

ESET NOD32 Antivirus

Manuale dell'utente

[Fare clic qui per visualizzare la versione della Guida di questo documento](#)

Copyright ©2024 ESET, spol. s r.o.

ESET NOD32 Antivirus è stato sviluppato da ESET, spol. s r.o.

Per ulteriori informazioni, visitare la pagina <https://www.eset.com>.

Tutti i diritti riservati. È vietato riprodurre, memorizzare in sistemi di recupero o trasmettere in qualsiasi forma o con qualsiasi mezzo, elettronico, meccanico, tramite fotocopia, registrazione, scansione o altro la presente documentazione o parti di essa in assenza di autorizzazione scritta dell'autore.

ESET, spol. s r.o. si riserva il diritto di modificare qualsiasi parte del software applicativo descritta senza alcun preavviso.

Supporto tecnico: <https://support.eset.com>

REV. 12/04/2024

1 ESET NOD32 Antivirus	1
1.1 Novità	2
1.2 Quale è il mio prodotto?	2
1.3 Requisiti di sistema	3
1.3 Versione obsoleta di Microsoft Windows	4
1.4 Prevenzione	5
1.5 Pagine della Guida	6
2 Installazione	7
2.1 Live installer	7
2.2 Installazione off-line	9
2.3 Attivazione prodotto	10
2.3 Inserimento della chiave di licenza durante l'attivazione	11
2.3 Utilizza ESET HOME account	11
2.3 Attiva licenza di valutazione	12
2.3 Chiave di licenza ESET gratuita	13
2.3 Attivazione non riuscita: scenari comuni	14
2.3 Stato licenza	14
2.3 Attivazione non riuscita a causa di un utilizzo eccessivo della licenza	15
2.3 Upgrade licenza	16
2.3 Aggiornamento prodotto	17
2.3 Downgrade licenza	18
2.3 Downgrade prodotto	18
2.4 Strumento di individuazione e risoluzione dei problemi di installazione	19
2.5 Primo controllo dopo l'installazione	19
2.6 Aggiornamento a una versione più recente	20
2.6 Aggiornamento automatico prodotto legacy	21
2.7 Presentare un prodotto ESET a un amico	21
2.7 Sarà installato ESET NOD32 Antivirus	22
2.7 Passaggio a una linea di prodotti diversa	22
2.7 Registrazione	22
2.7 Avanzamento attivazione	22
2.7 Attivazione avvenuta con successo	22
3 Guida introduttiva	23
3.1 La finestra principale del programma	23
3.2 Aggiornamenti	26
4 Utilizzo di ESET NOD32 Antivirus	27
4.1 Protezione del computer	29
4.1 Motore di rilevamento	30
4.1 Opzioni avanzate del motore di rilevamento	34
4.1 Rilevamento di un'infiltrazione	35
4.1 Protezione file system in tempo reale	37
4.1 Livelli di pulizia	39
4.1 Quando modificare la configurazione della protezione in tempo reale	40
4.1 Controllo della protezione in tempo reale	40
4.1 Cosa fare se la protezione in tempo reale non funziona	40
4.1 Esclusioni processi	41
4.1 Aggiungi o modifica esclusioni dei processi	42
4.1 Protezione basata sul cloud	42
4.1 Filtro di esclusione per la protezione basata sul cloud	45
4.1 Controllo del computer	45

4.1 Launcher controllo personalizzato	48
4.1 Avanzamento controllo	49
4.1 Rapporto controlli computer	51
4.1 Controlli malware	53
4.1 Controllo stato di inattività	53
4.1 Profili di controllo	54
4.1 Destinazioni di controllo	54
4.1 Controllo dispositivi	55
4.1 Editor regole controllo dispositivi	56
4.1 Dispositivi rilevati	57
4.1 Aggiunta di regole per il controllo dispositivi	57
4.1 Gruppi dispositivi	60
4.1 Host Intrusion Prevention System (HIPS)	61
4.1 Finestra interattiva HIPS	64
4.1 Rilevato potenziale comportamento ransomware	65
4.1 Gestione regole HIPS	66
4.1 Impostazioni regole HIPS	67
4.1 Aggiungi percorso applicazione/registro per l'HIPS	70
4.1 Configurazione avanzata di HIPS	70
4.1 Caricamento driver sempre consentito	71
4.1 Modalità giocatore	71
4.1 Controllo all'avvio	72
4.1 Controllo automatico file di avvio	72
4.1 Protezione documenti	73
4.1 Esclusioni	73
4.1 Esclusioni dal controllo	74
4.1 Aggiungi o modifica esclusione di prestazioni	75
4.1 Formato di esclusione percorso	76
4.1 Esclusioni dalla rilevazione	77
4.1 Aggiungi o modifica esclusione dal rilevamento	79
4.1 Crea procedura guidata di esclusione dal rilevamento	80
4.1 Esclusioni HIPS	80
4.1 Parametri di ThreatSense	81
4.1 Estensioni file esclusi dal controllo	84
4.1 Parametri ThreatSense aggiuntivi	85
4.2 Protezione Internet	85
4.2 Filtraggio protocolli	86
4.2 Applicazioni escluse	87
4.2 Indirizzi IP esclusi	88
4.2 Aggiungi indirizzo IPv4	89
4.2 Aggiungi indirizzo IPv6	89
4.2 SSL/TLS	90
4.2 Certificati	91
4.2 Traffico di rete crittografato	92
4.2 Elenco di certificati noti	92
4.2 Elenco di applicazioni filtrate tramite SSL/TLS	93
4.2 Protezione client di posta	94
4.2 Integrazione client di posta	94
4.2 Barra degli strumenti di Microsoft Outlook	95
4.2 Finestra di dialogo di conferma	95
4.2 Ripeti controllo messaggi	95

4.2 Protocolli e-mail	96
4.2 Filtro POP3, POP3S	97
4.2 Contrassegni e-mail	98
4.2 Protezione accesso Web	98
4.2 Configurazione avanzata Protezione accesso Web	101
4.2 Protocolli Web	101
4.2 Gestione indirizzi URL	102
4.2 Elenco indirizzi URL	103
4.2 Creare un nuovo elenco di indirizzi URL	104
4.2 Come aggiungere una maschera per l'URL	105
4.2 Protezione Anti-Phishing	105
4.3 Aggiornamento del programma	107
4.3 Configurazione dell'aggiornamento	110
4.3 Rollback aggiornamento	112
4.3 Intervallo temporale di rollback	114
4.3 Aggiornamenti del prodotto	114
4.3 Opzioni connessione	115
4.3 Come fare per creare attività di aggiornamento	115
4.3 Finestra di dialogo - Riavvio necessario	116
4.4 Strumenti	116
4.4 File di rapporto	117
4.4 Filtraggio rapporti	119
4.4 Registrazione della configurazione	121
4.4 Processi in esecuzione	122
4.4 Report di protezione	124
4.4 ESET SysInspector	125
4.4 Pianificazione attività	126
4.4 Opzioni controllo pianificato	128
4.4 Panoramica attività pianificata	129
4.4 Dettagli attività	129
4.4 Tempo attività	130
4.4 Frequenza attività: una volta	130
4.4 Frequenza attività: ogni giorno	130
4.4 Frequenza attività: ogni settimana	130
4.4 Frequenza attività: quando si verifica un evento	130
4.4 Attività ignorata	131
4.4 Dettagli attività: aggiornamento	131
4.4 Dettagli attività: esegui applicazione	132
4.4 Strumento di pulizia del sistema	132
4.4 Quarantena	133
4.4 Server proxy	136
4.4 Seleziona campione per analisi	137
4.4 Seleziona campione per analisi: file sospetto	138
4.4 Seleziona campione per analisi: sito sospetto	138
4.4 Seleziona campione per analisi: file falso positivo	139
4.4 Seleziona campione per analisi: sito falso positivo	139
4.4 Seleziona campione per analisi: altro	139
4.4 Aggiornamento Microsoft Windows®	139
4.4 Finestra di dialogo - Aggiornamenti del sistema	140
4.4 Informazioni sugli aggiornamenti	140
4.5 Guida e supporto tecnico	140

4.5 Informazioni su ESET NOD32 Antivirus	141
4.5 Novità ESET	142
4.5 Invia dati configurazione sistema	143
4.5 Supporto tecnico	144
4.6 Account ESET HOME	144
4.6 Esegui la connessione a ESET HOME	146
4.6 Effettua l'autenticazione a ESET HOME	147
4.6 Autenticazione non riuscita: errori comuni	148
4.6 Aggiungi il dispositivo in ESET HOME	149
4.7 Interfaccia utente	149
4.7 Elementi dell'interfaccia utente	149
4.7 Configurazione dell'accesso	150
4.7 Password per la configurazione avanzata	151
4.7 Icona della barra delle applicazioni	152
4.7 Supporto per la lettura dello schermo	153
4.8 Notifiche	153
4.8 Finestra di dialogo: stati dell'applicazione	154
4.8 Notifiche desktop	154
4.8 Elenco di notifiche desktop	155
4.8 Avvisi interattivi	157
4.8 Messaggi di conferma	158
4.8 Supporti rimovibili	159
4.8 Inoltro	160
4.9 Impostazioni privacy	163
4.10 Profili	164
4.11 Tasti di scelta rapida	165
4.12 Diagnostica	165
4.12 Supporto tecnico	167
4.12 Importa ed esporta impostazioni	167
4.12 Ripristina tutte le impostazioni nella sezione corrente	168
4.12 Ripristina impostazioni predefinite	168
4.12 Errore durante il salvataggio della configurazione	168
4.13 Scanner riga di comando	169
4.14 ESET CMD	171
4.15 Rilevamento stato di inattività	173
5 Domande comuni	173
5.1 Come aggiornare ESET NOD32 Antivirus	174
5.2 Come rimuovere un virus dal PC	175
5.3 Come fare per creare una nuova attività in Pianificazione attività	175
5.4 Come pianificare un controllo del computer settimanale	176
5.5 Procedura di sblocco della configurazione avanzata	176
5.6 Come risolvere la disattivazione del prodotto da ESET HOME	177
5.6 Prodotto disattivato, dispositivo disconnesso	178
5.6 Prodotto non attivato	178
6 Programma di miglioramento dell'esperienza degli utenti	178
7 Accordo di licenza per l'utente finale	179
8 Informativa sulla privacy	191

ESSENTIAL SECURITY

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 dannosi 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 in 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.
Modalità scura	Estensione che aiuta l'utente a impostare rapidamente lo schermo su un tema scuro. È possibile scegliere la combinazione di colori preferita in Elementi dell'interfaccia utente .
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 dispositivi	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.

Novità

Novità in ESET NOD32 Antivirus 16.1

Intel® Threat Detection Technology

Tecnologia basata su hardware in grado di individuare attacchi ransomware nel momento in cui tentano di eludere il rilevamento nella memoria. La sua integrazione potenzia la protezione ransomware mantenendo nel contempo elevate prestazioni generali del sistema. Consultare [Processori supportati](#).

Modalità scura

Questa funzione consente all'utente di scegliere una combinazione di colori chiari o scuri per l'interfaccia utente grafica di ESET NOD32 Antivirus. È ora possibile cambiare la combinazione di colori nell'angolo in alto a destra della [finestra principale del programma](#).

Supporto per Windows 7, 8 e 8.1 rimosso.

ESET NOD32 Antivirus 16.1 è supportato solo su Windows 10 e 11. Per ulteriori informazioni, consultare [Versioni non aggiornate di Microsoft Windows](#).



Per disabilitare **Notifiche sulle novità**, fare clic su **Configurazione avanzata > Notifiche > Notifiche desktop**. Fare clic su **Modifica** accanto a **Notifiche desktop**, deselezionare la casella di controllo **Visualizza le notifiche relative alle novità** e fare clic su **OK**. Per ulteriori informazioni sulle notifiche, consultare la sezione [Notifiche](#).

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](#) e sarà possibile leggere il nome del prodotto nella parte superiore della finestra (vedere l'[articolo di knowledgebase](#)).

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

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Motore di rilevamento	✓	✓	✓
Apprendimento automatico avanzato	✓	✓	✓
Exploit Blocker	✓	✓	✓
Protezione contro attacchi basati su script	✓	✓	✓

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Anti-Phishing	✓	✓	✓
Protezione accesso Web	✓	✓	✓
HIPS (compresa la Protezione ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Network Inspector		✓	✓
Protezione webcam		✓	✓
Protezione contro gli attacchi di rete		✓	✓
Protezione Botnet		✓	✓
Protezione pagamenti bancari		✓	✓
Controllo accessi		✓	✓
Anti-Furto		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

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

Requisiti di sistema

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

Processori supportati

Processore Intel o AMD, 32 bit (x86) con set di istruzioni SSE2 o 64 bit (x64), 1 GHz o superiore
processore basato su ARM64, 1 GHz o superiore

Sistemi operativi supportati

Microsoft® Windows® 11

Microsoft® Windows® 10

 Mantenere sempre aggiornato il sistema operativo.

Requisiti delle funzioni di ESET NOD32 Antivirus

Consultare i requisiti di sistema per le funzioni specifiche di ESET NOD32 Antivirus nella tabella sottostante:

Funzione	Requisiti
Intel® Threat Detection Technology	Consultare Processori supportati .

Funzione	Requisiti
Sfondo trasparente	Windows 10 versione RS4 e successive.
Strumento di pulizia specializzato	Processore non ARM64.
Strumento di pulizia del sistema	Processore non ARM64.
Exploit Blocker	Processore non ARM64.
Controllo approfondito comportamento	Processore non ARM64.

Altro

Per l'attivazione e per il corretto funzionamento degli aggiornamenti di ESET NOD32 Antivirus, è necessaria una connessione Internet.

L'esecuzione contemporanea di due programmi antivirus su un singolo dispositivo causa inevitabili conflitti di risorse di sistema, come ad esempio un rallentamento del sistema per renderlo inutilizzabile.

Versione obsoleta di Microsoft Windows

Problema

- Si desidera eseguire l'installazione della versione più recente di ESET NOD32 Antivirus su un computer con sistema operativo Windows 7, Windows 8 (8.1) o Windows Home Server 2011
- ESET NOD32 Antivirus consente di visualizzare l'errore **Sistema operativo obsoleto** durante l'installazione

Dettagli

La versione più recente di ESET NOD32 Antivirus (versione 16.1) richiede i sistemi operativi Windows 10 o Windows 11.

Soluzione

Sono disponibili le seguenti soluzioni:

Aggiornamento a Windows 10 o Windows 11

Il processo di aggiornamento è relativamente semplice e, in molti casi, puoi farlo senza perdere i file. Prima di eseguire l'aggiornamento a Windows 10:

1. Eseguire il backup dei dati importanti.
2. Consultare le [Domande frequenti \(FAQ\) sull'aggiornamento a Windows 10](#) o le [Domande frequenti \(FAQ\) sull'aggiornamento a Windows 11](#) e aggiornare il sistema operativo Windows in uso.

Installare ESET NOD32 Antivirus versione 16.0

Se non è possibile aggiornare Windows, [installare ESET NOD32 Antivirus versione 16.0](#). Per ulteriori informazioni,

consultare la [Guida online di ESET NOD32 Antivirus versione 16.0](#).

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 remoti](#). 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 ESET LiveGrid®, 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.

Pagine della Guida

Benvenuti nella Guida di ESET NOD32 Antivirus. Le informazioni fornite qui offrono all'utente dettagli utili sul prodotto e contribuiscono a migliorare la protezione del computer.

Avvio

Prima di utilizzare ESET NOD32 Antivirus, è possibile consultare informazioni relative a vari [tipi di rilevamenti](#) e [attacchi da remoto](#) che potrebbero verificarsi durante l'utilizzo del computer. È stato compilato anche un elenco delle [nuove funzioni](#) introdotte in ESET NOD32 Antivirus.

Iniziare dall'[installazione di ESET NOD32 Antivirus](#). Se l'applicazione ESET NOD32 Antivirus è già stata installata, consultare [Utilizzo di ESET NOD32 Antivirus](#).

Come utilizzare le pagine della Guida di ESET NOD32 Antivirus

La guida online è suddivisa in vari capitoli e sottocapitoli. Premere **F1** in ESET NOD32 Antivirus per visualizzare le informazioni sulla finestra attualmente aperta.

È possibile cercare un argomento della Guida oppure digitare parole o frasi da ricercare. La differenza tra questi due metodi consiste nel fatto che una parola chiave può essere correlata logicamente a pagine della Guida che non contengono la specifica parola chiave nel testo. La ricerca di parole e frasi verrà invece eseguita nel contenuto di tutte le pagine e verranno visualizzate solo le pagine contenenti la parola o frase ricercata nel testo.

Per motivi di coerenza e per evitare confusione, la terminologia utilizzata nella presente guida si basa sull'interfaccia utente di ESET NOD32 Antivirus. Inoltre, al fine di mettere in evidenza argomenti di particolare interesse o rilevanza, è stato utilizzato un insieme uniforme di simboli.



Una nota non è altro che una breve osservazione. Sebbene non siano obbligatori, questi elementi forniscono informazioni utili relative, ad esempio, a funzioni specifiche o collegamenti ad argomenti correlati.



Ciò richiede l'attenzione del lettore, che è pertanto invitato a non saltare l'argomento. Questo strumento fornisce solitamente informazioni non critiche ma importanti.



Queste informazioni richiedono una particolare attenzione e cautela. Questi contenuti vengono inseriti principalmente allo scopo di impedire all'utente di commettere errori potenzialmente dannosi. Leggere e comprendere il testo, in quanto fa riferimento a impostazioni di sistema altamente sensibili o a contenuti a rischio.



Questo è un esempio pratico che aiuta l'utente a comprendere la modalità di utilizzo di determinate funzioni o caratteristiche.

Convenzione	Significato
Grassetto	Nomi degli elementi delle interfacce come caselle e pulsanti delle opzioni.
<i>Corsivo</i>	Segnaposti per le informazioni fornite dall'utente. Ad esempio, nome del file o percorso indica che l'utente ha digitato il percorso o il nome effettivo di un file.
Courier New	Esempi di codici o comandi.
Collegamento ipertestuale	Fornisce un accesso facile e veloce ai riferimenti incrociati o ai percorsi Web esterni. I collegamenti ipertestuali sono evidenziati in blu e presentano talvolta una sottolineatura.
%ProgramFiles%	Directory di sistema di Windows nella quale vengono memorizzati i programmi installati su Windows.

La Guida on-line rappresenta il documento di supporto principale. L'ultima versione della guida online verrà visualizzata automaticamente in presenza di una connessione Internet funzionante.

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](#): scaricato dal sito web di ESET o da un CD/DVD. Il pacchetto di installazione è universale per tutte le lingue (scegliere la lingua appropriata). Live Installer è un file di piccole dimensioni; i file aggiuntivi necessari per installare ESET NOD32 Antivirus vengono scaricati automaticamente.
- [Installazione offline](#): utilizza un file .exe più grande del file di Live Installer e non richiede una connessione Internet o file aggiuntivi per completare l'installazione.



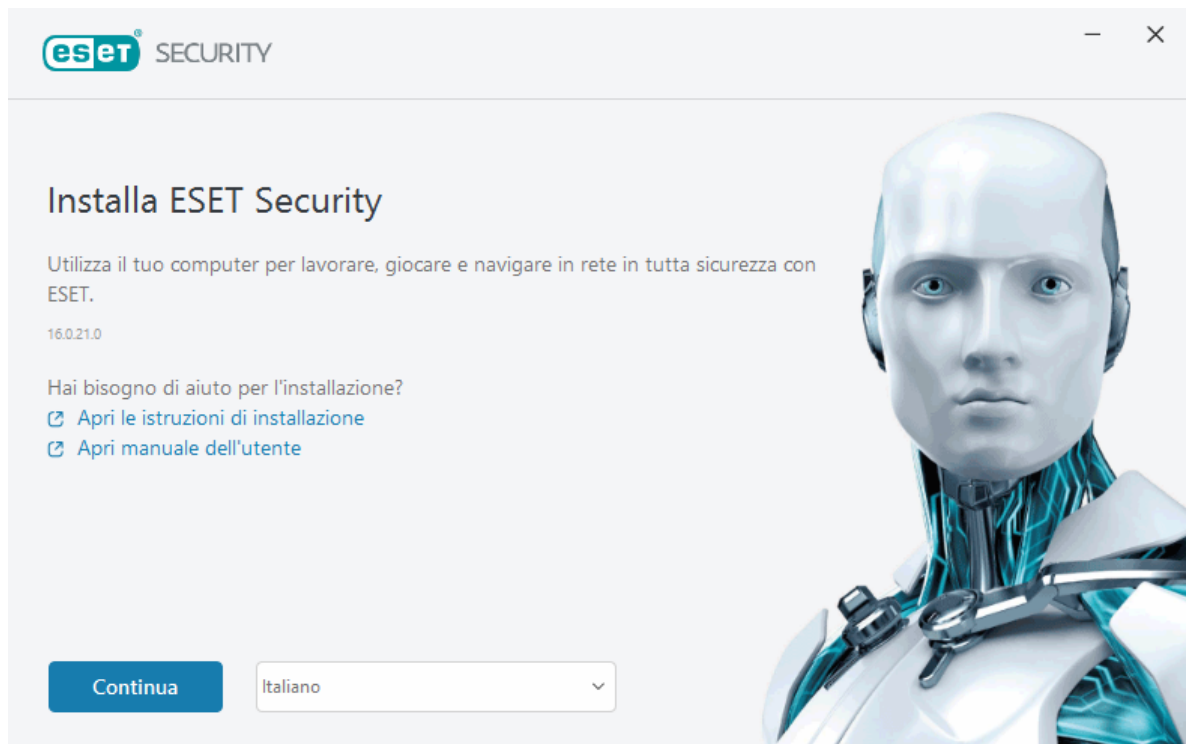
Verificare che nel computer non siano installati altri programmi antivirus prima dell'installazione di ESET NOD32 Antivirus. Se su un singolo computer sono installate due o più soluzioni antivirus, potrebbero entrare in conflitto tra loro. È consigliabile disinstallare gli altri programmi antivirus presenti 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).

Live installer

Dopo aver scaricato il [Pacchetto di installazione di Live Installer](#), fare doppio clic sul file di installazione e seguire le istruzioni dettagliate nella procedura guidata del programma di installazione.



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



1. Selezionare la lingua appropriata dal menu a discesa e fare clic su **Continua**.

i In caso di installazione di una versione più recente rispetto alla versione precedente con impostazioni protette da password, digitare la propria password. È possibile configurare la password delle impostazioni in [Configurazione dell'accesso](#).

2. Selezionare le preferenze relative alle seguenti funzioni, leggere l'[Accordo di licenza per l'utente finale](#) e l'[Informativa sulla privacy](#) e fare clic su **Continua** o su **Consenti tutto e continua** per abilitare tutte le funzioni:

- [Sistema di feedback ESET LiveGrid®](#)
- [Applicazioni potenzialmente indesiderate](#)
- [Programma di miglioramento dell'esperienza degli utenti](#)

i Facendo clic su **Continua** o su **Consenti tutto e continua**, l'utente accetta l'Accordo di licenza per l'utente finale e l'Informativa sulla privacy.

3. Per attivare, gestire e visualizzare la protezione del dispositivo utilizzando l'account ESET HOME, [collegare il dispositivo all'account ESET HOME](#). Fare clic su **Salta accesso** per continuare senza effettuare la connessione a ESET HOME. È possibile [collegare il dispositivo all'account ESET HOME in un secondo momento](#).


4. Se si continua senza effettuare la connessione a ESET HOME, scegliere un'[opzione di attivazione](#). Se sulla versione precedente se ne installa una più recente, la chiave di licenza viene inserita automaticamente.

5. La procedura guidata di installazione determina quale prodotto ESET è installato in base alla licenza dell'utente. La versione con il maggior numero di funzioni di protezione è sempre preselezionata. Fare clic su **Modifica prodotto** se si desidera [installare una versione differente del prodotto ESET](#). Fare clic su **Continua** per avviare il processo di installazione. L'operazione richiede alcuni istanti.

i Nel caso in cui sul computer in uso dovessero rimanere file o cartelle dei prodotti ESET disinstallati in passato, all'utente verrà richiesto di consentirne la rimozione. Fare clic su **Installa** per continuare.

6. Fare clic su **Fatto** per uscire dalla procedura guidata di installazione.

 [Strumento di individuazione e risoluzione dei problemi di installazione.](#)

 In seguito all'installazione e all'attivazione del prodotto, si avvia il download dei moduli. La protezione si avvia, ma alcune funzioni potrebbero non essere pienamente operative fino al completamento del download.

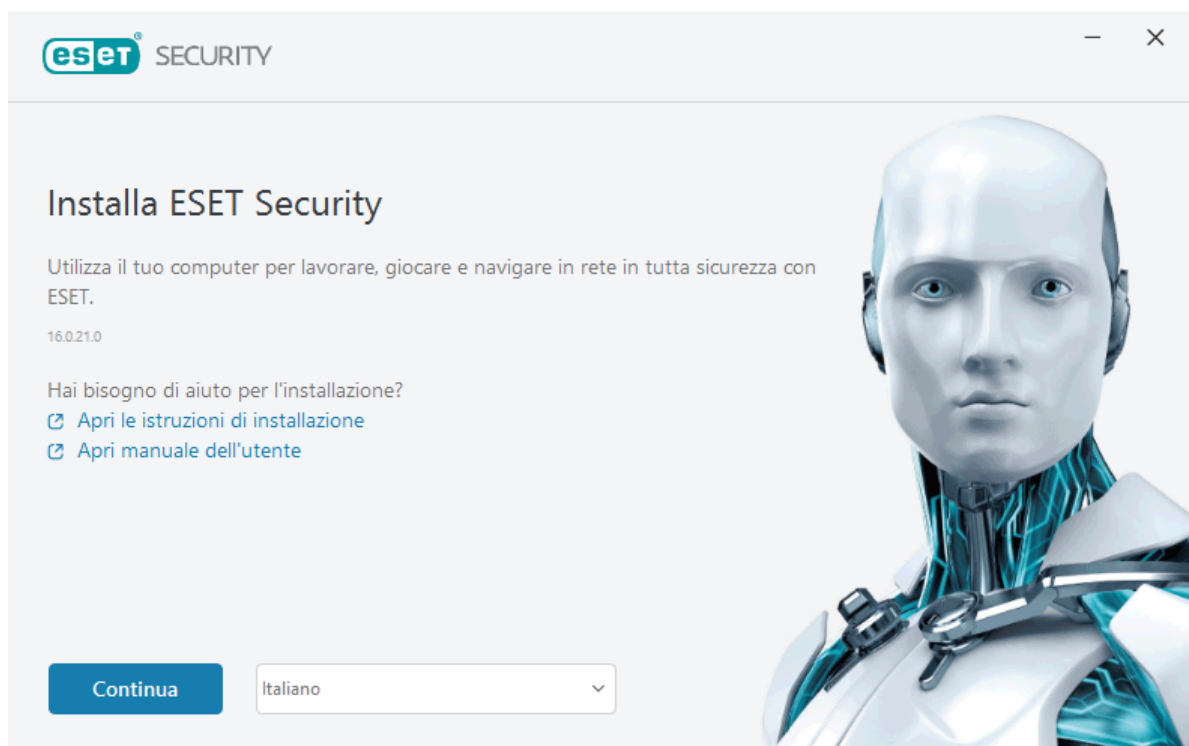
Installazione off-line

Scaricare e installare il prodotto ESET Windows Home utilizzando il programma di installazione offline (.exe) sottostante. [Scegliere la versione del prodotto ESET HOME da scaricare](#) (32 bit, 64 bit o ARM).


ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Download 64 bit	Download 64 bit	Download 64 bit
Download 32 bit	Download 32 bit	Download 32 bit
Download ARM	Download ARM	Download ARM

 In caso di connessione Internet attiva, [installare il prodotto ESET utilizzando un'istanza di Live Installer](#).

Dopo aver avviato il programma di installazione offline (.exe), la procedura di installazione guidata condurrà l'utente attraverso il processo di configurazione.



1. Selezionare la lingua appropriata dal menu a discesa e fare clic su **Continua**.

 In caso di installazione di una versione più recente rispetto alla versione precedente con impostazioni protette da password, digitare la propria password. È possibile configurare la password delle impostazioni in [Configurazione dell'accesso](#).

2. Selezionare le preferenze relative alle seguenti funzioni, leggere l'[Accordo di licenza per l'utente finale](#) e l'[Informativa sulla privacy](#) e fare clic su **Continua** o su **Consenti tutto e continua** per abilitare tutte le funzioni:

- [Sistema di feedback ESET LiveGrid®](#)
- [Applicazioni potenzialmente indesiderate](#)
- [Programma di miglioramento dell'esperienza degli utenti](#)

i Facendo clic su **Continua** o su **Consenti tutto e continua**, l'utente accetta l'Accordo di licenza per l'utente finale e l'Informativa sulla privacy.

3. Fare clic su **Salta autenticazione**. In caso di connessione Internet, è possibile [collegare il dispositivo all'account ESET HOME](#).

4. Fare clic su **Salta attivazione**. Per essere pienamente operativo, ESET NOD32 Antivirus deve essere attivato dopo l'installazione. L'[attivazione del prodotto](#) richiede una connessione Internet attiva.

5. La procedura guidata di installazione consente di visualizzare il prodotto ESET che verrà installato in base al programma di installazione offline scaricato. Fare clic su **Continua** per avviare il processo di installazione. L'operazione richiede alcuni istanti.

i Nel caso in cui sul computer in uso dovessero rimanere file o cartelle dei prodotti ESET disinstallati in passato, all'utente verrà richiesto di consentirne la rimozione. Fare clic su **Installa** per continuare.

6. Fare clic su **Fatto** per uscire dalla procedura guidata di installazione.

! [Strumento di individuazione e risoluzione dei problemi di installazione.](#)

Attivazione prodotto

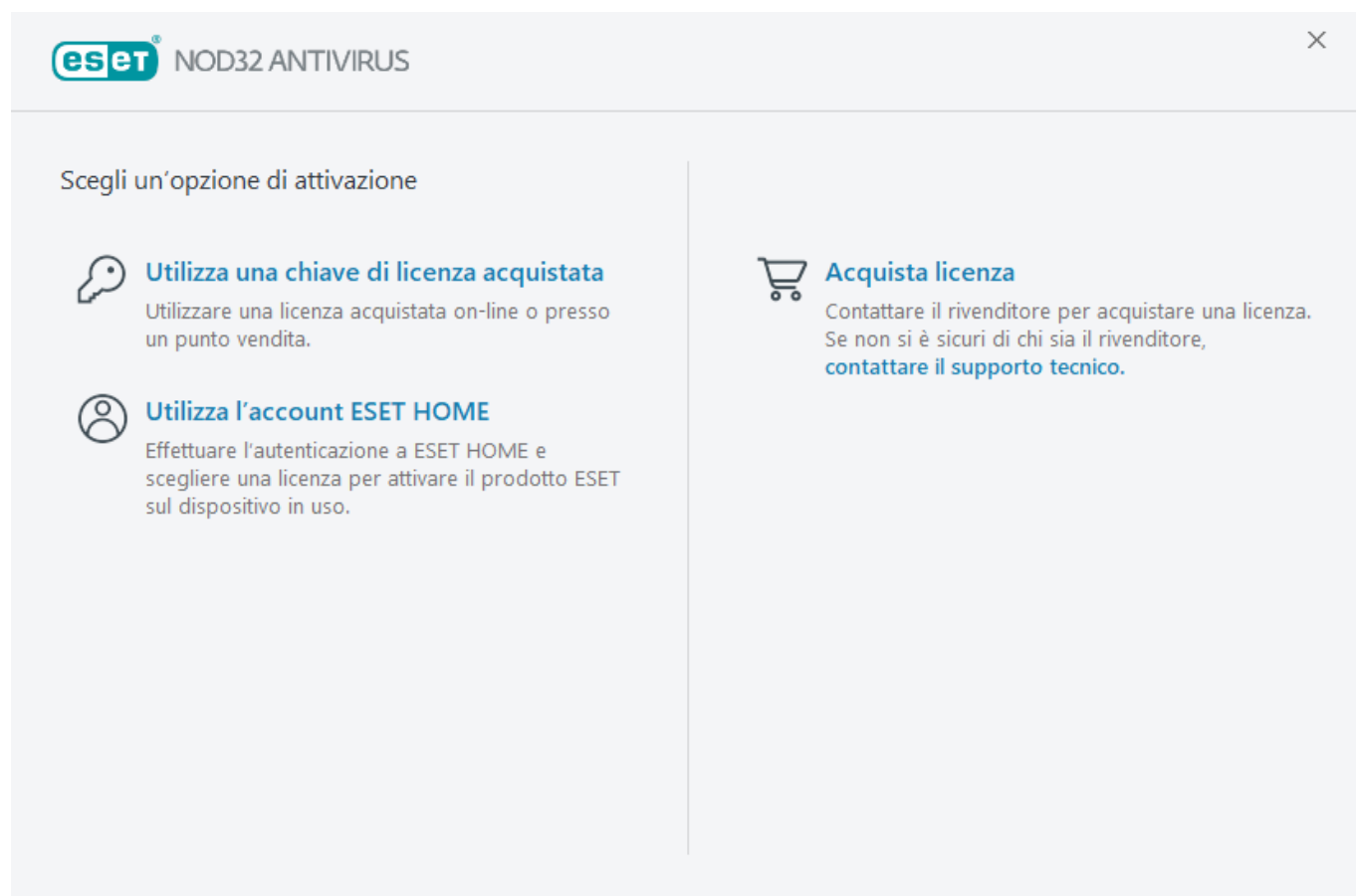
Sono disponibili vari metodi per attivare il prodotto. La disponibilità di uno scenario di attivazione specifico nella finestra di attivazione potrebbe variare in base al Paese e ai mezzi di distribuzione (CD/DVD, pagina Web ESET, ecc.):

- In caso di acquisto di una versione del prodotto presso un rivenditore al dettaglio o di ricezione di un'e-mail contenente i dettagli della licenza, attivare il prodotto facendo clic su **Utilizza una chiave di licenza acquistata**. 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 viene 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.
- Dopo aver selezionato [Utilizza account ESET HOME](#), verrà richiesto di effettuare l'autenticazione all'account ESET HOME.
- Se si desidera provare ESET NOD32 Antivirus prima di acquistarlo, selezionare [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. [Le licenze complete dei prodotti ESET Windows Home non sono gratuite.](#)

È possibile modificare la licenza del prodotto in qualsiasi momento. Per far ciò, fare clic su **Guida e supporto**

tecnico > Modifica licenza nella [finestra principale del programma](#). A questo punto, compare l'ID della licenza pubblica per consentire al Supporto ESET di identificare la licenza.

 [Attivazione del prodotto non riuscita?](#)



Inserimento della chiave di licenza durante l'attivazione

Gli aggiornamenti automatici sono importanti per la sicurezza. ESET NOD32 Antivirus riceverà gli aggiornamenti solo dopo l'attivazione.

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.

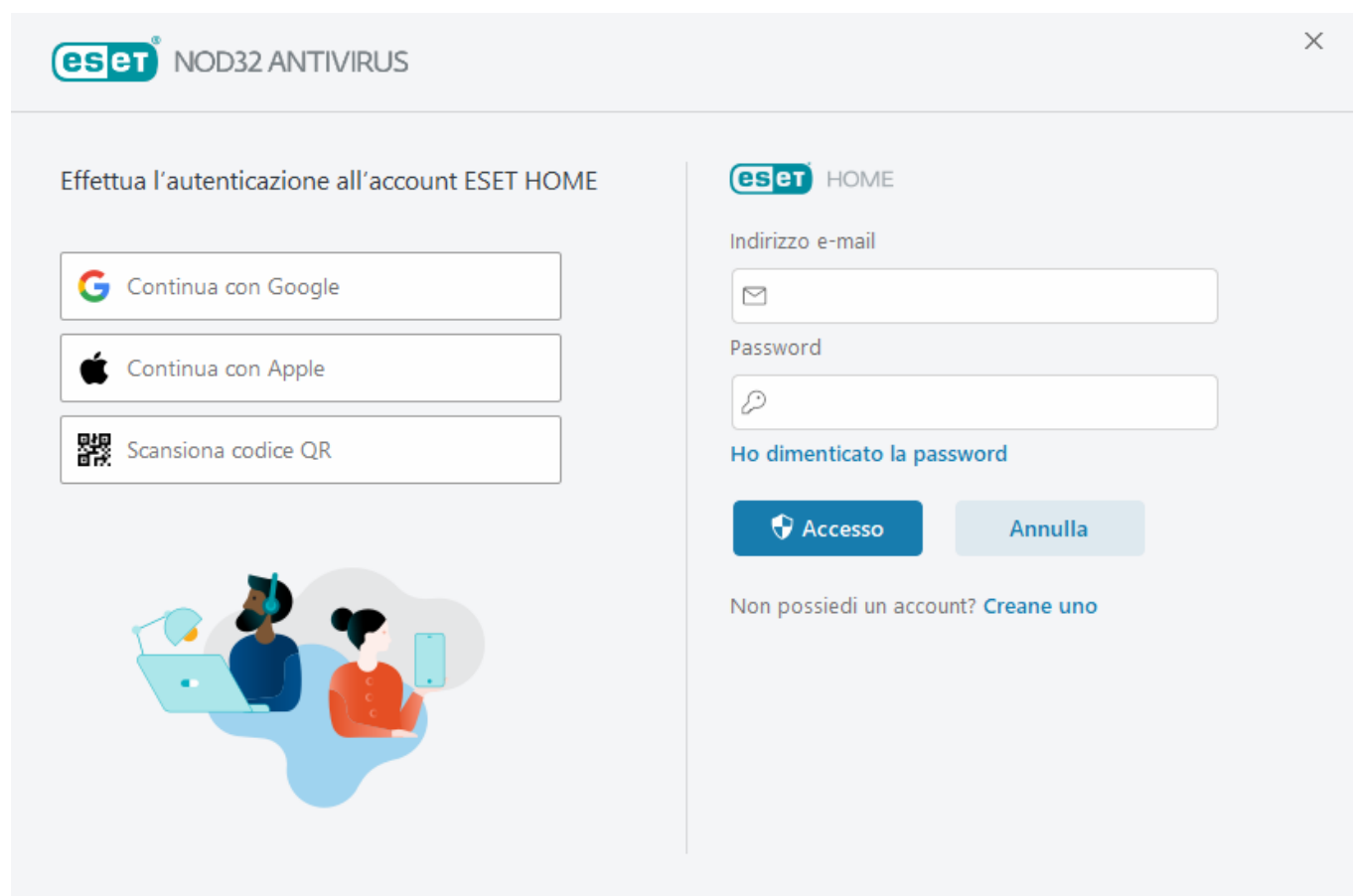
Se non si inserisce la chiave di licenza dopo l'installazione, il prodotto non sarà attivato. È possibile attivare ESET NOD32 Antivirus nella [finestra principale del programma](#) > **Guida e supporto tecnico** > **Attiva licenza**.

[Le licenze complete dei prodotti ESET Windows Home non sono gratuite.](#)

Utilizza ESET HOME account

Collegare il dispositivo all'account [ESET HOME](#) per visualizzare e gestire tutte le licenze e i dispositivi ESET attivati. È possibile rinnovare, aggiornare o estendere la licenza e visualizzare informazioni importanti su di essa. Nel

portale di gestione o nell'app per dispositivi mobili di ESET HOME è possibile aggiungere varie licenze, scaricare prodotti sui dispositivi, controllare lo stato di protezione dei prodotti o condividere licenze tramite e-mail. Per ulteriori informazioni, consultare la [Guida online di ESET HOME](#).



Dopo aver selezionato **Utilizza account ESET HOME** come metodo di attivazione o durante la connessione all'account ESET HOME durante l'installazione:

1. [Effettuare l'autenticazione all'account ESET HOME](#).



Se non si possiede un account ESET HOME, fare clic su **Crea account** per effettuare la registrazione o consultare le istruzioni contenute nella [Guida online di ESET HOME](#).

Se si dimentica la password, fare clic su **Ho dimenticato la password** e seguire i passaggi a schermo oppure consultare le istruzioni nella [Guida online di ESET HOME](#).

2. Impostare un **Nome del dispositivo** che verrà utilizzato in tutti i servizi ESET HOME e fare clic su **Continua**.
3. Scegliere una licenza per l'attivazione o [aggiungere una nuova licenza](#). Fare clic su **Continua** per attivare ESET NOD32 Antivirus.

Attiva licenza di valutazione

Per attivare la versione di prova di ESET NOD32 Antivirus, inserire un indirizzo e-mail valido nei campi **Indirizzo e-mail** e **Conferma indirizzo e-mail**. Dopo l'attivazione, la licenza ESET verrà generata e inviata all'utente tramite e-mail. L'indirizzo e-mail verrà inoltre utilizzato per inviare notifiche sulla scadenza del prodotto e altre comunicazioni da ESET. È possibile attivare la licenza di prova soltanto una volta.

Selezionare il paese di residenza dal menu a discesa **Paese** per registrare ESET NOD32 Antivirus presso il

distributore locale, il quale fornirà il supporto tecnico.

Chiave di licenza ESET gratuita

La licenza completa di ESET NOD32 Antivirus non è gratuita.

La Chiave di licenza di ESET è una sequenza univoca di lettere e numeri separati da un trattino e fornita da ESET per consentire l'utilizzo legale di ESET NOD32 Antivirus in conformità dell'[Accordo di licenza per l'utente finale](#). Ogni Utente finale ha facoltà di utilizzare la Chiave di licenza unicamente nella misura in cui sia autorizzato a utilizzare ESET NOD32 Antivirus in base al numero di licenze concesse da ESET. La Chiave di licenza è considerata un contenuto riservato che non dovrà essere condiviso. È tuttavia possibile [condividere le postazioni della licenza utilizzando l'account ESET HOME](#).

Sebbene su Internet siano disponibili siti Web in cui si forniscono chiavi di licenza ESET gratuite, è importante ricordare quanto segue:

- Facendo clic su un annuncio pubblicitario “Licenza ESET gratuita” il funzionamento del computer o del dispositivo potrebbe essere compromesso dall'attacco di un malware. I malware potrebbero nascondersi in contenuti web non ufficiali (p. es. video), siti web contenenti annunci pubblicitari che lucrano sulle visite degli utenti, ecc. Si tratta solitamente di contenuti ingannevoli.
- Avendone piena facoltà, ESET disattiva licenze contraffatte.
- Il possesso di una chiave di licenza contraffatta viola le condizioni stabilite nell'[Accordo di licenza per l'utente finale](#) che è necessario accettare per poter installare ESET NOD32 Antivirus.
- Acquistare licenze ESET esclusivamente tramite canali ufficiali quali www.eset.com, distributori o rivenditori ESET (non acquistarle da siti Web di rivenditori terzi non ufficiali come eBay o licenze condivise da terze parti).
- Anche se il [download](#) di un ESET NOD32 Antivirus è gratuito, l'attivazione durante l'installazione richiede una chiave di licenza ESET valida (è possibile scaricarla e installarla, ma senza attivazione non potrà funzionare).
- Non condividere la licenza su Internet o sui social network (potrebbe essere replicata).

Per identificare e segnalare una licenza ESET contraffatta, [fare riferimento a questo articolo della Knowledge Base](#) per consultare le istruzioni.

In caso di dubbi sull'acquisto di un prodotto ESET Security, è possibile utilizzare una versione di prova prima di decidere di:

1. [Attivare ESET NOD32 Antivirus utilizzando una licenza di prova gratuita](#)
2. [Partecipare al programma ESET Beta](#)
3. [Installare ESET Mobile Security](#) in caso di utilizzo di un dispositivo mobile Android (versione freemium).

Per ottenere uno sconto/estendere la licenza, [Rinnovare la licenza di ESET](#).

Attivazione non riuscita: scenari comuni

Se l'attivazione di ESET NOD32 Antivirus non viene eseguita correttamente, gli scenari più comuni sono:

- La chiave di licenza è già in uso.
- È stata inserita una chiave di licenza non valida.
- Le informazioni nel modulo di attivazione sono mancanti o non valide.
- Comunicazione con il server di attivazione non riuscita.
- Assenza di connessione o connessione disattivata ai server di attivazione ESET.

Verificare di aver inserito la chiave di licenza corretta e che la connessione Internet sia attiva. Provare a eseguire nuovamente l'attivazione di ESET NOD32 Antivirus. Se si utilizza l'account ESET HOME per l'attivazione, consultare Gestione licenze [ESET HOME - Guida online](#).

i Se viene visualizzato un errore specifico (ad esempio, Licenza sospesa o Licenza oggetto di un utilizzo eccessivo), seguire le istruzioni riportate nello [Stato della licenza](#).

Se non è ancora possibile eseguire l'attivazione ESET NOD32 Antivirus, [ESET Activation Troubleshooter](#) illustra domande, errori e problemi comuni relativi all'attivazione e alla gestione delle licenze (disponibile in inglese e in molte altre lingue).

Stato licenza

La licenza può essere associata a stati diversi. È possibile consultare lo stato della licenza in [ESET HOME](#). Per aggiungere la licenza all'account ESET HOME, consultare [Aggiungere una licenza](#).

i Se non si dispone di un account ESET HOME, è possibile [Creare un nuovo account ESET HOME](#).

Se lo stato della licenza è diverso da **Attivo**, verranno visualizzati un errore durante l'attivazione o una notifica nella [finestra principale del programma](#).

Per disabilitare le notifiche relative allo stato della licenza, aprire **Configurazione avanzata (F5) > Notifiche > Stati dell'applicazione**. Fare clic su **Modifica** accanto a **Stati dell'applicazione**, espandere **Gestione delle licenze** e deselezionare la casella di controllo accanto alla notifica che si desidera disabilitare. La disabilitazione della notifica non risolve il problema.

Consultare le descrizioni e le soluzioni consigliate per i vari stati della licenza nella tabella sottostante:

Stato licenza	Descrizione	Soluzione
Attivo	La licenza è valida e non è necessaria l'interazione dell'utente. È possibile attivare ESET NOD32 Antivirus e consultare i dettagli della licenza nella finestra principale del programma > Guida e supporto tecnico .	

Stato licenza	Descrizione	Soluzione
Utilizzo eccessivo	Il numero di dispositivi che utilizzano questa licenza è superiore a quello consentito. Verrà visualizzato un errore di attivazione.	Per maggiori informazioni, consultare Attivazione non riuscita a causa di un utilizzo eccessivo della licenza .
Sospesa	La licenza è stata sospesa a causa di problemi di pagamento. Per utilizzare la licenza, assicurarsi che i dettagli di pagamento in ESET HOME siano aggiornati o contattare il rivenditore della licenza. È possibile visualizzare questo errore durante l'attivazione o nella finestra principale del programma .	<p>Prodotto installato: se si possiede un account ESET HOME, nella notifica visualizzata nella finestra principale del programma fare clic su Gestisci la licenza in ESET HOME e rivedere i dettagli di pagamento. In caso contrario, contattare il rivenditore della licenza.</p> <p>Errore di attivazione: se si possiede un account ESET HOME, nella finestra dell'errore di attivazione fare clic su Apri ESET HOME e rivedere i dettagli di pagamento. In caso contrario, contattare il rivenditore della licenza.</p>
Scaduta	La licenza è scaduta e non è possibile utilizzarla per attivare ESET NOD32 Antivirus. È possibile visualizzare questo errore durante l'attivazione o nella finestra principale del programma . Se è già stata installata l'applicazione ESET NOD32 Antivirus, il computer in uso non è protetto.	<p>Prodotto installato: nella notifica visualizzata nella finestra principale del programma fare clic su Rinnova licenza e seguire le istruzioni riportate in Come faccio a rinnovare la licenza? oppure fare clic su Attiva prodotto e scegliere il metodo di attivazione.</p> <p>Errore di attivazione: nella finestra dell'errore di attivazione fare clic su Rinnova licenza e seguire le istruzioni riportate in Come faccio a rinnovare la licenza? oppure digitare una chiave di licenza nuova o rinnovata e fare clic su Rinnova licenza.</p>

Attivazione non riuscita a causa di un utilizzo eccessivo della licenza

Problema

- La licenza potrebbe essere utilizzata eccessivamente o in modo non corretto
- Attivazione non riuscita a causa di un utilizzo eccessivo della licenza

Soluzione

Il numero di dispositivi che utilizzano questa licenza è superiore rispetto a quello consentito. L'utente potrebbe essere vittima di pirateria o contraffazione di software. La licenza non può essere utilizzata per attivare altri prodotti ESET. Il problema può essere risolto direttamente se si è autorizzati a gestire la licenza nell'account ESET HOME o ad acquistarla da una fonte legittima. Se non si possiede ancora un account, crearne uno.

Se possiedi una licenza e non ti è stato richiesto di inserire l'indirizzo e-mail:

1. Per gestire la licenza ESET, aprire un web browser e portarsi in <https://home.eset.com>. Accedere a ESET License Manager e rimuovere o disattivare le postazioni. Per ulteriori informazioni, consultare [Cosa fare in caso di utilizzo di una licenza utilizzata eccessivamente](#).
2. Per identificare e segnalare una licenza ESET contraffatta, [consulta le istruzioni contenute nell'articolo Identificare e segnalare licenze ESET contraffatte](#).
3. In caso di dubbi, fai clic su **Indietro** e [invia un'e-mail al supporto tecnico di ESET](#).

Se non si è il proprietario della licenza, contattarlo informandolo del fatto che non è possibile attivare il prodotto ESET a causa di un utilizzo eccessivo della licenza. Il proprietario può risolvere il problema nel portale [ESET HOME](#).

Se ti viene richiesto di confermare l'indirizzo e-mail (solo in alcuni casi), inserisci l'indirizzo e-mail utilizzato originariamente per acquistare o attivare ESET NOD32 Antivirus.

Upgrade licenza

Questa finestra di notifica viene visualizzata in caso di modifica della licenza utilizzata per l'attivazione del prodotto ESET. La licenza modificata consente all'utente di attivare un prodotto con più funzioni di protezione. Se non è stata eseguita alcuna modifica, ESET NOD32 Antivirus consentirà di visualizzare una volta una finestra di avviso chiamata **Cambia in un prodotto con più funzioni**.

Sì (scelta consigliata): installerà automaticamente il prodotto con più funzioni di protezione.

No, grazie: non verrà apportata alcuna modifica e la notifica scomparirà in modo permanente.

Per modificare il prodotto in un secondo momento, consultare questo [Articolo della Knowledge Base di ESET](#). Per ulteriori informazioni sulle licenze ESET, consultare [Domande frequenti sulle licenze](#).

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

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Motore di rilevamento	✓	✓	✓
Apprendimento automatico avanzato	✓	✓	✓
Exploit Blocker	✓	✓	✓
Protezione contro attacchi basati su script	✓	✓	✓
Anti-Phishing	✓	✓	✓
Protezione accesso Web	✓	✓	✓
HIPS (compresa la Protezione ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Network Inspector		✓	✓
Protezione webcam		✓	✓
Protezione contro gli attacchi di rete		✓	✓
Protezione Botnet		✓	✓

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Protezione pagamenti bancari		✓	✓
Controllo accessi		✓	✓
Anti-Furto		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Aggiornamento prodotto

È stato scaricato un programma di installazione predefinito e si è deciso di modificare il prodotto da attivare oppure si desidera modificare il prodotto installato in uno con altre funzioni di protezione.

[Modifica il prodotto durante l'installazione.](#)

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

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Motore di rilevamento	✓	✓	✓
Apprendimento automatico avanzato	✓	✓	✓
Exploit Blocker	✓	✓	✓
Protezione contro attacchi basati su script	✓	✓	✓
Anti-Phishing	✓	✓	✓
Protezione accesso Web	✓	✓	✓
HIPS (compresa la Protezione ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Network Inspector		✓	✓
Protezione webcam		✓	✓
Protezione contro gli attacchi di rete		✓	✓
Protezione Botnet		✓	✓
Protezione pagamenti bancari		✓	✓
Controllo accessi		✓	✓
Anti-Furto		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Downgrade licenza

La finestra di dialogo viene visualizzata quando la licenza utilizzata per l'attivazione del prodotto ESET è stata modificata. La licenza modificata può essere utilizzata solo con un prodotto ESET diverso con meno funzioni di protezione. Il prodotto è stato modificato automaticamente allo scopo di prevenire la perdita di protezione.

Per ulteriori informazioni sulle licenze ESET, consultare [Domande frequenti sulle licenze](#).

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

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Motore di rilevamento	✓	✓	✓
Apprendimento automatico avanzato	✓	✓	✓
Exploit Blocker	✓	✓	✓
Protezione contro attacchi basati su script	✓	✓	✓
Anti-Phishing	✓	✓	✓
Protezione accesso Web	✓	✓	✓
HIPS (compresa la Protezione ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Network Inspector		✓	✓
Protezione webcam		✓	✓
Protezione contro gli attacchi di rete		✓	✓
Protezione Botnet		✓	✓
Protezione pagamenti bancari		✓	✓
Controllo accessi		✓	✓
Anti-Furto		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Downgrade prodotto

Il prodotto attualmente installato presenta più funzioni di protezione di quello che si sta per attivare.

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

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Motore di rilevamento	✓	✓	✓
Apprendimento automatico avanzato	✓	✓	✓
Exploit Blocker	✓	✓	✓

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Protezione contro attacchi basati su script	✓	✓	✓
Anti-Phishing	✓	✓	✓
Protezione accesso Web	✓	✓	✓
HIPS (compresa la Protezione ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Network Inspector		✓	✓
Protezione webcam		✓	✓
Protezione contro gli attacchi di rete		✓	✓
Protezione Botnet		✓	✓
Protezione pagamenti bancari		✓	✓
Controllo accessi		✓	✓
Anti-Furto		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Strumento di individuazione e risoluzione dei problemi di installazione

Se si verificano problemi durante l'installazione, la procedura guidata di installazione offre uno strumento di individuazione e risoluzione dei problemi che, se possibile, consente di risolverli.

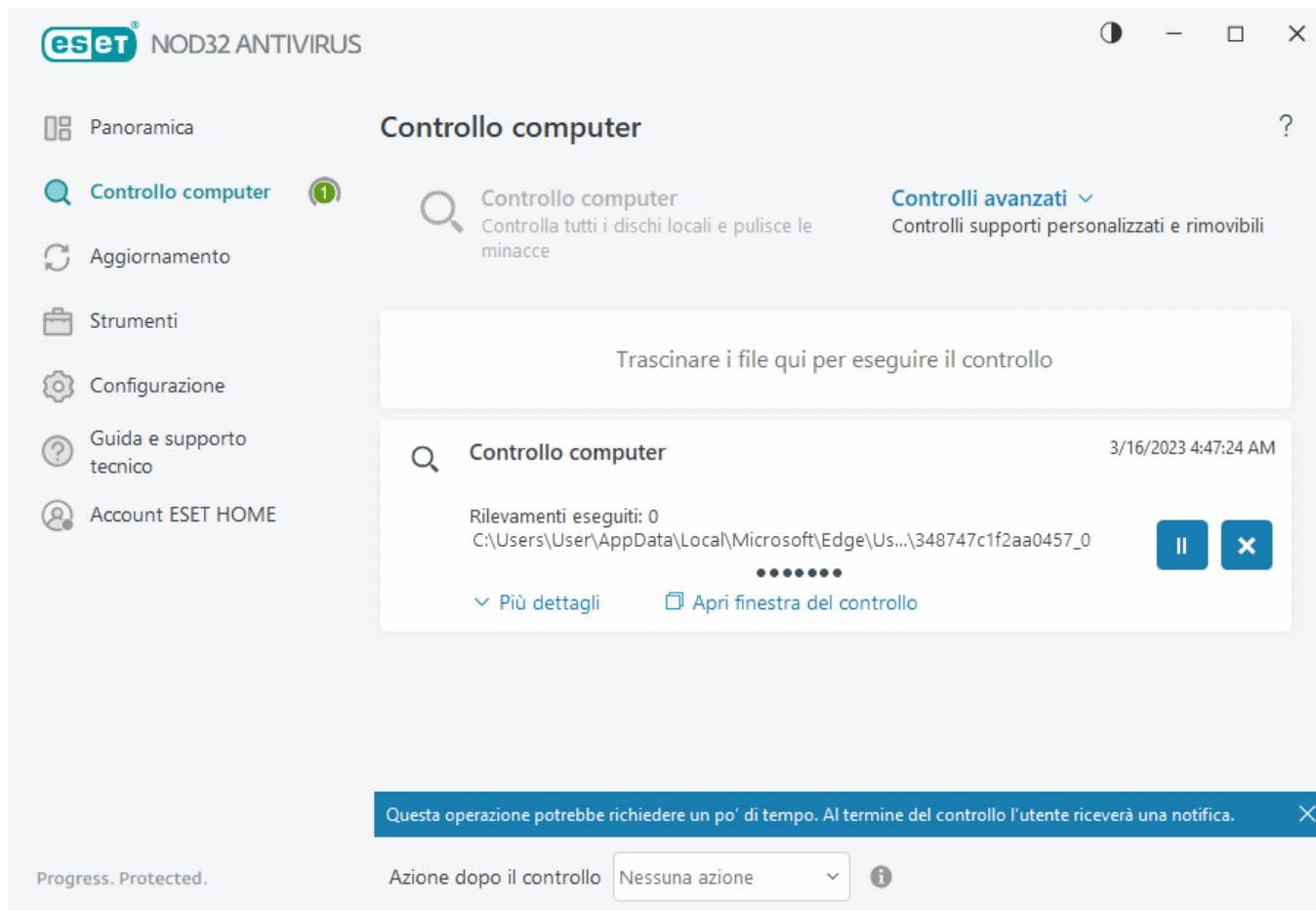
Fare clic su **Esegui strumento di individuazione e risoluzione dei problemi** per avviare la procedura di individuazione e risoluzione dei problemi. Al termine della procedura, seguire la soluzione consigliata.

Se il problema persiste, consultare l'elenco di [errori di installazione e risoluzioni comuni](#).

Primo controllo dopo l'installazione

Dopo aver installato ESET NOD32 Antivirus, verrà avviato automaticamente un controllo del computer 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](#) > **Controllo del computer** > **Controlla il computer in uso**. Per ulteriori informazioni sui controlli del computer, consultare [Controllo del computer](#).



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 successiva 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 subito dopo il rilascio, utilizzare uno dei metodi seguenti.

Assicurarsi di aver abilitato **Aggiornamenti delle funzionalità dell'applicazione** in **Configurazione avanzata** (F5) > **Aggiorna** > **Profili** > **Aggiornamenti**.

2. Manualmente nella [finestra principale del programma](#) facendo clic su **Ricerca aggiornamenti** nella sezione **Aggiorna**.

3. Manualmente scaricando e [installando una versione più recente](#) su quella precedente.

Per consultare ulteriori informazioni e le istruzioni illustrate, fare riferimento a:

- [Aggiornamento dei prodotti ESET: ricercare i moduli più aggiornati dei prodotti](#)
- [Quali sono i tipi di aggiornamento e le versioni dei prodotti ESET?](#)

Aggiornamento automatico prodotto legacy

La versione del prodotto ESET non è più supportata e il prodotto è stato aggiornato alla versione più recente.

[Problemi di installazione comuni](#)



Ciascuna nuova versione dei prodotti ESET presenta numerose correzioni di bug e miglioramenti. I clienti esistenti con una licenza valida per un prodotto ESET possono effettuare l'aggiornamento gratuito alla versione più recente dello stesso prodotto.

Per completare l'installazione:

1. Fare clic su **Accetto e continuo** per accettare l'[Accordo di licenza per l'utente finale](#) e confermare l'[Informativa sulla privacy](#). In caso di mancata accettazione dell'Accordo di licenza per l'utente finale, fare clic su **Disinstalla**. Non è possibile ripristinare la versione precedente.
2. Fare clic su **Consenti tutto e continua** per consentire sia il [sistema di feedback ESET LiveGrid®](#) sia il [Programma di miglioramento dell'esperienza degli utenti](#) oppure fare clic su **Continua** se non si desidera partecipare.
3. Dopo aver attivato il nuovo prodotto ESET con la chiave di licenza, comparirà la pagina iniziale. Se le informazioni sulla licenza non vengono trovate, continuare con una nuova licenza di prova. Se la licenza utilizzata nel prodotto precedente non è valida, [attivare il prodotto ESET](#).
4. Per completare l'installazione, è necessario riavviare il dispositivo.

Presentare un prodotto ESET a un amico

Questa versione di ESET NOD32 Antivirus prevede ora un programma di bonus di invito che consente agli utenti di condividere le proprie esperienze con i prodotti ESET con amici e parenti. Gli inviti potranno anche essere condivisi da un prodotto attivato con una licenza di prova. In tal caso, per ciascun invito andato a buon fine i cui risultati vengono inviati nell'attivazione di un prodotto, verrà offerta un'estensione della licenza di prova sia all'utente originale sia alla persona invitata.

È possibile effettuare la presentazione utilizzando il programma ESET NOD32 Antivirus installato. Il prodotto da presentare dipende da quello originale utilizzato per effettuare la presentazione. Per ulteriori informazioni, consultare la tabella sottostante.

Prodotto installato	Prodotto che è possibile presentare
ESET NOD32 Antivirus	ESET Internet Security
ESET Internet Security	ESET Internet Security
ESET Smart Security Premium	ESET Smart Security Premium

Presentazione di un prodotto

Per inviare un collegamento di invito, fare clic su **Invita un amico** nel menu principale di ESET NOD32 Antivirus. Fare clic su **Condividi collegamento di invito**. Il prodotto genera un collegamento di invito che compare in una nuova finestra. Copiare il collegamento e inviarlo ad amici e parenti. È possibile condividere il collegamento di

invito direttamente dal prodotto ESET, utilizzando le opzioni **Condividi su Facebook**, **Invita i tuoi contatti Gmail** e **Condividi su Twitter**.

Quando la persona invitata fa clic sul collegamento di invito inviato dall'utente, verrà reindirizzata a una pagina Web in cui potrà scaricare il prodotto e utilizzarlo per un altro mese di protezione GRATUITA. In qualità di titolare di una licenza di prova, l'utente riceverà una notifica per ciascun collegamento di invito attivato correttamente e la sua licenza verrà automaticamente estesa per un altro mese di protezione GRATUITA. In questo modo è possibile estendere GRATUITAMENTE la protezione fino a un massimo di 5 mesi. Per verificare il numero di collegamenti di inviti attivati con successo, utilizzare la finestra **Invita un amico** del prodotto ESET installato.

i La funzione di riferimento potrebbe non essere disponibile per la lingua in uso o la regione di utilizzo.

Sarà installato ESET NOD32 Antivirus

Questa finestra di dialogo può essere visualizzata:

- Durante il processo di installazione: fare clic su **Continua** per installare ESET NOD32 Antivirus.
- Quando si modifica una licenza in ESET NOD32 Antivirus: fare clic su **Attiva** per modificare la licenza e attivare ESET NOD32 Antivirus.

L'opzione **Cambia prodotto** consente all'utente di scegliere i vari prodotti ESET Windows Home in base alla licenza ESET in suo possesso. Per ulteriori informazioni, consultare [Qual è il mio prodotto?](#).

Passaggio a una linea di prodotti diversa

È possibile scegliere i vari prodotti ESET Windows Home in base alla licenza ESET in possesso. Per ulteriori informazioni, consultare [Qual è il mio prodotto?](#).

Registrazione

Registrare la licenza compilando i campi contenuti nel modulo di registrazione e facendo clic su Attiva. I campi contrassegnati come obbligatori tra parentesi devono essere necessariamente completati. Queste informazioni verranno utilizzate esclusivamente per motivi legati alla licenza ESET.

Avanzamento attivazione

Attendere qualche secondo per il completamento del processo di attivazione (il tempo richiesto varia in base alla velocità della connessione Internet o al computer).

Attivazione avvenuta con successo

Il processo di attivazione è completo.

Tra qualche secondo si avvierà un aggiornamento del modulo. Gli aggiornamenti periodici di ESET NOD32 Antivirus saranno avviati immediatamente.

Un controllo iniziale si avvia automaticamente entro 20 minuti dall'aggiornamento del modulo.

Guida introduttiva

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

La finestra principale del programma

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

Istruzioni illustrate

i Per consultare le istruzioni illustrate disponibili in lingua inglese e in molte altre lingue, consultare [Aprire la finestra principale del programma dei prodotti ESET Windows](#).

È possibile selezionare la combinazione di colori dell'interfaccia utente grafica (Graphical User Interface, GUI) di ESET NOD32 Antivirus nell'angolo in alto a destra della finestra principale del programma. Fare clic sull'icona **Combinazione di colori** (l'icona cambia in base alla combinazione di colori attualmente selezionata) accanto all'icona **Riduci a icona** e selezionare la combinazione di colori dal menu a discesa:

- **Uguale al colore del sistema:** consente di impostare la combinazione di colori di ESET NOD32 Antivirus in base alle impostazioni del sistema operativo in uso.
- **Scuro:** ESET NOD32 Antivirus avrà una combinazione di colori scuri (modalità scura).
- **Chiaro:** ESET NOD32 Antivirus avrà una combinazione di colori chiari e standard.

Opzioni principali del menu:

[Panoramica](#): 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.


[Aggiornamento](#): consente di visualizzare informazioni relative agli aggiornamenti del modulo e del motore di rilevamento.

[Strumenti](#): consente di accedere a funzioni che permettono di semplificare l'amministrazione del programma, offrendo opzioni aggiuntive per gli utenti esperti.

[Configurazione](#): offre opzioni di configurazione per le funzioni di protezione di ESET NOD32 Antivirus (Protezione computer e protezione Internet) e l'accesso alla Configurazione avanzata.

[Guida e supporto tecnico](#): consente di visualizzare informazioni sulla licenza, sul prodotto ESET installato e sui collegamenti alla [Guida online](#), alla [Knowledge Base di ESET](#) e al [Supporto tecnico](#).

Account [ESET HOME](#): [consente di connettere il dispositivo a ESET HOME](#) o di consultare lo stato di connessione dell'account ESET HOME. Utilizzare [ESET HOME](#) per visualizzare e gestire le licenze e i dispositivi ESET attivati.

 Per modificare la combinazione di colori dell'interfaccia utente grafica di ESET NOD32 Antivirus, consultare [Elementi dell'interfaccia utente](#).

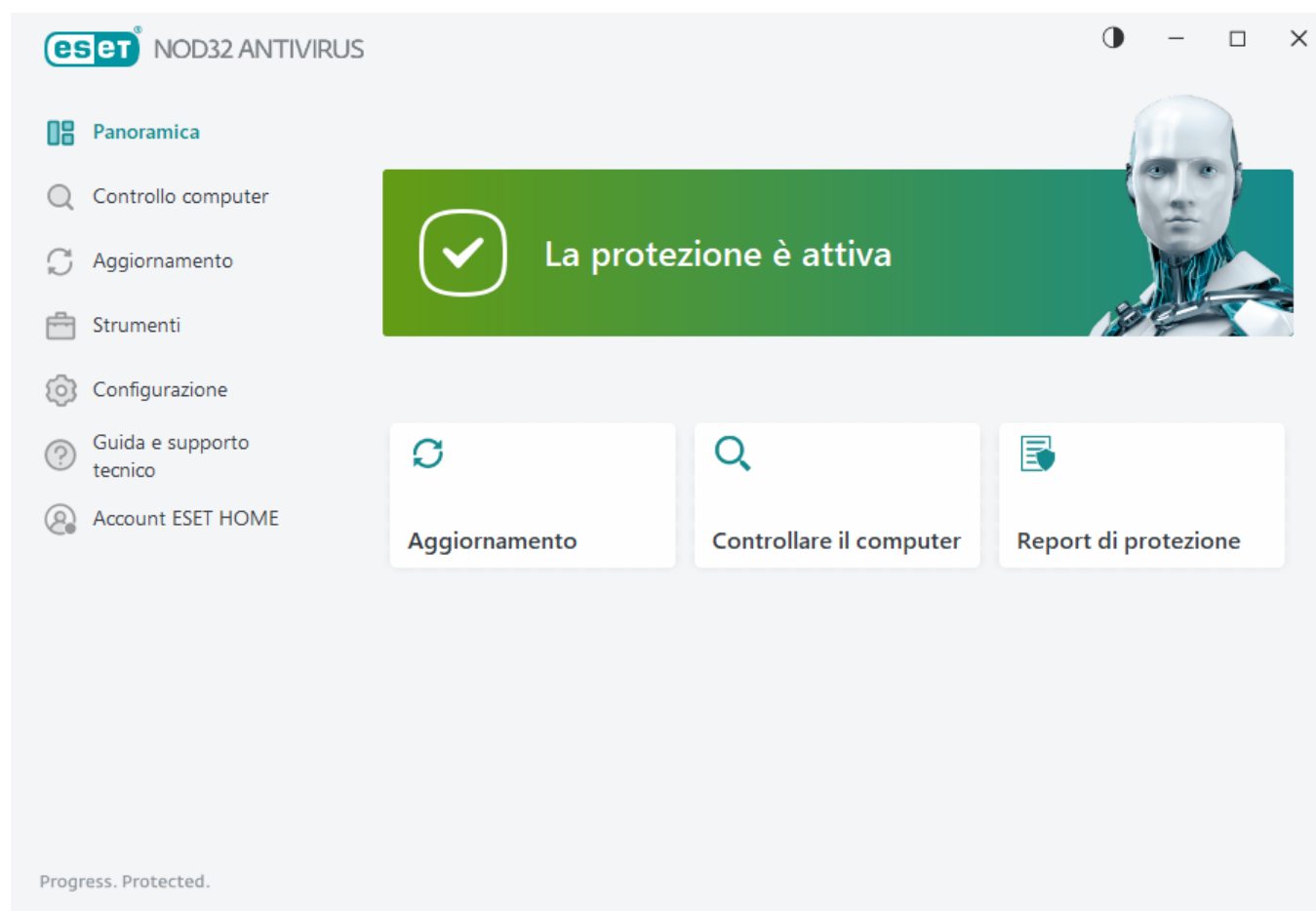
La finestra **Panoramica** consente di visualizzare informazioni sulla protezione attuale del computer, insieme a collegamenti rapidi alle funzioni di protezione in ESET NOD32 Antivirus.

La finestra **Panoramica** consente di visualizzare [notifiche](#) con informazioni dettagliate e soluzioni consigliate per migliorare la sicurezza di ESET NOD32 Antivirus, attivare funzioni aggiuntive o garantire la massima protezione. In presenza di più notifiche, fare clic su **X altre notifiche** per espanderle tutte.

Aggiornamento: consente di aprire la pagina [Aggiornamento](#) e di ricercare gli aggiornamenti.

Controlla computer in uso: consente di aprire la pagina [Controllo computer](#) e di avviare un [controllo del computer standard](#).

Report di protezione: consente di aprire il [Report di protezione](#).

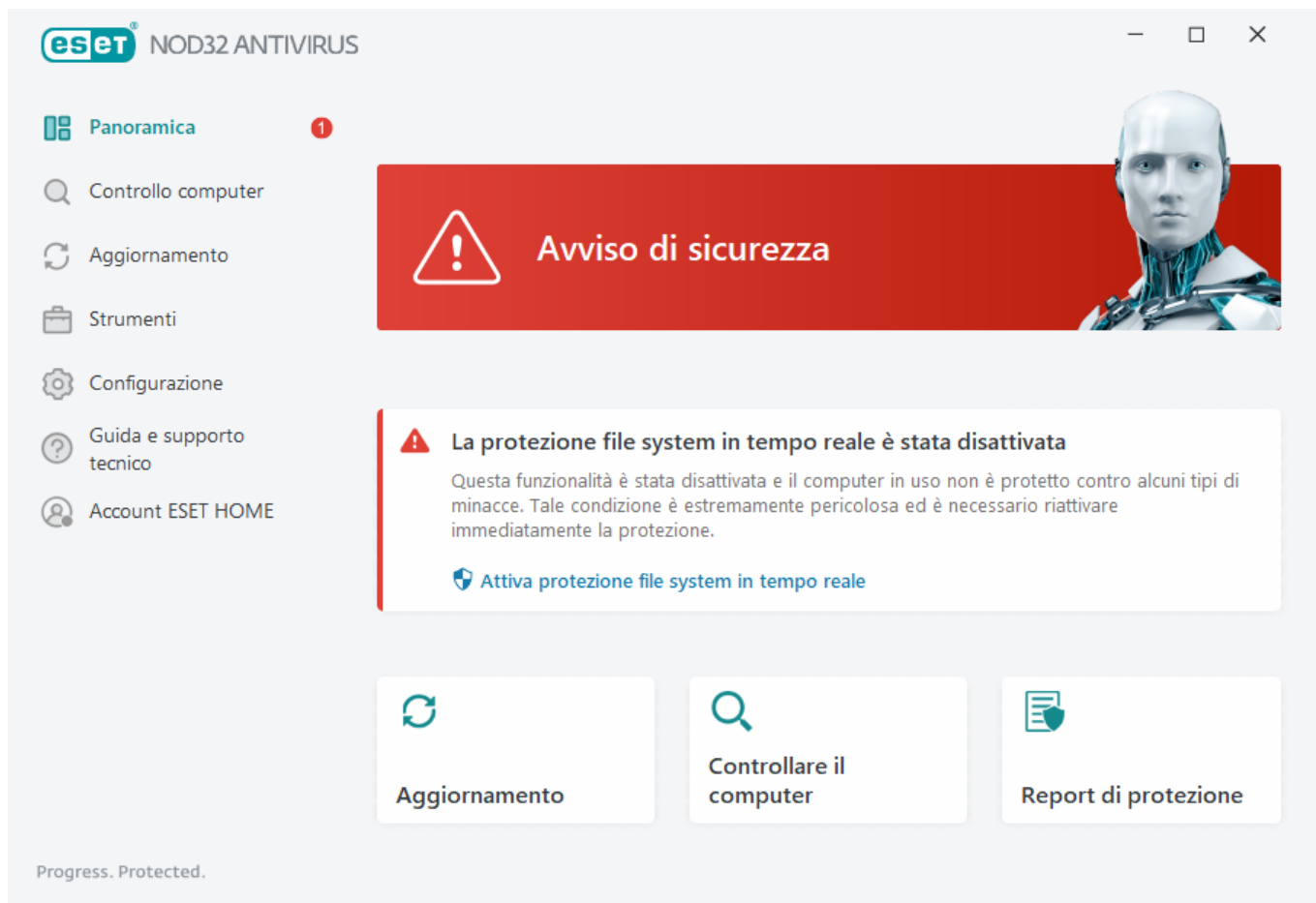


L'icona verde e il colore verde dello stato **Protezione attiva** indicano un livello di protezione massimo.

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. Nella finestra **Panoramica** verranno visualizzate come [notifica](#) 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 lo stato rosso dell'**Avviso di sicurezza** indicano problemi critici.

Esistono vari motivi alla base della visualizzazione di questo stato, tra cui:

- **Prodotto non attivato o 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.
- **Il motore di rilevamento è obsoleto:** questo errore viene visualizzato dopo diversi tentativi non riusciti di aggiornamento del motore di rilevamento. Si consiglia di controllare le impostazioni di aggiornamento. Spesso questo errore viene visualizzato perché i [dati di autenticazione](#) non vengono immessi correttamente o le [impostazioni di connessione](#) sono errate.
- **La protezione file system in tempo reale è stata disabilitata:** la protezione in tempo reale è stata disabilitata dall'utente. Il computer non è protetto contro le minacce. Fare clic su **Attiva protezione file system in tempo reale** per riabilitare questa funzionalità.
- **Protezione antivirus e antispyware disattivata:** è possibile riattivare la protezione antivirus e antispyware facendo clic su **Attiva protezione antivirus e antispyware**.



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'abilitazione di questa funzione determina la disabilitazione di tutte le finestre di notifica/avviso e l'interruzione di eventuali attività pianificate.
- **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.

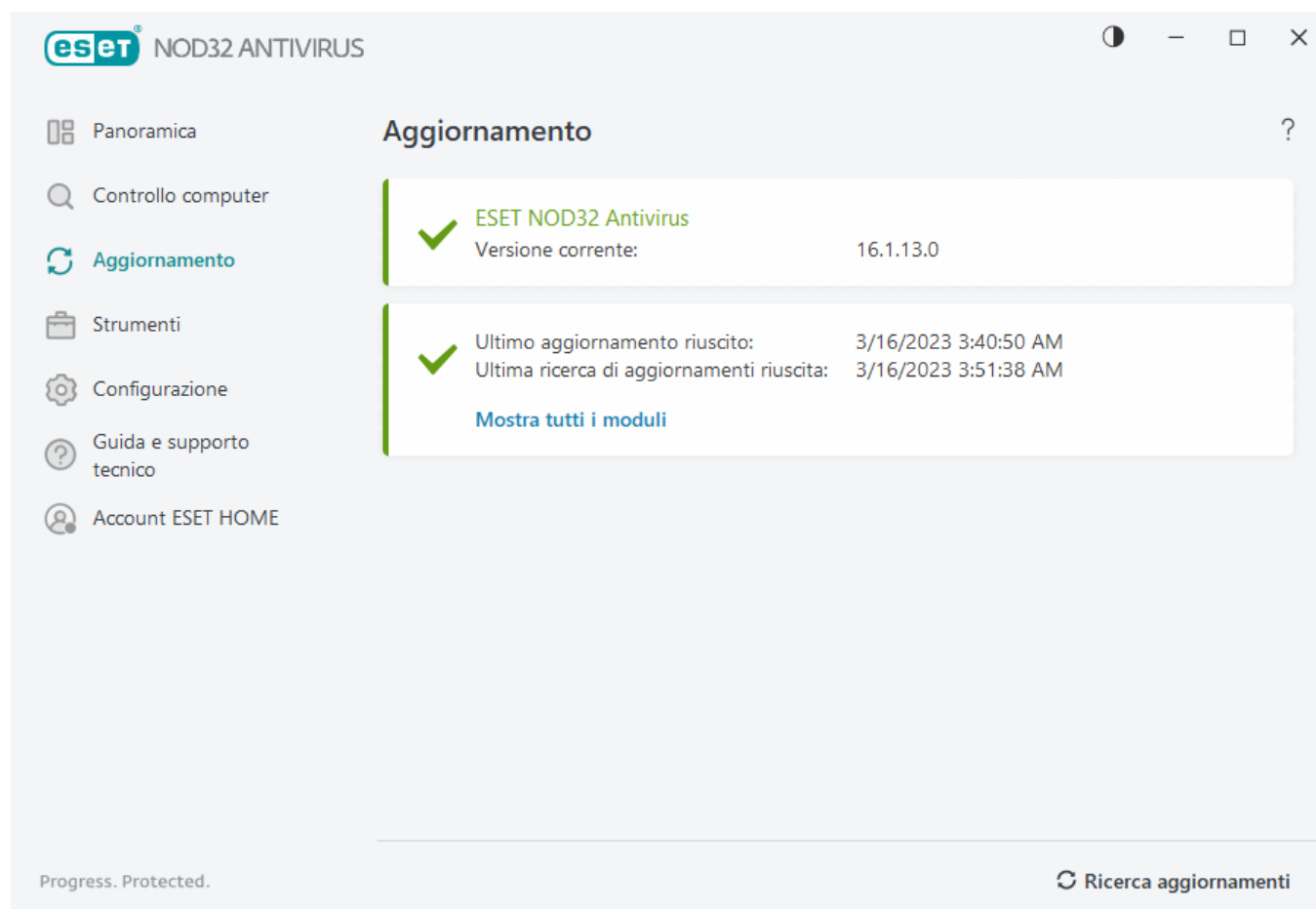
Qualora non si riuscisse a risolvere un problema ricorrendo alle soluzioni consigliate, fare clic su **Guida e supporto tecnico** per accedere ai file della Guida oppure effettuare una ricerca nella [Knowledge Base di ESET](#). Per ulteriore assistenza, è possibile inviare una richiesta di supporto.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

Aggiornamenti

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.

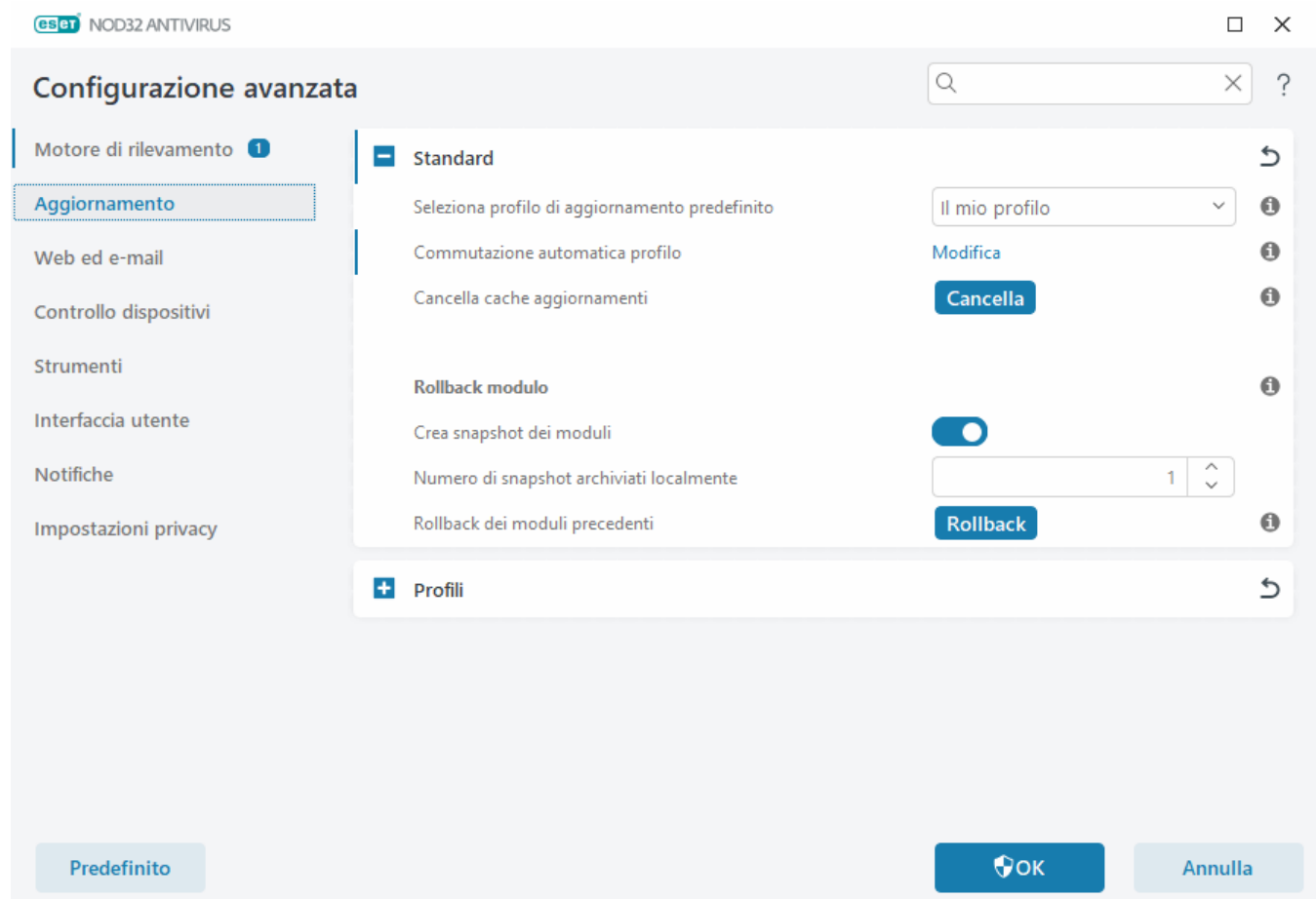
Facendo clic su **Aggiornamento** nella [finestra principale del programma](#), è possibile visualizzare lo stato corrente degli aggiornamenti, comprese la data e l'ora dell'ultimo aggiornamento eseguito correttamente, e valutare l'eventuale necessità di un aggiornamento.

Oltre agli aggiornamenti automatici, è possibile fare clic su **Cerca aggiornamenti** per attivare un aggiornamento manuale.



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 su **Aggiorna** nella struttura Configurazione avanzata.

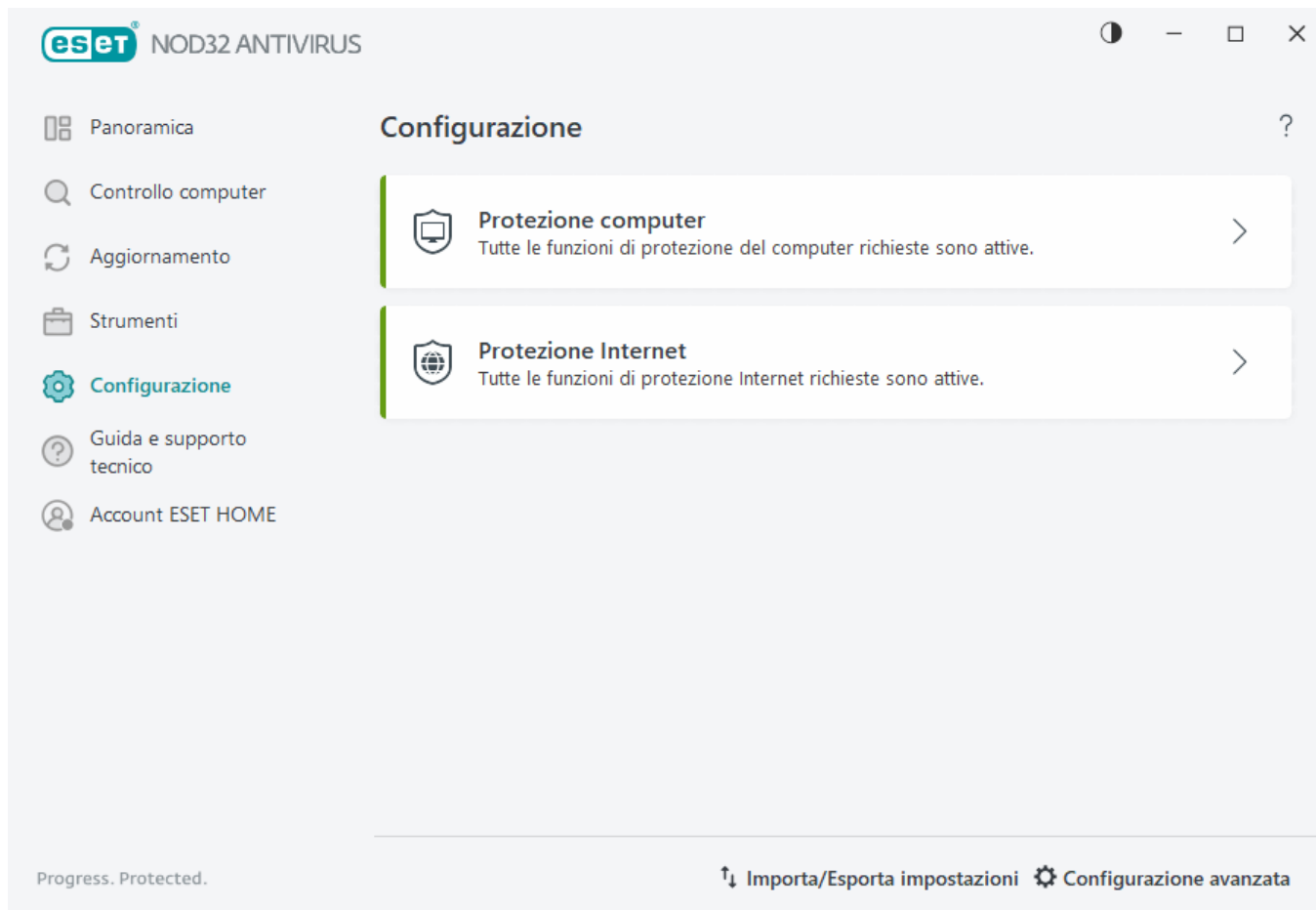
In caso di problemi con un aggiornamento, fare clic su **Cancella** per eliminare la cache dell'aggiornamento. Se non è ancora possibile aggiornare i moduli del programma, consultare la sezione [Risoluzione dei problemi relativi al messaggio "Aggiornamento moduli non riuscito"](#).



Utilizzo di ESET NOD32 Antivirus

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

i Consultare [Finestra principale del programma](#) per una spiegazione della pagina **Descrizione generale**.



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



Protezione del 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.
- **Controllo dispositivi:** questo modulo consente di controllare, bloccare o regolare l'estensione dei filtri o delle autorizzazioni e di selezionare le modalità di accesso e di utilizzo di un dato dispositivo (CD/DVD/USB...) da parte dell'utente.
- **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(S) e IMAP(S).
- **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 . Il componente di protezione abilitato presenta l'icona di un pulsante verde .

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.


Protezione del computer


Fare clic su **Protezione computer** nella finestra **Configurazione** per visualizzare una panoramica di tutti i moduli di protezione:

- [Protezione file system in tempo reale](#)
- [Controllo dispositivo](#)
- [Host Intrusion Prevention System \(HIPS\)](#)
- [Modalità giocatore](#)

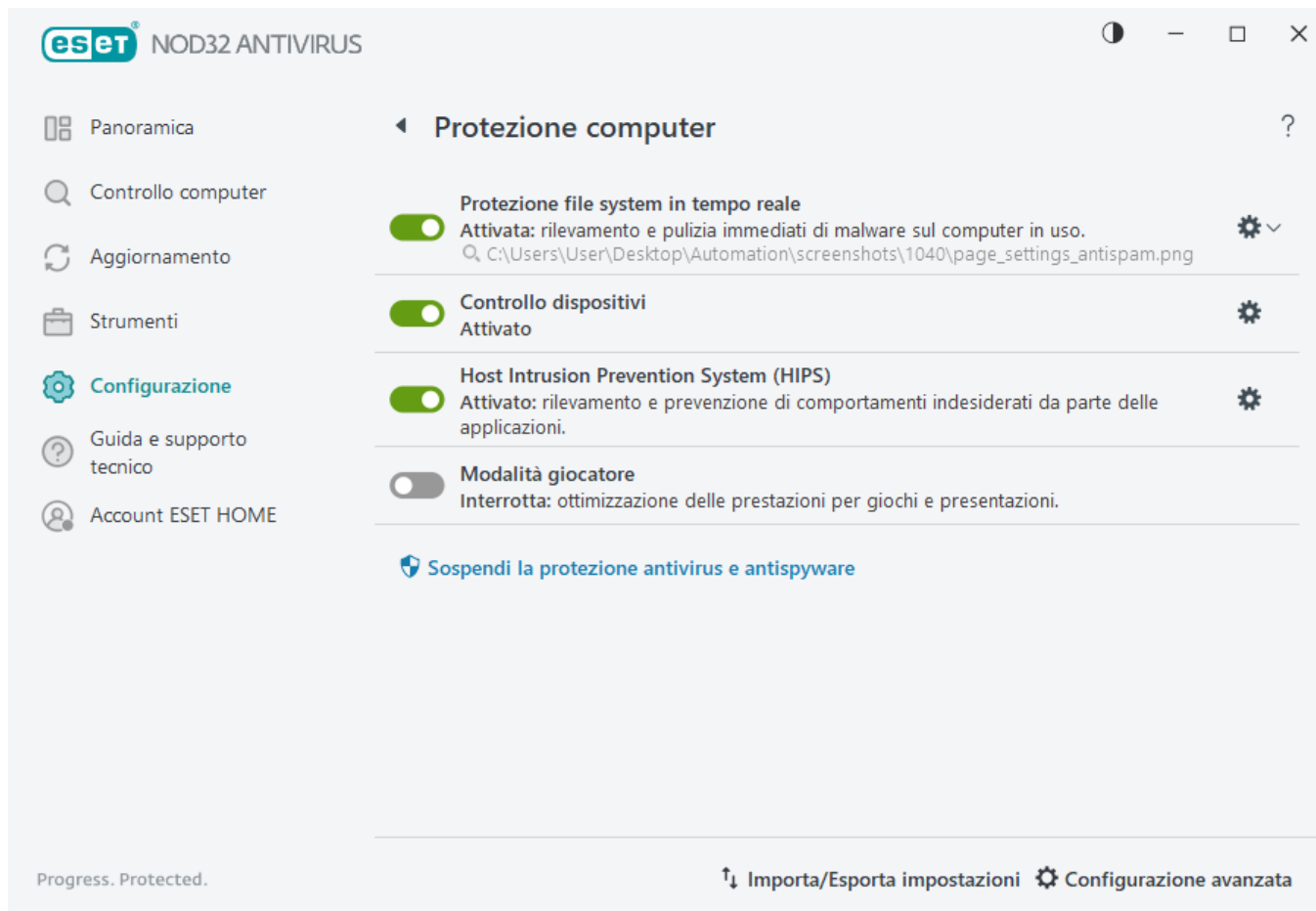
Per sospendere o disabilitare singoli moduli di protezione, fare clic sull'icona della barra di scorrimento .

 La disattivazione dei moduli di protezione potrebbe ridurre il livello di protezione del computer.

Fare clic sull'icona a forma di ingranaggio  accanto a un modulo di protezione per accedere alle relative impostazioni avanzate.

Per la **Protezione file system in tempo reale**, fare clic sull'icona a forma di ingranaggio  e scegliere una delle seguenti opzioni:

- **Configura:** consente di aprire la configurazione avanzata della protezione file system in tempo reale.
- **Modifica esclusioni:** consente di aprire la [finestra di configurazione delle esclusioni](#) in modo da poter escludere file e cartelle dal controllo.



Sospendi protezione antivirus e antispyware: consente di disabilitare tutti i moduli di protezione antivirus e antispyware. Disabilitando la protezione, si aprirà una finestra per determinare per quanto tempo la protezione verrà disabilitata utilizzando il menu a discesa **Intervallo di tempo**. Utilizzare questa opzione solo se si è utenti esperti o se sono state ricevute istruzioni dal Supporto tecnico di ESET.

Motore di rilevamento

Il motore di rilevamento protegge dagli attacchi dannosi al sistema controllando file, e-mail e comunicazioni Internet. Ad esempio, se viene rilevato un oggetto classificato come malware, si avvia la correzione. Il motore di rilevamento può eliminarlo prima bloccandolo e poi pulendolo, rimuovendolo o spostandolo in quarantena.

Per configurare nei dettagli le impostazioni del motore di rilevamento, fare clic su **Configurazione avanzata** oppure premere **F5**.



Le modifiche apportate alle impostazioni del motore di rilevamento devono essere eseguite solo da utenti esperti. Una configurazione non corretta delle impostazioni può causare una riduzione del livello di protezione.

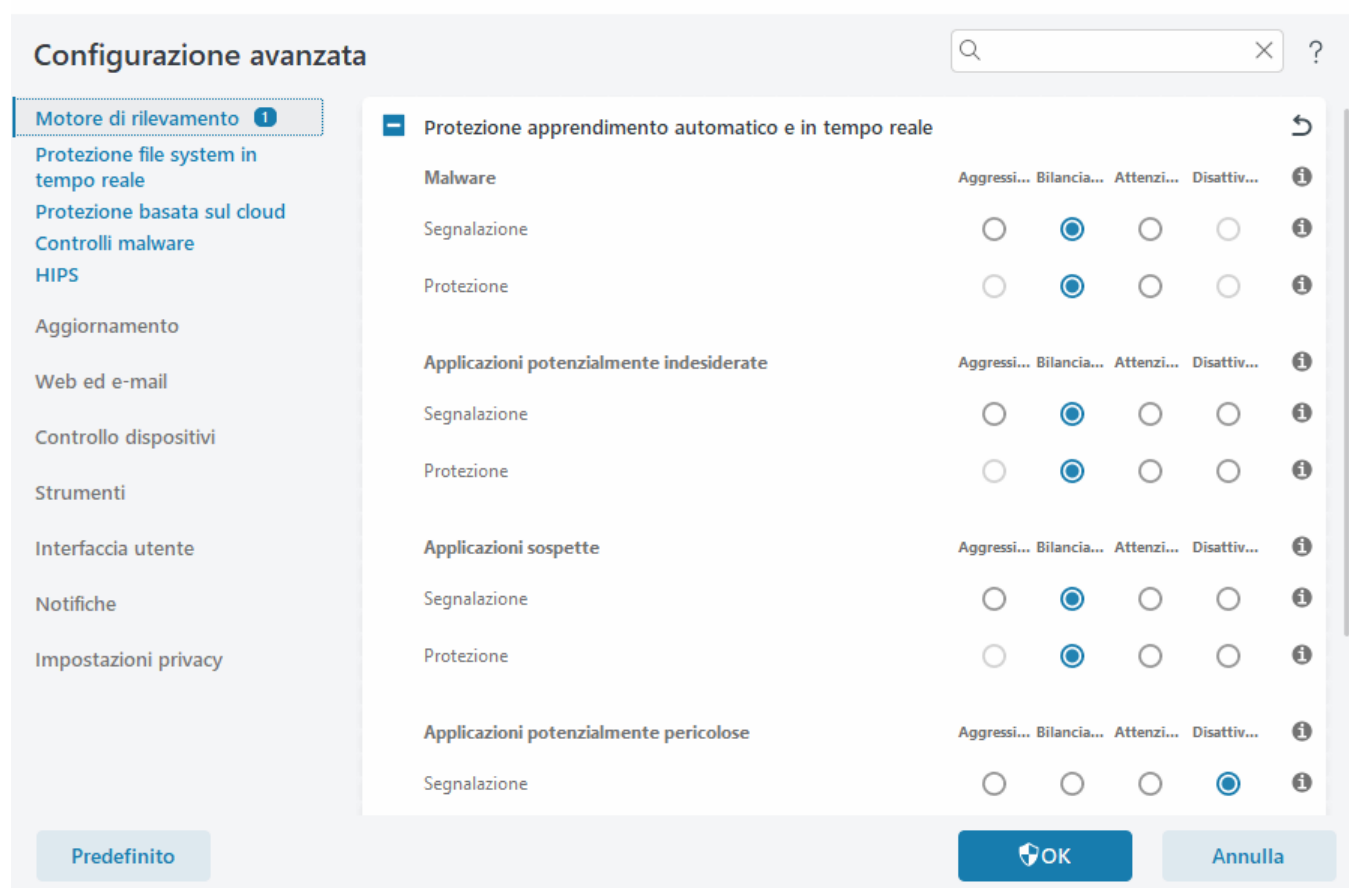
In questa sezione:

- [Categorie Protezione apprendimento automatico e in tempo reale](#)
- [Controlli malware](#)
- [Configurazione della segnalazione](#)

Categorie Protezione apprendimento automatico e in tempo reale

La **protezione apprendimento automatico e in tempo reale** per tutti i moduli di protezione (ad esempio protezione file system in tempo reale, protezione accesso web, ecc.) consente all'utente di configurare la segnalazione e i livelli di protezione delle seguenti categorie:

- **Malware:** un virus è un frammento di codice dannoso anteposto o allegato ai file esistenti sul computer. Tuttavia, il termine "virus" è spesso utilizzato in modo non consono. Il "malware" (software dannoso) rappresenta un termine più accurato. Il rilevamento malware viene eseguito dal modulo del motore di rilevamento insieme al componente apprendimento automatico. Ulteriori informazioni su questi tipi di applicazioni sono disponibili nel [Glossario](#).
- **Applicazioni potenzialmente indesiderate:** Grayware o applicazione potenzialmente indesiderata ("Potentially Unwanted Application", PUA) indica una vasta categoria di software, il cui intento non è inequivocabilmente dannoso come quello di altri tipi di malware, tra cui virus o trojan horse. Questo strumento potrebbe tuttavia installare software indesiderati aggiuntivi, modificare il comportamento di un dispositivo digitale o eseguire attività non autorizzate o inattese dall'utente. Ulteriori informazioni su questi tipi di applicazioni sono disponibili nel [Glossario](#).
- **Applicazioni sospette:** includono programmi compressi con [packer](#) o programmi di protezione. Questi tipi di programmi di protezione sono spesso utilizzati dagli autori di malware per eludere i rilevamenti.
- **Applicazioni potenzialmente pericolose:** software commerciali legittimi che potrebbero essere utilizzati in modo non conforme per scopi illegittimi. Esempi di applicazioni potenzialmente pericolose (PUA) sono strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano ciascuna battuta digitata da un utente). Ulteriori informazioni su questi tipi di applicazioni sono disponibili nel [Glossario](#).



Miglioramento della protezione



L'apprendimento automatico avanzato fa ora parte del motore di rilevamento come un livello avanzato di protezione che consente di migliorare il rilevamento in base all'apprendimento automatico. Maggiori informazioni su questo tipo di protezione sono disponibili nel [glossario](#).

Controlli malware

Le impostazioni dello scanner possono essere configurate separatamente per il controllo in tempo reale e il [controllo su richiesta](#). Per impostazione predefinita, è attivata l'opzione **Utilizza impostazioni della protezione in tempo reale**. Se l'opzione è attivata, le impostazioni del controllo su richiesta vengono ereditate dalla sezione **Protezione apprendimento automatico e in tempo reale**. Per ulteriori informazioni, consultare [controlli malware](#).

Configurazione della segnalazione

Quando si verifica un rilevamento (ad esempio viene trovata una minaccia e classificata come malware), le informazioni sono registrate nel [Rapporto rilevamenti](#) e vengono inviate [Notifiche desktop](#) se configurate in ESET NOD32 Antivirus.

Per ogni categoria (a cui si fa riferimento come "CATEGORIA") viene configurata una soglia di segnalazione:

1. Malware

2.Applicazioni potenzialmente indesiderate

3.Potenzialmente pericolose

4.Applicazioni sospette

La segnalazione viene eseguita con il motore di rilevamento, compreso il componente dell'apprendimento automatico. È possibile impostare una soglia di segnalazione superiore rispetto alla soglia di [protezione](#) attuale. Tali impostazioni di segnalazione non influenzano il blocco, la [pulizia](#) o la rimozione di [oggetti](#).

Consultare quanto segue prima di modificare una soglia (o livello) di segnalazione CATEGORIA:

Soglia	Spiegazione
Aggressivo	Segnalazione CATEGORIA configurata sul livello di sensibilità massimo. Vengono segnalati altri rilevamenti. L'impostazione aggressiva consente di identificare erroneamente gli oggetti come CATEGORIA.
Bilanciato	Segnalazione CATEGORIA configurata come bilanciata. Questa impostazione è ottimizzata per bilanciare le prestazioni e l'accuratezza dei tassi di rilevamento e il numero di oggetti segnalati erroneamente.
Attenzione	Segnalazione CATEGORIA configurata per ridurre al minimo gli oggetti identificati erroneamente, mantenendo allo stesso tempo un livello di protezione sufficiente. Gli oggetti vengono segnalati solo in caso di evidenti probabilità e corrispondono al comportamento della CATEGORIA.
Disattivato	La segnalazione per la CATEGORIA non è attiva e i rilevamenti di questo tipo non vengono trovati, segnalati o puliti. Di conseguenza, questa impostazione disattiva la protezione da questo tipo di rilevamento. L'opzione "Disattivato" non è disponibile per la segnalazione di malware ed è il valore predefinito per le applicazioni potenzialmente pericolose.

✓ [Disponibilità dei moduli di protezione ESET NOD32 Antivirus](#)

La disponibilità (attivato o disattivato) di un modulo di protezione per una soglia CATEGORIA selezionata è la seguente:

	Aggressivo	Bilanciato	Attenzione	Disattivato**
Modulo di riconoscimento automatico avanzato*	✓ (modalità aggressiva)	✓ (modalità conservativa)	X	X
Modulo del motore di rilevamento	✓	✓	✓	X
Altri moduli di protezione	✓	✓	✓	X

* Disponibile in ESET NOD32 Antivirus versione 13.1 e successive.

** Non consigliato.

✓ [Determinazione della versione del prodotto, delle versioni dei moduli del programma e delle date delle build](#)

1. Fare clic su **Guida e supporto tecnico > Informazioni su ESET NOD32 Antivirus**.
2. Nella schermata **Informazioni su**, nella prima riga di testo è visualizzato il numero di versione del prodotto ESET in uso.
3. Fare clic su **Componenti installati** per visualizzare le informazioni relative a moduli specifici.

Principi di base

Di seguito vengono riportati alcuni principi di base da tener presenti durante la configurazione di una soglia

appropriata per l'ambiente:

- La soglia **Bilanciato** è la scelta consigliata per la maggior parte delle configurazioni.
- La soglia **Attenzione** rappresenta un livello comparabile di protezione dalle precedenti versioni di ESET NOD32 Antivirus (13.0 e precedenti). È la scelta consigliata per gli ambienti dove la priorità è focalizzata sul ridurre al minimo gli oggetti segnalati erroneamente da parte del software di protezione.
- Più alta è la soglia di segnalazione, più elevati saranno i tassi di rilevamento ma anche il numero di oggetti segnalati erroneamente.
- Da un punto di vista pratico, non si garantisce una percentuale di rilevamento del 100%, così come una possibilità dello 0% di evitare una classificazione non corretta degli oggetti puliti come malware.
- [Tenere aggiornati ESET NOD32 Antivirus e i relativi moduli](#) per ottimizzare il bilanciamento tra prestazioni e accuratezza dei tassi di rilevamento e del numero di oggetti segnalati erroneamente.

Configurazione della protezione

Se viene segnalato un oggetto classificato come CATEGORIA, il programma blocca l'oggetto e quindi lo [pulisce](#), rimuove o sposta nella [Quarantena](#).

Consultare quanto segue prima di modificare una soglia (o livello) di protezione CATEGORIA:

Soglia	Spiegazione
Aggressivo	I rilevamenti dei livelli di aggressività segnalati (o inferiori) vengono bloccati e viene avviata la correzione automatica (ad es. pulizia). Questa impostazione è consigliata nel caso in cui tutti gli endpoint siano stati controllati con impostazioni aggressive e gli oggetti segnalati erroneamente siano stati aggiunti alle esclusioni di rilevamento.
Bilanciato	I rilevamenti dei livelli di bilanciamento segnalati (o inferiori) vengono bloccati e viene avviata la correzione automatica (ad es. pulizia).
Attenzione	I rilevamenti di livello "attenzione" segnalati vengono bloccati e viene avviata la correzione automatica (ad es. pulizia).
Disattivato	Opzione utile per identificare ed escludere gli oggetti segnalati erroneamente. L'opzione "Disattivato" non è disponibile per la protezione da malware ed è il valore predefinito per le applicazioni potenzialmente pericolose.

✓ [Tabella di conversione per ESET NOD32 Antivirus 13.0 e versioni precedenti](#)

Quando si passa dalle versioni 13.0 e precedenti alla versione 13.1 e successive, lo stato della nuova soglia sarà il seguente:

Pulsante categoria prima dell'aggiornamento		
Nuova soglia CATEGORIA dopo l'aggiornamento	Bilanciato	Disattivato

Opzioni avanzate del motore di rilevamento

Abilita controllo avanzato tramite AMSI è lo strumento dell'interfaccia di controllo anti-malware di Microsoft che consente di controllare gli script PowerShell, gli script eseguiti da Windows Script Host e i dati controllati

mediante AMSI SDK.

Rilevamento di un'infiltrazione

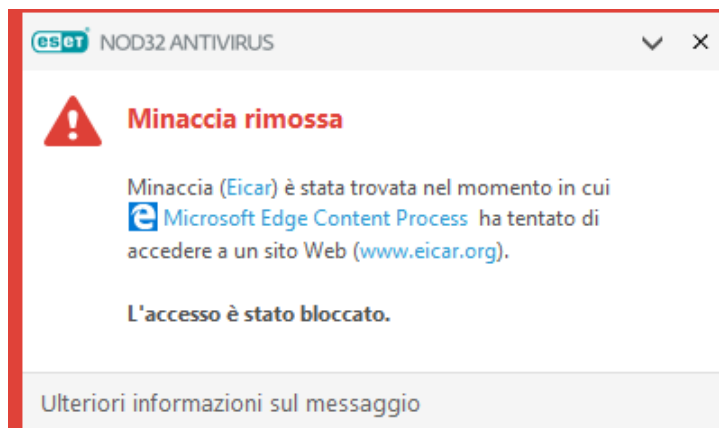
Le infiltrazioni possono raggiungere il sistema da diversi accessi, ad esempio [pagine Web](#), cartelle condivise, messaggi e-mail o [dispositivi rimovibili](#) (USB, dischi esterni, CD, DVD, dischetti e così via).

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 sugli oggetti rilevati/puliti, consultare [File di rapporto](#). Per ulteriori informazioni sui livelli di pulizia e sul comportamento, consultare [Livello di pulizia](#).



Controllo del computer per i file infetti

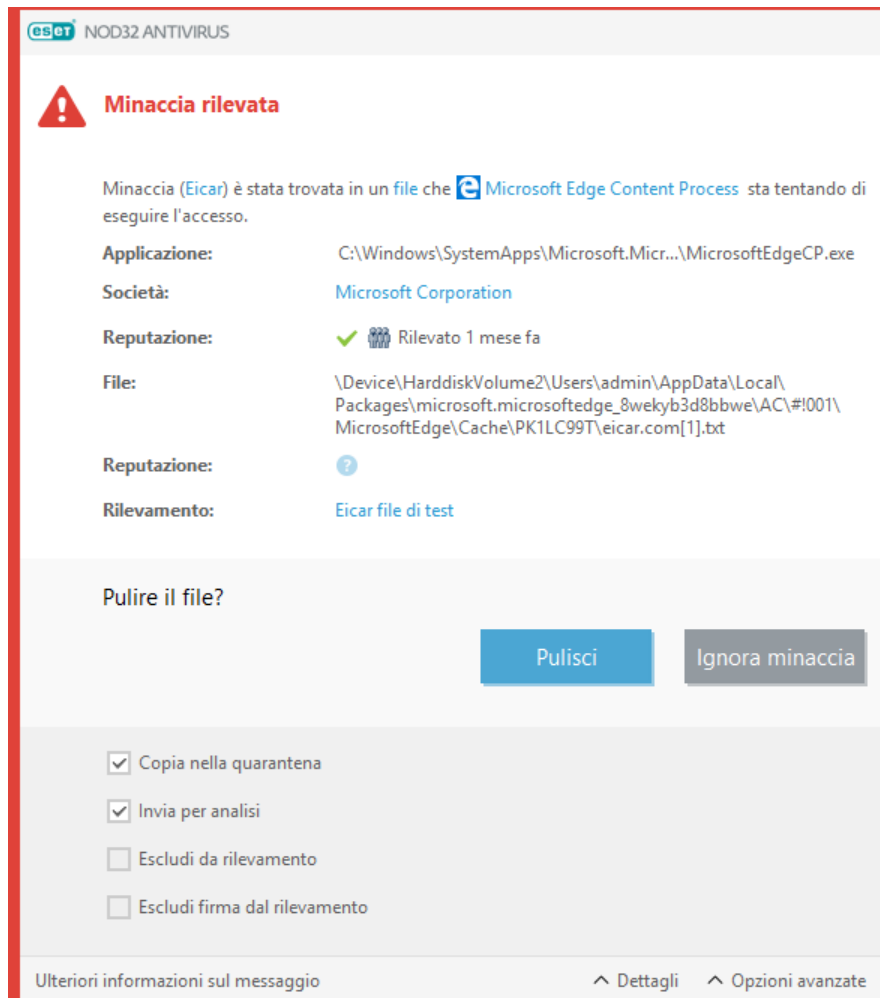
Se il computer mostra segnali di infezione malware, ad esempio appare più lento, si blocca spesso e così via, è consigliabile attenersi alle seguenti istruzioni:

1. Aprire ESET NOD32 Antivirus e fare clic su **Controllo del computer**.
2. Fare clic su **Controlla il computer in uso** (per ulteriori informazioni, consultare il paragrafo [Controllo del computer](#)).
3. Al termine del controllo, analizzare nel registro il numero di file sottoposti a controllo, 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.

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).

Ripristino dalla quarantena

È possibile accedere alla quarantena dalla [finestra principale del programma](#) ESET NOD32 Antivirus facendo clic su **Strumenti > Quarantena**.

I file messi in quarantena possono anche essere ripristinati nella posizione originale:

- A tale scopo, utilizzare la funzione di **Ripristino**, disponibile nel menu contestuale facendo clic con il pulsante destro del mouse su un determinato file nella quarantena.

- Se un file è contrassegnato come [applicazione potenzialmente indesiderata](#), l'opzione **Ripristina ed escludi dal controllo** è abilitata. Consultare anche [Esclusioni](#).
- Il menu contestuale offre anche l'opzione **Ripristina in**, che consente all'utente di ripristinare un file in un percorso diverso da quello in cui è stato rimosso.
- In alcuni casi, ad esempio, la funzionalità di ripristino non è disponibile per i file posizionati in una condivisione di rete di sola lettura.

Minacce multiple

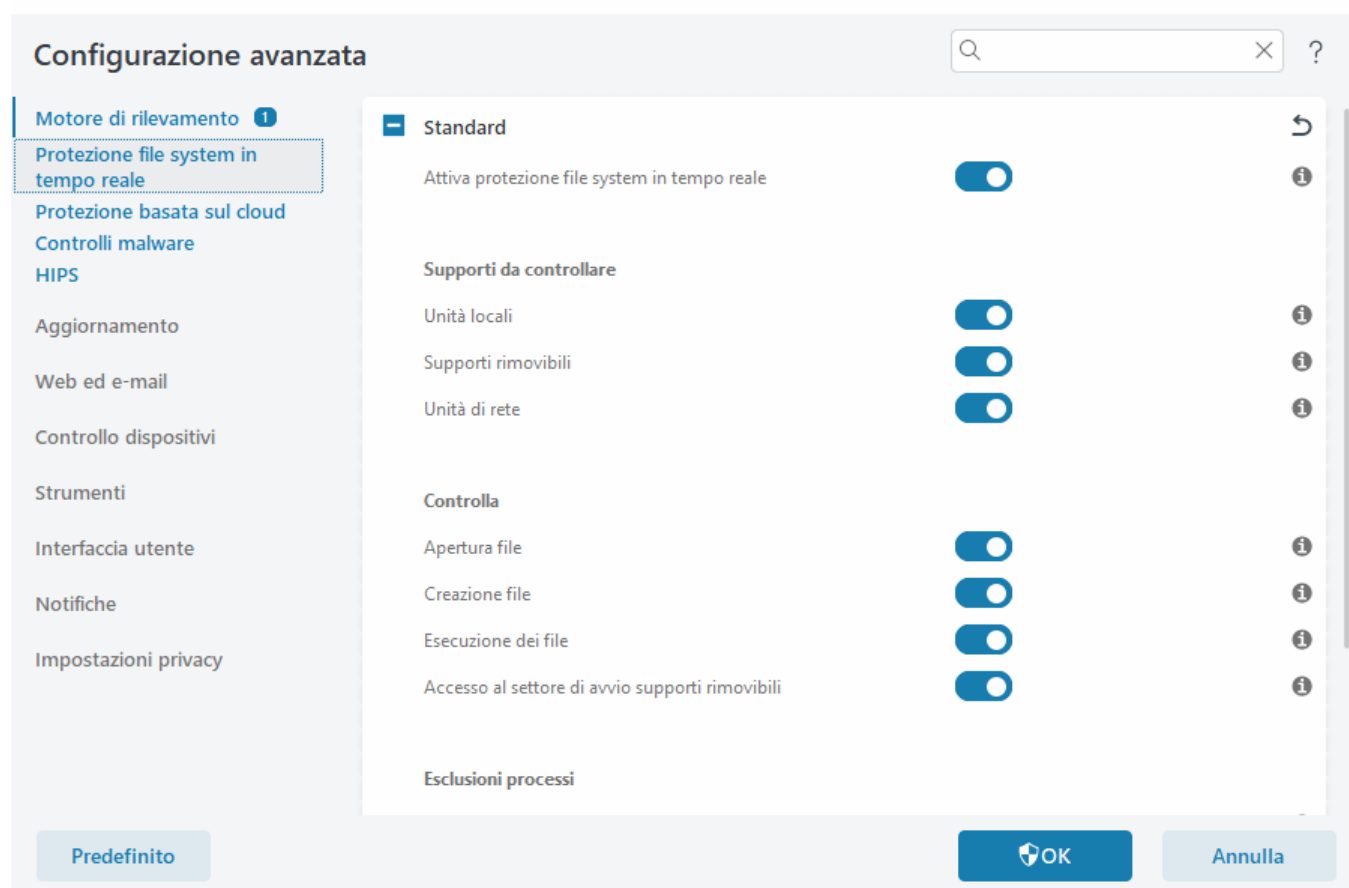
Se durante un controllo del computer i file infetti non sono stati puliti (o se il [Livello di pulizia](#) era impostato su **Nessuna pulizia**), viene visualizzata una finestra di avviso che richiede di selezionare le azioni per i file in questione. Selezionare le azioni da eseguire sui file (le azioni 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.

Protezione file system in tempo reale

La Protezione file system in tempo reale controlla tutti i file nel sistema alla ricerca di codice dannoso quando vengono aperti, creati o eseguiti.



Per impostazione predefinita, la Protezione file system in tempo reale viene avviata all'avvio del sistema e fornisce un controllo ininterrotto. Si sconsiglia di disabilitare **Attiva protezione file system in tempo reale** in **Configurazione avanzata** in **Motore di rilevamento** > **Protezione file system in tempo reale** > **Di base**.

Supporti da controllare

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

- **Unità locali:** controllo di tutti i dischi rigidi fissi e di sistema (ad esempio: *C:*, *D:*).
- **Supporti rimovibili:** controllo di CD/DVD, supporti di archiviazione USB, schede di memoria, ecc.
- **Unità di rete:** controllo di tutte le unità di rete mappate (ad esempio: *H:* come *\\store04*) o unità di rete ad accesso diretto (ad esempio: *\\store08*).

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, della creazione o dell'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 file:** controllo all'apertura di un file.

- **Creazione file:** controllo di un file creato o modificato.
- **Esecuzione dei file:** controllo durante l'esecuzione di un file.
- **Accesso settore di avvio dei supporti rimovibili:** quando un supporto rimovibile contenente un settore di avvio viene inserito nel dispositivo, il settore di avvio viene immediatamente controllato. Questa opzione non abilita il controllo dei file dei supporti rimovibili. Il controllo dei file dei supporti rimovibili è disponibile in **Supporti da controllare > Supporti rimovibili**. Per un corretto funzionamento di **Accesso settore di avvio dei supporti rimovibili**, mantenere l'opzione **Settori di avvio/UEFI** abilitata nei parametri ThreatSense.

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 **Motore di rilevamento > Protezione file system in tempo reale**. Fare clic su **parametro ThreatSense > Altro** e selezionare o deselezionare **Attiva ottimizzazione intelligente**.

Livelli di pulizia

Per accedere alle impostazioni dei livelli di pulizia di un modulo di protezione desiderato, espandere **Parametri ThreatSense** (ad esempio, **Protezione file system in tempo reale**), quindi individuare **Pulizia > Livello di pulizia**.

I parametri di ThreatSense presentano i seguenti livelli di correzione (ad es. pulizia).


Correzione in ESET NOD32 Antivirus

Livello di pulizia	Descrizione
Correggi sempre l'infezione	Tentativo di correzione del rilevamento durante la pulizia degli oggetti senza alcun intervento da parte dell'utente finale. In alcuni rari casi (ad esempio, file di sistema), se il rilevamento non può essere corretto, l'oggetto segnalato viene lasciato nella posizione originale.
Correggi infezione se l'operazione è sicura, altrimenti mantieni	Tentativo di correzione del rilevamento durante la pulizia degli oggetti senza alcun intervento da parte dell'utente finale. In alcuni casi (ad esempio, file di sistema o archivi con file puliti e infetti), se non è possibile correggere un rilevamento, l'oggetto segnalato viene lasciato nella posizione originale.
Correggi l'infezione se l'operazione è sicura, altrimenti chiedi	Tentativo di correzione del rilevamento durante la pulizia degli oggetti. In alcuni casi, se non è possibile eseguire alcuna azione, l'utente finale riceve un avviso interattivo e deve selezionare un'azione correttiva (ad esempio, Elimina o Ignora). Questa impostazione è consigliata nella maggior parte dei casi.

Livello di pulizia	Descrizione
Chiedi sempre all'utente finale	L'utente finale visualizza una finestra interattiva durante la pulizia degli oggetti e deve selezionare un'azione di correzione (p. es., Rimuovi o Ignora). Questo livello è stato pensato per gli utenti più avanzati che conoscono la procedura da adottare in caso di rilevamento.

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

Controllo della protezione in tempo reale

Per verificare che la protezione in tempo reale funzioni e sia in grado di rilevare virus, utilizzare il file di test *www.eicar.com*. Questo file di test è un file innocuo, speciale, 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.

Il file può essere scaricato qui <http://www.eicar.org/download/eicar.com>

Dopo aver digitato questo URL nel browser dovrebbe essere visualizzato un messaggio che informa che la minaccia è stata rimossa.

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 un utente disabilita inavvertitamente la protezione in tempo reale, è necessario riattivare la funzione. Per riattivare la protezione in tempo reale portarsi in **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 **Attiva 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 **Motore di rilevamento > 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 avviata all'avvio del sistema (e l'opzione **Abilita protezione file system in tempo reale** è attivata), questa condizione potrebbe essere dovuta a conflitti con altri programmi. Per risolvere il problema, [creare un rapporto ESET SysInspector e inviarlo al Supporto tecnico di ESET per l'analisi](#).

Esclusioni processi

La funzione Esclusioni processi consente di escludere i processi delle applicazioni da Protezione file system in tempo reale. Per migliorare la velocità di backup, l'integrità dei processi e la disponibilità dei servizi, durante il backup vengono utilizzate alcune tecniche note perché causano conflitti con la protezione dal malware a livello di file. L'unico modo efficace per evitare entrambe le situazioni è disattivare il software anti-malware. Escludendo processi specifici (ad esempio quelli della soluzione di backup), tutte le operazioni sui file attribuite a tale processo verranno ignorate e considerate sicure, riducendo così al minimo le interferenze con il processo di backup. Si consiglia di prestare attenzione durante la creazione di esclusioni: uno strumento di backup che è stato escluso può accedere a file infetti senza attivare un avviso. Per tale motivo, le autorizzazioni estese sono consentite solo nel modulo di protezione in tempo reale.



Da non confondere con [Estensioni file esclusi](#), [Esclusioni HIPS](#), [Esclusioni da rilevamento](#) o [Esclusioni da prestazioni](#).

Le esclusioni dei processi aiutano a ridurre al minimo il rischio di potenziali conflitti e migliorano le prestazioni delle applicazioni escluse, con un effetto positivo sulle prestazioni complessive e sulla stabilità del sistema operativo. L'esclusione di un processo o di un'applicazione è un'esclusione del relativo file eseguibile (.exe).

È possibile aggiungere i file eseguibili nell'elenco dei processi esclusi tramite **Configurazione avanzata (F5) > Motore di rilevamento > Protezione file system in tempo reale > Esclusioni processi**.

Questa funzione è stata progettata per escludere gli strumenti di backup. L'esclusione dal controllo del processo dello strumento di backup non solo garantisce la stabilità del sistema, ma non influisce sulle prestazioni di backup poiché il backup non viene rallentato durante l'esecuzione.




Fare clic su **Modifica** per aprire la finestra di gestione **Esclusioni processi**, in cui è possibile [aggiungere esclusioni](#) e selezionare il file eseguibile (ad esempio, *Backup-tool.exe*) che verrà escluso dal controllo.

Non appena il file .exe viene aggiunto alle esclusioni, l'attività di questo processo non viene monitorata da ESET NOD32 Antivirus e non viene eseguito alcun controllo su tutte le operazioni sui file eseguite da questo processo.



Se non si utilizza la funzione Sfoglia per selezionare l'eseguibile del processo, è necessario immettere manualmente il percorso completo dell'eseguibile. In caso contrario, l'esclusione non funzionerà correttamente e [HIPS](#) potrebbe segnalare errori.

È inoltre possibile **modificare** i processi esistenti o **eliminarli** dalle esclusioni.


 La [protezione accesso Web](#) non tiene conto di questa esclusione, quindi se si esclude il file eseguibile del browser Web, i file scaricati vengono comunque controllati. In questo modo, è ancora possibile rilevare un'infiltrazione. Questo scenario è solo un esempio e non è consigliabile creare esclusioni per i browser Web.

Aggiungi o modifica esclusioni dei processi

Questa finestra di dialogo consente all'utente di **aggiungere** i processi esclusi dal motore di rilevamento. Le esclusioni dei processi aiutano a ridurre al minimo il rischio di potenziali conflitti e migliorano le prestazioni delle applicazioni escluse, con un effetto positivo sulle prestazioni complessive e sulla stabilità del sistema operativo. L'esclusione di un processo o di un'applicazione è un'esclusione del relativo file eseguibile (.exe).

Selezionare il percorso del file di un'applicazione esclusa facendo clic su ... (ad esempio, *C:\Program Files\Firefox\Firefox.exe*). NON digitare il nome dell'applicazione.

✓ Non appena il file .exe viene aggiunto alle esclusioni, l'attività di questo processo non viene monitorata da ESET NOD32 Antivirus e non viene eseguito alcun controllo su tutte le operazioni sui file eseguite da questo processo.

 Se non si utilizza la funzione Sfoglia per selezionare l'eseguibile del processo, è necessario immettere manualmente il percorso completo dell'eseguibile. In caso contrario, l'esclusione non funzionerà correttamente e [HIPS](#) potrebbe segnalare errori.

È inoltre possibile **modificare** i processi esistenti o **eliminarli** dalle esclusioni.

Protezione basata sul cloud

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 sospetti, ESET LiveGrid® consente a ESET di soddisfare le esigenze dei clienti e di gestire le minacce più recenti in modo tempestivo.

Sono disponibili le seguenti opzioni:

Abilitare il sistema di reputazione ESET LiveGrid®

Il sistema di reputazione ESET LiveGrid® offre l'accesso alle whitelist e alle blacklist basate sul cloud.

È possibile controllare la reputazione dei [Processi in esecuzione](#) e dei file direttamente dall'interfaccia del programma o dal menu contestuale. Ulteriori informazioni sono disponibili in ESET LiveGrid®.

Abilitare il sistema di feedback ESET LiveGrid®

Oltre al sistema di reputazione ESET LiveGrid®, il sistema di feedback ESET LiveGrid® raccoglierà informazioni sul computer dell'utente relative alle nuove minacce rilevate. Queste informazioni possono includere:

- Campione o copia del file in cui è apparsa la minaccia
- Percorso al file
- Nome file

- Data e ora
- Processo in base al quale la minaccia è apparsa sul computer in uso
- Informazioni sul sistema operativo del computer

Per impostazione predefinita, ESET NOD32 Antivirus è configurato per l'invio di file sospetti ai laboratori antivirus ESET ai fini di un'analisi dettagliata. Sono sempre esclusi file con estensioni specifiche, ad esempio *.doc* o *.xls*. È inoltre possibile aggiungere altre estensioni in presenza di file specifici che l'utente o la relativa società preferisce non inviare.

i Maggiori informazioni sull'invio di dati pertinenti sono disponibili nell'[Informativa sulla privacy](#).

È possibile scegliere di non abilitare ESET LiveGrid®

Non verrà persa alcuna funzionalità del software. Tuttavia, in alcuni casi, ESET NOD32 Antivirus potrebbe offrire una risposta più rapida alle nuove minacce in caso di abilitazione di ESET LiveGrid®. Se ESET LiveGrid® è già stato utilizzato in precedenza ed è stato disattivato, potrebbero essere ancora presenti pacchetti di dati da inviare. I pacchetti verranno inviati a ESET anche dopo la disattivazione. Dopo l'invio delle informazioni correnti, non verranno creati ulteriori pacchetti.

i Per ulteriori informazioni su ESET LiveGrid®, consultare il [glossario](#). Consultare le [istruzioni illustrate](#) disponibili in inglese e in molte altre lingue per abilitare o disabilitare ESET LiveGrid® in ESET NOD32 Antivirus.

Configurazione della protezione basata sul cloud in Configurazione avanzata

Per accedere alle impostazioni per ESET LiveGrid®, aprire **Configurazione avanzata** (F5) > **Motore di rilevamento** > **Protezione basata sul cloud**.

- **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.
- **Attiva il sistema di feedback di ESET LiveGrid®:** consente di inviare i dati relativi all'invio (descritti nel paragrafo **Invio dei campioni** sottostante) insieme ai report di arresti anomali e alle statistiche al laboratorio di ricerca ESET per ulteriori analisi.
- **Invia report di arresti e dati diagnostici:** consente di inviare i dati diagnostici correlati a ESET LiveGrid® quali arresti anomali e dump di memoria dei moduli. Si consiglia di mantenere questa opzione abilitata per aiutare ESET a diagnosticare i problemi, migliorare i prodotti e garantire una protezione dell'utente finale ottimizzata.
- **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.
- **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.

Invio di campioni

Invio manuale dei campioni: consente di abilitare l'opzione per l'invio manuale dei campioni a ESET dal menu contestuale, dalla [Quarantena](#) o da [Strumenti](#).

Invio automatico dei campioni rilevati

Selezionare i tipi di campioni che verranno inviati a ESET per l'analisi e per migliorare il rilevamento futuro (le dimensioni massime predefinite del campione sono 64 MB). Sono disponibili le seguenti opzioni:

- **Tutti i campioni rilevati:** tutti gli [oggetti](#) rilevati dal [motore di rilevamento](#) (comprese le applicazioni potenzialmente indesiderate abilitate nelle impostazioni dello scanner).
- **Tutti i campioni tranne i documenti:** tutti gli oggetti rilevati tranne i **Documenti** (vedere la sezione sottostante).
- **Non inviare:** gli oggetti rilevati non saranno inviati a ESET.

Invio automatico dei campioni sospetti

Questi campioni saranno anche inviati a ESET in caso di mancato rilevamento da parte dell'apposito motore. Ad esempio, i campioni che hanno quasi saltato il rilevamento oppure se uno dei [moduli di protezione](#) di ESET NOD32 Antivirus considera questi campioni sospetti o con un comportamento non chiaro (le dimensioni massime predefinite del campione sono 64 MB).

- **Eseguibili:** comprende file eseguibili quali .exe, .dll, .sys.
- **Archivi:** comprende tipi di file di archivio quali .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Script:** comprende tipi di file di script quali .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Altri:** include tipi di file quali .jar, .reg, .msi, .sfw, .lnk.
- **Possibili e-mail indesiderate:** questa opzione consente di inviare parti di o intere e-mail indesiderate con allegato a ESET per un'ulteriore analisi. L'attivazione di questa opzione consente di potenziare il rilevamento globale dei messaggi indesiderati, compresi miglioramenti per la ricerca futura di messaggi indesiderati per l'utente.
- **Documenti:** comprende documenti Microsoft Office o PDF con o senza contenuto attivo.

✓ [Espandere per un elenco di tutti i tipi di file di documenti inclusi](#)

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Esclusioni

Esclusioni: 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, ecc.). Se lo si desidera, è possibile aggiungerli all'elenco di file esclusi.

✓ Per escludere i file scaricati da `download.domain.com`, portarsi in **Configurazione avanzata > Motore di rilevamento > Protezione basata sul cloud > Invio di campioni** e fare clic su **Modifica** accanto a **Esclusioni**. Aggiungere l'esclusione a `.download.domain.com`.

Dimensione massima dei campioni (MB): definisce la dimensione massima dei campioni (1-64 MB).

Filtro di esclusione per la protezione basata sul cloud

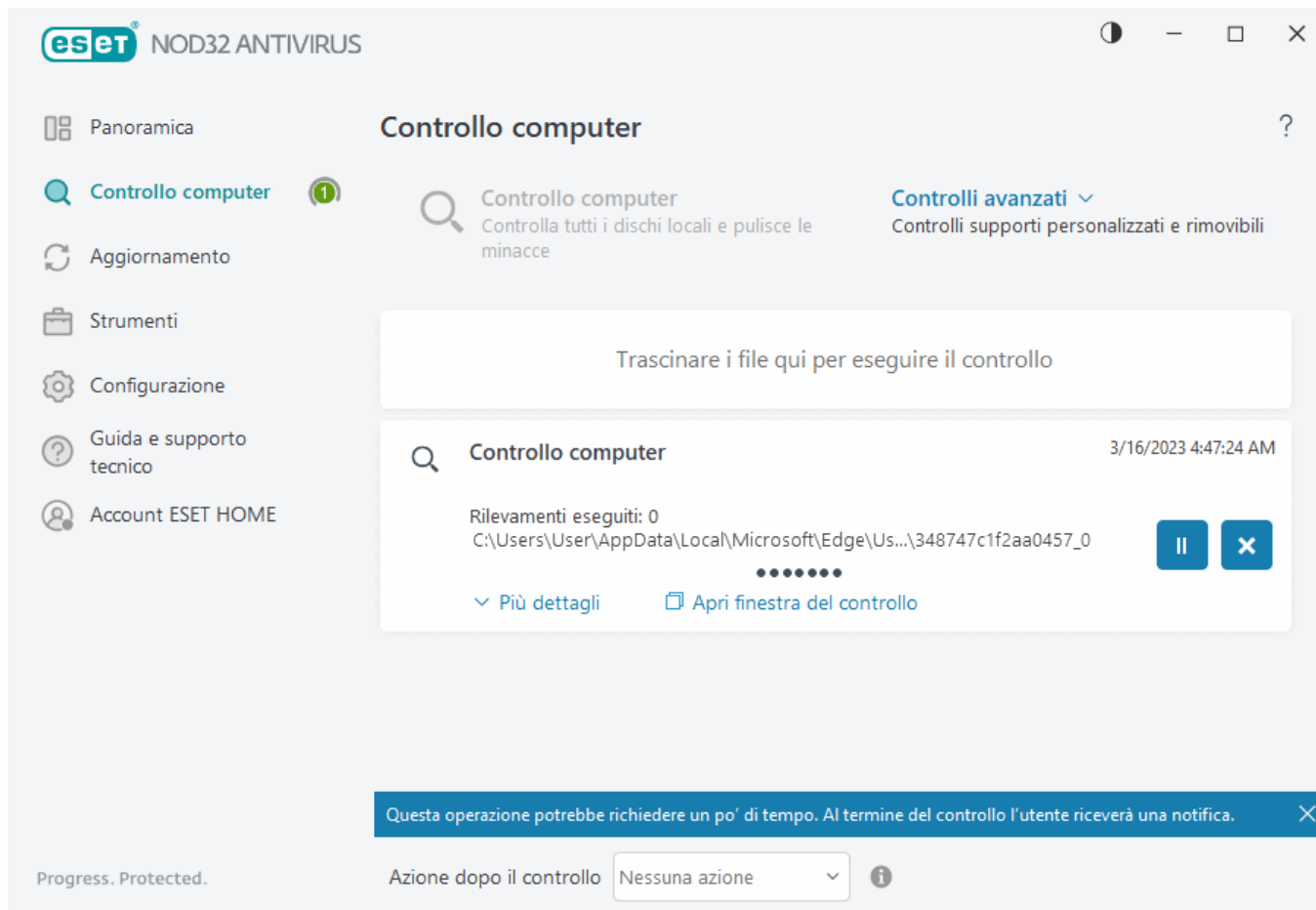
Il Filtro di esclusione consente di escludere dall'invio di campioni determinati file o cartelle. I file elencati non verranno mai inviati ai laboratori ESET ai fini dell'analisi, anche se contengono codice sospetto. I tipi di file comuni (come .doc, ecc.) sono esclusi per impostazione predefinita.

i Questa funzione è utile per escludere file che potrebbero contenere informazioni riservate, quali documenti o fogli di calcolo.

✓ Per escludere i file scaricati da `download.domain.com`, fare clic su **Configurazione avanzata > Motore di rilevamento > Protezione basata sul cloud > Invio di campioni > Esclusioni** e aggiungere l'esclusione `*download.domain.com*`.

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 motore di rilevamento 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 il computer in uso** consente di controllare rapidamente il sistema senza dover specificare i parametri di controllo. **Controllo personalizzato** (in Controlli avanzati) consente di selezionare uno dei profili di controllo predefiniti per l'analisi di percorsi specifici, nonché di scegliere specifiche destinazioni di controllo.

Per ulteriori informazioni sull'avanzamento del controllo, consultare il capitolo [Avanzamento controllo](#).



Per impostazione predefinita, ESET NOD32 Antivirus tenta di pulire o rimuovere automaticamente i rilevamenti trovati durante il controllo del computer. In alcuni casi, se non è possibile eseguire alcuna azione, l'utente riceve un avviso interattivo ed è necessario selezionare un'azione di pulizia (ad esempio, Rimuovi o Ignora). Per modificare il livello di pulizia e per informazioni più dettagliate, consultare [Pulizia](#). Per rivedere i precedenti controlli, consultare [File di rapporto](#).

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. In seguito a tale operazione, l'applicazione viene spostata in primo piano.

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. Il vantaggio offerto dal **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 stesse impostazioni.

Il menu a discesa **Azione al termine del controllo** consente all'utente di impostare un'azione da eseguire automaticamente al termine di un controllo:

- **Nessuna azione:** al termine di un controllo, non verrà eseguita alcuna azione.
- **Arresta:** il computer si spegne al termine di un controllo.
- **Riavvia se necessario:** il computer si riavvia solo se necessario per completare la pulizia delle minacce rilevate.
- **Riavvia:** chiude tutti i programmi aperti e riavvia il computer al termine di un controllo.
- **Forza riavvio se necessario:** il computer forza il riavvio solo se necessario per completare la pulizia delle minacce rilevate.
- **Forza riavvio:** consente di forzare la chiusura di tutti i programmi aperti senza attendere l'interazione dell'utente e di riavviare il computer al termine di un controllo.
- **Metti in stand-by:** salva la sessione in corso e mette il computer in modalità risparmio energetico che consente all'utente di riprendere velocemente il lavoro.
- **Metti in ibernazione:** sposta tutti i processi in esecuzione sulla RAM in un file speciale presente sul disco rigido. Il computer si arresterà ma i processi verranno ripresi dal punto in cui sono stati interrotti al successivo riavvio.

i Le azioni **Sospendi** e **Ibena** sono disponibili in base alle impostazioni del sistema operativo Alimentazione e Sospensione del computer in uso o delle capacità del computer/computer portatile. Tenere presente che un computer in sospensione è sempre un computer operativo. Sul quale vengono ancora eseguite funzioni di base e che utilizza l'elettricità in caso di alimentazione a batteria. Per prolungare la durata della batteria, ad esempio, in caso di viaggi fuori ufficio, si consiglia di utilizzare l'opzione Ibena.

L'azione selezionata si avvierà al termine di tutti i controlli in esecuzione. Se si seleziona **Arresta** o **Riavvia**, verrà visualizzata una finestra di dialogo di conferma del prodotto per 30 secondi (fare clic su **Annulla** per disattivare l'azione richiesta).

i 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?](#)

Launcher controllo personalizzato

È possibile utilizzare il Controllo personalizzato per analizzare la memoria operativa, la rete o sezioni specifiche di un disco, anziché l'intero disco. Per eseguire tale operazione, fare clic su **Controlli avanzati > Controllo personalizzato** selezionare destinazioni specifiche dalla struttura (ad albero) della cartella.

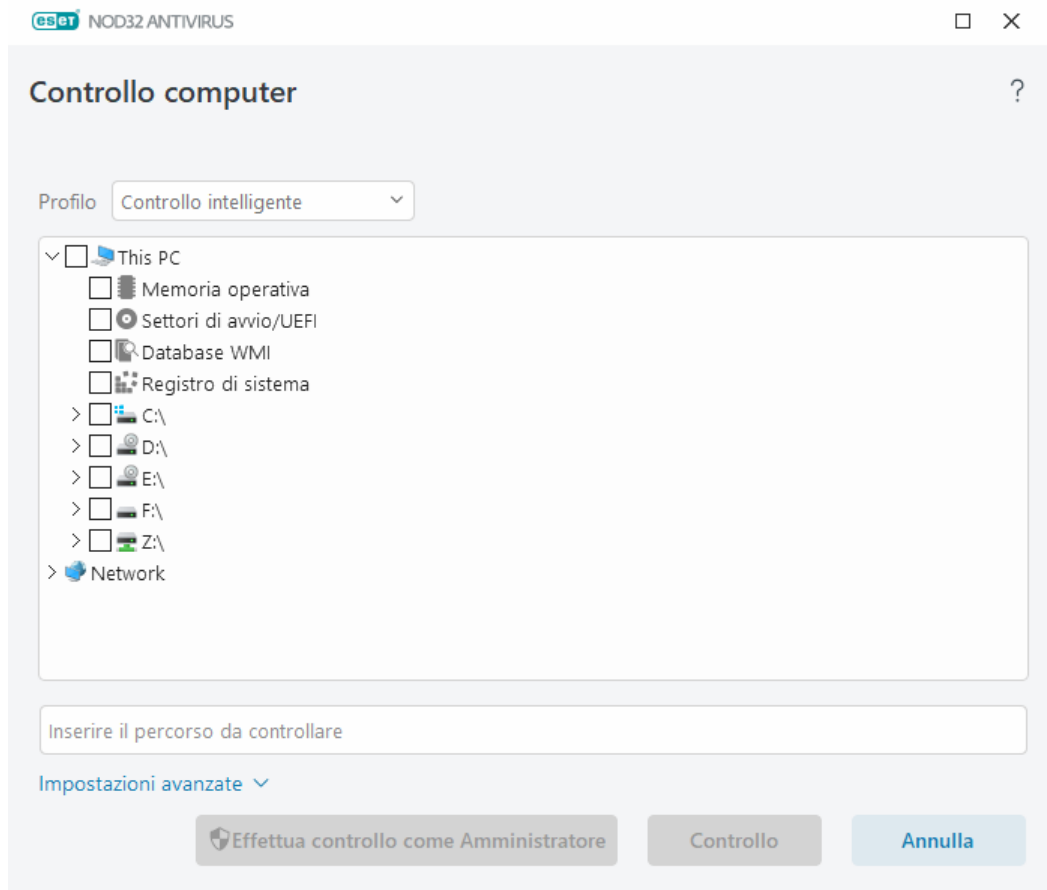
È possibile scegliere un profilo dal menu a discesa **Profilo** da utilizzare durante il controllo di specifiche destinazioni. Il profilo predefinito è **Controllo intelligente**. Esistono tre altri profili di controllo predefiniti chiamati **Controllo approfondito**, **Controllo menu contestuale** e **Controllo computer**. Questi profili di controllo utilizzano diversi [parametri di ThreatSense](#). Le opzioni disponibili sono descritte in **Configurazione avanzata (F5) > Motore di rilevamento > Controlli malware > Controllo su richiesta > [parametri di ThreatSense](#)**.

La struttura (ad albero) delle cartelle contiene anche destinazioni di controllo specifiche.

- **Memoria operativa:** consente di controllare tutti i processi e i dati attualmente utilizzati dalla memoria operativa.
- **Settori di avvio/UEFI:** consente di controllare i settori di avvio e UEFI alla ricerca di malware. Per ulteriori informazioni sullo scanner UEFI, consultare il [glossario](#).
- **Database WMI:** esegue il controllo dell'intero database Windows Management Instrumentation WMI, di tutti gli spazi dei nomi, di tutte le istanze della classe e di tutte le proprietà. Ricerca riferimenti a file infetti o malware incorporati come dati.
- **Registro di sistema:** consente di controllare l'intero registro di sistema, tutte le chiavi e le sottochiavi. Ricerca riferimenti a file infetti o malware incorporati come dati. Durante la pulizia dei rilevamenti, il riferimento rimane nel registro di sistema per garantire che non andranno persi dati importanti.

Per portarsi rapidamente in una destinazione di controllo (file o cartella), digitarne il percorso nel campo di testo sotto la struttura ad albero. Il percorso fa distinzione tra maiuscolo e minuscolo. Per includere la destinazione nel controllo, selezionare la relativa casella di controllo nella struttura ad albero.

i [Come pianificare un controllo del computer settimanale](#)
Per pianificare un'attività regolare, consultare il capitolo [Come pianificare un controllo del computer settimanale](#).



È possibile configurare i parametri di pulizia per il controllo in **Configurazione avanzata (F5) > Motore di rilevamento > Controllo su richiesta > Parametri ThreatSense > Pulizia**. Per eseguire un controllo senza azioni di pulizia, fare clic su **Impostazioni avanzate** e 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 verranno sottoposti al controllo senza alcuna eccezione.

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.

i È possibile visualizzare il rapporto del controllo computer al termine del controllo facendo clic su [Mostra rapporto](#).

Avanzamento controllo

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

i 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. Per ulteriori informazioni, consultare questo [articolo della Knowledge Base](#).

Come pianificare un controllo del computer settimanale

i Per pianificare un'attività regolare, consultare il capitolo [Come pianificare un controllo del computer settimanale](#).

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.

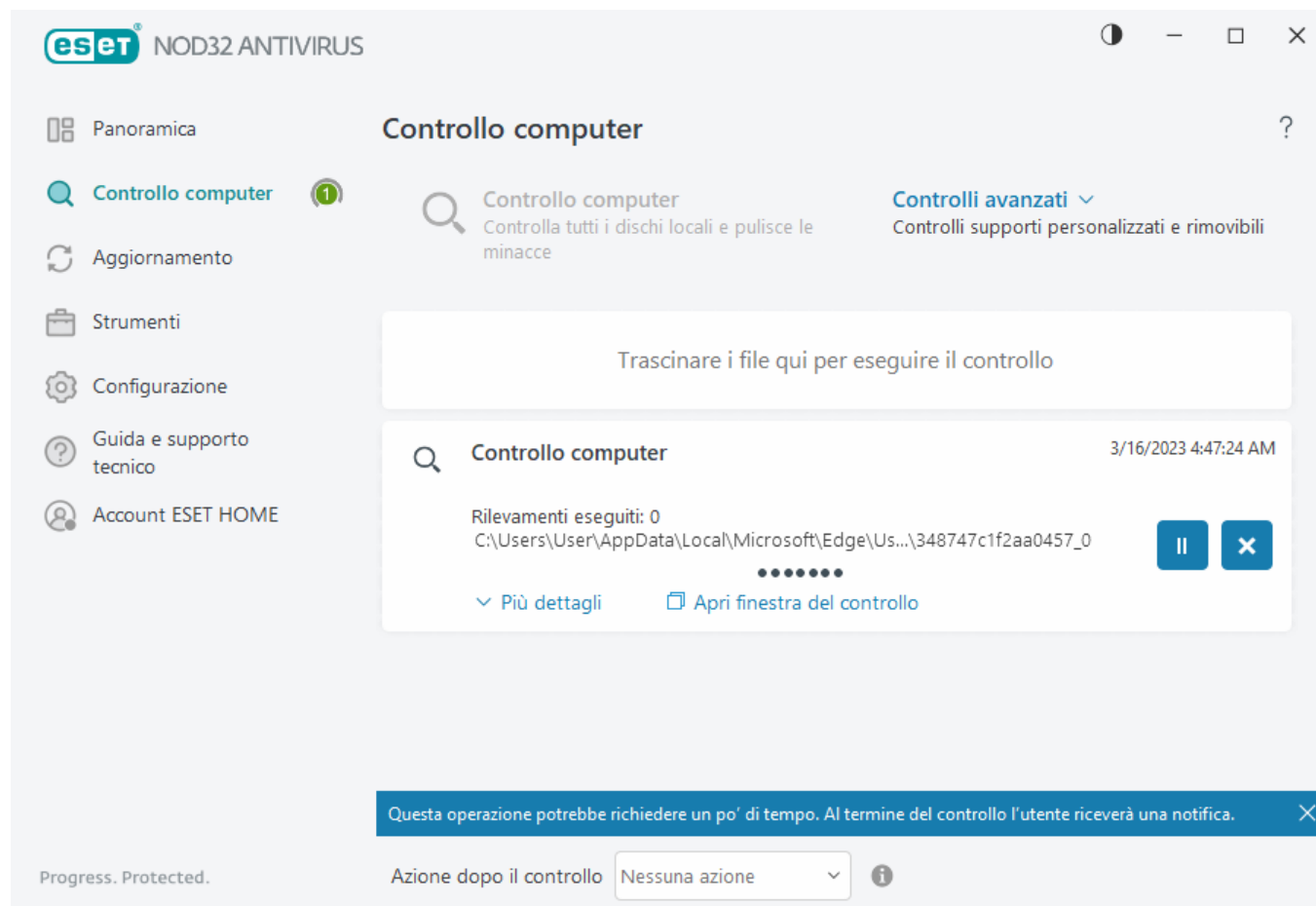
Sospendi: sospende un controllo.

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.

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



Il menu a discesa **Azione al termine del controllo** consente all'utente di impostare un'azione da eseguire automaticamente al termine di un controllo:

- **Nessuna azione:** al termine di un controllo, non verrà eseguita alcuna azione.
- **Arresta:** il computer si spegne al termine di un controllo.
- **Riavvia se necessario:** il computer si riavvia solo se necessario per completare la pulizia delle minacce rilevate.
- **Riavvia:** chiude tutti i programmi aperti e riavvia il computer al termine di un controllo.
- **Forza riavvio se necessario:** il computer forza il riavvio solo se necessario per completare la pulizia delle minacce rilevate.
- **Forza riavvio:** consente di forzare la chiusura di tutti i programmi aperti senza attendere l'interazione dell'utente e di riavviare il computer al termine di un controllo.
- **Metti in stand-by:** salva la sessione in corso e mette il computer in modalità risparmio energetico che consente all'utente di riprendere velocemente il lavoro.
- **Metti in ibernazione:** sposta tutti i processi in esecuzione sulla RAM in un file speciale presente sul disco rigido. Il computer si arresterà ma i processi verranno ripresi dal punto in cui sono stati interrotti al successivo riavvio.

i Le azioni **Sospendi** e **Iberna** sono disponibili in base alle impostazioni del sistema operativo Alimentazione e Sospensione del computer in uso o delle capacità del computer/computer portatile. Tenere presente che un computer in sospensione è sempre un computer operativo. Sul quale vengono ancora eseguite funzioni di base e che utilizza l'elettricità in caso di alimentazione a batteria. Per prolungare la durata della batteria, ad esempio, in caso di viaggi fuori ufficio, si consiglia di utilizzare l'opzione Iberna.

L'azione selezionata si avvierà al termine di tutti i controlli in esecuzione. Se si seleziona **Arresta** o **Riavvia**, verrà visualizzata una finestra di dialogo di conferma del prodotto per 30 secondi (fare clic su **Annulla** per disattivare l'azione richiesta).

Rapporto del controllo computer

Al termine del controllo, si apre il [Rapporto di controllo computer](#) contenente tutte le informazioni pertinenti correlate al controllo specifico. Il rapporto di controllo fornisce informazioni quali:

- Versione del motore di rilevamento
- Data e ora di inizio
- Elenco di dischi, cartelle e file controllati
- Nome del controllo pianificato (solo [controllo](#) pianificato)
- Stato controllo
- Numero di oggetti sottoposti a controllo

- Numero di rilevamenti trovati
- Ora di completamento
- Tempo di controllo totale




Un nuovo avvio di un'attività di controllo del computer pianificata viene ignorato se la stessa attività pianificata che è stata eseguita in precedenza è ancora in esecuzione. L'attività di controllo pianificata ignorata creerà un Rapporto del controllo del computer con 0 oggetti controllati e lo stato **Il controllo non è stato avviato in quanto quello precedente era ancora in esecuzione.**

Per trovare i rapporti di controllo precedenti, nella [finestra principale del programma](#), selezionare **Strumenti > File di rapporto**. Nel menu a discesa, selezionare **Controllo del computer** e fare doppio clic sul record desiderato.



Per ulteriori informazioni sui record “impossibili da aprire”, “errore di apertura” e/o “archivio danneggiato”, consultare questo [articolo della Knowledge Base di ESET](#).

Fare clic sull'icona della barra di scorrimento  **Filtraggio** per aprire la finestra [Filtraggio rapporti](#) in cui è possibile restringere la ricerca in base a criteri personalizzati. Per visualizzare il menu contestuale, fare clic con il pulsante destro del mouse su una specifica voce di registro:

Azione	Utilizzo
Filtra gli stessi record	Attiva il filtraggio dei rapporti. Il rapporto consentirà di visualizzare solo i record dello stesso tipo di quello selezionato.

Azione	Utilizzo
Filtra	Questa opzione consente di aprire la finestra Filtraggio dei rapporti e di definire i criteri per specifiche voci di rapporto. Scelta rapida da tastiera: Ctrl+Shift+F
Attiva filtro	Attiva le impostazioni del filtro. In caso di prima attivazione del filtro, è necessario definire le impostazioni. Questa operazione determina l'apertura della finestra Filtraggio dei rapporti.
Disattiva filtro	Disattiva il filtro (corrisponde all'attivazione dell'interruttore posizionato in basso).
Copia	Copia i record selezionati negli appunti. Scelta rapida da tastiera: Ctrl+C
Copia tutto	Copia tutti i record nella finestra.
Esporta	Esporta i record selezionati negli appunti in un file XML.
Esporta tutto	Questa opzione consente di esportare tutti i record nella finestra in un file XML.
Descrizione del rilevamento	Consente di aprire ESET Threat Encyclopedia, che contiene informazioni dettagliate sui pericoli e sui sintomi dell'infiltrazione evidenziata.

Controlli malware

La sezione **Controlli malware** è accessibile da **Configurazione avanzata (F5) > Motore di rilevamento > Controlli malware** e fornisce opzioni per selezionare i parametri di controllo. Questa sezione contiene le seguenti voci:

Profilo selezionato: serie specifica di parametri utilizzati dallo scanner su richiesta. Per crearne uno nuovo, fare clic su **Modifica** accanto a **Elenco di profili**. Per ulteriori informazioni, consultare [Profili di controllo](#).

Destinazioni di controllo: se si desidera controllare unicamente una destinazione specifica, fare clic su **Modifica** accanto a **Destinazioni di controllo** e scegliere un'opzione dal menu a discesa o selezionare destinazioni specifiche dalla struttura (ad albero) della cartella. Per ulteriori informazioni, consultare [Destinazioni di controllo](#).

Parametri ThreatSense: in questa sezione sono illustrate opzioni di configurazione avanzata, come le estensioni dei file da controllare, i metodi di rilevamento utilizzati e così via. Fare clic per aprire una scheda con le opzioni dello scanner avanzato.

Controllo stato di inattività

È possibile attivare il controllo stato inattivo in **Configurazione avanzata** da **Motore di rilevamento > Controlli malware > Controllo stato inattivo**.

Controllo stato di inattività

Abilitare la barra di scorrimento accanto ad **Abilita controllo stato inattivo** per abilitare questa funzionalità. Se il computer si trova nello stato di inattività, verrà eseguito un controllo silenzioso di tutte le unità locali.

Per impostazione predefinita, lo scanner dello stato di inattività non verrà eseguito in caso di alimentazione del computer (notebook) a batteria. È possibile ignorare questa impostazione abilitando la barra di scorrimento accanto a **Esegui anche se il computer è alimentato a batteria** in Configurazione avanzata.

Attivare il pulsante **Attiva registrazione** in Configurazione avanzata 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**).

Rilevamento stato di inattività

Consultare la sezione [Metodi di attivazione del rilevamento stato inattivo](#) per un elenco completo di condizioni che è necessario soddisfare per attivare il controllo stato inattivo.

Fare clic su [Configurazione parametri motore ThreatSense](#) per modificare i parametri di controllo (ad esempio, metodi di rilevamento) per lo scanner dello stato inattivo.

Profili di scansione

In ESET NOD32 Antivirus sono disponibili 4 profili di controllo predefiniti:

- **Controllo intelligente** – profilo di controllo avanzato predefinito. Utilizza la tecnologia di ottimizzazione intelligente che esclude i file che sono stati trovati puliti in un controllo precedente e che non sono stati modificati da allora. Ciò consente di ridurre i tempi di controllo con un impatto minimo sulla sicurezza del sistema.
- **Controllo menu contestuale** – dal menu contestuale è possibile avviare un controllo su richiesta di qualsiasi file. Il profilo di controllo del menu contestuale consente all'utente di definire una configurazione di controllo che verrà utilizzata durante questa tipologia di attivazione del controllo.
- **Controllo approfondito** – Per impostazione predefinita, il profilo Controllo approfondito non utilizza l'ottimizzazione intelligente, in modo che nessun file venga escluso dal controllo utilizzando questo profilo.
- **Controllo computer** – profilo predefinito utilizzato nel controllo del computer standard.

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 **Motore di rilevamento > Controlli malware > Controllo su richiesta > 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.

i 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 **Correggi sempre il rilevamento**. 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.

Destinazioni di controllo

Il menu a discesa **Destinazioni di controllo** consente di selezionare le destinazioni di controllo predefinite.

- **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.
- **Selezione personalizzata:** consente di annullare tutte le selezioni precedenti.

La struttura (ad albero) delle cartelle contiene anche destinazioni di controllo specifiche.

- **Memoria operativa:** consente di controllare tutti i processi e i dati attualmente utilizzati dalla memoria operativa.
- **Settori di avvio/UEFI:** consente di controllare i settori di avvio e UEFI alla ricerca di malware. Per ulteriori informazioni sullo scanner UEFI, consultare il [glossario](#).
- **Database WMI:** esegue il controllo dell'intero database Windows Management Instrumentation WMI, di tutti gli spazi dei nomi, di tutte le istanze della classe e di tutte le proprietà. Ricerca riferimenti a file infetti o malware incorporati come dati.
- **Registro di sistema:** consente di controllare l'intero registro di sistema, tutte le chiavi e le sottochiavi. Ricerca riferimenti a file infetti o malware incorporati come dati. Durante la pulizia dei rilevamenti, il riferimento rimane nel registro di sistema per garantire che non andranno persi dati importanti.

Per portarsi rapidamente in una destinazione di controllo (file o cartella), digitarne il percorso nel campo di testo sotto la struttura ad albero. Il percorso fa distinzione tra maiuscolo e minuscolo. Per includere la destinazione nel controllo, selezionare la relativa casella di controllo nella struttura ad albero.

Controllo dispositivi

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
- FireWire Archiviazione
- Bluetooth Dispositivo
- Lettore di smart card
- Dispositivo di acquisizione immagini

- Modem
- LPT/COM porta
- Dispositivo portatile
- Tutti i tipi di dispositivi

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

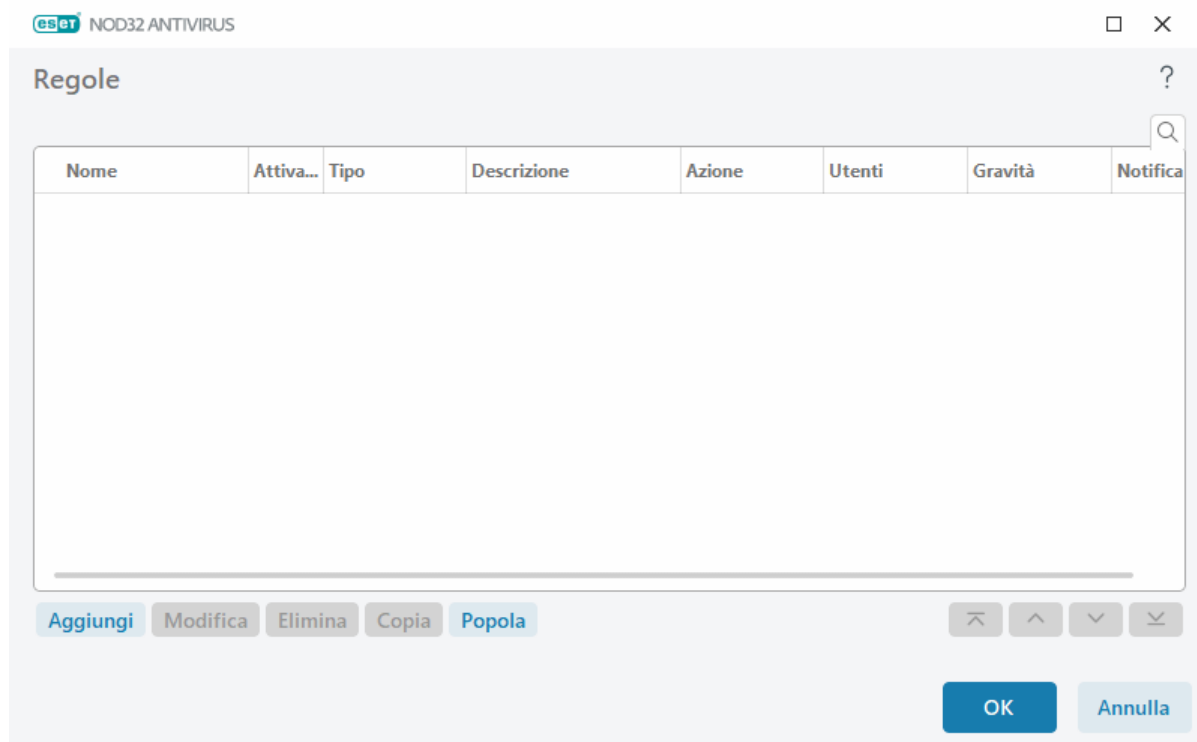
Abilitare la barra di scorrimento accanto ad **Abilita Controllo dispositivi** per attivare la funzione Controllo dispositivi in ESET NOD32 Antivirus. Per rendere effettiva questa modifica, sarà necessario riavviare il computer. Dopo aver abilitato il Controllo dispositivi, è possibile definire le **Regole** nella finestra [Editor regole](#).

i 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 **Consenti** o **Blocco di scrittura**. 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.

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. Consultare anche [Aggiunta di regole per il controllo dei dispositivi](#).

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 .

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 **Abilitata** consente di disabilitare o abilitare una regola; questa opzione può rivelarsi utile se si desidera mantenere la regola.

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 del programma](#) > **Strumenti** > [File di rapporto](#).

Il [rapporto Controllo dispositivi](#) registra tutte le occorrenze di attivazione del controllo dispositivi.

Dispositivi rilevati

Il pulsante **Popola** fornisce una panoramica di tutti i dispositivi attualmente connessi contenenti informazioni su: tipo di dispositivo, fornitore del dispositivo, modello e numero di serie (se disponibili).

Selezionare un dispositivo dall'elenco Dispositivi rilevati e fare clic su **OK** per [aggiungere una regola di controllo dispositivi](#) con informazioni predefinite (è possibile modificare tutte le impostazioni).

I dispositivi in modalità basso consumo (sospensione) sono contrassegnati con un'icona di avviso . Per abilitare il pulsante **OK** e aggiungere una regola per questo dispositivo:

- Ricollegare il dispositivo
- Utilizzare il dispositivo (p. es., avviare l'app Fotocamera in Windows per riattivare una webcam)

Aggiunta di regole per il controllo dispositivi

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

eset

NOD32 ANTIVIRUS

X

Aggiungi regola

?

Nome

Senza titolo

Regola attivata

☒

Tipo di dispositivo

Archiviazione su disco

▼

Azione

Consenti

▼

Tipo di criterio

Dispositivo

▼

Fornitore

Modello

Numero di serie

Livello registrazione

Sempre

▼

Elenco utente

Modifica

Notifica utente

☒

OK

Inserire una descrizione della regola nel campo **Nome** per consentire una migliore identificazione. Fare clic sulla barra di scorrimento accanto a **Regola abilitata** per disabilitare o abilitare questa regola. Questa opzione può essere utile se non si desidera rimuovere 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:

- **Consenti:** sarà consentito l'accesso completo al dispositivo.
- **Blocca:** l'accesso al supporto verrà bloccato.
- **Blocco di scrittura:** 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. I dispositivi non vengono memorizzati e continuerà a essere visualizzata una notifica in caso di successive connessioni dello

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 **Blocco di scrittura** non è disponibile per il sistema Bluetooth. Ciò significa che i dispositivi Bluetooth possono essere solo consentiti, bloccati o avvisati).

Tipo di criteri

Selezionare **Gruppo dispositivi** o **Dispositivo**.

I parametri aggiuntivi visualizzati di seguito possono essere utilizzati per ottimizzare le regole per i vari dispositivi. Tutti i parametri utilizzano la distinzione tra maiuscolo e minuscolo e supportano i caratteri jolly (*, ?):

- **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.

i 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 utilizzano la distinzione tra maiuscolo e minuscolo e supportano i caratteri jolly (un punto interrogativo (?) rappresenta un carattere singolo, mentre un asterisco (*) rappresenta una stringa di zero o più caratteri).

i Per visualizzare le informazioni relative a un dispositivo, creare una regola per quello specifico dispositivo, 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.

Elenco utente

Le regole possono essere limitate a determinati utenti o gruppi di utenti aggiungendoli all'elenco di utenti e facendo clic su **Modifica** accanto all'**Elenco di 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.

Limitazioni elenco di utenti

L'elenco di utenti non può essere definito per le regole con [tipi di dispositivi](#) specifici:



- Stampante USB
- Dispositivo Bluetooth
- Lettore di smart card
- Dispositivo di acquisizione immagini
- Modem
- Porta LPT/COM

Notifica utente: in caso di inserimento di un dispositivo bloccato mediante una regola esistente, verrà visualizzata una finestra di notifica.

Gruppi dispositivi



Il dispositivo connesso al computer in uso potrebbe rappresentare un rischio per la sicurezza.

La finestra Gruppi dispositivi è suddivisa in due parti. La parte destra contiene un elenco di dispositivi appartenenti al gruppo di riferimento i gruppi creati. Selezionare un gruppo per visualizzare i dispositivi nel riquadro sulla destra.

Aperto la finestra Gruppi dispositivi e selezionando un gruppo, è possibile aggiungere o rimuovere dispositivi dall'elenco. Un altro modo per aggiungere dispositivi nel gruppo consiste nell'importazione degli stessi da un file. In alternativa, è possibile fare clic sul pulsante **Popola**, che consente di inserire tutti i dispositivi connessi al computer in uso nella finestra **Dispositivi rilevati**. Selezionare i dispositivi dall'elenco compilato per aggiungerli al gruppo facendo clic su **OK**.

Elementi di controllo

Aggiungi: è possibile aggiungere un gruppo digitandone il nome o un dispositivo in un gruppo esistente, a seconda della parte della finestra in cui è stato selezionato il pulsante.

Modifica: consente all'utente di modificare il nome del gruppo selezionato o i parametri del dispositivo (fornitore, modello, numero di serie).

Elimina: elimina il gruppo o il dispositivo scelto in base alla parte di finestra selezionata.

Importa: consente di importare un elenco di dispositivi da un file di testo. L'importazione dei dispositivi da un file di testo richiede una formattazione corretta:

- Ciascun dispositivo inizia da una nuova riga.
- Per ciascun dispositivo devono essere indicati **Fornitore**, **Modello** e **Numero di serie** separati da una virgola.

✓ Segue un esempio del contenuto del file di testo:
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101

Esporta: consente di esportare un elenco di dispositivi in un file.

Il pulsante **Popola** fornisce una panoramica di tutti i dispositivi attualmente connessi contenenti informazioni su: tipo di dispositivo, fornitore del dispositivo, modello e numero di serie (se disponibili).

Aggiungi dispositivo

Fare clic su **Aggiungi** nella finestra sulla destra per aggiungere un dispositivo in un gruppo esistente. I parametri aggiuntivi visualizzati di seguito possono essere utilizzati per ottimizzare le regole per i vari dispositivi. Tutti i parametri utilizzano la distinzione tra maiuscolo e minuscolo e supportano i caratteri jolly (*, ?):

- **Fornitore:** filtraggio in base al nome o all'ID 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.
- **Descrizione:** descrizione del dispositivo da parte dell'utente finalizzata a una migliore organizzazione.

i 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 utilizzano la distinzione tra maiuscolo e minuscolo e supportano i caratteri jolly (un punto interrogativo [?] rappresenta un carattere singolo, mentre un asterisco [*] rappresenta una stringa di zero o più caratteri).

Fare clic su **OK** per salvare le modifiche. Fare clic su **Annulla** per abbandonare la finestra **Gruppi di dispositivi** senza salvare le modifiche.

i Dopo aver creato un gruppo di dispositivi, è necessario [aggiungere una nuova regola di controllo dei dispositivi](#) e scegliere l'azione da intraprendere.

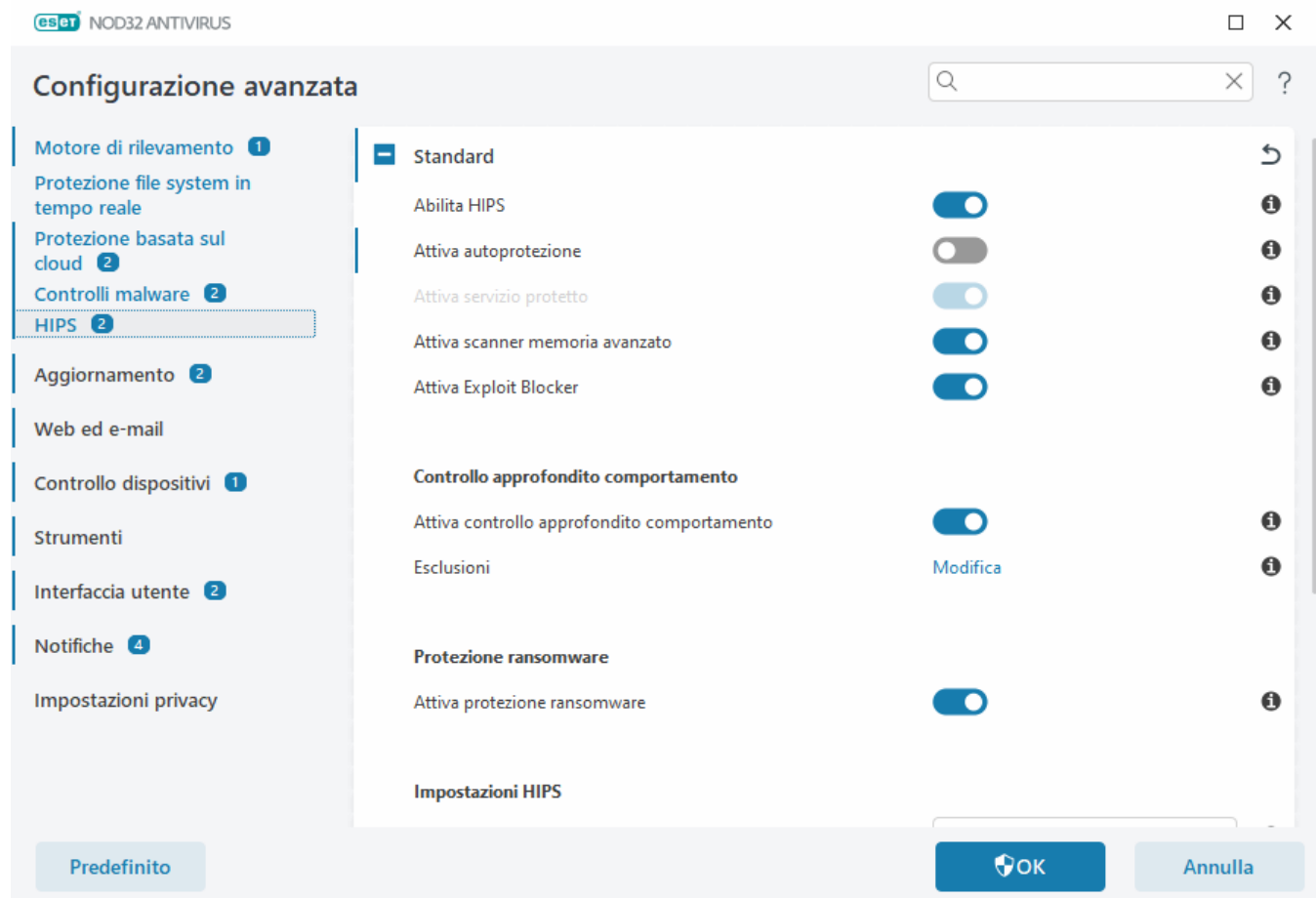
Tenere presente che non sono disponibili tutte le azioni (autorizzazioni) per tutti i tipi di dispositivi. Tutte e quattro le azioni sono disponibili in caso di un dispositivo di archiviazione. Per i dispositivi non di archiviazione, sono disponibili solo tre azioni (ad esempio, **Blocco di scrittura** non è disponibile per la funzione Bluetooth. Ciò significa che i dispositivi Bluetooth possono essere solo consentiti o bloccati oppure ricevere avvisi).

Host Intrusion Prevention System (HIPS)

⚠ Le modifiche delle impostazioni HIPS devono essere eseguite solo da utenti avanzati. Una configurazione non corretta delle impostazioni HIPS può causare instabilità di sistema.

L'**Host Intrusion Prevention System (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) > **Motore di rilevamento** > **HIPS** > **Standard**. Lo stato HIPS (attivato/disattivato) è visualizzato nella [finestra principale del programma](#) ESET NOD32 Antivirus in **Configurazione** > **Protezione computer**.



Di base

Attiva HIPS: HIPS è attivato per impostazione predefinita in ESET NOD32 Antivirus. Disattivando HIPS, verrà disattivato il resto delle funzionalità HIPS come Exploit Blocker.

Attiva autoprotezione: ESET NOD32 Antivirus utilizza la tecnologia integrata di **Autoprotezione** all'interno della funzione HIPS allo scopo di impedire a software dannosi di danneggiare o disattivare la protezione antivirus e antispyware. La funzione di Autoprotezione protegge processi ESET e di sistema cruciali, chiavi di registro e file da tentativi di manomissione.

Attiva servizio protetto: abilita la protezione per ESET Service (ekrn.exe). In caso di attivazione, il servizio viene attivato come processo Windows protetto per difendere il sistema da attacchi da parte di malware.

Attiva 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, viene attivato lo scanner di memoria avanzato. Per ulteriori informazioni su questo tipo di protezione, consultare il [glossario](#).

Attiva 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](#).

Controllo approfondito comportamento

Attiva controllo approfondito del comportamento: ulteriore livello di protezione integrato nella funzione HIPS. Questa estensione analizza il comportamento di tutti i programmi in esecuzione sul computer e avvisa l'utente in caso di comportamento dannoso del processo.

[Le esclusioni HIPS dal controllo approfondito del comportamento](#) consentono di escludere processi dall'analisi. Per garantire che la ricerca delle minacce venga eseguita su tutti i processi, si consiglia di creare esclusioni solo se assolutamente necessario.

Protezione da ransomware

Attiva protezione ransomware: un altro livello di protezione che opera all'interno della funzione HIPS. È necessario che il sistema di reputazione ESET LiveGrid® sia attivo per consentire il funzionamento della protezione ransomware. [Per ulteriori informazioni su questo tipo di protezione.](#)

Abilita Intel® Threat Detection Technology: aiuta a rilevare attacchi ransomware attraverso l'utilizzo della telemetria CPU univoca Intel per aumentare l'efficacia del rilevamento, ridurre gli avvisi falsi positivi ed espandere la visibilità per rilevare tecniche di evasione avanzate. Consultare [Processori supportati.](#)

Impostazioni HIPS

La **Modalità di filtraggio** può essere eseguita in una delle seguenti modalità:

Modalità di filtraggio	Descrizione
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	Blocca tutte le operazioni che non sono definite da una regola specifica che le consenta.
Modalità riconoscimento	Le operazioni sono abilitate e dopo ogni operazione viene creata una regola. Le regole create in questa modalità possono essere visualizzate nell'editor Regole HIPS , ma la loro priorità è inferiore rispetto alla priorità delle regole create manualmente o delle regole create in modalità automatica. Selezionando la Modalità riconoscimento dal menu a discesa Modalità di filtraggio , la Modalità riconoscimento terminerà nel momento in cui l'impostazione diventerà disponibile. 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 di filtraggio che verrà utilizzata dopo la scadenza della modalità di apprendimento. Dopo la scadenza, l'opzione **Chiedi all'utente** richiede privilegi amministrativi per eseguire il passaggio alla modalità di filtraggio HIPS.

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 l'editor **Regole HIPS**. Nella finestra Regole HIPS è possibile selezionare, aggiungere, modificare o rimuovere regole. Ulteriori informazioni sulla creazione

delle regole e sulle operazioni HIPS sono disponibili in [Modificare una regola HIPS](#).

Finestra interattiva HIPS

La finestra Notifica HIPS consente all'utente di creare una regola in base alle nuove azioni rilevate dall'HIPS e di definire le condizioni in base alle quali consentire o negare l'azione.

Le regole create dalla finestra di notifica sono considerate equivalenti a quelle create manualmente. Una regola creata da una finestra di notifica può essere meno specifica rispetto alla regola che ha attivato quella finestra di dialogo. Ciò significa che, dopo aver creato questo tipo di regola nella finestra di dialogo, la stessa operazione può attivare la stessa finestra. Per ulteriori informazioni, consultare [Priorità per le regole HIPS](#).

Se l'azione predefinita di una regola è impostata su **Chiedi sempre**, 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.

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.

L'opzione **Crea regola e memorizzala in modo permanente** crea una nuova regola HIPS, che può essere successivamente modificata nella sezione [Gestione regole HIPS](#) (richiede i privilegi di amministrazione).

Fare clic su **Dettagli** in basso per vedere quale applicazione ha attivato l'operazione, qual è la reputazione del file o quale tipo di operazione viene richiesto di consentire o negare.

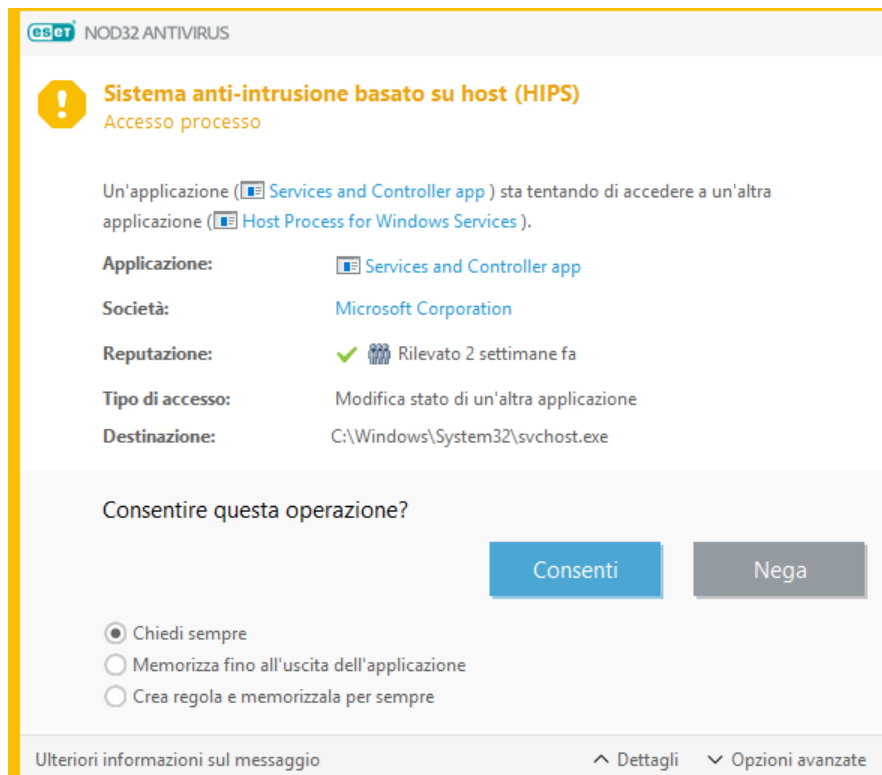
È possibile accedere alle impostazioni per i parametri delle regole più dettagliati facendo clic su **Opzioni avanzate**. Le opzioni seguenti sono disponibili se si sceglie **Crea regola e memorizzala in modo permanente**:

- **Crea una regola valida solo per questa applicazione:** se si deseleziona questa casella di controllo, la regola verrà creata per tutte le applicazioni di origine.
- **Solo per operazione:** scegliere le operazioni file/applicazione/registro della regola. [Consultare le descrizioni per tutte le operazioni HIPS](#).
- **Solo per destinazione:** scegliere le destinazioni file/applicazione/registro della regola.

Infinite notifiche HIPS?

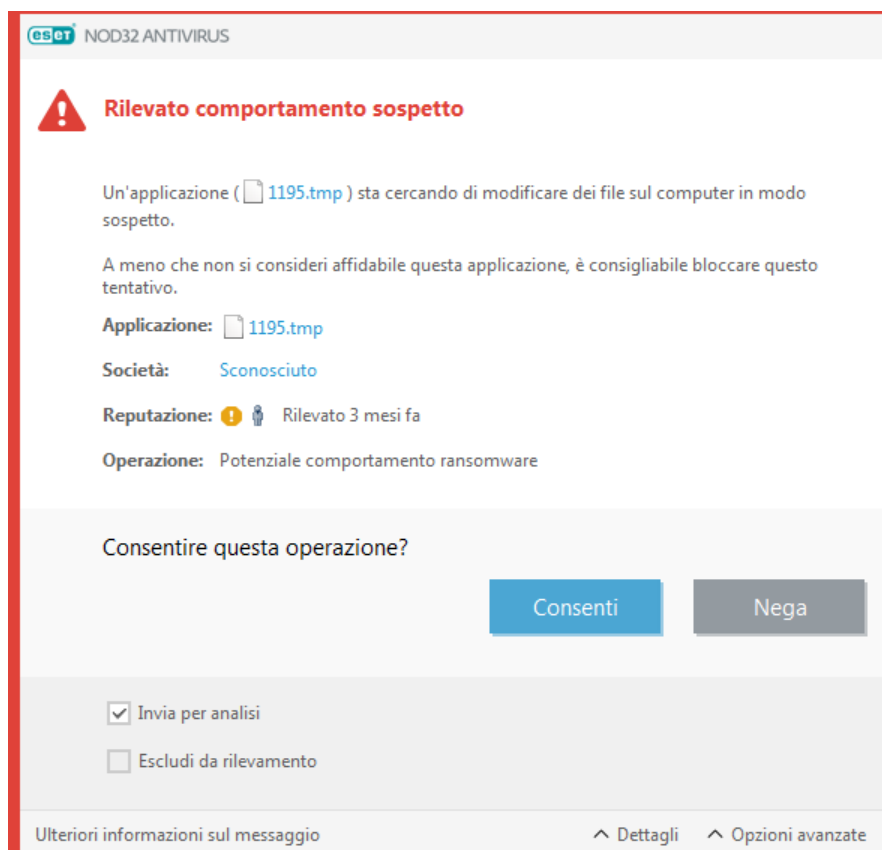


Per interrompere la visualizzazione delle notifiche, modificare la modalità di filtraggio su **Modalità automatica** in **Configurazione avanzata (F5) > Motore di rilevamento > HIPS > Di base**.



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.



Fare clic su **Dettagli** per visualizzare i parametri di rilevamento specifici. La finestra di dialogo contiene le opzioni

Invia per analisi o Escludi da rilevamento.

 ESET LiveGrid® deve essere attivo affinché la [protezione ransomware](#) funzioni correttamente.

Gestione regole HIPS

Elenco delle regole definite dall'utente e aggiunte automaticamente dal sistema HIPS. Per ulteriori informazioni sulla creazione delle regole e sulle operazioni HIPS, consultare il capitolo [Impostazioni regole HIPS](#). Consultare anche [Principio generale relativo a HIPS](#).

Colonne

Regola: nome della regola scelto automaticamente o definito dall'utente.

Abilitata: disabilitare la barra di scorrimento se si desidera mantenere la regola nell'elenco senza utilizzarla.

Azione: la regola specifica un'azione (**Consenti**, **Blocca** o **Chiedi**) che deve essere eseguita se sono soddisfatte le condizioni specificate.

Origini : la regola verrà utilizzata solo se l'evento viene attivato da una o più applicazioni.

Destinazioni: la regola verrà utilizzata esclusivamente se l'operazione è correlata a un file, un'applicazione o una voce di registro specifici.

Gravità registrazione: se si attiva questa opzione, le informazioni sulla regola verranno scritte nel [Rapporto HIPS](#).

Invia notifica: se viene attivato un evento, nell'angolo in basso a destra viene visualizzata una piccola finestra di notifica.

Elementi di controllo

Aggiungi: crea una nuova regola.

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

Elimina: rimuove le voci selezionate.

Priorità per le regole HIPS

Non sono disponibili opzioni per regolare il livello di priorità delle regole HIPS utilizzando i pulsanti In alto/In basso.

- Tutte le regole create hanno la stessa priorità
- Più specifica è la regola, maggiore è la priorità (ad esempio, la regola per un'applicazione specifica ha una priorità più alta della regola per tutte le applicazioni)
- Internamente, HIPS contiene regole con una priorità più alta che non sono accessibili per l'utente (ad esempio, non è possibile ignorare le regole di Autoprotezione definite)

- Una regola creata dall'utente che potrebbe bloccare il sistema operativo non verrà applicata (avrà la priorità più bassa)

Modifica una regola HIPS

Consultare prima [Gestione delle regole HIPS](#).

Nome regola: nome della regola scelto automaticamente o definito dall'utente.

Azione: specifica un'azione (**Consenti**, **Blocca** o **Chiedi**) che deve essere eseguita se sono soddisfatte le condizioni specificate.

Operazioni che influiscono: è necessario selezionare il tipo di operazione alla quale la regola verrà applicata. La regola verrà utilizzata solo per questo tipo di operazione e per la destinazione selezionata.

Abilitata: disabilitare la barra di scorrimento se si desidera mantenere la regola nell'elenco senza applicarla.

Gravità registrazione: se si attiva questa opzione, le informazioni sulla regola verranno scritte nel [Rapporto HIPS](#).

Invia notifica all'utente: se viene attivato un evento, nell'angolo in basso a destra viene visualizzata una piccola finestra di notifica.

La regola è formata da varie parti che illustrano le condizioni che la attivano:

Applicazioni di origine: la regola verrà utilizzata solo se l'evento viene attivato dall'applicazione. Selezionare **Applicazioni specifiche** dal menu a discesa e fare clic su **Aggiungi** per aggiungere nuovi file oppure selezionare **Tutte le applicazioni** dal menu a discesa per aggiungere tutte le applicazioni.

File di destinazione: la regola viene utilizzata solo se l'operazione è correlata a questa destinazione. Selezionare **File specifici** dal menu a discesa e fare clic su **Aggiungi** per aggiungere nuovi file o cartelle oppure selezionare **Tutti i file** dal menu a discesa per aggiungere tutti i file.

Applicazioni: la regola verrà utilizzata solo se l'operazione è correlata a questa destinazione. Selezionare **Applicazioni specifiche** dal menu a discesa e fare clic su **Aggiungi** per aggiungere nuovi file o cartelle oppure selezionare **Tutte le applicazioni** dal menu a discesa per aggiungere tutte le applicazioni.

Voci di registro: la regola verrà utilizzata solo se l'operazione è correlata a questa destinazione. Selezionare **Voci specifiche** dal menu a discesa e fare clic su **Aggiungi** per inserirla manualmente oppure fare clic su **Apri editor registro** per selezionare una chiave dal Registro. È inoltre possibile selezionare **Tutte le voci** dal menu a discesa per aggiungere tutte le applicazioni.



Non è possibile bloccare alcune operazioni di regole specifiche predefinite da HIPS. Per impostazione predefinita, tali operazioni saranno quindi consentite. Inoltre, non tutte le operazioni di sistema sono monitorate da HIPS. HIPS monitora le operazioni che possono essere considerate non sicure.

Descrizione delle operazioni importanti:

Operazioni del file

- **Elimina file:** l'applicazione richiede l'autorizzazione per l'eliminazione del file di destinazione.

- **Scrivi su file:** l'applicazione richiede l'autorizzazione per scrivere sul file di destinazione.
- **Accesso diretto al disco:** l'applicazione sta tentando di leggere o scrivere sul disco in modalità non standard, che eluderà le procedure di Windows comuni. Ciò potrebbe causare la modifica dei file senza che vengano applicate le regole corrispondenti. Questa operazione può essere causata da un malware che tenta di eludere il rilevamento, un software di backup che tenta di creare una copia esatta di un disco o un programma di gestione delle partizioni che tenta di riorganizzare i volumi del disco.
- **Installa hook globale:** fa riferimento alla chiamata della funzione SetWindowsHookEx dalla libreria MSDN.
- **Carica driver:** installazione e caricamento dei driver nel sistema.

Operazioni dell'applicazione

- **Esegui debug di un'altra applicazione:** associazione di un debugger al processo. Quando si esegue il debug di un'applicazione, è possibile visualizzare e modificare molti dettagli del relativo comportamento e accedere ai rispettivi dati.
- **Intercetta eventi da altra applicazione:** l'applicazione di origine sta tentando di intercettare gli eventi specifici su un'applicazione specifica (ad esempio, un keylogger che cerca di acquisire gli eventi del browser).
- **Termina/sospendi altra applicazione:** sospensione, ripresa o interruzione di un processo (è possibile accedervi direttamente da Process Explorer o dal riquadro Processi).
- **Avvia nuova applicazione:** avvio di nuove applicazioni o processi.
- **Modifica stato di un'altra applicazione:** l'applicazione di origine sta tentando di scrivere nella memoria delle applicazioni di destinazione o di eseguire un codice per suo conto. Questa funzionalità può risultare utile per proteggere un'applicazione essenziale configurandola come applicazione di destinazione in una regola che blocca l'utilizzo di tale operazione.

Operazioni del registro

- **Modifica impostazioni di avvio:** qualsiasi modifica nelle impostazioni che definisce quali applicazioni saranno eseguite all'avvio di Windows. Possono essere individuate, ad esempio, ricercando la chiave Run nel Registro di sistema di Windows.
- **Elimina dal registro:** eliminazione di una chiave del registro o del relativo valore.
- **Rinomina chiave del registro:** ridenominazione delle chiavi del registro.
- **Modifica registro:** creazione di nuovi valori delle chiavi del registro, modifica dei valori esistenti, spostamento dei dati nella struttura del database oppure impostazione dei diritti utente o di gruppo per le chiavi del registro.

Quando si inserisce una destinazione, è possibile utilizzare i caratteri jolly con alcune limitazioni. Al posto di una chiave particolare, nei percorsi dei Registri di sistema è possibile utilizzare il simbolo * (asterisco). Ad esempio `HKEY_USERS*\software` può significare `HKEY_USER\.default\software` ma non `HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software`.

i `HKEY_LOCAL_MACHINE\system\ControlSet*` non è un percorso valido della chiave di Registro del sistema. Un percorso della chiave del Registro di sistema contenente * indica "questo percorso o qualsiasi percorso a qualsiasi livello dopo tale simbolo". Nelle destinazioni dei file i caratteri jolly possono essere utilizzati solo in questo modo. Viene innanzitutto valutato la parte specifica di un percorso, quindi viene esaminato il percorso dopo il carattere jolly (*).

 In caso di creazione di una regola molto generica, verrà visualizzato un avviso.

Nell'esempio seguente viene spiegato come limitare il comportamento indesiderato di una specifica applicazione:

1. Denominare la regola e selezionare **Blocca** (o **Chiedi** se si preferisce scegliere in seguito) nel menu a discesa **Azione**.
2. Abilitare la barra di scorrimento accanto a **Invia una notifica all'utente** per visualizzare una notifica tutte le volte che viene applicata una regola.
3. Selezionare [almeno un'operazione](#) nella sezione **Operazioni che influiscono** per cui verrà applicata la regola.
4. Fare clic su **Avanti**.
5. Nella finestra **Applicazioni di origine** selezionare **Applicazioni specifiche** 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.
6. Fare clic su **Aggiungi** e su ... per scegliere il percorso di un'applicazione specifica, quindi scegliere **OK**.
Aggiungere altre applicazioni, se si preferisce.
Ad esempio: `C:\Program Files (x86)\Untrusted application\application.exe`
7. Selezionare l'operazione **Scrivi su file**.
8. Selezionare **Tutti i file** dal menu di scelta rapida. In tal modo, verrà bloccato qualsiasi tentativo di scrivere su qualsiasi file da parte delle applicazioni selezionate nel passaggio precedente.
9. Fare clic su **Fine** per salvare la nuova regola.

eset NOD32 ANTIVIRUS ×

Impostazioni regola HIPS ?

Nome regola

Azione ▼

Operazioni che influiscono

File di destinazione ☐

Applicazioni ☐

Voci di registro ☐

Attivata ☒

Livello registrazione ▼

Notifica utente ☐

Indietro Avanti Annulla

Aggiungi percorso applicazione/registro per l'HIPS

Fare clic sull'opzione ... per selezionare il percorso dell'applicazione del file. Se si seleziona una cartella, verranno incluse tutte le applicazioni nel percorso.

L'opzione **Apri editor registro** consente di avviare l'editor del Registro di sistema di Windows (regedit). Se si aggiunge un percorso del Registro di sistema, immettere la posizione corretta nel campo **Valore**.

Esempi del percorso del file o del Registro di sistema:

- *C:\Programmi\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Configurazione avanzata di HIPS

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. Utilizzare

questa funzione solo durante la procedura di risoluzione dei problemi o se richiesto dal Supporto tecnico ESET, in quanto potrebbe generare un file di registro di grandi dimensioni e rallentare le prestazioni del computer in uso.

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.

Caricamento driver sempre consentito

Il caricamento dei driver visualizzati in questo elenco è sempre consentito, indipendentemente dalla modalità di filtraggio dell'HIPS, eccetto nel caso in cui vengano bloccati esplicitamente da una regola dell'utente.

Aggiungi: aggiunge un nuovo driver.

Modifica: modifica un driver selezionato.

Rimuovi: rimuove un driver dall'elenco.



Reimposta: ricarica un set di driver di sistema.

i Fare clic su **Reimposta** se non si desidera includere i driver aggiunti manualmente. Questa funzione può rivelarsi utile nel caso in cui l'utente abbia aggiunto vari driver e non possa eliminarli manualmente dall'elenco.

i In seguito all'installazione, l'elenco di driver è vuoto. ESET NOD32 Antivirus completa automaticamente l'elenco nel tempo.

Modalità giocatore

La modalità giocatore è una funzione pensata per gli utenti che richiedono un utilizzo ininterrotto del software, non desiderano essere disturbati dalle finestre di notifica/avviso e mirano a 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 abilitare o disabilitare la modalità giocatore nella [finestra principale del programma](#) in **Configurazione** > **Protezione computer** facendo clic su  o  accanto a **Modalità giocatore**. L'abilitazione della modalità giocatore rappresenta un potenziale rischio per la sicurezza. Di conseguenza, l'icona dello stato di protezione nella barra delle applicazioni diventa arancione e consente di visualizzare un'avvertenza che comparirà anche nella [finestra principale del programma](#) dove il messaggio **Modalità giocatore attiva** è di colore arancione.

Attivare **Attiva modalità giocatore quando vengono eseguite automaticamente applicazioni in modalità a schermo intero** in **Configurazione avanzata (F5)** > **Strumenti** > **Modalità giocatore** 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.

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 della pianificazione attività e dalle attività](#).

Le opzioni di controllo all'avvio fanno parte della pianificazione dell'attività **Controllo del file di avvio del sistema**. Per modificarne le impostazioni, portarsi in **Strumenti > Pianificazione attività** e fare clic su **Controllo automatico 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, consultare [Creazione di nuove attività](#).

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 che seguono:

Il menu a discesa **Destinazione di controllo** 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 ciascun gruppo indicato in precedenza, vengono risolti elenchi di file da controllare. Se si sceglie una profondità di controllo inferiore per i file eseguiti all'avvio del sistema, i file non controllati verranno controllati all'apertura o all'esecuzione.

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.

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 **Configurazione avanzata (F5) > Motore di rilevamento > Controlli malware > Protezione documenti** e fare clic sulla barra di scorrimento accanto ad **Abilita protezione documenti**.

i 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).

Esclusioni

Le **esclusioni** consentono all'utente di escludere [oggetti](#) dal motore di rilevamento. Per garantire che il controllo venga eseguito su tutti gli oggetti, si consiglia di creare esclusioni solo se assolutamente necessario. Le situazioni in cui potrebbe essere necessario escludere un oggetto includono, 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.

[Esclusioni delle prestazioni](#): questa opzione consente di escludere file e cartelle dal controllo. Le esclusioni dal controllo sono utili per escludere il controllo a livello di file delle applicazioni di gioco o quando causano un comportamento anomalo del sistema o aumentano le prestazioni.

[Le esclusioni dal rilevamento](#) consentono all'utente di escludere oggetti del rilevamento utilizzando il nome del rilevamento, il percorso o il relativo hash. Non escludono file e cartelle dal controllo come le esclusioni dal controllo. Le esclusioni dal rilevamento escludono oggetti solo quando vengono rilevati dal motore di rilevamento e nell'elenco di esclusioni è presente una regola appropriata.

Da non confondere con altri tipi di esclusioni:

- [Esclusioni dei processi](#): tutte le operazioni dei file attribuite ai processi delle applicazioni esclusi sono escluse dal controllo (potrebbe essere necessario per migliorare la velocità di esecuzione del backup e la disponibilità del servizio).
- [Estensioni file escluse](#)
- [Esclusioni HIPS](#)
- [Filtro di esclusione per la protezione basata sul cloud](#)

Esclusioni dal controllo

Le esclusioni dal controllo consentono 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 dal controllo solo se assolutamente necessario. Tuttavia, esistono situazioni in cui potrebbe essere necessario escludere un oggetto, ad esempio, voci di database di grandi dimensioni che rallenterebbero il computer durante un controllo o un software che entra in conflitto con il controllo.

È possibile aggiungere file e cartelle da escludere dal controllo nell'elenco di esclusioni tramite **Configurazione avanzata (F5) > Motore di rilevamento > Esclusioni > Esclusioni di prestazioni > Modifica**.

i Da non confondere con [Esclusioni da rilevamento](#), [Estensioni file esclusi](#), [Esclusioni HIPS](#) o [Esclusioni processi](#).

Per [escludere un oggetto](#) (percorso: file o cartella) dal controllo, fare clic su **Aggiungi** e inserire il percorso applicabile oppure selezionarlo nella struttura ad albero.

i 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.

Elementi di controllo

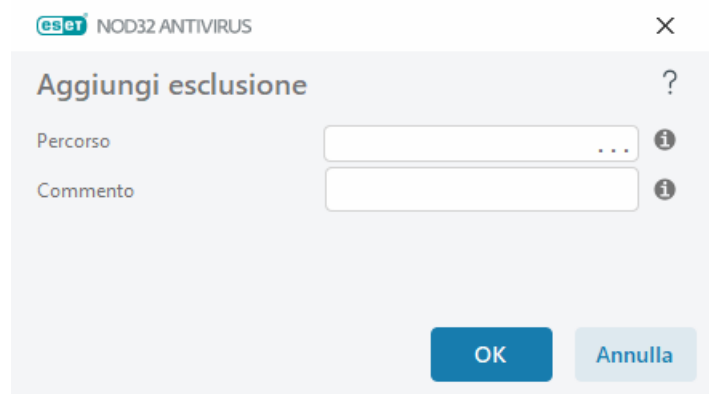
- **Aggiungi:** esclude gli oggetti dal rilevamento.
- **Modifica:** consente all'utente di modificare le voci selezionate.
- **Elimina:** rimuove le voci selezionate (CTRL + fare clic per selezionare voci multiple).

Aggiungi o modifica esclusione di prestazioni

Questa finestra di dialogo esclude un percorso specifico (file o directory) per il computer in uso.

Scegli percorso o immettilo manualmente

- i** Per scegliere un percorso appropriato, fare clic su ... nel campo **Percorso**.
In caso di digitazione manuale, consultare altri [esempi di formati di esclusione](#) di seguito.



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

Formato di esclusione

- Se si desiderano escludere tutti i file e le sottocartelle presenti in una cartella, digitare il percorso della cartella e utilizzare la maschera *
- 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 (variabili) 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)

✓ Esempi:

- C:\Tools*: il percorso deve terminare con la barra rovesciata (\) e l'asterisco (*) per indicare che si tratta di una cartella e che verranno esclusi tutti i contenuti delle cartelle (file e sottocartelle).
- C:\Tools*. *: stesso comportamento di C:\Tools*
- C:\Tools: la cartella Tools non sarà esclusa. Dal punto di vista dello scanner, anche Tools può essere un nome file.
- C:\Tools*.dat: escluderà i file .dat nella cartella Tools.
- C:\Tools\sg.dat: escluderà questo particolare file posizionato nel percorso esatto.

Variabili di sistema nelle esclusioni

È possibile utilizzare variabili di sistema come %PROGRAMFILES% per definire le esclusioni di controllo.

- Per escludere la cartella File di programma utilizzando questa variabile di sistema, utilizzare il percorso %PROGRAMFILES%* (ricordare di aggiungere la barra rovesciata e l'asterisco alla fine del percorso) durante l'aggiunta nelle esclusioni.
- Per escludere tutti i file e le cartelle in una sottodirectory %PROGRAMFILES%, utilizzare il percorso %PROGRAMFILES%\Excluded_Directory*

✓ Espandi l'elenco di variabili di sistema supportate

Le seguenti variabili possono essere utilizzate nel seguente formato di esclusione del percorso:

- %ALLUSERSPROFILE%
- %COMMONPROGRAMFILES%
- %COMMONPROGRAMFILES(X86)%
- %COMSPEC%
- %PROGRAMFILES%
- %PROGRAMFILES(X86)%
- %SystemDrive%
- %SystemRoot%
- %WINDIR%
- %PUBLIC%

Le variabili di sistema specifiche dell'utente (come %TEMP% o %USERPROFILE%) o le variabili di ambiente (come %PATH%) non sono supportate.

I caratteri jolly all'interno di un percorso non sono supportati

! L'utilizzo di caratteri jolly all'interno di un percorso (ad esempio C:\Tools*\Data\file.dat) potrebbe funzionare, ma non è ufficialmente supportato per le esclusioni relative alle prestazioni.

Se si utilizzano le [esclusioni di rilevamenti](#), non sono previste limitazioni relative all'utilizzo di caratteri jolly all'interno di un percorso.

Ordine delle esclusioni

- Non sono disponibili opzioni per regolare il livello di priorità delle esclusioni utilizzando i pulsanti su/giù.
- ✓ Se lo scanner trova la prima regola applicabile, la seconda regola applicabile non sarà valutata.
- Minore è il numero di regole, migliori saranno le prestazioni in termini di controllo.
- Evitare di creare regole concorrenti.

Formato di esclusione percorso

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

Formato di esclusione

- Se si desiderano escludere tutti i file e le sottocartelle presenti in una cartella, digitare il percorso della cartella e utilizzare la maschera *
- 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 (variabili) 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)

✓ Esempi:

- C:\Tools*: il percorso deve terminare con la barra rovesciata (\) e l'asterisco (*) per indicare che si tratta di una cartella e che verranno esclusi tutti i contenuti delle cartelle (file e sottocartelle).
- C:\Tools*. *: stesso comportamento di C:\Tools*
- C:\Tools: la cartella Tools non sarà esclusa. Dal punto di vista dello scanner, anche Tools può essere un nome file.
- C:\Tools*.dat: escluderà i file .dat nella cartella Tools.
- C:\Tools\sg.dat: escluderà questo particolare file posizionato nel percorso esatto.

Variabili di sistema nelle esclusioni

È possibile utilizzare variabili di sistema come %PROGRAMFILES% per definire le esclusioni di controllo.

- Per escludere la cartella File di programma utilizzando questa variabile di sistema, utilizzare il percorso %PROGRAMFILES%* (ricordare di aggiungere la barra rovesciata e l'asterisco alla fine del percorso) durante l'aggiunta nelle esclusioni.
- Per escludere tutti i file e le cartelle in una sottodirectory %PROGRAMFILES%, utilizzare il percorso %PROGRAMFILES%\Excluded_Directory*

✓ [Espandi l'elenco di variabili di sistema supportate](#)

Le seguenti variabili possono essere utilizzate nel seguente formato di esclusione del percorso:

- ✓
- %ALLUSERSPROFILE%
 - %COMMONPROGRAMFILES%
 - %COMMONPROGRAMFILES(X86)%
 - %COMSPEC%
 - %PROGRAMFILES%
 - %PROGRAMFILES(X86)%
 - %SystemDrive%
 - %SystemRoot%
 - %WINDIR%
 - %PUBLIC%

Le variabili di sistema specifiche dell'utente (come %TEMP% o %USERPROFILE%) o le variabili di ambiente (come %PATH%) non sono supportate.

Esclusioni dalla rilevazione

Le esclusioni dal rilevamento consentono di escludere oggetti dalla pulizia rilevamento il nome del rilevamento, il percorso dell'oggetto o il relativo hash.

Come funzionano le esclusioni dal rilevamento

Le esclusioni dal rilevamento non escludono file e cartelle dal controllo come le [Esclusioni dal controllo](#). Le esclusioni dal rilevamento escludono oggetti solo quando vengono rilevati dal motore di rilevamento e nell'elenco di esclusioni è presente una regola appropriata.

✓ Ad esempio (vedere la prima riga nell'immagine seguente), quando un oggetto viene rilevato come Win32/Adware.Optmedia e il file rilevato è C:\Recovery\file.exe. Sulla seconda riga, ogni file, che ha l'hash SHA-1 appropriato, verrà sempre escluso nonostante il nome del rilevamento.

Esclusioni dalla rilevazione



Criteri oggetto	Escludi rilevamento	Commento
C:\Recovery*.*	Win32/Advare.Optmedia	
678C1422DE867141B947EA700E8A2D6114FAFE97	Qualsiasi rilevamento	SuperApi.exe

Aggiungi

Modifica

Elimina

Importa

Esporta

OK

Annulla

Per assicurare il rilevamento di tutte le minacce, si consiglia di creare esclusioni dal rilevamento solo quando assolutamente necessario.

Per aggiungere file e cartelle all'elenco di esclusioni, fare clic su **Configurazione avanzata (F5) > Motore di rilevamento > Esclusioni > Esclusioni di rilevamento > Modifica**.



Da non confondere con [Esclusioni di prestazioni](#), [Estensioni di file esclusi](#), [Esclusioni dell'HIPS](#) o [Esclusioni di processi](#).

Per [escludere un oggetto \(mediante il relativo nome o hash di rilevamento\)](#) dal motore di rilevamento, fare clic su **Aggiungi**.

Per le [Applicazioni potenzialmente indesiderate](#) e le [Applicazioni potenzialmente pericolose](#), è anche possibile creare l'esclusione in base al nome del rilevamento:

- Nella finestra di avviso che segnala il rilevamento (fare clic su **Mostra opzioni avanzate**, quindi selezionare **Escludi dal rilevamento**).
- Dal menu contestuale File di rapporto utilizzando la [procedura guidata Crea esclusione rilevamento](#).
- Facendo clic su **Strumenti > Quarantena**, quindi facendo clic con il pulsante destro del mouse sul file in quarantena e selezionando **Ripristina ed escludi dal controllo** dal menu contestuale.

Criteri oggetto esclusione dal rilevamento

- **Percorso:** limita un'esclusione dal rilevamento per un percorso specifico (o qualsiasi percorso).
- **Nome del rilevamento:** se è presente il nome di un [rilevamento](#) accanto a un file escluso, ciò significa che il file viene escluso solo per quel rilevamento e non per tutti. Se il file si infetta successivamente con altri malware, esso verrà rilevato.

- **Hash:** esclude un file in base a un hash specificato SHA-1, indipendentemente dal tipo, dalla posizione, dal nome o dall'estensione.

Aggiungi o modifica esclusione dal rilevamento

Escludi rilevamento

È necessario fornire un nome del rilevamento ESET valido. Per fornire un nome del rilevamento valido, consultare i [File di rapporto](#) e selezionare **Rilevamenti** dal menu a discesa File di rapporto. Questa opzione è utile in caso di rilevamento di un [campione falso positivo](#) in ESET NOD32 Antivirus. Dal momento che le esclusioni per le infiltrazioni reali sono molto pericolose, provare a escludere solo i file/le directory interessati facendo clic su ... nel campo **Percorso** e/o solo per un periodo di tempo limitato. Le esclusioni si applicano anche alle [Applicazioni potenzialmente indesiderate](#), alle applicazioni potenzialmente pericolose e alle applicazioni sospette.

Consultare ancheo [Formato di esclusione percorso](#).



eset NOD32 ANTIVIRUS

Modifica esclusione

Percorso: C:\Recovery*.***

Hash:

Nome del rilevamento: Win32/Advare.Optmedia

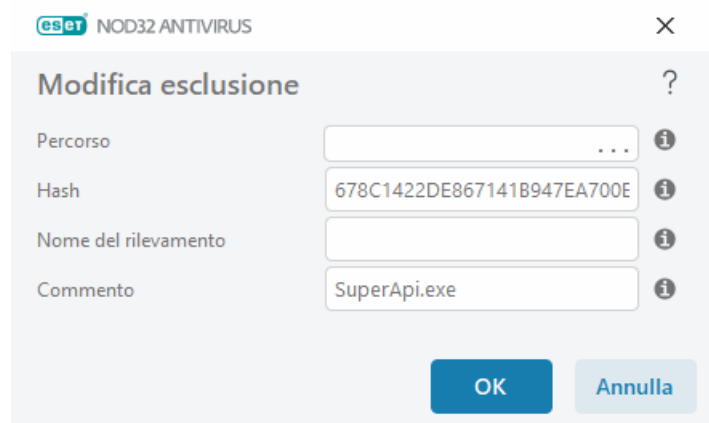
Commento:

OK Annulla

Vedere l'[esempio di esclusioni dal rilevamento](#) di seguito.

Escludi hash

Esclude un file in base a un hash specificato SHA-1, indipendentemente dal tipo, dalla posizione, dal nome o dall'estensione.



eset NOD32 ANTIVIRUS

Modifica esclusione

Percorso:

Hash: 678C1422DE867141B947EA700E

Nome del rilevamento:

Commento: SuperApi.exe

OK Annulla

Esclusioni in base al nome del rilevamento

Per escludere uno specifico rilevamento in base al nome, inserire un nome valido:

Win32/Adware.Optmedia

✓ È anche possibile utilizzare il formato specificato di seguito quando si esclude un rilevamento dalla finestra di avviso ESET NOD32 Antivirus:

@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt

@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan

@NAME=Win32/Bagle.D@TYPE=worm

Elementi di controllo

- **Aggiungi:** esclude gli oggetti dal rilevamento.
- **Modifica:** consente all'utente di modificare le voci selezionate.
- **Elimina:** rimuove le voci selezionate (CTRL + fare clic per selezionare voci multiple).

Crea procedura guidata di esclusione dal rilevamento

Dal menu contestuale [File di rapporto](#) è anche possibile creare un'esclusione dal rilevamento (non disponibile per i rilevamenti malware):

1. Nell' [finestra principale del programma](#), fare clic su **Strumenti > File di rapporto**.
2. Fare clic con il pulsante destro del mouse su un rilevamento nel **Rapporto rilevamenti**.
3. Fare clic su **Crea esclusione**.

Per escludere uno o più rilevamenti sulla base dei **Criteri di esclusione**, fare clic su **Modifica criteri**:

- **File esatti:** consente di escludere ciascun file in base all'hash SHA-1.
- **Rilevamento:** consente di escludere ciascun file in base al nome del rilevamento.
- **Percorso + Rilevamento:** consente di escludere ciascun file in base al nome del rilevamento e al percorso, compreso il nome file (ad es., *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

In base al tipo di rilevamento, viene preselezionata l'opzione consigliata.

Facoltativamente, è possibile aggiungere un **Commento** prima di fare clic su **Crea esclusione**.

Esclusioni HIPS

Le esclusioni consentono all'utente di escludere processi dal Controllo approfondito del comportamento dell'HIPS.

Per modificare le esclusioni HIPS, portarsi in **Configurazione avanzata (F5) > Motore di rilevamento > HIPS > Di base > Esclusioni > Modifica**.



Da non confondere con [Estensioni file esclusi](#), [Esclusioni da rilevamento](#), [Esclusioni da prestazioni](#) o [Esclusioni processi](#).

Per escludere un oggetto, fare clic su **Aggiungi** e immettere il percorso di un oggetto oppure selezionarlo nella struttura ad albero. È anche possibile modificare o rimuovere le voci selezionate.

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 di inattività
- 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'euristiche avanzate 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/UEFI: controlla i settori di avvio alla ricerca di malware nel record di avvio principale. [Per ulteriori informazioni su UEFI, consultare il glossario.](#)

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

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

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 (UPX, 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 conosciuti dalla versione precedente del motore di rilevamento. 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).

Pulizia

Le impostazioni di pulizia determinano il comportamento di ESET NOD32 Antivirus durante la pulizia degli oggetti. Sono disponibili 4 livelli di pulizia:

I parametri di ThreatSense presentano i seguenti livelli di correzione (ad es. pulizia).

Correzione in ESET NOD32 Antivirus

Livello di pulizia	Descrizione
Correggi sempre l'infezione	Tentativo di correzione del rilevamento durante la pulizia degli oggetti senza alcun intervento da parte dell'utente finale. In alcuni rari casi (ad esempio, file di sistema), se il rilevamento non può essere corretto, l'oggetto segnalato viene lasciato nella posizione originale.
Correggi infezione se l'operazione è sicura, altrimenti mantieni	Tentativo di correzione del rilevamento durante la pulizia degli oggetti senza alcun intervento da parte dell'utente finale. In alcuni casi (ad esempio, file di sistema o archivi con file puliti e infetti), se non è possibile correggere un rilevamento, l'oggetto segnalato viene lasciato nella posizione originale.
Correggi l'infezione se l'operazione è sicura, altrimenti chiedi	Tentativo di correzione del rilevamento durante la pulizia degli oggetti. In alcuni casi, se non è possibile eseguire alcuna azione, l'utente finale riceve un avviso interattivo e deve selezionare un'azione correttiva (ad esempio, Elimina o Ignora). Questa impostazione è consigliata nella maggior parte dei casi.
Chiedi sempre all'utente finale	L'utente finale visualizza una finestra interattiva durante la pulizia degli oggetti e deve selezionare un'azione di correzione (p. es., Rimuovi o Ignora). Questo livello è stato pensato per gli utenti più avanzati che conoscono la procedura da adottare in caso di rilevamento.

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 un carico elevato di risorse di sistema, è possibile attivare il controllo in background con priorità bassa e risparmiare risorse per le applicazioni.

Registra tutti gli oggetti: nel [Rapporto del controllo](#) verranno mostrati tutti i file controllati negli archivi autoestraenti, anche quelli non infetti (si potrebbero generare molti dati del rapporto del controllo e aumentarne di conseguenza le dimensioni).

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'ottimizzazione intelligente è disabilitata, durante l'esecuzione di un controllo vengono applicate solo le impostazioni definite dall'utente nella memoria centrale di ThreatSense per i 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. Valore predefinito: illimitato.

Durata massima del controllo dell'oggetto (sec.): definisce il valore temporale massimo per il controllo dei file in un oggetto contenitore (ad esempio, un archivio RAR/ZIP o un'e-mail con allegati multipli). Questa impostazione non si applica ai file indipendenti. Se è stato inserito un valore definito dall'utente e il tempo è trascorso, il controllo di ciascun file in un oggetto contenitore si interrompe il prima possibile, indipendentemente dal fatto che sia stato completato.


Nel caso di un archivio con file di grandi dimensioni, il controllo si interrompe non prima dell'estrazione di un file dall'archivio (ad esempio, se una variabile definita dall'utente è 3 secondi, ma l'estrazione di un file richiede 5 secondi). Al termine di tale intervallo di tempo, non verrà eseguito il controllo degli altri file presenti nell'archivio. Per limitare la durata del controllo, anche relativamente ad archivi di maggiori dimensioni, utilizzare **Dimensioni massime dell'oggetto** e **Dimensioni massime del file in archivio** (scelta non consigliata a causa di possibili rischi per la protezione).

Valore predefinito: illimitato.

Configurazione controllo degli archivi

Livello di nidificazione degli archivi: specifica il livello massimo di controllo degli archivi. Valore predefinito: 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 **3 GB**.

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

Estensioni file esclusi dal controllo

Le estensioni dei file esclusi fanno parte dei parametri [ThreatSense](#). Per configurare le estensioni dei file esclusi, fare clic sui parametri **ThreatSense** nella finestra Configurazione avanzata per i [moduli che utilizzano la tecnologia ThreatSense](#).

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.

 Da non confondere con [Esclusioni processi](#), [Esclusioni HIPS](#) o [Esclusioni file/cartelle](#).

Per impostazione predefinita, vengono controllati tutti i file. 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.

✓ Per aggiungere una nuova estensione all'elenco, fare clic su **Aggiungi**. Digitare l'estensione nel campo vuoto (ad esempio, `tmp`) 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 (ad esempio, scegliere **Punto e virgola** dal menu a discesa come separatore e digitare `edb;eml;tmp`). È possibile utilizzare un simbolo speciale ? (punto interrogativo). Il punto interrogativo rappresenta qualsiasi simbolo (ad esempio `?db`).

i Per visualizzare l'estensione esatta (se presente) di un file in un sistema operativo Windows, è necessario selezionare la casella di controllo **Estensioni nome file** in **Windows Explorer > Vista** (scheda).

Parametri ThreatSense aggiuntivi

Per modificare queste impostazioni, portarsi in **Configurazione avanzata (F5) > Motore di rilevamento > Protezione file system in tempo reale > Parametri ThreatSense aggiuntivi**.

Parametri ThreatSense aggiuntivi per i file appena creati e modificati

La probabilità di infezione nei file appena creati o modificati è relativamente superiore a quella dei file esistenti. Per questo motivo, il programma controlla questi file con parametri di controllo aggiuntivi. ESET NOD32 Antivirus utilizza l'euristica avanzata, in grado di rilevare nuove minacce prima del rilascio dell'aggiornamento del motore di rilevamento insieme ai metodi di controllo basati sulle firme.

Oltre ai file appena creati, il controllo viene eseguito anche sugli **Archivi autoestraenti (.sfx)** e sui **Packer runtime** (file eseguibili compressi internamente). Per impostazione predefinita, gli archivi vengono controllati fino al 10° livello di nidificazione e indipendentemente dalle dimensioni effettive. Per modificare le impostazioni del controllo degli archivi, 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.

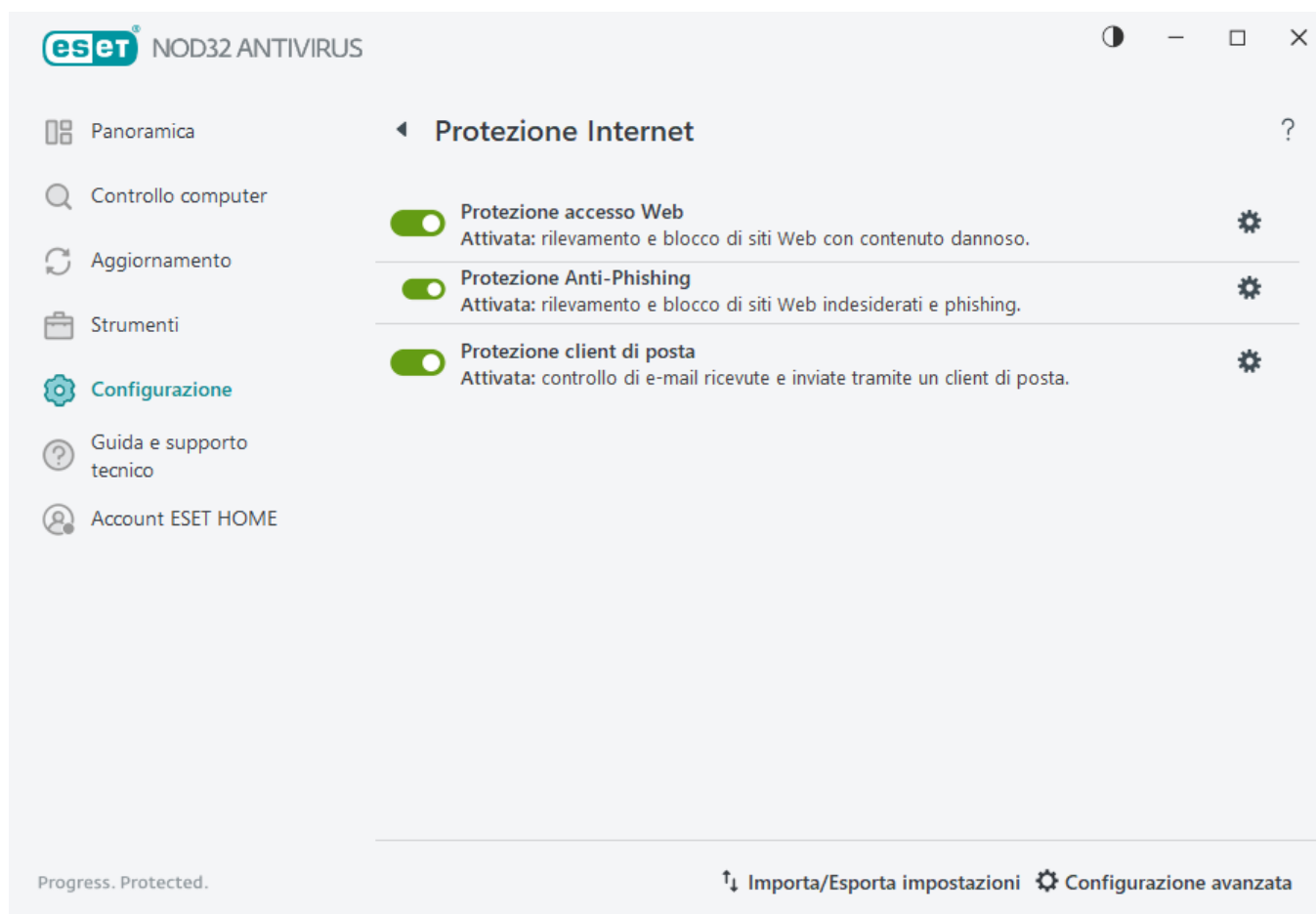
Euristica avanzata all'esecuzione dei file da supporti rimovibili: l'euristica avanzata emula il codice in un ambiente virtuale e ne valuta il comportamento prima che venga consentita l'esecuzione da supporti rimovibili.


Protezione Internet

Per configurare la protezione Internet e la protezione Web ed e-mail, fare clic su **Protezione Internet** nella finestra **Configurazione**. Da qui è possibile accedere a impostazioni del programma più dettagliate.

Per sospendere o disabilitare singoli moduli di protezione, fare clic sull'icona della barra di scorrimento .

 La disattivazione dei moduli di protezione potrebbe ridurre il livello di protezione del computer.



Fare clic sull'icona a forma di ingranaggio  accanto a un modulo di protezione per accedere alle relative impostazioni avanzate.

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](#).

La [Protezione Anti-Phishing](#) consente all'utente di bloccare le pagine Web che distribuiscono notoriamente contenuti phishing. Si consiglia vivamente di lasciare attiva l'opzione Anti-Phishing.

La [Protezione client di posta](#) garantisce il controllo delle comunicazioni via e-mail ricevute mediante i protocolli POP3(S) e IMAP(S). Mediante l'utilizzo del programma plug-in per il client di posta in uso, ESET NOD32 Antivirus controlla tutte le comunicazioni provenienti dal client di posta.

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 **Configurazione avanzata** (F5) > **Web e 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 accessi) 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.

Aggiunge (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*).

Esempio di indirizzi IP esclusi

Indirizzi IPv4 e maschera:

- *192.168.0.10*: aggiunge l'indirizzo IP di un singolo computer a cui deve essere applicata la regola.
- *192.168.0.1* a *192.168.0.99*: immettere il primo e l'ultimo indirizzo IP per specificare l'intervallo IP (di più computer) per cui deve essere applicata la regola.
- Subnet (gruppo di computer) definita da un indirizzo IP e 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*.

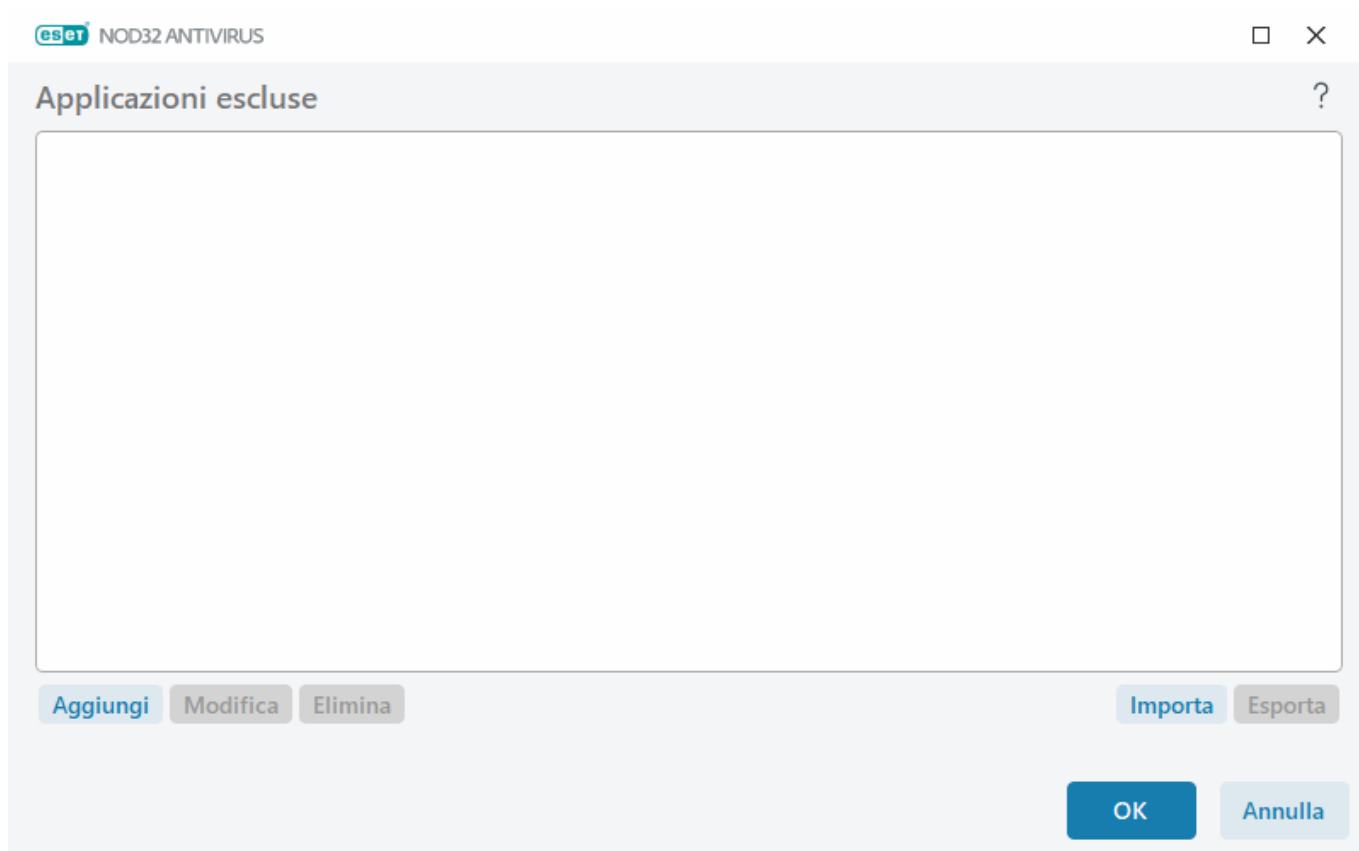
Indirizzo IPv6 e maschera:

- *2001:718:1c01:16:214:22ff:fec9:ca5*: aggiunge l'indirizzo IPv6 di un singolo computer a cui deve essere applicata la regola
- *2002:c0a8:6301:1::1/64*: indirizzo IPv6 con prefisso da 64 bit, che indica l'intervallo di indirizzi compreso tra *2002:c0a8:6301:0001:0000:0000:0000:0000* e *2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

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.

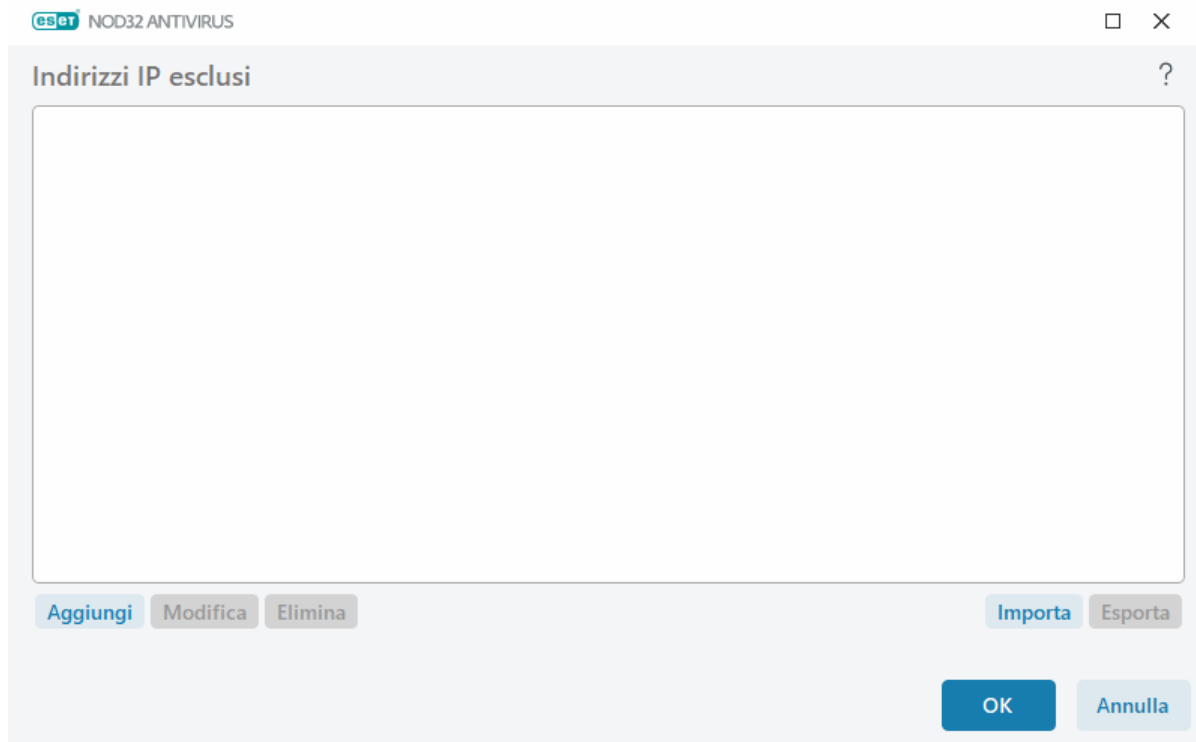


Indirizzi IP esclusi

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 **Elimina** per rimuovere le voci selezionate dall'elenco.



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*.

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 che sostituirà la precedente versione (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*).

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 filtraggio 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 di filtraggio	Descrizione
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	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.

L'**Elenco di applicazioni filtrate tramite SSL/TLS** può essere utilizzato dall'utente per 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 comunicazione con domini attendibili: se questa opzione è attivata, la comunicazione con i domini attendibili sarà esclusa dal controllo. L'attendibilità del dominio è determinata dalla whitelist predefinita.

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 abilitata, ESET NOD32 Antivirus aggiunge automaticamente il certificato ESET SSL Filter CA ai browser conosciuti (ad esempio, Opera). Per i browser che utilizzano l'archivio di certificazioni di sistema, il certificato viene aggiunto automaticamente. Ad esempio, Firefox viene configurato automaticamente sulle autorità Radice attendibili nell'archivio di certificazione del sistema.

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 l'attendibilità del certificato non può essere verificata: in alcuni casi, non è possibile verificare la validità del certificato di un sito web utilizzando l'archivio Autorità di certificazione radice attendibili (Trusted Root Certification Authorities, TRCA). Ciò significa che il certificato è 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. Gran parte delle aziende di maggior dimensioni (ad esempio, le banche) utilizza un certificato firmato dalla TRCA. Dopo aver selezionato **Chiedi conferma della validità del certificato** (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: ciò significa che la firma del certificato è errata o danneggiata. In questo caso, ESET consiglia di lasciare selezionata l'opzione **Blocca comunicazione che utilizza il certificato**. Se è selezionata l'opzione **Chiedi informazioni sulla validità del certificato**, all'utente verrà richiesto di selezionare un'azione da eseguire quando viene stabilita la comunicazione crittografata.

Esempi illustrati

I seguenti articoli della Knowledge Base ESET potrebbero essere disponibili solo in inglese:

- [Notifiche dei certificati nei prodotti ESET Windows Home](#)
- ["Traffico di rete crittografato: certificato non attendibile" compare durante la navigazione delle pagine Web](#)

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 (p. es. Internet Explorer). Per applicare il certificato a browser non supportati, fare clic su **Visualizza certificato > Dettagli > Copia su file** e 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.

Traffico di rete crittografato

Se il sistema in uso è configurato in modo da utilizzare il controllo del protocollo SSL, in due situazioni verrà visualizzata una finestra di dialogo che richiede all'utente di scegliere un'azione:

Innanzitutto, se un sito Web utilizza un certificato non verificabile o non valido e ESET NOD32 Antivirus è configurato in modo da chiedere la conferma dell'utente in tali casi (per impostazione predefinita, "sì" per i certificati non verificabili e "no" per quelli non validi), una finestra di dialogo chiederà all'utente di **Consentire** o **Bloccare** la connessione. Se il certificato non è posizionato in Trusted Root Certification Authorities store (TRCA), viene considerato inattendibile.

In secondo luogo, se la **Modalità filtraggio protocollo SSL** è impostata su **Modalità interattiva**, una finestra di dialogo per ciascun sito Web chiederà all'utente di **Controllare** o **Ignorare** il traffico. Alcune applicazioni verificano che il relativo traffico SSL non sia né modificato né ispezionato da terzi e, in casi come questo, ESET NOD32 Antivirus deve **Ignorare** il traffico per consentire all'applicazione di continuare a funzionare.

Esempi illustrati

I seguenti articoli della Knowledge Base ESET potrebbero essere disponibili solo in inglese:

- [Notifiche dei certificati nei prodotti ESET Windows Home](#)
- ["Traffico di rete crittografato: certificato non attendibile" compare durante la navigazione delle pagine Web](#)

In entrambi i casi, l'utente può scegliere di ricordare l'azione selezionata. Le azioni salvate vengono archiviate nell'[Elenco di certificati noti](#).

Elenco di certificati noti

L'**Elenco di certificati conosciuti** 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/TLS** 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 conosciuti**.

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**.

Elimina: 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.

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: scegliere un file eseguibile dalla struttura della directory, fare clic sull'opzione ... oppure immettere manualmente il percorso.

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 l'applicazione che si desidera configurare e fare clic su **Modifica**.

Rimuovi: selezionare l'applicazione che si desidera rimuovere e fare clic su **Rimuovi**.

Importa/Esporta: importare le applicazioni da un file o salvare l'elenco corrente di applicazioni in un file.

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

Protezione client di posta

Consultare [Integrazione di ESET NOD32 Antivirus con il client di posta](#) per configurare l'integrazione.

Le impostazioni relative al client di posta sono disponibili sotto a **Configurazione avanzata (F5) > Web ed email > Protezione client email > Client email**.


Client di posta

Abilita protezione e-mail con plug-in client: in caso di disabilitazione, la protezione tramite plug-in client di posta è disattivata.

E-mail da controllare

Selezionare le e-mail da controllare:

- E-mail ricevuta
- E-mail inviata
- E-mail letta
- E-mail modificata

 Si consiglia di mantenere l'opzione **Abilita protezione e-mail tramite plug-in client** abilitata. Anche se l'integrazione non è abilitata o funzionale, la comunicazione e-mail rimane comunque protetta tramite il [Filtraggio protocolli](#) (IMAP/IMAPS e POP3/POP3S).

Azione da eseguire sull'e-mail infetta

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 (azione predefinita): 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.

Integrazione 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 è supportato, è possibile abilitare 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, 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 > Integrazione client di posta**.

[Microsoft Outlook](#) è al momento l'unico client di posta supportato. 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. Consultare questo [articolo della Knowledge Base di ESET](#) per un elenco completo delle versioni di Microsoft Outlook supportate.

Ottimizzazione della gestione degli allegati: in caso di disabilitazione dell'ottimizzazione, tutti gli allegati vengono controllati immediatamente. Potrebbe verificarsi un rallentamento delle prestazioni del client di posta.

Elaborazione avanzata client di posta: disabilitare questa opzione in caso di rallentamenti del sistema durante l'utilizzo del client di posta.

Barra degli strumenti di Microsoft Outlook

La protezione Microsoft Outlook funziona come un modulo plug-in. Dopo aver installato ESET NOD32 Antivirus, questa barra degli strumenti contenente le opzioni di protezione antivirus/ viene aggiunta a Microsoft Outlook:

ESET NOD32 Antivirus: fare doppio clic sull'icona per aprire la finestra principale di ESET NOD32 Antivirus.

Ripeti controllo messaggi: consente di avviare manualmente il controllo e-mail. È possibile specificare i messaggi da controllare e attivare un nuovo controllo dei messaggi e-mail ricevuti. Per ulteriori informazioni, consultare [Protezione client di posta](#).

Configurazione scanner: consente di visualizzare le opzioni per la configurazione di [Protezione client di posta](#).

Finestra di dialogo di conferma

Questo messaggio di notifica serve a verificare che l'utente intenda davvero effettuare l'azione selezionata, evitando in questo modo possibili errori.

In questa finestra di dialogo è anche possibile disattivare le richieste di conferma tramite l'apposita opzione.

Ripeti controllo messaggi

La barra degli strumenti di ESET NOD32 Antivirus integrata nei client di posta consente agli utenti di indicare diverse opzioni di controllo e-mail. L'opzione **Ripeti controllo messaggi** offre due modalità di controllo:

Tutti i messaggi nella cartella corrente: esegue il controllo dei messaggi nella cartella visualizzata al momento.

Solo messaggi selezionati: esegue il controllo dei soli messaggi contrassegnati dall'utente.

La casella di controllo **Ripeti controllo sui messaggi già controllati** consente all'utente di eseguire un altro controllo sui messaggi che sono stati già controllati.

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. IMAP presenta alcuni vantaggi rispetto a POP3. Ad esempio, client multipli possono connettersi simultaneamente alla stessa casella di posta e mantenere le informazioni sullo stato dei messaggi, tra cui il fatto che il messaggio sia stato letto, rimosso o abbia ricevuto una risposta. Il modulo di protezione che fornisce questo controllo viene avviato automaticamente all'avvio del sistema e resta quindi attivo in memoria.

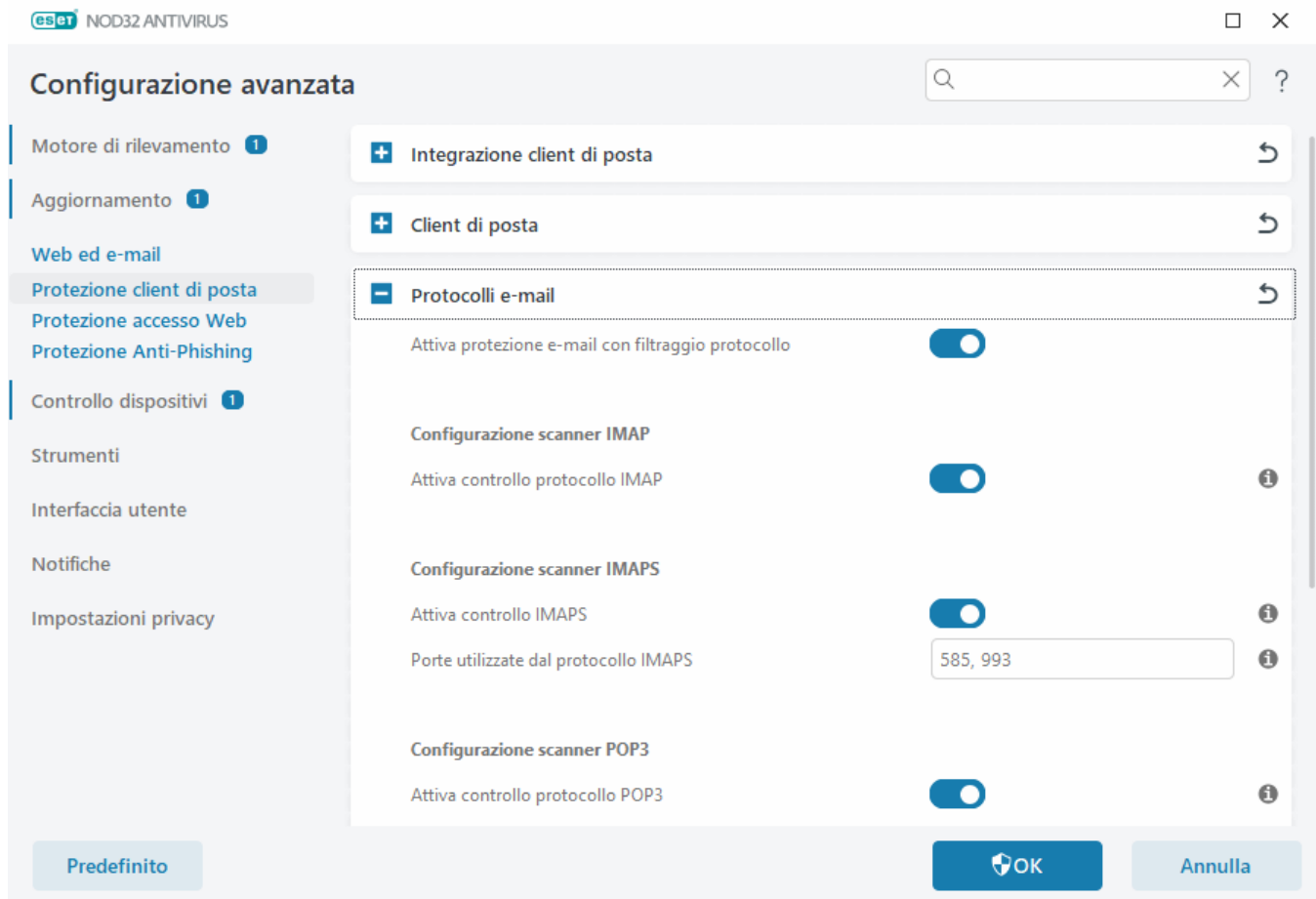
ESET NOD32 Antivirus offre protezione per questi protocolli indipendentemente dal client di posta utilizzato e senza richiederne la riconfigurazione. Per impostazione predefinita, tutte le comunicazioni sui protocolli POP3 e IMAP sono controllate, indipendentemente dai numeri di porta POP3/IMAP.

Il protocollo IMAP non è controllato. Tuttavia, la comunicazione con il server Microsoft Exchange può essere controllata dal [modulo di integrazione](#) nei client di posta quali Microsoft Outlook.

Si consiglia di tenere abilitata l'opzione **Abilita protezione di posta tramite il filtraggio protocolli**. Per configurare il controllo dei protocolli IMAP/IMAPS e POP3/POP3S, portarsi su **Configurazione avanzata > Web ed e-mail > Protezione client di posta > Protocolli e-mail**.

ESET NOD32 Antivirus supporta anche il controllo dei protocolli (585, 993) e POP3S (995) che utilizzano un canale crittografato per trasferire le informazioni tra il server e il 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 IMAPS/POP3S**, indipendentemente dalla versione del sistema operativo. Se necessario, è possibile aggiungere altre porte di comunicazione. I numeri delle porte devono essere delimitati da una virgola.

Le comunicazioni crittografate saranno controllate per impostazione predefinita. Per visualizzare la configurazione dello scanner, aprire Configurazione avanzata > **Web ed e-mail > [SSL/TLS](#)**.



Filtro POP3, POP3S

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

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.

Le comunicazioni crittografate saranno controllate per impostazione predefinita. Per visualizzare la configurazione dello scanner, aprire Configurazione avanzata > **Web ed e-mail** > [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).

Contrassegni e-mail

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

Dopo che un messaggio e-mail è stato controllato, è possibile aggiungere una notifica contenente i risultati del controllo. È possibile scegliere tra le opzioni **Aggiungi notifiche all'e-mail ricevuta e letta** o **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.
- **Quando si verifica un rilevamento:** solo i messaggi contenenti software dannoso vengono contrassegnati come controllati (impostazione predefinita).
- **A tutte le e-mail controllate:** il programma aggiunge le notifiche a tutte le e-mail sottoposte a controllo.

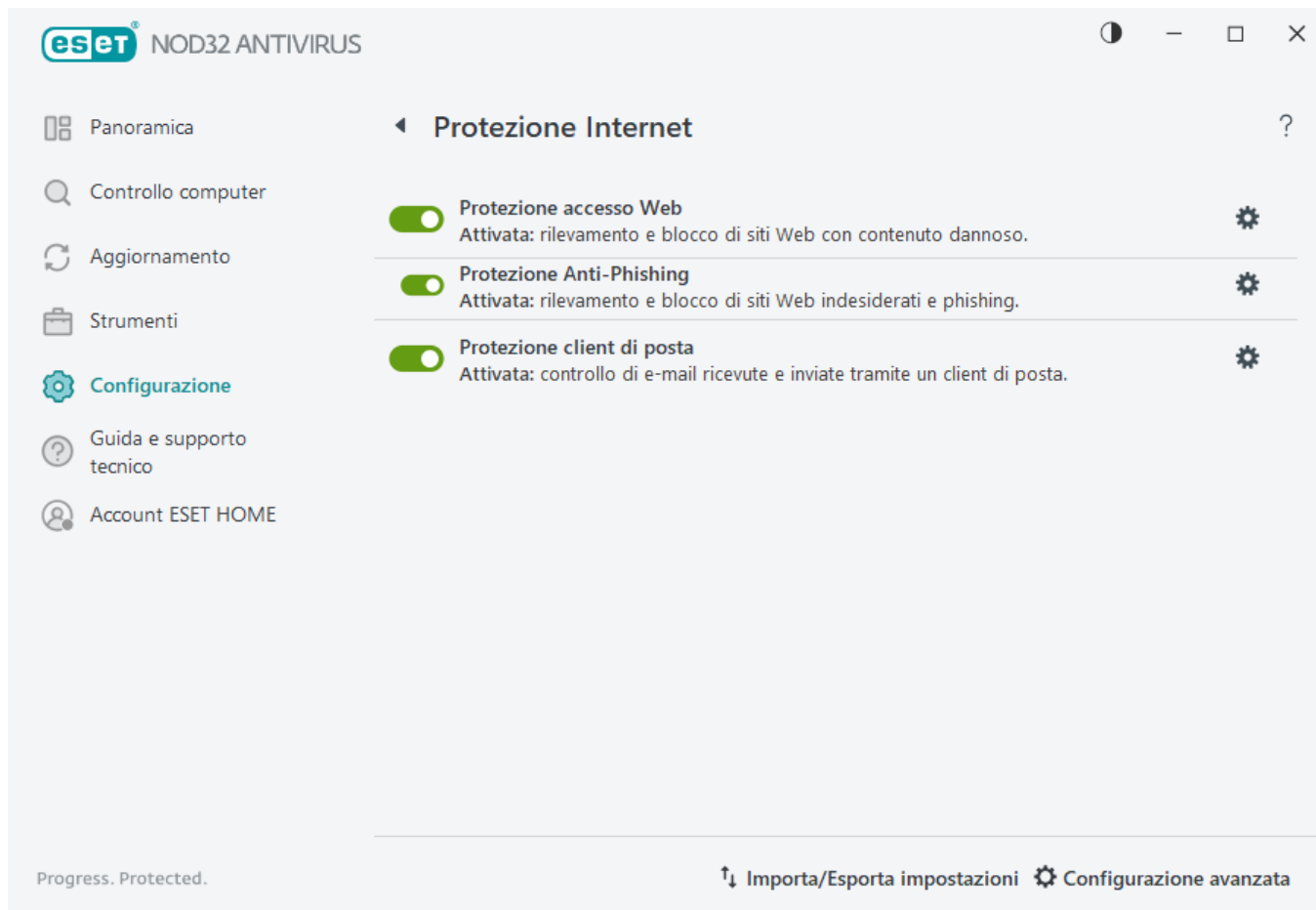
Testo da aggiungere all'oggetto dell'e-mail rilevata: modificare questo modello se si desidera cambiare il formato del prefisso dell'oggetto di un'e-mail infetta. Questa funzione sostituirà l'oggetto del messaggio "Ciao" nel seguente formato: "[detection %DETECTIONNAME%] Ciao". La variabile %DETECTIONNAME% rappresenta il rilevamento.

Protezione accesso Web

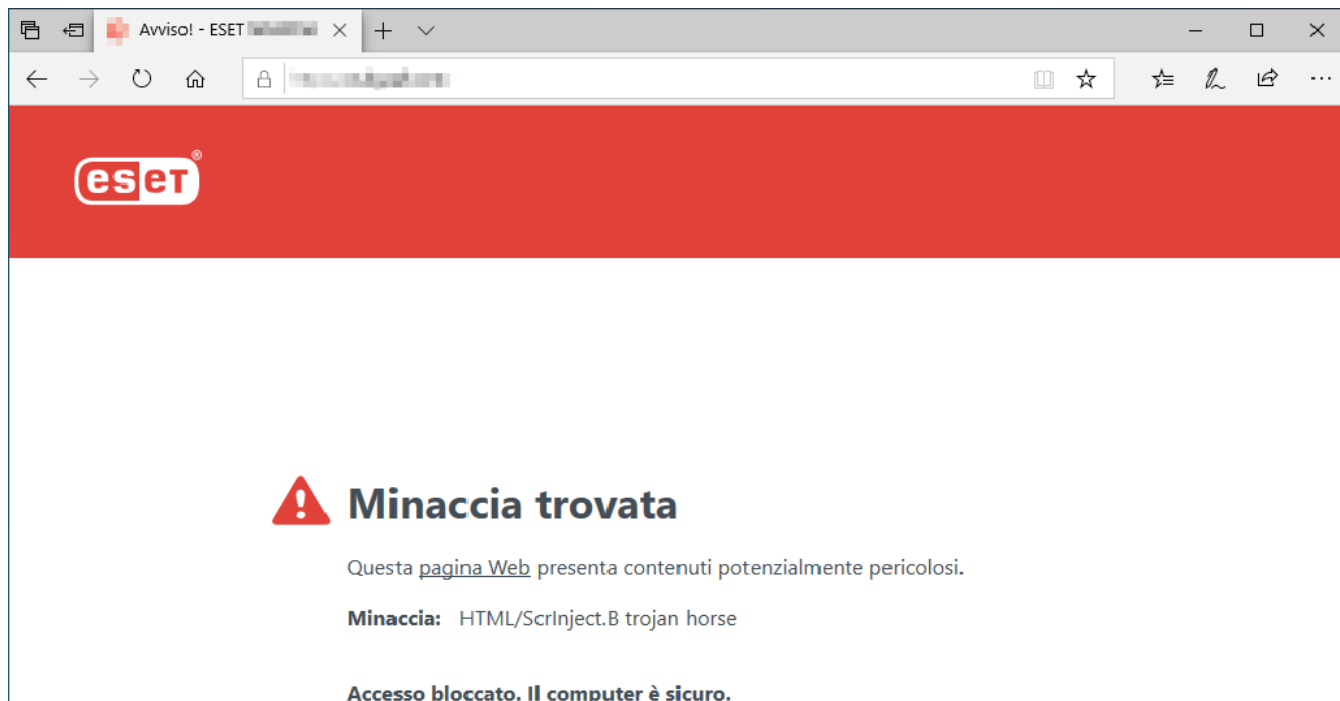
La connettività Internet è una funzione standard in un personal computer. Purtroppo è diventato anche lo strumento principale per il trasferimento di codice dannoso. La Protezione accesso Web controlla le comunicazioni HTTP (Hypertext Transfer Protocol) e HTTPS (comunicazione crittografata) tra i browser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

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 al momento del caricamento e bloccate in caso di rilevamento di contenuti dannosi. La Protezione accesso Web consente all'utente di [bloccare o consentire l'accesso agli indirizzi URL e di escludere indirizzi specifici dal controllo](#).

Si consiglia vivamente di attivare l'opzione Protezione accesso Web. L'opzione è disponibile dalla [finestra principale del programma](#) accedendo a **Configurazione > Protezione Internet > Protezione accesso Web**.



Quando il sito Web è bloccato, la Protezione accesso Web visualizzerà il seguente messaggio nel browser:



Istruzioni illustrate



I seguenti articoli della Knowledge Base ESET potrebbero essere disponibili solo in inglese:

- [Escludi un sito Web sicuro dal blocco attivato dalla Protezione accesso Web](#)
- [Blocca un sito Web utilizzando ESET NOD32 Antivirus](#)

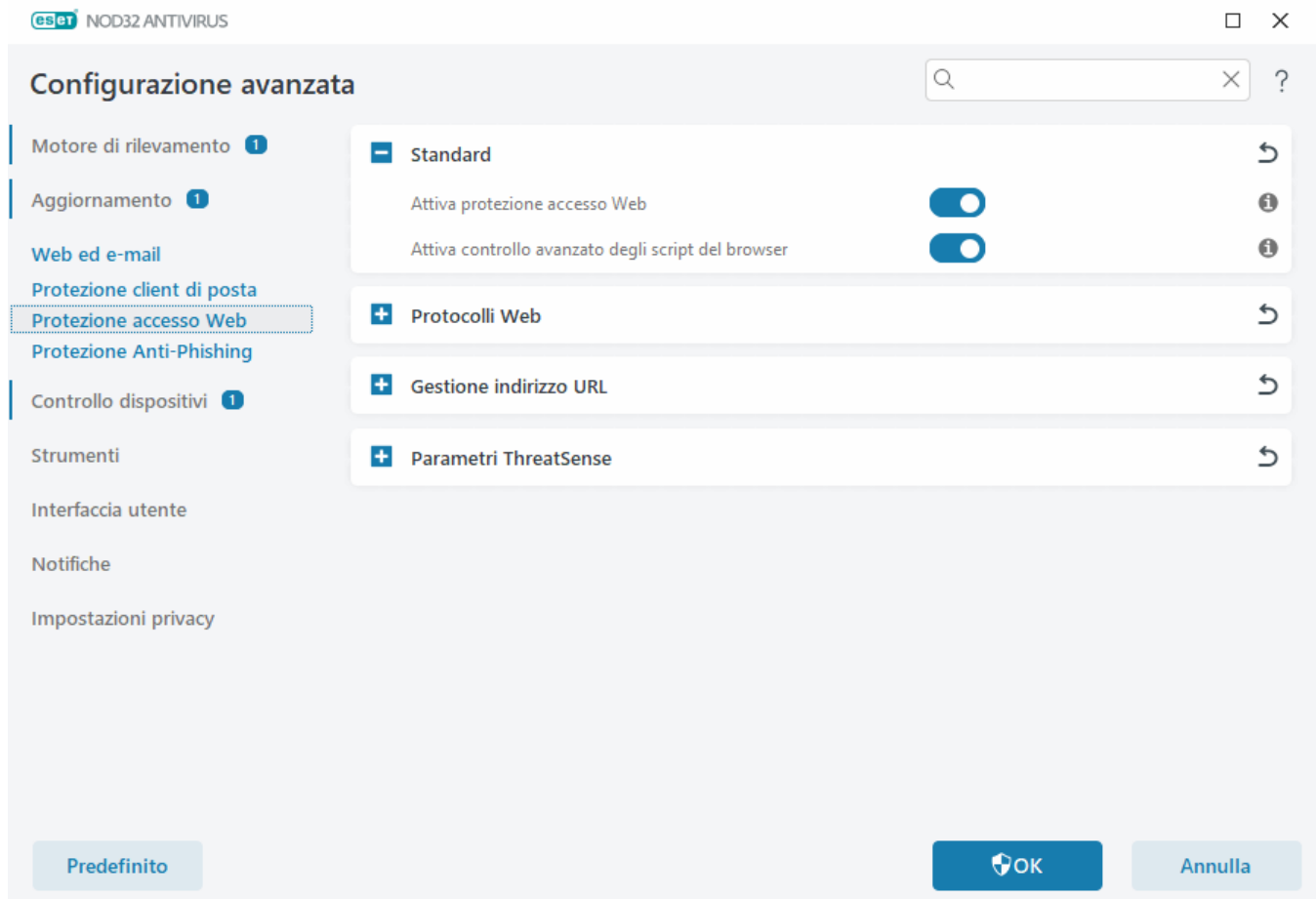
Le seguenti opzioni sono disponibili in **Configurazione avanzata (F5) > Web e e-mail > Protezione accesso Web**:

Di base : attivare o disattivare questa funzione dalla Configurazione avanzata.

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 URL 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.



Configurazione avanzata Protezione accesso Web

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

Attiva protezione accesso Web: se questa opzione è disattivata, la [Protezione accesso Web](#) e la [Protezione Anti-Phishing](#) non saranno eseguite. Questa opzione è disponibile solo in caso di abilitazione del filtraggio protocolli SSL/TLS.

Attiva controllo avanzato degli script del browser: se questa opzione è attivata, tutti i programmi JavaScript eseguiti dai browser Web verranno controllati dal motore di rilevamento.

i Si consiglia vivamente di lasciare l'opzione Protezione accesso Web attivata.

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

Il traffico HTTP viene sempre monitorato su tutte le porte e per tutte le applicazioni.

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 (443, 0-65535) definite in **Porte utilizzate dal protocollo HTTPS**, indipendentemente dalla versione del sistema operativo.

Le comunicazioni crittografate saranno controllate per impostazione predefinita. Per visualizzare la configurazione dello scanner, aprire Configurazione avanzata > **Web ed e-mail** > [SSL/TLS](#).

Gestione indirizzi URL

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

Se si desidera filtrare gli indirizzi HTTPS oltre alle pagine Web HTTP, è necessario selezionare [Attiva filtraggio protocolli SSL/TLS](#). Se questa operazione non viene eseguita, verranno aggiunti solo i domini dei siti HTTPS visitati e non l'intero indirizzo URL.

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 dei contenuti** non vengono ricercati codici dannosi al momento dell'accesso.

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. Prestare attenzione quando si specificano gli indirizzi esclusi, in quanto l'elenco deve contenere solo indirizzi attendibili 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**.

Domini attendibili



Gli indirizzi non saranno filtrati se l'impostazione **Web ed e-mail** > **SSL/TLS** > **Escludi comunicazione con domini attendibili** è attivata e il dominio è considerato attendibile.

Elenco indirizzi



Nome elenco	Tipi di indirizzi	Descrizione elenco
Elenco di indirizzi consentiti	Consentito	
Elenco di indirizzi bloccati	Bloccato	
Elenco di indirizzi esclusi dal controllo dei contenuti	Il malware trovato è stato ...	

Aggiungi

Modifica

Elimina

Importa

Esporta

Aggiungere un carattere jolly (*) all'elenco di indirizzi bloccati per bloccare tutti gli indirizzi URL ad eccezione di quelli presenti in un elenco di indirizzi consentiti.

OK

Annulla

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.

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

Elenco indirizzi URL

In questa sezione, è possibile specificare elenchi di indirizzi HTTP che verranno bloccati, consentiti o esclusi dal controllo.

Per impostazione predefinita, sono disponibili i tre elenchi riportati di seguito:

- **Elenco di indirizzi esclusi dal controllo dei contenuti:** per gli indirizzi aggiunti a questo elenco non verrà eseguita la ricerca di codice dannoso.
- **Elenco di indirizzi consentiti:** se è attivato Consenti accesso solo agli indirizzi HTTP dell'elenco indirizzi consentiti e l'elenco di indirizzi bloccati contiene * (ricerca tutto), l'utente potrà accedere solo agli indirizzi specificati in questo elenco. Gli indirizzi in questo elenco sono consentiti anche se inclusi nell'elenco di indirizzi bloccati.
- **Elenco di indirizzi bloccati:** all'utente non sarà consentito di accedere agli indirizzi indicati in questo elenco a meno che non siano anche presenti nell'elenco di indirizzi consentiti.

Per creare un nuovo elenco, fare clic su **Aggiungi**. Per eliminare gli elenchi selezionati, fare clic su **Elimina**.

Elenco indirizzi



Nome elenco	Tipi di indirizzi	Descrizione elenco
Elenco di indirizzi consentiti	Consentito	
Elenco di indirizzi bloccati	Bloccato	
Elenco di indirizzi esclusi dal controllo dei contenuti	Il malware trovato è stato ...	

Aggiungi

Modifica

Elimina

Importa

Esporta

Aggiungere un carattere jolly (*) all'elenco di indirizzi bloccati per bloccare tutti gli indirizzi URL ad eccezione di quelli presenti in un elenco di indirizzi consentiti.

OK

Annulla

Istruzioni illustrate



I seguenti articoli della Knowledge Base ESET potrebbero essere disponibili solo in inglese:

- [Escludi un sito Web sicuro dal blocco attivato dalla Protezione accesso Web](#)
- [Blocca un sito Web che utilizza prodotti ESET Windows Home](#)

Per ulteriori informazioni, consultare [Gestione indirizzi URL](#).

Creare un nuovo elenco di indirizzi URL

Questa finestra di dialogo consente all'utente di configurare un nuovo [elenco di indirizzi URL/maschere](#) che saranno bloccati, consentiti o esclusi dal controllo.

È possibile configurare le seguenti opzioni:

Tipo di elenco degli indirizzi: sono disponibili tre tipi di elenchi:

- **Il malware trovato è stato ignorato:** per gli indirizzi aggiunti a questo elenco non verrà eseguita la ricerca di codice dannoso.
- **Bloccato:** l'accesso agli indirizzi specificati in questo elenco verrà bloccato.
- **Consentito:** l'accesso agli indirizzi specificati in questo elenco sarà consentito. Gli indirizzi in questo elenco sono consentiti anche se corrispondono all'elenco di indirizzi bloccati.

Nome elenco: specificare il nome dell'elenco. Questo campo non sarà disponibile durante la modifica di uno degli elenchi predefiniti.

Descrizione elenco: digitare una breve descrizione per l'elenco (facoltativo). Non disponibile durante la modifica di uno degli elenchi predefiniti.

Per attivare un elenco, selezionare l'opzione **Elenco attivo** posizionata accanto. Se si desidera ricevere una

notifica in caso di utilizzo di un elenco specifico durante l'accesso ai siti web, selezionare **Invia notifica in caso di applicazione**. Ad esempio, verrà inviata una notifica se un sito web è bloccato o consentito perché incluso in un elenco di indirizzi bloccati o consentiti. La notifica conterrà il nome dell'elenco.

Gravità della registrazione: le informazioni sull'elenco specifico utilizzato durante l'accesso ai siti web possono essere scritte nei [File di rapporto](#).

Elementi di controllo

Aggiungi: aggiunge un nuovo indirizzo URL all'elenco (inserire valori multipli con separatore).

Modifica: modifica l'indirizzo esistente nell'elenco. Disponibile solo per gli indirizzi creati con **Aggiungi**.

Rimuovi: elimina gli indirizzi esistenti nell'elenco. Disponibile solo per gli indirizzi creati con **Aggiungi**.

Importa: importa un file con gli indirizzi URL (separare i valori con un'interruzione di riga, ad esempio *.txt, utilizzando la codifica UTF-8).

Come aggiungere una maschera per l'URL

Prima di inserire l'indirizzo/maschera di dominio desiderato, consultare le istruzioni fornite in questa finestra di dialogo.

ESET NOD32 Antivirus consente all'utente di bloccare l'accesso ai siti Web specificati e di impedire al browser Internet di visualizzarne il contenuto. Consente inoltre all'utente di specificare gli indirizzi che devono essere esclusi dal controllo. Se non si conosce il nome completo del server remoto oppure se l'utente desidera specificare un intero gruppo di server remoti, è possibile utilizzare le cosiddette maschere per identificare tale gruppo. Le maschere includono i simboli "?" e "*":

- utilizzare ? per sostituire un simbolo
- utilizzare * per sostituire una stringa di testo.

Ad esempio, *.c?m si applica a tutti gli indirizzi in cui l'ultima parte inizia con la lettera c, termina con la lettera m e contiene un simbolo sconosciuto tra di esse (.com, .cam e così via).

Alla sequenza "*" iniziale verrà riservato un trattamento speciale se utilizzata all'inizio del nome del dominio. Innanzitutto, in questo caso, il carattere jolly * non corrisponde alla barra ("/"). Ciò per evitare di eludere la maschera, ad esempio, la maschera *.domain.com non corrisponderà a *http://anydomain.com/anypath#.domain.com* (tale suffisso può essere aggiunto a qualsiasi URL senza influenzare il download). In secondo luogo, nel caso specifico, il carattere "*" corrisponde anche a una stringa vuota. Questo per consentire la corrispondenza dell'intero dominio, compresi eventuali sottodomini che utilizzano una singola maschera. Ad esempio, la maschera *.domain.com corrisponde anche a *http://domain.com*. L'utilizzo di **domain.com* non sarebbe corretto poiché corrisponderebbe anche a *http://anotherdomain.com*.

Protezione Anti-Phishing

Il phishing è un'attività illecita che si avvale dell'ingegneria sociale (utilizzata per manipolare gli utenti allo scopo di ottenere informazioni riservate). Consente di accedere a dati sensibili quali numeri di conti bancari, PIN e così via. Per ulteriori informazioni, consultare il [glossario](#). ESET NOD32 Antivirus integra sistemi di protezione anti-

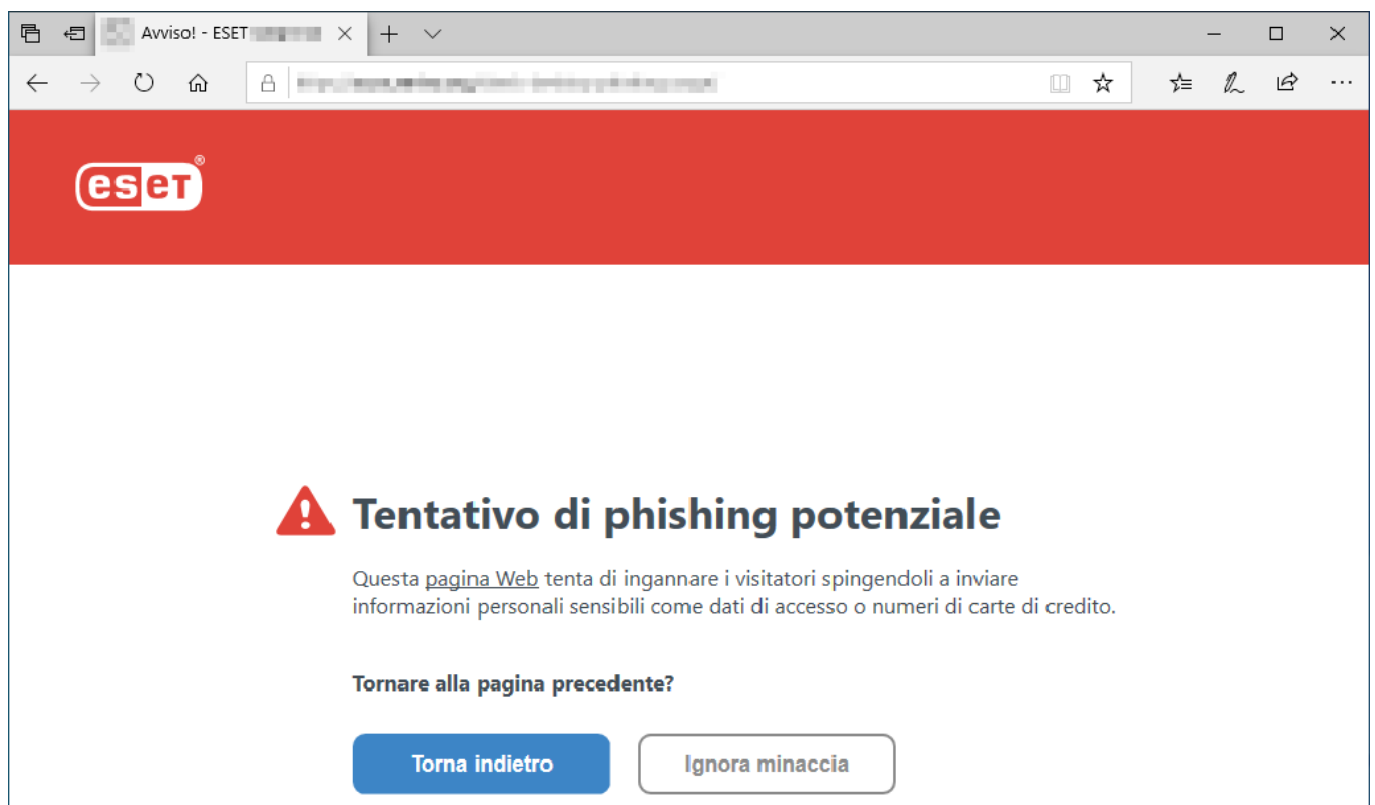
phishing in grado di bloccare pagine web note per distribuire questo tipo di contenuto.

La protezione anti-phishing è abilitata per impostazione predefinita. È possibile accedere a questa impostazione dalla [finestra principale del programma](#) > **Configurazione avanzata** (F5) > **Protezione 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 a un sito Web phishing

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



[Segnalare la pagina bloccata per errore](#)

[Ulteriori informazioni sul phishing](#) | www.eset.com



Per impostazione predefinita, i potenziali siti web di 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](#). In **Configurazione avanzata** (F5) > **Web ed e-mail** > **Protezione accesso web** > **Gestione indirizzi URL** > **Elenco di indirizzi**, fare clic su **Modifica** e aggiungere nell'elenco il sito web che si desidera modificare.

Segnala un sito phishing

Il collegamento **Segnala** consente di segnalare un sito Web phishing/dannoso a ESET per l'analisi.



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 samples@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.).

Aggiornamento del programma

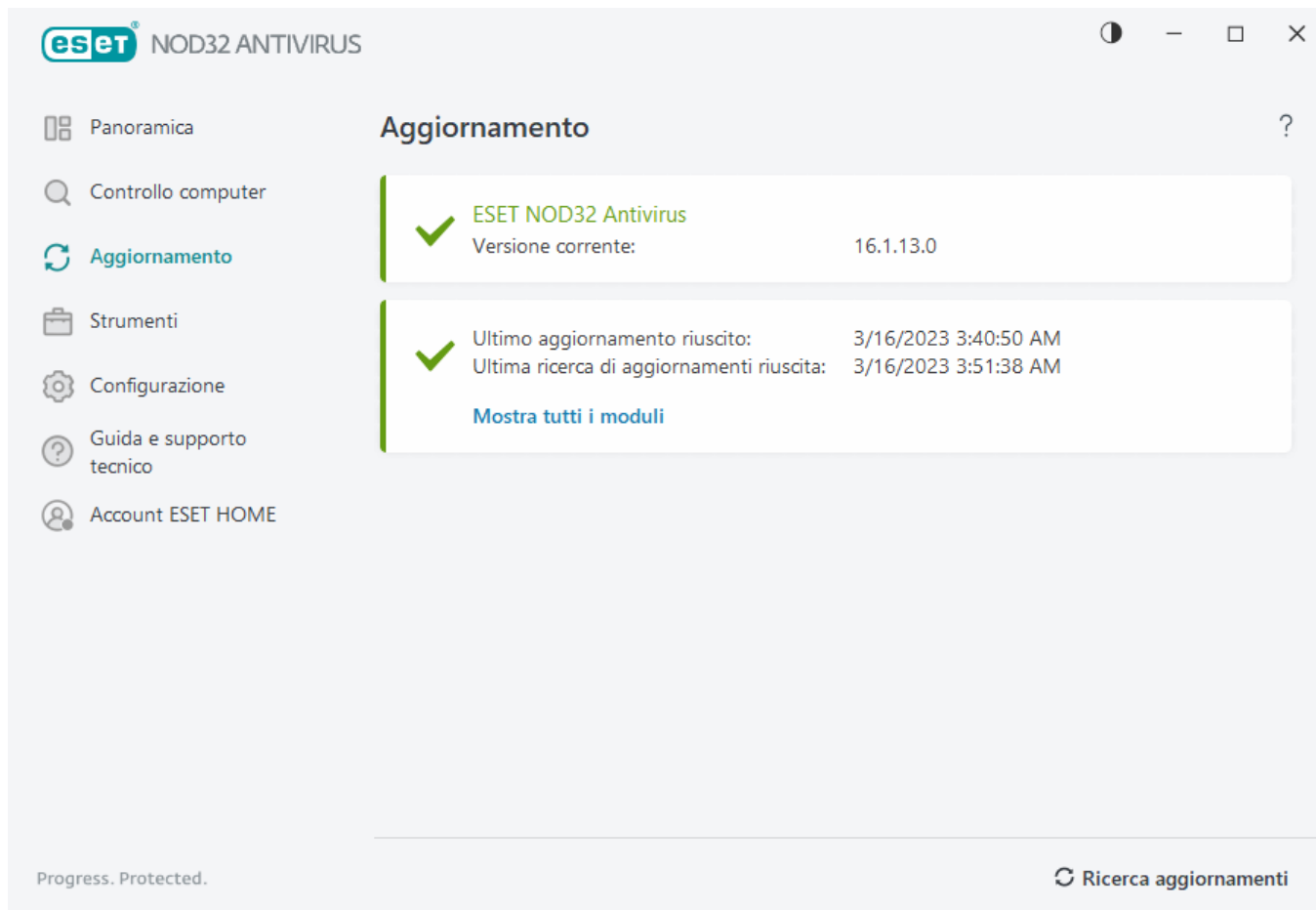
L'aggiornamento periodico di ESET NOD32 Antivirus rappresenta il metodo migliore per garantire il livello massimo di protezione del computer. Il modulo di aggiornamento garantisce il costante aggiornamento dei moduli del programma e dei componenti del sistema.

Facendo clic su **Aggiornamento** 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 **Cerca aggiornamenti** per attivare 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 configurazione e al funzionamento dei moduli del prodotto. Per ricevere gli aggiornamenti, è necessario attivare il prodotto tramite la chiave di licenza. Se durante l'installazione non è stata eseguita questa operazione, sarà necessario inserire la chiave di licenza per attivare il prodotto e accedere ai server di aggiornamento di ESET durante l'aggiornamento.



La chiave di licenza è stata inviata all'utente 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 riuscito: consente di visualizzare la data dell'ultimo aggiornamento riuscito. Se non viene visualizzata una data recente, i moduli del prodotto potrebbero non essere aggiornati.

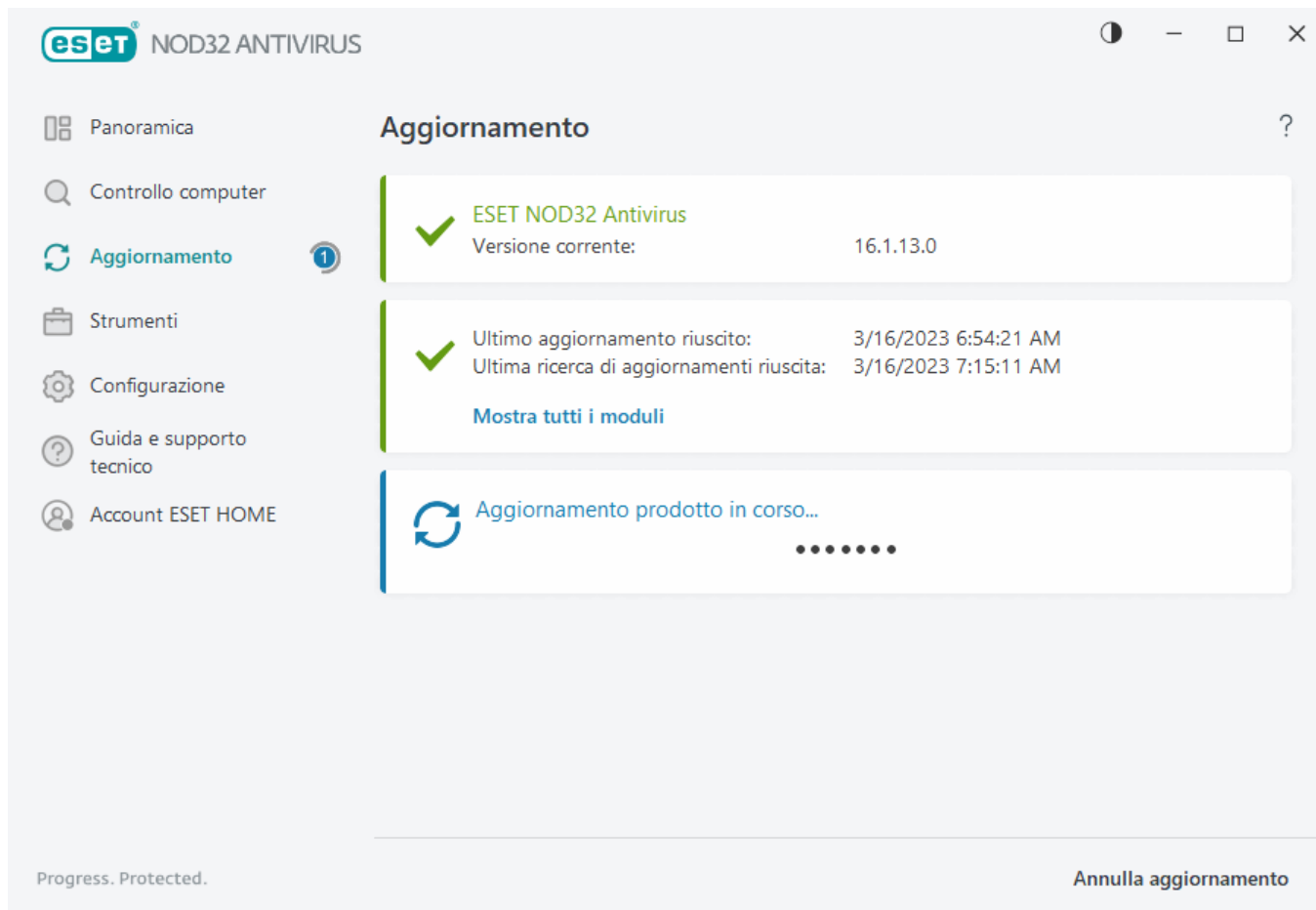
Ultima ricerca di aggiornamenti riuscita: consente di visualizzare la data dell'ultima ricerca di aggiornamenti riuscita.

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**.

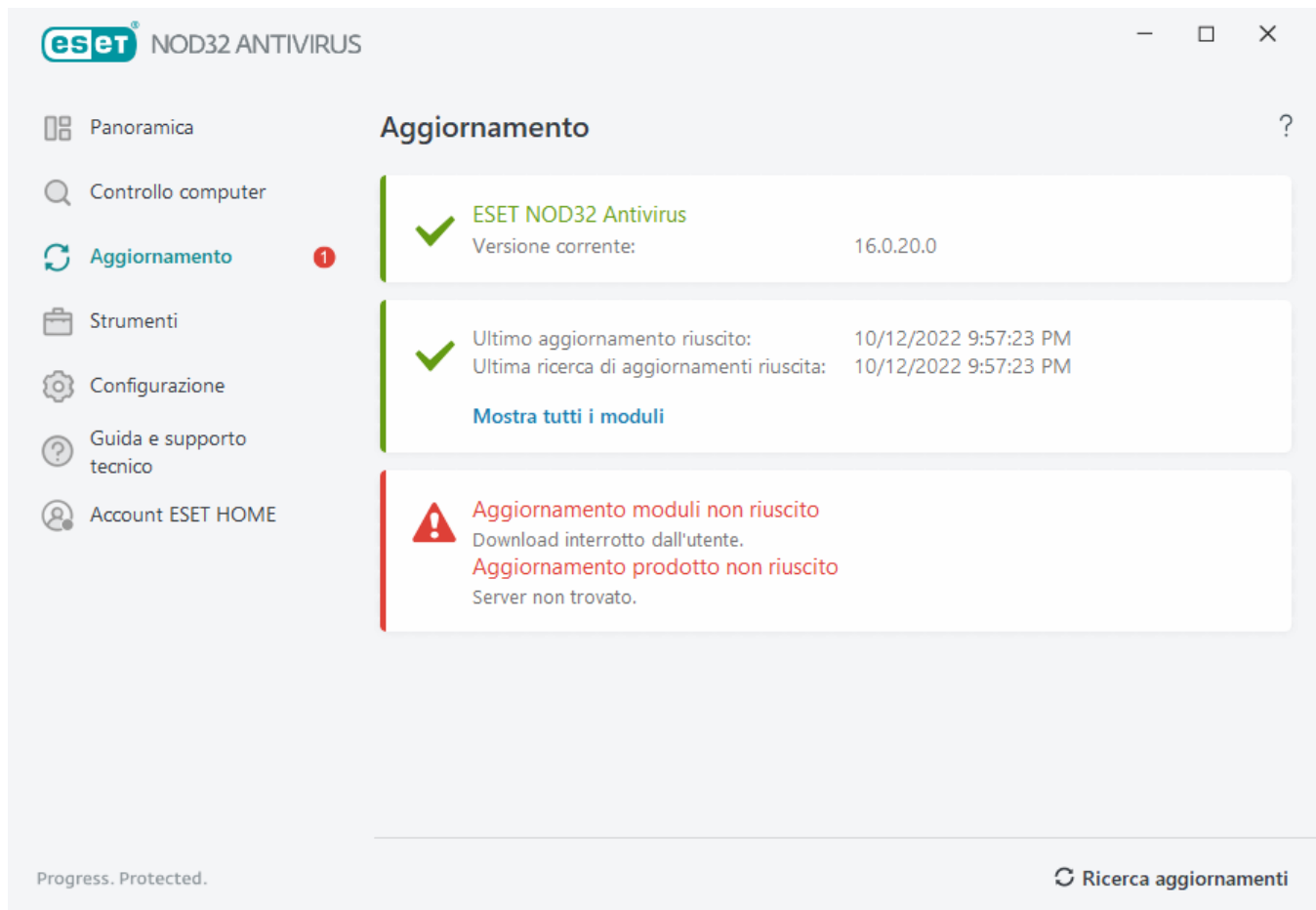


In condizioni normali, nella finestra **Aggiorna** comparirà il segno di spunta verde che indica che il programma è aggiornato. In caso contrario, il programma è obsoleto ed è maggiormente esposto alle infezioni. Aggiornare i moduli del programma il prima possibile.

Aggiornamento non riuscito

La ricezione di un messaggio relativo a un aggiornamento dei moduli non riuscito potrebbe essere dovuta ai problemi indicati di seguito:

1. **Licenza non valida:** la licenza utilizzata per l'attivazione non è valida o è scaduta. Nella [finestra principale del programma](#) fare clic su **Guida e supporto tecnico > Modifica licenza** e attivare il prodotto.
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).



Si consiglia di riavviare il computer in seguito all'installazione di una versione più recente del prodotto ESET NOD32 Antivirus per assicurarsi che tutti i moduli del programma siano stati aggiornati correttamente. Gli aggiornamenti periodici dei moduli non richiedono il riavvio del computer.

Per ulteriori informazioni, consultare [Risoluzione dei problemi relativi al messaggio "Aggiornamento moduli non riuscito"](#).

Configurazione dell'aggiornamento

Le opzioni di configurazione degli aggiornamenti sono disponibili nella struttura **Configurazione avanzata** (F5) sotto a **Aggiornamento > Standard**. 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.

Di base

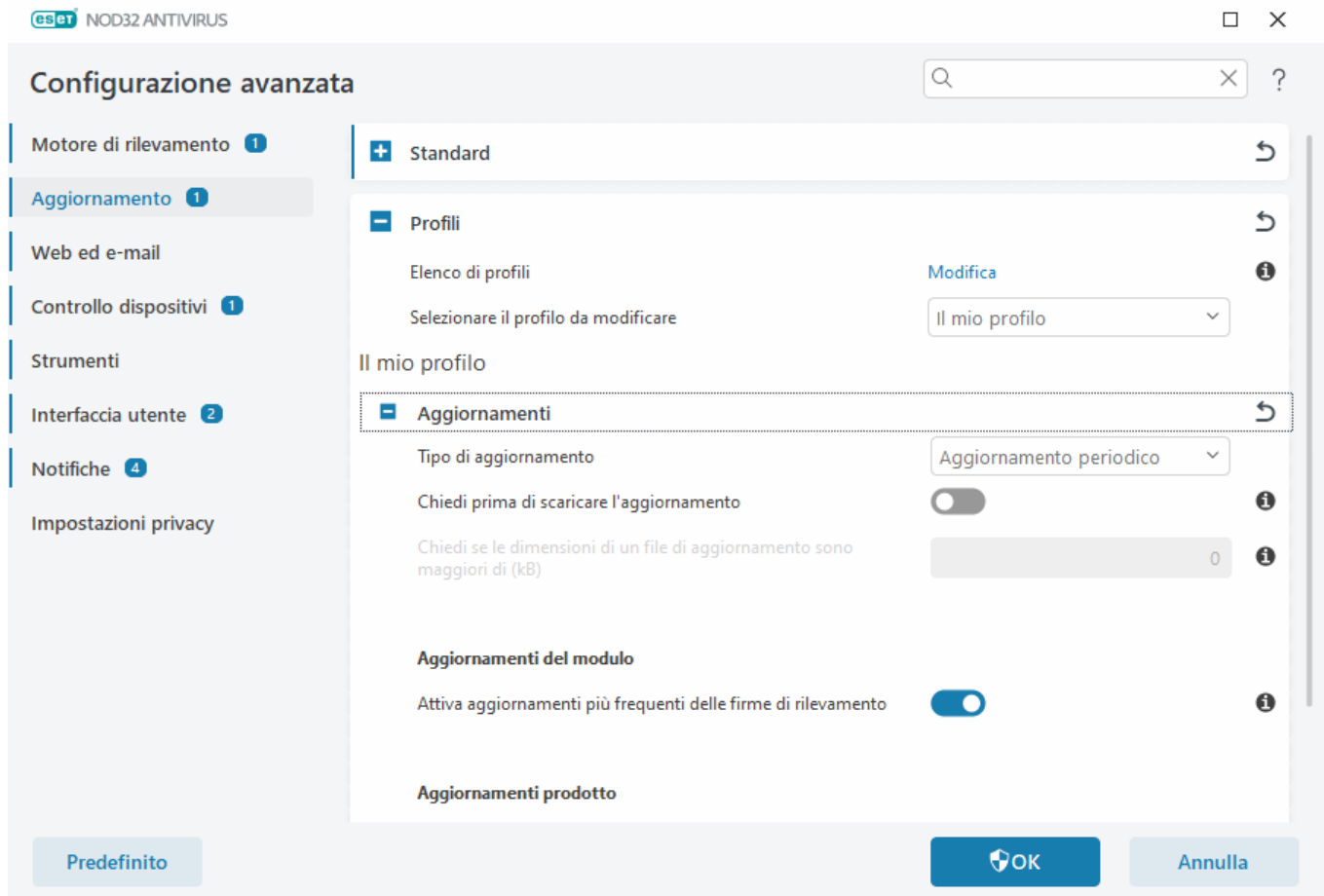
Il profilo di aggiornamento attualmente in uso (a meno che non ne venga impostato uno specifico in **Configurazione avanzata > Firewall > Reti note**) compare nel menu a discesa **Seleziona profilo di aggiornamento predefinito**.

Per creare un nuovo profilo, consultare la sezione [Profili di aggiornamento](#).

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

Rollback modulo

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.



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).

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 **Seleziona profilo da modificare** 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**.

Aggiornamenti

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.

Chiedi prima di scaricare l'aggiornamento: il programma mostra una notifica in cui l'utente può scegliere di confermare o non confermare il download dei file di aggiornamento.

Chiedi se le dimensioni di un file di aggiornamento sono maggiori di (kB): il programma consente di visualizzare una finestra di dialogo di conferma se la dimensione del file di aggiornamento è superiore al valore specificato. Se le dimensioni del file di aggiornamento sono impostate su 0, il programma mostra sempre una finestra di dialogo di conferma.

Aggiornamenti moduli

Attiva aggiornamenti più frequenti delle firme di rilevamento: le firme di rilevamento saranno aggiornate con maggiore frequenza. La disattivazione di questa impostazione potrebbe influire negativamente sulla velocità di rilevamento.

Aggiornamenti del prodotto

Aggiornamenti delle funzioni dell'applicazione: consente di installare automaticamente le nuove versioni di ESET NOD32 Antivirus.

Opzioni connessione

Per utilizzare un server proxy per il download degli aggiornamenti, consultare la sezione [Opzioni di connessione](#).

Rollback aggiornamento

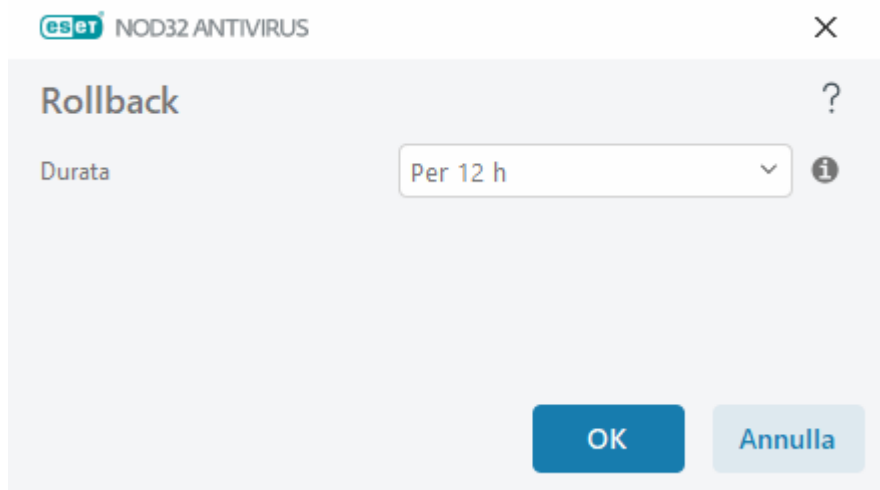
Se si sospetta che un nuovo aggiornamento del motore di rilevamento o dei moduli del programma possa essere instabile o danneggiato, è possibile ripristinare la versione precedente e disabilitare temporaneamente gli aggiornamenti. In alternativa, è possibile abilitare gli aggiornamenti precedentemente disabilitati 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 funzionalità rollback. Per creare snapshot del database dei virus, mantenere abilitata l'opzione **Crea snapshot dei moduli**. Quando l'opzione **Crea snapshot dei moduli** è abilitata, il primo snapshot viene creato durante il primo aggiornamento. Quello successivo viene creato dopo 48 ore. Il campo **Numero di snapshot archiviati localmente** definisce il numero di snapshot del motore di rilevamento archiviati.



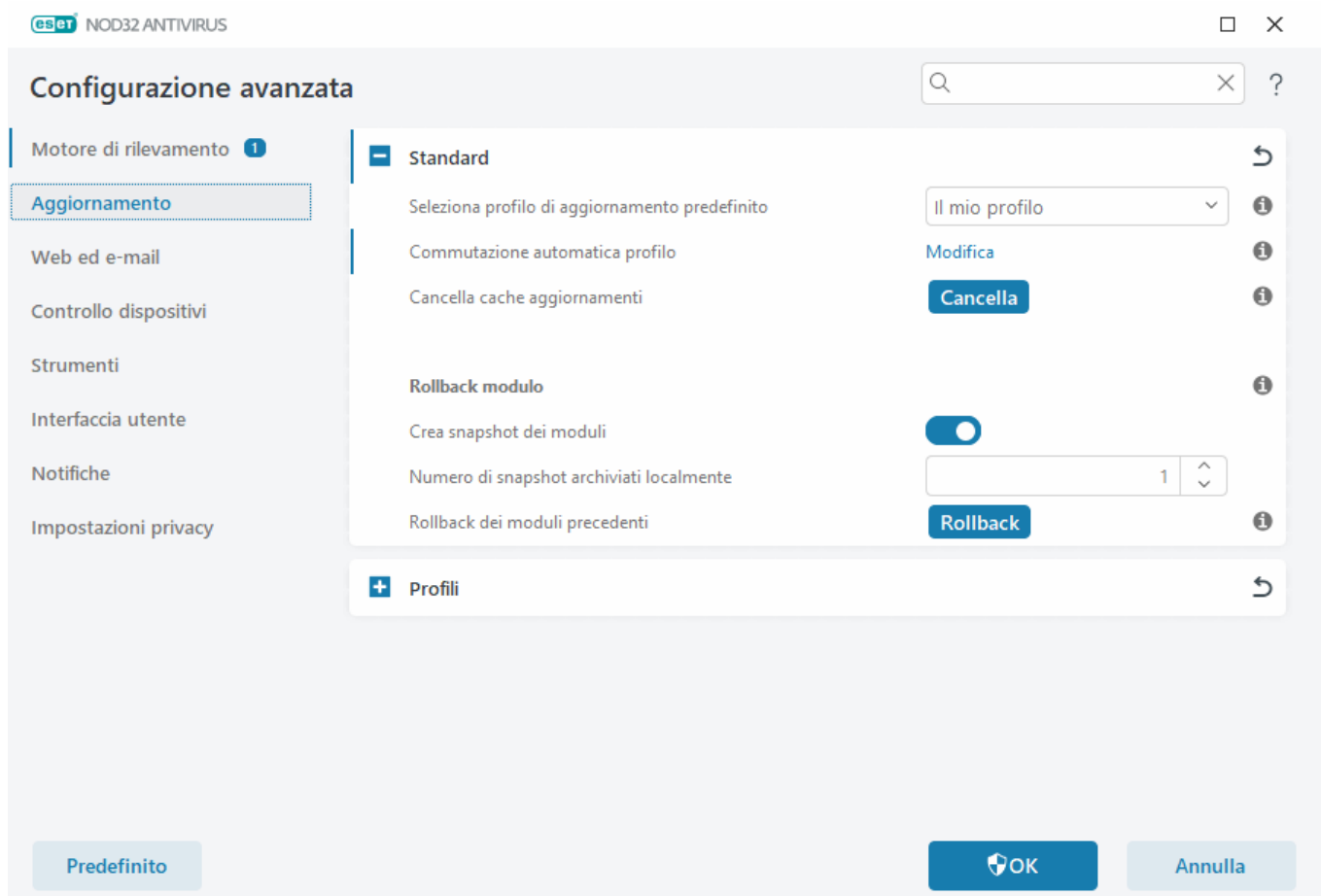
Quando viene raggiunto il numero massimo di snapshot (ad esempio, tre), lo snapshot meno recente viene sostituito con un nuovo snapshot ogni 48 ore. ESET NOD32 Antivirus ripristina le versioni meno recenti dell'aggiornamento del motore di rilevamento e del modulo del programma.

Se si seleziona **Rollback (Configurazione avanzata (F5) > Aggiornamento > Di base)**, 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. ESET sconsiglia di selezionare questa opzione in quanto rappresenta un potenziale rischio per la protezione.

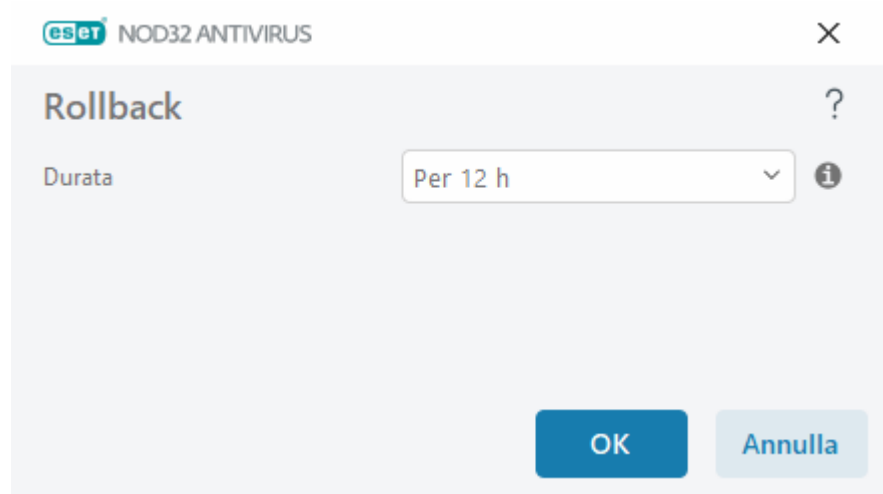
Se viene eseguito un rollback, il pulsante **Rollback** si trasforma in **Consenti aggiornamenti**. Non saranno consentiti aggiornamenti per l'intervallo di tempo selezionato nel menu a discesa **Sospendi aggiornamenti**. Il motore di rilevamento viene ripristinato alla versione meno recente disponibile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



✓ Si supponga che 22700 sia il numero della versione più recente del motore di rilevamento e che 22698 e 22696 siano archiviati come snapshot del motore di rilevamento. Si tenga presente che 22697 non è disponibile. In questo esempio, il computer era spento durante l'aggiornamento 22697 ed è stato reso disponibile un aggiornamento più recente prima del download di 22697. Se il campo **Numero di snapshot archiviati localmente** è due e si fa clic su **Rollback**, il motore di rilevamento (inclusi i moduli del programma) viene ripristinato sul numero di versione 22696. Questo processo potrebbe richiedere alcuni istanti. Verificare che nella schermata [Aggiornamento](#) sia stata ripristinata la versione precedente del motore di rilevamento.

Intervallo temporale di rollback

Se si seleziona **Rollback (Configurazione avanzata (F5) > Aggiornamento > Di base)**, 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. ESET sconsiglia di selezionare questa opzione in quanto rappresenta un potenziale rischio per la protezione.

Aggiornamenti del prodotto

La sezione **Aggiornamenti prodotto** consente all'utente di installare nuovi aggiornamenti delle funzioni, se disponibili automaticamente.

Gli aggiornamenti delle funzioni dell'applicazione introducono nuove funzioni o modificano quelle già esistenti nelle versioni precedenti. Possono essere eseguiti automaticamente senza alcun intervento da parte dell'utente oppure è possibile scegliere di ricevere una notifica. Dopo aver installato un aggiornamento delle funzioni dell'applicazione, potrebbe essere necessario riavviare il computer.

Aggiornamenti delle funzioni dell'applicazione: abilitando questa opzione, gli aggiornamenti delle funzioni dell'applicazione verranno eseguiti automaticamente.

Opzioni connessione

Per accedere alle opzioni di configurazione del server proxy per uno specifico profilo di aggiornamento, fare clic su **Aggiornamento** nella struttura ad albero **Configurazione avanzata** (F5), quindi su **Profili > Aggiornamenti > Opzioni di connessione**. 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 **Utilizza impostazioni server proxy globali** per utilizzare le opzioni di configurazione del server proxy già specificate in **Configurazione avanzata > Strumenti > Server proxy**.

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 **Configurazione avanzata > 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 conatterà 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 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.



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 e una password per accedere al server proxy. Questi campi devono essere completati solo se è necessaria una password per accedere a Internet mediante un server proxy.

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 periodico**
- **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](#).

Finestra di dialogo - Riavvio necessario

Dopo aver aggiornato ESET NOD32 Antivirus a una nuova versione, è necessario riavviare il computer. Le nuove versioni di ESET NOD32 Antivirus vengono rilasciate per introdurre miglioramenti o correggere problemi che gli aggiornamenti automatici dei moduli del programma non possono risolvere.

La nuova versione di ESET NOD32 Antivirus può essere installata automaticamente, in base alle [impostazioni di aggiornamento del programma](#), o manualmente [scaricando e installando una versione più recente](#) su quella precedente.

Fare clic su **Riavvia ora** per riavviare il computer. Se si prevede di riavviare il computer in un secondo momento, fare clic su **Visualizza in seguito**. In seguito, è possibile riavviare manualmente il computer dalla sezione **Panoramica** nella [finestra principale del programma](#).

Strumenti

Il menu **Strumenti** include funzioni che offrono un livello aggiuntivo di protezione e aiutano a semplificare l'amministrazione di ESET NOD32 Antivirus. Sono disponibili i seguenti strumenti:



[File di rapporto](#)



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



[Report di protezione](#)



[ESET SysInspector](#)



[Pianificazione attività](#)



[Strumento di pulizia del sistema](#)



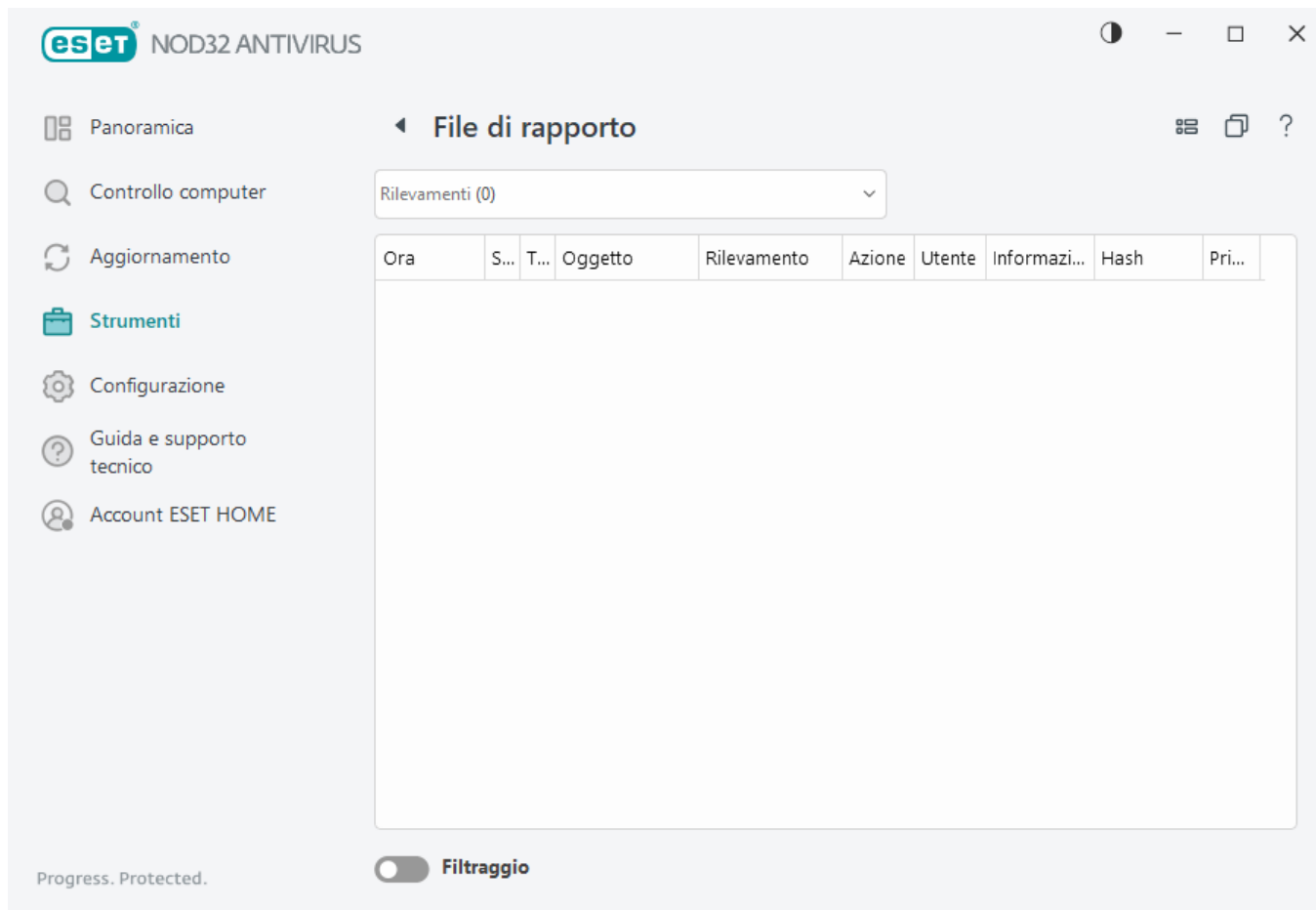
[Invia campione per l'analisi](#) (potrebbe non essere disponibile in base alla configurazione di [ESET LiveGrid®](#) da

parte dell'utente).



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 dall'archivio dei rapporti.



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.

- **Rilevamenti:** in questo rapporto sono contenute informazioni dettagliate sui rilevamenti e le infiltrazioni rilevati da ESET NOD32 Antivirus. Le informazioni relative ai rapporti includono l'ora del rilevamento, il tipo di scanner, il tipo di oggetto, la posizione dell'oggetto, il nome del rilevamento, l'azione eseguita, il nome dell'utente registrato nel momento in cui è stata rilevata l'infiltrazione, l'hash e la prima occorrenza. Le infiltrazioni non pulite vengono sempre indicate con un testo rosso su uno sfondo rosso chiaro. Mentre quelle pulite con un testo giallo su uno sfondo bianco. Le applicazioni potenzialmente pericolose non pulite vengono indicate con un testo giallo su uno sfondo bianco.
- **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 computer:** in questa finestra vengono visualizzati i risultati di tutti i controlli completati. Ogni riga corrisponde a un singolo controllo del computer. Fare doppio clic su una voce qualsiasi per visualizzare i [dettagli del selezionato 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 copiarli negli Appunti. Tenere premuto **CTRL** o **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.).
- **Filtra:** dopo aver selezionato questa opzione, la finestra [Filtraggio dei rapporti](#) 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 annullare tutte le impostazioni del filtro (come descritto in precedenza).
- **Copia/Copia tutto:** consente di copiare le informazioni sui record selezionati.
- **Copia cella:** consente di copiare il contenuto della cella selezionata con il pulsante destro del mouse.
- **Rimuovi/Rimuovi tutto:** consente di eliminare i record selezionati o tutti i record visualizzati. Per poter eseguire questa operazione è necessario disporre di privilegi amministrativi.
- **Esporta/Esporta tutto:** consente di esportare le informazioni sui record selezionati o su tutti i record nel formato XML.
- **Trova/Trova successivo/Trova precedente:** dopo aver fatto clic su questa opzione, è possibile definire i criteri di filtraggio per evidenziare la voce specifica utilizzando la finestra Filtraggio dei rapporti.
- **Descrizione rilevamento:** consente di aprire ESET Threat Encyclopedia, che contiene informazioni dettagliate sui pericoli e sui sintomi dell'infiltrazione registrata.
- **Crea esclusione:** consente di creare una nuova [Esclusione rilevamenti tramite una procedura guidata](#) (non disponibile per i rilevamenti malware).

Filtraggio rapporti

Fare clic su  **Filtraggio** in **Strumenti > File di rapporto** per definire i criteri di filtraggio.

La funzione di filtraggio dei rapporti rende più semplice trovare le informazioni desiderate, in particolare quando sono presenti numerosi record. Consente di restringere i record dei rapporti, ad esempio se si è interessati a uno specifico tipo di evento, stato o periodo. È possibile filtrare i record dei rapporti specificando determinate opzioni di ricerca: solo i record rilevanti (in base a tali opzioni di ricerca) verranno visualizzati nella finestra File di rapporto.

Digitare la parola chiave da cercare nel campo **Trova testo**. Utilizzare il menu a discesa **Cerca nelle colonne** per perfezionare la ricerca. Scegliere uno o più record dal menu a discesa **Tipi di record**. Definire il **periodo di tempo** per cui si desidera visualizzare i risultati. È anche possibile utilizzare ulteriori opzioni di ricerca, come **Solo parole intere** o **Maiuscole/minuscole**.

Trova testo

Digitare una stringa (una parola o parte di una parola). Verranno visualizzati solo i record che contengono tale stringa. Gli altri record verranno omessi.

Cerca nelle colonne

Selezionare le colonne da considerare durante la ricerca. È possibile selezionare una o più colonne da utilizzare per la ricerca.

Tipi di record

Scegliere uno o più tipi di record dei rapporti dal menu a discesa:

- **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 antivirus).

Periodo di tempo

Indicare l'intervallo di tempo rispetto al quale si desiderano visualizzare i risultati:

- **Non specificato** (predefinito): non esegue la ricerca entro il periodo di tempo, ma nell'intero rapporto.
- **Ultimo giorno**
- **Ultima settimana**
- **Ultimo mese**
- **Periodo di tempo:** è possibile specificare il periodo di tempo esatto (Da: e A:), in modo da filtrare solo i record del periodo di tempo specificato.

Solo parole intere

Utilizzare la casella di controllo per cercare parole intere e ottenere risultati più precisi.

Maiuscole/minuscole


Attivare questa opzione se è importante utilizzare lettere maiuscole o minuscole durante il filtraggio. Una volta configurate le opzioni di filtraggio/ricerca, fare clic su **OK** per visualizzare i record dei registri filtrati o su **Trova** per avviare la ricerca. I file di rapporto vengono cercati dall'alto verso il basso, a partire dalla posizione corrente (il record evidenziato). La ricerca si interrompe quando viene trovato il primo record corrispondente. Premere **F3** per cercare il record successivo o fare clic con il pulsante destro del mouse e selezionare **Trova** per affinare le opzioni di ricerca.

Registrazione della configurazione

La configurazione della registrazione di ESET NOD32 Antivirus è accessibile dalla [finestra principale del programma](#). Fare clic su **Configurazione > 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 antivirus.e così via).

 Tutte le connessioni bloccate verranno registrate al momento della selezione del livello di dettaglio minimo della diagnostica.

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 attiva 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 **Rilevamenti** 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 archiviati correntemente selezionati nel menu a discesa **Tipo**. Verrà visualizzata una notifica relativa all'avvenuta eliminazione dei rapporti.

i 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 questo articolo della [Knowledge Base di ESET](#).

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 [ESET LiveGrid®](#).



eset NOD32 ANTIVIRUS

Processi in esecuzione

In questa finestra viene visualizzato un elenco dei file selezionati, nonché le informazioni aggiuntive fornite da ESET LiveGrid®. Viene indicato il livello di rischio di ciascun file, oltre al numero di utenti e all'ora del primo rilevamento.

Livello di ...	Processo	PID	Numero di u...	Ora del ril...	Nome applicazione
■	smss.exe	364	■	1 anno fa	Microsoft® Windows® ...
■	csrss.exe	472	■	2 anni fa	Microsoft® Windows® ...
■	wininit.exe	552	■	3 mesi fa	Microsoft® Windows® ...
■	winlogon.exe	624	■	2 settiman...	Microsoft® Windows® ...
■	services.exe	696	■	1 anno fa	Microsoft® Windows® ...
■	lsass.exe	704	■	3 mesi fa	Microsoft® Windows® ...
■	svchost.exe	832	■	6 mesi fa	Microsoft® Windows® ...
■	fontdrvhost.exe	864	■	1 mese fa	Microsoft® Windows® ...
■	dwm.exe	436	■	2 anni fa	Microsoft® Windows® ...
■	wudfhost.exe	1532	■	6 mesi fa	Microsoft® Windows® ...
■	vboxservice.exe	1600	■	2 anni fa	Oracle VM VirtualBox G...
■	efwd.exe	1764	■	3 giorni fa	ESET Security
■	spoolsv.exe	2916	■	2 settiman...	Microsoft® Windows® ...
■	akvcamassistant.exe	3108	■	2 anni fa	AkVCamAssistant
■	sihost.exe	4652	■	2 anni fa	Microsoft® Windows® ...
■	taskhostw.exe	3336	■	6 mesi fa	Microsoft® Windows® ...
■	ctfmon.exe	4228	■	2 anni fa	Microsoft® Windows® ...

Progress. Protected. [Mostra dettagli](#)

Reputazione: nella maggior parte dei casi, ESET NOD32 Antivirus e la tecnologia ESET LiveGrid® 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).

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.

i 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 vengono raccolte mediante la tecnologia ESET LiveGrid®.

Ora del rilevamento: ora in cui l'applicazione è stata rilevata dalla tecnologia ESET LiveGrid®.

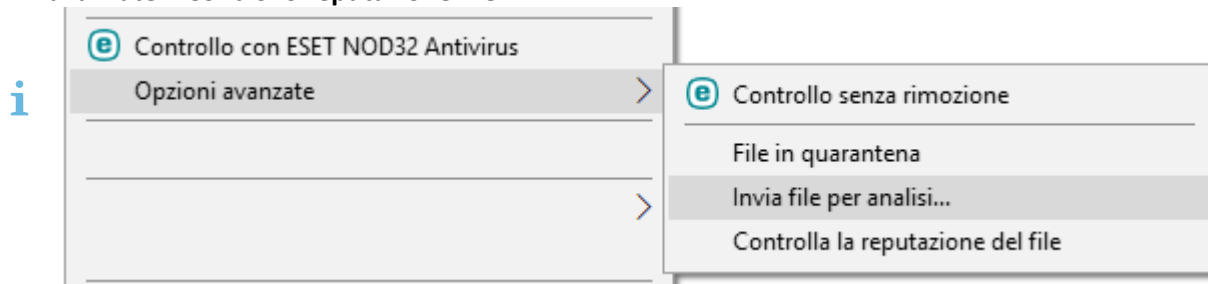
i Un'applicazione marchiata come Sconosciuta (arancio) non è necessariamente un software malevolo. In genere si tratta di una nuova applicazione. In caso di dubbi sul file, selezionare l'opzione [invia file per analisi](#) al laboratorio di ricerca ESET. Se il file si rivela essere un'applicazione dannosa,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

Nome applicazione: nome specifico di un programma o processo.

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

- **Percorso:** posizione di un'applicazione sul computer.
- **Dimensione:** dimensione del file in kB (kilobyte) o MB (megabyte).
- **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).

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 in una directory di esplorazione dei file e selezionare **Opzioni avanzate > Controllo reputazione file**.



Report di protezione

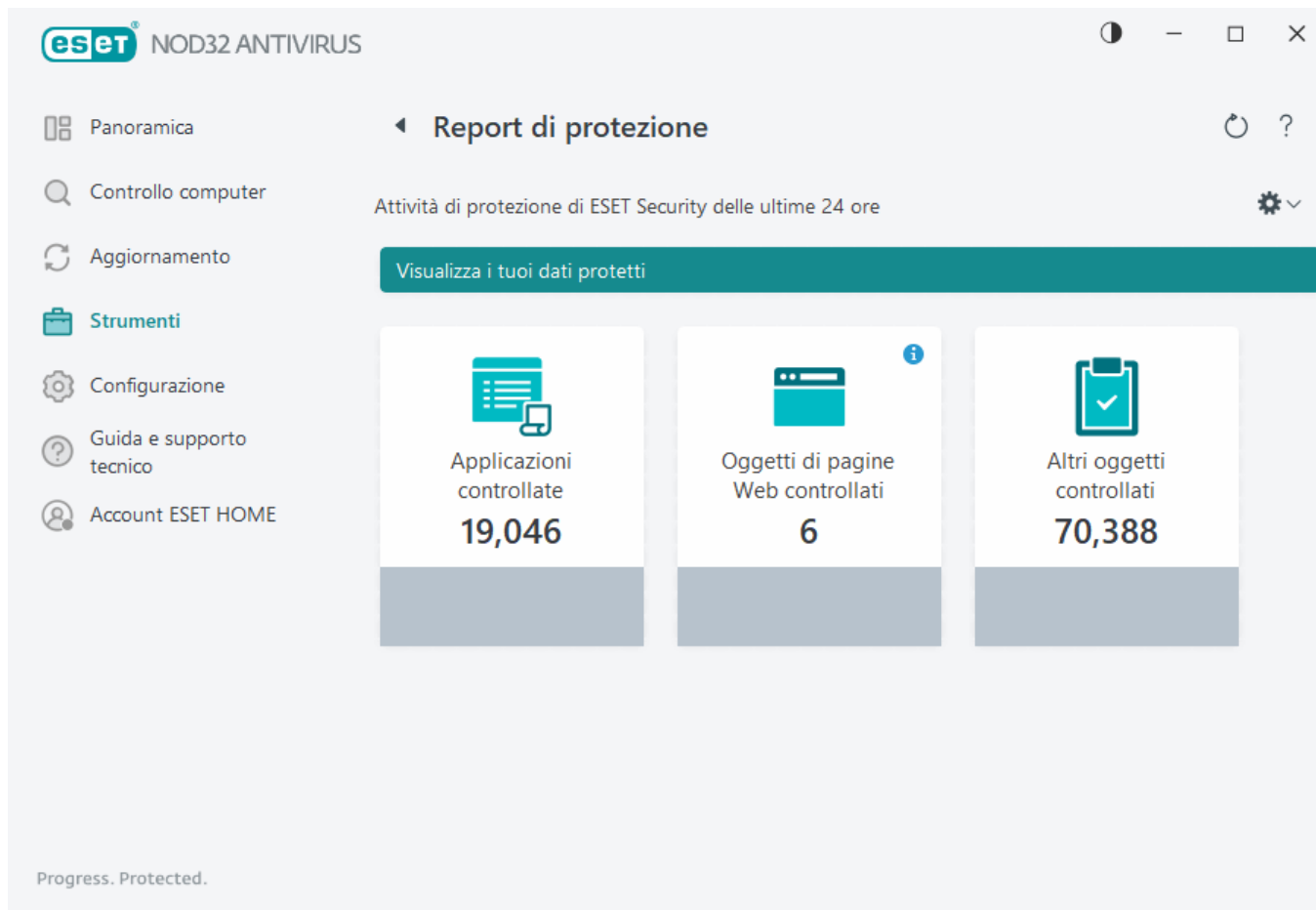
Questa funzione offre una panoramica delle statistiche relative alle categorie indicate di seguito:

- **Pagine Web bloccate:** consente di visualizzare il numero di pagine Web bloccate (indirizzi URL bloccati per le applicazioni potenzialmente indesiderate, phishing, router, IP o certificato oggetto di un attacco).
- **Oggetti di e-mail infetti rilevati:** consente di visualizzare il numero di [oggetti](#) di e-mail infetti che sono stati rilevati.
- **Applicazione potenzialmente indesiderata rilevata:** consente di visualizzare il numero di [applicazioni potenzialmente indesiderate](#).
- **Documenti controllati:** consente di visualizzare il numero di oggetti di documenti controllati.
- **Applicazioni controllate:** consente di visualizzare il numero di oggetti eseguibili controllati.
- **Altri oggetti controllati:** consente di visualizzare il numero di altri oggetti controllati.
- **Oggetti di pagine Web controllati:** consente di visualizzare il numero di oggetti di pagine Web controllati.
- **Oggetti di e-mail controllati:** consente di visualizzare il numero di oggetti di e-mail controllati.

L'ordine di queste categorie si basa su un valore numerico, dal più alto al più basso. Le categorie con valori pari a zero non vengono visualizzate. Fare clic su **Mostra altro** per espandere e visualizzare le categorie nascoste.

Dopo essere stata attivata, la funzione non compare più come non operativa nel Report di protezione.

Fare clic sull'icona a forma di ingranaggio ⚙️ nell'angolo in alto a destra per **Attivare/Disattivare le notifiche dei Report di protezione** o scegliere se si desidera visualizzare i dati relativi agli ultimi 30 giorni o a partire dal momento dell'attivazione del prodotto. In caso di installazione di ESET NOD32 Antivirus da meno di 30 giorni, è possibile selezionare solo il numero di giorni a partire dall'installazione. Il periodo di 30 giorni rappresenta l'impostazione predefinita.



Ripristina dati consente di cancellare tutte le statistiche e di rimuovere i dati esistenti per il Report di protezione. Questa azione deve essere confermata eccetto nel caso in cui l'utente deselezioni l'opzione **Chiedi prima di azzerare le statistiche** in **Configurazione avanzata > Notifiche > Avvisi interattivi > Messaggi di conferma > Modifica**.

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 voci di registro importanti e valuta il livello di rischio di ciascuno di essi. 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. Per ulteriori informazioni sulle modalità di utilizzo di ESET SysInspector, consultare la [Guida online di ESET SysInspector](#).

Nella finestra di ESET SysInspector vengono visualizzate le seguenti informazioni sui rapporti:

- **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:** consente di aprire il rapporto selezionato in ESET SysInspector. È inoltre possibile fare clic con il pulsante destro del mouse su uno specifico file di registro e selezionare **Mostra** dal menu contestuale.
- **Crea:** consente di creare un nuovo rapporto. Attendere fino a quando non viene generato ESET SysInspector (stato **Creato**) prima di tentare di accedere al rapporto.
- **Elimina:** rimuove dall'elenco i(l) rapporti/o selezionati/o.

I seguenti oggetti 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).
- **Crea:** consente di creare un nuovo rapporto. Attendere fino a quando non viene generato ESET SysInspector (stato **Creato**) prima di tentare di accedere al rapporto.
- **Elimina:** rimuove dall'elenco i(l) rapporti/o selezionati/o.
- **Elimina tutto:** consente di eliminare tutti i rapporti.
- **Esporta:** esporta il rapporto in un file .xml o un file .xml compresso. Il rapporto viene esportato in C:\ProgramData\ESET\ESET Security\SysInspector.

Pianificazione attività

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

Per accedere alla Pianificazione attività è possibile utilizzare la [finestra principale del programma](#) 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.

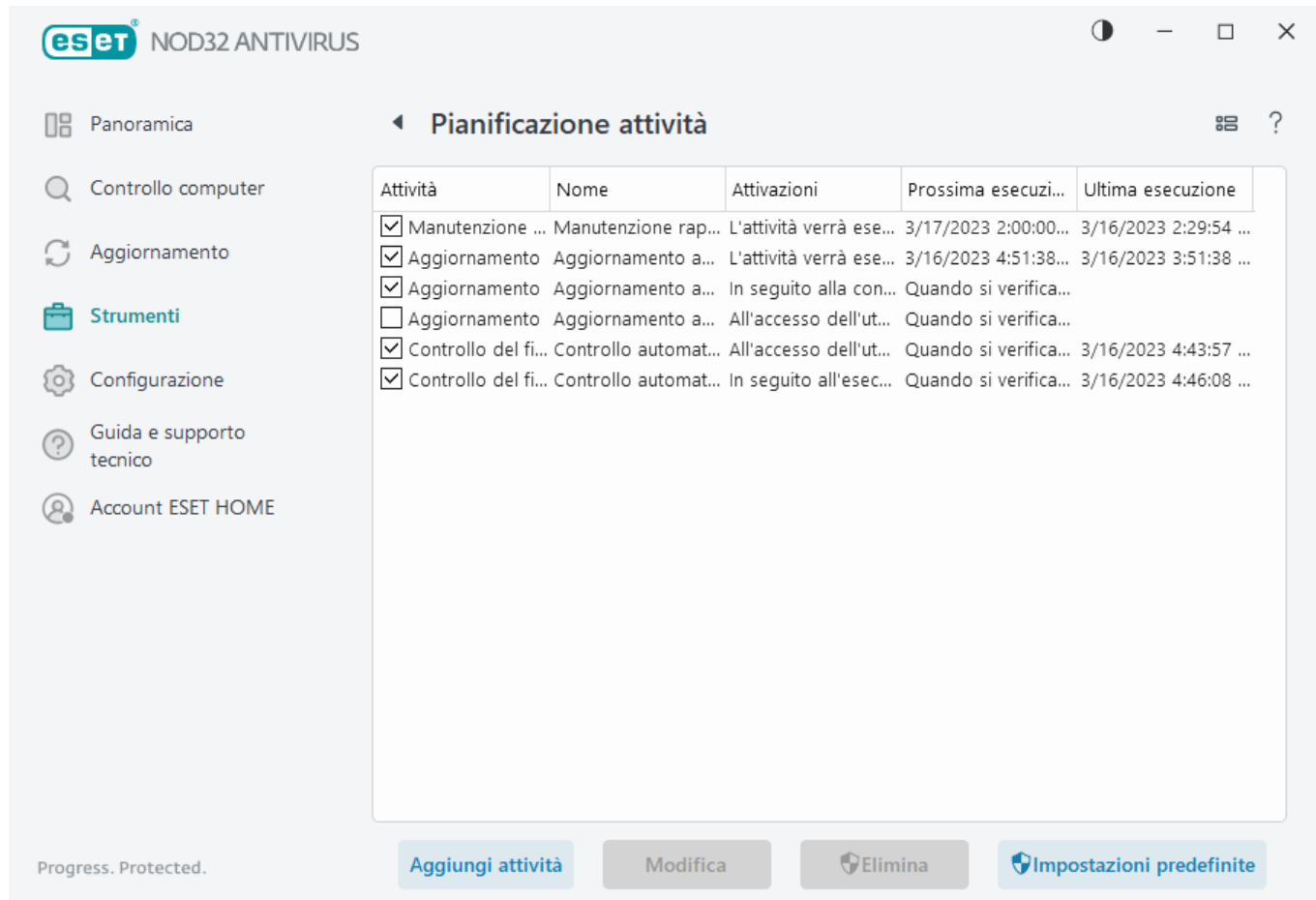
La Pianificazione attività consente di pianificare le attività seguenti: moduli di aggiornamento, attività di controllo, controllo dei file di avvio del sistema e manutenzione dei rapporti. È possibile aggiungere o eliminare attività direttamente dalla finestra principale Pianificazione attività (fare clic su **Aggiungi attività** o **Elimina** nella parte inferiore). È possibile ripristinare le impostazioni predefinite dell'elenco di attività pianificate ed eliminare tutte le modifiche facendo clic su **Impostazioni predefinite**. 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 periodico**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**

- **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**: file di rapporto contenenti 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.

4. Fare clic sulla barra di scorrimento accanto ad **Abilitata** per 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 (ore):** rappresenta il tempo trascorso dalla prima esecuzione ignorata dell'attività. In caso di superamento di questo limite di tempo, l'attività verrà eseguita immediatamente. Impostare l'ora utilizzando la casella di selezione sottostante.

Per rivedere l'attività pianificata, fare clic con il pulsante destro del mouse su di essa e selezionare **Mostra dettagli attività**.

Opzioni controllo pianificato

In questa finestra è possibile specificare le opzioni avanzate per un'attività di controllo del computer pianificata.

Per eseguire un controllo senza azioni di pulizia, fare clic su **Impostazioni avanzate** e 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.

Il menu a discesa **Azione al termine del controllo** consente all'utente di impostare un'azione da eseguire automaticamente al termine di un controllo:

- **Nessuna azione:** al termine di un controllo, non verrà eseguita alcuna azione.
- **Arresta:** il computer si spegne al termine di un controllo.
- **Riavvia se necessario:** il computer si riavvia solo se necessario per completare la pulizia delle minacce

rilevate.

- **Riavvia**: chiude tutti i programmi aperti e riavvia il computer al termine di un controllo.
- **Forza riavvio se necessario**: il computer forza il riavvio solo se necessario per completare la pulizia delle minacce rilevate.
- **Forza riavvio**: consente di forzare la chiusura di tutti i programmi aperti senza attendere l'interazione dell'utente e di riavviare il computer al termine di un controllo.
- **Metti in stand-by**: salva la sessione in corso e mette il computer in modalità risparmio energetico che consente all'utente di riprendere velocemente il lavoro.
- **Metti in ibernazione**: sposta tutti i processi in esecuzione sulla RAM in un file speciale presente sul disco rigido. Il computer si arresterà ma i processi verranno ripresi dal punto in cui sono stati interrotti al successivo riavvio.



Le azioni **Sospendi** e **Iberna** sono disponibili in base alle impostazioni del sistema operativo Alimentazione e Sospensione del computer in uso o delle capacità del computer/computer portatile. Tenere presente che un computer in sospensione è sempre un computer operativo. Sul quale vengono ancora eseguite funzioni di base e che utilizza l'elettricità in caso di alimentazione a batteria. Per prolungare la durata della batteria, ad esempio, in caso di viaggi fuori ufficio, si consiglia di utilizzare l'opzione Iberna.

L'azione selezionata si avvierà al termine di tutti i controlli in esecuzione. Se si seleziona **Arresta** o **Riavvia**, verrà visualizzata una finestra di dialogo di conferma del prodotto per 30 secondi (fare clic su **Annulla** per disattivare l'azione richiesta).

Selezionare **Il controllo non può essere annullato** per impedire agli utenti che non possiedono privilegi di interrompere le azioni intraprese in seguito al controllo.

Selezionare l'opzione **Il controllo può essere sospeso dall'utente per (min.)** se si desidera consentire all'utente con restrizioni di sospendere il controllo del computer per uno specifico periodo di tempo.

Consultare anche [Avanzamento del controllo](#).

Panoramica attività pianificata

Questa finestra di dialogo contiene informazioni dettagliate sull'attività pianificata selezionata, che è possibile visualizzare facendo doppio clic su un'attività personalizzata, quindi facendo clic con il pulsante destro del mouse su un'attività pianificata personalizzata e selezionando **Mostra dettagli attività**.

Dettagli attività

Digitare il **Nome dell'attività**, selezionare una delle opzioni relative al **Tipo di attività** e fare clic su **Avanti**:

- **Esegui applicazione esterna**: consente di pianificare l'esecuzione di un'applicazione esterna.
- **Manutenzione rapporto**: file di rapporto contenenti 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.

Tempo attività

L'attività verrà eseguita ripetutamente in base all'intervallo temporale specificato. Selezionare una delle seguenti opzioni temporali:

- **Una volta:** l'attività verrà eseguita solo una volta, alla data e all'ora predefinite.
- **Ripetutamente:** l'attività verrà eseguita in base all'intervallo specificato (in ore).
- **Ogni giorno:** l'attività verrà eseguita ogni giorno all'ora specificata.
- **Ogni settimana:** l'attività verrà eseguita una o più volte alla settimana, nei giorni e nelle ore specificati.
- **Quando si verifica un evento:** l'attività verrà eseguita quando si verifica un evento specifico.

Ignora attività se in esecuzione su un computer alimentato dalla batteria: un'attività non verrà eseguita al momento del lancio se il computer in uso è alimentato dalla batteria. Questa regola vale anche per i computer alimentati da gruppi di continuità.

Frequenza attività: una volta

Esecuzione attività: l'attività specificata verrà eseguita solo una volta alla data e all'ora indicate.

Frequenza attività: ogni giorno

L'attività verrà eseguita ogni giorno all'ora specificata.

Frequenza attività: ogni settimana

L'attività verrà eseguita ripetutamente ogni settimana nei giorni e nelle ore selezionati.

Frequenza attività: quando si verifica un evento

L'attività viene avviata da uno degli eventi seguenti:

- **A ogni avvio del computer**

- **Al primo avvio del computer ogni giorno**
- **Connessione remota a Internet/VPN**
- **In seguito all'esecuzione dell'aggiornamento dei moduli**
- **In seguito all'esecuzione dell'aggiornamento del prodotto**
- **Accesso utente**
- **Rilevamento delle minacce**

Quando si pianifica un'attività avviata da un evento, è possibile specificare l'intervallo minimo tra il completamento di un'attività e l'altra. Se si esegue ad esempio l'accesso al computer più volte al giorno, scegliere 24 ore per eseguire l'attività solo al primo accesso del giorno, quindi il giorno successivo.

Attività ignorata

Un'attività può essere [ignorata se il computer è alimentato dalla batteria o è spento](#). Selezionare una di queste opzioni relative all'attività e fare clic su **Avanti**:

- **Al prossimo orario pianificato**: l'attività verrà eseguita se il computer è acceso al successivo orario pianificato.
- **Appena possibile**: l'attività verrà eseguita quando il computer è acceso.
- **Immediatamente, se l'ora dall'ultima esecuzione pianificata supera (ore)**: rappresenta il tempo trascorso dalla prima esecuzione ignorata dell'attività. In caso di superamento di questo limite di tempo, l'attività verrà eseguita immediatamente.

Immediatamente, se l'ora dall'ultima esecuzione pianificata supera (ore) – esempi

Un esempio di attività è impostato in modo da essere eseguita ripetutamente ogni ora. L'opzione **Immediatamente, se l'ora dall'ultima esecuzione pianificata supera (ore)** è selezionata e l'ora superata è impostata su due ore. L'attività viene eseguita alle 13:00 e, al termine dell'operazione, il computer va in sospensione:

- Il computer si riattiva alle 15:30. La prima esecuzione dell'attività ignorata è stata alle 14:00. Dalle 14:00 sono trascorse solo 1,5 ore, pertanto l'attività verrà eseguita alle 16:00.
- Il computer si riattiva alle 16:30. La prima esecuzione dell'attività ignorata è stata alle 14:00. Dalle 14:00 sono trascorse due ore e mezzo, pertanto l'attività verrà eseguita immediatamente.

Dettagli attività: aggiornamento

Se si desidera aggiornare il programma da due server di aggiornamento, è necessario creare due profili di aggiornamento differenti. Se il primo non riesce a scaricare i file dell'aggiornamento, il programma passa automaticamente al secondo. Questa soluzione risulta utile, ad esempio, per i notebook, che generalmente vengono aggiornati da un server di aggiornamento LAN locale, sebbene i proprietari si connettano spesso a Internet utilizzando altre reti. In questo modo, se il primo profilo non riesce a completare l'operazione, il secondo esegue automaticamente il download dei file dai server di aggiornamento ESET.

Dettagli attività: esegui applicazione

Questa attività consente di pianificare l'esecuzione di un'applicazione esterna.

File eseguibile: scegliere un file eseguibile dalla struttura della directory, fare clic sull'opzione ... oppure immettere manualmente il percorso.

Cartella di lavoro: specificare la directory di lavoro dell'applicazione esterna. Tutti i file temporanei del **File eseguibile** selezionato verranno creati all'interno di questa directory.

Parametri: parametri della riga di comando per l'applicazione (facoltativo).

Fare clic su **Fine** per confermare l'attività.

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 e le impostazioni predefiniti del sistema con un solo clic.

Questo strumento segnala problemi appartenenti alle cinque categorie di impostazioni indicate di seguito:

- **Impostazioni di sicurezza:** modifiche delle impostazioni che possono causare un aumento del livello di vulnerabilità del computer, come Windows Update
- **Impostazioni di sistema:** modifiche delle impostazioni del sistema che incidono sul comportamento del computer, come le associazioni di file
- **Aspetto del sistema:** impostazioni che incidono sull'aspetto del sistema, come lo sfondo del desktop.
- **Funzioni disattivate:** alcune funzioni e applicazioni importanti che potrebbero essere disattivate.
- **Ripristino della configurazione di sistema di Windows:** impostazioni relative alla funzione di ripristino della configurazione di sistema di Windows che consente di ripristinare uno stato precedente 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.



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

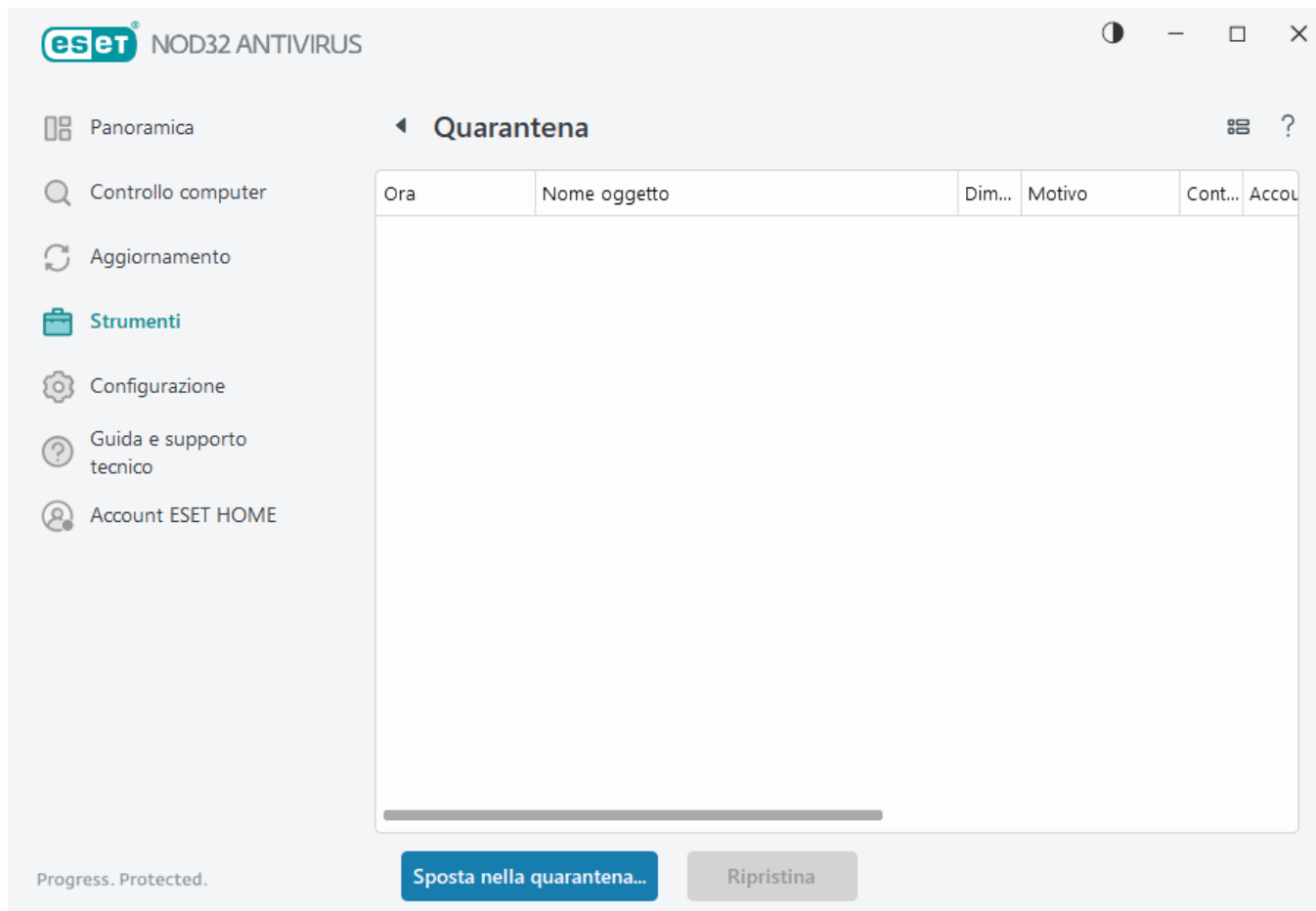
Quarantena

La funzione principale della quarantena consiste nell'archiviare in modo sicuro gli oggetti segnalati (come ad esempio malware, file infetti o applicazioni potenzialmente indesiderate).

È possibile accedere alla quarantena dalla [finestra principale del programma](#) ESET NOD32 Antivirus facendo clic su **Strumenti > Quarantena**.

I file salvati nella cartella della quarantena possono essere visualizzati in una tabella contenente le seguenti informazioni:

- la data e l'ora della quarantena,
- il percorso originale del file,
- le dimensione in byte,
- il motivo (ad esempio, oggetto aggiunto dall'utente),
- e un numero di rilevamenti (ad esempio, rilevamenti duplicati dello stesso file o archivio contenente più infiltrazioni).



Mettere file in quarantena

ESET NOD32 Antivirus mette automaticamente in quarantena i file rimossi (se questa opzione non è stata annullata nella [finestra di avviso](#)).

I file aggiuntivi devono essere messi in quarantena se:

- a. non possono essere puliti,
- b. non è sicuro o non è consigliabile rimuoverli,
- c. vengono erroneamente rilevati da ESET NOD32 Antivirus,
- d. o un file si comporta in modo sospetto ma non viene rilevato dallo [scanner](#).

Per mettere in quarantena un file, sono disponibili varie opzioni:

- a. Utilizzare la funzione trascinamento della selezione per mettere un file manualmente in quarantena, spostando il puntatore del mouse sull'area contrassegnata tenendo premuto il pulsante del mouse e rilasciandolo successivamente. In seguito a tale operazione, l'applicazione viene spostata in primo piano.
- b. Fare clic con il pulsante destro del mouse sul file > fare clic su **Opzioni avanzate > Metti il file in quarantena**.
- c. Fare clic su **Sposta in quarantena** dalla finestra **Quarantena**.
- d. A tale scopo, è possibile utilizzare anche il menu contestuale; fare clic con il pulsante destro del mouse

nella finestra della **Quarantena** e selezionare **Metti in quarantena**.

Ripristino dalla quarantena

I file messi in quarantena possono anche essere ripristinati nella posizione originale:

- A tale scopo, utilizzare la funzione di **Ripristino**, disponibile nel menu contestuale facendo clic con il pulsante destro del mouse su un determinato file nella quarantena.
- Se un file è contrassegnato come [applicazione potenzialmente indesiderata](#), l'opzione **Ripristina ed escludi dal controllo** è abilitata. Consultare anche [Esclusioni](#).
- Il menu contestuale offre anche l'opzione **Ripristina in**, che consente all'utente di ripristinare un file in un percorso diverso da quello in cui è stato rimosso.
- In alcuni casi, ad esempio, la funzionalità di ripristino non è disponibile per i file posizionati in una condivisione di rete di sola lettura.

Rimozione 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. Gli oggetti eliminati verranno rimossi in modo permanente dal dispositivo dell'utente e dalla quarantena.

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 [inviare il campione per l'analisi al laboratorio antivirus ESET](#). Per inviare un file, fare clic con il pulsante destro del mouse sul file e selezionare **Invia per analisi** dal menu contestuale.

Descrizione del rilevamento

Fare clic con il tasto destro del mouse su una voce e selezionare **Descrizione rilevamento** per aprire ESET Threat Encyclopedia, che contiene informazioni dettagliate sui pericoli e sui sintomi dell'infiltrazione registrata.

Istruzioni illustrate

I seguenti articoli della Knowledge Base ESET potrebbero essere disponibili solo in inglese:



- [Ripristino di un file in quarantena in ESET NOD32 Antivirus](#)
- [Rimozione di un file in quarantena in ESET NOD32 Antivirus](#)
- [Il mio prodotto ESET mi ha informato di un rilevamento, cosa devo fare?](#)

Quarantena non riuscita

Di seguito sono riportati i motivi che impediscono lo spostamento di file specifici in Quarantena:

- **L'utente non dispone delle autorizzazioni di lettura:** ciò significa che non è possibile visualizzare il contenuto di un file.

- **L'utente non dispone delle autorizzazioni di scrittura:** ciò significa che non è possibile modificare i contenuti del file, p. es. aggiungere nuovi contenuti o rimuovere quelli esistenti.
- **Il file che si sta tentando di mettere in quarantena è troppo grande:** è necessario ridurre le dimensioni del file.

Quando viene visualizzato il messaggio di errore “Quarantena non riuscita”, fare clic su **Maggiori informazioni**. Verrà visualizzata la finestra dell'elenco degli errori della quarantena contenente il nome del file e il motivo per cui non è possibile metterlo in quarantena.

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 essere configurate nella [finestra principale del programma](#) > **Configurazione** > **Configurazione avanzata** > **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.

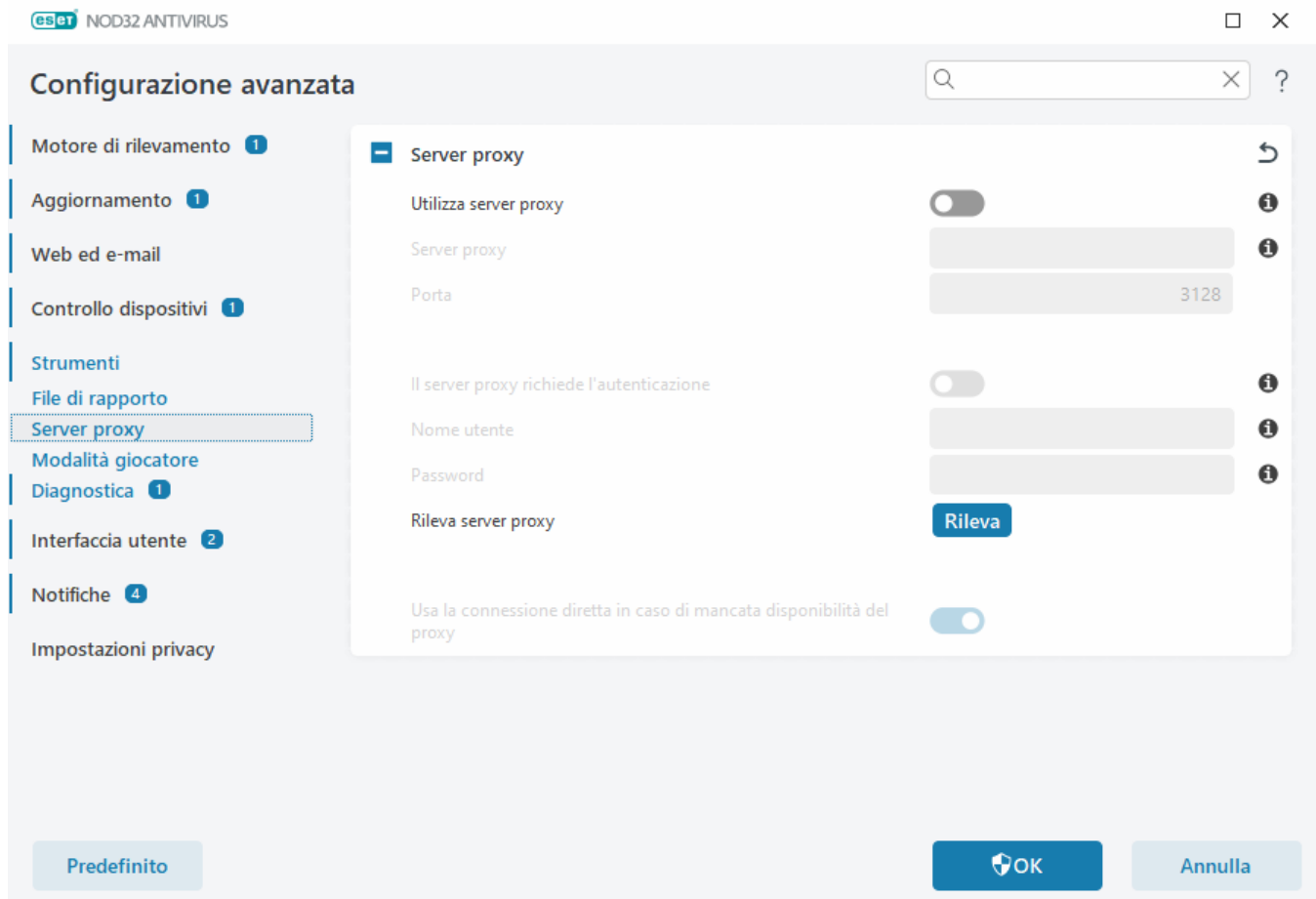
Per specificare le impostazioni del server proxy per questo livello, selezionare **Utilizza server proxy** e inserire l'indirizzo del server proxy nel campo **Server proxy**, insieme al numero di **Porta** del server proxy.

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 server proxy** per rilevare e inserire automaticamente le impostazioni del server proxy. Verranno copiati i parametri specificati nelle opzioni Internet per Internet Explorer o Google Chrome.

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

Utilizza la connessione diretta in caso di mancata disponibilità del proxy: se ESET NOD32 Antivirus è configurato per effettuare la connessione tramite proxy e questo non è raggiungibile, ESET NOD32 Antivirus disabiliterà il proxy e comunicherà direttamente con i server ESET.

Le impostazioni del server proxy possono anche essere definite nella Configurazione avanzata aggiornamento (**Configurazione avanzata** > **Aggiornamento** > **Profili** > **Aggiornamenti** > **Opzioni di connessione** 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 avanzata aggiornamento](#).



Seleziona campione per analisi

Se è stato trovato un file sospetto nel computer in uso o un sito sospetto su Internet, è possibile inviarlo al laboratorio di ricerca ESET per l'analisi (questa opzione potrebbe non essere disponibile in base alla configurazione di ESET LiveGrid®).

Prima di inviare i campioni a ESET

Non inviare un campione se non soddisfa almeno uno dei seguenti criteri:

- Il campione non è in alcun modo rilevato dal prodotto ESET
- Il campione viene erroneamente rilevato come una minaccia
- Non saranno accettati file personali (che si desidera analizzare con ESET per la ricerca di malware) come campioni (il laboratorio di ricerca ESET non esegue controlli su richiesta per gli utenti)
- Inserire una descrizione nel campo dell'oggetto e fornire il maggior numero di informazioni possibile sul file (ad esempio, lo screenshot o l'indirizzo del sito Web dal quale è stato scaricato)

È possibile inviare a ESET un campione (un file o un sito Web) da sottoporre ad analisi utilizzando uno dei metodi specificati di seguito:

1. Utilizza il modulo di invio del campione nel tuo prodotto. Si trova in **Strumenti > Invia campione per analisi**. La dimensione massima di un campione inviato è 256 MB.
2. In alternativa, è possibile inviare il file tramite e-mail. Se si preferisce questa opzione, comprimere il file o i file con WinRAR/WinZIP, proteggere l'archivio con la password "infected" e inviarlo a campioni@eset.com.
3. Per segnalare contenuti di spam o falsi positivi di spam, fare riferimento a questo [articolo della Knowledge Base di ESET](#).

Nel modulo **Seleziona campione per analisi**, selezionare la descrizione dal menu a discesa **Motivo per l'invio del campione** che si avvicina maggiormente alla propria motivazione:

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

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

E-mail di contatto: e-mail di contatto che viene inviata a ESET insieme ai file sospetti e che 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. Selezionare **Invia in modo anonimo** per lasciare il campo vuoto.

Assenza di risposta da parte di ESET

i ESET non invierà alcuna risposta a meno che non siano richieste ulteriori informazioni. Ogni giorno i server di ESET ricevono decine di migliaia di file e non è pertanto possibile rispondere a tutti. Se il campione si rivela essere un'applicazione o un sito Web dannoso, il suo rilevamento verrà aggiunto in un aggiornamento ESET successivo.

Seleziona campione per analisi: file sospetto

Segni e sintomi osservati dell'infezione malware: immettere una descrizione del comportamento del file sospetto osservato sul computer.

Origine file (indirizzo URL o fornitore): immettere un'origine del file (fonte) e in che modo è stato ottenuto il file.

Note e informazioni aggiuntive: qui è possibile inserire informazioni o descrizioni aggiuntive utili ai fini dell'elaborazione di un file sospetto.

i Il primo parametro – **Segni e sintomi osservati dell'infezione malware** – è obbligatorio, ma l'invio di informazioni aggiuntive aiuterà notevolmente i nostri laboratori nel processo di identificazione e nell'elaborazione dei campioni.

Seleziona campione per analisi: sito sospetto

Selezionare una delle opzioni che seguono dal menu a discesa **Problemi del sito**:

- **Infetto:** sito Web che contiene un virus o un altro malware distribuito con vari metodi.
- Il **phishing** viene utilizzato per ottenere l'accesso a dati sensibili quali numeri di conti bancari, codici PIN e così via. Per ulteriori informazioni su questo tipo di attacco, consultare il [glossario](#).
- **Scam:** sito web illegale o fraudolento, utilizzato soprattutto per ottenere rapidi guadagni.

- Selezionare **Altro** se le opzioni sopraindicate non fanno riferimento al sito che verrà inviato.

Note e informazioni aggiuntive: è possibile digitare informazioni aggiuntive o una descrizione utile per analizzare il sito web sospetto.

Seleziona campione per analisi: file falso positivo

All'utente è richiesto di inviare file rilevati come infezione, ma che in realtà non lo sono, allo scopo di potenziare il motore antivirus e antispyware e garantire la protezione degli altri utenti. I falsi positivi (FP) possono verificarsi quando il criterio di un file corrisponde al criterio contenuto in un motore di rilevamento.

Nome e versione dell'applicazione: titolo del programma e relativa versione (ad esempio, numero, alias o nome del codice).

Origine file (indirizzo URL o fornitore): specificare un'origine e le modalità di ottenimento del file (sorgente).

Scopo delle applicazioni: descrizione generale dell'applicazione, tipo di un'applicazione (ad esempio browser, lettore multimediale e così via) e relative funzionalità.

Note e informazioni aggiuntive: qui è possibile inserire informazioni o descrizioni aggiuntive utili ai fini dell'elaborazione di un file sospetto.



I primi tre parametri sono obbligatori allo scopo di identificare le applicazioni legali e di distinguerle dal codice dannoso. L'invio di informazioni aggiuntive aiuterà i laboratori ESET a potenziare notevolmente le capacità di identificazione e di elaborazione dei campioni.

Seleziona campione per analisi: sito falso positivo

All'utente è richiesto di inviare siti rilevati come infezione, scam o phishing ma che in realtà non lo sono. I falsi positivi (FP) possono verificarsi quando il criterio di un file corrisponde al criterio contenuto in un motore di rilevamento. All'utente è richiesto di segnalare questo sito Web per consentire agli sviluppatori di potenziare il motore antivirus e anti-phishing e per facilitare la protezione degli altri utenti.

Note e informazioni aggiuntive: qui è possibile inserire informazioni o descrizioni aggiuntive utili ai fini dell'elaborazione del sito web sospetto.

Seleziona campione per analisi: altro

Usare questo modulo se non è possibile classificare il file come **File sospetto** o **Falso positivo**.

Motivo per l'invio del file: immettere una descrizione dettagliata e il motivo dell'invio del file.

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 o di livello superiore da scaricare.
- **Aggiornamenti importanti:** vengono offerti aggiornamenti contrassegnati come importanti o di livello superiore da scaricare.
- **Aggiornamenti critici:** vengono offerti unicamente gli 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.

Finestra di dialogo - Aggiornamenti del sistema

In caso di aggiornamenti del sistema operativo in uso, ESET NOD32 Antivirus consente di visualizzare una notifica nella [finestra principale del programma](#) > **Panoramica**. Fare clic su **Maggiori informazioni** per aprire la finestra degli aggiornamenti di sistema.

Nella finestra Aggiornamenti del sistema è visualizzato un elenco di aggiornamenti disponibili per il download e l'installazione. Il tipo di aggiornamento è visualizzato accanto al nome dell'aggiornamento.

Fare doppio clic su una riga di aggiornamento per visualizzare la finestra [Informazioni di aggiornamento](#) contenente ulteriori informazioni.

Fare clic su **Esegui aggiornamento di sistema** per scaricare e installare tutti gli aggiornamenti del sistema operativo elencati.

Informazioni sugli aggiornamenti

Nella finestra Aggiornamenti del sistema è visualizzato un elenco di aggiornamenti disponibili per il download e l'installazione. Il livello di priorità è visualizzato accanto al nome dell'aggiornamento.

Fare clic su **Esegui aggiornamento di sistema** per avviare il download e l'installazione degli aggiornamenti del sistema operativo.

Fare clic con il pulsante destro del mouse su qualsiasi riga dell'aggiornamento e fare clic su **Visualizza informazioni** per visualizzare una nuova finestra contenente informazioni aggiuntive.

Guida e supporto tecnico


ESET NOD32 Antivirus contiene strumenti di risoluzione dei problemi e informazioni di supporto in grado di aiutare l'utente a risolvere eventuali problemi che potrebbero insorgere.

Licenza


- **[Risoluzione dei problemi relativi alla licenza](#)**: fare clic su questo collegamento per trovare le soluzioni ai problemi di attivazione o di modifica della licenza.
- **[Modifica licenza](#)**: fare clic per aprire la finestra di attivazione e attivare il prodotto. Se il dispositivo è [connesso a ESET HOME](#), scegliere una licenza dall'account ESET HOME o aggiungerne una nuova.

Prodotto installato

- **[Novità](#)**: fare clic qui per aprire la finestra delle informazioni sulle nuove funzioni e le funzionalità potenziate.
- **[Informazioni su ESET NOD32 Antivirus](#)**: consente di visualizzare le informazioni sulla copia di ESET NOD32 Antivirus posseduta dall'utente.
- **[Risoluzione dei problemi relativi al prodotto](#)**: fare clic su questo collegamento per trovare le soluzioni ai problemi riscontrati con maggiore frequenza.
- **Cambia prodotto**: fare clic per scoprire se è possibile cambiare ESET NOD32 Antivirus con [un'altra linea di prodotti](#) con la licenza corrente.

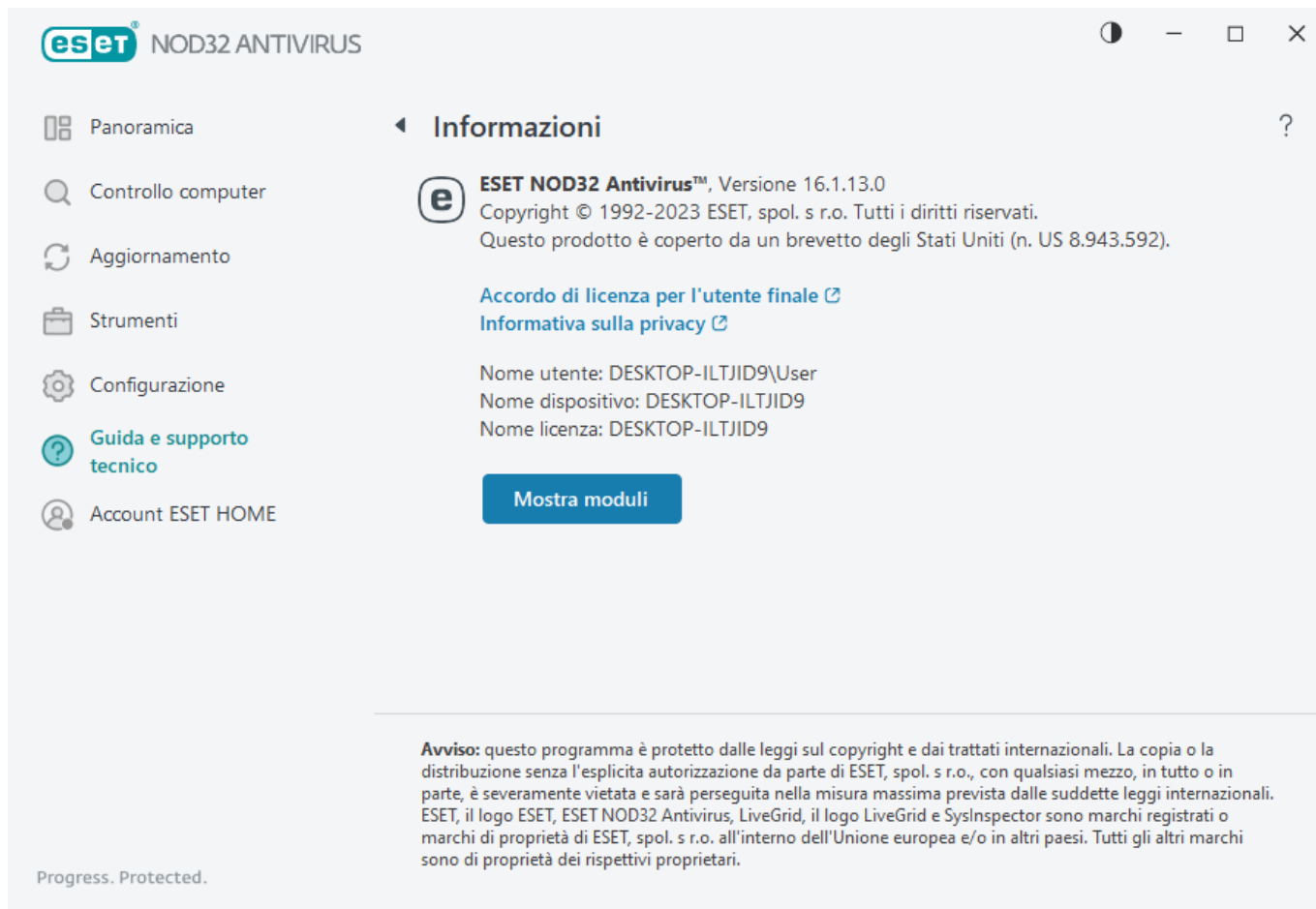
 **Pagina della Guida**: fare clic su questo collegamento per aprire le pagine della Guida di ESET NOD32 Antivirus.

[Supporto tecnico](#)

 **Knowledge Base**: la [Knowledge Base di ESET](#) contiene le risposte alle domande frequenti, nonché le soluzioni consigliate per i vari problemi. Grazie all'aggiornamento periodico effettuato dagli esperti del supporto tecnico di ESET, la Knowledge Base rappresenta lo strumento più potente per risolvere diversi problemi.

Informazioni su ESET NOD32 Antivirus

Questa finestra fornisce informazioni sulla versione installata di ESET NOD32 Antivirus e sul computer in uso.



Fare clic su **Mostra moduli** per visualizzare le informazioni sull'elenco di moduli del programma caricati.

- Per copiare le informazioni sui moduli negli Appunti, fare clic su **Copia**. Questa opzione potrebbe essere utile durante la procedura di risoluzione dei problemi o per contattare il Supporto tecnico.
- Fare clic su **Motore di rilevamento** nella finestra Moduli per aprire ESET Virus Radar, che contiene informazioni su ciascuna versione di ESET Detection Engine.

Novità ESET

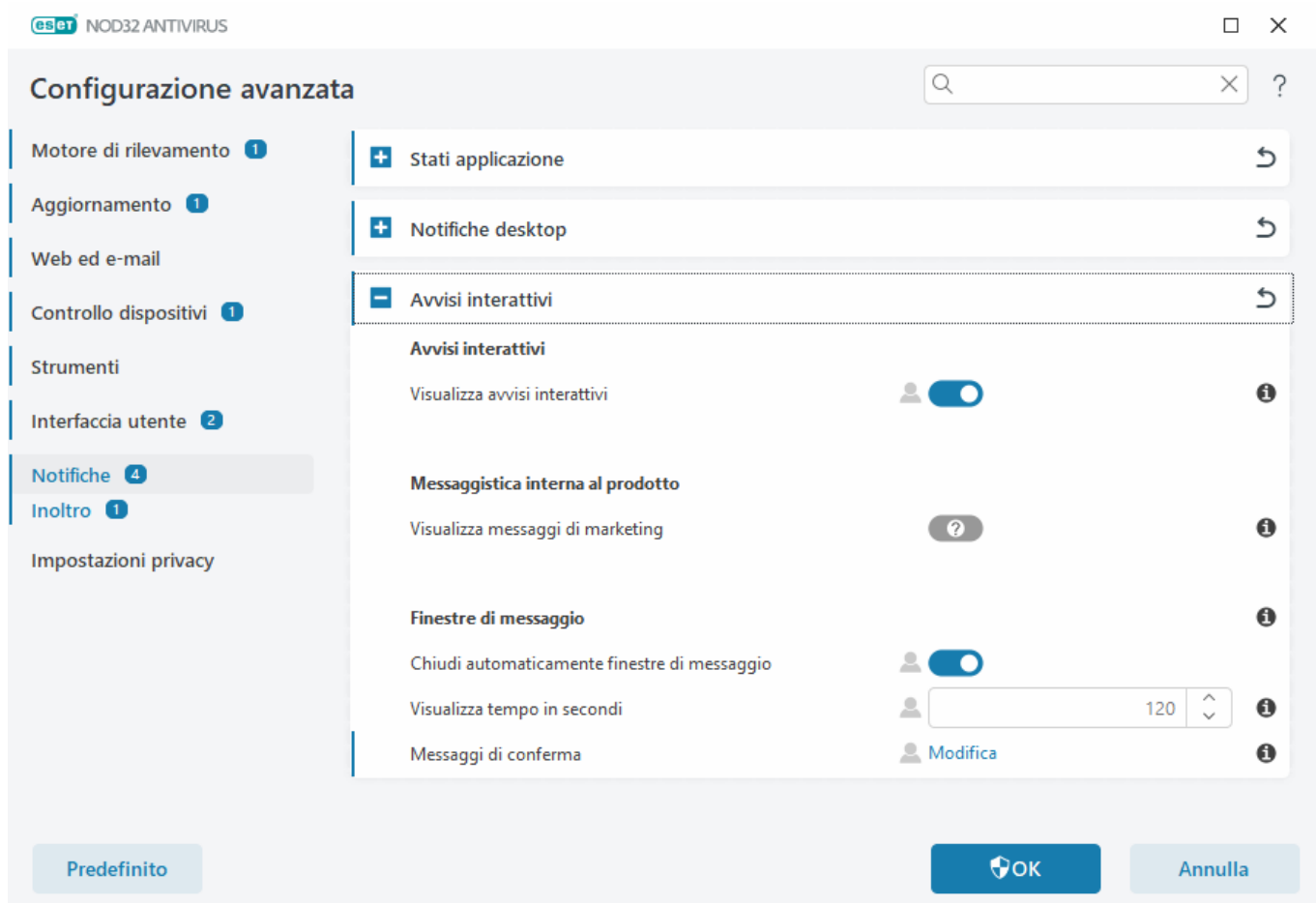
In questa finestra, ESET NOD32 Antivirus fornisce periodicamente all'utente informazioni sulle novità di ESET.

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. L'invio di messaggi promozionali richiede il consenso dell'utente. Di conseguenza, queste informazioni non vengono inviate all'utente per impostazione predefinita (tale aspetto viene indicato con un punto interrogativo). Abilitando questa opzione, l'utente accetta di ricevere messaggi promozionali da ESET. Disabilitare l'opzione **Visualizza messaggi di marketing** se non si desidera ricevere messaggi promozionali da ESET.

Per abilitare o disabilitare la ricezione di messaggi di marketing tramite la finestra di notifica, attenersi alle istruzioni sottostanti.

1. Aprire la finestra principale del prodotto ESET.
2. Premere il tasto **F5** per accedere alla **Configurazione avanzata**.

3. Fare clic su **Notifiche > Avvisi interattivi**.
4. Modificare l'opzione **Modifica messaggi di marketing**.



Invia dati configurazione sistema

Per offrire un servizio di assistenza il più rapido e accurato possibile, ESET richiede informazioni sulla configurazione di ESET NOD32 Antivirus, informazioni dettagliate sul sistema e i processi in esecuzione ([file di rapporto ESET SysInspector](#)) e i dati di registro. ESET utilizzerà questi dati esclusivamente per offrire assistenza tecnica ai propri clienti.

Quando si invia il [modulo web](#), i dati relativi alla configurazione del sistema verranno inviati a ESET. Selezionare **Invia sempre queste informazioni** se si desidera ricordare questa azione per il processo. Per inviare il modulo senza inviare i dati, fare clic su **Non inviare i dati**: in tal modo, sarà possibile contattare il Supporto tecnico ESET utilizzando il modulo di assistenza online.

Questa impostazione può essere configurata anche in **Configurazione avanzata > Strumenti > Diagnostica > Supporto tecnico**.



Se si è deciso di inviare i dati del sistema, è necessario compilare e inviare il modulo Web. La mancata osservanza di tale istruzione impedirà la creazione della richiesta di assistenza causando la perdita dei dati del sistema.

Supporto tecnico

Nella [finestra principale del programma](#) fare clic su **Guida e supporto tecnico > Supporto tecnico**.

Contatta il Supporto tecnico

Richiedi assistenza: se non si riesce a trovare una risposta al problema, è possibile utilizzare questo modulo disponibile sul sito web di ESET per contattare rapidamente il Supporto tecnico di ESET. In base alle impostazioni, prima di compilare il modulo web, verrà visualizzata la finestra di [invio dei dati di configurazione del sistema](#).

Ottieni informazioni per il Supporto tecnico

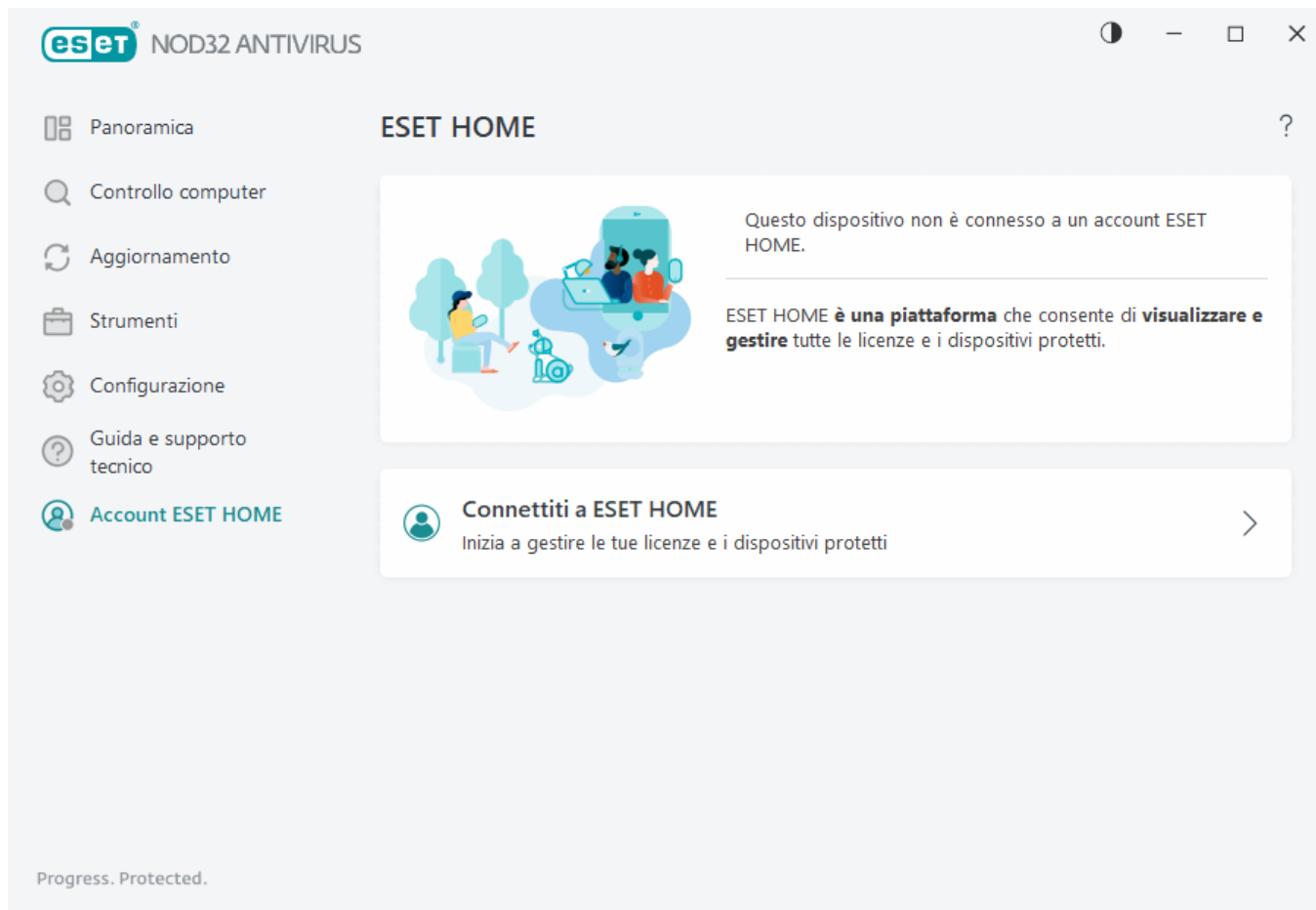
Dettagli per il Supporto tecnico: quando richiesto, è possibile copiare e inviare le informazioni al Supporto tecnico di ESET (ad esempio, dettagli della licenza, nome e versione del prodotto, sistema operativo e informazioni sul computer).

ESET Log Collector – rimanda all'articolo della [Knowledge Base di ESET](#), in cui è possibile scaricare l'utilità ESET Log Collector, un'applicazione che raccoglie automaticamente informazioni e rapporti dai computer allo scopo di risolvere i problemi in modo più rapido. Per ulteriori informazioni, fare clic [ESET Log Collector qui](#).

Attivare [Registrazione avanzata](#) per creare registri avanzati per tutte le funzioni disponibili e facilitare le operazioni di diagnosi e di risoluzione dei problemi da parte degli sviluppatori. Il livello di dettaglio di registrazione minimo è impostato su Diagnostico. La registrazione avanzata viene disattivata automaticamente dopo due ore, a meno che l'utente non decida di interromperla prima facendo clic su Interrompi registrazione avanzata. Al termine della creazione di tutti i rapporti, compare la finestra di notifica che fornisce l'accesso diretto alla cartella Diagnostica con i rapporti creati.

Account ESET HOME

È possibile rivedere lo stato di connessione dell'account ESET HOME nella [finestra principale del programma](#) > Account **ESET HOME**.



Questo dispositivo non è connesso a un account ESET HOME

Fare clic su [Connetti a ESET HOME](#) per connettere il dispositivo a [ESET HOME](#) e gestire le licenze e i dispositivi protetti. È possibile rinnovare, aggiornare o estendere la licenza e visualizzare informazioni importanti su di essa. Nel portale di gestione o nell'app per dispositivi mobili di ESET HOME è possibile aggiungere varie licenze, scaricare prodotti sui dispositivi, controllare lo stato di protezione dei prodotti o condividere licenze tramite e-mail. Per ulteriori informazioni, consultare la [Guida online di ESET HOME](#).

Questo dispositivo è connesso a un account ESET HOME

È possibile gestire la sicurezza del dispositivo da remoto utilizzando il [portale o l'app per dispositivi mobili di ESET HOME](#). Fare clic su **App Store** o **Google Play** per visualizzare un codice QR che è possibile scansionare con il telefono cellulare per scaricare l'app per dispositivi mobili di ESET HOME da App Store o Google Play.

Account **ESET HOME**: nome dell'account ESET HOME.

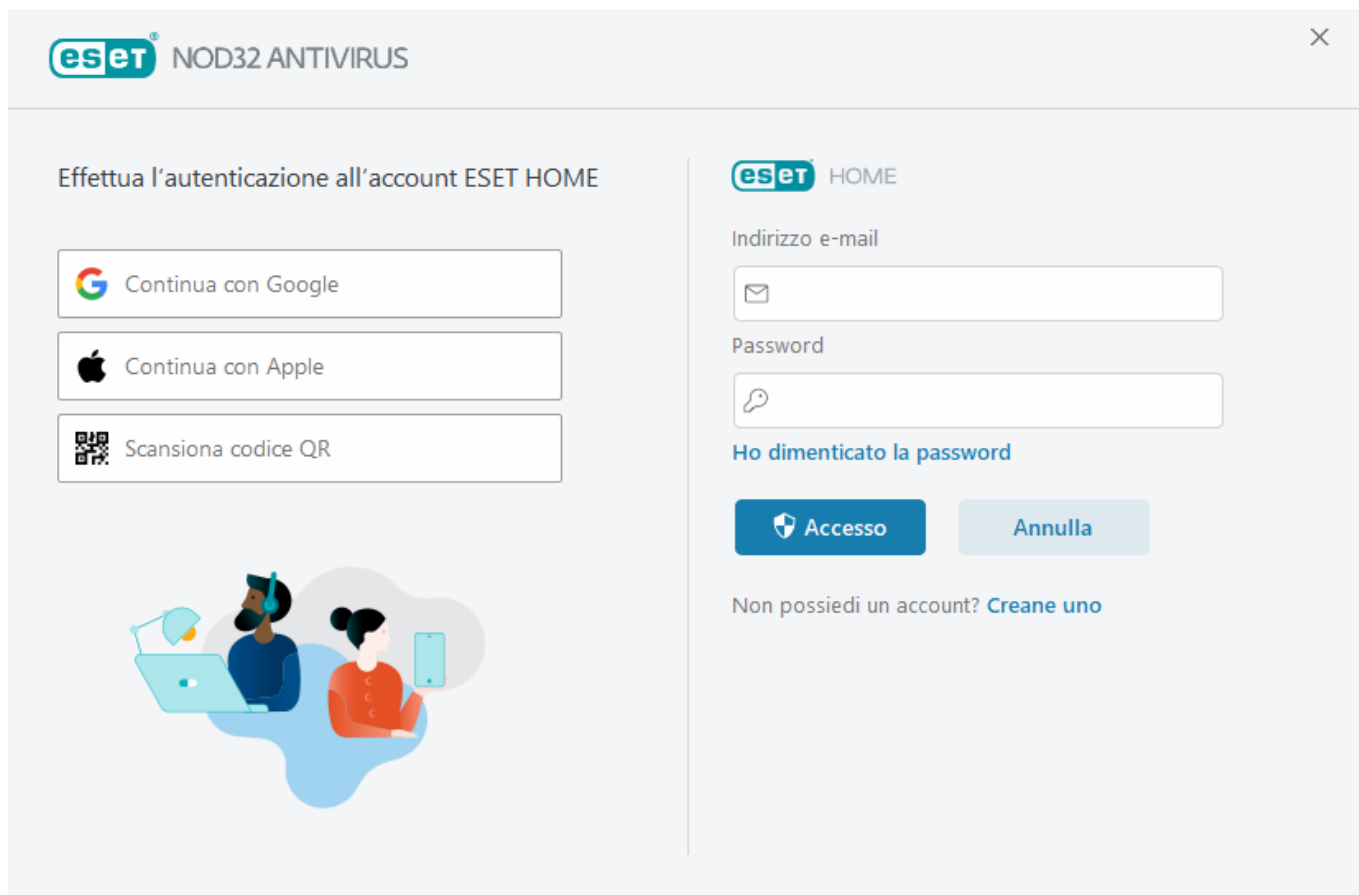
Nome dispositivo: nome del dispositivo visualizzato nell'account ESET HOME.

Apri ESET HOME: consente di aprire il portale di gestione di ESET HOME.

Per disconnettere il dispositivo dall'account ESET HOME, fare clic su **Effettua la disconnessione da ESET HOME > Disconnetti**. La licenza utilizzata per l'attivazione rimarrà attiva e il dispositivo sarà protetto.

Esegui la connessione a ESET HOME

Collegare il dispositivo all'account [ESET HOME](#) per visualizzare e gestire tutte le licenze e i dispositivi ESET attivati. È possibile rinnovare, aggiornare o estendere la licenza e visualizzare informazioni importanti su di essa. Nel portale di gestione o nell'app per dispositivi mobili di ESET HOME è possibile aggiungere varie licenze, scaricare prodotti sui dispositivi, controllare lo stato di protezione dei prodotti o condividere licenze tramite e-mail. Per ulteriori informazioni, consultare la [Guida online di ESET HOME](#).



Collegare il dispositivo al ESET HOME:

- i** In caso di connessione a ESET HOME durante l'installazione o la selezione dell'opzione **Utilizza l'account ESET HOME** come metodo di attivazione, seguire le istruzioni fornite nell'argomento [Utilizzare l'account ESET HOME](#).
- Se ESET NOD32 Antivirus è già stato installato e attivato con una licenza aggiunta nell'account ESET HOME, è possibile collegare il dispositivo a ESET HOME utilizzando il portale ESET HOME. Seguire le istruzioni contenute nella [Guida online di ESET HOME](#) e [consentire la connessione in ESET NOD32 Antivirus](#).

1. Nella [finestra principale del programma](#), fare clic su **un account ESET HOME > Connetti a ESET HOME** o su **Connetti a ESET HOME** nella notifica **Collegare il dispositivo a un account ESET HOME**.
2. [Effettuare l'autenticazione all'account ESET HOME](#).

- i** Se non si possiede un account ESET HOME, fare clic su **Crea account** per effettuare la registrazione o consultare le istruzioni contenute nella [Guida online di ESET HOME](#).
- Se si dimentica la password, fare clic su **Ho dimenticato la password** e seguire i passaggi a schermo oppure consultare le istruzioni nella [Guida online di ESET HOME](#).

3. Impostare un **Nome del dispositivo** e fare clic su **Continua**.

4. Dopo aver eseguito correttamente la connessione, viene visualizzata una finestra dei dettagli. Fare clic su **Fine**.

Effettua l'autenticazione a ESET HOME

Sono disponibili vari metodi per effettuare l'autenticazione all'account ESET HOME:

- **Utilizzare l'indirizzo e-mail e la password di ESET HOME:** digitare l'**indirizzo e-mail** e la **password** utilizzati per creare l'account ESET HOME e fare clic su **Effettua l'autenticazione**.
- **Utilizzare l'account Google/AppleID:** fare clic su **Continua con Google** o **Continua con Apple** ed effettuare l'autenticazione all'account appropriato. Dopo aver eseguito correttamente l'autenticazione, l'utente verrà reindirizzato alla pagina web di conferma di ESET HOME. Per continuare, tornare alla finestra del prodotto ESET. Per ulteriori informazioni sull'autenticazione all'account Google/AppleID, consultare le istruzioni nella [Guida online di ESET HOME](#).
- **Scansiona codice QR:** fare clic su **Scansiona codice QR** per visualizzare il codice QR. Aprire l'app mobile ESET HOME e scansionare il codice QR o puntare la fotocamera del dispositivo sul codice QR. Per ulteriori informazioni, consultare le istruzioni contenute nella [Guida online di ESET HOME](#).



Se non si possiede un account ESET HOME, fare clic su **Crea account** per effettuare la registrazione o consultare le istruzioni contenute nella [Guida online di ESET HOME](#).

Se si dimentica la password, fare clic su **Ho dimenticato la password** e seguire i passaggi a schermo oppure consultare le istruzioni nella [Guida online di ESET HOME](#).

[Autenticazione non riuscita: errori comuni](#).

Creane uno'."/>

eset NOD32 ANTIVIRUS

Effettua l'autenticazione all'account ESET HOME

Continua con Google

Continua con Apple

Scansiona codice QR

eset HOME

Indirizzo e-mail

Password

[Ho dimenticato la password](#)

Accesso Annulla

Non possiedi un account? [Creane uno](#)

Autenticazione non riuscita: errori comuni

Non è stato possibile trovare un account corrispondente all'indirizzo e-mail inserito

L'indirizzo e-mail inseriti non corrispondono ad alcun account ESET HOME. Fare clic su **Indietro** e digitare l'indirizzo e-mail e la password corretti.

Per effettuare l'autenticazione, è necessario creare un account ESET HOME. Se non si possiede un account ESET HOME, fare clic su **Indietro** > **Crea account** o consultare [Crea un nuovo account ESET HOME](#).

Il nome utente e la password non corrispondono

La password inserita non corrisponde all'indirizzo e-mail specificato. Fare clic su **Indietro**, digitare la password corretta e assicurarsi che l'indirizzo e-mail inserito sia corretto. Se non è ancora possibile effettuare l'autenticazione, fare clic su **Indietro** > **Ho dimenticato la password** per reimpostare la password e attenersi alle istruzioni a schermo oppure consultare [Ho dimenticato la password di ESET HOME](#).

L'opzione di autenticazione selezionata non corrisponde al tuo account

L'account dell'utente è collegato all'account sui social network. Per effettuare l'autenticazione a ESET HOME, fare clic su **Continua con Google** o su **Continua con Apple** ed effettuare l'autenticazione all'account appropriato. Dopo aver eseguito correttamente l'autenticazione, l'utente verrà reindirizzato alla pagina web di conferma di ESET HOME. È possibile scollegare l'account dei social network dall'account ESET HOME sul portale di ESET HOME.

Password non corretta

Questo errore può verificarsi se ESET NOD32 Antivirus è già connesso a ESET HOME e l'utente sta apportando modifiche che richiedono l'autenticazione (ad esempio, disabilitazione della funzione Anti-Furto) e la password inserita non corrisponde all'account dell'utente. Fare clic su **Indietro** e digitare la password corretta. Se non è ancora possibile effettuare l'autenticazione, fare clic su **Indietro** > **Ho dimenticato la password** per reimpostare la password e attenersi alle istruzioni a schermo oppure consultare [Ho dimenticato la password di ESET HOME](#).

Aggiungi il dispositivo in ESET HOME

Se ESET NOD32 Antivirus è già stato installato e attivato con una licenza aggiunta nell'account ESET HOME, è possibile collegare il dispositivo a ESET HOME utilizzando il portale ESET HOME:

1. [Invia una richiesta di connessione al dispositivo in uso](#).
2. ESET NOD32 Antivirus consente di visualizzare la finestra di dialogo **Collega il dispositivo a un account ESET HOME** con il nome dell'account ESET HOME. Fare clic su **Consenti** per connettere il dispositivo all'account ESET HOME menzionato.

i In assenza di interazione, la richiesta di connessione verrà annullata automaticamente dopo circa 30 minuti.

Interfaccia utente

Per configurare il comportamento dell'interfaccia utente grafica (Graphical User Interface, GUI) del programma, nella [finestra principale del programma](#) fare clic su **Configurazione** > **Configurazione avanzata (F5)** > **Interfaccia utente**.

Nella schermata Configurazione avanzata [Elementi dell'interfaccia utente](#) è possibile regolare l'aspetto e gli effetti visivi del programma.

Per garantire la massima efficacia del software di protezione, è possibile impedire la disinstallazione o l'esecuzione di modifiche non autorizzate attraverso la protezione delle impostazioni mediante una password con lo strumento [Configurazione dell'accesso](#).

i Per configurare il comportamento delle notifiche di sistema, degli avvisi di rilevamento e degli stati dell'applicazione, consultare la sezione [Notifiche](#).

Elementi dell'interfaccia utente

È possibile modificare l'ambiente di lavoro (interfaccia utente grafica, Graphical User Interface o GUI) di ESET NOD32 Antivirus in base alle proprie esigenze in **Configurazione avanzata (F5)** > **Interfaccia utente** > **Elementi dell'interfaccia utente**.

Modalità colore: selezionare la combinazione di colori dell'interfaccia utente grafica di ESET NOD32 Antivirus dal menu a discesa:

- **Uguale al colore del sistema:** consente di impostare la combinazione di colori di ESET NOD32 Antivirus in

base alle impostazioni del sistema operativo in uso.

- **Scuro:**ESET NOD32 Antivirus avrà una combinazione di colori scuri (modalità scura).
- **Chiaro:**ESET NOD32 Antivirus avrà una combinazione di colori chiari e standard.

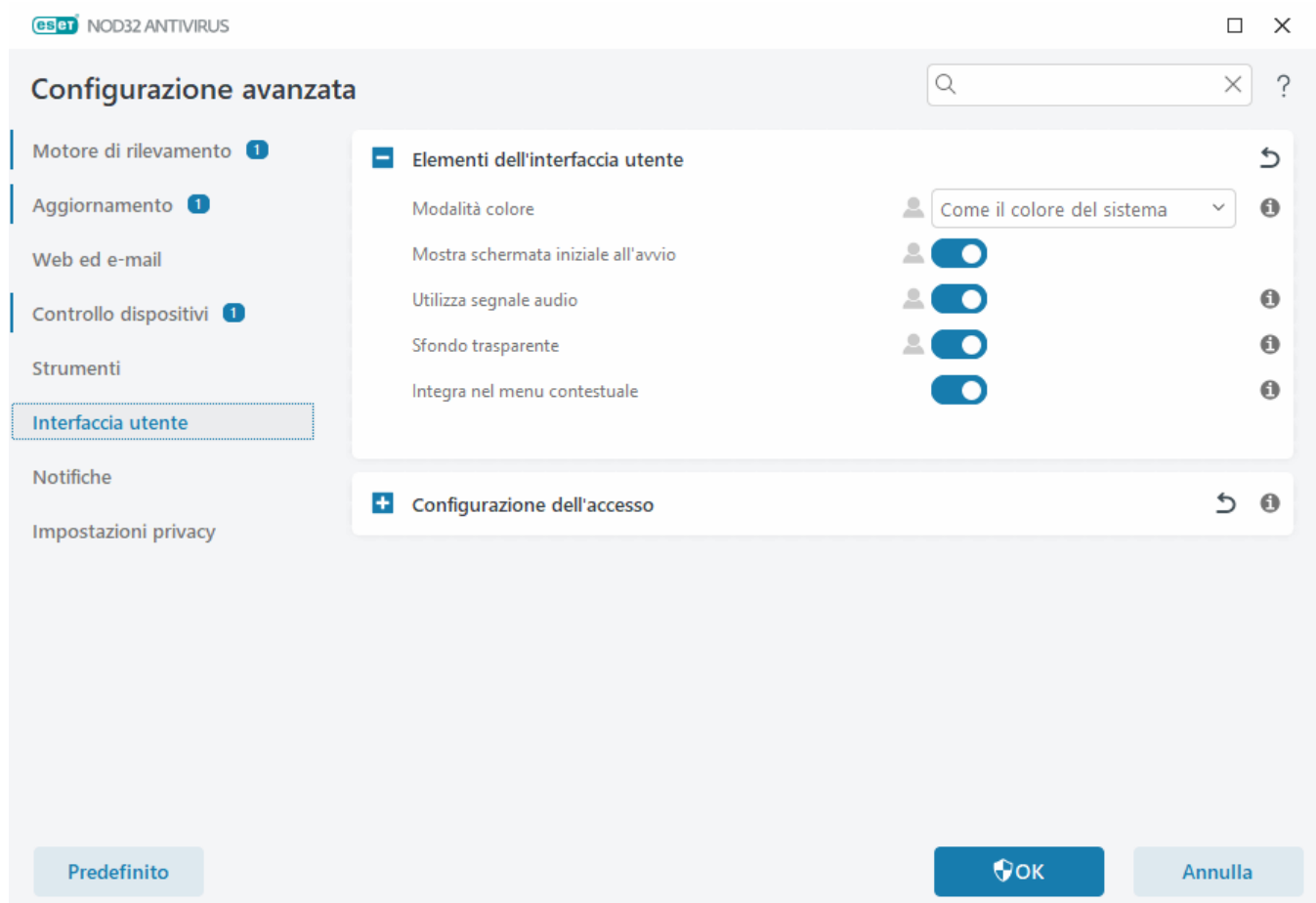
i È anche possibile selezionare la combinazione di colori dell'interfaccia utente grafica (Graphical User Interface, GUI) di ESET NOD32 Antivirus nell'angolo in alto a destra della [finestra principale del programma](#).

Mostra schermata iniziale all'avvio: consente di visualizzare la schermata iniziale di ESET NOD32 Antivirus durante l'avvio.

Utilizza segnale audio: riproduce un suono al verificarsi di eventi importanti durante un controllo, ad esempio in caso di rilevamento di una minaccia o al termine del processo.

Sfondo trasparente: abilita un effetto di sfondo trasparente per la [finestra principale del programma](#). Lo sfondo trasparente è disponibile solo per le versioni più recenti di Windows (RS4 e successive).

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



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 e la disinstallazione di ESET NOD32 Antivirus possono essere protetti con password.

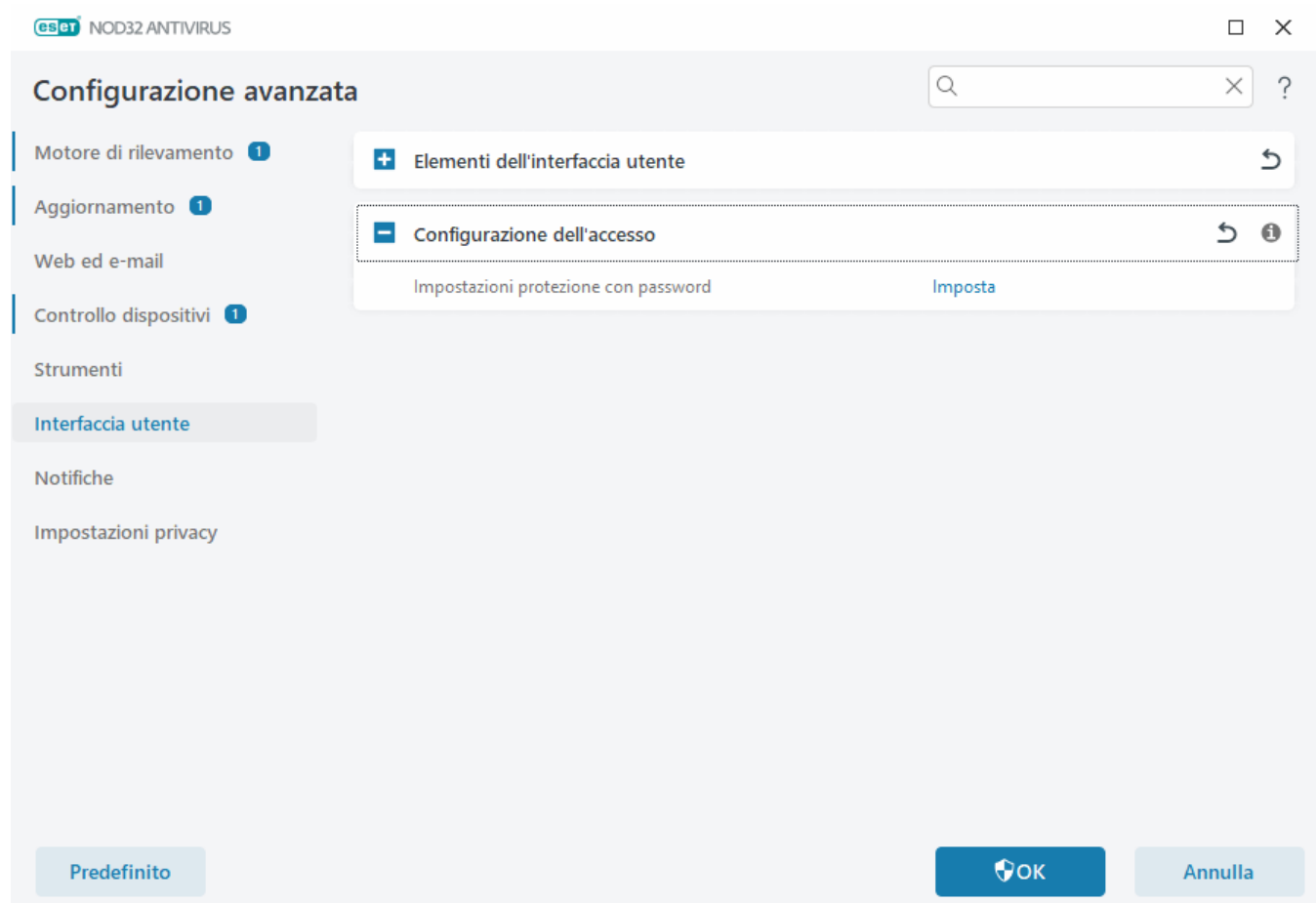
Per impostare una password per proteggere i parametri di configurazione e la disinstallazione di ESET NOD32 Antivirus, fare clic su **Imposta** accanto a **Impostazioni di protezione con password**.

i Se si desidera accedere alla Configurazione avanzata protetta, compare la finestra per l'inserimento della password. Se si dimentica o si smarrisce la password, fare clic sull'opzione **Ripristina password** sotto e inserire l'indirizzo di posta elettronica utilizzato per la registrazione della licenza. ESET invierà una e-mail contenente il codice di verifica e le istruzioni per la reimpostazione della password.

- [Procedura di sblocco della configurazione avanzata](#)

Per modificare la password, fare clic su **Cambia password** accanto a **Impostazioni di protezione con password**.

Per rimuovere la password, fare clic su **Rimuovi** accanto a **Impostazioni di protezione con password**.



Password per la configurazione avanzata

Per proteggere la Configurazione avanzata di ESET NOD32 Antivirus ed evitare modifiche non autorizzate, digitare la nuova password nei campi **Nuova password** e **Conferma password**. Fare clic su **OK**.

Se si desidera modificare una password esistente:


1. Digitare la vecchia password nel campo **Vecchia password**.
2. Inserire la nuova password nei campi **Nuova password** e **Conferma password**.
3. Fare clic su **OK**.

Questa password sarà richiesta per l'accesso alla Configurazione avanzata.

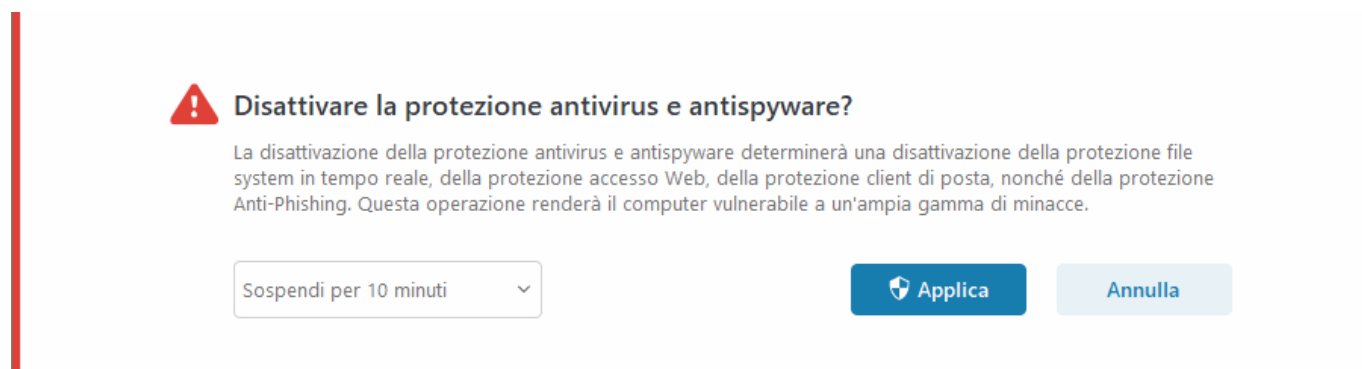
Se è stata dimenticata la password, consultare [Sbloccare la password delle impostazioni nei prodotti ESET HOME](#).

Per recuperare la chiave di licenza ESET smarrita, la data di scadenza della licenza o altre informazioni sulla licenza di ESET NOD32 Antivirus, consultare [Non ho smarrito la chiave di licenza](#).

Icona della barra delle applicazioni

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

Sospendi protezione: consente di visualizzare la finestra di dialogo di conferma per disattivare il [motore di rilevamento](#) che protegge il sistema da attacchi dannosi controllando file e comunicazioni Web e e-mail. Il menu a discesa **Intervallo di tempo** consente all'utente di specificare l'intervallo di tempo durante il quale la protezione verrà disabilitata.



Configurazione: apre la Configurazione avanzata di ESET NOD32 Antivirus. Per aprire Configurazione avanzata dalla [finestra principale del prodotto](#), premere F5 sulla tastiera o fare clic su **Configurazione** > **Configurazione avanzata**.

File di rapporto: i file di rapporto contengono informazioni relative a eventi di programma importanti che si sono verificati e forniscono una panoramica dei rilevamenti.

Apri ESET NOD32 Antivirus: consente di aprire la [finestra principale del programma](#) di ESET NOD32 Antivirus.

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

Modalità colore: consente di aprire le [Impostazioni dell'interfaccia utente](#) in cui è possibile modificare il colore dell'interfaccia utente grafica.

Ricerca aggiornamenti: consente di avviare un modulo o un aggiornamento del prodotto per garantire la protezione. ESET NOD32 Antivirus ricerca automaticamente gli aggiornamenti più volte al giorno.

Informazioni: vengono fornite informazioni sul sistema, sulla versione installata di ESET NOD32 Antivirus, sui moduli del programma installati, sul sistema operativo e sulle risorse di sistema.

Supporto per la lettura dello schermo

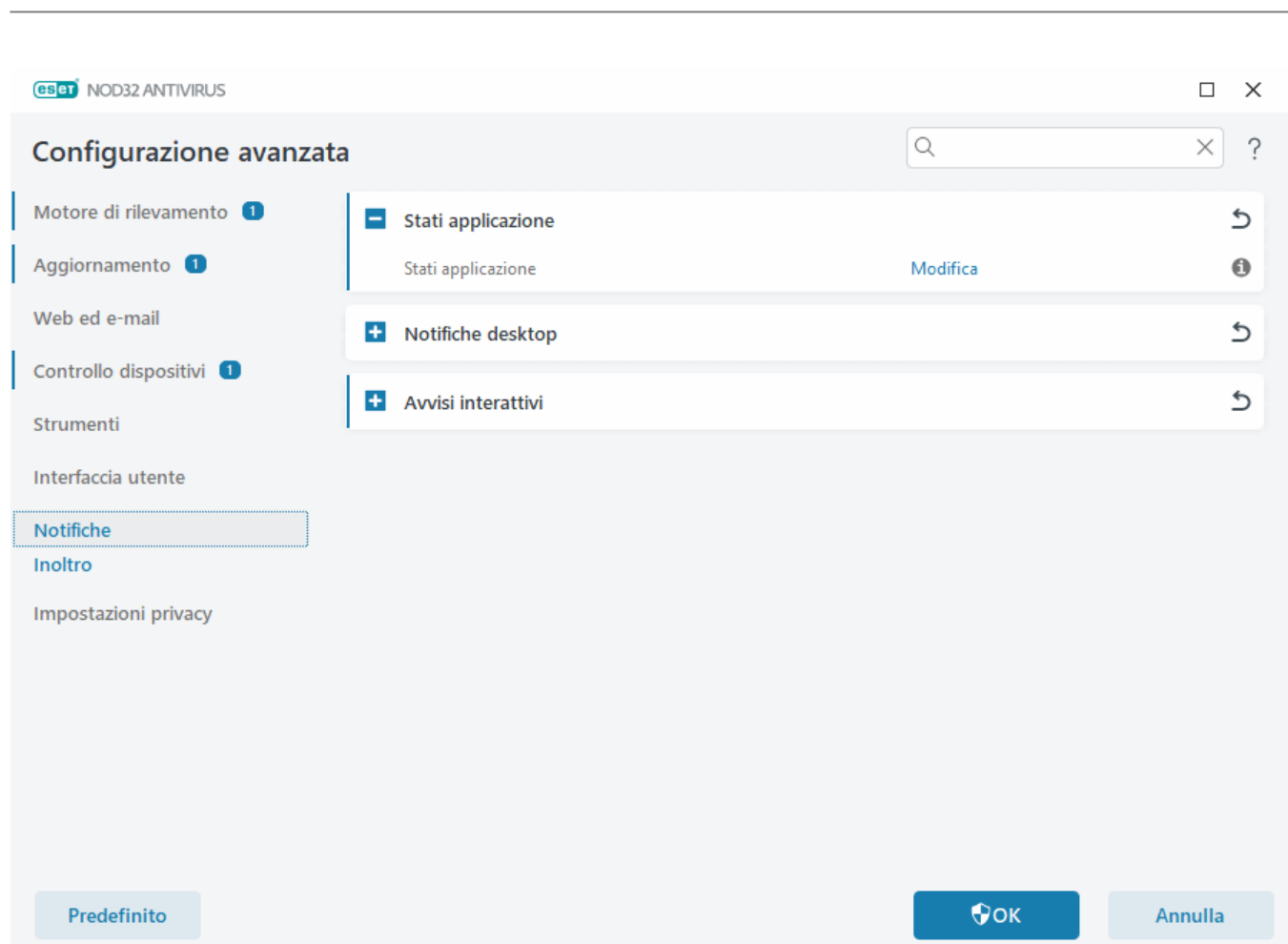
ESET NOD32 Antivirus può essere utilizzato insieme alle utilità per la lettura dello schermo allo scopo di consentire agli utenti ESET con problemi di vista di navigare nel prodotto o di configurare le impostazioni. Sono supportate le seguenti utilità per la lettura dello schermo (JAWS, NVDA, Narrator).

Per assicurarsi che l'utilità per la lettura dello schermo possa accedere correttamente all'interfaccia grafica utente di ESET NOD32 Antivirus, seguire le istruzioni contenute in questo [articolo della Knowledge Base](#).

Notifiche

Per gestire le notifiche di ESET NOD32 Antivirus, aprire la **Configurazione avanzata** (F5) > **Notifiche**. È possibile configurare i seguenti tipi di notifiche:

- Stati dell'applicazione: notifiche visualizzate nella [finestra principale del programma](#) > **Panoramica**.
- [Notifiche desktop](#): piccole finestre di notifica accanto alla barra delle applicazioni del sistema.
- [Avvisi interattivi](#): finestre di avviso e finestre di messaggio che richiedono l'interazione dell'utente.
- [Inoltro](#) (notifiche e-mail): le notifiche e-mail vengono inviate all'indirizzo e-mail specificato.



Stati applicazione

Stati dell'applicazione: fare clic su **Modifica** per selezionare gli stati dell'applicazione che saranno visualizzati nella sezione iniziale della [finestra principale del programma](#) > **Panoramica**.

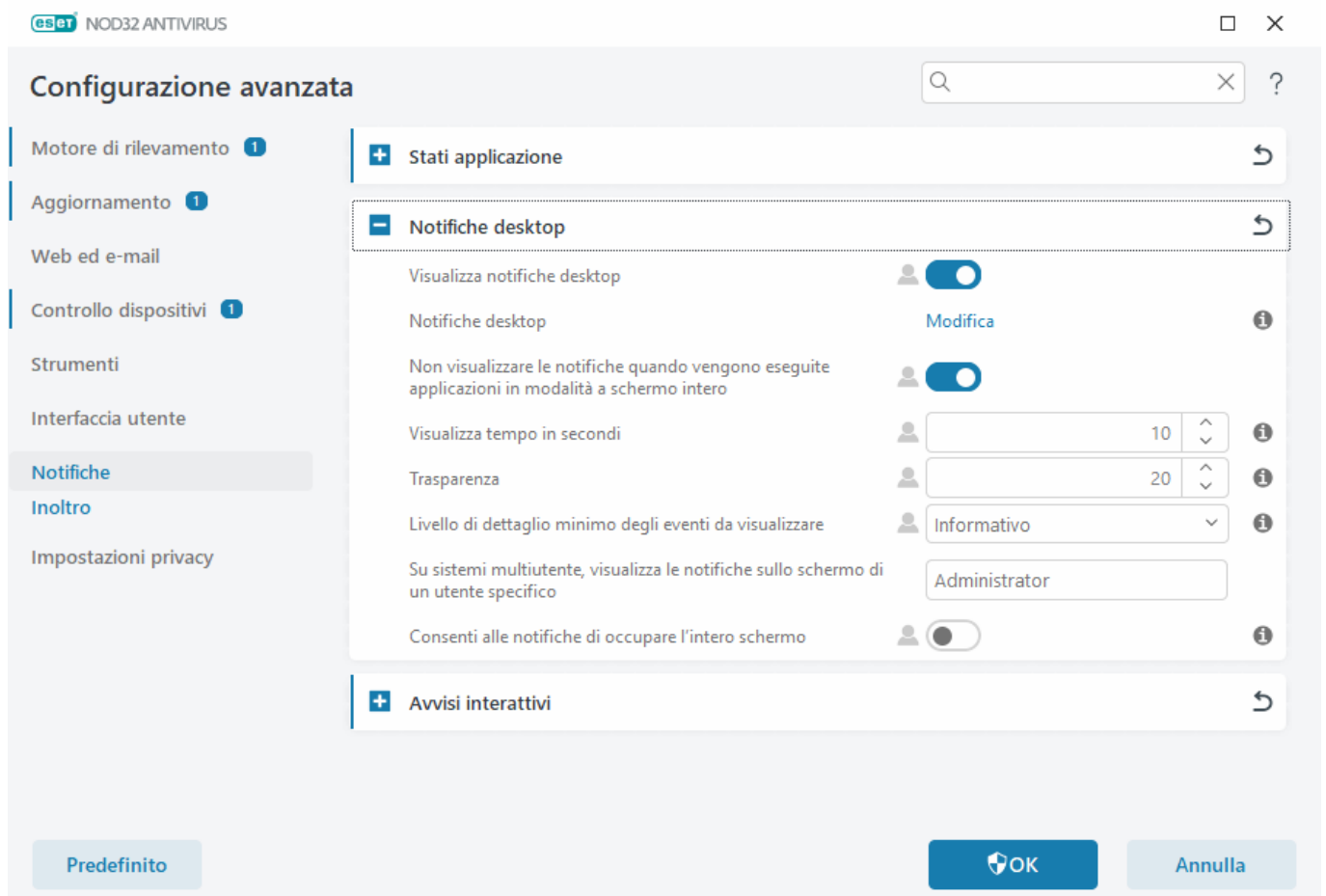
Finestra di dialogo: stati dell'applicazione

In questa finestra di dialogo è possibile selezionare gli stati dell'applicazione che verranno visualizzati. Ad esempio, quando si sospende la protezione antivirus e antispyware o si abilita la modalità giocatore.

Verrà inoltre visualizzato lo stato dell'applicazione se il prodotto non è attivato o la licenza è scaduta.

Notifiche desktop

Le notifiche desktop sono rappresentate da una piccola finestra di notifica accanto alla barra delle applicazioni del sistema. Per impostazione predefinita, vengono visualizzate per 10 secondi, per poi scomparire lentamente. Le notifiche includono aggiornamenti dei prodotti eseguiti correttamente, nuovi dispositivi connessi, completamento delle attività di controllo antivirus o nuove minacce trovate.



Visualizza notifiche sul desktop: si consiglia di mantenere questa opzione abilitata in modo che il prodotto possa informare l'utente quando si verifica un nuovo evento.

Notifiche del desktop: fare clic su **Modifica** per abilitare o disabilitare specifiche [Notifiche del desktop](#).

Non visualizzare le notifiche quando vengono eseguite applicazioni in modalità a schermo intero: elimina tutte le notifiche non interattive quando vengono eseguite applicazioni in modalità a schermo intero.

Timeout in secondi: consente di impostare la durata della visibilità della notifica. Il valore deve essere compreso tra 3 e 30 secondi.

Trasparenza: consente di impostare la percentuale di trasparenza della notifica. L'intervallo supportato è compreso tra 0 (nessuna trasparenza) e 80 (trasparenza molto elevata).

Livello di dettaglio minimo degli eventi da visualizzare: consente di impostare il livello di gravità della notifica iniziale visualizzato. Dal menu a discesa, selezionare una delle seguenti opzioni:

ODiagnostico: consente di visualizzare le informazioni necessarie ai fini dell'ottimizzazione del programma e di tutti i record indicati in precedenza.

OInformativo: consente di visualizzare i messaggi informativi, come gli eventi di rete non standard, compresi quelli relativi agli aggiornamenti riusciti, e tutti i record indicati in precedenza.

OAvvertenze: consente di visualizzare messaggi di avvertenza, errori ed errori critici (ad esempio, aggiornamento non riuscito).

OErrori: consente di visualizzare gli errori (ad esempio, protezione documenti non avviata) e gli errori critici.

OCritico: consente di registrare solo gli errori critici (errori che avviano la protezione antivirus o sistema infetto, ecc.).

Sui sistemi multi-utente, consenti di visualizzare le notifiche sullo schermo di questo utente: consente agli account selezionati di ricevere notifiche desktop. Ad esempio, se non si utilizza l'account Amministratore, digitare il nome completo dell'account per visualizzare le notifiche desktop per l'account in questione. Solo un account utente può ricevere le notifiche desktop.

Consenti di visualizzare le notifiche sullo schermo: consente alle notifiche di essere visualizzate sullo schermo e accessibili nel menu **ALT +Tab**.

Elenco di notifiche desktop

Per regolare la visibilità delle notifiche sul desktop (visualizzate nell'angolo in basso a destra della schermata), aprire la **Configurazione avanzata (F5) > Notifiche > Notifiche desktop**. Fare clic su **Modifica** accanto a **Notifiche desktop** e selezionare la casella di controllo **Mostra** appropriata.

Verranno visualizzate le notifiche desktop selezionate



Nome	Mostra sul desktop
AGGIORNAMENTO	
I moduli sono stati aggiornati correttamente	<input type="checkbox"/>
Il motore di rilevamento è stato aggiornato correttamente	<input type="checkbox"/>
L'aggiornamento dell'applicazione è stato preparato	<input checked="" type="checkbox"/>
GENERALE	
Il file è stato inviato per l'analisi	<input type="checkbox"/>
Visualizza le notifiche Novità	<input checked="" type="checkbox"/>
Visualizza notifiche report di protezione	<input type="checkbox"/>

OK

Annulla

Generale

Visualizza notifiche report di protezione: consente di ricevere una notifica quando viene generato un nuovo [Report di protezione](#).

Visualizza notifiche Novità: notifiche sulle funzioni nuove e avanzate dell'ultima versione del prodotto.

Il file è stato inviato per l'analisi: consente di ricevere una notifica ogni volta che ESET NOD32 Antivirus invia un file per l'analisi.

Aggiornamento

L'aggiornamento dell'applicazione è stato preparato: consente di ricevere una notifica se è disponibile un aggiornamento a una nuova versione dell'applicazione ESET NOD32 Antivirus preparata.

Motore di rilevamento aggiornato correttamente: consente di ricevere una notifica quando il prodotto aggiorna i moduli del motore di rilevamento.

I moduli sono stati aggiornati correttamente: consente di ricevere una notifica quando il prodotto aggiorna i componenti del programma.

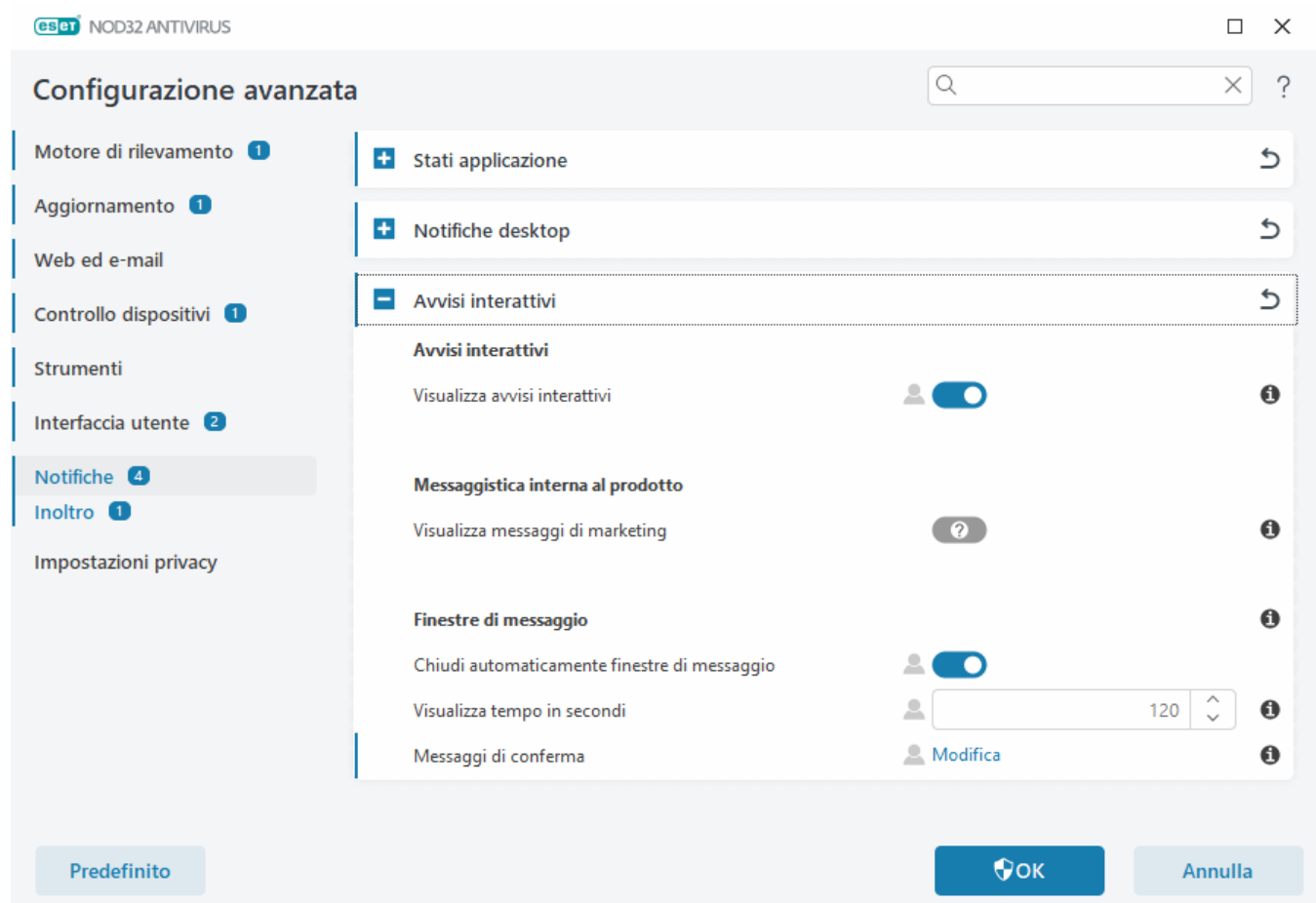
Per definire le impostazioni generali per le notifiche sul desktop, ad esempio, la durata di visualizzazione di un messaggio o il livello di dettaglio minimo degli eventi da visualizzare, consultare [Notifiche desktop](#) in **Configurazione avanzata (F5) > Notifiche**.

Avvisi interattivi

Hai bisogno di informazioni sugli avvisi e le notifiche comuni?

- [Minaccia trovata](#)
- [L'indirizzo è stato bloccato](#)
- [Prodotto non attivato](#)
- [Passa a un prodotto con più funzioni](#)
- ! • [Passa ad un prodotto con meno funzioni](#)
- [Aggiornamento disponibile](#)
- [Le informazioni di aggiornamento non sono coerenti](#)
- [Risoluzione dei problemi relativi al messaggio "Aggiornamento moduli non riuscito"](#)
- [Risolvi errori di aggiornamento moduli](#)
- [Certificato sito Web revocato](#)

La sezione **Avvisi interattivi** in **Configurazione avanzata** (F5) > **Notifiche** consente all'utente di configurare le modalità di gestione, da parte di ESET NOD32 Antivirus, delle finestre di messaggio e degli avvisi interattivi per i rilevamenti, in cui l'utente è chiamato a prendere una decisione (ad esempio, un potenziale sito web di phishing).



Avvisi interattivi

La disabilitazione dell'opzione **Visualizza avvisi interattivi** impedisce la visualizzazione delle finestre di avviso e delle finestre di dialogo all'interno del browser. Tale operazione è adatta solo a un numero limitato di situazioni specifiche. Si consiglia di mantenere questa opzione abilitata.

Messaggistica interna al prodotto

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. L'invio di messaggi promozionali richiede il consenso dell'utente. Di conseguenza, queste informazioni non vengono inviate all'utente per impostazione predefinita (tale aspetto viene indicato con un punto interrogativo). Abilitando questa opzione, l'utente accetta di ricevere messaggi promozionali da ESET. Disabilitare l'opzione **Visualizza messaggi di marketing** se non si desidera ricevere messaggi promozionali da ESET.

Finestre di messaggio

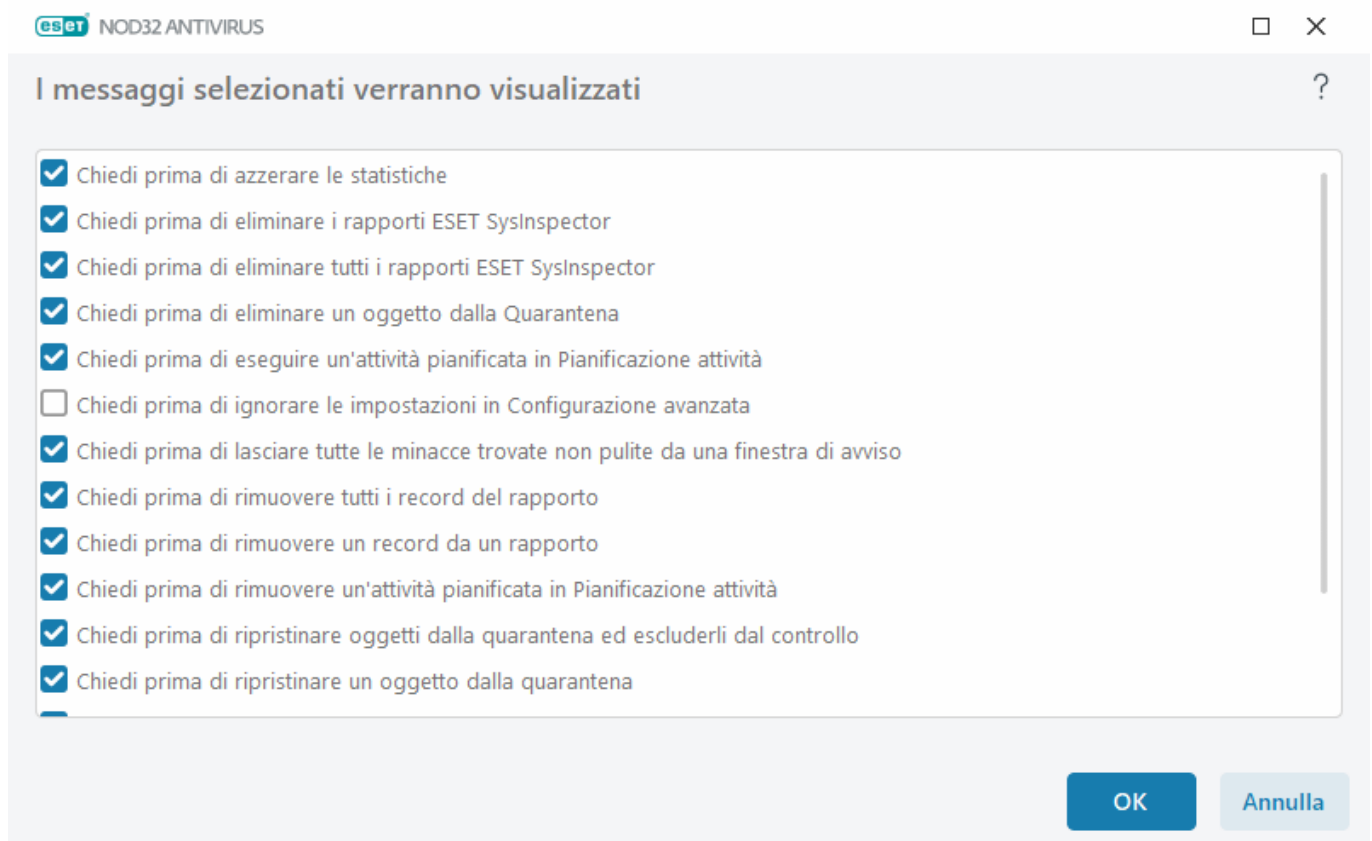
Per chiudere automaticamente le finestre di messaggio dopo un determinato periodo di tempo, selezionare **Chiudi automaticamente le finestre di messaggio**. Se non vengono chiuse manualmente, le finestre di avviso vengono chiuse automaticamente una volta trascorso il tempo specificato.

Timeout in secondi: consente di impostare la durata della visibilità dell'avviso. Il valore deve essere compreso tra 10 e 999 secondi.

Messaggi di conferma: fare clic su **Modifica** per visualizzare un [elenco di messaggi di conferma](#) che è possibile decidere di visualizzare o di non visualizzare.

Messaggi di conferma

Per modificare i messaggi di conferma, portarsi in **Configurazione avanzata (F5) > Notifiche > Avvisi interattivi** e fare clic su **Modifica** accanto a **Messaggi di conferma**.



Questa finestra di dialogo consente di visualizzare messaggi di conferma in ESET NOD32 Antivirus prima

dell'esecuzione di qualsiasi azione. Selezionare o deselezionare la casella di controllo accanto a ciascun messaggio di conferma per consentirlo o disattivarlo.

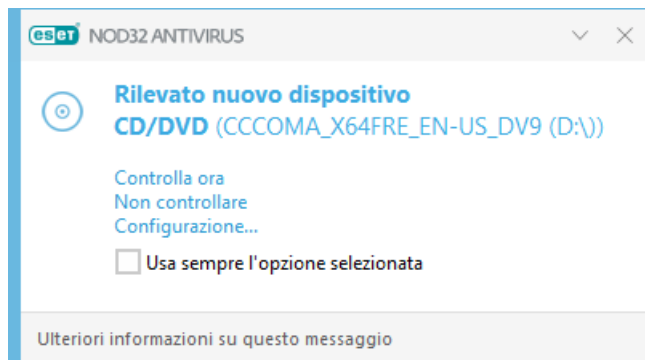
Ulteriori informazioni sulla funzione specifica correlata ai messaggi di conferma:

- [Chiedi prima di rimuovere i rapporti di ESET SysInspector](#)
- [Chiedi prima di rimuovere tutti i rapporti di ESET SysInspector](#)
- [Chiedi prima di eliminare un oggetto dalla Quarantena](#)
- Chiedi prima di ignorare le impostazioni in Configurazione avanzata
- [Chiedi prima di lasciare tutte le minacce trovate non pulite da una finestra di avviso](#)
- [Chiedi prima di rimuovere un record da un rapporto](#)
- [Chiedi prima di rimuovere un'attività pianificata in Pianificazione attività](#)
- [Chiedi prima di rimuovere tutti i record del rapporto](#)
- [Chiedi prima di azzerare le statistiche](#)
- [Chiedi prima di ripristinare un oggetto dalla quarantena](#)
- [Chiedi prima di ripristinare oggetti dalla quarantena ed escluderli dal controllo](#)
- [Chiedi prima di eseguire un'attività pianificata in Pianificazione attività](#)
- [Mostra finestre di dialogo di conferma del prodotto per i client di posta Outlook Express e Windows Mail](#)
- [Mostra finestre di dialogo di conferma del prodotto per Windows Live Mail](#)
- [Mostra finestre di dialogo di conferma del prodotto per il client di posta Outlook](#)

Supporti rimovibili

ESET NOD32 Antivirus offre un controllo automatico dei supporti rimovibili (CD/DVD/USB/...) una volta collegati a un computer. 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.

In caso di inserimento di un supporto rimovibile e di impostazione dell'opzione **Mostra opzioni di controllo** in ESET NOD32 Antivirus, verrà visualizzata la seguente finestra di dialogo:



Opzioni per questa finestra di dialogo:

- **Controlla ora:** avvia il controllo del supporto rimovibile.
- **Non controllare:** i supporti rimovibili non verranno controllati.
- **Configurazione:** apre la sezione **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](#).

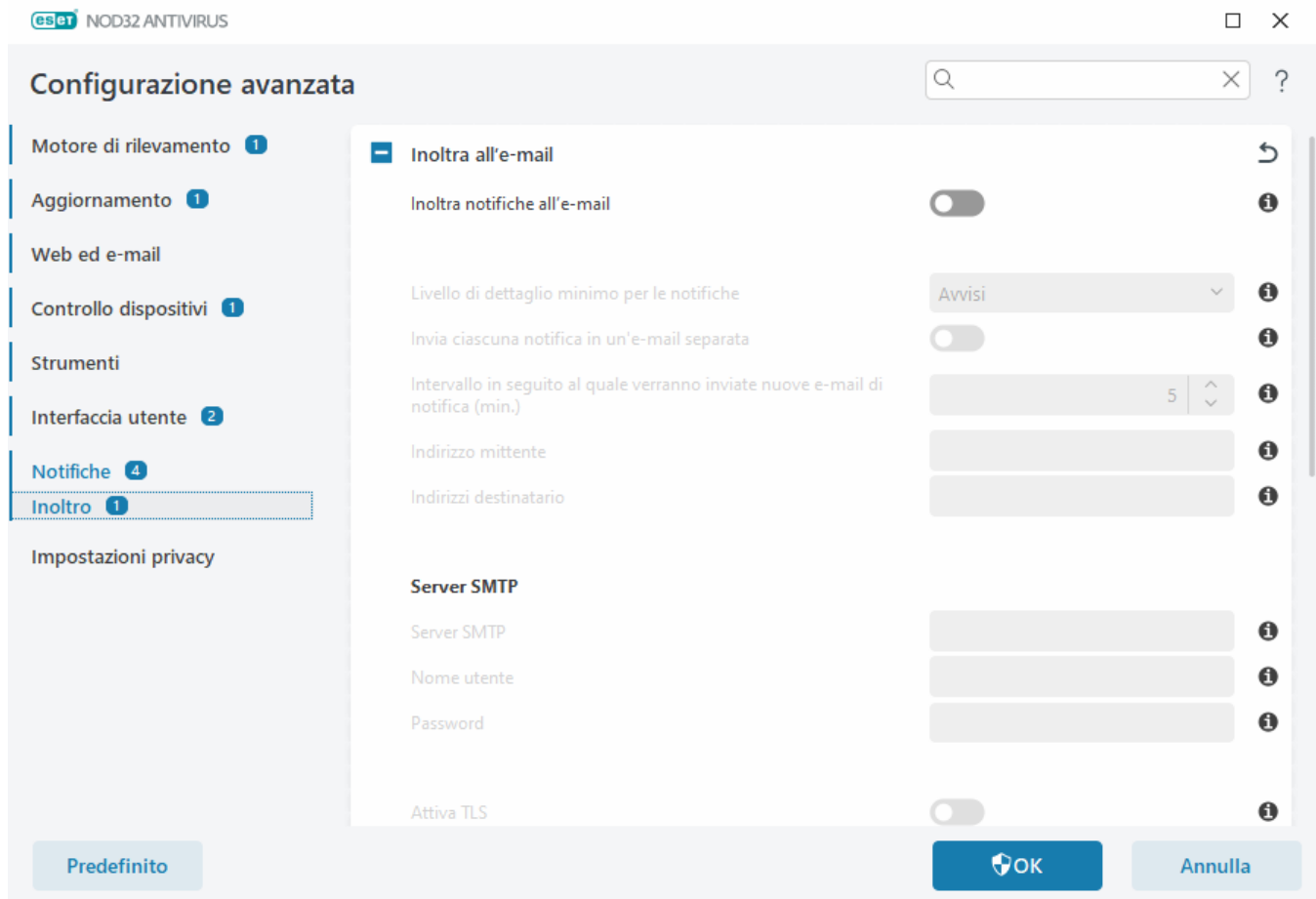
Per accedere alle impostazioni per il controllo dei supporti rimovibili, aprire Configurazione avanzata (**F5**) > **Motore di rilevamento** > **Controlli malware** > **Supporti rimovibili**.

Azione da eseguire in seguito all'inserimento dei supporti rimovibili: selezionare l'azione predefinita che verrà eseguita quando un supporto rimovibile viene inserito nel computer (CD/DVD/USB). Scegliere l'azione desiderata dopo aver inserito un supporto rimovibile in un computer:

- **Non controllare:** non verrà eseguita alcuna azione e la finestra **Nuovo dispositivo rilevato** non si aprirà.
- **Controllo automatico del dispositivo:** verrà eseguito un controllo del computer del supporto rimovibile inserito.
- **Mostra opzioni di controllo:** apre la sezione di configurazione dei **supporti rimovibili**.

Inoltro

ESET NOD32 Antivirus può inviare automaticamente e-mail di notifica nel caso in cui si verifichi un evento con il livello di dettaglio selezionato. Aprire la **Configurazione avanzata** (**F5**) > **Notifiche** > **Inoltro** e abilitare **Inoltra notifiche all'e-mail** per attivare le notifiche tramite e-mail.



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.
- **Avvertenze:** consente di registrare errori critici e messaggi di avvertenza (ad esempio, aggiornamento non riuscito).
- **Errori:** verranno registrati errori quali "Protezione del documento non avviata" ed errori critici.
- **Critico:** consente di registrare solo gli errori critici (ad esempio, errore che avvia la protezione antivirus o minaccia trovata).

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

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.

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

Indirizzi dei destinatari: definire gli indirizzi dei destinatari che verranno visualizzati nell'intestazione delle e-mail di notifica. Dal momento che è consentito più di un valore. Utilizzare il punto e virgola come separatore.

SMTP server

Server **SMTP**: server SMTP utilizzato per l'invio di notifiche (ad esempio, per smtp.provider.com:587, la porta predefinita è 25).

 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.

Abilita TLS: Secure Alert e notifiche che utilizzano la crittografia TLS.

Connessione SMTP di prova: un'e-mail di prova verrà inviata all'indirizzo e-mail del destinatario. È necessario compilare i campi Server SMTP, Nome utente, Password, Indirizzo del mittente e Indirizzi dei destinatari.

Formato del messaggio

Le comunicazioni tra il programma e un utente remoto o un amministratore di sistema avvengono tramite e-mail o messaggi LAN (utilizzando il servizio Messenger di Windows). Il **formato predefinito dei messaggi** e delle notifiche di avviso è adatto alla maggior parte delle situazioni. In alcune circostanze, potrebbe essere necessario modificare il formato dei messaggi di evento.

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 mantenere il formato predefinito. 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.

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

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).

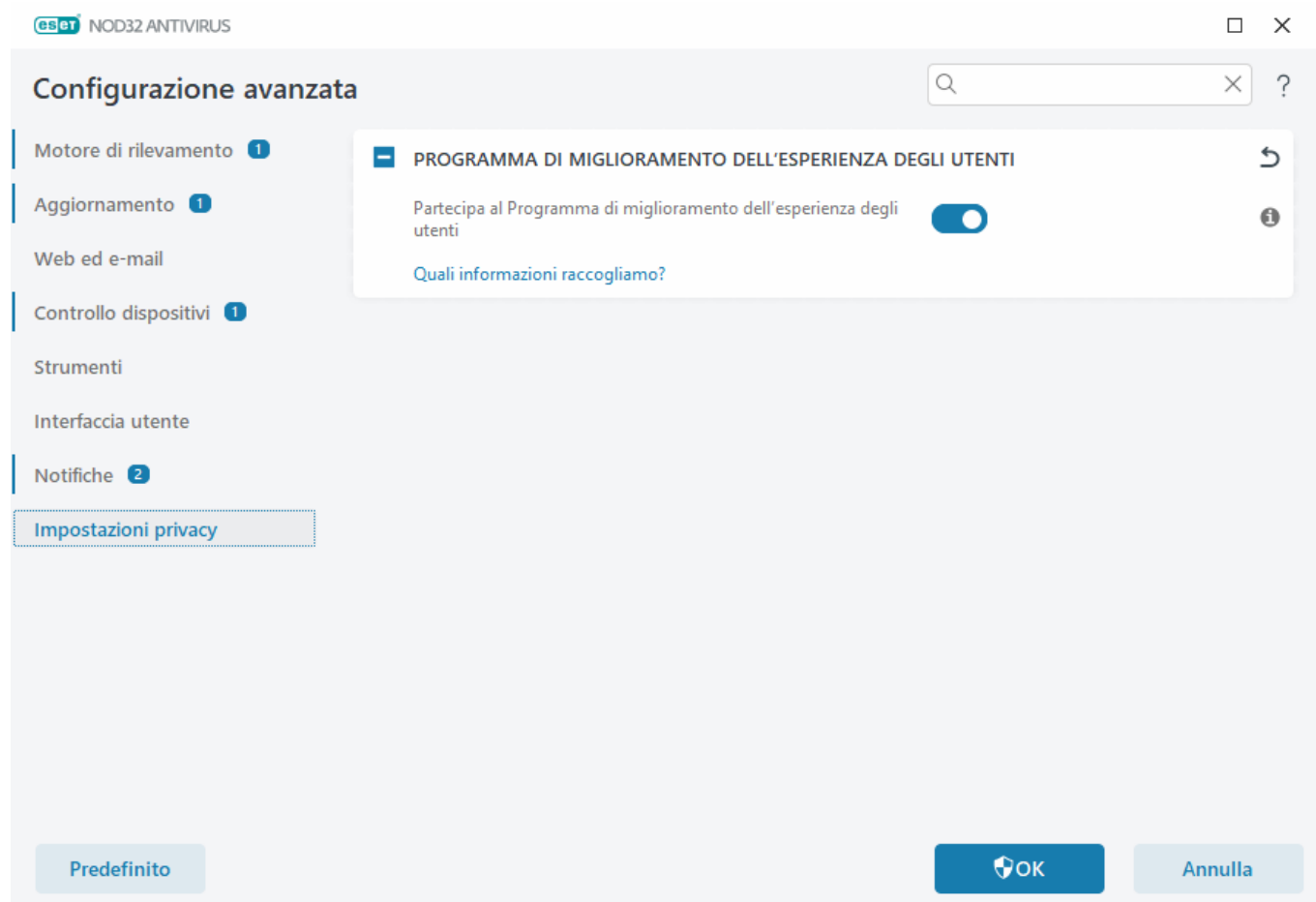
- **%TimeStamp%:** data e ora dell'evento
- **%Scanner%:** modulo interessato
- **%ComputerName%:** nome del computer in cui si è verificato l'avviso
- **%ProgramName%:** programma che ha generato l'avviso
- **%InfectedObject%:** nome del file infetto, messaggio, ecc.
- **%VirusName%:** identificazione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

- **%Action%** : azione intrapresa sull'infiltrazione
- **%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.

Impostazioni privacy

Nella [finestra principale del programma](#) fare clic su **Configurazione > Configurazione avanzata (F5) > Impostazioni privacy**.



Programma di miglioramento dell'esperienza degli utenti

Abilitare la barra di scorrimento accanto a **Partecipa al Programma di miglioramento dell'esperienza degli utenti** per partecipare al Programma di miglioramento dell'esperienza degli utenti. Partecipando, l'Utente fornisce a ESET informazioni anonime relative all'utilizzo dei propri prodotti. I dati raccolti, che aiuteranno l'azienda a migliorare l'esperienza degli utenti, non verranno mai condivisi con terze parti. [Che tipo di informazioni raccogliamo?](#)

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

In ESET NOD32 Antivirus sono disponibili 4 profili di controllo predefiniti:

- **Controllo intelligente** – profilo di controllo avanzato predefinito. Utilizza la tecnologia di ottimizzazione intelligente che esclude i file che sono stati trovati puliti in un controllo precedente e che non sono stati modificati da allora. Ciò consente di ridurre i tempi di controllo con un impatto minimo sulla sicurezza del sistema.
- **Controllo menu contestuale** – dal menu contestuale è possibile avviare un controllo su richiesta di qualsiasi file. Il profilo di controllo del menu contestuale consente all'utente di definire una configurazione di controllo che verrà utilizzata durante questa tipologia di attivazione del controllo.
- **Controllo approfondito** – Per impostazione predefinita, il profilo Controllo approfondito non utilizza l'ottimizzazione intelligente, in modo che nessun file venga escluso dal controllo utilizzando questo profilo.
- **Controllo computer** – profilo predefinito utilizzato nel controllo del computer standard.

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 **Motore di rilevamento > Controlli malware > Controllo su richiesta > 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.

i 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 **Correggi sempre il rilevamento**. 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.

Aggiornamento

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.

Tasti di scelta rapida

Per una migliore navigazione in ESET NOD32 Antivirus, è possibile utilizzare i seguenti tasti di scelta rapida:

Tasti di scelta rapida	Azione
F1	apre le pagine della Guida
F5	apre la Configurazione avanzata
Freccia in su/Freccia in giù	navigazione nelle voci del menu a discesa
TAB	spostamento verso l'elemento successivo dell'interfaccia utente grafica in una finestra
Shift+TAB	spostamento verso l'elemento precedente dell'interfaccia utente grafica in una finestra
ESC	chiude la finestra di dialogo attiva
Ctrl+U	consente di visualizzare le informazioni sulla licenza ESET e il computer (dettagli per il Supporto tecnico)
Ctrl+R	ripristina le dimensioni predefinite e la posizione sullo schermo della finestra del prodotto
ALT + Freccia a sinistra	spostamento indietro
ALT + Freccia a destra	spostamento in avanti
ALT+Home	navigazione nella pagina iniziale

Per la navigazione in avanti o indietro è anche possibile utilizzare i pulsanti del mouse.

Diagnostica

La diagnostica offre all'applicazione i dump di arresto anomalo dei processi ESET (ad esempio, ekrn). Se un'applicazione si arresta in modo anomalo, verrà generato un dump. Permette agli sviluppatori di facilitare la diagnosi e di correggere i problemi correlati a ESET NOD32 Antivirus.

Fare clic sul menu a discesa accanto a **Tipo di dump** e selezionare una delle tre opzioni disponibili:

- Selezionare **Disattiva** per disattivare questa funzionalità.
- **Mini** (predefinito): 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 contenere dati estrapolati dai processi in esecuzione quando è stato raccolto il dump di memoria.

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**.

Registrazione avanzata

Abilita registrazione avanzata nei messaggi di marketing: consente di registrare tutti gli eventi correlati ai messaggi di marketing all'interno del prodotto.

Abilita Registrazione avanzata scanner computer: consente di registrare tutti gli eventi che si verificano durante il controllo di file e cartelle da parte del Controllo computer.

Attiva registrazione avanzata Controllo dispositivi: registrazione di tutti gli eventi che si verificano nel Controllo dispositivi. Permette agli sviluppatori di facilitare diagnosi e correzione di eventuali problemi legati al Controllo dispositivi.

Abilita registrazione avanzata Direct Cloud: consente di registrare tutti gli eventi che si verificano in ESET LiveGrid®. Permette agli sviluppatori di facilitare la diagnosi e di correggere i problemi correlati a ESET LiveGrid®.

Abilita la registrazione avanzata protezione documenti: registrare tutti gli eventi che si verificano in Protezione documenti per consentire la diagnosi e la risoluzione dei problemi.

Abilita Registrazione avanzata della protezione client di posta: consente di registrare tutti gli eventi che si verificano nella Protezione client di posta e nel plug-in del client di posta per consentire la diagnosi e la risoluzione dei problemi.

Abilita registrazione avanzata kernel: consente di registrare tutti gli eventi che si verificano nel kernel ESET (ekrn).

Attiva registrazione avanzata licenze: registra tutte le comunicazioni del prodotto con i server di attivazione ESET o ESET License Manager.

Abilita tracciatura memoria: consente di registrare tutti gli eventi che aiutano gli sviluppatori a diagnosticare le perdite di memoria.

Abilita registrazione avanzata del sistema operativo: consente di registrare informazioni aggiuntive sul sistema operativo, tra cui i processi in esecuzione, l'attività della CPU e le operazioni del disco. Questa funzione aiuta gli sviluppatori a diagnosticare e a risolvere problemi correlati al prodotto ESET in esecuzione sul sistema operativo in uso.

Attiva registrazione avanzata filtraggio protocolli: registra tutti i dati che attraversano il motore di filtraggio protocolli in formato PCAP. Questa funzione aiuta gli sviluppatori a diagnosticare e risolvere problemi correlati al filtraggio protocolli.

Abilita registrazione avanzata messaggistica push: consente di registrare tutti gli eventi che si verificano durante la messaggistica push.

Abilita registrazione avanzata protezione file system in tempo reale: consente di registrare tutti gli eventi che si verificano durante il controllo di file e cartelle da parte della protezione file system in tempo reale.

Attivare registrazione avanzata motore di aggiornamento: registra tutti gli eventi che si verificano durante il processo di aggiornamento. Questa funzione aiuta gli sviluppatori a diagnosticare e risolvere problemi correlati al motore degli aggiornamenti.

I file di rapporto sono posizionati in *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Supporto tecnico

Quando [si contatta il Supporto tecnico di ESET](#) da ESET NOD32 Antivirus, è possibile inviare i dati di configurazione del sistema. Selezionare **Invia sempre** dal menu a discesa **Invia dati di configurazione del sistema** per inviare automaticamente i dati oppure selezionare **Chiedi prima di inviare una richiesta** per essere avvisati prima di inviare i dati.

Importa ed esporta impostazioni

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

Istruzioni illustrate

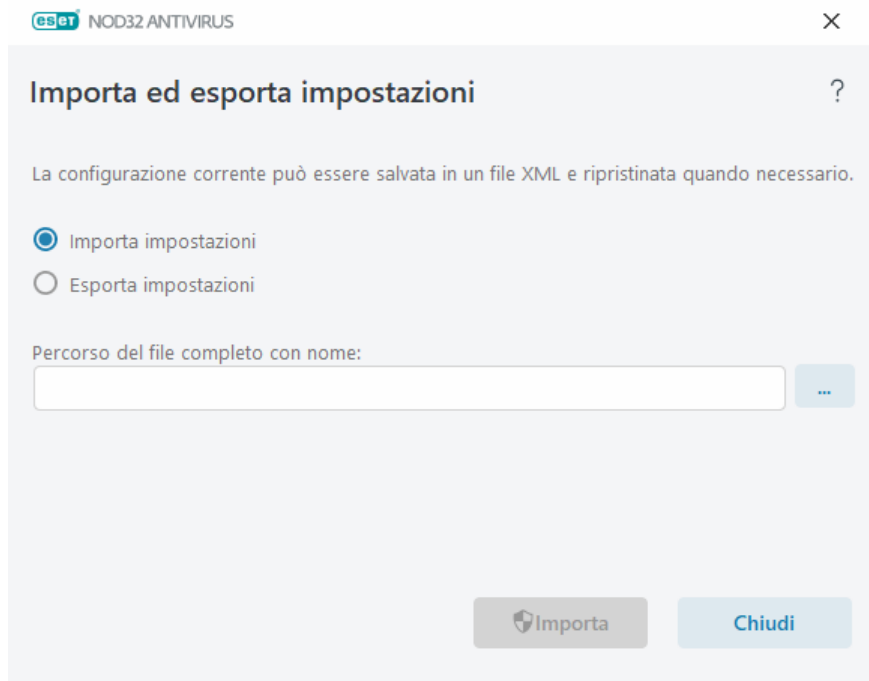
i Per consultare le istruzioni illustrate disponibili in lingua inglese e in molte altre lingue, consultare [Importa o esporta le impostazioni di configurazione ESET utilizzando un file .xml](#).

I file di importazione e di esportazione delle configurazioni sono utili se si desidera 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. È possibile importare un file .xml per il trasferimento di queste impostazioni.


Per importare una configurazione, nella [finestra principale del programma](#), fare clic su **Configurazione > Importa/esporta impostazioni** e selezionare **Importa impostazioni**. Digitare il nome del file di configurazione o fare clic sul pulsante ... per ricercare il file di configurazione che si desidera importare.

Per esportare una configurazione, nella [finestra principale del programma](#), fare clic su **Configurazione > Importa/esporta impostazioni**. Selezionare **Esporta impostazioni** e digitare il percorso completo del file con il nome. Fare clic su ... per portarsi in un percorso del computer in uso in cui salvare il file di configurazione.

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



Ripristina tutte le impostazioni nella sezione corrente

Fare clic sulla freccia che curca  per ripristinare tutte le impostazioni predefinite impostate da ESET nella sezione corrente.

Si tenga presente che le eventuali modifiche apportate andranno perse facendo clic su **Ripristina impostazione predefinita**.

Ripristina contenuti tabelle: attivando questa opzione, le regole, le attività o i profili aggiunti manualmente o automaticamente andranno persi.

Consultare anche [Importa ed esporta impostazioni](#).

Ripristina impostazioni predefinite

Fare clic su **Predefinito** in **Configurazione avanzata** (F5) per ripristinare le impostazioni del programma per tutti i moduli. Lo stato di tutte le impostazioni verrà ripristinato sui valori originali come dopo una nuova installazione.

Consultare anche [Importa ed esporta impostazioni](#).

Errore durante il salvataggio della configurazione

Questo messaggio di errore indica che le impostazioni non sono state salvate correttamente a causa di un errore.

Generalmente ciò significa che l'utente che ha tentato di modificare i parametri del programma:

- non dispone di diritti di accesso sufficienti o non dispone dei privilegi necessari sul sistema operativo per modificare i file di configurazione e il registro di sistema.
> Per eseguire le modifiche desiderate, l'accesso deve essere eseguito dall'amministratore del sistema.

- ha recentemente attivato la modalità di riconoscimento in HIPS o nel firewall e ha tentato di apportare modifiche alla Configurazione avanzata.
- > Per salvare la configurazione ed evitare conflitti, chiudere Configurazione avanzata senza salvare e provare ad apportare nuovamente le modifiche desiderate.

La seconda causa più comune potrebbe dipendere dal fatto che il programma non funziona più correttamente, è danneggiato e deve pertanto essere reinstallato.

Scanner 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 di ESET Command-Line Scanner:

```
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=CARTELLA	carica moduli da CARTELLA
/quar-dir=CARTELLA	CARTELLA di quarantena
/exclude=MASCHERA	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=LIVELLO	sottolivello massimo delle cartelle all'interno di cartelle su cui eseguire la scansione
/symlink	seguì 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)
/auid	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=DIMENSIONE	esegui solo la scansione dei file inferiori a DIMENSIONE megabyte (impostazione predefinita 0 = illimitato)
/max-arch-level=LIVELLO	sottolivello massimo degli archivi all'interno di archivi (archivi nidificati) su cui eseguire la scansione
/scan-timeout=LIMITE	esegui scansione degli archivi per LIMITE secondi al massimo
/max-arch-size=DIMENSIONE	esegui la scansione dei file di un archivio solo se inferiori a DIMENSIONE (impostazione predefinita 0 = illimitato)
/max-sfx-size=DIMENSIONE	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 di 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-exclude=ESTENSIONI	escludi dal controllo le ESTENSIONI dei file delimitate da due punti

/clean-mode=MODALITÀ	utilizza la MODALITÀ pulizia per gli oggetti infetti Sono disponibili le seguenti opzioni: <ul style="list-style-type: none"> • none (predefinito): non verrà eseguita alcuna pulizia automatica. • standard: 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.
/quarantine	copiare i file infettati (se puliti) in Quarantena (integra l'azione eseguita durante la pulizia)
/no-quarantine	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

i I codici di uscita superiori a 100 indicano che non è stata eseguita la scansione del file, il quale potrebbe quindi essere infetto.

ESET CMD

Questa funzione consente di attivare i comandi ecmd avanzati. Consente all'utente di esportare e importare impostazioni utilizzando la riga di comando (ecmd.exe). Finora era possibile esportare impostazioni utilizzando esclusivamente l'[interfaccia grafica utente \(Graphic User Interface, GUI\)](#). ESET NOD32 Antivirus la configurazione può essere esportata in un 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**: è richiesta una password per l'importazione di una configurazione da un file *.xml*, che deve essere firmato (consultare Firma del file di configurazione *.xml* di seguito). La password

specificata in [Configurazione dell'accesso](#) deve essere fornita prima dell'importazione di una nuova configurazione. Se la configurazione dell'accesso non è stata attivata, la password non corrisponde o il file di configurazione .xml non è stato firmato, la configurazione non sarà importata.

Dopo aver attivato ESET CMD, è possibile utilizzare la riga di comando per importare o esportare le configurazioni di ESET NOD32 Antivirus. È possibile eseguire questa operazione manualmente o creare uno script per l'automazione.

Per utilizzare i comandi `ecmd` avanzati, è necessario eseguirli con privilegi di amministratore o aprire un prompt dei comandi di Windows (`cmd`) utilizzando **Esegui come amministratore**. In caso contrario, comparirà il messaggio **Error executing command**. Inoltre, durante l'esportazione di una configurazione, la cartella di destinazione deve essere esistente. Il comando Esporta continua a funzionare anche in caso di disattivazione dell'impostazione ESET CMD.

Comando Esporta impostazioni:
`ecmd /getcfg c:\config\settings.xml`

Comando Importa impostazioni:
`ecmd /setcfg c:\config\settings.xml`

i I comandi `ecmd` avanzati possono essere eseguiti solo localmente.

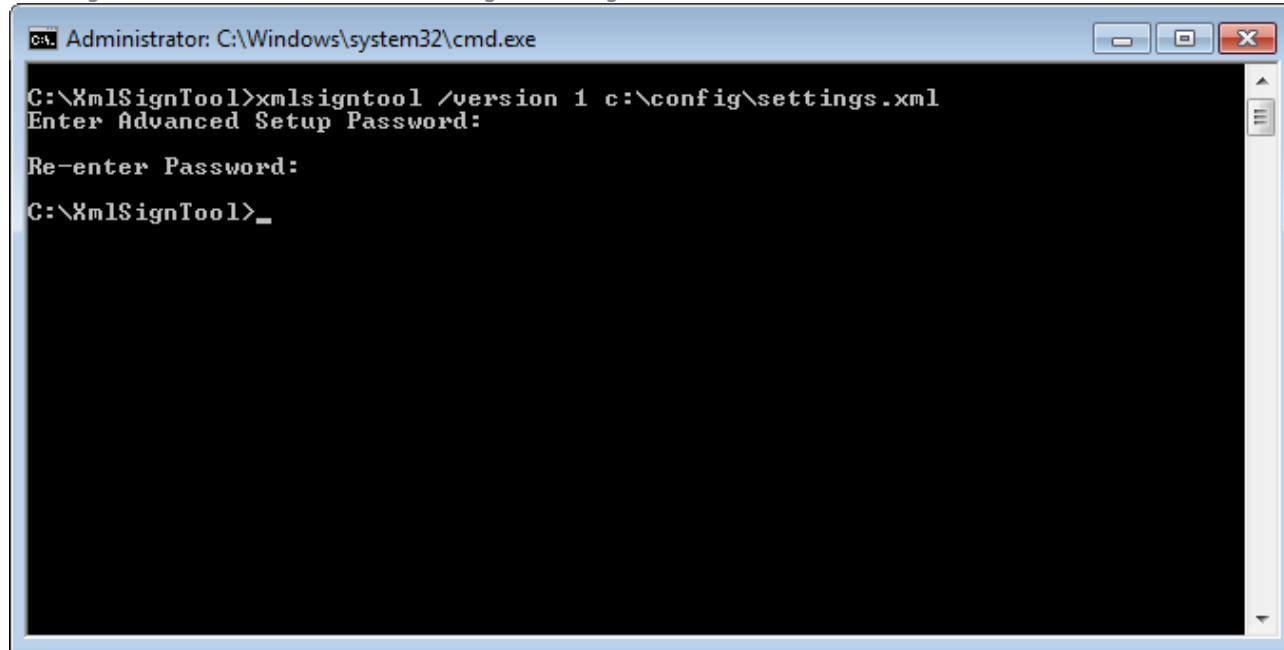
Firma di un file di configurazione .xml:

1. Scaricare l'eseguibile [XmlSignTool](#).
2. Aprire un prompt dei comandi di Windows (`cmd`) utilizzando **Esegui come amministratore**.
3. Accedere al percorso di salvataggio di `xmlsigntool.exe`
4. Eseguire un comando per firmare il file di configurazione .xml, utilizzo: `xmlsigntool /version 1|2 <xml_file_path>`

Il valore del parametro `/version` dipende dalla versione di ESET NOD32 Antivirus. Utilizzare `/version 1` per le versioni di ESET NOD32 Antivirus precedenti alla 11.1. Utilizzare `/version 2` per la versione corrente di ESET NOD32 Antivirus.

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 su un'altra istanza di ESET NOD32 Antivirus con ESET CMD mediante il metodo di autorizzazione con password.

Comando Firma file di configurazione esportato:
xmlsigntool /version 2 c:\config\settings.xml



Se la password della [Configurazione dell'accesso](#) viene modificata e si desidera importare una configurazione firmata in precedenza con una vecchia password, è necessario firmare nuovamente il file di configurazione .xml utilizzando la password corrente. Ciò consente all'utente di utilizzare un file di configurazione precedente senza doverlo esportare su un'altra macchina su cui è in esecuzione ESET NOD32 Antivirus prima dell'importazione.



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.

Rilevamento stato di inattività

Le impostazioni del rilevamento stato inattivo possono essere configurate in **Configurazione avanzata** da **Motore di rilevamento > Controlli malware > Controllo stato inattivo > Rilevamento stato inattivo**. Queste impostazioni specificano l'attivazione del [Controllo stato inattivo](#):

- Schermo o screen saver disattivato
- Blocco computer
- Uscita utente

Utilizzare le barre di scorrimento di ciascuno stato per abilitare o disabilitare i vari metodi di attivazione del rilevamento dello stato di inattività.

Domande comuni

Di seguito sono riportate alcune domande frequenti e viene fornita una panoramica dei 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 fare per creare una nuova attività in Pianificazione attività](#)
- [Come pianificare un'attività di controllo \(settimanalmente\)](#)
- [Procedura di sblocco della configurazione avanzata](#)
- [Come risolvere la disattivazione del prodotto da ESET HOME](#)

Se il problema riscontrato non è presente nell'elenco sopraindicato, provare a eseguire una ricerca nella Guida online di ESET NOD32 Antivirus.

Se non è stato possibile trovare la soluzione a un problema o la risposta a una domanda nella Guida online di ESET NOD32 Antivirus, consultare la [Knowledge Base di ESET](#) online che viene aggiornata periodicamente. Di seguito vengono forniti i collegamenti ai principali articoli della Knowledge Base:

- [Come faccio a rinnovare la licenza?](#)
- [Durante l'installazione del prodotto ESET visualizzo un messaggio di errore. Cosa significa?](#)
- [Attiva il prodotto ESET Windows Home utilizzando la chiave di licenza](#)
- [Disinstalla o reinstalla il mio prodotto ESET Home](#)
- [Ho ricevuto il messaggio che l'installazione di ESET è terminata prematuramente](#)
- [Cosa devo fare dopo aver rinnovato la licenza? \(Utenti privati\)](#)
- [Cosa succede se modifico il mio indirizzo di posta elettronica?](#)
- [Trasferisci il prodotto ESET in un nuovo computer o dispositivo](#)
- [Come faccio ad avviare Windows in Modalità provvisoria o in Modalità provvisoria senza rete?](#)
- [Escludi un sito web sicuro dal blocco](#)
- [Consenti accesso per software di lettura dello schermo all'interfaccia grafica utente di ESET](#)

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 .

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** nella [finestra principale del programma](#), quindi su **Ricerca aggiornamenti**.

Le impostazioni predefinite dell'installazione consentono di creare un'attività di aggiornamento automatico che viene eseguita ogni ora. Se occorre modificare l'intervallo, accedere a **Strumenti** > [Pianificazione attività](#).

Come rimuovere un virus dal PC

Se il computer mostra sintomi di infezione da 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 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 selezionata del disco, fare clic su **Controllo personalizzato** e selezionare le destinazioni su cui effettuare un controllo antivirus.

Per ulteriori informazioni, consultare l'[articolo della Knowledge Base ESET](#) aggiornato periodicamente.

Come fare per creare una nuova attività in Pianificazione attività

Per creare una nuova attività in **Strumenti > Pianificazione attività**, fare clic su **Aggiungi** o 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.

Come pianificare un controllo del computer settimanale

Per pianificare un'attività regolare, aprire la [finestra principale del programma](#) e fare clic su **Strumenti > Pianificazione attività**. Di seguito viene riportata in breve la procedura da seguire per pianificare un'attività che controllerà tutte le unità locali ogni settimana. Per ulteriori istruzioni dettagliate, consultare questo [articolo della Knowledge Base](#).

Per pianificare un'attività di controllo:

1. Fare clic su **Aggiungi** nella schermata principale di Pianificazione attività.
2. Inserire un nome per l'attività e selezionare **Controllo computer su richiesta** dal menu a discesa **Tipo di attività**.
3. Selezionare **Settimanalmente** come 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.

Procedura di sblocco della Configurazione avanzata protetta con password

Se si desidera accedere alla Configurazione avanzata protetta, viene visualizzata la finestra per l'inserimento della password. Se si dimentica o si smarrisce la password, fare clic sull'opzione **Ripristina password** e digitare

l'indirizzo e-mail utilizzato per la registrazione della licenza. ESET invia una e-mail contenente il codice di verifica. Digitare il codice di verifica, quindi inserire e confermare la nuova password. Il codice di verifica ha una validità di sette giorni.

Ripristina la password tramite l'account ESET HOME: utilizzare questa opzione se la licenza utilizzata per l'attivazione è associata all'account ESET HOME. Digitare l'indirizzo e-mail utilizzato per effettuare l'autenticazione all'account [ESET HOME](#).

Se non si ricorda l'indirizzo e-mail o si hanno problemi a ripristinare la password, fare clic su **Contatta il Supporto tecnico**. L'utente verrà reindirizzato al sito web di ESET per contattare il reparto del Supporto tecnico.

Genera il codice per il Supporto tecnico: questa opzione consente di generare un codice per il Supporto tecnico. Copiare il codice fornito dal Supporto tecnico e fare clic su **Possiedo un codice di verifica**. Digitare il codice di verifica, quindi inserire e confermare la nuova password. Il codice di verifica ha una validità di sette giorni.

Per ulteriori informazioni, consultare [Sblocca la password delle impostazioni nei prodotti ESET Windows Home](#).

Come risolvere la disattivazione del prodotto da ESET HOME

Prodotto non attivato

Questo messaggio di errore compare quando il proprietario della licenza disattiva ESET NOD32 Antivirus dal portale ESET HOME o la licenza condivisa con l'account ESET HOME in uso non è più condivisa. Per risolvere questo problema:

- Fare clic su **Attiva** e utilizzare uno dei [Metodi di attivazione](#) per attivare ESET NOD32 Antivirus.
- Contattare il proprietario della licenza fornendo informazioni relative alla disattivazione di ESET NOD32 Antivirus da parte del proprietario della licenza o all'interruzione della condivisione della licenza. Il proprietario può risolvere il problema in [ESET HOME](#).

Prodotto disattivato, dispositivo disconnesso

Questo messaggio di errore viene visualizzato dopo [aver rimosso un dispositivo dall'account ESET HOME](#). Per risolvere questo problema:

- Fare clic su **Attiva** e utilizzare uno dei [Metodi di attivazione](#) per attivare ESET NOD32 Antivirus.
- Contattare il proprietario della licenza fornendo informazioni relative alla disattivazione di ESET NOD32 Antivirus e alla disconnessione del dispositivo da ESET HOME.
- Se si è il proprietario della licenza e non si è al corrente di queste modifiche, rivedere il feed attività dell'account [ESET HOME](#). Se è stata individuata un'attività sospetta, [modificare la password dell'account ESET HOME](#) e [contattare il Supporto tecnico di ESET](#).

Prodotto disattivato, dispositivo disconnesso

Questo messaggio di errore viene visualizzato dopo [aver rimosso un dispositivo dall'account ESET HOME](#). Per risolvere questo problema:

- Fare clic su **Attiva** e utilizzare uno dei [Metodi di attivazione](#) per attivare ESET NOD32 Antivirus.
- Contattare il proprietario della licenza fornendo informazioni relative alla disattivazione di ESET NOD32 Antivirus e alla disconnessione del dispositivo da ESET HOME.
- Se si è il proprietario della licenza e non si è al corrente di queste modifiche, rivedere il feed attività dell'account [ESET HOME](#). Se è stata individuata un'attività sospetta, [modificare la password dell'account ESET HOME](#) e [contattare il Supporto tecnico di ESET](#).

Prodotto non attivato

Questo messaggio di errore compare quando il proprietario della licenza disattiva ESET NOD32 Antivirus dal portale ESET HOME o la licenza condivisa con l'account ESET HOME in uso non è più condivisa. Per risolvere questo problema:

- Fare clic su **Attiva** e utilizzare uno dei [Metodi di attivazione](#) per attivare ESET NOD32 Antivirus.
- Contattare il proprietario della licenza fornendo informazioni relative alla disattivazione di ESET NOD32 Antivirus da parte del proprietario della licenza o all'interruzione della condivisione della licenza. Il proprietario può risolvere il problema in [ESET HOME](#).

Programma di miglioramento dell'esperienza degli utenti

Attraverso la partecipazione al Programma di miglioramento dell'esperienza degli utenti, l'utente accetta di fornire a ESET informazioni anonime relative all'utilizzo dei suoi prodotti. Per ulteriori informazioni sulle modalità di trattamento dei dati, consultare l'Informativa sulla privacy.

Consenso dell'utente

La partecipazione al programma è volontaria e richiede il consenso dell'utente. Dopo aver accettato di aderire al programma, l'utente non è tenuto a compiere ulteriori azioni in quanto la partecipazione è di tipo passivo. È possibile revocare in qualsiasi momento il consenso modificando le impostazioni del prodotto. Tale azione interrompe l'elaborazione di ulteriori dati anonimi.

È possibile revocare in qualsiasi momento il consenso modificando le impostazioni del prodotto:

- [Modificare le impostazioni relative al Programma di miglioramento dell'esperienza degli utenti nei prodotti ESET Windows Home](#)

Che tipo di informazioni raccogliamo?

Dati sull'interazione con il prodotto

Questi dati forniscono informazioni sulle modalità di utilizzo dei prodotti ESET. Consentono, ad esempio, di individuare le funzionalità utilizzate con maggiore frequenza, le impostazioni modificate dagli utenti e la durata di utilizzo del prodotto.

Dati sui dispositivi

ESET raccoglie questo tipo di informazioni allo scopo di comprendere dove e su quali dispositivi vengono utilizzati i suoi prodotti. Si tratta tipicamente di informazioni relative al modello del dispositivo, al paese, alla versione e al nome del sistema operativo.

Dati diagnostici relativi agli errori

Vengono raccolte anche informazioni su errori e arresti anomali. Ad esempio, dati relativi all'errore verificatosi e alle azioni che lo hanno determinato.

Perché vengono raccolte queste informazioni?

Queste informazioni anonime consentono a ESET di migliorare i prodotti per garantire ai suoi utenti una migliore esperienza di utilizzo. Aiutano a renderli il più possibile pertinenti, di facile utilizzo e privi di errori.

Chi controlla queste informazioni?

ESET, spol. s r.o. rappresenta l'unico responsabile del trattamento dei dati raccolti nell'ambito del Programma. Queste informazioni non vengono condivise con terze parti.

Accordo di licenza per l'utente finale

Con decorrenza a partire dal 19 ottobre 2021.

IMPORTANTE: Leggere attentamente i termini e le condizioni delineati di seguito prima di scaricare, installare, duplicare o utilizzare il prodotto. **SCARICANDO, INSTALLANDO, DUPLICANDO O UTILIZZANDO IL SOFTWARE, L'UTENTE SI IMPEGNA AD ACCETTARE I TERMINI E LE CONDIZIONI DEL PRESENTE CONTRATTO E DELL'[INFORMATIVA SULLA PRIVACY](#).**

Accordo di licenza per l'utente finale

Ai sensi del presente Accordo di licenza per l'utente finale ("Accordo"), stipulato da e tra ESET, spol. s r. o., con sede legale presso Einsteinova 24, 85101 Bratislava, Slovak Republic, iscritta nel registro delle imprese di competenza del tribunale circoscrizionale Bratislava I, Sezione Sro, numero di registro 3586/B, numero di identificazione commerciale 31333532 ("ESET" o "il Fornitore") e l'utente, persona fisica o giuridica ("l'Utente" o "l'Utente finale") autorizzano l'Utente a utilizzare il Software specificato nell'Articolo 1 del presente Contratto. Il Software specificato nell'Articolo 1 del presente Accordo può essere memorizzato su un supporto informatico, inviato tramite posta elettronica, scaricato da Internet, scaricato dai server del Fornitore od ottenuto da altre fonti secondo i termini e le condizioni specificati di seguito.

IL PRESENTE CONTRATTO HA PER OGGETTO I DIRITTI DELL'UTENTE FINALE E NON COSTITUISCE UN CONTRATTO DI

VENDITA. Il Fornitore conserva la proprietà della copia del Software e dei supporti fisici contenuti nella confezione di vendita, nonché di ogni altra copia che l'Utente finale è autorizzato a effettuare in conformità al presente Contratto.

Facendo clic su "Accetto" o "Accetto..." durante l'installazione, il download, la copia o l'utilizzo del Software, l'Utente accetta i termini e le condizioni del presente Accordo e dell'Informativa sulla privacy. Qualora non intenda accettare integralmente i termini e le condizioni del presente Accordo e/o dell'Informativa sulla privacy, l'Utente dovrà prontamente fare clic sull'opzione di annullamento, interrompere l'installazione o il download oppure eliminare o restituire il Software, i supporti di installazione, la documentazione di accompagnamento e la prova di acquisto al Fornitore o presso il punto vendita in cui l'Utente ha acquistato il Software.

L'UTENTE CONVIENE CHE IL SUO UTILIZZO DEL SOFTWARE COSTITUISCE CONFERMA DELL'AVVENUTA LETTURA, COMPrensione E ACCETTAZIONE DEL PRESENTE CONTRATTO E ACCETTA DI RISPETTARE I TERMINI E LE CONDIZIONI INDICATI.

1. Software. Ai sensi del presente Accordo, il termine "Software" indica: (i) il programma accompagnato dal presente Accordo e tutti i suoi componenti; (ii) tutti i contenuti dei dischi, CD-ROM, DVD, e-mail ed eventuali allegati o altri supporti mediante i quali viene fornito il presente Contratto, compreso il formato del codice oggetto del Software fornito su un supporto informativo, tramite posta elettronica o scaricato da Internet; (iii) qualsiasi materiale cartaceo illustrativo correlato e qualsiasi altra possibile documentazione correlata al Software, soprattutto qualsiasi descrizione del Software, relative specifiche, qualsiasi descrizione delle proprietà o del funzionamento del Software, qualsiasi descrizione dell'ambiente operativo in cui il Software viene utilizzato, istruzioni di utilizzo o installazione del Software o qualsiasi descrizione delle modalità di utilizzo del Software ("Documentazione"); (iv) copie del Software, correzioni di possibili errori nel Software, aggiunte al Software, estensioni al Software, versioni modificate del Software ed eventuali aggiornamenti dei componenti del Software, concesso in licenza all'Utente dal Fornitore ai sensi dell'Articolo 3 del presente Contratto. Il Software deve essere fornito esclusivamente sotto forma di codice oggetto eseguibile.

2. Installazione, Computer e Chiave di licenza. Il Software fornito su un supporto informatico, inviato tramite posta elettronica, scaricato da Internet o dai server del Fornitore od ottenuto da altre fonti richiede una procedura di installazione. L'Utente finale è tenuto a installare il Software su un Computer correttamente configurato, conformemente ai requisiti minimi specificati nella Documentazione fornita. Il metodo di installazione è illustrato nella Documentazione. È vietato installare programmi per computer o componenti hardware che possano influire negativamente sul Software sullo stesso Computer su cui si installa il Software medesimo. Per Computer si intende qualsiasi componente hardware, compresi, a mero titolo esemplificativo e non limitativo, personal computer, computer portatili, workstation, computer palmari, smartphone, dispositivi elettronici portatili o altri dispositivi elettronici per i quali è stato concepito il Software e sui quali sarà installato e/o utilizzato. Per Chiave di licenza si intende una sequenza univoca di simboli, lettere, numeri o segni speciali forniti all'Utente finale per consentire un utilizzo legale del Software, la sua versione specifica o l'estensione della durata della Licenza in conformità del presente Accordo.

3. Licenza. Subordinatamente alla condizione che l'Utente abbia accettato i termini del presente Contratto e rispettato tutti i termini e le condizioni qui indicati, il Fornitore deve garantire all'Utente i seguenti diritti ("la Licenza"):

a) **Installazione e utilizzo.** L'Utente deve avere il diritto non esclusivo e non trasferibile che consente l'installazione del Software sul disco rigido di un computer o su altri supporti permanenti per la memorizzazione dei dati, l'installazione e la memorizzazione del Software sulla memoria di un computer e di implementare, memorizzare e visualizzare il Software.

b) **Indicazione del numero di licenze.** Il diritto di utilizzo del Software deve essere legato al numero di Utenti finali. Quanto segue fa riferimento a un Utente finale: (i) installazione del Software su un computer, o (ii) se una

licenza è legata al numero di caselle di posta, un Utente finale corrisponderà a un utente che accetta la posta elettronica tramite un Mail User Agent ("MUA"). Se un MUA accetta la posta elettronica e successivamente la distribuisce automaticamente a diversi utenti, il numero di Utenti finali sarà determinato in base al numero effettivo di utenti a cui viene distribuita la posta elettronica. Se un server di posta svolge la funzione di Mailgate, il numero di Utenti finali dovrà essere pari al numero di utenti del server di posta per cui tale gate fornisce i servizi. Se un numero non specificato di indirizzi di posta elettronica è diretto a e accettato da un utente (ad es., inclusi gli alias) e i messaggi non sono automaticamente distribuiti dal client a un numero maggiore di utenti, è richiesta una Licenza per un computer soltanto. L'Utente non deve utilizzare la stessa Licenza contemporaneamente su più di un computer. L'Utente finale ha facoltà di inserire la Chiave di licenza del Software unicamente nella misura in cui sia autorizzato a utilizzare il Software in conformità delle limitazioni derivanti dal numero di Licenze fornite dal Fornitore. La Chiave di licenza è considerata un contenuto riservato che non dovrà essere condiviso con terzi o utilizzato da terzi salvo quanto consentito dal presente Accordo o dal Fornitore. In caso di compromissione della Chiave di licenza, è necessario darne immediata comunicazione al Fornitore.

c) **Home/Business Edition.** Il diritto di utilizzo della versione Home Edition del Software sarà limitato esclusivamente ad ambienti privati e/o non commerciali per scopi domestici e familiari. Ai fini dell'utilizzo del Software in ambienti commerciali nonché su server di posta, mail relay, gateway di posta o gateway Internet, occorre procurarsi una versione Business Edition.

d) **Termine della Licenza.** Il diritto di utilizzo del Software deve essere limitato nel tempo.

e) **Software OEM.** L'utilizzo di software classificati come "OEM" sarà limitato al Computer con il quale sono stati ottenuti. Non è possibile trasferirlo su un computer diverso.

f) **Software di valutazione o di prova.** Non è possibile vendere il software classificato come "Not-for-resale" (versione di valutazione), NFR o TRIAL e deve essere utilizzato esclusivamente ai fini della verifica e della valutazione delle funzioni del Software.

g) **Risoluzione della Licenza.** La Licenza deve scadere automaticamente al termine del periodo stabilito. In caso di mancato rispetto di qualsiasi clausola del presente Contratto, il Fornitore è autorizzato a recedere dal Contratto, senza pregiudizio per i diritti o i rimedi legali disponibili al Fornitore in tali eventualità. In caso di annullamento della Licenza, l'Utente è tenuto a cancellare, distruggere o restituire immediatamente, a proprie spese, A fronte della risoluzione della Licenza, il Fornitore avrà facoltà di annullare il diritto dell'Utente finale di utilizzare le funzioni del Software, che richiedono la connessione ai server del Fornitore o a server di terzi.

4. **Funzioni che prevedono requisiti di raccolta di dati e di connessione a Internet.** Ai fini di un corretto funzionamento, il Software richiede una connessione a Internet, deve essere collegato a intervalli regolari ai server del Fornitore o di terzi e conforme ai requisiti applicabili in materia di raccolta di dati previsti dalla Politica sulla privacy. La connessione a Internet e la raccolta di dati sono requisiti necessari per le seguenti funzioni del Software:

a) **Aggiornamenti del Software.** Il Fornitore è autorizzato a rilasciare di tanto in tanto aggiornamenti o upgrade del Software ("Aggiornamenti") ma non è tenuto a fornirli. Questa funzione è abilitata nelle impostazioni standard del Software e gli Aggiornamenti vengono pertanto installati automaticamente, eccetto se l'Utente finale ha disabilitato l'installazione automatica degli Aggiornamenti. Ai fini del rilascio degli Aggiornamenti, è richiesta una verifica dell'autenticità della Licenza, comprese le informazioni sul Computer e/o sulla piattaforma di installazione del Software ai sensi dell'Informativa sulla privacy.

Il rilascio di eventuali Aggiornamenti potrebbe essere soggetto al Criterio di fine del ciclo di vita ("Criterio EOL"), disponibile alla pagina https://go.eset.com/eol_home. In seguito al raggiungimento della data di fine del ciclo di vita definita nel Criterio EOL per il Software o le relative funzioni, non verranno rilasciati aggiornamenti.

b) **Inoltro di infiltrazioni e di informazioni al Fornitore.** Il Software prevede funzioni in grado di raccogliere

campioni di virus e di altri programmi dannosi per il computer, nonché oggetti sospetti, problematici, potenzialmente indesiderati o potenzialmente pericolosi, come file, URL, pacchetti IP e frame Ethernet ("Infiltrazioni") e di inviarli al Fornitore, incluse, a titolo esemplificativo ma non esaustivo, informazioni relative al processo di installazione, al Computer e/o alla piattaforma su cui è installato il Software e informazioni relative alle operazioni e alle funzionalità del Software ("Informazioni"). Le Informazioni e le Infiltrazioni possono contenere dati (compresi dati personali ottenuti in modo casuale o accidentale) sull'Utente finale o altri utenti del computer sul quale è installato il Software, nonché file colpiti da Infiltrazioni con i metadati associati.

Le Informazioni e le Infiltrazioni possono essere raccolte mediante le seguenti funzioni del Software:

- i. La funzione del sistema di reputazione LiveGrid, che prevede la raccolta e l'invio al Fornitore di hash unidirezionali correlati alle Infiltrazioni. Questa funzione è attivata nelle impostazioni standard del Software.
- ii. La funzione del sistema di feedback LiveGrid, che prevede la raccolta e l'invio di Infiltrazioni al Fornitore con i metadati e le Informazioni associati. Questa funzione potrebbe essere attivata dall'Utente finale durante il processo di installazione del Software.

Il Fornitore dovrà utilizzare esclusivamente le Informazioni e le Infiltrazioni ricevute ai fini dell'analisi e della ricerca di Infiltrazioni, il miglioramento del Software e la verifica dell'autenticità della Licenza, e dovrà adottare misure appropriate per garantire la sicurezza delle Infiltrazioni e delle Informazioni ricevute. L'attivazione di questa funzione del Software consente al Fornitore di raccogliere ed elaborare Infiltrazioni e Informazioni in base a quanto specificato nella Politica sulla privacy e in conformità delle norme vigenti in materia. È possibile disattivare queste funzioni in qualsiasi momento.

Per le finalità previste dal presente Accordo, è necessario raccogliere, elaborare e conservare i dati che consentono al Fornitore di identificare l'Utente in conformità della Politica sulla privacy. L'Utente ivi accetta che il Fornitore verifichi con mezzi propri se l'utilizzo del Software da parte dell'Utente sia conforme alle disposizioni previste dal presente Accordo. Per le finalità del presente Accordo, l'Utente accetta il trasferimento dei propri dati, attraverso la comunicazione del Software con i sistemi informatici del Fornitore o dei relativi partner commerciali, nell'ambito della rete di distribuzione e di supporto del Fornitore, ai fini della garanzia della funzionalità e dell'autorizzazione all'utilizzo del Software, nonché della protezione dei diritti del Fornitore.

Alla risoluzione del presente Accordo, il Fornitore o qualsiasi suo partner commerciale nell'ambito della rete di distribuzione e di supporto del Fornitore deve essere autorizzato al trasferimento, all'elaborazione e alla memorizzazione dei dati fondamentali che identificano l'Utente, a scopo di fatturazione e ai fini dell'esecuzione del presente Accordo, e alla trasmissione delle notifiche sul proprio Computer.

Ulteriori informazioni sulla tutela della privacy, sulla protezione dei dati personali e sui diritti dell'Utente in qualità di persona interessata sono disponibili nella Politica sulla privacy sul sito Web del Fornitore e accessibili direttamente dal processo di installazione. È ALTRESÌ DISPONIBILE LA SEZIONE "GUIDA" DEL SOFTWARE.

5. Esercizio dei diritti dell'Utente finale. L'Utente è tenuto a esercitare i diritti dell'Utente finale di persona o attraverso i propri dipendenti. L'Utente è autorizzato a utilizzare il Software al solo scopo di salvaguardare le proprie operazioni e di proteggere i(l) Computer per cui è stata ottenuta una Licenza.

6. Limitazioni dei diritti. È vietata la copia, la distribuzione, la separazione dei componenti o la creazione di prodotti derivati del Software. Durante l'utilizzo del Software, l'Utente è tenuto ad attenersi alle seguenti limitazioni:

a) È autorizzata una copia del Software su supporto per l'archivio permanente come copia di backup, a condizione che quest'ultima non venga installata o utilizzata su altri computer. Ogni altra copia del Software effettuata dall'Utente rappresenta una violazione del presente Contratto.

- b) L'Utente non può utilizzare, modificare, tradurre o riprodurre il Software, né trasferire i diritti all'utilizzo del Software, né copiare il Software, eccetto laddove espressamente indicato nel presente Contratto.
- c) La rivendita, la sublicenza, il noleggio, il prestito del Software o l'utilizzo del Software per la fornitura di servizi commerciali non sono consentiti.
- d) Sono vietate la decodificazione, la decomposizione o il disassemblaggio del Software o qualsivoglia tentativo di determinazione del codice sorgente del software, fatto salvo laddove tale divieto è espressamente proibito per legge.
- e) L'Utente accetta di utilizzare il Software esclusivamente secondo modalità conformi a tutte le leggi applicabili nella giurisdizione in cui avviene l'utilizzo dello stesso, incluse, a titolo esemplificativo ma non esaustivo, le limitazioni relative al copyright e ad altri diritti sulla proprietà intellettuale.
- f) L'Utente accetta di utilizzare esclusivamente il Software e le relative funzioni in base a modalità che non limitino le possibilità dell'Utente finale di accedere a questi servizi. Il Fornitore si riserva il diritto di limitare l'ambito dei servizi forniti ai singoli Utenti finali e di attivare l'utilizzo dei servizi da parte del maggior numero possibile di Utenti finali. La limitazione dell'ambito dei servizi potrà altresì significare l'interruzione completa della possibilità di utilizzo di qualsiasi funzione del Software e l'eliminazione dei Dati e delle informazioni sui server del Fornitore o sui server di terze parti correlati ad una specifica funzione del Software.
- g) L'Utente accetta di non eseguire alcuna attività basata sull'utilizzo della Chiave di licenza, in violazione dei termini del presente Accordo e di non fornire la Chiave di licenza a soggetti non autorizzati a utilizzare il Software, tra cui il trasferimento di Chiavi di licenza utilizzate o non utilizzate in qualsiasi forma, nonché la riproduzione o la distribuzione non autorizzata di Chiavi di licenza duplicate o generate o l'utilizzo del Software in conseguenza dell'uso di una Chiave di licenza ottenuta da una fonte diversa dal Fornitore.

7. Copyright. Il Software e tutti i relativi diritti, inclusi, a titolo esemplificativo ma non esaustivo, i diritti di esclusiva e i diritti di proprietà intellettuale associati, appartengono a ESET e/o ai suoi licenziatari. Sono protetti dalle disposizioni dei trattati internazionali, nonché da ogni altra legge nazionale applicabile nel paese di utilizzo del Software. La struttura, l'organizzazione e il codice del Software costituiscono preziosi segreti industriali e dati sensibili di proprietà di ESET e/o dei suoi licenziatari. È vietata la copia del Software, fatta eccezione per i casi previsti all'Articolo 6 (a). Ogni copia autorizzata ai sensi del presente Contratto deve contenere le stesse note sul copyright e sulla proprietà riportate sul Software. Se l'utente effettua la decodificazione, la decompilazione, il disassemblaggio o qualsivoglia tentativo di determinazione del codice sorgente in violazione delle disposizioni del presente Contratto, qualsiasi informazione in tal modo ottenuta sarà irrevocabilmente e automaticamente ritenuta trasferita al Fornitore e di completa proprietà del Fornitore dal momento della sua origine, nonostante i diritti del Fornitore relativi alla violazione del presente Contratto.

8. Riserva di diritti. Il Fornitore si riserva tutti i diritti correlati al Software, ad eccezione dei diritti espressamente concessi all'Utente finale del Software nel presente Contratto.

9. Versioni in più lingue, software su due supporti, duplicati. Se il Software supporta più piattaforme o lingue o se l'Utente ha ricevuto più copie del Software, questi è autorizzato a utilizzare il Software unicamente per il numero di computer e per le versioni per i quali ha ottenuto una Licenza. La vendita, il noleggio, l'affitto, la sublicenza, il prestito o il trasferimento di versioni o copie del Software non utilizzato dall'Utente non sono consentiti.

10. Entrata in vigore e risoluzione del Contratto. Il presente Contratto entra in vigore alla data dell'accettazione dei termini del presente Contratto da parte dell'Utente. Quest'ultimo potrà recedere dal Contratto in qualsiasi momento disinstallando, distruggendo e restituendo in modo permanente, a sue spese, il Software, tutte le copie di backup e tutto il materiale correlato ricevuto dal Fornitore o dai suoi Business Partner. Il diritto di utilizzo del Software e di qualsiasi altra funzione potrebbe essere soggetto alle disposizioni di cui al Criterio EOL. In seguito al

raggiungimento della data di fine del ciclo di vita definita nel Criterio EOL per il Software o una delle relative funzioni, decade il diritto di utilizzo del Software da parte dell'Utente. Indipendentemente dalla modalità di risoluzione del presente Contratto, le disposizioni previste agli Articoli 7, 8, 11, 13, 19 e 21 resteranno valide senza limiti di tempo.

11. DICHIARAZIONI DELL'UTENTE FINALE. L'UTENTE FINALE RICONOSCE CHE IL SOFTWARE VIENE FORNITO "COSÌ COM'È" SENZA GARANZIE DI ALCUN TIPO, NÉ ESPLICITE NÉ IMPLICITE, E CHE, SALVO QUANTO INDEROGABILMENTE PREVISTO DALLA LEGGE. IL FORNITORE, I SUOI LICENZIATARI O AFFILIATI COME ANCHE I TITOLARI DEL COPYRIGHT, NON RILASCIANO ALCUNA DICHIARAZIONE O GARANZIA ESPLICITA O IMPLICITA, COMPRESE, A MERO TITOLO ESEMPLIFICATIVO MA NON LIMITATIVO, GARANZIE DI COMMERCIALIZZABILITÀ O IDONEITÀ PER UNO SCOPO SPECIFICO O LA GARANZIA CHE IL SOFTWARE NON VIOLI BREVETTI, COPYRIGHT, MARCHI O ALTRI DIRITTI DI TERZE PARTI. IL FORNITORE O ALTRE PARTI NON GARANTISCONO CHE LE FUNZIONI CONTENUTE NEL SOFTWARE SODDISFERANNO I REQUISITI DELL'UTENTE, NÉ CHE L'USO DEL SOFTWARE NON SUBIRÀ INTERRUZIONI O CHE LO STESSO SIA ESENTE DA ERRORI. L'UTENTE SI ASSUME TUTTE LE RESPONSABILITÀ E I RISCHI INERENTI LA SCELTA DEL SOFTWARE AL FINE DI OTTENERE I RISULTATI DESIDERATI, NONCHÉ L'INSTALLAZIONE, L'UTILIZZO E I RISULTATI OTTENUTI DALL'UTILIZZO DEL SOFTWARE.

12. Assenza di altri obblighi. Il presente Contratto non pone in essere altri obblighi a carico del Fornitore e dei suoi licenziatari oltre a quanto qui specificamente stabilito.

13. LIMITAZIONE DI RESPONSABILITÀ. SALVO QUANTO INDEROGABILMENTE PREVISTO DALLA LEGGE, IN NESSUNA CIRCOSTANZA IL FORNITORE, I SUOI DIPENDENTI O LICENZIATARI POTRANNO ESSERE RITENUTI RESPONSABILI PER LUCRO CESSANTE, PERDITA DI RICAVI, VENDITE, DATI O PER COSTI DERIVANTI DALLA SOSTITUZIONE DI BENI O SERVIZI, DANNI ALLA PROPRIETÀ, LESIONI PERSONALI, INTERRUZIONE DELL'ATTIVITÀ COMMERCIALE, SMARRIMENTO DI INFORMAZIONI COMMERCIALI, O PER QUALSIASI DANNO SPECIALE, DIRETTO, INDIRETTO, ACCIDENTALE, ECONOMICO, ESEMPLARE, PUNITIVO O CONSEGUENZIALE, INDIPENDENTEMENTE DALLA CAUSA E DAL FATTO CHE TALE EVENTO DERIVI DA CONTRATTO, FATTO ILLECITO, NEGLIGENZA O ALTRA INTERPRETAZIONE DI RESPONSABILITÀ DERIVANTE DALL'INSTALLAZIONE, DALL'UTILIZZO OPPURE DALL'IMPOSSIBILITÀ DI UTILIZZARE IL SOFTWARE, ANCHE QUALORA IL FORNITORE O I SUOI LICENZIATARI O AFFILIATI SIANO STATI AVVISATI DELLA POSSIBILITÀ DI TALI DANNI. POICHÉ ALCUNI PAESI E GIURISDIZIONI NON AMMETTONO L'ESCLUSIONE DI RESPONSABILITÀ DI CUI SOPRA, MA POTREBBERO CONSENTIRE DI LIMITARE LA RESPONSABILITÀ, IN QUESTI CASI LA RESPONSABILITÀ DEL FORNITORE, DEI SUOI DIPENDENTI O DEI SUOI LICENZIATARI O AFFILIATI SARÀ LIMITATA AL PREZZO CORRISPONDO PER LA LICENZA.

14. Nessuna disposizione contenuta nel presente Contratto costituirà pregiudizio per i diritti legali di qualsiasi parte in veste di consumatore in caso di funzionamento contrario a quanto esposto.

15. Supporto tecnico. ESET o terze parti commissionate da ESET forniranno supporto tecnico a propria discrezione, senza garanzie né dichiarazioni. In seguito al raggiungimento della data di fine del ciclo di vita definita nel Criterio EOL per il Software o le relative funzioni, non verrà offerta alcuna forma di supporto tecnico. Verrà richiesto all'Utente finale di salvare tutti i dati, i software e i programmi prima della fornitura del supporto tecnico. ESET e/o terze parti commissionate da ESET non possono accettare la responsabilità per danni o perdite di dati, proprietà, software o hardware o perdita di profitti legati alla fornitura del supporto tecnico. ESET e/o terze parti commissionate da ESET si riservano il diritto di decidere che la risoluzione del problema va al di là della pertinenza del supporto tecnico. ESET si riserva il diritto di rifiutare, interrompere o concludere la fornitura del supporto tecnico a sua discrezione. Per le finalità legate all'offerta di un servizio di assistenza tecnica, potrebbero essere richieste informazioni sulla Licenza, le Informazioni e altri dati in conformità dell'Informativa sulla privacy.

16. Trasferimento della Licenza. È possibile trasferire il software da un computer a un altro, eccetto se in contrasto con i termini del Contratto. Se non in contrasto con i termini del Contratto, l'Utente finale sarà autorizzato a trasferire permanentemente la Licenza e tutti i diritti derivanti dal presente Contratto a un altro Utente finale solo con il consenso del Fornitore, secondo la condizione che (i) l'Utente finale originale non

conservi copie del Software; (ii) il trasferimento dei diritti deve essere diretto, ossia dall'Utente finale originale al nuovo Utente finale; (iii) il nuovo Utente finale deve assumersi tutti i diritti e gli obblighi incombenti sull'Utente finale originale secondo i termini del presente Contratto; (iv) l'Utente finale originale deve fornire al nuovo Utente finale la documentazione che consente la verifica dell'autenticità del Software, come specificato all'Articolo 17.

17. Verifica dell'autenticità del Software. L'Utente finale può dimostrare il diritto a utilizzare il Software in uno dei modi seguenti: (i) tramite un certificato di licenza emesso dal Fornitore o da terzi designati dal Fornitore; (ii) tramite un contratto di licenza scritto, qualora sia stato stipulato; (iii) tramite l'invio di un'e-mail inviata dal Fornitore contenente i dettagli della licenza (nome utente e password). Per le finalità legate alla verifica dell'autenticità del Software, potrebbero essere richieste informazioni sulla Licenza e dati di identificazione dell'Utente finale in conformità dell'Informativa sulla privacy.

18. Licenze per enti pubblici e governo degli Stati Uniti. Il Software sarà fornito agli enti pubblici, incluso il governo degli Stati Uniti, con i diritti e le limitazioni della licenza descritti nel presente Contratto.

19. Conformità alle disposizioni in materia di controllo del commercio.

a) L'utente non esporterà, riesporterà, trasferirà o cederà, in modo diretto o indiretto, il Software a terzi e non lo utilizzerà in alcun modo ovvero si asterrà dal compimento di azioni che potrebbero spingere ESET o le relative società controllanti, le relative sussidiarie e le sussidiarie di una società controllante, nonché le entità controllate dalle relative società controllanti ("Affiliate") ad agire in violazione di o a essere esposte alle eventuali conseguenze negative previste dalle Leggi in materia di controllo del commercio che comprendono

i. leggi che controllano, limitano o impongono requisiti di licenza sulle esportazioni, le riesportazioni o il trasferimento di merci, software, tecnologie o servizi, emanate o adottate da governi, Stati o autorità di regolamentazione degli Stati Uniti d'America, di Singapore, del Regno Unito, dell'Unione europea o dei relativi Stati membri ovvero di un paese che impone il rispetto degli obblighi ai sensi del presente Contratto o in cui ESET o le relative Affiliate sono costituite o operano ("Leggi in materia di controllo delle esportazioni") e

ii. leggi in materia economica, finanziaria, commerciale o di altra natura, sanzioni, restrizioni, embarghi, divieti di importazione o esportazione, divieti sul trasferimento di fondi o beni o sull'esecuzione di servizi o misure equivalenti imposte da governi, Stati o autorità di regolamentazione degli Stati Uniti d'America, di Singapore, del Regno Unito, dell'Unione europea o dei relativi Stati membri ovvero di un paese che impone il rispetto degli obblighi ai sensi del presente Contratto o in cui ESET o le relative Affiliate sono costituite o operano.

(gli atti legali di cui ai punti i e ii. sopra sono denominati "Leggi sul controllo del commercio").

b) ESET avrà facoltà di sospendere i propri obblighi ai sensi o a fronte della risoluzione dei presenti Termini con effetto immediato nei casi di seguito specificati:

i. ESET stabilisce, a sua ragionevole discrezione, che l'Utente abbia violato o abbia commesso una possibile violazione delle disposizioni di cui all'Articolo 19 a) del presente Contratto; oppure

ii. l'Utente finale e/o il Software diventino soggetti alle disposizioni di cui alle Leggi in materia di controllo del commercio e, conseguentemente, ESET stabilisca, a sua ragionevole discrezione, che l'adempimento in forma continuativa dei propri obblighi ai sensi del presente Contratto potrebbe causare la violazione o l'esposizione di ESET o delle relative Affiliate alle eventuali conseguenze negative previste dalle Leggi in materia di controllo del commercio.

c) Nessuna disposizione di cui al presente Contratto è intesa e dovrebbe essere concepita o interpretata allo scopo di indurre o richiedere a una delle parti di agire o astenersi dall'agire (o di accettare di agire o astenersi dall'agire) in base a modalità incompatibili con, penalizzate o vietate ai sensi delle Leggi in materia di controllo del commercio applicabili.

20. Avvisi. Tutti gli avvisi e i resi del Software e della Documentazione devono essere inviati a: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, fatto salvo il diritto di ESET di comunicare all'Utente eventuali modifiche al presente Accordo, alle Informative sulla privacy, al Criterio EOL e alla Documentazione ai sensi dell'art. 22 dell'Accordo. ESET potrebbe inviare all'Utente e-mail o notifiche in-app tramite il Software ovvero pubblicare le comunicazioni sul proprio sito web. L'Utente accetta di ricevere comunicazioni legali da ESET in formato elettronico, comprese eventuali comunicazioni in caso di modifica dei Termini, dei Termini speciali o delle Informative sulla privacy, eventuali proposte/accettazioni di contratti o inviti a trattare, avvisi o altre comunicazioni legali. Tali comunicazioni elettroniche saranno considerate ricevute per iscritto, fatto salvo il caso in cui le leggi applicabili non richiedano specificamente un tipo di comunicazione differente.

21. Legge applicabile. Il presente Accordo è disciplinato e interpretato in base alle leggi in vigore nella Repubblica Slovacca. L'Utente finale e il Fornitore accettano che gli eventuali conflitti con la Convenzione delle Nazioni Unite sui contratti per la compravendita internazionale di merci non sono applicabili. L'Utente accetta espressamente che qualsiasi reclamo o disputa derivante dal presente Contratto con il Fornitore o correlata all'utilizzo del Software sia di competenza del Tribunale di Bratislava I e accetta espressamente l'esercizio della giurisdizione da parte del suddetto tribunale.

22. Disposizioni generali. Qualora alcune disposizioni del presente Contratto fossero giudicate non valide o non applicabili, ciò non avrà alcun effetto sulla parte restante del Contratto, che resterà valido e applicabile nei termini e nelle condizioni qui indicati. Il presente Accordo è stato sottoscritto in lingua inglese. In caso di traduzione dell'Accordo per motivi di praticità di fruizione o altri scopi ovvero in caso di discrepanza tra le versioni nelle varie lingue del presente Accordo, prevarrà la versione in lingua inglese.

ESET si riserva il diritto di apportare modifiche al Software nonché di rivedere i termini del presente Accordo, gli Allegati, gli Addendum, l'Informativa sulla privacy, il Criterio EOL e la Documentazione o parti degli stessi in qualsiasi momento, attraverso l'aggiornamento dei relativi documenti (i) allo scopo di integrare le modifiche apportate al Software o alle modalità di conduzione delle attività aziendali da parte di ESET, (ii) per motivi legali, normativi o di sicurezza o (iii) per prevenire situazioni di abuso o danno. Eventuali revisioni dell'Accordo verranno segnalate all'Utente tramite e-mail, notifiche in-app o con altri mezzi elettronici. Qualora l'Utente non esprima il suo consenso alle modifiche all'Accordo proposte, avrà facoltà di recedere in base a quanto previsto dall'Art. 10 entro 30 giorni dalla ricezione di un avviso relativo a dette modifiche. Fatto salvo il caso in cui l'Utente receda dall'Accordo entro questo limite di tempo, le modifiche proposte saranno considerate accettate e diventeranno effettive a far data dalla ricezione di un avviso relativo a dette modifiche.

Il presente Contratto costituisce il Contratto completo tra il Fornitore e l'Utente in relazione al Software e sostituisce qualsiasi precedente dichiarazione, intesa, impegno, comunicazione o avviso relativo al Software.

ADDENDUM ALL'ACCORDO

Valutazione della sicurezza dei dispositivi connessi alla rete. Alla sezione Valutazione della sicurezza dei dispositivi connessi alla rete si applicano le seguenti disposizioni supplementari:

Il Software contiene una funzione per controllare la sicurezza della rete locale dell'Utente finale e la sicurezza dei dispositivi nella rete locale che richiede il nome della rete locale e informazioni sui dispositivi in tale rete quali la presenza, il tipo, il nome, l'indirizzo IP e l'indirizzo MAC del dispositivo nella rete locale correlate alle informazioni sulla licenza. Le informazioni comprendono anche il tipo di sicurezza e di crittografia wireless per i dispositivi router. Tale funzione potrebbe inoltre fornire informazioni in merito alla disponibilità di una soluzione software di sicurezza per proteggere i dispositivi nella rete locale.

Protezione da uso illegittimo dei dati Alla sezione Protezione da uso illegittimo dei dati si applicano le seguenti disposizioni supplementari:

Il Software prevede una funzione in grado di impedire la perdita o l'utilizzo non legittimo di dati critici

direttamente correlati al furto di un Computer. Questa funzione viene disattivata in base alle impostazioni predefinite del Software. Per poterlo attivare, l'Account ESET HOME deve essere creato e tramite esso la funzione attiva la raccolta di dati in caso di furto del computer. In caso di attivazione di questa funzione del Software, verranno raccolti e inviati al Fornitore i dati relativi al Computer rubato. Tali dati possono includere informazioni relative alla localizzazione della rete del Computer, al contenuto visualizzato sulla schermata del Computer, alla configurazione del Computer e/o ai dati registrati da una fotocamera collegata al Computer (qui di seguito denominati "Dati"). L'Utente finale avrà facoltà di utilizzare i Dati ottenuti attraverso tale funzione e forniti tramite l'Account ESET HOME esclusivamente per la risoluzione di una situazione avversa causata dal furto di un Computer. Per le sole finalità previste da tale funzione, il Fornitore elaborerà i Dati specificati nell'Informativa sulla privacy e in conformità della normativa vigente in materia. Il Fornitore dovrà consentire all'Utente finale di accedere ai Dati per il periodo necessario al raggiungimento dell'obiettivo per cui sono stati ottenuti che non dovrà superare il periodo di conservazione specificato nell'Informativa sulla privacy. La protezione contro l'utilizzo non legittimo dei dati dovrà essere utilizzata esclusivamente con i Computer e gli account ai quali l'Utente finale è autorizzato ad accedere. Eventuali utilizzi non legittimi verranno segnalati all'autorità competente. Il Fornitore agirà in conformità delle leggi vigenti e offrirà assistenza alle autorità incaricate dell'applicazione della legge in caso di utilizzi non legittimi. L'Utente accetta e riconosce di essere responsabile della salvaguardia della password per l'accesso all'account ESET HOME e di non divulgare la propria password a terzi. L'Utente finale è responsabile di qualsiasi attività che utilizzi la funzione di protezione contro l'utilizzo non legittimo di dati e l'account ESET HOME, indipendentemente dal fatto che sia stato o meno autorizzato. Qualora l'account ESET HOME sia compromesso, è necessario darne immediata comunicazione al Fornitore. Le disposizioni supplementari relative alla sezione Protezione da uso illegittimo dei dati si applicano esclusivamente nel caso degli Utenti finali di ESET Internet Security e ESET Smart Security Premium.

ESET Secure Data. All'applicazione ESET Secure Data si applicano le seguenti disposizioni supplementari:

1. Definizioni. Nelle disposizioni supplementari relative a ESET Secure Data, ai termini e alle espressioni specificati di seguito si applicano i seguenti significati:

- a) "Informazione" qualsiasi informazione o dato crittografato o decrittografato utilizzando il software;
- b) "Prodotti" Il software ESET Secure Data e la relativa documentazione;
- c) "ESET Secure Data" uno o più software utilizzati per la crittografia e decrittografia di dati in formato elettronico;

Tutti i riferimenti al plurale comprenderanno anche l'equivalente singolare e tutti i riferimenti maschili comprenderanno anche gli equivalenti femminili e neutri e viceversa. I termini e le espressioni non accompagnati da una specifica definizione dovranno essere utilizzati in base alle definizioni specificate nel presente Accordo.

2. Dichiarazione aggiuntiva dell'Utente finale. L'Utente riconosce e accetta quanto segue:

- a) È sua responsabilità proteggere, mantenere e eseguire copie di backup delle Informazioni;
- b) L'Utente finale deve eseguire copie di backup complete di tutte le informazioni e dei dati (comprese, senza limiti, eventuali informazioni critiche e dati sensibili) sul proprio computer prima dell'installazione di ESET Secure Data;
- c) L'Utente finale è tenuto a mantenere un registro sicuro di tutte le password o di altre informazioni utilizzate per configurare e utilizzare ESET Secure Data e a eseguire copie di backup di tutte le chiavi di crittografia, i codici di licenza, i file chiave e altri dati generati su supporti di memorizzazione separati;
- d) L'Utente finale è responsabile dell'utilizzo dei Prodotti. Il Fornitore è sollevato da qualsiasi responsabilità per eventuali perdite, reclami o danni subiti in conseguenza di operazioni non autorizzate o errate di crittografia o decrittografia delle Informazioni o di altri dati ovunque e in qualsiasi modo memorizzati;

e) Sebbene il Fornitore abbia adottato tutte le misure ragionevolmente necessarie per garantire l'integrità e la sicurezza di ESET Secure Data, i Prodotti (o parti di essi) non devono essere utilizzati in luoghi dipendenti da un livello di sicurezza fail-safe o potenzialmente pericolosi, compresi, a mero titolo esemplificativo e non limitativo, impianti nucleari, postazioni aeree, sistemi di controllo o comunicazione, sistemi di armi o di difesa e sistemi di sopravvivenza o monitoraggio vitale;

f) È responsabilità dell'Utente finale garantire che il livello di sicurezza e di crittografia forniti dai prodotti sia adeguato alle proprie esigenze;

g) Di essere responsabile del proprio utilizzo dei Prodotti, compresa, a mero titolo esemplificativo e non limitativo, la garanzia che detto utilizzo sia conforme a tutte le leggi e i regolamenti applicabili della Repubblica slovacca o di altri paesi, regioni o stati in cui vengono utilizzati i Prodotti. L'Utente è tenuto ad assicurare preventivamente che l'utilizzo dei Prodotti non violi in alcun modo le disposizioni dei governi (nella Repubblica slovacca o altrove) in materia di embargo;

h) ESET Secure Data potrebbe contattare di tanto in tanto i server del Fornitore per verificare le informazioni di licenza, le patch disponibili, i service pack e altri aggiornamenti che possono migliorare, mantenere, modificare o aggiornare il funzionamento di ESET Secure Data e potrebbe inviare informazioni di sistema di carattere generale relative al suo funzionamento in conformità della Politica sulla privacy.

i) Il Provider è sollevato da qualsiasi responsabilità per eventuali perdite, danni, spese o richieste di danni derivanti da perdita, furto, uso errato, danneggiamento o distruzione di password, informazioni di configurazione, chiavi di crittografia, codici di attivazione della licenza e altri dati generati o memorizzati durante l'utilizzo del software.

Le disposizioni supplementari relative a ESET Secure Data si applicano esclusivamente nel caso degli Utenti finali di ESET Smart Security Premium.

Password Manager Software. Le disposizioni supplementari che si applicano a Password Manager Software sono specificate di seguito:

1. Dichiarazione aggiuntiva dell'Utente finale. L'Utente riconosce e accetta di non compiere le azioni indicate di seguito:

a) utilizzare il software Password Manager per gestire applicazioni mission-critical che potrebbero mettere in gioco la proprietà privata o la vita umana. L'Utente finale riconosce che il software Password Manager non è progettato per tali utilizzi e che la mancata osservazione di questo principio potrebbe portare a morte, lesioni personali, o gravi danni ambientali o alla proprietà privata, per i quali il Provider è sollevato da qualunque responsabilità.

IL SOFTWARE PASSWORD MANAGER NON È PROGETTATO, DESTINATO O CONCESSO IN LICENZA PER L'UTILIZZO IN AMBIENTI PERICOLOSI CHE RICHIEDONO CONTROLLI FAIL-SAFE COMPRESI, SENZA LIMITAZIONI, LA PROGETTAZIONE, LA COSTRUZIONE, LA MANUTENZIONE O LA GESTIONE DI IMPIANTI NUCLEARI, SISTEMI DI COMUNICAZIONE O DI NAVIGAZIONE AEREA, SISTEMI DI CONTROLLO DEL TRAFFICO E SISTEMI D'ARMI O PER IL SOSTEGNO DELLE FUNZIONI VITALI. IL PROVIDER DECLINA ESPLICITAMENTE QUALSIASI GARANZIA ESPRESSA O IMPLICITA DI ADEGUATEZZA PER TALISCOPI.

b) utilizzare il software Password Manager in modalità che violino il presente accordo o le leggi della Repubblica Slovacca o della giurisdizione di appartenenza. Nello specifico, l'Utente non è autorizzato a utilizzare Password Manager Software per condurre o promuovere attività illecite, compreso il caricamento di dati con contenuti pericolosi o contenuti che possano essere utilizzati per attività illecite o che violino le leggi o i diritti di terze parti (compresi i diritti di proprietà intellettuale), compresi, a mero titolo informativo e non esaustivo, eventuali tentativi di accedere agli account in Storage (ai fini dei presenti termini supplementari relativi a Password

Manager Software, "Storage" indica lo spazio di memorizzazione dati gestito dal Fornitore o da terzi diversi dal Fornitore e dall'Utente allo scopo di consentire la sincronizzazione e il backup dei dati dell'Utente) o a eventuali account e dati di altri utenti di Password Manager Software o di Storage. In caso di violazione di tali clausole, il Fornitore sarà autorizzato a recedere immediatamente dall'Accordo trasferendo all'Utente finale i costi di eventuali rimedi, nonché a intraprendere le azioni necessarie per impedire ulteriori usi del software Password Manager, senza alcuna possibilità di rimborso.

2. LIMITAZIONE DI RESPONSABILITÀ. IL SOFTWARE PASSWORD MANAGER VIENE FORNITO "NELLO STATO ATTUALE". NON È PREVISTA ALCUNA GARANZIA DI ALCUN TIPO, ESPRESSA O IMPLICITA. L'UTENTE UTILIZZA IL SOFTWARE A PROPRIO RISCHIO. IL PRODUTTORE È SOLLEVATO DA OGNI RESPONSABILITÀ RELATIVA A PERDITA DI DATI, DANNI, LIMITAZIONI ALLA DISPONIBILITÀ DEL SERVIZIO, COMPRESI EVENTUALI DATI INVIATI DAL SOFTWARE PASSWORD MANAGER SOFTWARE A SPAZI DI MEMORIZZAZIONE ESTERNI ALLO SCOPO DI SINCRONIZZARE I DATI ED ESEGUIRNE IL BACKUP. LA CRITTOGRAFIA DEI DATI UTILIZZANDO IL SOFTWARE PASSWORD MANAGER NON IMPLICA ALCUNA RESPONSABILITÀ DA PARTE DEL PROVIDER RELATIVAMENTE ALLA SICUREZZA DEI DATI. L'UTENTE FINALE ACCETTA ESPRESSAMENTE CHE I DATI ACQUISITI, UTILIZZATI, CRITTOGRAFATI, MEMORIZZATI, SINCRONIZZATI O INVIATI UTILIZZANDO IL SOFTWARE PASSWORD MANAGER POSSONO ANCHE ESSERE MEMORIZZATI SU SERVER DI TERZI (VALE SOLO PER L'UTILIZZO DEL SOFTWARE PASSWORD MANAGER PER CUI I SERVIZI DI SINCRONIZZAZIONE E BACKUP SIANO STATI ATTIVATI). SE IL PROVIDER, A PROPRIA ESCLUSIVA DISCREZIONE, DECIDE DI UTILIZZARE UN SERVIZIO DI MEMORIZZAZIONE, SITO O PORTALE WEB, SERVER O SERVIZIO, IL PROVIDER NON POTRÀ ESSERE CONSIDERATO RESPONSABILE PER LA QUALITÀ, SICUREZZA E DISPONIBILITÀ DI TALE SERVIZIO DI TERZI; INOLTRE, IN NESSUN CASO, IL PROVIDER POTRÀ ESSERE CONSIDERATO RESPONSABILE NEI CONFRONTI DELL'UTENTE FINALE PER EVENTUALI VIOLAZIONI DI NORME CONTRATTUALI O OBBLIGHI LEGALI DA PARTE DI TERZI, NEPPURE PER DANNI, PROFITTI MANCATI, DANNI FINANZIARI O NON FINANZIARI, O ALTRI TIPI DI PERDITE UTILIZZANDO QUESTO SOFTWARE. IL PROVIDER NON È RESPONSABILE PER I CONTENUTI DEI DATI ACQUISITI, UTILIZZATI, CRITTOGRAFATI, MEMORIZZATI, SINCRONIZZATI O INVIATI UTILIZZANDO IL SOFTWARE PASSWORD MANAGER NELLO STORAGE. L'UTENTE RICONOSCE CHE IL PROVIDER NON HA ACCESSO AI CONTENUTI DEI DATI MEMORIZZATI E NON È IN GRADO DI MONITORARE O RIMUOVERE LEGALMENTE I CONTENUTI PERICOLOSI.

Il Provider è proprietario di tutti i diritti relativi a miglioramenti, aggiornamenti e fix relativi al software Password Manager („Miglioramenti“) anche nel caso in cui tali miglioramenti siano stati sviluppati in base a feedback, idee o suggerimenti inviati dall'Utente in qualsiasi forma. L'Utente non avrà diritto ad alcuna compensazione, comprese eventuali royalty collegate a tali Miglioramenti.

GLI ENTI E I LICENZIATARI DEL PROVIDER NON AVRANNO ALCUNA RESPONSABILITÀ PER DANNI O CITAZIONI DI ALCUN TIPO DERIVANTI O IN QUALCHE MODO COLLEGATI ALL'UTILIZZO DEL SOFTWARE PASSWORD MANAGER DA PARTE DELL'UTENTE O DA PARTE DI TERZI, ALL'USO O NON USO DI EVENTUALI AZIENDE D'INTERMEDIAZIONE O RIVENDITORI, O ALLA VENDITA O ACQUISTO DI EVENTUALI TITOLI, ANCHE SE BASATI SU TEORIE LEGALI O ECONOMICHE.

GLI ENTI E I LICENZIATARI DEL PROVIDER NON SONO RESPONSABILI NEI CONFRONTI DELL'UTENTE FINALE PER DANNI DIRETTI, INCIDENTALI, SPECIALI, INDIRETTI O CONSEGUENZIALI DERIVANTI O COLLEGATI A SOFTWARE DI TERZI, AD EVENTUALI DATI CUI SI È AVUTO ACCESSO TRAMITE IL SOFTWARE PASSWORD MANAGER, ALL'UTILIZZO O IMPOSSIBILITÀ DI UTILIZZO O ACCESSO A PASSWORD MANAGER DA PARTE DELL'UTENTE FINALE, O EVENTUALI DATI FORNITI TRAMITE IL SOFTWARE PASSWORD MANAGER, SIA NEL CASO CHE TALI DANNI SIANO RAPPRESENTATI NELL'AMBITO DI UNA TEORIA LEGALE O ECONOMICA. I DANNI ESCLUSI DA QUESTA CLAUSOLA COMPRENDONO, SENZA LIMITAZIONI, QUELLI RELATIVI A PERDITA DI PROFITTI AZIENDALI, LESIONI A PERSONE O PROPRIETÀ, INTERRUZIONI DELL'ATTIVITÀ AZIENDALE, PERDITA DI AFFARI O DI DATI PERSONALI. ALCUNE GIURISDIZIONI NON CONSENTONO LIMITAZIONI DI DANNI INCIDENTALI O CONSEGUENZIALI, PERTANTO QUESTA RESTRIZIONE POTREBBE NON VALERE IN CASI SPECIFICI. IN TAL CASO ILLIMITATE DELLA RESPONSABILITÀ DEL PROVIDER SARÀ IL MINIMO CONSENTITO DALLA LEGGE VIGENTE.

LE INFORMAZIONI FORNITE TRAMITE IL SOFTWARE PASSWORD MANAGER, COMPRESI QUOTAZIONI AZIONARIE, ANALISI, DATI DI MERCATO, NOTIZIE E DATI FINANZIARI POTREBBERO ESSERE RITARDATI, IMPRECISI O CONTENERE ERRORI O OMISSIONI, E GLI ENTI E I LICENZIATARI DEL PROVIDER NON AVRANNO ALCUNA RESPONSABILITÀ IN TAL SENSO. IL PROVIDER POTRÀ MODIFICARE O INTERROMPERE QUALSIASI SEZIONE O FUNZIONE DEL SOFTWARE PASSWORD MANAGER OPPURE L'UTILIZZO DI TUTTE O DI ALCUNE FUNZIONALITÀ O TECNOLOGIE IMPIEGATE NEL SOFTWARE PASSWORD MANAGER, IN QUALSIASI MOMENTO SENZA PREAVVISO.

QUALORA LE CLAUSOLE PRESENTI IN QUESTO ARTICOLO SIANO NULLE PER QUALSIASI RAGIONE OPPURE IL PROVIDER VENGA RITENUTO RESPONSABILE PER PERDITE, DANNI ECC. NELL'AMBITO DELLE LEGGI VIGENTI, LE PARTI CONCORDANO CHE LA RESPONSABILITÀ DEL PROVIDER NEI CONFRONTI DELL'UTENTE FINALE SIA LIMITATA AL SOLO IMPORTO DELLA LICENZA PAGATA.

L'UTENTE ACCETTA DI INDENNIZZARE, TUTELARE E SOLLEVARE DA RESPONSABILITÀ IL PROVIDER E I SUOI DIPENDENTI, LE SUE FILIALI, I SUOI AFFILIATI, DISTRIBUTORI E ALTRI PARTNER DA E CONTRO TUTTE LE EVENTUALI RICHIESTE DA PARTE DI TERZI (COMPRESI I PROPRIETARI DEL DISPOSITIVO O LE PARTI I CUI DIRITTI SIANO STATI INFLUENZATI DAI DATI UTILIZZATI NEL SOFTWARE PASSWORD MANAGER SOFTWARE O IN STORAGE) COMPRESI RICHIESTE DI DANNI, RESPONSABILITÀ, DANNI, PERDITE, COSTI, SPESE, ADDEBITI CHE TALI TERZE PARTI POTREBBERO AVER DOVUTO SOSTENERE A SEGUITO DELL'UTILIZZO DEL SOFTWARE PASSWORD MANAGER DA PARTE DELL'UTENTE FINALE.

3. Dati nel software Password Manager. Salvo diversamente ed esplicitamente deciso da parte dell'Utente finale, tutti i dati inseriti dall'Utente finale verranno salvati in un database del software Password Manager Software memorizzato in formato crittografato sul computer dell'Utente, o in altri dispositivi di memorizzazione da questi definiti. L'Utente finale comprende che, in caso di cancellazione o altri danni, al database o ad altri file del software Password Manager, tutti i dati ivi contenuti verranno irreversibilmente persi; inoltre l'Utente finale comprende ed accetta il rischio di tale perdita. Il fatto che i dati personali dell'Utente siano memorizzati in formato crittografato sul computer non significa che le informazioni non possano essere rubate o utilizzate in modo improprio da chiunque scopra la Password Master o riesca ad accedere al dispositivo di attivazione definito dal cliente per l'apertura del database. L'Utente finale è responsabile per il mantenimento della sicurezza di tutti i metodi di accesso.

4. Trasmissione di dati personali al Provider o allo Storage. Se l'Utente finale decide in tal senso ed esclusivamente allo scopo di garantire backup e sincronizzazioni dati tempestive, il software Password Manager trasmette o invia dati personali dal database di Password Manager - in particolare le password, i dati di accesso, Account e Identità - tramite internet allo Storage. I dati vengono trasmessi esclusivamente in formato crittografato. L'utilizzo del software Password Manager per compilare automaticamente i moduli on line con password, dati di accesso o altri dati potrebbe richiedere l'invio di tali informazioni attraverso internet al sito web identificato dall'Utente. Questa trasmissione di dati non viene avviata dal software Password Manager e pertanto il Provider non ha alcuna responsabilità per la sicurezza di tali interazioni con siti web supportati da diversi provider. Eventuali transazioni attraverso internet, in relazione o meno al software Password Manager, vengono eseguite a discrezione e rischio dell'Utente, che rimarrà l'unico responsabile per eventuali danni al computer o perdite di dati risultanti dal download e/o utilizzo di tale materiale o servizio. Per ridurre al minimo il rischio di perdere dati preziosi, il Provider consiglia ai clienti di eseguire periodicamente delle copie di backup del database e di altri file sensibili su supporti esterni. Il Provider non è in grado di fornire assistenza nel recupero di dati persi o danneggiati. Se il Provider fornisce dei servizi di backup per i file del database dell'Utente, in caso di danni o cancellazioni dei file sui PC dell'Utente, tale servizio di backup sarà comunque privo di garanzia e non implicherà alcuna responsabilità di alcun genere da parte del Provider.

Utilizzando il software Password Manager, l'Utente accetta che il software possa contattare di tanto in tanto i server del Fornitore per verificare le informazioni di licenza, le patch disponibili, i service pack e altri aggiornamenti che possono migliorare, mantenere, modificare o aggiornare il funzionamento del software Password Manager. Il software potrebbe inviare informazioni di sistema di carattere generale correlate al

funzionamento del software Password Manager in conformità della Politica sulla privacy.

5. Disinstallare informazioni e istruzioni. Eventuali informazioni che si desidera conservare dal database dovranno essere esportate prima di disinstallare il software Password Manager.

Le disposizioni supplementari relative a Password Manager Software si applicano esclusivamente nel caso degli Utenti finali di ESET Smart Security Premium.

ESET LiveGuard. All'applicazione ESET LiveGuard si applicano le seguenti disposizioni supplementari:

Il Software contiene una funzione di analisi aggiuntiva dei file inviati dall'Utente finale. Il Fornitore dovrà utilizzare esclusivamente i file inviati dall'Utente finale e i risultati dell'analisi nel rispetto dell'Informativa sulla privacy e in conformità delle norme vigenti in materia.

Le disposizioni supplementari relative a ESET LiveGuard si applicano esclusivamente nel caso degli Utenti finali di ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Informativa sulla privacy

La protezione dei dati personali rappresenta un aspetto particolarmente importante per ESET, spol. s r. o., con sede legale presso Einsteinova 24, 851 01 Bratislava, Slovak Republic, registrata presso il registro delle imprese di competenza del tribunale circoscrizionale Bratislava I, Sezione Sro, numero di registro 3586/B, numero di identificazione commerciale 31333532 in qualità di titolare del trattamento dei dati ("ESET" o "la Società"). ESET desidera attenersi ai requisiti in materia di trasparenza legalmente standardizzati ai sensi del Regolamento generale sulla protezione dei dati dell'UE ("GDPR"). Per raggiungere tale obiettivo, la Società pubblica la presente Informativa sulla privacy al solo scopo di informare il cliente ("Utente finale" o "Utente") in qualità di soggetto interessato relativamente agli argomenti in materia di protezione dei dati personali:

- Base legale dell'elaborazione dei dati personali,
- Condivisione e riservatezza dei dati,
- Protezione dei dati,
- Diritti dell'Utente finale in qualità di soggetto interessato,
- Elaborazione dei dati personali dell'Utente
- Informazioni di contatto.

Base legale dell'elaborazione dei dati personali

Il trattamento dei dati in base alla normativa applicabile in materia di protezione dati personali da parte di ESET si fonda su poche basi legali. L'elaborazione dei dati personali in ESET è necessaria principalmente ai fini dell'esecuzione dei termini dell' [Accordo di licenza per l'utente finale](#) ("EULA") con l'Utente finale (Art. 6 (1) (b) GDPR), applicabile nell'ambito della fornitura di prodotti o servizi ESET, salvo diversamente specificato in modo esplicito, p. es.:

- Base legale dell'interesse legittimo (Art. 6 (1) (f) GDPR), che consente alla Società di eseguire il trattamento dei dati in base alle modalità di utilizzo dei Servizi aziendali da parte dei clienti e sulla relativa soddisfazione allo

scopo di offrire agli Utenti protezione, supporto ed esperienza ottimali. Anche il marketing è riconosciuto dalla legislazione applicabile come interesse legittimo. Pertanto, ESET utilizza questo strumento nelle comunicazioni di marketing con i propri clienti.

- Consenso (Art. 6 (1) (a) GDPR), che viene richiesto all'Utente in situazioni specifiche qualora ritenga che tale base legale sia la più idonea o se richiesto per legge.
- Conformità agli obblighi legali (Art. 6 (1) (c) GDPR), ad esempio definizione di requisiti per le comunicazioni elettroniche, conservazione per scopi di fatturazione o documenti di fatturazione.

Condivisione e riservatezza dei dati

La Società non condivide i dati dell'Utente con terze parti. Tuttavia, ESET è un'azienda che opera in tutto il mondo tramite società affiliate o partner che fanno parte della rete di distribuzione, assistenza e supporto. Le informazioni relative alla gestione delle licenze, alla fatturazione e al supporto tecnico elaborate da ESET potrebbero essere trasferite da e verso le società affiliate o i partner ai fini dell'esecuzione dei termini dell'Accordo di licenza per l'utente finale, tra cui l'erogazione dei servizi o l'assistenza.

ESET preferisce elaborare i propri dati all'interno dell'Unione europea (UE). Tuttavia, in base alla posizione dell'Utente (utilizzo dei prodotti e/o servizi della Società al di fuori dell'UE) e/o del servizio scelto dall'Utente, potrebbe essere necessario trasferire i dati dell'Utente in un paese al di fuori dell'UE. Ad esempio, in relazione al cloud computing, la Società utilizza servizi di terze parti. In questi casi, la Società seleziona attentamente i fornitori di servizi e garantisce un livello adeguato di protezione dei dati attraverso misure contrattuali, tecniche e organizzative. Di norma, se necessario, la Società conviene sulle clausole contrattuali tipo dell'UE con le normative contrattuali supplementari.

Per alcuni paesi al di fuori dell'UE, tra cui il Regno Unito e la Svizzera, l'UE ha già stabilito un livello comparabile di protezione dei dati. Grazie al sistema del livello comparabile di protezione dei dati, il trasferimento dei dati verso questi paesi non richiede particolari autorizzazioni o accordi.

Protezione dei dati

ESET implementa appropriate misure tecniche e organizzative per garantire un livello di sicurezza appropriato da potenziali rischi. ESET si impegna per garantire la costante riservatezza, integrità, disponibilità e resilienza dei sistemi di elaborazione e dei servizi. Tuttavia, in caso di violazione dei dati che comporti un rischio per i diritti e le libertà dell'Utente, ESET è pronta a informare l'ente di supervisione competente, oltre che gli Utenti finali in qualità di soggetti interessati.

Diritti dei soggetti titolari dei dati

Data la centralità dei diritti di ogni Utente finale, la Società desidera informare l'Utente che tutti gli Utenti finali (provenienti da qualsiasi paese UE o extra-UE) hanno i seguenti diritti garantiti in ESET. Per esercitare i diritti del soggetto interessato, l'Utente può contattare la Società tramite il modulo di supporto o tramite e-mail all'indirizzo dpo@eset.sk. Ai fini dell'identificazione, l'Utente dovrà fornire le seguenti informazioni: Nome, indirizzo e-mail e, se disponibile, chiave di licenza o numero cliente e affiliazione aziendale. Non inviare altri dati personali, tra cui la data di nascita. Tenere presente che, per poter elaborare la richiesta dell'Utente, oltre che per scopi di identificazione, la Società provvederà al trattamento dei dati personali dello stesso.

Diritto di revoca del consenso. Il diritto di revoca del consenso è valido in caso di un'elaborazione basata solo sul consenso. Nel caso in cui la Società elabori i dati personali dell'Utente in base al consenso, quest'ultimo ha facoltà di recedere dal consenso in qualsiasi momento senza fornire la motivazione. La revoca del consenso dell'Utente

ha effetto futuro e non incide sulla legalità dei dati elaborati in precedenza.

Diritto di opposizione. Il diritto di opporsi all'elaborazione è valido in caso di trattamento basato sul legittimo interesse di ESET o di terze parti. Nel caso in cui la Società elabori i dati personali dell'Utente al fine di tutelare un interesse legittimo, in quanto soggetto interessato, l'Utente ha il diritto di opporsi in qualsiasi momento all'interesse legittimo invocato dalla Società e all'elaborazione dei propri dati personali. Il diritto di opposizione dell'Utente ha effetto futuro e non incide sulla legalità dei dati elaborati prima dell'opposizione. Nel caso in cui la Società elabori i dati personali dell'Utente per finalità di marketing diretto, non è necessario fornire le motivazioni dell'opposizione. Ciò vale anche per la profilazione, nella misura in cui è collegata a tali attività di marketing diretto. In tutti gli altri casi, la Società richiede all'Utente di informarla brevemente in relazione ai propri reclami contro l'interesse legittimo di ESET a elaborare i suoi dati personali.

Tenere presente che, in alcuni casi, nonostante la revoca del consenso da parte dell'Utente, la Società ha facoltà di elaborare ulteriormente i suoi dati personali sulla base di altri requisiti legali, ad esempio ai fini dell'esecuzione di un contratto.

Diritto di accesso. In quanto soggetto interessato, l'Utente ha diritto a ottenere in qualsiasi momento e gratuitamente da ESET informazioni sui propri dati memorizzati.

Diritto di rettifica. In caso di trattamento non intenzionale di dati personali non corretti sull'Utente, quest'ultimo ha il diritto di correggere il problema.

Diritto di cancellazione e diritto di limitazione dell'elaborazione. In qualità di soggetto interessato, l'Utente ha il diritto di richiedere la cancellazione o la limitazione dell'elaborazione dei propri dati personali. Se la Società elabora i dati personali dell'Utente (ad esempio, con il suo consenso) quest'ultimo ha il diritto di recedere e, se non sussistono altre basi legali (ad esempio, un contratto), i dati personali vengono rimossi immediatamente. I dati personali dell'Utente verranno rimossi anche nel momento in cui non saranno più richiesti per gli scopi indicati al termine del periodo di conservazione.

Se la Società utilizza i dati personali dell'Utente al solo scopo di eseguire attività di marketing diretto e l'Utente ha revocato il proprio consenso o si è opposto all'interesse legittimo sottostante di ESET, la Società limiterà l'elaborazione dei suoi dati personali nella misura in cui i dati di contatto dell'Utente sono inclusi nella blacklist interna al fine di evitare contatti indesiderati. In caso contrario, i dati personali dell'Utente verranno rimossi.

Tenere presente che la Società potrebbe richiedere la memorizzazione dei dati dell'Utente fino alla scadenza degli obblighi di conservazione e dei periodi stabiliti dal legislatore o dalle autorità di supervisione. Gli obblighi e i periodi di conservazione potrebbero anche essere stabiliti dalla legislazione della Repubblica Slovacca. Successivamente, i dati corrispondenti verranno sistematicamente rimossi.

Diritto di portabilità dei dati. ESET è lieta di fornire all'Utente, in quanto soggetto interessato, i dati personali elaborati in formato xls.

Diritto di presentazione di un reclamo. In qualità di soggetto interessato, l'Utente ha facoltà di presentare un reclamo in qualsiasi momento dinanzi a un'autorità di supervisione. ESET è subordinata alla normativa delle leggi vigenti in Slovacchia e come membro dell'Unione Europea è vincolata alla legislazione inerente la protezione dei dati. L'autorità responsabile della supervisione dei dati competente è l'Office for Personal Data Protection della Repubblica Slovacca, con sede al seguente indirizzo: Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Elaborazione dei dati personali dell'Utente

I servizi offerti da ESET integrati nei relativi prodotti sono forniti ai sensi dell' [EULA](#). Tuttavia, alcuni di essi potrebbero richiedere un'attenzione particolare. Con la presente la Società desidera fornire all'Utente ulteriori

informazioni relative alla raccolta dei dati relativamente alla fornitura dei propri servizi. La Società offre vari servizi descritti nell'Accordo di licenza per l'utente finale e nella [documentazione](#). Per garantire un funzionamento corretto delle varie applicazioni, la Società richiede all'Utente di fornire le informazioni di seguito indicate:

Gestione delle licenze e dati di fatturazione. Il nome, l'indirizzo e-mail, la chiave di licenza e (se applicabile) l'indirizzo, l'affiliazione dell'azienda e i dati di pagamento vengono raccolti ed elaborati da ESET al fine di facilitare l'attivazione della licenza, l'invio della chiave di licenza, i promemoria sulla scadenza, le richieste di assistenza, la verifica dell'autenticità della licenza, l'offerta del servizio e di altre notifiche, compresi messaggi di marketing in linea con la legislazione applicabile o il consenso dell'Utente. ESET è legalmente obbligata a conservare le informazioni di fatturazione per un periodo di 10 anni. Tuttavia, le informazioni sulla gestione delle licenze saranno rese anonime entro 12 mesi dalla scadenza della licenza.

Aggiornamento e altre statistiche. Le informazioni elaborate includono dati relativi al processo di installazione e al computer dell'Utente, compresa la piattaforma su cui è installato il prodotto e informazioni sulle operazioni e le funzionalità dei prodotti, tra cui sistema operativo, informazioni sui dispositivi hardware, ID di installazione, ID delle licenze, indirizzi IP, indirizzi MAC, impostazioni di configurazione del prodotto. Il loro trattamento viene eseguito allo scopo di fornire servizi di aggiornamento e di upgrade e di effettuare la manutenzione e garantire la sicurezza e il miglioramento dell'infrastruttura di backend.

Tali informazioni vengono tenute separate dalle informazioni di identificazione richieste ai fini della gestione delle licenze e della fatturazione, in quanto non richiedono l'identificazione dell'Utente finale. Il periodo di conservazione è fino a 4 anni.

Sistema di reputazione **ESET LiveGrid®**. Hash unidirezionali correlati alle infiltrazioni vengono processati per il sistema di reputazione ESET LiveGrid® che garantisce un potenziamento delle prestazioni delle soluzioni anti-malware proposte eseguendo un confronto tra i file controllati e un database di oggetti inseriti nelle whitelist o nelle blacklist nel cloud. Durante questo processo, l'Utente finale non viene identificato.

Sistema di feedback **ESET LiveGrid®**. I campioni sospetti e i metadati "from the wild" prodotti da ESET LiveGrid® Feedback System che consente a ESET di fornire una risposta tempestiva alle esigenze degli Utenti finali e alle minacce più recenti. Le attività della Società dipendono strettamente dall'invio, da parte degli Utenti finali, di

- Infiltrazioni, quali campioni potenziali di virus e altri programmi dannosi e sospetti; oggetti problematici, potenzialmente indesiderati o pericolosi, come file eseguibili, messaggi di posta elettronica segnalati dagli Utenti finali come spam o contrassegnati dal prodotto;
- Informazioni relative all'uso di Internet, tra cui indirizzi IP e dati geografici, pacchetti IP, URL e frame Ethernet;
- File di arresti anomali e le informazioni in essi contenute.

La Società non raccoglie dati degli Utenti che non rientrano nelle finalità ivi specificate, sebbene talvolta tale operazione risulti inevitabile. Accidentalmente i dati raccolti potrebbero essere inclusi negli stessi malware (a insaputa di ESET e senza la sua previa autorizzazione) o all'interno di nomi di file o URL ed ESET non desidera che diventino parte dei propri sistemi o che siano elaborati per le finalità di cui alla presente Informativa sulla privacy.

Tutte le informazioni ottenute ed elaborate attraverso il sistema di feedback ESET LiveGrid® sono concepite per essere utilizzate senza l'identificazione dell'Utente finale.

Valutazione della sicurezza dei dispositivi connessi alla rete. Allo scopo di fornire la funzione di valutazione della protezione, la Società elabora il nome della rete locale e le informazioni sui dispositivi in tale rete quali presenza, tipo, nome, indirizzo IP e indirizzo MAC del dispositivo nella rete locale correlate ai dati sulla licenza. Le informazioni comprendono anche il tipo di sicurezza e di crittografia wireless per i dispositivi router. Le

informazioni sulla gestione delle licenze che identificano l'Utente finale saranno rese anonime entro 12 mesi dalla scadenza della licenza.

Supporto tecnico. Le informazioni di contatto e relative alla gestione delle licenze e i dati contenuti nelle richieste di assistenza potrebbero essere necessari ai fini dell'offerta dei servizi di assistenza. In base al canale scelto dall'Utente finale per contattare ESET, quest'ultima potrebbe raccogliere l'indirizzo e-mail, il numero di telefono, informazioni sulle licenze, dettagli sui prodotti e descrizione della richiesta di assistenza. All'Utente finale potrebbe essere chiesto di fornire altre informazioni per facilitare il servizio di assistenza. I dati elaborati per il supporto tecnico vengono archiviati per 4 anni.

Protezione da uso illegittimo dei dati In caso di creazione dell'Account ESET HOME sul sito web <https://home.eset.com> e di attivazione della funzione da parte dell'Utente finale in relazione al furto del computer, verranno raccolte ed elaborate le seguenti informazioni: dati relativi alla posizione, screenshot, informazioni sulla configurazione del computer e dati registrati dalla fotocamera del computer. I dati raccolti vengono memorizzati sui server della Società o su quelli dei relativi fornitori di servizi con un periodo di conservazione di 3 mesi.

Password Manager. Se si sceglie di attivare la funzione Password Manager, i dati correlati ai dettagli di autenticazione vengono memorizzati in formato crittografato solo sul computer dell'Utente o su altri dispositivi specificati. In caso di attivazione del servizio di sincronizzazione, i dati crittografati vengono memorizzati sui server della Società o su quelli dei relativi fornitori di servizi per garantire tale servizio. Né ESET né il fornitore di servizi hanno accesso ai dati crittografati. Solo l'Utente finale è in possesso della chiave per decrittografare i dati. I dati saranno rimossi a fronte della disattivazione della funzione.

ESET LiveGuard. Se si sceglie di attivare la funzione ESET LiveGuard, è necessario inviare campioni quali file predefiniti e selezionati dall'Utente finale. I campioni scelti per l'analisi da remoto saranno caricati sul servizio ESET e il risultato dell'analisi verrà inviato nuovamente al computer dell'Utente. I campioni sospetti vengono elaborati in base alle informazioni raccolte dal sistema di feedback ESET LiveGrid®.

Programma di miglioramento dell'esperienza degli utenti. Se si sceglie di attivare il [Programma di miglioramento dell'esperienza degli utenti](#), verranno raccolte e utilizzate le informazioni di telemetria anonime relative all'utilizzo dei prodotti della Società in base al consenso fornito dall'Utente.

Si tenga presente che se la persona che utilizza i prodotti e i servizi della Società non è l'Utente finale che ha acquistato il prodotto o il servizio e ha stipulato l'Accordo di licenza per l'utente finale con essa (ad esempio, un dipendente dell'Utente finale, un familiare o una persona altrimenti autorizzata a utilizzare il prodotto o il servizio dall'Utente finale in conformità dell'Accordo di licenza per l'utente finale), l'elaborazione dei dati viene eseguita nell'interesse legittimo di ESET in base al significato specificato nell'Art. 6 (1) f) GDPR per consentire all'utente autorizzato dall'Utente finale di utilizzare i prodotti e i servizi forniti dalla Società nel rispetto dei termini dell'Accordo di licenza per l'utente finale.

Informazioni di contatto

Qualora desideri esercitare i propri diritti in qualità di soggetto titolare dei dati o in caso di domande o dubbi, l'Utente potrà inviare un messaggio ai seguenti recapiti:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk