ESET NOD32 Antivirus 3.0

Componenti integrati:
ESET NOD32 Antivirus
ESET NOD32 Antispyware

Guida dell'utente:

proteggiamo il vostro mondo digitale

sommario

ESET NOD32 Antivirus 3.0

Supporto tecnico globale: www.eset.eu/support
Supporto tecnico America del nord: www.eset.com/support

REV.20081020-002

1. ESET NOD32 Antivirus 3.0

ESET NOD32 Antivirus 3.0 è la nuova versione del pluripremiato prodotto ESET NOD32 Antivirus 2.*, che utilizza la velocità e la precisione di ESET NOD32 Antivirus grazie alla versione più recente del motore di scansione ThreatSense®.

Le tecniche avanzate implementate sono in grado di bloccare in modo proattivo virus, spyware, trojan, worm, adware e rootkit senza rallentare il sistema o richiedere intervento dell'utente che lavora o gioca al computer.

1.1 Novità

La lunga esperienza di sviluppo degli esperti ESET è dimostrata dall'architettura completamente nuova del programma ESET NOD32 Antivirus, che garantisce la massima capacità di rilevamento con requisiti di sistema minimi.

- **Antivirus e antispyware**

Questo modulo si basa sul motore di scansione ThreatSense®, utilizzato per la prima volta nel pluripremiato sistema NOD32 Antivirus. Nella nuova architettura di ESET NOD32 Antivirus, il motore ThreatSense® è stato ottimizzato e migliorato.

Funzione	Descrizione
Pulizia migliorata	Il sistema antivirus ora pulisce ed elimina in modo intelligente la maggior parte delle infiltrazioni rilevate, senza richiedere l'intervento dell'utente.
Modalità di controllo in background	Il controllo del computer può essere eseguito in background, senza rallentare le prestazioni del computer.
File di aggiornamento di minori dimensioni	I processi di ottimizzazione principali consentono di generare file di aggiornamento di dimensioni minori rispetto alla versione 2.7. Inoltre, è stata migliorata la protezione dei file di aggiornamento da eventuali danni.
Protezione dei client di posta più diffusi	Ora è possibile effettuare il controllo della posta in arrivo non solo in MS Outlook, ma anche in Outlook Express e Windows Mail.
Altri miglioramenti	– Accesso diretto ai file system per una maggiore velocità e un miglior rendimento. – Accesso bloccato ai file infetti. – Ottimizzazione per il Centro sicurezza PC Windows, incluso Vista.

1.2 Requisiti di sistema

Per il corretto funzionamento di ESET NOD32 Antivirus, il sistema deve soddisfare i seguenti requisiti hardware e software:

ESET NOD32 Antivirus:

Windows 2000, XP	400 MHz a 32 bit/64 bit (x86/x64) 128 MB di memoria di sistema RAM 35 MB di spazio disponibile su disco Super VGA (800 × 600)
Windows Vista	1 GHz a 32 bit/64 bit (x86/x64) 512 MB di memoria di sistema RAM 35 MB di spazio disponibile su disco Super VGA (800 × 600)

ESET NOD32 Antivirus Business Edition:

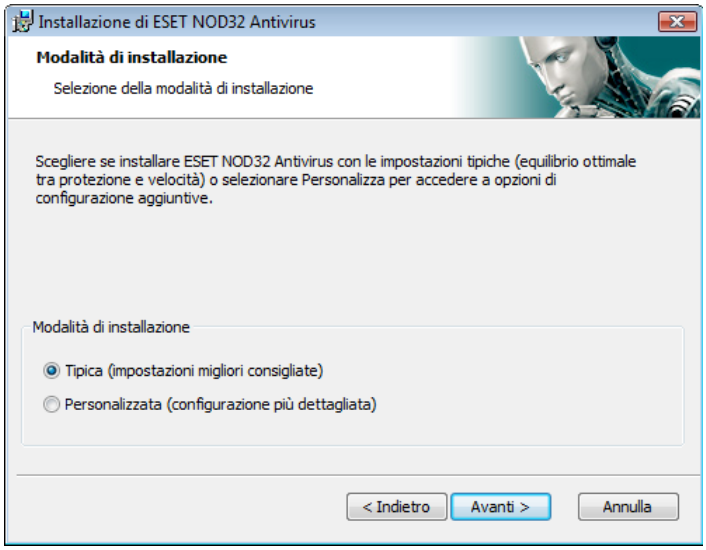
Windows 2000, 2000 Server, XP, 2003 Server	400 MHz a 32 bit/64 bit (x86/x64) 128 MB di memoria di sistema RAM 35 MB di spazio disponibile su disco Super VGA (800 × 600)
Windows Vista, Windows Server 2008	1 GHz a 32 bit/64 bit (x86/x64) 512 MB di memoria di sistema RAM 35 MB di spazio disponibile su disco Super VGA (800 × 600)

2. Installazione

Dopo l'acquisto, è possibile scaricare il programma di installazione di ESET NOD32 Antivirus come pacchetto .msi dal sito Web di ESET. Dopo l'avvio del programma di installazione, l'installazione guidata condurrà l'utente attraverso le fasi della configurazione di base. Esistono due tipi di installazione disponibile con diversi livelli di dettagli di configurazione:

1. Installazione tipica

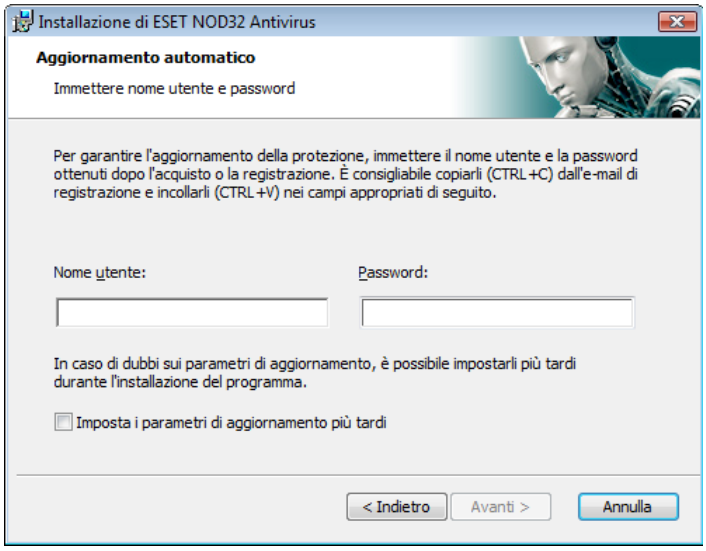
2. Installazione personalizzata



2.1 Installazione tipica

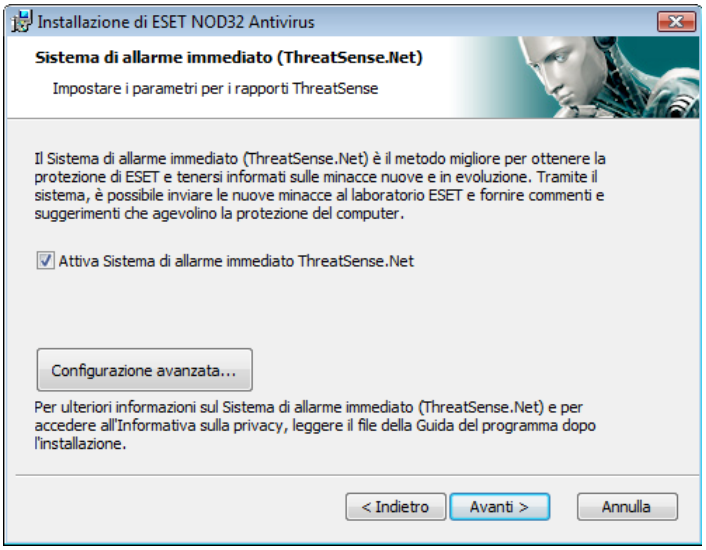
L'installazione tipica è consigliata agli utenti che desiderano installare ESET NOD32 Antivirus con le impostazioni predefinite. Le impostazioni predefinite del programma offrono il massimo livello di protezione, caratteristica apprezzata soprattutto dagli utenti che non desiderano configurare impostazioni in modo dettagliato.

La prima importante operazione da eseguire è l'inserimento del nome utente e della password per l'aggiornamento automatico del programma, funzione fondamentale per garantire una protezione costante del sistema.



Immettere nei campi corrispondenti **Nome utente** e **Password**, ovvero i dati di autenticazione ottenuti dopo l'acquisto o la registrazione del prodotto. Se non si dispone ancora di nome utente e password, selezionare l'opzione **Imposta i parametri di aggiornamento più tardi**. È possibile inserire i dati di autenticazione anche in seguito, direttamente dal programma.

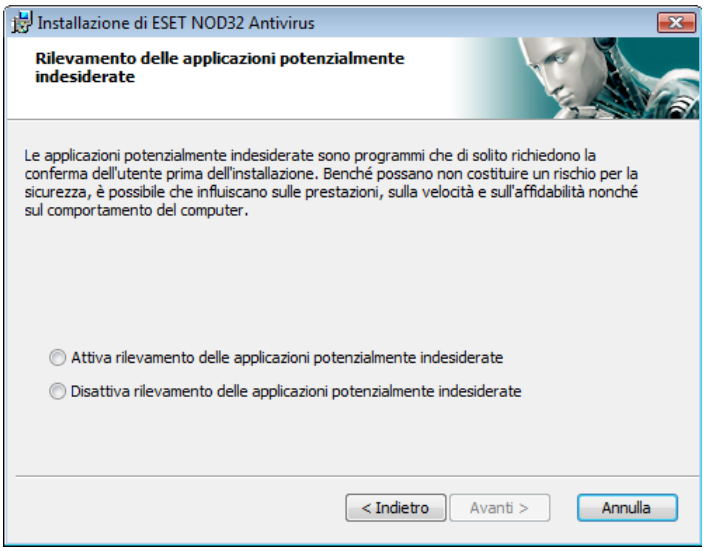
Il passaggio successivo dell'installazione prevede la configurazione del Sistema di allarme immediato (ThreatSense.Net). Il Sistema di allarme immediato (ThreatSense.Net) garantisce che ESET venga informata in modo tempestivo e continuato sulle nuove infiltrazioni, per proteggere gli utenti in modo immediato. Il sistema consente l'invio di nuovi malware ai laboratori dei virus ESET, dove verranno analizzati, elaborati e aggiunti al database delle firme antivirali.



Nell' impostazione predefinita, la casella di controllo **Attiva Sistema di allarme immediato ThreatSense.Net** è selezionata in modo da attivare questa funzione. Per modificare le impostazioni dettagliate per l'invio di file sospetti, fare clic su **Configurazione avanzata...**

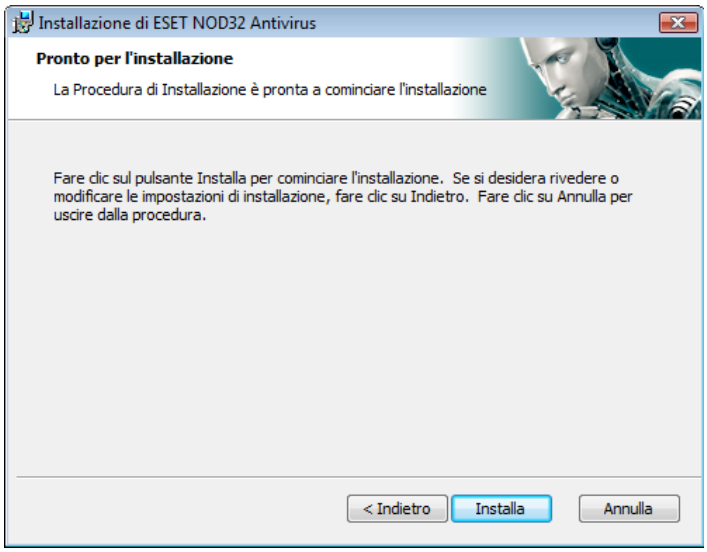
Il passaggio successivo del processo di installazione consiste nella configurazione dell'opzione **Rilevamento delle applicazioni potenzialmente indesiderate**. Le applicazioni potenzialmente indesiderate non sono necessariamente dannose, tuttavia potrebbero influire negativamente sul comportamento del sistema operativo.

Applicazioni di questo tipo spesso fanno parte dell'istallazione di altri programmi e può essere difficile notarle durante l'istallazione. In genere viene, infatti, visualizzata una notifica durante l'installazione di queste applicazione, ma è frequente il caso di applicazioni installate senza il consenso dell'utente.



Selezionare l'opzione **Attiva rilevamento delle applicazioni potenzialmente indesiderate** per consentire a ESET NOD32 Antivirus di rilevare questo tipo di minaccia (scelta consigliata).

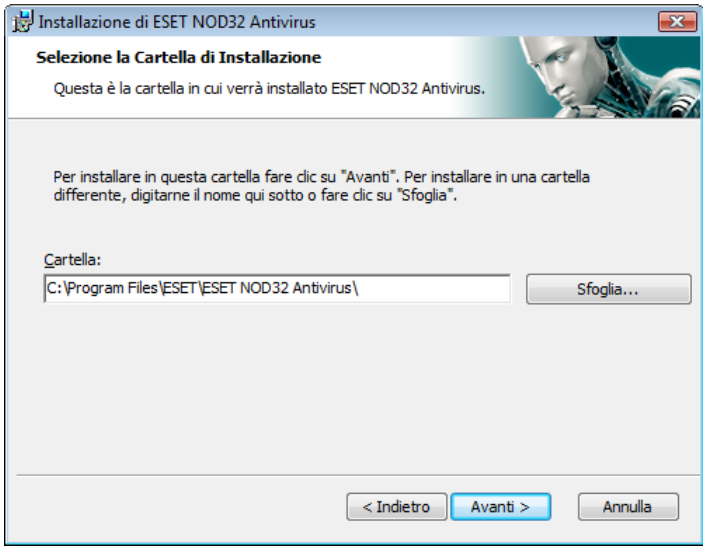
L'ultimo passaggio dell'installazione tipica permette di confermare l'installazione cliccando sul pulsante **Installa**.



2.2 Installazione personalizzata

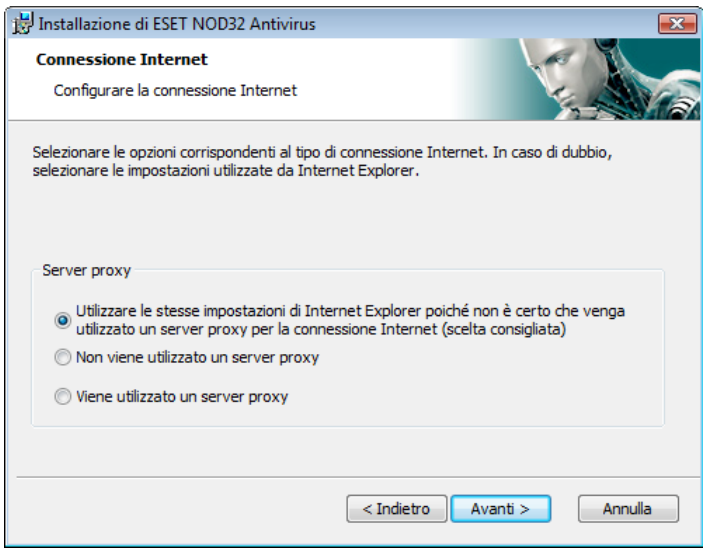
L'installazione **personalizzata** è indicata per gli utenti con esperienza nella configurazione dettagliata dei programmi e che desiderano modificare le impostazioni avanzate durante l'installazione.

La prima operazione da eseguire consiste nel selezionare il percorso della cartella di installazione. Nell' impostazione predefinita, il programma viene installato nella cartella C:\Programmi\ESET\ESET NOD32 Antivirus \. Per specificare un percorso diverso, scegliere **Sfoglia...** (scelta non consigliata).

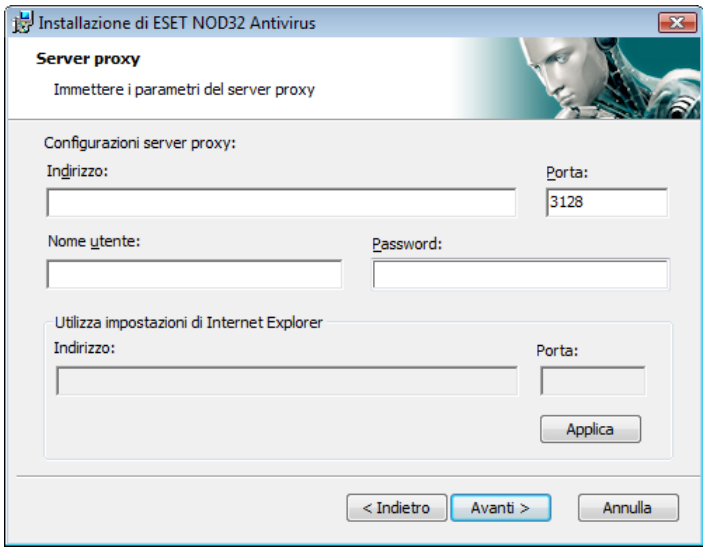


Quindi **Inserire nome utente e password**. Questo passaggio è analogo a quello dell'installazione tipica (vedere a pagina 5).

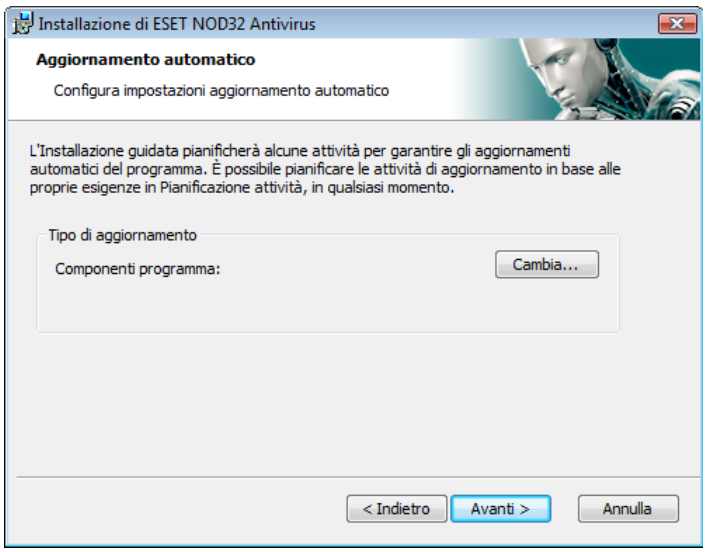
Dopo aver immesso nome utente e password, fare clic su **Avanti** per **Configurare la connessione Internet**.



Se si utilizza un server proxy, questo deve essere configurato in modo corretto per consentire la ricezione degli aggiornamenti delle firme antivirali. Se non si è certi dell'utilizzo di un server proxy per la connessione a Internet, selezionare **Utilizzare le stesse impostazioni di Internet Explorer poiché non è certo che venga utilizzato un server proxy per la connessione Internet (scelta consigliata)**, quindi scegliere **Avanti**. Se non si utilizza un server proxy, selezionare l'opzione corrispondente.

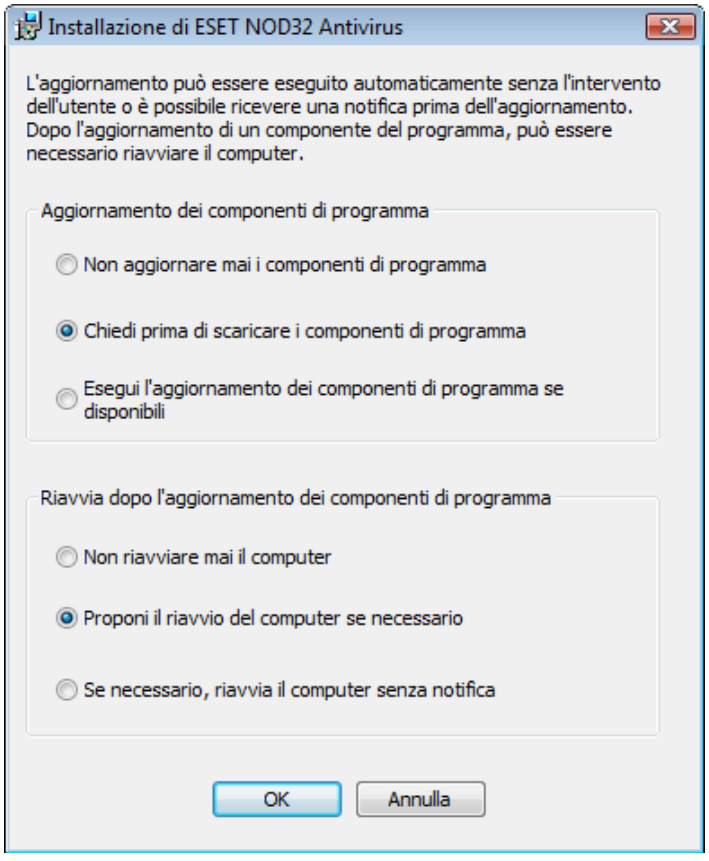


Per configurare le impostazioni del server proxy, selezionare **Viene utilizzato un server proxy** e scegliere **Avanti**. Immettere l'indirizzo IP o l'URL del server proxy nel campo **Indirizzo.** Nel campo **Porta** specificare la porta sulla quale il server proxy accetta le connessioni (per impostazione predefinita, la porta 3128). Se il server proxy richiede l'autenticazione, sarà necessario immettere un nome utente e una password validi per consentire l'accesso al server proxy. Se necessario, è possibile anche copiare le impostazioni del server proxy da Internet Explorer. A tal fine, scegliere **Applica** e confermare la selezione.



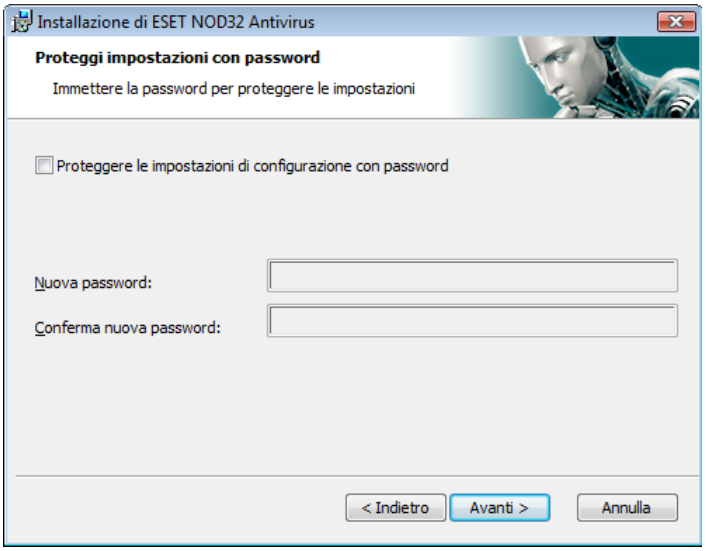
Fare clic su **Avanti** per passare alla finestra **Configura impostazioni aggiornamento automatico**. In questa fase è possibile specificare come si desidera che vengano gestiti gli aggiornamenti dei componenti di programma automatici sul sistema. Scegliere **Cambia...** per accedere alle impostazioni avanzate.

Se non si desidera aggiornare i componenti di programma, selezionare **Non aggiornare mai i componenti di programma**. L'opzione **Chiedi prima di scaricare i componenti di programma** consente di visualizzare una finestra di conferma prima di scaricare i componenti di programma. Per attivare l'aggiornamento automatico dei componenti di programma, selezionare l'opzione **Esegui l'aggiornamento dei componenti di programma se disponibili**.



NOTA: dopo l'aggiornamento di un componente del programma, è in genere necessario riavviare il sistema. L'impostazione consigliata è: **Se necessario, riavvia il computer senza notifica**.

Il passaggio successivo dell'istallazione consiste nell'immissione di una password per proteggere le impostazioni del programma. Scegliere una password con cui si desidera proteggere il programma. Immettere nuovamente la password per conferma.



I passaggi di **Configurazione del Sistema di allarme immediato (ThreatSense.Net)** e **Rilevamento delle applicazioni potenzialmente indesiderate** sono analoghi a quelli dell'Installazione tipica e non vengono riportati qui (vedere a pagina 5).

Nell'ultimo passaggio viene visualizzata una finestra con cui si richiede il consenso per l'installazione.

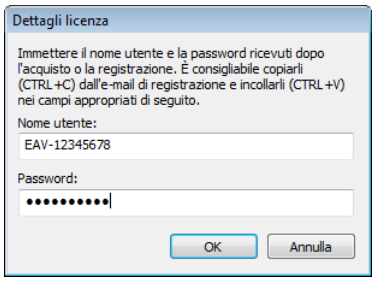
2.3 Utilizzo delle impostazioni originali

Quando si reinstalla ESET NOD32 Antivirus, viene visualizzata l'opzione **Utilizza impostazioni correnti**. Selezionare questa opzione per trasferire i parametri di configurazione dall'installazione originale alla nuova.

2.4 Immissione di nome utente e password

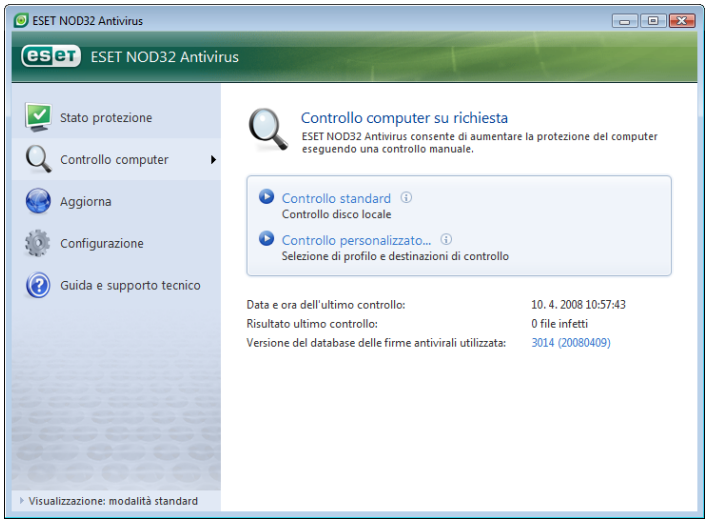
Per garantire un funzionamento ottimale è di fondamentale importanza che il programma venga aggiornato automaticamente. Ciò è possibile solo se il nome utente e la password vengono immessi correttamente nel setup dell'aggiornamento.

Se nome utente e password non sono stati immessi durante l'installazione, è possibile farlo a questo punto. Nella finestra principale del programma scegliere **Aggiorna**, quindi **Impostazione nome utente e password...** Immettere nella finestra **Dettagli licenza** i dati ricevuti con la licenza del prodotto.



2.5 Controllo computer su richiesta

Dopo l'installazione di ESET NOD32 Antivirus, è opportuno eseguire un controllo del computer per rilevare l'eventuale presenza di codice dannoso. Per avviare rapidamente un controllo, selezionare **Controllo computer** nella finestra principale del programma, quindi scegliere **Controllo standard**. Per ulteriori informazioni sulla funzione di controllo del computer, vedere il capitolo "Controllo del computer".



3. Guida introduttiva

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

3.1 Introduzione all'interfaccia utente: modalità

La finestra principale di ESET NOD32 Antivirus è suddivisa in due sezioni principali. Nella colonna a sinistra è possibile accedere al menu principale semplice da utilizzare. A destra si trova la finestra principale del programma in cui vengono mostrate le informazioni relative all'opzione selezionata nel menu principale.

Di seguito è riportata una descrizione dei pulsanti del menu principale:

Stato protezione: in un formato di facile lettura, sono riportate informazioni sullo stato di protezione di ESET NOD32 Antivirus. Se è attivata la modalità avanzata, verrà visualizzato lo stato di tutti i moduli di protezione. Fare clic su un modulo per visualizzarne lo stato corrente.

Controllo computer: in questa sezione l'utente può configurare e avviare il controllo del computer su richiesta.

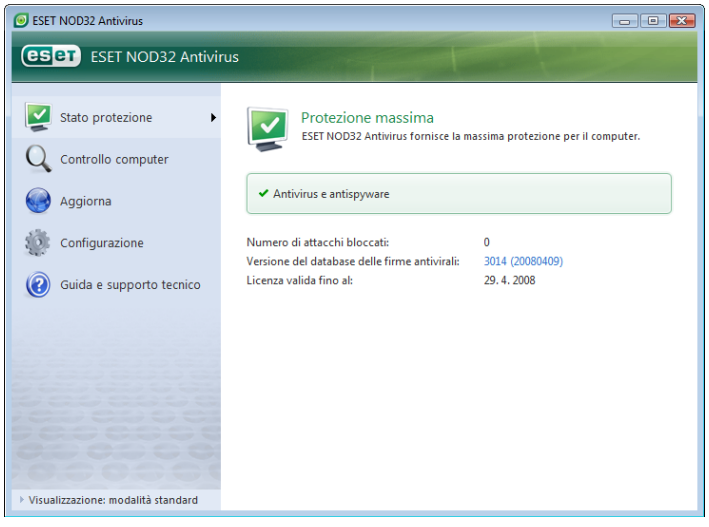
Aggiorna: selezionare questa opzione per accedere al modulo di aggiornamento con cui gestire gli aggiornamenti del database delle firme antivirali.

Configurazione: selezionare questa opzione per regolare il livello di protezione del computer. Se è attivata la modalità avanzata, verranno visualizzati i sottomenu del modulo Protezione antivirus e antispyware.

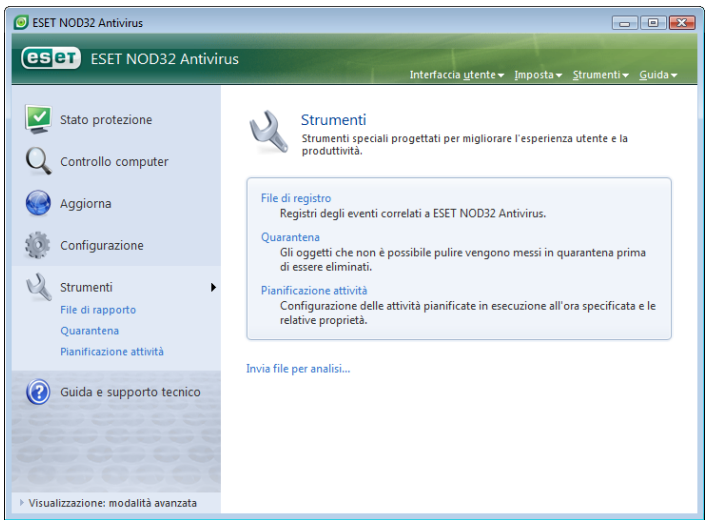
Strumenti: questa opzione è disponibile solo in modalità avanzata. Consente di accedere ai file di rapporto e alle informazioni su quarantena e pianificazione.

Guida e supporto tecnico: selezionare questa opzione per accedere alla guida del programma, alla Knowledgebase di ESET, al sito Web di ESET e alle richieste di supporto tecnico.

L'interfaccia utente di ESET NOD32 Antivirus consente agli utenti di scegliere tra le modalità standard e avanzata. Per passare da una modalità all'altra, cercare il collegamento **Visualizza** nell'angolo in basso a sinistra della schermata principale di ESET NOD32 Antivirus. Fare clic su questo pulsante per selezionare la modalità di visualizzazione desiderata.



La modalità standard consente l'accesso alle funzioni necessarie per le normali operazioni. In questa modalità non vengono visualizzate opzioni avanzate.

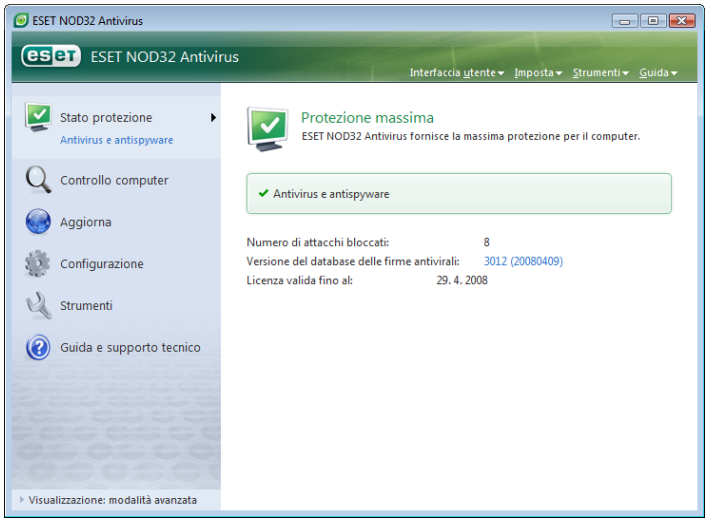


Quando si passa alla modalità avanzata, viene aggiunta l'opzione **Strumenti** al menu principale. L'opzione Strumenti consente all'utente di accedere a Pianificazione attività e Quarantena o di visualizzare i file di rapporto di ESET NOD32 Antivirus.

NOTA: tutte le istruzioni rimanenti della guida si riferiscono alla modalità avanzata.

3.1.1 Verifica del funzionamento del sistema

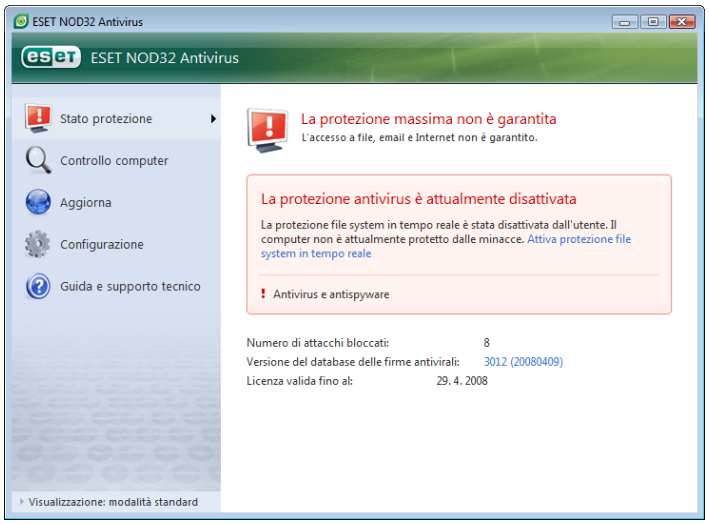
Per visualizzare lo **Stato protezione**, fare clic su questa opzione nella parte superiore del menu principale. Il sottomenu **Antivirus e antispyware** verrà visualizzato subito sotto, mentre nella finestra principale del programma verrà visualizzato un riepilogo dello stato sul funzionamento di ESET NOD32 Antivirus. Fare clic su Antivirus e antispyware e nella finestra principale del programma verrà visualizzato lo stato dei singoli moduli di protezione.



Se i moduli attivati funzionano correttamente, verrà visualizzato un indicatore di colore verde. In caso contrario, verrà visualizzato un punto esclamativo rosso o un'icona di notifica arancione e, nella parte superiore della finestra, verranno visualizzate ulteriori informazioni sul modulo che presenta dei problemi. Verrà inoltre visualizzata una soluzione consigliata per la riparazione del modulo. Per modificare lo stato dei singoli moduli, scegliere **Configurazione** dal menu principale e fare clic sul modulo desiderato.

3.1.2 Cosa fare se il programma non funziona correttamente

Se ESET NOD32 Antivirus rileva un problema in alcuni moduli di protezione, il problema verrà segnalato nella schermata **Stato protezione**, in cui viene proposta una possibile soluzione del problema.

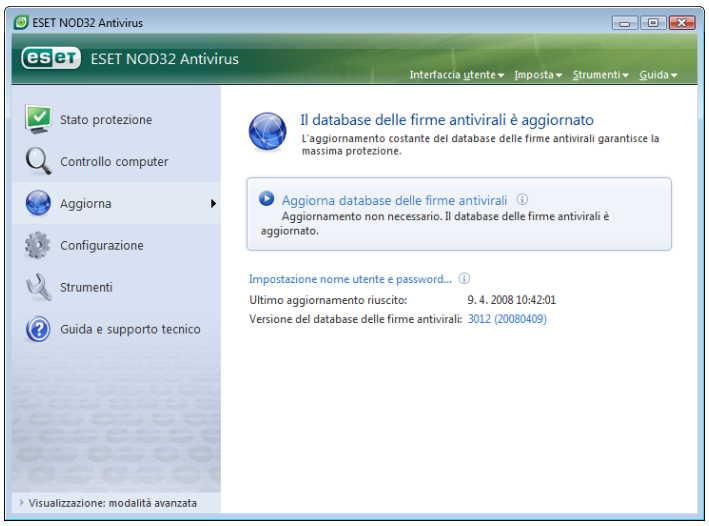


Nel caso in cui non sia possibile risolvere il problema ricorrendo all'elenco di problemi e soluzioni noti e descritti, fare clic su **Guida e supporto tecnico** per accedere ai file della Guida o eseguire una ricerca nella Knowledgebase. Se non si riesce comunque a trovare una soluzione, è possibile inviare una richiesta di assistenza al supporto tecnico di ESET. In base ai commenti e ai suggerimenti degli utenti, gli specialisti di ESET possono rispondere rapidamente alle domande degli utenti e proporre delle soluzioni per i problemi.

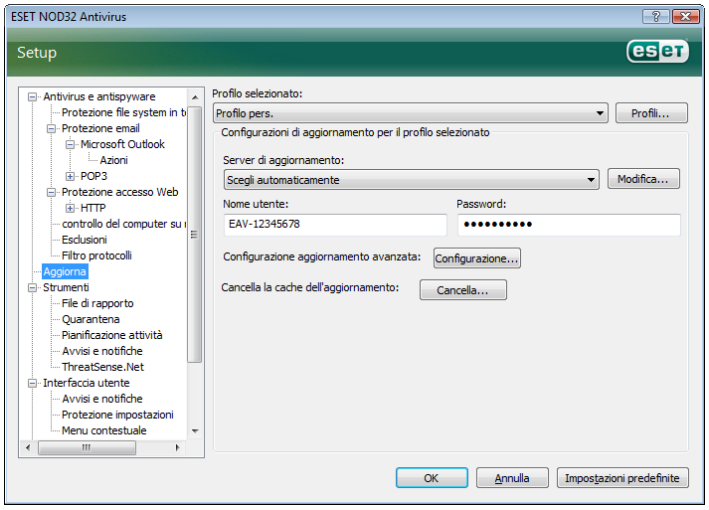
3.2 Configurazione dell'aggiornamento

L'aggiornamento del database delle firme antivirali e dei componenti del programma costituisce un aspetto importante per garantire una protezione completa contro codici dannosi. È opportuno prestare particolare attenzione alla configurazione e al funzionamento dell'aggiornamento. Nel menu principale selezionare **Aggiorna**, quindi fare clic su **Aggiorna database delle firme antivirali** nella finestra principale del programma per verificare immediatamente la disponibilità di un aggiornamento del database. **Impostazione nome utente e password...** consente di visualizzare la finestra di dialogo in cui inserire il nome utente e la password ricevuti al momento dell'acquisto.

Se nome utente e password sono stati specificati durante l'installazione di ESET NOD32 Antivirus, questa finestra di dialogo non verrà visualizzata.

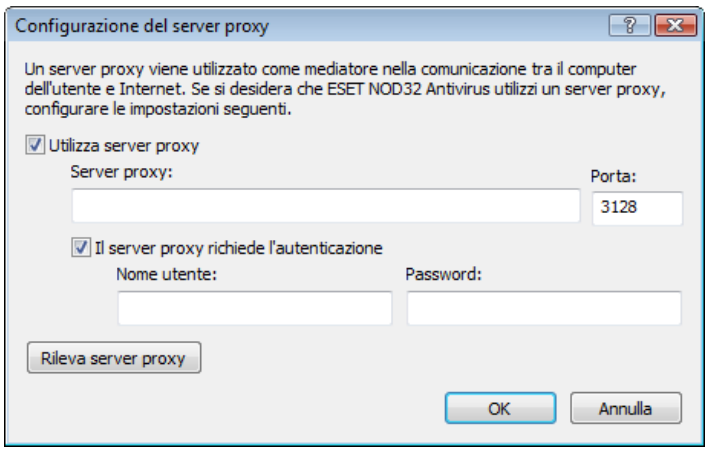


Nella finestra **Configurazione avanzata** (per accedere, premere F5) sono disponibili altre particolari opzioni per l'aggiornamento. Il menu a discesa **Server di aggiornamento:** deve essere impostato su **Scegli automaticamente**. Per configurare le opzioni di aggiornamento avanzate, tra cui la modalità di aggiornamento, l'accesso al server proxy, l'accesso agli aggiornamenti su un server locale e la creazione di copie delle firme antivirali (in ESET NOD32 Antivirus Business Edition), fare clic sul pulsante **Configurazione...**.



3.3 Configurazione del server proxy

Per permettere alla ESET NOD32 Antivirus di accedere a Internet in un sistema che utilizza un server proxy, questo deve essere specificato nella Configurazione avanzata. Per accedere alla finestra di configurazione del **Server proxy**, scegliere **Varie > Server proxy** dalla struttura Configurazione avanzata. Selezionare la casella di controllo **Utilizza server proxy**, quindi immettere l'indirizzo IP e la porta del server proxy, oltre ai dati di autenticazione.



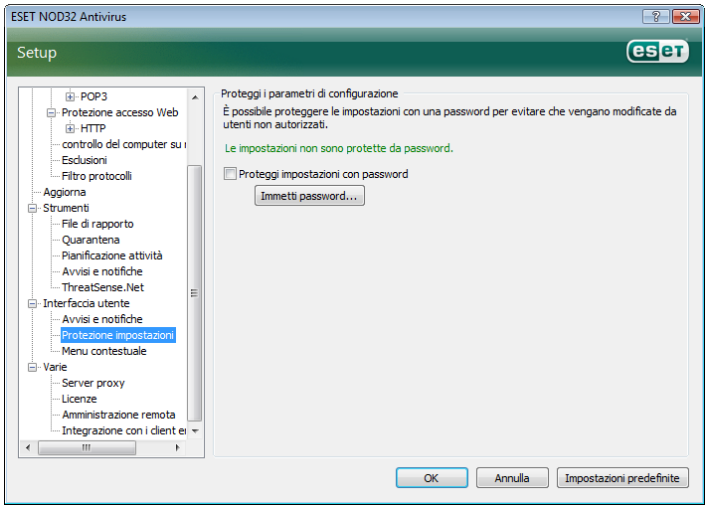
Nel caso in cui queste informazioni non siano disponibili, è possibile tentare di rilevare automaticamente le impostazioni del server proxy per ESET NOD32 Antivirus facendo clic sul pulsante **Rileva server proxy**.

NOTA: le opzioni del server proxy potrebbero essere diverse in base ai diversi profili di aggiornamento. In questo caso, configurare il server proxy nella Configurazione aggiornamento avanzata.

3.4 Configurazione della protezione

La configurazione di ESET NOD32 Antivirus ha una grande importanza nella struttura del tuo sistema di sicurezza. Le modifiche non autorizzate possono mettere a rischio la stabilità e la protezione del sistema. Per proteggere con una password i parametri di configurazione, nel menu principale fare clic su **Configurazione > Immettere struttura di impostazione avanzata completa... > Interfaccia utente > Protezione impostazioni** e fare clic sul pulsante **Immetti password...**

Immettere una password, confermarla immettendola di nuovo, quindi scegliere **OK**. Questa password verrà richiesta per tutte le modifiche future alle impostazioni di ESET NOD32 Antivirus.



4. Utilizzo di ESET NOD32 Antivirus

4.1 Protezione antivirus e antispyware

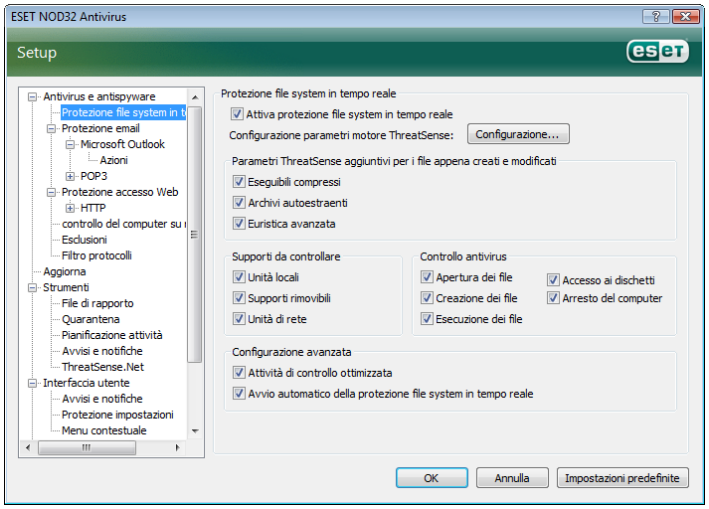
La protezione antivirus difende il sistema da attacchi dannosi controllando file, messaggi e-mail e comunicazioni su Internet. In caso di rilevamento di una minaccia costituita da codice dannoso, il modulo antivirus è in grado di risolvere il problema bloccando la minaccia, quindi disinfettando, eliminando o mettendo in quarantena i relativi file.

4.1.1 Protezione del file system in tempo reale

La funzione di protezione del file system in tempo reale consente di controllare tutti gli eventi di sistema relativi all'antivirus. Tutti i file vengono controllati alla ricerca di codice dannoso nel momento in cui vengono aperti, creati o eseguiti sul computer. La funzione di protezione del file system in tempo reale viene eseguita all'avvio del sistema

4.1.1.1 Impostazione del controllo

La protezione del file system in tempo reale prevede il controllo di tutti i tipi di supporto quando si verificano determinati eventi. Il controllo utilizza i metodi di rilevamento della tecnologia ThreatSense (come descritto in Configurazione parametri del motore ThreatSense). Il funzionamento del controllo può risultare diverso, ad esempio, per i file appena creati e i file già esistenti. Nel caso di file appena creati è possibile applicare un livello di controllo maggiore.



4.1.1.1.1 Controllo dei supporti

Nella configurazione predefinita, vengono controllati alla ricerca di potenziali minacce tutti i tipi di supporto.

Unità locali: controllo di tutte le unità disco rigido locali
Supporti rimovibili: dischetti, dispositivi di memorizzazione USB e così via
Unità di rete: controllo di tutte le unità mappate

È consigliabile mantenere le impostazioni predefinite e modificare tali impostazioni solo in casi specifici, ad esempio quando il controllo di alcuni supporti rallenta notevolmente il trasferimento dei dati.

4.1.1.1.2 Controlli eseguiti quando si verifica un evento

Per impostazione predefinita, tutti i file sono sottoposti a controllo all'apertura, durante l'esecuzione o la creazione. È consigliabile mantenere le impostazioni predefinite che offrono il massimo livello di protezione in tempo reale per il computer.

L'opzione **Accesso ai dischetti** garantisce il controllo del settore di avvio del dischetto durante l'accesso all'unità. L'opzione **Arresto del computer** garantisce il controllo dei settori di avvio del disco rigido durante l'arresto del computer. Sebbene i virus del settore di avvio siano oggi piuttosto rari, è consigliabile lasciare attivata questa opzione, poiché esiste ancora la possibilità di infezione di un virus del settore di avvio da fonti alternative.

4.1.1.1.3 Controllo dei file appena creati

La probabilità di infezione nei file appena creati è maggiore in confronto ai file già esistenti. Per questo motivo il programma controlla i nuovi file con parametri di controllo aggiuntivi. Insieme ai comuni metodi di controllo basati sulle firme, viene utilizzata l'euristica avanzata, che consente un notevole miglioramento delle percentuali di rilevamento. Oltre ai file appena creati, il controllo viene eseguito anche sui file autoestraenti (SFX) e sugli eseguibili compressi (file eseguibili compressi internamente).

4.1.1.1.4 Impostazione avanzata

Per garantire un impatto minimo sul sistema durante l'uso della protezione in tempo reale, il controllo dei file già esaminati non viene eseguito di nuovo (a meno che i file non siano stati modificati). I file vengono controllati di nuovo a controllo subito dopo ogni aggiornamento del database di firme antivirali. Questo comportamento viene configurato con l'opzione **Attività di controllo ottimizzata**. Quando questa funzione è disattivata, tutti i file vengono controllati a ogni accesso.

Per impostazione predefinita, la protezione in tempo reale viene avviata automaticamente all'avvio del sistema operativo e procede a un controllo continuo. In casi particolari (ad esempio, in caso di conflitto con un altro programma di controllo in tempo reale), la protezione in tempo reale può essere arrestata disattivando l'opzione **Avvio automatico della protezione file system in tempo reale.**

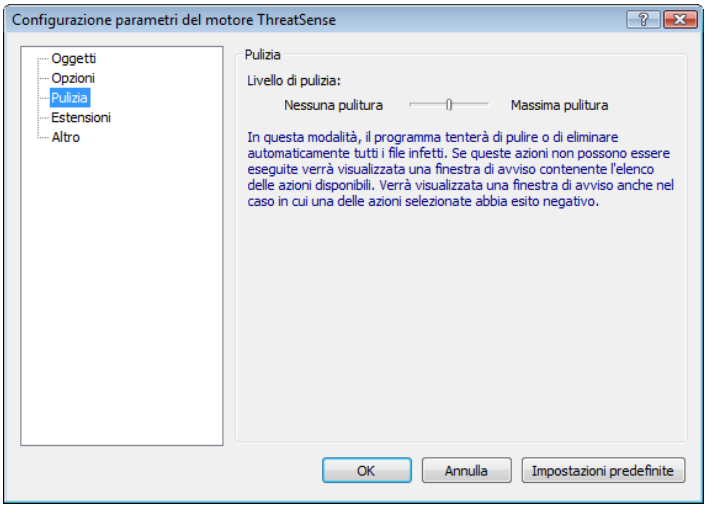
4.1.1.2 Livelli di pulizia

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

- **Con il primo livello si visualizza una finestra di avviso con opzioni disponibili per ciascuna infiltrazione rilevata. L'utente deve scegliere l'azione più adatta a ciascuna infiltrazione. Questo livello è indicato per utenti più esperti, in grado di gestire tutti i tipi di infiltrazione.**

- **Il livello medio prevede la selezione ed esecuzione automatica di un'azione predefinita (in base al tipo di infiltrazione). Un messaggio nell'angolo inferiore destro della schermata segnalerà il rilevamento e l'eliminazione di un file infetto. Non viene, tuttavia, eseguita un'azione automatica quando l'infiltrazione si trova in un archivio che contiene anche file puliti, come pure non viene eseguita su oggetti per i quali non è prevista un'azione predefinita.**

- **Il terzo livello è il più "aggressivo" e prevede la pulizia di tutti gli oggetti infetti. Questo livello potrebbe portare alla perdita di file validi ed è pertanto consigliabile utilizzarlo solo in particolari situazioni.**



4.1.1.3 Quando modificare la configurazione della protezione in tempo reale

La protezione in tempo reale è il componente più importante per la sicurezza di un sistema. È pertanto necessario prestare attenzione quando si modificano i relativi parametri. È consigliabile modificarli solo in casi specifici, ad esempio quando si verifica un conflitto con una determinata applicazione o con il controllo in tempo reale di un altro programma antivirus.

Dopo l'installazione di ESET NOD32 Antivirus, tutte le impostazioni vengono ottimizzate per offrire agli utenti il massimo livello di protezione del sistema. Per ripristinare le impostazioni predefinite, fare clic sul pulsante **Configurazioni predefinite** presente nell'angolo in basso a destra della finestra **Protezione file system in tempo reale** (**Configurazione avanzata > Antivirus e antispyware > Protezione file system in tempo reale**).

4.1.1.4 Controllo della protezione in tempo reale

Per verificare che la protezione in tempo reale funzioni e sia in grado di rilevare virus, utilizzare un file di test da eicar.com. Il 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 verificare la funzionalità dei programmi antivirus. È scaricabile dal sito all'indirizzo http://www.eicar.org/download/eicar.com.

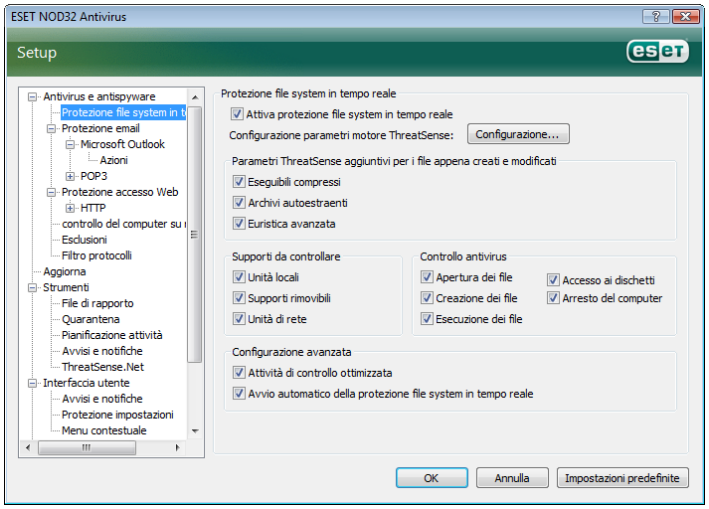
4.1.1.5 Cosa fare se la protezione in tempo reale non funziona

Nel prossimo capitolo verranno illustrati dei problemi che si verificano quando si utilizza la protezione in tempo reale e verrà descritto come risolverli.

La protezione in tempo reale è disattivata

Se la protezione in tempo reale è stata inavvertitamente disattivata da un utente, sarà necessario riattivarla. Per riattivare la protezione in tempo reale, selezionare **Configurazione > Antivirus e antispyware** quindi scegliere **Attiva** nella sezione **Protezione file system in tempo reale** della finestra principale del programma.

Se la protezione in tempo reale non viene avviata all'avvio del sistema, è probabile che l'opzione **Avvio automatico della protezione file system in tempo reale non sia attivata**. Per attivare l'opzione, selezionare **Configurazione avanzata** (F5) e fare clic su **Protezione file system in tempo reale** nella struttura della Configurazione avanzata. Nella sezione **Configurazione avanzata** alla fine della finestra, accertarsi che la casella di controllo **Avvio automatico della protezione file system in tempo reale** sia selezionata.



La protezione in tempo reale non rileva e disinfetta le infiltrazioni

Verificare che nel computer non siano installati altri programmi antivirus. Se attivati contemporaneamente, due sistemi di protezione in tempo reale possono entrare in conflitto. È consigliabile disinstallare gli altri programmi antivirus presenti nel sistema.

La protezione in tempo reale non viene avviata

Se la protezione in tempo reale non viene avviata all'avvio del sistema (e l'opzione **Avvio automatico della protezione file system in tempo reale** è attivata), il motivo può essere il conflitto con altri programmi. In questo caso, contattare gli specialisti del Supporto tecnico di ESET.

4.1.2 Protezione email

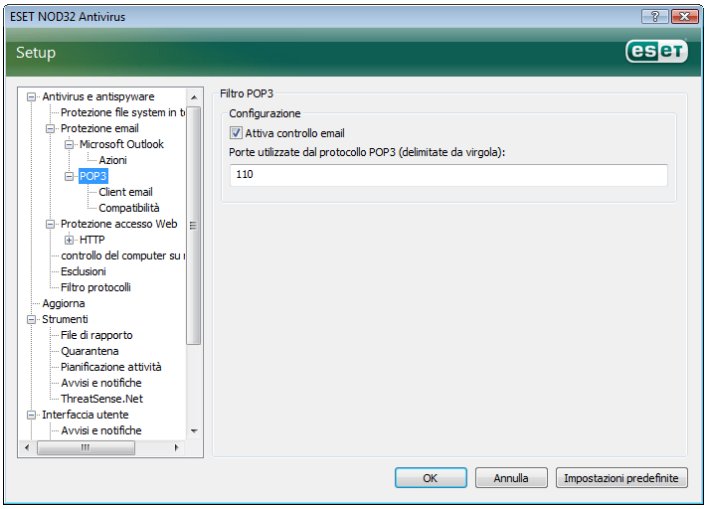
La protezione email garantisce il controllo delle email ricevute attraverso il protocollo POP3. Utilizzando il plug-in per Microsoft Outlook, ESET NOD32 Antivirus controlla tutte le comunicazioni dal client email (POP3, MAPI, IMAP, HTTP). Durante la verifica dei messaggi in arrivo, vengono utilizzati tutti i metodi di controllo avanzato forniti dal motore di scansione ThreatSense. Quindi il rilevamento di programmi dannosi viene eseguito ancora prima del confronto con il database di firme antivirali. Il controllo delle comunicazioni mediante protocollo POP3 non dipende dal client email utilizzato.

4.1.2.1 Controllo POP3

Il protocollo POP3 è il più diffuso per la ricezione di comunicazioni email in un'applicazione client email. ESET NOD32 Antivirus offre la protezione di questo protocollo, indipendentemente dal client email utilizzato.

Il modulo che garantisce 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 email. Nella configurazione predefinita, vengono controllate tutte le comunicazioni sulla 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 non vengono controllate.



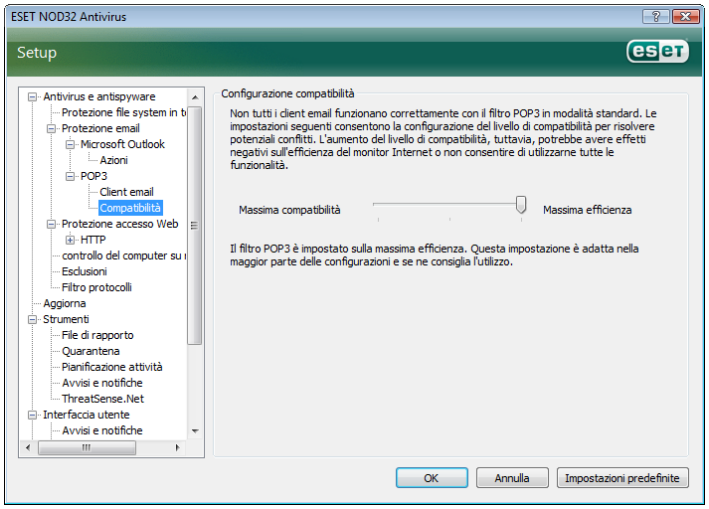
4.1.2.1.1 Compatibilità

Con alcuni programmi email è possibile che si verifichino dei problemi durante le operazioni di filtro POP3 (ad esempio, se si ricevono messaggi con una connessione a Internet lenta, possono verificarsi dei timeout a causa del controllo). In questo caso, provare a modificare la modalità di esecuzione del controllo. È possibile rendere il processo di disinfezione più veloce riducendo il livello di controllo. Per modificare il livello di controllo del filtro POP3, passare a **Antivirus e antispyware > Protezione email > POP3 > Compatibilità**.

Se si è attivata l'opzione **Massima efficienza**, il malware viene rimosso dai messaggi infetti (se le opzioni **Elimina** o **Pulisci** sono attivate o se è attivato il livello di disinfezione **massimo** o **predefinito**) e le informazioni sull'infiltrazione vengono inserite all'inizio dell'oggetto originale del messaggio di email.

Media compatibilità modifica la modalità di ricezione dei messaggi. I messaggi vengono inviati al client email in modo graduale: una volta trasferita l'ultima parte del messaggio, questo verrà sottoposto a controllo alla ricerca di malware. Tuttavia, il rischio di infezioni aumenta con questo livello di controllo. Il livello di disinfezione e la gestione delle notifiche (avvisi aggiunti alla riga dell'oggetto e al corpo dei messaggi di email) è identico all'impostazione di massima efficienza.

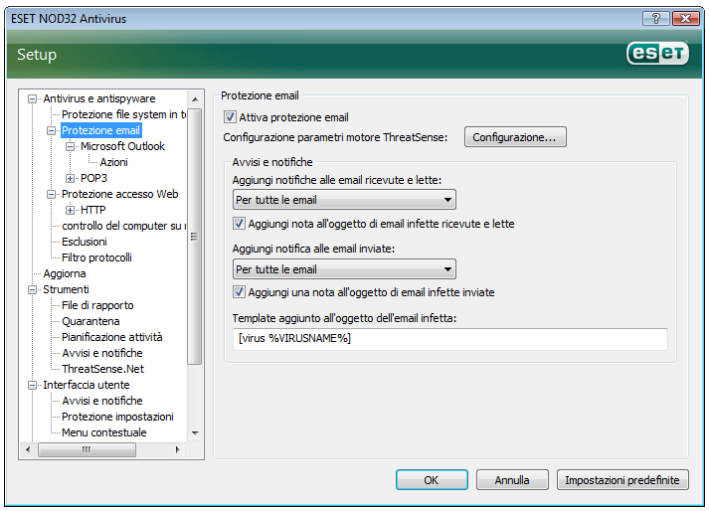
Con il livello **Massima compatibilità**, l'utente viene avvisato da una finestra di avviso che indica la ricezione di un messaggio infetto. Alla riga dell'oggetto o al corpo del messaggio email recapitato non viene aggiunta alcuna informazione sui file infetti e il malware non viene rimosso automaticamente. L'eliminazione del malware deve essere eeseguita dall'utente direttamente dal client email.



4.1.2.2 Integrazione con Microsoft Outlook, Outlook Express e Windows Mail

L'integrazione di ESET NOD32 Antivirus con i client email aumenta il livello di protezione attiva contro codici dannosi nei messaggi email. L'integrazione può essere attivata in ESET NOD32 Antivirus solo se il client email è supportato. Se è attivata l'integrazione, la barra degli strumenti di ESET NOD32 Antivirus viene inserita direttamente nel client email, contribuendo ad aumentare la protezione delle comunicazioni via email. Le impostazioni di integrazione sono disponibili in **Configurazione > Immettere struttura di impostazione avanzata completa... > Varie > Integrazione con client email**. In questa finestra di dialogo è possibile attivare l'integrazione con i client email supportati. I client email attualmente supportati sono Microsoft Outlook, Outlook Express e Windows Mail.

La protezione email si avvia selezionando la casella **Attiva la protezione email** in **Configurazione avanzata (F5)** > **Antivirus e antispyware** > **Protezione email**.



4.1.2.2.1 Aggiunta di notifiche al corpo di un messaggio email

È possibile contrassegnare ciascun messaggio email controllato da ESET NOD32 Antivirus aggiungendo una notifica all'oggetto o al corpo del messaggio. Questa funzione aumenta l'attendibilità dei messaggi inviati ai destinatari e, se viene rilevato un malware, fornisce informazioni utili sul livello di minaccia costituito dal mittente.

Le opzioni per questa funzione sono disponibili in **Configurazione avanzata > Protezione antivirus e antispyware > Protezione email**. In ESET NOD32 Antivirus sono disponibili le funzioni **Aggiungi notifiche alle email ricevute e lette** e **Aggiungi notifica alle email inviate**. Gli utenti possono scegliere se aggiungere le note a tutti i messaggi email, solo ai messaggi infetti o a nessun messaggio.

Con ESET NOD32 Antivirus è possibile anche aggiungere messaggi all'oggetto originale dei messaggi infetti. Per aggiungere delle note all'oggetto, utilizzare le opzioni **Aggiungi nota all'oggetto di email infette ricevute e lette** e **Aggiungi una nota all'oggetto di email infette inviate**.

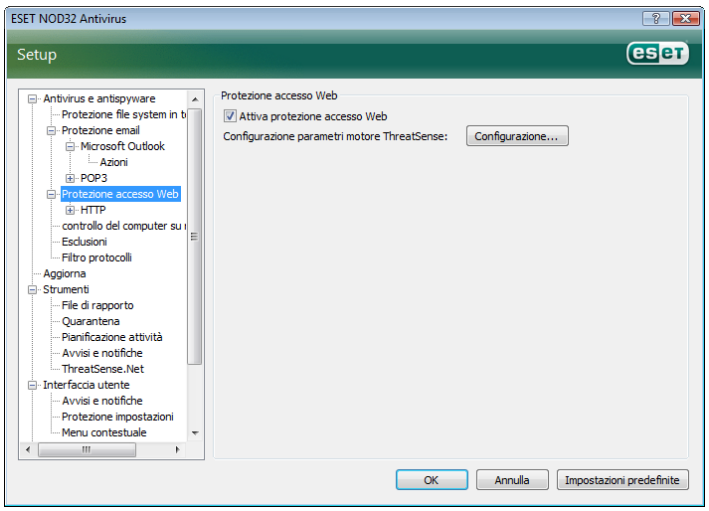
Il contenuto delle notifiche può essere modificato nel Template aggiunto all'oggetto dell'email infetta. Le modifiche menzionate consentono di automatizzare il processo di filtro dei messaggi email infetti, poiché questi messaggi vengono spostati in una cartella a parte (se previsto dal client email in uso).

4.1.2.3 Eliminazione delle infiltrazioni

In caso di ricezione di messaggi email infetti, verrà visualizzata un avviso con il nome del mittente, il messaggio email e il nome del malware. Nella parte inferiore della finestra, sono disponibili le opzioni **Pulisci**, **Elimina** o **Nessuna azione** per l'oggetto rilevato. Nella maggior parte dei casi è consigliabile selezionare **Pulisci** o **Elimina**. In situazioni particolari in cui si desidera comunque ricevere il file infetto, selezionare **Nessuna azione**. Se è attivato il livello **Massima pulitura**, verrà visualizzata una finestra di informazioni, senza nessuna opzione disponibile per gli oggetti infetti.

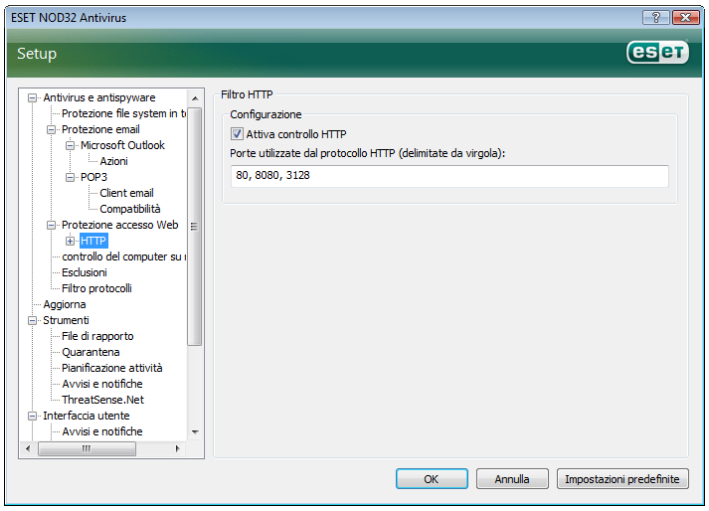
4.1.3 Protezione accesso Web

La connettività Internet è una funzione standard in un personal computer. Purtroppo è diventata anche lo strumento principale per il trasferimento di codice dannoso. Per questo motivo, è essenziale considerare con attenzione la protezione dell'accesso al Web. È importante controllare che l'opzione **Attiva la protezione accesso Web** sia attivata. Per accedere a questa opzione, scegliere **Configurazione avanzata (F5) > Protezione antivirus e antispyware > Protezione accesso Web**.



4.1.3.1 HTTP

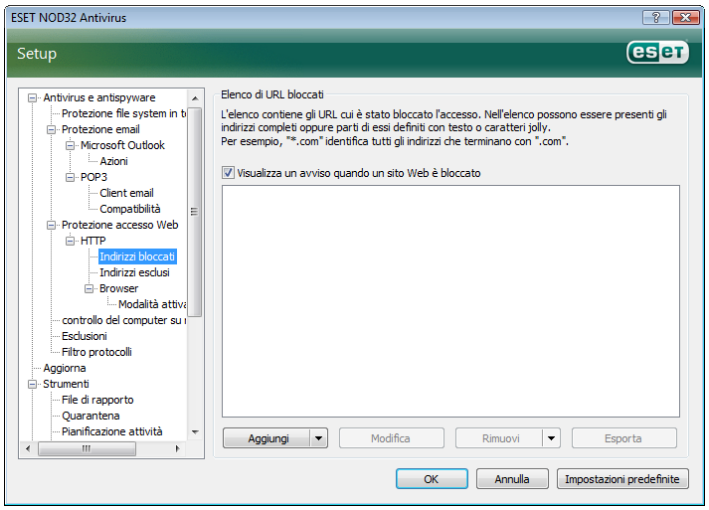
La protezione dell'accesso al Web consiste prevalentemente nel controllo della comunicazione dei browser con server remoti, secondo le regole del protocollo HTTP (Hypertext Transfer Protocol). ESET NOD32 Antivirus nella configurazione predefinita è impostato in modo da utilizzare gli standard HTTP della maggior parte dei browser. Le opzioni di impostazione del controllo HTTP possono, tuttavia, essere parzialmente modificate nella sezione **Protezione accesso Web > HTTP**. Nella finestra **Configurazione filtro HTTP** è possibile attivare o disattivare il controllo HTTP con l'opzione **Attiva controllo HTTP**. L'utente può inoltre stabilire i numeri delle porte utilizzate dal sistema per la comunicazione HTTP. L'impostazione predefinita per i numeri delle porte è 80, 8080 e 3128. Il traffico HTTP sulle porte può essere automaticamente rilevato e sottoposto a controllo, aggiungendo altri numeri di porta separati da una virgola.



4.1.3.1.1 Indirizzi bloccati/esclusi

La configurazione del controllo HTTP consente di creare elenchi definiti dall'utente di **indirizzi** URL (Uniform Resource Locator) **Bloccati** ed **Esclusi**.

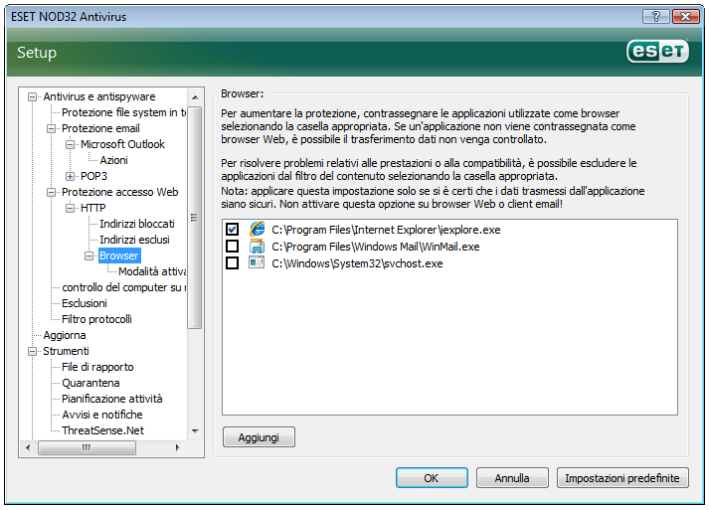
Entrambe le finestre di dialogo contengono i pulsanti **Aggiungi**, **Modifica**, **Rimuovi** ed **Esporta**, con cui è possibile gestire facilmente gli elenchi degli indirizzi specificati. Se un indirizzo richiesto dall'utente è incluso nell'elenco degli indirizzi bloccati, non sarà possibile accedere all'indirizzo. D'altro canto, è possibile accedere agli indirizzi presenti nell'elenco degli indirizzi esclusi senza che venga controllata l'eventuale presenza di codice dannoso. In entrambi gli elenchi, è possibile utilizzare i simboli speciali * (asterisco) e **?** (punto interrogativo). L'asterisco sostituisce qualsiasi stringa di caratteri e il punto interrogativo sostituisce qualsiasi simbolo. Prestare particolare attenzione quando si specificano gli indirizzi esclusi dal controllo, poiché l'elenco deve contenere solo indirizzi affidabili e sicuri. Allo stesso modo, è necessario verificare che in questo elenco i simboli * e **?** siano utilizzati correttamente.



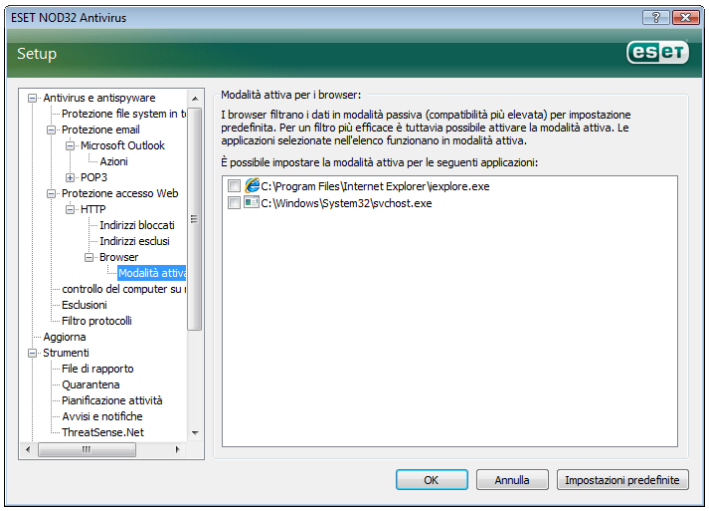
4.1.3.1.2 Browser

ESET NOD32 Antivirus contiene inoltre la funzione **Browser**, che consente all'utente di stabilire se l'applicazione specificata è o non è un browser. Se un'applicazione è contrassegnata dall'utente come browser, tutte le comunicazioni di quest'applicazione verranno controllate indipendentemente dal numero di porte coinvolte nella comunicazione.

La funzionalità Browser integra la funzione di controllo HTTP, poiché quest'ultima copre solo porte predefinite. Molti servizi Internet, tuttavia, utilizzano un numero sconosciuto o sempre diverso di porte. Per questo motivo la funzione Browser può stabilire il controllo delle porte di comunicazione indipendentemente dai parametri di connessione.



L'elenco delle applicazioni contrassegnate come browser è accessibile direttamente dal sottomenu **Browser** della sezione **HTTP**. In questa sezione è presente anche il sottomenu **Modalità attiva** che definisce la modalità di controllo per i browser. La **Modalità attiva** consente di verificare l'insieme dei dati trasferiti. Se non viene attivata, la comunicazione delle applicazioni viene controllata gradualmente in batch. Questo può ridurre l'efficacia del processo di verifica dei dati, ma garantisce anche una maggiore compatibilità per le applicazioni elencate. Se non si verificano problemi durante l'utilizzo, è consigliabile attivare questa modalità di controllo selezionando la casella accanto all'applicazione desiderata.



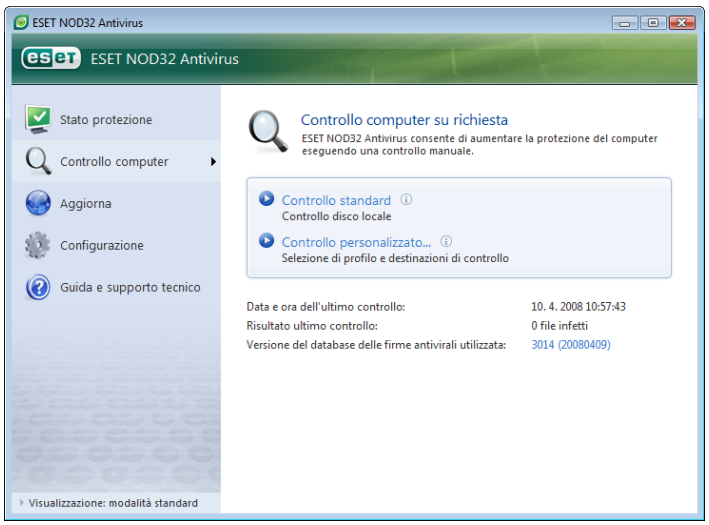
4.1.4 Controllo del computer

Se si sospetta che il computer sia infetto perché non funziona normalmente, eseguire un controllo del computer su richiesta per cercare eventuali malware nel computer. Dal punto di vista della protezione, è essenziale che i controlli del computer non vengano eseguiti solo quando si sospetta un'infezione, ma regolarmente, come parte delle normali misure di protezione. Il controllo regolare garantisce il rilevamento del malware non rilevato dallo scanner in tempo reale quando è stato salvato sul disco. Ciò accade se, al momento dell'infezione, lo scanner in tempo reale è disattivato o quando il database di firme antivirali è obsoleto.

È consigliabile eseguire un controllo su richiesta almeno una o due volte al mese. Il controllo può essere configurato come attività pianificata in **Strumenti > Pianificazione attività**.

4.1.4.1 Tipo di controllo

Sono disponibili due tipi di controllo: il **Controllo standard**, che consente di eseguire rapidamente il controllo del sistema senza che sia necessario configurare ulteriori parametri, e il **Controllo personalizzato**..., che consente all'utente di selezionare uno dei profili predefiniti, oltre a scegliere oggetti da controllare nel menu.



4.1.4.1.1 Controllo standard

Il controllo standard è un metodo facile da utilizzare che consente di avviare velocemente un controllo del computer e di pulire i file infetti senza l'intervento dell'utente. Il vantaggio principale è la semplicità della procedura, che non richiede configurazione del controllo particolarmente dettagliata. Con il controllo standard si sottopongono a controllo tutti i file presenti sulle unità locali e si puliscono o eliminano automaticamente le infiltrazioni trovate. Il livello di disinfezione viene impostato automaticamente sul valore predefinito. Per ulteriori informazioni sui tipi di disinfezione, vedere la sezione corrispondente a pagina 18.

Il profilo di controllo standard è studiato per gli utenti che desiderano eseguire un controllo rapido e semplice del proprio computer. Infatti offre una soluzione di controllo e disinfezione efficace senza richiedere un processo di configurazione lungo.

4.1.4.1.2 Controllo personalizzato

Il controllo personalizzato è una soluzione ottimale quando si desidera specificare parametri quali destinazioni e metodi di controllo. Il vantaggio del controllo personalizzato è la possibilità di configurare i parametri in modo dettagliato. Questi profili sono particolarmente utili se il controllo viene eseguito più volte con gli stessi parametri definiti dall'utente.

Per selezionare gli oggetti da controllare, utilizzare il menu a discesa per la selezione rapida dell'oggetto o selezionarli tra tutti i dispositivi disponibili nel computer. È inoltre possibile scegliere tra tre livelli di disinfezione selezionando **Configurazione... > Pulizia**. Se si desidera eseguire solo il controllo del sistema senza eseguire altre operazioni, selezionare la casella di controllo **Controllo senza rimozione**.

L'esecuzione di controlli del computer mediante la modalità personalizzata è un'operazione adatta a utenti esperti con precedenti esperienze di utilizzo di programmi antivirus.

4.1.4.2 Destinazioni di controllo

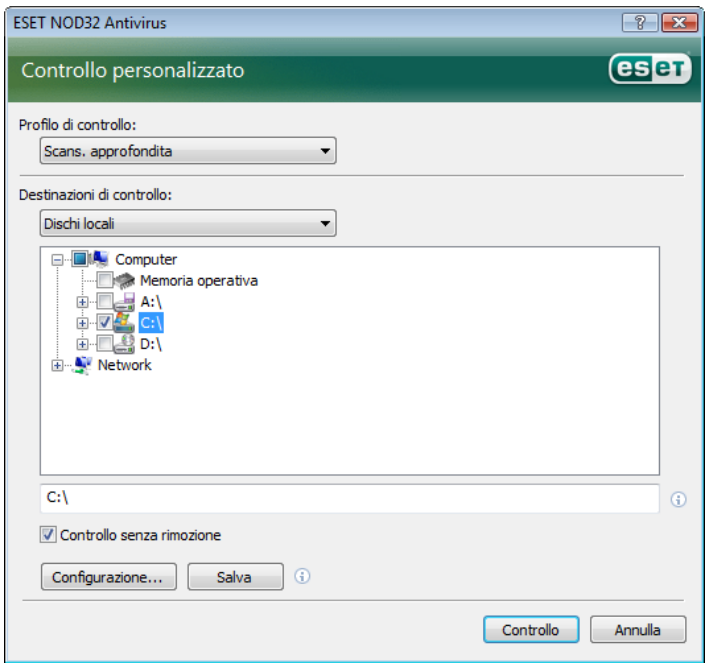
Il menu Oggetti da controllare consente di selezionare file, cartelle e dispositivi da controllare alla ricerca di virus.

Utilizzando l'opzione nel menu di scelta rapida Oggetti da controllare, è possibile selezionare le seguenti destinazioni:

Unità locali: controllo di tutte le unità disco rigido locali

Supporti rimovibili: dischetti, dispositivi di memorizzazione USB, CD/DVD

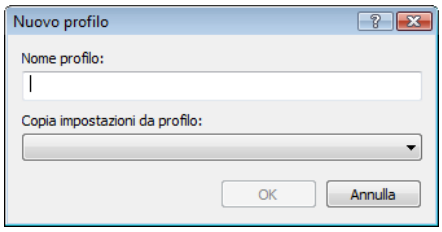
Unità di rete: tutte le unità mappate



Una destinazione di controllo può anche essere specificata in modo più preciso, immettendo il percorso alla cartella dei file che si desidera includere nel controllo. Selezionare le destinazioni dal menu che contiene tutti i dispositivi disponibili nel computer.

4.1.4.3 Profili di controllo

I parametri preferiti di controllo del computer possono essere salvati in profili di controllo. Il vantaggio di creare profili di controllo è costituito dalla possibilità di utilizzarli regolarmente per i controlli futuri. È consigliabile creare un numero di profili di controllo (con diverse destinazioni di controllo, metodi di controllo e altri parametri) pari a quelli utilizzati regolarmente dall'utente.



Per creare un nuovo profilo da utilizzare più volte per i controlli futuri, selezionare **Configurazione avanzata** (F5) > Controllo **computer su richiesta**. Fare clic sul pulsante **Profili...** sulla destra per visualizzare l'elenco di profili di controllo esistenti e l'opzione per la creazione di un nuovo profilo. **Configurazione parametri del motore ThreatSense** descrive ciascun parametro di configurazione del controllo. Sarà utile per creare un profilo di controllo adatto alle proprie esigenze.

Esempio:
si supponga di dover creare un proprio profilo di controllo e che la configurazione assegnata al profilo **Smart Scan** sia adatta almeno in parte. Tuttavia non si desidera eseguire il controllo di eseguibili compressi o di applicazioni potenzialmente pericolose, ma si desidera applicare l'opzione **Massima pulitura**. Nella finestra **Profili di configurazione** scegliere il pulsante **Aggiungi...** Immettere il nome del nuovo profilo nel campo **Nome profilo**, quindi scegliere **Smart scan** dal menu a discesa **Copia impostazioni da profilo.** Specificare quindi gli altri parametri in base alle proprie esigenze.

4.1.5 Configurazione dei parametri del motore ThreatSense

ThreatSense è il nome di una tecnologia che consiste in una serie di complessi metodi di rilevamento del malware.. Si tratta di una tecnologia proattiva, in grado di garantire la protezione anche durante le prime ore di diffusione di una nuova minaccia. Utilizza una combinazione di diversi metodi (analisi del codice, emulazione del codice, firme generiche, firme antivirali) che operano in modo integrato per potenziare la protezione del sistema. Il motore di scansione è in grado di controllare contemporaneamente diversi flussi di dati, ottimizzando l'efficienza e la percentuale di rilevamento. La tecnologia ThreatSense è inoltre in grado di eliminare i rootkit.

Le opzioni di impostazione della tecnologia ThreatSense consentono all'utente di specificare diversi parametri di controllo:

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

Per aprire la finestra di configurazione, fare clic sul pulsante **Configurazione...** in qualsiasi finestra di impostazione del modulo che utilizza la tecnologia ThreatSense (vedere di seguito). Scenari di protezione diversi possono richiedere configurazioni diverse. ThreatSense è configurabile singolarmente per i seguenti moduli di protezione:

- **Protezione del file system in tempo reale**
- **Controllo del file di avvio del sistema**
- **Protezione email**
- **Protezione accesso Web**
- **Controllo computer su richiesta**

I parametri di ThreatSense sono 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 il controllo euristico avanzato nel modulo di protezione del file system in tempo reale potrebbe provocare un rallentamento del sistema (in genere con questi metodi vengono controllati solo i file appena creati). È quindi consigliabile non modificare i parametri predefiniti di ThreatSense per tutti i moduli, con l'eccezione di Controllo computer.

4.1.5.1 Configurazione degli oggetti

Nella sezione **Oggetti** è possibile definire i componenti e i file del computer che verranno controllati alla ricerca di infiltrazioni.

Memoria operativa: consente di eseguire il controllo alla ricerca di minacce nella memoria operativa del sistema.

Settori di avvio: consente di eseguire il controllo alla ricerca di virus nei settori di avvio.

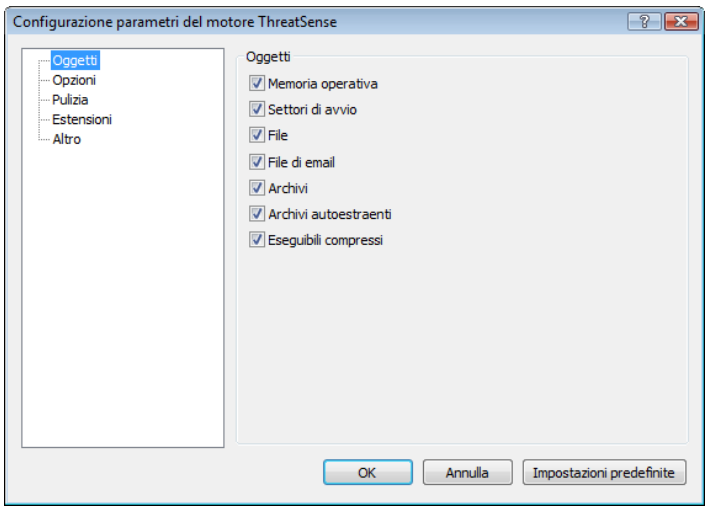
File: consente di eseguire il controllo di tutti i tipi di file più comuni (programmi, immagini, file audio, file video, database e così via).

File di email: consente di eseguire il controllo nei file speciali in cui sono contenuti i messaggi email.

Archivi: consente di eseguire il controllo dei file compressi in archivi (.rar, .zip, .arj, .tar e così via).

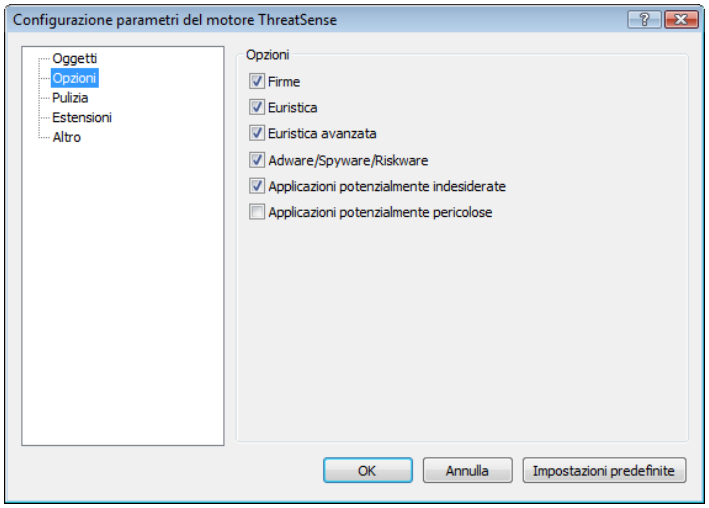
Archivi autoestraenti: consente di eseguire il controllo sui file contenuti in file archivio autoestraenti, che in genere si presentano con un'estensione .exe.

Eseguibili compressi: i file eseguibili compressi (a differenza dei file di archivio standard) vengono decompressi in memoria, in aggiunta agli eseguibili statici standard (UPX, yoda, ASPack, FGS e così via).



4.1.5.2 Opzioni

Nella sezione **Opzioni** l'utente può selezionare i metodi da utilizzare per il controllo del sistema alla ricerca di malware.. Sono disponibili le seguenti opzioni:



Firme: le firme consentono di rilevare e identificare in modo esatto e affidabile il malware in base al relativo nome, utilizzando le firme antivirali.

Euristica: Euristica è un algoritmo che analizza le attività (dannose) dei programmi. Il vantaggio principale del rilevamento euristico consiste nella possibilità di rilevare nuovo software dannoso che in precedenza non esisteva o che non era incluso nell'elenco dei virus conosciuti (database di firme antivirali).

Euristica avanzata: Euristica avanzata comprende un algoritmo di euristica esclusivo sviluppato da ESET e ottimizzato per il rilevamento di worm e trojan horse scritto in linguaggi di programmazione di alto livello. Grazie alle funzioni di euristica avanzata, la capacità di rilevamento del programma è decisamente maggiore.

Adware/Spyware/Riskware: questa categoria comprende software che raccoglie informazioni riservate sugli utenti senza il loro consenso e comprende anche il software che visualizza pubblicità.

Applicazioni potenzialmente pericolose: Applicazioni potenzialmente pericolose è la classificazione utilizzata per software commerciale legittimo. Comprende programmi quali strumenti di accesso remoto e, per questo motivo, questa opzione è disattivata nella configurazione predefinita.

Applicazioni potenzialmente indesiderate: per Applicazioni potenzialmente indesiderate non si intendono applicazioni necessariamente dannose, ma in grado di influire in modo negativo sulle prestazioni del computer. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se sono presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. I cambiamenti più significativi comprendono finestre popup indesiderate, attivazione ed esecuzione di processi nascosti, aumento dell'utilizzo delle risorse di sistema, modifiche dei risultati delle ricerche e applicazioni che comunicano con server remoti.

4.1.5.3 Pulizia

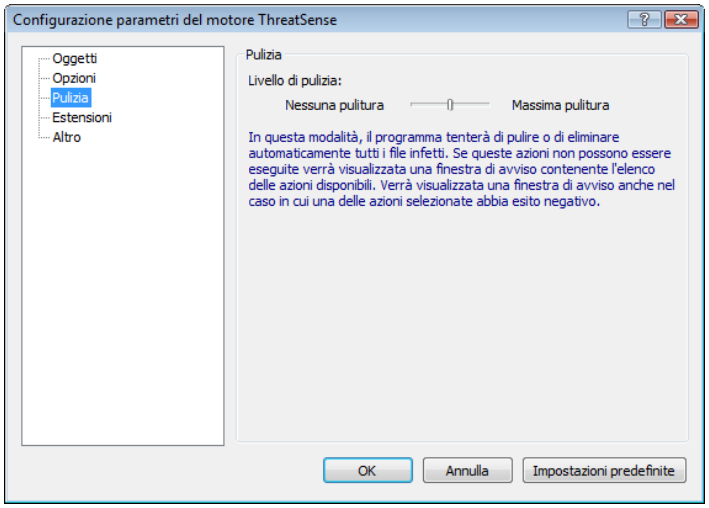
Le impostazioni di disinfezione determinano il comportamento dello scanner durante la disinfezione di file infetti. Sono disponibili 3 livelli di disinfezione:

Nessuna pulitura
I file infetti non vengono puliti automaticamente. Viene invece visualizzata una finestra di avviso per consentire all'utente di scegliere un'azione.

Livello predefinito
Il programma tenta di pulire o eliminare automaticamente i file infetti. Se non è possibile selezionare automaticamente l'azione corretta, il programma proporrà una serie di azioni. La scelta tra queste azioni viene visualizzata anche nel caso in cui non possa essere completata un'azione predefinita.

Massima pulitura
Il programma pulisce o elimina tutti i file infetti (compresi gli archivi). Le uniche eccezioni sono rappresentate dai file di sistema. Quando non è possibile pulirli, viene visualizzata una finestra di avviso con la possibilità di intraprendere un'azione.

Avvertenza:
Nella modalità predefinita viene eliminato l'intero file di archivio solo se tutti i file che contiene sono infetti. Se contiene anche file non infetti, l'archivio non verrà eliminato. Se viene rilevato un file di archivio infetto nella modalità Massima pulitura, verrà eliminato l'intero file, anche se sono presenti file puliti.



4.1.5.4 Estensioni

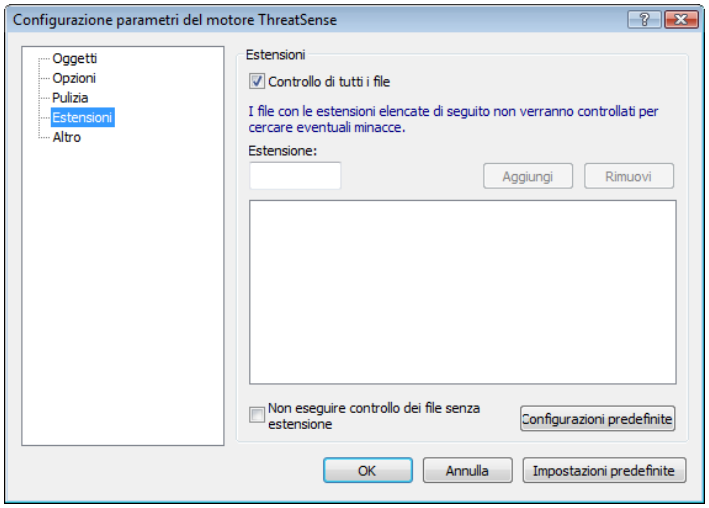
Un'estensione è la parte di nome del file delimitata da un punto. L'estensione definisce il tipo e il contenuto del file. Questa sezione delle impostazioni parametri ThreatSense consente di definire i tipi di file da controllare.

Per impostazione predefinita, tutti i file vengono controllati indipendentemente dall'estensione. È possibile aggiungere qualunque estensione all'elenco dei file esclusi dal controllo. Se la casella **Controllo di**

tutti i file è deselezionata, l'elenco viene modificato in modo da visualizzare le estensioni dei file controllati. I pulsanti **Aggiungi** e **Rimuovi** consentono di attivare o impedire il controllo delle estensioni desiderate.

Per attivare il controllo dei file senza estensione, scegliere l'opzione **Controlla file senza estensione**.

L'esclusione di file dal controllo è utile nel caso in cui il controllo di determinati tipi di file causi operazioni non corrette nel programma che utilizza le estensioni. Ad esempio, è consigliabile escludere le estensioni .edb, .eml e .tmp durante l'utilizzo di MS Exchange Server.



4.1.6 Rilevamento di un'infiltrazione

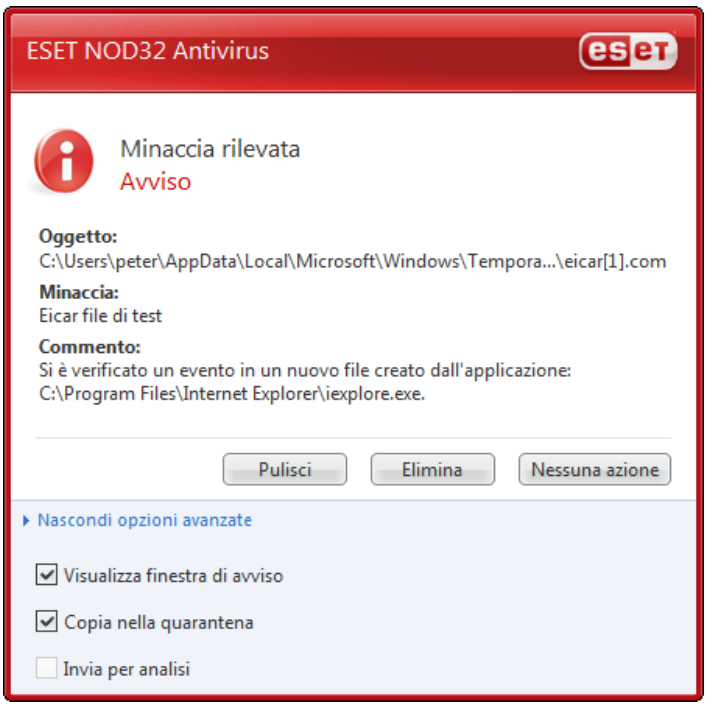
Il malware può raggiungere il sistema utilizzando veicoli diversi: pagine Web, cartelle condivise, messaggi email o periferiche rimovibili (USB, dischi esterni, CD, DVD, dischetti e così via).

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

- **Avviare ESET NOD32 Antivirus e scegliere Controllo computer.**
- **Fare clic sul pulsante Controllo standard (per ulteriori informazioni, vedere Controllo standard).**
- **Al termine del controllo, consultare nel rapporto il numero di file sottoposti a controllo, file infetti e file puliti.**

Se si desidera effettuare il controllo solo di una parte del disco, scegliere **Controllo personalizzato** e selezionare le destinazioni da controllare alla ricerca di virus.

Per un esempio di come ESET NOD32 Antivirus gestisca il malware, si supponga che il monitor del file system in tempo reale, che utilizza il livello di disinfezione predefinito, rilevi un'infiltrazione. Verrà eseguito il tentativo di pulire o eliminare il file. In assenza di azioni predefinite nel modulo di protezione in tempo reale, verrà chiesto all'utente di selezionare un'opzione in una finestra di avviso. Le opzioni in genere disponibili sono **Pulisci**, **Elimina** e **Nessuna azione**. Non è consigliabile selezionare **Nessuna azione**, perché con tale opzione si lasciano i file infetti inalterati. È opportuno selezionare questa opzione solo quando si è certi che il file non è pericoloso e che si tratta di un errore di rilevamento.



Pulizia ed eliminazione
Applicare la pulizia nel caso in cui un file pulito sia stato attaccato da un virus che ha aggiunto al file pulito del codice dannoso. In tal caso, tentare prima di pulire il file infetto per ripristinarne lo stato originale. Se il file è costituito 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 (in genere dopo il riavvio del sistema).

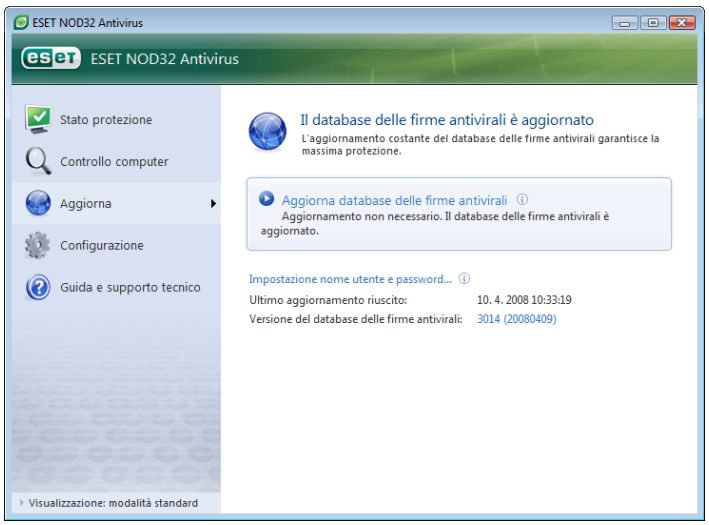
Eliminazione dei file negli archivi
In modalità di pulizia predefinita, l'intero archivio viene eliminato solo quando contiene tutti file infetti, senza alcun file pulito. In pratica gli archivi non vengono eliminati quando contengono anche file puliti non dannosi. È tuttavia consigliabile essere prudenti durante l'esecuzione di un controllo di tipo Massima pulitura, poiché in questa modalità l'archivio viene eliminato anche se contiene un solo file infetto, indipendentemente dallo stato degli altri file dell'archivio.

4.2 Aggiornamento del programma

L'aggiornamento periodico del sistema rappresenta un punto fondamentale per ottenere il massimo livello di protezione garantito da ESET NOD32 Antivirus. Il Modulo di aggiornamento assicura che il programma sia sempre aggiornato. Questo risultato si ottiene in due modi: aggiornando il database di firme antivirali e aggiornando tutti i componenti del sistema.

È possibile visualizzare alcune informazioni sullo stato corrente degli aggiornamenti facendo clic su **Aggiorna**, tra cui la versione del database delle firme antivirali e l'eventuale necessità di un aggiornamento. Sono inoltre disponibili l'opzione che consente di attivare il processo di aggiornamento immediatamente, **Aggiorna database delle firme antivirali**, e le opzioni per la configurazione dell'aggiornamento di base, come il nome utente e la password per i server di aggiornamento di ESET.

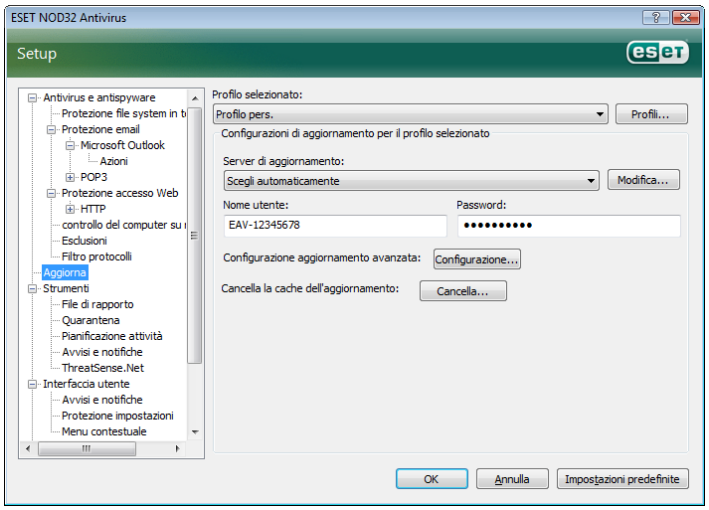
La finestra delle informazioni contiene anche ulteriori dettagli, quali la data e l'ora dell'ultimo aggiornamento eseguito correttamente e il numero del database di firme antivirali. Questa indicazione numerica è un collegamento attivo al sito Web di ESET, in cui vengono riportate tutte le firme aggiunte nel corso dell'aggiornamento in questione.



NOTA: il nome utente e la password vengono forniti da ESET dopo l'acquisto di ESET NOD32 Antivirus.

4.2.1 Configurazione dell'aggiornamento

La sezione di configurazione dell'aggiornamento consente di specificare informazioni sull'origine dell'aggiornamento, come i server di aggiornamento e i dati per l'autenticazione presso tali server. Per impostazione predefinita, il campo **Server di aggiornamento:** è impostato su **Scegli automaticamente**. Questo valore garantisce che i file di aggiornamento vengano scaricati automaticamente dal server ESET con meno traffico di rete. Le opzioni di configurazione dell'aggiornamento sono disponibili nella struttura Configurazione avanzata (F5), sotto **Aggiorna**.



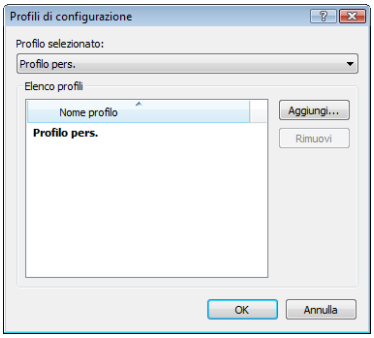
L'elenco dei server di aggiornamento esistenti è accessibile tramite il menu a discesa in **Server di aggiornamento.** Per aggiungere un nuovo server di aggiornamento, scegliere **Modifica** nella sezione **Configurazioni di aggiornamento per il profilo selezionato** e quindi fare clic sul pulsante **Aggiungi**.

L'autenticazione per i server di aggiornamento è garantita da **Nome utente** e **Password** che vengono generati e inviati all'utente da ESET dopo l'acquisto della licenza del prodotto.

4.2.1.1 Profili di aggiornamento

Per diverse configurazioni di aggiornamento, è possibile creare profili di aggiornamento definiti dall'utente, da utilizzare per determinate attività di aggiornamento. La creazione di diversi profili di aggiornamento è particolarmente utile per gli utenti mobili, per i quali le proprietà di connessione a Internet cambiano regolarmente. Se si modifica l'attività di aggiornamento, gli utenti mobili possono specificare che, quando non è possibile aggiornare il programma utilizzando la configurazione specificata in **Profilo personale**, l'aggiornamento deve essere eseguito utilizzando un profilo alternativo.

Nel menu a discesa **Profilo selezionato** viene visualizzato il profilo selezionato. Nella configurazione predefinita, questa opzione è impostata su **Profilo personale**. Per creare un nuovo profilo, fare clic sul pulsante **Profili**, quindi sul pulsante **Aggiungi** e immettere il proprio **Nome profilo**. Quando si crea un nuovo profilo, è possibile copiare le impostazioni da un profilo esistente selezionandolo dal menu a discesa **Copia impostazioni da profilo**.



Durante l'impostazione del profilo, è possibile specificare il server di aggiornamento a cui il programma si connetterà e da cui scaricherà gli aggiornamenti; è possibile utilizzare qualsiasi server dell'elenco di server disponibili oppure aggiungere un nuovo server. L'elenco dei server di aggiornamento esistenti è accessibile tramite il menu a discesa in **Server di aggiornamento**. Per aggiungere un nuovo server di aggiornamento, scegliere **Modifica** nella sezione **Configurazioni di aggiornamento per il profilo selezionato** e fare clic sul pulsante **Aggiungi**.

4.2.1.2 Configurazione aggiornamento avanzata

Per visualizzare **Configurazione aggiornamento avanzata**, fare clic sul pulsante **Configurazione**. Nella configurazione aggiornamento avanzata è possibile impostare **Modalità di aggiornamento, Proxy HTTP, LAN** e **Mirror**.

4.2.1.2.1 Modalità di aggiornamento

Nella scheda **Modalità di aggiornamento** sono disponibili le opzioni relative all'aggiornamento dei componenti del programma.

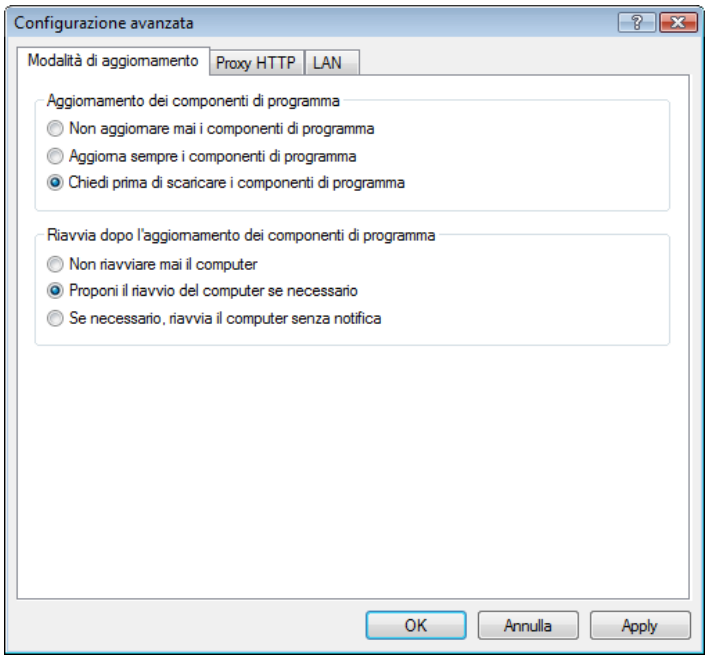
Nella sezione **Aggiornamento dei componenti di programma** sono disponibili tre opzioni:

- **Non aggiornare mai i componenti di programma**
- **Aggiorna sempre i componenti di programma**
- **Chiedi prima di scaricare i componenti di programma**

La selezione dell'opzione **Non aggiornare mai i componenti di programma** garantisce che non verrà scaricato alcun nuovo aggiornamento dei componenti di programma rilasciato da ESET e che non verrà eseguito alcun aggiornamento dei componenti di programma sulla workstation specificata. La selezione dell'opzione **Aggiorna sempre i componenti di programma** implica che gli aggiornamenti dei componenti di programma verranno eseguiti ogni volta che sui server di aggiornamento ESET è disponibile un nuovo aggiornamento e che i componenti di programma verranno aggiornati alla versione scaricata.

La selezione della terza opzione, **Chiedi prima di scaricare i componenti di programma**, garantisce che nel programma verrà visualizzato un messaggio con cui si chiede all'utente di confermare il download degli aggiornamenti dei componenti di programma, quando questi saranno disponibili. In tal caso, verrà visualizzata una finestra di dialogo con informazioni sugli aggiornamenti dei componenti di programma disponibili e le opzioni che consentono di scegliere se accettare il download o rifiutarlo. In caso di conferma, gli aggiornamenti verranno scaricati e verranno installati i nuovi componenti di programma.

L'opzione predefinita per l'aggiornamento dei componenti di programma è **Chiedi prima di scaricare i componenti di programma**.



Una volta installato un aggiornamento dei componenti di programma, è necessario riavviare il sistema in modo da garantire il corretto funzionamento di tutti i moduli. La sezione **Riavvia dopo l'aggiornamento dei componenti di programma** consente di selezionare una delle tre opzioni seguenti:

- **Non riavviare mai il computer**
- **Proponi il riavvio del computer se necessario**
- **Se necessario, riavvia il computer senza notifica.**

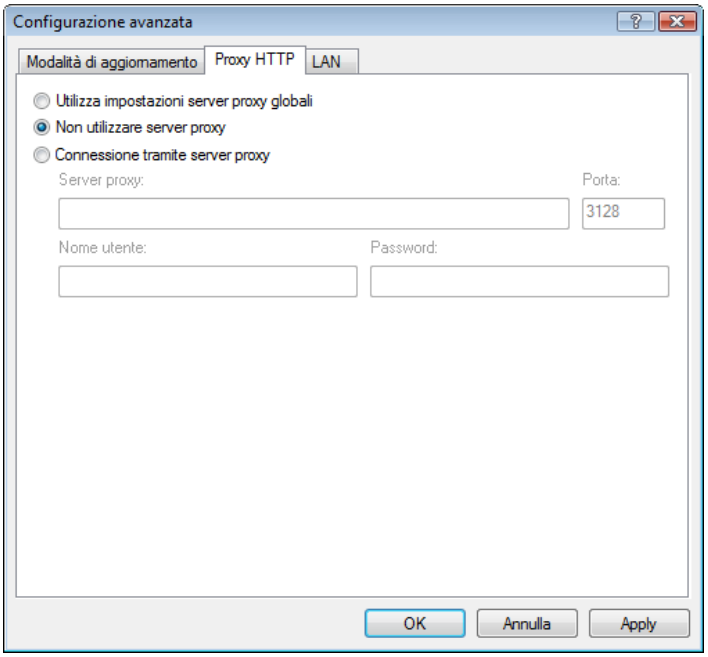
L'opzione predefinita per il riavvio è **Proponi il riavvio del computer se necessario**. La selezione delle opzioni più appropriate per gli aggiornamenti dei componenti di programma all'interno della scheda **Modalità di aggiornamento** dipende dalla workstation in uso. Esistono alcune differenze tra le workstation e i server. Il riavvio automatico del server dopo un aggiornamento di un componente di programma potrebbe, ad esempio, causare gravi danni al sistema.

4.2.1.2.2 Server proxy

Per accedere alle opzioni di configurazione del server proxy per un determinato profilo di aggiornamento: fare clic su **Aggiorna** nella sezione Configurazione avanzata (F5), quindi fare clic sul pulsante **Configurazione** alla destra di **Configurazione aggiornamento avanzata**. Scegliere la scheda **Proxy HTTP** e selezionare una delle tre opzioni seguenti:

- **Utilizza impostazioni server proxy globali**
- **Non utilizzare server proxy**
- **Connessione tramite server proxy (connessione definita dalle proprietà della connessione).**

La selezione dell'opzione **Utilizza impostazioni server proxy globali** consente di utilizzare le opzioni di configurazione del server proxy già specificate in **Varie > Server proxy** nel menu di configurazione avanzata.



Selezionare l'opzione **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** se per l'aggiornamento di ESET NOD32 Antivirus si desidera utilizzare un server proxy diverso dal server proxy specificato nelle impostazioni globali (**Varie > Server Proxy**). In tal caso, sarà necessario specificare delle informazioni aggiuntive: l'indirizzo del **server proxy**, la **porta** di comunicazione e il **nome utente** e la **password** per il server proxy, se necessario.

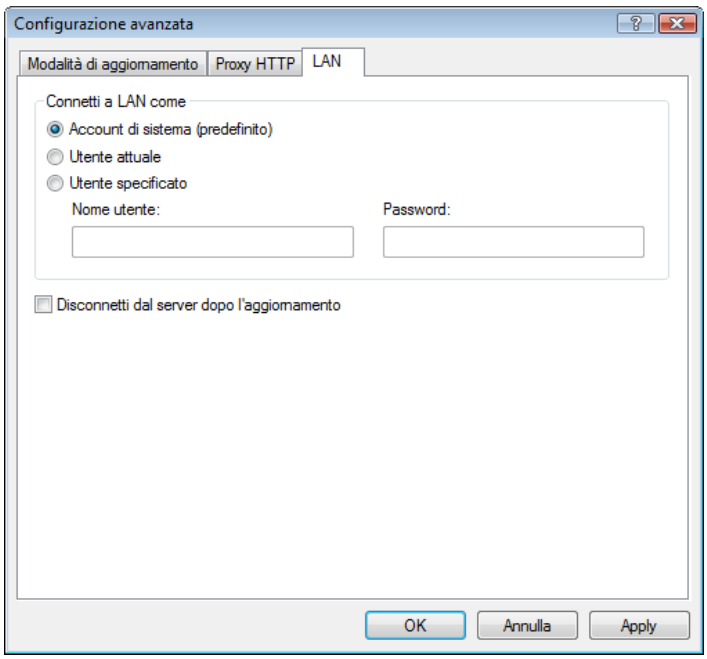
Questa opzione deve essere inoltre selezionata quando le impostazioni del server proxy non sono state impostate globalmente, ma ESET NOD32 Antivirus utilizzerà per gli aggiornamenti la connessione tramite un server proxy.

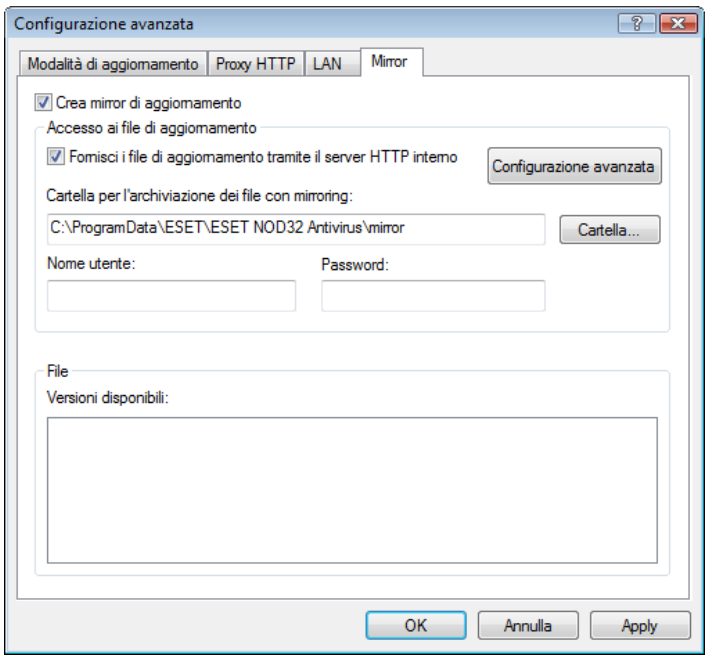
L'impostazione predefinita per il server proxy è **Utilizza impostazioni server proxy globali**.

4.2.1.2.3 Connessione alla LAN

Durante l'aggiornamento da un server locale con un sistema operativo basato su NT, nella configurazione predefinita è richiesta l'autenticazione per ciascuna connessione di rete. Nella maggior parte dei casi, un account di sistema locale non dispone di diritti di accesso sufficienti per la cartella Mirror (che contiene le copie dei file di aggiornamento). In questo caso, immettere nome utente e password nelle impostazioni dell'aggiornamento o specificare un account esistente che il programma utilizzerà per il server di aggiornamento (Mirror).

Per configurare un account di questo tipo, fare clic sulla scheda **LAN**. Nella sezione **Connetti a LAN come** sono disponibili le opzioni **Account di sistema (predefinito)**, **Utente attuale** e **Utente specificato**.





Selezionare l'opzione **Account di sistema** per utilizzare l'account di sistema per l'autenticazione. In genere se nel menu principale dell'aggiornamento non sono specificati i dati di autenticazione, non viene eseguito alcun processo di autenticazione.

Per accertarsi che il programma esegua l'autenticazione utilizzando l'account di un utente che ha eseguito l'accesso, selezionare **Utente attuale**. Lo svantaggio di questa soluzione è che, se nessun utente ha eseguito l'accesso, il programma non sarà in grado di connettersi al server di aggiornamento.

Selezionare **Utente specificato** quando si desidera che il programma utilizzi un account utente specifico per l'autenticazione.

L'opzione predefinita per la connessione alla LAN è **Account di sistema**.

Avvertenza:
Se è attivata l'opzione **Utente attuale** o l'opzione **Utente specificato**, è possibile che si verifichi un errore quando si modifica l'identità del programma per l'utente desiderato. Per questo motivo, è consigliabile immettere i dati di autenticazione della LAN nel menu principale dell'aggiornamento. In questa sezione dell'aggiornamento, i dati di autenticazione vanno immessi come segue: nome_dominio\utente (se si tratta di un gruppo di lavoro, immettere nome_gruppodilavoro\nome) e la password dell'utente. Per l'aggiornamento HTTP del server locale, non è richiesta alcuna autenticazione.

4.2.1.2.4 Creazione di copie di aggiornamento: Mirror

ESET NOD32 Antivirus Business Edition consente di creare copie di file di aggiornamento da utilizzare per aggiornare altre workstation della rete. L'aggiornamento delle workstation client da un Mirror consente di ottimizzare il bilanciamento del carico di rete e di risparmiare banda per la connessione a Internet.

Le opzioni di configurazione per il Mirror del server locale sono disponibili (dopo aver inserito una chiave di licenza valida nella gestione delle licenze, che si trova nella sezione sezione avanzata della configurazione di ESET NOD32 Antivirus Business Edition) nella sezione **Configurazione aggiornamento avanzata** (per accedere a questa sezione, premere F5 e fare clic su **Aggiorna** nella struttura Configurazione avanzata. Fare clic sul pulsante **Configurazione** accanto a **Configurazione aggiornamento avanzata**, quindi selezionare la scheda **Mirror**).

La prima operazione da eseguire per configurare il Mirror consiste nel selezionare la casella **Crea mirror di aggiornamento**. Quando si seleziona questa opzione vengono attivate altre opzioni di configurazione del Mirror, come la modalità di accesso ai file di aggiornamento e il percorso di aggiornamento per i file del mirror.

I metodi di attivazione del mirror sono descritti in dettaglio nel capitolo successivo "Varianti di accesso al mirroring". Per ora basta notare che sono disponibili due varianti di base per l'accesso al Mirror: la cartella con i file di aggiornamento può essere presentata come Mirror come cartella di rete condivisa o come Mirror come server HTTP.

La cartella dedicata alla memorizzazione dei file di aggiornamento per il Mirror è definita nella sezione **Cartella per l'archiviazione dei file con mirroring**. Fare clic su **Cartella...** per cercare la cartella desiderata sul computer locale o sulla cartella di rete condivisa. Se è necessaria l'autorizzazione per la cartella specificata, i dati di autenticazione devono essere specificati nei campi **Nome utente** e **Password**. Nome utente e Password devono essere specificati nel formato *Dominio/Utente* o *Gruppodilavoro/Utente*. È necessario specificare le password corrispondenti.

Quando si specificano i dettagli di configurazione del Mirror, l'utente può anche specificare le versioni della lingua per le quali desidera scaricare le copie di aggiornamento. L'impostazione della versione della lingua è disponibile nella sezione **File > Versioni disponibili**.

4.2.1.2.4.1 Aggiornamento dal Mirror

Sono disponibili due metodi di base per la configurazione del mirror: la cartella con i file di aggiornamento può essere presentata come Mirror di una cartella di rete condivisa o come Mirror di un server HTTP.

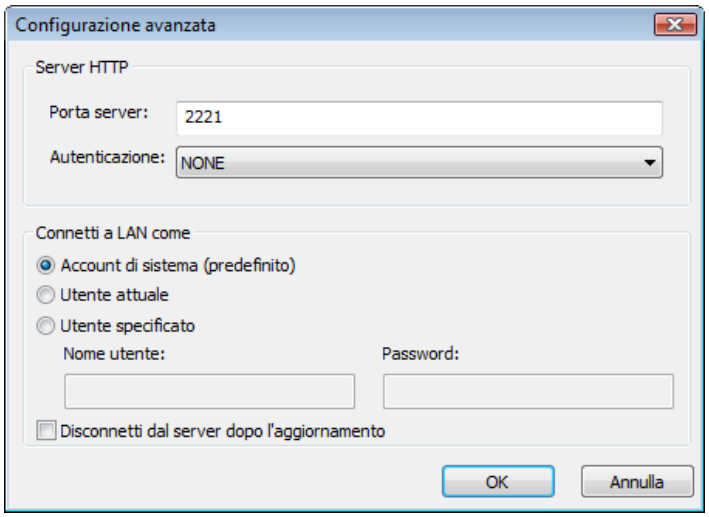
Accesso al Mirror mediante un server HTTP interno

Questa è la configurazione iniziale, specificata nelle impostazioni predefinite del programma. Per accedere al Mirror utilizzando il server HTTP, passare a **Configurazione aggiornamento avanzata** (la scheda **Mirror**) e scegliere l'opzione **Crea mirror di aggiornamento**.

Nella sezione **Configurazione avanzata** della scheda **Mirror** è possibile specificare la **Porta server** del server HTTP, oltre al tipo di **Autenticazione:** utilizzata dal server HTTP. Nella configurazione predefinita, la porta del server è impostata sul valore **2221**. Con l'opzione **Autenticazione:** si definisce il metodo di autenticazione utilizzato per l'accesso ai file di aggiornamento. Sono disponibili le seguenti opzioni: **NESSUNO, Base** e **NTLM**.

Selezionare **Base** per utilizzare la codifica base64 con l'autenticazione di base di nome utente e password. L'opzione **NTLM** consente di utilizzare un metodo di codifica sicuro. Per l'autenticazione, viene utilizzato l'utente creato sulla workstation per la condivisione dei file di aggiornamento. L'impostazione predefinita è **NESSUNO**, che consente l'accesso ai file di aggiornamento senza alcuna autenticazione.

Avvertenza:
Se si desidera consentire l'accesso ai file di aggiornamento tramite il server HTTP, la cartella Mirror deve essere posizionata sullo stesso computer dell'istanza di ESET NOD32 Antivirus che la crea.



Al termine della configurazione del Mirror, passare alle workstation e aggiungere un nuovo server di aggiornamento nel formato **http://indirizzo_IP_del_server:2221**. A tal fine, eseguire le operazioni seguenti:

- **Aprire Configurazione avanzata di ESET NOD32 Antivirus e fare clic su Aggiorna.**
- **Fare clic su Modifica alla destra del menu a discesa Server di aggiornamento e aggiungere un nuovo server utilizzando il seguente formato: http://indirizzo_IP_del_server:2221**
- **Selezionare il server appena aggiunto dall'elenco dei server di aggiornamento.**

Accesso al Mirror tramite le condivisioni del sistema

È innanzitutto necessario creare una cartella condivisa su un dispositivo locale o di rete. Durante la creazione della cartella per il Mirror, è necessario garantire l'accesso in scrittura all'utente che salverà i file di aggiornamento nella cartella e l'accesso in lettura a tutti gli utenti che aggiorneranno ESET NOD32 Antivirus dalla cartella Mirror.

Configurare quindi l'accesso al Mirror nella sezione **Configurazione aggiornamento avanzata** (scheda **Mirror**) disattivando l'opzione **Fornisci i file di aggiornamento tramite il server HTTP interno**. Questa opzione è attivata nella configurazione predefinita del pacchetto di installazione del programma.

Se la cartella condivisa è su un altro computer della rete, sarà necessario specificare i dati di autenticazione per l'accesso all'altro computer. Per specificare i dati di autenticazione, passare alla Configurazione avanzata di ESET NOD32 Antivirus e fare clic sulla sezione **Aggiorna**. Fare clic sul pulsante **Configurazione** quindi sulla scheda **LAN**. Questa impostazione è la stessa anche per l'aggiornamento, come illustrato nel capitolo "Connessione alla LAN".

Una volta completata la configurazione del Mirror, passare alle workstation e impostare \\UNC\PATH come server di aggiornamento. Questa operazione può essere effettuata come riportato di seguito:

- **Aprire la Configurazione avanzata di ESET NOD32 Antivirus e fare clic su Aggiorna.**
- **Fare clic su Modifica accanto al Server di aggiornamento e aggiungere un nuovo server utilizzando il seguente formato \\UNC\PATH.**
- **Selezionare il server appena aggiunto dall'elenco dei server di aggiornamento.**

NOTA: per un funzionamento corretto, il percorso alla cartella Mirror deve essere specificato come percorso UNC. Gli aggiornamenti dalle unità mappate potrebbero non funzionare.

4.2.1.2.4.2 Risoluzione dei problemi di aggiornamento Mirror

A seconda del metodo di accesso alla cartella Mirror, è possibile che si verifichino diversi tipi di problemi. Nella maggior parte dei casi, i problemi durante un aggiornamento da un server Mirror sono causati da uno o più dei motivi seguenti: specifica non corretta delle opzioni della cartella Mirror, autenticazione non corretta dei dati nella cartella Mirror, configurazione non corretta sulle workstation locali che tentano di scaricare i file di aggiornamento dal Mirror o una combinazione di questi motivi. Di seguito è riportata una panoramica sui più frequenti problemi che possono verificarsi durante un aggiornamento dal Mirror:

- **ESET NOD32 Antivirus riporta un errore di collegamento al server Mirror: errore probabilmente causato da una specifica non corretta del server di aggiornamento (percorso di rete alla cartella Mirror) da cui le workstation locali scaricano gli aggiornamenti. Per verificare la cartella, fare clic sul menu Start di Windows, scegliere Esegui, digitare il nome della cartella e fare clic su OK. Deve essere visualizzato il contenuto della cartella.**
- **ESET NOD32 Antivirus richiede un nome utente e una password: problema probabilmente causato dall'immissione non corretta dei dati di autenticazione (Nome utente e Password) nella sezione di aggiornamento. Nome utente e Password sono utilizzati per concedere l'accesso al server di aggiornamento da cui il programma si aggiorna. Verificare che i dati di autenticazione siano corretti e immessi nel formato appropriato. Ad esempio, *Dominio/Nome utente* o *Gruppo di lavoro/Nome utente*, più le password corrispondenti. Se il server Mirror è accessibile a "Tutti", non significa che sia garantito l'accesso a qualsiasi utente. Con "Tutti" non si intendono utenti non autorizzati, si intende solo che la cartella è accessibile a tutti gli utenti del dominio. Di conseguenza, se una cartella è accessibile a "Tutti", sarà comunque necessario specificare nella sezione di configurazione dell'aggiornamento un nome utente di dominio e una password.**
- **ESET NOD32 Antivirus riporta un errore di connessione al server Mirror: la comunicazione sulla porta definita per l'accesso alla versione HTTP del Mirror è bloccata.**

4.2.2 Come creare attività di aggiornamento

È possibile avviare gli aggiornamenti manualmente, selezionando l'opzione **Aggiorna database delle firme antivirali** nella finestra delle informazioni visualizzata dopo aver selezionato l'opzione **Aggiorna** dal menu principale**.**

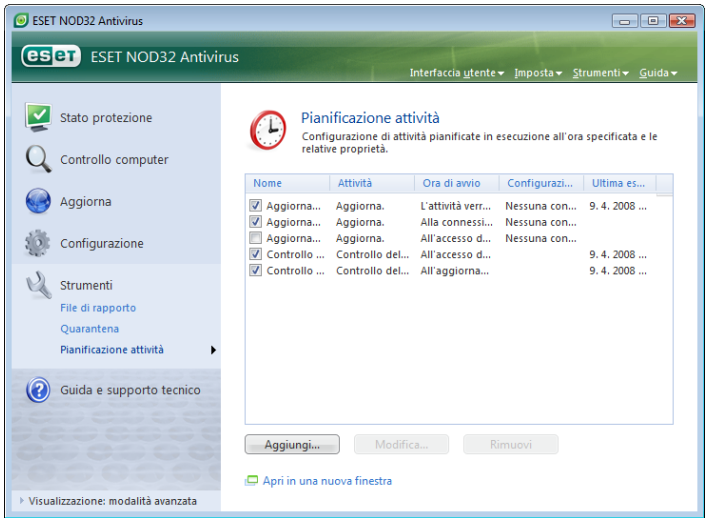
Gli aggiornamenti possono inoltre essere eseguiti come attività pianificate. Per configurare un'attività pianificata, fare clic su **Strumenti > Pianificazione attività**. Nella configurazione predefinita, di ESET NOD32 Antivirus sono attivate le seguenti attività:

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

È possibile modificare ciascuna di queste 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, vedere "Pianificazione attività".

4.3 Pianificazione attività

Lo strumento di pianificazione attività è disponibile se in ESET NOD32 Antivirus è attivata la modalità avanzata. **Pianificazione attività** è nel menu principale di ESET NOD32 Antivirus, sotto **Strumenti**. Nella pianificazione attività è disponibile un elenco di tutte le attività pianificate e delle relative impostazioni, come data, ora e profilo di controllo predefinito utilizzato.



Nella configurazione predefinita, in **Pianificazione attività** vengono visualizzate le attività pianificate seguenti:

- **Aggiornamento automatico regolare**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**
- **Controllo automatico file di avvio dopo l'accesso dell'utente**
- **Controllo automatico file di avvio dopo il completamento dell'aggiornamento del database delle firme antivirali**

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 scegliere **Modifica** o selezionare l'attività che si desidera modificare e fare clic sul pulsante **Modifica**.

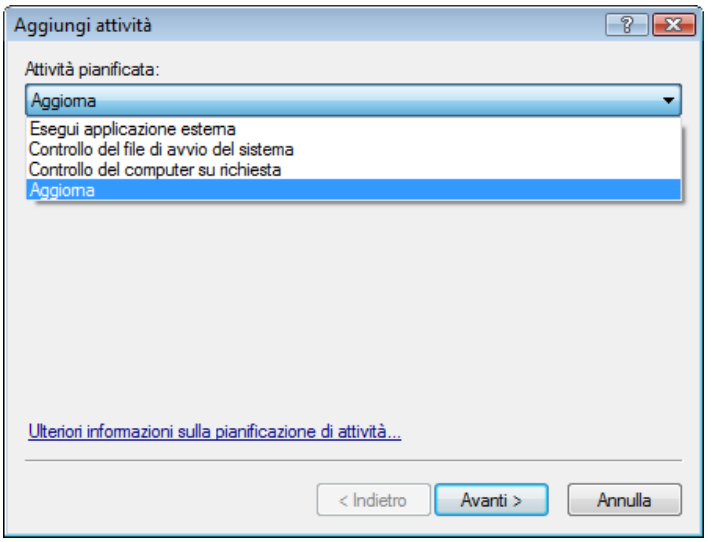
4.3.1 Scopo della pianificazione attività

La pianificazione attività consente di gestire e avviare attività pianificate con le impostazioni e le proprietà predefinite. Le impostazioni e le proprietà contengono informazioni quali la data e l'ora, oltre ai profili specificati da utilizzare durante l'esecuzione dell'attività.

4.3.2 Creazione di nuove attività

Per creare una nuova attività in Pianificazione attività, fare clic sul pulsante **Aggiungi** oppure fare clic con il pulsante destro del mouse e scegliere **Aggiungi** dal menu di scelta rapida. Sono disponibili cinque tipi di attività pianificate:

- **Esegui applicazione esterna**
- **Manutenzione rapporto**
- **Controllo del file di avvio del sistema**
- **Controllo computer su richiesta**
- **Aggiorna**



Poiché **Controllo computer su richiesta** e **Aggiorna** sono le attività pianificate utilizzate più spesso, di seguito verrà illustrato come aggiungere una nuova attività di aggiornamento.

Dal menu a discesa **Attività pianificata:** scegliere **Aggiorna**. Fare clic su **Avanti** e immettere il nome dell'attività nel campo **Nome attività:**. Selezionare la frequenza dell'attività. Sono disponibili le seguenti opzioni: **Una volta, Ripetutamente, Ogni giorno**, **Ogni settimana** e **Quando si verifica un evento**. In base alla frequenza selezionata, verrà richiesto di specificare i diversi parametri di aggiornamento. È quindi possibile definire l'azione da intraprendere se l'attività non può essere eseguita o completata nei tempi programmati. Sono disponibili le tre opzioni riportate di seguito:

- **Attendi il successivo intervallo pianificato**
- **Esegui attività appena possibile**
- **Esegui subito l'attività se il periodo trascorso dall'ultima esecuzione supera l'intervallo specificato (è possibile definire l'intervallo immediatamente utilizzando la casella di scorrimento Intervallo attività).**

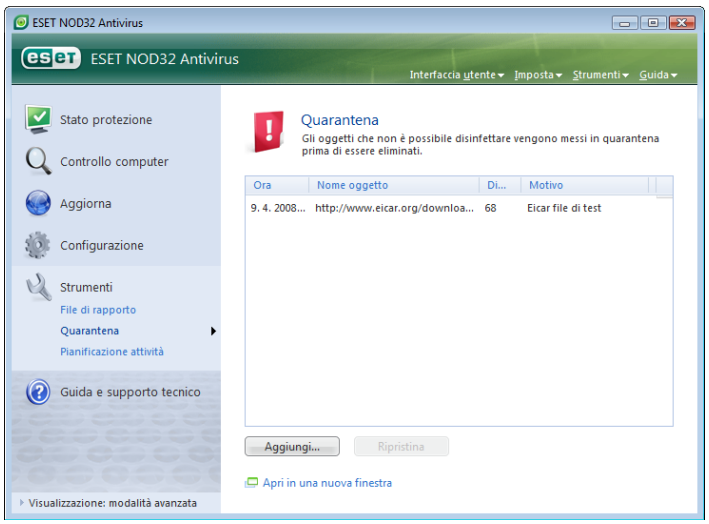
Nel passaggio successivo viene visualizzata una finestra con un rapporto completo delle attività pianificate; l'opzione Esegui attività con i parametri specificati dovrebbe essere automaticamente abilitata. Fare clic sul pulsante Fine.

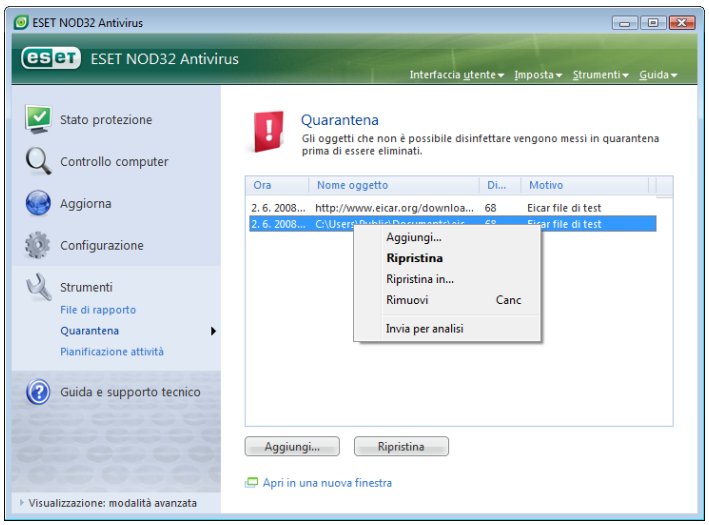
Viene visualizzata una finestra di dialogo in cui è possibile scegliere i profili da utilizzare per l'attività pianificata. Qui si può specificare un profilo principale e uno alternativo, da utilizzare nel caso in cui l'attività non possa essere completata con il profilo principale. Confermare facendo clic su OK nella finestra Aggiorna profili. La nuova attività pianificata verrà aggiunta all'elenco delle attività pianificate correnti.

4.4 Quarantena

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

L'utente può scegliere di mettere in quarantena qualsiasi tipo di file. È una procedura consigliata nel caso in cui un file si comporti in modo sospetto, ma non viene rilevato dallo scanner antivirus. I file messi in quarantena possono essere inviati ai laboratori ESET in cui si studiano i virus più recenti.





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

4.4.1 Mettere i file in quarantena

Il programma mette automaticamente in quarantena i file eliminati (se l'utente non ha annullato questa opzione nella finestra di avviso). Se necessario, è possibile mettere manualmente in quarantena i file sospetti con un clic sul pulsante **Aggiungi**. In tal caso il file originale non viene rimosso dalla posizione di origine. Per questa operazione è possibile utilizzare anche il menu contestuale. Fare clic con il pulsante destro del mouse nella finestra della quarantena e selezionare l'opzione **Aggiungi**.

4.4.2 Ripristino dalla quarantena

È possibile ripristinare nella posizione originale i file messi in quarantena. Utilizzare a tale scopo la funzione **Ripristina**, disponibile nel menu di scelta rapida visualizzato quando si fa clic con il pulsante destro del mouse sul file desiderato nella finestra di quarantena. Il menu di scelta rapida contiene anche l'opzione **Ripristina in**, che consente di ripristinare i file in una posizione diversa da quella originale da cui sono stati eliminati.

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

4.4.3 Invio di file dalla cartella Quarantena

Se si è messo in quarantena un file sospetto non rilevato dal programma oppure se un file è stato valutato erroneamente come infetto (ad esempio, da un'analisi euristica del codice) e quindi messo in quarantena, inviare il file al laboratorio ESET per lo studio dei virus. Per inviare un file dalla cartella di quarantena, fare clic sul file con il pulsante destro del mouse e selezionare **Invia per analisi** dal menu di scelta rapida.

4.5 File di rapporto

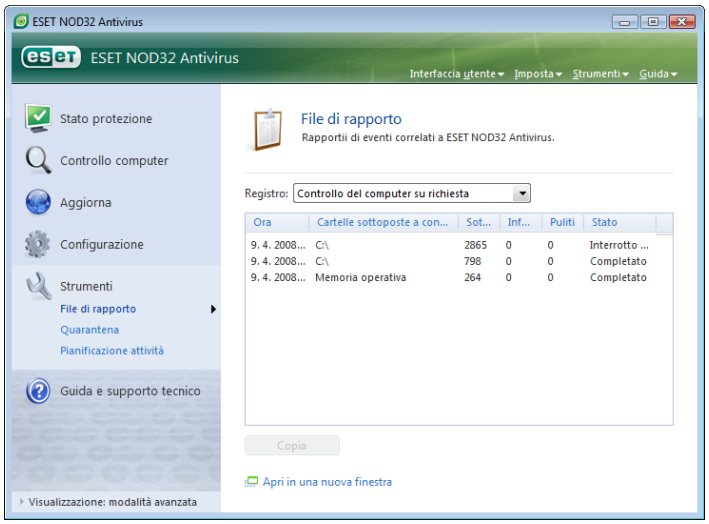
I file di rapporto contengono informazioni relative a tutti gli eventi importanti del programma che si sono verificati e forniscono una panoramica sul malware rilevato. Il rapporto rappresenta uno strumento essenziale per l'analisi del sistema, per il rilevamento delle minacce e per la risoluzione dei problemi. Il rapporto viene eseguito attivamente in background, senza che sia richiesta l'interazione 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 di ESET NOD32 Antivirus, facendo clic su **Strumenti > File di rapporto**. Selezionare il tipo di rapporto desiderato dal menu a discesa **Registro:** nella parte alta della finestra. Sono disponibili i seguenti rapporti:

1. **Minacce rilevate:** scegliere questa opzione per visualizzare tutte le informazioni sugli eventi relativi al rilevamento del malware.

2. **Eventi:** questa opzione è utile agli amministratori del sistema e agli utenti per risolvere i problemi. Tutte le azioni importanti eseguite da ESET NOD32 Antivirus vengono registrate nei registri Eventi.

3. **Controllo computer su richiesta:** in questa finestra vengono visualizzati i risultati di tutti i controlli completati. Fare doppio clic su una voce per visualizzare i dettagli del rispettivo controllo su richiesta.

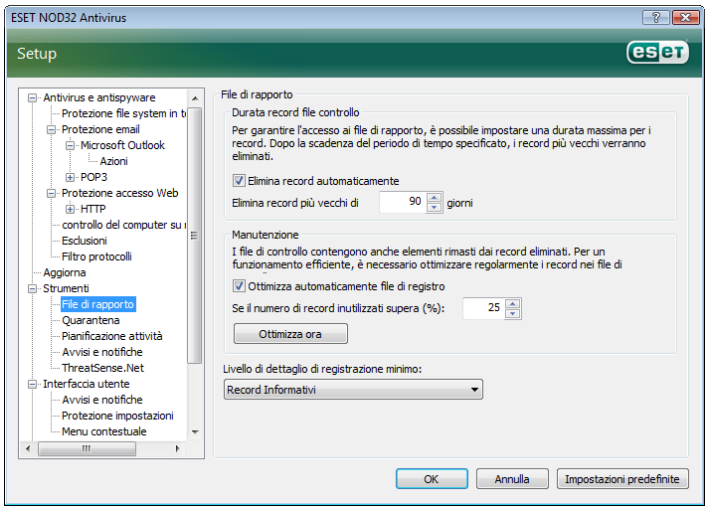


In ciascuna sezione, le informazioni visualizzate possono essere copiate direttamente negli Appunti, selezionando la voce desiderata e facendo clic sul pulsante **Copia**. Per selezionare più voci, utilizzare la combinazione di tasti CRTL e MAIUSC.

4.5.1 Manutenzione rapporto

La configurazione del rapporto di ESET NOD32 Antivirus è accessibile dalla finestra principale del programma. Fare clic su **Configurazione > Immettere struttura di impostazione avanzata completa > Strumenti > File di rapporto**. È possibile specificare le opzioni seguenti per i file di rapporto:

- **Elimina record automaticamente: le voci del registro con data precedente al numero di giorni specificato vengono automaticamente eliminate**
- **Ottimizza automaticamente file di registro: consente di abilitare la deframmentazione automatica dei file di rapporto, se viene superata la percentuale specificata di record inutilizzati**
- **Livello di dettaglio di registrazione minimo: consente di specificare il livello di dettaglio di registrazione. Opzioni disponibili:**
  - **Errori critici:** consente di registrare solo gli errori critici (errori di avvio di Protezione antivirus e così via)
  - **Errori:** consente di registrare messaggi di errore relativi al download di un file, oltre agli errori critici
  - **Allarmi:** consente di registrare errori critici, errori generici e messaggi di allarme
  - **Record informativi:** consente di registrare messaggi informativi compresi i messaggi relativi ad aggiornamenti riusciti, oltre tutti i record riportati sopra
  - **Record diagnostici:** consente di registrare le informazioni necessarie per la configurazione dettagliata del programma e di tutti i record riportati sopra



4.6 Interfaccia utente

Le opzioni di configurazione dell'interfaccia utente di ESET NOD32 Antivirus possono essere modificate in modo da impostare l'ambiente di lavoro in base alle esigenze personali. A queste opzioni di configurazione è possibile accedere dalla sezione **Interfaccia utente** della struttura di configurazione avanzata di ESET NOD32 Antivirus.

Nella sezione **Elementi dell'interfaccia utente** è possibile, se necessario, passare alla modalità avanzata. In modalità avanzata vengono visualizzate impostazioni più dettagliate e controlli aggiuntivi per ESET NOD32 Antivirus.

L'opzione **Interfaccia grafica utente** deve essere disattivata se gli elementi grafici rallentano le prestazioni del computer o causano altri problemi. Allo stesso modo, può rivelarsi necessario disattivare l'interfaccia grafica per gli utenti con problemi di vista, perché potrebbe creare conflitto con determinate applicazioni utilizzate per leggere il testo visualizzato sullo schermo.

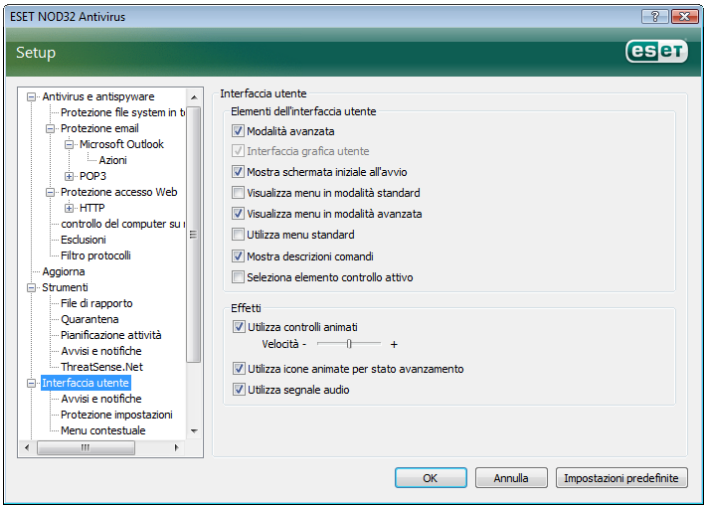
Per disattivare la schermata iniziale di ESET NOD32 Antivirus, disabilitare l'opzione **Mostra schermata iniziale all'avvio.**

Nella parte superiore della finestra principale del programma ESET NOD32 Antivirus, è presente un menu standard che può essere attivato o disattivato in base all'opzione **Utilizza menu standard**.

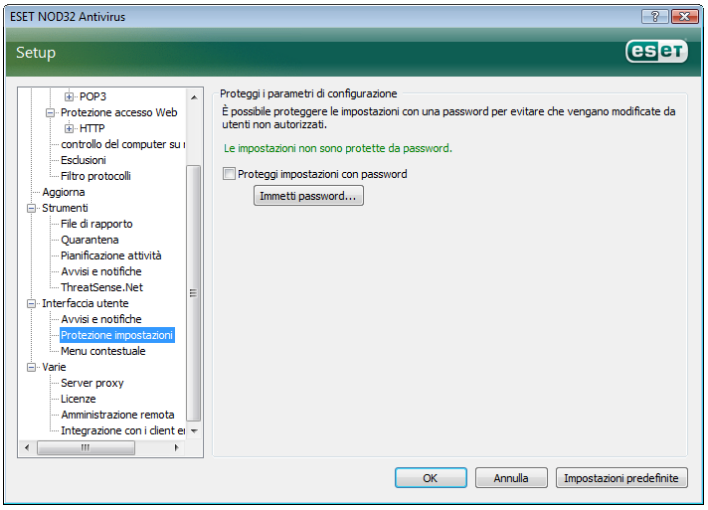
Se l'opzione **Mostra descrizioni comandi** è attivata, verrà visualizzata una breve descrizione quando si passa con il cursore sulle singole opzioni. Scegliendo l'opzione **Seleziona elemento controllo attivo**, verrà evidenziato l'elemento presente al momento nell'area attiva del cursore del mouse. L'elemento evidenziato verrà attivato con un clic del mouse.

Per ridurre o aumentare la velocità degli effetti animati, scegliere l'opzione **Utilizza controlli animati** e spostare il cursore **Velocità** a sinistra o a destra.

Per attivare l'utilizzo delle icone animate per visualizzare l'avanzamento delle diverse operazioni, selezionare la casella di controllo **Utilizza icone animate per stato avanzamento**. Per ottenere che venga riprodotto un segnale acustico di allarme in occasione di eventi importanti, scegliere l'opzione **Utilizza segnale audio**.



Le funzioni di **Interfaccia utente** comprendono anche l'opzione per proteggere la configurazione di ESET NOD32 Antivirus con una password. Questa opzione è nel sottomenu **Configurazione protezione** sotto **Interfaccia utente**. Per garantire la massima sicurezza per il sistema, è necessario configurare correttamente il programma. Qualsiasi modifica non autorizzata può provocare la perdita di dati importanti. Per impostare una password a protezione dei parametri di configurazione,, fare clic su **Immetti password**.



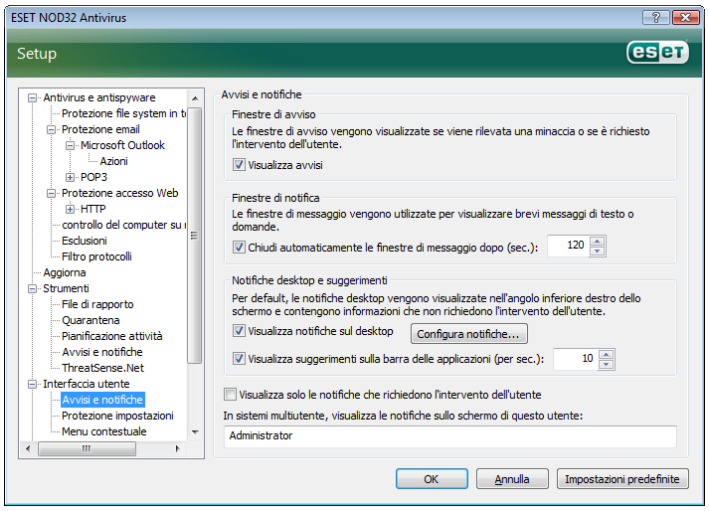
4.6.1 Avvisi e notifiche

La sezione di configurazione **Avvisi e notifiche** in **Interfaccia utente** consente di configurare la gestione dei messaggi di avviso e delle notifiche di sistema in ESET NOD32 Antivirus.

La prima voce da considerare è **Visualizza avvisi**. Se questa opzione viene disattivata, tutte le finestre di avviso vengono annullate, per cui è adatta solo a un numero limitato di particolari situazioni. Per la maggior parte dei casi, è consigliabile non modificare l'opzione predefinita (attivata).

Per chiudere automaticamente le finestre popup dopo un determinato periodo di tempo, selezionare l'opzione **Chiudi automaticamente le finestre di messaggio dopo (sec.)**. Se non vengono chiuse manualmente dall'utente, le finestre di avviso vengono chiuse automaticamente una volta trascorso il periodo di tempo specificato.

Le notifiche visualizzate sul desktop e i suggerimenti sono strumenti esclusivamente informativi, che non consentono né richiedono l'interazione dell'utente. Vengono visualizzati nell'area di notifica posta nell'angolo in basso a destra dello schermo. Per attivare la visualizzazione delle notifiche sul desktop, selezionare l'opzione **Visualizza notifiche sul desktop**. Per modificare le opzioni più dettagliate, come l'orario di in cui visualizzare la notifica e la trasparenza della finestra, fare clic sul pulsante **Configura notifiche**. Per visualizzare in anteprima il funzionamento delle notifiche, fare clic sul pulsante **Anteprima**. Per configurare la durata per cui visualizzare i dei suggerimenti, vedere l'opzione **Visualizza suggerimenti sulla barra delle applicazioni (per sec.)**.



Nella sezione inferiore della finestra di configurazione **Avvisi e notifiche** , è disponibile l'opzione **Visualizza solo le notifiche che richiedono l'intervento dell'utente**. L'opzione consente di attivare/disattivare la visualizzazione di avvisi e notifiche che non richiedono l'intervento dell'utente. L'ultima funzione di questa sezione è la possibilità di specificare gli indirizzi di notifica per un ambiente multi-utente.

Nel campo **In sistemi multiutente, visualizza le notifiche sullo schermo di questo utente:** è possibile definire l'utente che dovrà ricevere notifiche importanti da ESET NOD32 Antivirus. In genere si tratta di un amministratore di sistema o di rete. Questa opzione è utile soprattutto per i terminal server, quando tutte le notifiche di sistema vengono inviate all'amministratore.

4.7 ThreatSense.Net

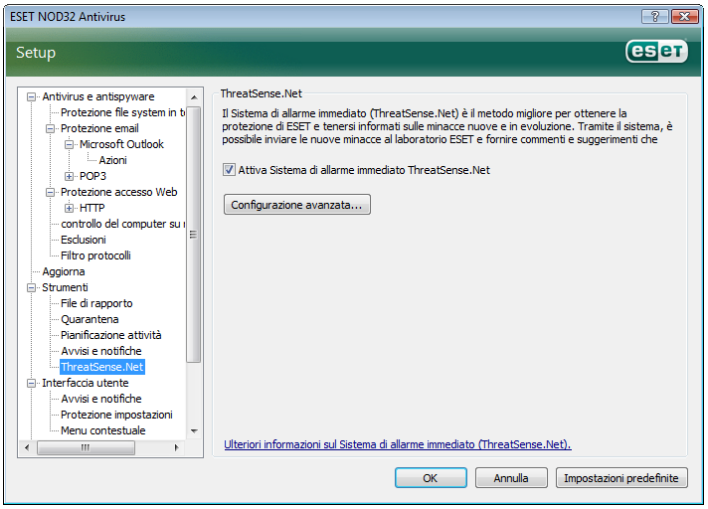
Il sistema di allarme immediato ThreatSense.Net è uno strumento che informa in modo tempestivo e continuato ESET sui nuovi malware. Il sistema di allarme immediato bidirezionale ThreatSense.Net ha un unico scopo: migliorare la protezione offerta da ESET. Il metodo migliore per garantire che le nuove minacce vengano riconosciute da ESET non appena appaiono è rappresentato dal "collegamento" con il maggior numero possibile di clienti, da utilizzare come "esploratori di minacce". Sono disponibili due opzioni:

- **È possibile decidere di non abilitare il sistema di allarme immediato ThreatSense.Net. Non si perderà alcuna funzionalità del software e si otterrà comunque la migliore protezione che ESET è in grado di offrire.**
- **È possibile configurare il sistema di allarme immediato per l'invio di informazioni sulle nuove minacce in forma anonima, laddove sia presente del nuovo codice dannoso, in un unico file. Il file può essere inviato a ESET per un'analisi dettagliata. Lo studio di queste minacce consente a ESET di migliorare le proprie capacità di rilevamento del malware. Il sistema di allarme immediato ThreatSense.Net raccoglie le informazioni sul computer degli utenti relative alle nuove minacce rilevate. Tali informazioni possono includere un campione o una copia del file in cui è contenuta il malware, il percorso del file, il nome del file, informazioni su data e ora, il processo irelativo alla la minaccia sul computer e informazioni sul sistema operativo del computer. Alcune delle informazioni possono includere dati personali sull'utente del computer, come il nome utente in un percorso di directory e così via. Di seguito è riportato un esempio delle informazioni contenute nel file inviato.**

Sebbene esista la possibilità che, occasionalmente, vengano trasmesse informazioni sull'utente o sul computer ai laboratori di ESET in cui si studiano le minacce, tali informazioni non saranno utilizzate per ALCUNO scopo diverso da quello di consentire a ESET di rispondere in modo immediato alle nuove minacce.

Nella configurazione predefinita, ESET NOD32 Antivirus è impostato per la richiesta di conferma prima di inviare file sospetti per l'analisi ai laboratori di ESET. È importante notare che file con determinate estensioni, come .doc o .xls sono sempre esclusi dall'invio, anche qualora fosse rilevata una minaccia al loro interno. È inoltre possibile aggiungere altre estensioni qualora sussistano specifici file che l'utente o l'organizzazione di cui fa parte l'utente desidera evitare di inviare.

La configurazione di ThreatSense.Net è accessibile dalla struttura di configurazione avanzata, in **Strumenti > ThreatSense.Net**. Selezionare la casella **Attiva Sistema di allarme immediato ThreatSense.Net**. Ciò consentirà di attivarlo e di fare quindi clic sul pulsante **Configurazione avanzata**.

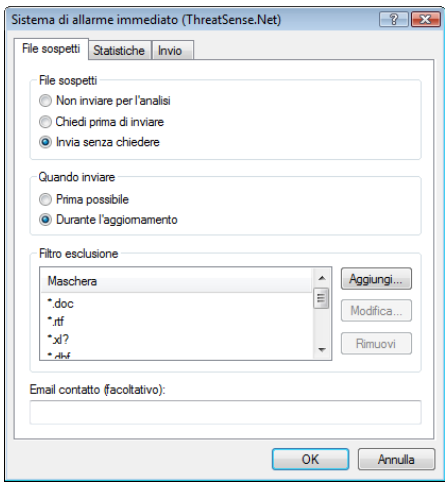


4.7.1 File sospetti

Nella scheda **File sospetti** è possibile configurare il modo in cui le minacce vengono inviate al laboratorio ESET per l'analisi.

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

L'invio dei file può essere impostato in modo da essere eseguito automaticamente, senza l'intervento dell'utente. Se si seleziona questa opzione, i file sospetti vengono inviati in background. Per conoscere i file inviati per l'analisi e confermare l'invio, selezionare l'opzione **Chiedi prima di inviare**.



Se non si desidera inviare i file, selezionare **Non inviare per l'analisi**. Se si sceglie di non inviare file per l'analisi, questa decisione non influisce sull'invio delle informazioni statistiche a ESET. Le informazioni statistiche sono configurate in una sezione a parte, descritta nel capitolo successivo.

Quando inviare
I file sospetti vengono inviati ai laboratori ESET per l'analisi appena possibile. Questa impostazione è consigliabile quando si dispone di una connessione permanente a Internet e se i file sospetti possono essere inviati in tempi brevi. L'altra opzione consiste nell'inviare i file sospetti **Durante l'aggiornamento**. Se si seleziona questa seconda opzione, i file sospetti vengono raccolti e caricati sui server del sistema di allarme immediato durante un aggiornamento.

Filtro esclusione
Non è necessario che vengano inviati per l'analisi tutti i file. L'opzione Filtro esclusione consente di escludere dall'invio determinati file e/o cartelle. È utile, ad esempio, escludere file che possono contenere informazioni potenzialmente riservate, ovvero documenti o fogli di calcolo. Nella configurazione predefinita, i tipi di file più comuni sono esclusi (Microsoft Office, OpenOffice). Se necessario, è possibile espandere l'elenco dei file esclusi.

Email contatto
L'indirizzo email per il contatto viene inviato a ESET insieme ai file sospetti e può essere utilizzato per contattare l'utente qualora fossero richieste ulteriori informazioni sui file ai fini dell'analisi. Dopo l'invio, l'utente non riceve una risposta da ESET, a meno che non siano richieste ulteriori informazioni.

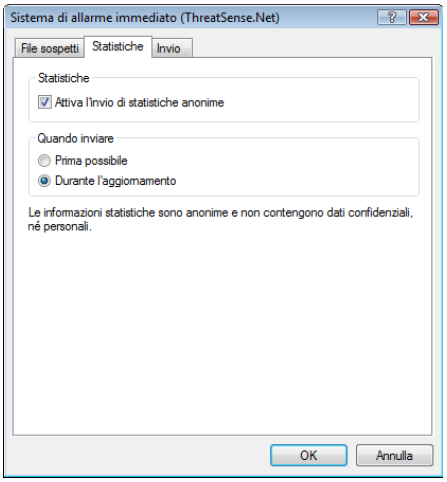
4.7.2 Statistiche

Il sistema di allarme immediato ThreatSense.Net raccoglie informazioni in forma anonima dal computer sulle nuove minacce rilevate. Le informazioni possono comprendere il nome del malware, la data e l'ora del rilevamento, la versione di ESET NOD32 Antivirus, la versione del sistema operativo in uso e le impostazioni di ubicazione. Le statistiche vengono inviate in genere ai server ESET una o due volte al giorno.

Di seguito è riportato un esempio di pacchetto delle statistiche inviato:

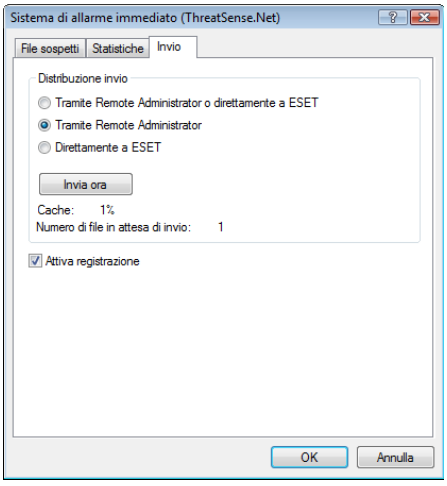
```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\
Local Settings\Temporary Internet Files\Content.IE5\
C14J8NS7\rdgFR1463[1].exe
```

Quando inviare
Nella sezione **Quando inviare** è possibile definire quando inviare le informazioni statistiche. Se si sceglie di eseguire l'invio **Prima possibile**, le informazioni statistiche verranno inviate subito dopo essere state create. Questa impostazione è adatta per chi utilizza una connessione permanente a Internet. Se si seleziona l'opzione **Durante l'aggiornamento**, le informazioni statistiche vengono salvate per essere quindi inviate tutte insieme al successivo aggiornamento.



4.7.3 Invio

In questa sezione è possibile scegliere se inviare file e informazioni statistiche tramite il Remote Administrator di ESET o direttamente a ESET. Per accertarsi che le informazioni statistiche e i file sospetti vengano recapitati a ESET, selezionare l'opzione **Tramite Remote Administrator o direttamente a ESET**. In tal modo i file e le statistiche vengono inviati con tutti gli strumenti disponibili. Impostando l'invio di file sospetti tramite il Remote Administrator, i file e le statistiche vengono inviati al server di amministrazione remota, che assicura il successivo invio ai laboratori ESET per lo studio dei virus. Se viene selezionata l'opzione **Direttamente a ESET**, tutti i file sospetti e i dati statistici vengono inviati al laboratorio ESET per lo studio dei virus direttamente dal programma.



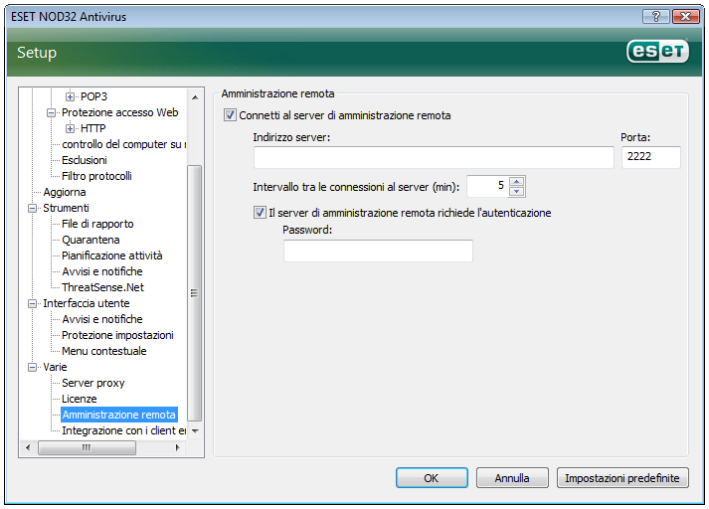
Se esistono file in attesa di invio, è possibile attivare il pulsante **Invia ora** in questa finestra. Fare clic sul pulsante per inviare immediatamente i file e i dati statistici.

Selezionare l'opzione **Attiva registrazione** per attivare la registrazione dell'invio di dati statistici e dei file.. Dopo ogni invio di file sospetto o di dati statistici, viene creata una voce nel rapporto degli eventi.

4.8 Amministrazione remota

L'amministrazione remota è uno strumento utile per la gestione dei criteri di protezione e per avere una panoramica sulla gestione globale della sicurezza all'interno della rete. È particolarmente utile quando si applica a reti di una certa estensione. L'amministrazione remota non solo garantisce un aumento del livello di sicurezza, ma è anche uno strumento facile da utilizzare per l'amministrazione di ESET NOD32 Antivirus sulle workstation client.

Le opzioni di configurazione dell'amministrazione remota sono disponibili nella schermata principale di ESET NOD32 Antivirus. Fare clic su **Configurazione > Immettere struttura di impostazione avanzata completa > Varie > Amministrazione remota**.



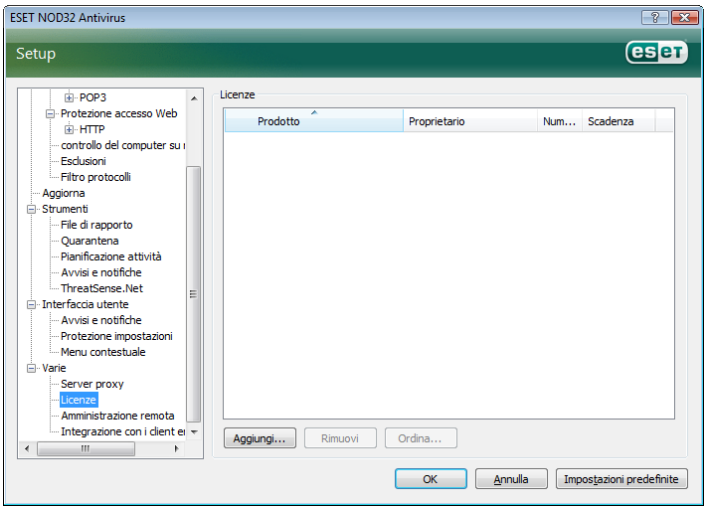
Nella finestra Configurazione è possibile attivare la modalità di amministrazione remota, selezionando la casella **Connetti al server di amministrazione remota**. È possibile quindi accedere alle altre opzioni descritte di seguito:

- **Indirizzo server: l'indirizzo di rete del server su cui è installato il server di amministrazione remota.**
- **Porta: questo campo contiene la porta server predefinita utilizzata per la connessione. È consigliabile conservare l'impostazione predefinita della porta su 2222.**
- **Intervallo tra le connessioni al server (min): indica la frequenza con cui ESET NOD32 Antivirus si connette al server ERA per inviare i dati. In altri termini, le informazioni vengono inviate in base agli intervalli di tempo definiti in questo campo. Se il valore impostato è 0, le informazioni vengono inviate ogni 5 secondi.**
- **Il server di amministrazione remota richiede l'autenticazione: consente di immettere una password per la connessione al server di amministrazione remota, se necessario.**

Scegliere **OK** per confermare le modifiche e applicare le impostazioni. ESET NOD32 Antivirus utilizza queste impostazioni per connettersi al server remoto.

4.9 Licenze

Nella sezione **Licenze** è possibile gestire le chiavi di licenza per ESET NOD32 Antivirus e altri prodotti ESET. Dopo l'acquisto, le chiavi di licenza vengono inviate insieme a Nome utente e Password. Per **aggiungere o rimuovere** una chiave di licenza, fare clic sul pulsante corrispondente della finestra di gestione delle licenze. È possibile accedere alla gestione licenze dalla struttura di configurazione avanzata in **Varie > Licenze**.



La chiave di licenza è un file di testo che contiene informazioni sul prodotto acquistato: il proprietario, il numero di licenze e la data di scadenza.

Nella finestra di gestione delle licenze è possibile caricare e visualizzare il contenuto di una chiave di licenza utilizzando il pulsante **Aggiungi**. Le informazioni contenute nella chiave vengono visualizzate nella finestra. Per eliminare i file di licenza dall'elenco, fare clic su **Rimuovi**.

Se una chiave di licenza è scaduta e si desidera acquistarne un rinnovo, fare clic sul pulsante **Ordina.** L'utente verrà reindirizzato al negozio in linea.

5. Utente avanzato

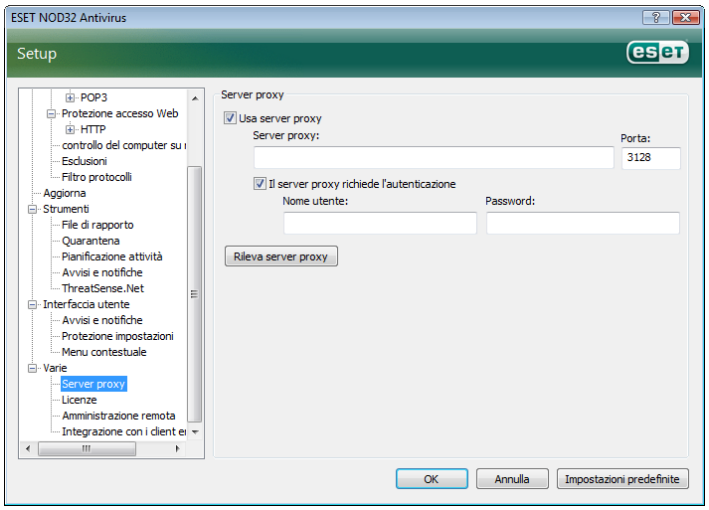
In questo capitolo vengono descritte le funzioni di ESET NOD32 Antivirus progettate per gli utenti più esperti. Alle opzioni di configurazione di queste funzioni è possibile accedere solo in modalità avanzata. Per passare alla modalità avanzata, fare clic su **Attiva/disattiva modalità avanzata** nell'angolo in basso a sinistra della finestra del programma principale oppure premere CTRL + M sulla tastiera.

5.1 Configurazione del server proxy

In ESET NOD32 Antivirus la configurazione del server proxy è disponibile in due diverse sezioni all'interno del menu di Configurazione avanzata.

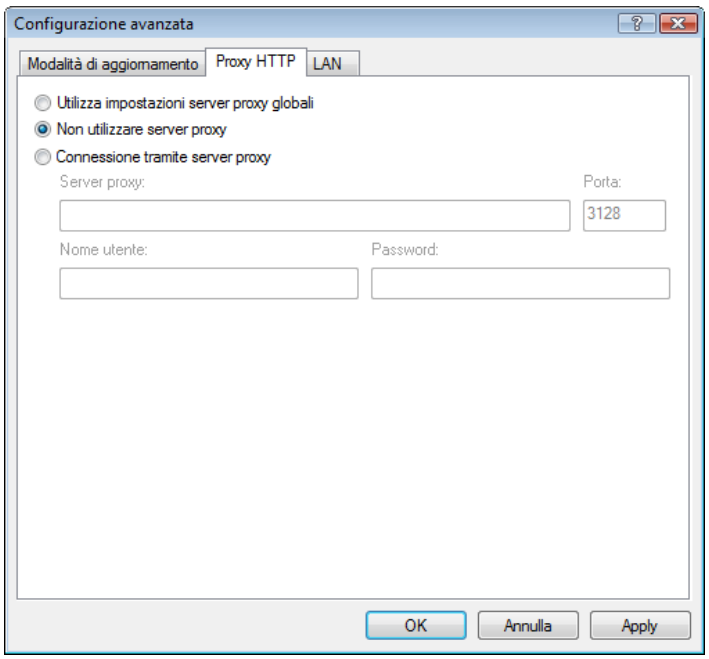
Le impostazioni del server proxy si possono configurare sotto **Varie > Server proxy**. Se si specifica il server proxy a questo livello, si definiscono globalmente le impostazioni del server proxy per l'intera applicazione ESET NOD32 Antivirus. Questi parametri vengono utilizzati da tutti i moduli che richiedono una connessione a Internet.

Per specificare le impostazioni del server proxy a questo livello, selezionare la casella **Usa server proxy**, quindi immettere 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 la casella **Il server proxy richiede l'autenticazione** e immettere **Nome utente** e **Password** validi nei rispettivi campi. Fare clic sul pulsante **Rileva server proxy** per rilevare automaticamente e immettere le impostazioni del server proxy. Verranno copiati i parametri specificati in Internet Explorer. Con questa funzione non si recuperano i dati di autenticazione (Nome utente e Password), che devono essere immessi dall'utente.

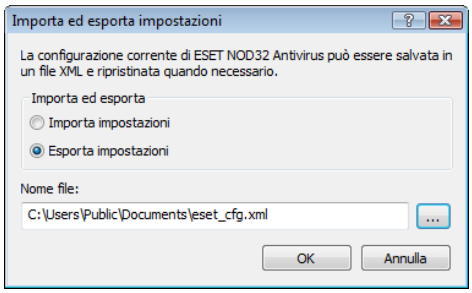
È possibile specificare le impostazioni del server proxy anche all'interno di **Configurazione aggiornamento avanzata** (sezione **Aggiorna** della struttura Configurazione avanzata). L'impostazione viene applicata al profilo di aggiornamento specificato ed è consigliata per i computer portatili, che spesso ricevono aggiornamenti delle firme antivirali da altri percorsi di rete. Per ulteriori informazioni su questa impostazione, vedere la Sezione 4.4, "Aggiornamento del sistema".



5.2 Esportazione o importazione di impostazioni

È possibile eseguire l'esportazione e l'importazione della configurazione corrente di ESET NOD32 Antivirus nella modalità avanzata sotto **Configurazione**.

Sia per l'importazione che per l'esportazione si utilizzano file .xml. Queste operazioni sono utili per eseguire una copia di backup della configurazione corrente di ESET NOD32 Antivirus da utilizzare in un secondo momento (per qualsiasi motivo). La funzione di esportazione delle impostazioni sarà apprezzata in particolare da chi desidera utilizzare la propria configurazione preferita di ESET NOD32 Antivirus su più sistemi (in cui importare il file .xml).



5.2.1 Esportazione delle impostazioni

L'esportazione della configurazione è molto semplice. Per salvare la configurazione corrente di ESET NOD32 Antivirus, fare clic su **Configurazione > Importa ed esporta impostazioni**. Selezionare l'opzione **Esporta impostazioni** e immettere il nome del file di configurazione. Scegliere il percorso sul computer in cui salvare il file di configurazione.

5.2.2 Importazione delle impostazioni

Le operazioni per l'importazione di una configurazione sono molto simili. Anche in questo caso, selezionare **Importa ed esporta impostazioni**, quindi selezionare l'opzione **Importa impostazioni**. Fare clic sul pulsante **...** e cercare il file di configurazione da importare.

5.3 Riga di comando

Il modulo antivirus di ESET NOD32 Antivirus può essere avviato da riga di comando, manualmente con il comando "ecls" oppure con un file batch ("bat").

È possibile utilizzare i parametri e le opzioni riportate di seguito quando viene eseguito un controllo su richiesta dalla riga di comando:

Opzioni generali:

- help — mostra Guida ed esci
- version — mostra informazioni sulla versione ed esci
- base-dir = CARTELLA — carica moduli da CARTELLA
- quar-dir = CARTELLA — CARTELLA quarantena
- aind — mostra indicatore di attività
- auto — esegue il controllo di tutte le unità in modalità disinfezione

Destinazioni:

- files — eseguire controllo dei file (impostazione predefinita)
- no-files — non eseguire controllo dei file
- boots — esegui controllo dei settori di avvio (impostazione predefinita)
- no-boots — non eseguire controllo dei settori di avvio
- arch — esegui controllo degli archivi (impostazione predefinita)
- no-arch — non eseguire controllo degli archivi
- max-archive-level = LIVELLO — LIVELLO di nidificazione massima degli archivi
- scan-timeout = LIMIT — eseguire controllo degli archivi al massimo per il LIMITE di secondi. Se la durata del controllo raggiunge questo limite, il controllo dell'archivio viene interrotto e si passa al file successivo
- max-arch-size=DIMENSIONE — esegui controllo solamente della dimensione dei primi byte predefinita 0 = illimitato
- mail — esegui controllo dei file di email
- no-mail — non eseguire controllo dei file di email
- sfx — eseguire controllo degli archivi autoestraenti
- no-sfx — non eseguire controllo degli archivi autoestraenti
- rtp — eseguire controllo degli eseguibili compressi
- no-rtp — non eseguire controllo degli eseguibili compressi
- exclude = CARTELLA — escludi CARTELLA dal controllo
- subdir — eseguire controllo delle sottocartelle (impostazione predefinita)
- no-subdir — non eseguire controllo delle sottocartelle
- max-subdir-level = LIVELLO — LIVELLO di nidificazione massima delle sottocartelle (valore predefinito 0 = illimitato)
- symlink — segui i collegamenti simbolici (impostazione predefinita)
- no-symlink — ignora collegamenti simbolici
- ext-remove = ESTENSIONI
- ext-exclude = ESTENSIONI — escludi dal controllo le ESTENSIONI delimitate da due punti

Metodi:

- adware — esegui controllo di Adware/Spyware/Riskware
- no-adware — non eseguire controllo di Adware/Spyware/Riskware
- unsafe — eseguire controllo delle applicazioni potenzialmente pericolose
- no-unsafe — non eseguire controllo delle applicazioni potenzialmente pericolose
- unwanted — eseguire controllo delle applicazioni potenzialmente indesiderate
- no-unwanted — non eseguire controllo delle applicazioni potenzialmente indesiderate
- pattern — utilizza le firme digitali
- no-pattern — non utilizzare le firme digitali
- heur — attivare l'euristica
- no-heur — disattiva l'euristica
- adv-heur — attiva Euristica avanzata
- no-adv-heur — disattiva Euristica avanzata

Pulizia:

- action = AZIONE — esegui AZIONE sugli oggetti infetti. Azioni disponibili: none, clean, prompt (nessuna, disinfezione, chiedi)
- quarantine — copiare i file infettati in Quarantena (integra AZIONE)
- no-quarantine — non copiare file infettati in Quarantena

Registro:

- log-file=FILE — registra output nel FILE
- log-rewrite — sovrascrivi il file di output (impostazione predefinita: aggiungi)
- log-all — registra anche file puliti
- no-log-all — non registrare file puliti (impostazione predefinita)

I codici restituiti dal controllo possono essere i seguenti:

0 – nessuna minaccia rilevata
1 – minaccia rilevata ma non pulita
10 – sono rimasti alcuni file infetti
101 – errore archivio
102 – errore accesso
103 – errore interno

NOTA:
I codici restituiti superiori a 100 indicano che non è stato eseguito il controllo del file, che potrebbe quindi essere infetto.

6. Glossario

6.1 Tipi di malware

Un malware è una parte di software dannoso che tenta di accedere e/o danneggiare il computer di un utente.

6.1.1 Virus

Un virus è un malware che danneggia i file esistenti sul computer. I virus prendono il nome dai virus biologici, poiché utilizzano tecniche simili per diffondersi da un computer all'altro.

I virus attaccano principalmente i file eseguibili e i documenti. Per replicarsi, un virus allega se stesso all'interno di un file bersaglio. In breve, un virus funziona nel seguente modo: dopo l'esecuzione del file infetto, il virus si attiva (prima dell'applicazione originale) ed esegue la sua attività predefinita. L'applicazione originale viene eseguita solo dopo questa operazione. Un virus non può infettare un computer, a meno che un utente (accidentalmente o deliberatamente) esegua o apra il programma dannoso.

I virus possono essere classificati in base a diversi livelli di attività e gravità. Alcuni sono estremamente dannosi poiché hanno la capacità di eliminare di proposito i file da un disco rigido. Altri, invece, non causano veri e propri danni, poiché il loro scopo è di infastidire l'utente e dimostrare le competenze tecniche dei rispettivi autori.

È importante sottolineare che i virus (se paragonati a trojan e spyware) stanno diventando una rarità, poiché non sono commercialmente allettanti per gli autori di software dannoso. Inoltre, il termine "virus" è spesso utilizzato in modo scorretto per indicare tutti i tipi di malware. Attualmente, questo termine è stato superato dalla nuova e più accurata definizione di "malware" (software dannoso).

Se il computer in uso è infettato da un virus, è necessario ripristinare i file infetti al loro stato originale, ovvero pulirli utilizzando un programma antivirus.

Tra i virus più noti si segnalano: OneHalf, Tenga e Yankee Doodle.

6.1.2 Worm

Un worm è un programma che contiene codice dannoso, attacca i computer ospiti e si diffonde tramite una rete. La differenza fondamentale tra un virus e un worm è che i worm hanno la capacità di replicarsi e viaggiare autonomamente. Non dipendono dai file ospite o dai settori di avvio.

I worm proliferano per mezzo di pacchetti di email o di rete. Pertanto, i worm possono essere classificati in due categorie:

- **Email: si distribuiscono autonomamente agli indirizzi email dell'elenco dei contatti dell'utente**
- **Rete: sfruttano le vulnerabilità di diverse applicazioni.**

I worm sono pertanto molto più attivi rispetto ai virus. Grazie all'ampia disponibilità di connessioni Internet, possono espandersi in tutto il mondo entro poche ore dal rilascio e, in alcuni casi, perfino entro pochi minuti. Questa capacità di replicarsi indipendentemente e rapidamente li rende molto più pericolosi rispetto ad altri tipi di malware, ad esempio i virus.

Un worm attivato in un sistema può provocare diversi inconvenienti: può eliminare file, ridurre le prestazioni del sistema e perfino disattivare alcuni programmi. La sua natura lo qualifica come "mezzo di trasporto" per altri tipi di infiltrazioni.

Se il computer è infettato da un worm, si consiglia di eliminare i file infetti poiché è probabile che contengano codice dannoso.

Tra i worm più noti si segnalano: Lovsan/Blaster, Stration/Warezov, Bagle e Netsky.

6.1.3 Trojan horse

Storicamente, i cavalli di Troia sono stati definiti come una classe di malware che tentano di presentarsi come programmi utili per ingannare gli utenti e indurli a eseguirli. Tuttavia, è importante notare che ciò era vero per i trojan horse del passato, perché oggi tali programmi non hanno più la necessità di camuffarsi. Il loro unico scopo è quello di infiltrarsi e portare a termine i loro scopi dannosi. Il termine "Trojan horse" ha assunto un'accezione molto generale, che indica un malware che non ricade in una classe specifica.

Poiché si tratta di una categoria molto ampia, è spesso suddivisa in diverse sottocategorie. Le più conosciute sono:

- **downloader: un programma dannoso in grado di scaricare altri malware da Internet.**
- **dropper: un tipo di trojan horse concepito per installare sui computer compromessi altri tipi di programmi dannosi.**
- **backdoor: un'applicazione che comunica con gli aggressori remoti, consentendo loro di ottenere l'accesso a un sistema e prenderne il controllo.**
- **keylogger (registratore delle battute dei tasti): un programma che registra ogni informazione digitata dall'utente e che invia l'informazione agli aggressori remoti.**
- **dialer: i dialer sono programmi progettati per connettersi a numeri con tariffe telefoniche molto elevate. È quasi impossibile che un utente noti che è stata creata una nuova connessione. I dialer possono causare danni solo agli utenti con connessione remota che ormai viene utilizzata sempre più di rado.**

Di solito, i trojan horse assumono la forma di file eseguibili con estensione .exe. Se sul computer in uso viene rilevato un file classificato come trojan horse, è consigliabile eliminarlo, poiché probabilmente contiene codice dannoso.

Tra i trojan horse più noti si segnalano: NetBus, Trojandownloader. Small.ZL, Slapper

6.1.4 Rootkit

I rootkit sono programmi dannosi che forniscono agli aggressori di Internet l'accesso illimitato a un sistema, nascondendo tuttavia la loro presenza. I rootkit, dopo aver effettuato l'accesso a un sistema (di norma, sfruttando una vulnerabilità del sistema), utilizzano le funzioni del sistema operativo per evitare il rilevamento da parte del software antivirus: nascondono i processi, i file e le chiavi del Registro di sistema di Windows. Per questa ragione, è quasi impossibile rilevarli utilizzando le tradizionali tecniche di test.

Per la prevenzione dei rootkit, occorre tenere presente che esistono due livelli di rilevamento:

1. Quando tentano di accedere a un sistema. Non sono ancora presenti e, pertanto, sono inattivi. La maggior parte dei sistemi antivirus è in grado di eliminare i rootkit a questo livello (presupponendo che riescano effettivamente a rilevare tali file come infetti).

2. Quando sono nascosti ai normali controlli. Il sistema antivirus ESET dispone della tecnologia Antistealth in grado di rilevare ed eliminare anche i rootkit attivi.

6.1.5 Adware

Adware è l'abbreviazione di software con supporto della pubblicità (advertising-supported software). Rientrano in questa categoria i programmi in cui viene visualizzato materiale pubblicitario. Le applicazioni adware spesso aprono automaticamente una nuova finestra popup con della pubblicità in un browser oppure modificano

la pagina iniziale. I programmi adware vengono spesso caricati insieme a programmi freeware, che consentono agli sviluppatori di coprire i costi di sviluppo delle proprie applicazioni (in genere utili).

L'adware di per sé non è pericoloso, ma gli utenti possono essere infastiditi dai messaggi pubblicitari. Il pericolo sta nel fatto che l'adware può svolgere funzioni di rilevamento e registrazione, allo stesso modo dei programmi spyware.

Se si decide di utilizzare un prodotto freeware, è opportuno prestare particolare attenzione al programma di installazione. Nei programmi di installazione viene in genere visualizzata una notifica dell'installazione di un programma adware aggiuntivo. Spesso è possibile annullarla e installare il programma senza adware. Tuttavia, in alcuni casi i programmi non vengono installati senza adware oppure le funzioni del programma risultano limitate. Ne consegue che l'adware può spesso accedere al sistema in modo "legale", perché l'utente ha in realtà acconsentito. In questi casi vale il proverbio secondo il quale la prudenza non è mai troppa.

Se sul computer in uso viene rilevato un file classificato come adware, è consigliabile eliminarlo, poiché probabilmente contiene codice dannoso.

6.1.6 Spyware

Questa categoria include tutte le applicazioni che inviano informazioni riservate senza il consenso dell'utente. Si avvalgono di funzioni di monitoraggio per inviare dati statistici di vario tipo, ad esempio l'elenco dei siti Web visitati, gli indirizzi email della rubrica dell'utente o l'elenco dei tasti digitati dall'utente.

Gli autori di spyware affermano che queste tecniche hanno l'obiettivo di raccogliere informazioni su esigenze e interessi degli utenti per l'invio di pubblicità più mirate. Il problema è che non esiste una distinzione chiara tra applicazioni utili e dannose e che nessuno può essere sicuro del fatto che le informazioni raccolte vengano utilizzate correttamente. I dati ottenuti dalle applicazioni spyware possono contenere codici di sicurezza, PIN, numeri di conti correnti bancari e così via. I programmi spyware spesso sono associati a versioni gratuite di un programma dal relativo autore, per generare profitti o offrire un incentivo all'acquisto del software. Spesso, gli utenti si accorgono della presenza di un'applicazione spyware durante l'installazione di un programma che li esorta a eseguire l'aggiornamento a una versione a pagamento.

Esempi di prodotti freeware noti che contengono programmi spyware sono le applicazioni client delle reti P2P (peer-to-peer). Spyfalcon o Spy Sheriff (e altri ancora) appartengono a una sottocategoria di spyware specifica, poiché si fanno passare per programmi antispyware ma in realtà sono essi stessi applicazioni spyware.

Se sul computer in uso viene rilevato un file classificato come spyware, è consigliabile eliminarlo, poiché probabilmente contiene codice dannoso.

6.1.7 Applicazioni potenzialmente pericolose

Esistono molti programmi sicuri, che servono a semplificare l'amministrazione dei computer in rete. Tuttavia, nelle mani sbagliate, possono essere utilizzati per scopi illegittimi. Ecco perché ESET ha creato questa particolare categoria. I clienti ESET possono scegliere se il sistema antivirus deve rilevare tali minacce o meno.

"Applicazioni potenzialmente pericolose" è la classificazione utilizzata per il software sicuro e commerciale. Questa classificazione include programmi quali gli strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano tutte le battute dei tasti premuti da un utente).

Se si rileva la presenza di un'applicazione potenzialmente pericolosa in esecuzione sul computer (che non è stata installata dall'utente) rivolgersi all'amministratore di rete o rimuovere l'applicazione.

6.1.8 Applicazioni potenzialmente indesiderate

Le applicazioni potenzialmente indesiderate non sono necessariamente dannose, tuttavia possono influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se sono presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. Le modifiche più significative sono:

- **apertura di nuove finestre mai viste in precedenza**
- **attivazione ed esecuzione di processi nascosti**
- **maggior utilizzo delle risorse del sistema**
- **modifiche nei risultati di ricerca**
- **applicazioni che comunicano con server remoti**