

Corretta installazione di Onyx Rip o Thrive

Di seguito è riportato un riepilogo del sistema seguito da informazioni più dettagliate sulle specifiche del sistema software ONYX.

Sistema operativo	Windows 11 Pro 64-Bit
Processore	Intel o AMD multi-core (10 cores minimo)
Memoria	32 GB minimo (64 raccomandato)
Disco	480 GB SSD minio (960 GB raccomandato per i dati)
Monitor	1280 x 1024 minimo
Hardware	Porte USB, Porte per stampanti, taglierine e dispositivi a colori
Internet	Internet disponibile per la licenza
Alimentazione	Impostazioni di alimentazione di Windows impostate su Prestazioni ottimali/elevate
Browser (ONYX Hub)	Chrome, Firefox, Edge, Safari (Ultima Versione)

ONYX non consiglia alcun software antivirus specifico, tuttavia alcuni sistemi operativi tra i quali Windows 10 o 11 hanno implementato sia un sistema Firewall che antivirus e questi devono essere configurati con eccezioni per le applicazioni ONYX e per le porte della stampante per consentire il corretto funzionamento e le massime prestazioni.

Quindi prima di installare Onyx assicurarsi che:

- L'antivirus sia disabilitato
- Il pc sia amministratore
- User Account Control (UAC) sia impostato al minimo

Questo esempio presuppone che il software ONYX sia installato su C:\ONYXThrive25\

Nessuno dei file eseguibili all'interno delle directory ONYX dovrebbe essere bloccato dall'antivirus.

Modificare le impostazioni antivirus per aggiungere eccezioni per singoli file di programma o l'intera directory di installazione.

Le impostazioni antivirus tipiche per consentire ai programmi sono denominate processi "a basso rischio" o "sicuri".

Il programma più importante sono:

Coda RIP - C:\ONYXThrive25\Server\postershop.exe

Media Manager - C:\ONYXThrive25\MediaManager\bin\ MediaManager.exe

Job Editor – C:\ONYXThrive25\Preflight\preflightLauncher.exe

Apppe: C:\ONYXThrive25\PDFRip\appeui.exe

Apppe EPS: C:\ONYXThrive25\PDFRip\ApppeNorm\appenormalizer.exe

Meglio disabilitare completamente la scansione della cartella di Onyx.

Anche i file del programma di licenza devono essere consentiti senza restrizioni:

C:\Windows\System32\hasplms.exe

Le cartelle utilizzate da ONYX dovrebbero disabilitare la scansione / monitoraggio antivirus.

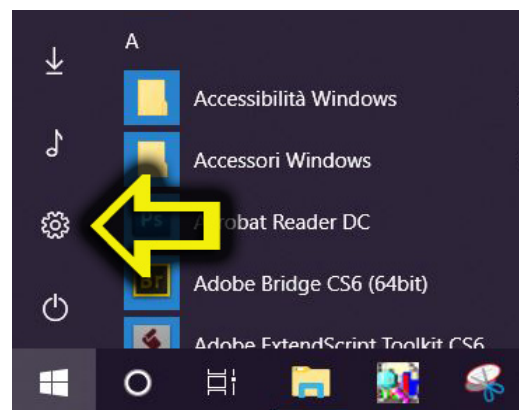
Tutte le cartelle nell'installazione ONYX (C:\ ONYXThrive25 e tutte le sottodirectory).

Le cartelle "di lavoro" specifiche della stampante potrebbero dover essere aggiunte come eccezioni separate se la cartella di lavoro per una stampante è stata configurata per essere al di fuori del percorso di installazione principale (C:\ONYXThrive25 nel nostro esempio).

Le comunicazioni di rete non possono essere bloccate da antivirus o firewall.

TCP/IP deve essere consentito sulle porte:

80, 515, 1947, 5093, 8085, 8086, 8090, 8889, 9100, 10000, 11110, 11111, 27017, 30651



Disabilitare ogni antivirus e **creare le nuove regole firewall**, su Windows seguire le immagini come indicato:

Impostazioni di Windows

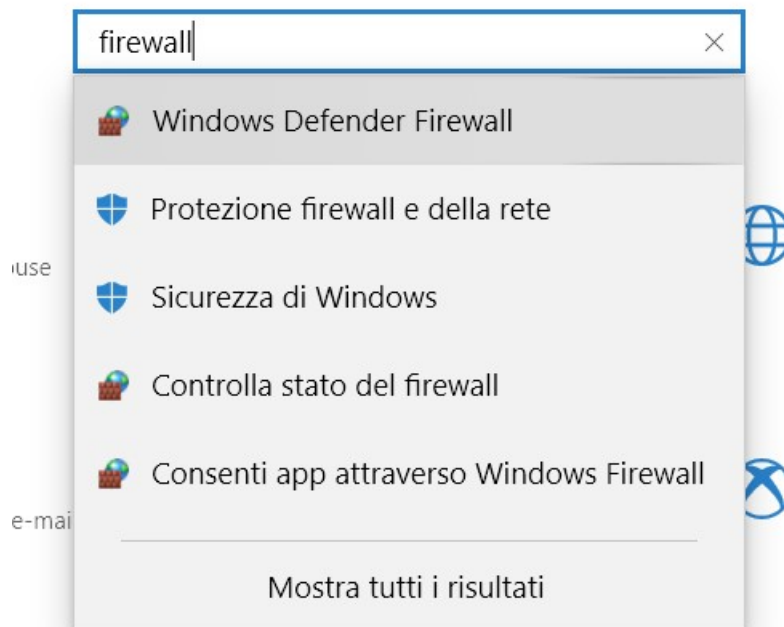


Figura 1: Nella casella di ricerca digitare Windows Firewall

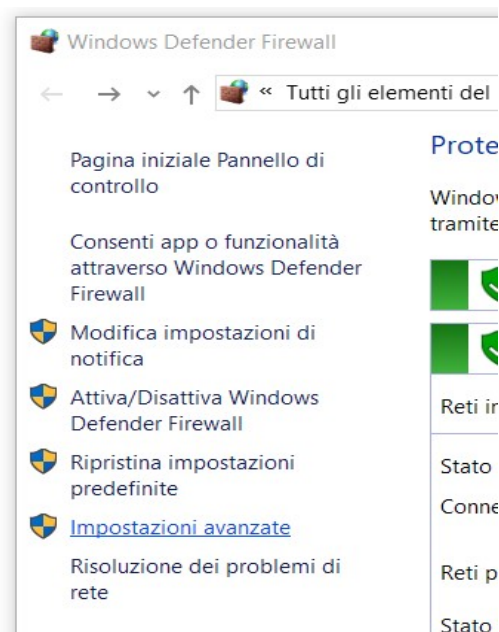


Figura 2: Selezionare impostazioni avanzate

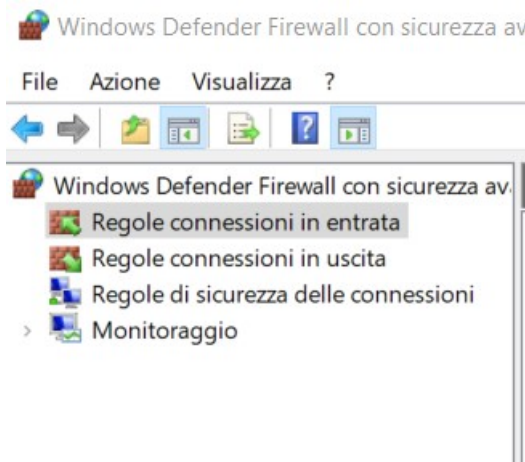


Figura 3: Creare una nuova regola in entrata



Figura 4: ...selezionando sulla destra "nuova regola"

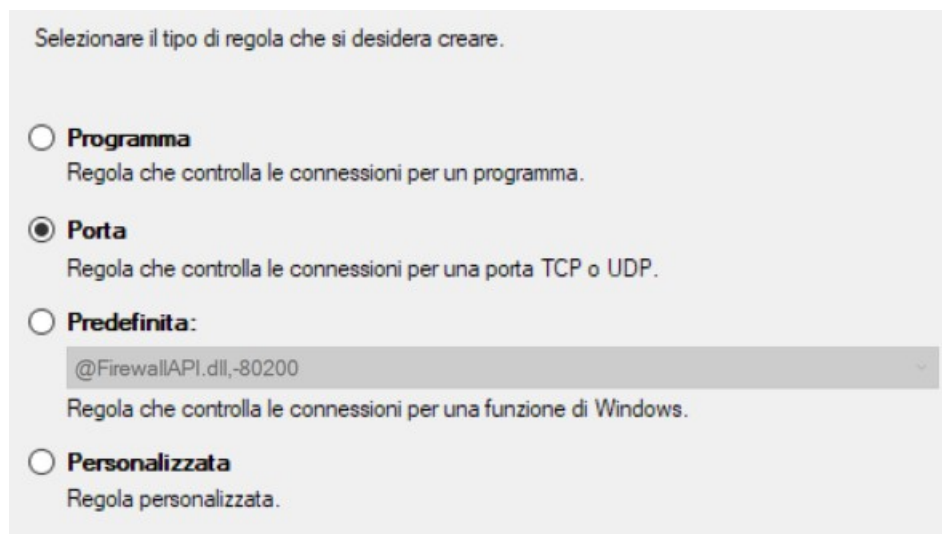


Figura 5: selezionare "porta"

Selezionare se applicare la regola al protocollo TCP o UDP.

☒ **TCP**
☐ **UDP**

Selezionare se applicare la regola a tutte le porte locali o a porte locali specifiche.

☐ **Tutte le porte locali**
☒ **Porte locali specifiche:**
Esempio: 80, 443, 5000-5010

Figura 6: inserire le porte (*fare riferimento alle porte come da pag. 2*) da aprire e premere avanti

Selezionare l'azione desiderata per le connessioni che soddisfano le condizioni specificate.

☒ **Consenti la connessione**
Include le connessioni protette con IPsec e quelle non protette.

☐ **Consenti solo connessioni protette**
Include solo le connessioni autenticate mediante IPsec. Le connessioni saranno protette con le impostazioni delle regole e proprietà IPsec nel nodo Regole di sicurezza delle connessioni.

☐ **Blocca la connessione**

Figura 7: consentire la connessione

Selezionare il tipo di applicazione della regola.

☒ **Dominio**
Regola applicabile ai computer connessi al rispettivo dominio aziendale.

☒ **Privato**
Regola applicabile ai computer connessi a un percorso di rete privato, come una rete domestica o la rete di un ufficio.

☒ **Pubblico**
Regola applicabile ai computer connessi ad un percorso di rete pubblico.

Figura 8: flaggare come indicato



Nome:
Onyx TCP

Descrizione (facoltativa):

Figura 9: Indicare il nome della regola

Ripetere lo stesso passaggio creando una nuova regola UDP, successivamente creare due nuove regole “in uscita” sia TCP che UDP.

Ora disattivare l’antivirus:

Impostazioni di Windows

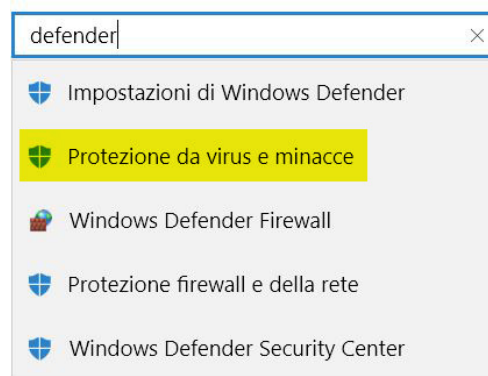


Figura 10: in impostazioni di Windows selezionare "Protezione da virus e minacce"

Protezione da virus e minacce

Visualizza la cronologia minacce, esegui un'analisi alla ricerca di virus e altre minacce, specifica le impostazioni di protezione e ottieni gli aggiornamenti della protezione.

Cronologia minacce

Ultima analisi: 11/04/2019 (analisi veloce)

0 51054

Minacce rilevate File analizzati

Avvia analisi

[Esegui una nuova analisi avanzata](#)

Impostazioni di Protezione da virus e minacce

Nessuna azione necessaria.

Aggiornamenti della protezione da virus e minacce

Le definizioni della protezione sono aggiornate.

Ultimo aggiornamento: 21:54 Lunedì 15 aprile 2019

Figura 11: selezionare "Impostazioni di Protezione da virus e minacce"

Protezione in tempo reale

Consente di individuare il malware e interromperne l'installazione o l'esecuzione nel tuo dispositivo. Puoi disattivare l'impostazione per un breve periodo prima che venga riattivata automaticamente.

La protezione in tempo reale è disattivata e il dispositivo è vulnerabile.

Disattivato

Protezione fornita dal cloud

Garantisce una protezione superiore e più veloce con l'accesso ai dati più recenti della protezione nel cloud. Per un funzionamento ottimale, l'invio automatico dei campioni deve essere attivato.

La protezione fornita dal cloud è disattivata e il dispositivo può essere vulnerabile. [Ignora](#)

Disattivato

[Informativa sulla privacy](#)

Invio automatico di file di esempio

Invia file di esempio a Microsoft per proteggere te stesso e gli altri dalle potenziali minacce. Verrà visualizzata una richiesta se il file necessario potrebbe contenere informazioni personali.

L'invio automatico di file di esempio è disattivato e il dispositivo può essere vulnerabile. [Ignora](#)

Disattivato

Figura 12: disattivare tutte le opzioni

Installazione di Onyx

- In caso di aggiornamento di una vecchia versione effettuare il backup delle stampanti (prninst), disinstallare il vecchio Onyx e pulire i registri di sistema (si può utilizzare Revo Uninstaller Portable che disinstalla e pulisce i registri in automatico).
- Installare l'ultima versione di Onyx.
- Installare i drivers delle stampanti. In caso di aggiornamento da vecchia versione, dopo aver reinstallato i prninst di backup, scaricare i nuovi driver tramite Printer-&-Profile-DL-Manager e aggiornare i vecchi drivers.

Aggiornare sempre la versione e i drivers stampanti

Configurare l'antivirus

Sconsigliamo vivamente l'utilizzo di ogni antivirus di terzi. Impostare le eccezioni di Windows Defender:

Esclusioni

Windows Defender Antivirus non analizzerà gli elementi che hai escluso.
Gli elementi esclusi potrebbero contenere minacce che rendono vulnerabile il dispositivo.

[Aggiungi o rimuovi esclusioni](#)

*Figura 13: sempre in "Protezione da virus e minacce",
selezionare "Aggiungi o rimuovi esclusioni"*

Esclusioni

Aggiungi o rimuovi elementi da escludere dalle analisi di Windows Defender Antivirus.

+ Aggiungi un'esclusione

C:\Thrive19\MediaManager\bin\MediaManager.exe
File

C:\Thrive19\PDFRip\AppeNorm\AppeNormalizer.exe
File

C:\Thrive19\PDFRip\appeui.exe
File

C:\Thrive19\Preflight\preflightLauncher.exe
File

C:\Thrive19\Server\PosterShop.exe
File

C:\Windows\System32\hasplms.exe
File

Riabilitare l'antivirus.

Condividere la cartella Input posizionata dentro la cartella di Onyx aggiungendo l'utente everyone con permesso di lettura e scrittura.

*Figura 14: Escludere i processi e la cartella
di Onyx – questa immagine è riferita a
Thrive 19 installato in C:*