

# Uso di Antivirus nelle installazioni eXtraWay

La presenza di un antivirus nelle installazioni della piattaforma eXtraWay può comportare due distinti ordini di problemi: di natura prestazionale e di natura funzionale.

## Aspetto Prestazionale

I software antivirus più diffusi eseguono scansioni "Real-time" sul sistema operativo e sui processi. Può accadere quindi che scansioni e blocchi troppo invasivi rallentino o fermino del tutto i componenti Tomcat (applicativo) o eXtraWay (motore del database).

## Aspetto Funzionale

E' prassi comune che gli antivirus riconoscano come comportamento rischioso, potenzialmente maligno, uno dei comportamenti del server eXtraWay. Per ovviare a quest'inconveniente è necessario agire sulle impostazioni dell'antivirus.

## Esclusioni

Per poter utilizzare comunque il software antivirus è necessario impostare una o più liste di esclusione: esistono principalmente 2 tipi di lista a seconda del software utilizzato. Esse si riferiscono ai files/cartelle delle quali non si richiede che venga compiuta verifica e l'elenco degli eseguibili che possono essere considerati affidabili.

## Interventi di tipo prestazionale

E' evidente come l'attività di un antivirus non possa essere priva di impatti sulle prestazioni dell'intero sistema. In particolare, gran parte degli antivirus operano in tempo reale ed intercettano, per così dire, tutte le operazioni di lettura e scrittura che hanno luogo sui dischi. Ciò comporta un naturale rallentamento di tali processi.

Per non incorrere in limitazioni prestazionali, ed in generale considerando la natura dei dati scritti da eXtraWay, gli antivirus possono (e dovrebbero) essere configurati per ignorare l'attività afferente alle cartelle che ospitano i dati, gli indici e le registrazioni di servizio<sup>1)</sup>

### Lista esclusioni per cartelle

E' necessario impostare come esclusione la cartella del database, la cartella degli eseguibili e le cartelle dei file temporanei:

Cartella	Contenuto
\3di.it\extraway\xw\db	Cartella database eXtraWay
\3di.it\extraway\xw\bin	Cartella eseguibili eXtraWay
\3di.it\extraway\xw\logs	Cartella logs eXtraWay
\3di.it\extraway\xw\xreg	Dove presente, cartella di servizio per il registro di eXtraWay
\3di.it\extraway\xw\lazy	Dove presente, cartella di servizio per le attività <i>near on line</i> di eXtraWay
\Programmi\Apache Software Foundation\Tomcat 6.0\bin	Cartella eseguibili Apache Tomcat
\Programmi\Apache Software Foundation\Tomcat 6.0\work	Cartella cache Tomcat
%temp%\hwtemp	Cartella file temporanei di eXtraWay

La cartella %temp% solitamente corrisponde a \windows\temp ma dipende direttamente dall'impostazione della variabile di sistema Windows.

## Interventi di tipo Funzionale

Come precedentemente annunciato un comportamento del modulo eXtraWay Server viene considerato malevolo dalla maggioranza degli antivirus.

L'architettura di eXtraWay Server prevede che esista un'istanza del modulo in ascolto per nuove connessioni. Quando un'applicazione client richiede una nuova connessione il server in ascolto, detto *Master*, duplica se stesso producendo una copia figlia, detta *Slave*, che di fatto instaura la connessione con l'applicazione client e ne esegue le richieste.

Il processo così generato eredita dal processo principale alcune risorse condivise.

Un simile comportamento viene considerato pericoloso in quanto rappresenta uno dei più comuni sistemi che hanno i virus per avviare processi in grado di produrre danni e/o appropriarsi di importanti informazioni presenti nel sistema.

Per ovviare a questo bisogna necessariamente istruire il sistema antivirus perché consideri eXtraWay Server come processo affidabile, quindi *trusted*, e non ne impedisca il corretto comportamento.

### Lista esclusioni per eseguibili

E' necessario impostare come esclusione l'eseguibile di eXtraWay e l'eseguibile di Tomcat

Modulo
\3di.it\extraway\xw\bin\xw.exe
\Programmi\Apache Software Foundation\Tomcat 6.0\bin\tomcat6.exe

*I percorsi in entrambe le liste possono variare a seconda delle installazioni, tuttavia è possibile recuperare l'esatta posizione controllando nelle proprietà dei servizi di Windows.*



## Configurazioni antivirus già testate con eXtraWay

Nel corso del tempo sono state verificate diverse installazioni nelle quali è stato possibile compiere con successo gli interventi descritti nei capitoli precedenti.

Dal momento che ogni software antivirus ha propria configurazione e che essi evolvono naturalmente nel tempo, non viene descritto in questa sede il procedimento da seguire rimandando il dettaglio alla documentazione degli stessi.

### Antivirus efficacemente verificati:

- Norton Antivirus
- NOD32 (Versione esistente al 2010)
- Kaspersky Anti-Virus

Va altresì detto che qualora un antivirus imponga limiti funzionali ma senza dare la possibilità di compilare liste di esclusione, esso risulta di fatto incompatibile con le installazioni eXtraWay.

Allo stato attuale risultano

### Antivirus incompatibili:

- Panda Antivirus Titanium 2004

---

**N.B.:** Gli elenchi riportati sono da considerarsi meramente indicativi e non esaustivi. 3D Informatica non può considerarsi responsabile qualora nuove versioni di antivirus verificati risultassero incompatibili ne può garantire che nuove versioni degli antivirus noti come incompatibili risultino di fatto utilizzabili.  
Chi fosse intenzionato ad acquisire un software antivirus per proteggere le proprie installazioni eXtraWay dovrà, sotto la propria responsabilità, raccogliere informazioni sufficienti per garantirsi la possibilità di sottoporre a tale software liste di esclusioni quanto meno per gli aspetti funzionali.

1)

Quali, ad esempio, le cartelle dei logs etc. etc.