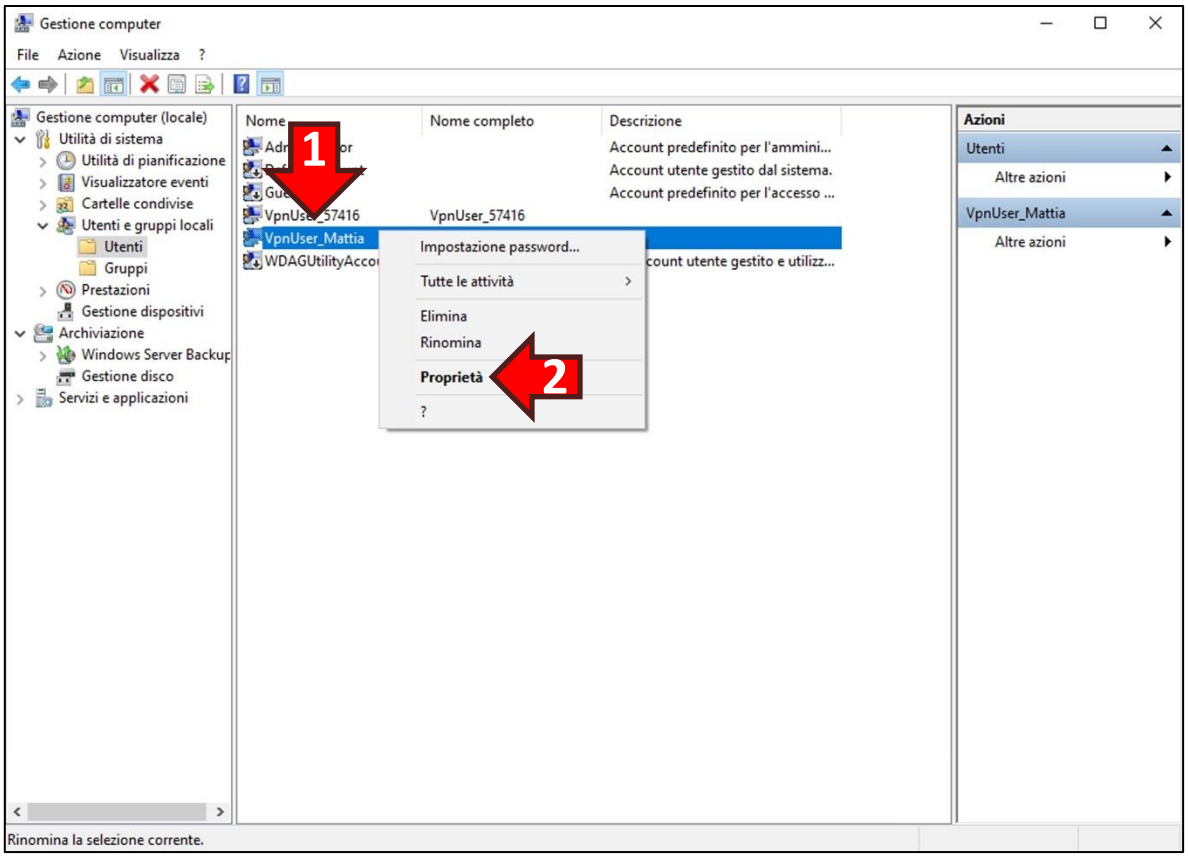
Infine cliccare il pulsante **Crea (6)** per creare l'utente:



Una volta creato l'utente i dati della finestra Nuovo utente verranno azzerati per permettere l'inserimento di più utenti in sequenza. Se non è necessario inserire ulteriori utenti cliccare il tasto **Chiudi**:



Per l'utente appena creato si consiglia la rimozione dei ruoli predefiniti in quanto non necessari all'accesso OpenVPN. Quindi dall'elenco al centro della finestra *Gestione computer* cliccare con il tasto destro del mouse sul nome dell'**utente appena creato (1)** e dal menù pop-up selezionare l'opzione **Proprietà (2)**:



Nelle proprietà dell'utente cliccare sulla scheda **Membro di (1)**. A quel punto cliccare sull'opzione **Users (2)** presente nell'elenco e cliccare il tasto **Rimuovi (3)**.

Qualora vi fossero ulteriori voci in elenco procedere alla loro rimozione selezionandole una ad una e rimuovendole con il tasto Rimuovi.

Quando l'elenco è vuoto cliccare il tasto **OK (4)**: