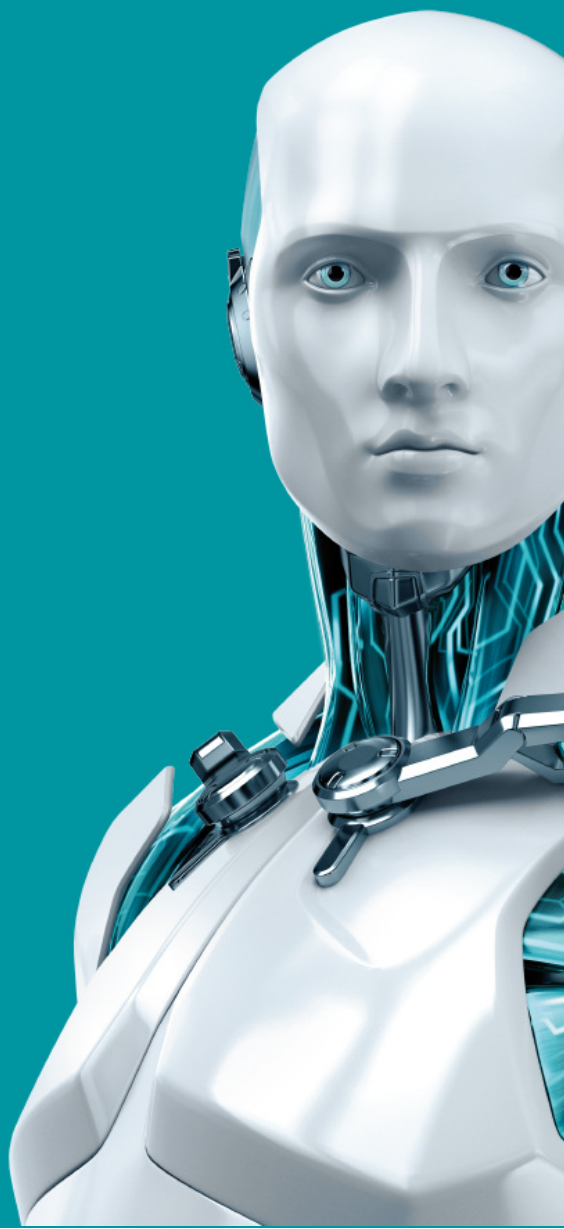
NOD32® ANTIVIRUS

Manuale dell'utente

(per la versione 11.0 e le versioni successive del prodotto)

Microsoft® Windows® 10 / 8.1 / 8 / 7 / Vista / Home Server 2011

Fare clic qui per scaricare la versione più recente di questo documento



ENJOY SAFER TECHNOLOGY™

ESET NOD32 ANTIVIRUS

Assistenza clienti nel mondo: www.eset.it/supporto

REV. 20/11/2017

Contenuti

1. ESET NOD32 Antivirus

ESET NOD32 Antivirus rappresenta un nuovo approccio alla protezione effettivamente integrata del computer. La versione più recente del motore di controllo ESET LiveGrid® sfrutta la velocità e la precisione per proteggere il computer dell'utente. Il risultato è un sistema intelligente che rileva continuamente attacchi e software dannoso che potrebbero minacciare il computer.

ESET NOD32 Antivirus è una soluzione di protezione completa che associa massime prestazioni a un impatto minimo sul sistema. Le tecnologie avanzate utilizzano l'intelligenza artificiale per prevenire l'infiltrazione da parte di virus, spyware, trojan horse, worm, adware, rootkit e altre minacce senza ripercussioni sulle prestazioni del sistema o interruzioni del computer.

Funzioni e vantaggi

Interfaccia utente rinnovata	L'interfaccia utente di questa versione è stata notevolmente migliorata e semplificata a seguito dei risultati dei test di usabilità. Tutti i termini e le notifiche dell'interfaccia grafica utente sono stati accuratamente rivisti e l'interfaccia offre ora il supporto per le lingue scritte da destra a sinistra quali l'ebraico e l'arabo. **La Guida online** è ora integrata in ESET NOD32 Antivirus e offre contenuti di supporto aggiornati a livello dinamico.
Antivirus e antispyware	Rileva e pulisce in modo proattivo virus, worm, trojan e rootkit noti e sconosciuti. L'**Euristica avanzata** rileva persino malware mai rilevati in precedenza, proteggendo l'utente da minacce sconosciute e neutralizzandole prima che possano arrecare danni al sistema. La **Protezione accesso Web** e **Anti-Phishing** monitora la comunicazione tra i browser Web e i server remoti (compreso il protocollo SSL). La **Protezione client di posta** garantisce il controllo delle comunicazioni via e-mail ricevute mediante i protocolli POP3(S) e IMAP(S).
Aggiornamenti periodici	L'aggiornamento periodico del motore di rilevamento (precedentemente noto con il nome di "database delle firme antivirali") e dei moduli del programma rappresenta la soluzione migliore per ottenere il livello massimo di protezione del computer.
ESET LiveGrid® (Reputazione basata sul cloud)	È possibile controllare la reputazione dei processi e dei file in esecuzione direttamente da ESET NOD32 Antivirus.
Controllo dispositivo	Controlla automaticamente tutte le memorie USB, le schede di memoria e i CD/DVD. Blocca i supporti rimovibili in base al tipo di supporto, al produttore, alle dimensioni e ad altri attributi.
Funzionalità HIPS	È possibile personalizzare il comportamento del sistema in maggiori dettagli, specificando le regole per il registro di sistema, i processi e i programmi attivi e ottimizzando il livello di protezione.
Modalità giocatore	Rimanda tutte le finestre popup, gli aggiornamenti o altre attività di sistema intensive allo scopo di preservare le risorse di sistema per le attività di gioco e altre attività a schermo intero.

Affinché le funzioni di ESET NOD32 Antivirus siano attive, è necessario attivare una licenza. Si consiglia di rinnovare la licenza di ESET NOD32 Antivirus alcune settimane prima della scadenza.

1.1 Novità di questa versione

La nuova versione di ESET NOD32 Antivirus prevede i seguenti miglioramenti:

- **Protezione contro gli attacchi basati su script**: protegge in modo proattivo da attacchi dinamici basati su script e con vettori di attacco non tradizionali. Per ulteriori informazioni, fare clic qui.
- **Prestazioni elevate e impatto limitato sul sistema**: questa versione è progettata per un uso efficiente delle risorse di sistema, tutelando le prestazioni del computer e mantenendo la difesa contro i nuovi tipi di minacce.
- **Compatibilità con Windows 10**: ESET è pienamente compatibile con Microsoft Windows 10.
- **JAWS**: ESET NOD32 Antivirus supporta l'utilità per la lettura dello schermo più popolare JAWS.
- **Controllo trascina e rilascia**: è possibile controllare manualmente un file o una cartella spostando semplicemente uno dei due elementi nell'area contrassegnata.
- ESET NOD32 Antivirus informerà l'utente in caso di connessione a una rete wireless non protetta o a una rete con protezione vulnerabile.

Per ulteriori informazioni sulle nuove funzionalità di ESET NOD32 Antivirus, consultare il seguente articolo della Knowledge base di ESET:
Novità di questa versione dei prodotti ESET Home

1.2 Quale è il mio prodotto?

ESET offre diversi livelli di sicurezza con nuovi prodotti che spaziano dalla potente e rapida soluzione antivirus alla soluzione all-in-one per la sicurezza con un impatto minimo sul sistema:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**

Per determinare quale prodotto è installato aprire la finestra principale del programma (vedere l'articolo di knowledgebase) e sarà possibile leggere il nome del prodotto nella parte superiore della finestra (intestazione).

La tabella in basso riepiloga in dettaglio le funzionalità disponibili per ogni prodotto specifico.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Antivirus	✔	✔	✔
Antispyware	✔	✔	✔
Exploit Blocker	✔	✔	✔
Protezione contro attacchi basati su script	✔	✔	✔
Anti-Phishing	✔	✔	✔
Protezione accesso Web	✔	✔	✔
HIPS (compresa la **protezione anti-ransomware**)	✔	✔	✔
Antispam		✔	✔
Firewall		✔	✔
Protezione rete domestica		✔	✔
Protezione webcam		✔	✔
Protezione contro gli attacchi di rete		✔	✔

Protezione Botnet		✔	✔
Protezione siti Web di banche e di sistemi di pagamento		✔	✔
Controllo accessi		✔	✔
Anti-Furto		✔	✔
ESET Password Manager			✔
ESET Secure Data			✔

NOTA
Alcuni prodotti indicati in precedenza potrebbero non essere disponibili per tutte le lingue/le regioni.

1.3 Requisiti di sistema

Il sistema deve rispettare i seguenti requisiti hardware e software per un funzionamento ottimale di ESET NOD32 Antivirus:

Processori supportati

Intel® o AMD x86-x64

Sistemi operativi supportati

Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7
Microsoft® Windows® Vista
Microsoft® Windows® Home Server 2011 64-bit

1.4 Prevenzione

Quando si utilizza il computer, e in particolare quando si naviga in Internet, occorre tenere presente che nessun sistema antivirus al mondo può eliminare completamente il rischio di infiltrazioni e attacchi. Per garantire la massima protezione e comodità, è essenziale utilizzare correttamente la soluzione antivirus e attenersi ad alcune regole utili:

Eseguire regolarmente l'aggiornamento

In base alle statistiche ottenute da ThreatSense, ogni giorno vengono create migliaia di infiltrazioni nuove e uniche per aggirare le misure di sicurezza esistenti e generare profitti per i rispettivi autori, a spese di altri utenti. Gli specialisti del laboratorio di ricerca ESET analizzano queste minacce su base giornaliera, preparando e rilasciando gli aggiornamenti per migliorare costantemente il livello di protezione degli utenti. Per garantire l'efficacia massima di questi aggiornamenti, è importante che questi vengano configurati correttamente sul sistema. Per ulteriori informazioni su come configurare gli aggiornamenti, consultare il capitolo Impostazione dell'aggiornamento.

Scaricare le patch di protezione

Gli autori di software dannoso sfruttano spesso le varie vulnerabilità dei sistemi per aumentare l'efficacia della diffusione di codice dannoso. In considerazione di ciò, le società di software esaminano attentamente eventuali vulnerabilità nelle applicazioni create e rilasciano regolarmente gli aggiornamenti di protezione allo scopo di eliminare le potenziali minacce. È importante scaricare questi aggiornamenti della protezione non appena vengono rilasciati. Microsoft Windows e i Web browser quali Internet Explorer sono due esempi di programmi per cui gli aggiornamenti di protezione vengono rilasciati periodicamente.

Eseguire il backup dei dati importanti

Di norma, gli autori di malware non sono interessati alle esigenze degli utenti e l'attività dei programmi dannosi comporta spesso un malfunzionamento generale del sistema operativo e la perdita di dati importanti. È importante

eseguire un backup periodico dei dati importanti e sensibili su un supporto esterno, ad esempio un DVD o un'unità hard disk esterna. Ciò consente di recuperare i dati in modo semplice e veloce in caso di errore del sistema.

Eseguire regolarmente la scansione antivirus

Il rilevamento di virus, worm, trojan e rootkit più noti e sconosciuti è gestito dal modulo della protezione file system in tempo reale. Ciò significa che ad ogni accesso ad un file o apertura dello stesso da parte dell'utente, questo viene controllato per la ricerca di attività malware. Si consiglia di eseguire un Controllo del computer completo almeno una volta al mese, in quanto le firme dei malware cambiano continuamente e il motore di rilevamento si aggiorna con frequenza giornaliera.

Seguire le regole di protezione di base

Questa è la regola più utile e più efficace di tutte: essere sempre prudenti. Oggi, molte infiltrazioni richiedono l'intervento dell'utente affinché possano essere eseguite e distribuite. Adottando un comportamento prudente all'apertura di nuovi file, non sarà più necessario perdere tempo ed energie per pulire le infiltrazioni. Seguono alcune linee guida utili:

- Non visitare siti Web sospetti, con molte finestre popup e pubblicità che attirano l'attenzione.
- Prestare attenzione durante l'installazione di programmi freeware, pacchetti codec e così via. Utilizzare solo programmi sicuri e visitare solo siti Web Internet sicuri.
- Essere prudenti quando si aprono gli allegati e-mail, in particolare quelli inviati da programmi massmailer a destinatari multipli e quelli inviati da mittenti sconosciuti.
- Non utilizzare un account Amministratore per eseguire le attività quotidiane sul computer.

2. Installazione

Esistono vari metodi di installazione di ESET NOD32 Antivirus sul computer. I metodi di installazione possono variare in base al Paese e ai mezzi di distribuzione:

- Live installer può essere scaricato dal sito Web ESET. Il pacchetto di installazione è universale per tutte le lingue (scegliere la lingua desiderata). Di per sé, il Live installer è un file di piccole dimensioni; i file aggiuntivi necessari per l'installazione di ESET NOD32 Antivirus verranno scaricati automaticamente.

- Installazione off-line: questo tipo di installazione viene utilizzato per le installazioni mediante il CD/DVD di un prodotto. Questa installazione utilizza un file *.exe* più grande rispetto al file Live installer e non richiede una connessione a Internet o file aggiuntivi per il completamento del processo.

IMPORTANTE
Verificare che nel computer non siano installati altri programmi antivirus prima dell'installazione di ESET NOD32 Antivirus. Se su un singolo computer sono installate due o più soluzioni antivirus, potrebbero entrare in conflitto tra loro. È consigliabile disinstallare gli altri programmi antivirus presenti nel sistema. Per un elenco degli strumenti di disinstallazione dei software antivirus comuni, consultare l'articolo della Knowledge Base ESET (disponibile in inglese e in altre lingue).

2.1 Live installer

Dopo aver scaricato il pacchetto di installazione *Live installer*, fare doppio clic sul file di installazione e seguire le istruzioni dettagliate nella finestra del programma di installazione.

IMPORTANTE
per questo tipo di installazione, è necessario effettuare la connessione a Internet.

Selezionare la lingua desiderata dal menu a discesa e fare clic su **Continua**. Attendere alcuni istanti per il download dei file di installazione.

Dopo aver accettato l'**Accordo di licenza per l'utente finale**, all'utente verrà richiesto di configurare **ESET LiveGrid®** e il **rilevamento di applicazioni potenzialmente indesiderate**. ESET LiveGrid® garantisce il costante e immediato aggiornamento di ESET sulle nuove minacce allo scopo di proteggere gli utenti. Il sistema consente l'invio di nuove minacce al laboratorio di ricerca ESET, dove i virus verranno analizzati, elaborati e aggiunti al motore di rilevamento.

Per impostazione predefinita, è selezionato **Attiva il sistema di feedback ESET LiveGrid® (scelta consigliata)**, che attiverà questa funzione.

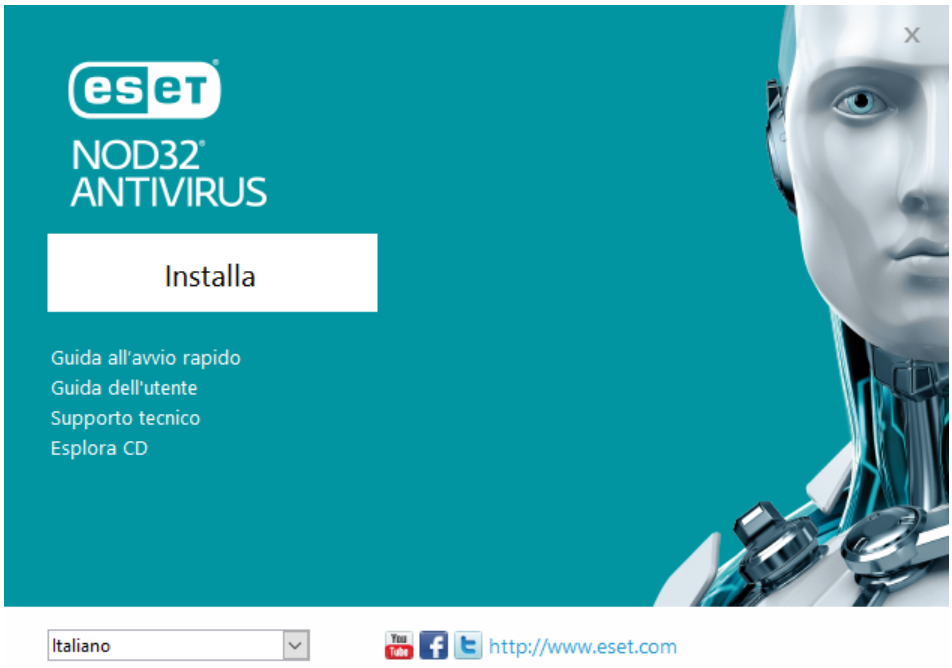
Il passaggio successivo del processo di installazione consiste nella configurazione dell'opzione di rilevamento delle applicazioni potenzialmente indesiderate. Le applicazioni potenzialmente indesiderate non sono necessariamente dannose. Tuttavia, potrebbero influire negativamente sul comportamento del sistema operativo. Per ulteriori informazioni, consultare il capitolo Applicazioni potenzialmente indesiderate.

Fare clic su **Installa** per avviare il processo di installazione. L'operazione potrebbe richiedere qualche minuto. Fare clic su **Fatto** per completare la configurazione del prodotto e avviare il processo di attivazione.

NOTA
Se si è in possesso di una licenza che consente di installare altre versioni di un prodotto, è possibile selezionare il prodotto in base alle proprie preferenze. Per ulteriori informazioni sulle funzioni di ciacun prodotto specifico, fare clic qui.

2.2 Installazione off-line

Dopo aver avviato il pacchetto di installazione off-line (.exe), la procedura di installazione guidata condurrà l'utente attraverso il processo di configurazione.



Selezionare la lingua desiderata dal menu a discesa e fare clic su **Continua**. Attendere alcuni istanti per il download dei file di installazione.

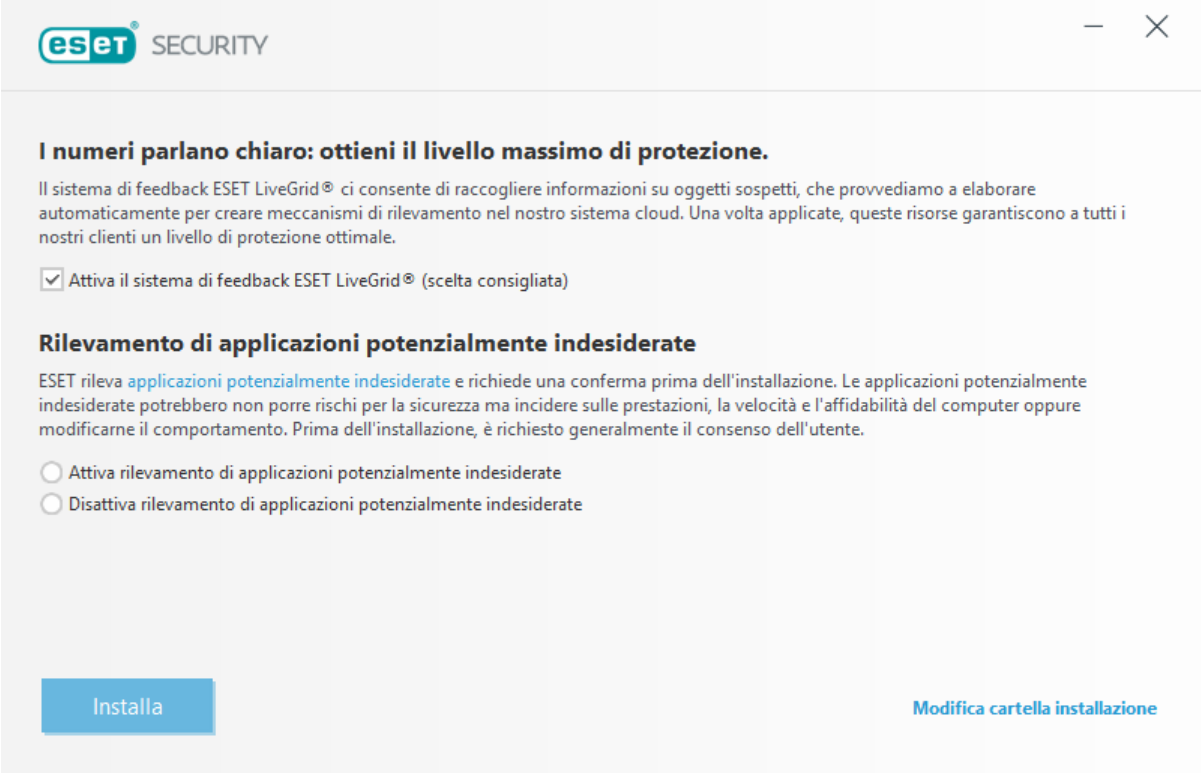
Dopo aver accettato l'**Accordo di licenza per l'utente finale**, all'utente verrà richiesto di **Inserire una chiave di licenza** o **Utilizzare License Manager**.

Se non si possiede una licenza, selezionare **Prova gratuita** per provare il prodotto ESET per un periodo di tempo limitato oppure **Acquista licenza**. In alternativa, è possibile selezionare **Salta attivazione** per procedere con l'installazione senza attivazione. All'utente verrà richiesto di inserire una chiave di licenza in un secondo momento.

2.2.1 Inserire una chiave di licenza

La procedura di installazione guidata seleziona il prodotto da installare in base alla chiave di licenza e consente di visualizzare il nome del prodotto durante l'installazione. Per visualizzare un elenco di prodotti che possono essere attivati con la licenza, fare clic su **Cambia prodotto**. Per ulteriori informazioni sulle funzioni di ciascun prodotto specifico, fare clic qui.

Fare clic su **Continua** e selezionare le impostazioni desiderate per **ESET LiveGrid®** e il **rilevamento di applicazioni potenzialmente indesiderate**. ESET LiveGrid® garantisce il costante e immediato aggiornamento di ESET sulle nuove minacce allo scopo di proteggere gli utenti. Il sistema consente l'invio di nuove minacce al laboratorio di ricerca ESET, dove i virus verranno analizzati, elaborati e aggiunti al motore di rilevamento. Le **Applicazioni potenzialmente indesiderate** non sono necessariamente dannose. Tuttavia, potrebbero influire negativamente sul comportamento del sistema operativo. Per ulteriori informazioni, consultare il capitolo Applicazioni potenzialmente indesiderate.



Fare clic su **Installa** per avviare il processo di installazione. L'operazione potrebbe richiedere qualche minuto. Fare clic su **Fatto** per completare la configurazione del prodotto e avviare il processo di attivazione.

NOTA
Se si è in possesso di una licenza che consente di selezionare vari prodotti, è possibile installare un prodotto in base alle proprie preferenze. Per ulteriori informazioni sulle funzioni di ciascun prodotto specifico, fare clic qui.

Per ulteriori informazioni sui passaggi di installazione, **ESET LiveGrid®** e **Rilevamento di applicazioni potenzialmente indesiderate**, seguire le istruzioni fornite nella sezione "Live installer".

2.2.2 Usa License Manager

Dopo aver selezionato **Usa License Manager**, all'utente verranno richieste le credenziali di my.eset.com in una nuova finestra. Inserire le credenziali di my.eset.com e fare clic su **Accedi** per utilizzare una licenza in License Manager. Scegliere una licenza per l'attivazione e fare clic su **Continua** per attivare ESET NOD32 Antivirus.

NOTA
Se non si possiede un account my.eset.com, effettuare la registrazione facendo clic sul pulsante **Crea account**.

NOTA
Se si dimentica la password, fare clic su **Ho dimenticato la password** e seguire la procedura contenuta nella pagina Web alla quale si è reindirizzati.

ESET License Manager aiuta gli utenti a gestire tutte le licenze ESET. È possibile rinnovare, aggiornare o estendere in modo pratico la licenza e visualizzarne i dettagli importanti. Inserire dapprima la chiave di licenza. A questo punto, sarà possibile visualizzare il prodotto, il dispositivo associato, il numero di licenze disponibili e la data di scadenza. È possibile disattivare o rinominare dispositivi specifici. Facendo clic su **Estendi**, si verrà reindirizzati a un negozio on-line in cui è possibile confermare l'acquisto e acquistare il rinnovo.

Se si desidera effettuare l'aggiornamento della licenza (per esempio da ESET NOD32 Antivirus a ESET Smart Security Premium) o installare un prodotto di protezione ESET su un altro dispositivo, si verrà reindirizzati al negozio on-line per completare l'acquisto.

In ESET License Manager è anche possibile aggiungere varie licenze, scaricare prodotti sui dispositivi o condividere licenze tramite e-mail.

2.2.3 Impostazioni avanzate

Dopo aver selezionato **Modifica cartella installazione**, all'utente verrà richiesto di selezionare un percorso per l'installazione. Per impostazione predefinita, il programma viene installato nella directory seguente:

C:\Programmi\ESET\ESET NOD32 Antivirus

Scegliere **Sfoglia** per selezionare un percorso diverso (scelta non consigliata).

Per completare i successivi passaggi di installazione, **ESET LiveGrid®** e **Rilevamento di applicazioni potenzialmente indesiderate**, seguire le istruzioni nella sezione Live Installer (vedere "Live installer").

Fare clic su **Continua**, quindi su **Installa** per completare l'installazione.

2.3 Problemi di installazione comuni

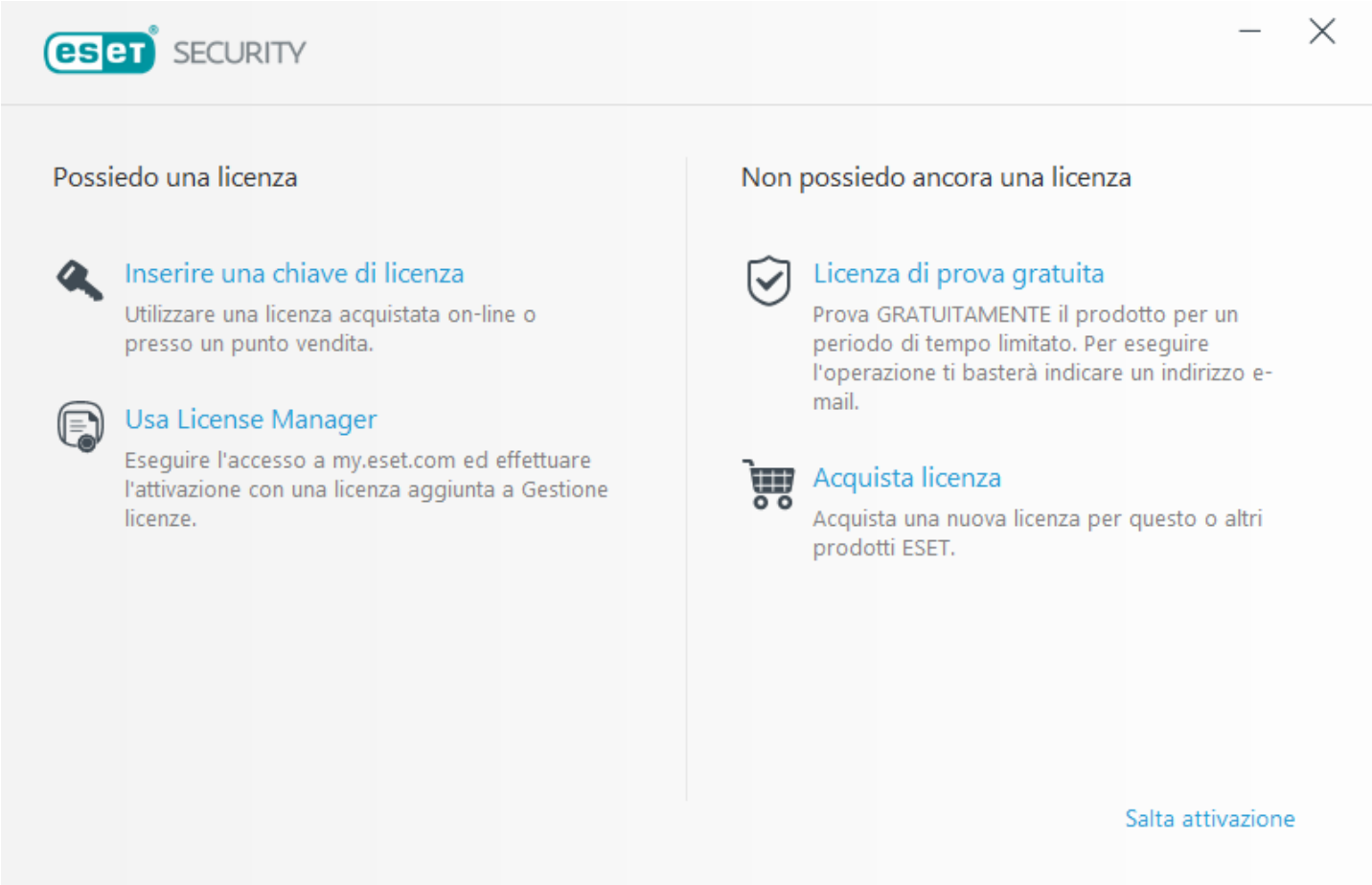
Se durante l'installazione si verificano problemi, consultare l'elenco di errori di installazione comuni e risoluzioni per trovare una soluzione al problema.

2.4 Attivazione prodotto

Al termine dell'installazione, all'utente verrà richiesto di attivare il prodotto.

Sono disponibili vari metodi per attivare il prodotto. La disponibilità di uno scenario di attivazione specifico nella finestra di attivazione potrebbe variare in base al Paese e ai mezzi di distribuzione (CD/DVD, pagina Web ESET, ecc.).

- Se è stata acquistata una versione presso un rivenditore al dettaglio del prodotto, attivare il prodotto tramite una **Chiave di licenza**. La chiave di licenza si trova generalmente all'interno o sul retro della confezione del prodotto. Per eseguire correttamente l'attivazione, è necessario inserire la chiave di licenza così come fornita. Chiave di licenza: stringa univoca nel formato XXXX-XXXX-XXXX-XXXX-XXXX o XXXX-XXXXXXXX, utilizzata per l'identificazione del proprietario della licenza e per l'attivazione della licenza.
- Se si desidera provare ESET NOD32 Antivirus prima di acquistarlo, selezionare **Licenza di prova gratuita**. Inserire l'indirizzo e-mail e il Paese per attivare ESET NOD32 Antivirus per un periodo di tempo limitato. La licenza di prova verrà inviata all'indirizzo indicato dall'utente. È possibile attivare una sola licenza di prova per cliente.
- Qualora non si disponga di una licenza e si desideri acquistarne una, fare clic su Acquista licenza. In tal modo si verrà reindirizzati al sito Web o al distributore locale ESET.



2.5 Inserimento della chiave di licenza

Gli aggiornamenti automatici sono importanti per la sicurezza. ESET NOD32 Antivirus riceverà gli aggiornamenti solo dopo l'attivazione tramite la **Chiave di licenza**.

Se non si inserisce la chiave di licenza dopo l'installazione, il prodotto non sarà attivato. La licenza può essere modificata dalla finestra principale del programma. Per fare ciò, fare clic su **Guida e supporto tecnico** > **Attiva licenza** e inserire i dati di licenza ricevuti insieme al prodotto di protezione ESET nella finestra Attivazione prodotto.

Quando si immette la **Chiave di licenza**, è importante immetterla esattamente come è scritta:

- La chiave di licenza è una stringa univoca nel formato XXXX-XXXX-XXXX-XXXX-XXXX, utilizzata per l'identificazione del proprietario della licenza e per l'attivazione della stessa.

Per evitare errori, si consiglia di copiare e incollare la chiave di licenza dal messaggio e-mail di registrazione.

2.6 Aggiornamento a una versione più recente

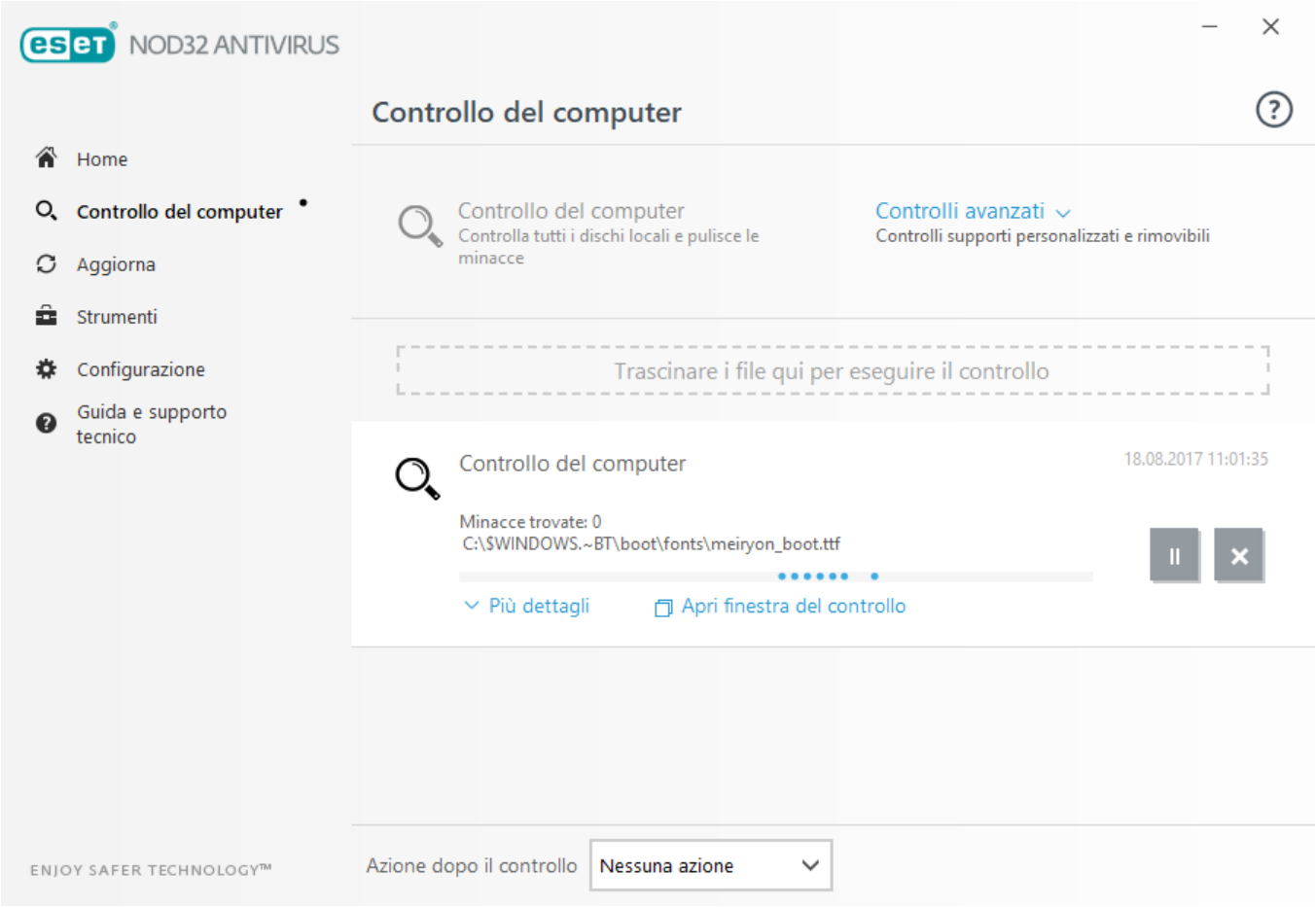
Le nuove versioni di ESET NOD32 Antivirus vengono rilasciate ai fini dell'implementazione di miglioramenti o della correzione di errori che non è possibile risolvere mediante aggiornamenti automatici dei moduli del programma. L'aggiornamento a una versione più recente può essere eseguito in diversi modi:

1. Automaticamente tramite un aggiornamento del programma.
   L'upgrade del programma, che viene distribuito a tutti gli utenti e che potrebbe incidere su alcune configurazioni di sistema, viene rilasciato dopo un lungo periodo di prova per garantire un livello di compatibilità massimo. Se è necessario eseguire l'aggiornamento a una versione più recente nel momento in cui viene rilasciato, usare uno dei metodi seguenti.
2. Manualmente nella finestra principale del programma selezionando **Verifica aggiornamenti** nella sezione **Aggiorna**.
3. Manualmente scaricando e installando una versione più recente su quella precedente.

2.7 Primo controllo dopo l'installazione

Dopo aver installato ESET NOD32 Antivirus, verrà avviato automaticamente un controllo del computer dopo dopo il primo aggiornamento ai fini della ricerca di codice dannoso.

È inoltre possibile avviare manualmente un controllo del computer dalla finestra principale del programma facendo clic su **Controllo del computer** > **Controlla il computer in uso**. Per ulteriori informazioni sui controlli del computer, consultare la sezione Controllo del computer.



3. Guida introduttiva

In questo capitolo viene fornita una panoramica su ESET NOD32 Antivirus e sulle configurazioni di base.

3.1 La finestra principale del programma

La finestra principale di ESET NOD32 Antivirus è suddivisa in due sezioni principali. La finestra principale sulla destra contiene informazioni corrispondenti all'opzione selezionata dal menu principale sulla sinistra.

Di seguito è riportata una descrizione delle opzioni del menu principale:

Stato protezione: fornisce informazioni relative allo stato di protezione di ESET NOD32 Antivirus.

Controllo del computer: consente di configurare e avviare un controllo del computer o di creare un controllo personalizzato.

Aggiorna: consente di visualizzare informazioni relative agli aggiornamenti del motore di rilevamento.

Strumenti: consente di accedere ai File di rapporto, alle Statistiche di protezione, all'Attività di verifica, ai Processi in esecuzione, Pianificazione attività, ESET SysInspector e ESET SysRescue.

Configurazione: selezionare questa opzione per regolare il livello di protezione per Computer, Internet.

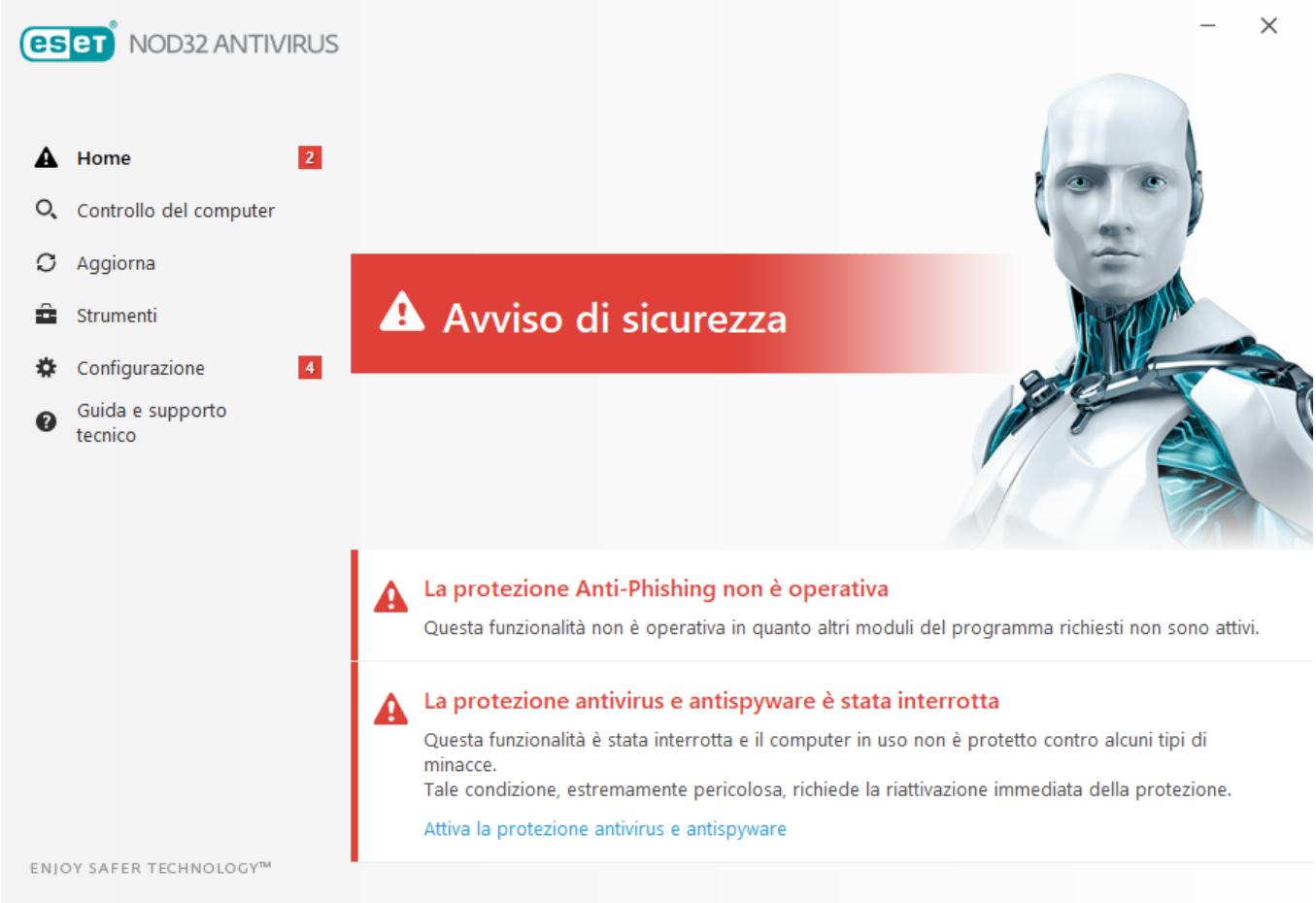
Guida e supporto tecnico: consente di accedere ai file della Guida, alla Knowledge Base di ESET, al sito Web di ESET e ai collegamenti per inviare una richiesta di assistenza.

Nella schermata **Home** vengono visualizzate informazioni importanti sul livello di protezione corrente del computer in uso. Nella finestra di stato sono visualizzate le funzionalità di ESET NOD32 Antivirus usate più frequentemente. In questa finestra sono inoltre visualizzate le informazioni sull'aggiornamento più recente e la data di scadenza del programma.

L'icona verde e il colore verde dello stato **Protezione massima** indicano un livello di protezione massimo.

Cosa fare se il programma non funziona correttamente?

Se un modulo di protezione attivo funziona correttamente, la relativa icona dello stato di protezione sarà verde. Un punto esclamativo rosso o un'icona di notifica arancione indica che non è garantito il livello massimo di protezione. In **Home** verranno visualizzate informazioni aggiuntive sullo stato di protezione di ciascun modulo, nonché le soluzioni consigliate per il ripristino della protezione completa. Per modificare lo stato dei singoli moduli, fare clic su **Configurazione** e selezionare il modulo desiderato.



L'icona rossa e il colore rosso della sezione Home indicano la presenza di problemi critici da parte dello stato. Esistono vari motivi alla base della visualizzazione di questo stato, tra cui:

- **Prodotto non attivato** : è possibile attivare ESET NOD32 Antivirus da **Home** facendo clic su **Attiva prodotto** o **Acquista ora** in Stato protezione.
- **Motore di rilevamento obsoleto**: questo errore viene visualizzato dopo diversi tentativi non riusciti di aggiornamento del database delle firme antivirali. Si consiglia di controllare le impostazioni di aggiornamento. I motivi più comuni alla base di questo errore consistono in un inserimento errato dei dati di autenticazione o in una configurazione non corretta delle impostazioni di connessione.
- **Protezione antivirus e antispyware disattivata**: è possibile riattivare la protezione antivirus e antispyware facendo clic su **Attiva protezione antivirus e antispyware**.
- **Licenza scaduta**: questa condizione è indicata dalla presenza di un'icona rossa dello stato di protezione. Allo scadere della licenza, non sarà possibile aggiornare il programma. Seguire le istruzioni nella finestra di avviso per rinnovare la licenza.

L'icona arancione indica una protezione limitata. Ad esempio, potrebbe essersi verificato un problema nell'aggiornamento del programma o la licenza potrebbe essere in fase di scadenza.
Esistono vari motivi alla base della visualizzazione di questo stato, tra cui:

- **Modalità giocatore attivata**: l'attivazione della Modalità giocatore è un potenziale rischio di protezione. L'attivazione di questa funzionalità disattiva tutte le finestre popup e interrompe qualsiasi attività pianificata.

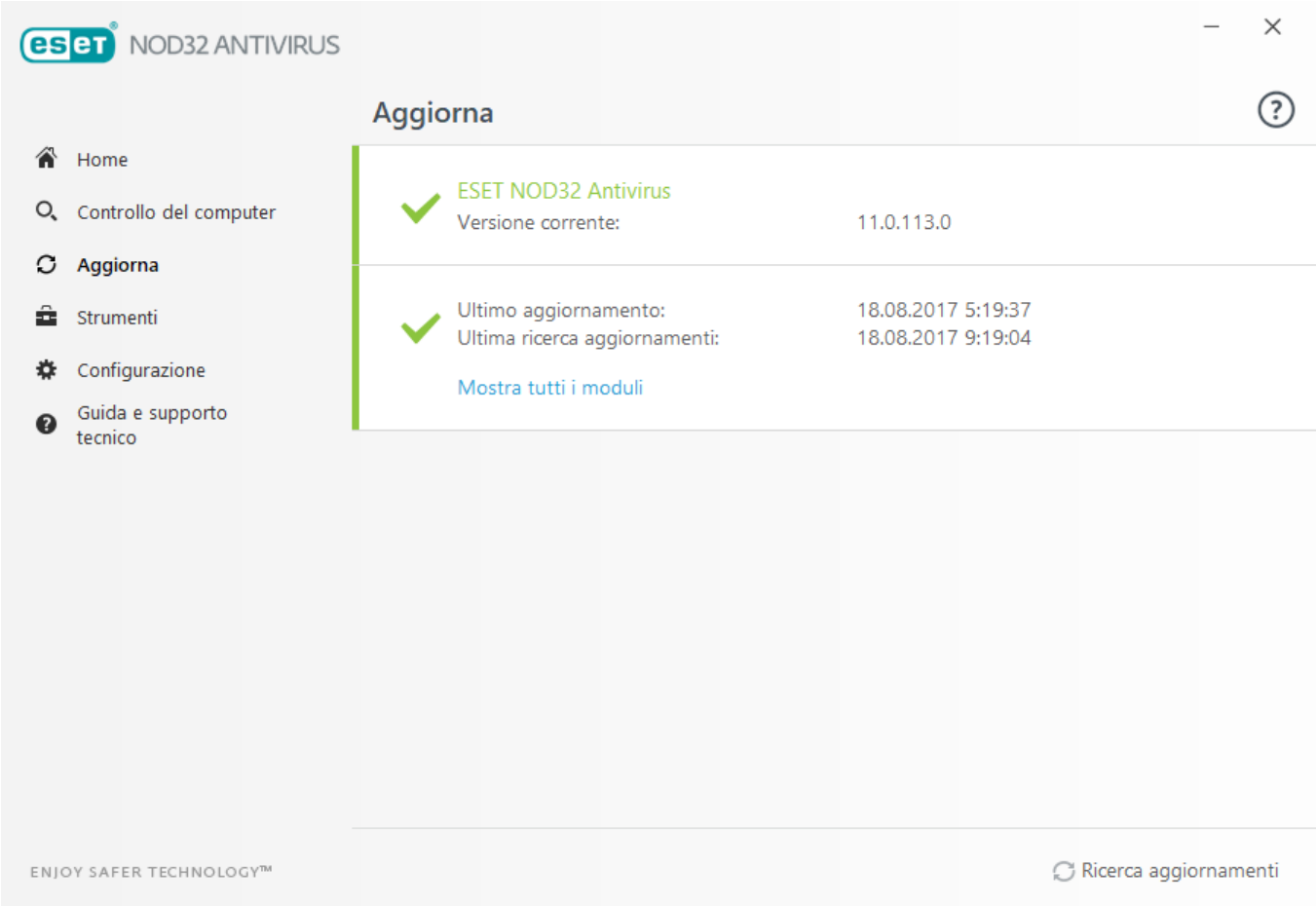
- **La licenza scadrà a breve**: questa condizione è indicata dalla presenza di un'icona dello stato di protezione contenente un punto esclamativo vicino all'orologio di sistema. Allo scadere della licenza, non sarà possibile aggiornare il programma e l'icona dello stato di protezione diventerà rossa.

Qualora non si riuscisse a risolvere un problema ricorrendo alle soluzioni consigliate, fare clic su **Guida e supporto tecnico** per accedere ai file della Guida oppure effettuare una ricerca nella Knowledge Base ESET. Per ulteriore assistenza, è possibile inviare una richiesta di supporto. Il Supporto tecnico ESET risponderà rapidamente alle domande degli utenti e li aiuterà a trovare una soluzione ai loro problemi.

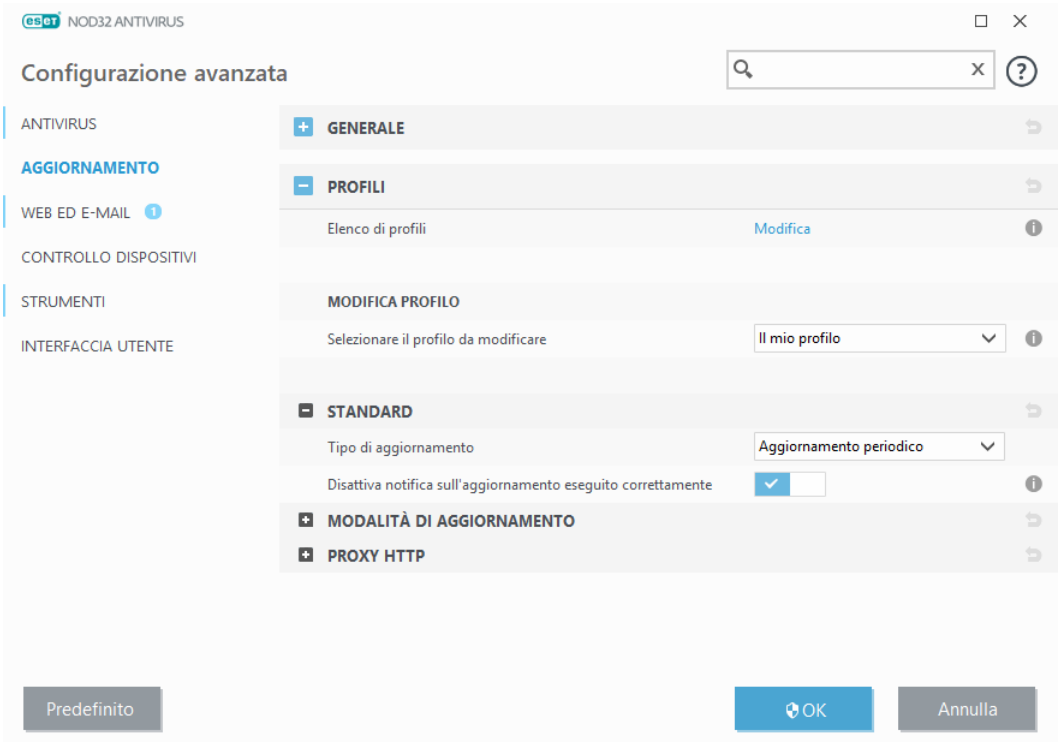
3.2 Aggiornamenti

L'aggiornamento del motore di rilevamento e dei componenti del programma costituisce un aspetto importante per garantire la protezione del sistema contro codici dannosi. È opportuno prestare particolare attenzione alla relativa configurazione e al funzionamento. Nel menu principale, fare clic su **Aggiorna**, quindi su **Aggiorna adesso** per verificare la disponibilità di un aggiornamento del motore di rilevamento.

Se durante l'attivazione di ESET NOD32 Antivirus non è stata inserita la chiave di licenza, verrà richiesto di inserirla in questa fase.

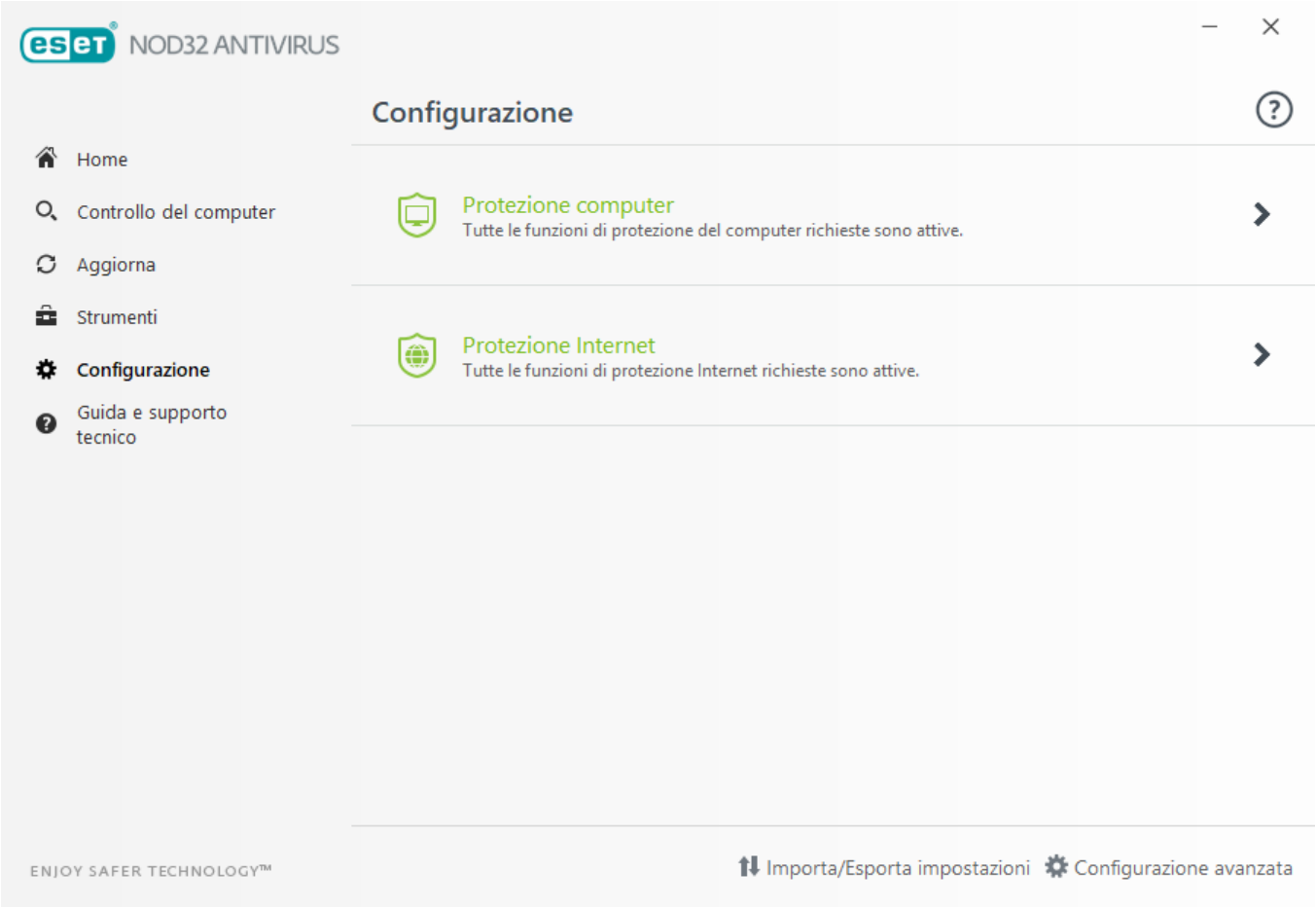


Nella finestra Configurazione avanzata (fare clic su **Configurazione** nel menu principale, quindi su **Configurazione avanzata** oppure premere **F5** sulla tastiera), sono disponibili ulteriori opzioni di aggiornamento. Per configurare le opzioni di aggiornamento avanzate, come ad esempio la modalità di aggiornamento, l'accesso al server proxy e le connessioni LAN, fare clic sulla scheda specifica nella finestra **Aggiornamento**.



4. Utilizzo di ESET NOD32 Antivirus

Le opzioni di configurazione di ESET NOD32 Antivirus consentono di regolare i livelli di protezione del computer.



Il menu **Configurazione** è suddiviso nelle seguenti sezioni:

Protezione computer

Protezione Internet

Fare clic su un componente per regolare le impostazioni avanzate del modulo di protezione corrispondente.

L'impostazione della **Protezione computer** consente di attivare o disattivare i componenti seguenti:

- **Protezione file system in tempo reale**: tutti i file vengono sottoposti a controllo per la ricerca di codici dannosi al momento dell'apertura, creazione o esecuzione sul computer.
- **HIPS**: il sistema HIPS monitora gli eventi all'interno del sistema operativo e reagisce in base a un set personalizzato di regole.
- **Modalità giocatore**: attiva o disattiva la Modalità giocatore. Quando si attiva la Modalità giocatore, viene visualizzato un messaggio di avviso (potenziale rischio per la protezione) e la finestra principale diventa arancione.

L'impostazione della **Protezione Internet** consente di attivare o disattivare i componenti seguenti:

- **Protezione accesso Web**: se questa opzione è attiva, viene eseguito il controllo di tutto il traffico HTTP o HTTPS per la ricerca di software dannoso.
- **Protezione client di posta**: monitora le comunicazioni ricevute mediante il protocollo POP3 e IMAP.
- **Protezione Anti-Phishing**: filtra i siti Web per i quali si sospetta una distribuzione di contenuti concepiti allo scopo di manipolare gli utenti facendo loro inviare informazioni riservate.

Per riattivare un componente di protezione disattivato, fare clic sul cursore affinché sia visualizzato un segno di spunta verde.

NOTA
quando si disattiva la protezione mediante questo metodo, tutti i moduli di protezione disattivati saranno attivati dopo aver riavviato il computer.

Nella parte inferiore della finestra di configurazione sono disponibili ulteriori opzioni. Utilizzare il collegamento **Configurazione avanzata** per configurare parametri più dettagliati per ciascun modulo. Utilizzare **Importa/esporta impostazioni** per caricare i parametri di configurazione mediante un file di configurazione *.xml* o per salvare i parametri di configurazione correnti in un file di configurazione.

4.1 Protezione computer

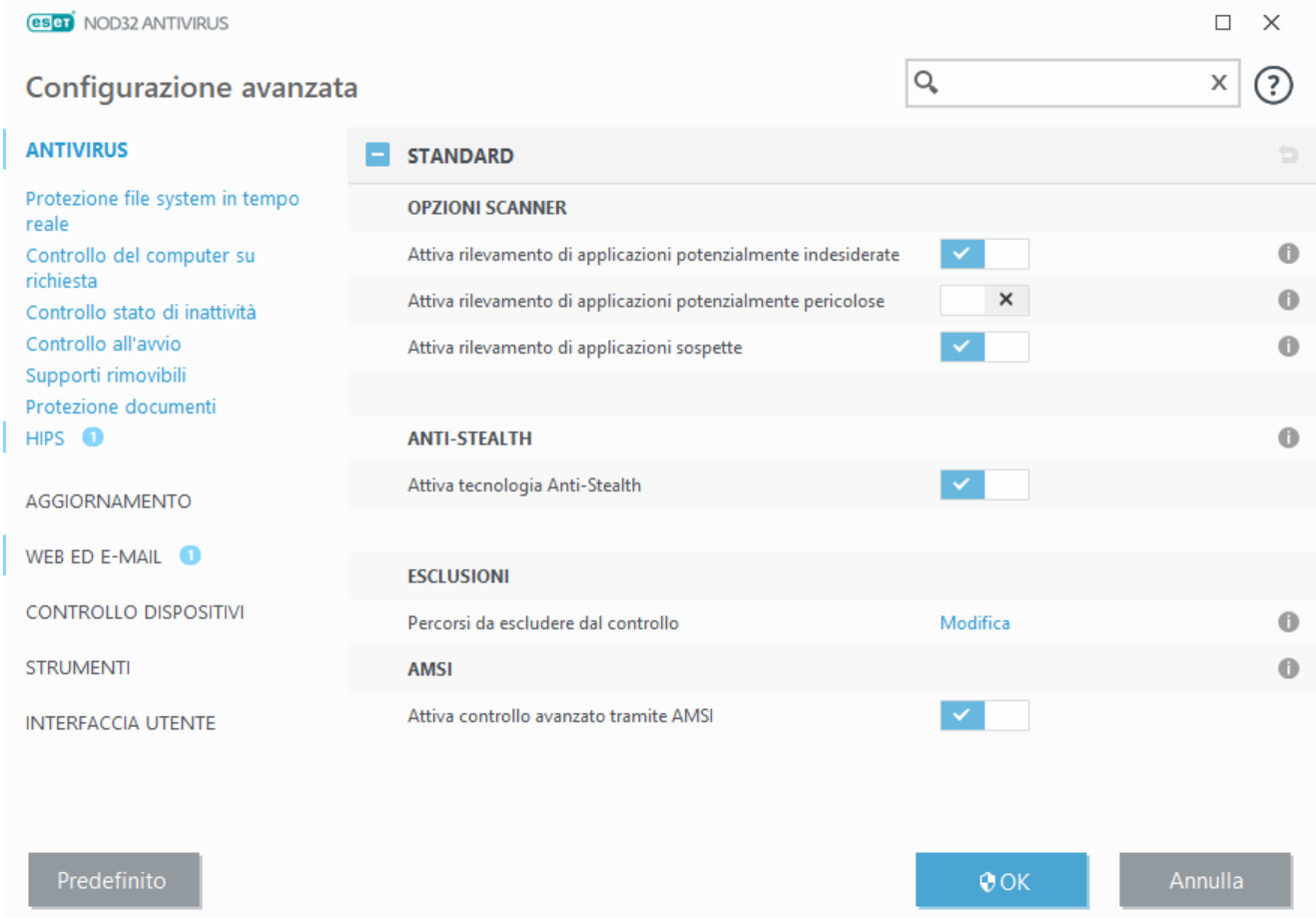
Fare clic su Protezione computer nella finestra Configurazione per visualizzare una panoramica di tutti i moduli di protezione. Per disattivare temporaneamente i singoli moduli, fare clic su . Tenere presente che in questo modo si potrebbe ridurre il livello di protezione del computer. Fare clic su accanto a un modulo di protezione per accedere alle impostazioni avanzate di tale modulo.

Fare clic su > **Modifica esclusioni** accanto a **Protezione file system in tempo reale** per aprire la finestra di configurazione Esclusioni che consente all'utente di escludere file e cartelle dal controllo.

Sospendi la protezione antivirus e antispyware: disattiva tutti i moduli di protezione antivirus e antispyware. Una volta disattivata la protezione, comparirà una finestra che consente all'utente di determinare la durata della disattivazione della protezione mediante il menu a discesa **Intervallo di tempo**. Fare clic su **Applica** per confermare.

4.1.1 Antivirus

La protezione antivirus difende il sistema da attacchi dannosi controllando file, e-mail e comunicazioni su Internet. Il modulo antivirus è in grado di eliminare una minaccia con codice dannoso rilevata. L'oggetto viene dapprima bloccato, poi pulito, cancellato o messo in quarantena.



Le **opzioni scanner** per tutti i moduli di protezione (ad esempio, protezione file system in tempo reale, protezione accesso Web, ecc.) consentono di attivare o disattivare il rilevamento dei seguenti elementi:

- Le **Applicazioni potenzialmente indesiderate** (PUA) non sono necessariamente dannose. Potrebbero tuttavia influire negativamente sulle prestazioni del computer in uso.
  Per ulteriori informazioni su questi tipi di applicazione, consultare la relativa voce del glossario.
- Le **Applicazioni potenzialmente pericolose** sono software legali e commerciali che potrebbero essere utilizzati in modo non legale per scopi illegittimi. Esempi di applicazioni potenzialmente pericolose sono strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano tutte le battute dei tasti premuti da un utente). Questa opzione è disattivata per impostazione predefinita.
  Per ulteriori informazioni su questi tipi di applicazione, consultare la relativa voce del glossario.
- Le **Applicazioni sospette** includono programmi compressi mediante programmi di compressione o protettori. Questi tipi di programmi di protezione sono spesso utilizzati dagli autori di malware per eludere il rilevamento.

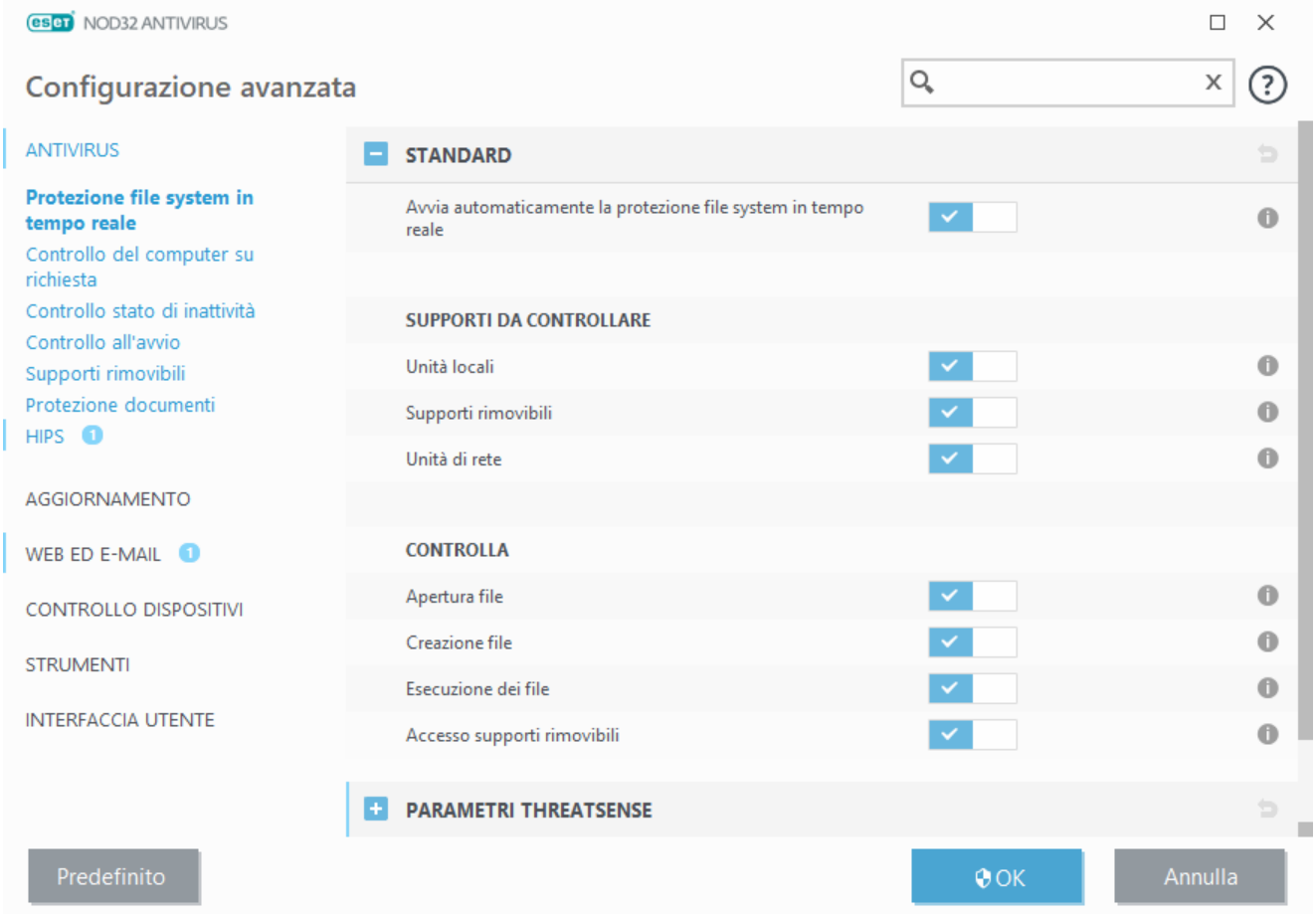
La **tecnologia Anti-Stealth** è un sistema sofisticato che consente di rilevare programmi pericolosi, come ad esempio i rootkit, che sono in grado di nascondersi dal sistema operativo. Ciò significa che non è possibile rilevarli utilizzando le normali tecnologie di testing.

Le **Esclusioni** consentono all'utente di escludere file e cartelle dal controllo. Per garantire che la ricerca delle minacce venga eseguita su tutti gli oggetti, si consiglia di creare esclusioni solo se assolutamente necessario. Le situazioni in cui potrebbe essere necessario escludere un oggetto potrebbero includere, ad esempio, il controllo di voci di database di grandi dimensioni che rallenterebbero il computer durante un controllo o di un software che entra in conflitto con il controllo. Per escludere un oggetto dal controllo, consultare il paragrafo Esclusioni.

Attiva controllo avanzato tramite AMSI: strumento di interfaccia analisi anti-malware Microsoft che permette agli sviluppatori di implementare nuove difese contro il malware (solo Windows 10).

4.1.1.1 Protezione file system in tempo reale

La funzione di Protezione file system in tempo reale consente di controllare tutti gli eventi correlati all'antivirus nel sistema. Su tutti i file vengono ricercati codici dannosi al momento dell'apertura, creazione o esecuzione sul computer. La funzione Protezione file system in tempo reale viene avviata all'avvio del sistema.



Per impostazione predefinita, la Protezione file system in tempo reale viene avviata all'avvio del sistema e fornisce un controllo ininterrotto. In casi particolari (ad esempio, in caso di conflitto con un altro scanner in tempo reale), la Protezione in tempo reale può essere disattivata deselezionando **Avvia automaticamente la protezione file system in tempo reale** in **Configurazione avanzata** sotto a **Protezione file system in tempo reale** > **Di base**.

Supportida controllare

Per impostazione predefinita, vengono controllati tutti i tipi di supporto alla ricerca di eventuali minacce:

Dischi locali: controlla tutti gli hard disk del sistema.
Supporti rimovibili: controlla CD/DVD, supporti di archiviazione USB, dispositivi Bluetooth e così via.
Dischi di rete: esegue il controllo di tutte le unità mappate.

Si consiglia di utilizzare le impostazioni predefinite e di modificarle solo in casi specifici, ad esempio quando il controllo di alcuni supporti rallenta notevolmente il trasferimento dei dati.

Controlla

Per impostazione predefinita, tutti i file vengono controllati al momento dell'apertura, creazione o esecuzione. Si consiglia di mantenere le seguenti impostazioni predefinite per garantire il massimo livello di protezione in tempo reale per il computer in uso:

- **Apertura dei file**: attiva o disattiva il controllo al momento dell'apertura dei file.
- **Creazione dei file**: attiva o disattiva il controllo al momento della creazione dei file.
- **Esecuzione dei file**: attiva o disattiva il controllo al momento dell'esecuzione dei file.
- **Accesso supporti rimovibili**: attiva o disattiva il controllo attivato dall'accesso a determinati supporti rimovibili dotati di uno spazio di archiviazione.
- **Arresto computer**: attiva o disattiva il controllo attivato dall'arresto del computer.

La Protezione file system in tempo reale, che viene attivata da vari eventi di sistema, tra cui l'accesso a un file, controlla tutti i tipi di supporti. Grazie ai metodi di rilevamento della tecnologia ThreatSense (descritti nella sezione Configurazione parametri motore ThreatSense), è possibile configurare la Protezione file system in tempo reale allo scopo di gestire i file di nuova creazione in base a modalità diverse rispetto a quelle utilizzate per i file esistenti. Ad esempio, la Protezione file system in tempo reale può essere configurata in modo da monitorare più da vicino i file di nuova creazione.

Per ridurre al minimo l'impatto sul sistema della protezione in tempo reale, i file che sono già stati controllati verranno ignorati, eccetto nel caso in cui siano state apportate modifiche. I file vengono ricontrollati immediatamente in seguito a ogni aggiornamento del motore di rilevamento. Questo comportamento viene controllato mediante l'utilizzo dell'**Ottimizzazione intelligente**. Se l'**Ottimizzazione intelligente** è disattivata, tutti i file verranno controllati a ogni accesso. Per modificare questa impostazione, premere **F5** per aprire **Configurazione avanzata** ed espandere **Antivirus** > **Protezione file system in tempo reale**. Fare clic su **parametro ThreatSense** > **Altro** e selezionare o deselezionare **Attiva ottimizzazione intelligente**.

4.1.1.1.1 Parametri ThreatSense aggiuntivi

Parametri ThreatSense aggiuntivi per i file appena creati e modificati

I file appena creati o modificati hanno maggiore possibilità di essere infettati rispetto a quelli esistenti. Per tale motivo, il programma controlla tali file con parametri di controllo aggiuntivi. ESET NOD32 Antivirus utilizza la funzione di euristica avanzata che è in grado di rilevare le nuove minacce prima del rilascio dell'aggiornamento del motore di rilevamento insieme a metodi di controllo basati sulle firme. Oltre che sui file appena creati, il controllo viene eseguito anche sugli **Archivi autoestraenti** (SFX) e sugli **Eseguibili compressi** (file eseguibili compressi a livello interno). Per impostazione predefinita, gli archivi vengono analizzati fino al 10° livello di nidificazione e controllati indipendentemente dalla loro dimensione effettiva. Per modificare le impostazioni di controllo dell'archivio, deselezionare **Impostazioni predefinite controllo degli archivi**.

Parametri ThreatSense aggiuntivi per i file eseguiti

Euristica avanzata all'esecuzione dei file: per impostazione predefinita, all'esecuzione dei file viene utilizzata l'Euristica avanzata. Una volta attivata, si consiglia vivamente di mantenere attivi l'Ottimizzazione intelligente ed ESET LiveGrid®, allo scopo di ridurre l'impatto sulle prestazioni del sistema.

Euristica avanzata all'esecuzione dei file da supporti rimovibili: l'euristica avanzata emula il codice in un ambiente virtuale e ne valuta il comportamento prima che venga consentita l'esecuzione da supporti rimovibili.

4.1.1.1.2 Livelli di pulizia

La protezione in tempo reale prevede tre livelli di pulizia (per accedere alle impostazioni dei livelli di pulizia, fare clic su **Configurazione parametri motore ThreatSense** nella sezione **Protezione file system in tempo reale**, quindi su **Pulizia**).

Nessuna pulizia: i file infetti non vengono puliti automaticamente. Verrà visualizzata una finestra di avviso per consentire all'utente di scegliere un'azione. Questo livello è indicato per utenti più esperti in grado di eseguire le azioni appropriate in caso di infiltrazione.

Pulizia normale: il programma tenterà di pulire o eliminare automaticamente un file infetto in base a un'azione predefinita (a seconda del tipo di infiltrazione). Una notifica nell'angolo in basso a destra della schermata segnalerà il rilevamento e l'eliminazione di un file infetto. Se non è possibile selezionare automaticamente l'azione corretta, il programma offre altre azioni di follow-up. Lo stesso si verifica se non è stato possibile completare un'azione predefinita.

Massima pulizia: il programma pulirà o eliminerà tutti i file infetti. Le uniche eccezioni sono costituite dai file di sistema. Nel caso in cui non sia possibile pulirli, verrà visualizzata una finestra di avviso con la possibilità di scegliere un'azione da eseguire.

AVVERTENZA
se un archivio contiene uno o più file infetti, sono disponibili due opzioni per gestire tale archivio. In modalità standard (Pulitura normale), l'intero archivio viene eliminato se tutti i file in esso contenuti sono infetti. In modalità **Massima pulizia**, l'archivio viene eliminato se contiene almeno un file infetto, indipendentemente dallo stato degli altri file contenuti nell'archivio.

4.1.1.1.3 Quando modificare la configurazione della protezione in tempo reale

La protezione in tempo reale è il componente più importante per la sicurezza di un sistema. Prestare la massima attenzione quando si modificano i relativi parametri. È consigliabile modificarli solo in casi specifici.

Dopo aver installato ESET NOD32 Antivirus, tutte le impostazioni vengono ottimizzate al fine di offrire agli utenti il massimo livello di protezione del sistema. Per ripristinare le impostazioni predefinite, fare clic su accanto a ciascuna scheda nella finestra (**Configurazione avanzata** > **Antivirus** > **Protezione file system in tempo reale**).

4.1.1.1.4 Controllo della protezione in tempo reale

Per verificare che la protezione in tempo reale funzioni e sia in grado di rilevare virus, utilizzare un file di test da eicar.com. Questo file di test è un file innocuo e rilevabile da tutti i programmi antivirus. Il file è stato creato da EICAR (European Institute for Computer Antivirus Research) per testare la funzionalità dei programmi antivirus. Può essere scaricato all'indirizzo http://www.eicar.org/download/eicar.com

4.1.1.1.5 Cosa fare se la protezione in tempo reale non funziona

In questo capitolo, verranno illustrati i problemi che potrebbero verificarsi durante l'utilizzo della protezione in tempo reale e le modalità di risoluzione.

La protezione in tempo reale è disattivata

Se la protezione in tempo reale è stata inavvertitamente disattivata da un utente, sarà necessario riattivarla. Per riattivare la protezione in tempo reale, selezionare **Configurazione** nella finestra principale del programma e fare clic su **Protezione computer** > **Protezione file system in tempo reale**.

Se la protezione in tempo reale non viene lanciata all'avvio del sistema, è probabile che l'opzione **Avvia automaticamente la protezione file system in tempo reale** non sia selezionata. Per garantire che questa opzione sia attivata, accedere a **Configurazione avanzata** (**F5**) e fare clic su **Antivirus** > **Protezione file system in tempo reale**.

La protezione in tempo reale non rileva né pulisce le infiltrazioni

Verificare che nel computer non siano installati altri programmi antivirus. Se sono installate contemporaneamente due o più soluzioni antivirus, potrebbero entrare in conflitto tra loro. È consigliabile disinstallare gli altri programmi antivirus presenti nel sistema prima di installare ESET.

La protezione in tempo reale non viene avviata

Se la protezione in tempo reale non viene lanciata all'avvio del sistema (e l'opzione **Avvia automaticamente la protezione file system in tempo reale** è attivata), ciò potrebbe dipendere da un conflitto con altri programmi. Per ricevere assistenza nella risoluzione del problema, si prega di contattare il Supporto tecnico ESET.

4.1.1.2 Controllo del computer

Lo scanner su richiesta è una parte importante della soluzione antivirus. Viene utilizzato per eseguire il controllo di file e di cartelle sul computer in uso. Dal punto di vista della protezione, è essenziale che i controlli del computer non vengano eseguiti solo quando si sospetta un'infezione, ma periodicamente, nell'ambito delle normali misure di protezione. Si consiglia di eseguire periodicamente controlli approfonditi del sistema per rilevare virus non individuati dalla Protezione file system in tempo reale quando vengono scritti sul disco. Ciò può verificarsi se la protezione file system in tempo reale era disattivata in quel momento, il database antivirus era obsoleto o il file non è stato rilevato come virus nel momento in cui è stato salvato sul disco.

Sono disponibili due tipologie di **Controllo del computer**. **Controlla computer in uso** consente di controllare rapidamente il sistema senza dover specificare i parametri di controllo. **Controllo personalizzato** che consente di selezionare uno dei profili di controllo predefiniti per l'analisi di percorsi specifici, nonché di scegliere specifiche destinazioni di controllo.


Controlla computer in uso

La funzione Controlla computer in uso consente di avviare velocemente un controllo del computer e di pulire i file infetti senza l'intervento dell'utente. Il vantaggio della funzione Controlla computer in uso consiste nella facilità di utilizzo e nel fatto che non è richiesta una configurazione di controllo dettagliata. Questo tipo di controllo consente di effettuare un controllo di tutti i file presenti nelle unità locali, nonché una pulizia o un'eliminazione automatica delle infiltrazioni rilevate. Il livello di pulizia viene impostato automaticamente sul valore predefinito. Per ulteriori informazioni sui tipi di pulizia, consultare il paragrafo Pulizia.

È anche possibile utilizzare la funzione **Controllo trascina e rilascia** per controllare manualmente un file o una cartella facendo clic su uno dei due elementi, spostando il puntatore del mouse sull'area contrassegnata tenendo premuto il pulsante del mouse e rilasciandolo successivamente.

Le seguenti opzioni di controllo sono disponibili sotto a **Controlli avanzati**:


Controllo personalizzato

Il controllo personalizzato consente di specificare parametri di controllo quali destinazioni e metodi di controllo. Il vantaggio del Controllo personalizzato consiste nella possibilità di configurare i parametri in dettaglio. È possibile salvare le configurazioni come profili di controllo definiti dagli utenti che risultano particolarmente utili se il controllo viene eseguito più volte con gli stessi parametri.


Controllo supporti rimovibili

Simile alla funzione Controlla computer in uso, consente di avviare velocemente un controllo dei supporti rimovibili (come ad esempio CD/DVD/USB) collegati al computer. Questa opzione può rivelarsi utile in caso di connessione di una memoria USB a un computer e nel caso in cui si desideri ricercare malware e altre potenziali minacce.

Questo tipo di controllo può anche essere avviato facendo clic su **Controllo personalizzato**, selezionando **Supporti rimovibili** dal menu a discesa **Oggetti da controllare** e facendo clic su **Controllo**.


Ripeti ultimo controllo

Consente all'utente di avviare rapidamente il controllo eseguito in precedenza utilizzando le stessa impostazioni.

Per ulteriori informazioni sull'avanzamento del controllo, consultare il capitolo Avanzamento controllo.

NOTA
È consigliabile eseguire un controllo del computer almeno una volta al mese. Il controllo può essere configurato come attività pianificata in **Strumenti** > **Pianificazione attività**. Come pianificare un controllo del computer settimanale

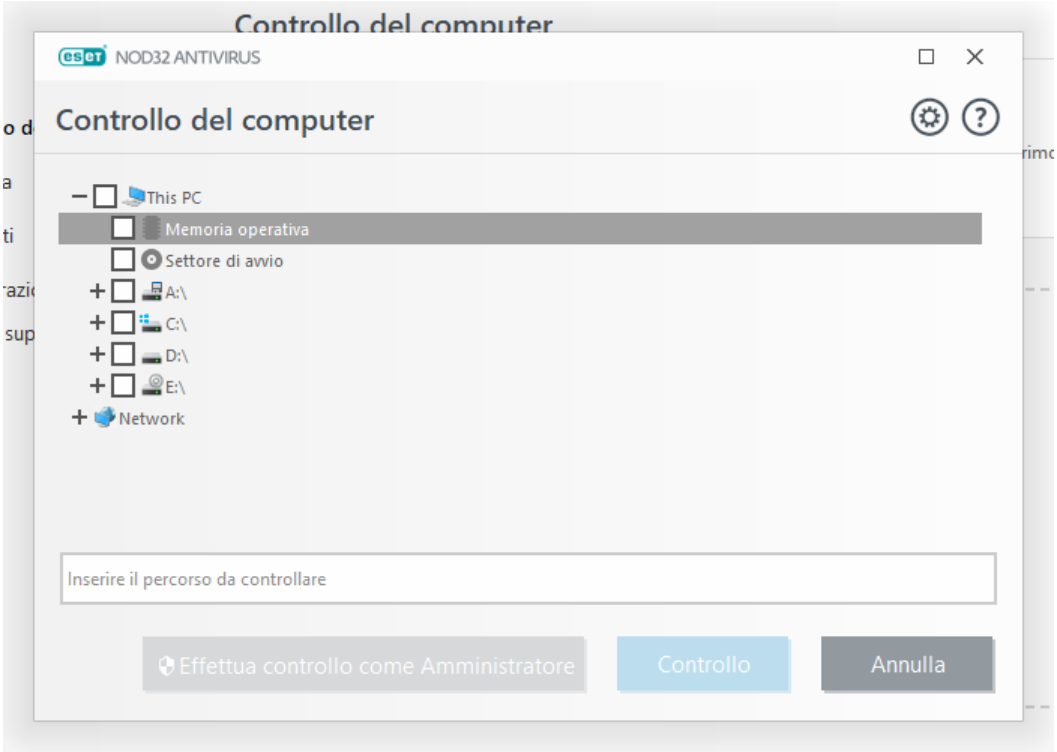
4.1.1.2.1 Launcher controllo personalizzato

È possibile utilizzare il Controllo personalizzato per analizzare sezioni specifiche di un disco, anziché l'intero disco. Per scegliere gli oggetti da controllare, selezionare **Controllo computer** > **Controllo personalizzato**, quindi selezionare un'opzione dal menu a discesa **Oggetti da controllare** oppure selezionare oggetti specifici dalla struttura ad albero.

Il menu a discesa **Oggetti da controllare** consente di selezionare gli oggetti da controllare predefiniti.

- **Attraverso le impostazioni di profilo**: consente di selezionare le destinazioni nel profilo di controllo selezionato.
- **Supporti rimovibili**: consente di selezionare dischi, supporti di archiviazione USB, CD/DVD.
- **Unità locali**: consente di selezionare tutti gli hard disk del sistema.
- **Unità di rete**: consente di selezionare tutte le unità di rete mappate.
- **Nessuna selezione**: consente di annullare tutte le selezioni.

Per visualizzare rapidamente una destinazione di controllo o per aggiungere direttamente una destinazione desiderata (cartella o file), inserirla nel campo vuoto sotto all'elenco delle cartelle. Ciò è possibile solo se nella struttura ad albero non sono state selezionate destinazioni e il menu **Oggetti da controllare** è impostato su **Nessuna selezione**.



È possibile configurare i parametri di pulizia per il controllo sotto a **Configurazione avanzata** > **Antivirus** > **Controllo computer su richiesta** > **Parametri ThreatSense** > **Pulizia.** Per eseguire un controllo senza pulizia, selezionare **Controllo senza pulizia**. La cronologia dei controlli viene salvata nei rapporti di controllo.

Se l'opzione **Ignora esclusioni** è selezionata, i file con estensioni precedentemente escluse dal controllo verranno sottoposti al controllo senza alcuna eccezione.

È possibile scegliere un profilo dal menu a discesa **Profilo di controllo** da utilizzare per il controllo delle destinazioni scelte. Il profilo predefinito è **Controllo intelligente**. Esistono due altri profili predefiniti chiamati **Controllo approfondito** e **Controllo menu contestuale**. Questi profili di controllo utilizzano diversi parametri ThreatSense. Fare clic su **Configurazione...** per impostare un profilo di controllo personalizzato. Le opzioni per profilo di controllo sono descritte nella sezione **Altro** in Parametri ThreatSense.

Fare clic su **Controlla** per eseguire il controllo utilizzando i parametri personalizzati configurati dall'utente.

Effettua controllo come Amministratore consente di eseguire il controllo mediante l'account Amministratore. Selezionare questa opzione se l'utente corrente non dispone dei privilegi per accedere ai file da controllare. Questo pulsante non è disponibile se l'utente corrente non può invocare operazioni UAC come Amministratore.

NOTA
è possibile visualizzare il rapporto del controllo computer al termine del controllo facendo clic su **Mostra rapporto**.

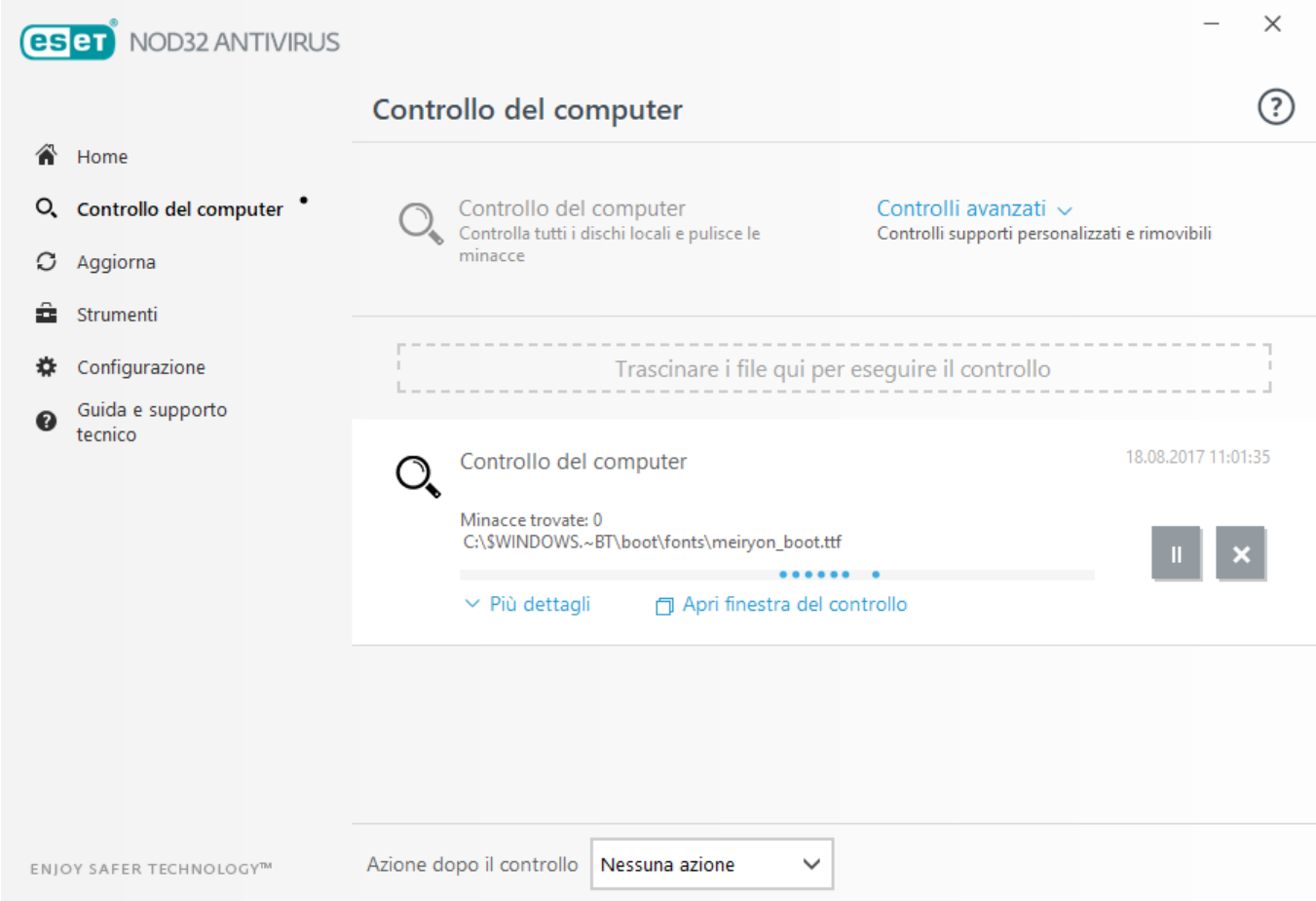
4.1.1.2.2 Avanzamento controllo

Nella finestra di avanzamento del controllo viene mostrato lo stato attuale del controllo e informazioni sul numero di file rilevati che contengono codice dannoso.

NOTA
è normale che alcuni file, ad esempio file protetti con password o file che vengono utilizzati esclusivamente dal sistema (in genere il file *pagefile.sys* e alcuni file di registro), non possano essere sottoposti al controllo.

Avanzamento controllo: la barra di avanzamento mostra lo stato di oggetti già sottoposti al controllo rispetto a quelli in attesa. Lo stato di avanzamento del controllo viene ricavato dal numero totale di oggetti inclusi nel controllo.
Destinazione: nome dell'oggetto in fase di controllo e relativo percorso.
Minacce trovate: mostra il numero totale di file sottoposti al controllo, minacce trovate e minacce pulite durante un controllo.
Sospendi: sospende un controllo.
Riprendi: questa opzione è visibile quando l'avanzamento del controllo è sospeso. Fare clic su **Riprendi** per continuare il controllo.
Interrompi: interrompe il controllo.
Scorri rapporto di controllo: se questa opzione è attiva, il rapporto di controllo scorrerà automaticamente quando vengono aggiunte nuove voci in modo da rendere visibili le voci più recenti.

NOTA
Fare clic sulla lente di ingrandimento o sulla freccia per visualizzare i dettagli sul controllo attualmente in esecuzione. È possibile eseguire un altro controllo parallelo facendo clic su **Controlla il computer in uso** o **Controllo personalizzato**.



Azione dopo il controllo: attiva un arresto, un riavvio o una sospensione pianificata al termine del controllo del computer. Una volta terminato il controllo, verrà visualizzata una finestra di dialogo in cui viene richiesto all'utente di confermare l'arresto entro 60 secondi.

4.1.1.2.3 Profili di scansione

È possibile salvare i parametri di scansione preferiti per i controlli futuri. È consigliabile creare un profilo di scansione differente (con diversi oggetti da controllare, metodi di scansione e altri parametri) per ciascuna scansione utilizzata abitualmente.

Per creare un nuovo profilo, aprire la finestra Configurazione avanzata (F5) e fare clic su **Antivirus** > **Controllo computer su richiesta** > **Di base** > **Elenco di profili**. Nella finestra **Gestione profili** è disponibile un menu a discesa **Profili selezionati** contenente i profili di scansione esistenti e l'opzione per crearne di nuovi. Per ricevere assistenza durante la creazione di un profilo di controllo adatto alle proprie esigenze, consultare la sezione Configurazione parametri motore ThreatSense contenente una descrizione di ciascun parametro di configurazione del controllo.

NOTA
Si supponga di voler creare il proprio profilo di controllo e che la configurazione **Controlla il computer in uso** sia appropriata solo in parte, in quanto non si desidera eseguire il controllo di eseguibili compressi o di applicazioni potenzialmente pericolose e si intende applicare l'opzione **Massima pulizia**. Inserire il nome del nuovo profilo nella finestra **Gestione profili** e fare clic su **Aggiungi**. Selezionare il nuovo profilo dal menu a discesa **Profilo selezionato**, modificare i parametri rimanenti in base alle proprie esigenze e fare clic su **OK** per salvare il nuovo profilo.

4.1.1.2.4 Rapporto scansioni computer

Il rapporto scansioni computer fornisce informazioni generali sulla scansione, quali:

- Ora di completamento
- Tempo di controllo totale
- Numero di minacce trovate
- Numero di oggetti sottoposti a controllo
- Dischi, cartelle e file sottoposti a controllo
- Data e ora dell'evento
- Versione del motore di rilevamento

4.1.1.3 Controllo stato inattivo

Fare clic sull'interruttore accanto a **Attiva controllo stato inattivo** in **Configurazione avanzata** > **Antivirus** > **Controllo stato inattivo** > **Di base** per consentire controlli automatici del sistema quando il computer non viene utilizzato.

Per impostazione predefinita, lo scanner dello stato inattivo non verrà eseguito in caso di alimentazione del computer (notebook) a batteria. È possibile sovrascrivere questa impostazione con la funzione **Esegui anche se il computer è alimentato a batteria**.

Attivare **Attiva registrazione** per registrare il risultato di un controllo del computer nella sezione File di rapporto (nella finestra principale del programma, fare clic su **Strumenti** > **File di rapporto** e selezionare **Controllo del computer** dal menu a discesa **Rapporto**).

Il rilevamento dello stato di inattività verrà eseguito se il computer si trova nei seguenti stati:

- Screen saver
- Blocco computer
- Disconnessione utente

Fare clic su Parametri ThreatSense per modificare i parametri di controllo (ad esempio, metodi di rilevamento) per il controllo dello stato di inattività.

4.1.1.4 Controllo all'avvio

Per impostazione predefinita, all'avvio del sistema e durante gli aggiornamenti del motore di rilevamento, verrà eseguito il controllo automatico del file di avvio. Questo controllo dipende dalla configurazione di Pianificazione configurazione e attività.

Le opzioni di controllo all'avvio fanno parte della pianificazione dell'attività **Controllo del file di avvio del sistema**. Per modificarne le impostazioni, accedere a **Strumenti** > **Pianificazione attività**, fare clic su **Verifica automaticamente file di avvio**, quindi su **Modifica**. Nell'ultimo passaggio verrà visualizzata la finestra Controllo automatico file di avvio (per ulteriori informazioni, vedere il capitolo seguente).

Per ulteriori informazioni sulla creazione e sulla gestione di Pianificazione attività, vedere Creazione di nuove attività.

4.1.1.4.1 Controllo automatico file di avvio

Durante la creazione di un'attività pianificata di controllo del file di avvio del sistema, sono disponibili varie opzioni per regolare i parametri seguenti:

Il menu a discesa **File utilizzati comunemente** specifica il livello di controllo dei file eseguiti all'avvio del sistema in base a un sofisticato algoritmo segreto. I file sono visualizzati in ordine decrescente in base ai seguenti criteri:

- **Tutti i file registrati** (la maggior parte dei file sottoposti al controllo)
- **File utilizzati raramente**
- **File utilizzati comunemente**
- **File utilizzati di frequente**
- **Solo i file utilizzati più di frequente** (ultimi file sottoposti al controllo)

Sono inoltre inclusi due gruppi specifici:

- **File eseguiti prima dell'accesso utente**: contiene file da posizioni a cui è possibile accedere senza che l'utente abbia eseguito la registrazione (include quasi tutte le posizioni di avvio quali servizi, oggetti browser helper, notifiche Winlogon, voci della pianificazione attività di Windows, dll note e così via).
- **File eseguiti dopo l'accesso utente** - Contiene file da posizioni a cui è possibile accedere solo dopo che un utente ha eseguito la registrazione (include file che sono eseguiti solo per un utente specifico, in genere i file in *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Per ogni gruppo summenzionato, vengono definiti elenchi di file da sottoporre al controllo.

Priorità di controllo: livello di priorità utilizzato per determinare il momento di avvio di un controllo:

- **Se in stato di inattività**: l'attività verrà eseguita solo quando il sistema è inattivo,
- **Più basso**: quando il carico di sistema è il più basso possibile,
- **Basso**: con un carico di sistema basso,
- **Normale**: con un carico di sistema medio.

4.1.1.5 Esclusioni

Le esclusioni consentono di escludere file e cartelle dalla scansione. Per garantire che la ricerca delle minacce venga eseguita su tutti gli oggetti, si consiglia di creare esclusioni solo se assolutamente necessario. Tuttavia, esistono situazioni in cui potrebbe essere necessario escludere un oggetto, ad esempio il caso di voci di database di grandi dimensioni che rallenterebbero il computer durante il controllo o di un software che entra in conflitto con il controllo.

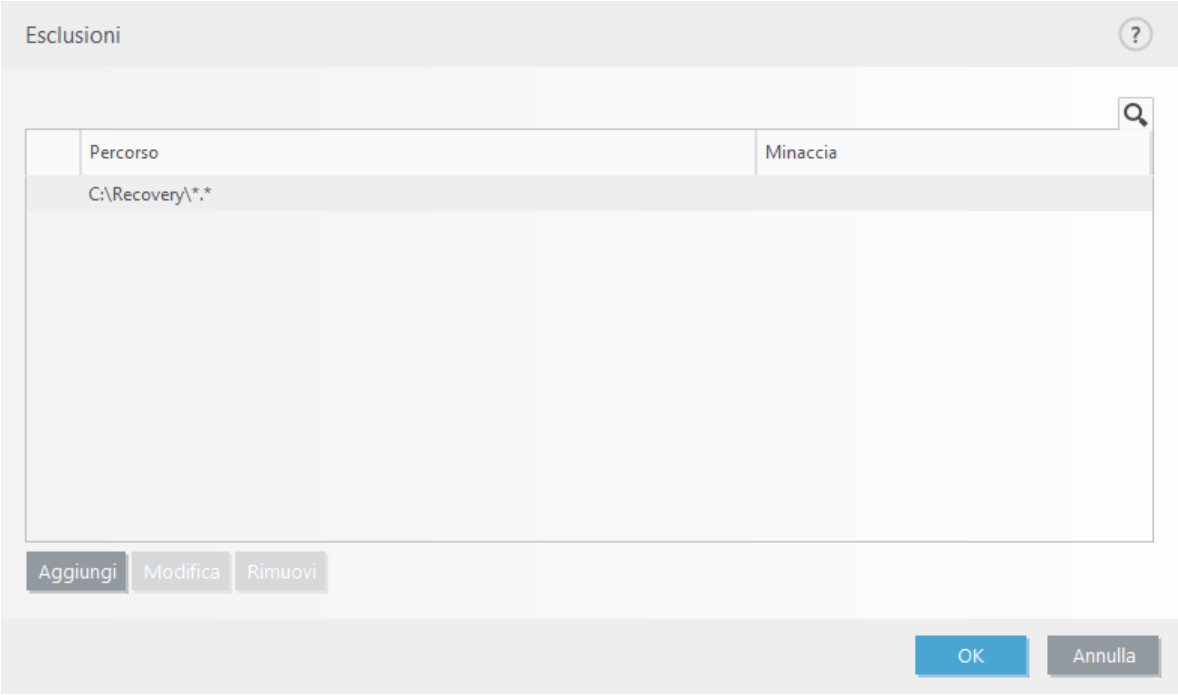
Per escludere un oggetto dalla scansione:

1. Fare clic su **Aggiungi**,
2. Immettere il percorso di un oggetto oppure selezionarlo nella struttura ad albero.

È possibile utilizzare i caratteri jolly per includere un gruppo di file. Un punto interrogativo (?) rappresenta un carattere variabile singolo, mentre un asterisco (*) rappresenta una stringa variabile di zero o più caratteri.

Esempi

- Se si desidera escludere tutti i file presenti in una cartella, digitare il percorso della cartella e utilizzare la maschera "*.*".
- Per escludere un'unità intera, compresi tutti i file e le sottocartelle, usare la maschera "D:*".
- Se si desidera escludere solo i file doc, utilizzare la maschera "*.doc".
- Se il nome di un file eseguibile contiene un determinato numero di caratteri (e i caratteri variano) e si è sicuri solo della prima lettera (ad esempio "D"), utilizzare il formato seguente: “D????.exe”. I punti interrogativi sostituiscono i caratteri mancanti (sconosciuti).



NOTA
una minaccia all'interno di un file non sarà rilevata dal modulo di protezione file system in tempo reale o dal modulo del controllo del computer se un file soddisfa i criteri dell'esclusione dal controllo.

Colonne

Percorso: percorso dei file e delle cartelle esclusi.

Minaccia: se è presente il nome di una minaccia accanto a un file escluso, ciò significa che il file viene escluso solo per la minaccia indicata e non per tutte. Se il file si infetta successivamente con altri malware, verrà rilevato dal modulo antivirus. Questo tipo di esclusione può essere utilizzato solo per alcuni tipi di infiltrazioni e può essere creato nella finestra di avviso minaccia che segnala l'infiltrazione (fare clic su **Mostra opzioni avanzate**, quindi selezionare **Escludi dal rilevamento**), oppure fare clic su **Strumenti** > **Quarantena**, quindi fare clic con il pulsante destro del mouse sul file in quarantena e selezionare **Ripristina ed escludi dal rilevamento** dal menu contestuale.

Elementi di controllo

Aggiungi: esclude gli oggetti dal rilevamento.

Modifica: consente all'utente di modificare le voci selezionate.

Rimuovi: rimuove le voci selezionate.

4.1.1.6 Parametri di ThreatSense

ThreatSense prevede numerosi metodi di rilevamento di minacce complesse. Questa tecnologia è proattiva, ovvero fornisce protezione anche durante le prime ore di diffusione di una nuova minaccia. Il programma utilizza una combinazione di analisi del codice, emulazione del codice, firme generiche e firme antivirali che operano in modo integrato per potenziare enormemente la protezione del sistema. Il motore di controllo è in grado di controllare contemporaneamente diversi flussi di dati, ottimizzando l'efficienza e la velocità di rilevamento. La tecnologia ThreatSense è inoltre in grado di eliminare i rootkit.

Le opzioni di configurazione del motore ThreatSense consentono all'utente di specificare vari parametri di controllo:

- Tipi ed estensioni dei file da controllare
- Combinazione di diversi metodi di rilevamento
- Livelli di pulizia e così via.

Per aprire la finestra di configurazione, fare clic su **Parametri di ThreatSense** nella finestra Configurazione avanzata di qualsiasi modulo che utilizza la tecnologia ThreatSense (vedere sezione sottostante). Scenari di protezione diversi potrebbero richiedere configurazioni diverse. Partendo da questo presupposto, ThreatSense è configurabile singolarmente per i seguenti moduli di protezione:

- Protezione file system in tempo reale
- Controllo stato inattivo
- Controllo all'avvio
- Protezione documenti
- Protezione client di posta
- Protezione accesso Web
- Controllo del computer

I parametri di ThreatSense vengono ottimizzati per ciascun modulo e la relativa modifica può influire in modo significativo sul funzionamento del sistema. Ad esempio, la modifica dei parametri per il controllo degli eseguibili compressi o per consentire l'euristica avanzata nel modulo della protezione file system in tempo reale potrebbe causare un rallentamento del sistema (questi metodi di controllo vengono applicati generalmente solo ai file di nuova creazione). È quindi consigliabile non modificare i parametri predefiniti di ThreatSense per tutti i moduli, ad eccezione di Controllo del computer.

Oggetti da controllare

Questa sezione consente all'utente di definire i componenti e i file del computer nei quali verranno ricercate le infiltrazioni.

Memoria operativa: ricerca le minacce che attaccano la memoria operativa del sistema.

Settori di avvio: controlla i settori di avvio alla ricerca di virus nel record di avvio principale.

File di e-mail: il programma supporta le seguenti estensioni: DBX (Outlook Express) ed EML.

Archivi: il programma supporta le seguenti estensioni: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE e molte altri ancora.

Archivi autoestraenti: si tratta di archivi (SFX) in grado di eseguire automaticamente l'estrazione del proprio contenuto.

Eseguibili compressi: dopo essere stati eseguiti, gli eseguibili compressi (diversamente dai tipi di archivi standard) si decomprimono nella memoria. Oltre agli eseguibili compressi statici standard (UPS, yoda, ASPack, FSG e così via), lo scanner è in grado di riconoscere numerosi altri tipi di programmi di compressione grazie all'utilizzo dell'emulazione del codice.

Opzioni di controllo

Selezionare i metodi utilizzati durante la ricerca di infiltrazioni nel sistema. Sono disponibili le seguenti opzioni:

Euristica: l'euristica è un algoritmo che analizza l'attività (dannosa) dei programmi. Il vantaggio principale offerto da questa tecnologia consiste nella capacità di identificare software dannosi precedentemente inesistenti o non coperti dal database delle firme antivirali precedente. Lo svantaggio è una probabilità (minima) di falsi allarmi.

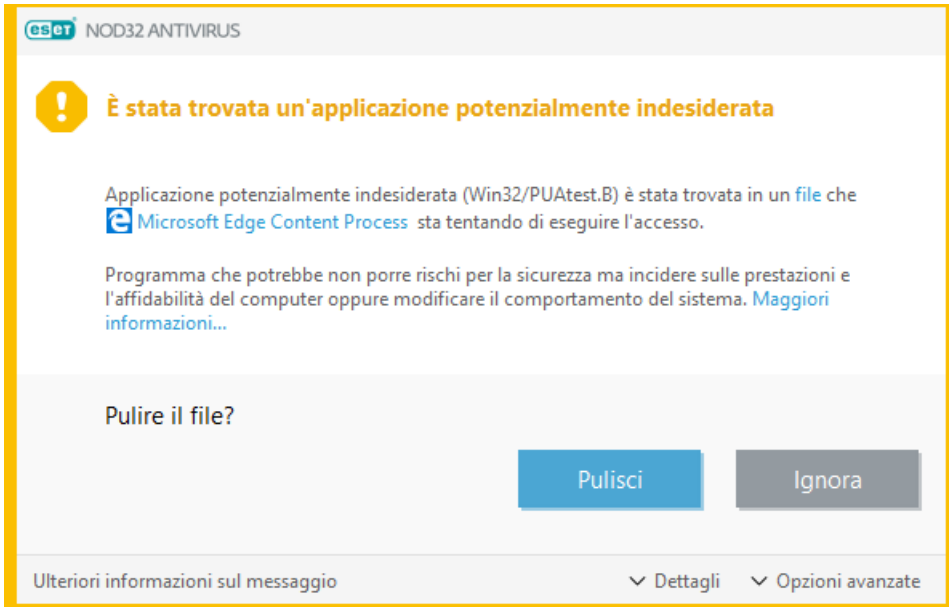
Euristica avanzata/Firme DNA: l'euristica avanzata si basa su un algoritmo di euristica esclusivo sviluppato da ESET, ottimizzato per il rilevamento dei worm e dei trojan horse e scritto in linguaggi di programmazione di alto livello. L'utilizzo dell'euristica avanzata determina un aumento esponenziale delle capacità di rilevamento delle minacce dei prodotti ESET. Le firme sono in grado di rilevare e identificare i virus in modo affidabile. Grazie al sistema di aggiornamento automatico, le nuove firme sono disponibili entro poche ore dal rilevamento di una minaccia. Lo svantaggio delle firme consiste nel fatto che tali strumenti rilevano solo i virus conosciuti (o versioni leggermente diverse di questi virus).

Un'applicazione potenzialmente indesiderata è un programma che contiene adware, installa barre degli strumenti o si prefigge altri obiettivi poco chiari. In alcuni casi, un utente potrebbe percepire che i vantaggi di un'applicazione potenzialmente indesiderata superano i rischi. Per questo motivo, ESET assegna a tali applicazioni una categoria a rischio ridotto rispetto ad altri tipi di software dannosi, come trojan horse o worm.

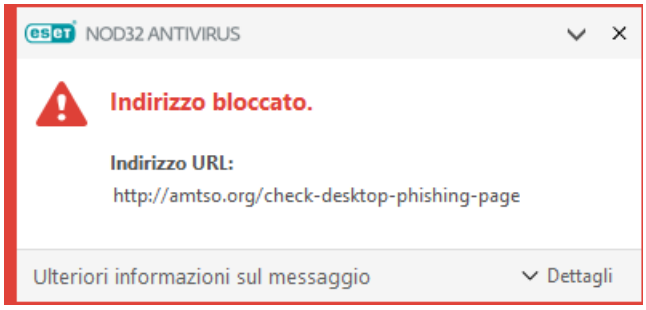
Avviso: trovata minaccia potenziale

In caso di rilevamento di un'applicazione potenzialmente indesiderata, l'utente può scegliere l'azione da intraprendere:

1. **Pulisci/Disconnetti**: questa opzione termina l'azione e impedisce alla minaccia potenziale di entrare nel sistema in uso.
2. **Ignora**: questa opzione consente a una minaccia potenziale di entrare nel sistema in uso.
3. Per consentire l'esecuzione futura dell'applicazione sul computer in uso senza interruzioni, fare clic su **Opzioni avanzate** e selezionare la casella di controllo accanto a **Escludi dal rilevamento**.

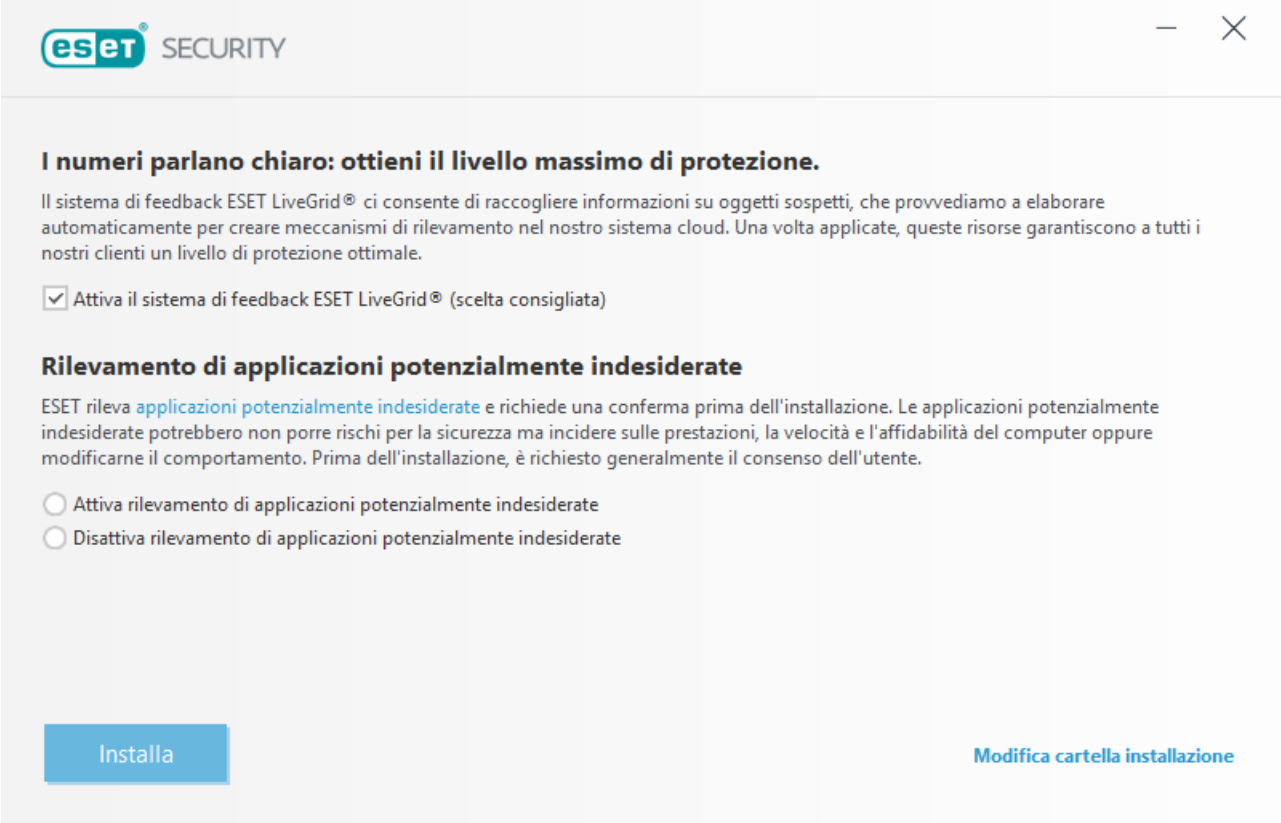


Quando viene rilevata un'applicazione potenzialmente indesiderata che non può essere cancellata, viene visualizzata una notifica **L'indirizzo è stato bloccato**. Per ulteriori informazioni su questo evento, accedere a **Strumenti** > **File di rapporto** > **Siti Web filtrati** dal menu principale.



Applicazioni potenzialmente indesiderate: impostazioni

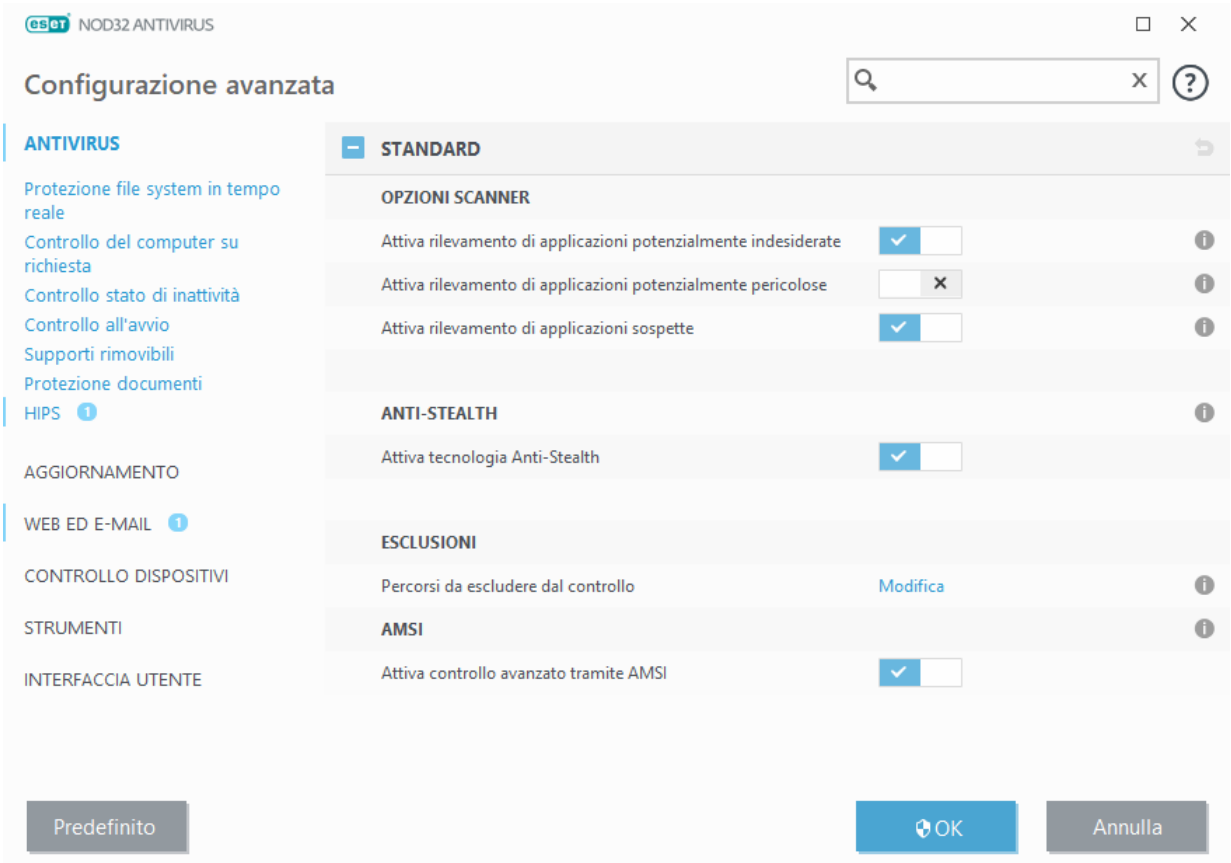
Durante l'installazione di un prodotto ESET, l'utente può decidere di attivare il rilevamento di applicazioni potenzialmente indesiderate, come illustrato di seguito:



AVVERTENZA
Le applicazioni potenzialmente indesiderate possono installare adware e barre degli strumenti o contenere altre funzioni di programma non sicure e indesiderate.

Queste impostazioni possono essere modificate in qualsiasi momento. Per attivare o disattivare il rilevamento di applicazioni potenzialmente indesiderate, pericolose o sospette, attenersi alle seguenti istruzioni:

1. Aprire il prodotto ESET. Come faccio ad aprire il mio prodotto ESET?
2. Premere il tasto **F5** per accedere alla **Configurazione avanzata**.
3. Fare clic su **Antivirus** e attivare o disattivare le opzioni **Attiva rilevamento di applicazioni potenzialmente indesiderate**, **Attiva rilevamento di applicazioni potenzialmente pericolose** e **Attiva rilevamento di applicazioni sospette** in base alle proprie preferenze. Confermare facendo clic su **OK**.



Applicazioni potenzialmente indesiderate: wrapper di software

Il wrapper di un software è un tipo speciale di modifica di un'applicazione utilizzato da alcuni siti Web che offrono servizi di file hosting. Si tratta di uno strumento di terze parti che installa il programma che si intende scaricare aggiungendo, però, altri software, come ad esempio barre degli strumenti o adware. I software aggiuntivi possono inoltre apportare modifiche alla pagina iniziale del browser Web in uso e alle impostazioni di ricerca. Inoltre, i siti Web che offrono servizi di file hosting non comunicano al fornitore del software o al destinatario del download le modifiche apportate e non consentono di rifiutarle facilmente. Per tali motivi, ESET classifica i wrapper di software tra le applicazioni potenzialmente indesiderate per consentire agli utenti di decidere se accettare o meno il download.

Per una versione aggiornata di questa pagina della Guida, consultare questo articolo della Knowledge Base ESET.

Applicazioni potenzialmente pericolose: applicazioni potenzialmente pericolose è la classificazione utilizzata per programmi commerciali e legittimi, quali strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano le battute digitate da un utente). Questa opzione è disattivata per impostazione predefinita.

Le impostazioni di pulizia determinano il comportamento dello scanner durante la pulizia di file infetti. Sono disponibili 3 livelli di pulizia.

Esclusioni

Un'estensione è la parte del nome di un file delimitata da un punto. Un'estensione definisce il tipo e il contenuto di un file. Questa sezione della configurazione dei parametri di ThreatSense consente di definire i tipi di file da sottoporre a controllo.

Altro

Quando si configurano i parametri del motore ThreatSense per l'esecuzione di un Controllo computer su richiesta, nella sezione **Altro** sono disponibili anche le seguenti opzioni:

Controlla flussi di dati alternativi (ADS): i flussi di dati alternativi utilizzati dal file system NTFS sono associazioni di file e cartelle invisibili alle normali tecniche di controllo. Molte infiltrazioni tentano di eludere il rilevamento camuffandosi in flussi di dati alternativi.

Esegui controlli in background con priorità bassa: ogni sequenza di controllo utilizza una determinata quantità di risorse del sistema. Se si utilizzano programmi che necessitano di molte risorse di sistema, è possibile attivare il controllo in background con priorità bassa e risparmiare risorse per le applicazioni.

Registra tutti gli oggetti: se questa opzione è selezionata, il file di rapporto riporta tutti i file sottoposti a controllo, anche quelli non infetti. Se ad esempio viene individuata un'infiltrazione all'interno di un archivio, nel rapporto verranno elencati anche i file puliti presenti all'interno dell'archivio.

Attiva ottimizzazione intelligente: al fine di garantire un livello di controllo ottimale, l'attivazione dell'ottimizzazione intelligente consente l'utilizzo delle impostazioni più efficienti mantenendo nel contempo la velocità di controllo più elevata. I vari moduli di protezione eseguono il controllo in modo intelligente, utilizzando metodi di controllo differenti e applicandoli a tipi di file specifici. Se l'opzione di ottimizzazione intelligente non è attivata, durante il controllo verranno applicate solo le impostazioni definite dall'utente nell'architettura ThreatSense dei moduli specifici.

Mantieni indicatore data e ora dell'ultimo accesso: selezionare questa opzione per mantenere l'ora di accesso originale ai file controllati anziché aggiornarli (ad esempio, per l'utilizzo con sistemi di backup di dati).

Limiti

La sezione Limiti consente all'utente di specificare la dimensione massima degli oggetti e i livelli di nidificazione degli archivi sui quali eseguire il controllo:

Impostazioni oggetti

Dimensione massima oggetto: definisce la dimensione massima degli oggetti su cui eseguire il controllo. Il modulo antivirus specifico eseguirà unicamente il controllo degli oggetti di dimensioni inferiori rispetto a quelle specificate. Questa opzione dovrebbe essere modificata solo da utenti esperti che abbiano ragioni particolari per escludere oggetti di maggiori dimensioni dal controllo. Il valore predefinito è: *illimitato*.

Durata massima controllo dell'oggetto (sec.): definisce il valore temporale massimo per il controllo di un oggetto. Se è stato immesso un valore definito dall'utente, il modulo antivirus interromperà il controllo dell'oggetto una volta raggiunto tale valore, indipendentemente dal fatto che il controllo sia stato completato. Il valore predefinito è: *illimitato*.

Configurazione controllo degli archivi

Livello di nidificazione degli archivi: specifica il livello massimo di controllo degli archivi. Il valore predefinito è: *10*.

Dimensione massima file in archivio: questa opzione consente all'utente di specificare le dimensioni massime dei file contenuti all'interno degli archivi, i quali, una volta estratti, saranno sottoposti a controllo. Il valore predefinito è: *illimitato*.

NOTA
si consiglia di non modificare i valori predefiniti. In circostanze normali, non vi sono motivi particolari per eseguire tale operazione.

4.1.1.6.1 Pulizia

Le impostazioni di pulizia determinano il comportamento dello scanner durante la pulizia di file infetti. Sono disponibili 3 livelli di pulizia.

4.1.1.6.2 Estensioni file esclusi dal controllo

Un'estensione è una parte del nome di un file delimitata da un punto. Un'estensione definisce il tipo e il contenuto di un file. Questa sezione delle impostazioni parametri ThreatSense consente di definire i tipi di file da sottoporre a controllo.

Per impostazione predefinita, tutti i file vengono sottoposti a scansione indipendentemente dall'estensione. È possibile aggiungere qualunque estensione all'elenco dei file esclusi dalla scansione.

L'esclusione di file è un'operazione utile nel caso in cui il controllo di determinati tipi di file impedisca il corretto funzionamento di uno specifico programma che utilizza determinate estensioni. Ad esempio, potrebbe essere consigliabile escludere le estensioni EDB, EML e TMP durante l'utilizzo dei server Microsoft Exchange.

I pulsanti **Aggiungi** e **Rimuovi** consentono all'utente di attivare o impedire il controllo di estensioni di file specifiche. Per aggiungere una nuova estensione all'elenco, fare clic su **Aggiungi**, digitare l'estensione nel campo vuoto e fare clic su **OK**. Dopo aver selezionato **Inserisci valori multipli**, è possibile aggiungere estensioni di file multiple delimitate da righe, virgole o punti e virgola. Attivando selezioni multiple, sarà possibile visualizzare le estensioni nell'elenco. Per eliminare un'estensione dall'elenco, selezionarla e fare clic su **Rimuovi**. Se si desidera modificare un'estensione selezionata, fare clic su **Modifica**.

È possibile utilizzare i simboli speciali ? (punto interrogativo). L' il punto interrogativo rappresenta qualsiasi simbolo.

NOTA
Per visualizzare l'estensione esatta (se disponibile) di un file in un sistema operativo Windows, è necessario disattivare l'opzione **Nascondi estensioni dei tipi di file conosciuti** in **Pannello di controllo** > **Opzioni cartella** > **Visualizza** (scheda) e applicare la modifica.

4.1.1.7 Rilevamento di un'infiltrazione

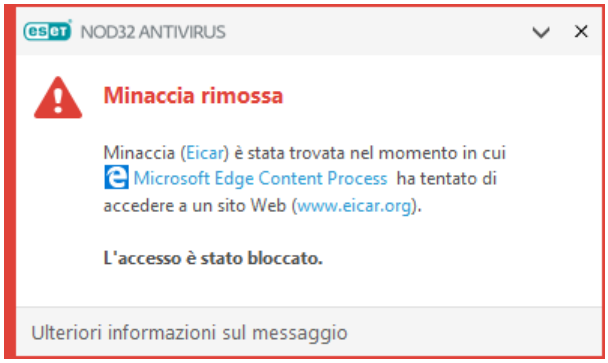
Le infiltrazioni possono raggiungere il sistema da diversi accessi, ad esempio pagine Web, cartelle condivise, messaggi e-mail o dispositivi rimovibili (USB, dischi esterni, CD, DVD, dischetti e così via).

Comportamento standard

In linea generale, ESET NOD32 Antivirus gestisce le infiltrazioni utilizzando i seguenti strumenti per la rilevazione:

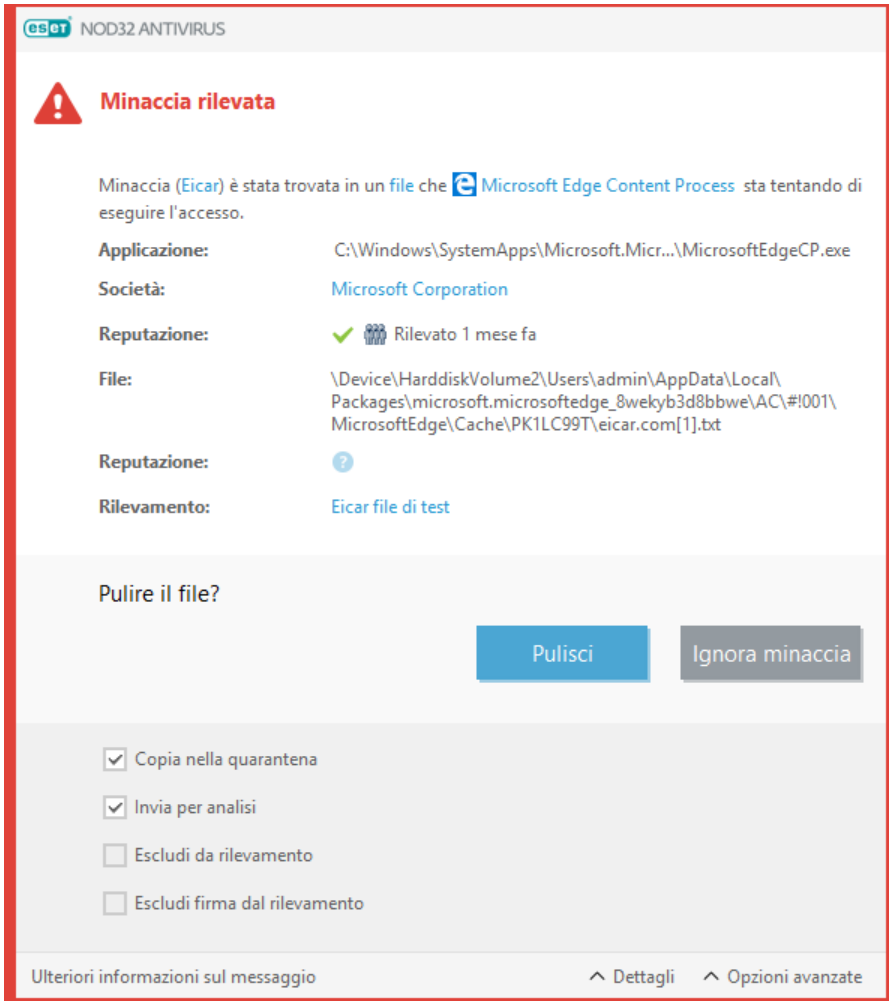
- Protezione file system in tempo reale
- Protezione accesso Web
- Protezione client di posta
- Controllo del computer su richiesta

Ciascuna di tali opzioni utilizza il livello di pulizia standard e tenta di pulire il file e di spostarlo nella Quarantena o di interrompere la connessione. Una finestra di avviso viene visualizzata nell'area di notifica posta nell'angolo in basso a destra della schermata. Per ulteriori informazioni sui livelli di pulizia e sul comportamento, consultare il paragrafo Pulizia.



Pulizia ed eliminazione

In assenza di azioni predefinite per l'esecuzione della Protezione file system in tempo reale, verrà chiesto all'utente di selezionare un'opzione nella finestra di avviso. Le opzioni generalmente disponibili sono **Pulisci**, **Elimina** e **Nessuna azione**. Non è consigliabile selezionare **Nessuna azione**, in quanto i file infettati non verranno puliti. È opportuno selezionare questa opzione solo quando si è certi che un file non è pericoloso e che si tratta di un errore di rilevamento.



Applicare la pulizia nel caso in cui un file sia stato attaccato da un virus che ha aggiunto un codice dannoso. In tal caso, tentare innanzitutto di pulire il file infetto per ripristinarne lo stato originale. Nel caso in cui il file sia composto esclusivamente da codice dannoso, verrà eliminato.

Se un file infetto è "bloccato" o utilizzato da un processo del sistema, verrà eliminato solo dopo essere stato rilasciato (generalmente dopo il riavvio del sistema).

Più minacce

Se durante un controllo del computer i file infetti non sono stati puliti (o se il Livello di pulizia era impostato su **Nessuna pulizia**), viene visualizzata una finestra di avviso che richiede di selezionare le azioni per i file in questione. Selezionare le azioni da eseguire sui file (le azioni vengono impostate singolarmente per ciascun file presente nell'elenco), quindi fare clic su **Fine**.

Eliminazione dei file negli archivi

In modalità di pulizia predefinita, l'intero archivio verrà eliminato solo nel caso in cui contenga file infetti e nessun file pulito. In pratica, gli archivi non vengono eliminati nel caso in cui dovessero contenere anche file puliti non dannosi. Durante l'esecuzione di un controllo di massima pulizia, si consiglia di agire con estrema prudenza, in quanto, in caso di rilevamento di un file infetto, verrà eliminato l'intero archivio di appartenenza dell'oggetto, indipendentemente dallo stato degli altri file.

Se il computer mostra segnali di infezione malware, ad esempio appare più lento, si blocca spesso e così via, è consigliabile attenersi alle seguenti istruzioni:

- Aprire ESET NOD32 Antivirus e fare clic su Controllo del computer
- Fare clic su **Controlla il computer in uso** (per ulteriori informazioni, consultare il paragrafo Controllo del computer)
- Al termine del controllo, consultare il rapporto per conoscere il numero di file controllati, infetti e puliti

Se si desidera controllare solo una parte del disco, fare clic su **Controllo personalizzato** e selezionare le destinazioni su cui effettuare un controllo antivirus.

4.1.1.8 Protezione documenti

La funzione Protezione documenti consente di eseguire il controllo dei documenti di Microsoft Office prima della loro apertura e dei file scaricati automaticamente da Internet Explorer, ad esempio gli elementi di Microsoft ActiveX. La funzione Protezione documenti offre un livello di protezione aggiuntivo rispetto alla protezione file system in tempo reale e può essere disattivata per ottimizzare le prestazioni di sistemi che non gestiscono volumi elevati di documenti Microsoft Office.

Per attivare la protezione documenti, aprire la finestra **Configurazione avanzata** (premere F5) > **Antivirus** > **Protezione documenti** e fare clic sull'interruttore **Integra nel sistema**.

NOTA
Questa funzione è attivata dalle applicazioni che utilizzano Microsoft Antivirus API (ad esempio, Microsoft Office 2000 e versioni successive o Microsoft Internet Explorer 5.0 e versioni successive).

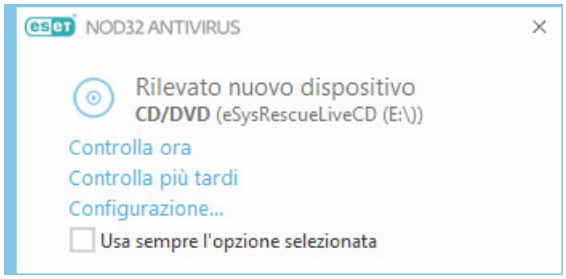
4.1.2 Supporti rimovibili

ESET NOD32 Antivirus offre il controllo automatico dei supporti rimovibili (CD/DVD/USB/...). Questo modulo consente di controllare un supporto inserito. Questa funzionalità può essere utile se l'amministratore del computer desidera impedire l'utilizzo di supporti rimovibili con contenuti non desiderati da parte degli utenti.

Azione da eseguire all'inserimento dei supporti rimovibili: selezionare l'azione predefinita che verrà eseguita quando un supporto rimovibile viene inserito nel computer (CD/DVD/USB). Selezionando **Mostra opzioni di controllo**, verrà visualizzata una notifica che consente all'utente di scegliere un'azione desiderata:

- **Non controllare**: non verrà eseguita alcuna azione e la finestra **Rilevato nuovo dispositivo** verrà chiusa.
- **Controllo automatico del dispositivo**: viene eseguito il controllo del computer su richiesta del supporto rimovibile inserito.
- **Mostra opzioni di controllo**: apre la sezione di configurazione dei supporti rimovibili.

All'inserimento di un supporto rimovibile, viene visualizzata la seguente finestra di dialogo:



Controlla ora: avvia il controllo del supporto rimovibile.

Controlla più tardi: il controllo del supporto rimovibile verrà posticipato.

Configurazione: apre la Configurazione avanzata.

Usa sempre l'opzione selezionata: se l'opzione è selezionata, verrà eseguita la stessa azione quando viene inserito nuovamente un supporto rimovibile.

In ESET NOD32 Antivirus è inoltre disponibile la funzionalità Controllo dispositivi che consente all'utente di definire regole per l'utilizzo dei dispositivi esterni su un determinato computer. Per ulteriori informazioni sul Controllo dispositivi, consultare il paragrafo Controllo dispositivi.

4.1.3 Controllo dispositivo

Controllo dispositivo

ESET NOD32 Antivirus offre un controllo automatico dei dispositivi (CD/DVD/USB/...). Questo modulo consente di bloccare o modificare le estensioni dei filtri/delle autorizzazioni e di definire la capacità dell'utente di accedere e di utilizzare un determinato dispositivo. Questa funzionalità potrebbe rivelarsi utile nel caso in cui l'amministratore di un computer desideri impedire l'utilizzo di dispositivi con contenuti non desiderati.

Dispositivi esterni supportati:

- Archiviazione su disco (HDD, disco rimovibile USB)
- CD/DVD
- Stampante USB
- Archiviazione FireWire
- Dispositivo Bluetooth
- Lettore di smart card
- Dispositivo di acquisizione immagini
- Modem
- Porta LPT/COM
- Dispositivo portatile
- Microfono
- Tutti i tipi di dispositivi

Le opzioni di configurazione del controllo dispositivi possono essere modificate in **Configurazione avanzata** (F5) > **Controllo dispositivi**.

Attivando il pulsante accanto a **Integra nel sistema**, è possibile attivare la funzione Controllo dispositivi in ESET NOD32 Antivirus. Per rendere effettiva questa modifica, sarà necessario riavviare il computer. Dopo aver attivato il Controllo dispositivi, si attiverà **Regole**, che consentirà all'utente di aprire la finestra Editor regole.

NOTA
è possibile creare vari gruppi di dispositivi ai quali verranno applicate regole diverse. È inoltre possibile creare solo un gruppo di dispositivi per i quali verrà applicata la regola con l'azione **Lettura/Scrittura** o **Solo lettura**. Ciò consente al Controllo dispositivi di bloccare i dispositivi non riconosciuti che si connettono al computer in uso.

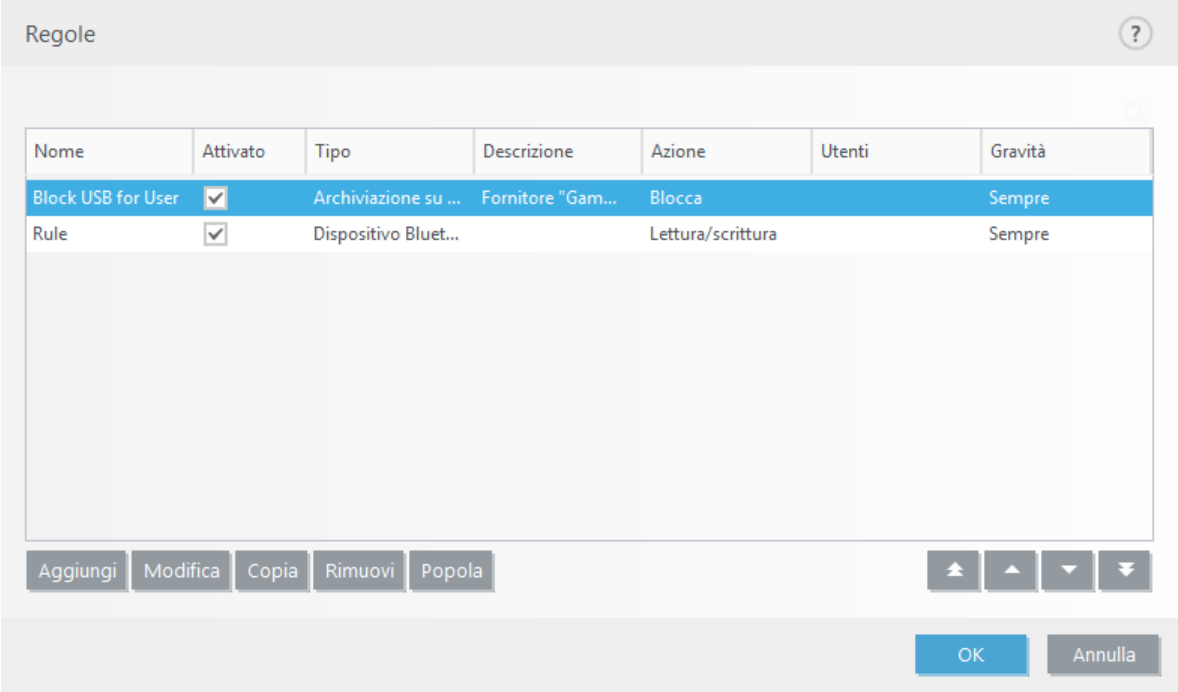
In caso di inserimento di un dispositivo bloccato mediante una regola esistente, verrà visualizzata una finestra di notifica e l'accesso al dispositivo non verrà concesso.

Protezione webcam

Azionando l'interruttore accanto a **Integra nel sistema** si attiva la funzione di protezione webcam in ESET NOD32 Antivirus. Dopo aver attivato la protezione webcam, si attiverà **Regole**, che consentirà all'utente di aprire la finestra Editor regole.

4.1.3.1 Editor regole controllo dispositivi

Nella finestra **Editor regole controllo dispositivi**, in cui vengono visualizzate le regole esistenti, è possibile effettuare un controllo accurato dei dispositivi esterni collegati dagli utenti al computer.



È possibile consentire o bloccare specifici dispositivi per ciascun utente o gruppo di utenti e sulla base di parametri aggiuntivi del dispositivo che è possibile specificare nella configurazione delle regole. L'elenco delle regole contiene varie descrizioni tra cui nome, tipo di dispositivo esterno, azione da eseguire dopo aver collegato un dispositivo esterno al computer e gravità del rapporto.

Fare clic su **Aggiungi** o **Modifica** per gestire una regola. Fare clic su **Copia** per creare una nuova regola con le opzioni predefinite utilizzate per un'altra regola selezionata. Le stringhe XML visualizzate quando si seleziona una regola possono essere copiate negli Appunti in modo da aiutare gli amministratori di sistema a esportare/importare questi dati e utilizzarli, ad esempio, in ESET Remote Administrator.

Premere CTRL e fare clic per selezionare più regole e applicare azioni, come ad esempio elimina o sposta in alto o in basso nell'elenco, a tutte le regole selezionate. La casella di controllo **Attivata** consente di disattivare o attivare una regola. Questa opzione è utile se non si desidera eliminare definitivamente una regola in modo da poterla utilizzare in futuro.

Il controllo viene eseguito mediante regole classificate in base al rispettivo ordine di priorità (le regole con priorità maggiore saranno posizionate in alto).

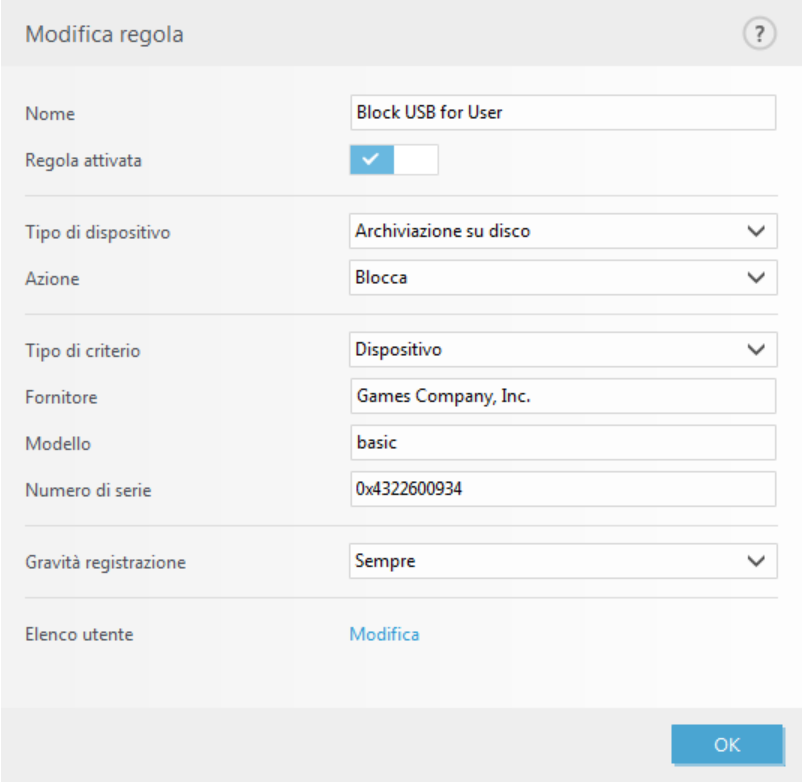
Le voci del rapporto possono essere visualizzate nella finestra principale di ESET NOD32 Antivirus in **Strumenti** > **File di rapporto**.

Il rapporto Controllo dispositivi registra tutte le occorrenze di attivazione del controllo dispositivi.

Fare clic su **Popola** per popolare automaticamente i parametri dei supporti rimovibili per i dispositivi collegati al computer.

4.1.3.2 Aggiunta di regole per il controllo dispositivi

Una regola per il controllo dispositivi definisce l'azione che verrà intrapresa quando viene effettuata una connessione tra il computer e un dispositivo che soddisfa i criteri della regola.



Inserire una descrizione della regola nel campo **Nome** per consentire una migliore identificazione. Fare clic sul pulsante accanto a **Regola attivata** per disattivare o attivare questa regola. Questa opzione può essere utile se non si desidera eliminare definitivamente la regola.

Tipo di dispositivo

Scegliere il tipo di dispositivo esterno dal menu a discesa (Archiviazione su disco/Dispositivo portatile/Bluetooth/FireWire/...). Le informazioni relative al tipo di dispositivo vengono raccolte dal sistema operativo e possono essere visualizzate in Gestione dispositivi del sistema se un dispositivo è collegato al computer. I supporti di archiviazione includono dischi esterni o lettori tradizionali di schede di memoria collegati tramite USB o FireWire. I lettori di smart card includono circuiti integrati incorporati, come ad esempio schede SIM o schede di autenticazione. Esempi di dispositivi di acquisizione immagini sono gli scanner o le fotocamere. Poiché tali dispositivi non forniscono informazioni sugli utenti, ma solo sulle azioni, possono essere bloccati solo a livello globale.

Azione

È possibile consentire o bloccare l'accesso ai dispositivi non adatti all'archiviazione. Le regole dei dispositivi di archiviazione consentono invece all'utente di scegliere uno dei seguenti diritti:

- **Lettura/Scrittura**: sarà consentito l'accesso completo al dispositivo.
- **Blocca**: l'accesso al dispositivo verrà bloccato.
- **Solo lettura**: sul dispositivo sarà consentito l'accesso di sola lettura.
- **Avvisa**: tutte le volte che un dispositivo effettua la connessione, all'utente verrà inviata una notifica che lo avvisa in merito all'eventuale autorizzazione/blocco e verrà creata una voce di rapporto. Poiché i dispositivi non vengono memorizzati, l'utente visualizzerà sempre una notifica relativa alle successive connessioni di uno stesso dispositivo.

Tenere presente che non sono disponibili tutte le azioni (autorizzazioni) per tutti i tipi di dispositivi. Se si tratta di un dispositivo di archiviazione, saranno disponibili tutte e quattro le azioni. Per i dispositivi non di archiviazione, sono disponibili solo tre azioni (ad esempio, l'azione **Solo lettura** non è disponibile per il sistema Bluetooth. Ciò significa che i dispositivi Bluetooth possono essere solo consentiti, bloccati o avvisati).

Tipo di criterio : selezionare **Gruppo dispositivi** o **Dispositivo.**

I parametri aggiuntivi visualizzati di seguito possono essere utilizzati per ottimizzare le regole e personalizzarle in base ai dispositivi in uso. Tutti i parametri non fanno distinzione tra lettere maiuscole e minuscole:

- **Fornitore**: filtraggio in base al nome o all'identificativo del fornitore.
- **Modello**: nome specifico del dispositivo.
- **Numero di serie**: generalmente, a ogni dispositivo esterno è associato un numero di serie. Nel caso di CD/DVD, il numero di serie è associato al supporto specifico e non all'unità CD.

NOTA
se i parametri non sono definiti, la regola ignorerà questi campi durante la ricerca delle corrispondenze. I parametri di filtraggio in tutti i campi di testo non fanno distinzione tra maiuscole e minuscole e i caratteri jolly (*, ?) non sono supportati.

NOTA
per visualizzare le informazioni relative a un dispositivo, creare una regola per tale dispositivo specifico, collegare il dispositivo al computer in uso e verificare i dettagli relativi al dispositivo nel Rapporto controllo dispositivi.

Gravità registrazione

ESET NOD32 Antivirus salva tutti gli eventi importanti in un file di rapporto, che può essere visualizzato direttamente dal menu principale. Fare clic su **Strumenti** > **File di rapporto**, quindi selezionare **Controllo dispositivo** dal menu a discesa **Rapporto**.

- **Sempre**: registra tutti gli eventi.
- **Diagnostica**: registra le informazioni necessarie ai fini dell'ottimizzazione del programma.
- **Informazioni**: registra i messaggi informativi, compresi quelli relativi agli aggiornamenti riusciti, e tutti i record indicati in precedenza.
- **Allarme**: registra errori critici e messaggi di allarme.
- **Nessuno**: non verrà registrato alcun rapporto.

Le regole possono essere limitate a determinati utenti o gruppi di utenti aggiunti all'**Elenco utenti**:

- **Aggiungi**: apre la finestra di dialogo **Tipi di oggetto: Utenti o Gruppi**, che consente di selezionare gli utenti desiderati.
- **Rimuovi**: rimuove l'utente selezionato dal filtro.

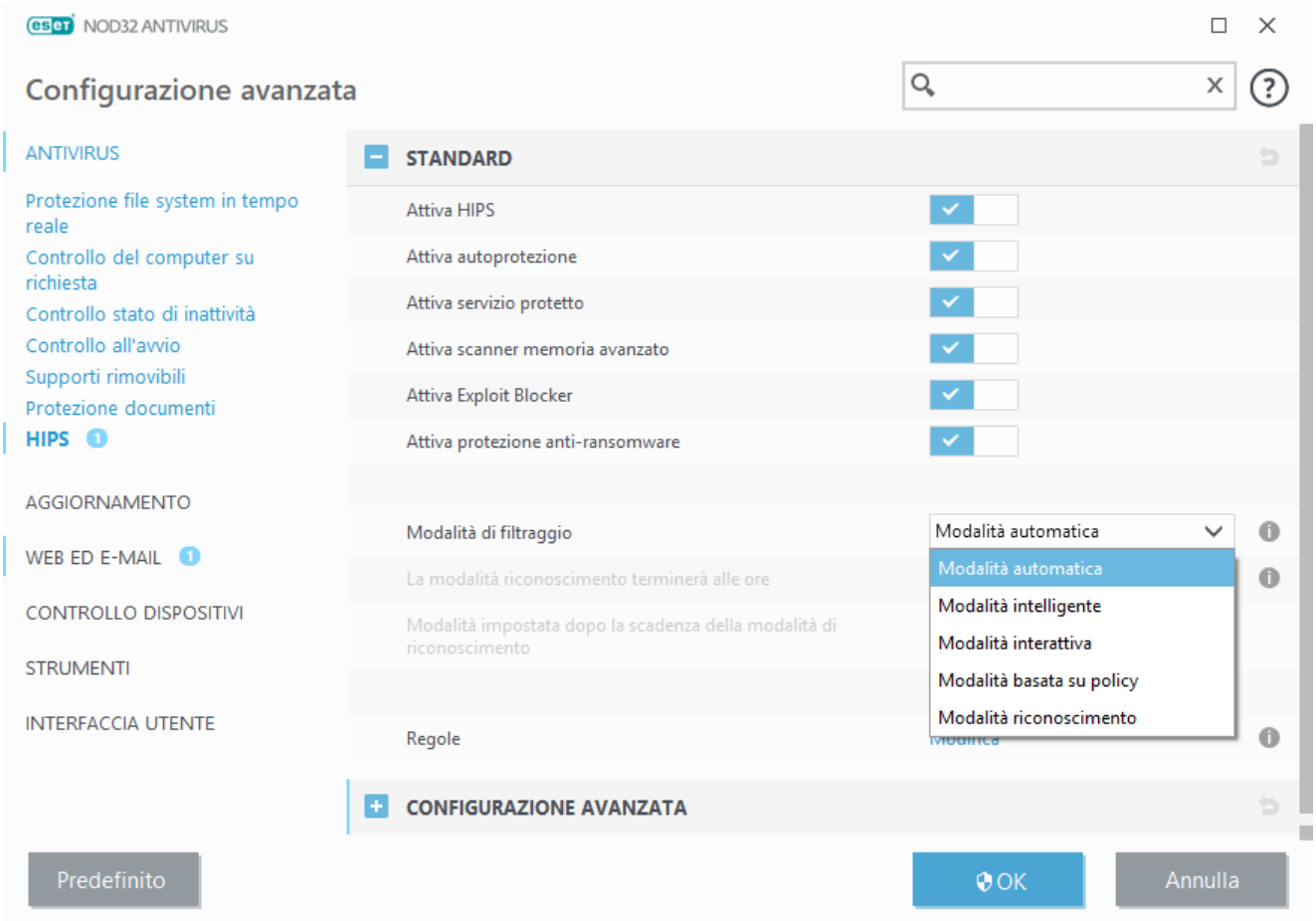
NOTA
tutti i dispositivi possono essere filtrati dalle regole dell'utente (ad esempio, i dispositivi di acquisizione di immagini non forniscono informazioni sugli utenti, ma solo sulle azioni).

4.1.4 Sistema anti-intrusione basato su host (HIPS)

AVVERTENZA
È consigliabile che le modifiche delle impostazioni HIPS siano apportate solo dagli utenti avanzati. Una configurazione non corretta delle impostazioni HIPS può causare instabilità di sistema.

Il **Sistema anti-intrusione basato su host** (HIPS) protegge il sistema da malware e attività indesiderate che tentano di compromettere la sicurezza del computer. L'HIPS utilizza un'analisi comportamentale avanzata unita alle capacità di rilevamento del filtraggio di rete per il monitoraggio dei processi in esecuzione, dei file e delle chiavi del registro. L'HIPS è indipendente dalla protezione file system in tempo reale e non è un firewall, in quanto monitora solo i processi eseguiti all'interno del sistema operativo.

Le impostazioni HIPS sono disponibili in **Configurazione avanzata** (F5) > **Antivirus** > **HIPS** > **Di base**. Lo stato HIPS (attivato/disattivato) è visualizzato nella finestra principale del programma ESET NOD32 Antivirus in **Configurazione** > **Protezione computer**.



ESET NOD32 Antivirus utilizza una tecnologia di **Autoprotezione** integrata che impedisce a software dannosi di danneggiare o disattivare la protezione antivirus e antispyware, in modo da garantire costantemente la protezione del sistema. È necessario riavviare Windows per disattivare l'HIPS o l'Autoprotezione.

Servizio protetto: attiva la protezione kernel (Windows 8.1, 10).

Lo **Scanner memoria avanzato** lavora congiuntamente all'Exploit Blocker per rafforzare il livello di protezione contro malware concepiti allo scopo di eludere il rilevamento dei prodotti antimalware mediante l'utilizzo di pratiche di offuscamento o crittografia. Per impostazione predefinita, lo scanner di memoria avanzato è attivato. Per ulteriori informazioni su questo tipo di protezione, consultare il glossario.

L'**Exploit Blocker** è progettato per rafforzare i tipi di applicazione comunemente utilizzati come browser Web, lettori PDF, client di posta e componenti di MS Office. L'exploit blocker è attivato per impostazione predefinita. Per ulteriori informazioni su questo tipo di protezione, consultare il glossario.

Protezione anti-ransomware è un altro livello di protezione che opera all'interno della funzione HIPS. È necessario disporre del sistema di reputazione LiveGrid attivo per fare funzionare la protezione anti-ransomware. Per ulteriori informazioni su questo tipo di protezione, fare clic qui.

Il filtraggio può essere eseguito in una delle quattro seguenti modalità:

Modalità automatica: le operazioni sono attivate, ad eccezione di quelle bloccate dalle regole predefinite che proteggono il sistema.

Modalità intelligente: all'utente verranno segnalati solo gli eventi molto sospetti.

Modalità interattiva: all'utente verrà richiesto di confermare le operazioni.

Modalità basata su criteri: le operazioni sono bloccate.

Modalità riconoscimento: le operazioni sono attivate e dopo ogni operazione viene creata una regola. Le regole create in questa modalità possono essere visualizzate nell'Editor regole, ma la loro priorità è inferiore rispetto alla priorità delle regole create manualmente o delle regole create nella modalità automatica. Selezionando la Modalità riconoscimento dal menu a discesa Modalità filtraggio HIPS, sarà disponibile l'impostazione **La modalità**

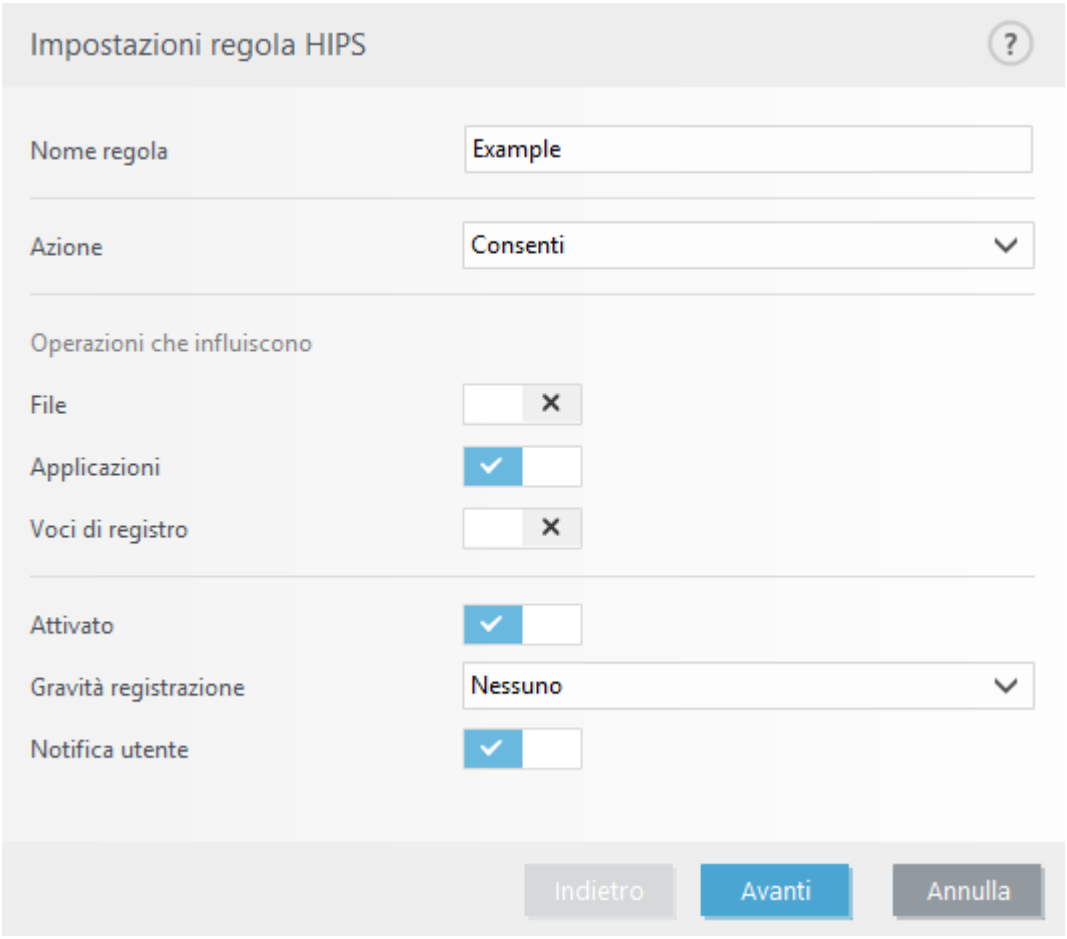
riconoscimento terminerà alle ore. Selezionare l'intervallo per il quale si desidera attivare la modalità riconoscimento, tenendo presente che il limite massimo è di 14 giorni. Una volta trascorsa la durata specificata, all'utente verrà richiesto di modificare le regole create dall'HIPS quando si trovava in modalità riconoscimento. È inoltre possibile scegliere un'altra modalità di filtraggio oppure posticipare la decisione e continuare a utilizzare la modalità riconoscimento.

Impostazione modalità dopo la scadenza della modalità apprendimento: selezionare la modalità filtraggio che verrà utilizzata dopo la scadenza della modalità apprendimento.

Il sistema HIPS monitora gli eventi all'interno del sistema operativo e reagisce in base a regole simili a quelle utilizzate dal Firewall. Fare clic su **Modifica** accanto a Regole per aprire la finestra di gestione delle regole HIPS. Nella finestra Regole HIPS è possibile selezionare, aggiungere, modificare o rimuovere regole.

Nell'esempio seguente viene spiegato come limitare il comportamento indesiderato delle applicazioni:

1. Denominare la regola e selezionare **Blocca** nel menu a discesa **Azione**.
2. Attivare il pulsante **Notifica utente** per visualizzare una notifica tutte le volte che viene applicata una regola.
3. Selezionare almeno un'operazione alla quale verrà applicata la regola. Nella finestra **Applicazioni di origine**, selezionare**Tutte le applicazioni** dal menu a discesa per applicare la nuova regola a tutte le applicazioni che tentano di eseguire una delle operazioni dell'applicazione selezionata sulle applicazioni specificate dall'utente.
4. Selezionare **Modifica stato di un'altra applicazione** (tutte le operazioni sono descritte nella guida del prodotto, a cui è possibile accedere premendo F1).
5. Selezionare **Applicazioni specifiche** dal menu a discesa, quindi **Aggiungi** per aggiungere una o più applicazioni che si desidera proteggere.
6. Fare clic su **Fine** per salvare la nuova regola.



4.1.4.1 Configurazione avanzata

Le seguenti opzioni sono utili per eseguire il debug e l'analisi del comportamento di un'applicazione:

Caricamento driver sempre consentito: i driver selezionati sono sempre autorizzati a caricare indipendentemente dalla modalità di filtraggio configurata, eccetto nel caso in cui vengano bloccati esplicitamente da una regola dell'utente.

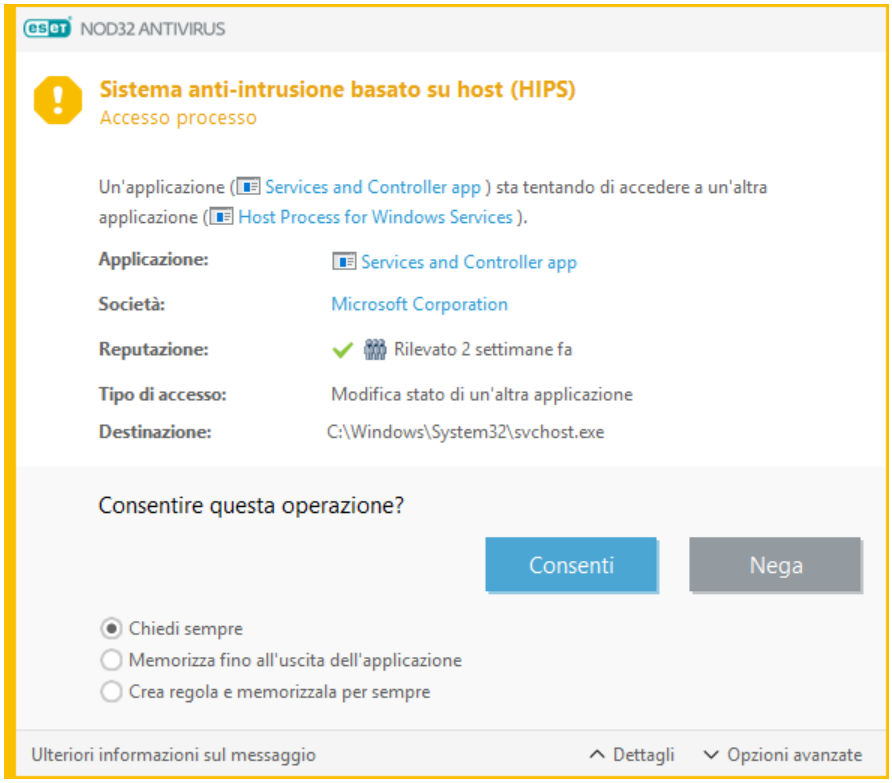
Registra tutte le operazioni bloccate: tutte le operazioni bloccate verranno scritte sul registro HIPS.

Notifica quando si verificano modifiche nelle applicazioni all'avvio: consente di visualizzare una notifica sul desktop ogni volta che un'applicazione viene aggiunta o rimossa dall'avvio del sistema.

Per una versione aggiornata di questa pagina della Guida, consultare l'articolo della Knowledge Base ESET.

4.1.4.2 Finestra interattiva HIPS

Se l'azione predefinita di una regola è impostata su **Chiedi**, verrà visualizzata una finestra di dialogo tutte le volte che la regola verrà attivata. È possibile scegliere di **Negare** o **Consentire** l'operazione. Se l'utente non sceglie un'azione nell'intervallo di tempo specifico, verrà selezionata una nuova azione in base alle regole.

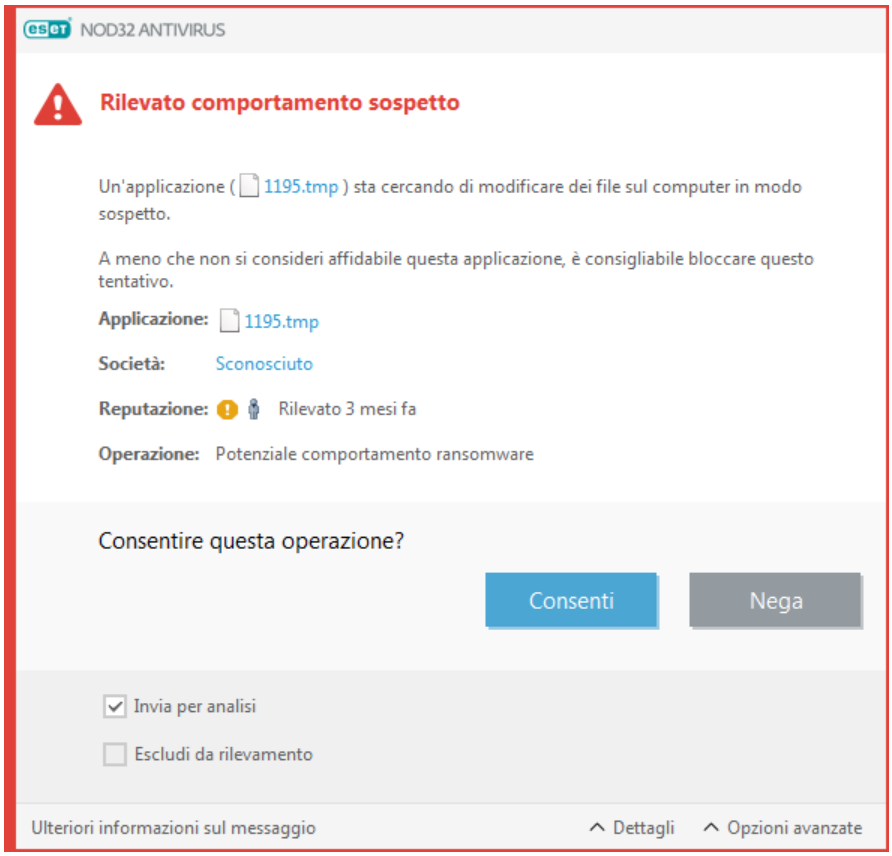


La finestra di dialogo consente all'utente di creare una regola in base a una qualsiasi nuova azione rilevata dall'HIPS e di definire le condizioni in base alle quali consentire o negare l'azione. Per accedere ai parametri corretti, fare clic su **Dettagli**. Le regole create in questo modo sono considerate equivalenti a quelle create manualmente. Una regola creata da una finestra di dialogo può quindi essere meno specifica rispetto alla regola che ha attivato tale finestra di dialogo. Ciò significa che, dopo aver creato questo tipo di regola, la stessa operazione può attivare la stessa finestra.

Memorizza fino all'uscita dell'applicazione causa un'azione (**Consenti/Nega**) da utilizzare finché non verrà apportata una modifica alle regole o alla modalità di filtraggio oppure non verrà eseguito un aggiornamento del modulo HIPS o un riavvio del sistema. In seguito a una di queste tre azioni, le regole temporanee verranno eliminate.

4.1.4.3 Rilevato potenziale comportamento ransomware

Questa finestra interattiva comparirà quando viene rilevato un comportamento che indica la presenza potenziale di ransomware. È possibile scegliere di **Negare** o **Consentire** l'operazione.



La finestra di dialogo consente di **inviare il file per l'analisi** o **escluderlo dalla rilevazione**. Fare clic su **Dettagli** per visualizzare i parametri specifici di rilevazione.

IMPORTANTE
ESET Live Grid deve essere attivo affinché la protezione ransomware funzioni correttamente.

4.1.5 Modalità giocatore

La modalità giocatore è una funzionalità pensata per gli utenti che richiedono un utilizzo ininterrotto del software, non desiderano essere disturbati dalle finestre popup e desiderano ridurre al minimo l'utilizzo della CPU. La modalità giocatore può essere utilizzata anche durante le presentazioni che non possono essere interrotte dall'attività antivirus. Attivando questa funzionalità, tutte le finestre popup vengono disattivate e l'attività di Pianificazione attività verrà completamente interrotta. La protezione del sistema è ancora in esecuzione in background ma non richiede alcun intervento da parte dell'utente.

È possibile attivare o disattivare la modalità giocatore nella finestra principale del programma in **Configurazione** > **Protezione computer** facendo clic su o accanto a **Modalità giocatore**. L'attivazione della modalità giocatore rappresenta un potenziale rischio per la protezione. Per tale motivo, l'icona relativa allo stato della protezione sulla barra delle attività diventa di colore arancione e viene visualizzato un avviso. Questo avviso verrà inoltre visualizzato nella finestra principale del programma dove **Modalità giocatore attivata** comparirà in arancione.

Attivare **Attiva modalità giocatore quando vengono eseguite automaticamente applicazioni in modalità a schermo intero** in **Configurazione avanzata** (F5) > **Strumenti** per attivare la modalità giocatore all'avvio di un'applicazione in modalità a schermo intero e interromperla all'uscita dall'applicazione.

Attivare **Disattiva automaticamente modalità giocatore dopo** per definire l'intervallo di tempo dopo il quale la modalità giocatore verrà automaticamente disattivata.

4.2 Protezione Internet

Le opzioni di configurazione del Web ed e-mail sono disponibili nel riquadro **Configurazione** facendo clic su **Protezione Internet**. Da qui è possibile accedere a impostazioni del programma più dettagliate.

La connettività Internet è una funzione standard dei personal computer. Purtroppo, Internet è diventato lo strumento principale per la distribuzione di codice dannoso. Per questo motivo, è essenziale gestire attentamente le impostazioni di **Protezione accesso Web**.

Fare clic su per aprire le impostazioni di protezione Web/e-mail/anti-phishing in Configurazione avanzata.

La **Protezione client di posta** garantisce il controllo delle comunicazioni via e-mail ricevute mediante i protocolli POP3 e IMAP. Utilizzando il programma plug-in per il client di posta in uso, ESET NOD32 Antivirus controlla tutte le comunicazioni da e verso il client di posta (POP3, MAPI, IMAP, HTTP).

La **Protezione Anti-Phishing** consente all'utente di bloccare le pagine Web che distribuiscono notoriamente contenuti phishing. Si consiglia vivamente di lasciare attivata l'opzione Anti-Phishing.

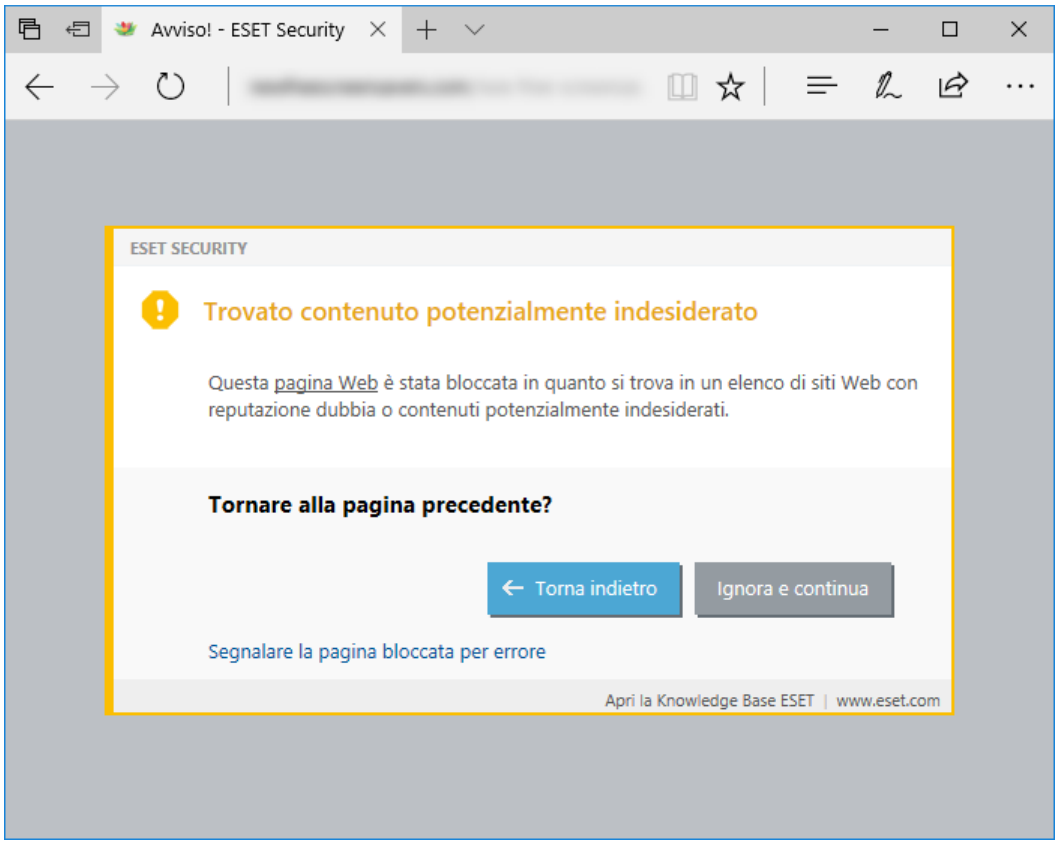
È possibile disattivare temporaneamente il modulo di protezione Web/e-mail Web/e-mail/anti-phishing facendo clic su .

4.2.1 Protezione accesso Web

La connettività Internet è una funzione standard in un personal computer. Purtroppo è diventato anche lo strumento principale per il trasferimento di codice dannoso. La Protezione accesso Web monitora la comunicazione tra i browser Web e i server remoti ed è conforme alle regole HTTP (Hypertext Transfer Protocol) e HTTPS (comunicazione crittografata).

L'accesso a pagine Web note per essere dannose è bloccato prima del download dei relativi contenuti. Tutte le altre pagine Web vengono controllate dal motore di controllo ThreatSense nel momento in cui vengono caricate e bloccate in caso di rilevamento di contenuti dannosi. La protezione accesso Web offre due livelli di protezione: il blocco in base alla blacklist e il blocco in base ai contenuti.

Si consiglia vivamente di attivare l'opzione Protezione accesso Web. L'opzione è disponibile dalla finestra principale di ESET NOD32 Antivirus accedendo a **Configurazione** > **Protezione Internet** > **Protezione accesso Web**.



Le seguenti opzioni sono disponibili in **Configurazione avanzata** (F5) > **Web ed e-mail** > **Protezione accesso Web**:

- **Protocolli Web**: consente all'utente di configurare il monitoraggio di questi protocolli standard utilizzati dalla maggior parte dei browser Internet.
- **Gestione indirizzi URL**: consente all'utente di specificare gli indirizzi HTTP da bloccare, consentire o escludere dal controllo.
- **Parametri di ThreatSense** – configurazione avanzata scanner antivirus: consente all'utente di configurare impostazioni quali tipi di oggetti da controllare (e-mail, archivi e così via.), metodi di rilevamento della protezione accesso Web, ecc.

4.2.1.1 Di base

Attiva protezione accesso Web: se questa opzione è disattivata, la protezione accesso Web e la protezione Anti-Phishing non saranno eseguite.

Attiva controllo avanzato degli script del browser: se questa opzione è attivata, tutti i programmi JavaScript eseguiti dai browser Internet verranno controllati dallo scanner antivirus.

NOTA
si consiglia vivamente di lasciare l'opzione Protezione accesso Web attivata.

4.2.1.2 Protocolli Web

Per impostazione predefinita, ESET NOD32 Antivirus è configurato per monitorare il protocollo HTTP utilizzato dalla maggior parte dei browser Internet.

Configurazione scanner HTTP

In Windows Vista e nelle versioni successive, il traffico HTTP viene monitorato sempre su tutte le porte di tutte le applicazioni. In Windows XP, è possibile modificare le **Porte utilizzate dal protocollo HTTP** in **Configurazione avanzata** (F5) > **Web ed e-mail** > **Protezione accesso Web** > **Protocolli Web**. Il traffico HTTP viene monitorato sulle porte specifiche di tutte le applicazioni e su tutte le porte delle applicazioni contrassegnate come Client Web e di posta.

Configurazione scanner HTTPS

ESET NOD32 Antivirus supporta anche il controllo del protocollo HTTPS. La comunicazione HTTPS utilizza un canale crittografato per trasferire le informazioni tra server e client. ESET NOD32 Antivirus controlla la comunicazione utilizzando i protocolli SSL (Secure Socket Layer) e TLS (Transport Layer Security). Il programma controllerà esclusivamente il traffico sulle porte definite in **Porte utilizzate dal protocollo HTTPS**, indipendentemente dalla versione del sistema operativo in uso.

La comunicazione crittografata non verrà controllata. Per attivare il controllo sulla comunicazione crittografata e visualizzare la configurazione dello scanner, accedere a SSL/TLS nella sezione Configurazione avanzata, fare clic su **Web e e-mail** > **SSL/TLS** e attivare l'opzione **Attiva filtraggio protocollo SSL/TLS**.

4.2.1.3 Gestione indirizzo URL

La sezione Gestione indirizzo URL consente di specificare gli indirizzi HTTP da bloccare, consentire o escludere dal controllo.

I siti Web presenti nell'**Elenco di indirizzi bloccati** non saranno accessibili a meno che non vengano anche inclusi nell'**Elenco di indirizzi consentiti**. Nei siti Web presenti nell'**Elenco di indirizzi esclusi dal controllo** non vengono ricercati codici dannosi al momento dell'accesso.

Se si desidera filtrare gli indirizzi HTTPS oltre alle pagine Web HTTP, è necessario selezionare **Attiva filtraggio protocollo SSL/TLS**. In caso contrario, verranno aggiunti solo i domini dei siti HTTPS visitati e non l'intero indirizzo URL.

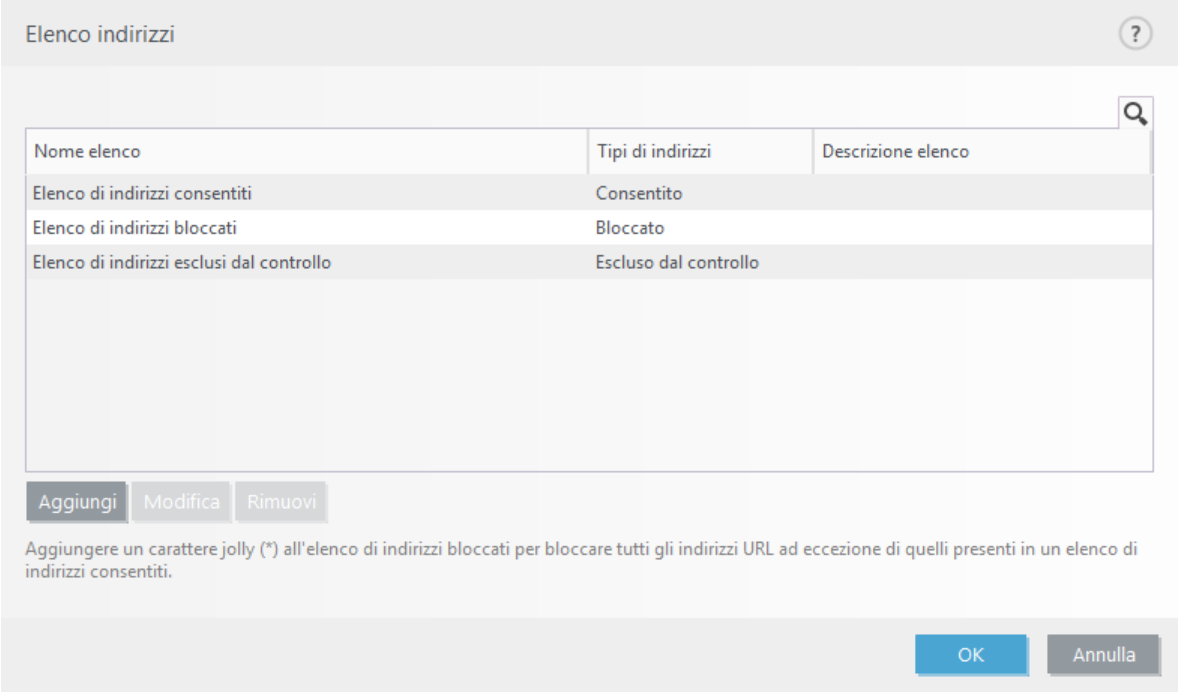
Se si aggiunge un indirizzo URL all'**Elenco indirizzi esclusi dal filtro**, l'indirizzo verrà escluso dal controllo. È inoltre possibile consentire o bloccare determinati indirizzi aggiungendoli all'**Elenco di indirizzi consentiti** o all'**Elenco di indirizzi bloccati**.

Se si desidera bloccare tutti gli indirizzi HTTP ad eccezione di quelli presenti nell'**Elenco di indirizzi consentiti** attivo, è necessario aggiungere * all'**Elenco di indirizzi bloccati** attivo.

Negli elenchi possono essere utilizzati i simboli speciali * (asterisco) e ? (punto interrogativo). L'asterisco sostituisce qualsiasi stringa di caratteri, mentre il punto interrogativo sostituisce qualsiasi simbolo. È necessario prestare particolare attenzione quando si specificano gli indirizzi esclusi, in quanto l'elenco dovrebbe contenere esclusivamente indirizzi affidabili e sicuri. Allo stesso modo, è necessario verificare che in questo elenco i simboli * e ? siano utilizzati correttamente. Consultare Aggiungi indirizzo HTTP/maschera di dominio per ulteriori

informazioni su come associare in maniera sicura un intero dominio, compresi tutti i sottodomini. Per attivare un elenco, selezionare **Elenco attivo**. Se si desidera ricevere una notifica relativa all'inserimento di un indirizzo contenuto nell'elenco corrente, selezionare **Notifica in caso di applicazione**.

NOTA
la gestione degli indirizzi URL consente inoltre di bloccare o consentire l'apertura di specifici tipi di file mentre l'utente naviga in Internet. Ad esempio, se l'utente non desidera aprire file eseguibili, selezionare l'elenco dove si desidera bloccare questi file dal menu a discesa, quindi immettere la maschera "**.exe".



Elementi di controllo

Aggiungi: crea un nuovo elenco oltre a quelli predefiniti. Questa opzione è utile se si desidera suddividere vari gruppi di indirizzi in base a criteri logici. Ad esempio, un elenco di indirizzi bloccati potrebbe contenere indirizzi provenienti da una blacklist pubblica esterna e un altro la blacklist dell'utente. In tal modo, si facilita l'aggiornamento dell'elenco esterno mantenendo nel contempo intatto quello dell'utente.

Modifica: modifica gli elenchi esistenti. Utilizzare questa funzione per aggiungere o rimuovere indirizzi.

Rimuovi: rimuove gli elenchi esistenti. Questa funzione è disponibile esclusivamente per gli elenchi creati con **Aggiungi** e non per quelli predefiniti.

4.2.2 Protezione client di posta

4.2.2.1 Client di posta

L'integrazione di ESET NOD32 Antivirus con il client e-mail aumenta il livello di protezione attiva contro codici dannosi nei messaggi e-mail. Se il client di posta in uso è supportato, è possibile attivare l'integrazione in ESET NOD32 Antivirus. In caso di integrazione nel client di posta, la barra degli strumenti di ESET NOD32 Antivirus viene inserita direttamente nel client di posta (ad eccezione di quella relativa alle versioni più recenti di Windows Live Mail), garantendo in tal modo una protezione più efficiente dei messaggi di posta elettronica. Le impostazioni relative all'integrazione sono disponibili sotto a **Configurazione avanzata** (F5) > **Web ed email** > **Protezione client email** > **Client email**.

Integrazione con client di posta

I client di posta attualmente supportati sono Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail. Per questi programmi, la protezione e-mail funziona come un plug-in. Il vantaggio principale offerto dal plug-in consiste nella sua indipendenza dal protocollo utilizzato. Quando il client di posta riceve un messaggio

crittografato, questo viene decodificato e inviato allo scanner antivirus. Per un elenco completo dei client di posta supportati e delle relative versioni, consultare il seguente articolo della Knowledge Base ESET.

Anche se l'integrazione non è attivata, la comunicazione e-mail rimane comunque protetta tramite il modulo di protezione client di posta (POP3, IMAP).

Attivare **Disattiva controllo in caso di variazione dei contenuti della casella** se si riscontrano rallentamenti del sistema quando si utilizza MS Outlook. Ciò può accadere durante il recupero di messaggi e-mail da Kerio Outlook Connector Store.

Messaggi e-mail da controllare

Attiva protezione e-mail tramite plug-in client: in caso di disattivazione della protezione delle e-mail attraverso il client di posta, continuerà a essere attivo il controllo del client di posta tramite il filtraggio protocolli.
E-mail ricevuta: attiva/disattiva il controllo dei messaggi ricevuti.
E-mail inviata: attiva/disattiva il controllo dei messaggi inviati.
E-mail letta: attiva/disattiva il controllo dei messaggi letti.

Azione da eseguire sui messaggi e-mail infetti

Nessuna azione: se questa opzione è attivata, il programma identificherà gli allegati infetti senza tuttavia eseguire alcuna azione.
Elimina e-mail: il programma notificherà all'utente l'eventuale o le eventuali infiltrazioni ed eliminerà il messaggio.
Sposta e-mail nella cartella Posta eliminata: le e-mail infette verranno spostate automaticamente nella cartella Posta eliminata.
Sposta e-mail nella cartella: i messaggi e-mail infetti verranno spostati automaticamente nella cartella specificata.

Cartella: specificare la cartella personalizzata in cui si desidera spostare le e-mail infette una volta rilevate.

Ripeti controllo dopo l'aggiornamento: attiva/disattiva un nuovo controllo dopo un aggiornamento del motore di rilevamento.

Accetta i risultati del controllo da altri moduli: selezionando questa opzione, il modulo di protezione e-mail accetterà i risultati del controllo eseguito da altri moduli di protezione (controllo protocolli POP3, IMAP).

NOTA
si consiglia di attivare le opzioni **Attiva protezione e-mail tramite plug-in client** e **Attiva protezione e-mail tramite filtraggio protocolli**. Queste impostazioni sono disponibili sotto a Configurazione avanzata (F5) > Web ed email > Protezione client email > Protocolli email).

4.2.2.2 Protocolli e-mail

IMAP e POP3 sono i protocolli più comunemente utilizzati per ricevere comunicazioni e-mail in un'applicazione client di posta. IMAP (Internet Message Access Protocol) è un altro protocollo Internet per il recupero dei messaggi e-mail. Il protocollo IMAP offre alcuni vantaggi rispetto al protocollo POP3, tra cui, ad esempio, la possibilità di connettere simultaneamente più di un client alla stessa casella di posta e conservare informazioni sullo stato del messaggio (lettura, invio di risposta o eliminazione). ESET NOD32 Antivirus offre protezione per questi protocolli, indipendentemente dal client di posta utilizzato e senza richiedere la riconfigurazione del client di posta.

Il modulo di protezione che fornisce questo controllo viene avviato automaticamente all'avvio del sistema e resta quindi attivo in memoria. Il controllo del protocollo IMAP viene eseguito automaticamente senza che sia necessario riconfigurare il client di posta. Per impostazione predefinita, vengono controllate tutte le comunicazioni della porta 143, ma se necessario è possibile aggiungere altre porte di comunicazione. I numeri delle porte devono essere separati da una virgola.

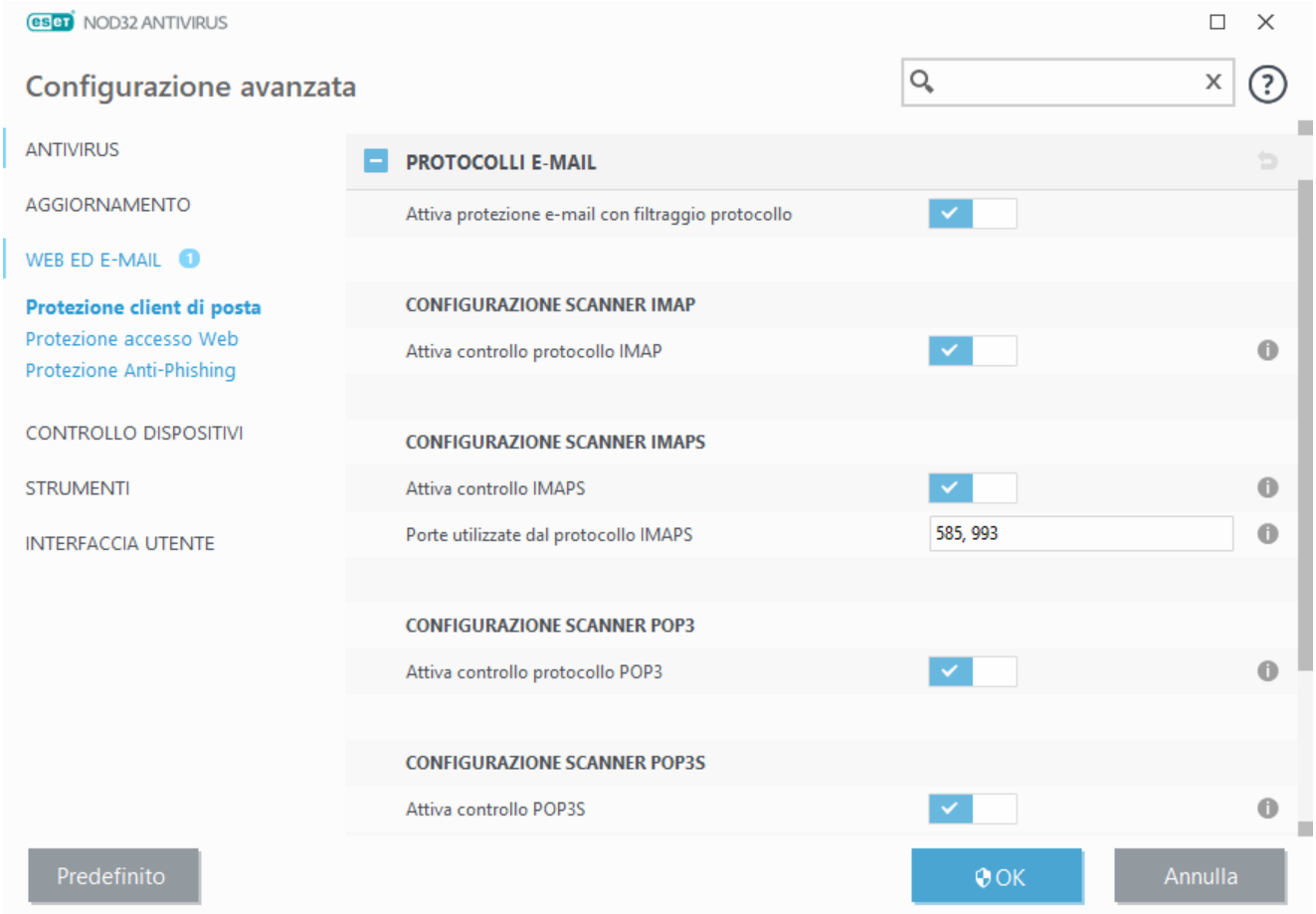
È possibile configurare il controllo dei protocolli IMAP/IMAPS e POP3/POP3S in Configurazione avanzata. Per accedere a questa impostazione, espandere **Web e e-mail** > **Protezione client di posta** > **Protocolli e-mail**.

Attiva protezione e-mail tramite filtraggio protocollo: attiva il controllo dei protocolli e-mail.

In Windows Vista e nelle versioni successive, i protocolli IMAP e POP3 vengono rilevati e controllati automaticamente su tutte le porte. In Windows XP, per tutte le applicazioni vengono controllate solo le **Porte utilizzate dal protocollo IMAP/POP3**, mentre per le applicazioni contrassegnate come Client Web e di posta vengono controllate tutte le porte.

ESET NOD32 Antivirus supporta anche il controllo dei protocolli IMAPS e POP3S che utilizzano un canale crittografato per trasferire le informazioni tra server e client. ESET NOD32 Antivirus controlla la comunicazione utilizzando i protocolli SSL (Secure Socket Layer) e TLS (Transport Layer Security). Il programma controllerà esclusivamente il traffico sulle porte definite in **Porte utilizzate dal protocollo HTTPS/POP3S**, indipendentemente dalla versione del sistema operativo utilizzato dall'utente.

La comunicazione crittografata non verrà controllata. Per attivare il controllo sulla comunicazione crittografata e visualizzare la configurazione dello scanner, accedere a SSL/TLS nella sezione Configurazione avanzata, fare clic su **Web e e-mail** > **SSL/TLS** e attivare l'opzione **Attiva filtraggio protocollo SSL/TLS**.



4.2.2.3 Avvisi e notifiche

La Protezione client di posta garantisce il controllo delle comunicazioni e-mail ricevute mediante i protocolli POP3 e IMAP. Utilizzando il plug-in per Microsoft Outlook e altri client e-mail, ESET NOD32 Antivirus controlla tutte le comunicazioni dal client e-mail (POP3, MAPI, IMAP, HTTP). Durante la verifica dei messaggi in arrivo, il programma utilizza tutti i metodi di controllo avanzato previsti nel motore di controllo ThreatSense. Ciò significa che il rilevamento di programmi dannosi viene eseguito ancora prima del confronto con il motore di rilevamento. La scansione delle comunicazioni mediante i protocolli POP3 e IMAP non dipende dal client e-mail in uso.

Le opzioni di questa funzionalità sono disponibili in **Configurazione avanzata** sotto a **Web ed e-mail** > **Protezione client di posta** > **Avvisi e notifiche**.

Dopo che un messaggio e-mail è stato controllato, una notifica contenente i risultati di scansione può essere aggiunta al messaggio. È possibile scegliere le opzioni **Aggiungi notifiche all'e-mail ricevuta e letta**, **Aggiungi nota all'oggetto dell'e-mail infetta ricevuta e letta** o l'opzione **Aggiungi notifiche all'e-mail inviata**. Tenere presente che, in rare occasioni, le notifiche potrebbero essere omesse in messaggi HTML problematici o creati da malware. Le

notifiche possono essere aggiunte sia alle e-mail ricevute e lette sia alle e-mail inviate. Sono disponibili le seguenti opzioni:

- **Mai**: non viene aggiunto alcun messaggio.
- **Solo per l'e-mail infetta**: solo i messaggi contenenti software dannoso vengono contrassegnati come controllati (impostazione predefinita).
- **A tutte le e-mail controllate**: il programma aggiunge i messaggi a tutte le e-mail sottoposte a controllo.

Aggiungi nota all'oggetto dell'e-mail infetta inviata: disattivare questa opzione se non si desidera che la protezione e-mail includa un avviso antivirus nell'oggetto di un'e-mail infetta. Questa funzione consente di filtrare in modo semplice le e-mail infette in base all'oggetto (se supportata dal programma e-mail in uso). Permette anche di aumentare il livello di credibilità del destinatario. Se viene rilevata un'intrusione, fornisce informazioni preziose sul livello di minaccia di un indirizzo email o mittente.

Template aggiunto all'oggetto dell'e-mail infetta: modificare questo template se si desidera cambiare il formato predefinito dell'oggetto di un'e-mail infetta. Questa funzione sostituirà l'oggetto del messaggio *"Ciao"* con un determinato valore predefinito *"[virus]"* nel seguente formato: *"[virus] Ciao"*. La variabile *%VIRUSNAME%* rappresenta la minaccia rilevata.

4.2.2.4 Integrazione con client e-mail

L'integrazione di ESET NOD32 Antivirus con i client e-mail aumenta il livello di protezione attiva contro codici dannosi nei messaggi e-mail. Se il client di posta in uso è supportato, è possibile attivare l'integrazione in ESET NOD32 Antivirus. In caso di attivazione dell'integrazione, la barra degli strumenti di ESET NOD32 Antivirus viene inserita direttamente nel client di posta, garantendo in tal modo una protezione e-mail più efficace. Le impostazioni relative all'integrazione sono disponibili in **Configurazione** > **Configurazione avanzata** > **Web e e-mail** > **Protezione client di posta** > **Client di posta**.

I client di posta attualmente supportati sono Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail. Per un elenco completo dei client e-mail supportati e delle relative versioni, fare riferimento al seguente articolo della Knowledge Base ESET.

Selezionare la casella di controllo accanto a **Disattiva il controllo alla modifica del contenuto della posta in arrivo** se si riscontra un rallentamento del sistema durante l'utilizzo del client di posta. Ciò può accadere durante il recupero di e-mail da Kerio Outlook Connector Store.

Anche se l'integrazione non è attivata, la comunicazione e-mail rimane comunque protetta tramite il modulo di protezione client e-mail (POP3, IMAP).

4.2.2.4.1 Configurazione della protezione client di posta

Il modulo di protezione client di posta supporta i seguenti client di posta: Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail. Per questi programmi la protezione e-mail esegue la stessa funzione di un plugin. Il vantaggio principale offerto dal plugin consiste nella sua indipendenza dal protocollo utilizzato. Quando il client di posta riceve un messaggio crittografato, questo viene decodificato e inviato al programma di scanner antivirus.

4.2.2.5 Filtro POP3, POP3S

Il protocollo POP3 è quello più diffuso per la ricezione di comunicazioni e-mail in un'applicazione client e-mail. ESET NOD32 Antivirus offre la protezione per questo protocollo, indipendentemente dal client e-mail in uso.

Il modulo di protezione che fornisce questo controllo viene avviato automaticamente all'avvio del sistema e resta quindi attivo in memoria. Perché il modulo funzioni correttamente, verificare che sia attivato: il controllo del protocollo POP3 viene eseguito automaticamente senza che sia necessario riconfigurare il client di posta. Per impostazione predefinita, vengono sottoposte a scansione tutte le comunicazioni della porta 110, ma se necessario è possibile aggiungere altre porte di comunicazione. I numeri delle porte devono essere separati da una virgola.

La comunicazione crittografata non verrà controllata. Per attivare il controllo sulla comunicazione crittografata e visualizzare la configurazione dello scanner, accedere a SSL/TLS nella sezione Configurazione avanzata, fare clic su **Web e e-mail** > **SSL/TLS** e attivare l'opzione **Attiva filtraggio protocollo SSL/TLS**.

In questa sezione è possibile configurare il controllo dei protocolli POP3 e POP3S.

Attiva controllo protocollo POP3: se questa opzione è attivata, tutto il traffico POP3 viene monitorato per rilevare il software dannoso.

Porte utilizzate dal protocollo POP3: elenco delle porte utilizzate dal protocollo POP3 (110 per impostazione predefinita).

ESET NOD32 Antivirus supporta anche il controllo del protocollo POP3S. Questo tipo di comunicazione utilizza un canale crittografato per trasferire le informazioni tra server e client. ESET NOD32 Antivirus controlla le comunicazioni utilizzando i metodi di crittografia SSL (Secure Socket Layer) e TLS (Transport Layer Security).

Non effettuare il controllo POP3S: la comunicazione crittografata non verrà controllata.

Effettua controllo protocollo POP3S per le porte selezionate: selezionare questa opzione per attivare il controllo POP3S solo per le porte definite in **Porte utilizzate dal protocollo POP3S**.

Porte utilizzate dal protocollo POP3S: elenco delle porte POP3S da controllare (995 per impostazione predefinita).

4.2.3 Filtraggio protocolli

La protezione antivirus per i protocolli delle applicazioni viene offerta dal motore di controllo ThreatSense, che integra perfettamente tutte le tecniche di controllo avanzato dei malware. Il filtraggio protocolli funziona automaticamente, indipendentemente dal browser Internet o dal client di posta in uso. Per modificare le impostazioni crittografate (SSL/TLS), accedere a **Web ed e-mail** > **SSL/TLS**.

Attiva filtraggio contenuto protocollo applicazioni: può essere utilizzato per disattivare il filtraggio dei protocolli. Tenere presente che il funzionamento di numerosi componenti di ESET NOD32 Antivirus (protezione accesso Web, protezione protocolli e-mail, Anti-Phishing, controllo Web) dipende interamente da questa funzione.

Applicazioni escluse: consente all'utente di escludere applicazioni specifiche dal filtraggio protocolli. Questa funzione è utile in caso di problemi di compatibilità causati dal filtraggio protocolli.

Indirizzi IP esclusi: consente all'utente di escludere indirizzi remoti specifici dal filtraggio protocolli. Questa funzione è utile in caso di problemi di compatibilità causati dal filtraggio protocolli.

Client Web e di posta: questa funzione, utilizzata solo sui sistemi operativi Windows XP, consente all'utente di selezionare le applicazioni per cui l'intero traffico viene filtrato dalla funzione di filtraggio protocolli, indipendentemente dalle porte utilizzate.

4.2.3.1 Web e client di posta

NOTA
in Windows Vista Service Pack 1 e Windows Server 2008 per il controllo delle comunicazioni di rete viene utilizzata la nuova architettura Windows Filtering Platform (WFP). Poiché la tecnologia WPF utilizza speciali tecniche di monitoraggio, la sezione **Web e client di posta** non è disponibile.

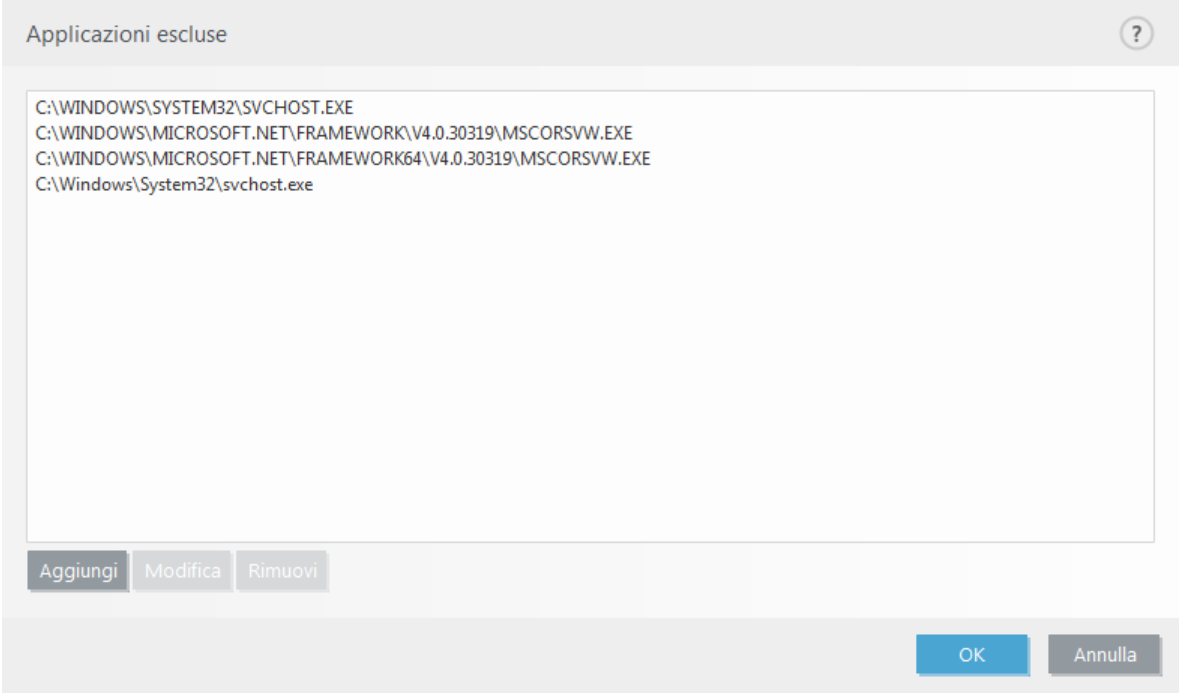
A causa dell'enorme quantità di codice dannoso che circola su Internet, una navigazione Internet sicura è essenziale per la protezione del computer. Le vulnerabilità dei browser Web e i collegamenti fraudolenti aiutano il codice dannoso a penetrare inosservato nel sistema. Per tale motivo, ESET NOD32 Antivirus si focalizza sulla sicurezza dei browser Web. Ogni applicazione che accede alla rete può essere contrassegnata come un browser. La casella di controllo presenta due stati:

- **Deselezionata**: la comunicazione delle applicazioni viene filtrata solo per le porte specificate.
- **Selezionata**: la comunicazione viene sempre filtrata (anche se viene impostata una porta differente).

4.2.3.2 Applicazioni escluse

Per escludere la comunicazione di specifiche applicazioni di rete dal filtraggio dei contenuti, selezionarle nell'elenco. Sulla comunicazione HTTP/POP3/IMAP delle applicazioni selezionate non verrà eseguito il rilevamento delle minacce. È consigliabile usare questa opzione solo per le applicazioni che non funzionano correttamente se la rispettiva comunicazione viene sottoposta a controllo.

L'esecuzione di applicazioni e servizi sarà disponibile automaticamente. Fare clic su **Aggiungi** per aggiungere manualmente un'applicazione non visualizzata nell'elenco del filtraggio protocolli.

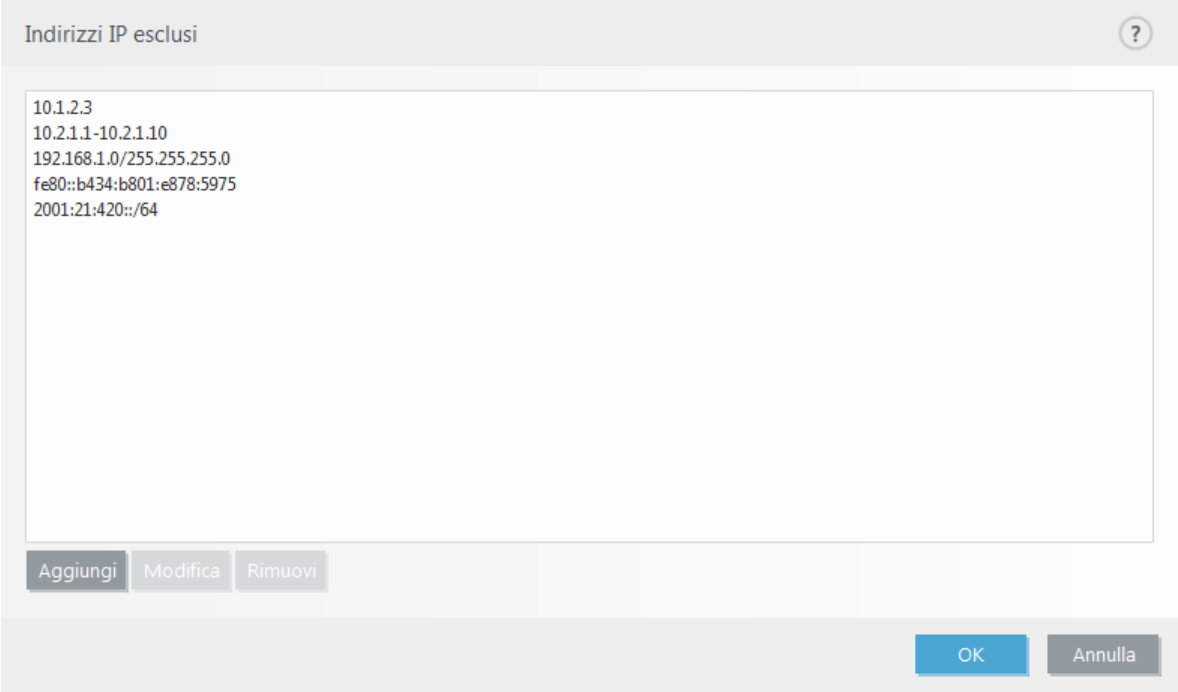


4.2.3.3 Indirizzi IP esclusi

Le voci presenti nell'elenco saranno escluse dal filtraggio del contenuto del protocollo. Sulla comunicazione HTTP/POP3/IMAP da/verso gli indirizzi selezionati non verrà eseguito il rilevamento delle minacce. È consigliabile utilizzare questa opzione solo per gli indirizzi di cui è nota l'affidabilità.

Fare clic su **Aggiungi** per escludere un indirizzo IP/intervallo di indirizzi/subnet di un punto remoto non visualizzato sull'elenco del filtro protocolli.

Fare clic su **Rimuovi** per rimuovere le voci selezionate dall'elenco.



4.2.3.3.1 Aggiungi indirizzo IPv4

Ciò consente di aggiungere un indirizzo/intervallo di indirizzi/subnet IP di un punto remoto a cui si applica la regola. Sebbene sia il più vecchio, il protocollo Internet versione 4 è quello maggiormente utilizzato.

Indirizzo singolo: aggiunge l'indirizzo IP di un singolo computer a cui deve essere applicata la regola (ad esempio *192.168.0.10*).

Intervallo di indirizzi: immettere il primo e l'ultimo indirizzo IP per specificare l'intervallo IP (di più computer) per cui deve essere applicata la regola (ad esempio da *192.168.0.1* a *192.168.0.99*).

Subnet: subnet (gruppo di computer) definita da un indirizzo IP e da una maschera.

Ad esempio, *255.255.255.0* è la maschera di rete per il prefisso *192.168.1.0/24*, che indica l'intervallo di indirizzi compreso tra *192.168.1.1* e *192.168.1.254*.

4.2.3.3.2 Aggiungi indirizzo IPv6

Ciò consente di aggiungere un indirizzo/una subnet IPv6 di un punto remoto a cui si applica la regola. Si tratta della versione più recente del protocollo Internet e sostituirà la versione precedente 4.

Indirizzo singolo: aggiunge l'indirizzo IP di un singolo computer a cui deve essere applicata la regola (ad esempio *2001:718:1c01:16:214:22ff:fec9:ca5*).

Subnet: subnet (gruppo di computer) definita da un indirizzo IP e da una maschera (ad esempio: *2002:c0a8:6301:1::1/64*).

4.2.3.4 SSL/TLS

ESET NOD32 Antivirus è in grado di ricercare le minacce contenute nelle comunicazioni che utilizzano il protocollo SSL. È possibile utilizzare varie modalità di controllo per l'analisi delle comunicazioni protette dal protocollo SSL con certificati attendibili, certificati sconosciuti o certificati che sono esclusi dal controllo delle comunicazioni protette dal protocollo SSL.

Attiva filtraggio protocollo SSL/TLS: se il filtraggio protocolli è disattivato, il programma non controllerà le comunicazioni sull'SSL.

La **Modalità filtraggio protocollo SSL/TLS** è disponibile nelle seguenti opzioni:

Modalità automatica: la modalità predefinita eseguirà il controllo esclusivamente delle applicazioni appropriate quali browser Web e client di posta. È possibile ignorare questa funzione selezionando le applicazioni per le quali le comunicazioni verranno sottoposte al controllo.

Modalità interattiva: all'accesso a un nuovo sito protetto da SSL (con un certificato sconosciuto), viene visualizzata una finestra di dialogo per la scelta dell'azione. Questa modalità consente di creare un elenco di certificati / applicazioni SSL che verranno esclusi dal controllo.

Modalità criteri: selezionare questa opzione per controllare tutte le comunicazioni protette dal protocollo SSL ad eccezione delle comunicazioni protette dai certificati esclusi dal controllo. Se viene stabilita una nuova comunicazione usando un certificato firmato sconosciuto, all'utente non verrà inviata alcuna notifica e la comunicazione verrà filtrata in modo automatico. Quando si accede a un server con un certificato non attendibile contrassegnato come attendibile (presente nell'elenco dei certificati attendibili), la comunicazione con il server è consentita e il contenuto del canale di comunicazione viene filtrato.

Elenco di applicazioni filtrate tramite SSL: consente all'utente di personalizzare il comportamento di ESET NOD32 Antivirus per specifiche applicazioni.

Elenco di certificati noti: consente all'utente di personalizzare il comportamento di ESET NOD32 Antivirus per specifici certificati SSL.

Escludi comunicazioni protette con certificati con validità estesa (EV): se questa opzione è attivata, la comunicazione con questo tipo di certificato SSL sarà esclusa dal controllo. I certificati SSL con validità estesa assicurano all'utente che sta visitando il sito Web desiderato e non un sito contraffatto assolutamente identico a quello desiderato (in genere i siti di phishing).

Blocca le comunicazioni crittografate che utilizzano il protocollo obsoleto SSL v2: la comunicazione che utilizza la versione precedente del protocollo SSL verrà automaticamente bloccata.

Certificato radice

Aggiungi il certificato radice ai browser conosciuti: affinché la comunicazione SSL funzioni in modo adeguato nei browser/client di posta dell'utente, è fondamentale che il certificato radice di ESET venga aggiunto all'elenco dei certificati radice noti (autori). Quando questa opzione è attivata, ESET NOD32 Antivirus aggiungerà automaticamente il certificato radice di ESET ai browser conosciuti (ad esempio, Opera e Firefox). Per i browser che utilizzano l'archivio di certificazioni di sistema, il certificato viene aggiunto automaticamente (ad esempio, Internet Explorer).

Per applicare il certificato a browser non supportati, fare clic su **Visualizza certificato** > **Dettagli** > **Copia su file...** e importarlo manualmente nel browser.

Validità del certificato

Se il certificato non può essere verificato mediante l'utilizzo dell'archivio certificati TRCA: in alcuni casi, non è possibile verificare la validità del certificato di un sito Web utilizzando l'archivio Autorità di certificazione radice attendibili (TRCA). Ciò significa che il certificato è firmato da qualcuno (ad esempio, l'amministratore di un server Web o di una piccola azienda) e considerare questo certificato come attendibile non rappresenta sempre un rischio per la sicurezza. Gran parte delle aziende di grandi dimensioni (ad esempio, le banche) utilizza un certificato firmato dal TRCA. Dopo aver selezionato **Chiedi conferma della validità dei certificati** (impostazione predefinita), all'utente verrà richiesto di selezionare un'azione da eseguire in caso di comunicazione

crittografata. È possibile selezionare **Blocca comunicazioni che utilizzano il certificato** per terminare sempre le connessioni crittografate ai siti con certificati non verificati.

Se il certificato è danneggiato o non valido: ciò significa che il certificato è scaduto o che la firma era errata. In questo caso, è consigliabile lasciare selezionata l'opzione **Blocca comunicazioni che utilizzano il certificato**.

4.2.3.4.1 Certificati

Affinché le comunicazioni SSL funzionino in modo adeguato nei browser/client di posta, è fondamentale che il certificato radice per ESET sia aggiunto all'elenco dei certificati radice noti (autori). È necessario attivare **Aggiungi il certificato radice ai browser conosciuti**. Selezionare questa opzione per aggiungere automaticamente il certificato radice di ESET ai browser conosciuti (ad esempio, Opera e Firefox). Per i browser che utilizzano l'archivio di certificazioni di sistema, il certificato viene aggiunto automaticamente (ad esempio, Internet Explorer). Per applicare il certificato a browser non supportati, fare clic su **Visualizza certificato** > **Dettagli** > **Copia su file...**, quindi importarlo manualmente nel browser.

In alcuni casi non è possibile verificare la validità del certificato mediante l'archivio Autorità di certificazione radice attendibili (ad esempio VeriSign). Ciò significa che il certificato è auto-firmato da qualcuno (ad esempio, l'amministratore di un server Web o una piccola azienda) e considerare questo certificato come attendibile non rappresenta sempre un rischio per la sicurezza. La maggior parte delle principali aziende (ad esempio, le banche) utilizza un certificato firmato da TRCA. Dopo aver selezionato **Chiedi conferma della validità dei certificati** (impostazione predefinita), all'utente verrà richiesto di selezionare un'azione da eseguire in caso di comunicazione crittografata. Verrà visualizzata una finestra di dialogo in cui l'utente potrà scegliere se contrassegnare il certificato come attendibile o escluso. Nel caso in cui il certificato non sia presente nell'elenco TRCA, la finestra sarà rossa. In caso contrario, sarà di colore verde.

È possibile selezionare **Blocca la comunicazione che utilizza il certificato** per terminare sempre una connessione crittografata al sito che utilizza il certificato non verificato.

Se il certificato non è valido oppure è danneggiato, significa che è scaduto o che l'auto-firma era errata. In questo caso, è consigliabile bloccare la comunicazione che utilizza il certificato.

4.2.3.4.1.1 Traffico di rete crittografato

Se il computer è configurato per la scansione del protocollo SSL, potrebbe essere visualizzata una finestra di dialogo mediante la quale viene chiesto di scegliere un'azione da eseguire quando si tenta di stabilire una connessione crittografata (usando un certificato sconosciuto).

La finestra di dialogo contiene le seguenti informazioni:

- nome dell'applicazione che ha avviato la comunicazione
- nome del certificato utilizzato
- azione da eseguire - se effettuare il controllo della comunicazione crittografata e se ricordare l'azione per l'applicazione / certificato

Se non si trova nell'Archivio Autorità di certificazione radice attendibili (TRCA), il certificato è considerato non attendibile.

4.2.3.4.2 Elenco di certificati noti

L'**Elenco di certificati noti** può essere utilizzato per la personalizzazione del comportamento di ESET NOD32 Antivirus per specifici certificati SSL e per ricordare le azioni scelte se in **Modalità filtraggio protocollo SSL/TSL** viene selezionata la **Modalità interattiva**. L'elenco può essere visualizzato e modificato in **Configurazione avanzata** (F5) > **Web e e-mail** > **SSL/TLS** > **Elenco di certificati noti**.

La finestra **Elenco di certificati noti** è formata da:

Colonne

Nome: nome del certificato.

Autorità di certificazione emittente: nome del creatore del certificato.

Oggetto certificato: campo dell'oggetto che identifica l'entità associata alla chiave pubblica archiviata nel campo Chiave pubblica dell'oggetto.

Accesso: selezionare **Consenti** o **Blocca** come **Azione di accesso** per consentire/bloccare la comunicazione protetta da questo certificato indipendentemente dalla sua attendibilità. Selezionare **Auto** per consentire i certificati attendibili e richiedere quelli inattendibili. Selezionare **Chiedi** per chiedere sempre all'utente cosa fare.

Controlla: selezionare **Controlla** o **Ignora** come **Azione di controllo** per controllare o ignorare la comunicazione protetta da questo certificato. Selezionare **Auto** per eseguire il controllo in modalità automatica e attivare la richiesta in modalità interattiva. Selezionare **Chiedi** per chiedere sempre all'utente cosa fare.

Elementi di controllo

Aggiungi: aggiungere un nuovo certificato e configurare le impostazioni relative all'accesso e le opzioni di controllo.

Modifica: selezionare il certificato che si desidera configurare e fare clic su **Modifica**.

Rimuovi: selezionare il certificato che si desidera eliminare e fare clic su **Rimuovi**.

OK/Annulla: fare clic su **OK** se si desidera salvare le modifiche o su **Annulla** per uscire senza salvare.

4.2.3.4.3 Elenco di applicazioni filtrate tramite SSL/TLS

L'**Elenco di applicazioni filtrate tramite SSL/TLS** può essere utilizzato per la personalizzazione del comportamento di ESET NOD32 Antivirus per specifiche applicazioni e per ricordare le azioni scelte se in **Modalità filtraggio protocollo SSL/TLS** viene selezionata la **Modalità interattiva**. L'elenco può essere visualizzato e modificato in **Configurazione avanzata** (F5) > **Web ed e-mail** > **SSL/TLS** > **Elenco di applicazioni filtrate tramite SSL/TLS**.

La finestra **Elenco di applicazioni filtrate tramite SSL/TLS** è formata da:

Colonne

Applicazione : nome dell'applicazione.

Azione di controllo: selezionare **Controlla** o **Ignora** per controllare o ignorare la comunicazione. Selezionare **Auto** per eseguire il controllo in modalità automatica e attivare la richiesta in modalità interattiva. Selezionare **Chiedi** per chiedere sempre all'utente cosa fare.

Elementi di controllo

Aggiungi : consente di aggiungere l'applicazione filtrata.

Modifica: selezionare il certificato che si desidera configurare e fare clic su **Modifica**.

Rimuovi: selezionare il certificato che si desidera eliminare e fare clic su **Rimuovi**.

OK/Annulla: fare clic su **OK** se si desidera salvare le modifiche o su **Annulla** per uscire senza salvare.

4.2.4 Protezione Anti-Phishing

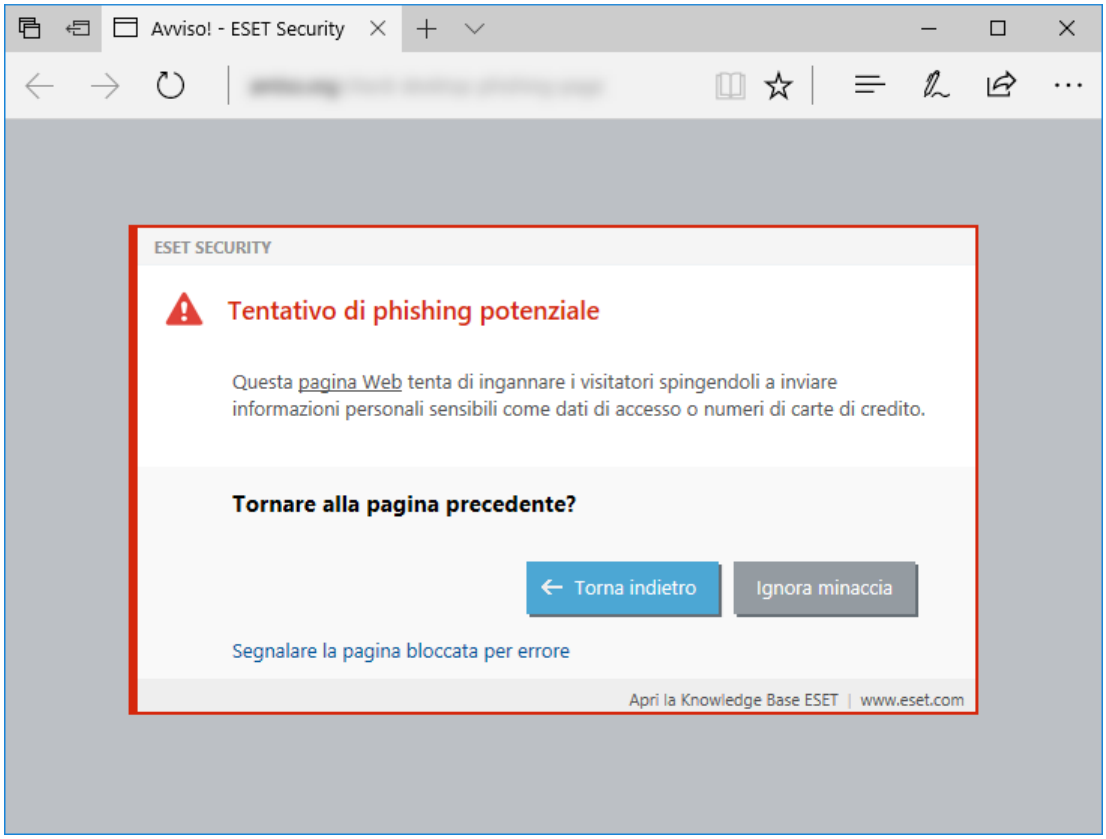
Il termine phishing definisce un'attività illegale che si avvale dell'ingegneria sociale (ovvero di manipolazione degli utenti al fine di ottenere informazioni riservate). Il phishing viene spesso utilizzato per ottenere l'accesso a dati sensibili quali numeri di conti bancari, codici PIN e così via. Per ulteriori informazioni su questa attività, consultare il glossario. ESET NOD32 Antivirus integra sistemi di protezione anti-phishing, ovvero una funzione che blocca pagine Web note per distribuire questo tipo di contenuto.

Si consiglia vivamente di attivare la funzione Anti-Phishing in ESET NOD32 Antivirus. A tale scopo, aprire **Configurazione avanzata** (F5) e accedere a **Web ed e-mail** > **Protezione Anti-Phishing**.

Consultare l'articolo della Knowledge Base per ulteriori informazioni sulla protezione Anti-Phishing in ESET NOD32 Antivirus.

Accesso ad un sito Web phishing

Accedendo a un sito Web phishing riconosciuto, nel browser Web in uso comparirà la seguente finestra di dialogo. Se si desidera ancora accedere al sito Web, fare clic su **Ignora minaccia** (scelta non consigliata).



NOTA
per impostazione predefinita, i potenziali siti Web phishing che sono stati inseriti nella whitelist scadranno dopo alcune ore. Per consentire un sito Web in modo permanente, utilizzare lo strumento Gestione indirizzi URL. Da **Configurazione avanzata** (F5), espandere **Web ed e-mail** > **Protezione accesso Web** > **Gestione indirizzi URL** > **Elenco indirizzi**, fare clic su **Modifica** e aggiungere all'elenco il sito Web che si desidera modificare.

Segnalazione di un sito phishing

Il collegamento Segnala consente di segnalare un sito Web phishing/dannoso a ESET ai fini dell'analisi.

NOTA
prima di inviare un sito Web a ESET, assicurarsi che soddisfi uno o più dei criteri seguenti:

- il sito Web non viene rilevato,
- il sito Web viene erroneamente rilevato come una minaccia. In questo caso, è possibile Segnalare la pagina bloccata per errore.

In alternativa, è possibile inviare il sito Web tramite e-mail. Inviare l'e-mail a campioni@eset.com. Ricordare di utilizzare un oggetto descrittivo e di fornire il maggior numero di informazioni possibile sul sito Web (ad esempio, il sito Web che ha condotto l'utente sulla pagina in questione, come si è venuti a conoscenza del sito Web, ecc.).

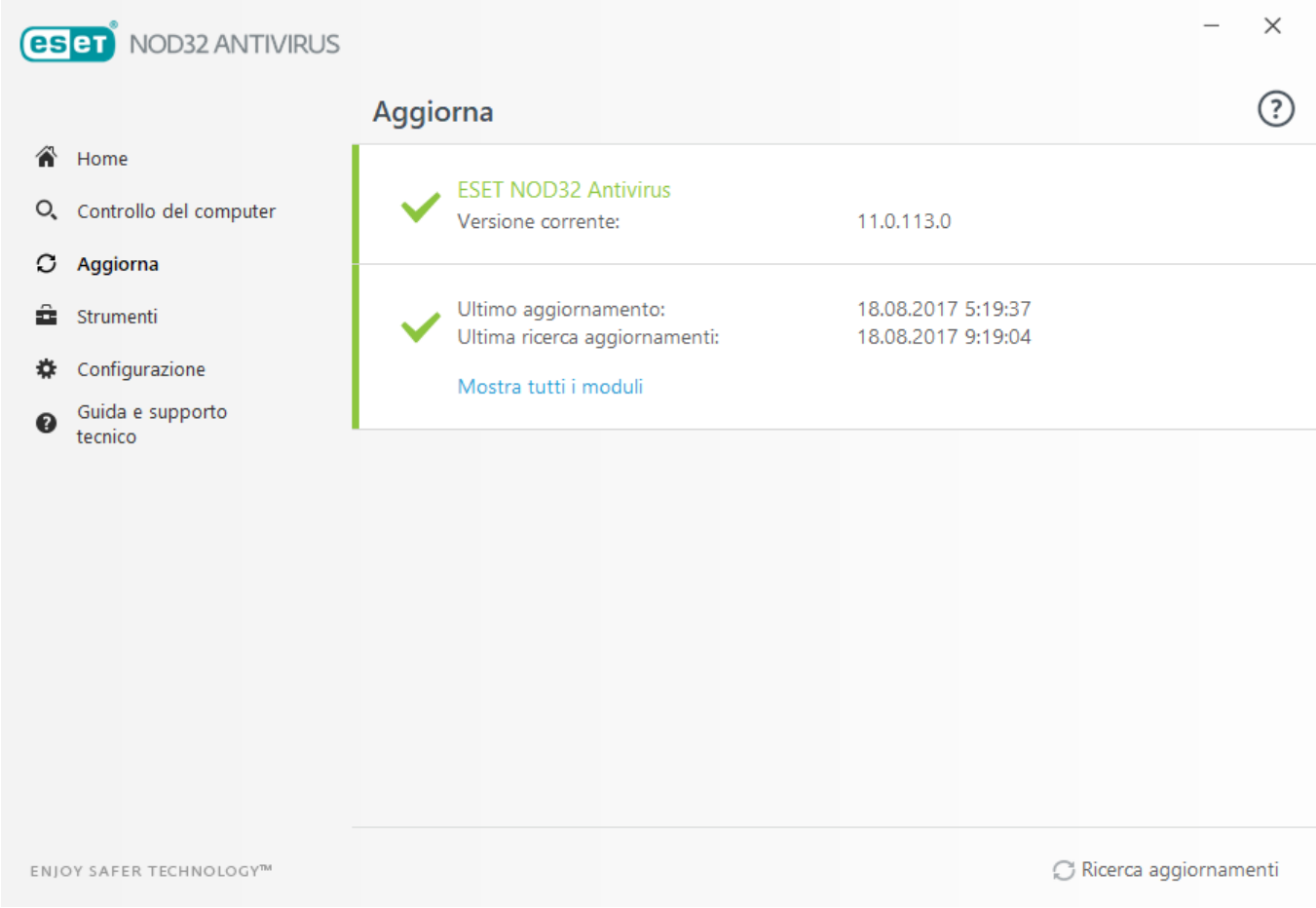
4.3 Aggiornamento del programma

L'aggiornamento periodico di ESET NOD32 Antivirus rappresenta il metodo migliore per garantire il livello massimo di protezione del computer. Il modulo di aggiornamento garantisce il costante aggiornamento dei moduli del programma e dei componenti del sistema.

Facendo clic su **Aggiorna** nella finestra principale del programma, è possibile visualizzare lo stato corrente degli aggiornamenti, comprese la data e l'ora dell'ultimo aggiornamento eseguito correttamente, e valutare l'eventuale necessità di un aggiornamento.

Oltre agli aggiornamenti automatici, è possibile fare clic su **Ricerca aggiornamenti** per avviare un aggiornamento manuale. L'aggiornamento periodico dei moduli e dei componenti del programma garantisce il mantenimento di una protezione completa contro codici dannosi. È opportuno prestare particolare attenzione alla relativa configurazione e al funzionamento. Per ricevere gli aggiornamenti, è necessario attivare il prodotto tramite la Chiave di licenza. Se durante l'installazione non è stata eseguita questa operazione, è possibile inserire la chiave di licenza per attivare il prodotto durante l'aggiornamento per accedere ai server di aggiornamento di ESET.

NOTA
la chiave di licenza viene inviata tramite e-mail da ESET dopo l'acquisto di ESET NOD32 Antivirus.



Versione corrente: consente di visualizzare il numero della versione corrente del prodotto installata.

Ultimo aggiornamento: consente di visualizzare la data dell'ultimo aggiornamento. Se non viene visualizzata una data recente, i moduli del prodotto potrebbero non essere aggiornati.

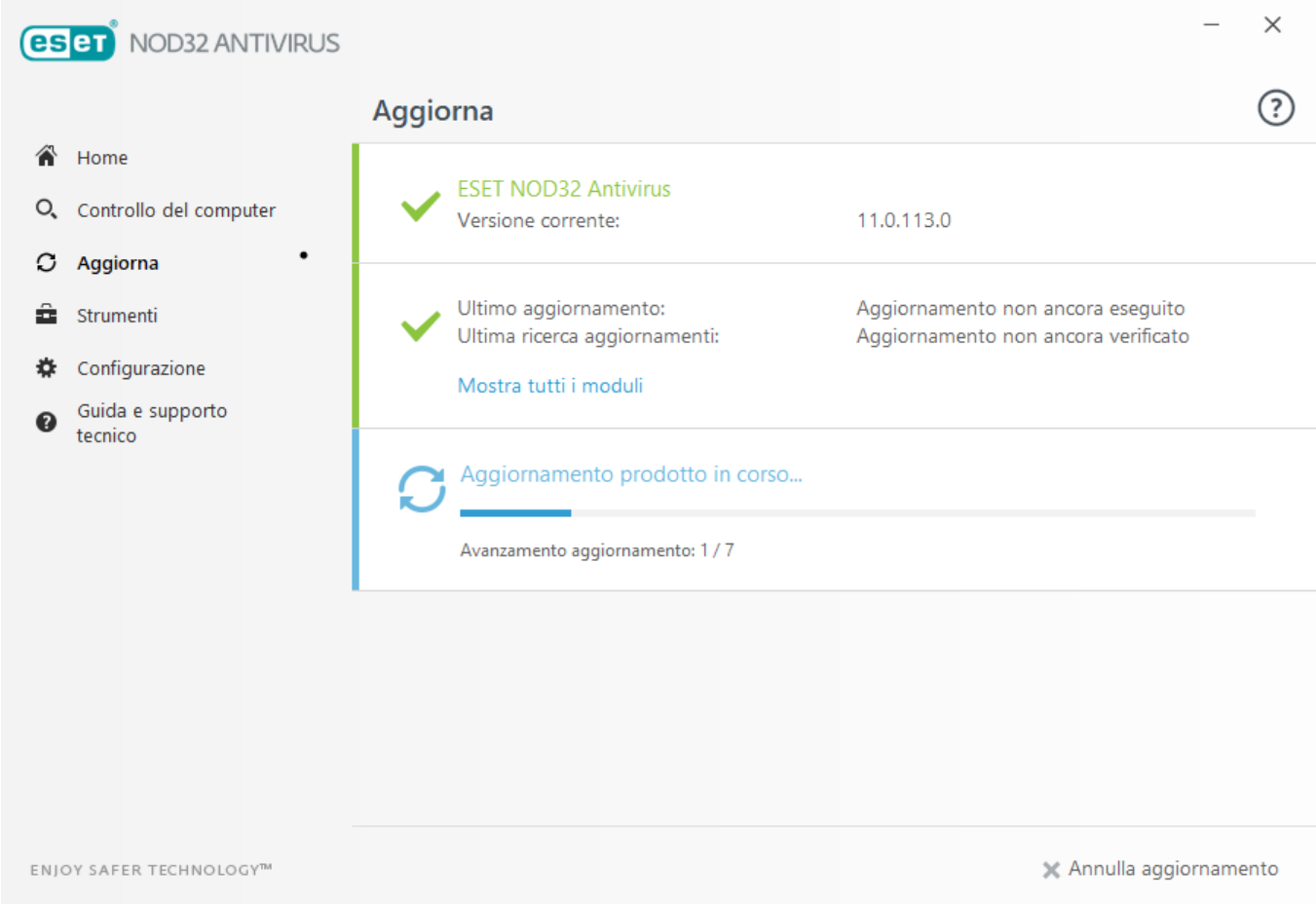
Ultima ricerca aggiornamenti: consente di visualizzare la data dell'ultima ricerca degli aggiornamenti.

Mostra tutti i moduli: consente di visualizzare le informazioni sull'elenco dei moduli del programma installati.

Fare clic su **Ricerca aggiornamenti** per verificare la disponibilità della versione di ESET NOD32 Antivirus più recente.

Processo di aggiornamento

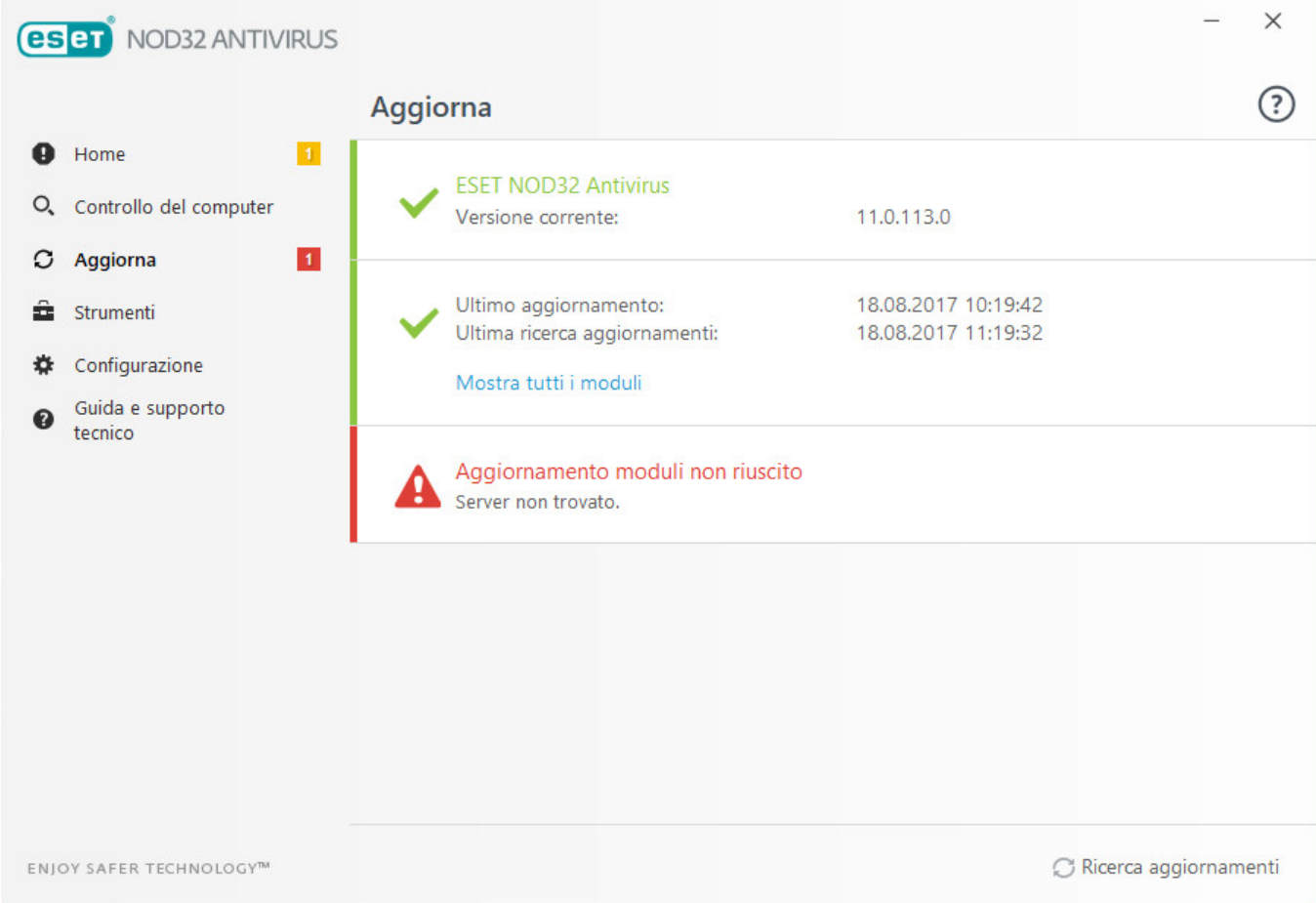
Dopo aver selezionato **Ricerca aggiornamenti**, verrà avviato il download. Verranno visualizzati una barra di avanzamento del download e il tempo rimanente per il completamento dell'operazione. Per interrompere l'aggiornamento, fare clic su **Annulla l'aggiornamento**.



IMPORTANTE
In condizioni normali, nella finestra **Aggiorna** compare il segno di spunta verde che indica che il programma è aggiornato. In caso contrario, il programma è obsoleto ed è maggiormente esposto alle infezioni. Aggiornare i moduli il prima possibile.

Il messaggio di notifica precedente è correlato ai due messaggi che seguono, relativi ad aggiornamenti non riusciti:

1. **Licenza non valida**: la chiave di licenza non è stata inserita correttamente durante la configurazione dell'aggiornamento. Si consiglia di verificare i dati di autenticazione. Nella finestra Configurazione avanzata (fare clic su **Configurazione** nel menu principale, quindi su **Configurazione avanzata** oppure premere **F5** sulla tastiera), sono disponibili ulteriori opzioni di aggiornamento. Fare clic su **Guida e supporto tecnico** > **Modifica licenza** nel menu principale per inserire una nuova chiave di licenza.
2. **Si è verificato un errore durante il download dei file di aggiornamento**: questo errore potrebbe essere causato da Impostazioni di connessione Internet non corrette. Si consiglia di verificare la connettività Internet (aprendo un qualsiasi sito Web nel browser). Se il sito Web non si apre, è possibile che la connessione Internet non sia presente o che si siano verificati problemi di connettività nel computer in uso. Se la connessione Internet non è attiva, contattare il proprio Provider di servizi Internet (ISP).



NOTA
Per ulteriori informazioni, consultare questo articolo della Knowledge Base di ESET.

4.3.1 Aggiorna impostazioni

Le opzioni di configurazione degli aggiornamenti sono disponibili nella struttura **Configurazione avanzata** (F5) sotto a **Aggiornamento** > **Di base**. Questa sezione consente di specificare informazioni sull'origine degli aggiornamenti, come ad esempio i server di aggiornamento e i dati per l'autenticazione di tali server.

Generale

Il profilo di aggiornamento attualmente in uso viene visualizzato nel menu a discesa **Profilo di aggiornamento**. Per creare un nuovo profilo, fare clic su **Modifica** accanto a **Elenco di profili**, inserire il proprio **Nome profilo**, quindi fare clic su **Aggiungi**.

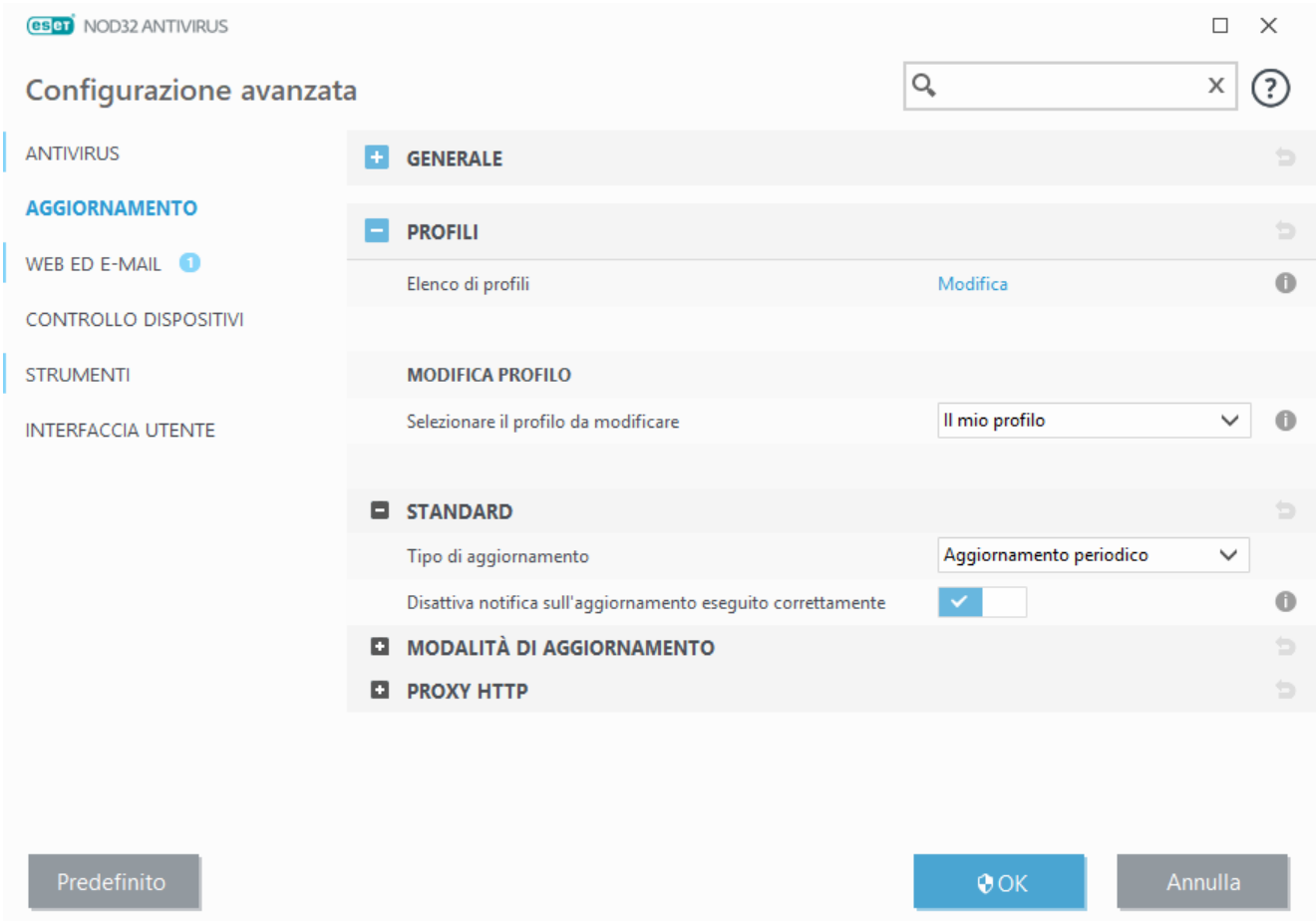
In caso di problemi durante il download degli aggiornamenti del motore di rilevamento, fare clic su **Cancella** per eliminare i file/la cache di aggiornamento temporanei.

Rollback

Se si sospetta che un nuovo aggiornamento del database delle firme antivirali e/o dei moduli del programma possa essere instabile o danneggiato, è possibile ripristinare la versione precedente e disattivare gli aggiornamenti per un determinato periodo di tempo. In alternativa, è possibile attivare gli aggiornamenti precedentemente disattivati in caso di rimando indefinito da parte dell'utente.

ESET NOD32 Antivirus registra gli snapshot del motore di rilevamento e dei moduli del programma da utilizzare con la funzione *rollback*. Per creare snapshot del database delle firme antivirali, lasciare selezionato il pulsante **Crea snapshot dei file di aggiornamento**. Il campo **Numero di snapshot memorizzati localmente** definisce il numero di snapshot del database delle firme antivirali precedentemente archiviati.

Se si seleziona **Rollback** (**Configurazione avanzata** (F5) > **Aggiorna** > **Generale**), è necessario scegliere un intervallo temporale dal menu a discesa che indica il periodo di tempo nel quale gli aggiornamenti del motore di rilevamento e del modulo di programma verranno sospesi.



Per scaricare correttamente gli aggiornamenti, occorre inserire tutti i parametri di aggiornamento richiesti. Se si utilizza un firewall, assicurarsi che al programma ESET sia consentito di comunicare con Internet (ad esempio, comunicazione HTTP).

Di base

Per impostazione predefinita, il **Tipo di aggiornamento** è impostato su **Aggiornamento periodico** per garantire che i file di aggiornamento vengano scaricati automaticamente dal server ESET che presenta il traffico di rete minore. Gli aggiornamenti pre-rilascio (opzione **Aggiornamento pre-rilascio**) sono aggiornamenti sottoposti ad approfondite verifiche interne che saranno presto disponibili per tutti. Gli aggiornamenti pre-rilascio consentono di accedere ai metodi di rilevamento e alle correzioni più recenti. È tuttavia probabile che tali aggiornamenti non siano sempre sufficientemente stabili e NON devono pertanto essere utilizzati su server di produzione e workstation dove è richiesta massima disponibilità e stabilità.

Disattiva visualizzazione notifiche relative agli aggiornamenti eseguiti correttamente: disattiva la notifica sulla barra delle applicazioni nell'angolo in basso a destra della schermata. È utile selezionare questa opzione se è in esecuzione un'applicazione a schermo intero o un videogioco. Tenere presente che la modalità giocatore disattiverà tutte le notifiche.

4.3.1.1 Aggiorna profili

Per varie configurazioni e attività di aggiornamento è possibile creare profili di aggiornamento. La creazione dei profili di aggiornamento è particolarmente utile per gli utenti mobili che necessitano di un profilo alternativo per le proprietà di connessione a Internet, soggette a periodici cambiamenti.

Nel menu a discesa **Profilo di aggiornamento** è possibile visualizzare il profilo correntemente selezionato, configurato per impostazione predefinita come **Profilo personale**. Per creare un nuovo profilo, fare clic su **Modifica** accanto a **Elenco di profili**, inserire il proprio **Nome profilo**, quindi fare clic su **Aggiungi**.

4.3.1.2 Impostazione aggiornamento avanzata

Le opzioni avanzate della configurazione dell'aggiornamento includono l'impostazione della **Modalità di aggiornamento**, **Proxy HTTP**.

4.3.1.2.1 Modalità di aggiornamento

La scheda **Modalità di aggiornamento** contiene opzioni correlate agli aggiornamenti periodici dei programmi. Queste impostazioni consentono all'utente di definire preventivamente il comportamento del programma in caso di disponibilità di una nuova versione del motore di rilevamento o degli aggiornamenti dei componenti di programma.

Gli aggiornamenti dei componenti di programma, che prevedono nuove funzioni oppure modifiche relative alle funzioni delle versioni precedenti, sono inclusi negli aggiornamenti periodici (motore di rilevamento). Una volta installato l'aggiornamento dei componenti di programma, potrebbe essere necessario riavviare il computer.

Sono disponibili le seguenti impostazioni:

Aggiornamento applicazione: se questa opzione è attivata, l'aggiornamento di ciascun componente del programma sarà eseguito automaticamente e senza avvisi senza eseguire l'aggiornamento completo del prodotto.

Attiva aggiornamento manuale componenti del programma: disattivato per impostazione predefinita. Se questa opzione è attivata ed è disponibile una versione più recente di ESET NOD32 Antivirus, è possibile ricercare gli aggiornamenti nel riquadro **Aggiorna** e **installare** la versione più recente.

Chiedi prima di scaricare l'aggiornamento: se questa opzione è attiva, l'utente visualizzerà una notifica e il sistema chiederà di confermare l'installazione di eventuali aggiornamenti disponibili prima che venga eseguita l'operazione.

Chiedi se le dimensioni di un file di aggiornamento sono maggiori di (kB): se le dimensioni del file di aggiornamento superano i valori specificati qui, l'utente visualizzerà una notifica e il sistema chiederà di confermare l'installazione di eventuali aggiornamenti disponibili prima che venga eseguita l'operazione.

4.3.1.2.2 Proxy HTTP

Per accedere alle opzioni di configurazione del server proxy per uno specifico profilo di aggiornamento, fare clic su **Aggiorna** nella struttura **Configurazione avanzata** (F5), quindi su **Proxy HTTP**. Fare clic sul menu a discesa **Modalità proxy** e selezionare una delle tre seguenti opzioni:

- Non utilizzare server proxy
- Connessione tramite server proxy
- Utilizza impostazioni server proxy globali

Selezionare l'opzione **Utilizza impostazioni server proxy globali**, per utilizzare le opzioni di configurazione del server proxy già specificate all'interno della sottostruttura **Strumenti** > **Server proxy** della struttura Configurazione avanzata.

Selezionare **Non utilizzare server proxy** per specificare che non verrà utilizzato alcun server proxy per l'aggiornamento di ESET NOD32 Antivirus.

Selezionare l'opzione **Connessione tramite server proxy** nei seguenti casi:

- Viene utilizzato un server proxy diverso da quello definito in **Strumenti** > **Server proxy** per aggiornare ESET NOD32 Antivirus. In questa configurazione, le informazioni per il nuovo proxy devono essere specificate sotto indirizzo **Server proxy**, **Porta** di comunicazione (3128 di default) e **Nome utente** e **Password** per il server proxy, se richiesta.
- Le impostazioni del server proxy non sono impostate a livello globale. ESET NOD32 Antivirus si connetterà tuttavia a un server proxy per verificare la disponibilità di aggiornamenti.
- Il computer è connesso a Internet tramite un server proxy. Le impostazioni vengono estrapolate da Internet Explorer durante l'installazione del programma, ma se successivamente vengono modificate, ad esempio se si cambia il provider di servizi Internet (ISP), verificare che le impostazioni del proxy HTTP visualizzate in questa finestra siano corrette. In caso contrario, il programma non sarà in grado di connettersi ai server di aggiornamento.

L'impostazione predefinita per il server proxy è **Utilizza impostazioni server proxy globali**.

Utilizza la connessione diretta in assenza di proxy: se irraggiungibile, il proxy sarà disabilitato durante l'aggiornamento.

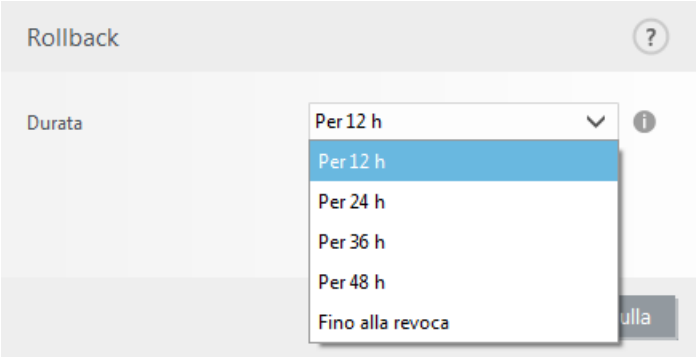
NOTA
I campi **Nome utente** e **Password** di questa sezione sono specifici per il server proxy. Compilare questi campi solo se è necessario inserire un nome utente ed una password per accedere al server proxy. Questi campi non costituiscono nome utente e password per ESET NOD32 Antivirus e devono essere completati solo se è necessaria una password per accedere a Internet mediante un server proxy.

4.3.2 Rollback aggiornamento

Se si sospetta che un nuovo aggiornamento del motore di rilevamento e/o dei moduli del programma possa essere instabile o danneggiato, è possibile ripristinare la versione precedente e disattivare gli aggiornamenti per un determinato periodo di tempo. In alternativa, è possibile attivare gli aggiornamenti precedentemente disattivati in caso di rimando indefinito da parte dell'utente.

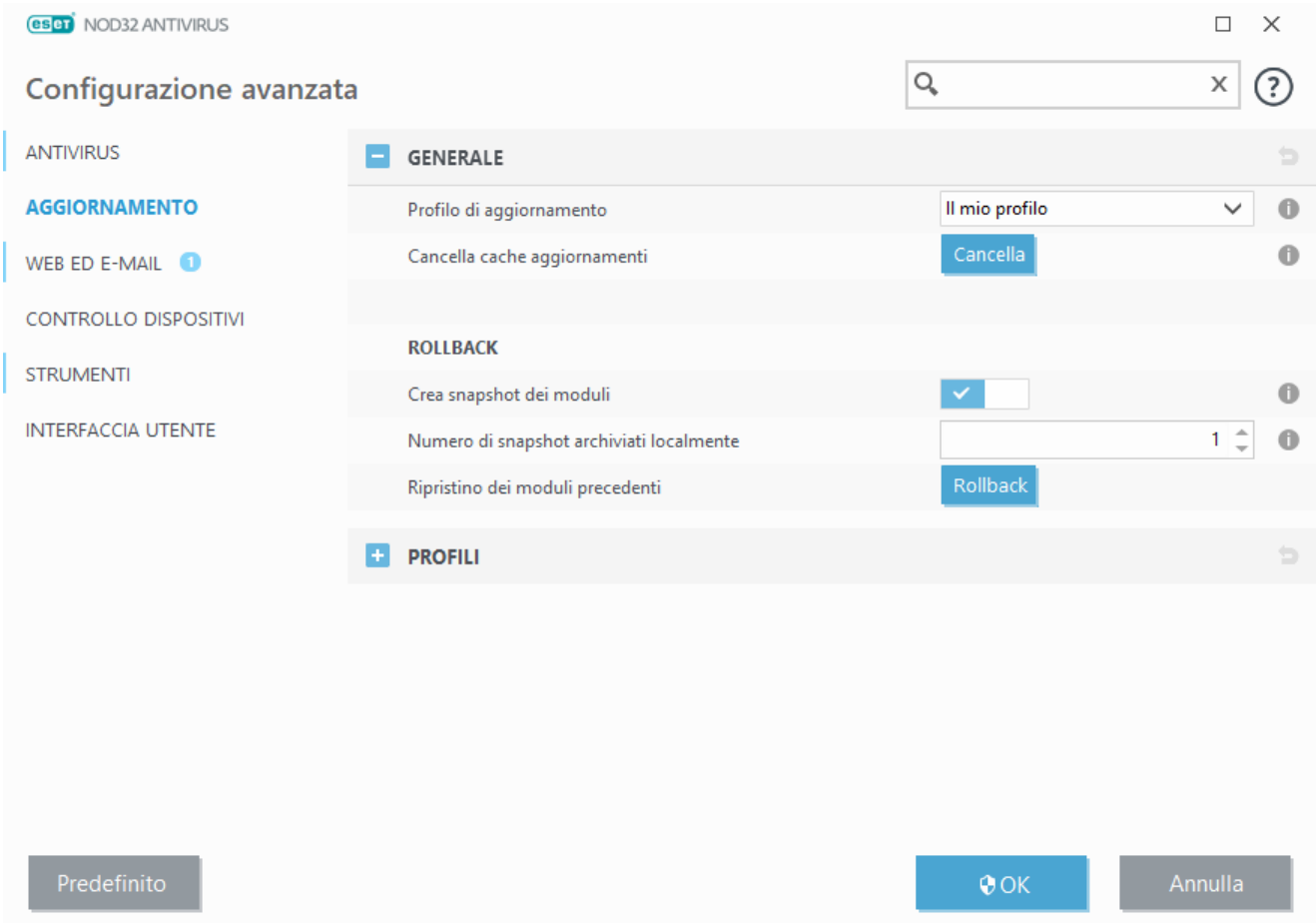
ESET NOD32 Antivirus registra gli snapshot del motore di rilevamento e dei moduli del programma da utilizzare con la funzione *rollback*. Per creare snapshot del motore di rilevamento, lasciare selezionata la casella di controllo **Crea snapshot dei file di aggiornamento**. Il campo **Numero di snapshot memorizzati localmente** definisce il numero di snapshot del motore di rilevamento precedentemente archiviati.

Se si seleziona **Rollback** (**Configurazione avanzata** (F5) > **Aggiorna** > **Generale**), è necessario scegliere un intervallo temporale dal menu a discesa **Durata** che indica il periodo di tempo nel quale gli aggiornamenti del motore di rilevamento e del modulo di programma verranno sospesi.



Selezionare **Fino a revoca** per rimandare in modo indefinito gli aggiornamenti periodici finché l'utente non avrà ripristinato la funzionalità degli aggiornamenti manualmente. Non è consigliabile selezionare questa opzione in quanto rappresenta un potenziale rischio per la protezione.

Se viene eseguito un rollback, il pulsante **Annulla** si trasforma in **Consenti aggiornamenti**. Non saranno consentiti aggiornamenti per l'intervallo di tempo selezionato nel menu a discesa **Sospendi aggiornamenti**. Il motore di rilevamento viene ripristinato alla versione più vecchia disponibile e memorizzato come snapshot nel file system del computer locale.



NOTA

Si supponga che la versione più recente del motore di rilevamento corrisponde al numero 6871. Le versioni 6870 e 6868 sono memorizzate come snapshot del motore di rilevamento. Si noti che la versione 6869 non è disponibile poiché, ad esempio, il computer è stato spento ed è stato reso disponibile un aggiornamento più recente prima che venisse scaricata la versione 6869. Se il campo **Numero di snapshot memorizzati localmente** è impostato su 2 e si fa clic su **Roll back**, il motore di rilevamento (compresi i moduli del programma) viene ripristinato al numero di versione 6868. L'operazione potrebbe richiedere alcuni minuti. Controllare che il motore di rilevamento sia stato ripristinato a una versione precedente dalla finestra principale del programma di ESET NOD32 Antivirus nella sezione Aggiorna.

4.3.3 Come fare per creare attività di aggiornamento

È possibile avviare gli aggiornamenti manualmente facendo clic su **Ricerca aggiornamenti** nella finestra principale visualizzata dopo aver selezionato **Aggiorna** dal menu principale.

Gli aggiornamenti possono essere eseguiti anche come attività programmate. Per configurare un'attività programmata, fare clic su **Strumenti** > **Pianificazione attività**. Per impostazione predefinita, in ESET NOD32 Antivirus sono attivate le seguenti attività:

- **Aggiornamento automatico regolare**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**

È possibile modificare ciascuna delle attività di aggiornamento in base alle proprie esigenze. Oltre alle attività di aggiornamento predefinite, è possibile creare nuove attività di aggiornamento con una configurazione definita dall'utente. Per ulteriori dettagli sulla creazione e sulla configurazione delle attività di aggiornamento, consultare la sezione Pianificazione attività.

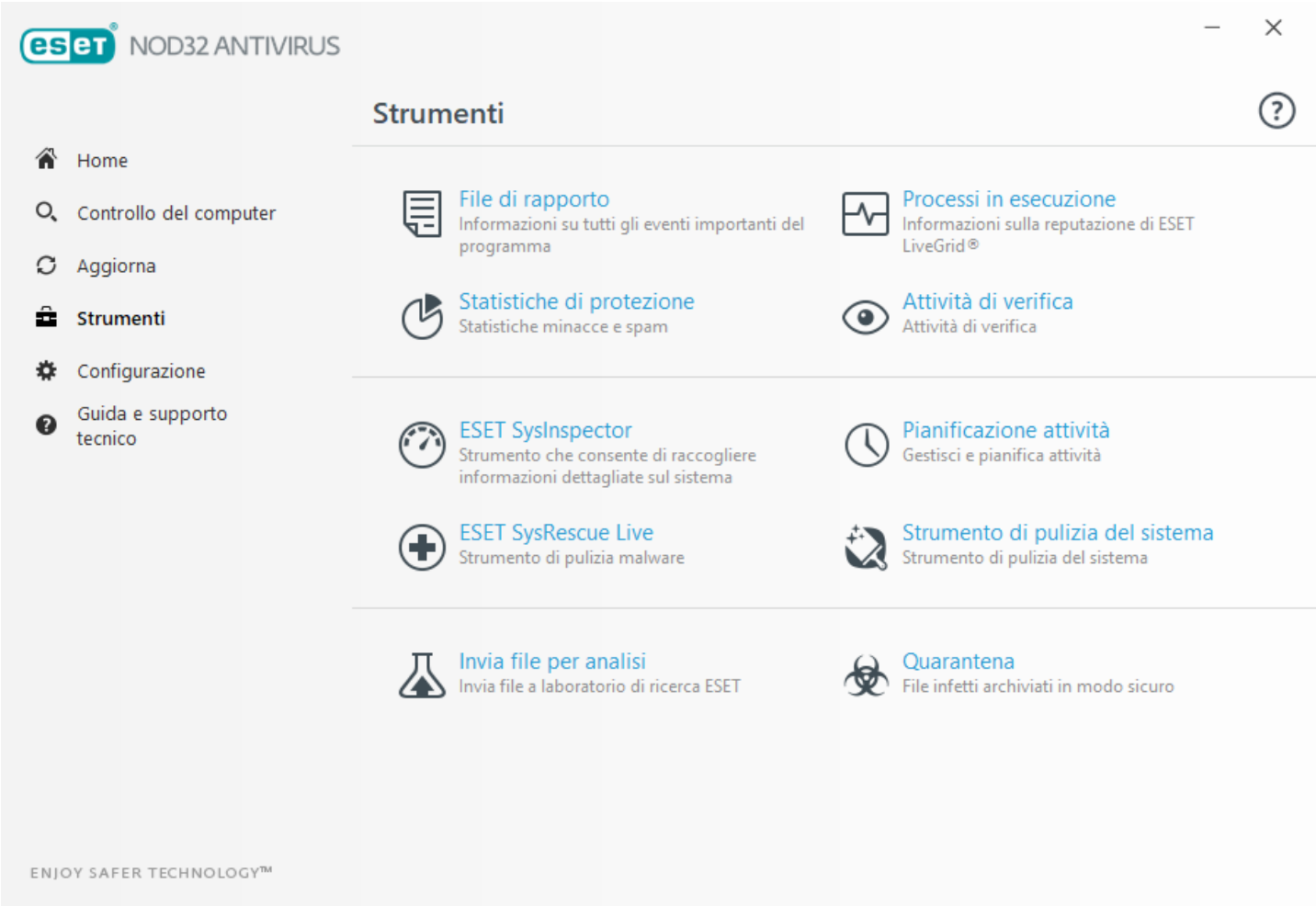
4.4 Strumenti

Il menu **Strumenti** include moduli che consentono di semplificare l'amministrazione del programma, offrendo opzioni aggiuntive per gli utenti esperti.

Fare clic su Altri strumenti per visualizzare altri strumenti per proteggere il computer.

4.4.1 Strumenti in ESET NOD32 Antivirus

Il menu **Strumenti** include moduli che consentono di semplificare l'amministrazione del programma, offrendo opzioni aggiuntive per gli utenti esperti.



Questo menu contiene i seguenti strumenti:

 File di rapporto

 Statistiche di protezione

 Attività di verifica

 Processi in esecuzione (se ESET LiveGrid® è attivato in ESET NOD32 Antivirus)

 ESET SysInspector

 ESET SysRescue Live: reindirizza l'utente alla pagina di ESET SysRescue Live, dove è possibile scaricare l'immagine di ESET SysRescue Live o il Live CD/USB Creator per i sistemi operativi Microsoft Windows.

 Pianificazione attività

 Strumento di pulizia del sistema: aiuta l'utente a ripristinare lo stato di usabilità del computer in seguito alla pulizia di una minaccia.

 Invia campione per analisi: consente all'utente di inviare un file sospetto al laboratorio di ricerca ESET per l'analisi. La finestra di dialogo visualizzata dopo aver selezionato questa opzione è descritta in questa sezione.

 Quarantena

NOTA
ESET SysRescue potrebbe non essere disponibile per Windows 8 in versioni precedenti di prodotti di protezione ESET. In questo caso, si consiglia di effettuare l'upgrade del prodotto o di creare un disco ESET SysRescue su un'altra versione di Microsoft Windows.

4.4.1.1 File di rapporto

I file di rapporto contengono informazioni relative agli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate. La registrazione rappresenta una parte essenziale dell'analisi del sistema, del rilevamento delle minacce e della risoluzione dei problemi. La registrazione viene eseguita attivamente in background, senza che sia richiesto l'intervento da parte dell'utente. Le informazioni vengono registrate in base alle impostazioni del livello di dettaglio di rapporto correnti. È possibile visualizzare i messaggi di testo e i rapporti direttamente dall'ambiente di ESET NOD32 Antivirus, nonché dai registri di archivio.

È possibile accedere ai file di rapporto dalla finestra principale del programma facendo clic su **Strumenti** > **File di rapporto**. Selezionare il tipo di rapporto desiderato nel menu a discesa **Rapporto**. Sono disponibili i rapporti seguenti:

- **Minacce rilevate**: nel rapporto delle minacce sono contenute informazioni dettagliate sulle infiltrazioni rilevate da ESET NOD32 Antivirus. Le informazioni contenute nel rapporto includono l'ora del rilevamento, il nome dell'infiltrazione, la posizione, l'azione eseguita e il nome dell'utente registrato nel momento in cui è stata rilevata l'infiltrazione. Fare doppio clic su una voce qualsiasi del rapporto per visualizzarne il contenuto dettagliato in una finestra separata.
- **Eventi**: tutte le azioni importanti eseguite da ESET NOD32 Antivirus vengono registrate nel rapporto eventi. Il rapporto eventi contiene informazioni sugli eventi e sugli errori che si sono verificati nel programma. È utile agli amministratori di sistema e agli utenti per risolvere i problemi. Spesso le informazioni visualizzate in questo rapporto consentono di trovare la soluzione a un problema che si verifica nel programma.
- **Controllo del computer**: in questa finestra vengono visualizzati i risultati di tutti i controlli manuali o pianificati completati. Ogni riga corrisponde a un singolo controllo del computer. Fare doppio clic su una voce qualsiasi per visualizzare i dettagli del rispettivo controllo.
- **HIPS**: contiene i record di specifiche regole HIPS che sono contrassegnati per la registrazione. Nel protocollo viene mostrata l'applicazione che ha attivato l'operazione, il risultato (ovvero se la regola era consentita o vietata) e il nome della regola.

- **Siti Web filtrati**: Questo elenco è utile se si desidera visualizzare un elenco di siti Web che sono stati bloccati dalla Protezione accesso Web. In questi rapporti è possibile visualizzare l'ora, l'indirizzo URL, l'utente e l'applicazione che hanno creato una connessione a un sito Web specifico.
- **Controllo dispositivi**: contiene record relativi ai supporti rimovibili o ai dispositivi collegati al computer. Nel file di rapporto saranno registrati solo i dispositivi con le rispettive regole di Controllo dispositivi. Se la regola non corrisponde a un dispositivo collegato, non verrà creata alcuna voce di rapporto relativa a tale evento. Qui è possibile visualizzare anche dettagli relativi al tipo di dispositivo, numero di serie, nome del fornitore e dimensioni del supporto (ove disponibili).

Selezionare i contenuti di un rapporto e premere **Ctrl + C** per copiare i contenuti negli Appunti . Tenere premuti **Ctrl** e **Shift** per selezionare più voci.

Fare clic su **Filtraggio** per aprire la finestra **Filtraggio rapporti** in cui è possibile definire i criteri di filtraggio.

Fare clic con il tasto destro del mouse su un record specifico per aprire il menu contestuale. Nel menu contestuale sono disponibili le seguenti opzioni:

- **Mostra:** consente di visualizzare informazioni più dettagliate relative al rapporto selezionato in una nuova finestra.
- **Filtra gli stessi record**: dopo aver attivato questo filtro, verranno visualizzati esclusivamente i record dello stesso tipo (diagnostica, avvisi, ecc.).
- **Filtro.../Trova...**: dopo aver selezionato questa opzione, la finestra Cerca nel rapporto consentirà all'utente di definire i criteri di filtraggio per specifiche voci dei rapporti.
- **Attiva filtro**: attiva le impostazioni del filtro.
- **Disattiva filtro**: consente di cancellare tutte le impostazioni del filtro (come descritto in precedenza).
- **Copia/Copia tutto**: copia le informazioni su tutti i record nella finestra.
- **Elimina/Elimina tutto**: elimina i record selezionati o tutti i record visualizzati. Per poter eseguire questa operazione è necessario disporre dei privilegi di amministratore.
- **Esporta...**: esporta le informazioni sul/i record in formato XML.
- **Esporta tutto...**: esporta le informazioni sui record in formato XML.
- **Scorri registro**: lasciare attivata questa opzione per scorrere automaticamente i rapporti meno recenti e visualizzare i rapporti attivi nella finestra **File di rapporto**.

4.4.1.1.1 File di rapporto

La configurazione della registrazione di ESET NOD32 Antivirus è accessibile dalla finestra principale del programma. Fare clic su **Configurazione** > **Accedi a configurazione avanzata...** > **Strumenti** > **File di rapporto**. La sezione relativa ai rapporti viene utilizzata per definire come verranno gestiti. Il programma elimina automaticamente i rapporti meno recenti per liberare spazio sull'unità disco rigido. Per i file di rapporto è possibile specificare le opzioni seguenti:

Livello di dettaglio di registrazione minimo: specifica il livello di dettaglio minimo degli eventi da registrare.

- **Diagnostica**: registra le informazioni necessarie ai fini dell'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativo**: registra i messaggi informativi, compresi quelli relativi agli aggiornamenti riusciti, e tutti i record indicati in precedenza.
- **Allarmi**: registra errori critici e messaggi di allarme.
- **Errori**: verranno registrati errori quali *"Errore durante il download del file"* ed errori critici.
- **Critico**: registra solo gli errori critici (errore che avvia la protezione antiviruse così via).

Le voci del rapporto più vecchie del numero specificato di giorni nel campo **Elimina automaticamente i record più vecchi di (giorni)** verranno eliminate automaticamente.

Ottimizza automaticamente file di rapporto: se questa opzione è selezionata, i file di rapporto vengono automaticamente deframmentati se la percentuale è superiore al valore specificato nel campo **Se il numero di record inutilizzati supera (%)**.

Fare clic su **Ottimizza** per avviare la deframmentazione dei file di rapporto. Per migliorare le prestazioni e potenziare la velocità di elaborazione dei rapporti, durante questo processo vengono rimosse le voci vuote. Tale miglioramento può essere rilevato in particolare se i rapporti contengono un numero elevato di elementi.

Attiva protocollo di testo consente di attivare l'archiviazione dei rapporti in un altro formato di file separato da File di rapporto:

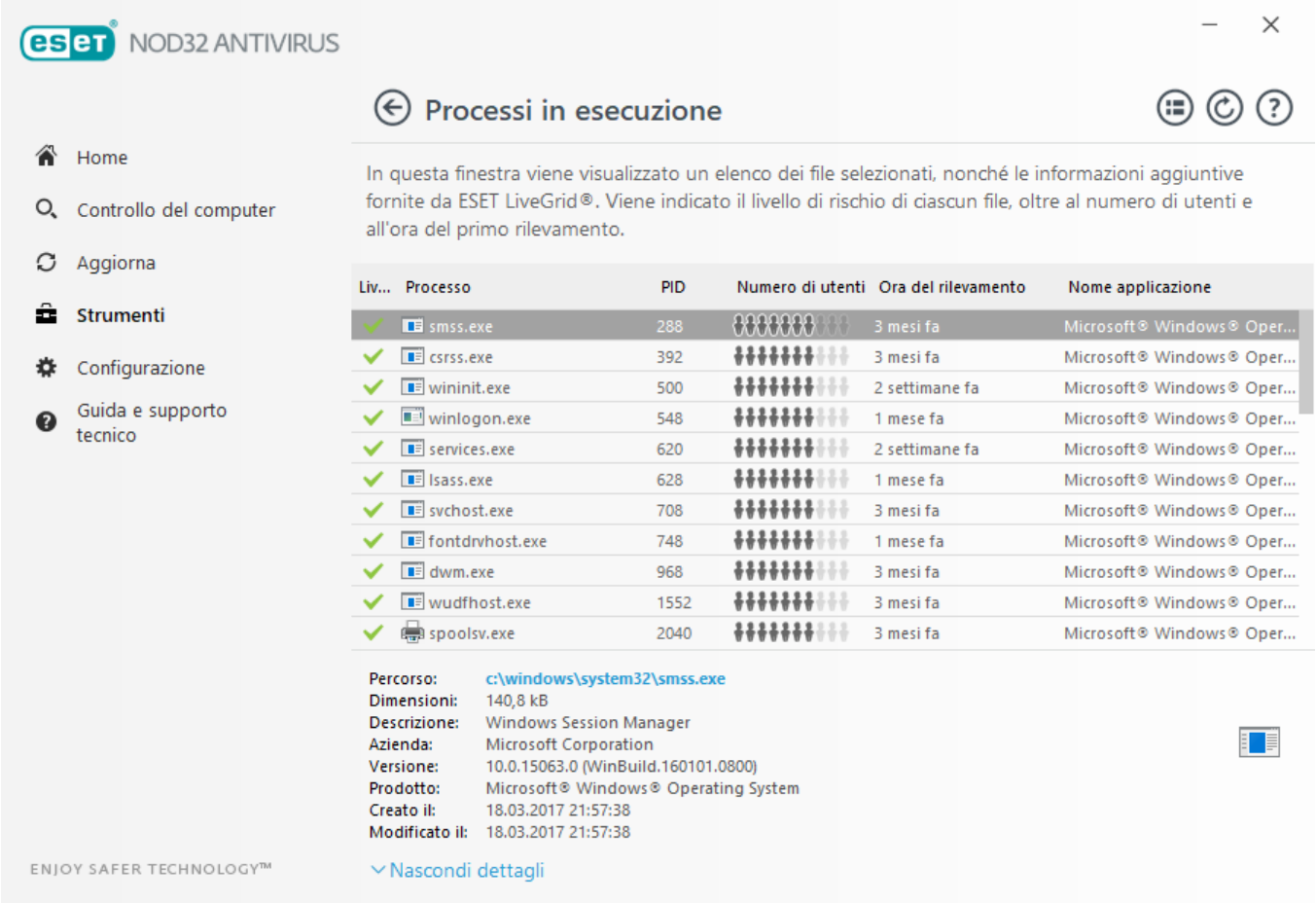
- **Directory di destinazione**: directory in cui verranno archiviati i file di rapporto (si applica solo ai file di testo/CSV). Ciascuna sezione del rapporto presenta il proprio file con un nome predefinito (ad esempio, *virlog.txt* per la sezione **Minacce rilevate** dei file di rapporto, se si utilizza un formato di file testo normale per l'archiviazione dei rapporti).
- **Tipo**: selezionando il formato di file **Testo**, i rapporti verranno archiviati in un file di testo e i dati saranno suddivisi in schede. Le stesse condizioni si applicano al formato di file **CSV** separato da virgole. Se si sceglie **Evento**, i rapporti verranno archiviati nel rapporto eventi Windows (che è possibile visualizzare utilizzando il visualizzatore eventi nel Pannello di controllo) anziché nel file.

Elimina tutti i file del rapporto: elimina tutti i rapporti correntemente archiviati selezionati nel menu a discesa **Tipo**. Verrà visualizzata una notifica relativa all'avvenuta eliminazione dei rapporti.

NOTA
per una più rapida risoluzione dei problemi, ESET potrebbe richiedere all'utente di fornire i rapporti archiviati sul computer. ESET Log Collector facilita la raccolta delle informazioni necessarie. Per ulteriori informazioni su ESET Log Collector, consultare l'articolo della Knowledge Base ESET.

4.4.1.2 Processi in esecuzione

I processi in esecuzione consentono di visualizzare i programmi o processi in esecuzione sul computer e inviare informazioni tempestive e costanti a ESET sulle nuove infiltrazioni. ESET NOD32 Antivirus fornisce informazioni dettagliate sui processi in esecuzione allo scopo di proteggere gli utenti che utilizzano la tecnologia ThreatSense.



Processo: nome immagine del programma o del processo in esecuzione sul computer. Per visualizzare tutti i processi in esecuzione sul computer è inoltre possibile utilizzare Windows Task Manager. Per aprire il Task Manager, fare clic con il pulsante destro del mouse su un'area vuota della barra delle attività, quindi scegliere **Task Manager**, oppure premere **Ctrl**+**Shift**+**Esc** sulla tastiera.

Livello di rischio: nella maggior parte dei casi, ESET NOD32 Antivirus e la tecnologia ThreatSense assegnano livelli di rischio agli oggetti (file, processi, chiavi di registro, ecc.), utilizzando una serie di regole euristiche che esaminano le caratteristiche di ciascun oggetto valutandone le potenzialità come attività dannosa. Sulla base di tali regole, agli oggetti viene assegnato un livello di rischio da 1: non a rischio (verde) a 9: a rischio (rosso).

NOTA
Le applicazioni note contrassegnate di verde sono definitivamente pulite (inserite nella whitelist) e saranno escluse dal controllo, per migliorare le prestazioni.

PID: numero identificativo del processo, che può essere utilizzato come parametro in diverse funzioni tra cui la regolazione della priorità del processo.

Numero di utenti: numero di utenti che utilizzano una determinata applicazione. Queste informazioni sono raccolte mediante la tecnologia ThreatSense.

Ora di rilevamento: ora in cui l'applicazione è stata rilevata dalla tecnologia ThreatSense.

NOTA
Un'applicazione marchiata come Sconosciuta (arancio) non è necessariamente un software malevolo. In genere si tratta di una nuova applicazione. In caso di dubbi sul file, selezionare l'opzione invia file per analisi al laboratorio di ricerca ESET. Se il file si rivela essere un'applicazione dannosa, la sua rilevazione verrà aggiunta in un aggiornamento successivo.

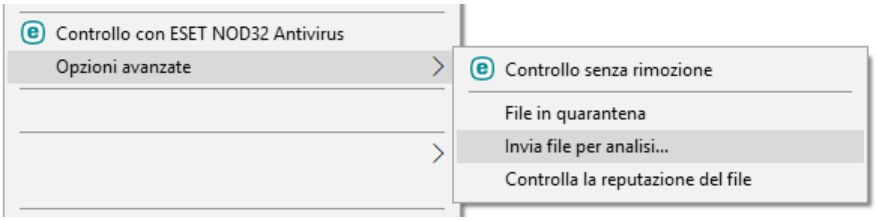
Nome applicazione: nome specifico di un programma o processo.

Apri in una nuova finestra: le informazioni sui processi in esecuzione verranno visualizzate in una nuova finestra.

Fare clic su un'applicazione per visualizzarne i seguenti dati:

- **Percorso**: posizione di un'applicazione sul computer.
- **Dimensione**: dimensione del file in B (byte).
- **Descrizione**: caratteristiche del file basate sulla descrizione ottenuta dal sistema operativo.
- **Società**: nome del fornitore o del processo applicativo.
- **Versione**: informazioni estrapolate dall'autore dell'applicazione.
- **Prodotto**: nome dell'applicazione e/o nome commerciale.
- **Creato/modificato il**: data e ora di creazione (modifica).

NOTA
è anche possibile verificare la reputazione di file che non operano come eseguibili/processi. Per fare ciò, fare clic con il tasto destro del mouse e selezionare **Opzioni avanzate** > **Controllo reputazione file**.



4.4.1.3 Statistiche di protezione

Per visualizzare un grafico dei dati statistici relativi ai moduli di protezione ESET NOD32 Antivirus, fare clic su **Strumenti** > **Statistiche di protezione**. Selezionare il modulo di protezione desiderato dal menu a discesa **Statistiche** per visualizzare il grafico e la legenda corrispondenti. Se si passa il mouse su un elemento nella legenda, verranno visualizzati solo i dati di quell'elemento nel grafico.

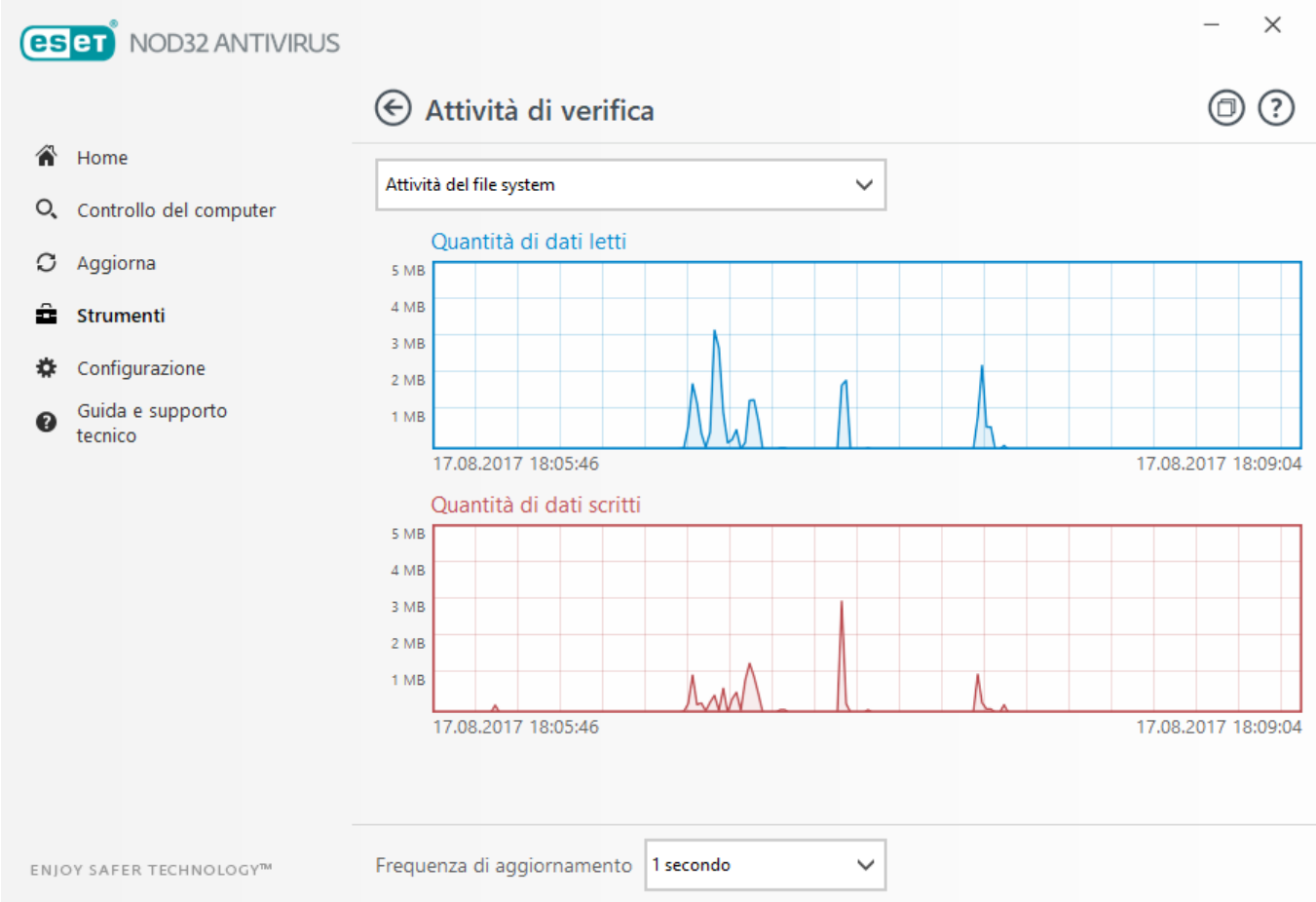
Sono disponibili i seguenti grafici statistici:

- **Protezione antivirus e antispyware**: consente di visualizzare il numero di oggetti infetti e puliti.
- **Protezione file system**: consente di visualizzare solo gli oggetti che sono stati scritti o letti sul file system.
- **Protezione client di posta**: consente di visualizzare solo gli oggetti inviati o ricevuti dai client di posta.
- **Protezione accesso Web e Anti-Phishing**: consente di visualizzare solo gli oggetti scaricati dai browser Web.

Sotto il grafico delle statistiche è visualizzato il numero degli oggetti totali sottoposti a controllo, l'ultimo oggetto sottoposto a controllo e la data e l'ora delle statistiche. Fare clic su **Azzeramento** per cancellare tutte le informazioni statistiche.

4.4.1.4 Attività di verifica

Per visualizzare l'**Attività di file system** corrente in un grafico, fare clic su **Strumenti** > **Attività di verifica**. Nella parte inferiore del grafico è presente una linea cronologica che registra in tempo reale le attività del file system in base all'intervallo di tempo selezionato. Per modificare l'intervallo di tempo, selezionarlo nel menu a discesa **Frequenza di aggiornamento**.



Sono disponibili le seguenti opzioni:

- **Passaggio: 1 secondo**: il grafico si aggiorna ogni secondo e l'intervallo di tempo copre gli ultimi 10 minuti.
- **Passaggio: 1 minuto (ultime 24 ore)**: il grafico si aggiorna ogni minuto e l'intervallo di tempo copre le ultime 24 ore.
- **Passaggio: 1 ora (ultimo mese)**: il grafico si aggiorna ogni ora e l'intervallo di tempo copre l'ultimo mese.
- **Passaggio: 1 ora (mese selezionato)**: il grafico si aggiorna ogni ora e l'intervallo di tempo copre gli ultimi X mesi selezionati.

L'asse verticale del **Grafico dell'attività del file system** rappresenta i dati letti (blu) e scritti (rosso). Entrambi i valori sono espressi in KB (kilobyte)/MB/GB. Facendo scorrere il mouse sui dati letti o scritti nella didascalia sottostante il grafico, è possibile visualizzare unicamente i dati relativi a quella specifica attività.

4.4.1.5 ESET SysInspector

ESET SysInspector è un'applicazione che esamina a fondo il computer, raccoglie informazioni dettagliate sui componenti del sistema, quali driver e applicazioni, le connessioni di rete o le voci di registro importanti e valuta il livello di rischio di ciascun componente. Tali informazioni possono risultare utili per determinare la causa di comportamenti sospetti del sistema, siano essi dovuti a incompatibilità software o hardware o infezioni malware.

Nella finestra di dialogo SysInspector sono visualizzate le seguenti informazioni sui rapporti creati:

- **Ora**: ora di creazione del rapporto.
- **Commento**: breve commento.
- **Utente**: nome dell'utente che ha creato il rapporto.
- **Stato**: stato di creazione del rapporto.

Sono disponibili le azioni seguenti:

- **Mostra**: apre il rapporto creato. È inoltre possibile fare clic con il pulsante destro del mouse su uno specifico file di registro e selezionare **Mostra** dal menu contestuale.
- **Confronta**: consente di mettere a confronto due rapporti esistenti.
- **Crea...**: consente di creare un nuovo rapporto. Attendere fino al termine di ESET SysInspector (lo stato del rapporto comparirà come Creato) prima di provare ad accedere al rapporto.
- **Elimina**: rimuove dall'elenco il rapporto o i rapporti selezionati.

Le seguenti opzioni sono disponibili nel menu contestuale in caso di selezione di uno o più file di rapporto:

- **Mostra**: apre il rapporto selezionato in ESET SysInspector (funzione uguale a un doppio clic su un rapporto).
- **Confronta**: consente di mettere a confronto due rapporti esistenti.
- **Crea...**: consente di creare un nuovo rapporto. Attendere fino al termine di ESET SysInspector (lo stato del rapporto comparirà come Creato) prima di provare ad accedere al rapporto.
- **Elimina**: rimuove dall'elenco il rapporto o i rapporti selezionati.
- **Elimina tutto**: consente di eliminare tutti i rapporti.
- **Esporta...**: esporta il rapporto in un file *.xml* o un file *.xml* compresso.

4.4.1.6 Pianificazione attività

La Pianificazione attività consente di gestire e avviare attività pianificate con configurazione e proprietà predefinite.

È possibile accedere alla Pianificazione attività nella finestra principale del programma di ESET NOD32 Antivirus facendo clic su **Strumenti** > **Pianificazione attività**. La **Pianificazione attività** contiene un elenco di tutte le attività pianificate e delle relative proprietà di configurazione, ad esempio data, ora e profilo di controllo predefiniti utilizzati.

La Pianificazione attività consente di pianificare le attività seguenti: moduli di aggiornamento, attività di controllo, controllo dei file di avvio del sistema e manutenzione dei rapporti. È possibile aggiungere o modificare attività direttamente dalla finestra principale Pianificazione attività, facendo clic su **Aggiungi...** o **Elimina** nella parte inferiore della finestra. Fare clic con il pulsante destro del mouse in qualsiasi punto della finestra Pianificazione attività per eseguire le azioni seguenti: visualizzare informazioni dettagliate, eseguire immediatamente l'attività,

aggiungere una nuova attività ed eliminare un'attività esistente. Utilizzare le caselle di controllo accanto a ciascuna voce per attivare o disattivare le attività.

Per impostazione predefinita, in **Pianificazione attività** vengono visualizzate le attività pianificate seguenti:

- **Manutenzione rapporto**
- **Aggiornamento automatico regolare**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**
- **Controlla periodicamente la disponibilità di una versione del prodotto più recente** (vedere Modalità di aggiornamento)
- **Controllo automatico file di avvio** (dopo l'accesso utente)
- **Controllo automatico file di avvio** (dopo il completamento dell'aggiornamento del motore di rilevamento)

Per modificare la configurazione di un'attività pianificata esistente (predefinita o definita dall'utente), fare clic con il pulsante destro del mouse sull'attività e selezionare **Modifica...** oppure selezionare l'attività che si desidera modificare e fare clic su **Modifica...**.

Aggiunta di un nuova attività

1. Fare clic su **Aggiungi attività** nella parte inferiore della finestra.
2. Inserire il nome dell'attività.
3. Selezionare l'attività desiderata dal menu a discesa:

- **Esegui applicazione esterna**: consente di pianificare l'esecuzione di un'applicazione esterna.
- **Manutenzione rapporto**: i file di rapporto contengono anche elementi rimasti dai record eliminati. Questa attività ottimizza periodicamente i record nei file di rapporto allo scopo di garantire un funzionamento efficiente.
- **Controllo del file di avvio del sistema**: consente di controllare i file la cui esecuzione è consentita all'avvio del sistema o all'accesso.
- **Crea un controllo computer**: crea uno snapshot ESET SysInspector del computer, raccoglie informazioni dettagliate sui componenti del sistema (ad esempio, driver e applicazioni) e valuta il livello di rischio di ciascun componente.
- **Controllo computer su richiesta**: consente di eseguire un controllo di file e di cartelle sul computer in uso.
- **Aggiornamento**: pianifica un'attività di aggiornamento attraverso un aggiornamento dei moduli.

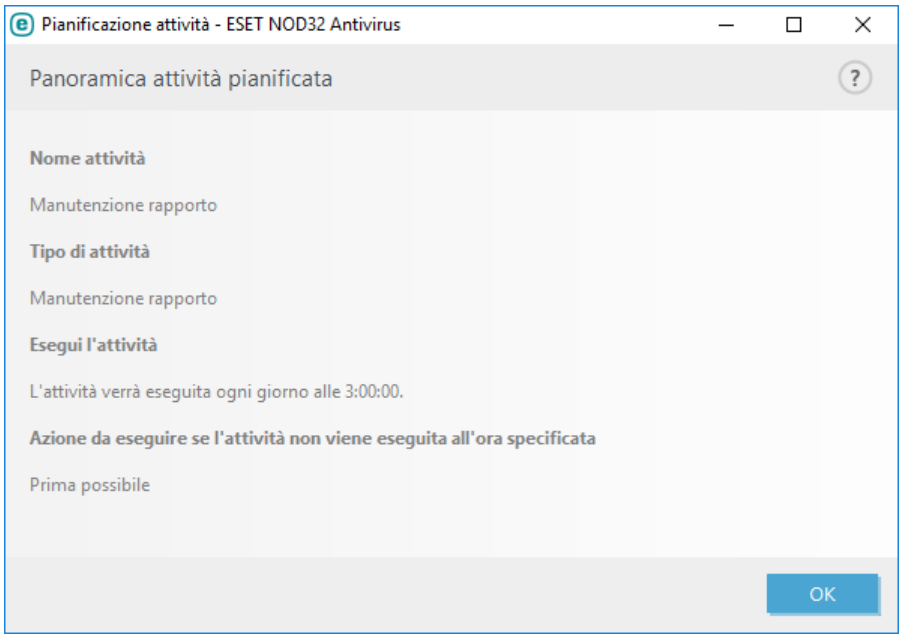
4. Premere il pulsante **Attivata** se si desidera attivare l'attività (è possibile eseguire questa operazione in un secondo momento selezionando/deselezionando la casella di controllo nell'elenco di attività pianificate), fare clic su **Avanti** e selezionare una delle opzioni relative alla frequenza di esecuzione:

- **Una volta**: l'attività verrà eseguita alla data e all'ora predefinite.
- **Ripetutamente**: l'attività verrà eseguita in base all'intervallo di tempo specificato.
- **Ogni giorno**: l'attività verrà eseguita periodicamente ogni giorno all'ora specificata.
- **Ogni settimana**: l'attività verrà eseguita nel giorno e all'ora selezionati.
- **Quando si verifica un evento**: l'attività verrà eseguita quando si verifica un evento specifico.

5. Selezionare **Ignora attività se in esecuzione su un computer alimentato dalla batteria** per ridurre al minimo le risorse di sistema in caso di utilizzo della batteria del computer portatile. L'attività verrà eseguita alla data e all'ora specificate nei campi **Esecuzione attività**. Se l'attività non è stata eseguita all'ora predefinita, è possibile specificare il momento in cui dovrà essere nuovamente eseguita:

- **Al prossimo orario pianificato**
- **Prima possibile**
- **Immediatamente, se l'ora dall'ultima esecuzione supera un valore specificato** (è possibile definire l'intervallo utilizzando la casella di scorrimento **Ora dall'ultima esecuzione**)

È possibile rivedere l'attività pianificata facendo clic con il pulsante tasto destro del mouse, quindi su **Mostra dettagli attività**.



4.4.1.7 Strumento di pulizia del sistema

Lo strumento di pulizia del sistema è una funzione che aiuta l'utente a ripristinare lo stato di usabilità del computer in seguito alla pulizia di una minaccia. I malware sono in grado di disattivare utilità di sistema quali Editor del Registro di sistema, Gestione attività o Aggiornamenti di Windows. Lo strumento di pulizia ripristina i valori predefiniti del sistema.

È possibile richiedere la pulizia del sistema:

- in caso di rilevamento di una minaccia
- se un utente fa clic su **Ripristina**

Se lo si desidera, è possibile rivedere le modifiche e ripristinare le impostazioni.

NOTA
Lo strumento di pulizia del sistema può essere utilizzato esclusivamente da utenti con diritti di amministratore.

4.4.1.8 ESET SysRescue

ESET SysRescue è un'utilità che consente all'utente di creare un disco di avvio contenente una delle soluzioni ESET Security: ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security, ESET Smart Security Premium o alcuni prodotti per server. Il vantaggio principale offerto da ESET SysRescue consiste nel fatto che la soluzione ESET Security viene eseguita indipendentemente dal sistema operativo che la ospita ma con un accesso diretto al disco e al file system. Ciò consente di rimuovere infiltrazioni che non sarebbe stato possibile eliminare in una situazione ordinaria, ad esempio durante l'esecuzione del sistema operativo.

4.4.1.9 ESET LiveGrid®

ESET LiveGrid® (sviluppato sul sistema avanzato di allarme immediato ESET ThreatSense.Net) utilizza i dati inviati dagli utenti ESET di tutto il mondo e li invia al laboratorio di ricerca ESET. Grazie all'invio di campioni e metadati "from the wild" sospetti, ESET LiveGrid® consente a ESET di soddisfare le esigenze dei clienti e di gestire le minacce più recenti in modo tempestivo. Per ulteriori informazioni su ESET LiveGrid®, consultare il glossario.

Un utente può controllare la reputazione dei processi in esecuzione e dei file direttamente dall'interfaccia del programma o dal menu contestuale. Ulteriori informazioni sono disponibili su ESET LiveGrid®. Sono disponibili due opzioni:

1. È possibile scegliere di non attivare ESET LiveGrid®. Non verrà persa alcuna funzionalità del software, ma, in alcuni casi, ESET NOD32 Antivirus potrebbe rispondere più rapidamente alle nuove minacce rispetto all'aggiornamento del motore di rilevamento quando ESET Live Grid è attivato.
2. È possibile configurare ESET LiveGrid® per l'invio di informazioni anonime sulle nuove minacce e laddove sia presente il nuovo codice dannoso. Il file può essere inviato a ESET per un'analisi dettagliata. Lo studio di queste minacce sarà d'aiuto ad ESET per aggiornare le proprie capacità di rilevamento.

ESET LiveGrid® raccoglierà informazioni sul computer dell'utente in relazione alle nuove minacce rilevate. Tali informazioni possono includere un campione o una copia del file in cui è contenuta la minaccia, il percorso del file, il nome del file, informazioni su data e ora, il processo in base al quale la minaccia è apparsa sul computer e informazioni sul sistema operativo del computer.

Per impostazione predefinita, ESET NOD32 Antivirus viene configurato per l'invio di file sospetti al laboratorio antivirus ESET per l'analisi dettagliata. Sono sempre esclusi file con determinate estensioni, ad esempio *DOC* o *XLS*. È inoltre possibile aggiungere altre estensioni qualora sussistano specifici file che l'utente o la società dell'utente non desidera inviare.

Nel menu di configurazione ESET LiveGrid® sono disponibili varie opzioni di attivazione/disattivazione di ESET LiveGrid®, uno strumento utile per l'invio di file sospetti e di informazioni statistiche anonime ai laboratori ESET. È accessibile dalla struttura di Configurazione avanzata selezionando **Strumenti** > **ESET LiveGrid®**.

Attiva il sistema di reputazione ESET LiveGrid® (scelta consigliata): il sistema di reputazione ESET LiveGrid® potenzia le prestazioni delle soluzioni anti-malware ESET eseguendo un confronto tra i file controllati e un database di oggetti inseriti nelle whitelist o nelle blacklist all'interno del cloud.

Invia statistiche anonime: consente a ESET di raccogliere informazioni sulle nuove minacce rilevate, tra cui il nome della minaccia, la data e l'ora del rilevamento, il metodo di rilevamento e i metadati associati, la versione e la configurazione del prodotto, incluse le informazioni sul sistema in uso.

Invia file: i file sospetti simili alle minacce e/o i file con caratteristiche o comportamenti insoliti vengono inviati a ESET ai fini dell'analisi.

Selezionare **Attiva registrazione** per creare un rapporto di eventi sul quale vengono registrati gli invii dei file e delle informazioni statistiche. Ciò attiverà la registrazione sul Rapporto eventi dell'invio di file o statistiche.

Contatto e-mail (facoltativo): il contatto e-mail può essere incluso insieme ai file sospetti e utilizzato per contattare l'utente qualora fossero richieste ulteriori informazioni ai fini dell'analisi. Tenere presente che non si riceverà alcuna risposta da ESET, a meno che non siano richieste ulteriori informazioni.

Esclusione: il filtro Esclusioni consente all'utente di escludere alcuni file o alcune cartelle dall'invio (ad esempio, potrebbe essere utile escludere i file contenenti informazioni riservate, come documenti o fogli di calcolo). I file elencati non verranno mai inviati ai laboratori ESET ai fini dell'analisi, anche se contengono codice sospetto. Per impostazione predefinita, vengono esclusi i tipi di file più comuni (con estensione DOC e così via). È possibile aggiungerli all'elenco di file esclusi.

Se ESET LiveGrid® è già stato utilizzato in precedenza ed è stato disattivato, potrebbero essere ancora presenti pacchetti di dati da inviare. Tali pacchetti verranno inviati a ESET anche dopo la disattivazione. Dopo l'invio delle informazioni correnti, non verranno creati ulteriori pacchetti.

4.4.1.9.1 File sospetti

Se si rileva un file sospetto, è possibile inviarlo al laboratorio di ricerca ESET per l'analisi. Se viene individuata un'applicazione dannosa, essa verrà aggiunta al successivo aggiornamento delle firme antivirali.

Filtro di esclusione: il filtro Esclusione consente di escludere dall'invio determinati file/cartelle. I file elencati non verranno mai inviati ai laboratori di ricerca ESET per l'analisi, anche se contengono codice sospetto. È ad esempio utile escludere file che potrebbero contenere informazioni riservate, quali documenti o fogli di calcolo. Per impostazione predefinita, vengono esclusi i tipi di file più comuni (.doc, ecc.). Se lo si desidera, è possibile aggiungerli all'elenco di file esclusi.

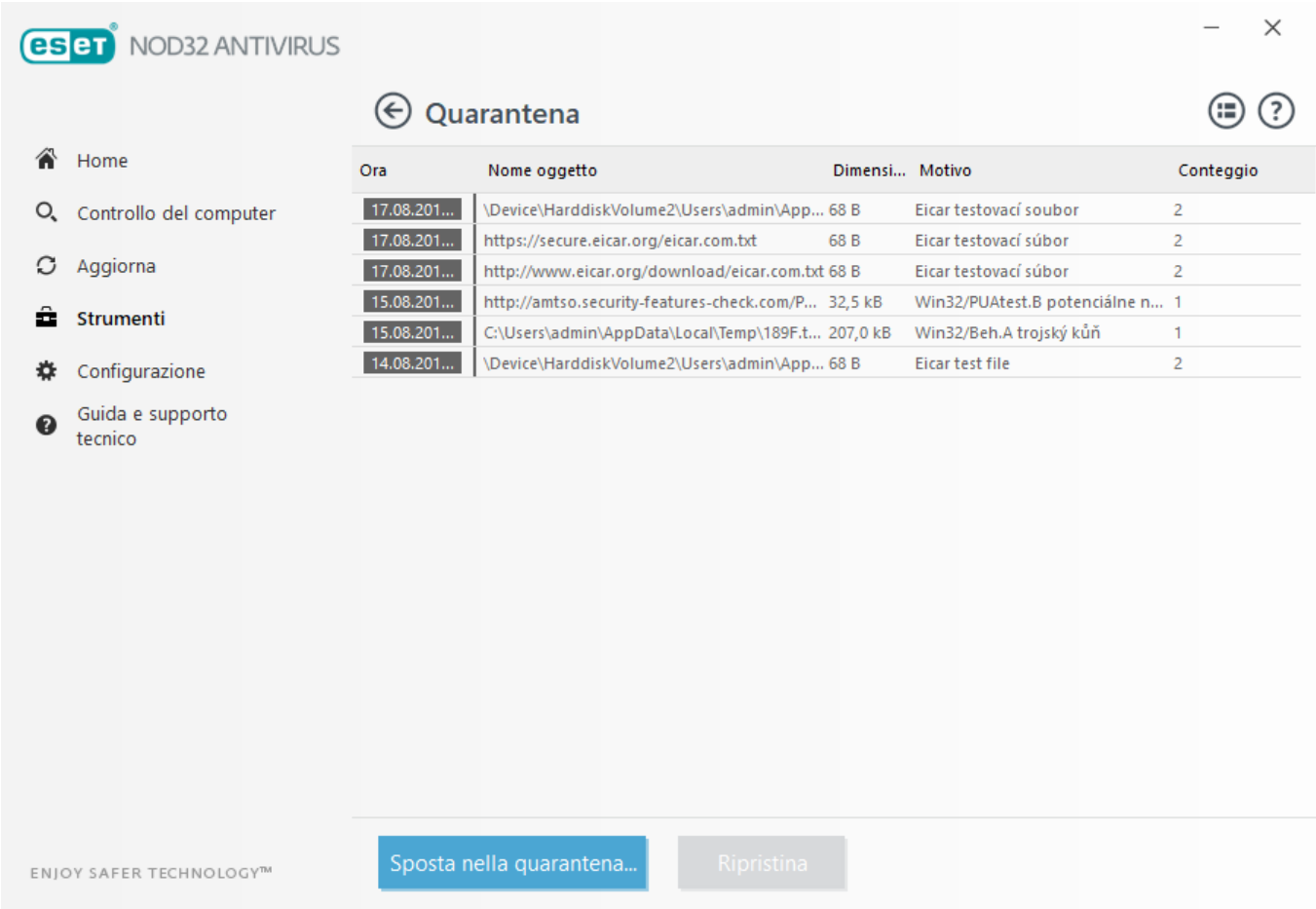
Contatto e-mail (facoltativo): il contatto e-mail può essere incluso insieme ai file sospetti e utilizzato per contattare l'utente qualora fossero richieste ulteriori informazioni ai fini dell'analisi. Tenere presente che non si riceverà alcuna risposta da ESET, a meno che non siano richieste ulteriori informazioni.

Selezionare **Attiva registrazione** per creare un rapporto di eventi sul quale vengono registrati gli invii dei file e delle informazioni statistiche. Ciò attiverà la registrazione sul Rapporto eventi dell'invio di file o statistiche.

4.4.1.10 Quarantena

La funzione principale della quarantena è archiviare i file infetti in modo sicuro. I file devono essere messi in quarantena se non è possibile pulirli, se non è sicuro o consigliabile eliminarli o, infine, se vengono erroneamente rilevati come minacce da ESET NOD32 Antivirus.

È possibile mettere in quarantena qualsiasi tipo di file. È una procedura consigliata nel caso in cui un file si comporti in modo sospetto ma non viene rilevato dallo scanner antivirus. I file messi in quarantena possono essere inviati al laboratorio di ricerca ESET per l'analisi.



I file salvati nella cartella della quarantena possono essere visualizzati in una tabella contenente la data e l'ora della quarantena, il percorso originale del file infetto, la dimensione in byte, il motivo (ad esempio, oggetto aggiunto dall'utente) e il numero di minacce (ad esempio, se si tratta di un archivio contenente più infiltrazioni).

Mettere file in quarantena

ESET NOD32 Antivirus mette automaticamente in quarantena i file eliminati (qualora l'utente non abbia provveduto ad annullare questa opzione nella finestra di avviso). Se necessario, è possibile mettere manualmente in quarantena i file sospetti selezionando **Quarantena...**. In tal caso, il file originale non verrà rimosso dalla posizione di origine. Per questa operazione è possibile utilizzare anche il menu contestuale: fare clic con il pulsante destro del mouse sulla finestra **Quarantena** e selezionare l'opzione **Quarantena...**.

Ripristino dalla quarantena

È possibile ripristinare nella posizione di origine i file messi in quarantena. Utilizzare a tale scopo la funzione **Ripristina**, disponibile nel menu contestuale visualizzato facendo clic con il pulsante destro del mouse su un file specifico nella finestra Quarantena. Se un file è contrassegnato come applicazione potenzialmente indesiderata, l'opzione **Ripristina ed escludi dal controllo** è attivata. Per ulteriori informazioni su questo tipo di applicazione, consultare la relativa voce del glossario. Il menu contestuale contiene anche l'opzione **Ripristina in...**, che consente di ripristinare i file in una posizione diversa da quella di origine da cui sono stati eliminati.

Eliminazione dalla quarantena: fare clic con il pulsante destro del mouse su un oggetto specifico e selezionare **Elimina dalla quarantena** oppure selezionare l'oggetto che si desidera eliminare e premere **Elimina** sulla tastiera. È inoltre possibile selezionare vari oggetti ed eliminarli contemporaneamente.

NOTA
se il programma ha messo in quarantena per errore un file non dannoso, escludere il file dal controllo dopo averlo ripristinato e inviarlo al Supporto tecnico ESET.

Invio di un file dalla cartella Quarantena

Se un file sospetto che non è stato rilevato dal programma è stato messo in quarantena o se un file è stato segnalato erroneamente come infetto (ad esempio, mediante un'analisi euristica del codice) e quindi messo in quarantena, è necessario inviarlo al laboratorio antivirus ESET. Per inviare un file dalla cartella di quarantena, fare clic con il pulsante destro del mouse sul file e selezionare **Invia per analisi** dal menu contestuale.

4.4.1.11 Server proxy

Nelle reti LAN di grandi dimensioni, le comunicazioni tra il computer dell'utente e Internet possono essere mediate da un server proxy. Se si utilizza questa configurazione, è necessario definire le seguenti impostazioni. In caso contrario, il programma non sarà in grado di aggiornarsi automaticamente. In ESET NOD32 Antivirus, il server proxy può essere configurato da due sezioni differenti della struttura Configurazione avanzata.

Le impostazioni del server proxy possono innanzitutto essere configurate in **Configurazione avanzata** da **Strumenti** > **Server proxy**. Specificando il server proxy a questo livello, si definiscono le impostazioni globali del server proxy per l'intera applicazione ESET NOD32 Antivirus. Questi parametri vengono utilizzati da tutti i moduli che richiedono una connessione a Internet.

Per specificare le impostazioni del server proxy per questo livello, selezionare **Utilizza server proxy** e inserire l'indirizzo del server proxy nel campo **Server proxy**, insieme al numero di **Porta** del server proxy.

Se per la comunicazione con il server proxy è necessaria l'autenticazione, selezionare **Il server proxy richiede l'autenticazione** e inserire un **Nome utente** e una **Password** validi nei rispettivi campi. Fare clic su **Rileva** per rilevare e inserire automaticamente le impostazioni del server proxy. Verranno copiati i parametri specificati in Internet Explorer.

NOTA
nelle impostazioni del **Server proxy**, è necessario inserire manualmente il nome utente e la password.

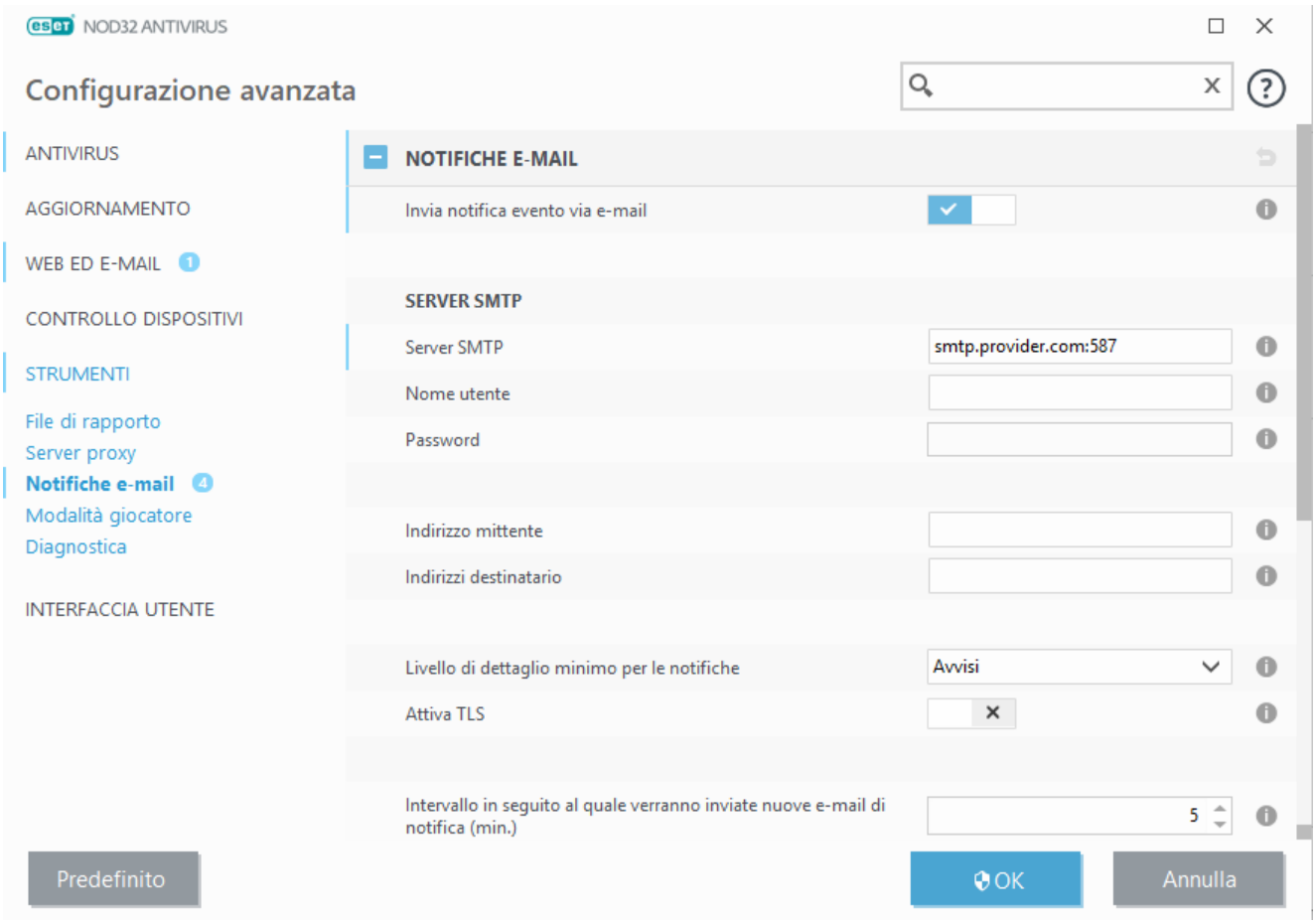
Utilizza la connessione diretta in assenza di proxy: se un prodotto è configurato per utilizzare il proxy HTTP e questo non è raggiungibile, il prodotto disabiliterà il proxy e comunicherà direttamente con i server ESET.

Le impostazioni del server proxy possono anche essere definite nella Configurazione aggiornamento avanzata (**Configurazione avanzata** > **Aggiornamento** > **Proxy HTTP** selezionando **Connessione tramite un server proxy** dal menu a discesa **Modalità proxy**). Questa impostazione è applicabile al profilo di aggiornamento fornito ed è

consigliata per i notebook che ricevono spesso aggiornamenti delle firme antivirali da postazioni remote. Per ulteriori informazioni su questa impostazione, consultare Configurazione aggiornamento avanzata.

4.4.1.12 Notifiche e-mail

ESET NOD32 Antivirus invia automaticamente e-mail di notifica nel caso in cui si verifichi un evento con il livello di dettaglio selezionato. Attivare **Invia notifiche di eventi via e-mail** per attivare le notifiche e-mail.



Server SMTP

Server SMTP: server SMTP utilizzato per l'invio delle notifiche (ad es. *smtp.provider.com:587*, porta predefinita 25).

NOTA
ESET NOD32 Antivirus supporta i server SMTP con crittografia TLS.

Nome utente e **password**: se il server SMTP richiede l'autenticazione, questi campi devono essere compilati con nome utente e password validi per l'accesso al server SMTP.

Indirizzo mittente: questo campo specifica l'indirizzo del mittente che verrà visualizzato nell'intestazione delle e-mail di notifica.

Indirizzo destinatario: questo campo specifica l'indirizzo del destinatario che verrà visualizzato nell'intestazione delle e-mail di notifica.

Dal menu a discesa **Livello di dettaglio minimo per le notifiche**, è possibile selezionare il livello di dettaglio di partenza delle notifiche da inviare.

- **Diagnostica**: registra le informazioni necessarie ai fini dell'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativo**: registra i messaggi informativi, come gli eventi di rete non standard, compresi quelli relativi agli aggiornamenti riusciti, e tutti i record indicati in precedenza.
- **Avvisi**: registra gli errori critici e i messaggi di avviso (la funzione Anti-Stealth non funziona correttamente o l'aggiornamento non è riuscito).
- **Errori**: verranno registrati errori quali "Protezione del documento non avviata" ed errori critici.
- **Critico**: registra solo gli errori critici (errore che avvia la protezione antivirus o il sistema infetto).

Attiva TLS: attiva l'invio di messaggi di avviso e notifiche supportati dalla crittografia TLS.

Intervallo in seguito al quale verranno inviate nuove e-mail di notifica (min.): intervallo in minuti in seguito al quale verranno inviate nuove notifiche all'indirizzo e-mail. Se il valore viene impostato su 0, le notifiche verranno inviate immediatamente.

Invia ciascuna notifica in un'e-mail separata: attivando questa opzione, il destinatario riceverà una nuova e-mail per ogni singola notifica. Tale operazione potrebbe determinare la ricezione di un numero elevato di messaggi e-mail in un periodo di tempo ridotto.

Formato dei messaggi

Formato dei messaggi di evento: formato dei messaggi di evento che vengono visualizzati sui computer remoti.

Formato dei messaggi di avviso per le minacce: i messaggi di avviso e notifica delle minacce presentano un formato predefinito. Si consiglia di non modificare questo formato. Tuttavia, in alcuni casi (ad esempio, se si dispone di un sistema di elaborazione delle e-mail automatizzato) potrebbe essere necessario modificare il formato dei messaggi.

Charset: applica la codifica dei caratteri ANSI a un messaggio di posta elettronica in base alle impostazioni internazionali di Windows (ad esempio, windows-1250), Unicode (UTF-8), ACSII a 7 bit (ad esempio, "á" verrà modificata in "a" e un simbolo sconosciuto verrà modificato in "?") o giapponese (ISO-2022-JP).

Usa codifica Quoted-printable: l'origine del messaggio e-mail verrà codificata in formato Quoted-printable (QP) che utilizza i caratteri ASCII ed è in grado di trasmettere correttamente speciali caratteri nazionali tramite e-mail nel formato a 8 bit (áéíóú).

4.4.1.12.1 Formato del messaggio

In questa sezione è possibile configurare il formato dei messaggi di evento che vengono visualizzati sui computer remoti.

Gli avvisi di minaccia e i messaggi di notifica dispongono di un formato predefinito. Si consiglia di non modificare questo formato. Tuttavia, in alcuni casi (ad esempio, se si dispone di un sistema di elaborazione della posta automatizzato) potrebbe essere necessario modificare il formato dei messaggi.

Nel messaggio, le parole chiave (stringhe separate dai segni %) vengono sostituite dalle informazioni effettive specificate. Sono disponibili le parole chiave seguenti:

- **%TimeStamp%**: data e ora dell'evento
- **%Scanner%**: modulo interessato
- **%ComputerName%**: nome del computer in cui si è verificato l'avviso
- **%ProgramName%**: programma che ha generato l'avviso
- **%InfectedObject%**: nome del file, del messaggio, ecc. infetto
- **%VirusName%**: identificazione dell'infezione
- **%ErrorDescription%**: descrizione di un evento non virale

Le parole chiave **%InfectedObject%** e **%VirusName%** vengono utilizzate solo nei messaggi di allarme delle minacce, mentre **%ErrorDescription%** viene utilizzata solo nei messaggi di evento.

Utilizza caratteri alfabetici locali: applica la codifica dei caratteri ANSI a un messaggio e-mail in base alle impostazioni internazionali di Windows (ad esempio windows-1250). Se si lascia deselezionata questa opzione, il messaggio verrà convertito e codificato in ACSII a 7 bit (ad esempio, "á" verrà modificata in "a" e un simbolo sconosciuto verrà modificato in "?").

Utilizza codifica caratteri locali: l'origine del messaggio e-mail verrà codificata in formato Quoted-printable (QP) che utilizza i caratteri ASCII ed è in grado di trasmettere correttamente speciali caratteri internazionali tramite e-mail nel formato a 8 bit (áéíóú).

4.4.1.13 Seleziona campione per analisi

La finestra di dialogo per l'invio dei file consente di inviare un file o un sito a ESET ai fini dell'analisi ed è disponibile in **Strumenti**. > **Invia campione per l'analisi**. Se è stato trovato un file con un comportamento sospetto nel computer in uso o un sito sospetto su Internet, è possibile inviarlo al laboratorio di ricerca ESET per l'analisi. Se il file si rivela essere un'applicazione o un sito Web dannoso, il suo rilevamento verrà aggiunto in un aggiornamento successivo.

In alternativa, è possibile inviare il file tramite e-mail. Se si preferisce questa opzione, comprimere il file o i file con WinRAR/ZIP, proteggere l'archivio con la password "infected" e inviarlo a campioni@eset.com. Ricordare di inserire una descrizione nel campo dell'oggetto e di fornire il maggior numero di informazioni possibile sul file (ad esempio, l'indirizzo del sito Web dal quale è stato scaricato).

NOTA
Prima di inviare un file a ESET, assicurarsi che soddisfi uno o più dei criteri seguenti:

- il file non viene rilevato
- il file viene erroneamente rilevato come una minaccia

Non verrà inviata alcuna risposta a meno che non siano richieste ulteriori informazioni ai fini dell'analisi.

Selezionare la descrizione dal menu a discesa **Motivo per l'invio del file** che si avvicina maggiormente alla propria motivazione:

- **File sospetto**
- **Sito sospetto** (un sito Web infettato da un malware),
- **File falso positivo** (file che è stato rilevato come un'infezione ma che in realtà non è infetto),
- **Sito falso positivo**
- **Altro**

File/sito: percorso del file o del sito Web che si intende inviare.

E-mail contatto: una e-mail di contatto viene inviata a ESET insieme ai file sospetti e può essere utilizzata per contattare il mittente qualora fossero necessarie ulteriori informazioni ai fini dell'analisi. L'immissione dell'indirizzo e-mail di contatto è facoltativa. Il campione può essere **inviato in forma anonima**. ESET non invierà alcuna risposta a meno che non siano richieste ulteriori informazioni. Ogni giorno i server ESET ricevono decine di migliaia di file e non è pertanto possibile rispondere a tutti.

4.4.1.14 Aggiornamento Microsoft Windows®

La funzione di aggiornamento di Windows è un componente importante per la protezione del computer da software dannosi. Per questo motivo, è fondamentale installare gli aggiornamenti di Microsoft Windows non appena disponibili. ESET NOD32 Antivirus invia notifiche all'utente relative agli aggiornamenti mancanti in base al livello specificato. Sono disponibili i livelli seguenti:

- **Nessun aggiornamento**: non viene offerto alcun aggiornamento del sistema da scaricare.
- **Aggiornamenti facoltativi**: vengono offerti aggiornamenti con priorità bassa e di livello superiore da scaricare.
- **Aggiornamenti consigliati**: vengono offerti aggiornamenti contrassegnati come comuni e di livello superiore da scaricare.
- **Aggiornamenti importanti**: vengono offerti aggiornamenti contrassegnati come importanti e di livello superiore da scaricare.
- **Aggiornamenti critici**: vengono offerti unicamente aggiornamenti critici da scaricare.

Fare clic su **OK** per salvare le modifiche. Dopo la verifica dello stato mediante il server di aggiornamento, viene visualizzata la finestra Aggiornamenti del sistema. Le informazioni sull'aggiornamento del sistema non saranno pertanto disponibili immediatamente dopo il salvataggio delle modifiche.

4.4.1.15 ESET CMD

Questa funzione consente di attivare i comandi ecmd avanzati. Offre all'utente la possibilità di esportare e importare impostazioni utilizzando la riga di comando (ecmd.exe). Finora era possibile esportare e importare impostazioni utilizzando esclusivamente l'interfaccia utente grafica (Graphical User Interface, GUI). È ora possibile esportare la configurazione di ESET NOD32 Antivirus nel file *.xml*.

In caso di attivazione di ESET CMD sono disponibili due metodi di autorizzazione:

- **Nessuna**: nessuna autorizzazione. Si sconsiglia di utilizzare questo metodo in quanto consente di importare configurazioni non firmate che rappresentano un rischio potenziale.
- **Password configurazione avanzata**: utilizza la protezione con password. In caso di importazione della configurazione da un file *.xml*, questo deve essere firmato (vedere Firma del file di configurazione *.xml* di seguito). Questo metodo di autorizzazione verifica la password durante l'importazione della configurazione per controllare che vi sia una corrispondenza con la password specificata in Configurazione dell'accesso. Se la configurazione dell'accesso non è stata attivata, la password non corrisponde o il file di configurazione *.xml* non è firmato, la configurazione non sarà importata.

Dopo aver attivato ESET CMD, è possibile iniziare a utilizzare la riga di comando per l'esportazione/l'importazione della configurazione di ESET NOD32 Antivirus. È possibile eseguire questa operazione manualmente o creare uno script per l'automazione.

IMPORTANTE
Per utilizzare i comandi ecmd avanzati, è necessario eseguirli con privilegi di amministratore o aprire il prompt dei comandi di Windows (cmd) utilizzando **Esegui come amministratore**. In caso contrario, comparirà il messaggio **Error executing command.**. Inoltre, durante l'esportazione della configurazione, deve essere presente una cartella di destinazione.

NOTA
I comandi ecmd avanzati possono essere eseguiti solo localmente. L'esecuzione di un'attività client **Esegui comando** con ERA non funzionerà.

ESEMPIO
Comando Esporta impostazioni:

```
ecmd /getcfg c:\config\settings.xml
```

Comando Importa impostazioni:

```
ecmd /setcfg c:\config\settings.xml
```

Firma del file di configurazione *.xml*:

1. Scaricare **XmlSignTool** dalla pagina dei download degli strumenti e delle utilità ESET ed estrarlo. Questo strumento è stato appositamente sviluppato per la firma dei file di configurazione ESET *.xml*.
2. Aprire il prompt dei comandi di Windows (cmd) utilizzando **Esegui come amministratore**.
3. Accedere a un percorso con `XmlSignTool.exe`.
4. Eseguire un comando per firmare il file di configurazione *.xml*, utilizzo: `XmlSignTool <xml_file_path>`
5. Inserire e reinserire la password della Configurazione avanzata richiesta da XmlSignTool. Il file di configurazione *.xml* è ora firmato e può essere utilizzato per l'importazione di un'altra istanza di ESET NOD32 Antivirus con ESET CMD utilizzando il metodo di autorizzazione con password della configurazione avanzata.

AVVERTENZA
Si sconsiglia di attivare ESET CMD senza un'autorizzazione, in quanto tale operazione consentirà l'importazione di configurazioni non firmate. Impostare la password in **Configurazione avanzata** > **Interfaccia utente** > **Configurazione dell'accesso** per prevenire modifiche non autorizzate da parte degli utenti.

4.5 Interfaccia utente

La sezione **Interfaccia utente** consente di configurare il comportamento dell'interfaccia utente grafica (GUI) del programma.

Tramite lo strumento Grafica, è possibile regolare l'aspetto e gli effetti del programma.

Configurando Avvisi e notifiche, è possibile modificare il comportamento degli avvisi sulle minacce rilevate e le notifiche di sistema. in modo da adattarli alle proprie esigenze.

Per assicurare la massima protezione del software di protezione, è possibile impedire l'esecuzione di modifiche non autorizzate proteggendo le impostazioni mediante una password tramite lo strumento Impostazione dell'accesso.

4.5.1 Elementi dell'interfaccia utente

Le opzioni di configurazione dell'interfaccia utente in ESET NOD32 Antivirus consentono di modificare l'ambiente di lavoro per adattarlo alle esigenze specifiche dell'utente. Queste opzioni di configurazione sono accessibili nel ramo **Interfaccia utente** > **Elementi dell'interfaccia utente** della struttura Configurazione avanzata di ESET NOD32 Antivirus.

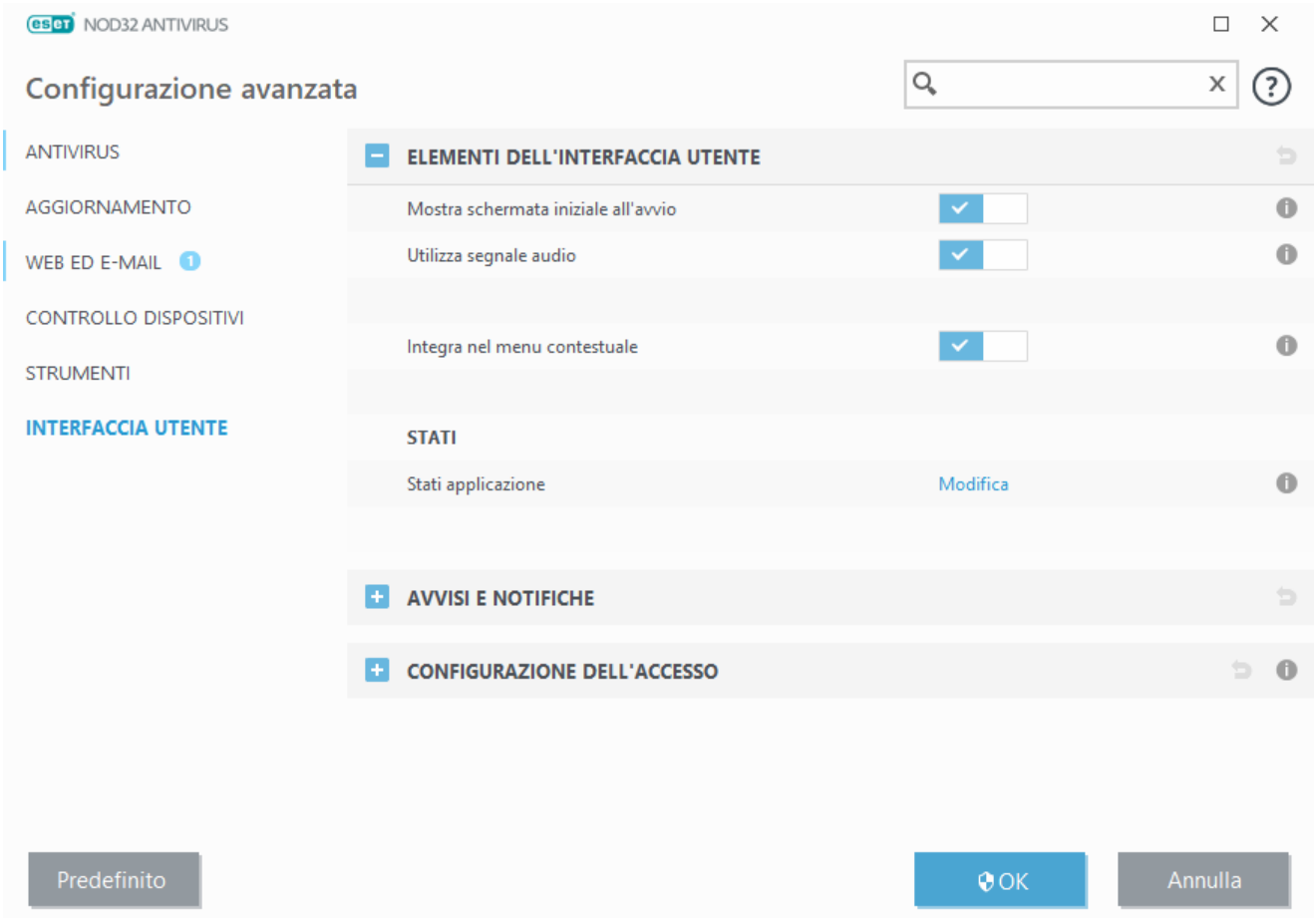
Se si desidera disattivare la schermata iniziale di ESET NOD32 Antivirus, deselezionare **Mostra schermata iniziale all'avvio**.

Per far sì che ESET NOD32 Antivirus emetta un suono al verificarsi di eventi importanti durante un controllo, ad esempio in caso di rilevamento di una minaccia o al termine del controllo, selezionare **Utilizza segnale audio**.

Integra nel menu contestuale: integra gli elementi di controllo di ESET NOD32 Antivirus nel menu contestuale.

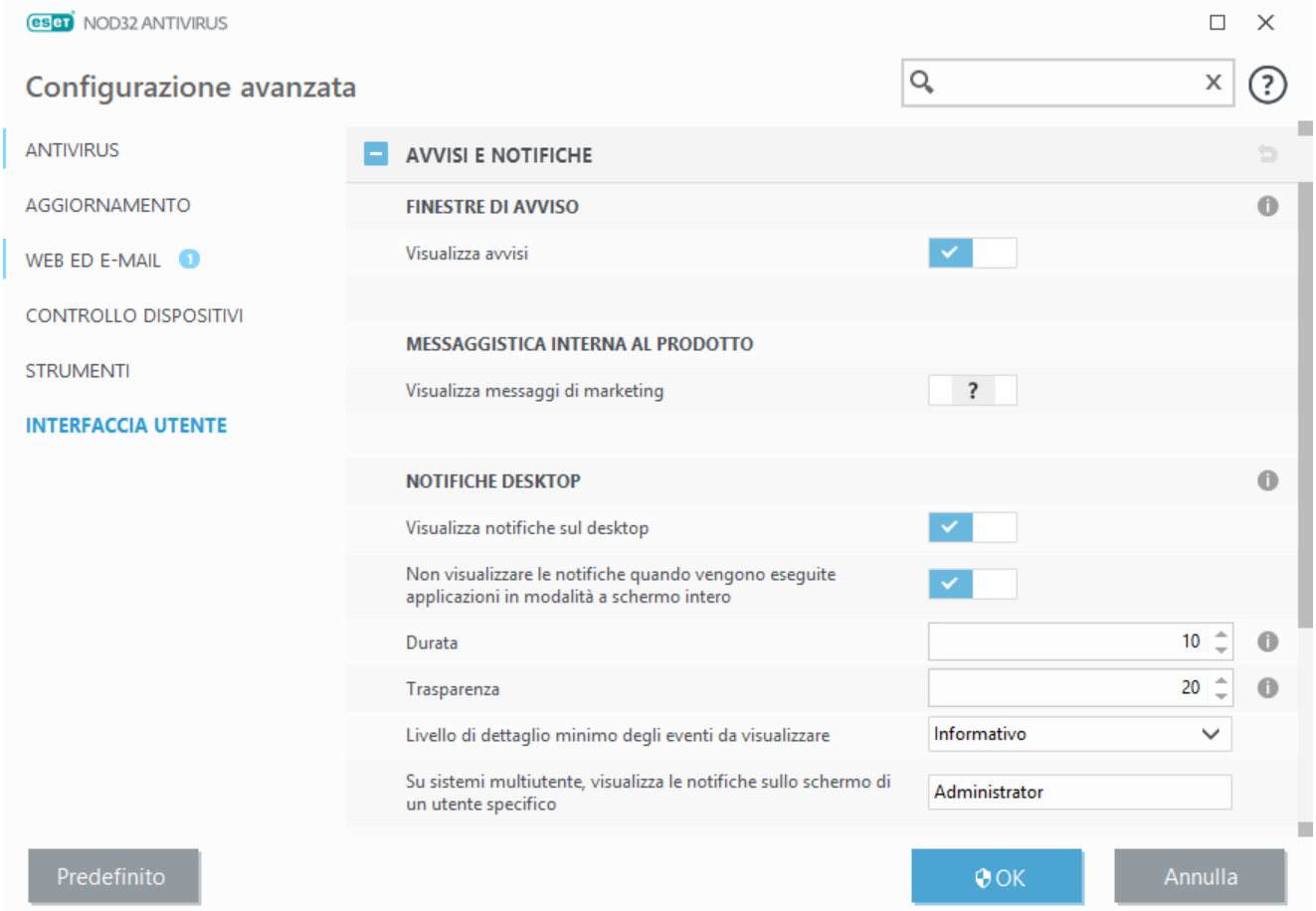
Stati

Stati applicazione: fare clic sul pulsante **Modifica** per gestire (disattivare) gli stati visualizzati nel riquadro **Stato protezione** nel menu principale.


NOD32 ANTIVIRUS
Configurazione avanzata
ANTIVIRUS
AGGIORNAMENTO
WEB ED E-MAIL
CONTROLLO DISPOSITIVI
STRUMENTI
INTERFACCIA UTENTE
ELEMENTI DELL'INTERFACCIA UTENTE
Mostra schermata iniziale all'avvio
Utilizza segnale audio
Integra nel menu contestuale
STATI
Stati applicazione
Modifica
AVVISI E NOTIFICHE
CONFIGURAZIONE DELL'ACCESSO
Predefinito
OK
Annulla

4.5.2 Avvisi e notifiche

La sezione **Avvisi e notifiche** sotto a **Interfaccia utente** consente di configurare la gestione dei messaggi di avviso relativi alle minacce e delle notifiche di sistema (ad esempio, messaggi di aggiornamenti riusciti) da parte di ESET NOD32 Antivirus. È inoltre possibile impostare l'ora di visualizzazione e il livello di trasparenza delle notifiche sulla barra delle applicazioni del sistema (applicabile solo ai sistemi che supportano le notifiche sulla barra delle applicazioni).



Finestre di avviso

Disattivando **Visualizza avvisi**, tutte le finestre di avviso verranno annullate. Per tale motivo, è consigliabile eseguire tale operazione solo in un numero limitato di situazioni specifiche. Nella maggior parte dei casi, si consiglia di non modificare l'impostazione predefinita (opzione attivata).

Messaggistica interna al prodotto

Visualizza messaggi di marketing: il servizio di messaggistica interno al prodotto è stato pensato allo scopo di informare gli utenti in merito alle novità di ESET e di inviare altri tipi di comunicazioni. Disattivare questa opzione qualora non si desideri ricevere messaggi di marketing.

Notifiche desktop

Le notifiche visualizzate sul desktop e i suggerimenti sono forniti esclusivamente a titolo informativo e non richiedono l'interazione dell'utente. Vengono visualizzati nell'area di notifica posta nell'angolo in basso a destra della schermata. Per attivare la visualizzazione delle notifiche sul desktop, selezionare **Visualizza notifiche sul desktop**.

Attivare **Non visualizzare le notifiche quando vengono eseguite applicazioni in modalità a schermo intero** per eliminare tutte le notifiche non interattive. È possibile modificare opzioni più dettagliate, ad esempio l'orario di visualizzazione della notifica e la trasparenza della finestra seguendo le istruzioni fornite di seguito.

Il menu a discesa **Livello di dettaglio minimo degli eventi da visualizzare** consente all'utente di selezionare il livello di gravità degli avvisi e delle notifiche da visualizzare. Sono disponibili le seguenti opzioni:

- **Diagnostica**: registra le informazioni necessarie ai fini dell'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativo**: registra i messaggi informativi, compresi quelli relativi agli aggiornamenti riusciti, e tutti i record indicati in precedenza.
- **Allarmi**: registra errori critici e messaggi di allarme.
- **Errori**: verranno registrati errori quali "Errore durante il download del file" ed errori critici.
- **Critico**: registra solo gli errori critici (errore che avvia la protezione antiviruse così via).

L'ultima funzione in questa sezione consente di configurare la destinazione delle notifiche in un ambiente multiutente. Nel campo **In sistemi multiutente, visualizza le notifiche sullo schermo di questo utente** viene specificato l'utente che riceverà le notifiche di sistema e di altro tipo sui sistemi che consentono la connessione simultanea di più utenti. In genere si tratta di un amministratore di sistema o di rete. Questa opzione è utile soprattutto per i server di terminali, a condizione che tutte le notifiche di sistema vengano inviate all'amministratore.

Finestre di messaggio

Per chiudere automaticamente le finestre popup dopo un determinato periodo di tempo, selezionare **Chiudi automaticamente le finestre di messaggio**. Se non vengono chiuse manualmente, le finestre di avviso vengono chiuse automaticamente una volta trascorso il periodo di tempo specificato.

Messaggi di conferma: consente all'utente di visualizzare un elenco di messaggi di conferma che è possibile decidere di visualizzare o non visualizzare.

4.5.2.1 Configurazione avanzata

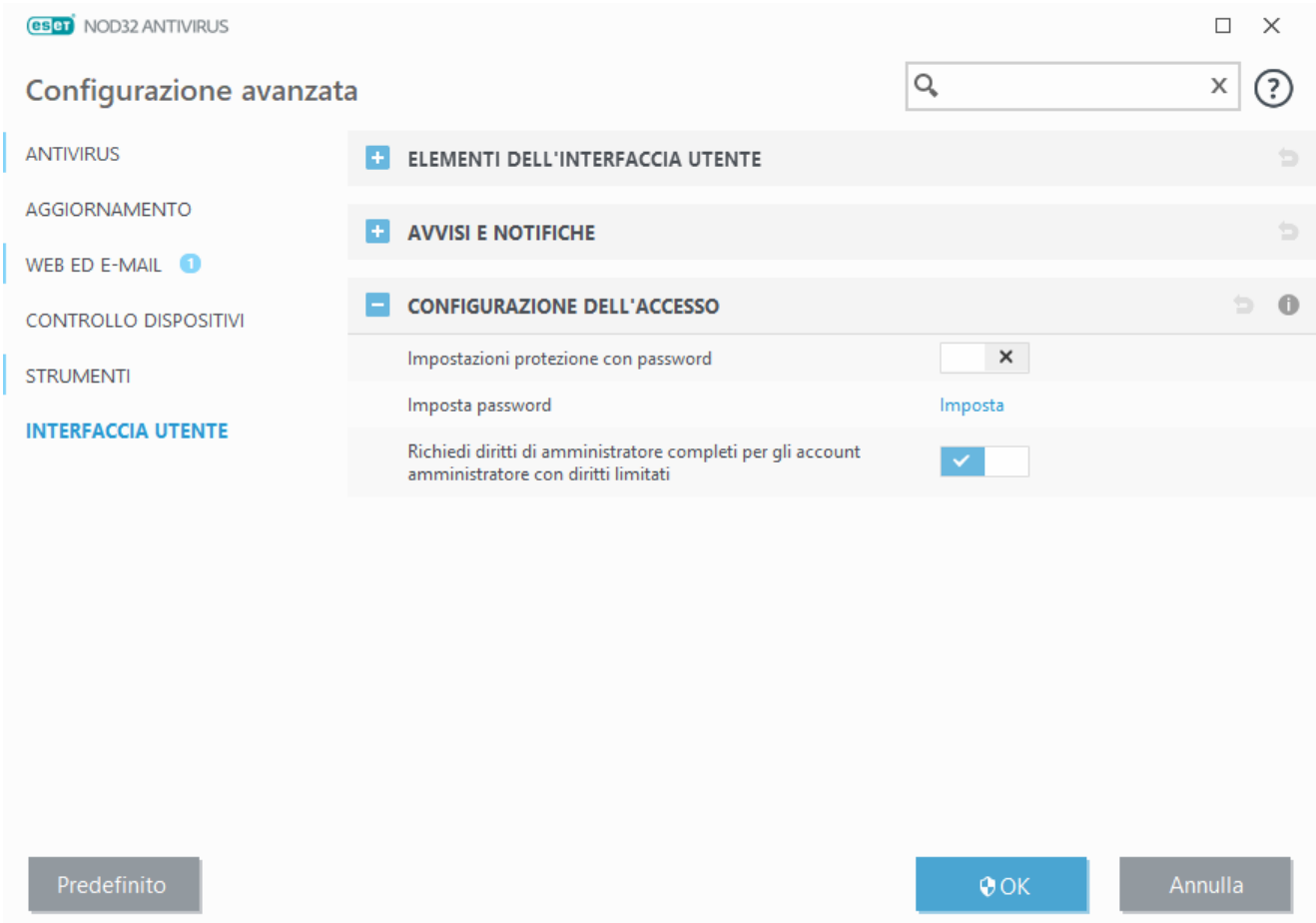
Nel menu a discesa **Livello di dettaglio minimo degli eventi da visualizzare** è possibile selezionare il livello iniziale di gravità degli avvisi e delle notifiche da visualizzare.

- **Diagnostica**: registra le informazioni necessarie ai fini dell'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativo**: registra i messaggi informativi, compresi quelli relativi agli aggiornamenti riusciti, e tutti i record indicati in precedenza.
- **Allarmi**: registra errori critici e messaggi di allarme.
- **Errori**: verranno registrati errori quali *"Errore durante il download del file"* ed errori critici.
- **Critico**: registra solo gli errori critici (errore che avvia la protezione antiviruse così via).

L'ultima funzione in questa sezione consente di configurare la destinazione delle notifiche in un ambiente multi-utente. Nel campo **In sistemi multiutente, visualizza le notifiche sullo schermo di questo utente** viene specificato l'utente che riceverà le notifiche di sistema e di altro tipo sui sistemi che consentono la connessione simultanea di più utenti. In genere si tratta di un amministratore di sistema o di rete. Questa opzione è utile soprattutto per i server di terminali, a condizione che tutte le notifiche di sistema vengano inviate all'amministratore.

4.5.3 Configurazione dell'accesso

Le impostazioni ESET NOD32 Antivirus rappresentano una parte cruciale dei criteri di protezione. Modifiche non autorizzate potrebbero mettere a rischio la stabilità e la protezione del sistema. Per evitare modifiche non autorizzate, i parametri di configurazione di ESET NOD32 Antivirus possono essere protetti con password.



Impostazioni protette con password: indica le impostazioni relative alla password. Fare clic per aprire la finestra di configurazione della password.

Per impostare o modificare una password al fine di proteggere i parametri di configurazione, fare clic su **Imposta**.

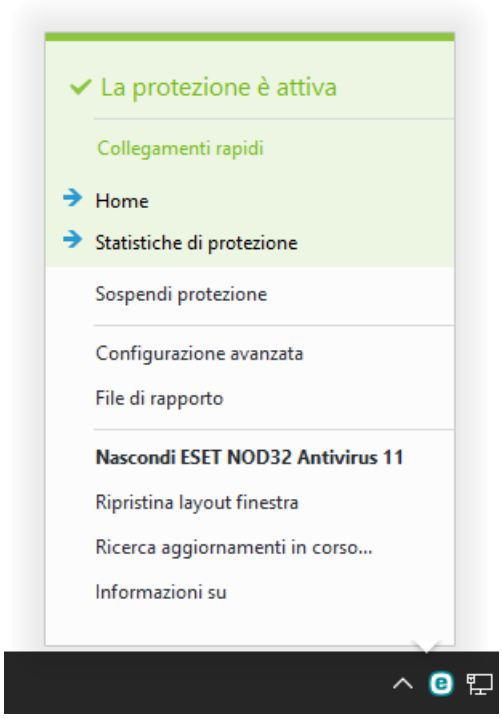
Richiedi diritti di amministratore completi per gli account con diritti limitati: selezionare questa opzione per richiedere all'utente corrente (nel caso non disponga dei diritti di amministratore) di inserire un nome utente e una password di amministratore per la modifica di alcuni parametri del sistema (analogo a Controllo dell'account utente (UAC) in Windows Vista e Windows 7). Tali modifiche includono la disattivazione dei moduli di protezione. Sui sistemi Windows XP, in cui l'UAC non è in esecuzione, gli utenti avranno a disposizione l'opzione **Richiedi diritti di amministratore (sistema senza supporto Controllo dell'account utente)**.

Solo per Windows XP:

Richiedi diritti di amministratore (sistema senza supporto Controllo dell'account utente): attivare questa opzione per ottenere il prompt di ESET NOD32 Antivirus relativo alle credenziali dell'amministratore.

4.5.4 Menu del programma

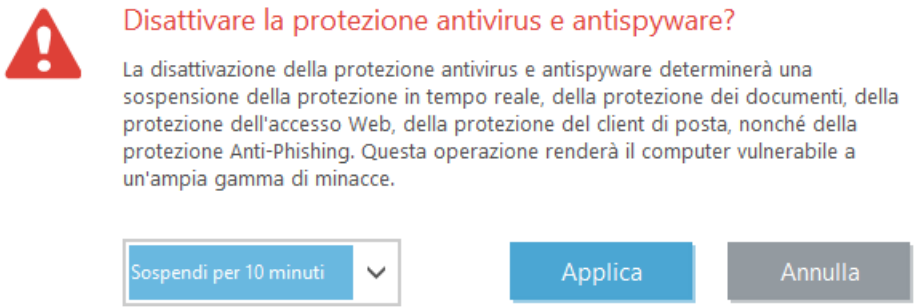
Alcune delle principali opzioni di configurazione e funzionalità sono disponibili facendo clic con il pulsante destro del mouse sull'icona della barra delle applicazioni .



Collegamenti rapidi: consente di visualizzare le parti di ESET NOD32 Antivirus che vengono utilizzate più frequentemente. È possibile accedervi rapidamente dal menu del programma.

Sospendi protezione: consente di visualizzare la finestra di dialogo di conferma per disattivare la Protezione antivirus e antispyware che protegge il sistema da attacchi dannosi controllando file e comunicazioni Web ed e-mail.

Il menu a discesa **Intervallo di tempo** rappresenta l'intervallo di tempo durante il quale la Protezione antivirus e antispyware verrà disattivata.



Configurazione avanzata: selezionare questa opzione per accedere alla struttura **Configurazione avanzata**. Vi sono anche altri modi per aprire la Configurazione avanzata, ad esempio, premendo il tasto F5 oppure accedendo a **Configurazione** > **Configurazione avanzata**.

File di rapporto: i file di rapporto contengono informazioni relative agli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate.

Nascondi ESET NOD32 Antivirus: nasconde la finestra di ESET NOD32 Antivirus dalla schermata.

Ripristina layout finestra: ripristina le dimensioni predefinite e la posizione sullo schermo della finestra di ESET NOD32 Antivirus.

Ricerca aggiornamenti: avvia l'aggiornamento del motore di rilevamento (precedentemente noto con il nome di "database delle firme antivirali") per garantire il livello di protezione stabilito dall'utente contro codici dannosi.

Informazioni: vengono fornite informazioni sul sistema, sulla versione installata di ESET NOD32 Antivirus e sui moduli di programma installati. In questa sezione è anche possibile trovare la data di scadenza della licenza e le informazioni relative al sistema operativo e alle risorse di sistema.

5. Utente avanzato

5.1 Profili

La Gestione profili viene utilizzata in due modi all'interno di ESET NOD32 Antivirus: nella sezione **Controllo computer su richiesta** e nella sezione **Aggiorna**.

Controllo del computer

È possibile salvare i parametri di scansione preferiti per i controlli futuri. È consigliabile creare un profilo di scansione differente (con diversi oggetti da controllare, metodi di scansione e altri parametri) per ciascuna scansione utilizzata abitualmente.

Per creare un nuovo profilo, aprire la finestra Configurazione avanzata (F5) e fare clic su **Antivirus** > **Controllo computer su richiesta** > **Di base** > **Elenco di profili**. Nella finestra **Gestione profili** è disponibile un menu a discesa **Profili selezionati** contenente i profili di scansione esistenti e l'opzione per crearne di nuovi. Per ricevere assistenza durante la creazione di un profilo di controllo adatto alle proprie esigenze, consultare la sezione Configurazione parametri motore ThreatSense contenente una descrizione di ciascun parametro di configurazione del controllo.

NOTA
Si supponga di voler creare il proprio profilo di controllo e che la configurazione **Controlla il computer in uso** sia appropriata solo in parte, in quanto non si desidera eseguire il controllo di eseguibili compressi o di applicazioni potenzialmente pericolose e si intende applicare l'opzione **Massima pulizia**. Inserire il nome del nuovo profilo nella finestra **Gestione profili** e fare clic su **Aggiungi**. Selezionare il nuovo profilo dal menu a discesa **Profilo selezionato**, modificare i parametri rimanenti in base alle proprie esigenze e fare clic su **OK** per salvare il nuovo profilo.

Aggiorna

L'editor dei profili nella sezione Impostazione aggiornamento consente agli utenti di creare nuovi profili di aggiornamento. Creare e utilizzare i profili personalizzati (diversi dal **Profilo personale** predefinito) solo se il computer utilizza vari metodi di connessione ai server di aggiornamento.

Ad esempio, un computer portatile che si connette normalmente a un server locale (Mirror) nella rete locale ma scarica gli aggiornamenti direttamente dai server di aggiornamento ESET durante la disconnessione (trasferta di lavoro) potrebbe utilizzare due profili: il primo per connettersi al server locale e il secondo per connettersi ai server ESET. Dopo aver configurato questi profili, accedere a **Strumenti** > **Pianificazione attività** e modificare i parametri delle attività di aggiornamento. Indicare un profilo come principale e l'altro come secondario.

Profilo di aggiornamento: profilo di aggiornamento attualmente utilizzato. Per modificarlo, scegliere un profilo dal menu a discesa.

Elenco di profili: crea nuovi profili di aggiornamento o rimuove quelli esistenti.

5.2 Tasti di scelta rapida

Per una migliore navigazione del prodotto ESET, è possibile utilizzare i seguenti tasti di scelta rapida:

F1	apre le pagine della Guida
F5	apre la Configurazione avanzata
Tasti Su/Giù	navigazione all'interno delle voci del prodotto
-	comprime i nodi della struttura Configurazione avanzata
TAB	sposta il cursore in una finestra
Esc	chiude la finestra di dialogo attiva

5.3 Diagnostica

La diagnostica fornisce dump sulle interruzioni delle applicazioni correlate ai processi ESET (ad esempio, *ekrn*). In caso di interruzione di un'applicazione, verrà generato un dump, che aiuta gli sviluppatori a eseguire il debug e correggere vari problemi di ESET NOD32 Antivirus. Fare clic sul menu a discesa accanto a **Tipo di dump** e selezionare una delle tre opzioni disponibili:

- Selezionare **Disattiva** (impostazione predefinita) per disattivare questa funzionalità.
- **Mini**: registra il minor numero di informazioni utili che potrebbero contribuire all'identificazione del motivo alla base dell'arresto inaspettato dell'applicazione. Questo tipo di file dump risulta utile in caso di limitazioni di spazio. Tuttavia, a causa delle informazioni limitate incluse, gli errori che non sono stati causati direttamente dalla minaccia in esecuzione quando si è verificato il problema potrebbero non essere rilevati a seguito di un'analisi del file in questione.
- **Completo**: registra tutti i contenuti della memoria di sistema quando l'applicazione viene interrotta inaspettatamente. Un dump memoria completo può contenete dati estrapolati dai processi in esecuzione quando è stato raccolto il dump di memoria.

Attiva registrazione avanzata filtraggio protocolli: registra tutti i dati che attraversano il motore di filtraggio protocolli in formato PCAP. Tale operazione consente agli sviluppatori di diagnosticare e risolvere problemi correlati al filtraggio protocolli.

Attiva registrazione avanzata motore aggiornamenti: registra tutti gli eventi che si verificano durante il processo di aggiornamento. Permette agli sviluppatori di facilitare diagnosi e correzione di eventuali problemi legati al motore degli aggiornamenti.

I file di rapporto sono disponibili in:
C:\ProgramData\ESET\ESET NOD32 Antivirus\Diagnostics su Windows Vista e versioni successive o *C:\Documents and Settings\All Users\...* sulle versioni precedenti di Windows.

Directory di destinazione: directory nella quale verrà generato il dump durante l'arresto imprevisto.

Apri cartella diagnostica: fare clic su **Apri** per aprire questa directory in una nuova finestra di *Windows Explorer*.

Crea dump diagnostico: fare clic su **Crea** per creare file di dump diagnostici nella **Directory di destinazione**.

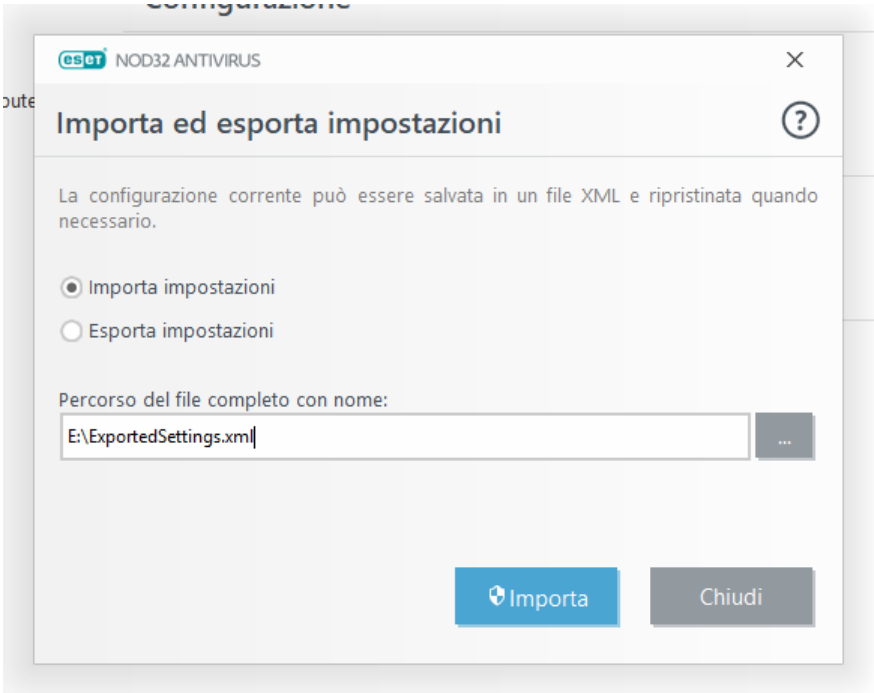
5.4 Importa ed esporta impostazioni

È possibile importare o esportare il file di configurazione personalizzato in formato .xml di ESET NOD32 Antivirus dal menu **Configurazione**.

I file di importazione e di esportazione sono utili se si necessita effettuare un backup della configurazione corrente di ESET NOD32 Antivirus da utilizzare in un secondo momento. L'opzione di esportazione delle impostazioni è utile anche per gli utenti che desiderano utilizzare la configurazione preferita su più sistemi. In tal modo, sarà possibile importare facilmente un file *.xml* per il trasferimento di queste impostazioni.

L'importazione della configurazione è molto semplice. Nella finestra principale del programma, fare clic su **Configurazione** > **Importa ed esporta impostazioni**, quindi selezionare **Importa impostazioni**. Inserire il percorso del file di configurazione o fare clic sul pulsante **...** per ricercare il file di configurazione che si vuole importare.

Le operazioni per esportare una configurazione sono molto simili. Nella finestra principale del programma, fare clic su **Configurazione** > **Importa ed esporta impostazioni**. Selezionare **Esporta impostazioni** e inserire il percorso del file di configurazione (ad esempio, *export.xml*). Utilizzare il browser per selezionare un percorso sul computer in cui salvare il file di configurazione.



NOTA
durante l'esportazione delle impostazioni potrebbe comparire un errore se non si dispone degli idonei diritti di scrittura del file esportato nella directory specificata.

5.5 ESET SysInspector

5.5.1 Introduzione a ESET SysInspector

ESET SysInspector è un'applicazione che effettua un controllo approfondito del computer e consente di visualizzare i dati raccolti in modo completo. Informazioni quali driver e applicazioni installati, connessioni di rete o voci di registro importanti aiutano l'utente ad analizzare comportamenti sospetti del sistema dovuti, ad esempio, a incompatibilità di software o hardware o a infezioni causate da malware.

Esistono due modi per accedere a ESET SysInspector: Dalla versione integrata nelle soluzioni ESET Security oppure scaricando gratuitamente la versione indipendente (SysInspector.exe) dal sito Web di ESET. Le versioni presentano le stesse funzioni e gli stessi comandi. L'unica differenza consiste nella gestione dei risultati. La versione indipendente e quella integrata consentono all'utente di esportare gli snapshot di sistema in un file *.xml* e di salvarli sul disco. La versione integrata offre inoltre la possibilità di archiviare gli snapshot di sistema direttamente in **Strumenti** > **ESET SysInspector** (eccetto ESET Remote Administrator). Per ulteriori informazioni, consultare la sezione ESET SysInspector come parte di ESET NOD32 Antivirus.

Attendere alcuni istanti per consentire a ESET SysInspector di effettuare il controllo del computer. L'operazione potrebbe richiedere dai 10 secondi a pochi minuti, a seconda della configurazione hardware, del sistema operativo e del numero di applicazioni installate sul computer.

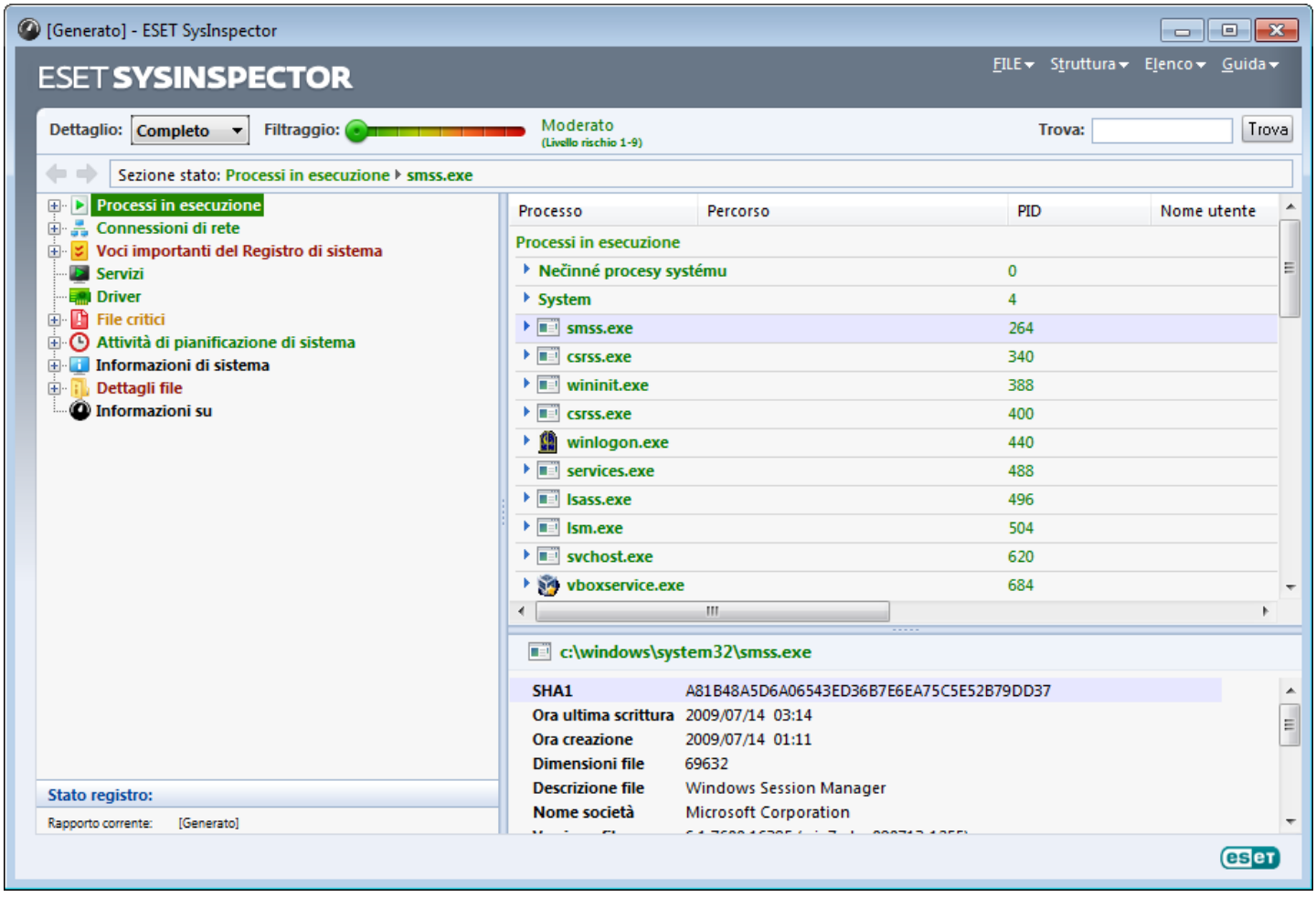
5.5.1.1 Avvio di ESET SysInspector

Per avviare ESET SysInspector, basta eseguire l'eseguibile *SysInspector.exe* scaricato dal sito Web di ESET. Se è già installata una delle soluzioni ESET Security, è possibile eseguire ESET SysInspector direttamente dal menu Start (fare clic su **Programmi** > **ESET** > **ESET NOD32 Antivirus**).

Si prega di attendere che l'applicazione abbia esaminato il sistema in uso. Questa operazione potrebbe richiedere diversi minuti.

5.5.2 Interfaccia utente e uso dell'applicazione

Per chiarezza, la finestra principale del programma è stata divisa in quattro sezioni principali: i comandi del programma sono posizionati nella parte superiore della finestra; a sinistra viene visualizzata la finestra di spostamento, a destra è disponibile la finestra Descrizione e, infine, nella parte inferiore della schermata, viene visualizzata la finestra Dettagli. La sezione Stato del rapporto contiene un elenco dei parametri di base di un rapporto (filtro utilizzato, tipo di filtro, il rapporto è il risultato di un confronto, ecc.).



5.5.2.1 Comandi del programma

Questa sezione contiene una descrizione di tutti i comandi del programma disponibili in ESET SysInspector.

File

Facendo clic su **File**, è possibile memorizzare lo stato corrente del sistema per analisi successive o aprire un rapporto memorizzato in precedenza. Ai fini della pubblicazione, si consiglia di generare un rapporto **Adatto per l'invio**. Questa visualizzazione del rapporto consente di omettere informazioni sensibili (nome dell'utente corrente, nome del computer, nome del dominio, privilegi dell'utente corrente, variabili d'ambiente, ecc.).

NOTA: è possibile aprire i rapporti di ESET SysInspector precedentemente archiviati trascinandoli nella finestra principale del programma.

Struttura

Consente di espandere o comprimere tutti i nodi e di esportare le sezioni selezionate nello script di servizio.

Elenco

Contiene funzionalità per una più agevole navigazione del programma insieme ad altre funzionalità quali la ricerca di informazioni on-line.

Guida

Contiene informazioni sull'applicazione e le relative funzionalità.

Dettaglio

Questa impostazione influenza le informazioni visualizzate nella finestra principale del programma al fine di semplificarne l'utilizzo. In modalità "Base", l'utente ha accesso alle informazioni utilizzate per ricercare soluzioni a problemi comuni del sistema. In modalità "Media", il programma consente di visualizzare dettagli utilizzati con minore frequenza. In modalità "Completa", ESET SysInspector consente di visualizzare tutte le informazioni necessarie per risolvere problemi molto specifici.

Filtraggio

Il filtraggio delle voci viene utilizzato preferibilmente per ricercare file sospetti o voci di registro nel sistema. Regolando il dispositivo di scorrimento, è possibile filtrare le voci in base al livello di rischio. Se il dispositivo di scorrimento è posizionato tutto a sinistra (Livello di rischio 1), verranno visualizzate tutte le voci. Spostando il cursore a destra, il programma esclude tutti gli elementi meno rischiosi rispetto al livello di rischio corrente, consentendo di visualizzare solo gli elementi che risultano più sospetti rispetto al livello visualizzato. Se il dispositivo di scorrimento è posizionato tutto a destra, il programma consentirà di visualizzare solo le voci pericolose conosciute.

Tutti gli elementi contrassegnati con un livello di rischio compreso tra 6 e 9 rappresentano un rischio per la sicurezza. Se non si utilizza una soluzione di protezione ESET, si consiglia di controllare il sistema con ESET Online Scanner, in caso di rilevamento di una voce che presenta queste caratteristiche da parte di ESET SysInspector. ESET Online Scanner è un servizio gratuito.

NOTA: il livello di rischio di una voce può essere determinato rapidamente confrontando il colore della voce con il colore del dispositivo di scorrimento del livello di rischio.

Confronta

Durante il confronto di due rapporti, è possibile scegliere di visualizzare tutti gli elementi, solo gli elementi aggiunti, solo gli elementi rimossi o solo gli elementi sostituiti.

Trova

È possibile utilizzare la funzione di ricerca per ricercare rapidamente una voce specifica in base al nome o parte di esso. I risultati della ricerca vengono visualizzati nella finestra Descrizione.

Ritorna

Facendo clic sulle frecce indietro o avanti, è possibile tornare alle informazioni precedentemente visualizzate nella finestra Descrizione. È possibile utilizzare i tasti Cancella e Barra spaziatrice anziché fare clic su Avanti e Indietro.

Sezione Stato

Consente di visualizzare il nodo corrente nella finestra Navigazione.

Importante: le voci evidenziate in rosso sono voci sconosciute che vengono quindi contrassegnate dal programma come potenzialmente pericolose. Se una voce è contrassegnata in rosso, ciò non significa necessariamente che è possibile eliminare il file. Prima dell'eliminazione, assicurarsi che i file siano realmente pericolosi o non necessari.

5.5.2.2 Navigazione in ESET SysInspector

ESET SysInspector suddivide vari tipi di informazioni in diverse sezioni di base chiamate nodi. Espandendo ciascun nodo nei vari sottonodi eventualmente disponibili, è possibile trovare dettagli aggiuntivi. Per espandere o comprimere un nodo, fare doppio clic sul nome del nodo oppure fare clic su ⊞ o ⊟ accanto al nome del nodo. Durante l'esplorazione della struttura ad albero dei nodi e dei sottonodi nella finestra Navigazione, è possibile visualizzare vari dettagli per ciascun nodo presente nella finestra Descrizione. Durante l'esplorazione delle voci nella finestra Descrizione, è possibile visualizzare dettagli aggiuntivi nella finestra Dettagli.

Seguono le descrizioni dei nodi principali nella finestra Navigazione e le informazioni correlate nelle finestre Descrizione e Dettagli.

Processi in esecuzione

Il nodo contiene informazioni sulle applicazioni e sui processi in esecuzione al momento della generazione del rapporto. Nella finestra Descrizione, è possibile trovare dettagli aggiuntivi per ciascun processo, tra cui librerie dinamiche utilizzate dal processo e la relativa posizione nel sistema, il nome del rivenditore dell'applicazione e il livello di rischio del file.

La finestra Dettagli contiene informazioni aggiuntive relative alle voci selezionate nella finestra Descrizione, tra cui le dimensioni o l'hash del file.

NOTA: un sistema operativo è basato su diversi componenti kernel, costantemente in esecuzione, che forniscono funzioni fondamentali e di base per le altre applicazioni utente. In alcuni casi, questi processi vengono visualizzati nello strumento ESET SysInspector, il cui percorso del file inizia per \??\. Questi simboli, che offrono un'ottimizzazione pre-lancio dei processi, sono sicuri per il sistema.

Connessioni di rete

La finestra Descrizione contiene un elenco di processi e di applicazioni che comunicano in rete mediante il protocollo selezionato nella finestra Navigazione (TCP o UDP) insieme all'indirizzo remoto al quale è connessa l'applicazione. È inoltre possibile verificare gli indirizzi IP dei server DNS.

La finestra Dettagli contiene informazioni aggiuntive relative alle voci selezionate nella finestra Descrizione, tra cui le dimensioni o l'hash del file.

Voci di registro importanti

Contiene un elenco di voci di registro selezionate che sono spesso correlate a vari problemi del sistema in uso, tra cui quelli che specificano i programmi di avvio, gli oggetti helper browser (BHO), ecc.

Nella finestra Descrizione è possibile individuare i file correlati a specifiche voci di registro. La finestra Dettagli contiene dettagli aggiuntivi.

Servizi

La finestra Descrizione contiene un elenco di file registrati come Servizi di Windows. È possibile verificare la configurazione dell'avvio del servizio e consultare dettagli specifici del file nella finestra Dettagli.

Driver

Elenco di driver installati nel sistema.

File critici

La finestra Descrizione consente di visualizzare il contenuto di file critici correlati al sistema operativo Microsoft Windows.

Attività dell'utilità di pianificazione del sistema

Contiene un elenco di attività attivate dall'utilità di pianificazione di Windows a un'ora o un intervallo specificati.

Informazioni di sistema

Contiene informazioni dettagliate sull'hardware e il software, nonché dettagli relativi alle variabili ambientali impostate, ai diritti dell'utente e ai rapporti degli eventi di sistema.

Dettagli dei file

Elenco dei file importanti di sistema e dei file della cartella Programmi. Ulteriori informazioni specifiche dei file sono disponibili nelle finestre Descrizione e Dettagli.

Informazioni su

Informazioni sulla versione di ESET SysInspector ed elenco dei moduli di programma.

5.5.2.2.1 Tasti di scelta rapida

Segue un elenco dei tasti di scelta rapida che è possibile utilizzare con il programma ESET SysInspector:

File

Ctrl+O	apre il rapporto esistente
Ctrl+S	salva i rapporti creati

Genera

Ctrl+G	genera uno snapshot di stato di un computer standard
Ctrl+H	genera lo snapshot di stato di un computer che potrebbe anche registrare informazioni sensibili

Filtraggio delle voci

1, O	sicuro, vengono visualizzate le voci con un livello di rischio compreso tra 1 e 9
2	sicuro, vengono visualizzate le voci con un livello di rischio compreso tra 2 e 9
3	sicuro, vengono visualizzate le voci con un livello di rischio compreso tra 3 e 9
4, U	sconosciuto, vengono visualizzate le voci con un livello di rischio compreso tra 4 e 9
5	sconosciuto, vengono visualizzate le voci con un livello di rischio compreso tra 5 e 9
6	sconosciuto, vengono visualizzate le voci con un livello di rischio compreso tra 6 e 9
7, B	a rischio, vengono visualizzate le voci con un livello di rischio compreso tra 7 e 9
8	a rischio, vengono visualizzate le voci con un livello di rischio compreso tra 8 e 9
9	a rischio, vengono visualizzate le voci con un livello di rischio 9
-	riduce il livello di rischio
+	aumenta il livello di rischio
Ctrl+9	modalità di filtraggio, livello equivalente o superiore
Ctrl+0	modalità di filtraggio, solo livello equivalente

Visualizza

Ctrl+5	visualizza in base al rivenditore, tutti i rivenditori
Ctrl+6	visualizza in base al rivenditore, solo Microsoft
Ctrl+7	visualizza in base al rivenditore, tutti gli altri rivenditori
Ctrl+3	consente di visualizzare tutti i dettagli
Ctrl+2	consente di visualizzare un livello di dettaglio medio
Ctrl+1	visualizzazione di base
BackSpace	si sposta indietro di uno
Barra spaziatrice	si sposta in avanti di uno
Ctrl+W	espande la struttura ad albero
Ctrl+Q	comprime la struttura ad albero

Altri comandi

Ctrl+T	raggiunge la posizione originale della voce selezionata nei risultati di ricerca
Ctrl+P	consente di visualizzare informazioni di base su una voce

Ctrl+A	consente di visualizzare informazioni complete su una voce
Ctrl+C	copia la struttura ad albero della voce corrente
Ctrl+X	copia le voci
Ctrl+B	cerca informazioni sui file selezionati su Internet
Ctrl+L	apre la cartella in cui si trova il file selezionato
Ctrl+R	apre la voce corrispondente nell'editor del registro
Ctrl+Z	copia un percorso in un file (se la voce è correlata a un file)
Ctrl+F	passa al campo di ricerca
Ctrl+D	chiude i risultati di ricerca
Ctrl+E	esegue lo script di servizio

Confronto

Ctrl+Alt+O	apre il rapporto originale/comparativo
Ctrl+Alt+R	annulla il confronto
Ctrl+Alt+1	consente di visualizzare tutte le voci
Ctrl+Alt+2	consente di visualizzare solo le voci aggiunte, il rapporto consentirà di visualizzare le voci presenti nel rapporto corrente
Ctrl+Alt+3	consente di visualizzare solo le voci rimosse, il rapporto consentirà di visualizzare le voci presenti nel rapporto precedente
Ctrl+Alt+4	consente di visualizzare solo le voci sostituite (file compresi)
Ctrl+Alt+5	consente di visualizzare solo le differenze tra i rapporti
Ctrl+Alt+C	consente di visualizzare il confronto
Ctrl+Alt+N	consente di visualizzare il rapporto corrente
Ctrl+Alt+P	apre il rapporto precedente

Varie

F1	visualizza guida
Alt+F4	chiudi il programma
Alt+Shift+F4	chiudi il programma senza chiedere
Ctrl+I	statistiche del rapporto

5.5.2.3 Confronta

La funzionalità Confronta consente all'utente di confrontare due rapporti esistenti. Il risultato di questa funzionalità consiste in una serie di voci non comuni a entrambi i rapporti. È la soluzione ideale se si desidera individuare le modifiche nel sistema ed è un utile strumento per il rilevamento di codice dannoso.

Dopo essere stata lanciata, l'applicazione crea un nuovo rapporto visualizzato in una nuova finestra. Fare clic su **File** > **Salva rapporto** per salvare un rapporto in un file. I file di rapporto possono essere aperti e visualizzati in un secondo momento. Per aprire un rapporto esistente, fare clic su **File** > **Apri rapporto**. Nella finestra principale del programma, ESET SysInspector consente di visualizzare sempre un rapporto alla volta.

Il vantaggio di confrontare due rapporti consiste nella possibilità di visualizzare un rapporto attualmente attivo e un rapporto salvato in un file. Per confrontare i rapporti, fare clic su **File** > **Confronta rapporto** e scegliere **Seleziona file**. Il rapporto selezionato verrà confrontato con quello attivo nelle finestre principali del programma. Il rapporto comparativo consentirà di visualizzare esclusivamente le differenze tra questi due rapporti.

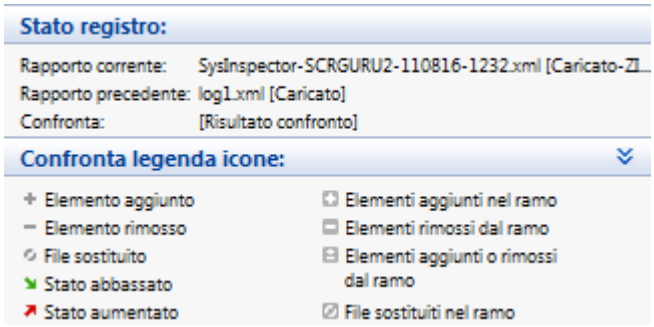
NOTA: se si mettono a confronto due file di rapporto, facendo clic su **File** > **Salva rapporto** e salvandoli in un file ZIP, verranno salvati entrambi i file. Se si apre il file in un secondo momento, i rapporti contenuti vengono confrontati automaticamente.

Vicino alle voci visualizzate, ESET SysInspector consente di visualizzare i simboli che identificano le differenze tra i rapporti confrontati.

Segue una descrizione dei simboli visualizzati vicino alle voci:

- nuovo valore, non presente nel rapporto precedente
- la sezione della struttura ad albero contiene nuovi valori
- valore rimosso, presente solo nel rapporto precedente
- la sezione della struttura ad albero contiene valori rimossi
- il valore/file è stato modificato
- la sezione della struttura ad albero contiene valori/file modificati
- il livello di rischio è diminuito/era superiore nel rapporto precedente
- il livello di rischio è aumentato/era inferiore nel rapporto precedente

La sezione esplicativa visualizzata nell'angolo in basso a sinistra contiene una descrizione di tutti i simboli e consente inoltre di visualizzare i nomi dei rapporti confrontati.



I rapporti comparativi possono essere salvati in un file e aperti in un secondo momento.

Esempio

Generare e salvare un rapporto registrando le informazioni originali sul sistema in un file chiamato previous.xml. Dopo aver apportato le modifiche al sistema, aprire ESET SysInspector e consentire all'applicazione di generare un nuovo rapporto. Salvarlo in un file chiamato *current.xml*.

Al fine di rilevare le modifiche tra i due rapporti, fare clic su **File** > **Confronta rapporti**. Il programma creerà un rapporto comparativo contenente le differenze tra i rapporti.

Lo stesso risultato può essere ottenuto utilizzando la seguente opzione della riga di comando:

SysIsnpector.exe current.xml previous.xml

5.5.3 Parametri della riga di comando

ESET SysInspector supporta la generazione di rapporti dalla riga di comando mediante l'utilizzo dei seguenti parametri:

/gen	genera rapporto direttamente dalla riga di comando senza avviare l'interfaccia grafica utente (GUI)
/privacy	genera rapporto omettendo le informazioni sensibili
/zip	salva rapporto in un archivio zip compresso
/silent	non visualizzare finestra di avanzamento durante la creazione del rapporto dalla riga di comando
/blank	avvia ESET SysInspector senza generare/caricare il rapporto

Esempi

Utilizzo:

```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

Per caricare un rapporto specifico direttamente nel browser, utilizzare: *SysInspector.exe .\clientlog.xml*
Per generare il rapporto dalla riga di comando, utilizzare: *SysInspector.exe /gen=.\mynewlog.xml*
Per generare un rapporto escludendo le informazioni sensibili direttamente in un file compresso, utilizzare: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Per confrontare due file di rapporto ed esaminare le differenze, utilizzare: *SysInspector.exe new.xml old.xml*

NOTA: se il nome del file o della cartella contiene uno spazio, è necessario utilizzare le virgolette.

5.5.4 Script di servizio

Lo script di servizio è uno strumento che offre assistenza ai clienti che utilizzano ESET SysInspector rimuovendo facilmente oggetti indesiderati dal sistema.

Lo script di servizio consente all'utente di esportare l'intero rapporto ESET SysInspector oppure le parti selezionate. Dopo l'esportazione, è possibile contrassegnare gli oggetti indesiderati per l'eliminazione. È quindi possibile eseguire il rapporto modificato per eliminare gli oggetti contrassegnati.

Lo script di servizio è adatto per utenti avanzati con esperienze pregresse nella diagnosi di problemi correlati al sistema. Modifiche apportate da personale non qualificato potrebbero danneggiare il sistema operativo.

Esempio

Se si sospetta che il computer sia infettato da un virus non rilevato dal programma antivirus, attenersi alle seguenti istruzioni dettagliate:

1. Eseguire ESET SysInspector per generare un nuovo snapshot del sistema.
2. Selezionare la prima voce nella sezione sulla sinistra (nella struttura ad albero), premere Shift e selezionare l'ultima voce per contrassegnarle tutte.
3. Fare clic con il pulsante destro del mouse sugli oggetti selezionati e scegliere **Esporta sezioni selezionate a script di servizio**.
4. Gli oggetti selezionati verranno esportati in un nuovo rapporto.
5. Segue il passaggio più cruciale dell'intera procedura: aprire il nuovo rapporto e modificare l'attributo - in + per tutti gli oggetti che si desidera rimuovere. Assicurarsi di non contrassegnare file/oggetti importanti del sistema operativo.
6. Aprire ESET SysInspector, fare clic su **File** > **Esegui script di servizio** e inserire il percorso allo script.
7. Fare clic su **OK** per eseguire lo script.

5.5.4.1 Generazione dello script di servizio

Per generare uno script, fare clic con il pulsante destro del mouse su una voce qualsiasi nella struttura ad albero del menu (nel riquadro sulla sinistra) nella finestra principale di ESET SysInspector. Selezionare l'opzione **Esporta tutte le sezioni a script di servizio** o **Esporta sezioni selezionate a script di servizio** nel menu contestuale.

NOTA: non è possibile esportare lo script di servizio durante il confronto di due rapporti.

5.5.4.2 Struttura dello script di servizio

Nella prima riga dell'intestazione dello script, è possibile trovare informazioni sulla versione del motore (ev), sulla versione dell'interfaccia grafica dell'utente o GUI (gv) e sulla versione del rapporto (lv). È possibile utilizzare questi dati per tenere traccia di possibili modifiche apportate al file .xml che genera lo script e impedisce il verificarsi di incongruenze durante l'esecuzione. Questa parte dello script non deve essere modificata.

Il resto del file è suddiviso in sezioni in cui è possibile modificare le voci (indicare quelle che verranno elaborate dallo script). È possibile contrassegnare le voci da elaborare sostituendo il carattere "-" davanti a una voce con il carattere "+". Le varie sezioni dello script sono separate da una riga vuota. Ciascuna sezione presenta un numero e un titolo.

01) Processi in esecuzione

Questa sezione contiene un elenco di tutti i processi in esecuzione sul sistema. Ciascun processo è identificato da un percorso UNC e, di conseguenza, dal relativo codice hash CRC16 accompagnato da asterischi (*).

Esempio:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In questo esempio, è stato selezionato il processo module32.exe (contrassegnato dal carattere "+") che terminerà in seguito all'esecuzione dello script.

02) Moduli caricati

Questa sezione contiene un elenco dei moduli di sistema attualmente utilizzati.

Esempio:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In questo esempio, il modulo khbekhb.dll è stato contrassegnato con un "+". Lo script in esecuzione riconoscerà e terminerà i processi utilizzando quel modulo specifico.

03) Connessioni TCP

Questa sezione contiene informazioni sulle connessioni TCP esistenti.

Esempio:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Lo script in esecuzione individuerà il proprietario del socket nelle connessioni TCP contrassegnate e interromperà il socket, liberando le risorse di sistema.

04) Endpoint UDP

Questa sezione contiene informazioni sugli endpoint UDP esistenti.

Esempio:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Lo script in esecuzione isolerà il proprietario del socket negli endpoint UDP contrassegnati e interromperà il socket.

05) Voci del server DNS

Questa sezione contiene informazioni relative alla configurazione del server DNS corrente.

Esempio:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Le voci del server DNS contrassegnate verranno rimosse al momento dell'esecuzione dello script.

06) Voci di registro importanti

Questa sezione contiene informazioni sulle voci di registro importanti.

Esempio:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Lo script in esecuzione eliminerà le voci contrassegnate, ridurrà i valori a 0 byte o ripristinerà i rispettivi valori predefiniti. L'azione da applicare a una voce specifica dipenderà dalla categoria di appartenenza della voce e dal valore della chiave nel registro specifico.

07) Servizi

Questa sezione contiene un elenco dei servizi registrati all'interno del sistema.

Esempio:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

All'esecuzione dello script, i servizi contrassegnati e i relativi servizi dipendenti verranno interrotti e disinstallati.

08) Driver

Questa sezione contiene un elenco dei driver installati.

Esempio:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:
\windows\system32\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Lo script in esecuzione interromperà i driver selezionati. Tenere presente che alcuni driver non potranno essere interrotti.

09) File critici

Questa sezione contiene informazioni sui file critici per il corretto funzionamento del sistema operativo.

Esempio:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Le voci selezionate verranno eliminate o reimpostate in base ai valori originali.

10) Attività pianificate

Questa sezione contiene informazioni sulle attività pianificate.

Esempio:

```
10) Scheduled tasks
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe /c
- c:\users\admin\appdata\local\google\update\googleupdate.exe /ua /installsource
- %windir%\system32\appidpolicyconverter.exe
- %windir%\system32\appidcertstorecheck.exe
- aitagent
[...]
```

5.5.4.3 Esecuzione degli script di servizio

Contrassegnare tutte le voci desiderate, quindi salvare e chiudere lo script. Eseguire lo script modificato direttamente dalla finestra principale di ESET SysInspector selezionando l'opzione **Esegui script di servizio** dal menu File. All'apertura di uno script, il programma consentirà all'utente di visualizzare il seguente messaggio: **Eseguire lo script di servizio "%Scriptname%"?** Dopo aver confermato, verrà visualizzato un altro messaggio per segnalare che lo script di servizio che si sta cercando di eseguire non è stato firmato. Fare clic su **Esegui** per avviare lo script.

Una finestra di dialogo confermerà l'effettiva esecuzione dello script.

In caso di elaborazione parziale dello script, comparirà una finestra di dialogo contenente il seguente messaggio: **Lo script di servizio è stato eseguito parzialmente. Si desidera visualizzare il rapporto dell'errore?** Selezionare **Sì** per visualizzare un rapporto dell'errore complesso in cui sono elencate le operazioni che non sono state eseguite.

In caso di mancato riconoscimento dello script, comparirà una finestra di dialogo contenente il seguente messaggio: **Il servizio selezionato non è firmato. L'esecuzione di script non firmati e sconosciuti potrebbe danneggiare gravemente i dati contenuti nel computer. Si è sicuri di voler eseguire lo script e di eseguire le azioni?** Tale situazione potrebbe essere causata da incongruenze all'interno dello script (intestazione danneggiata, titolo della sezione corrotto, assenza di una riga vuota tra le sezioni, ecc.). È possibile aprire nuovamente il file dello script e correggere gli errori oppure creare uno script di servizio.

5.5.5 Domande frequenti

Per l'esecuzione di ESET SysInspector sono necessari privilegi di amministratore?

Sebbene l'esecuzione di ESET SysInspector non richieda privilegi di amministratore, alcune delle informazioni raccolte dall'applicazione sono accessibili esclusivamente da un account Amministratore. L'esecuzione dell'applicazione come Utente standard o Utente con restrizioni causerà la raccolta di un numero inferiore di informazioni sull'ambiente operativo.

ESET SysInspector crea un file di rapporto?

ESET SysInspector crea un file di rapporto della configurazione del computer in uso. Per salvarne uno, fare clic su **File** > **Salva rapporto** nella finestra principale del programma. I rapporti vengono salvati in formato XML. Per impostazione predefinita, i file vengono salvati nella directory *%USERPROFILE%\Documenti*, con una convenzione di denominazione file "SysInpsector-%COMPUTERNAME%-AAMMGG-HHMM.XML". È possibile modificare la posizione e il nome del file di rapporto prima di salvarlo, in base alle preferenze.

Come faccio a visualizzare un file di rapporto ESET SysInspector?

Per visualizzare un file di rapporto creato da ESET SysInspector, eseguire il programma e fare clic su **File** > **Apri rapporto** nella finestra principale del programma. È anche possibile trascinare i file di rapporto nell'applicazione ESET SysInspector. Se è necessario visualizzare con una certa frequenza i file di rapporto ESET SysInspector, si consiglia di creare un collegamento al file SYSINSPECTOR.EXE sul Desktop e trascinare i file di rapporto per poterli visualizzare. Per motivi di sicurezza, Windows Vista/7 non consentono il trascinamento tra le finestre che presentano autorizzazioni di protezione diverse.

È disponibile una specifica per il formato del file di rapporto? Cos'è un SDK?

Attualmente, non sono disponibili specifiche né per il file di rapporto né per un SDK, in quanto il programma è ancora in fase di sviluppo. Dopo il rilascio del programma, queste informazioni verranno fornite in base ai commenti e alle richieste dei clienti.

In che modo ESET SysInspector valuta il rischio causato da un oggetto specifico?

Nella maggior parte dei casi, ESET SysInspector assegna livelli di rischio agli oggetti (file, processi, chiavi di registro e così via) utilizzando una serie di regole euristiche che esaminano le caratteristiche di ciascun oggetto e misurano il potenziale di attività dannose. Sulla base di questo approccio euristico, agli oggetti viene assegnato un livello di rischio che va da 1 - Sicuro (verde) a 9 - A rischio (rosso). Nel riquadro di navigazione sulla sinistra, le sezioni presentano colori diversi a seconda del livello di rischio degli oggetti contenuti.

Un livello di rischio "6 - Sconosciuto (rosso)" indica un oggetto pericoloso?

Le valutazioni di ESET SysInspector non bastano a stabilire che un oggetto sia dannoso o meno, ma è necessario l'intervento di un esperto di protezione. ESET SysInspector è stato pensato allo scopo di fornire agli esperti di protezione una rapida valutazione che consenta loro di individuare gli oggetti di un sistema che presentano un comportamento anomalo e che richiedono ulteriori analisi.

Perché, durante l'esecuzione, ESET SysInspector effettua la connessione a Internet?

Come accade per numerose applicazioni, ESET SysInspector è accompagnato da un "certificato" di firma digitale che garantisce che il software è stato pubblicato da ESET e non è stato modificato. Allo scopo di verificare il certificato, il sistema operativo contatta un'autorità di certificazione che controlla l'identità dell'autore della pubblicazione del software. Si tratta di una procedura normalmente adottata per tutti i programmi Microsoft Windows con firma digitale.

Cos'è la tecnologia Anti-Stealth?

La tecnologia Anti-Stealth offre un efficace rilevamento dei rootkit.

Se il sistema viene attaccato da codice dannoso che agisce come rootkit, l'utente potrebbe essere esposto a perdite o furti di dati. Il rilevamento di rootkit si rivela praticamente impossibile senza uno speciale strumento anti-rootkit.

Perché talvolta ci sono file contrassegnati come "Firmato da MS", ma con una voce diversa nel campo "Nome dell'azienda"?

Quando si tenta di identificare la firma digitale di un eseguibile, ESET SysInspector ricerca innanzitutto la firma digitale all'interno del file. Se la firma digitale viene trovata, il file verrà convalidato in base a queste informazioni. In caso contrario, il controllo ESI avvia la ricerca del file CAT corrispondente (Catalogo di protezione - *%systemroot%\system32\catroot*) contenente informazioni sul file eseguibile elaborato. Se il file CAT rilevante viene trovato, la relativa firma digitale verrà applicata al processo di convalida dell'eseguibile.

Questo è il motivo per cui talvolta ci sono file contrassegnati come "Firmati da MS" ma con una voce diversa nel campo "Nome dell'azienda".

Esempio:

Windows 2000 comprende l'applicazione HyperTerminal posizionata in *C:\Programmi\Windows NT*. Sebbene il file eseguibile principale dell'applicazione non presenti una firma digitale, ESET SysInspector lo contrassegna come file firmato da Microsoft. Il motivo alla base di tale meccanismo è la presenza di un riferimento in *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* che punta a *C:\Programmi\Windows NT\hypertrm.exe* (eseguibile principale dell'applicazione HyperTerminal) e di una firma digitale di Microsoft in *sp4.cat*.

5.5.6 ESET SysInspector come parte di ESET NOD32 Antivirus

Per aprire la sezione di ESET SysInspector in ESET NOD32 Antivirus, fare clic su **Strumenti** > **ESET SysInspector**. Il sistema di gestione nella finestra ESET SysInspector è simile a quello dei rapporti di controllo del computer o attività pianificate. Tutte le operazioni con gli snapshot di sistema (creazione, visualizzazione, confronto, rimozione ed esportazione) sono accessibili con uno o due clic.

La finestra ESET SysInspector contiene informazioni di base sugli snapshot creati, tra cui l'ora di creazione, un breve commento, il nome dell'utente che ha creato lo snapshot e lo stato dello snapshot.

Per confrontare, creare o eliminare gli snapshot, utilizzare i pulsanti corrispondenti collocati sotto l'elenco di snapshot nella finestra ESET SysInspector. Queste opzioni sono disponibili anche nel menu contestuale. Per visualizzare lo snapshot di sistema selezionato, scegliere **Mostra** dal menu contestuale. Per esportare lo snapshot selezionato in un file, fare clic con il pulsante destro del mouse su di esso e selezionare **Esporta...**.

Segue una descrizione dettagliata delle opzioni disponibili:

- **Confronta** - Consente di confrontare due rapporti esistenti. È utile se si desidera tenere traccia delle modifiche tra il rapporto corrente e un rapporto più vecchio. Per attivare questa opzione, è necessario selezionare due snapshot da confrontare.
- **Crea...** - Crea un nuovo record. Prima di eseguire questa operazione, è necessario inserire un breve commento sul record. Per visualizzare l'avanzamento della creazione dello snapshot (generato correntemente), consultare la colonna **Stato**. Tutti gli snapshot completati sono contrassegnati dallo stato **Creato**.
- **Elimina/Elimina tutto** - Rimuove le voci dall'elenco.
- **Esporta...** - Salva la voce selezionata in un file XML (anche in formato compresso).

5.6 Riga di comando

Il modulo antivirus di ESET NOD32 Antivirus può essere avviato dalla riga di comando, manualmente con il comando “ecls” oppure con un file batch (“bat”). Utilizzo dello scanner della riga di comando ESET:

```
ecls [OPTIONS..] FILES..
```

È possibile utilizzare i parametri e le opzioni riportati di seguito quando viene eseguita una scansione su richiesta dalla riga di comando:

Opzioni

/base-dir=FOLDER	carica moduli da CARTELLA
/quar-dir=FOLDER	CARTELLA di quarantena

/exclude=MASK	escludi dalla scansione i file corrispondenti a MASCHERA
/subdir	esegui controllo delle sottocartelle (impostazione predefinita)
/no-subdir	non eseguire controllo delle sottocartelle
/max-subdir-level=LEVEL	sottolivello massimo delle cartelle all'interno di cartelle su cui eseguire la scansione
/symlink	segui i collegamenti simbolici (impostazione predefinita)
/no-symlink	ignora collegamenti simbolici
/ads	esegui la scansione di ADS (impostazione predefinita)
/no-ads	non eseguire la scansione di ADS
/log-file=FILE	registra output nel FILE
/log-rewrite	sovrascrivi il file di output (impostazione predefinita: aggiungi)
/log-console	registra l'output nella console (impostazione predefinita)
/no-log-console	non registrare l'output nella console
/log-all	registra anche file puliti
/no-log-all	non registrare file puliti (impostazione predefinita)
/aind	mostra indicatore di attività
/auto	controlla e disinfetta automaticamente tutti i dischi locali

Opzioni scanner

/files	esegui controllo dei file (impostazione predefinita)
/no-files	non eseguire controllo dei file
/memory	esegui scansione della memoria
/boots	esegui la scansione dei settori di avvio
/no-boots	non eseguire la scansione dei settori di avvio (impostazione predefinita)
/arch	esegui controllo degli archivi (impostazione predefinita)
/no-arch	non eseguire controllo degli archivi
/max-obj-size=SIZE	esegui solo la scansione dei file inferiori a DIMENSIONE megabyte (impostazione predefinita 0 = illimitato)
/max-arch-level=LEVEL	sottolivello massimo degli archivi all'interno di archivi (archivi nidificati) su cui eseguire la scansione
/scan-timeout=LIMIT	esegui scansione degli archivi per LIMITE secondi al massimo
/max-arch-size=SIZE	esegui la scansione dei file di un archivio solo se inferiori a DIMENSIONE (impostazione predefinita 0 = illimitato)
/max-sfx-size=SIZE	esegui la scansione dei file di un archivio autoestraente solo se inferiori a DIMENSIONE megabyte (impostazione predefinita 0 = illimitato)
/mail	esegui la scansione dei file di e-mail (impostazione predefinita)
/no-mail	non eseguire controllo dei file di e-mail
/mailbox	esegui la scansione delle caselle di posta (impostazione predefinita)
/no-mailbox	non eseguire la scansione delle caselle di posta
/sfx	esegui la scansione degli archivi autoestraenti (impostazione predefinita)
/no-sfx	non eseguire controllo degli archivi autoestraenti
/rtp	esegui la scansione degli eseguibili compressi (impostazione predefinita)
/no-rtp	non eseguire la scansione degli eseguibili compressi
/unsafe	esegui la scansione delle applicazioni potenzialmente pericolose
/no-unsafe	non eseguire la scansione delle applicazioni potenzialmente pericolose (impostazione predefinita)
/unwanted	esegui la scansione delle applicazioni potenzialmente indesiderate
/no-unwanted	non eseguire la scansione delle applicazioni potenzialmente indesiderate (impostazione predefinita)
/suspicious	ricerca applicazioni sospette (impostazione predefinita)
/no-suspicious	non ricercare applicazioni sospette
/pattern	utilizza le firme digitali (impostazione predefinita)
/no-pattern	non utilizzare le firme digitali
/heur	attiva l'euristica (impostazione predefinita)
/no-heur	disattiva l'euristica
/adv-heur	attiva l'euristica avanzata (impostazione predefinita)
/no-adv-heur	disattiva l'euristica avanzata

/ext=EXTENSIONS	esegui scansione solo di ESTENSIONI delimitate da due punti
/ext-exclude=EXTENSIONS	escludi dal controllo le ESTENSIONI delimitate da due punti
/clean-mode=MODE	utilizza la MODALITÀ pulizia per gli oggetti infetti

Sono disponibili le seguenti opzioni:

- **nessuna**: non verrà eseguita alcuna pulizia automatica.
- **standard** (impostazione predefinita): ecls.exe tenterà di eseguire la pulizia o l'eliminazione automatica di file infetti.
- **massima**: ecls.exe tenterà di eseguire la pulizia o l'eliminazione automatica di file infetti senza l'intervento dell'utente (all'utente non verrà richiesto di confermare l'eliminazione dei file).
- **rigorosa**: ecls.exe eliminerà i file senza tentare di effettuarne la pulizia e indipendentemente dalla loro tipologia.
- **eliminazione**: ecls.exe eliminerà i file senza tentare di effettuarne la pulizia, ma eviterà di eliminare file sensibili come quelli del sistema Windows.

/quarantena	copiare i file infettati (se puliti) in Quarantena (integra l'azione eseguita durante la pulizia)
/no-quarantena	non copiare file infettati in Quarantena

Opzioni generali

/help	mostra guida ed esci
/version	mostra informazioni sulla versione ed esci
/preserve-time	mantieni indicatore data e ora dell'ultimo accesso

Codici di uscita

0	nessuna minaccia rilevata
1	minaccia rilevata e pulita
10	impossibile controllare alcuni file (potrebbero essere minacce)
50	trovata minaccia
100	errore

NOTA
i codici di uscita superiori a 100 indicano che non è stata eseguita la scansione del file, il quale potrebbe quindi essere infetto.

6. Glossario

6.1 Tipi di infiltrazioni

Un'infiltrazione è una parte di software dannoso che tenta di entrare e/o danneggiare il computer di un utente.

6.1.1 Virus

Un virus è un pezzo di codice dannoso che è pre-incorporato o viene aggiunto ai file esistenti nel computer. I virus prendono il nome dai virus biologici, poiché utilizzano tecniche simili per diffondersi da un computer all'altro. Il termine “virus” viene spesso utilizzato in maniera errata per indicare qualsiasi tipo di minaccia. Attualmente, l'utilizzo di questo termine è stato superato e sostituito dalla nuova e più accurata definizione di “malware” (software dannoso).

I virus attaccano principalmente i file eseguibili e i documenti. In breve, un virus funziona nel seguente modo: dopo aver eseguito un file infetto, il codice dannoso viene chiamato ed eseguito prima dell'esecuzione dell'applicazione originale. Un virus può infettare qualsiasi file sul quale l'utente corrente dispone dei diritti di scrittura.

I virus possono essere classificati in base agli scopi e ai diversi livelli di gravità. Alcuni di essi sono estremamente dannosi poiché sono in grado di eliminare deliberatamente i file da un disco rigido. Altri, invece, non causano veri e propri danni, poiché il loro scopo consiste esclusivamente nell'infastidire l'utente e dimostrare le competenze tecniche dei rispettivi autori.

Se il computer è stato infettato da un virus e non è possibile rimuoverlo, inviarlo ai laboratori di ricerca ESET ai fini di un esame accurato. In alcuni casi, i file infetti possono essere modificati a un livello tale da impedirne la pulizia. In questo caso, è necessario sostituire i file con una copia non infetta.

6.1.2 Worm

Un worm è un programma contenente codice dannoso che attacca i computer host e si diffonde tramite la rete. La differenza fondamentale tra un virus e un worm è che i worm hanno la capacità di propagarsi autonomamente, in quanto non dipendono da file host (o settori di avvio). I worm si diffondono attraverso indirizzi e-mail all'interno della lista dei contatti degli utenti oppure sfruttano le vulnerabilità delle applicazioni di rete.

I worm sono pertanto molto più attivi rispetto ai virus. Grazie all'ampia disponibilità di connessioni Internet, possono espandersi in tutto il mondo entro poche ore o persino pochi minuti dal rilascio. Questa capacità di replicarsi in modo indipendente e rapido li rende molto più pericolosi rispetto ad altri tipi di malware.

Un worm attivato in un sistema può provocare diversi inconvenienti: può eliminare file, ridurre le prestazioni del sistema e perfino disattivare programmi. La sua natura lo qualifica come "mezzo di trasporto" per altri tipi di infiltrazioni.

Se il computer è infettato da un worm, si consiglia di eliminare i file infetti poiché è probabile che contengano codice dannoso.

6.1.3 Trojan horse

Storicamente, i trojan horse sono stati definiti come una classe di minacce che tentano di presentarsi come programmi utili per ingannare gli utenti e indurli così a eseguirli.

Poiché si tratta di una categoria molto ampia, è spesso suddivisa in diverse sottocategorie:

- **Downloader**: programmi dannosi in grado di scaricare altre minacce da Internet.
- **Dropper**: programmi dannosi in grado di installare sui computer compromessi altri tipi di malware.
- **Backdoor**: programmi dannosi che comunicano con gli autori degli attacchi remoti, consentendo loro di ottenere l'accesso al computer e assumerne il controllo.
- **Keylogger** – (registratore delle battute dei tasti): programma che registra ogni battuta di tasto effettuata da un utente e che invia le informazioni agli autori degli attacchi remoti.
- **Dialer** : programmi dannosi progettati per connettersi a numeri con tariffe telefoniche molto elevate anziché ai provider dei servizi Internet dell'utente. È quasi impossibile che un utente noti che è stata creata una nuova connessione. I dialer possono causare danni solo agli utenti con connessione remota che ormai viene utilizzata sempre meno frequentemente.

Se sul computer in uso viene rilevato un trojan horse, si consiglia di eliminarlo, poiché probabilmente contiene codice dannoso.

6.1.4 Rootkit

I rootkit sono programmi dannosi che forniscono agli autori degli attacchi su Internet l'accesso illimitato a un sistema, nascondendo tuttavia la loro presenza. I rootkit, dopo aver effettuato l'accesso a un sistema (di norma, sfruttando una vulnerabilità del sistema), utilizzano le funzioni del sistema operativo per non essere rilevate dal software antivirus: nascondono i processi, i file e i dati del Registro di sistema di Windows. Per tale motivo, è quasi impossibile rilevarli utilizzando le tradizionali tecniche di testing.

Per bloccare i rootkit, sono disponibili due livelli di rilevamento:

1. Quando tentano di accedere ad un sistema: Non sono ancora presenti e pertanto sono inattivi. La maggior parte dei sistemi antivirus è in grado di eliminare i rootkit a questo livello (presupponendo che riescano effettivamente a rilevare tali file come infetti).
2. Quando sono nascosti dal normale testing: ESET NOD32 Antivirus gli utenti hanno il vantaggio di poter utilizzare la tecnologia Anti-Stealth che è in grado di rilevare ed eliminare anche i rootkit attivi.

6.1.5 Adware

Adware è l'abbreviazione di software con supporto della pubblicità (advertising-supported software). Rientrano in questa categoria i programmi che visualizzano materiale pubblicitario. Le applicazioni adware spesso aprono automaticamente una nuova finestra popup contenente pubblicità all'interno di un browser Internet oppure ne modificano la pagina iniziale. I programmi adware vengono spesso caricati insieme a programmi freeware, che consentono ai loro sviluppatori di coprire i costi di sviluppo delle applicazioni che, in genere, sono molto utili.

L'adware non è di per sé pericoloso, anche se gli utenti possono essere infastiditi dai messaggi pubblicitari. Il pericolo sta nel fatto che l'adware può svolgere anche funzioni di rilevamento e registrazione, al pari dei programmi spyware.

Se si decide di utilizzare un prodotto freeware, è opportuno prestare particolare attenzione al programma di installazione. Nei programmi di installazione viene in genere visualizzata una notifica dell'installazione di un programma adware aggiuntivo. Spesso è possibile annullarla e installare il programma senza adware.

Alcuni programmi non vengono installati senza adware. In caso contrario, le rispettive funzionalità saranno limitate. Ciò significa che l'adware potrebbe accedere di frequente al sistema in modo "legale", poiché l'utente ne ha dato il consenso. In questi casi, vale il proverbio secondo il quale la prudenza non è mai troppa. Se in un computer viene rilevato un file adware, l'operazione più appropriata è l'eliminazione dello stesso, in quanto esistono elevate probabilità che il file contenga codice dannoso.

6.1.6 Spyware

Questa categoria include tutte le applicazioni che inviano informazioni riservate senza il consenso/consapevolezza dell'utente. Gli spyware si avvalgono di funzioni di monitoraggio per inviare dati statistici di vario tipo, tra cui un elenco dei siti Web visitati, indirizzi e-mail della rubrica dell'utente o un elenco dei tasti digitati.

Gli autori di spyware affermano che lo scopo di tali tecniche è raccogliere informazioni aggiuntive sulle esigenze e sugli interessi degli utenti per l'invio di pubblicità più mirate. Il problema è legato al fatto che non esiste una distinzione chiara tra applicazioni utili e dannose e che nessuno può essere sicuro del fatto che le informazioni raccolte verranno utilizzate correttamente. I dati ottenuti dalle applicazioni spyware possono contenere codici di sicurezza, PIN, numeri di conti bancari e così via. I programmi spyware sono frequentemente accoppiati a versioni gratuite di un programma creato dal relativo autore per generare profitti o per offrire un incentivo all'acquisto del software. Spesso, gli utenti sono informati della presenza di un'applicazione spyware durante l'installazione di un programma che li esorta a eseguire l'aggiornamento a una versione a pagamento che non lo contiene.

Esempi di prodotti freeware noti associati a programmi spyware sono le applicazioni client delle reti P2P (peer-to-peer). Spyfalcon o Spy Sheriff (e molti altri ancora) appartengono a una sottocategoria di spyware specifica, poiché si fanno passare per programmi antispyware ma in realtà sono essi stessi applicazioni spyware.

Se in un computer viene rilevato un file spyware, è consigliabile eliminarlo in quanto è molto probabile che contenga codice dannoso.

6.1.7 Programmi di compressione

Un programma di compressione è un eseguibile compresso autoestraente che riunisce vari tipi di malware in un unico pacchetto.

I programmi di compressione più comuni sono UPX, PE_Compact, PKLite e ASPack. Lo stesso malware può essere rilevato in modo diverso se compresso mediante l'utilizzo di un programma di compressione diverso. I programmi di compressione sono anche in grado di mutare le proprie "firme" nel tempo, rendendo più complessi il rilevamento e la rimozione dei malware.

6.1.8 Applicazioni potenzialmente pericolose

Esistono molti programmi legali utili per semplificare l'amministrazione dei computer in rete. Tuttavia, nelle mani sbagliate, possono essere utilizzati per scopi illegittimi. ESET NOD32 Antivirus offre la possibilità di rilevare tali minacce.

Applicazioni potenzialmente pericolose è la classificazione utilizzata per il software legale e commerciale. Questa classificazione include programmi quali strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano tutte le battute dei tasti premuti da un utente).

Se si rileva la presenza di un'applicazione potenzialmente pericolosa in esecuzione sul computer (che non è stata installata dall'utente) rivolgersi all'amministratore di rete o rimuovere l'applicazione.

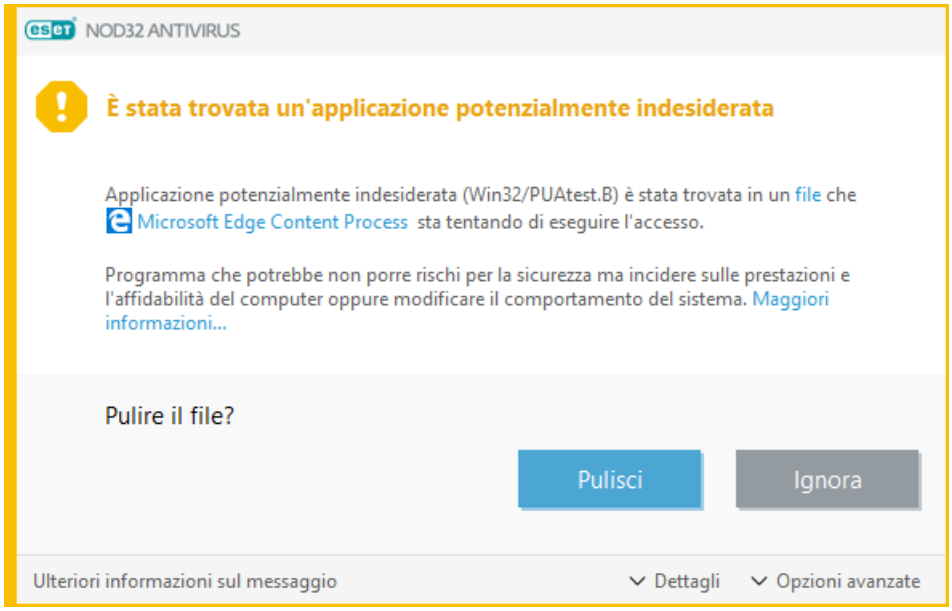
6.1.9 Applicazioni potenzialmente indesiderate

Un'applicazione potenzialmente indesiderata è un programma che contiene adware, installa barre degli strumenti o si prefigge altri obiettivi poco chiari. In alcuni casi, un utente potrebbe percepire che i vantaggi di un'applicazione potenzialmente indesiderata superano i rischi. Per questo motivo, ESET assegna a tali applicazioni una categoria a rischio ridotto rispetto ad altri tipi di software dannosi, come trojan horse o worm.

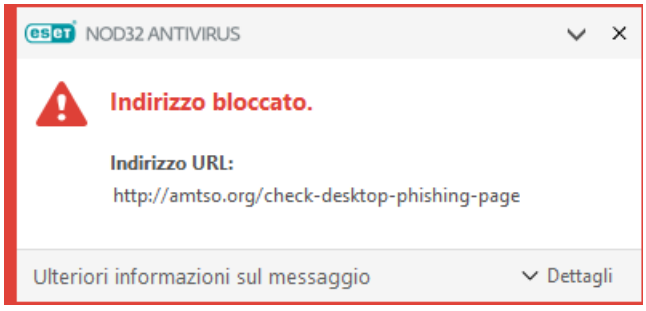
Avviso: trovata minaccia potenziale

In caso di rilevamento di un'applicazione potenzialmente indesiderata, l'utente può scegliere l'azione da intraprendere:

1. **Pulisci/Disconnetti**: questa opzione termina l'azione e impedisce alla minaccia potenziale di entrare nel sistema in uso.
2. **Ignora**: questa opzione consente a una minaccia potenziale di entrare nel sistema in uso.
3. Per consentire l'esecuzione futura dell'applicazione sul computer in uso senza interruzioni, fare clic su **Opzioni avanzate** e selezionare la casella di controllo accanto a **Escludi dal rilevamento**.

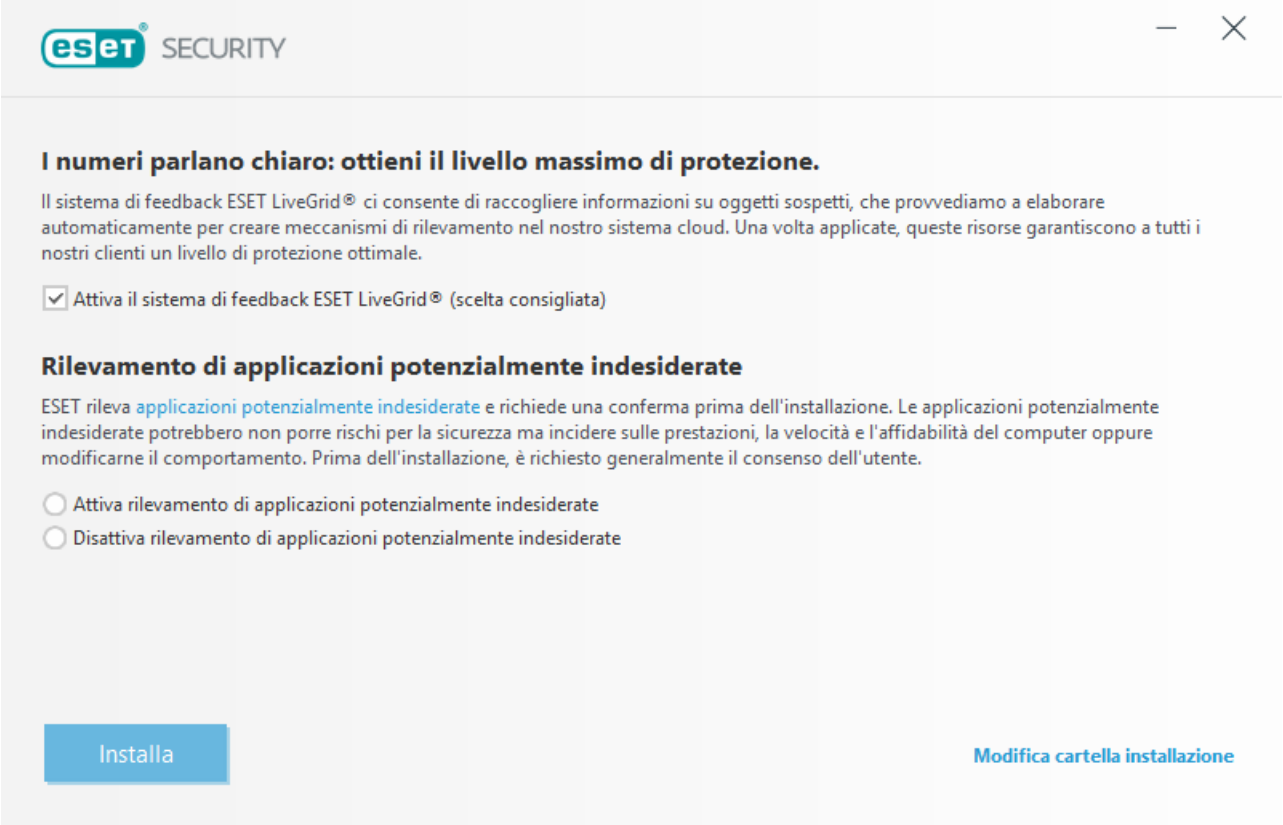


Quando viene rilevata un'applicazione potenzialmente indesiderata che non può essere cancellata, viene visualizzata una notifica **L'indirizzo è stato bloccato**. Per ulteriori informazioni su questo evento, accedere a **Strumenti** > **File di rapporto** > **Siti Web filtrati** dal menu principale.



Applicazioni potenzialmente indesiderate: impostazioni

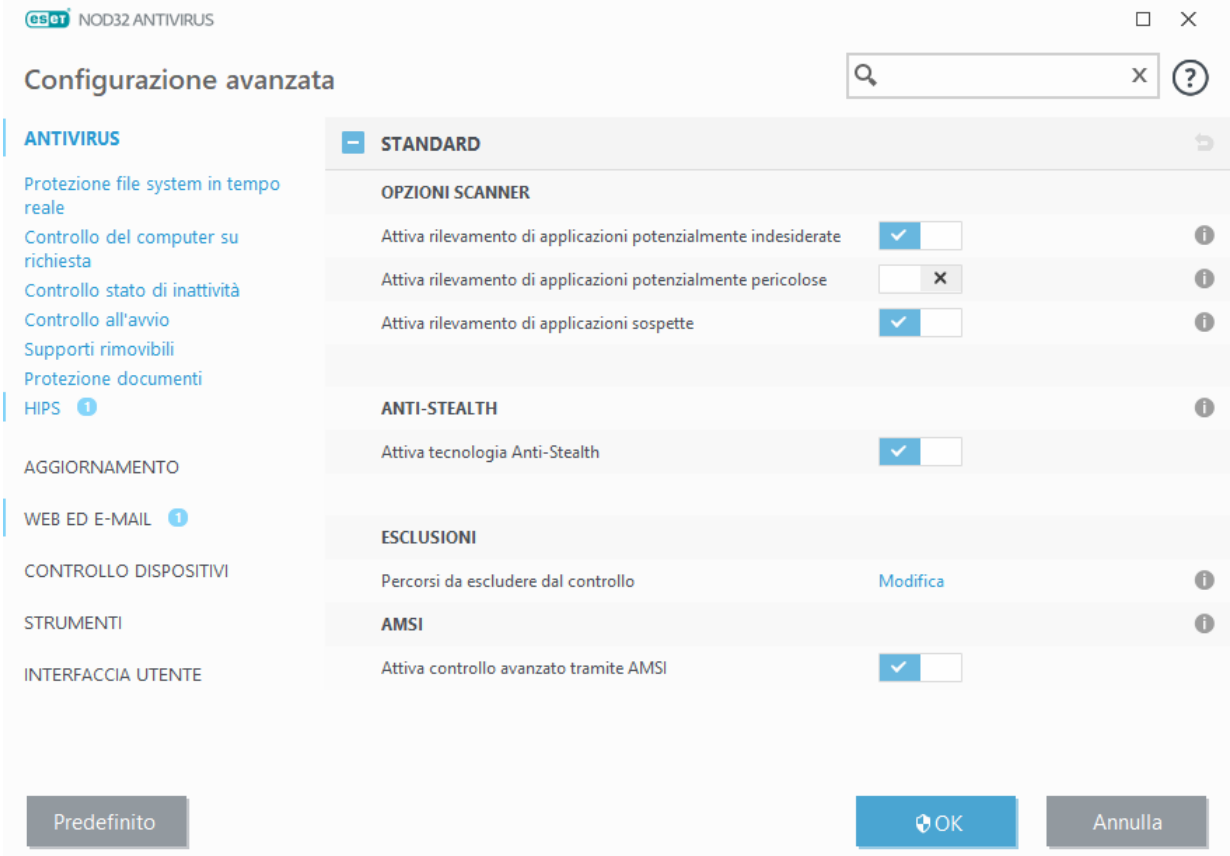
Durante l'installazione di un prodotto ESET, l'utente può decidere di attivare il rilevamento di applicazioni potenzialmente indesiderate, come illustrato di seguito:



AVVERTENZA
Le applicazioni potenzialmente indesiderate possono installare adware e barre degli strumenti o contenere altre funzioni di programma non sicure e indesiderate.

Queste impostazioni possono essere modificate in qualsiasi momento. Per attivare o disattivare il rilevamento di applicazioni potenzialmente indesiderate, pericolose o sospette, attenersi alle seguenti istruzioni:

1. Aprire il prodotto ESET. Come faccio ad aprire il mio prodotto ESET?
2. Premere il tasto **F5** per accedere alla **Configurazione avanzata**.
3. Fare clic su **Antivirus** e attivare o disattivare le opzioni **Attiva rilevamento di applicazioni potenzialmente indesiderate**, **Attiva rilevamento di applicazioni potenzialmente pericolose** e **Attiva rilevamento di applicazioni sospette** in base alle proprie preferenze. Confermare facendo clic su **OK**.



Applicazioni potenzialmente indesiderate: wrapper di software

Il wrapper di un software è un tipo speciale di modifica di un'applicazione utilizzato da alcuni siti Web che offrono servizi di file hosting. Si tratta di uno strumento di terze parti che installa il programma che si intende scaricare aggiungendo, però, altri software, come ad esempio barre degli strumenti o adware. I software aggiuntivi possono inoltre apportare modifiche alla pagina iniziale del browser Web in uso e alle impostazioni di ricerca. Inoltre, i siti Web che offrono servizi di file hosting non comunicano al fornitore del software o al destinatario del download le modifiche apportate e non consentono di rifiutarle facilmente. Per tali motivi, ESET classifica i wrapper di software tra le applicazioni potenzialmente indesiderate per consentire agli utenti di decidere se accettare o meno il download.

Per una versione aggiornata di questa pagina della Guida, consultare questo articolo della Knowledge Base ESET.

6.2 Tecnologia ESET

6.2.1 Exploit Blocker

L'Exploit Blocker è progettato per rafforzare i tipi di applicazione comunemente utilizzati come browser Web, lettori PDF, client di posta e componenti di MS Office. Il sistema si basa sul monitoraggio del comportamento dei processi ai fini del rilevamento di attività sospette che potrebbero indicare un exploit.

Nel momento in cui l'Exploit Blocker identifica un processo sospetto, lo interrompe immediatamente e registra i dati relativi alla minaccia, che vengono quindi inviati al sistema cloud di ThreatSense. Le informazioni vengono elaborate dal laboratorio di ricerca ESET e utilizzate ai fini di una maggiore protezione degli utenti contro minacce sconosciute e attacchi zero-day (malware di nuova concezione per i quali non sono disponibili soluzioni preconfigurate).

6.2.2 Scanner memoria avanzato

Lo Scanner memoria avanzato lavora congiuntamente all'Exploit Blocker per rafforzare il livello di protezione contro malware concepiti allo scopo di eludere il rilevamento dei prodotti antimalware mediante l'utilizzo di pratiche di offuscazione e/o crittografia. Qualora i metodi di emulazione o di euristica ordinari non siano in grado di rilevare una minaccia, lo Scanner memoria avanzato identifica il comportamento sospetto ed effettua un controllo delle minacce presenti nella memoria del sistema. Questa soluzione si rivela efficace persino contro i malware che utilizzano pratiche di offuscamento ottimizzate.

Diversamente dall'Exploit Blocker, lo Scanner memoria avanzato rappresenta un metodo post-esecuzione. Ciò implica un rischio di esecuzione di attività dannose prima del rilevamento di una minaccia. Tuttavia, qualora le varie tecniche di rilevamento disponibili non si rivelino efficaci, questo sistema offre un livello aggiuntivo di sicurezza.

6.2.3 ESET LiveGrid®

Sviluppato sul sistema avanzato di allarme immediato ThreatSense.Net®, ESET LiveGrid® utilizza i dati inviati dagli utenti ESET di tutto il mondo e li invia al laboratorio di ricerca ESET. Grazie all'invio di campioni e metadati "from the wild" sospetti, ESET LiveGrid® consente a ESET di soddisfare le esigenze dei clienti e di gestire le minacce più recenti in modo tempestivo. I ricercatori dei malware ESET utilizzano le informazioni per creare un'istantanea accurata della natura e dell'ambito delle minacce globali, che consente a ESET di puntare il mirino sugli obiettivi appropriati. I dati ESET LiveGrid® giocano un ruolo importante nella definizione delle priorità nell'ambito dei sistemi di elaborazione automatici.

Questo strumento consente inoltre di implementare un sistema di reputazione che contribuisce al potenziamento dell'efficienza complessiva delle soluzioni anti-malware ESET. Durante l'analisi di un file eseguibile o di un archivio sul sistema di un utente, il relativo hashtag viene dapprima confrontato rispetto a un database di oggetti della whitelist e della blacklist. Se presente nella whitelist, il file analizzato viene considerato pulito e contrassegnato ai fini dell'esclusione da controlli futuri. Se presente nella blacklist, verranno intraprese azioni appropriate in base alla natura della minaccia. In caso di mancata corrispondenza, il file viene sottoposto a un controllo completo. Sulla base dei risultati del controllo, i file vengono categorizzati come minacce o non minacce. Questo approccio registra un impatto positivo importante sulle prestazioni del controllo.

Il sistema di reputazione consente di effettuare un rilevamento efficace di campioni di malware anche prima dell'invio delle relative firme al computer dell'utente, mediante il database antivirus aggiornato (tale azione si ripete più di una volta al giorno).

6.2.4 Java Exploit Blocker

Java Exploit Blocker è un'estensione della protezione Exploit Blocker esistente. Monitora Java e ricerca comportamento simile a exploit. I campioni bloccati possono essere segnalati agli analisti di malware i quali possono creare firme per bloccarli su differenti livelli (blocco URL, download di file e così via).

6.2.5 Protezione contro gli attacchi basati su script

La protezione contro attacchi basati su script comprende una protezione contro il codice javascript nei browser web e una protezione Antimalware Scan Interface (AMSI) contro gli script in Powershell.

AVVERTENZA
HIPS deve essere attivato perché questa funzionalità operi correttamente.

La protezione contro gli attacchi basati su script supporta i seguenti browser web:

- Mozilla Firefox
- Google Chrome
- Internet Explorer
- Microsoft Edge

NOTA

Le versioni minime supportate dei browser possono variare, in quanto le firme file dei browser variano spesso. L'ultima versione del browser è sempre supportata.

6.2.6 Protezione anti-ransomware

Ransomware è un tipo di malware che blocca gli utenti impedendo l'accesso al sistema tramite un blocco dello schermo o crittografando dei file. La protezione anti-ransomware monitora il comportamento delle applicazioni e dei processi che cercano di modificare i dati personali. Se il comportamento di un'applicazione è considerato malevolo, oppure se la scansione della reputazione segnala un'applicazione come sospetta, l'applicazione viene bloccata, oppure viene chiesto all'utente se bloccarla o consentirla.

IMPORTANTE
ESET Live Grid deve essere attivo affinché la protezione anti-ransomware funzioni correttamente.

6.3 E-mail

L'e-mail o electronic mail è una moderna forma di comunicazione che presenta numerosi vantaggi. È flessibile, veloce e diretta e ha svolto un ruolo cruciale nella proliferazione di Internet all'inizio degli anni novanta.

Purtroppo, a causa dell'elevato livello di anonimità, i messaggi e-mail e Internet lasciano ampio spazio ad attività illegali come lo spam. Lo spam include annunci pubblicitari non desiderati, hoax e proliferazione di software dannoso o malware. Ad aumentare ulteriormente i disagi e i pericoli è il fatto che i costi di invio dello spamming sono minimi e gli autori dispongono di numerosi strumenti per acquisire nuovi indirizzi e-mail. Il volume e la varietà dello spamming ne rende inoltre estremamente difficoltoso il monitoraggio. Maggiore è il periodo di utilizzo dell'indirizzo e-mail, più elevata sarà la possibilità che finisca in un database per motori di spamming. Di seguito sono riportati alcuni suggerimenti per la prevenzione di messaggi e-mail indesiderati:

- Se possibile, evitare di pubblicare il proprio indirizzo e-mail su Internet
- Fornire il proprio indirizzo e-mail solo a utenti considerati attendibili
- Se possibile, non utilizzare alias comuni. Maggiore è la complessità degli alias, minore sarà la probabilità che vengano rilevati
- Non rispondere a messaggi di spam già recapitati nella posta in arrivo
- Quando si compilano moduli su Internet, prestare particolare attenzione a selezionare opzioni quali "Sì, desidero ricevere informazioni".
- Utilizzare indirizzi e-mail "specifici", ad esempio uno per l'ufficio, uno per comunicare con gli amici e così via.
- Cambiare di tanto in tanto l'indirizzo e-mail
- Utilizzare una soluzione antispam

6.3.1 Pubblicità

La pubblicità su Internet è una delle forme di pubblicità in maggior crescita. I vantaggi principali dal punto di vista del marketing sono i costi ridotti e un livello elevato di immediatezza. I messaggi vengono inoltre recapitati quasi immediatamente. Molte società utilizzano strumenti di marketing via e-mail per comunicare in modo efficace con i clienti attuali e potenziali.

Questo tipo di pubblicità è legittimo, perché si potrebbe essere interessati a ricevere informazioni commerciali su determinati prodotti. Molte società inviano tuttavia messaggi di contenuto commerciale non desiderati. In questi casi, la pubblicità tramite e-mail supera il limite e diventa spam.

La quantità di messaggi e-mail non desiderati diventa così un problema e non sembra diminuire. Gli autori di messaggi e-mail non desiderati tentano spesso di mascherare i messaggi spam come messaggi legittimi.

6.3.2 Hoax: truffe e bufale

Un hoax è un messaggio contenente informazioni non veritiere diffuso su Internet. che viene in genere inviato via e-mail e tramite strumenti di comunicazione come ICQ e Skype. Il messaggio stesso è in genere una burla o una leggenda metropolitana.

Gli hoax virus tentano di generare paura, incertezza e dubbio ("Fear, Uncertainty and Doubt", FUD) nei destinatari, inducendoli a credere che nei relativi sistemi è presente un "virus non rilevabile" in grado di eliminare file e recuperare password o di eseguire altre attività dannose.

Alcuni hoax richiedono ai destinatari di inoltrare messaggi ai loro contatti, aumentandone così la diffusione. Esistono hoax via cellulare, richieste di aiuto, offerte di denaro dall'estero e così via. Spesso è impossibile determinare l'intento dell'autore del messaggio.

È molto prababile che i messaggi che invitano ad essere inoltrati a tutti i propri conoscenti siano hoax. Su Internet sono presenti molti siti Web in grado di verificare l'autenticità di un messaggio e-mail. Prima di inoltrarlo, effettuare una ricerca in Internet per qualsiasi messaggio si sospetti essere hoax.

6.3.3 Phishing

Il termine phishing definisce un'attività illegale che si avvale di tecniche di ingegneria sociale (ovvero di manipolazione degli utenti al fine di ottenere informazioni confidenziali). Lo scopo è quello di ottenere l'accesso a dati sensibili quali numeri di conti bancari, codici PIN e così via.

Di norma, l'accesso viene ricavato tramite l'invio di messaggi e-mail che imitano quelli di una persona o società affidabile (istituto finanziario, compagnia di assicurazioni). Il messaggio e-mail sembra autentico e presenta immagini e contenuti che possono indurre a credere che provenga effettivamente da un mittente affidabile. Tali messaggi chiedono all'utente, con vari pretesti (verifica dati, operazioni finanziarie), di immettere alcuni dati personali: numeri di conti bancari o nomi utente e password. Tali dati, se inviati, possono essere rubati e utilizzati in modo illegale.

Le banche, le compagnie di assicurazioni e altre società legittime non chiederanno mai di rivelare nomi utente e password in messaggi e-mail non desiderati.

7. Domande comuni

In questo capitolo sono illustrate alcune delle domande frequenti e i problemi riscontrati. Fare clic sul titolo dell'argomento per trovare la soluzione al problema:

Come aggiornare ESET NOD32 Antivirus
Come rimuovere un virus dal PC
Come creare una nuova attività nella Pianificazione attività
Come pianificare un'attività di scansione (ogni 24 ore)

Se non è stato possibile trovare la soluzione del problema nelle pagine della Guida di cui sopra, consultare le pagine della guida di ESET NOD32 Antivirus.

Se non è stato possibile trovare la soluzione a un problema o la risposta a una domanda nelle pagine della Guida, consultare la Knowledge Base ESET on-line, sottoposta a periodici aggiornamenti. Seguono i collegamenti ai principali articoli della Knowledge base per la risoluzione di problemi comuni:

Durante l'installazione del prodotto ESET visualizzo un messaggio di errore. Cosa significa?
Attiva il mio prodotto ESET Windows Home utilizzando nome utente, password o chiave di licenza
Disinstalla o reinstalla il mio prodotto ESET Home
Ho ricevuto un messaggio relativo al termine anticipato della mia installazione ESET
Cosa devo fare dopo aver rinnovato la licenza? (utenti Home)
Cosa succede se modifico il mio indirizzo di posta elettronica?
Come faccio ad avviare Windows in Modalità provvisoria o in Modalità provvisoria senza rete?

Se necessario, contattare il Supporto tecnico per eventuali domande o problemi riscontrati. Il modulo di contatto è disponibile nella scheda **Guida e supporto tecnico** di ESET NOD32 Antivirus.

7.1 Come aggiornare ESET NOD32 Antivirus

L'aggiornamento di ESET NOD32 Antivirus può essere eseguito manualmente o automaticamente. Per avviare l'aggiornamento, fare clic su **Aggiorna adesso** nella sezione **Aggiorna**.

Le impostazioni predefiniti dell'installazione consentono di creare un'attività di aggiornamento automatica che viene eseguita ogni ora. Se occorre modificare l'intervallo, accedere a **Strumenti** > **Pianificazione attività** (per ulteriori informazioni sulla Pianificazione attività, fare clic qui).

7.2 Come rimuovere un virus dal PC

Se il computer mostra sintomi di infezione malware, ad esempio appare più lento o si blocca spesso, è consigliabile attenersi alle seguenti istruzioni:

1. Nella finestra principale del programma, fare clic su **Controllo del computer**.
2. Fare clic su **Controllo del computer** per avviare il controllo del sistema.
3. Al termine del controllo, verificare nel registro il numero di file sottoposti a controllo, file infetti e file puliti.
4. Se si desidera controllare solo una parte del disco, fare clic su **Controllo personalizzato** e selezionare gli oggetti da controllare per la ricerca di virus.

Per ulteriori informazioni, consultare l'articolo della Knowledge Base ESET aggiornato periodicamente.

7.3 Come fare per creare una nuova attività in Pianificazione attività

Per creare una nuova attività in **Strumenti** > **Pianificazione attività**, fare clic su **Aggiungi** oppure fare clic con il pulsante destro del mouse e selezionare **Aggiungi...** dal menu contestuale. Sono disponibili cinque tipi di attività pianificate:

- **Esegui applicazione esterna**: consente di pianificare l'esecuzione di un'applicazione esterna.
- **Manutenzione rapporto**: i file di rapporto contengono anche elementi rimasti dai record eliminati. Questa attività ottimizza periodicamente i record nei file di rapporto allo scopo di garantire un funzionamento efficiente.
- **Controllo del file di avvio del sistema**: consente di controllare i file la cui esecuzione è consentita all'avvio del sistema o all'accesso.
- **Crea snapshot di stato computer**: crea uno snapshot del computer ESET SysInspector, raccoglie informazioni dettagliate sui componenti del sistema (ad esempio, driver e applicazioni) e valuta il livello di rischio di ciascun componente.
- **Controllo computer su richiesta**: consente di eseguire un controllo di file e di cartelle sul computer in uso.
- **Aggiornamento**: pianifica un'attività di aggiornamento attraverso un aggiornamento dei moduli.

Poiché **Aggiorna** rappresenta una delle attività pianificate utilizzata con maggiore frequenza, di seguito verranno illustrate le modalità in cui è possibile aggiungere una nuova attività di aggiornamento:

Dal menu a discesa **Attività pianificata**, selezionare **Aggiorna**. Inserire il nome dell'attività nel campo **Nome attività** e fare clic su **Avanti**. Selezionare la frequenza dell'attività. Sono disponibili le seguenti opzioni: **Una volta**, **Ripetutamente**, **Ogni giorno**, **Ogni settimana** e **Quando si verifica un evento.** Selezionare **Ignora attività se in esecuzione su un computer alimentato dalla batteria** per ridurre al minimo le risorse di sistema in caso di utilizzo della batteria del computer portatile. L'attività verrà eseguita alla data e all'ora specificate nei campi **Esecuzione attività**. È quindi possibile definire l'azione da intraprendere se l'attività non può essere eseguita o completata nei tempi programmati. Sono disponibili le seguenti opzioni:

- **Al prossimo orario pianificato**
- **Prima possibile**
- **Immediatamente, se l'ora dall'ultima esecuzione supera un valore specificato** (è possibile definire l'intervallo utilizzando la casella di scorrimento **Ora dall'ultima esecuzione (ore)**)

Nel passaggio successivo, viene visualizzata una finestra contenente un riepilogo delle informazioni sull'attività pianificata corrente. Fare clic su **Fine** una volta terminate le modifiche.

Verrà visualizzata una finestra di dialogo in cui è possibile scegliere i profili da utilizzare per l'attività pianificata. Qui è possibile impostare il profilo primario e alternativo. Il profilo alternativo viene utilizzato se l'attività non può essere completata mediante l'utilizzo del profilo primario. Confermare facendo clic su **Fine**. A questo punto, la nuova attività pianificata verrà aggiunta all'elenco delle attività pianificate correnti.

7.4 Come pianificare un controllo del computer settimanale

Per programmare un'attività periodica, aprire la finestra principale del programma e fare clic su **Strumenti** > **Pianificazione attività**. Di seguito viene riportata la procedura da seguire per pianificare un'attività che controllerà tutti i dischi locali ogni 24 ore. Per ulteriori istruzioni dettagliate, consultare questo articolo della Knowledge Base di ESET.

Per pianificare un'attività di scansione:

1. Fare clic su **Aggiungi** nella schermata principale di Pianificazione attività.
2. Selezionare **Controllo computer su richiesta** dal menu a discesa.
3. Immettere un nome per l'attività, quindi selezionare **Ogni settimana** per impostare la frequenza dell'attività.
4. Impostare l'ora e il giorno di esecuzione dell'attività.
5. Selezionare **Esegui l'attività appena possibile** per eseguire l'attività in un secondo momento nel caso in cui, per qualsiasi motivo, l'esecuzione dell'attività pianificata non si avvia (ad esempio se il computer era spento).

6. Esaminare il riepilogo dell'attività pianificata e fare clic su **Fine**.
7. Selezionare **Unità locali** nel menu a discesa **Destinazioni**.
8. Fare clic su **Fine** per confermare l'attività.