ESET ENDPOINT SECURITY 6

Manuale dell'utente

Microsoft® Windows® 10/8.1/8/7/Vista/XP x86 SP3/XP x64 SP2

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

ENJOY SAFER TECHNOLOGY™

ESET **ENDPOINT SECURITY 6**

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

REV. 9/3/2015

Contenuti

Contenuti

1. ESET Endpoint Security

ESET Endpoint Security 6 rappresenta un nuovo approccio a una protezione effettivamente integrata del computer. La versione più recente del motore di controllo ThreatSense®, associata ai moduli personalizzati del rapporto del Personal firewall e antispam, sfrutta la velocità e la precisione per proteggere il computer. Il risultato è un sistema intelligente che rileva continuamente attacchi e software dannosi che minacciano il computer.

ESET Endpoint Security 6 è una soluzione di protezione completa nata dall'impegno continuo basato su una combinazione tra prestazioni massime e impatto sul sistema minimo. Le tecnologie avanzate, basate sull'intelligenza artificiale, sono in grado di eliminare in modo proattivo l'infiltrazione da parte di virus, spyware, trojan horse, worm, adware, rootkit e altri attacchi Internet senza ripercussioni sulle prestazioni del sistema o interruzioni del computer.

ESET Endpoint Security 6 è progettato per essere utilizzato principalmente su workstation in ambienti aziendali o commerciali di piccole dimensioni. Grazie a un utilizzo combinato con ESET Remote Administrator, consente di gestire facilmente qualsiasi numero di workstation client, applicare criteri e regole, monitorare i rilevamenti ed eseguire la configurazione remota da qualsiasi computer collegato in rete.

1.1 Novità

L'interaccia utente grafica di ESET Endpoint Security è stata completamente rinnovata allo scopo di garantire una visibilità ottimizzata e un'esperienza utente più intuitiva. Seguono alcuni dei principali miglioramenti apportati alla versione 6 di ESET Endpoint Security:

Miglioramenti funzionali e in termini di usabilità

- Controllo Web - Consente di definire una singola regola per indirizzi URL multipli o diversi criteri per diversi percorsi di rete. I criteri di blocco "debole", insieme alla capacità di personalizzare parzialmente la pagina di blocco e di avviso, rappresentano una novità della versione 6.
- Personal firewall - È ora possibile creare regole firewall direttamente dal rapporto o dalla finestra di notifica dell'IDS e assegnare profili alle interfacce di rete.
- Una nuova protezione botnet - aiuta a individuare malware tramite l'analisi dei rispettivi modelli e protocolli di comunicazione di rete.
- Controllo dispositivi - Da oggi, è possibile stabilire il tipo e il numero di serie dei dispositivi e definire singole regole per dispositivi multipli.
- Una nuova Modalità intelligente per HIPS - posizionata tra la Modalità automatica e la Modalità interattiva. Consente di identificare le attività sospette e i processi dannosi nel sistema.
- Miglioramenti dello strumento di aggiornamento e del mirror - D'ora in poi, è possibile riprendere i download non riusciti dei database delle firme antivirali e/o dei moduli dei prodotti.
- Nuovo approccio alla gestione da remoto dei computer con ESET Remote Administrator - Possibilità di inviare nuovamente i rapporti in caso di reinstallazione o di attività di testing di ERA, installazione remota delle soluzioni di protezione ESET, panoramica dello stato di protezione dell'ambiente di rete e ordinamento dei vari dati per un utilizzo futuro.
- Miglioramenti dell'interfaccia utente - Aggiunge l'opzione "con un solo clic" per l'esecuzione di un aggiornamento manuale del database delle firme antivirali e dei moduli dalla barra delle applicazioni di Windows. Supporto per touch-screen e display ad alta risoluzione.
- Opzioni potenziate di rilevamento e rimozione delle soluzioni di protezione di terze parti.

Nuova funzionalità

- Anti-Phishing - Protegge il sistema dell'utente da tentativi di acquisizione di password e altre informazioni sensibili restringendo l'accesso a siti Web dannosi camuffati da siti legittimi.
- Potenziamenti della velocità di controllo - Utilizzo della cache locale condivisa in ambienti virtuali.

Tecnologie di rilevamento e protezione

- Velocità e affidabilità potenziate dei processi di installazione.
- Scanner memoria avanzato - Monitora il comportamento dei processi e controlla i processi dannosi smascherati nella memoria.
- Exploit Blocker migliorato - Progettato per rafforzare i tipi di applicazione comunemente utilizzati come browser Web, lettori PDF, client di posta e componenti di MS Office. Exploit blocker supporta ora Java e aiuta a migliorare il rilevamento e la protezione da questi tipi di vulnerabilità.
- Opzioni potenziate di rilevamento e rimozione dei rootkit.
- Vulnerability shield - Nuove opzione di filtraggio avanzato per il rilevamento dei vari tipi di attacchi e vulnerabilità.
- Controllo stato inattivo - Esegue un controllo silenzioso su tutti i dischi locali quando il computer si trova nello stato inattivo.

1.2 Requisiti di sistema

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

Processori supportati: Intel® o AMD x86-x64

Sistemi operativi: Microsoft® Windows® 8.1/8/7/Vista/XP SP3 32 bit/XP SP2 64 bit

1.3 Prevenzione

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

Eseguire regolarmente l'aggiornamento

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

Scaricare le patch di protezione

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

Eseguire il backup dei dati importanti

Di norma, gli autori di malware non sono interessati alle esigenze degli utenti e l'attività dei programmi dannosi comporta spesso un malfunzionamento generale del sistema operativo e la perdita di dati importanti. È importante eseguire un backup periodico dei dati importanti e sensibili su un supporto esterno, ad esempio un DVD o un'unità hard disk esterna. Ciò consente di recuperare i dati in modo semplice e veloce in caso di errore del sistema.

Eseguire regolarmente la scansione antivirus

Il rilevamento di virus, worm, trojan e rootkit più noti e sconosciuti è gestito dal modulo della protezione file system in tempo reale. Ciò significa che ad ogni accesso ad un file o apertura dello stesso da parte dell'utente, questo viene controllato per la ricerca di attività malware. Si consiglia di eseguire un Controllo del computer

completo almeno una volta al mese, in quanto le firme dei malware cambiano continuamente e il database delle firme antivirali si aggiorna con frequenza giornaliera.

Seguire le regole di protezione di base

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

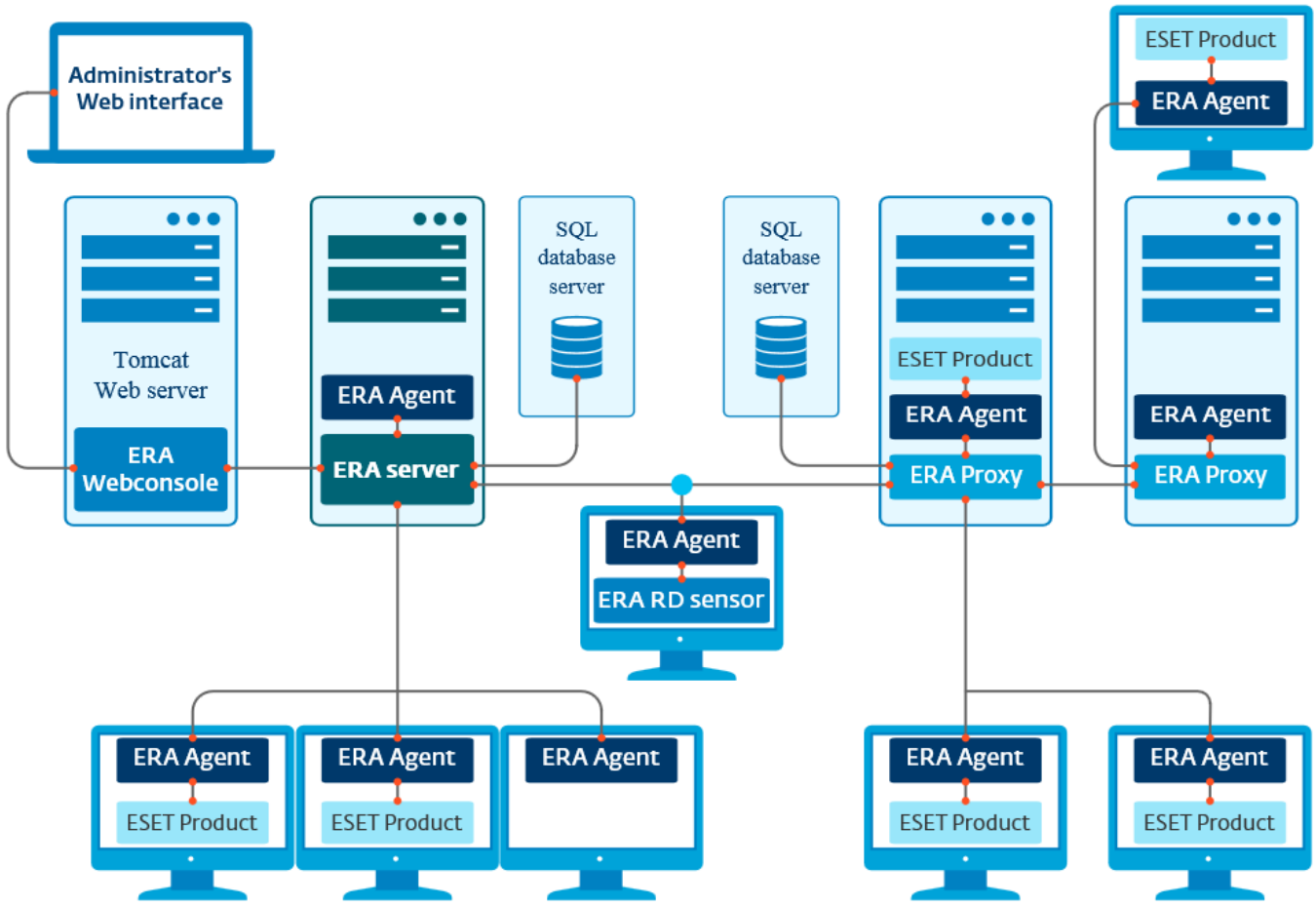
- Non visitare siti Web sospetti, con molte finestre popup e pubblicità che attirano l'attenzione.
- Prestare attenzione durante l'installazione di programmi freeware, pacchetti codec e così via. Utilizzare solo programmi sicuri e visitare solo siti Web Internet sicuri.
- Essere prudenti quando si aprono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

2. Documentazione per gli utenti connessi tramite ESET Remote Administrator

ESET Remote Administrator (ERA) è un'applicazione che consente all'utente di gestire i prodotti ESET in un ambiente di rete da una postazione centrale. Il sistema di gestione delle attività ESET Remote Administrator consente all'utente di installare soluzioni di protezione ESET su computer remoti e di rispondere rapidamente ai nuovi problemi e alle nuove minacce. ESET Remote Administrator non offre di per sé protezione contro codici dannosi, ma si affida alla presenza di una soluzione di protezione ESET su ciascun client.

Le soluzioni di protezione ESET supportano reti che includono vari tipi di piattaforme. Una rete può integrare, ad esempio, una combinazione degli attuali sistemi operativi Microsoft, Linux e Mac OS e dei sistemi operativi eseguiti sui dispositivi mobili (cellulari e tablet).

L'immagine sottostante illustra un esempio di architettura per una rete protetta mediante soluzioni di protezione ESET gestite da ERA:



NOTA: per ulteriori informazioni, consultare il Manuale dell'utente di ESET Remote Administrator.

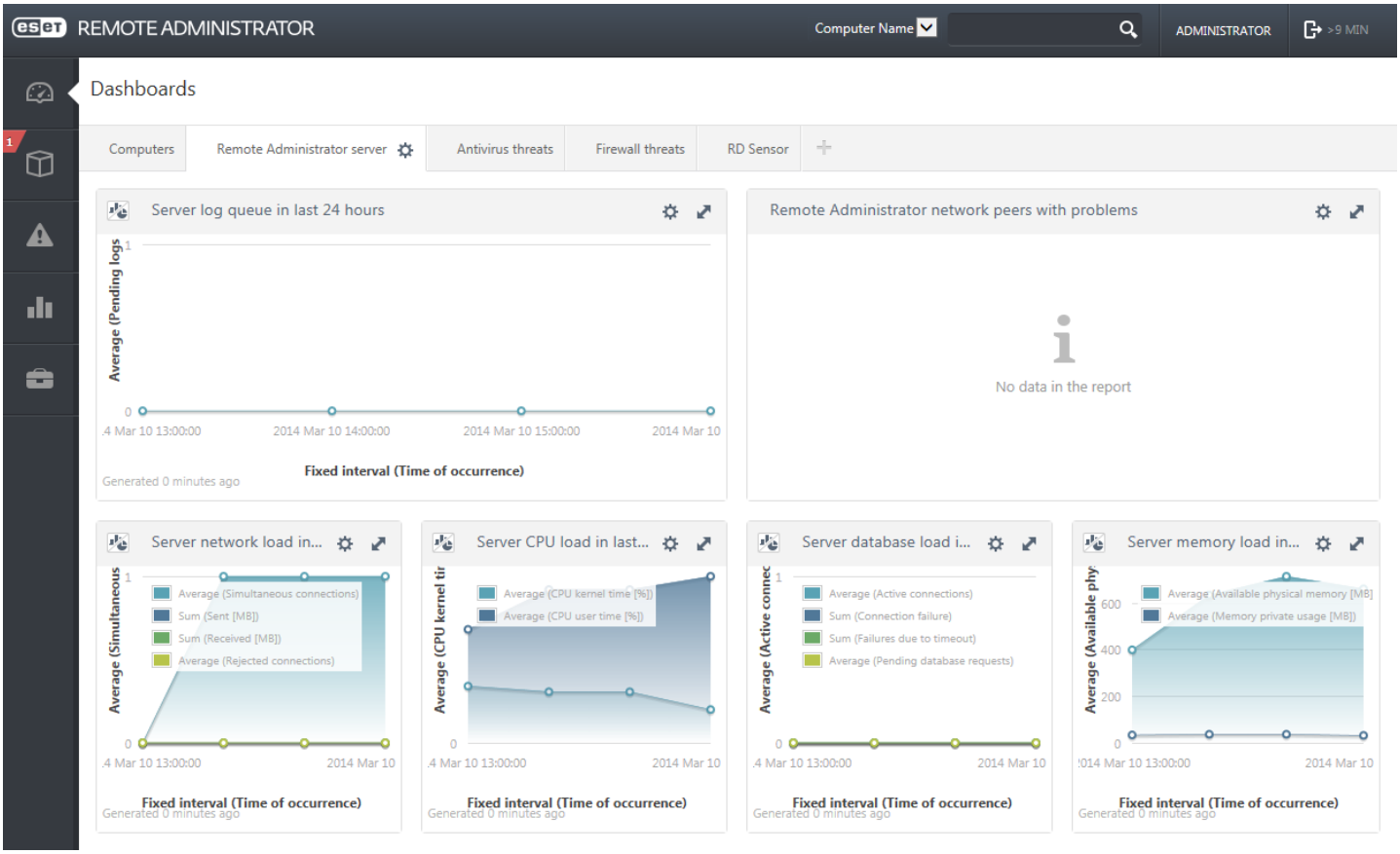
2.1 Server ESET Remote Administrator

Il **Server ESET Remote Administrator** è un componente fondamentale di ESET Remote Administrator. È l'applicazione esecutiva che elabora tutti i dati ricevuti dai client che si connettono al server (attraverso l'Agente ERA). L'agente ERA facilita le comunicazioni tra il client e il server. I dati (rapporti del client, configurazione, replica dell'agente, ecc.) sono archiviati in un database. Per una corretta elaborazione dei dati, il server ERA richiede una connessione stabile al server di un database. Per ottenere prestazioni ottimali, si consiglia di installare il server ERA e il database su server separati. È necessario configurare la macchina sulla quale è installato il server ERA in modo da accettare tutte le connessioni dell'agente, del proxy o di RD Sensor, che vengono verificate mediante l'utilizzo dei certificati. Una volta eseguita l'installazione, è possibile aprire ERA Web Console che si connette al server ERA (come illustrato nel diagramma). Dalla console Web, vengono eseguite tutte le operazioni del server ERA quando si gestiscono le soluzioni di protezione ESET dall'interno della rete.

2.2 Console Web

ERA Web Console è un'interfaccia utente basata sul Web che presenta i dati provenienti dal Server ERA e consente all'utente di gestire le soluzioni di protezione ESET nella rete in uso. È possibile accedere alla console Web tramite un browser che consente di visualizzare una panoramica dello stato dei client sulla rete e di utilizzare da remoto soluzioni ESET su computer non gestiti. È possibile decidere di rendere il server Web accessibile da Internet per consentire l'utilizzo di ESET Remote Administrator praticamente da qualsiasi posizione o dispositivo.

Il dashboard della console Web è strutturato come segue:



Nella parte superiore della console Web, è disponibile lo strumento **Ricerca rapida**. Nel menu a discesa, selezionare **Nome computer**, **Indirizzo IPv4/IPv6** o **Nome minaccia**, digitare la stringa di ricerca nel campo di testo e fare clic sul simbolo della lente di ingrandimento oppure premere **Invio** per avviare la ricerca. L'utente verrà reindirizzato alla sezione **Gruppi**, dove sarà possibile visualizzare i risultati della ricerca.

NOTA: per ulteriori informazioni, consultare il Manuale dell'utente di ESET Remote Administrator.

2.3 Proxy

Il **Proxy ERA** è un altro componente di ESET Remote Administrator che consente di soddisfare due requisiti. In reti di medie dimensioni o aziendali caratterizzate dalla presenza di numerosi client (ad esempio, 10.000 client o più), è possibile utilizzare il proxy ERA per distribuire il carico tra molteplici proxy ERA, allo scopo di facilitare i compiti del Server ERA principale. L'altro vantaggio del proxy ERA consiste nella possibilità di utilizzarlo per connettersi a una filiale aziendale da remoto con un collegamento debole. Ciò significa che l'agente ERA su ciascun client non si connette al server ERA principale direttamente attraverso il proxy ERA che si trova sulla stessa rete locale della filiale. Questa configurazione libera il collegamento alla filiale. Il proxy ERA accetta connessioni da tutti gli agenti ERA locali, ne compila i dati e li carica sul server ERA principale (o un altro proxy ERA). Tale operazione consente alla rete di adattare altri client senza compromettere le proprie prestazioni e la qualità delle query relative al database.

In base alla configurazione della rete in uso, il proxy ERA può connettersi a un altro proxy ERA per poi connettersi al server ERA principale.

Per un corretto funzionamento del proxy ERA, il computer host sul quale è stato installato il proxy ERA deve prevedere un agente ESET installato ed essere connesso al livello superiore (l'eventuale server ERA o un proxy ERA superiore) della rete in uso.

2.4 Agente

L'**Agente ERA** costituisce una parte essenziale del prodotto ESET Remote Administrator. Le soluzioni di protezione ESET sulle macchine client (ad esempio, ESET Endpoint Security) comunicano con il server ERA attraverso l'agente. Queste comunicazioni rendono possibile la gestione delle soluzioni di protezione ESET su tutti i client remoti da una posizione centrale. L'agente raccoglie informazioni dal client e le invia al server. Se il server invia un'attività a un client, ciò significa che l'attività viene inviata all'agente che comunica quindi con il client. Tutte le comunicazioni di rete avvengono tra l'agente e la parte superiore della rete ERA, ovvero il server e il proxy.

Per connettersi al server, l'agente ERA utilizza uno dei tre metodi seguenti:

1. L'agente del client è connesso direttamente al server.
2. L'agente del client è connesso mediante un proxy a sua volta connesso al server.
3. L'agente del client è connesso al server mediante proxy multipli.

L'agente ESET comunica con le soluzioni ESET installate su un client, raccoglie informazioni dai programmi installati su quel client e passa le informazioni di configurazione ricevute dal server al client.

NOTA: il proxy ESET possiede il proprio agente che gestisce tutte le attività di comunicazione tra i client, altri proxy e il server.

2.5 RD Sensor

RD (Rogue Detection) Sensor è un componente di ESET Remote Administrator pensato per ricercare computer all'interno della rete in uso. È uno strumento che consente di aggiungere in modo pratico nuovi computer in ESET Remote Administrator senza che sia necessario ricercarli e aggiungerli manualmente. Ogni computer trovato nella rete viene visualizzato nella console Web e aggiunto al gruppo predefinito **Tutti**. Da qui, è possibile eseguire ulteriori azioni con singoli computer client.

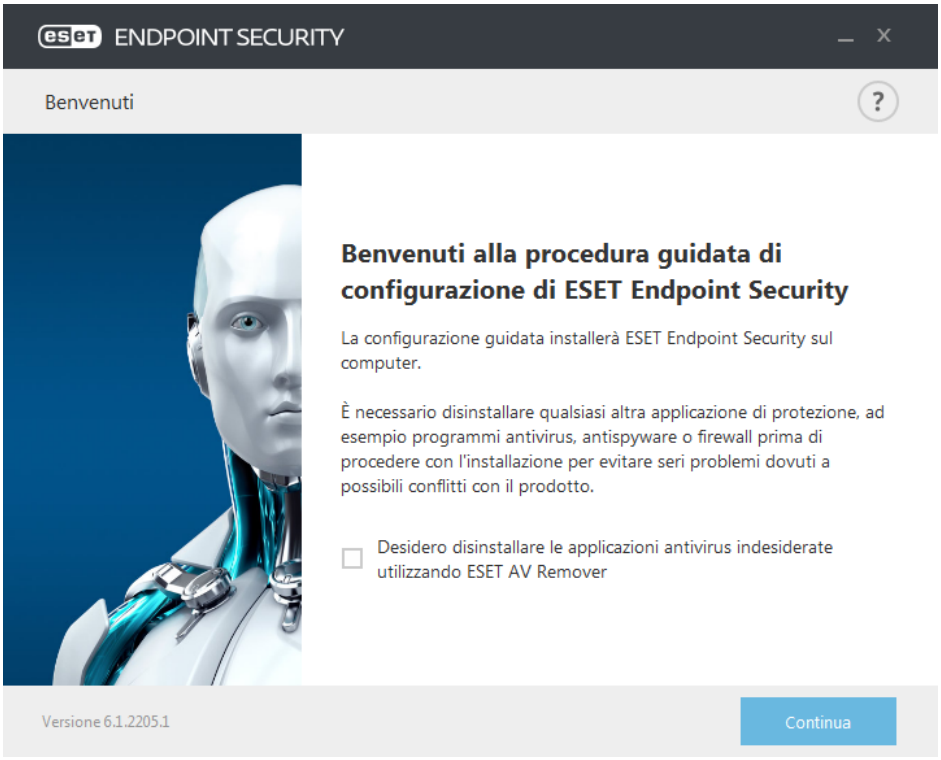
RD Sensor è un ascoltatore passivo che rileva i computer presenti nella rete e invia le relative informazioni al server ERA. Il server ERA valuta se i PC trovati nella rete sono sconosciuti o già gestiti.

3. Utilizzo autonomo di ESET Endpoint Security

Questa sezione del Manuale dell'utente è dedicata agli utenti che utilizzano ESET Endpoint Security senza ESET Remote Administrator. Tutte le caratteristiche e le funzionalità di ESET Endpoint Security sono completamente accessibili in base ai diritti dell'account dell'utente.

3.1 Installazione con ESET AV Remover

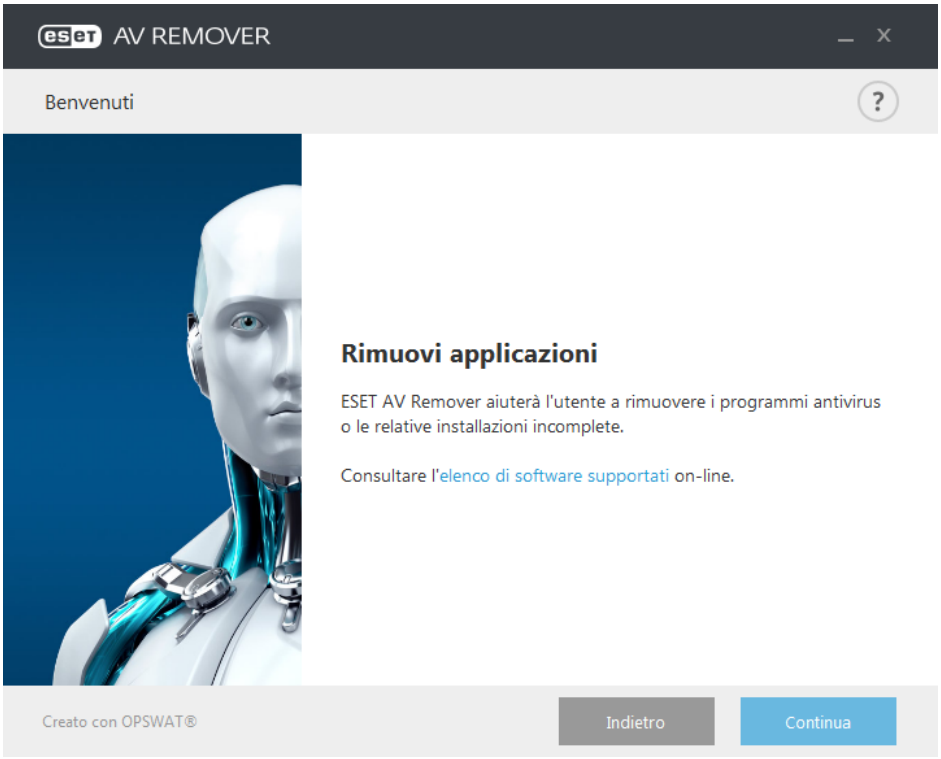
Prima di procedere con il processo di installazione, è necessario disinstallare qualsiasi altra applicazione di protezione presente sul computer. Selezionare la casella di controllo accanto a **Desidero disinstallare le applicazioni antivirus indesiderate utilizzando ESET AV Remover** per consentire a ESET AV Remover di controllare il sistema e rimuovere eventuali applicazioni di protezione supportate. Lasciare la casella di controllo deselezionata e fare clic su **Continua** per installare ESET Endpoint Security senza eseguire ESET AV Remover.



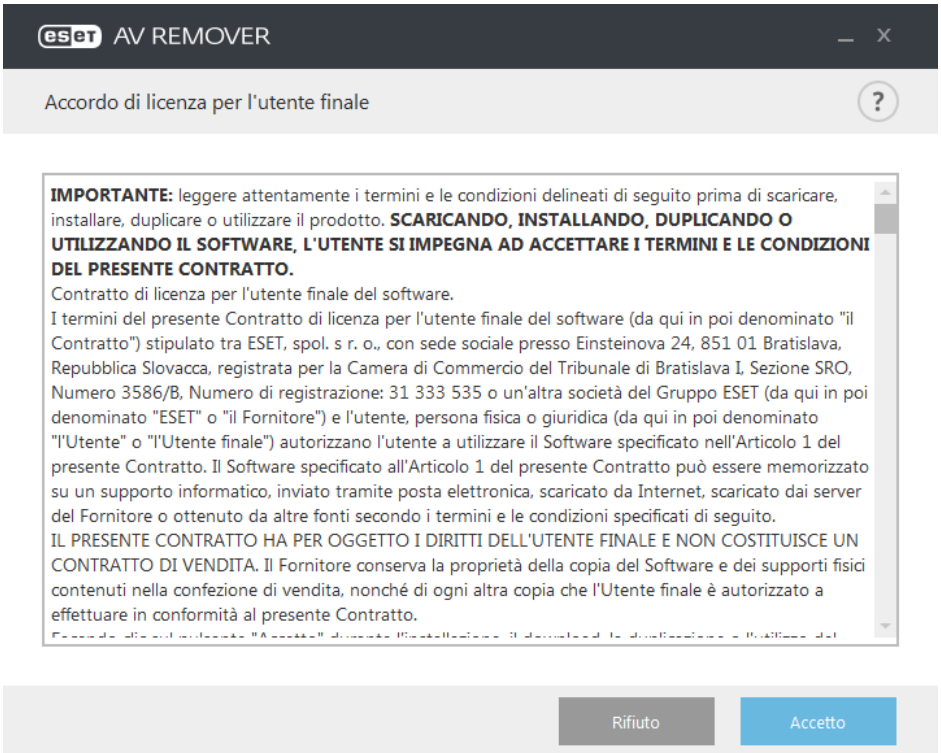
3.1.1 ESET AV Remover

ESET AV Remover è uno strumento che consente all'utente di rimuovere la maggior parte dei software antivirus precedentemente installati sul sistema. Seguire le istruzioni sottostanti per rimuovere un programma antivirus esistente utilizzando ESET AV Remover:

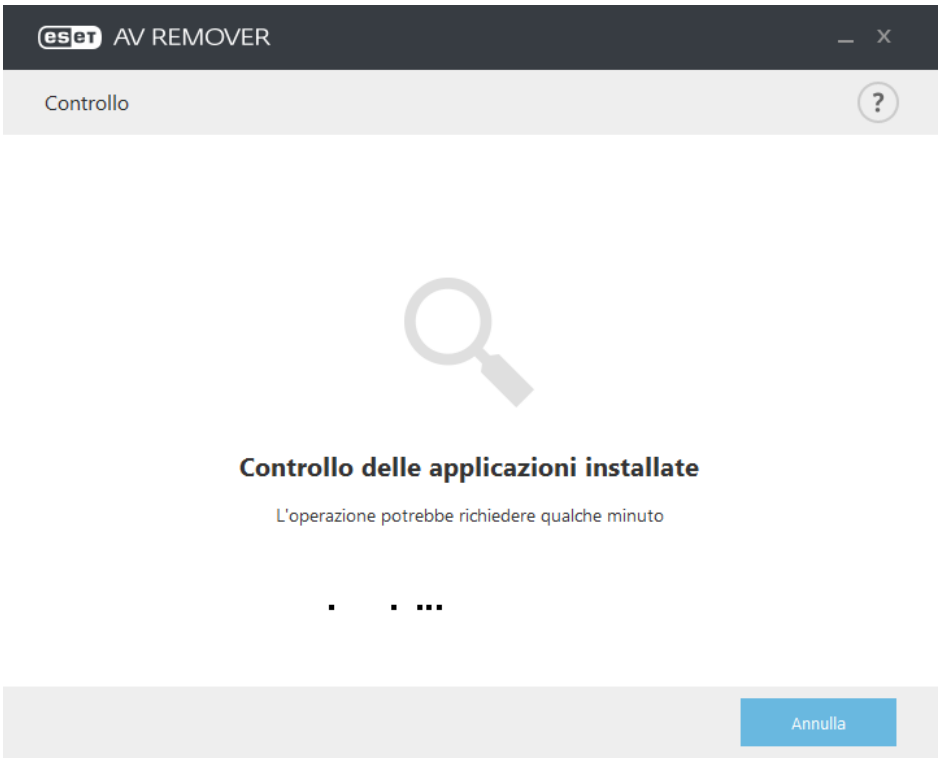
1. Per visualizzare un elenco di software antivirus che ESET AV Remover è in grado di rimuovere, consultare l'articolo della Knowledge Base ESET.



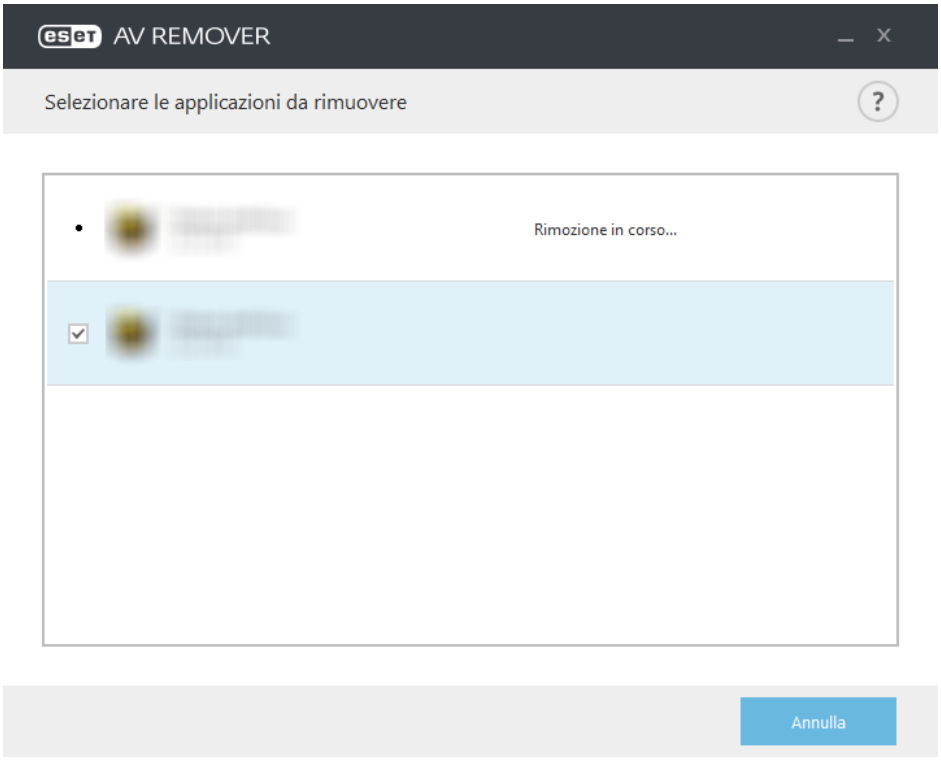
2. Leggere e fare clic su **Accetto** per confermare l'accettazione dei termini dell'Accordo di licenza per l'utente finale. Facendo clic su **Non accetto**, l'installazione di ESET Endpoint Security continuerà senza la rimozione dell'applicazione di protezione presente sul computer.



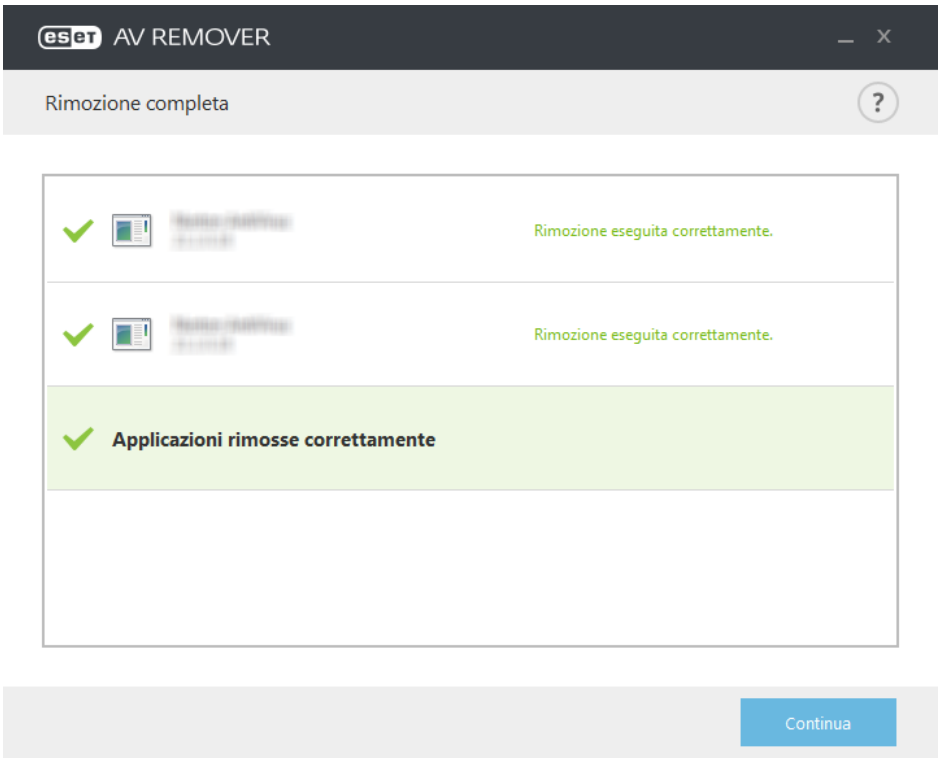
3. ESET AV Remover avvierà la ricerca di software antivirus all'interno del sistema.



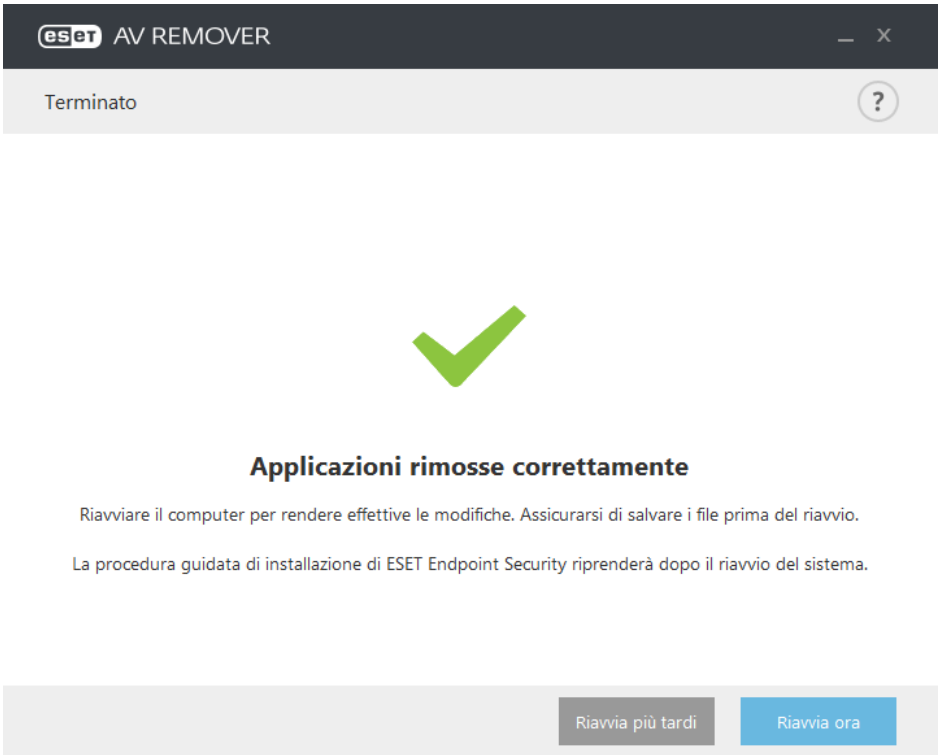
4. Selezionare una delle applicazioni antivirus presenti nell'elenco e fare clic su Rimuovi. La rimozione potrebbe richiedere qualche minuto.



5. Una volta completata la rimozione, fare clic su **Continua**.



6. Riavviare il computer per applicare le modifiche e procedere con l'installazione di ESET Endpoint Security. Se la disinstallazione non è andata a buon fine, consultare la sezione La disinstallazione con ESET AV Remover è terminata con un errore di questa guida.



3.1.2 La disinstallazione con ESET AV Remover è terminata con un errore

Qualora non sia possibile rimuovere un programma antivirus utilizzando ESET AV Remover, l'utente riceverà una notifica relativa al fatto che l'applicazione che sta tentando di rimuovere potrebbe non essere supportata da ESET AV Remover. Consultare l'elenco di prodotti supportati o di programmi di disinstallazione per software antivirus comuni di Windows nella Knowledge Base ESET per valutare la possibilità di rimuovere questo specifico programma.

Se la disinstallazione del prodotto di protezione non è riuscita oppure è stata eseguita la disinstallazione parziale dei relativi componenti, all'utente verrà richiesto di **Riavviare ed eseguire nuovamente il controllo**. Confermare il Controllo dell'account utente (UAC) in seguito all'avvio e continuare con il processo di controllo e di disinstallazione.

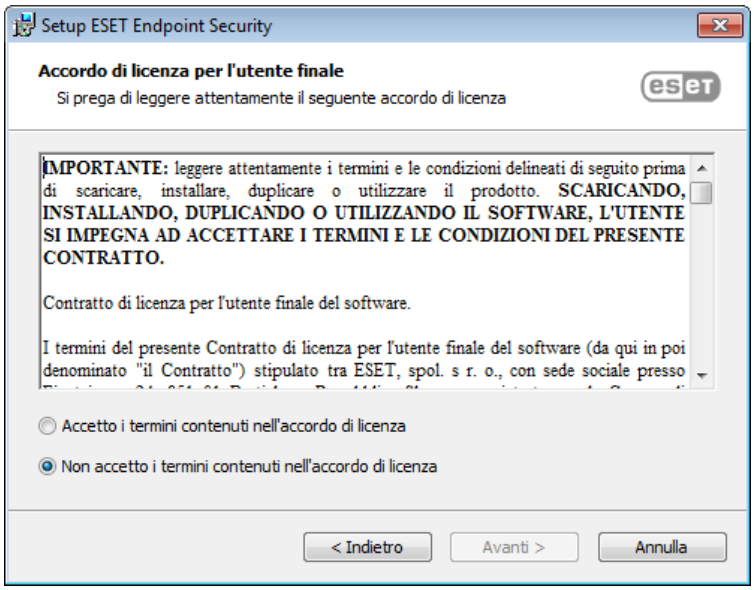
Se necessario, contattare il Supporto tecnico ESET per inviare una richiesta di assistenza e ottenere il file **AppRemover.log** da inviare ai tecnici ESET. Il file **AppRemover.log** è posizionato nella cartella **eset**. Per accedere alla cartella, aprire *%TEMP%* in Windows Explorer. Il Supporto tecnico ESET offrirà assistenza immediata per la risoluzione del problema.

3.2 Installazione

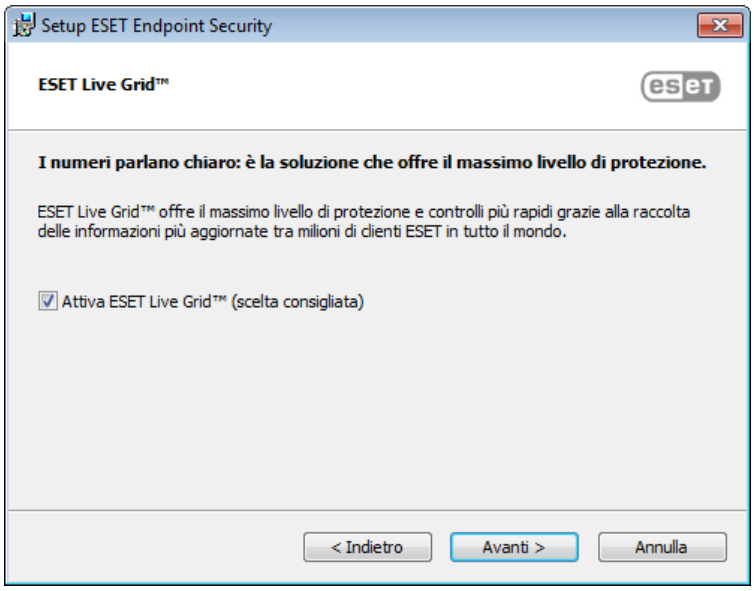
Dopo aver avviato il programma di installazione, l'installazione guidata condurrà l'utente attraverso le varie fasi del processo.

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

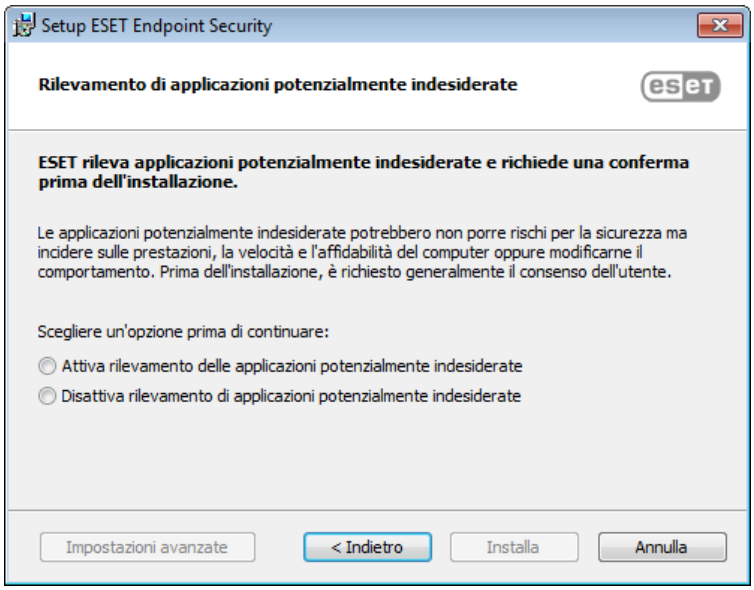
Nel passaggio successivo, verrà visualizzato l'Accordo di Licenza per l'Utente finale. Leggere e selezionare **Accetto** per confermare l'accettazione dei termini dell'Accordo di licenza per l'utente finale. Fare clic su **Avanti** dopo aver accettato i termini per procedere con l'installazione.



Dopo aver selezionato "Accetto..." e **Avanti**, all'utente verrà richiesto di configurare ESET Live Grid. ESET Live Grid garantisce un aggiornamento immediato e continuo di ESET sulle nuove infiltrazioni, allo scopo di offrire una protezione potenziata a tutti gli utenti. Il sistema consente di inviare nuove minacce al laboratorio antivirus ESET, dove i virus verranno analizzati, elaborati e aggiunti al database delle firme antivirali.



Il passo successivo del processo di installazione consiste nella configurazione del rilevamento di applicazioni potenzialmente indesiderate che non sono necessariamente dannose, ma che potrebbero influire negativamente sul comportamento del sistema operativo. Per ulteriori informazioni, consultare il capitolo Applicazioni potenzialmente indesiderate. È possibile accedere alle impostazioni aggiuntive facendo clic su **Impostazioni avanzate** (ad esempio, per installare il prodotto ESET in una cartella specifica o attivare il controllo automatico dopo l'installazione).



Il passaggio finale consiste nella conferma dell'installazione facendo clic su **Installa**.

3.2.1 Installazione avanzata

Installazione avanzata consente all'utente di personalizzare numerosi parametri di installazione non disponibili durante l'esecuzione di un'installazione tipica.

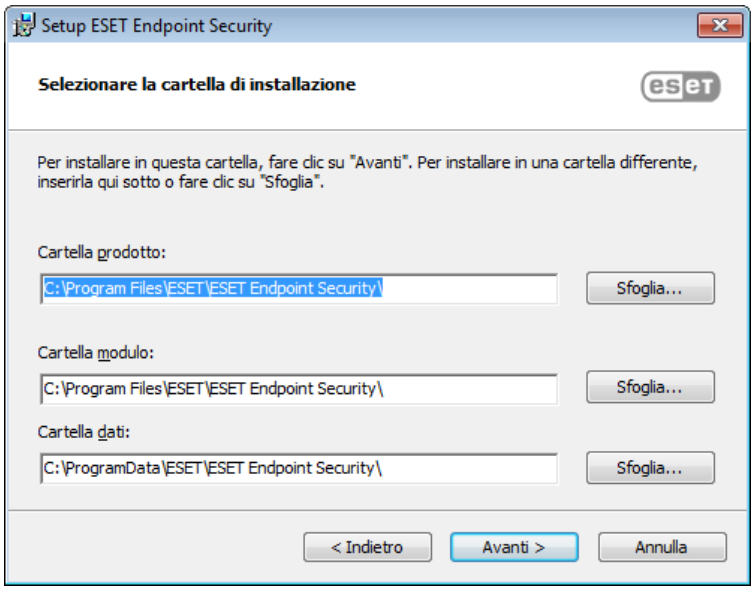
Dopo aver selezionato le preferenze relative al rilevamento delle applicazioni potenzialmente indesiderate e **Impostazioni avanzate**, all'utente verrà di richiesto di selezionare un percorso per la cartella Prodotto da installare. Per impostazione predefinita, il programma viene installato nella directory seguente:

C:\Programmi\ESET\ESET Endpoint Security

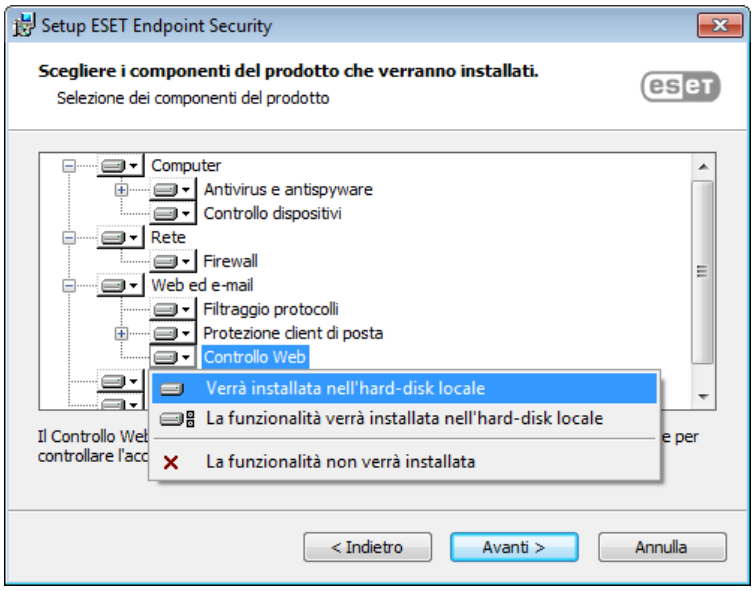
È possibile specificare un percorso per i moduli e i dati del programma. Per impostazione predefinita, questi vengono installati rispettivamente nelle directory seguenti:

C:\Programmi\ESET\ESET Endpoint Security
C:\Dati applicazioni\ESET\ESET Endpoint Security

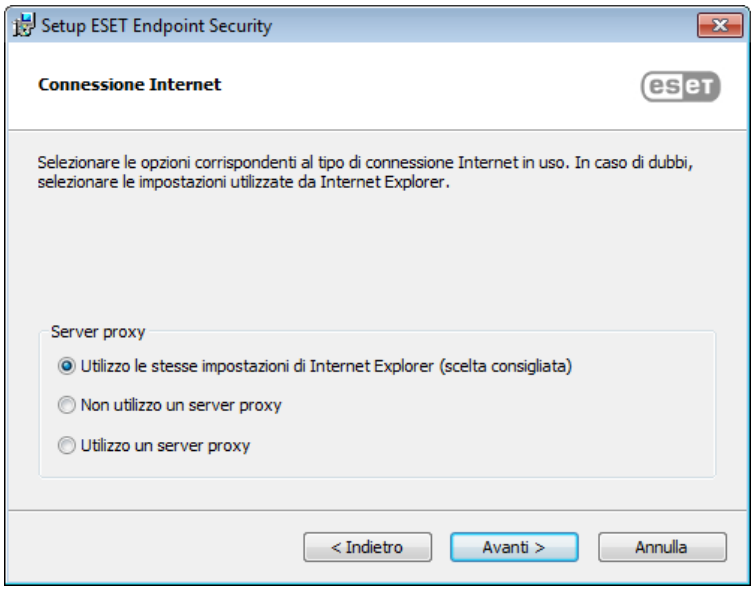
Scegliere **Sfoglia...** per modificare questi percorsi (scelta non consigliata).



Nella finestra successiva, è possibile scegliere i componenti del prodotto che verranno installati. I componenti del prodotto nella sezione Computer includono la protezione file system in tempo reale, il controllo computer, la protezione documenti e il controllo dispositivi. Si tenga presente che i primi due componenti sono obbligatori per un corretto funzionamento della soluzione di protezione. La sezione Rete offre l'opzione di installare il rapporto del Personal firewall, che monitora tutto il traffico di rete in entrata e in uscita e applica le regole alle singole connessioni. Personal firewall offre inoltre protezione contro gli attacchi provenienti dai computer remoti. I componenti nella sezione Web e e-mail sono responsabili della protezione dell'utente durante la navigazione in Internet e le comunicazioni via e-mail. Il componente Mirror di aggiornamento può essere utilizzato per aggiornare altri computer presenti nella rete. La sezione di assistenza Microsoft NAP offre un agente ESET in grado di garantire una compatibilità completa con l'architettura NAP.



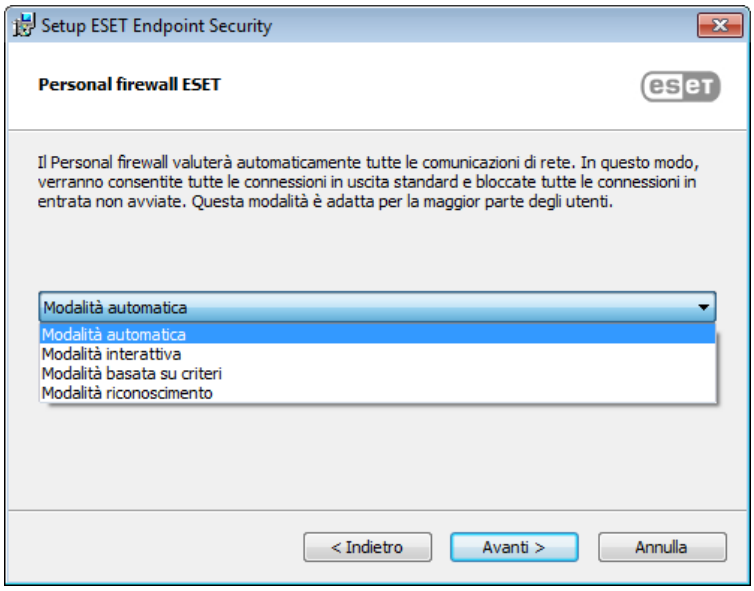
Per configurare le impostazioni del server proxy, selezionare **Utilizzo un server proxy**, quindi fare clic su **Avanti**. Immettere l'indirizzo IP o l'URL del server proxy nel campo **Indirizzo**. Se non si è sicuri se si sta utilizzando un server proxy per la connessione a Internet, selezionare **Utilizzo le stesse impostazioni di Internet Explorer (scelta consigliata)** e fare clic su **Avanti**. Se non si utilizza un server proxy, selezionare **Non utilizzo un server proxy**. Per ulteriori informazioni, consultare Server proxy.



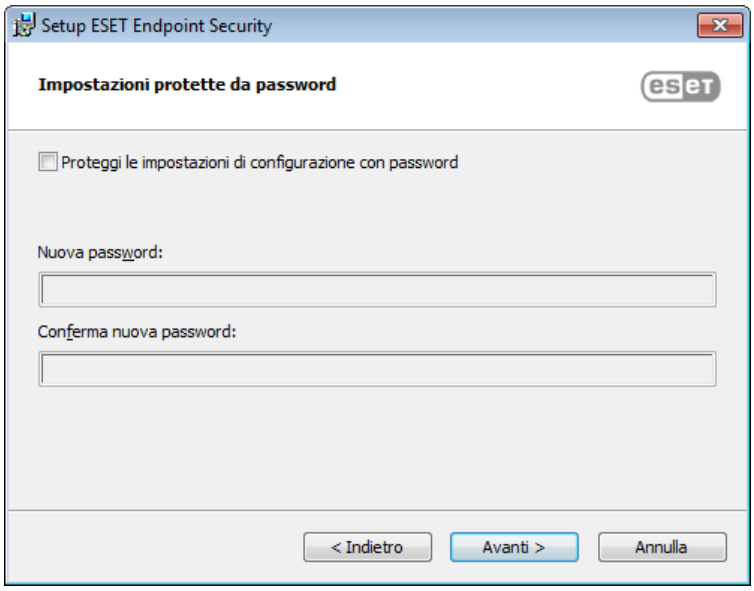
L'installazione personalizzata consente all'utente di definire le modalità di gestione degli aggiornamenti automatici del programma sul sistema. Fare clic su **Modifica...** per accedere alle Impostazioni avanzate.

Se non si desidera aggiornare i componenti di programma, selezionare **Non aggiornare mai i componenti di programma**. Selezionare **Chiedi prima di scaricare i componenti di programma** per visualizzare una finestra di conferma ogni volta che il sistema tenta di scaricare i componenti di programma. Per scaricare automaticamente gli aggiornamenti dei componenti di programma, selezionare **Aggiorna sempre i componenti di programma**.

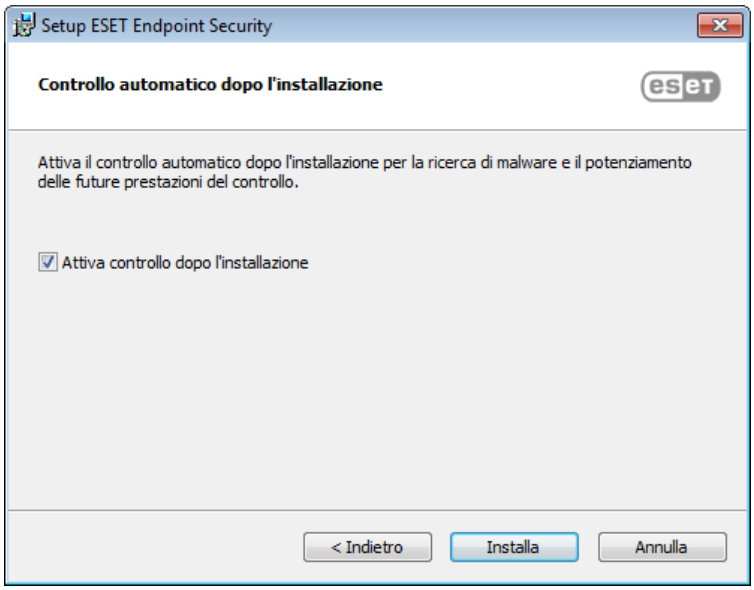
Quindi, selezionare la modalità di filtraggio di ESET Personal firewall. Per ESET Endpoint Security Personal Firewall, sono disponibili quattro modalità di filtraggio. Il comportamento del firewall cambia in base alla modalità selezionata. Le modalità di filtraggio influenzano anche il livello di interazione da parte dell'utente.



Nella finestra di installazione successiva è disponibile l'opzione per impostare una password per proteggere le impostazioni del programma. Selezionare **Proteggi le impostazioni di configurazione con password** e inserire la password nei campi **Nuova password** e **Conferma nuova password**. Questa password verrà richiesta per modificare o accedere alle impostazioni di ESET Endpoint Security. Se i campi delle password corrispondono, fare clic su **Avanti** per continuare.



Per disattivare il primo controllo dopo l'installazione, eseguito normalmente al termine dell'installazione, deselezionare la casella di controllo accanto a **Attiva controllo dopo l'installazione**.



Fare clic su **Installa** per avviare l'installazione.

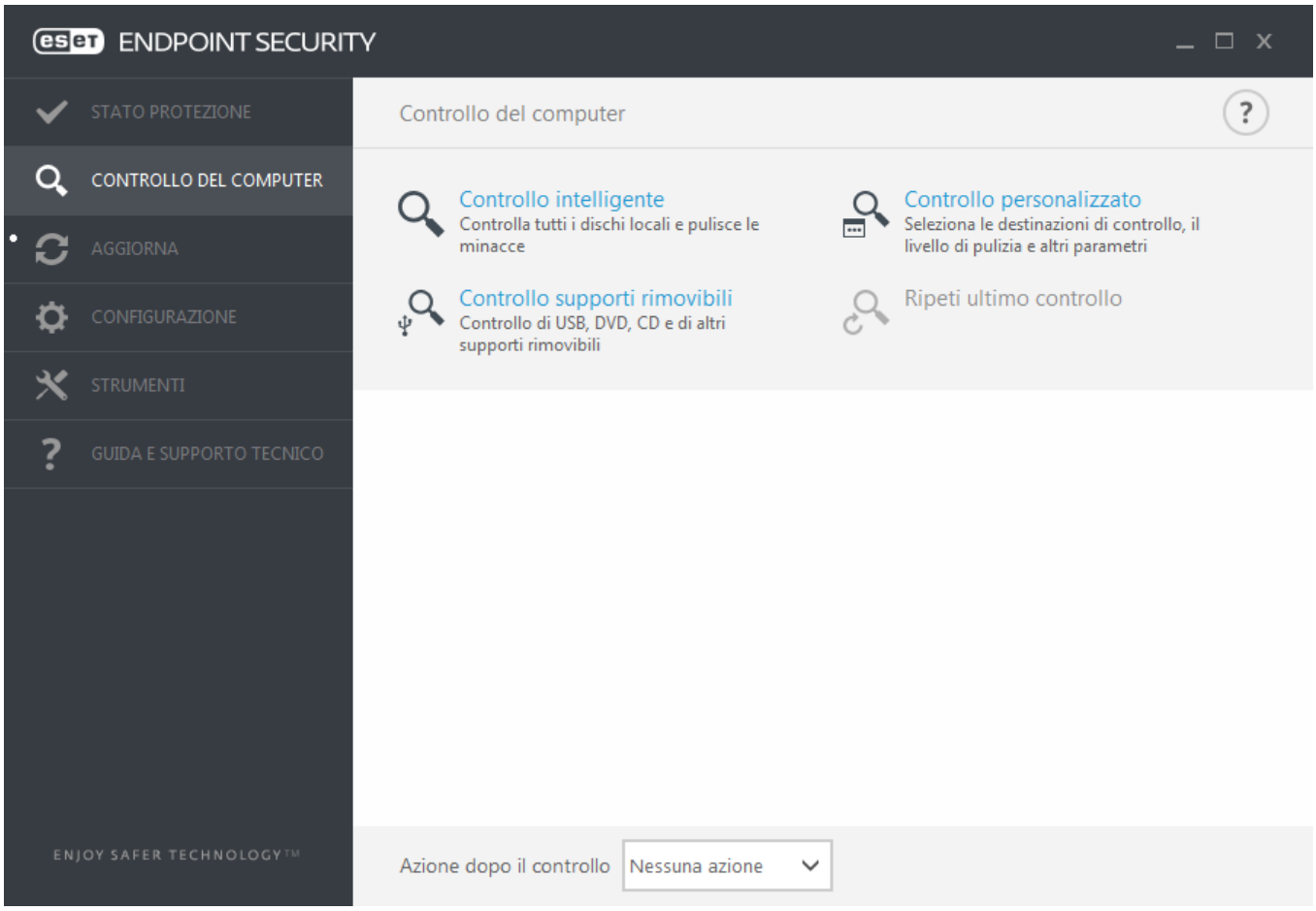
3.3 Attivazione prodotto

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

Selezionare uno dei metodi disponibili per attivare ESET Endpoint Security. Per ulteriori informazioni, consultare il paragrafo Come fare per attivare ESET Endpoint Security.

3.4 Controllo del computer

Non più di 15 minuti dopo il completamento dell'installazione (potrebbe essere necessario un riavvio del computer), ESET Endpoint Security eseguirà automaticamente un controllo del computer. Oltre al controllo iniziale, si consiglia di eseguire controlli del computer periodici oppure programmare un'attività periodica per il controllo delle minacce. Nella finestra principale del programma, fare clic su **Controllo del computer**, quindi selezionare **Controllo intelligente**. Per ulteriori informazioni sui controlli del computer, consultare Controllo del computer.



3.5 Aggiornamento a una versione più recente

Le nuove versioni di ESET Endpoint Security vengono rilasciate per offrire miglioramenti o correggere errori che non è possibile risolvere mediante gli aggiornamenti automatici dei moduli del programma. L'aggiornamento a una versione più recente può essere eseguito in diversi modi:

1. Automaticamente tramite un aggiornamento del programma.
   Poiché viene distribuito a tutti gli utenti e potrebbe influenzare alcune configurazioni del sistema, l'aggiornamento del programma viene rilasciato dopo un lungo periodo di prova per garantirne un funzionamento con tutte le possibili configurazioni di sistema. Se è necessario eseguire l'aggiornamento a una versione più recente subito dopo il rilascio, utilizzare uno dei metodi seguenti.
2. Manualmente scaricando e installando una versione più recente su quella precedente.
3. Manualmente con il sistema di distribuzione automatica in un ambiente di rete tramite ESET Remote Administrator.

3.6 Guida introduttiva

In questo capitolo viene fornita una panoramica su ESET Endpoint Security e sulle configurazioni di base.

3.6.1 L'interfaccia utente

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

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

Stato protezione: fornisce informazioni relative allo stato di protezione di ESET Endpoint Security.

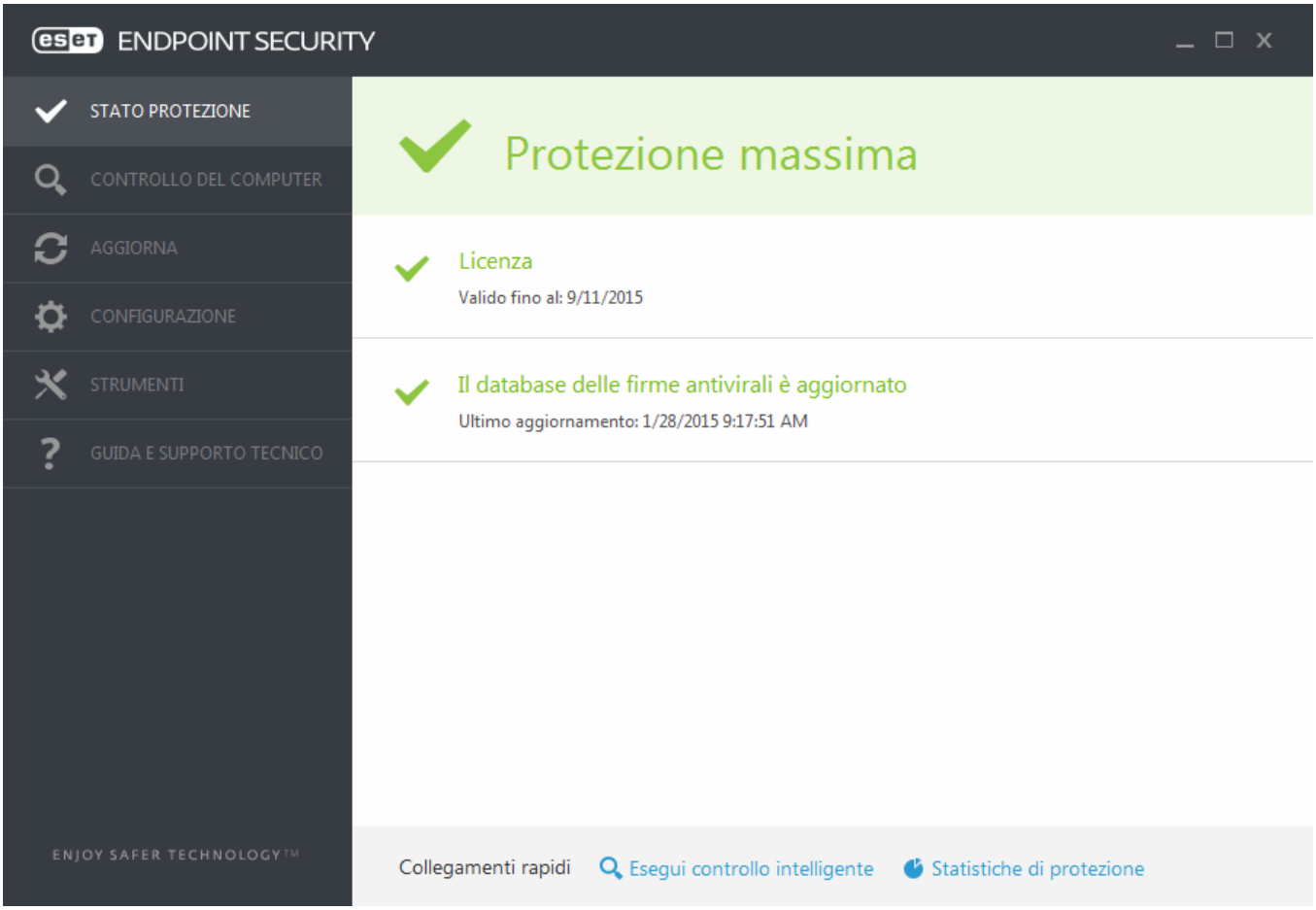
Controllo computer: questa opzione consente all'utente di configurare e avviare un controllo intelligente, un controllo personalizzato o un controllo di supporti rimovibili. È inoltre possibile ripetere l'ultimo controllo eseguito.

Aggiorna: consente di visualizzare informazioni relative al database delle firme antivirali.

Configura: selezionare questa opzione per configurare le impostazioni di protezione del computer,, la rete o il Web e le e-mail.

Strumenti: consente di accedere ai file di rapporto, le statistiche di protezione, l'attività di verifica, i processi in esecuzione, la pianificazione attività, la quarantena, connessioni di rete, ESET SysInspector e ESET SysRescue per creare un CD di ripristino. È inoltre possibile inviare un campione per l'analisi.

Guida e supporto tecnico: consente di accedere ai file della Guida, alla Knowledge Base ESET e al sito Web dell'azienda ESET. Sono inoltre disponibili collegamenti per l'invio di una richiesta di assistenza al Supporto tecnico, strumenti di assistenza e informazioni relative all'attivazione del prodotto.



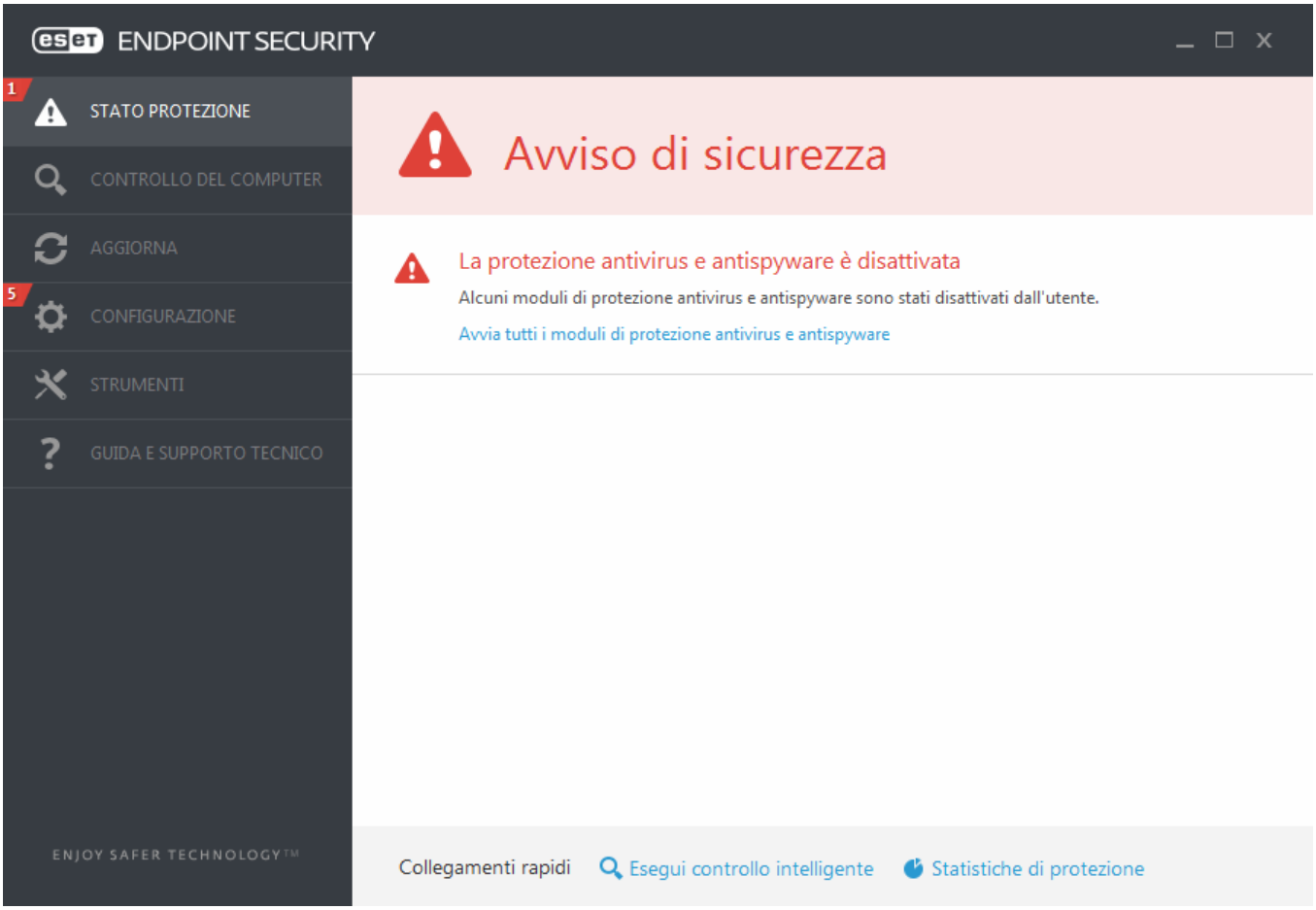
Nella schermata **Stato protezione** sono disponibili informazioni sulla sicurezza e sul livello di protezione corrente del computer. Lo stato **Massima protezione** (di colore verde) indica che è garantito il livello massimo di protezione.

La finestra Stato consente inoltre di visualizzare collegamenti rapidi alle funzioni utilizzate più frequentemente in

ESET Endpoint Security e alle informazioni relative all'ultimo aggiornamento.

Cosa fare se il programma non funziona correttamente?

Se i moduli attivati funzionano correttamente, verrà assegnato un segno di spunta di colore verde. In caso contrario, verrà visualizzato un punto esclamativo di colore rosso o un'icona di notifica di colore arancione. Nella parte superiore della finestra verranno visualizzate ulteriori informazioni sul modulo. Verrà inoltre visualizzata una soluzione consigliata per la riparazione del modulo. Per modificare lo stato di un singolo modulo, fare clic su **Configurazione** nel menu principale, quindi sul modulo desiderato.



L'icona di colore rosso con un punto esclamativo ("!") indica la presenza di problemi critici, ovvero che non è garantito il livello massimo di protezione del computer in uso. Le cause possibili sono:

- **Protezione antivirus e antispyware disattivata**:è possibile riattivare la protezione antivirus e antispyware facendo clic su **Attiva protezione in tempo reale** nel riquadro **Stato protezione** o su **Attiva protezione antivirus e antispyware** nel riquadro **Configurazione** nella finestra principale del programma.
- **ESET Personal firewall è disattivato**: questo problema è segnalato da un'icona di colore rosso e da una notifica di protezione accanto alla voce **Rete**. È possibile riattivare la protezione della rete facendo clic su **Attiva modalità di filtraggio**.
- **Il database delle firme antivirali è obsoleto**: si sta utilizzando un database delle firme antivirali obsoleto.
- **Il prodotto non è attivato** o **Licenza scaduta**: questa condizione è indicata dalla presenza di un'icona rossa dello stato di protezione. Allo scadere della licenza, non sarà possibile aggiornare il programma. Si consiglia di seguire le istruzioni nella finestra di avviso per rinnovare la licenza.

L'icona di colore arancione con una lettera i minuscola ("i") indica che il prodotto ESET richiede attenzione per un problema non critico. Le cause possibili sono:

- **La protezione accesso Web è disattivata**: è possibile riattivare la protezione accesso Web facendo clic sulla notifica di protezione, quindi su **Attiva protezione accesso Web**.
- **La licenza scadrà a breve**: questa condizione è indicata dalla presenza dell'icona dello stato di protezione con un

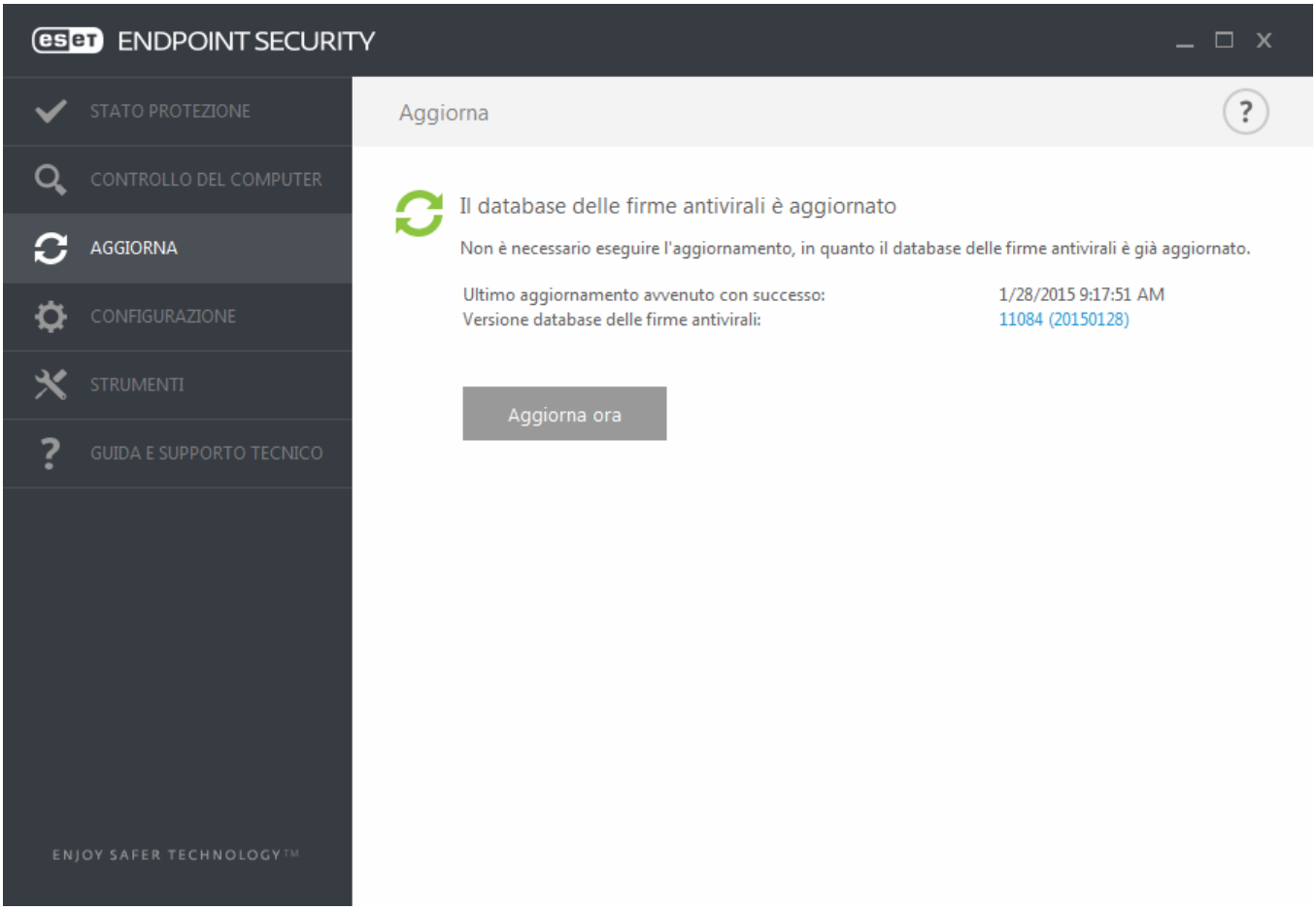
punto esclamativo. Allo scadere della licenza, non sarà possibile aggiornare il programma e l'icona dello stato di protezione diventerà rossa.

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

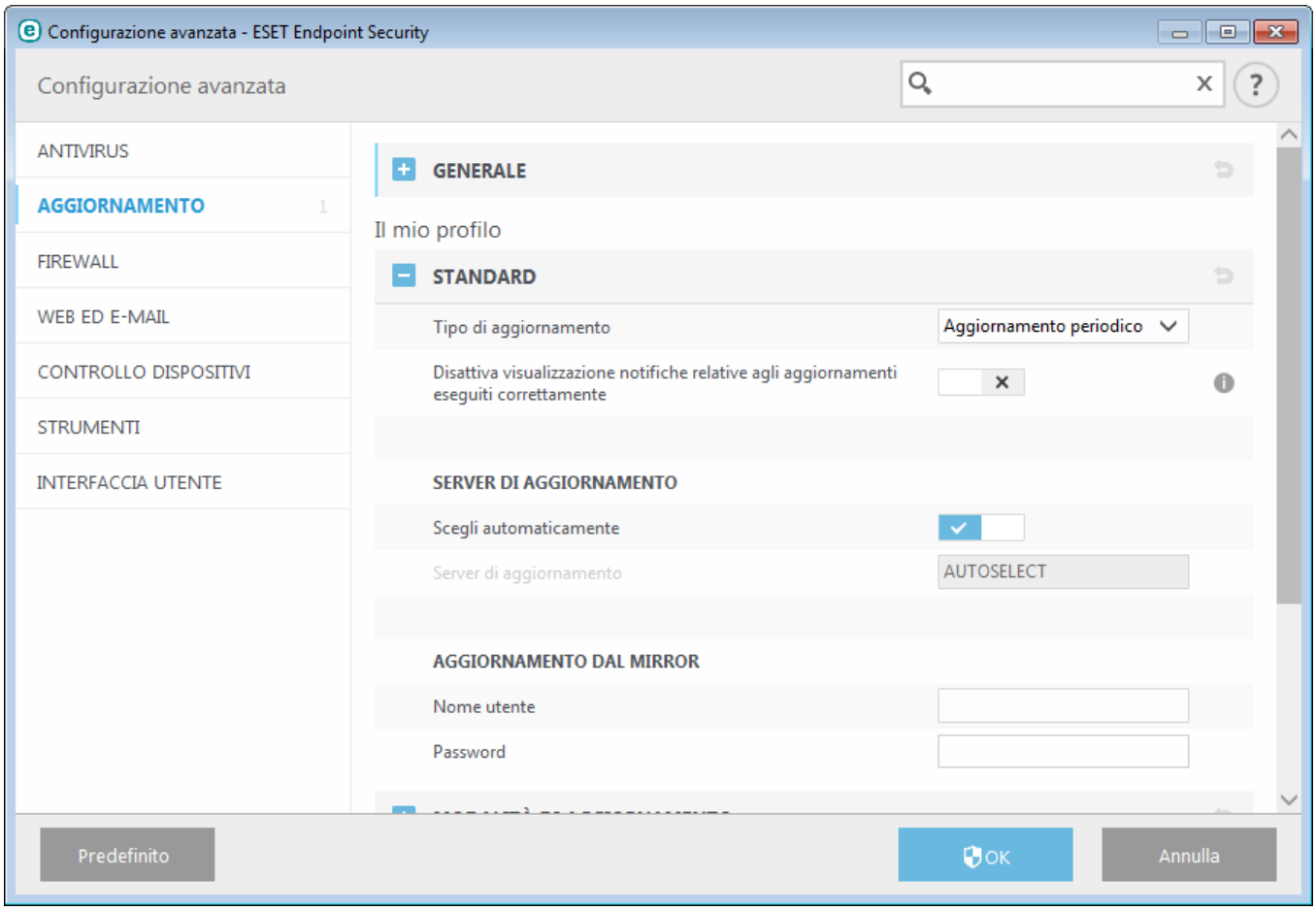
3.6.2 Configurazione dell'aggiornamento

L'aggiornamento del database delle firme antivirali e dei componenti del programma costituisce un aspetto importante per il mantenimento di una protezione completa contro codici dannosi. È opportuno prestare particolare attenzione all'aggiornamento della configurazione e del funzionamento. Nel menu principale, selezionare **Aggiorna** > **Aggiorna ora** per verificare la disponibilità di un aggiornamento più recente del database.

In caso di mancato inserimento della **Chiave di licenza**, l'utente non potrà ricevere i nuovi aggiornamenti e il programma richiederà l'attivazione del prodotto.



Nella finestra Configurazione avanzata (fare clic su **Configurazione** > **Configurazione avanzata** nel menu principale oppure premere **F5** sulla tastiera), sono disponibili ulteriori opzioni di aggiornamento. Per configurare le opzioni di aggiornamento avanzate, come ad esempio la modalità di aggiornamento, l'accesso al server proxy, le connessioni LAN e le impostazioni relative alla creazione di copie delle firme antivirali, fare clic su **Aggiorna** nella struttura Configurazione avanzata. In caso di problemi con un aggiornamento, fare clic su **Cancella** per eliminare la cache dei file di aggiornamento temporanei. Per impostazione predefinita, il menu **Server di aggiornamento** è impostato su **SELEZIONE AUTOMATICA**. Se si utilizza un server ESET, si consiglia di lasciare selezionata l'opzione **Scegli automaticamente**. Se non si desidera visualizzare la notifica sulla barra delle applicazioni del sistema nell'angolo in basso a destra della schermata, selezionare **Disattiva visualizzazione notifiche relative agli aggiornamenti eseguiti correttamente**.



Per garantire un livello di funzionalità ottimale, è fondamentale che il programma venga aggiornato automaticamente. Questa operazione può essere eseguita soltanto dopo aver inserito la **Chiave di licenza** corretta in **Guida e supporto tecnico** > **Attiva prodotto**.

In caso di mancato inserimento della **Chiave di licenza** dopo l'installazione, è possibile farlo in qualsiasi momento. Per ulteriori informazioni sull'attivazione, consultare Come attivare ESET Endpoint Security e inserire le credenziali ricevute insieme al prodotto di protezione ESET nella finestra **Dettagli licenza**.

3.6.3 Configurazione aree

È necessario configurare le aree attendibili per proteggere il computer in uso in un ambiente di rete. Attraverso la configurazione di un'area attendibile ai fini della condivisione, è possibile consentire l'accesso al computer da parte di altri utenti. Fare clic su **Configurazione avanzata** (F5) > **Personal firewall** > **Aree** per accedere alle impostazioni delle aree attendibili.

Il rilevamento dell'area attendibile viene eseguito dopo l'installazione di ESET Endpoint Security e ogni volta che il computer si connette a una nuova rete. Solitamente, non è pertanto necessario definire l'area attendibile. Per impostazione predefinita, al rilevamento di una nuova area verrà visualizzata una finestra di dialogo che consente all'utente di impostare il livello di protezione per quell'area.

Avviso: una configurazione dell'area affidabile non corretta potrebbe costituire un rischio per la protezione del computer.

NOTA: per impostazione predefinita, le workstation di un'area attendibile possono accedere a file e stampanti condivisi; è attivata, inoltre, la comunicazione RPC in entrata ed è disponibile la condivisione del desktop remoto.

3.6.4 Strumenti per il controllo Web

Se è già stato attivato il Controllo Web in ESET Endpoint Security, per garantirne un corretto funzionamento, è necessario configurare questa opzione anche per gli account utente desiderati. Consultare il capitolo Controllo Web per ulteriori informazioni su come creare restrizioni specifiche per le workstation client allo scopo di proteggerle da materiale potenzialmente inappropriato.

3.7 Domande comuni

In questo capitolo sono illustrate alcune delle domande frequenti e i problemi riscontrati. Fare clic sul titolo di un argomento per trovare la soluzione al problema:

Come fare per aggiornare ESET Endpoint Security
Come fare per attivare ESET Endpoint Security
Come utilizzare le credenziali correnti per l'attivazione di un nuovo prodotto
Come rimuovere un virus dal PC
Come consentire la comunicazione per una determinata applicazione
Come fare per creare una nuova attività in Pianificazione attività
Come fare per pianificare un'attività di controllo (ogni 24 ore)
Come connettere il prodotto a ESET Remote Administrator
Come configurare un mirror

Se il problema non è presente nell'elenco delle pagine della Guida riportate sopra, provare a eseguire una ricerca in base a una parola chiave o frase che descrive il problema nelle pagine della Guida di ESET Endpoint Security.

Se non si riesce a trovare la soluzione a un problema o una domanda nelle pagine della Guida, visitare la Knowledge Base ESET, dove è possibile trovare le risposte a domande e problemi comuni.

Come si fa a rimuovere il trojan Sirefef (ZeroAccess)?
Lista di controllo risoluzione dei problemi di aggiornamento del mirror
Quali indirizzi e porte presenti sui firewall di terze parti è necessario aprire per consentire la funzionalità completa dei prodotti ESET?

Se necessario, contattare il centro di supporto tecnico on-line per eventuali domande o problemi riscontrati. Il collegamento al modulo di contatto on-line è disponibile nel riquadro **Guida e supporto tecnico** nella finestra principale del programma.

3.7.1 Come fare per aggiornare ESET Endpoint Security

L'aggiornamento di ESET Endpoint Security può essere eseguito manualmente o automaticamente. Per attivare l'aggiornamento, fare clic su **Aggiorna ora** nella sezione **Aggiorna** del menu principale.

Le impostazioni predefinite dell'installazione consentono di creare un'attività di aggiornamento automatica che viene eseguita ogni ora. Per modificare l'intervallo, accedere a **Strumenti** > **Pianificazione attività** (per ulteriori informazioni sulla Pianificazione attività, fare clic qui).

3.7.2 Come fare per attivare ESET Endpoint Security

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

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

Per attivare la copia di ESET Endpoint Security direttamente dal programma, fare clic sull'icona della barra delle applicazioni e selezionare **Attiva licenza prodotto** dal menu. È inoltre possibile attivare il prodotto dal menu principale sotto a **Guida e supporto tecnico** > **Attiva prodotto** o **Stato protezione** > **Attiva prodotto**.

È inoltre possibile utilizzare uno dei metodi che seguono per attivare ESET Endpoint Security:

- **Chiave di licenza**: stringa univoca nel formato XXXX-XXXX-XXXX-XXXX-XXXX, utilizzata per l'identificazione del proprietario della licenza e per l'attivazione del prodotto.
- **Security Admin** : account creato sul portale di ESET License Administrator con le credenziali (indirizzo e-mail + password). Questo metodo consente all'utente di gestire licenze multiple da un'unica posizione.
- **Licenza off-line**: file generato automaticamente che verrà trasferito al prodotto ESET allo scopo di fornire le informazioni sulla licenza. Se una licenza consente all'utente di scaricare un file di licenza off-line (.lf), esso potrà essere utilizzato per eseguire l'attivazione off-line. Il numero di licenze off-line verrà sottratto dal numero totale di licenze disponibili. Per ulteriori informazioni sulla generazione di un file off-line, consultare il Manuale

dell'utente di ESET License Administrator.

Fare clic su **Attiva in seguito** se il computer in uso fa parte di una rete gestita: in tal modo, l'amministratore eseguirà l'attivazione da remoto attraverso ESET Remote Administrator. È inoltre possibile utilizzare questa opzione se si desidera attivare il client in un momento successivo.

Se si è in possesso di un nome utente e di una password e non si conoscono le modalità di attivazione di ESET Endpoint Security, fare clic su **Possiedo un nome utente e una password, cosa devo fare?**. A questo punto, si verrà reindirizzati a ESET License Administrator, dove sarà possibile convertire le credenziali in una chiave di licenza.

È possibile modificare la licenza del prodotto in qualsiasi momento. Per far ciò, fare clic su **Guida e supporto tecnico** > **Gestisci licenza** nella finestra principale del prodotto. A questo punto comparirà l'ID della licenza pubblica per consentire al Supporto ESET di identificare la licenza. Il nome utente con il quale il computer è registrato è disponibile nella sezione **Informazioni** che comparirà facendo clic con il pulsante destro del mouse sull'icona della barra delle applicazioni  .

NOTA: ESET Remote Administrator attiva i computer client in modo automatico attraverso l'utilizzo delle licenze messe a disposizione dall'amministratore. Per ulteriori informazioni, consultare il Manuale dell'utente ESET Remote Administrator.

3.7.3 Come utilizzare le credenziali correnti per l'attivazione di un nuovo prodotto

Se si è già in possesso di un nome utente e una password e si desidera ricevere una chiave di licenza, visitare il portale di ESET License Administrator, dove è possibile convertire le credenziali in una nuova chiave di licenza.

3.7.4 Come rimuovere un virus dal PC

Se il computer mostra sintomi di infezione da malware, ad esempio, appare più lento o si blocca spesso, è consigliabile attenersi alle seguenti istruzioni:

1. Nella finestra principale del programma, fare clic su **Controllo computer**.
2. Fare clic su **Controllo intelligente** per avviare il controllo del sistema.
3. Al termine del controllo, verificare nel registro il numero di file sottoposti a controllo, file infetti e file puliti.
4. Se si desidera controllare solo una parte del disco, fare clic su **Controllo personalizzato** e selezionare gli oggetti nei quali ricercare l'eventuale presenza di virus.

Per ulteriori informazioni, consultare l'articolo della Knowledge Base ESET aggiornato periodicamente.

3.7.5 Come consentire la comunicazione per una determinata applicazione

Se in modalità interattiva viene rilevata una nuova connessione e non vengono individuate regole corrispondenti, verrà chiesto se consentire o rifiutare la connessione. Se si desidera che ESET Endpoint Security esegua la stessa azione ogni volta che l'applicazione tenta di stabilire una connessione, selezionare la casella di controllo **Ricorda azione (crea regola)**.

È possibile creare nuove regole del rapporto del Personal firewall per le applicazioni prima che queste vengano rilevate da ESET Endpoint Security nella finestra di configurazione del rapporto del Personal firewall, disponibile sotto a **Configurazione avanzata** > **Personal firewall** > **Standard** > **Regole** facendo clic su **Modifica**.

Fare clic su **Aggiungi** per aggiungere la regola. Nella scheda **Generale**, inserire il nome, la direzione e il protocollo di comunicazione per la regola. In questa finestra è possibile definire l'azione da intraprendere quando la regola viene applicata.

Inserire il percorso del file eseguibile dell'applicazione e la porta di comunicazione locale nella scheda **Locale**. Fare clic sulla scheda **Remoto** per inserire l'indirizzo remoto e la porta remota (se applicabile). La regola appena creata verrà applicata non appena l'applicazione tenta di stabilire nuovamente la comunicazione.

3.7.6 Come fare per creare una nuova attività in Pianificazione attività

Per creare una nuova attività in **Strumenti** > **Pianificazione attività**, fare clic su **Aggiungi attività** oppure fare clic con il pulsante destro del mouse e selezionare **Aggiungi...** dal menu contestuale. Sono disponibili cinque tipi di attività pianificate:

- **Esegui applicazione esterna**: consente di pianificare l'esecuzione di un'applicazione esterna.
- **Manutenzione rapporto**: file di rapporto contenenti elementi rimasti dai record eliminati. Questa attività ottimizza periodicamente i record nei file di rapporto allo scopo di garantire un funzionamento efficiente.
- **Controllo del file di avvio del sistema**: consente di controllare i file la cui esecuzione è consentita all'avvio del sistema o all'accesso.
- **Crea snapshot di stato computer**: crea uno snapshot del computer ESET SysInspector, raccoglie informazioni dettagliate sui componenti del sistema (ad esempio, driver e applicazioni) e valuta il livello di rischio di ciascun componente.
- **Controllo computer su richiesta**: consente di eseguire un controllo di file e di cartelle sul computer in uso.
- **Primo controllo**: per impostazione predefinita, 20 minuti dopo l'installazione o il riavvio, verrà eseguito un Controllo del computer come attività con priorità bassa.
- **Aggiorna**: pianifica un'attività di aggiornamento aggiornando il database delle firme antivirali e i moduli del

programma.

Poiché **Aggiorna** rappresenta una delle attività pianificate utilizzata con maggiore frequenza, di seguito verranno illustrate le modalità in cui è possibile aggiungere una nuova attività di aggiornamento:

Dal menu a discesa **Attività pianificata**, selezionare **Aggiorna**. Inserire il nome dell'attività nel campo **Nome attività** e fare clic su **Avanti**. Selezionare la frequenza dell'attività. Sono disponibili le seguenti opzioni: **Una volta**, **Ripetutamente**, **Ogni giorno**, **Ogni settimana** e **Quando si verifica un evento.** Selezionare **Ignora attività se in esecuzione su un computer alimentato dalla batteria** per ridurre al minimo le risorse di sistema in caso di utilizzo della batteria del computer portatile. L'attività verrà eseguita alla data e all'ora specificate nei campi **Esecuzione attività**. È quindi possibile definire l'azione da intraprendere se l'attività non può essere eseguita o completata nei tempi programmati. Sono disponibili le seguenti opzioni:

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

Nel passaggio successivo, viene visualizzata una finestra contenente un riepilogo delle informazioni sull'attività pianificata corrente. Fare clic su **Fine** una volta terminate le modifiche.

Verrà visualizzata una finestra di dialogo in cui è possibile scegliere i profili da utilizzare per l'attività pianificata. Qui è possibile impostare il profilo primario e alternativo. Il profilo alternativo viene utilizzato se l'attività non può essere completata mediante l'utilizzo del profilo primario. Confermare facendo clic su **Fine**. A questo punto, la nuova attività pianificata verrà aggiunta all'elenco delle attività pianificate correnti.

3.7.7 Come fare per pianificare un'attività di controllo (ogni 24 ore)

Per programmare un'attività periodica, aprire la finestra principale del programma e fare clic su **Strumenti** > **Pianificazione attività**. Di seguito viene riportata la procedura da seguire per pianificare un'attività che controllerà tutti i dischi locali ogni 24 ore.

Per pianificare un'attività di controllo:

1. Fare clic su **Aggiungi** nella schermata principale di Pianificazione attività.
2. Selezionare **Controllo computer su richiesta** dal menu a discesa.
3. Immettere un nome per l'attività, quindi selezionare **Ripetutamente**.
4. Specificare di eseguire l'attività ogni 24 ore.
5. Selezionare un'azione da eseguire nel caso in cui, per qualsiasi motivo, non fosse possibile completare l'esecuzione dell'attività.
6. Esaminare il riepilogo dell'attività pianificata e fare clic su **Fine**.
7. Selezionare **Unità locali** nel menu a discesa **Destinazioni**.
8. Fare clic su **Fine** per confermare l'attività.

3.7.8 Come fare per connettere ESET Endpoint Security a ESET Remote Administrator

Se, dopo aver installato ESET Endpoint Security sul computer in uso, si desidera effettuare la connessione mediante ESET Remote Administrator, assicurarsi di aver installato anche l'agente ERA sulla workstation client. L'agente ERA rappresenta una parte essenziale di ogni soluzione client che comunica con il server ERA. ESET Remote Administrator utilizza lo strumento RD Sensor per ricercare i computer nella rete. Ogni computer nella rete rilevato da RD Sensor viene visualizzato nella console Web.

Dopo aver eseguito la distribuzione dell'agente, è possibile installare i prodotti di protezione ESET da remoto sul computer client in uso. I passaggi relativi all'installazione remota sono descritti nel Manuale dell'utente di ESET Remote Administrator.

3.7.9 Come configurare un mirror

È possibile configurare ESET Endpoint Security per archiviare copie dei file di aggiornamento delle firme antivirali e distribuire aggiornamenti ad altre workstation sulle quali è in esecuzione ESET Endpoint Security o ESET Endpoint Antivirus.

Configurare ESET Endpoint Security come server mirror per fornire aggiornamenti mediante un server HTTP interno

Premere **F5** per accedere a Configurazione avanzata ed espandere **Aggiornamento** > **Di base**. Assicurarsi che il **Server di aggiornamento** sia impostato su **SELEZIONE AUTOMATICA**. Selezionare **Crea mirror di aggiornamento** e **Fornisci i file di aggiornamento tramite il server HTTP interno** da **Configurazione avanzata** > **Standard** > **Mirror**.

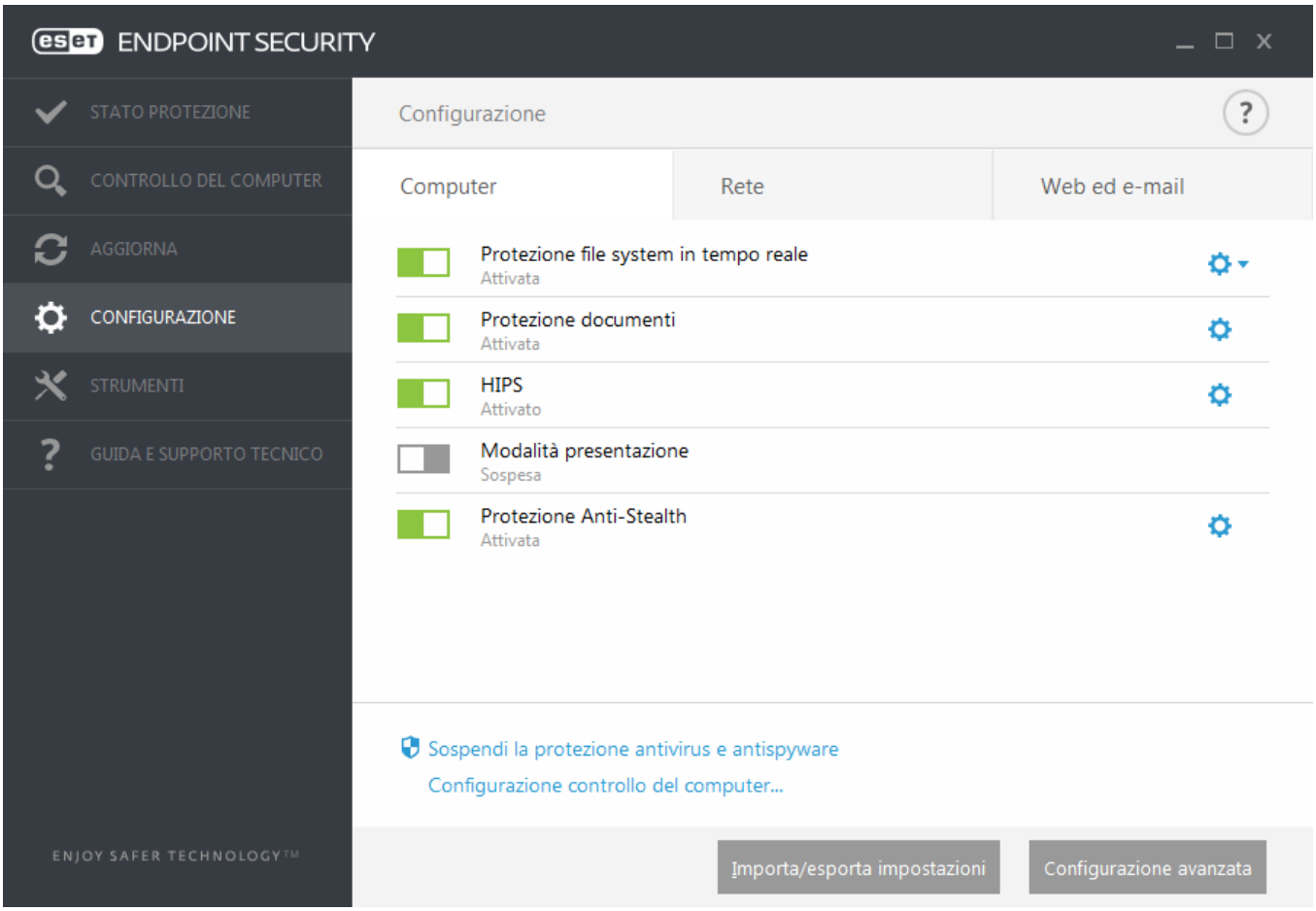
Configurare un server mirror per fornire aggiornamenti mediante una cartella di rete condivisa

Creare una cartella condivisa su un dispositivo locale o di rete. Questa cartella deve essere leggibile per tutti gli utenti sui cui sistemi vengono eseguite soluzioni di protezione ESET e scrivibile dall'account locale SISTEMA. Attivare **Crea mirror di aggiornamento** sotto a **Configurazione avanzata** > **Di base** > **Mirror**. Ricercare e selezionare la cartella condivisa creata.

NOTA: se non si desidera effettuare l'aggiornamento attraverso il server HTTP interno, disattivare **Fornisci i file di aggiornamento tramite il server HTTP interno**.

3.8 Utilizzo di ESET Endpoint Security

Le opzioni di configurazione di ESET Endpoint Security consentono all'utente di configurare il livello di protezione del computer in uso, del Web, delle e-mail e della rete.



Il menu **Configurazione** contiene le seguenti sezioni:

- **Computer**
- **Rete**
- **Web e e-mail**

L'impostazione della protezione **Computer** consente di attivare o disattivare i componenti seguenti:

- **Protezione file system in tempo reale**: tutti i file vengono sottoposti a controllo per la ricerca di codici dannosi al momento dell'apertura, creazione o esecuzione sul computer.
- **Protezione documenti**: la funzione protezione documenti consente di eseguire il controllo dei documenti di Microsoft Office prima della loro apertura e dei file scaricati automaticamente da Internet Explorer, ad esempio gli elementi di Microsoft ActiveX.
- **HIPS**: il sistema HIPS monitora gli eventi che avvengono all'interno del sistema operativo e reagisce in base a un set personalizzato di regole.
- **Modalità presentazione**: funzionalità per gli utenti che desiderano utilizzare il software senza interruzioni, non essere disturbati dalle finestre popup e ridurre al minimo l'utilizzo della CPU. Dopo aver attivato la Modalità presentazione, l'utente riceverà un messaggio di avviso (potenziale rischio per la protezione) e la finestra principale del programma diventerà di colore arancione.
- **Protezione Anti-Stealth**: consente di rilevare programmi pericolosi, ad esempio rootkit, che riescono a nascondersi dal sistema operativo. Ciò significa che non è possibile rilevarli utilizzando le normali tecniche di testing.

La sezione **Rete** consente all'utente di attivare o disattivare il **Personal firewall**.

La configurazione di protezione **Web e e-mail** consente di attivare o disattivare i seguenti componenti:

- **Controllo Web** - Blocca le pagine Web che potrebbero contenere materiale potenzialmente inappropriato. Inoltre, gli amministratori di sistema possono specificare le preferenze di accesso per 27 categorie di siti Web predefinite.
- **Protezione accesso Web**: se questa opzione è attiva, viene eseguito il controllo di tutto il traffico HTTP o HTTPS per la ricerca di software dannoso.
- **Protezione client di posta**: monitora le comunicazioni ricevute mediante il protocollo POP3 e IMAP.
- **Protezione antispam** - Controlla i messaggi e-mail non desiderati o lo spam.
- **Protezione Anti-Phishing**: protegge l'utente da tentativi di acquisizione di password, dati bancari e altre informazioni sensibili da parte di siti Web illegittimi camuffati da siti legittimi.

Per disattivare temporaneamente i singoli moduli, fare clic sul pulsante verde  accanto al modulo desiderato. Tenere presente che in questo modo si potrebbe ridurre il livello di protezione del computer.

Per riattivare la protezione di un componente di protezione disattivato, fare clic sul pulsante rosso  per far ritornare un componente allo stato attivato.

NOTA: tutte le misure di protezione disattivate in base a questa modalità verranno riattivate dopo un riavvio del computer.

Per accedere alle impostazioni dettagliate di un particolare componente di protezione, fare clic sulla rotella a forma di ingranaggio  . accanto a un qualsiasi componente**.**

Nella parte inferiore della finestra di configurazione sono disponibili ulteriori opzioni. Per caricare i parametri di configurazione mediante un file di configurazione *.xml* o per salvare i parametri di configurazione correnti su un file di configurazione, utilizzare **Importa/esporta impostazioni**. Per ulteriori informazioni, consultare il paragrafo Importa/esporta impostazioni.

Per opzioni più specifiche, fare clic su **Configurazione avanzata** oppure premere **F5**.

3.8.1 Computer

Il modulo **Computer** , disponibile sotto a **Configurazione** > **Computer**, consente di visualizzare una panoramica dei moduli di protezione descritti nel capitolo precedente. In questa sezione, sono disponibili le seguenti impostazioni:

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

NOTA: lo stato di protezione dei documenti potrebbe non essere disponibile finché non verrà attivato in **Configurazione avanzata** (F5) > **Antivirus** > **Protezione documenti**. In seguito all'attivazione, è necessario riavviare il computer dal riquadro Configurazione > Computer facendo clic su **Riavvia** sotto a Controllo dispositivi oppure dal riquadro Stato di protezione facendo clic su **Riavvia il computer**.

Sospendi protezione antivirus e antispyware: tutte le volte che viene disattivata temporaneamente la protezione antivirus e antispyware, è possibile selezionare il periodo di tempo per il quale si desidera disattivare il componente selezionato utilizzando il menu a discesa e facendo clic su **Applica** per disattivare il componente di protezione. Per riattivare la protezione, fare clic su **Attiva protezione antivirus e antispyware**.

Configurazione controllo computer... - Fare clic per regolare i parametri del controllo del computer (controllo eseguito manualmente).

3.8.1.1 Antivirus

La protezione antivirus difende il sistema da attacchi dannosi controllando file, e-mail e comunicazioni su Internet. In caso di rilevamento di una minaccia, il modulo antivirus provvede a eliminarla. Il processo prevede le seguenti fasi: blocco, pulizia e cancellazione o spostamento in quarantena.

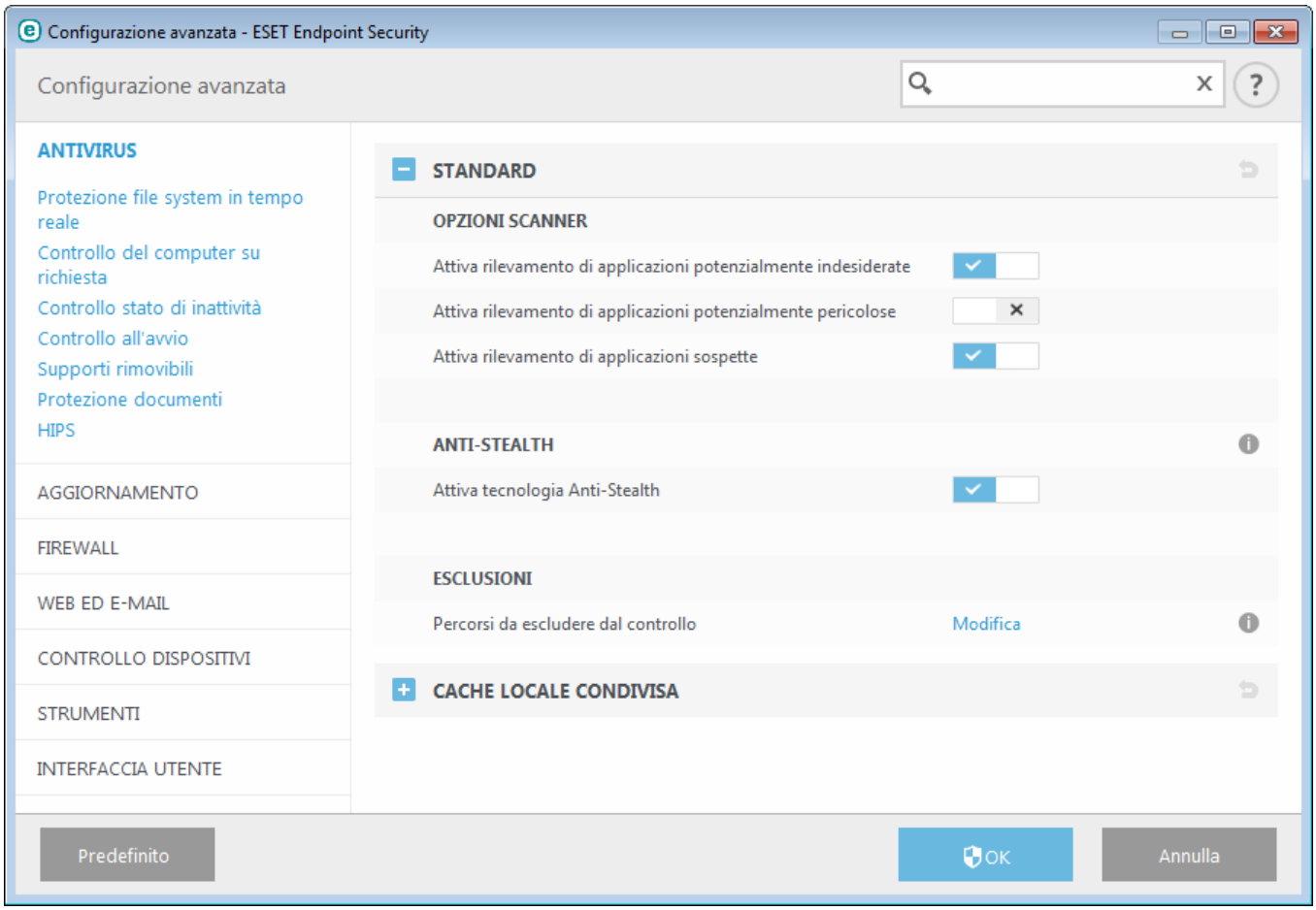
Per configurare nei dettagli le impostazioni del modulo antivirus, fare clic su **Configurazione avanzata** oppure premere **F5**.

Le **Opzioni di controllo** per tutti i moduli di protezione (ad esempio, protezione file system in tempo reale, protezione accesso Web,...) consentono all'utente di attivare o disattivare il rilevamento dei seguenti elementi:

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

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

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



3.8.1.1.1 Rilevamento di un'infiltrazione

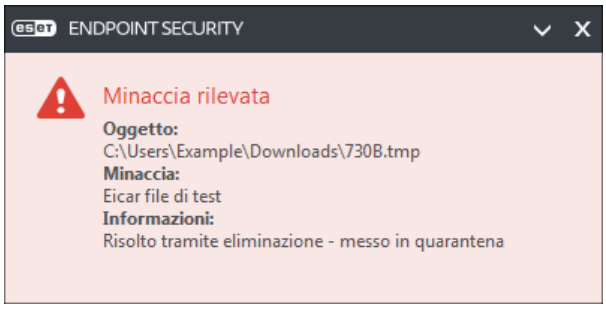
Le infiltrazioni possono raggiungere il sistema da diversi accessi, ad esempio pagine Web, cartelle condivise, messaggi e-mail o dispositivi rimovibili (USB, dischi esterni, CD, DVD, dischi e così via).

Comportamento standard

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

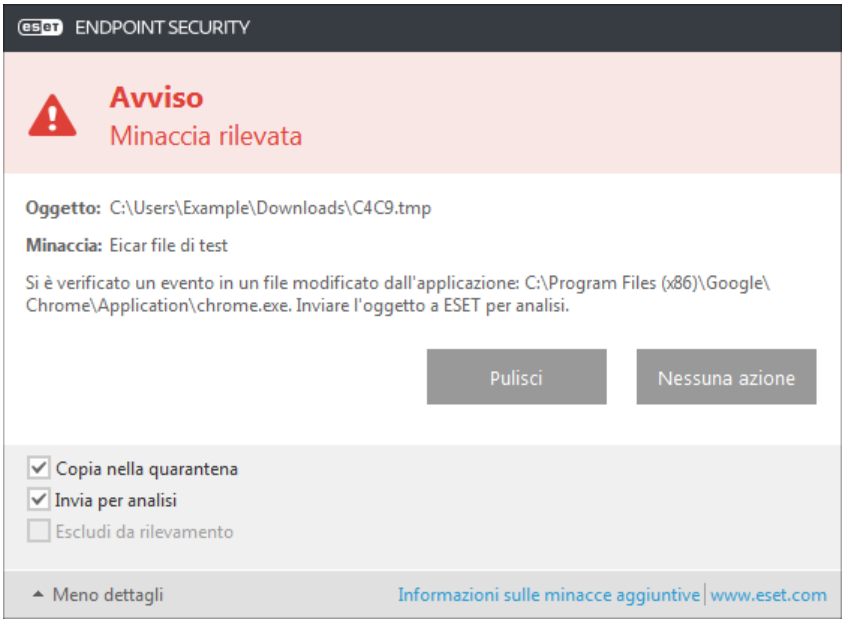
- Protezione file system in tempo reale
- Protezione accesso Web
- Protezione client di posta
- Controllo del computer su richiesta

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



Pulizia ed eliminazione

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



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

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

Minacce multiple

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

Eliminazione dei file negli archivi

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

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

- Aprire ESET Endpoint Security e fare clic su Controllo del computer
- Fare clic su **Controllo intelligente** (per ulteriori informazioni, consultare Controllo del computer)
- Al termine del controllo, consultare il rapporto per conoscere il numero di file controllati, infetti e puliti

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

3.8.1.2 Cache locale condivisa

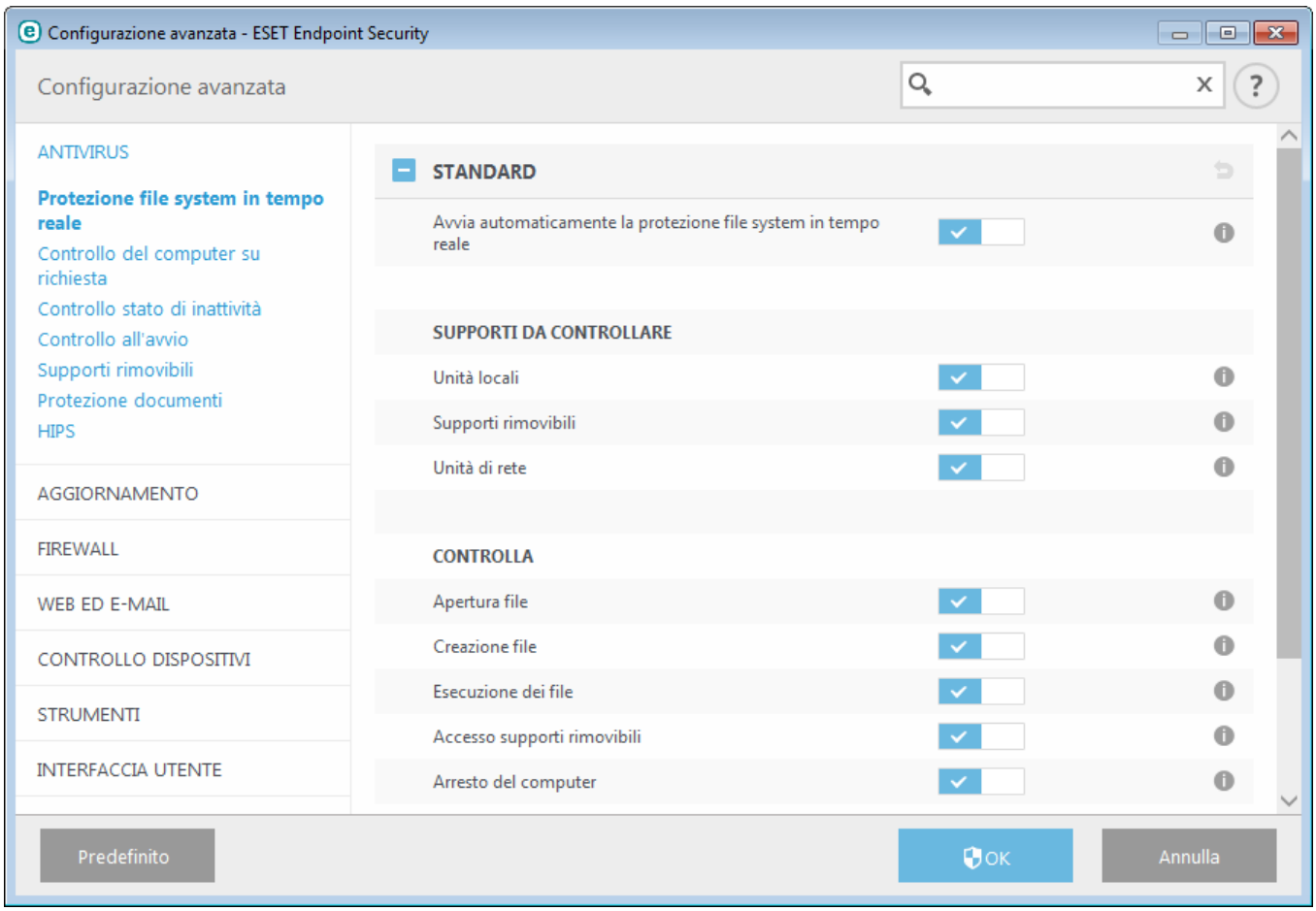
La cache locale condivisa potenzierà le prestazioni negli ambienti virtuali eliminando i controlli duplicati nella rete. Ciò garantisce un controllo unico di ciascun file e l'archiviazione nella cache condivisa. Attivare il pulsante **Opzione memorizzazione nella cache** per salvare le informazioni relative ai controlli di file e cartelle presenti nella rete dell'utente nella cache locale. Se si esegue un nuovo controllo, ESET Endpoint Security ricercherà i file controllati nella cache. In caso di corrispondenza tra i file, questi verranno esclusi dal controllo.

La configurazione del **Server cache** contiene i seguenti elementi**:**

- **Nome host**: nome o indirizzo IP del computer in cui è collocata la cache.
- **Porta**: numero della porta utilizzata per le comunicazioni (identico a quello impostato nella cache locale condivisa).
- **Password**: specificare la password della cache locale condivisa ESET (se necessario).

3.8.1.3 Protezione file system in tempo reale

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



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

Supporti da controllare

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

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

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

Controlla

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

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

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

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

3.8.1.3.1 Parametri ThreatSense aggiuntivi

Parametri ThreatSense aggiuntivi per i file appena creati e modificati: i file appena creati registrano una maggiore probabilità di essere infettati rispetto a quelli esistenti. Per questo motivo il programma controlla tali file con parametri aggiuntivi. Oltre ai comuni metodi di controllo basati sulle firme, viene utilizzata anche la funzione di euristica avanzata, che è in grado di rilevare le nuove minacce prima del rilascio dell'aggiornamento del database delle firme antivirali. Oltre che sui file appena creati, il controllo viene eseguito sui file autoestraenti (SFX) e sugli eseguibili compressi, ovvero file eseguibili compressi internamente. Per impostazione predefinita, gli archivi vengono analizzati fino al 10° livello di nidificazione e controllati indipendentemente dalla loro dimensione effettiva. Per modificare le impostazioni di controllo dell'archivio, disattivare **Impostazioni predefinite controllo degli archivi**.

Per ulteriori informazioni sugli **Eseguibili compressi**, gli **Archivi autoestraenti** e l'**Euristica avanzata**, consultare Configurazione parametri motore ThreatSense.

Parametri ThreatSense aggiuntivi per i file eseguiti: per impostazione predefinita, durante l'esecuzione dei file, viene utilizzata l'Euristica avanzata. Una volta attivata, si consiglia vivamente di mantenere attivi l'Ottimizzazione intelligente e ESET Live Grid, allo scopo di ridurre l'impatto sulle prestazioni del sistema.

3.8.1.3.2 Livelli di pulizia

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

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

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

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

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

3.8.1.3.3 Controllo della protezione in tempo reale

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

NOTA: prima di eseguire un controllo della protezione in tempo reale, è necessario disattivare il firewall. Se il firewall è attivato, rileverà e impedirà di scaricare i file di test. Assicurarsi di riattivare il firewall subito dopo aver controllato la protezione file system in tempo reale.

3.8.1.3.4 Quando modificare la configurazione della protezione in tempo reale

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

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

3.8.1.3.5 Cosa fare se la protezione in tempo reale non funziona

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

La protezione in tempo reale è disattivata

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

Se la protezione in tempo reale non viene lanciata all'avvio del sistema, è probabile che l'opzione **Avvia automaticamente la protezione file system in tempo reale** non sia stata selezionata. Per attivare questa opzione, accedere a **Configurazione avanzata** (**F5**) e fare clic su **Antivirus** > **Protezione file system in tempo reale** > **Di base**. Assicurarsi di aver attivato il pulsante **Avvia automaticamente la protezione file system in tempo reale**.

La protezione in tempo reale non rileva né pulisce le infiltrazioni

verificare che nel computer non siano installati altri programmi antivirus. Se sono attivati contemporaneamente due scudi di protezione in tempo reale, possono entrare in conflitto. È consigliabile disinstallare gli altri programmi antivirus presenti nel sistema prima di installare ESET.

La protezione in tempo reale non viene avviata

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

3.8.1.4 Controllo del computer su richiesta

Lo scanner su richiesta rappresenta un componente importante di ESET Endpoint Security. Viene utilizzato per eseguire il controllo di file e di cartelle sul computer in uso. Dal punto di vista della protezione, è essenziale che i controlli del computer non vengano eseguiti solo quando si sospetta un'infezione, ma periodicamente, nell'ambito delle normali misure di protezione. Si consiglia di eseguire controlli approfonditi periodici (ad esempio, una volta al mese) del sistema allo scopo di rilevare virus non trovati dalla Protezione file system in tempo reale. Ciò può verificarsi se la protezione file system in tempo reale era disattivata in quel momento, il database antivirus era obsoleto o il file non è stato rilevato come virus nel momento in cui è stato salvato sul disco.

Sono disponibili due tipologie di **Controllo del computer**. **Controllo intelligente**, che consente di eseguire rapidamente il controllo del sistema senza che sia necessario configurare ulteriori parametri. **Controllo personalizzato**, che consente all'utente di selezionare un qualsiasi profilo di controllo predefinito e di definire specifiche destinazioni di controllo.

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

Controllo intelligente

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

Controllo personalizzato

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

Per scegliere le destinazioni di controllo, selezionare **Controllo computer** > **Controllo personalizzato** e scegliere un'opzione dal menu a discesa **Destinazioni di controllo** oppure specifiche destinazioni di controllo dalla struttura ad albero. Una destinazione di controllo può anche essere specificata immettendo il percorso della cartella o del/i file che si desidera includere. Se si desidera effettuare solo un controllo del sistema senza azioni di pulizia aggiuntive, selezionare **Controlla senza pulire**. Durante l'esecuzione di un controllo, è possibile scegliere uno dei tre livelli di pulizia facendo clic su **Configurazione...** > **Parametri ThreatSense** > **Pulizia**.

L'esecuzione di controlli del computer attraverso il controllo personalizzato è adatta a utenti avanzati con precedenti esperienze di utilizzo di programmi antivirus.

Controllo supporti rimovibili

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

Questo tipo di controllo può anche essere avviato facendo clic su **Controllo personalizzato**, quindi selezionando

Supporti rimovibili dal menu a discesa **Destinazioni di controllo** e facendo clic su **Controllo**.

È possibile utilizzare il menu a discesa **Azione dopo il controllo** per scegliere l'azione (Nessuna azione, Arresto, Riavvio e Metti in stand-by) da eseguire dopo il controllo.

Attiva arresto al termine del controllo: attiva un arresto pianificato al termine del controllo su richiesta del computer. Verrà visualizzata una finestra di dialogo in cui viene richiesto all'utente di confermare l'arresto entro 60 secondi. Fare clic su **Annulla** per disattivare l'arresto richiesto.

NOTA: è consigliabile eseguire un controllo del computer almeno una volta al mese. Il controllo può essere configurato come attività pianificata da **Strumenti** > **Pianificazione attività**.

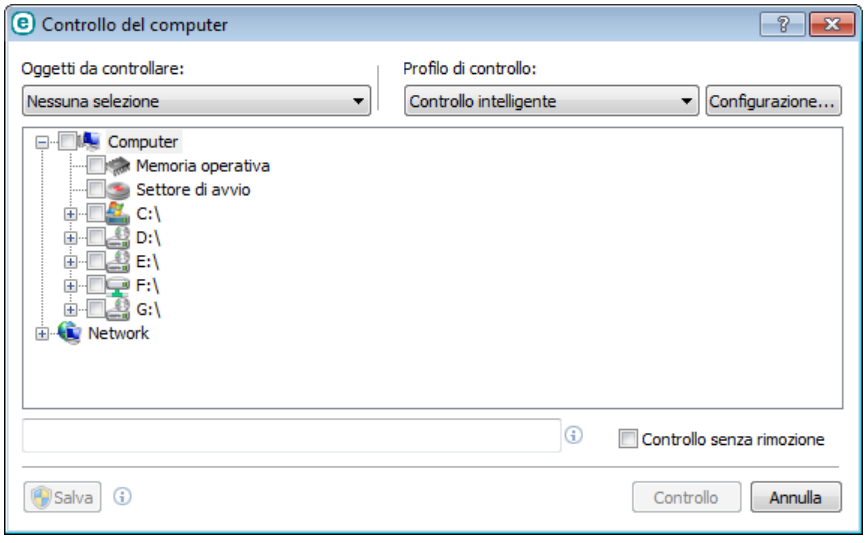
3.8.1.4.1 Launcher controllo personalizzato

Se si desidera controllare solo una specifica destinazione, è possibile utilizzare lo strumento del controllo personalizzato facendo clic su **Controllo computer** > **Controllo personalizzato** e selezionando un'opzione dal menu a discesa **Destinazioni di controllo** oppure scegliendo destinazioni specifiche dalla struttura (ad albero) della cartella.

La finestra destinazioni di controllo consente all'utente di definire gli oggetti (memoria, unità, settori, file e cartelle) sui quali verranno ricercate le infiltrazioni. Selezionare gli oggetti dalla struttura ad albero contenente un elenco di tutti i supporti disponibili nel computer. Il menu a discesa **Destinazioni di controllo** consente di selezionare gli oggetti da controllare predefiniti.

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

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



Gli elementi infetti non vengono puliti automaticamente. Il controllo senza rimozione può essere utilizzato per ottenere una panoramica dello stato di protezione corrente. Se si desidera effettuare solo un controllo del sistema senza azioni di pulizia aggiuntive, selezionare **Controlla senza pulire**. È inoltre possibile scegliere tra tre livelli di pulizia facendo clic su **Configurazione...** > **Parametri ThreatSense** > **Pulizia**. Le informazioni relative al controllo vengono salvate in un rapporto del controllo.

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

ThreatSense.

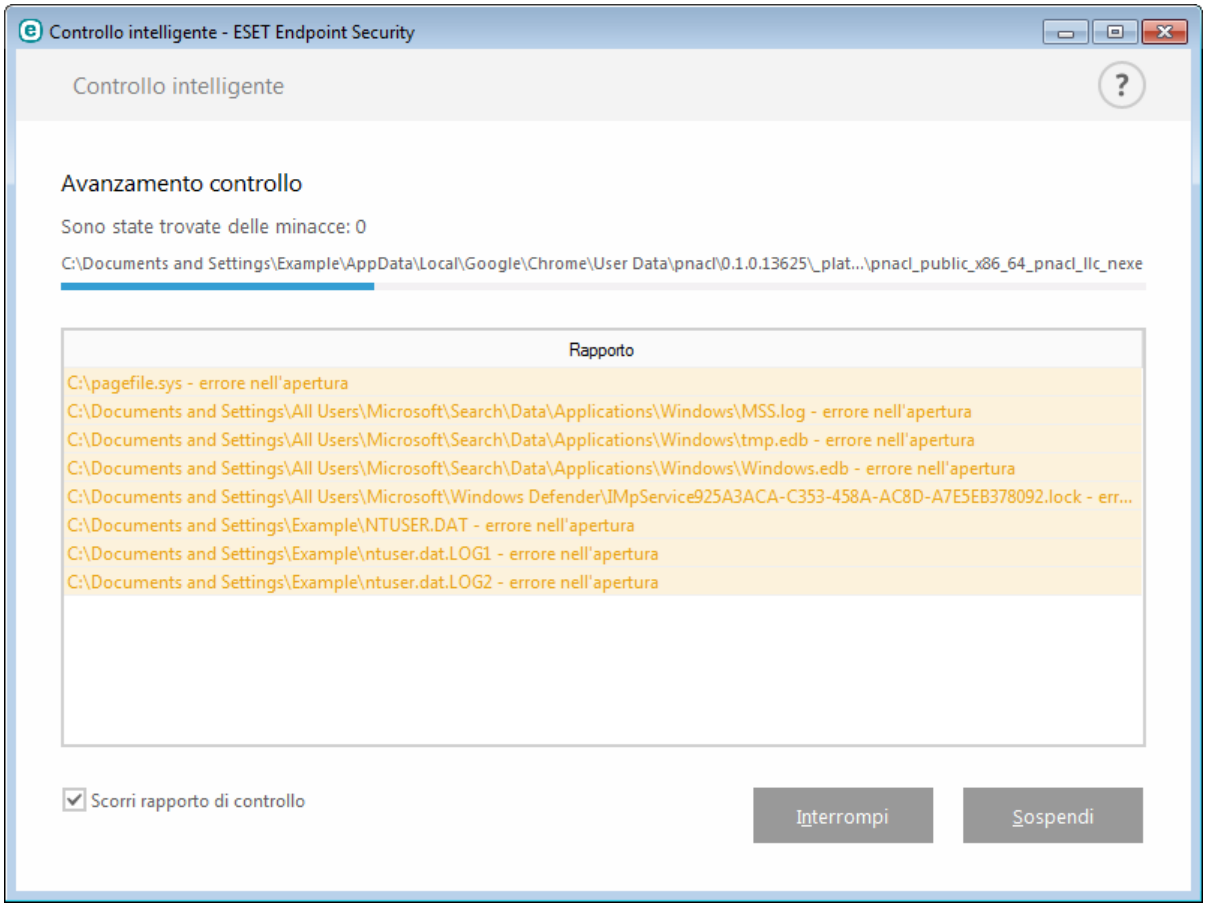
Fare clic su **Salva** per salvare le modifiche apportate alle selezioni di destinazioni, comprese quelle relative alla struttura delle cartelle.

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

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

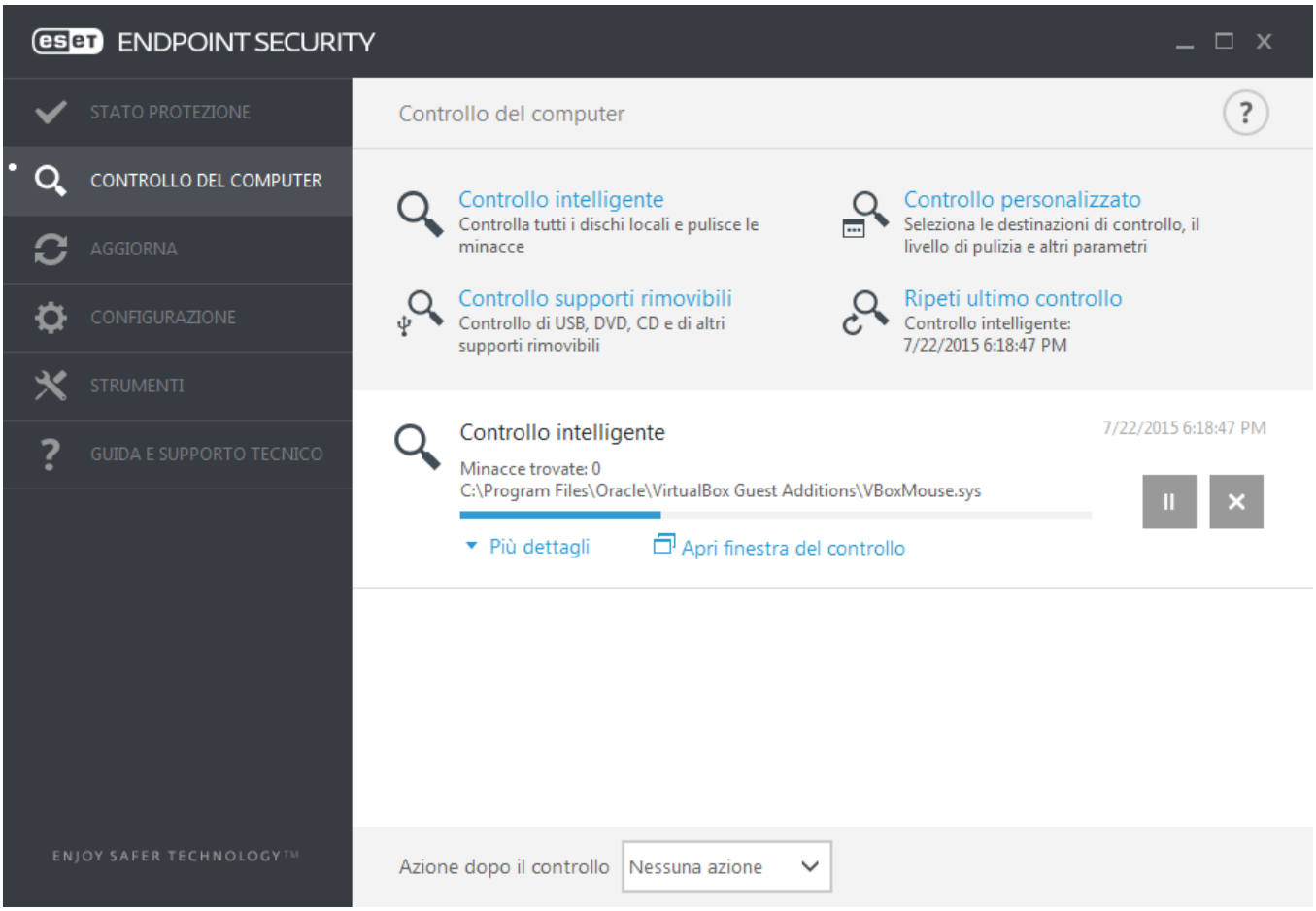
3.8.1.4.2 Avanzamento controllo

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



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

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



3.8.1.5 Controllo dispositivo

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

Dispositivi esterni supportati:

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

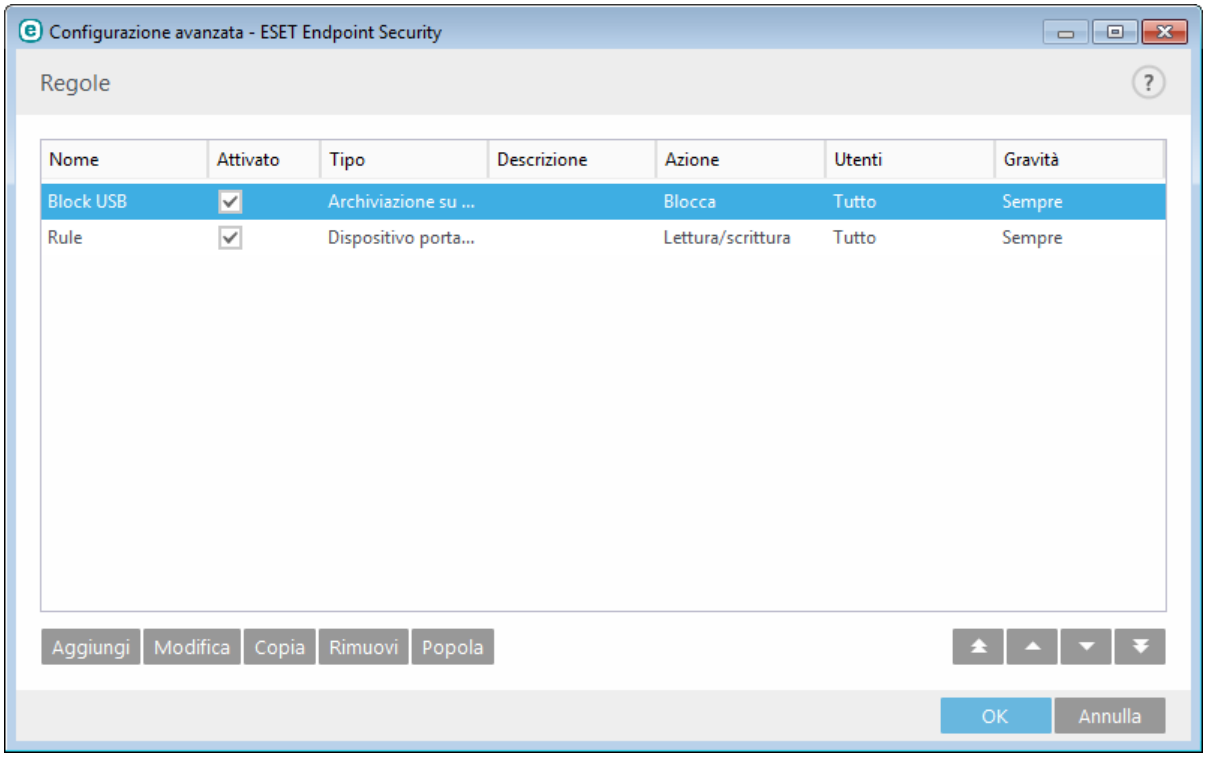
Le opzioni di configurazione del controllo dispositivi possono essere modificate in **Configurazione avanzata** (F5) > **Controllo dispositivi**.

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

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

3.8.1.5.1 Editor regole controllo dispositivi

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



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

Fare clic su **Aggiungi** o **Modifica** per gestire una regola. Deselezionare la casella di controllo **Attivata** accanto a una regola per disattivarla finché non si desidera utilizzarla nuovamente. Selezionare una o più regole e fare clic su **Rimuovi** per eliminarle in modo permanente.

Copia: crea una nuova regola con le opzioni predefinite utilizzate per un'altra regola selezionata.

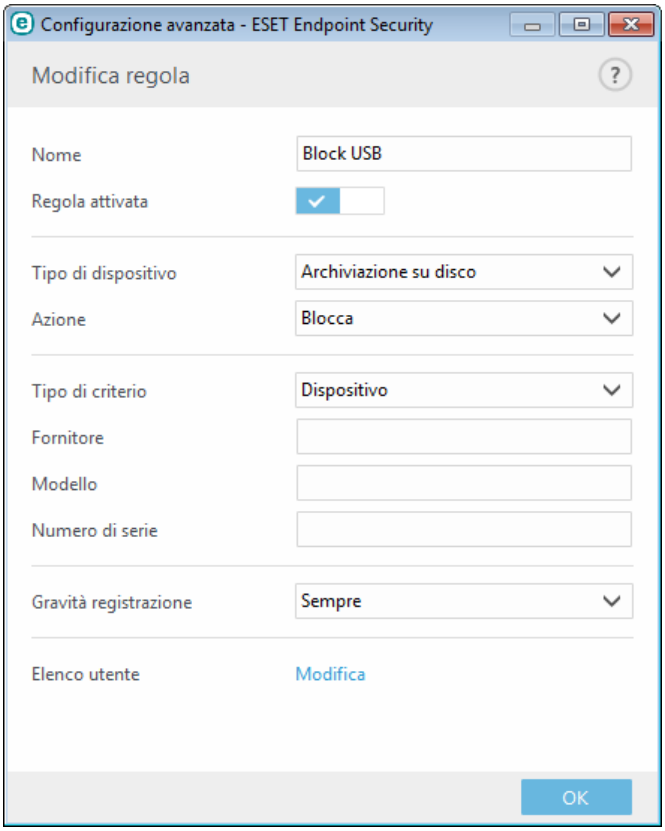
Fare clic su **Popola** per popolare automaticamente i parametri dei supporti rimovibili per i dispositivi collegati al computer.

Le regole sono disposte in ordine di priorità, partendo da quelle con priorità più elevata. È possibile spostare le regole (singolarmente o in gruppo) facendo clic su **In alto/Su/Giù/In basso**.

Il rapporto Controllo dispositivi registra tutte le occorrenze di attivazione del controllo dispositivi. Le voci del rapporto possono essere visualizzate nella finestra principale del programma di ESET Endpoint Security in **Strumenti** > **File di rapporto**.

3.8.1.5.2 Aggiunta di regole per il controllo dispositivi

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



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

Tipo di dispositivo

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

Azione

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

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

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

significa che i dispositivi Bluetooth possono essere solo consentiti, bloccati o avvisati).

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

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

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

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

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

Gravità

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

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

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

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

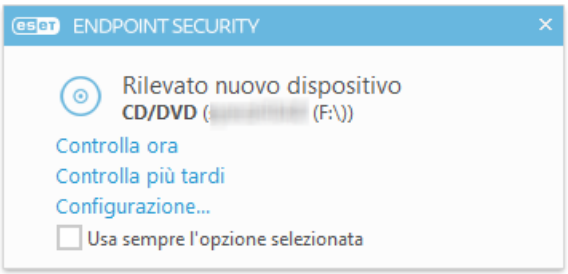
3.8.1.6 Supporti rimovibili

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

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

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

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



Controlla ora - Avvia il controllo del supporto rimovibile.

Controlla più tardi - Il controllo del supporto rimovibile verrà posticipato.

Configurazione - Apre la Configurazione avanzata.

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

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

3.8.1.7 Controllo stato di inattività

È possibile attivare lo scanner dello stato di inattività in **Configurazione avanzata** sotto a **Antivirus** > **Controllo stato di inattività** > **Standard**. Impostare il pulsante accanto a **Attiva controllo stato inattivo** su **On** per attivare questa funzionalità. Se il computer si trova nello stato di inattività, verrà eseguito un controllo silenzioso di tutti i dischi locali. Consultare la sezione Metodi di attivazione del rilevamento stato inattivo per un elenco completo di condizioni che è necessario soddisfare per attivare lo scanner dello stato inattivo.

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

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

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

- Screen saver
- Blocco computer
- Uscita utente

Fare clic su Configurazione parametri motore ThreatSense per modificare i parametri di controllo (ad esempio,

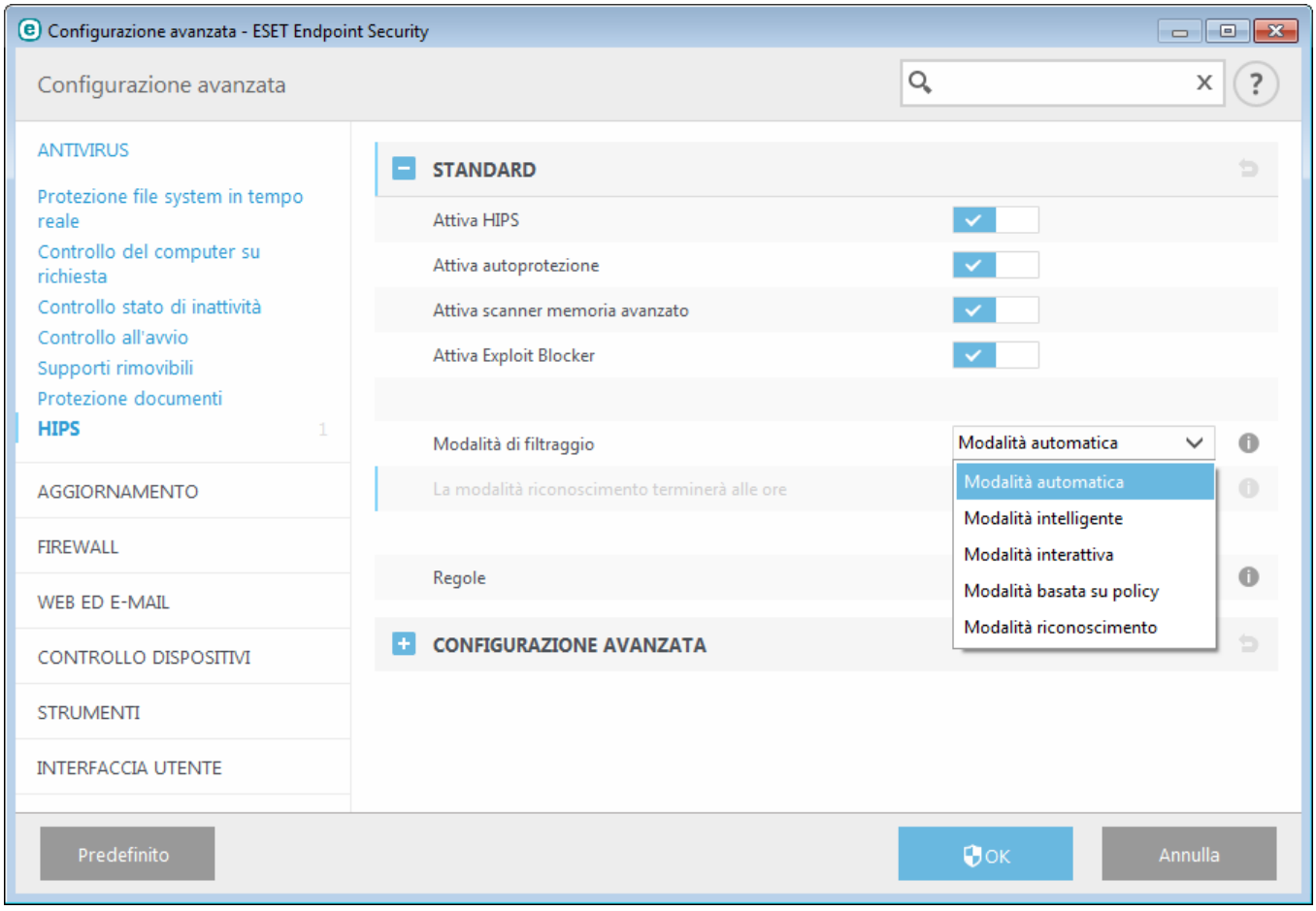
metodi di rilevamento) per lo scanner dello stato inattivo.

3.8.1.8 Sistema anti-intrusione basato su host (HIPS)

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

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

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



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

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

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

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

Modalità automatica - Le operazioni sono attivate, ad eccezione di quelle bloccate dalle regole predefinite che

proteggono il sistema.

Modalità interattiva - All'utente verrà richiesto di confermare le operazioni.

Modalità basata su criteri - Le operazioni sono bloccate.

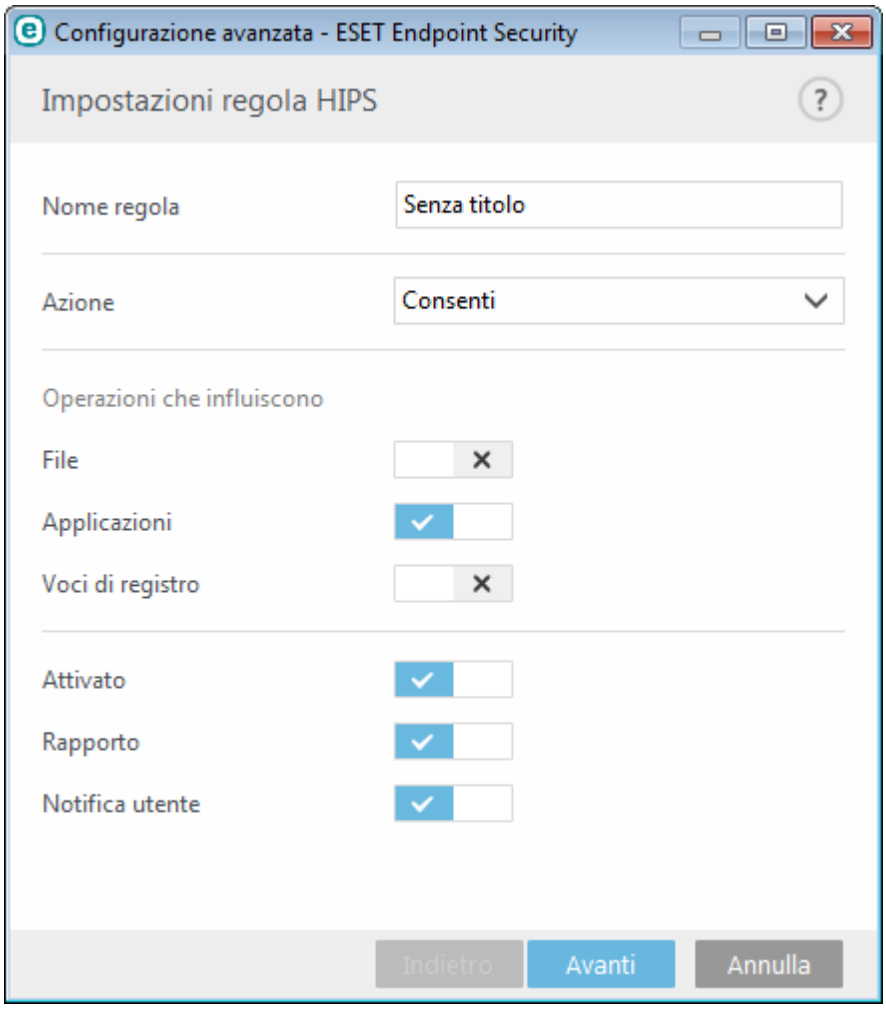
Modalità riconoscimento: le operazioni sono attivate e dopo ogni operazione viene creata una regola. Le regole create in questa modalità possono essere visualizzate nell'Editor regole, ma la loro priorità è inferiore rispetto alla priorità delle regole create manualmente o delle regole create nella modalità automatica. Selezionando la Modalità riconoscimento dal menu a discesa Modalità filtraggio HIPS, sarà disponibile l'impostazione **La modalità riconoscimento terminerà alle ore**. Selezionare la durata per la quale si desidera attivare la modalità riconoscimento, tenendo presente che il limite massimo è di 14 giorni. Una volta trascorsa la durata specificata, all'utente verrà richiesto di modificare le regole create dall'HIPS quando si trovava in modalità riconoscimento. È inoltre possibile scegliere un'altra modalità di filtraggio oppure posticipare la decisione e continuare a utilizzare la modalità riconoscimento.

Modalità intelligente - All'utente verranno segnalati solo gli eventi molto sospetti.

Il sistema HIPS monitora gli eventi all'interno del sistema operativo e reagisce in base a regole simili a quelle utilizzate dal rapporto del Personal firewall. Fare clic su **Modifica** per aprire la finestra di gestione delle regole HIPS. In questa sezione è possibile selezionare, creare, modificare o eliminare regole.

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

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



3.8.1.8.1 Configurazione avanzata

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

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

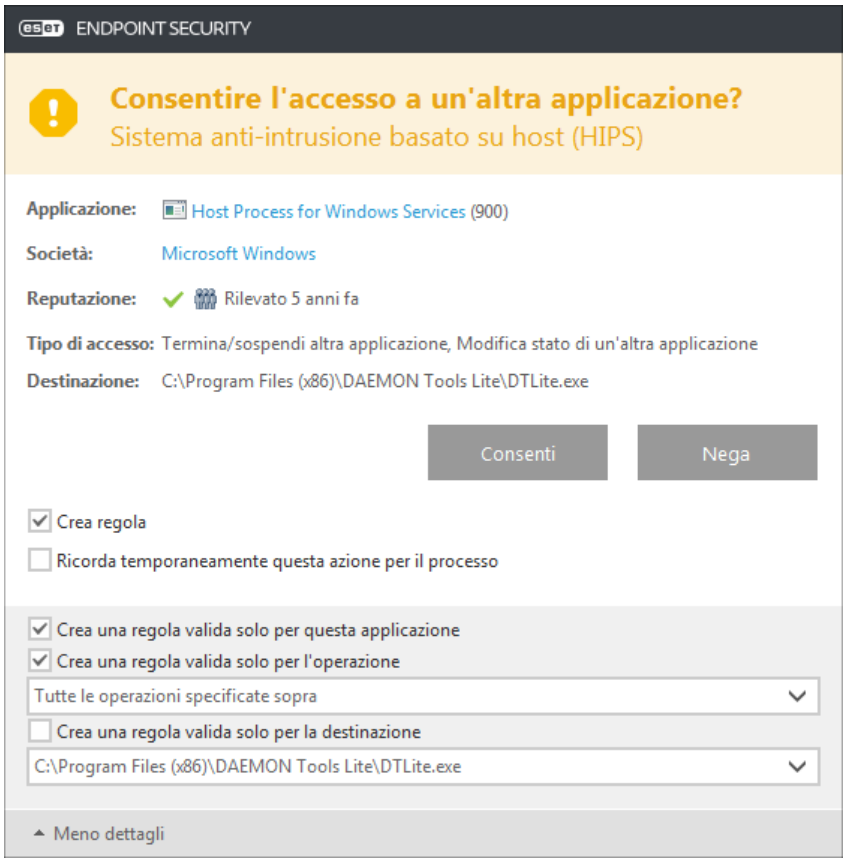
Registra tutte le operazioni bloccate: tutte le operazioni bloccate verranno scritte sul registro HIPS.

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

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

3.8.1.8.2 Finestra interattiva HIPS

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



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

Ricorda temporaneamente questa azione per il processo causa un'azione (**Consenti/Nega**) da utilizzare finché non verrà apportata una modifica alle regole o alla modalità di filtraggio oppure non verrà eseguito un aggiornamento del modulo HIPS o un riavvio del sistema. In seguito a una di queste tre azioni, le regole temporanee verranno eliminate.

3.8.1.9 Modalità presentazione

La modalità presentazione è una funzionalità pensata per gli utenti che richiedono un utilizzo ininterrotto del software, non desiderano essere disturbati dalle finestre popup e desiderano ridurre al minimo l'utilizzo della CPU. La modalità presentazione può essere utilizzata anche durante le presentazioni che non possono essere interrotte dall'attività antivirus. Se attivata, tutte le finestre popup verranno disattivate e le attività pianificate non verranno eseguite. La protezione del sistema è ancora in esecuzione in background, ma non richiede l'interazione dell'utente.

Fare clic su **Configurazione** > **Computer**, quindi sul pulsante accanto a **Modalità presentazione** per attivare la modalità presentazione manualmente. In **Configurazione avanzata** (F5), fare clic su **Strumenti** > **Modalità presentazione**, quindi sul pulsante accanto a **Attiva automaticamente modalità Presentazione quando vengono eseguite applicazioni in modalità a schermo intero** per far sì che la funzione ESET Endpoint Security attivi automaticamente la modalità presentazione quando vengono eseguite applicazioni in modalità a schermo intero. L'attivazione della modalità presentazione rappresenta un potenziale rischio per la protezione. Per tale motivo, l'icona relativa allo stato della protezione sulla barra delle attività diventa di colore arancione e viene visualizzato un avviso. Questo avviso verrà visualizzato anche nella finestra principale del programma dove **Modalità**

presentazione attivata comparirà in arancione.

Dopo aver attivato **Attiva automaticamente modalità presentazione quando vengono eseguite applicazioni in modalità a schermo intero**, la modalità presentazione si attiverà all'avvio di un'applicazione in modalità a schermo intero e si interromperà automaticamente all'uscita dall'applicazione. Questa funzionalità si rivela particolarmente utile per l'attivazione della modalità presentazione subito dopo l'avvio di un gioco, l'apertura di un'applicazione in modalità a schermo intero o l'avvio di una presentazione.

È inoltre possibile selezionare **Disattiva automaticamente modalità presentazione** per definire l'intervallo di tempo espresso in minuti dopo il quale la modalità presentazione verrà automaticamente disattivata.

NOTA: se il rapporto del Personal Firewall è in modalità interattiva e la modalità presentazione è attivata, potrebbero verificarsi dei problemi di connessione a Internet. Ciò potrebbe causare problemi se si inizia un gioco che necessita della connessione a Internet. In genere, all'utente viene richiesto di confermare tale azione (se non sono state definite regole o eccezioni di comunicazione). Tuttavia, in modalità presentazione, l'interazione dell'utente è disattivata. La soluzione consiste nel definire una regola di comunicazione per ogni applicazione che potrebbe entrare in conflitto con questo comportamento o utilizzare una Modalità di filtro differente nel rapporto del Personal firewall. Tenere presente che se la modalità presentazione è attivata e si accede a una pagina Web o un'applicazione che potrebbe rappresentare un rischio per la protezione, questa potrebbe essere bloccata, ma non verranno visualizzati avvisi o spiegazioni a causa della disattivazione dell'interazione dell'utente.

3.8.1.10 Controllo all'avvio

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

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

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

3.8.1.10.1 Controllo automatico file di avvio

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

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

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

Sono inoltre inclusi due gruppi specifici:

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

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

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

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

3.8.1.11 Protezione documenti

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

Integrazione nel sistema consente di attivare il sistema di protezione. Per modificare questa opzione, premere F5 per aprire la finestra Configurazione avanzata e fare clic su **Antivirus** > **Protezione documenti** nella struttura Configurazione avanzata.

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

3.8.1.12 Esclusioni

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

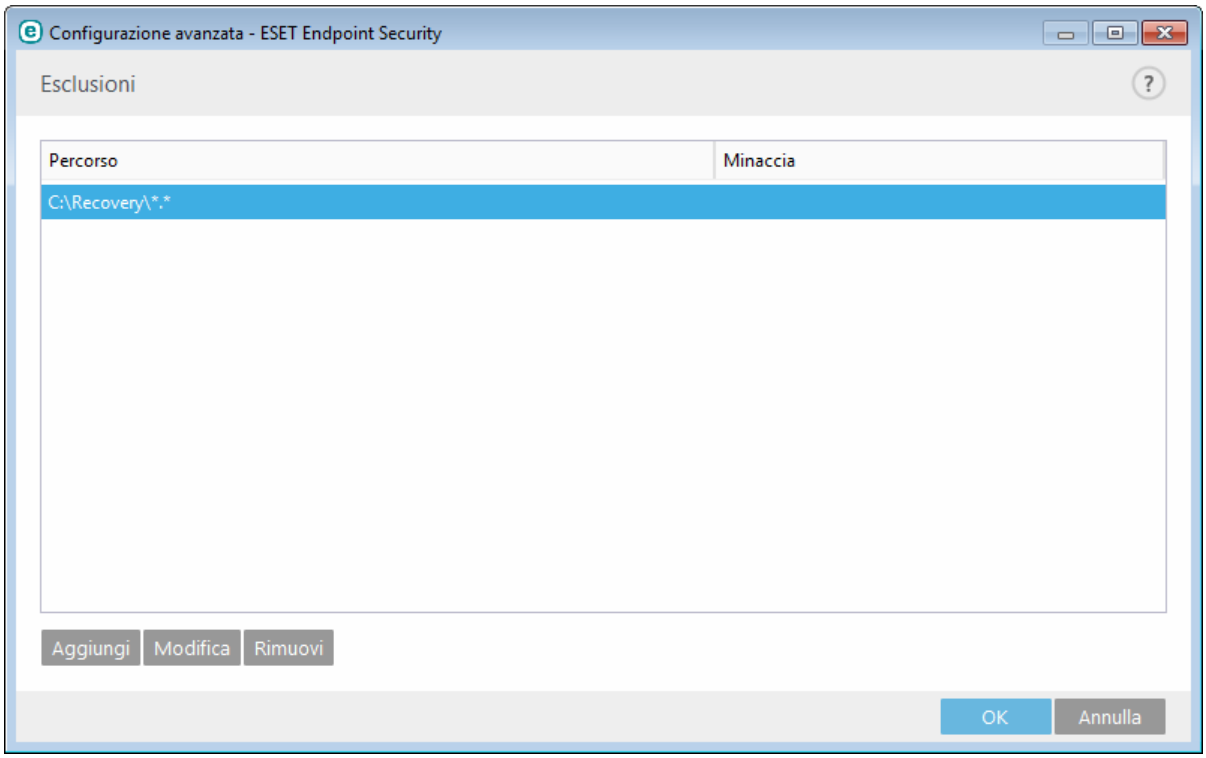
Per escludere un oggetto dal controllo:

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

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

Esempi

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



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

Colonne

Percorso - Percorso dei file e delle cartelle esclusi.

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

Elementi di controllo

Aggiungi - Esclude gli oggetti dal rilevamento.

Modifica - Consente all'utente di modificare le voci selezionate.

Rimuovi: rimuove le voci selezionate.

3.8.1.13 Configurazione parametri motore ThreatSense

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

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

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

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

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

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

Oggetti da controllare

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

Memoria operativa - Ricerca le minacce che attaccano la memoria operativa del sistema.

Settori di avvio - Controlla i settori di avvio alla ricerca di virus nel record di avvio principale.

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

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

Archivi autoestraenti - Gli archivi autoestraenti (SFX) sono archivi che non necessitano di programmi speciali, ovvero archivi, per decomprimersi.

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

Opzioni di controllo

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

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

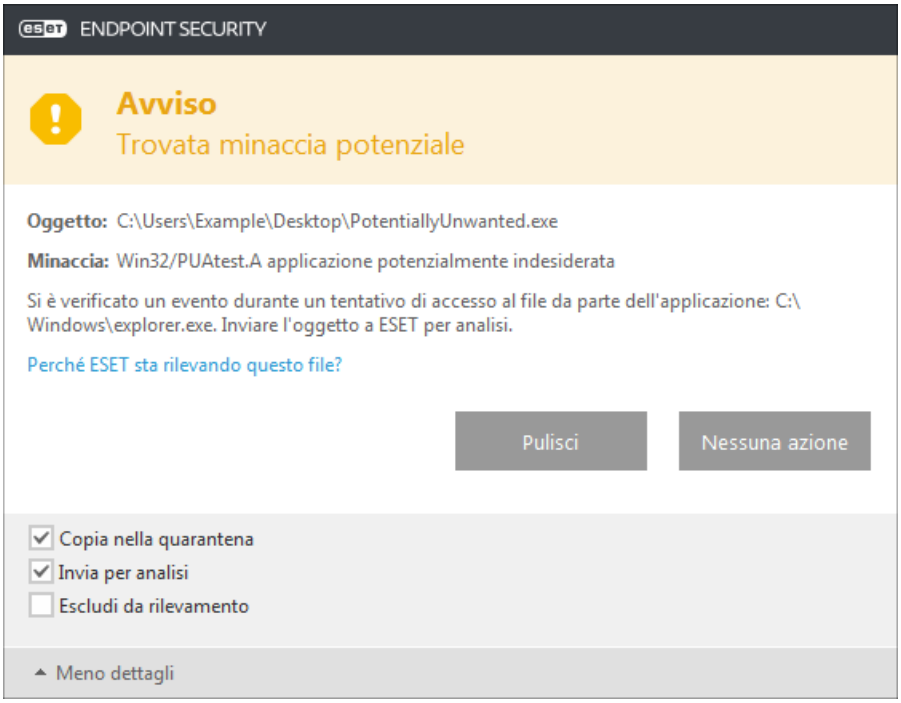
Euristica avanzata/DNA/Firme Smart: l'euristica avanzata si basa su un algoritmo di euristica esclusivo sviluppato da ESET, ottimizzato per il rilevamento dei worm e dei trojan horse e scritto in linguaggi di programmazione di alto livello. L'utilizzo dell'euristica avanzata determina un aumento esponenziale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

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

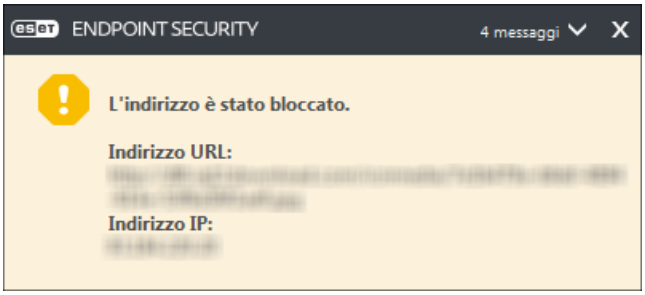
Avviso: trovata minaccia potenziale

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

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

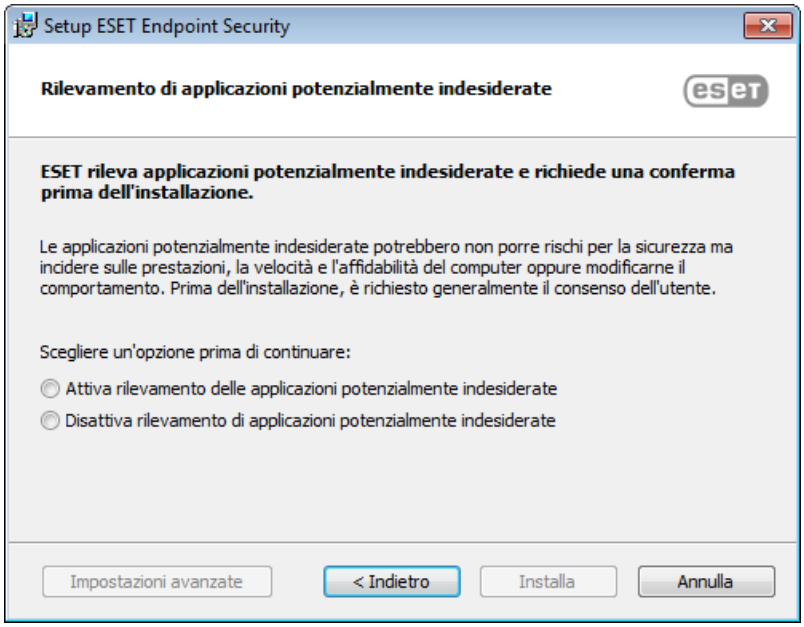


Se un'applicazione potenzialmente indesiderata viene rilevata e non può essere pulita, verrà visualizzata la finestra di notifica **L'indirizzo è stato bloccato** nell'angolo in basso a destra della scherma. Per ulteriori informazioni su questo evento, accedere a **Strumenti** > **File di rapporto** > **Siti Web filtrati** dal menu principale.



Applicazioni potenzialmente indesiderate: impostazioni

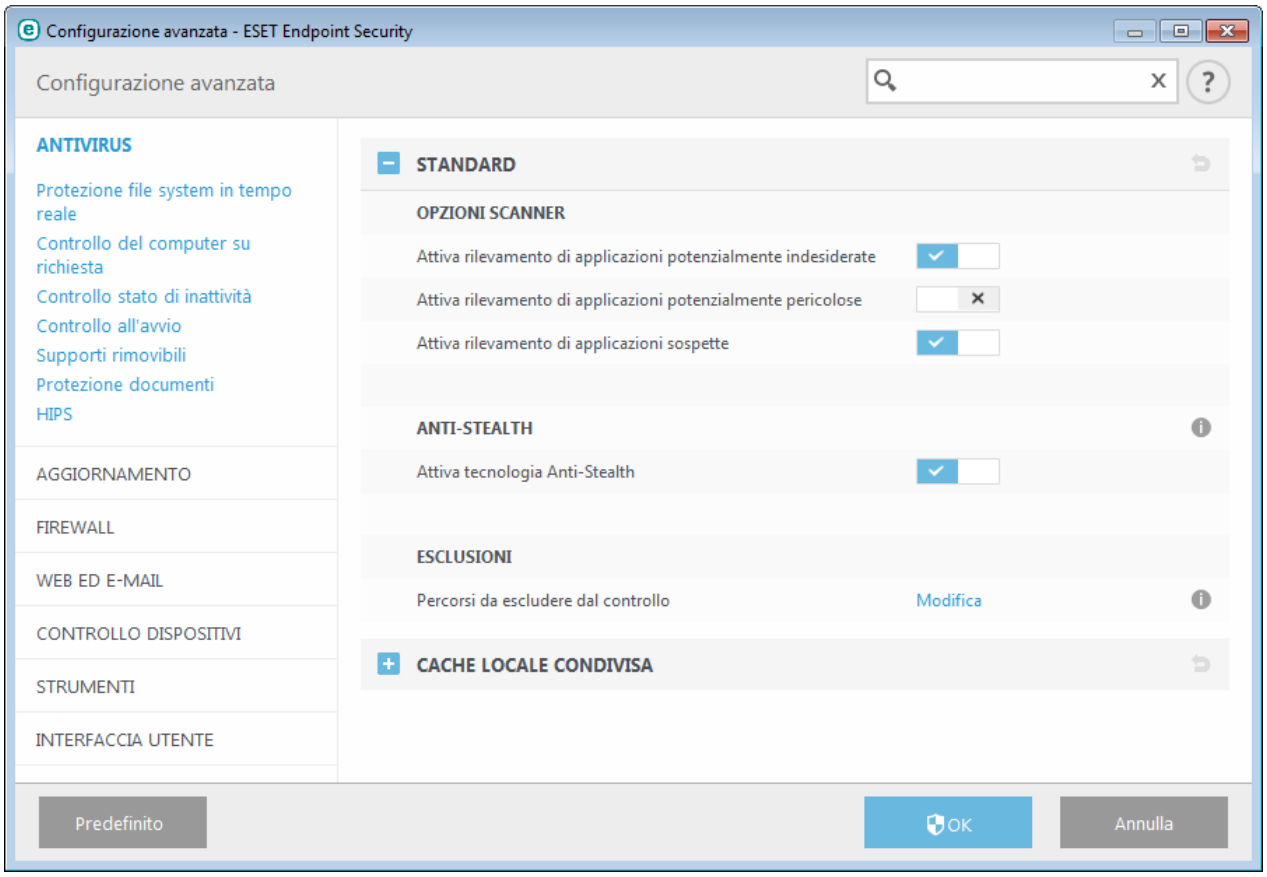
Durante l'installazione di un prodotto ESET, l'utente può decidere di attivare il rilevamento di applicazioni potenzialmente indesiderate, come illustrato di seguito:



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

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

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



Applicazioni potenzialmente indesiderate: wrapper di software

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

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

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

Pulizia

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

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

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

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

un'azione da eseguire.

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

Esclusioni

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

Altro

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

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

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

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

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

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

Limiti

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

Impostazioni oggetti

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

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

Configurazione controllo degli archivi

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

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

predefinito è: *illimitato*.

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

3.8.1.13.1 Esclusioni

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

Per impostazione predefinita, vengono controllati tutti i file. È possibile aggiungere qualunque estensione all'elenco dei file esclusi dal controllo.

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

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

I simboli speciali * (asterisco) e ? (punto interrogativo). L'asterisco rappresenta qualsiasi stringa di caratteri, mentre il punto interrogativo rappresenta qualsiasi simbolo.

3.8.2 Rete

Il rapporto del Personal firewall controlla tutto il traffico di rete in entrata e in uscita dal sistema, consentendo o rifiutando singole connessioni di rete in base alle regole di filtraggio dell'utente. Offre protezione contro gli attacchi di computer remoti e consente di bloccare servizi potenzialmente pericolosi. Il rapporto del Personal Firewall offre anche la funzionalità IDS/IPS mediante l'ispezione del contenuto del traffico di rete consentito e il blocco del traffico considerato potenzialmente dannoso.

La configurazione del **Rapporto del Personal firewall** è disponibile nel riquadro **Configurazione** sotto a **Rete**. Qui è possibile regolare la modalità di filtraggio per ESET Personal firewall. È inoltre possibile accedere a impostazioni più dettagliate facendo clic sulla rotella a forma di ingranaggio > **Configura** accanto a **Personal firewall**, oppure premendo **F5** per accedere a Configurazione avanzata.

Protezione attacchi di rete (IDS) : analizza il contenuto del traffico di rete e offre protezione dagli attacchi di rete. Tutto il traffico ritenuto dannoso verrà bloccato. È possibile disattivare la protezione attacchi di rete per uno specifico periodo di tempo facendo clic su .

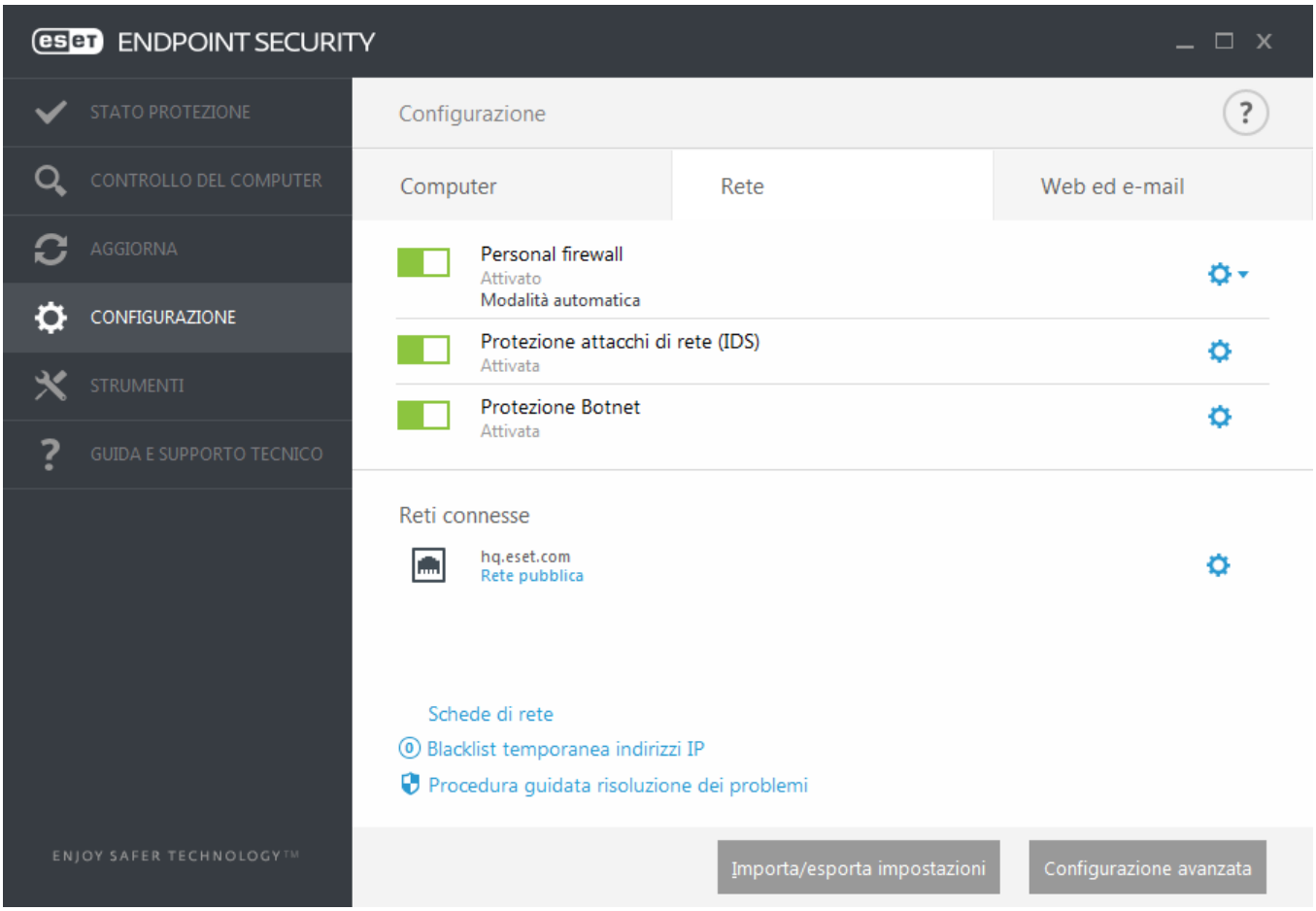
Protezione botnet - Consente di individuare in maniera rapida e accurata il malware sul sistema. È possibile disattivare la protezione botnet per uno specifico periodo di tempo facendo clic su .

Reti connesse: consente di visualizzare le reti alle quali si connettono le schede di rete. Dopo aver selezionato la rotella a forma di ingranaggio, all'utente verrà richiesto di selezionare un tipo di protezione per la rete alla quale è connesso mediante la scheda di rete.

Schede di rete: qui è possibile visualizzare ciascuna scheda di rete insieme al relativo profilo firewall assegnato e l'area attendibile. Per ulteriori informazioni, consultare il paragrafo Schede di rete.

Blacklist temporanea indirizzi IP: consente di visualizzare un elenco di indirizzi IP rilevati come la fonte degli attacchi e aggiunti alla blacklist per il blocco delle connessioni per uno specifico periodo di tempo. Per ulteriori informazioni, fare clic su questa opzione e premere F1.

Procedura guidata per la risoluzione dei problemi: aiuta l'utente a risolvere problemi di connettività causati da ESET Personal firewall. Per ulteriori informazioni, consultare il paragrafo Procedura guidata per la risoluzione dei problemi.



Fare clic sulla rotella a forma di ingranaggio accanto al **Rapporto del Personal firewall** per accedere alle seguenti impostazioni:

Configura...: apre la finestra del rapporto del Personal firewall in Configurazione avanzata, dove è possibile definire le modalità di gestione della comunicazione di rete dal parte del firewall.

Blocca tutto il traffico: tutte le altre comunicazioni in entrata e in uscita saranno bloccate dal rapporto del Personal firewall. Utilizzare questa opzione se si sospetta un rischio di protezione critico che richiede la disconnessione del sistema dalla rete. Se il Filtraggio traffico di rete è in modalità **Blocca tutto il traffico**, fare clic su **Smetti di bloccare tutto il traffico** per ripristinare il normale funzionamento del firewall.

Interrompi firewall (consenti tutto il traffico): è l'esatto contrario della funzione Blocca tutto il traffico di rete. Se selezionata, tutte le opzioni di filtraggio del Firewall personale saranno disattivate e tutte le connessioni in ingresso e in uscita saranno consentite. Se il filtraggio del traffico di rete si trova in questa modalità, fare clic su **Attiva firewall** per riattivare il firewall.

Modalità automatica: (in caso di attivazione di un'altra modalità di filtraggio) - Fare clic per impostare la modalità di filtraggio automatica (con regole definite dall'utente).

Modalità interattiva: (in caso di attivazione di un'altra modalità di filtraggio) - Fare clic per impostare la modalità di filtraggio interattiva.

3.8.2.1 Rapporto del Personal firewall

Il rapporto del Personal firewall controlla tutto il traffico di rete in entrata e in uscita dal sistema, consentendo o rifiutando singole connessioni di rete in base a specifiche regole di filtraggio. Il sistema offre protezione contro gli attacchi provenienti da computer remoti e attiva il blocco di alcuni servizi. Il rapporto del Personal Firewall offre anche protezione antivirus per i protocolli HTTP, POP3 e IMAP. Questa funzionalità rappresenta un elemento molto importante nella protezione del computer.

Attiva protezione attacchi di rete (IDS) : analizza il contenuto del traffico di rete e offre protezione dagli attacchi di rete. Tutto il traffico ritenuto dannoso verrà bloccato.

Attiva protezione Botnet: rileva e blocca le comunicazioni con comandi dannosi e controlla i server in base a modelli tipici in caso di infezione del computer e di tentativo di comunicazione di un bot.

Per ESET Endpoint Security Personal Firewall, sono disponibili quattro modalità di filtraggio. Le impostazioni delle modalità di filtraggio sono disponibili in **Configurazione avanzata** (F5) facendo clic su **Personal firewall**. Il comportamento del firewall varia in base alla modalità di filtraggio. Le modalità di filtraggio influenzano anche il livello di interazione da parte dell'utente.

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

Modalità automatica: modalità predefinita. Questa modalità è adatta agli utenti che preferiscono un utilizzo semplice e comodo del firewall, senza dover definire delle regole. In modalità automatica, è possibile, ma non obbligatorio, creare regole personalizzate e definite dall'utente. La modalità automatica consente tutto il traffico in uscita per il sistema specifico e blocca la maggior parte del traffico in entrata (ad eccezione di porzioni di traffico provenienti dall'area attendibile, in base alle autorizzazioni specificate in IDS e opzioni avanzate/Servizi consentiti e al traffico in entrata che risponde alla recente comunicazione in uscita verso lo stesso sito remoto).

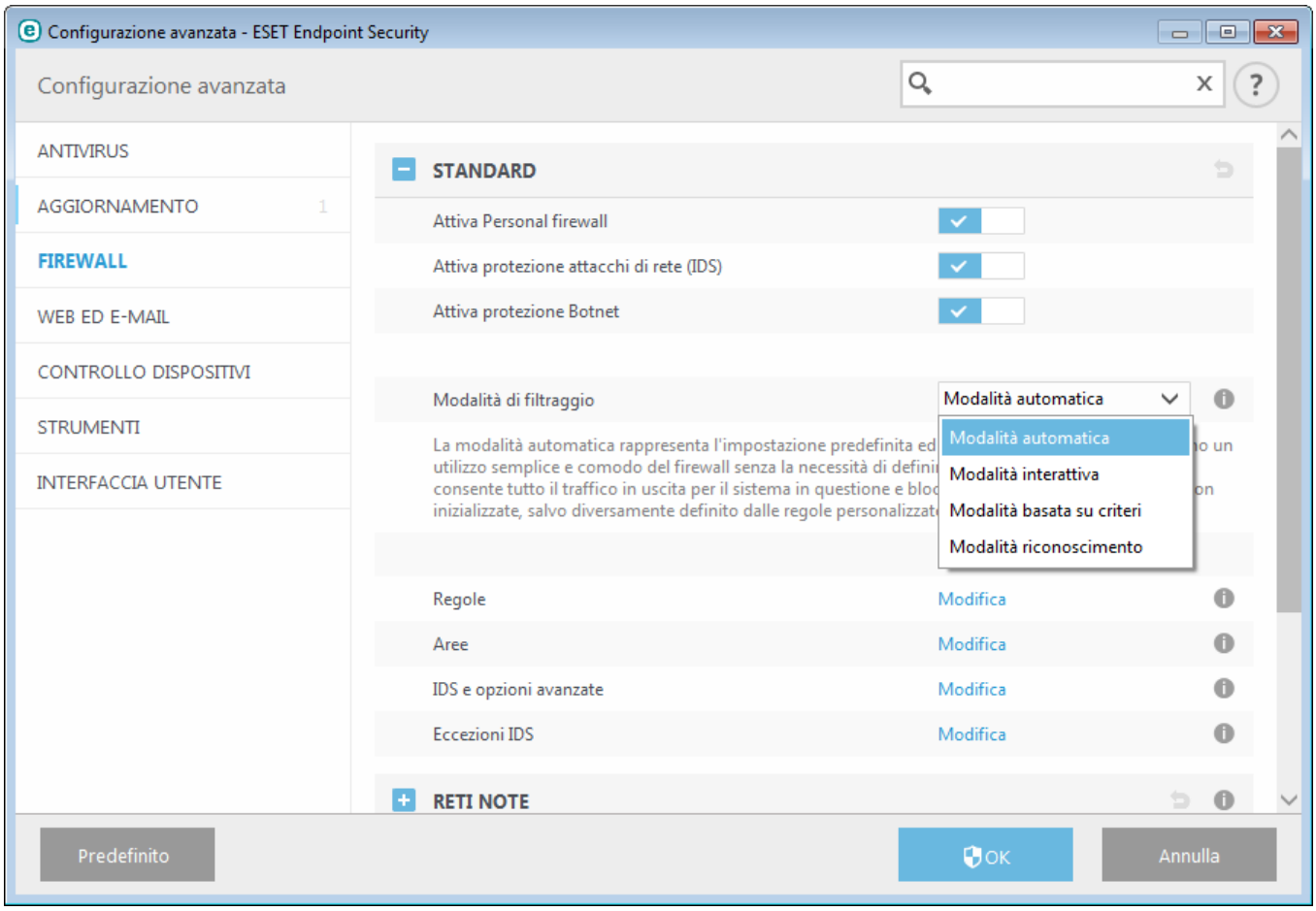
Modalità interattiva: consente all'utente di creare una configurazione personalizzata per il rapporto del Personal firewall. Quando viene rilevata una comunicazione per la quale non esiste alcuna regola applicabile, viene visualizzata una finestra di dialogo che segnala una connessione sconosciuta. La finestra di dialogo consente di accettare o rifiutare la comunicazione e la decisione può essere salvata come nuova regola per il rapporto del Personal firewall. Se si decide di creare una nuova regola, tutte le connessioni future di questo tipo saranno consentite o bloccate in base a questa regola.

Modalità basata su criteri: blocca tutte le connessioni non definite da una regola specifica che le consente. Questa modalità consente agli utenti esperti di definire regole che consentono solo connessioni sicure e desiderate. Tutte le altre connessioni non specificate saranno bloccate dal rapporto del Personal firewall.

Modalità riconoscimento: crea e salva automaticamente le regole. È inoltre ideale per la configurazione iniziale del rapporto del Personal firewall. Non è richiesta alcuna interazione da parte dell'utente, poiché ESET Endpoint Security salva le regole in base a parametri predefiniti. La modalità riconoscimento non è una modalità protetta. Pertanto, è consigliabile utilizzarla solo fino a quando non siano state create tutte le regole per le comunicazioni richieste.

I profili possono essere utilizzati per personalizzare il comportamento del rapporto del Personal firewall ESET Endpoint Security specificando set di regole diversi in situazioni diverse.

Valuta anche le regole di Windows Firewall: in modalità automatica, consente il traffico in entrata consentito da Windows Firewall, a meno che non venga bloccato dalle regole del rapporto del Personal Firewall.



Regole: qui è possibile aggiungere regole e definire le modalità di gestione del traffico di rete da parte del rapporto del Personal firewall.

Aree: qui è possibile creare aree costituite da vari indirizzi IP.

IDS e opzioni avanzate: consente all'utente di configurare le opzioni di filtraggio avanzate e la funzionalità IDS (utilizzata ai fini del rilevamento di vari tipi di attacchi ed exploit).

Eccezioni IDS: consente all'utente di aggiungere eccezioni IDS e personalizzare le reazioni alle attività dannose.

3.8.2.1.1 Modalità riconoscimento

La modalità riconoscimento crea e salva automaticamente una regola per ciascuna comunicazione stabilita all'interno del sistema. Non è richiesta alcuna interazione da parte dell'utente, poiché ESET Endpoint Security salva le regole in base a parametri predefiniti.

Questa modalità espone il sistema a rischi ed è consigliata esclusivamente per la configurazione iniziale del rapporto del Personal firewall.

Attivare la modalità riconoscimento in **Configurazione avanzata** (F5) > **Personal firewall** > **Impostazioni modalità riconoscimento** per visualizzarne le opzioni specifiche. Questa sezione contiene le seguenti voci:

Avviso: in modalità riconoscimento, il Firewall personale non filtra le comunicazioni. Sono consentite tutte le comunicazioni in entrata e in uscita. In questa modalità il computer non viene protetto completamente dal Firewall personale.

Tipo di comunicazione - Selezionare i parametri di creazione delle regole specifiche di ciascun tipo di comunicazione. Sono disponibili quattro tipi di comunicazione:

Traffico in entrata dall'area attendibile - Un esempio di connessione in entrata all'interno dell'area attendibile è rappresentato da un computer remoto all'interno dell'area attendibile che tenta di stabilire una comunicazione con un'applicazione locale in esecuzione sul computer dell'utente.

Traffico in uscita all'area attendibile - Un'applicazione locale che tenta di stabilire una connessione a un altro computer nella rete locale o all'interno di una rete dell'area attendibile.

Traffico Internet in entrata - Un computer remoto che tenta di comunicare con un'applicazione in esecuzione sul computer.

Traffico Internet in uscita - Un'applicazione locale che tenta di stabilire una connessione a un altro computer.

Ciascuna sezione consente all'utente di definire i parametri da aggiungere alle regole appena create:

Aggiungi porta locale - Contiene il numero della porta locale da destinare alle comunicazioni di rete. In linea generale, per le comunicazioni in uscita vengono generati numeri in modo casuale. Per questo motivo, è consigliabile attivare questa opzione unicamente per le comunicazioni in entrata.

Aggiungi applicazione - Contiene il nome dell'applicazione locale. Questa opzione è adatta per le future regole a livello di applicazioni (regole che definiscono la comunicazione per un'intera applicazione). È ad esempio possibile attivare le comunicazioni solo per un browser Web o per un client e-mail.

Aggiungi porta remota - Contiene il numero della porta remota da destinare alle comunicazioni di rete. È ad esempio possibile accettare o rifiutare un servizio specifico associato a un numero di porta standard (HTTP - 80, POP3 - 110 e così via).

Aggiungi indirizzo IP remoto/area attendibile - Una zona o un indirizzo IP remoto può essere utilizzato come parametro per le nuove regole che definiscono tutte le connessioni di rete tra il sistema locale e tale area o indirizzo remoto. Questa opzione è ideale se si desidera definire le azioni destinate a un determinato computer o a un gruppo di computer collegati in rete.

Numero massimo di regole diverse per un'applicazione - Se un'applicazione comunica a vari indirizzi IP ecc., attraverso porte differenti, il firewall nella modalità riconoscimento creerà un numero di regole appropriato per tale applicazione. Questa opzione consente all'utente di ridurre il numero di regole che è possibile creare per un'applicazione.

3.8.2.2 Profili firewall

I profili possono essere utilizzati per controllare il comportamento di ESET Endpoint Security Personal firewall. Quando si crea o si modifica una regola del rapporto del Personal firewall, è possibile assegnarla a un profilo specifico o applicarla a tutti i profili. Quando un profilo è attivo su un'interfaccia di rete, vengono applicate solo le regole globali (regole senza profilo specificato) e le regole assegnate a tale profilo. È possibile creare profili multipli con regole diverse assegnate alle schede di rete o alle reti per agevolare la modifica del comportamento del rapporto del Personal firewall.

Fare clic su **Modifica** accanto a **Elenco di profili** per aprire la finestra **Profili firewall** in cui è possibile modificare i profili.

È possibile configurare una scheda di rete per utilizzare un profilo configurato per una rete specifica alla quale è collegata. È inoltre possibile assegnare un profilo specifico da utilizzare su una rete specifica in **Configurazione avanzata** (F5) > **Personal firewall** > **Reti note**. Selezionare una rete dall'elenco di **Reti note** e fare clic su **Modifica**per assegnare un profilo firewall alla rete specifica dal menu a discesa **Profilo firewall**. Se alla rete non è stato assegnato alcun profilo, verrà utilizzato il profilo predefinito della scheda. Se la scheda di rete è configurata in modo da non utilizzare il profilo di rete, il relativo profilo predefinito verrà utilizzato indipendentemente dalla rete a cui è connessa. Se non è disponibile alcun profilo per la configurazione di una rete o di una scheda, verrà utilizzato il profilo predefinito globale. Per assegnare un profilo a una scheda di rete, selezionare la scheda di rete, fare clic su **Modifica** accanto a **Profili assegnati alle schede di rete**, selezionare il profilo dal menu a discesa **Profilo firewall predefinito** e fare clic su **Salva**.

Quando il rapporto del Personal firewall passa a un altro profilo, viene visualizzata una notifica nell'angolo in basso a destra vicino all'orologio di sistema.

3.8.2.2.1 Profili assegnati alle schede di rete

Cambiando profili, è possibile apportare rapidamente varie modifiche al comportamento del firewall. Ad esempio, è possibile impostare regole personalizzate e applicarle a specifici profili. Le voci relative a tutte le schede di rete presenti sulla macchina vengono aggiunte automaticamente all'elenco di **Schede di rete**.

Colonne

Nome - Nome della scheda di rete.

Profilo firewall predefinito - Il profilo predefinito viene utilizzato nel momento in cui la rete a cui l'utente è connesso non presenta alcun profilo configurato oppure la scheda di rete è impostata in modo tale da non utilizzare un profilo di rete.

Profilo rete preferito - Attivando **Imposta il profilo firewall della rete connessa come preferito**, la scheda di rete utilizzerà il profilo firewall assegnato a una rete connessa tutte le volte che ciò risulta possibile.

Elementi di controllo

Aggiungi - Aggiunge una nuova scheda di rete.

Modifica - Consente all'utente di modificare una scheda di rete esistente.

Rimuovi - Selezionare una scheda di rete e fare clic su **Rimuovi** se si desidera rimuovere una scheda di rete dall'elenco.

OK/Annulla - Fare clic su **OK** se si desidera salvare le modifiche oppure su **Annulla** per lasciare l'impostazione invariata.

3.8.2.3 Configurazione e uso delle regole

Le regole rappresentano un set di condizioni utilizzato per testare tutte le connessioni di rete e tutte le azioni assegnate a queste condizioni. Le regole del rapporto del Personal firewall consentono all'utente di definire l'azione da intraprendere nel caso in cui vengano stabiliti vari tipi di connessioni di rete. Per accedere alla configurazione del filtraggio regole, aprire **Configurazione avanzata** (F5) > **Personal firewall** > **Standard**. Alcune regole predefinite sono legate alle caselle di controllo dai **servizi consentiti** (IDS e opzioni avanzate) e non possono essere disattivate direttamente. È invece possibile utilizzare le specifiche caselle di controllo per eseguire tale operazione.

Diversamente dalla versione precedente di ESET Endpoint Security, le regole vengono valutate dall'alto in basso. L'azione della regola della prima corrispondenza viene utilizzata per la connessione di ciascuna rete valutata. Si tratta di un'importante modifica comportamentale rispetto alla versione precedente, in cui la priorità delle regole era automatica e le regole più specifiche registravano una priorità superiore rispetto a quelle più generali.

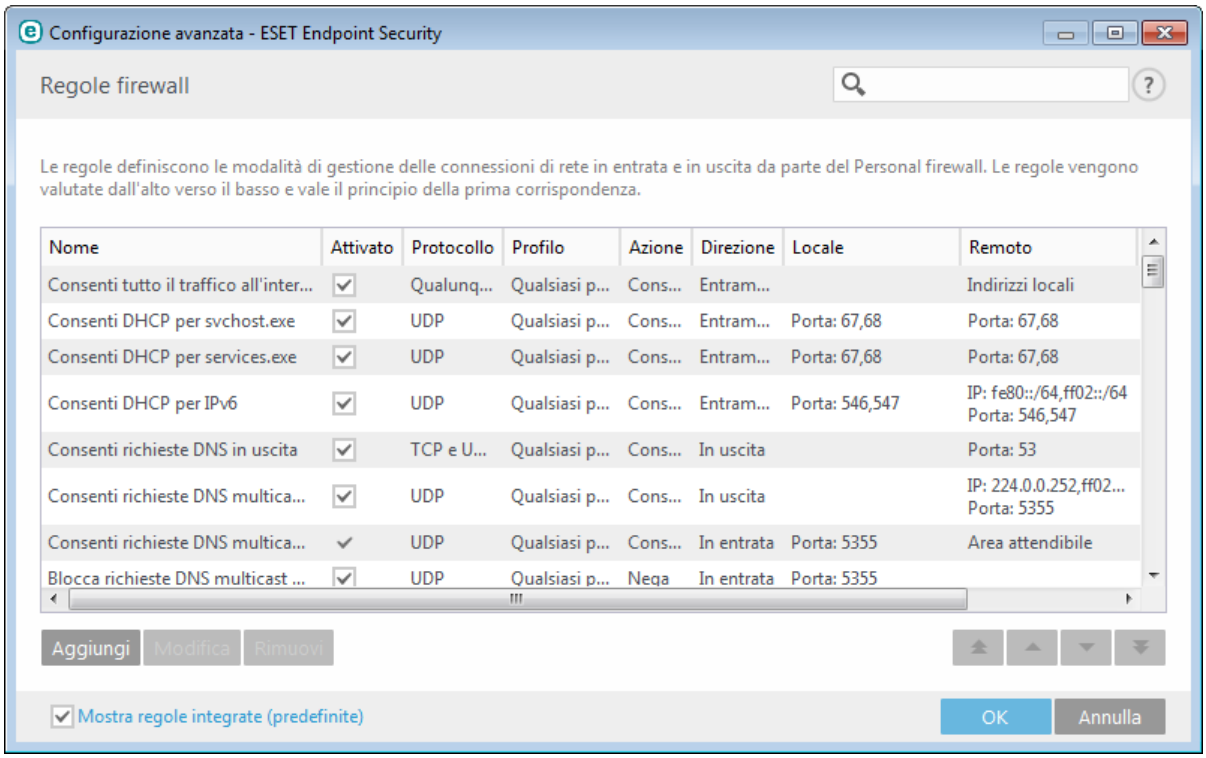
Le connessioni possono essere suddivise in connessioni in entrata e in uscita. Le connessioni in entrata vengono avviate da un computer remoto che tenta di stabilire una connessione con il sistema locale. Le connessioni in uscita funzionano in senso opposto: il sistema locale contatta un computer remoto.

Quando viene rilevata una nuova comunicazione sconosciuta, è necessario considerare con attenzione se consentirla o negarla. Le connessioni non desiderate, non sicure o sconosciute costituiscono un rischio per la protezione del sistema. Se si stabilisce una connessione di questo tipo, è opportuno prestare particolare attenzione al computer remoto e all'applicazione che tenta di connettersi al computer. Molte infiltrazioni cercano di ottenere e inviare dati privati o scaricare altre applicazioni dannose sulle workstation host. Il rapporto del Personal firewall consente di rilevare e interrompere queste connessioni.

3.8.2.3.1 Regole firewall

Fare clic su **Modifica** accanto a **Regole** nella sezione della scheda **Di base** per visualizzare la finestra **Regole firewall**, dove è presente l'elenco di tutte le regole. **Aggiungi**, **Modifica** e **Rimuovi** consentono all'utente di aggiungere, configurare o eliminare le regole. È possibile regolare il livello di priorità di una regola selezionando una o più regole e facendo clic su **In alto/Su/Giù/In basso**.

SUGGERIMENTO: è possibile utilizzare il campo **Cerca** per ricercare una o più regole in base al nome, al protocollo o alla porta.



Colonne

Nome - Nome della regola.

Attivata - Mostra lo stato di attivazione/disattivazione delle regole; per attivare una regola, è necessario selezionare la casella di controllo corrispondente.

Protocollo - Protocollo per il quale la regola è valida.

Profilo - Mostra il profilo del firewall per il quale la regola è valida.

Azione - Mostra lo stato della comunicazioni (blocca/consenti/chiedi).

Direzione - Direzione della comunicazione (in entrata/in uscita/entrambe).

Locale - Indirizzo IP e porta del computer locale.

Remoto - Indirizzo IP e porta del computer remoto.

Applicazioni - Applicazione alla quale viene applicata la regola.

Elementi di controllo

Aggiungi - Crea una nuova regola.

Modifica - Consente all'utente dimodificare le regole esistenti.

Rimuovi - Rimuove le regole esistenti.

Mostra regole integrate (predefinite) - Regole predefinite da ESET Endpoint Security per consentire o negare comunicazioni specifiche. È possibile disattivare queste regole, ma non è possibile eliminare una regola predefinita.

In alto/Su/Giù/In basso: consente all'utente di regolare il livello di priorità delle regole (le regole vengono eseguite dall'alto in basso).

3.8.2.3.2 Utilizzo delle regole

La modifica è necessaria ogni volta che i parametri monitorati vengono cambiati. In caso di applicazione di modifiche che impediscono a una regola di soddisfare le condizioni e di applicare l'azione specificata, la connessione specifica potrebbe essere rifiutata. Ciò potrebbe comportare problemi di funzionamento dell'applicazione sulla quale è stata applicata una regola. Un esempio è la modifica di un indirizzo di rete o di un numero di porta per il lato remoto.

La parte superiore della finestra contiene tre schede:

- **Generale** - Specificare il nome della regola, la direzione della connessione, l'azione (**Consenti**, **Nega**, **Chiedi**), il protocollo e il profilo al quale verrà applicata la regola.
- **Locale** - In questa scheda sono visualizzate informazioni sul lato locale della connessione, compreso il numero della porta locale o l'intervallo di porte e il nome dell'applicazione coinvolta nella comunicazione. Consente inoltre di aggiungere un'area predefinita o creata con un intervallo di indirizzi IP qui facendo clic su **Aggiungi**.
- **Remoto** - Questa scheda contiene informazioni sulla porta remota (intervallo porte). Consente di definire un elenco di indirizzi IP remoti o aree per una specifica regola. È possibile inoltre aggiungere un'area predefinita o creata con un intervallo di indirizzi IP qui facendo clic su **Aggiungi**.

Quando si crea una nuova regola, è necessario immettere il relativo nome nel campo **Nome**. Selezionare la direzione di applicazione della regola dal menu a discesa **Direzione** e l'azione da eseguire nel momento in cui una comunicazione è conforme alla regola dal menu a discesa **Azione**.

Protocollo indica il protocollo di trasferimento utilizzato per la regola. Selezionare il protocollo da utilizzare per una data regola dal menu a discesa.

Codice/tipo di ICMP rappresenta un messaggio ICMP identificato da un numero (ad esempio, 0 rappresenta "risposta Echo").

Per impostazione predefinita, tutte le regole vengono attivate per **Qualsiasi profilo**. In alternativa, selezionare un profilo firewall personalizzato utilizzando il menu a discesa **Profili**.

Se si attiva **Rapporto**, l'attività correlata alla regola verrà memorizzata in un registro. **Notifica utente** consente di visualizzare una notifica quando la regola viene applicata.

Segue un esempio nel quale viene creata una nuova regola per consentire all'applicazione del browser Web di accedere alla rete. In questo esempio, è necessario adottare la seguente configurazione:

- Nella scheda **Generale**, attivare le comunicazioni in uscita mediante il protocollo TCP e UDP.
- Aggiungere l'applicazione del browser in uso (iexplore.exe per Internet Explorer) nella scheda **Locale**.
- Nella scheda **Remota**, attivare il numero di porta 80 se si desidera consentire una navigazione Internet standard.

NOTA: tenere presente che la modifica delle regole predefinite è soggetta ad alcune limitazioni.

3.8.2.4 Area attendibile

L'area attendibile rappresenta un gruppo di indirizzi di rete dai quali il rapporto del Personal firewall consente parte del traffico in entrata mediante l'utilizzo di impostazioni predefinite. Le impostazioni per le funzioni quali la condivisione dei file e il desktop remoto all'interno dell'area attendibile vengono stabilite in IDS e opzioni avanzate.

L'area attendibile effettiva viene calcolata in modo dinamico e separato per ciascuna scheda di rete in base alla rete a cui il computer è connesso. Gli indirizzi definiti come interni all'area attendibile nell'Editor aree sono sempre attendibili. Se una scheda di rete è connessa a una rete nota, gli **Indirizzi attendibili aggiuntivi** configurati per quella rete vengono aggiunti all'area attendibile della scheda. Se una rete utilizza il tipo di protezione domestica/aziendale, tutte le subnet di rete direttamente connesse vengono incluse nell'area attendibile. L'area attendibile effettiva per ciascuna scheda di rete può essere visualizzata dalla finestra **Configurazione** sotto a **Rete** > **Schede di rete**.

NOTA: l'area attendibile dell'interfaccia Per non è supportata sui sistemi operativi Windows XP. Per questi sistemi operativi, tutte le schede di rete possiedono la stessa area attendibile e ciò è visibile anche nella pagina Schede di rete.

3.8.2.5 Configurazione aree

Le aree sono gruppi di indirizzi IP utili nel caso in cui fosse necessario riutilizzare lo stesso set di indirizzi in regole multiple. Le aree possono essere configurate in **Configurazione avanzata** > **Personal firewall** > **Di base**, facendo clic sul pulsante **Modifica** accanto ad **Aree**. Per aggiungere una nuova area, fare clic su **Aggiungi**, inserire un **Nome** dell'area, una **Descrizione** e un indirizzo IP remoto nel campo **Indirizzo computer remoto (IPv4, IPv6, intervallo, maschera)**.

Nella finestra di configurazione delle **Aree firewall** , è possibile specificare il nome, la descrizione e l'elenco di indirizzi di rete (consultare anche il paragrafo Editor delle reti note).

3.8.2.6 Reti note

Quando si utilizza un computer che effettua connessioni frequenti a reti pubbliche o a reti esterne alla normale rete di lavoro, si consiglia di verificarne la credibilità. Una volta definite le reti, ESET Endpoint Security riconosce quelle attendibili (domestiche/aziendali) che utilizzando vari parametri di rete configurati in **Identificazione di rete**. Spesso i computer accedono alle reti con indirizzi IP simili alla rete attendibile. In tali casi, ESET Endpoint Security potrebbe considerare una rete sconosciuta come attendibile (domestica/aziendale). Si consiglia di utilizzare **Autenticazione di rete** per evitare questo tipo di situazione.

Se una scheda di rete è connessa a una rete o le relative impostazioni vengono riconfigurate, ESET Endpoint Security ricercherà nell'elenco di reti note un record che corrisponde alla nuova rete. In caso di corrispondenza tra **Identificazione di rete** e **Autenticazione di rete** (facoltativo), la rete verrà contrassegnata come connessa in questa interfaccia. Se non vengono trovate reti note, ne viene creata una nuova contenente la configurazione dell'identificazione di rete che consente di identificarla alla successiva connessione. Per impostazione predefinita, la nuova connessione di rete utilizza il tipo di protezione **Pubblica**. La finestra di dialogo **Rilevata nuova connessione di rete** richiederà all'utente di scegliere tra il tipo di protezione **Pubblica** e **Domestica/aziendale**. In caso di connessione di una scheda di rete a una rete nota e qualora la rete sia contrassegnata come **Domestica/aziendale**, le subnet locali della scheda vengono aggiunte all'area attendibile.

NOTA: attivando **Contrassegna automaticamente le nuove reti come pubbliche**, la finestra di dialogo **Rilevata nuova connessione di rete** non comparirà e la rete a cui è stata effettuata la connessione verrà contrassegnata automaticamente come pubblica. Ciò impedirà ad alcune funzionalità (ad esempio, la condivisione di file e il desktop remoto) di diventare inaccessibili dalle nuove reti.

Le reti note possono essere configurate manualmente nella finestra Editor reti note.

3.8.2.6.1 Editor reti note

È possibile configurare manualmente le reti note in **Configurazione avanzata** > **Personal firewall** > **Reti note** facendo clic su **Modifica**.

Colonne

Nome - Nome della rete nota.

Tipo d protezione - Consente di visualizzare se la rete è impostata su **Domestica/aziendale** o **Pubblica**.

Profilo firewall - Selezionare un profilo dal menu a discesa **Visualizza regole utilizzate nel profilo** per visualizzare il filtro delle regole del profilo.

Elementi di controllo

Aggiungi - Crea una nuova rete nota.

Modifica - Fare clic per modificare una rete nota esistente.

Rimuovi - Selezionare una rete e fare clic su **Rimuovi** per rimuoverla dall'elenco di reti note.

In alto/Su/Giù/In basso - Consente all'utente di regolare il livello di priorità delle reti note (le reti vengono valutate dall'alto in basso).

Le impostazioni relative alla configurazione di rete sono suddivise nelle seguenti schede:

Rete

Qui è possibile definire il nome della rete e selezionare il tipo di protezione (**Pubblica** o **Domestica/aziendale**) per la rete. Utilizzare il menu a discesa **Profilo firewall** per selezionare il profilo per questa rete. Se la rete utilizza il tipo di protezione **Domestica/aziendale**, tutte le subnet di rete direttamente connesse vengono considerate attendibili. Ad esempio, se una scheda di rete è connessa a questa rete con l'indirizzo IP 192.168.1.5 e la maschera subnet 255.255.255.0, la subnet 192.168.1.0/24 viene aggiunta all'area attendibile della scheda. Se la scheda presenta più indirizzi/subnet, questi verranno considerati tutti attendibili, indipendentemente dalla configurazione dell'**Identificazione di rete** della rete nota.

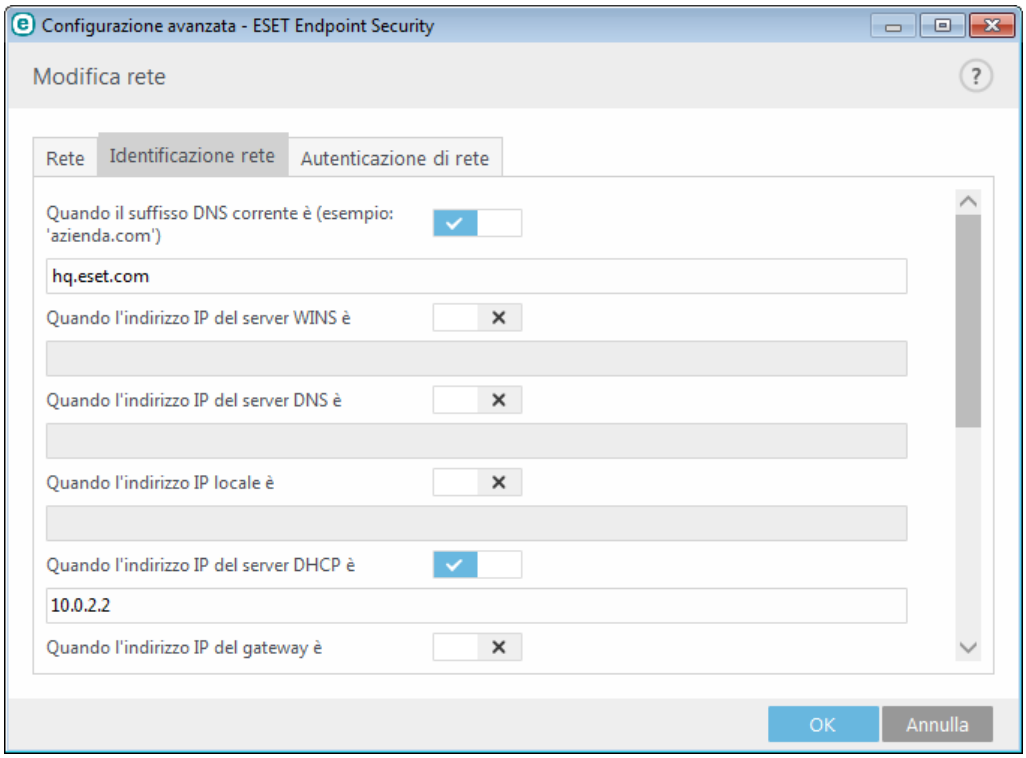
Inoltre, gli indirizzi aggiunti sotto a **Indirizzi attendibili aggiuntivi** vengono sempre aggiunti all'area attendibile delle schede connesse a questa rete (indipendentemente dal tipo di protezione della rete).

Per contrassegnare una rete come connessa nell'elenco di reti connesse, è necessario che vengano soddisfatte le seguenti condizioni:

- Identificazione di rete - Tutti i parametri compilati devono corrispondere ai parametri della connessione attiva.
- Autenticazione di rete - in caso di selezione del server di autenticazione, è necessario che avvenga l'autenticazione con il server di autenticazione ESET.
- Restrizioni di rete (solo per Windows XP) - è necessario che vengano rispettate tutte le restrizioni globali selezionate.

Identificazione di rete

L'identificazione di rete viene eseguita in base ai parametri della scheda di rete locale. Tutti i parametri selezionati vengono confrontati con i parametri effettivi delle connessioni di rete attive. Sono consentiti gli indirizzi IPv4 e IPv6.



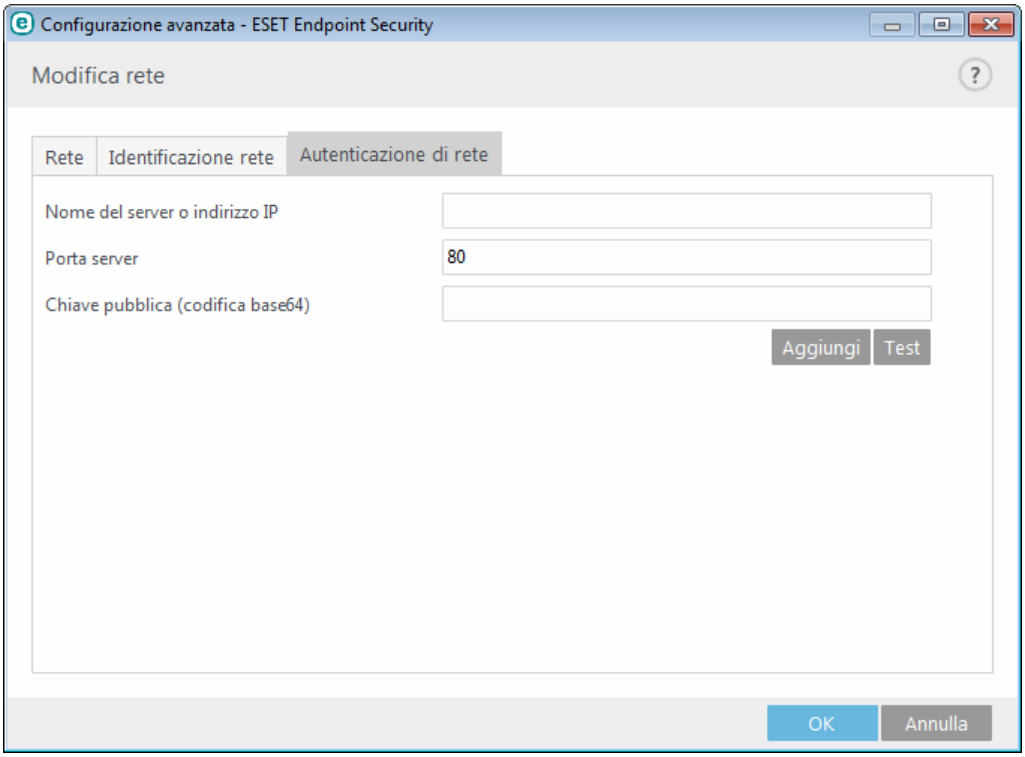
Autenticazione di rete

L'autenticazione di rete ricerca un server specifico nella rete e utilizza la crittografia asimmetrica (RSA) per autenticare il server. Il nome della rete autenticata deve corrispondere al nome dell'area definito nelle impostazioni del server di autenticazione. Il nome fa distinzione tra lettere maiuscole e minuscole. Specificare il nome del server, una porta di ascolto del server e una chiave pubblica che corrisponde alla chiave privata del server (consultare Autenticazione di rete - Configurazione del server). Il nome del server può essere specificato sotto

forma di indirizzo IP, DNS o nome NetBios e seguito da un percorso che indica la posizione della chiave sul server (ad esempio, nome_server_/directory1/directory2/autenticazione). È possibile specificare server alternativi da utilizzare aggiungendoli al percorso e utilizzando punti e virgola come separatori.

La chiave pubblica può essere importata utilizzando uno qualsiasi dei seguenti tipi di file:

- Chiave pubblica crittografata PEM (.pem), che può essere generata utilizzando ESET Authentication Server (consultare Autenticazione di rete - Configurazione del server).
- Chiave pubblica crittografata
- Certificato di chiave pubblica (.crt)



Fare clic su **Test** per testare le impostazioni. Se l'autenticazione viene eseguita correttamente, verrà visualizzato *Autenticazione server riuscita*. Se l'autenticazione non è configurata correttamente, verrà visualizzato uno dei seguenti messaggi di errore:

Autenticazione server non riuscita. Firma non valida o senza corrispondenza.
La firma del server non corrisponde alla chiave pubblica inserita.

Autenticazione server non riuscita. Il nome della rete non corrisponde.
Il nome della rete configurata non corrisponde al nome dell'area del server di autenticazione. Ricontrollare entrambi i nomi e assicurarsi che siano identici.

Autenticazione server non riuscita. Risposta non valida o nessuna risposta dal server.
Se il server non è in esecuzione o è inaccessibile, non verrà ricevuta alcuna risposta. È possibile ricevere una risposta non valida se un altro server HTTP viene eseguito sull'indirizzo specificato.

È stata inserita una chiave pubblica non valida.
Verificare che il file della chiave pubblica inserito non sia danneggiato.

Restrizioni di rete (solo per Windows XP)

Sui sistemi operativi moderni (Windows Vista e versioni più recenti), ciascuna scheda di rete presenta la propria area attendibile e il proprio profilo firewall attivo. Purtroppo, su Windows XP questo layout non è supportato e, di conseguenza, tutte le schede di rete condividono sempre la stessa area attendibile e lo stesso profilo firewall attivo. Ciò causa un rischio di protezione potenziale se la macchina è connessa contemporaneamente a più di una rete. In questi casi, il traffico proveniente da una rete inattendibile può essere valutato mediante l'utilizzo dell'area attendibile e del profilo firewall configurato per l'altra rete connessa. Per attenuare eventuali rischi di protezione, è possibile utilizzare le seguenti restrizioni che consentono di evitare l'applicazione globale di una configurazione di rete durante la connessione di un'altra rete (potenzialmente inattendibile).

Su Windows XP, le impostazioni delle reti connesse (area attendibile e profilo firewall) vengono applicate globalmente a meno che non venga soddisfatta almeno una delle seguenti restrizioni attivate:

a. Solo una connessione attiva
b. Non sono state stabilite connessioni wireless
c. Non sono state stabilite connessioni wireless non sicure

3.8.2.6.2 Autenticazione di rete: configurazione del server

Il processo di autenticazione può essere eseguito da qualsiasi computer/server collegato alla rete da autenticare. L'applicazione Server di autenticazione ESET deve essere installata su un computer/server sempre accessibile per l'autenticazione ogniqualvolta un client tenti di collegarsi alla rete. Il file d'installazione per l'applicazione Server di autenticazione ESET è disponibile per il download sul sito Web ESET.

Dopo aver installato l'applicazione ESET Authentication Server, verrà visualizzata una finestra di dialogo (è possibile accedere all'applicazione facendo clic su **Start** > **Programmi** > **ESET** > **ESET Authentication Server**).

Per configurare il server di autenticazione, immettere il nome della rete di autenticazione, la porta di ascolto del server (l'impostazione predefinita è 80) e il percorso di archiviazione della coppia di chiavi pubblica e privata. Generare quindi le chiavi pubblica e privata che saranno utilizzate nel processo di autenticazione. La chiave privata rimarrà sul server, mentre quella pubblica dovrà essere importata sul lato client nella sezione Autenticazione di rete durante la configurazione di una rete nella configurazione del firewall.

3.8.2.7 Registrazione

Il Firewall ESET Endpoint Security salva tutti gli eventi importanti in un file di rapporto, che può essere visualizzato direttamente dal menu principale. Fare clic su **Strumenti** > **File di rapporto**, quindi selezionare **Personal firewall** dal menu a discesa **Rapporto**. Per attivare la registrazione del rapporto del Personal firewall, accedere a **Configurazione avanzata** > **Strumenti** > **File di rapporto** e impostare il livello minimo di dettaglio del rapporto su **Diagnostica.** Tutte le connessioni rifiutate verranno registrate.

I file di rapporto possono essere utilizzati per il rilevamento di errori e di intrusioni nel sistema. I rapporti di ESET Personal firewall contengono le informazioni seguenti:

- **Tempo**: data e ora dell'evento.
- **Evento**: nome dell'evento.
- **Origine**: indirizzo di rete di origine.
- **Destinazione**: indirizzo di rete della destinazione.
- **Protocollo**: protocollo della comunicazione di rete.
- **Nome regola/worm**: nome della regola applicata o del worm, qualora identificato.
- **Applicazione**: specifica applicazione interessata.
- **Utente**: nome dell'utente che ha eseguito l'accesso al momento del rilevamento dell'infiltrazione.

Un'analisi approfondita di questi dati consente di rilevare i tentativi di compromissione della sicurezza del sistema. Molti altri fattori indicano potenziali rischi per la protezione e consentono all'utente di ridurne al minimo l'impatto. Alcuni esempi di indicatori di minacce potenziali includono: connessioni frequenti da posizioni sconosciute, tentativi ripetuti di stabilire connessioni, comunicazione da parte di applicazioni sconosciute o utilizzo di numeri di porte insoliti.

3.8.2.8 Stabilire la connessione - rilevamento

Il Firewall personale rileva tutte le connessioni di rete non appena vengono create. La modalità firewall attivo determina le azioni eseguite per la nuova connessione. Se è attivata la **Modalità automatica** o la **Modalità basata su policy**, il Firewall personale eseguirà azioni predefinite senza alcun intervento da parte dell'utente.

In Modalità interattiva viene visualizzata una finestra informativa che segnala il rilevamento di una nuova connessione di rete, con informazioni dettagliate sulla connessione. È possibile scegliere se consentire o rifiutare la connessione (bloccarla). Se si consente ripetutamente la stessa connessione nella finestra di dialogo, è consigliabile creare una nuova regola per tale connessione. Per eseguire questa operazione, selezionare **Ricorda azione (crea regola)** e salvare l'azione come nuova regola per il rapporto del Personal firewall. Se il firewall riconosce la stessa connessione in futuro, applicherà la regola esistente senza richiedere l'intervento da parte dell'utente.

Ricorda temporaneamente azione per il processo causa un'azione (**Consenti**/**Nega**) da utilizzare finché non verrà riavviata l'applicazione, non verrà apportata una modifica alle regole o alle modalità di filtraggio oppure non verrà eseguito un aggiornamento del modulo Firewall o un riavvio del sistema. In seguito a una di queste azioni, le regole temporanee verranno eliminate.

Prestare attenzione durante la creazione di nuove regole e consentire solo le connessioni sicure. Se si consentono tutte le connessioni, il Firewall personale non potrà svolgere la funzione per la quale è stato installato. Sono riportati di seguito importanti parametri per le connessioni:

- **Lato remoto** - Consentire la connessione solo a indirizzi affidabili e noti.
- **Applicazione locale** - Non è consigliabile consentire la connessione di applicazioni e processi sconosciuti.
- **Numero porta** - Consentire la comunicazione sulle porte comuni (ad esempio, il traffico Web sulla porta 80) in circostanze normali.

Per poter proliferare, le infiltrazioni utilizzano spesso la connessione a Internet e connessioni nascoste per infettare sistemi remoti. Se le regole sono configurate correttamente, un Personal firewall diventa uno strumento utile per la protezione contro numerosi attacchi di codice dannoso.

3.8.2.9 Risoluzione dei problemi con ESET Personal firewall

In caso di problemi di connettività dopo aver installato ESET Endpoint Security, esistono vari modi per stabilire se ESET Personal Firewall ne è la causa. Inoltre, ESET Personal firewall aiuta l'utente a creare nuove regole o eccezioni per la risoluzione di problemi di connettività.

Consultare i seguenti argomenti per provare a risolvere i problemi con ESET Personal Firewall:

- Procedura guidata per la risoluzione dei problemi
- Registrazione e creazione di regole o eccezioni a partire dal rapporto
- Creazione di eccezioni a partire dalle notifiche del firewall
- Registrazione PCAP avanzata
- Risoluzione dei problemi con il filtraggio protocolli

3.8.2.9.1 Procedura guidata per la risoluzione dei problemi

La procedura guidata per la risoluzione dei problemi monitora in modo silenzioso tutte le connessioni bloccate guidando l'utente nel processo di risoluzione dei problemi allo scopo di correggere problemi relativi al firewall con applicazioni o dispositivi specifici. Successivamente, la procedura guidata suggerirà un nuovo set di regole da applicare in caso di approvazione da parte dell'utente. La **Procedura guidata per la risoluzione dei problemi** è disponibile nel menu principale sotto a **Configurazione** > **Rete**.

3.8.2.9.2 Registrazione e creazione di regole o eccezioni a partire dal rapporto

Per impostazione predefinita, ESET Personal firewall non registra tutte le connessioni bloccate. Se si desidera visualizzare gli elementi bloccati dal rapporto del Personal firewall, è necessario attivare la registrazione nella sezione **Risoluzione dei problemi** di **Configurazione avanzata** sotto a **Personal firewall** > **IDS e opzioni avanzate**. Se il rapporto contiene elementi che non si desidera far bloccare dal rapporto del Personal firewall, è possibile creare una regola o eccezione IDS specifica facendo clic con il pulsante destro del mouse su quegli oggetti e selezionando **Non bloccare eventi simili in futuro**. Si tenga presente che il rapporto di tutte le connessioni bloccate contiene migliaia di oggetti e potrebbe essere difficile trovare una connessione specifica. È possibile disattivare la registrazione dopo aver risolto il problema.

Per ulteriori informazioni sul rapporto, visualizzare File di rapporto.

Nota: utilizzare la registrazione per visualizzare l'ordine in cui rapporto del Personal firewall blocca connessioni specifiche. Inoltre, la creazione di regole dal rapporto consente all'utente di creare regole che seguono esattamente ciò di cui ha bisogno.

3.8.2.9.2.1 Crea regola da rapporto

La nuova versione di ESET Endpoint Security consente all'utente di creare una regola dal rapporto. Dal menu principale, fare clic su **Strumenti** > **File di rapporto**. Scegliere **Personal firewall** dal menu a discesa, fare clic con il pulsante destro del mouse sulla voce del rapporto desiderata e selezionare **Non bloccare eventi simili in futuro** dal menu contestuale. La nuova regola verrà visualizzata in una finestra di notifiche.

Per consentire la creazione di nuove regole dal rapporto, ESET Endpoint Securitydeve essere configurato utilizzando le seguenti impostazioni:

- impostare il livello minimo di dettaglio del rapporto su **Diagnostica** in **Configurazione avanzata** (F5) > **Strumenti** > **File di rapporto**,
- attivare **Visualizza notifiche anche per gli attacchi in ingresso contro problemi di sicurezza** in **Configurazione avanzata** (F5) > **Rapporto del Personal firewall** > **IDS e opzioni avanzate** > **Rilevamento intrusioni**.

3.8.2.9.3 Creazione di eccezioni a partire dalle notifiche del rapporto del Personal firewall

Quando ESET Personal firewall rileva un'attività di rete dannosa, verrà visualizzata una finestra di notifica contenente una descrizione dell'evento. Questa notifica contiene un collegamento che consente all'utente di avere maggiori informazioni sull'evento e, se lo desidera, configurare un'eccezione.

NOTA: se un'applicazione di rete o un dispositivo non implementa correttamente gli standard di rete, potrebbero essere attivate notifiche IDS firewall ripetitive. È possibile creare un'eccezione direttamente dalla notifica per impedire a ESET Personal firewall di rilevare l'applicazione o il dispositivo in questione.

3.8.2.9.4 Registrazione PCAP avanzata

Questa funzione è stata pensata allo scopo di fornire file di rapporto più complessi per il Supporto tecnico ESET. Utilizzare questa funzione solo se richiesto dal Supporto tecnico ESET, in quanto potrebbe generare un file di rapporto enorme e rallentare le prestazioni del computer in uso.

1. Accedere a **Configurazione avanzata** > **Rapporto del Personal firewall** > **IDS e opzioni avanzate** > **Risoluzione dei problemi** e abilitare **Attiva registrazione PCAP avanzata**.
2. Tentativo di riproduzione del problema verificatosi.
3. Disattiva registrazione PCAP avanzata.
4. Il file di rapporto PCAP è disponibile nella stessa directory in cui vengono generati i dump di memoria diagnostici:

- Microsoft Windows Vista o versioni successive

  C:\Programmi\ESET\ESET Endpoint Sicurezza\Diagnostica

- Microsoft Windows XP

  C:\Documents and Settings\All Users\...

3.8.2.9.5 Risoluzione dei problemi con il filtraggio protocolli

In caso di problemi con il browser o il client di posta, il primo passo consiste nel capire se una possibile causa possa essere il filtraggio protocolli. A tal fine, tentare di disattivare temporaneamente il filtraggio protocolli dell'applicazione in Configurazione avanzata (ricordarsi di riattivarlo una volta terminata l'operazione, per impedire al browser e al client di posta di rimanere senza protezione). Se il problema scompare in seguito alla disattivazione, è possibile consultare un elenco di problemi comuni e dei rispettivi metodi di risoluzione:

Problemi relativi all'aggiornamento o alla sicurezza delle comunicazioni

Se l'applicazione non riesce ad aggiornarsi o un canale di comunicazione non è sicuro:

- Se il filtraggio del protocollo SSL è attivato, tentare di disattivarlo temporaneamente. In caso di esito positivo, è possibile continuare a utilizzare il filtraggio del protocollo SSL e garantire il funzionamento degli aggiornamenti escludendo la comunicazione problematica:
  Impostare la modalità di filtraggio del protocollo SSL su interattiva. Eseguire nuovamente l'aggiornamento. Dovrebbe comparire una finestra di dialogo che informa l'utente sul traffico di rete crittografato. Assicurarsi che l'applicazione corrisponda a quella problematica analizzata e che il certificato provenga dal server dal quale sono stati scaricati gli aggiornamenti. Scegliere quindi di ricordare l'azione per questo certificato e fare clic su Ignora. Se non compaiono altre finestre di dialogo, è possibile reimpostare la modalità di filtraggio su Automatica. A questo punto, il problema dovrebbe essere risolto.
- Se l'applicazione in questione non è un browser o un client di posta, è possibile escluderlo completamente dal filtraggio protocolli (eseguendo questa operazione sul browser o il client di posta si potrebbe esporre il sistema a rischi). Le applicazioni le cui comunicazioni sono state filtrate in passato dovrebbero già essere presenti nell'elenco fornito all'utente nel momento in cui è stata aggiunta l'eccezione. Di conseguenza, non è necessario aggiungerle manualmente.

Problema relativo all'accesso a un dispositivo sulla rete

Se non si è in grado di utilizzare una funzionalità di un dispositivo presente nella rete (ovvero aprire una pagina Web della webcam o riprodurre un video su un lettore multimediale personale), provare ad aggiungere i relativi indirizzi IPv4 e IPv6 all'elenco di indirizzi esclusi.

Problemi con un sito Web specifico

È possibile escludere siti Web specifici dal filtraggio protocolli utilizzando la funzione Gestione indirizzo URL. Ad esempio, se non è possibile accedere a https://www.gmail.com/intl/en/mail/help/about.html, provare ad aggiungere *gmail.com* all'elenco di indirizzi esclusi.

Errore "Alcune delle applicazioni in grado di importare il certificato radice sono ancora in funzione."

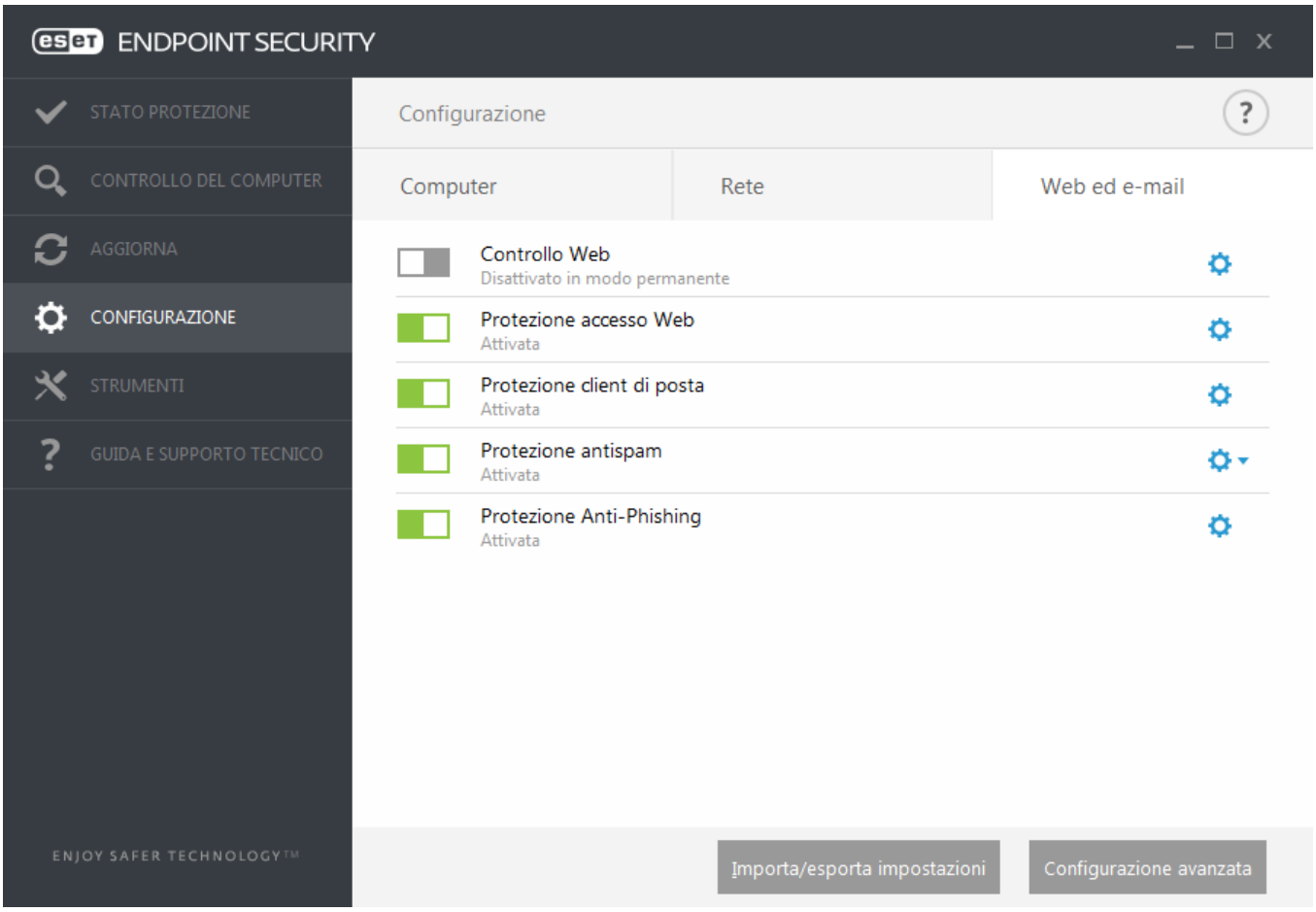
Quando si attiva il filtraggio del protocollo SSL, ESET Endpoint Security si assicura che le applicazioni installate considerino le modalità di filtraggio attendibili importando un certificato nel relativo archivio. Per alcune applicazioni, questa operazione non è possibile durante l'esecuzione. L'elenco comprende Firefox e Opera. Assicurarsi che nessuna di esse sia in esecuzione (il modo migliore per farlo è aprire Task Manager e assicurarsi che nella scheda Processi non siano presenti firefox.exe o opera.exe), quindi premere su Riprova.

Errore relativo a un'autorità emittente inattendibile o una firma non valida

Gli errori più comuni si verificano quando l'importazione descritta in precedenza non viene eseguita correttamente. Assicurarsi dapprima che nessuna delle applicazioni menzionate sia in esecuzione. Disattivare e riattivare quindi il filtraggio del protocollo SSL. Questa operazione consentirà di eseguire nuovamente l'importazione.

3.8.3 Web e e-mail

La configurazione Web e e-mail è disponibile sotto a **Configurazione** > **Web e e-mail**. Da qui è possibile accedere a impostazioni del programma più dettagliate.



Il modulo **Controllo Web** consente all'utente di configurare le impostazioni che forniscono agli amministratori strumenti automatici per garantire la protezione delle workstation e impostare restrizioni sulla navigazione

Internet. L'obiettivo della funzionalità del controllo Web consiste nel prevenire l'accesso alle pagine con contenuti inappropriati o dannosi. Per ulteriori informazioni, consultare il paragrafo Controllo Web.

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

La **Protezione client di posta** garantisce il controllo delle comunicazioni via e-mail ricevute mediante i protocolli POP3 e IMAP. Mediante l'utilizzo del programma plug-in per il client di posta in uso, ESET Endpoint Security controlla tutte le comunicazioni provenienti dal client di posta (POP3, IMAP, HTTP, MAPI).

La **Protezione antispam** consente di filtrare i messaggi e-mail indesiderati.

Facendo clic sulla rotella a forma di ingranaggio accanto a **Protezione antispam**, sono disponibili le seguenti opzioni:

Configura... - Apre le impostazioni avanzate per la protezione antispam del client di posta.

Whitelist/Blacklist/Elenco di eccezioni utente - Apre una finestra di dialogo che consente di aggiungere, modificare o eliminare indirizzi e-mail considerati sicuri o non sicuri. In base alle regole definite qui, le e-mail provenienti da questi indirizzi non verranno controllate o verranno considerate come spam. Fare clic su **Elenco eccezioni utente** per aprire una finestra di dialogo che consente di aggiungere, modificare o eliminare indirizzi e-mail che potrebbero essere contraffatti e utilizzati per inviare messaggi di spam. I messaggi e-mail ricevuti da indirizzi presenti nell'elenco Eccezione verranno sempre sottoposti al controllo alla ricerca di spamming.

La **Protezione Anti-Phishing** è un altro livello di protezione che garantisce una difesa potenziata da siti Web illegittimi che tentano di acquisire password e altre informazioni sensibili. La protezione Anti-Phishing è disponibile nel riquadro **Configurazione** sotto a **Web e e-mail**. Per ulteriori informazioni, consultare il paragrafo Protezione Anti-Phishing.

Disattiva - Fare clic sul pulsante per disattivare la protezione Web/e-mail/antispam per i browser Web e i client di posta .

3.8.3.1 Filtraggio protocolli

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

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

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

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

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

Registra le informazioni necessarie al supporto ESET per diagnosticare i problemi correlati al filtraggio dei protocolli - Attiva la registrazione avanzata dei dati diagnostici; utilizzare questa funzione solo se richiesto dal supporto ESET.

3.8.3.1.1 Web e client di posta

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

A causa dell'enorme quantità di codice dannoso che circola su Internet, una navigazione Internet sicura è essenziale per la protezione del computer. Le vulnerabilità dei browser Web e i collegamenti fraudolenti aiutano il codice dannoso a penetrare inosservato nel sistema. Per tale motivo, ESET Endpoint Security si focalizza sulla sicurezza dei browser Web. Ogni applicazione che accede alla rete può essere contrassegnata come un browser. Nell'elenco di client Web e di posta, è possibile inserire le applicazioni che utilizzavano già protocolli di comunicazione o l'applicazione proveniente dal percorso selezionato.

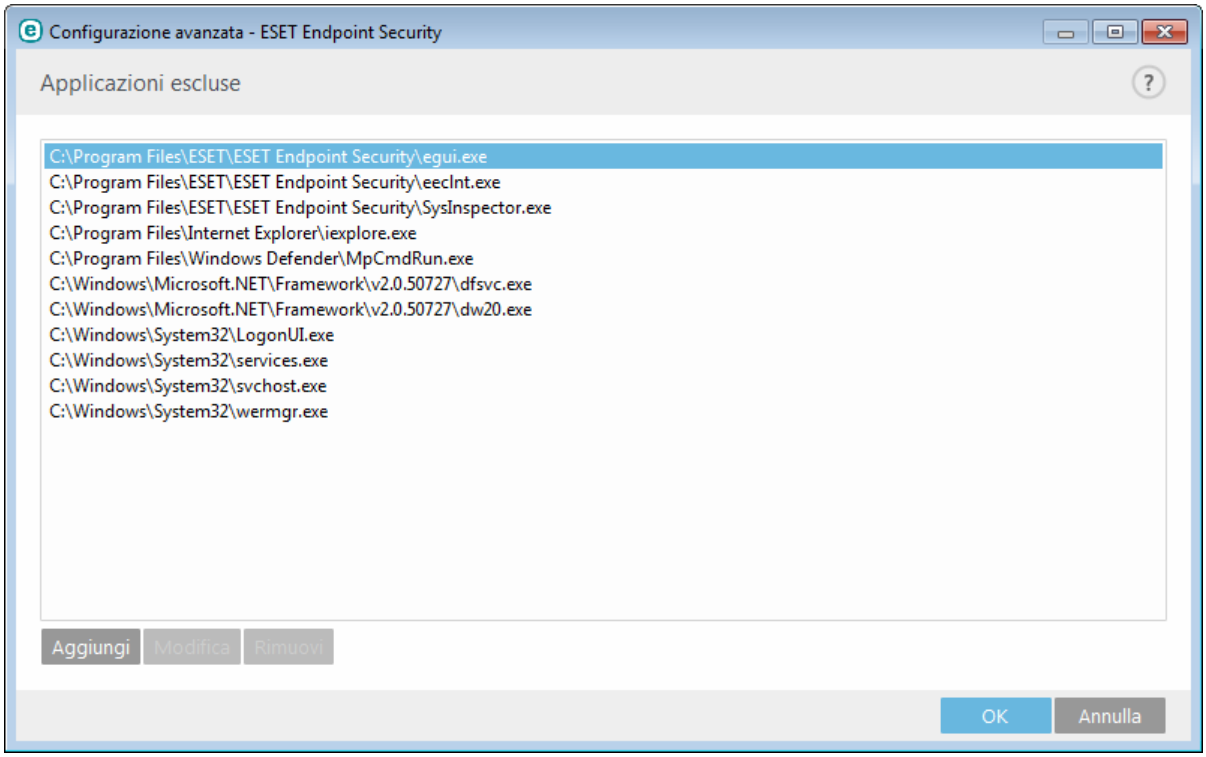
3.8.3.1.2 Applicazioni escluse

Per escludere le comunicazioni di specifiche applicazioni di rete dal filtraggio del protocollo, è necessario aggiungerle all'elenco. Sulla comunicazione HTTP/POP3/IMAP delle applicazioni selezionate non verrà eseguito un controllo finalizzato al rilevamento delle minacce. Si consiglia di utilizzare questa tecnica solo in caso di malfunzionamento delle applicazioni con il filtraggio protocolli attivato.

Le applicazioni e i servizi sui quali è già stato attivato il filtraggio protocolli verranno visualizzati automaticamente facendo clic su **Aggiungi**.

Modifica: modifica le voci selezionate dall'elenco.

Rimuovi: rimuove dall'elenco le voci selezionate.



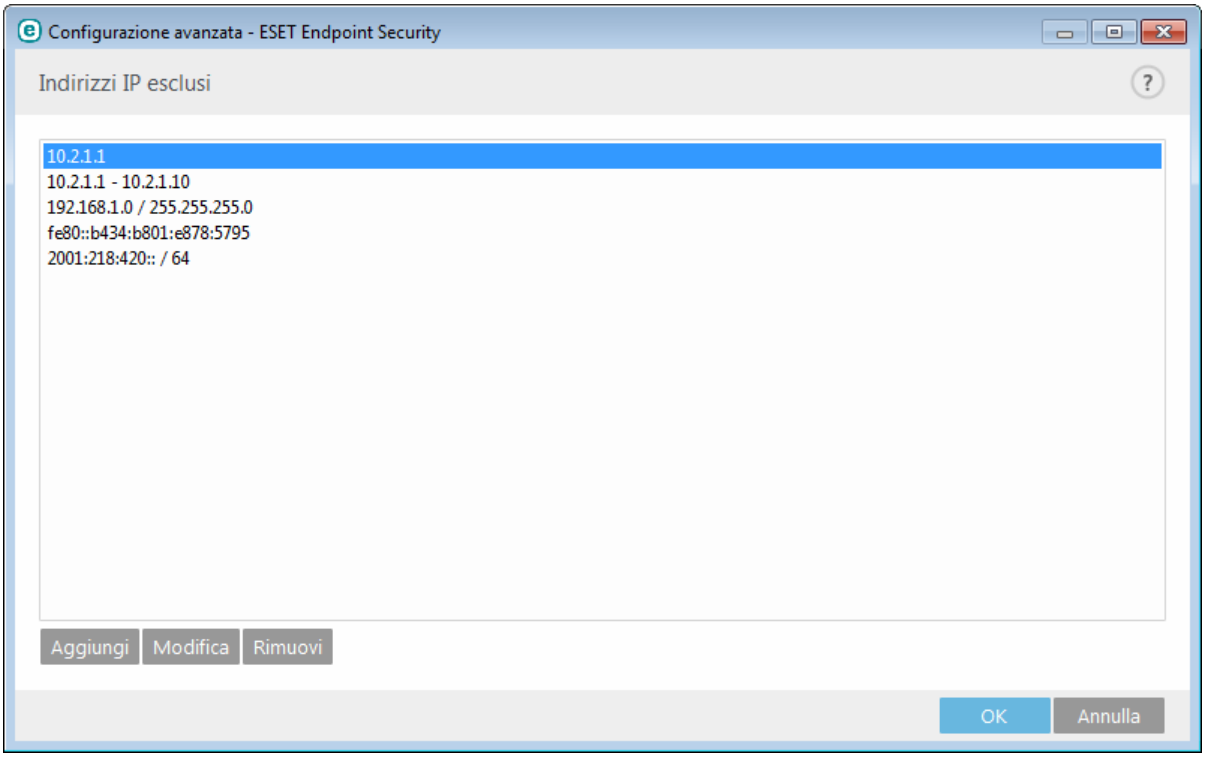
3.8.3.1.3 Indirizzi IP esclusi

Gli indirizzi IP presenti in questo elenco verranno esclusi dal filtraggio dei contenuti del protocollo. Sulla comunicazione HTTP/POP3/IMAP da/verso gli indirizzi selezionati non verrà eseguito il rilevamento delle minacce. È consigliabile utilizzare questa opzione solo per gli indirizzi di cui è nota l'affidabilità.

Aggiungi: fare clic per aggiungere un indirizzo IP/intervallo di indirizzi/subnet di un punto remoto a cui viene applicata una regola.

Modifica: modifica le voci selezionate dall'elenco.

Rimuovi: rimuove dall'elenco le voci selezionate.



3.8.3.1.4 SSL/TLS

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

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

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

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

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

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

Certificato radice

Certificato radice - Affinché la comunicazione SSL funzioni in modo adeguato nei browser/client di posta dell'utente, è fondamentale che il certificato radice di ESET venga aggiunto all'elenco dei certificati radice noti (autori). È necessario attivare **Aggiungi il certificato radice ai browser conosciuti**. Selezionare questa opzione per aggiungere automaticamente il certificato radice di ESET ai browser conosciuti (ad esempio, Opera e Firefox). Per i browser che utilizzano l'archivio di certificazioni di sistema, il certificato viene aggiunto automaticamente (ad esempio, Internet Explorer).

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

Validità del certificato

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

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

L'**Elenco di certificati noti** consente all'utente di personalizzare il comportamento di ESET Endpoint Security per specifici certificati SSL.

3.8.3.1.4.1 Comunicazioni SSL crittografate

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

Innanzitutto, se un sito Web utilizza un certificato non verificabile o non valido e ESET Endpoint Security è configurato in modo da chiedere la conferma dell'utente in tali casi (per impostazione predefinita, sì per i certificati non verificabili e no per quelli non validi), una finestra di dialogo chiederà all'utente di **Consentire** o **Bloccare** la connessione.

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

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

3.8.3.1.4.2 Elenco di certificati noti

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

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

Colonne

Nome : nome del certificato.

Autorità di certificazione emittente: nome del creatore del certificato.

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

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

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

Elementi di controllo

Aggiungi: è possibile caricare manualmente un certificato come file con estensione *.cer*, *.crt* o *.pem*. Fare clic su File per caricare un certificato locale o su **URL** per specificare il percorso di un certificato on-line.

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

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

OK/Annulla: fare clic su **OK** se si desidera salvare le modifiche oppure su **Annulla** per lasciare l'impostazione invariata.

3.8.3.2 Protezione client di posta

3.8.3.2.1 Client di posta

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

Integrazione client di posta

I client di posta attualmente supportati sono Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail. Per questi programmi, la protezione e-mail funziona come un plug-in. Il vantaggio principale offerto dal plug-in consiste nella sua indipendenza dal protocollo utilizzato. Quando il client di posta riceve un messaggio crittografato, questo viene decodificato e inviato allo scanner antivirus. Per un elenco completo dei client di posta supportati e delle relative versioni, consultare il seguente articolo della Knowledge Base ESET.

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

Attivare **Disattiva il controllo alla modifica del contenuto della posta in arrivo** se si riscontra un rallentamento del sistema durante l'utilizzo del client di posta (solo MS Outlook). Ciò può accadere durante il recupero di e-mail da Kerio Outlook Connector Store.

E-mail da controllare

E-mail ricevuta: attiva/disattiva il controllo dei messaggi ricevuti.
E-mail inviata: attiva/disattiva il controllo dei messaggi inviati.
E-mail letta: attiva/disattiva il controllo dei messaggi letti.

Azione da eseguire sull'e-mail infetta

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

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

Ripeti controllo dopo l'aggiornamento: attiva/disattiva un nuovo controllo dopo l'aggiornamento del database delle firme antivirali.

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

3.8.3.2.2 Protocolli e-mail

IMAP e POP3 sono i protocolli più comunemente utilizzati per ricevere comunicazioni e-mail in un'applicazione client di posta. ESET Endpoint Security offre protezione per questi protocolli indipendentemente dal client di posta utilizzato e senza richiederne la riconfigurazione.

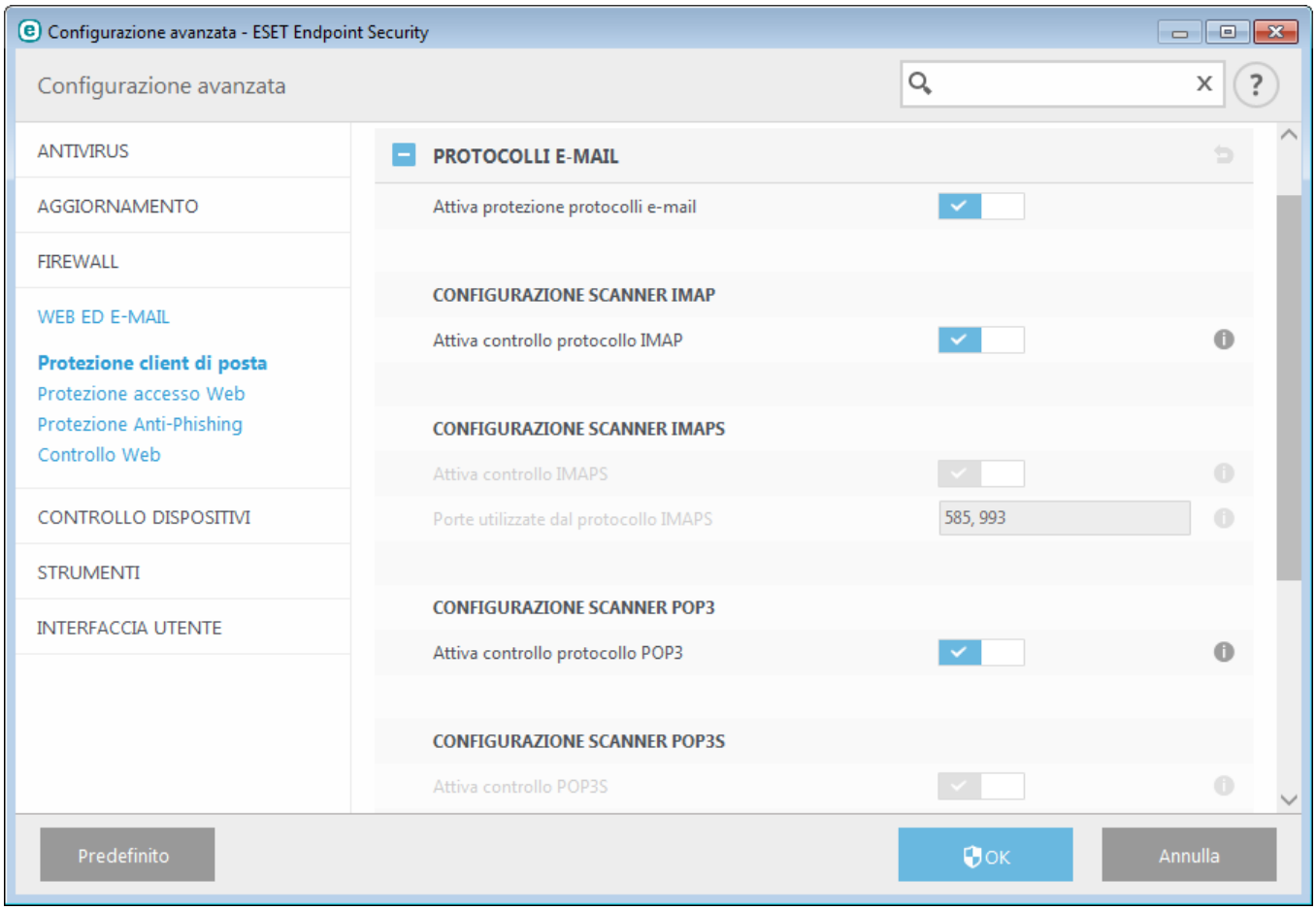
È possibile configurare il controllo dei protocolli IMAP/IMAPS e POP3/POP3S in Configurazione avanzata. Per accedere a questa impostazione, espandere **Web e e-mail** > **Protezione client di posta** > **Protocolli e-mail**.

Attiva protezione protocolli e-mail: attiva il controllo dei protocolli di posta elettronica.

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

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

Le comunicazioni crittografate non verranno controllate durante l'utilizzo delle impostazioni predefinite. Per attivare il controllo della comunicazione crittografata, accedere a SSL/TLS in Configurazione avanzata, fare clic su **Web e e-mail** > **SSL/TLS** e selezionare **Attiva filtraggio protocollo SSL**.



3.8.3.2.3 Avvisi e notifiche

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

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

Configurazione parametri motore ThreatSense - La configurazione avanzata dello scanner antivirus consente all'utente di configurare le destinazioni di controllo, i metodi di rilevamento e così via. Fare clic per visualizzare la finestra della configurazione dettagliata dello scanner antivirus.

Dopo che un messaggio e-mail è stato controllato, è possibile aggiungere una notifica contenente i risultati del controllo. È possibile scegliere le opzioni **Aggiungi notifiche all'e-mail ricevuta e letta, Aggiungi nota all'oggetto dell'e-mail infetta ricevuta e letta** o l'opzione **Aggiungi notifiche all'e-mail inviata**. Tenere presente che, in rare occasioni, le notifiche potrebbero essere omesse in messaggi HTML problematici o creati da malware. Le notifiche possono essere aggiunte sia alle e-mail ricevute e lette sia alle e-mail inviate. Le opzioni disponibili sono:

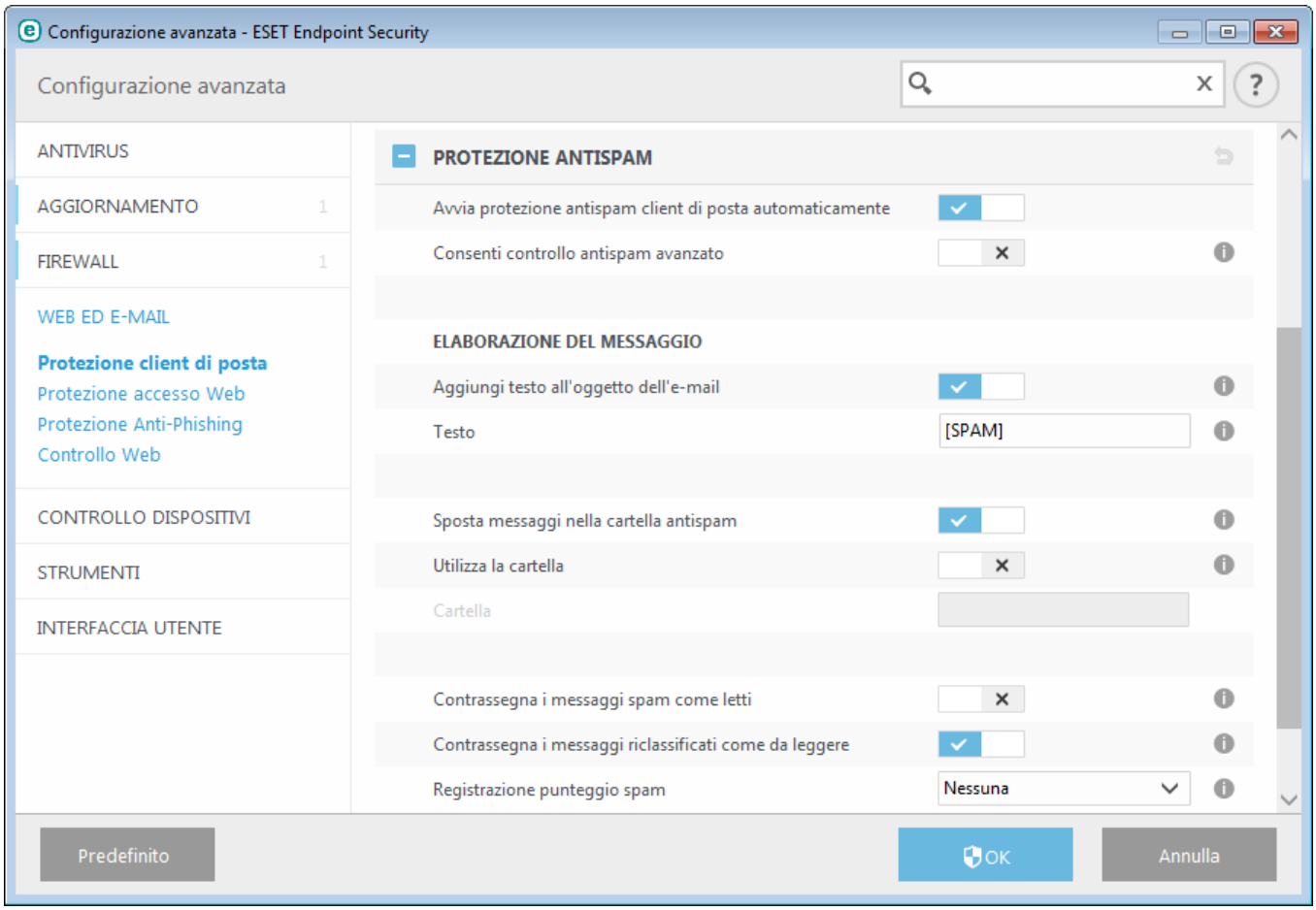
- **Mai**: non viene aggiunta alcuna notifica.
- **Solo per l'e-mail infetta**: solo i messaggi contenenti software dannoso vengono contrassegnati come controllati (impostazione predefinita).
- **Per tutte le e-mail** : il programma aggiunge la notifica a tutte le e-mail sottoposte a controllo.

Aggiungi nota all'oggetto dell'e-mail infetta inviata: disattivare questa opzione se non si desidera che la protezione e-mail includa un avviso antivirus nell'oggetto di un'e-mail infetta. Questa funzione consente di filtrare in modo semplice le e-mail infette in base all'oggetto (se supportata dal programma e-mail in uso). Aumenta inoltre il livello di credibilità del destinatario e, in caso di rilevamento di un'infiltrazione, fornisce informazioni utili sul livello di minaccia di un determinato messaggio e-mail o mittente.

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

3.8.3.2.4 Protezione antispam

I messaggi e-mail non desiderati, definiti spam, costituiscono uno dei maggiori problemi delle comunicazioni elettroniche. Lo spamming rappresenta fino all'80% di tutte le comunicazioni e-mail. La protezione antispam consente di prevenire questo problema. Associando una serie di principi di protezione e-mail, il modulo antispam offre un filtraggio di livello superiore per mantenere pulita la cartella Posta in arrivo.



Un principio essenziale per il rilevamento dello spam è la capacità di riconoscere messaggi indesiderati in base a indirizzi affidabili predefiniti (whitelist) e a indirizzi di spam (blacklist). Tutti gli indirizzi dell'elenco contatti dell'utente vengono aggiunti automaticamente alla whitelist, oltre a tutti gli altri indirizzi contrassegnati dall'utente come sicuri.

Il metodo principale per rilevare lo spam consiste nella scansione delle proprietà di un messaggio e-mail. I messaggi ricevuti vengono sottoposti a scansione secondo i criteri antispam di base (definizioni di messaggi, euristica statistica, riconoscimento di algoritmi e altri metodi univoci) e dal valore di indice risultante è possibile determinare se un messaggio è spam o meno.

Avvia protezione antispam client di posta automaticamente - Selezionando questa opzione, la protezione antispam verrà attivata automaticamente all'avvio del sistema.

Consenti controllo antispam avanzato - Verranno scaricati periodicamente dati antispam aggiuntivi, con il conseguente miglioramento delle capacità antispam e dei risultati.

La protezione Antispam in ESET Endpoint Security consente di impostare differenti parametri per gestire le mailing list. Le opzioni disponibili sono le seguenti:

Elaborazione del messaggio

Aggiungi testo all'oggetto dell'e-mail - Consente di aggiungere una stringa di testo predefinita e personalizzata nell'oggetto dei messaggi classificati come spam. La stringa predefinita è "[SPAMMING]".

Sposta messaggi nella cartella antispam - Attivando questa opzione, i messaggi di spam verranno spostati nella cartella della posta indesiderata predefinita e i messaggi riclassificati come non spam verranno spostati nella cartella della posta in arrivo. Facendo clic con il pulsante destro del mouse su un messaggio e-mail e selezionando ESET Endpoint Security dal menu contestuale, è possibile scegliere una delle opzioni disponibili.

Utilizza la cartella - Questa opzione sposta i messaggi di spam in una cartella definita dall'utente.

Contrassegna i messaggi di spam come letti - Attivare questa opzione per contrassegnare automaticamente come letti i messaggi di spamming. Consente di mettere in evidenza solo i messaggi "puliti".

Contrassegna il messaggio riclassificato come da leggere - I messaggi originariamente classificati come spam ma contrassegnati come "puliti" in un secondo tempo verranno visualizzati come da leggere.

Rapporto classificazione spam - Il motore antispam ESET Endpoint Security assegna un punteggio spam a ogni messaggio sottoposto a controllo. Il messaggio verrà registrato nel rapporto antispam (**ESET Endpoint Security** > **Strumenti** > **File di rapporto** > **Protezione antispam**).

- **Nessuno** - Il punteggio ricavato dal controllo antispam non verrà registrato.
- **Riclassificato e contrassegnato come spam** - Selezionare questa opzione se si desidera registrare un punteggio spam ai messaggi contrassegnati come SPAM.
- **Tutti** - Tutti i messaggi verranno registrati sul rapporto con un punteggio spam.

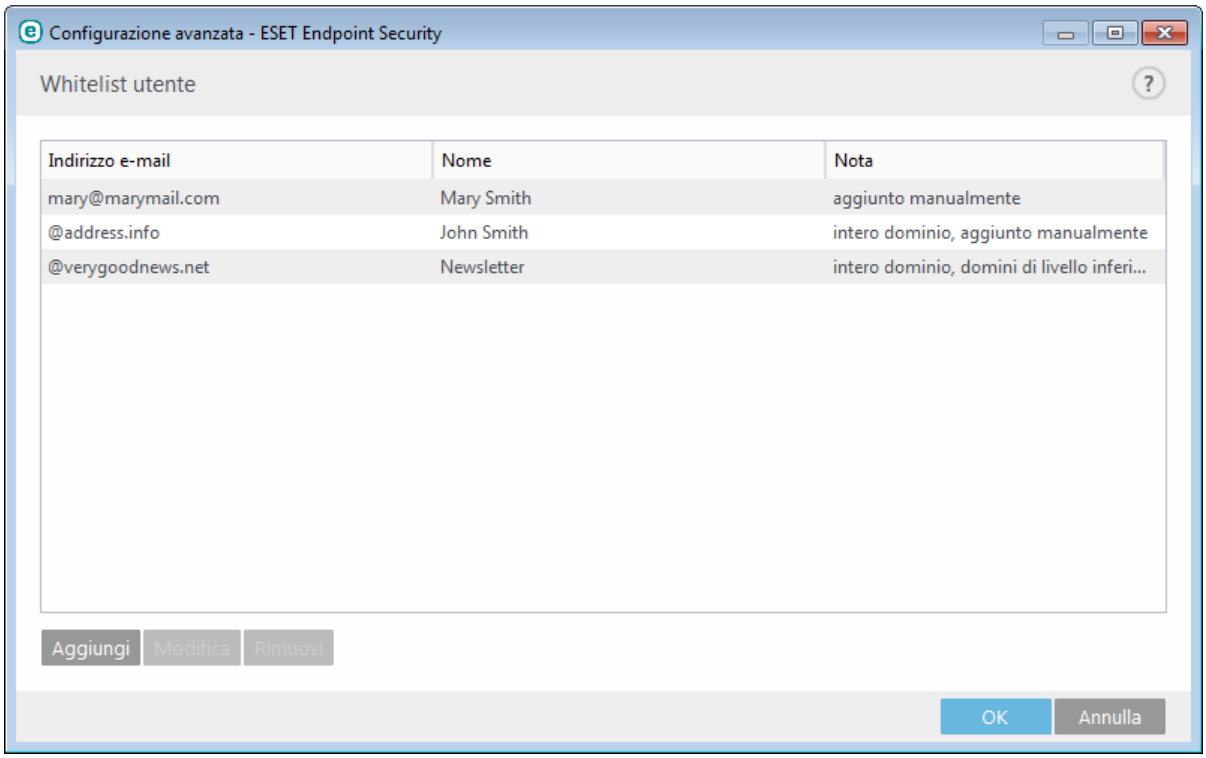
NOTA: dopo aver selezionato un messaggio contenuto nella cartella della posta indesiderata, è possibile scegliere l'opzione **Riclassifica messaggi selezionati come NON spam** per spostare il messaggio nella cartella della posta in arrivo. Dopo aver selezionato un messaggio considerato come spam nella cartella della posta in arrivo, selezionando **Riclassifica messaggi come spam**, è possibile spostare il messaggio nella cartella della posta indesiderata. È possibile selezionare più di un messaggio ed eseguire l'azione su tutti i messaggi contemporaneamente.

NOTA: ESET Endpoint Security supporta la protezione antispam per Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail.

3.8.3.2.4.1 Elenco blacklist/whitelist/eccezioni

Per proteggere gli utenti da messaggi e-mail indesiderati, ESET Endpoint Security consente di classificare gli indirizzi e-mail utilizzando elenchi specifici. La Whitelist contiene gli indirizzi e-mail che l'utente considera sicuri. I messaggi inviati dagli utenti presenti nella Whitelist sono sempre disponibili nella cartella della posta in arrivo. La Blacklist contiene gli indirizzi e-mail classificati come spam. Tutti i messaggi provenienti dai mittenti presenti nella blacklist vengono pertanto contrassegnati come spam. L'elenco eccezioni contiene gli indirizzi e-mail su cui viene sempre effettuato il controllo antispam. Tuttavia, può contenere anche indirizzi di messaggi e-mail non desiderati che, inizialmente, potrebbero non essere riconosciuti come spam.

È possibile modificare gli elenchi dalla finestra principale del programma ESET Endpoint Security in **Configurazione avanzata** > **Web e e-mail** > **Protezione client di posta** > **Rubriche antispam** utilizzando i pulsanti Aggiungi, Modifica e Rimuovi nella finestra di dialogo di ciascun elenco oppure da **Configurazione** > **Web e e-mail** dopo aver selezionato la rotella a forma di ingranaggio accanto a **Protezione antispam**.



Per impostazione predefinita, ESET Endpoint Security aggiunge tutti gli indirizzi della rubrica dei client e-mail supportati alla whitelist. Per impostazione predefinita, la blacklist è vuota. Per impostazione predefinita, l'Elenco eccezioni contiene solo gli indirizzi e-mail dell'utente.

3.8.3.2.4.2 Aggiunta di indirizzi alla whitelist e alla blacklist

Gli indirizzi e-mail appartenenti alle persone con le quali si comunica frequentemente possono essere aggiunti alla whitelist per essere certi che nessun messaggio proveniente da un indirizzo presente nella whitelist sia classificato come spam. Gli indirizzi spam noti possono essere aggiunti alla blacklist ed essere sempre classificati come spam. Per aggiungere un nuovo indirizzo alla whitelist o alla blacklist, fare clic con il pulsante destro del mouse sul messaggio e-mail e selezionare **ESET Endpoint Security** > **Aggiungi alla whitelist** o **Aggiungi alla blacklist**, oppure fare clic sul pulsante **Indirizzo affidabile** o **Indirizzo spam** sulla barra degli strumenti antispam di ESET Endpoint Security nel client e-mail.

Questa procedura può essere applicata anche agli indirizzi spam. Se un indirizzo e-mail viene riportato nella blacklist, tutti i messaggi e-mail provenienti da questo indirizzo saranno classificati come spam.

3.8.3.2.4.3 Contrassegnare i messaggi come spam o non spam

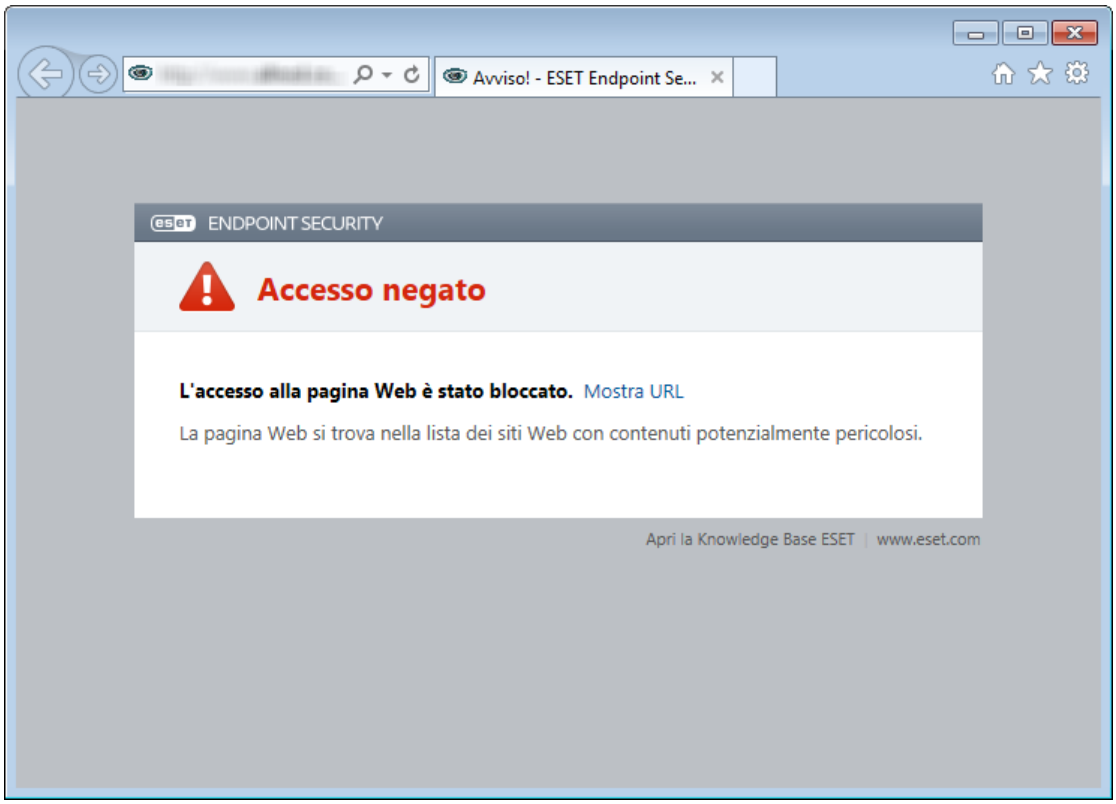
Qualsiasi messaggio visualizzato nel client e-mail può essere contrassegnato come spamming. A tale scopo, fare clic con il pulsante destro del mouse sul messaggio e selezionare **ESET Endpoint Security** > **Riclassifica messaggi selezionati come spam** oppure fare clic su **Spam** sulla barra degli strumenti antispam di ESET Endpoint Security collocata nella parte superiore del client di posta.

I messaggi riclassificati vengono spostati automaticamente nella cartella SPAM, ma l'indirizzo e-mail del mittente non viene aggiunto alla **Blacklist**. Allo stesso modo, i messaggi possono essere classificati come "non spam" facendo clic su **ESET Endpoint Security** > **Riclassifica messaggi selezionati come non spam** oppure su **Non spam** sulla barra degli strumenti antispam di ESET Endpoint Security nella sezione superiore del client di posta. Se i messaggi della cartella **Posta indesiderata** vengono classificati come non spam, verranno spostati nella cartella **Posta in arrivo**. Se un messaggio viene contrassegnato come non spam, l'indirizzo del mittente verrà aggiunto automaticamente alla **Whitelist**.

3.8.3.3 Protezione accesso Web

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

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



Si consiglia vivamente di lasciare l'opzione Protezione accesso Web attivata. L'opzione è disponibile dalla finestra principale del programma di ESET Endpoint Security accedendo a **Configurazione** > **Web e e-mail** > **Protezione accesso Web**.

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

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

3.8.3.3.1 Protocolli Web

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

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

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

La comunicazione crittografata non verrà controllata durante l'utilizzo delle impostazioni predefinite. Per attivare il controllo della comunicazione crittografata, accedere a SSL/TLS in Configurazione avanzata, fare clic su **Web e e-mail** > **SSL/TLS** e selezionare **Attiva filtraggio protocollo SSL**.

3.8.3.3.2 Gestione indirizzi URL

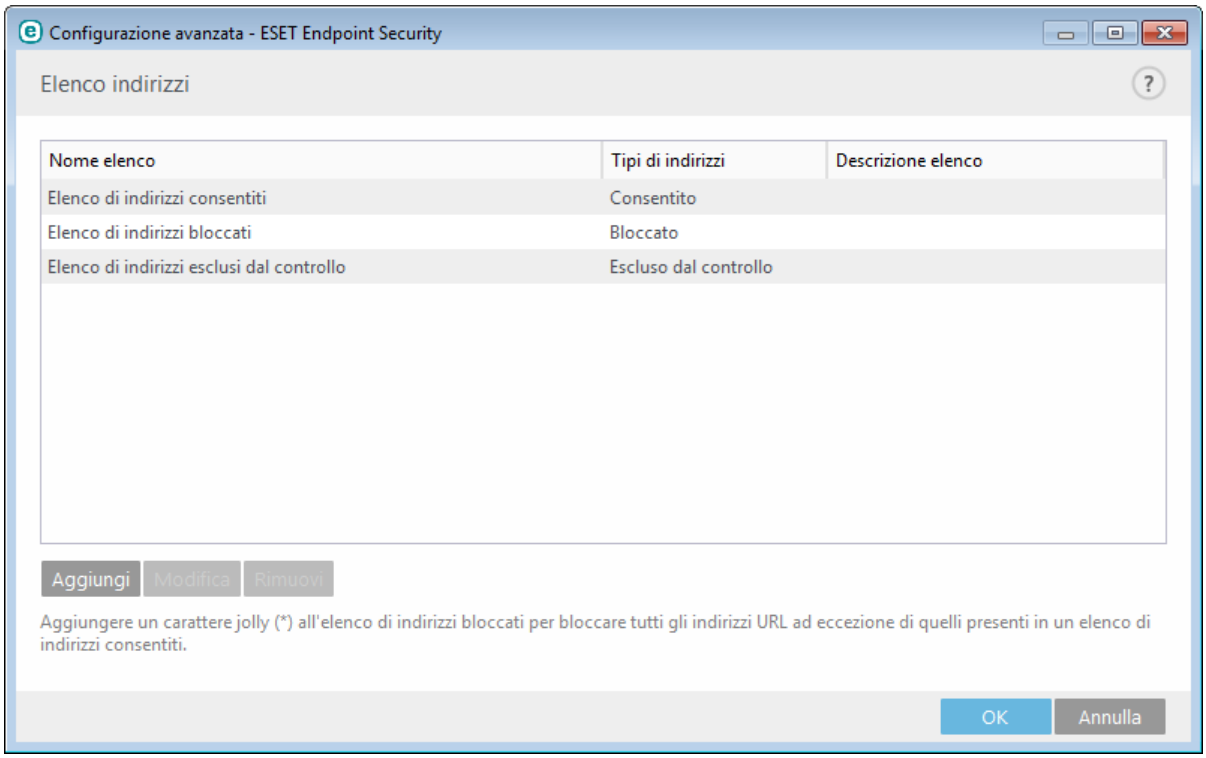
La sezione Gestione indirizzi URL consente all'utente di specificare gli indirizzi HTTP da bloccare, consentire o escludere dal controllo.

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

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

In tutti gli elenchi è possibile utilizzare i simboli speciali * (asterisco) e ? (punto interrogativo). L'asterisco rappresenta un qualsiasi numero o carattere, mentre il punto interrogativo rappresenta un qualsiasi carattere. Prestare particolare attenzione quando si specificano gli indirizzi esclusi dal controllo, in quanto l'elenco deve contenere solo indirizzi attendibili e sicuri. Allo stesso modo, è necessario verificare che in questo elenco i simboli * e ? siano utilizzati correttamente. Consultare Aggiungi indirizzo HTTP/maschera di dominio per ulteriori informazioni su come associare in maniera sicura un intero dominio, compresi tutti i sottodomini. Per attivare un elenco, abilitare l'opzione **Elenco attivo**. Se si desidera ricevere una notifica relativa all'inserimento di un indirizzo contenuto nell'elenco corrente, attivare **Notifica in caso di applicazione**.

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



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

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

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

3.8.3.4 Protezione Anti-Phishing

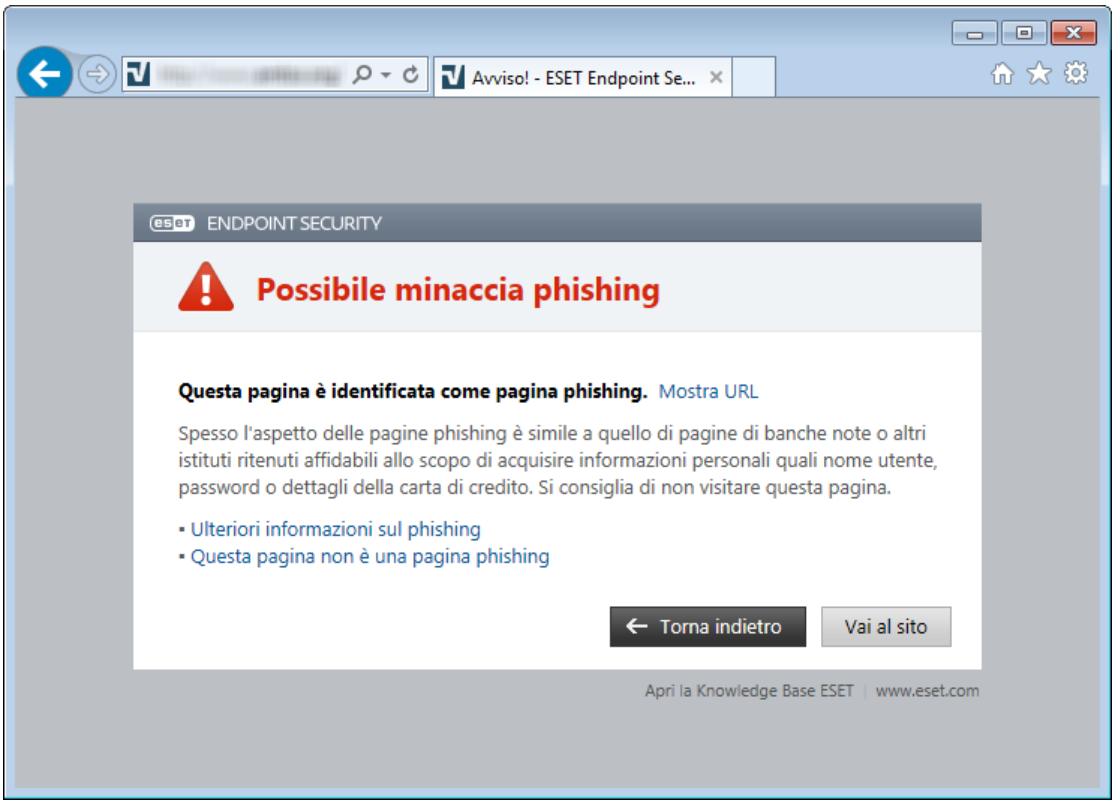
Il termine phishing definisce un'attività illegale che si avvale dell'ingegneria sociale (ovvero di manipolazione degli utenti al fine di ottenere informazioni riservate). Il phishing viene spesso utilizzato per ottenere l'accesso a dati sensibili quali numeri di conti bancari, codici PIN e così via.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

Si consiglia vivamente di attivare la funzione Anti-Phishing in ESET Endpoint Security. Per far ciò, aprire **Configurazione avanzata** (F5) > e accedere a **Web e e-mail** > **Protezione Anti-Phishing**.

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

Accesso a un sito Web phishing

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



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

Segnalazione di un sito phishing

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

NOTA: prima di inviare un sito Web a ESET, assicurarsi che soddisfi uno o più dei criteri seguenti:
- il sito Web non viene rilevato,
- il sito Web viene erroneamente rilevato come una minaccia. In questo caso, è possibile Segnalare un sito phishing falso positivo.

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

3.8.4 Controllo Web

La sezione Controllo Web consente all'utente di configurare impostazioni che proteggono l'azienda da rischi di responsabilità legale. Il controllo Web regola l'accesso a siti Web che violano i diritti di proprietà intellettuale. Lo scopo consiste nell'impedire ai dipendenti di accedere a pagine con contenuti inappropriati o dannosi o pagine che potrebbero avere un impatto negativo sulla produttività.

Il controllo Web consente di bloccare le pagine Web che possono contenere materiale potenzialmente inappropriato. I datori di lavoro o gli amministratori di sistema possono inoltre vietare l'accesso a più di 27 categorie predefinite e a più di 140 sottocategorie di siti Web.

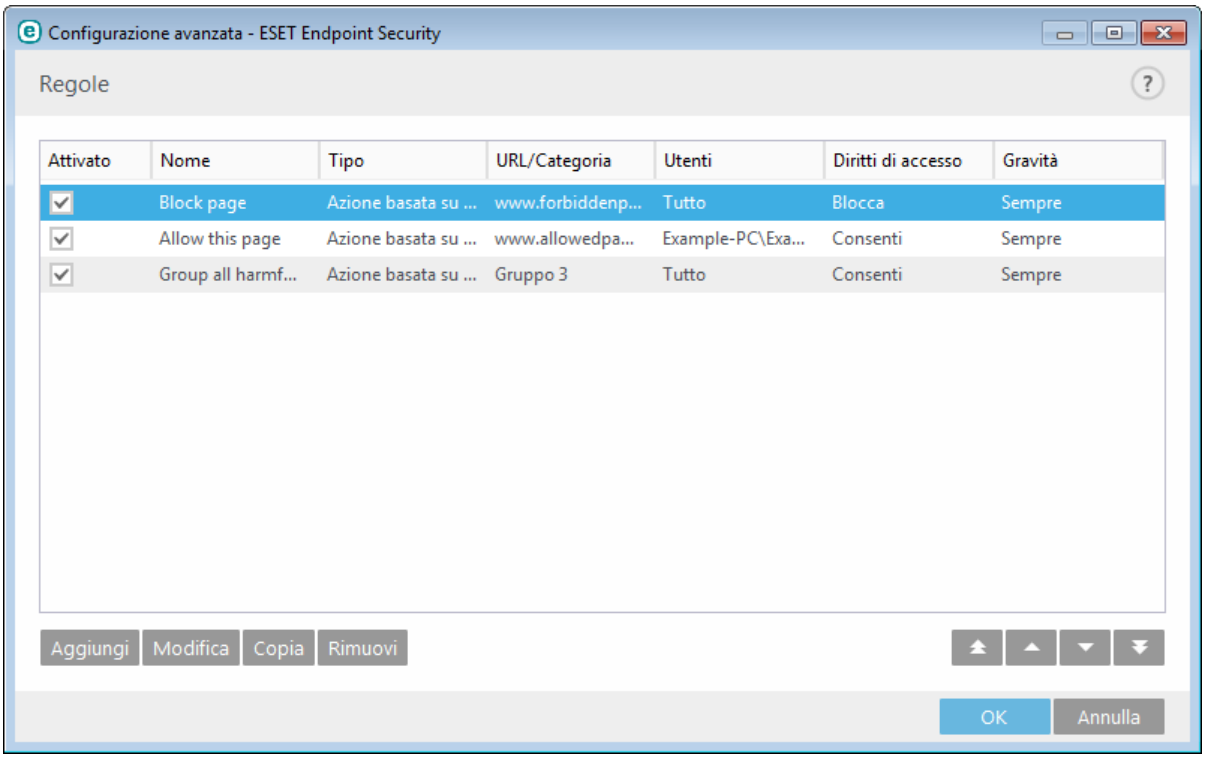
Per impostazione predefinita, il controllo Web è disattivato. Per attivare il controllo Web, premere F5 per accedere a **Configurazione avanzata** ed espandere **Web e e-mail** > **Controllo Web**. Selezionare **Integra nel sistema** per attivare il controllo Web in ESET Endpoint Security. Fare clic su **Modifica** accanto a **Regole**, per accedere alla finestra Editor regole controllo Web.

I campi **Messaggio pagina Web bloccata** e **Grafica pagina Web bloccata** consentono all'utente di personalizzare agevolmente il messaggio visualizzato in caso di blocco di un sito Web.

SUGGERIMENTO: un esempio di messaggio relativo a una pagina Web bloccata potrebbe essere *La pagina web è stata bloccata perché considerata inadeguata o a causa della presenza di contenuti dannosi. Contattare l'amministratore per ulteriori dettagli*. È inoltre possibile inserire un indirizzo Web o un percorso di rete con un'immagine personalizzata (ad esempio, *http://test.com/test.jpg*). Le dimensioni personalizzate dell'immagine sono impostate automaticamente su 90 x 30; se questi valori non sono impostati, le immagini verranno adattate automaticamente.

3.8.4.1 Regole

La finestra dell'editor **Regole** consente di visualizzare le regole basate su URL o basate su categorie esistenti.



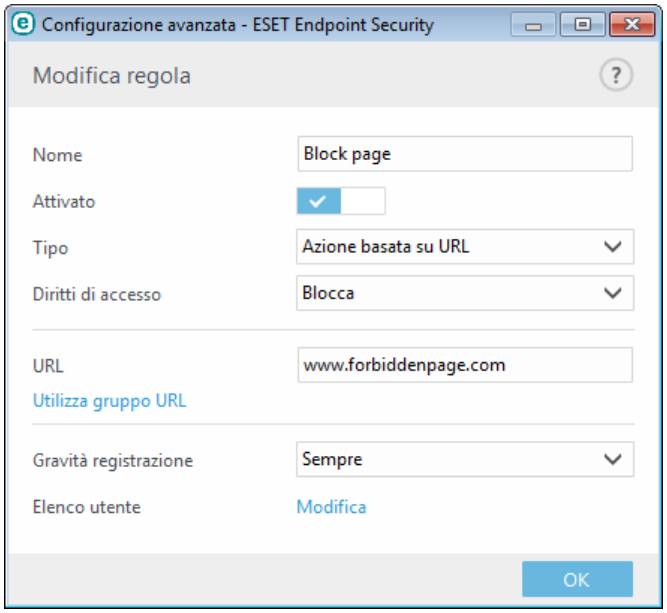
L'elenco delle regole contiene varie descrizioni di regole quali nome, tipo di blocco, azione da eseguire quando viene rilevata una corrispondenza con una regola del controllo Web e gravità del rapporto.

Fare clic su **Aggiungi** o **Modifica** per gestire una regola. Fare clic su **Copia** per creare una nuova regola con le opzioni predefinite utilizzate per un'altra regola selezionata. Premere **Ctrl** e fare clic per selezionare regole multiple ed eliminare tutte le regole selezionate. La casella di controllo **Attivata** consente di disattivare o attivare una regola. Questa opzione è utile se non si desidera eliminare definitivamente una regola in modo da poterla utilizzare in futuro.

Le regole vengono classificate in base al rispettivo ordine di priorità (le regole con priorità maggiore saranno posizionate in alto). La valutazione delle regole sulla base degli indirizzi URL presenta sempre una priorità maggiore rispetto alla valutazione basata sulla categoria. Ad esempio, se una regola basata su un indirizzo URL si trova sotto a una regola basata sulla categoria nell'elenco di regole, la prima regola presenterà un livello di priorità maggiore e verrà valutata per prima.

3.8.4.1.1 Aggiunta di regole del controllo Web

La finestra Regole del controllo Web consente all'utente di creare o modificare manualmente una regola di filtraggio del controllo Web esistente.



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

Tipo di azione

- **Azione basata su URL** - Per le regole che consentono di controllare l'accesso a un dato sito Web, inserire l'URL nel campo **URL**.
- **Azione basata su categoria** - Dopo aver selezionato questa opzione, impostare la relativa categoria utilizzando il menu a discesa.

I simboli speciali * (asterisco) e ? (punto interrogativo) non possono essere utilizzati nell'elenco di indirizzi URL. Durante la creazione di un gruppo di URL contenente un sito Web con vari domini di livello superiore (TLD), ciascuno di essi deve essere aggiunto separatamente. Se si aggiunge un dominio nel gruppo, tutti i contenuti presenti in tale dominio e in tutti i sottodomini (ad esempio, *sub.paginadiesempio.com*) saranno bloccati o consentiti in base all'azione basata su URL scelta dall'utente.

Diritti di accesso

- **Consenti**: l'accesso all'indirizzo o alla categoria di URL sarà consentito.
- **Avvisa**: invia un avviso all'utente sull'indirizzo o la categoria di URL.
- **Blocca**: blocca l'indirizzo o la categoria di URL.

URL o **Utilizza gruppo URL** : utilizza il collegamento URL o il gruppo di collegamenti per consentire, bloccare o avvisare l'utente in caso di rilevamento di uno di questi URL.

Gravità registrazione:

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

Elenco utente

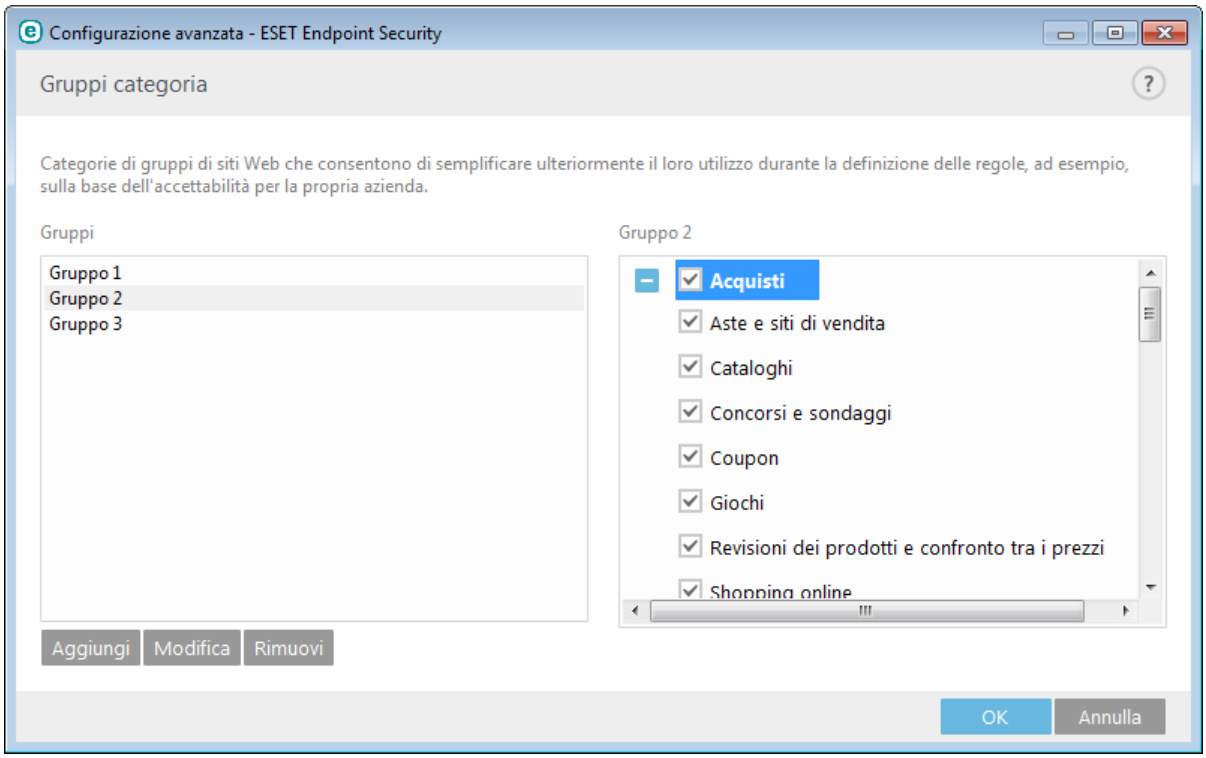
- **Aggiungi** - Apre la finestra di dialogo **Seleziona utenti o gruppi**, che consente di selezionare gli utenti desiderati. Se non si inserisce alcun utente, la regola verrà applicata per tutti gli utenti.
- **Rimuovi** - Rimuove l'utente selezionato dal filtro.

3.8.4.2 Gruppi categorie

La finestra Gruppi categorie è suddivisa in due parti. La parte sulla destra contiene un elenco di categorie e sottocategorie. Selezionare una categoria nell'elenco Categoria per visualizzare le rispettive sottocategorie.

Ciascun gruppo contiene sottocategorie per adulti e/o con contenuti generalmente inappropriati, nonché categorie considerate generalmente accettate. Aprendo la finestra Gruppi categorie e facendo clic sul primo gruppo, è possibile aggiungere o rimuovere le categorie/sottocategorie dall'elenco di gruppi appropriati (ad esempio, Violenza o Armi). È possibile bloccare le pagine Web con contenuti inappropriati oppure informare gli utenti in seguito alla creazione di una regola con azioni predefinite.

Selezionare la casella di controllo per aggiungere o rimuovere una sottocategoria da un gruppo specifico.



Seguono alcuni esempi di categorie con cui gli utenti potrebbero non avere dimestichezza:

Varie: generalmente indirizzi IP privati (locali) quali Intranet, 192.168.0.0/16 e così via. Se si visualizza un codice di errore 403 o 404, il sito Web troverà una corrispondenza anche con questa categoria.
Non risolto: questa categoria comprende pagine Web che non vengono risolte a causa di un errore di connessione al motore del database del Controllo Web.
Non classificato: pagine Web sconosciute che non sono ancora presenti nel database del Controllo Web.
Proxy: pagine Web quali anonymizer, redirector o server proxy pubblici che possono essere utilizzati per ottenere l'accesso (anonimo) a pagine Web generalmente vietate dal filtro del Controllo Web.
Condivisione file: queste pagine Web contengono una grande quantità di dati quali foto, video o libri elettronici. Vi è il rischio che questi siti contengano materiale potenzialmente inappropriato o contenuti per adulti.

NOTA: una sottocategoria può appartenere a un gruppo qualsiasi. Alcune sottocategorie non sono incluse nei gruppi predefiniti (ad esempio, Giochi). Per trovare una corrispondenza per una sottocategoria specifica mediante l'utilizzo del filtro controllo Web, è necessario aggiungerla al gruppo desiderato.

3.8.4.3 Gruppi URL

I gruppi di URL consentono all'utente di creare un gruppo contenente vari collegamenti URL per i quali desidera creare una regola (consenti/nega uno specifico sito Web).

Per creare un nuovo gruppo di URL, fare clic su **Aggiungi**. Selezionare un gruppo di URL e fare clic su **Aggiungi** nell'angolo in basso a destra della finestra per aggiungere un nuovo indirizzo URL nell'elenco oppure su **Importa** per importare un file con un elenco di indirizzi URL (separare i valori con un'interruzione di riga, ad esempio, *.txt utilizzando la codifica UTF-8). Se si desidera impostare un'azione da eseguire per un gruppo di URL specifico, aprire l'**Editor regole controllo Web**, selezionare il gruppo di URL utilizzando il menu a discesa, regolare gli altri parametri e fare clic su **OK**.

NOTA: può risultare più efficace bloccare o consentire una pagina Web specifica anziché bloccare o consentire un'intera categoria di pagine Web. Prestare attenzione quando si modificano queste impostazioni e si aggiunge una categoria o una pagina Web all'elenco.

3.8.5 Aggiornamento del programma

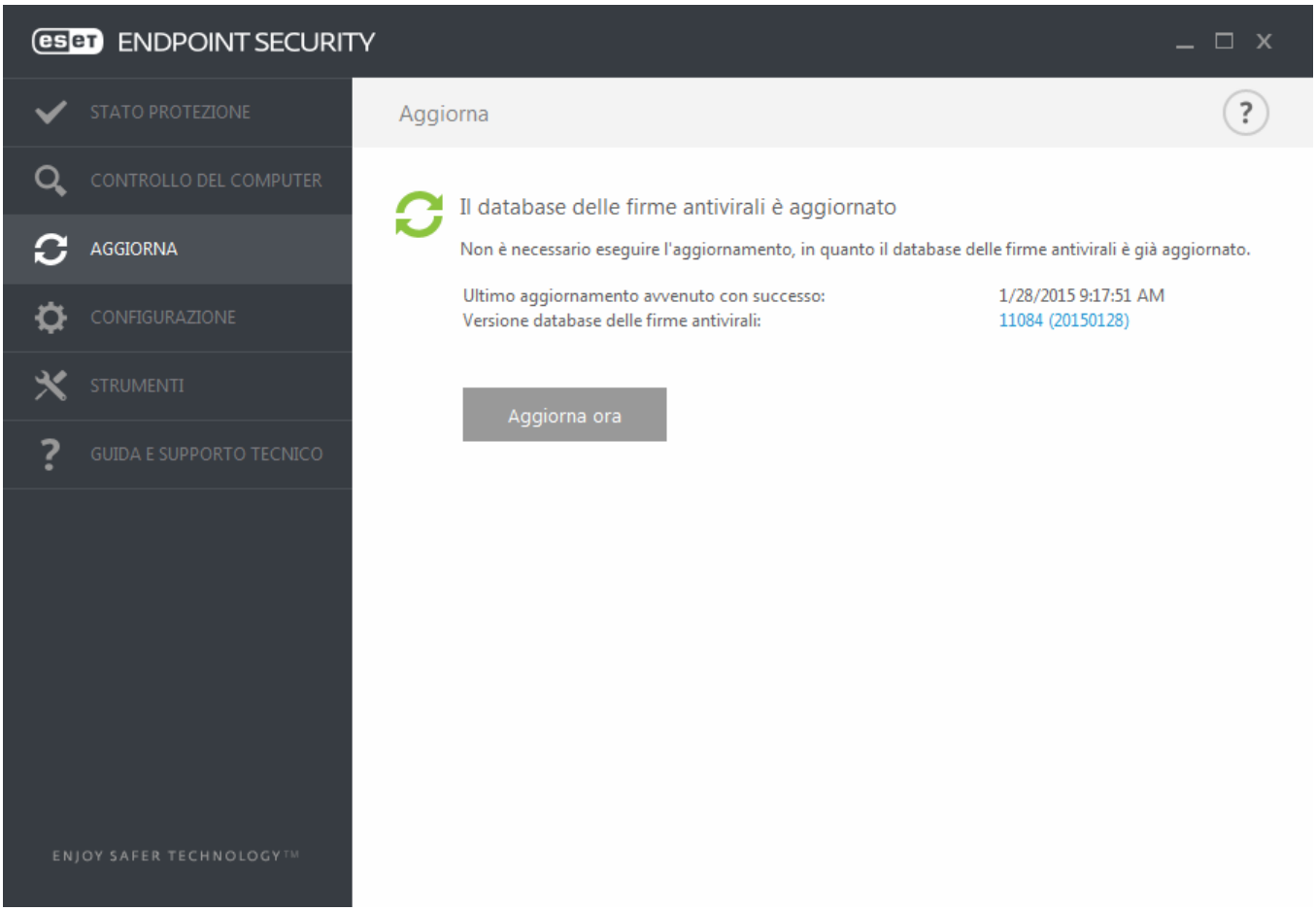
L'aggiornamento periodico di ESET Endpoint Security rappresenta il metodo migliore per ottenere il livello massimo di protezione del computer. Il modulo di aggiornamento garantisce l'aggiornamento ininterrotto del programma in due modi: attraverso l'aggiornamento rispettivamente del database delle firme antivirali e dei componenti del sistema.

Facendo clic su **Aggiorna** nella finestra principale del programma, è possibile visualizzare lo stato corrente degli aggiornamenti, comprese la data e l'ora dell'ultimo aggiornamento eseguito correttamente, e valutare l'eventuale necessità di un aggiornamento. Nella finestra principale sono inoltre contenute informazioni sulla versione del database delle firme antivirali. Questo indicatore numerico rappresenta un collegamento attivo al sito Web di ESET, in cui vengono riportate tutte le firme aggiunte nel corso dell'aggiornamento in questione.

È inoltre disponibile l'opzione per avviare manualmente il processo di aggiornamento: **Aggiorna database delle firme antivirali**. 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 relativa configurazione e al funzionamento. Se durante l'installazione non sono stati inseriti i dettagli della licenza, è possibile inserire la chiave di licenza facendo clic su **Attiva prodotto** durante l'aggiornamento per accedere ai server di aggiornamento ESET.

Se si attiva ESET Endpoint Security con il file della licenza off-line senza nome utente e password e si tenta di eseguire l'aggiornamento, il messaggio informativo in rosso **Aggiornamento del database delle firme antivirali terminato con un errore** indica che è possibile scaricare gli aggiornamenti esclusivamente dal mirror.

NOTA: la chiave di licenza è fornita da ESET dopo l'acquisto di ESET Endpoint Security.

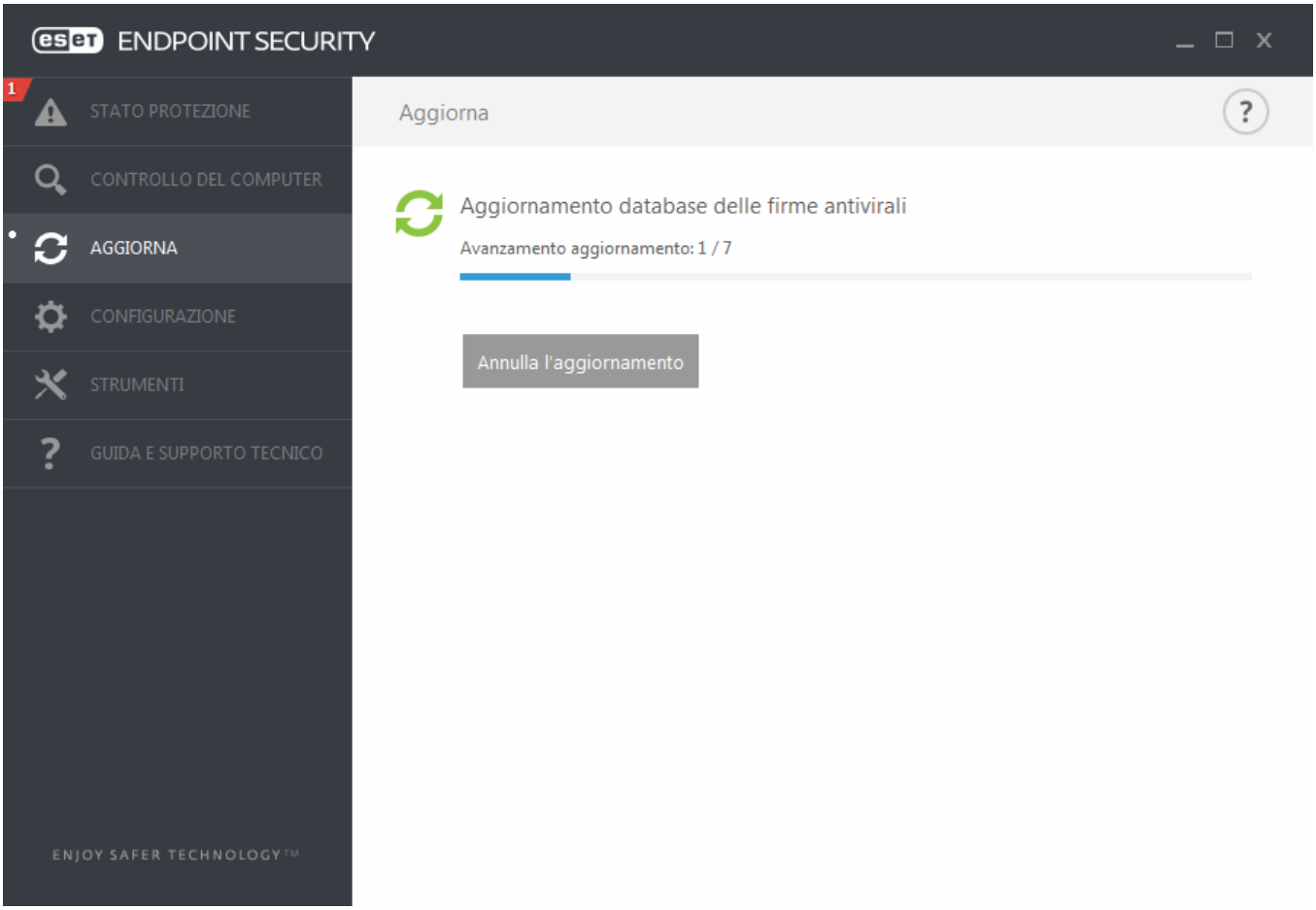


Ultimo aggiornamento riuscito: data dell'ultimo aggiornamento. Accertarsi che la data sia recente: ciò significa che il database delle firme antivirali è aggiornato.

Versione del database delle firme antivirali - Numero del database delle firme antivirali, ma anche collegamento attivo al sito Web di ESET. Selezionare per visualizzare un elenco di tutte le firme aggiunte in un aggiornamento specifico.

Processo di aggiornamento

Dopo aver selezionato **Aggiornamento del database delle firme antivirali**, viene avviato il processo di download. Verranno visualizzati una barra di avanzamento del download e il tempo rimanente per il completamento dell'operazione. Per interrompere l'aggiornamento, fare clic su **Annulla l'aggiornamento**.

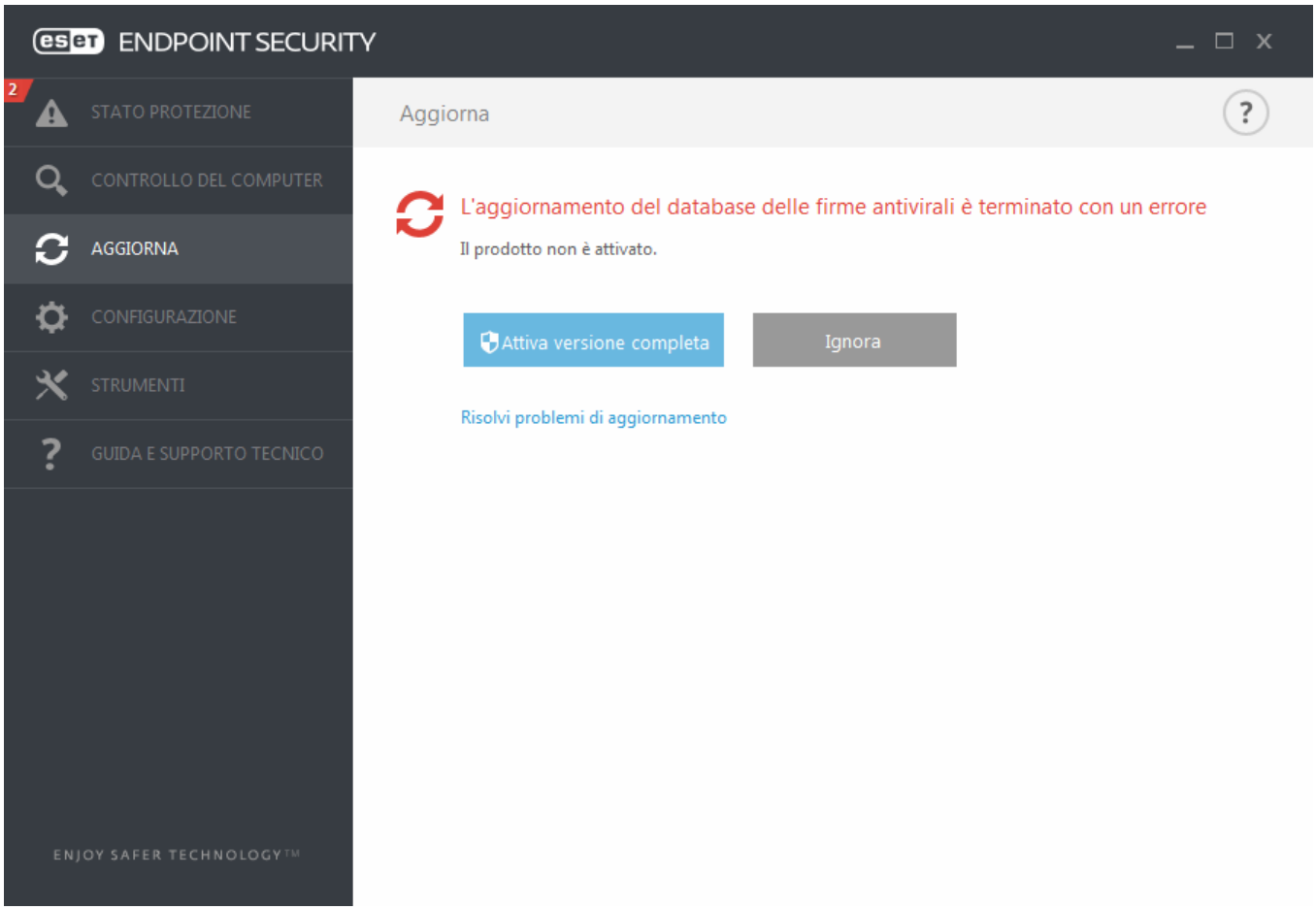


Importante: in circostanze normali, quando gli aggiornamenti sono scaricati correttamente, nella finestra **Aggiorna** viene visualizzato il messaggio **Aggiornamento non necessario. Il database delle firme antivirali è aggiornato**. In caso contrario, il programma è obsoleto ed è maggiormente esposto alle infezioni. Aggiornare il database delle firme antivirali appena possibile. In caso contrario, viene visualizzato uno dei seguenti messaggi:

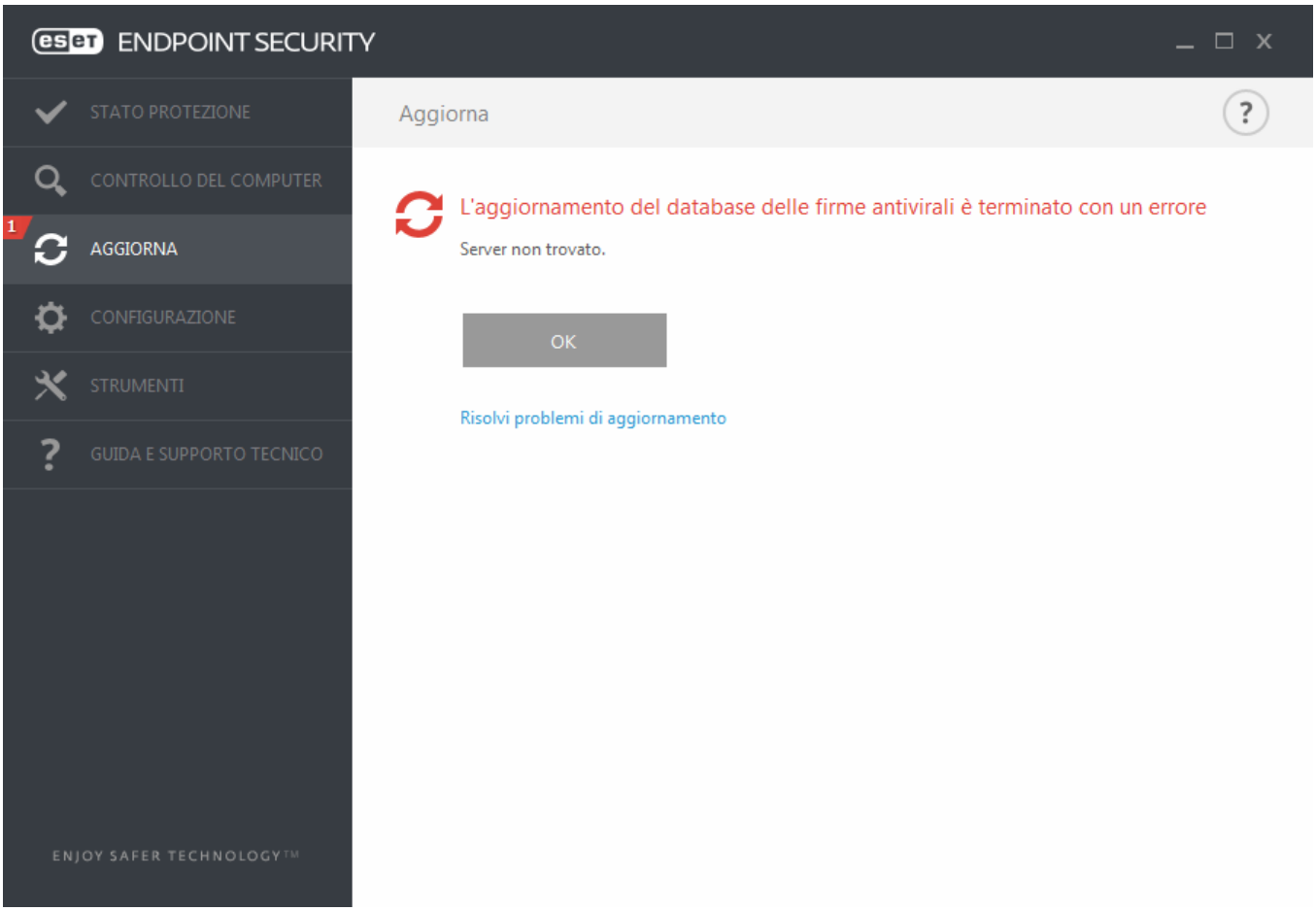
Il database delle firme antivirali è obsoleto: questo errore viene visualizzato dopo diversi tentativi non riusciti di aggiornamento del database delle firme antivirali. Si consiglia di controllare le impostazioni di aggiornamento. Spesso questo errore viene visualizzato perché i dati di autenticazione non vengono immessi correttamente o le impostazioni di connessione sono errate.

Il messaggio di notifica precedente è correlato ai due messaggi che seguono, relativi ad aggiornamenti non riusciti (**Aggiornamento del database delle firme antivirali non riuscito**):

1. **Licenza non valida** - La chiave di licenza non è stata inserita correttamente durante la configurazione dell'aggiornamento. Si consiglia di verificare i dati di autenticazione. Nella finestra Configurazione avanzata (fare clic su **Configurazione** nel menu principale, quindi su **Configurazione avanzata** oppure premere F5 sulla tastiera), sono disponibili ulteriori opzioni di aggiornamento. Fare clic su **Guida e supporto tecnico** > **Gestisci licenza** nel menu principale per inserire una nuova chiave di licenza.



2. **Si è verificato un errore durante il download dei file di aggiornamento** - L'errore potrebbe essere causato da Impostazioni di connessione Internet non corrette. Si consiglia di verificare la connettività Internet (aprendo un qualsiasi sito Web nel browser). Se il sito Web non si apre, è possibile che la connessione Internet non sia presente o che si siano verificati problemi di connettività nel computer in uso. Se la connessione Internet non è attiva, contattare il proprio Provider di servizi Internet (ISP).



NOTA: per ulteriori informazioni, consultare questo articolo della Knowledge Base ESET.

3.8.5.1 Configurazione dell'aggiornamento

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

Generale

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

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

Avvisi database firme antivirali obsoleto

Imposta automaticamente l'età massima del database: consente di impostare il tempo massimo (in giorni) dopo il quale il database delle firme antivirali verrà segnalato come obsoleto. Il valore predefinito è 7.

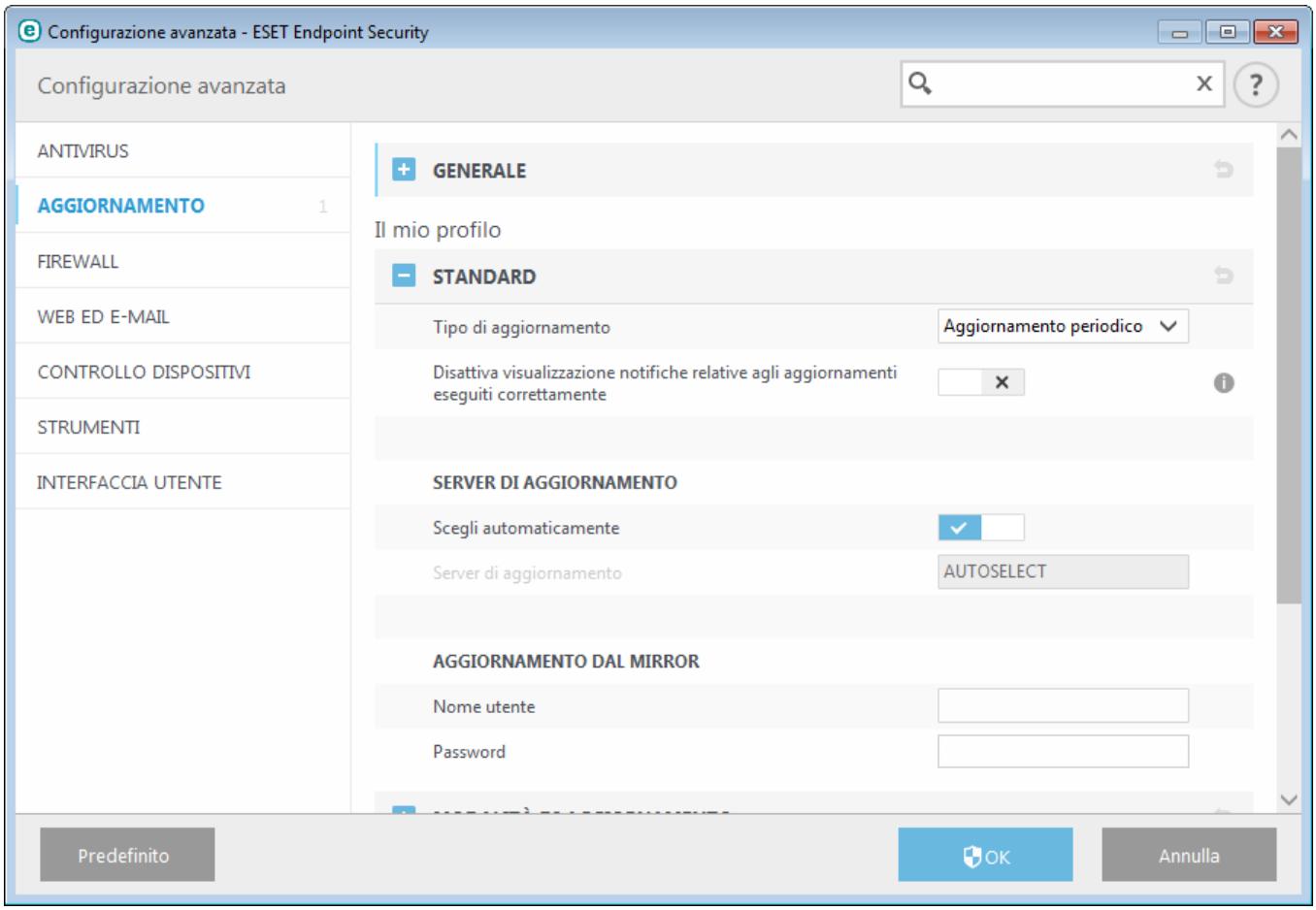
Rollback

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

caso di rimando indefinito da parte dell'utente.

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

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



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

Di base

Per impostazione predefinita, il **Tipo di aggiornamento** è impostato su **Aggiornamento periodico** per garantire che i file di aggiornamento vengano scaricati automaticamente dal server ESET che presenta il traffico di rete minore. Gli aggiornamenti pre-rilascio (opzione **Aggiornamento pre-rilascio**) sono aggiornamenti sottoposti ad approfondite verifiche interne che saranno presto disponibili per tutti. Gli aggiornamenti pre-rilascio consentono di accedere ai metodi di rilevamento e alle correzioni più recenti. È tuttavia probabile che tali aggiornamenti non siano sempre sufficientemente stabili e NON devono pertanto essere utilizzati su server di produzione e workstation dove è richiesta massima disponibilità e stabilità. **Aggiornamento ritardato** consente di eseguire l'aggiornamento da server di aggiornamento speciali che mettono a disposizione nuove versioni dei database delle firme antivirali con un ritardo di almeno X ore (ad esempio, database testati in un ambiente reale e considerati, pertanto, stabili).

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

Per impostazione predefinita, il menu **Server di aggiornamento** è impostato su SELEZIONE AUTOMATICA. Il server di

aggiornamento rappresenta il luogo di archiviazione degli aggiornamenti. Se si utilizza un server ESET, si consiglia di lasciare selezionata l'opzione predefinita.

Quando si utilizza un server HTTP locale (noto anche come mirror), il server di aggiornamento deve essere impostato come riportato di seguito:
http://nome_computer_o_relativo_indirizzo_IP:2221

Quando si utilizza un server HTTP locale con SSL, il server di aggiornamento deve essere impostato come riportato di seguito:
https://nome_computer_o_relativo_indirizzo_IP:2221

Quando si utilizza una cartella locale condivisa, il server di aggiornamento deve essere impostato come riportato di seguito:
\\nome_computer__o_relativo_indirizzo_IP\cartella_condivisa

Aggiornamento dal mirror

L'autenticazione per i server di aggiornamento si basa sulla **Chiave di licenza** generata e inviata dopo l'acquisto. In caso di utilizzo di un server mirror locale, è possibile definire le credenziali per consentire ai client di accedere al server mirror prima di ricevere gli aggiornamenti. Per impostazione predefinita, non è richiesta alcuna verifica e i campi **Nome utente** e **Password** sono lasciati vuoti.

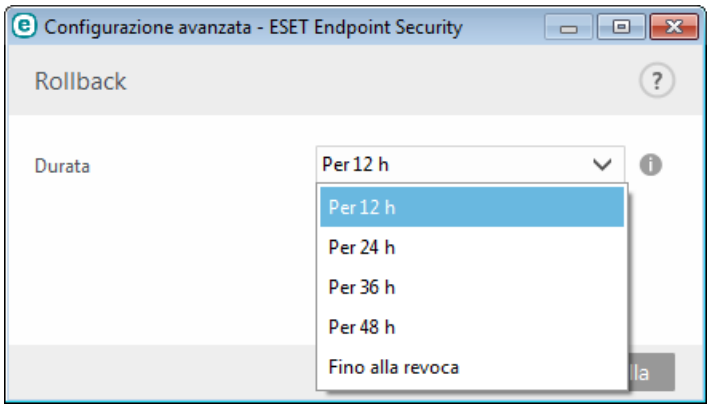
3.8.5.1.1 Profili di aggiornamento

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

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

3.8.5.1.2 Rollback aggiornamento

Se si fa clic su **Rollback** (**Configurazione avanzata** (F5) > **Aggiornamento** > **Profilo**), è necessario scegliere un intervallo temporale dal menu a discesa che indica il periodo di tempo nel quale gli aggiornamenti del database delle firme antivirali e del modulo di programma verranno sospesi.



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

Il database delle firme antivirali viene ripristinato alla versione più vecchia disponibile e memorizzato come snapshot nel file system del computer locale.

Esempio: si supponga che la versione più recente del database delle firme antivirali corrisponde al numero 10646. Le versioni 10645 e 10643 sono memorizzate come snapshot del database delle firme antivirali. Si tenga presente che la versione 10644 non è disponibile poiché, ad esempio, il computer è stato spento ed è stato reso disponibile un aggiornamento più recente prima che venisse scaricata la versione 10644. Se il campo **Numero di snapshot**

memorizzati localmente è impostato su 2 e si fa clic su **Rollback**, il database delle firme antivirali (compresi i moduli del programma) verrà ripristinato al numero di versione 10643. Il processo potrebbe richiedere alcuni minuti. Verificare se il database delle firme antivirali è stato ripristinato a una versione precedente dalla finestra principale del programma di ESET Endpoint Security nella sezione Aggiornamento.

3.8.5.1.3 Modalità di aggiornamento

La scheda **Modalità di aggiornamento** contiene opzioni correlate all'aggiornamento dei componenti di programma. Il programma consente di preimpostare le azioni da eseguire quando è disponibile un nuovo aggiornamento dei componenti di programma.

Gli aggiornamenti dei componenti di programma aggiungono nuove funzioni o introducono modifiche alle funzioni già esistenti nelle versioni precedenti. Possono essere eseguiti automaticamente senza alcun intervento da parte dell'utente oppure è possibile scegliere di ricevere una notifica. Una volta installato l'aggiornamento dei componenti di programma, potrebbe essere necessario riavviare il computer. Nella sezione **Aggiornamento componenti programma** sono disponibili tre opzioni:

- **Chiedi prima di scaricare i componenti di programma**: opzione predefinita. All'utente verrà chiesto di confermare o rifiutare gli aggiornamenti dei componenti di programma, se disponibili.
- **Aggiorna sempre i componenti di programma** - L'aggiornamento dei componenti di programma verrà scaricato e installato automaticamente. Ricordare che potrebbe essere necessario riavviare il computer.
- **Non aggiornare mai i componenti di programma**: l'aggiornamento dei componenti di programma non viene eseguito. Questa opzione è adatta alle installazioni su server, poiché di norma i server possono essere riavviati solo durante la manutenzione.

NOTA: la scelta dell'opzione più adatta dipende dalla workstation sulla quale saranno applicate le impostazioni. Tenere presente che esistono alcune differenze tra le workstation e i server. Ad esempio, il riavvio automatico del server dopo un aggiornamento di un programma potrebbe causare gravi danni.

Se è attiva l'opzione **Chiedi prima di scaricare l'aggiornamento**, verrà visualizzata una notifica ogni volta che è disponibile un nuovo aggiornamento.

Se la dimensione del file di aggiornamento supera il valore specificato nel campo **Chiedi se un file di aggiornamento è maggiore di (KB)**, verrà visualizzata una notifica.

3.8.5.1.4 Proxy HTTP

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

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

Se si seleziona l'opzione **Utilizza impostazioni server proxy globali**, verranno utilizzate le opzioni di configurazione del server proxy già specificate all'interno della sottostruttura **Strumenti** > **Server proxy** della struttura Configurazione avanzata.

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

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

- È necessario utilizzare un server proxy per aggiornare ESET Endpoint Security e tale server è differente da quello specificato nelle impostazioni globali (**Strumenti** > **Server proxy**). In questo caso, sarà necessario fornire alcune informazioni aggiuntive: Indirizzo del **Server proxy**, **Porta** di comunicazione (3128 per impostazione predefinita), più **Nome utente** e **Password** per il server del proxy, se necessario.
- Le impostazioni del server proxy non sono state configurate a livello globale. ESET Endpoint Security effettuerà tuttavia la connessione a un server proxy per verificare la disponibilità di aggiornamenti.
- Il computer è connesso a Internet tramite un server proxy. Le impostazioni vengono estrapolate da Internet

Explorer durante l'installazione del programma. Tuttavia, in caso di modifiche successive, ad esempio, se si cambia il provider di servizi Internet (ISP), è necessario verificare che le impostazioni del proxy HTTP elencate in questa finestra siano corrette. In caso contrario, il programma non sarà in grado di connettersi ai server di aggiornamento.

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

NOTA: i dati di autenticazione, come ad esempio il **Nome utente** e la **Password**, sono necessari per accedere al server proxy. Compilare questi campi solo se sono richiesti un nome utente e una password. Tenere presente che questi campi, in cui non è necessario inserire il Nome utente e la Password per ESET Endpoint Security, devono essere completati solo se è richiesta una password di accesso a Internet mediante un server proxy.

3.8.5.1.5 Connetti a LAN come

Durante l'aggiornamento da un server locale con una versione del sistema operativo Windows NT, per impostazione predefinita è richiesta l'autenticazione per ciascuna connessione di rete.

Per configurare un account simile, selezionare dal menu a discesa **Tipo di utente locale**:

- **Account di sistema (predefinito)**,
- **Utente corrente**,
- **Utente specificato**.

Selezionare **Account di sistema (predefinito)** per utilizzare l'account di sistema per l'autenticazione. In genere non viene eseguito alcun processo di autenticazione se nella sezione principale di impostazione dell'aggiornamento non sono specificati dati di autenticazione.

Per essere certi che il programma esegua l'autenticazione utilizzando l'account di un utente che ha eseguito correntemente l'accesso, selezionare **Utente corrente**. Lo svantaggio di questa soluzione consiste nel fatto che il programma non è in grado di connettersi al server di aggiornamento se nessun utente ha eseguito l'accesso in quel momento.

Selezionare **Utente specificato** se si desidera che il programma utilizzi un account utente specifico per l'autenticazione. Utilizzare questo metodo quando la connessione con l'account di sistema predefinito non riesce. Tenere presente che l'account dell'utente specificato deve disporre dell'accesso alla directory dei file di aggiornamento sul server locale. In caso contrario, il programma non sarà in grado di stabilire una connessione e scaricare gli aggiornamenti.

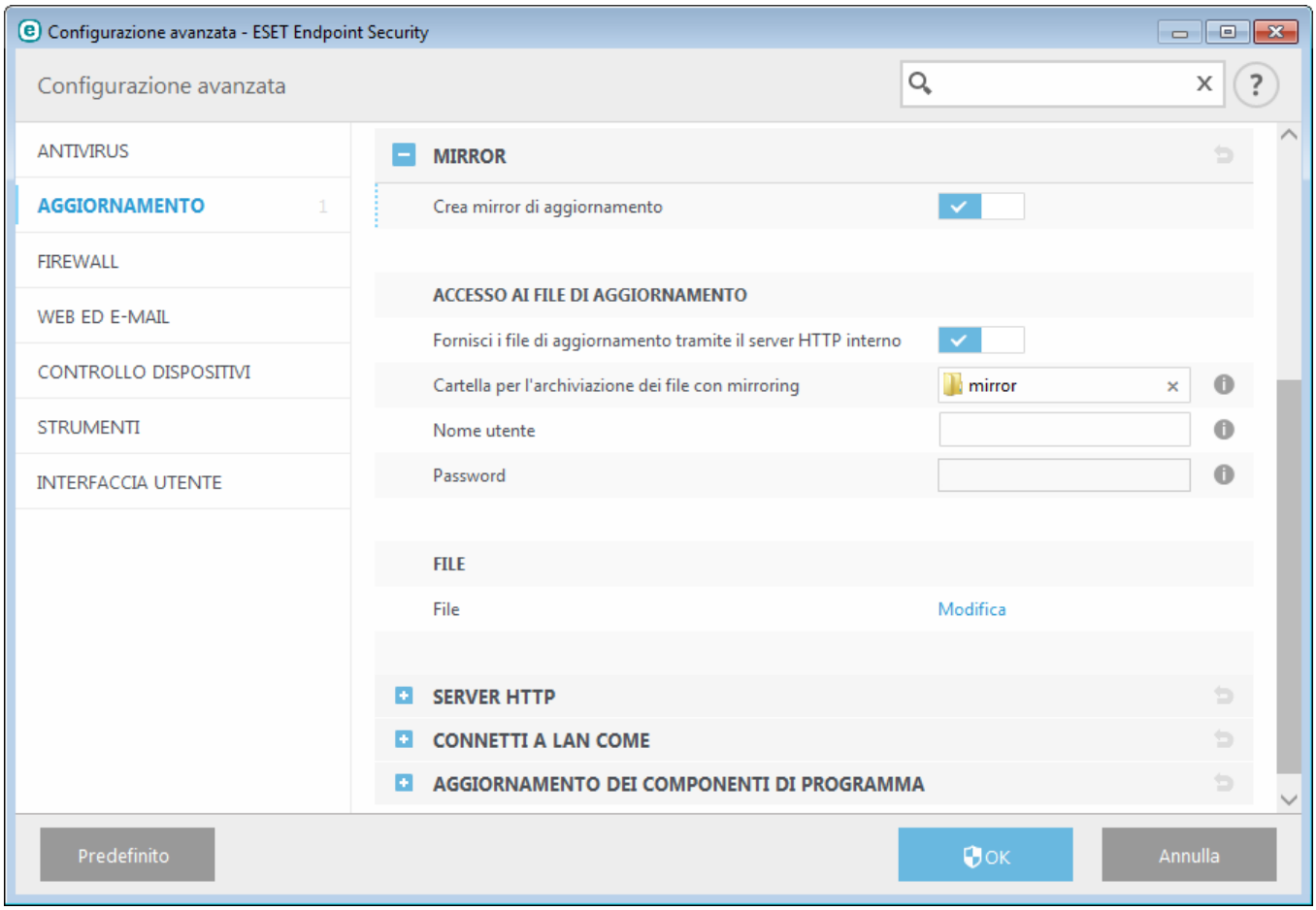
Avviso: se si seleziona **Utente corrente** o **Utente specificato**, è possibile che si verifichi un errore quando si modifica l'identità del programma per l'utente desiderato. È consigliabile immettere i dati di autenticazione della LAN nella sezione principale di configurazione dell'aggiornamento. In questa sezione di impostazione dell'aggiornamento, i dati di autenticazione devono essere inseriti come segue: *nome_dominio\utente* (se si tratta di un gruppo di lavoro, immettere *none_gruppodilavoro\nome*) e la password utente. Per l'aggiornamento dalla versione HTTP del server locale, non è richiesta alcuna autenticazione.

Attivare **Disconnetti dal server dopo l'aggiornamento** per forzare una disconnessione se una connessione al server dovesse rimanere attiva anche dopo il download degli aggiornamenti.

3.8.5.1.6 Mirror

ESET Endpoint Security consente all'utente di creare copie dei file di aggiornamento che è possibile utilizzare per aggiornare altre workstation della rete. Utilizzo di un *"mirror"*: è utile disporre di una copia dei file di aggiornamento nell'ambiente LAN, in quanto in questo modo i file di aggiornamento non devono essere scaricati ripetutamente dal server di aggiornamento del fornitore da ogni singola workstation. Gli aggiornamenti vengono scaricati sul server del mirror locale e distribuiti a tutte le workstation, allo scopo di evitare il rischio di un sovraccarico del traffico di rete. L'aggiornamento delle workstation client da un mirror consente di ottimizzare il bilanciamento del carico di rete e di risparmiare ampiezza di banda per la connessione a Internet.

Le opzioni di configurazione del server del mirror locale sono collocate in Configurazione avanzata sotto a **Aggiornamento**. Per accedere a questa sezione, premere **F5**; per accedere a Configurazione avanzata, fare clic su **Aggiornamento** e selezionare la scheda **Mirror**.



Per creare un mirror su una workstation client, attivare **Crea mirror di aggiornamento**. Attivando 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 con mirroring.

Accesso ai file di aggiornamento

Fornisci i file di aggiornamento tramite il server HTTP interno: se questa opzione è attiva, è possibile accedere ai file di aggiornamento tramite HTTP senza che vengano richieste le credenziali.

NOTA: Windows XP richiede il Service Pack 2 o versioni successive per l'utilizzo del server HTTP.

I metodi per accedere al server del mirror sono descritti in dettaglio in Aggiornamento dal mirror. Sono disponibili due metodi di base per l'accesso al mirror: la cartella con i file di aggiornamento può essere presentata come cartella di rete condivisa oppure i client possono accedere al mirror collocato su un server HTTP.

La cartella dedicata alla memorizzazione dei file di aggiornamento per il mirror è definita sotto a **Cartella per l'archiviazione dei file con mirroring**. Fare clic su **Cartella** per cercare una cartella sul computer locale o una cartella di rete condivisa. Se è necessaria l'autorizzazione per la cartella specificata, i dati di autenticazione devono essere inseriti nei campi **Nome utente** e **Password**. Se la cartella di destinazione selezionata si trova su un disco di rete sul quale viene eseguito un sistema operativo Windows NT/2000/XP, il nome utente e la password specificati devono possedere i privilegi di scrittura per la cartella selezionata. Nome utente e password devono essere specificati nel formato *Dominio/Utente* o *Gruppodilavoro/Utente*. È necessario specificare le password corrispondenti.

File: durante la configurazione del mirror, è possibile specificare le lingue degli aggiornamenti che si desidera scaricare. Le lingue selezionate devono essere supportate dal server del mirror configurato dall'utente.

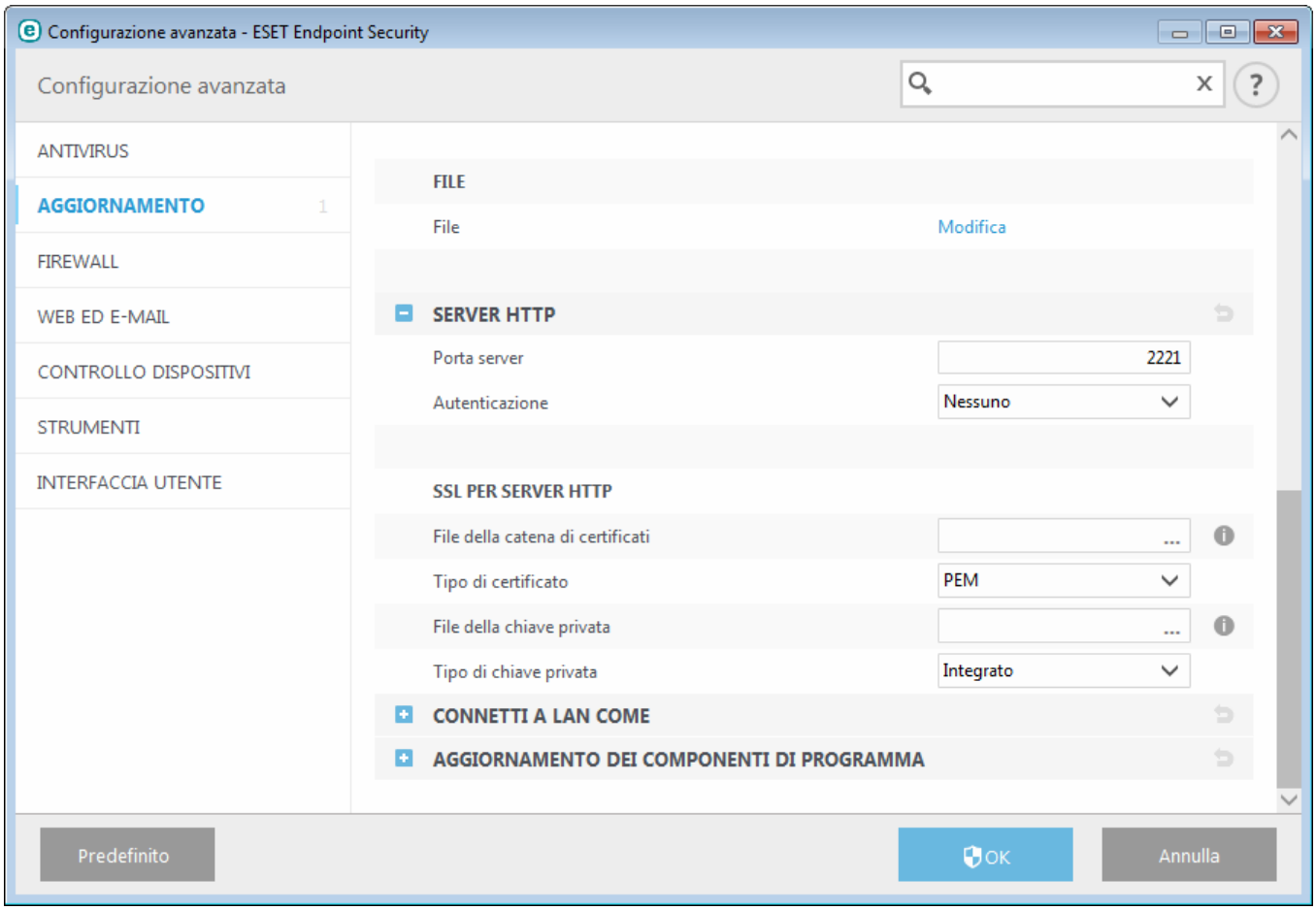
Server HTTP

Porta server: per impostazione predefinita, la porta del server è impostata su 2221.

Autenticazione: definisce il metodo di autenticazione utilizzato per l'accesso ai file di aggiornamento. Sono disponibili le seguenti opzioni: **Nessuno**, **Di base** e **NTLM**. Selezionare **Di base** per utilizzare la codifica base64 con l'autenticazione di base di nome utente e password. L'opzione **NTLM** offre una codifica basata sull'utilizzo di un metodo sicuro. Per l'autenticazione, viene utilizzato l'utente creato sulla workstation che condivide i file di

aggiornamento. L'impostazione predefinita è **Nessuno**, che garantisce l'accesso ai file di aggiornamento senza che sia necessaria l'autenticazione.

Se si desidera eseguire il server HTTP con il supporto HTTPS (SSL), è necessario aggiungere il **File della catena di certificato** o generare un certificato autofirmato. Sono disponibili i seguenti tipi di certificati: ASN, PEM e PFX. Per un livello di protezione aggiuntivo, è possibile utilizzare il protocollo HTTPS per scaricare i file di aggiornamento. Tramite questo protocollo, è quasi impossibile tenere traccia dei trasferimenti di dati e delle credenziali di accesso. Per impostazione predefinita, l'opzione **Tipo di chiave privata** è impostata su **Integrato** (e, di conseguenza, per impostazione predefinita, l'opzione **File della chiave privata** è disattivata). Ciò significa che la chiave privata fa parte del file della catena di certificati selezionato.



Connetti a LAN come

Tipo di utente locale: le impostazioni **Account di sistema (predefinito)**, **Utente corrente** e **Utente specificato** verranno visualizzate nei menu a discesa corrispondenti. Le impostazioni **Nome utente** e **Password** sono facoltative. Consultare Connetti a LAN come.

Selezionare **Disconnetti dal server dopo l'aggiornamento** per forzare una disconnessione se una connessione al server rimane attiva dopo il download degli aggiornamenti.

Aggiornamento dei componenti di programma

Aggiorna automaticamente i componenti: consente di eseguire l'installazione di nuove funzionalità e degli aggiornamenti di quelle esistenti. Un aggiornamento può essere eseguito automaticamente senza alcun intervento da parte dell'utente oppure è possibile scegliere di ricevere una notifica. Una volta installato l'aggiornamento dei componenti di programma, potrebbe essere necessario riavviare il computer.

Aggiorna componenti ora: installa l'ultima versione dei componenti del programma.

3.8.5.1.6.1 Aggiornamento dal mirror

Per configurare un mirror, che rappresenta essenzialmente un archivio in cui i client possono scaricare i file di aggiornamento, è possibile adottare due metodi di base. La cartella con i file di aggiornamento può essere presentata come cartella di rete condivisa o server HTTP.

Accesso al mirror mediante un server HTTP interno

Si tratta della configurazione predefinita specificata nell'impostazione originale del programma. Per consentire l'accesso al mirror tramite il server HTTP, accedere a **Configurazione avanzata** > **Aggiornamento** > **Mirror** e selezionare **Crea mirror di aggiornamento**.

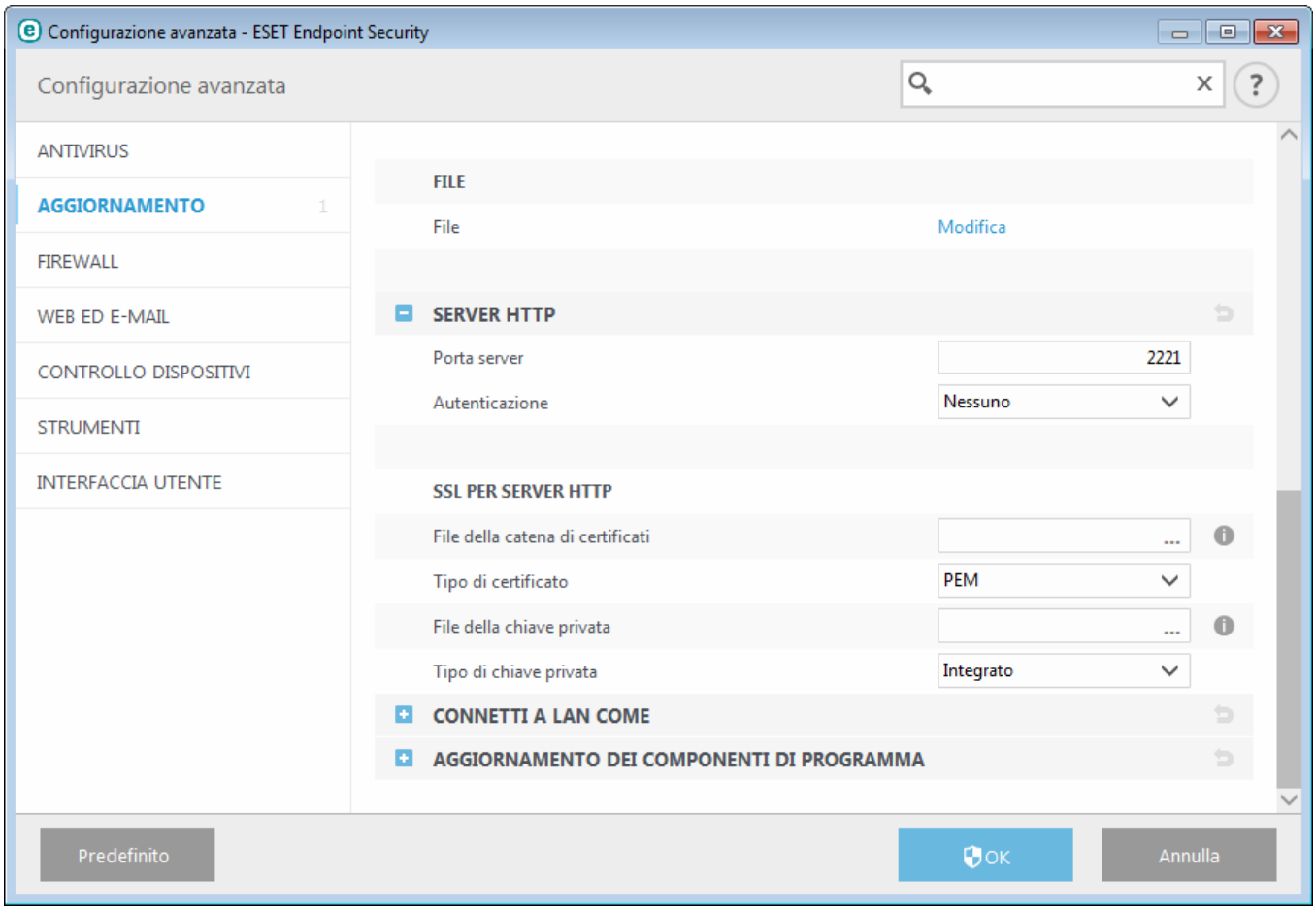
Nella sezione **Server HTTP** della scheda **Mirror**, è possibile specificare la **Porta server** di ascolto del server HTTP oltre al tipo di **Autenticazione** utilizzata dal server HTTP. Per impostazione predefinita, la porta del server è configurata su **2221**. L'opzione **Autenticazione** definisce il metodo di autenticazione utilizzato per l'accesso ai file di aggiornamento. Sono disponibili le seguenti opzioni: **Nessuno**, **Standard** e **NTLM**. Selezionare **Di base** per utilizzare la codifica base64 con l'autenticazione di base di nome utente e password. L'opzione **NTLM** offre una codifica basata sull'utilizzo di un metodo sicuro. Per l'autenticazione, viene utilizzato l'utente creato sulla workstation che condivide i file di aggiornamento. L'impostazione predefinita è **Nessuno**, che garantisce l'accesso ai file di aggiornamento senza che sia necessaria l'autenticazione.

Avviso: 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 Endpoint Security che la crea.

SSL per server HTTP

Se si desidera eseguire il server HTTP con il supporto HTTPS (SSL), è necessario aggiungere il **File della catena di certificato** o generare un certificato autofirmato. Sono disponibili i seguenti tipi di certificati: **PEM, PFX** e **ASN**. Per un livello di protezione aggiuntivo, è possibile utilizzare il protocollo HTTPS per scaricare i file di aggiornamento. Tramite questo protocollo, è quasi impossibile tenere traccia dei trasferimenti di dati e delle credenziali di accesso. L'opzione **Tipo di chiave privata** è impostata su **Integrata** per impostazione predefinita e ciò significa che la chiave privata fa parte del file della catena di certificati selezionato.

NOTA: nel riquadro Aggiornamento del menu principale comparirà l'errore **Nome utente e/o password non validi** dopo vari tentativi non riusciti di aggiornamento del database delle firme antivirali dal mirror. Si consiglia di accedere a **Configurazione avanzata** > **Aggiornamento**> **Mirror** e controllare il nome utente e la password. Il motivo più comune alla base di questo errore consiste in un inserimento errato dei dati di autenticazione.



Dopo aver configurato il server mirror, è necessario aggiungere il nuovo server di aggiornamento sulle workstation client. Per eseguire questa operazione, effettuare i seguenti passaggi:

- Accedere a **Configurazione avanzata** (F5) e fare clic su **Aggiornamento** > **Di base**.
- Disattivare **Scegli automaticamente** e aggiungere un nuovo server nel campo **Server di aggiornamento** utilizzando uno dei seguenti formati:
  http://indirizzo_IP_del_server:2221
  https://indirizzo_IP_del_server_in_uso:2221 (in caso di utilizzo di SSL)

Accesso al mirror tramite le condivisioni di 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 Endpoint Security dalla cartella Mirror.

Configurare quindi l'accesso al mirror nella scheda **Configurazione avanzata** > **Aggiornamento** > **Mirror** disattivando **Fornisci i file di aggiornamento tramite il server HTTP interno**. Questa opzione è attivata per impostazione predefinita nel pacchetto di installazione del programma.

Se la cartella condivisa è posizionata su un altro computer della rete, sarà necessario immettere i dati di autenticazione per l'accesso all'altro computer. Per immettere i dati di autenticazione, aprire **Configurazione avanzata di** ESET Endpoint Security (F5) e fare clic su **Aggiornamento** > **Connetti a LAN come**. Questa è la stessa impostazione utilizzata per l'aggiornamento, come illustrato nella sezione Connetti a LAN come.

Una volta completata la configurazione del mirror, sulle workstation client impostare *UNC**PERCORSO* come server di aggiornamento seguendo la procedura sottostante:

1. Aprire **Configurazione avanzata di ESET Endpoint Security** e fare clic su **Aggiornamento** > **Di base**.
2. Fare clic sul campo **Server di aggiornamento** e aggiungere un nuovo server utilizzando il formato *UNC* *PERCORSO*.

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

L'ultima sezione controlla i componenti di programma (PCU). Per impostazione predefinita, i componenti di programma scaricati vengono preparati per la copia sul mirror locale. Se **Aggiornamento dei componenti di programma** è attivo, non è necessario fare clic su **Aggiorna**, in quanto i file vengono copiati automaticamente sul mirror locale nel momento in cui sono disponibili. Per ulteriori informazioni sugli aggiornamenti dei componenti di programma, consultare Modalità di aggiornamento.

3.8.5.1.6.2 Risoluzione dei problemi di aggiornamento del mirror

Nella maggior parte dei casi, i problemi durante un aggiornamento da un server mirror sono causati da uno o più motivi, tra cui: 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 viene riportata una panoramica dei problemi più frequenti che potrebbero verificarsi durante un aggiornamento eseguito dal mirror:

ESET Endpoint Security riporta un errore di connessione al server mirror: probabilmente causato da una specifica non corretta del server di aggiornamento (percorso di rete alla cartella Mirror) dal quale le workstation locali scaricano gli aggiornamenti. Per verificare la cartella, selezionare il menu **Start** di Windows, fare clic su **Esegui**, immettere il nome della cartella e selezionare **OK**. Dovrebbe essere visualizzato il contenuto della cartella.

ESET Endpoint Security richiede un nome utente e una password: probabilmente causato dall'immissione di dati di autenticazione (nome utente e password) non corretti nella sezione di aggiornamento. Il nome utente e la password sono utilizzati per concedere l'accesso al server di aggiornamento dal quale il programma si aggiornerà. Verificare che i dati di autenticazione siano corretti e immessi nel formato appropriato. Ad esempio, *Dominio/Nome utente* o *Gruppo di lavoro/Nome utente*, oltre alle password corrispondenti. Se il server mirror è accessibile a "Tutti", tenere presente che ciò non significa che l'accesso è concesso a qualsiasi utente. Con "Tutti" non si intendono tutti gli 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 un nome utente di dominio e una password nella sezione di configurazione dell'aggiornamento.

ESET Endpoint Security riporta un errore di connessione al server mirror: la comunicazione sulla porta definita per l'accesso alla versione HTTP del mirror è bloccata.

3.8.5.2 Come fare per creare attività di aggiornamento

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

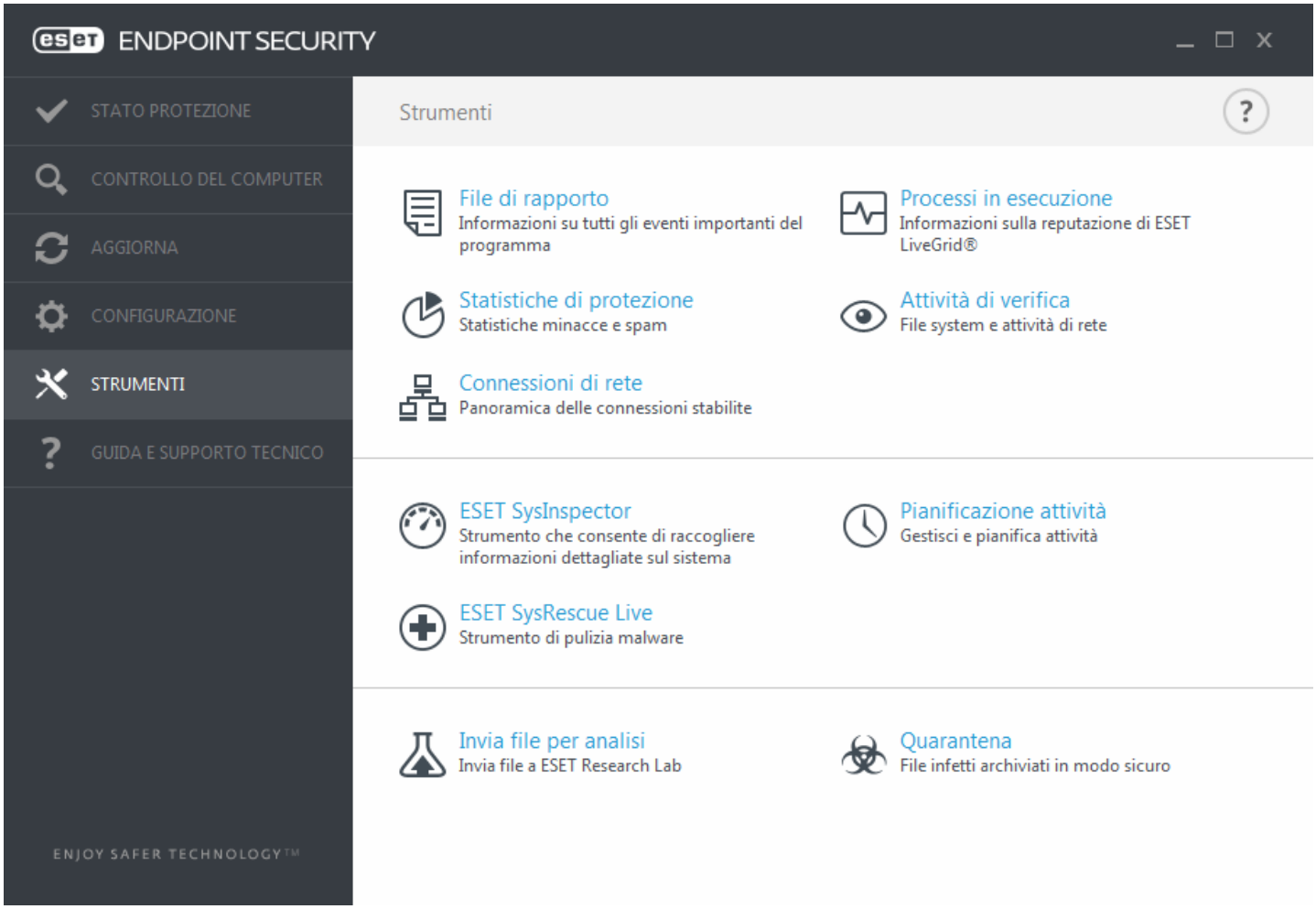
Gli aggiornamenti possono essere eseguiti anche come attività programmate. Per configurare un'attività programmata, fare clic su **Strumenti** > **Pianificazione attività**. Per impostazione predefinita, in ESET Endpoint Security sono attivate le seguenti attività:

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

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

3.8.6 Strumenti

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



Questo menu contiene i seguenti strumenti:

- File di rapporto
- Statistiche di protezione
- Attività di verifica
- Processi in esecuzione (se ESET Live Grid è attivato in ESET Endpoint Security)
- Pianificazione attività
- Quarantena
- Connessioni di rete (se il è attivato in ESET Endpoint Security)
- ESET SysInspector

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

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

3.8.6.1 File di rapporto

I file di rapporto contengono informazioni relative a tutti gli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate. I rapporti rappresentano uno strumento essenziale per l'analisi del sistema, il rilevamento delle minacce e la risoluzione dei problemi. La registrazione viene eseguita attivamente in background, senza che sia richiesto l'intervento da parte dell'utente. Le informazioni vengono registrate in base alle impostazioni del livello di dettaglio di rapporto correnti. È possibile visualizzare i messaggi di testo e i rapporti direttamente dall'ambiente di ESET Endpoint Security, nonché archiviare i file dei rapporti.

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

- **Minacce rilevate**: nel rapporto delle minacce sono contenute informazioni dettagliate sulle infiltrazioni rilevate dai moduli ESET Endpoint Security. Le informazioni includono l'ora del rilevamento, il nome dell'infiltrazione, la posizione, l'azione eseguita e il nome dell'utente registrato nel momento in cui è stata rilevata l'infiltrazione. Fare doppio clic su una voce qualsiasi del rapporto per visualizzarne il contenuto dettagliato in una finestra separata.
- **Eventi**: tutte le azioni importanti eseguite da ESET Endpoint Security vengono registrate nel rapporto eventi. Il rapporto eventi contiene informazioni sugli eventi e sugli errori che si sono verificati nel programma. È stato progettato per aiutare gli amministratori di sistema e gli utenti a risolvere i problemi. Spesso le informazioni visualizzate in questo rapporto consentono di trovare la soluzione a un problema che si verifica nel programma.
- **Controllo del computer**: tutti i risultati del controllo possono essere visualizzati in questa finestra. Ogni riga corrisponde a un singolo controllo del computer. Fare doppio clic su una voce qualsiasi per visualizzare i dettagli del rispettivo controllo.
- **HIPS**: contiene i record di regole specifiche che sono stati contrassegnati per la registrazione. Nel protocollo è possibile visualizzare l'applicazione che ha invocato l'operazione, il risultato (ovvero se la regola era consentita o vietata) e il nome della regola creata.
- **Rapporto del Personal Firewall**: nel rapporto del Personal Firewall sono visualizzati tutti gli attacchi remoti rilevati dal Personal Firewall. In questo rapporto è possibile trovare informazioni su tutti gli attacchi al computer in uso. Nella colonna *Evento* sono elencati gli attacchi rilevati. Nella colonna *Origine* vengono fornite ulteriori informazioni sull'autore dell'attacco. Nella colonna *Protocollo* viene indicato il protocollo di comunicazione usato per l'attacco. L'analisi del rapporto Firewall aiuta a rilevare le infiltrazioni al sistema in tempo utile per impedire l'accesso non autorizzato al sistema. Per ulteriori informazioni su particolari attacchi di rete, vedere Opzioni IDS e avanzate.
- **Siti Web filtrati**: Questo elenco è utile se si desidera visualizzare un elenco di siti Web che sono stati bloccati dalla Protezione accesso Web o dal Controllo Web. In questi rapporti è possibile visualizzare l'ora, l'indirizzo URL, l'utente e l'applicazione che hanno aperto una connessione a un sito Web specifico.
- **Protezione antispam**: contiene record correlati ai messaggi e-mail contrassegnati come spam.
- **Controllo Web**: consente di visualizzare gli indirizzi URL bloccati o consentiti e i dettagli relativi alle modalità di categorizzazione. La colonna *Azione eseguita* contiene informazioni relative alle modalità di applicazione delle regole di filtraggio.
- **Controllo dispositivi**: contiene record relativi ai supporti rimovibili o ai dispositivi collegati al computer. Nel file di rapporto saranno registrati solo i dispositivi con una regola di controllo dispositivi. Se la regola non corrisponde a un dispositivo collegato, non verrà creata alcuna voce di rapporto relativa a tale evento. Qui è possibile visualizzare anche dettagli relativi al tipo di dispositivo, numero di serie, nome del fornitore e dimensioni del supporto (ove disponibili).

In ciascuna sezione, le informazioni visualizzate possono essere copiate negli Appunti (tasto di scelta rapida **Ctrl + C**), selezionando la voce desiderata e facendo clic su **Copia**. Per selezionare più voci, utilizzare i tasti **Ctrl** e **Maiusc**.

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

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

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

3.8.6.1.1 Cerca nel rapporto

Nei rapporti sono memorizzate le informazioni relative a eventi importanti di sistema. La funzione di filtraggio dei rapporti consente di visualizzare i record di un determinato tipo di evento.

Immettere la parola chiave da ricercare nel campo **Trova testo**. Se si desidera ricerca la parola chiave in colonne specifiche, modificare il filtro nel menu a discesa **Cerca nelle colonne**.

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

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

Periodo: indicare l'intervallo di tempo rispetto al quale si desiderano visualizzare i risultati.

Solo parole intere: selezionare questa casella di controllo per ricercare specifiche parole intere e ottenere risultati più precisi.

Maiuscole/minuscole: attivare questa opzione se è importante utilizzare lettere maiuscole o minuscole durante l'applicazione del filtro.

Cerca in alto - I risultati di ricerca che compaiono nella parte superiore del documento verranno visualizzati per primi.

3.8.6.2 Configurazione del server proxy

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

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

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

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

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

Le impostazioni del server proxy possono anche essere definite in Configurazione aggiornamento avanzata (**Configurazione avanzata** > **Aggiornamento** > **Proxy HTTP** selezionando **Connessione tramite un server proxy** dal menu a discesa **Modalità proxy**). Questa impostazione è applicabile al profilo di aggiornamento fornito ed è consigliata per i notebook che ricevono spesso aggiornamenti delle firme antivirali da postazioni remote. Per ulteriori informazioni su questa impostazione, consultare Configurazione aggiornamento avanzata.

3.8.6.3 Pianificazione attività

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

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

La Pianificazione attività consente di pianificare le attività seguenti: aggiornamento del database delle firme antivirali, attività di controllo, controllo dei file di avvio del sistema e manutenzione dei rapporti. È possibile aggiungere o eliminare attività direttamente dalla finestra principale Pianificazione attività (fare clic su **Aggiungi attività** o **Elimina** nella parte inferiore). Fare clic con il pulsante destro del mouse in qualsiasi punto della finestra Pianificazione attività per eseguire le azioni seguenti: visualizzare informazioni dettagliate, eseguire immediatamente l'attività, aggiungere una nuova attività ed eliminare un'attività esistente. Utilizzare le caselle di controllo accanto a ciascuna voce per attivare o disattivare le attività.

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

- **Manutenzione rapporto**
- **Aggiornamento automatico periodico**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**
- **Controllo automatico file di avvio** (dopo l'accesso utente)
- **Controllo automatico file di avvio** (dopo il completamento dell'aggiornamento del database delle firme antivirali)
- **Primo controllo automatico**

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

Aggiunta di un nuova attività

1. Fare clic su **Aggiungi attività** nella parte inferiore della finestra.
2. Inserire il nome dell'attività.

3. Selezionare l'attività desiderata dal menu a discesa:

- **Esegui applicazione esterna**: consente di pianificare l'esecuzione di un'applicazione esterna.
- **Manutenzione rapporto**: file di rapporto contenenti elementi rimasti dai record eliminati. Questa attività ottimizza periodicamente i record nei file di rapporto allo scopo di garantire un funzionamento efficiente.
- **Controllo del file di avvio del sistema**: consente di controllare i file la cui esecuzione è consentita all'avvio del sistema o all'accesso.
- **Crea un controllo computer**: crea uno snapshot ESET SysInspector del computer, raccoglie informazioni dettagliate sui componenti del sistema (ad esempio, driver e applicazioni) e valuta il livello di rischio di ciascun componente.
- **Controllo computer su richiesta**: consente di eseguire un controllo di file e di cartelle sul computer in uso.
- **Primo controllo**: per impostazione predefinita, 20 minuti dopo l'installazione o il riavvio, verrà eseguito un controllo del computer come attività con priorità bassa.
- **Aggiorna**: pianifica un'attività di aggiornamento aggiornando il database delle firme antivirali e i moduli del programma.

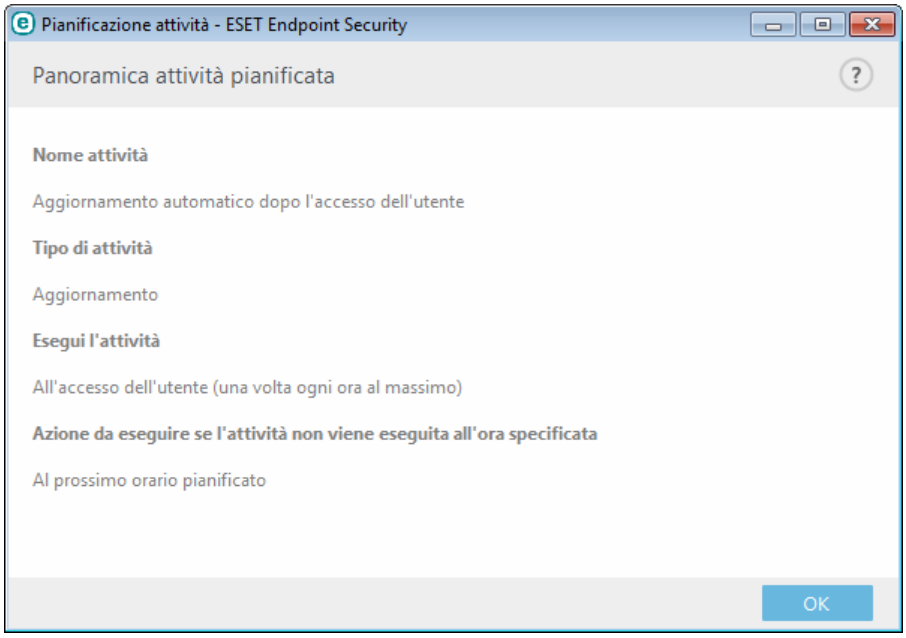
4. Premere il pulsante **Attivata** se si desidera attivare l'attività (è possibile eseguire questa operazione in un secondo momento selezionando/deselezionando la casella di controllo nell'elenco di attività pianificate), fare clic su **Avanti** e selezionare una delle opzioni relative alla frequenza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

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

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

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

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



3.8.6.4 Statistiche di protezione

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

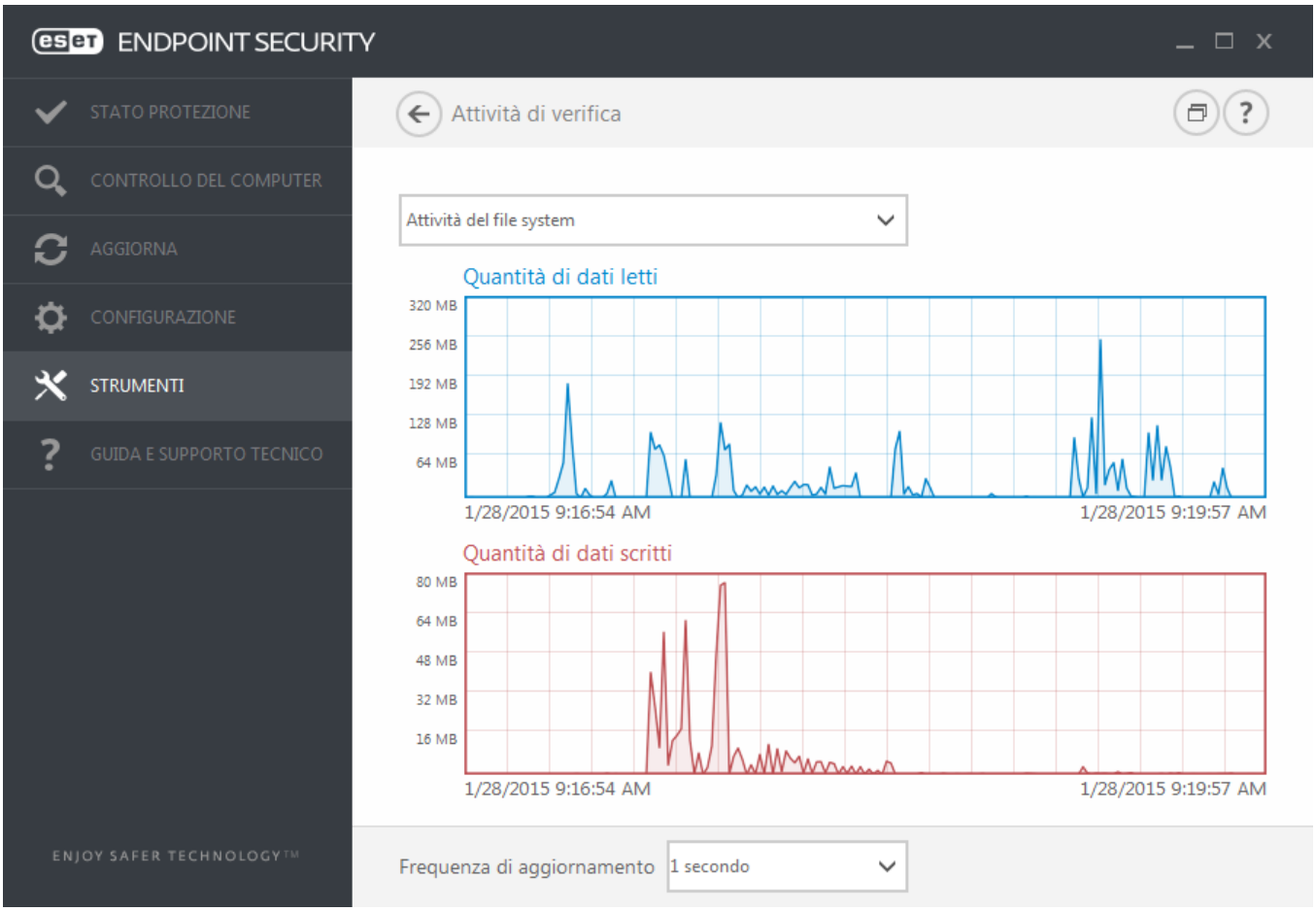
Sono disponibili i seguenti grafici statistici:

- **Protezione antivirus e antispyware** - Consente di visualizzare il numero di oggetti infetti e puliti.
- **Protezione file system** - Consente di visualizzare solo gli oggetti che sono stati scritti o letti sul file system.
- **Protezione client e-mail** - Consente di visualizzare solo gli oggetti inviati o ricevuti dai client e-mail.
- **Protezione accesso Web e Anti-Phishing** - Consente di visualizzare solo gli oggetti scaricati dai browser Web.
- **Protezione antispam client e-mail** - Consente di visualizzare la cronologia delle statistiche antispam dall'ultimo avvio.

Accanto al grafico delle statistiche, è possibile visualizzare il numero degli oggetti sottoposti a controllo, infetti, sottoposti a pulizia e puliti. Fare clic su **Reimposta** per cancellare le informazioni statistiche oppure su **Reimposta tutto** per cancellare e rimuovere tutti i dati esistenti.

3.8.6.5 Attività di verifica

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



Sono disponibili le seguenti opzioni:

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

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

È inoltre possibile selezionare **Attività di rete** dal menu a discesa. La visualizzazione del grafico e le opzioni dell'**Attività di file system** e l'**Attività di rete** sono uguali, tranne per il fatto che in quest'ultima è possibile visualizzare il numero di dati ricevuti (blu) di quelli inviati (rosso).

3.8.6.6 ESET SysInspector

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

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

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

Sono disponibili le azioni seguenti:

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

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

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

3.8.6.7 ESET Live Grid

ESET Live Grid è un sistema avanzato di allarme immediato basato su diverse tecnologie cloud che consente di rilevare minacce emergenti in base alla reputazione e di migliorare le prestazioni del controllo attraverso l'utilizzo di sistemi di whitelist. Le informazioni sulle nuove minacce vengono inserite in flussi in tempo reale indirizzati verso il cloud, che consentono al laboratorio di ricerca di malware ESET di offrire risposte tempestive e un livello di protezione costante. Gli utenti possono controllare la reputazione dei processi in esecuzione e dei file direttamente dall'interfaccia del programma o dal menu contestuale. Ulteriori informazioni sono disponibili su ESET Live Grid. Durante l'installazione di ESET Endpoint Security, selezionare una delle seguenti opzioni:

1. È possibile decidere di non attivare ESET Live Grid. Il software non perderà alcuna funzionalità ma, in alcuni casi, ESET Endpoint Security potrebbe rispondere più lentamente alle nuove minacce rispetto all'aggiornamento del database delle firme antivirali.
2. È possibile configurare ESET Live Grid per l'invio di informazioni anonime sulle nuove minacce e laddove sia stato rilevato il nuovo codice dannoso. Il file può essere inviato a ESET per un'analisi dettagliata. Lo studio di queste minacce sarà d'aiuto a ESET per aggiornare le proprie capacità di rilevamento.

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

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

Il sistema di reputazione ESET Live Grid utilizza metodi di whitelist e blacklist basati sul cloud. Per accedere alle impostazioni di ESET Live Grid, premere **F5** per accedere alla Configurazione avanzata ed espandere **Strumenti** > **ESET Live Grid**.

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

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

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

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

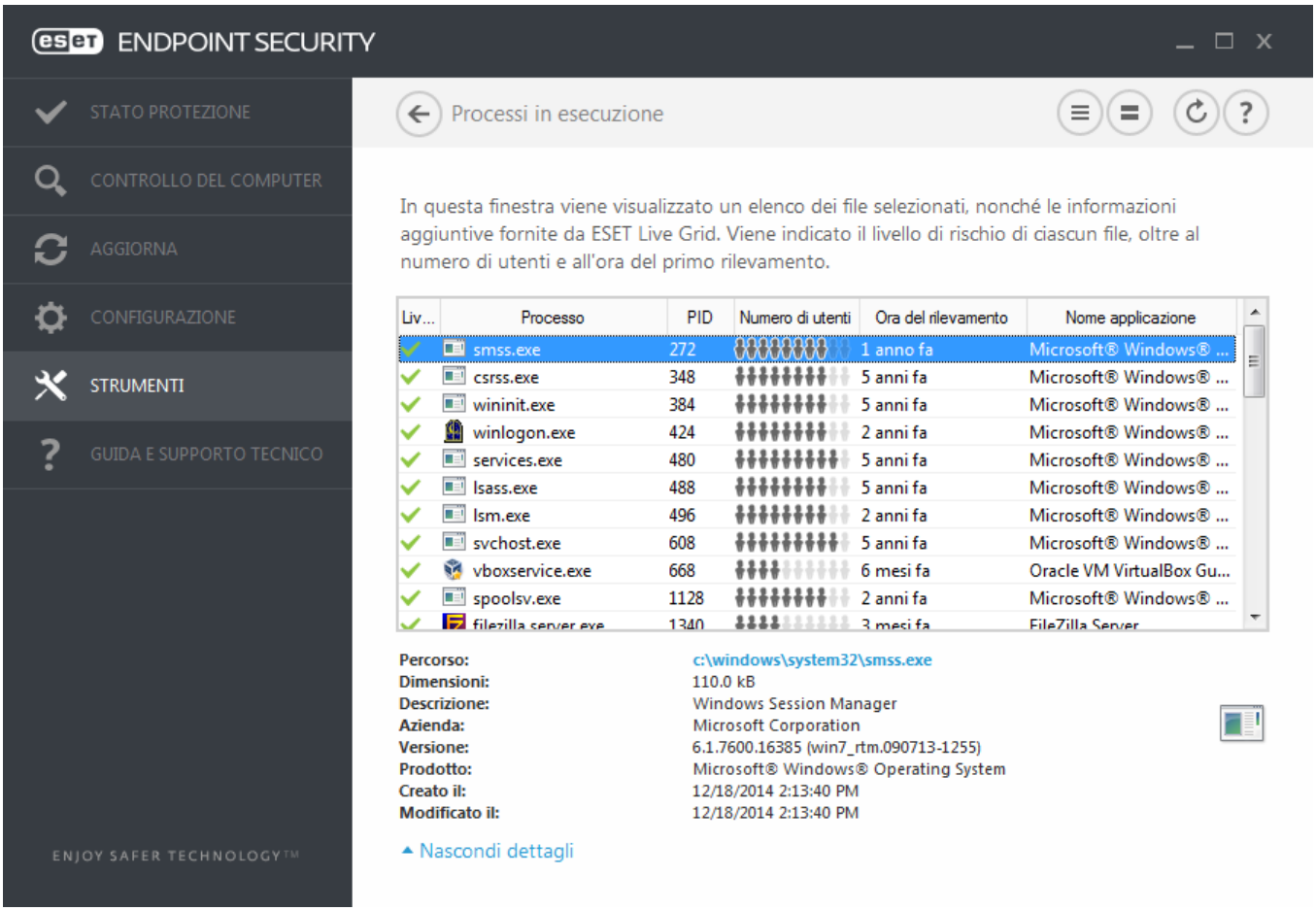
Contatto e-mail (facoltativo): il contatto e-mail può essere incluso insieme ai file sospetti e utilizzato per contattare l'utente qualora fossero richieste ulteriori informazioni ai fini dell'analisi. Tenere presente che non si riceverà alcuna risposta da ESET, a meno che non siano richieste ulteriori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

Esclusione: il filtro Esclusioni consente all'utente di escludere alcuni file o alcune cartelle dall'invio (ad esempio, potrebbe essere utile escludere i file contenenti informazioni riservate, come documenti o fogli di calcolo). I file elencati non verranno mai inviati ai laboratori ESET per l'analisi, anche se contengono codici sospetti. Per impostazione predefinita, vengono esclusi i tipi di file più comuni (.doc, ecc.). Se lo si desidera, è possibile aggiungerli all'elenco di file esclusi.

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

3.8.6.8 Processi in esecuzione

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



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

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

PID: ID di alcuni processi in esecuzione sui sistemi operativi Windows.

NOTA: le applicazioni note contrassegnate come Non a rischio (verde) sono definite pulite (inserite nella whitelist) e saranno escluse dal controllo in modo da aumentare la velocità di esecuzione del controllo del computer su richiesta o della protezione file system in tempo reale sul computer.

Numero di utenti: numero di utenti che utilizzano una determinata applicazione. Queste informazioni vengono raccolte mediante la tecnologia ESET Live Grid.

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

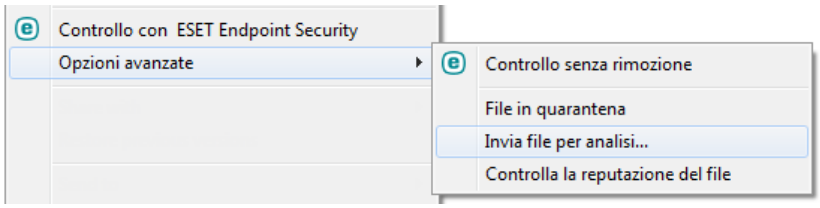
Nota: se un'applicazione è contrassegnata con un livello di rischio Sconosciuto (arancione), non si tratta necessariamente di software dannoso. In genere si tratta di una nuova applicazione. In caso di dubbi sul file, utilizzare la funzione invia file per analisi per inviare il file al laboratorio antivirus ESET. Se il file si rivela essere un'applicazione dannosa, il suo rilevamento verrà aggiunto a uno degli aggiornamenti successivi del database delle firme antivirali.

Nome applicazione - Nome specifico di un programma o processo.

Fare clic sulla parte inferiore di una determinata applicazione per visualizzare le seguenti informazioni nella parte inferiore della finestra:

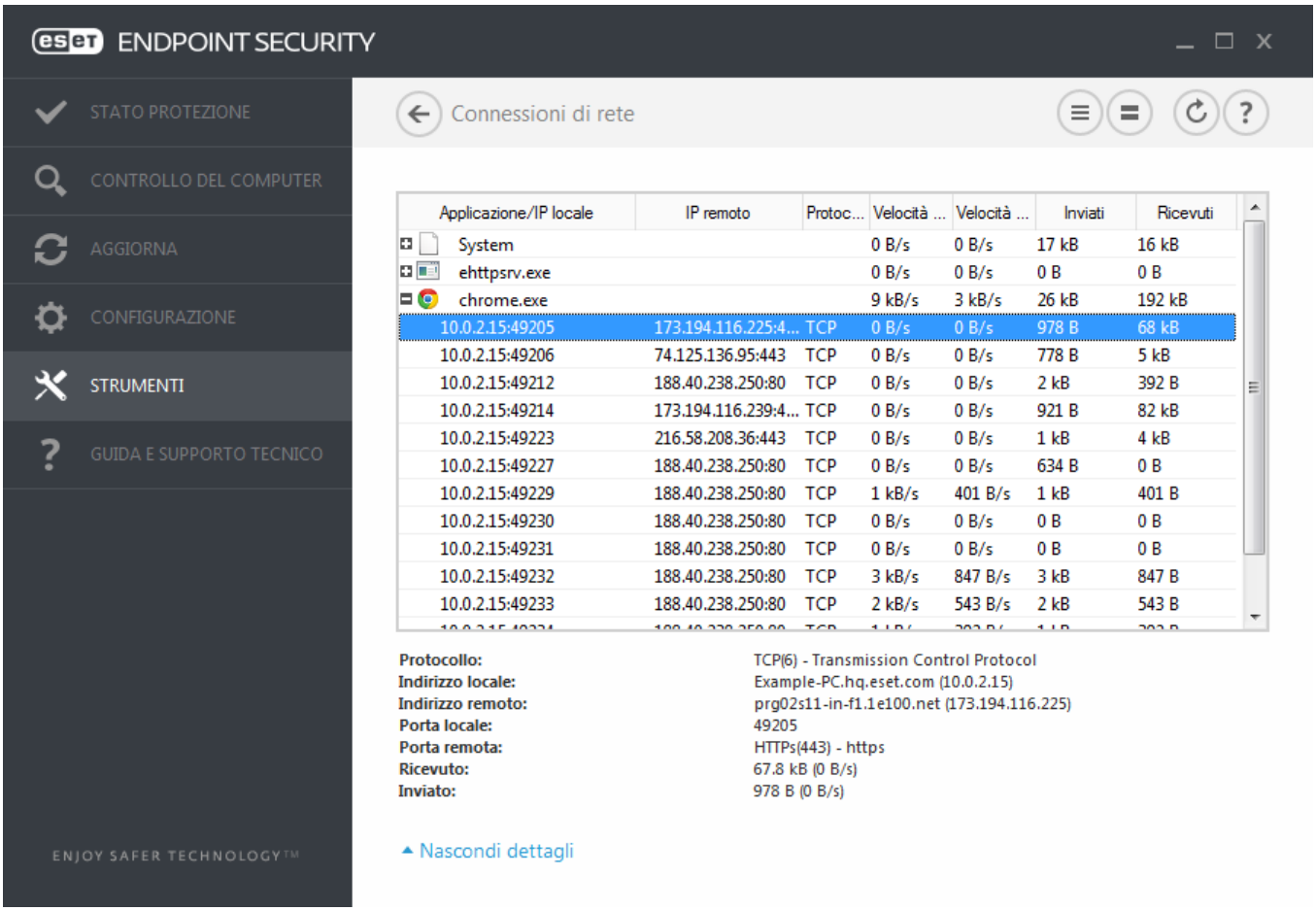
- **Percorso**: posizione di un'applicazione sul computer.
- **Dimensione**: dimensione del file in KB (kilobyte) o MB (megabyte).
- **Descrizione**: caratteristiche del file basate sulla descrizione ottenuta dal sistema operativo.
- **Società**: nome del fornitore o del processo applicativo.
- **Versione**: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

NOTA: la reputazione può essere controllata anche sui file che non agiscono come programmi/processi in esecuzione: contrassegnare i file che si desidera controllare, fare clic con il pulsante destro del mouse su di essi e nel menu contestuale selezionare **Opzioni avanzate** > **Controlla la reputazione del file tramite ESET Live Grid**.



3.8.6.9 Connessioni di rete

Nella sezione Connessioni di rete è possibile visualizzare l'elenco delle connessioni attive e in attesa. In questo modo, è possibile controllare tutte le applicazioni che stabiliscono connessioni in uscita.



Sulla prima riga viene visualizzato il nome dell'applicazione e la relativa velocità di trasferimento dati. Per visualizzare l'elenco delle connessioni effettuate dall'applicazione (e per maggiori informazioni), fare clic su **+**.

Colonne

Applicazione/IP locale - Nome dell'applicazione, indirizzi IP e porte di comunicazione locali.

IP remoto - Indirizzo IP e numero di porta di un determinato computer remoto.

Protocollo - Protocollo di trasferimento utilizzato.

Velocità massima/Velocità minima - Velocità corrente dei dati in uscita e in entrata.

Inviati/Ricevuti - Quantità di dati scambiati durante la connessione.

Mostra dettagli - Scegliere questa opzione per visualizzare informazioni dettagliate sulla connessione selezionata.

Selezionare un'applicazione o un indirizzo IP nella schermata Connessioni di rete e fare clic con il pulsante destro del mouse per visualizzare il menu contestuale con la seguente struttura:

Risolvi nomi host - Se possibile, tutti gli indirizzi di rete sono visualizzati in formato DNS e non in formato indirizzo IP numerico.

Mostra solo connessioni TCP - Nell'elenco vengono visualizzate esclusivamente le connessioni che appartengono al protocollo TCP.

Visualizza connessioni in ascolto- Selezionare questa opzione per visualizzare esclusivamente le connessioni in cui non è attualmente stabilita alcuna comunicazione ma per cui il sistema ha aperto una porta ed è in attesa di una connessione.

Visualizza connessioni all'interno del computer - Selezionare questa opzione per visualizzare esclusivamente le connessioni in cui il lato remoto è costituito da un sistema locale, ovvero le cosiddette connessioni *localhost*.

Fare clic con il pulsante destro del mouse per visualizzare le opzioni aggiuntive che includono:

Nega comunicazione per la connessione - Interrompe la comunicazione stabilita. Questa opzione è disponibile solo dopo aver selezionato una connessione attiva.

Aggiorna velocità - Scegliere la frequenza di aggiornamento delle connessioni attive.

Aggiorna ora - Carica nuovamente la finestra Connessioni di rete.

Le seguenti opzioni sono disponibili solo dopo aver selezionato un'applicazione o un processo e non una connessione attiva:

Nega temporaneamente comunicazione per il processo - Rifiuta le connessioni correnti dell'applicazione specificata. Se viene stabilita una nuova connessione, il firewall utilizzerà una regola predefinita. Per una descrizione delle impostazioni, consultare la sezione Regole e aree.

Consenti temporaneamente comunicazione per il processo - Consente le connessioni correnti dell'applicazione specificata. Se viene stabilita una nuova connessione, il firewall utilizzerà una regola predefinita. Per una descrizione delle impostazioni, consultare la sezione Regole e aree.

3.8.6.10 Invio di campioni per l'analisi

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

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

NOTA: prima di inviare un campione a ESET, assicurarsi che soddisfi uno o più dei criteri seguenti:
- il file o il sito Web non viene rilevato
- il file o il sito Web viene erroneamente rilevato come minaccia

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

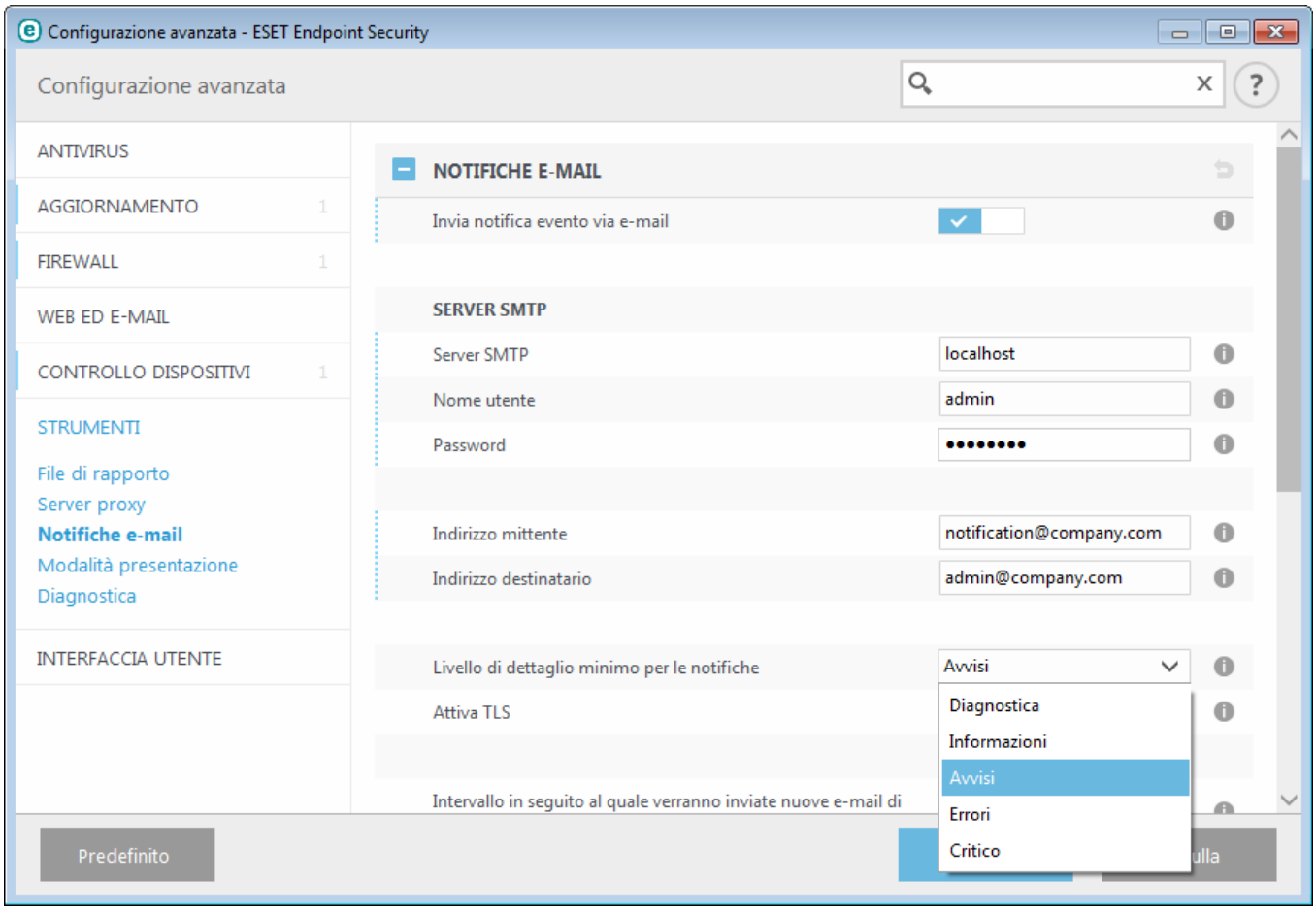
Selezionare la descrizione dal menu a discesa **Motivo per l'invio del campione** che si avvicina maggiormente alla propria motivazione:
- **File sospetto**
- **Sito sospetto** (un sito Web infettato da un malware),
- **File falso positivo** (file che è stato rilevato come un'infezione ma che in realtà non è infetto),
- **Sito falso positivo**
- **Altro**

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

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

3.8.6.11 Notifiche e-mail

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



Server SMTP

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

NOTA: ESET Endpoint Security supporta i server SMTP con crittografia TLS.

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

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

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

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

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

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

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

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

Formato del messaggio

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

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

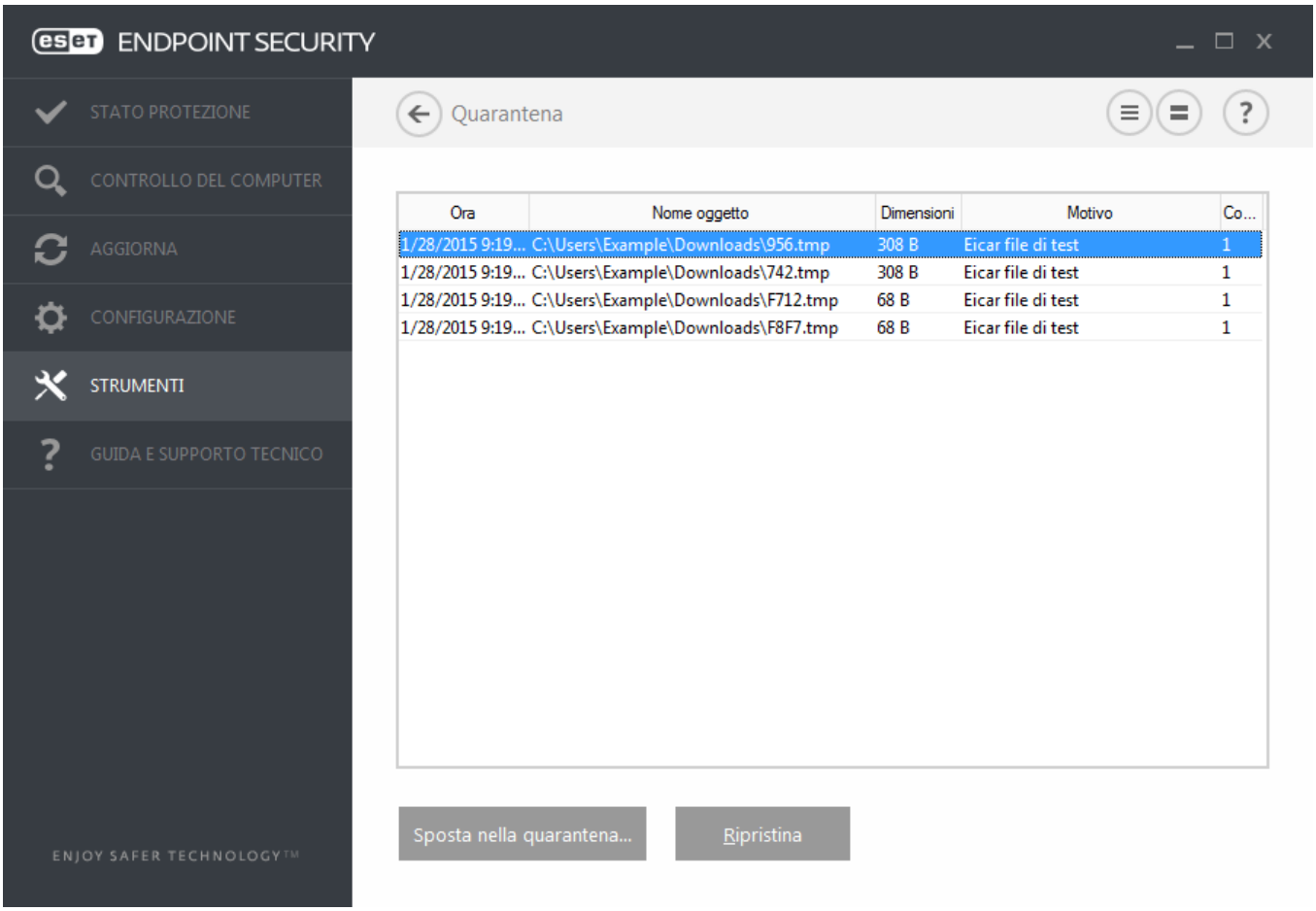
Utilizza caratteri alfabetici locali - Converte un messaggio e-mail nella codifica dei caratteri ANSI in base alle impostazioni della lingua di Windows (ad esempio, windows-1250). Se si lascia deselezionata questa opzione, il messaggio verrà convertito e codificato in ACSII a 7 bit (ad esempio, "á" verrà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

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

3.8.6.12 Quarantena

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

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



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

Mettere file in quarantena

ESET Endpoint Security mette automaticamente in quarantena i file eliminati (qualora l'utente non abbia provveduto a disattivare questa opzione nella finestra di avviso). Se lo si desidera, è possibile mettere manualmente in quarantena i file sospetti facendo clic su **Quarantena**. Il file originale verrà rimosso dalla posizione di origine. Per questa operazione è possibile utilizzare anche il menu contestuale: fare clic con il pulsante destro del mouse sulla finestra **Quarantena** e selezionare **Quarantena**.

Ripristino dalla quarantena

È possibile ripristinare nella posizione di origine i file messi in quarantena. Per ripristinare un file messo in quarantena, fare clic con il pulsante destro del mouse nella finestra Quarantena e selezionare **Ripristina** dal menu contestuale. Se un file è contrassegnato come applicazione potenzialmente indesiderata, sarà disponibile anche l'opzione **Ripristina ed escludi dal controllo**. Il menu contestuale contiene anche l'opzione **Ripristina in...**, che consente di ripristinare un file in una posizione diversa da quella di origine da cui è stato eliminato.

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

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

Invio di un file dalla cartella Quarantena

Se un file sospetto che non è stato rilevato dal programma è stato messo in quarantena o se un file è stato rilevato erroneamente come minaccia e successivamente messo in quarantena, inviarlo ai laboratori antivirus ESET. Per inviare un file dalla cartella Quarantena, fare clic con il pulsante destro del mouse su di esso e selezionare **Invia per analisi** dal menu contestuale.

3.8.6.13 Aggiornamento Microsoft Windows

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

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

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

3.8.7 Interfaccia utente

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

Tramite lo strumento Elementi dell'interfaccia utente, è possibile regolare l'aspetto e gli effetti del programma.

Per offrire un livello massimo di protezione, è possibile impedire eventuali modifiche non autorizzate del software mediante l'utilizzo dello strumento Configurazione dell'accesso.

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

Se si sceglie di non visualizzare alcune notifiche, queste verranno visualizzate in **Elementi dell'interfaccia utente** > **Stati applicazione**. Qui è possibile controllarne lo stato oppure impedire la visualizzazione delle notifiche.

L'Integrazione menu contestuale verrà visualizzata facendo clic con il pulsante destro del mouse sull'oggetto selezionato. Utilizzare questo strumento per integrare gli elementi di controllo di ESET Endpoint Security nel menu contestuale.

La Modalità presentazione è utile per gli utenti che desiderano utilizzare un'applicazione senza essere interrotti dalle finestre popup, dalle attività pianificate e da qualsiasi componente che potrebbe sovraccaricare il processore e la RAM.

3.8.7.1 Elementi dell'interfaccia utente

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

Nella sezione **Elementi dell'interfaccia utente**, è possibile regolare l'ambiente di lavoro. Utilizzare il menu a discesa **Modalità di avvio GUI** per selezionare una delle seguenti modalità di avvio dell'interfaccia utente grafica (GUI):

Completa: verrà visualizzata l'interfaccia grafica utente completa.

Minima: la GUI è disponibile, ma l'utente può visualizzare solo le notifiche.

Manuale: non verranno visualizzati avvisi o notifiche.

Silenziosa: non verranno visualizzati né la GUI né avvisi e notifiche. Questa modalità si rivela utile in situazioni in cui è necessario preservare le risorse di sistema. La modalità silenziosa può essere avviata dall'amministratore.

NOTA: dopo aver selezionato la modalità di avvio silenziosa della GUI e riavviato il computer, verranno visualizzate le notifiche e non l'interfaccia grafica. Per ritornare alla modalità interfaccia utente grafica intera, eseguire la GUI dal menu Start sotto a **Tutti i programmi** > **ESET** > ESET Endpoint Security come amministratore oppure attraverso ESET Remote Administrator utilizzando un criterio.

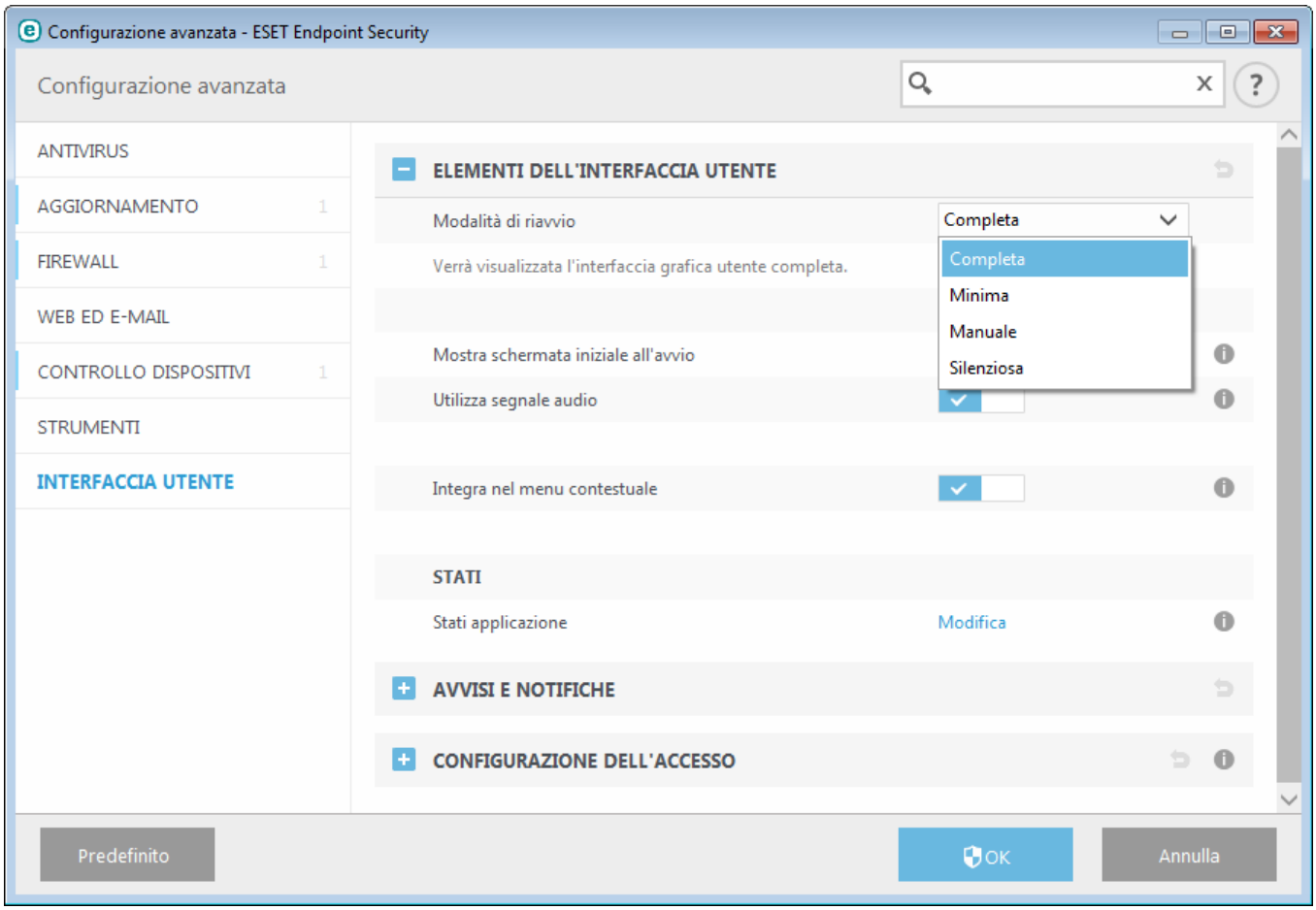
Se si desidera disattivare la schermata iniziale di ESET Endpoint Security, deselezionare **Mostra schermata iniziale all'avvio**.

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

Integra nel menu contestuale: integra gli elementi di controllo di ESET Endpoint Security nel menu contestuale.

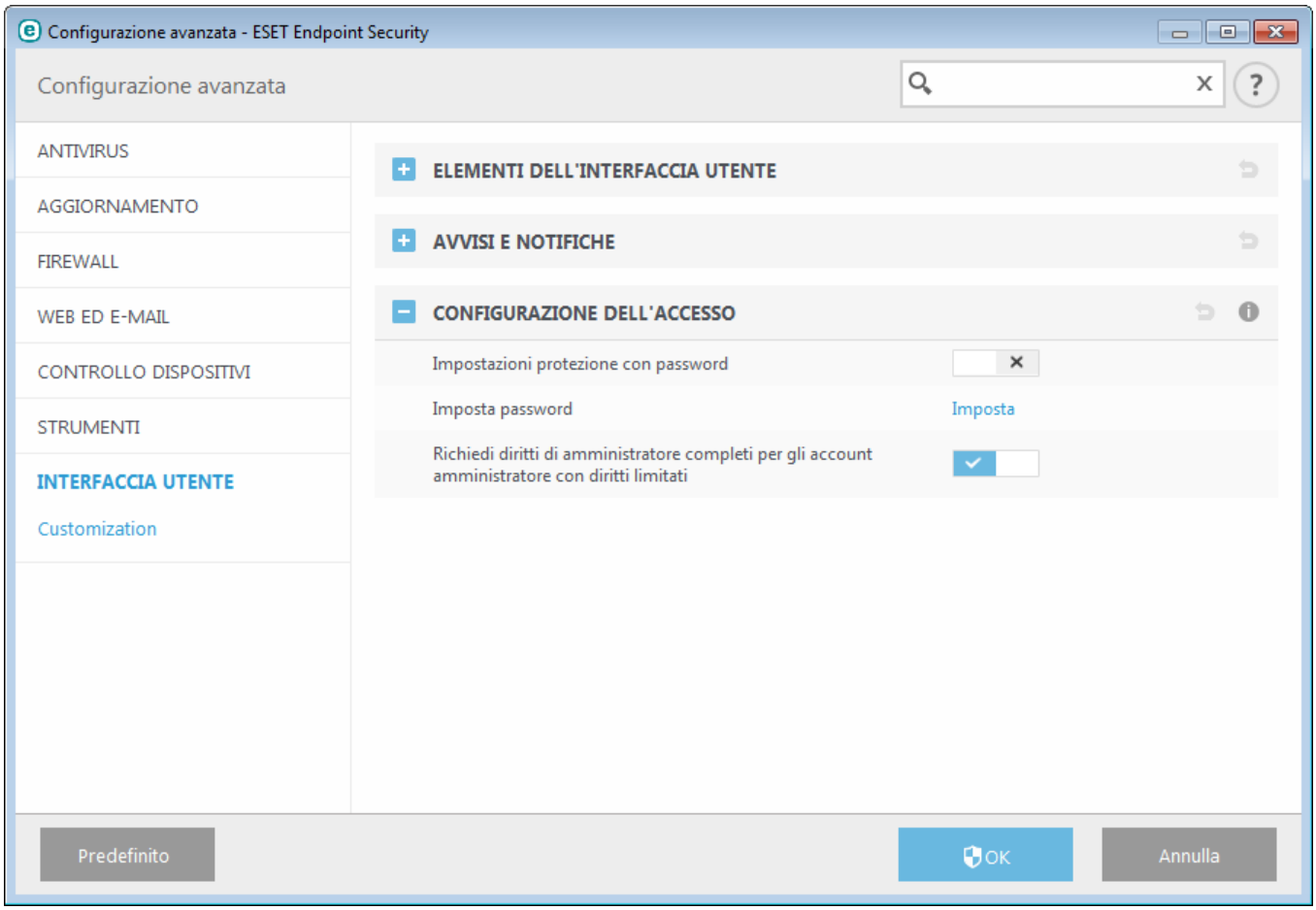
Stati

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


Configurazione avanzata - ESET Endpoint Security
Configurazione avanzata
ANTIVIRUS
AGGIORNAMENTO 1
FIREWALL 1
WEB ED E-MAIL
CONTROLLO DISPOSITIVI 1
STRUMENTI
INTERFACCIA UTENTE
ELEMENTI DELL'INTERFACCIA UTENTE
Modalità di riavvio
Completa
Verrà visualizzata l'interfaccia grafica utente completa.
Completa
Minima
Manuale
Silenziosa
Mostra schermata iniziale all'avvio
Utilizza segnale audio
Integra nel menu contestuale
STATI
Stati applicazione
Modifica
AVVISI E NOTIFICHE
CONFIGURAZIONE DELL'ACCESSO
Predefinito
OK
Annulla

3.8.7.2 Configurazione dell'accesso

Per garantire un livello di protezione massimo del sistema, è fondamentale che ESET Endpoint Security sia configurato correttamente. Qualsiasi modifica non appropriata potrebbe causare la perdita di dati importanti. Per evitare modifiche non autorizzate, i parametri di configurazione di ESET Endpoint Security possono essere protetti con password. Le impostazioni di configurazione per la protezione con password sono disponibili in **Configurazione avanzata** (F5) sotto a **Configurazione dell'accesso** > **Interfaccia utente**.



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

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

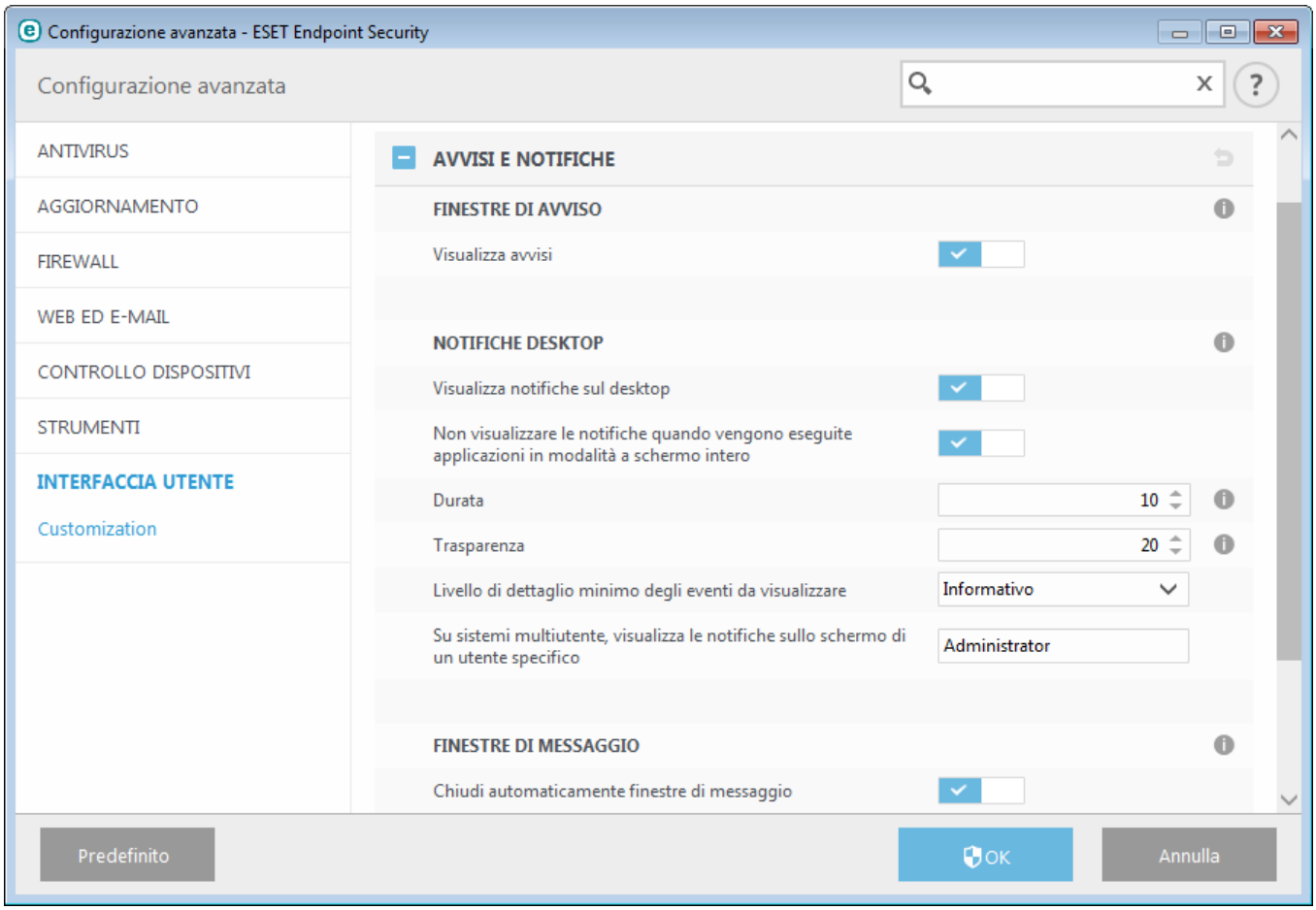
Richiedi diritti di amministratore completi per gli account con diritti limitati - Lasciare attiva questa opzione per richiedere all'utente corrente (nel caso in cui non disponga di diritti di amministratore) di inserire il nome utente e la password dell'amministratore per la modifica di alcuni parametri del sistema (analogo a Controllo dell'account utente o UAC in Windows Vista). Tali modifiche includono la disattivazione dei moduli di protezione o del firewall.

Solo per Windows XP:

Richiedi diritti di amministratore (sistema senza supporto Controllo dell'account utente) - Attivare questa opzione per ottenere il prompt di ESET Endpoint Security relativo alle credenziali dell'amministratore.

3.8.7.3 Avvisi e notifiche

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



Finestre di avviso

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

Messaggistica interna al prodotto

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

Notifiche desktop

Le notifiche visualizzate sul desktop e i suggerimenti sono forniti esclusivamente a titolo informativo e non richiedono l'interazione dell'utente. Vengono visualizzate nell'area di notifica posta nell'angolo in basso a destra della schermata. Per attivare la visualizzazione delle notifiche sul desktop, selezionare **Visualizza notifiche sul desktop**. Attivare il pulsante **Non visualizzare le notifiche quando vengono eseguite applicazioni in modalità a schermo intero** per eliminare tutte le notifiche non interattive. È possibile modificare opzioni più dettagliate, ad esempio l'orario di visualizzazione della notifica e la trasparenza della finestra seguendo le istruzioni fornite di seguito.

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

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

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

Finestre di messaggio

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

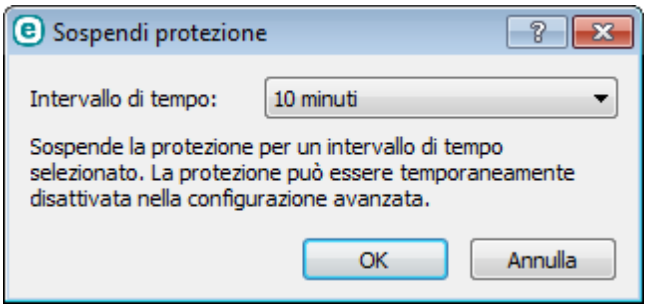
Messaggi di conferma: consente all'utente di visualizzare un elenco di messaggi di conferma che è possibile decidere di visualizzare o non visualizzare.

3.8.7.4 Icona della barra delle applicazioni

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

Blocca rete: il rapporto del Personal Firewall personale bloccherà tutto il traffico Internet e di rete in uscita/in entrata.

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



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

Interrompi firewall (consenti tutto il traffico): imposta il firewall su uno stato inattivo. Per ulteriori informazioni, consultare il paragrafo Rete.

Blocca tutto il traffico di rete: blocca tutto il traffico di rete. È possibile riattivarlo facendo clic su **Smetti di bloccare tutto il traffico di rete**.

Configurazione avanzata: selezionare questa opzione per accedere alla struttura **Configurazione avanzata**. È inoltre possibile accedere alla configurazione avanzata premendo il tasto F5 oppure accedendo a **Configurazione** > **Configurazione avanzata**.

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

Nascondi ESET Endpoint Security: nasconde la finestra di ESET Endpoint Security dalla schermata.

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

Aggiornamento database firme antivirali: avvia l'aggiornamento del database delle firme antivirali per garantire il livello di protezione stabilito dall'utente contro codici dannosi.

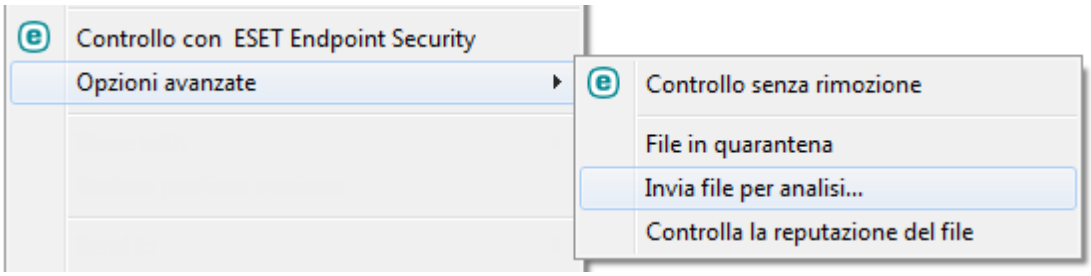
Informazioni su: fornisce informazioni sul sistema, dettagli sulla versione installata di ESET Endpoint Security e sui relativi moduli dei programmi installati, nonché la data di scadenza della licenza. Le informazioni sul sistema operativo e le risorse di sistema sono disponibili in fondo alla pagina.

3.8.7.5 Menu contestuale

Il menu contestuale viene visualizzato facendo clic con il pulsante destro del mouse su un oggetto (file). Nel menu sono elencate tutte le azioni che è possibile eseguire su un oggetto.

Nel menu contestuale è possibile integrare gli elementi del controllo di ESET Endpoint Security. Le opzioni di configurazione per questa funzionalità sono disponibili nella struttura Configurazione avanzata sotto a **Interfaccia utente** > **Elementi dell'interfaccia utente**.

Integra nel menu contestuale: integra gli elementi di controllo di ESET Endpoint Security nel menu contestuale.



3.9 Utente avanzato

3.9.1 Gestione profili

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

Controllo del computer su richiesta

È possibile salvare i parametri di controllo preferiti per i controlli futuri. È consigliabile creare un profilo di controllo differente (con diverse destinazioni di controllo, metodi di controllo e altri parametri) per ciascun controllo utilizzato abitualmente.

Per creare un nuovo profilo, aprire la finestra Configurazione avanzata (F5) e fare clic su **Antivirus** > **Controllo computer su richiesta** , quindi su **Modifica** accanto a **Elenco di profili**. Nel menu a discesa del **Profilo selezionato** sono elencati i profili di controllo esistenti. Per ricevere assistenza durante la creazione di un profilo di controllo adatto alle proprie esigenze, consultare la sezione Configurazione parametri motore ThreatSense contenente una descrizione di ciascun parametro di configurazione del controllo.

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

Aggiornamento

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

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

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

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

3.9.2 Diagnostica

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

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

Attiva registrazione avanzata filtraggio protocolli: registra tutti i dati che attraversano il motore di filtraggio

protocolli in formato PCAP. Tale operazione consente agli sviluppatori di diagnosticare e risolvere problemi correlati al filtraggio protocolli.

I file di rapporto sono disponibili in:
C:\Programmi\ESET\ESET Smart Security\Diagnostica su Windows Vista e versioni successive o *C:\Documents and Settings\All Users\...* sulle versioni precedenti di Windows.

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

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

3.9.3 Importa ed esporta impostazioni

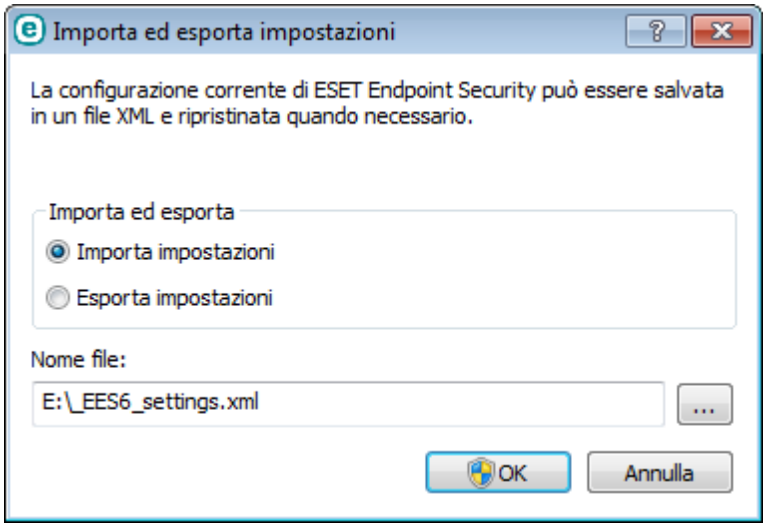
È possibile importare o esportare il file di configurazione personalizzato in formato .xml di ESET Endpoint Security dal menu **Configurazione**.

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

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

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

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



3.9.4 Riga di comando

Il modulo antivirus di ESET Endpoint Security può essere avviato dalla riga di comando, manualmente con il comando "ecls" oppure con un file batch ("bat"). Utilizzo dello scanner della riga di comando ESET:

```
ecls [OPTIONS..] FILES..
```

È possibile utilizzare i parametri e le opzioni riportati di seguito quando viene eseguita una scansione su richiesta dalla riga di comando:

Opzioni

/base-dir=FOLDER	carica moduli da CARTELLA
/quar-dir=FOLDER	CARTELLA di quarantena

/exclude=MASK	escludi dalla scansione i file corrispondenti a MASCHERA
/subdir	esegui controllo delle sottocartelle (impostazione predefinita)
/no-subdir	non eseguire controllo delle sottocartelle
/max-subdir-level=LEVEL	sottolivello massimo delle cartelle all'interno di cartelle su cui eseguire la scansione
/symlink	segui i collegamenti simbolici (impostazione predefinita)
/no-symlink	ignora collegamenti simbolici
/ads	esegui la scansione di ADS (impostazione predefinita)
/no-ads	non eseguire la scansione di ADS
/log-file=FILE	registra output nel FILE
/log-rewrite	sovrascrivi il file di output (impostazione predefinita: aggiungi)
/log-console	registra l'output nella console (impostazione predefinita)
/no-log-console	non registrare l'output nella console
/log-all	registra anche file puliti
/no-log-all	non registrare file puliti (impostazione predefinita)
/aind	mostra indicatore di attività
/auto	controlla e disinfetta automaticamente tutti i dischi locali

Opzioni scanner

/files	esegui controllo dei file (impostazione predefinita)
/no-files	non eseguire controllo dei file
/memory	esegui scansione della memoria
/boots	esegui la scansione dei settori di avvio
/no-boots	non eseguire la scansione dei settori di avvio (impostazione predefinita)
/arch	esegui controllo degli archivi (impostazione predefinita)
/no-arch	non eseguire controllo degli archivi
/max-obj-size=SIZE	esegui solo la scansione dei file inferiori a DIMENSIONE megabyte (impostazione predefinita 0 = illimitato)
/max-arch-level=LEVEL	sottolivello massimo degli archivi all'interno di archivi (archivi nidificati) su cui eseguire la scansione
/scan-timeout=LIMIT	esegui scansione degli archivi per LIMITE secondi al massimo
/max-arch-size=SIZE	esegui la scansione dei file di un archivio solo se inferiori a DIMENSIONE (impostazione predefinita 0 = illimitato)
/max-sfx-size=SIZE	esegui la scansione dei file di un archivio autoestraente solo se inferiori a DIMENSIONE megabyte (impostazione predefinita 0 = illimitato)
/mail	esegui la scansione dei file di e-mail (impostazione predefinita)
/no-mail	non eseguire controllo dei file di e-mail
/mailbox	esegui la scansione delle caselle di posta (impostazione predefinita)
/no-mailbox	non eseguire la scansione delle caselle di posta
/sfx	esegui la scansione degli archivi autoestraenti (impostazione predefinita)
/no-sfx	non eseguire controllo degli archivi autoestraenti
/rtp	esegui la scansione degli eseguibili compressi (impostazione predefinita)
/no-rtp	non eseguire la scansione degli eseguibili compressi
/unsafe	esegui la scansione delle applicazioni potenzialmente pericolose
/no-unsafe	non eseguire la scansione delle applicazioni potenzialmente pericolose (impostazione predefinita)
/unwanted	esegui la scansione delle applicazioni potenzialmente indesiderate
/no-unwanted	non eseguire la scansione delle applicazioni potenzialmente indesiderate (impostazione predefinita)
/suspicious	ricerca di applicazioni sospette (impostazione predefinita)
/no-suspicious	non ricercare applicazioni sospette
/pattern	utilizza le firme digitali (impostazione predefinita)
/no-pattern	non utilizzare le firme digitali
/heur	attiva l'euristica (impostazione predefinita)
/no-heur	disattiva l'euristica
/adv-heur	attiva l'euristica avanzata (impostazione predefinita)
/no-adv-heur	disattiva l'euristica avanzata
/ext=EXTENSIONS	esegui scansione solo di ESTENSIONI delimitate da due punti
/ext-exclude=EXTENSIONS	escludi dal controllo le ESTENSIONI delimitate da due punti

/clean-mode=MODE	utilizza la MODALITÀ pulizia per gli oggetti infetti Sono disponibili le seguenti opzioni: • nessuna - non verrà eseguita alcuna pulizia automatica. • standard (impostazione predefinita) - ecls.exe tenterà di eseguire la pulizia o l'eliminazione automatica di file infetti. • massima - ecls.exe tenterà di eseguire la pulizia o l'eliminazione automatica di file infetti senza l'intervento dell'utente (all'utente non verrà richiesto di confermare l'eliminazione dei file). • rigorosa - ecls.exe eliminerà i file senza tentare di effettuarne la pulizia e indipendentemente dalla loro tipologia. • eliminazione - ecls.exe eliminerà i file senza tentare di effettuarne la pulizia, ma eviterà di eliminare file sensibili come quelli del sistema Windows.
/quarantena	copiare i file infettati (se puliti) in Quarantena (integra l'azione eseguita durante la pulizia)
/no-quarantena	non copiare file infettati in Quarantena

Opzioni generali

/help	mostra guida ed esci
/version	mostra informazioni sulla versione ed esci
/preserve-time	mantieni indicatore data e ora dell'ultimo accesso

Codici di uscita

0	nessuna minaccia rilevata
1	minaccia rilevata e pulita
10	impossibile controllare alcuni file (potrebbero essere minacce)
50	trovata minaccia
100	errore

NOTA: i codici di uscita superiori a 100 indicano che non è stata eseguita la scansione del file, il quale potrebbe quindi essere infetto.

3.9.5 Rilevamento stato di inattività

Le impostazioni del rilevamento stato inattivo possono essere configurate in **Configurazione avanzata** sotto a **Antivirus** > **Controllo stato inattivo** > **Rilevamento stato inattivo**. Queste impostazioni specificano l'attivazione del Controllo stato inattivo se:

- è attivo lo screen saver,
- il computer è bloccato,
- un utente si disconnette.

Utilizzare i pulsanti di ciascuno stato per attivare o disattivare i vari metodi di attivazione del rilevamento dello stato di inattività.

3.9.6 ESET SysInspector

3.9.6.1 Introduzione a ESET SysInspector

L'applicazione ESET SysInspector ispeziona il computer in modo approfondito e visualizza i dati raccolti in modo globale. La raccolta di informazioni su driver e applicazioni, su connessioni di rete o importanti voci di registro semplifica il controllo di comportamenti sospetti del sistema, siano essi dovuti a incompatibilità software o hardware o infezioni malware.

È possibile accedere a ESET SysInspector in due modi: dalla versione integrata nelle soluzioni ESET Security o scaricando gratuitamente la versione indipendente (SysInspector.exe) dal sito Web ESET. Le funzionalità e i comandi di entrambe le versioni sono identici. L'unica differenza consiste nella gestione dei risultati. La versione indipendente e quella integrata consentono entrambe di esportare snapshot del sistema su un file *XML* e salvarli su disco. La versione integrata consente tuttavia anche di memorizzare gli snapshot di sistema direttamente in **Strumenti** > **ESET SysInspector** (tranne ESET Remote Administrator). Per ulteriori informazioni, vedere la sezione ESET SysInspector come componente di ESET Endpoint Security.

È necessario attendere qualche minuto per consentire a ESET SysInspector di controllare il computer. A seconda della configurazione hardware, del sistema operativo e del numero di applicazioni installate nel computer in uso, questa operazione potrebbe richiedere da 10 secondi ad alcuni minuti.

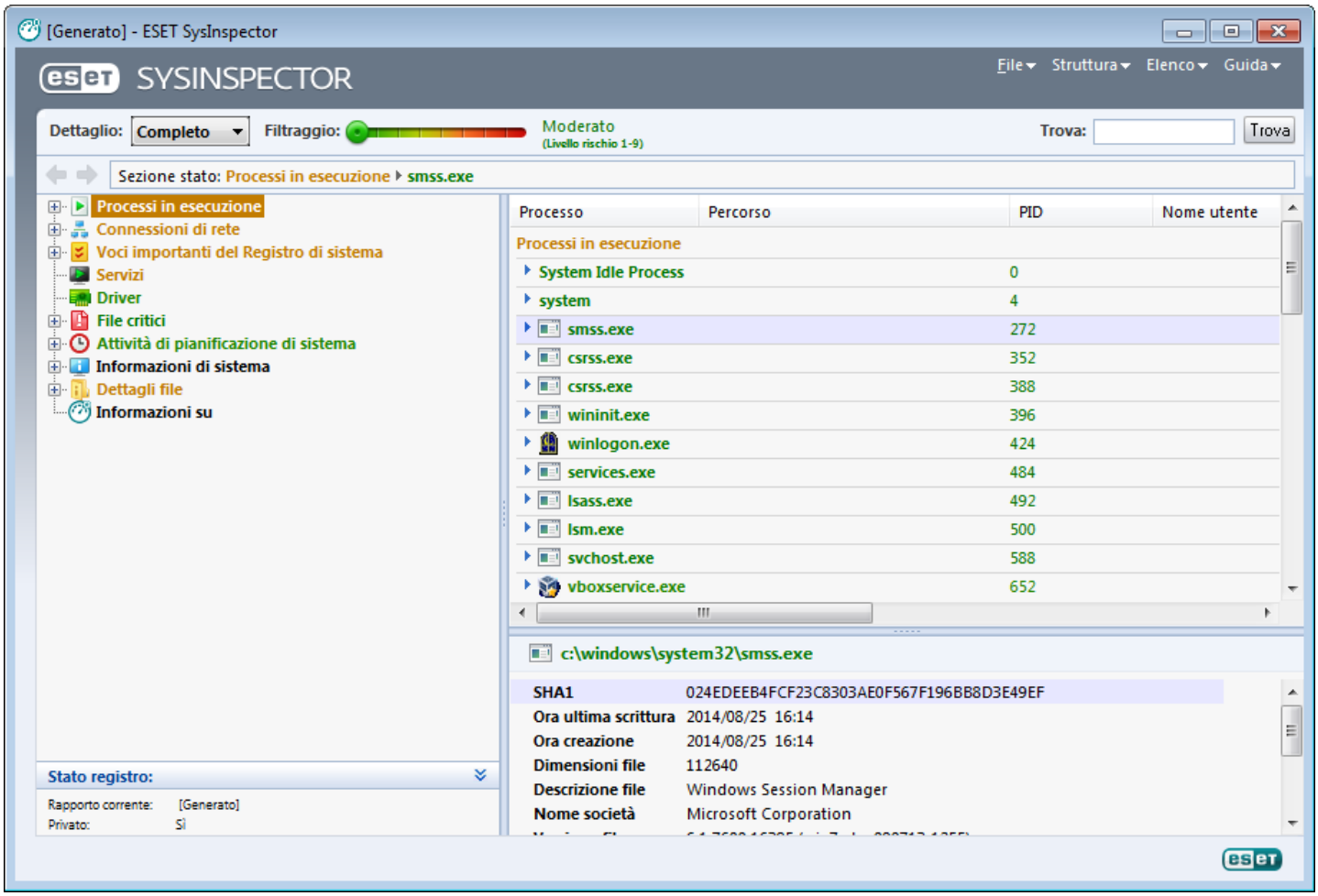
3.9.6.1.1 Avvio di ESET SysInspector

Per avviare ESET SysInspector è sufficiente eseguire il file eseguibile *SysInspector.exe* scaricato dal sito Web ESET. Se è già installata una delle soluzioni ESET Security, è possibile eseguire ESET SysInspector direttamente dal menu Start (fare clic su **Programmi** > **ESET** > **ESET Endpoint Security**).

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

3.9.6.2 Interfaccia utente e utilizzo dell'applicazione

Per chiarezza, la finestra principale del programma è stata divisa in quattro sezioni principali: i comandi del programma sono posizionati nella parte superiore della finestra; a sinistra viene visualizzata la finestra di spostamento, a destra è disponibile la finestra Descrizione e, infine, nella parte inferiore della schermata, viene visualizzata la finestra Dettagli. Nella sezione Stato registro sono elencati i parametri principali di un rapporto (filtro usato, tipo di filtro, se il rapporto è il risultato di un confronto e così via).



3.9.6.2.1 Comandi del programma

La presente sezione contiene la descrizione di tutti i comandi del programma disponibili in ESET SysInspector.

File

Selezionare **File** per memorizzare lo stato attuale del sistema per un'analisi futura oppure aprire un rapporto precedentemente archiviato. Ai fini della pubblicazione, è consigliabile generare un rapporto **Idoneo all'invio**. In questo formato, nel rapporto vengono omesse informazioni riservate (nome utente attuale, nome computer, nome dominio, privilegi utente attuale, variabili d'ambiente e così via).

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

Struttura

Consente di espandere o chiudere tutti i nodi e di esportare le sezioni selezionate sullo script di servizio.

Elenco

Contiene funzioni per uno spostamento più pratico all'interno del programma e varie altre funzioni, ad esempio la ricerca di informazioni su Internet.

Guida

Contiene informazioni sull'applicazione e sulle relative funzioni.

Dettaglio

Questa impostazione influenza le informazioni visualizzate nella finestra principale del programma al fine di semplificarne l'utilizzo. Nella modalità "Base" si ha accesso alle informazioni utilizzate per trovare soluzioni a problemi comuni del sistema. Nella modalità "Media" il programma visualizza i dettagli meno utilizzati, mentre nella modalità "Completa", ESET SysInspector mostra tutte le informazioni necessarie alla soluzione di problemi specifici.

Filtraggio

Il filtraggio elementi viene utilizzato soprattutto per individuare file o voci di registro sospetti all'interno del sistema. Regolando il cursore, è possibile filtrare gli elementi in base al livello di rischio. Se il cursore si trova all'estrema sinistra (Livello di rischio 1) vengono visualizzati tutti gli elementi. Spostando il cursore a destra, il programma esclude tutti gli elementi meno rischiosi rispetto al livello di rischio corrente, consentendo di visualizzare solo gli elementi che risultano più sospetti rispetto al livello visualizzato. Quando il cursore si trova all'estrema destra, il programma visualizza solo gli elementi dannosi conosciuti.

Tutti gli elementi contrassegnati con un livello di rischio compreso tra 6 e 9 rappresentano un rischio per la sicurezza. Se ESET SysInspector ha rilevato un elemento di questo tipo, si consiglia di eseguire il controllo del sistema con ESET Online Scanner, se non si utilizza una soluzione di protezione di ESET. ESET Online Scanner è un servizio gratuito.

NOTA: il Livello di rischio di un elemento può essere determinato rapidamente confrontandone il colore con quello del cursore Livello di rischio.

Confronta

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

Trova

L'opzione Cerca può essere utilizzata per individuare rapidamente un elemento specifico in base al nome o parte di esso. I risultati della richiesta di ricerca vengono visualizzati nella finestra Descrizione.

Ritorna

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

Sezione stato

Visualizza il nodo corrente nella finestra di spostamento.

Importante: gli elementi evidenziati in rosso sono sconosciuti. Per tale motivo, il programma li segna come potenzialmente pericolosi. Se un elemento è segnalata in rosso, non significa automaticamente che sia possibile eliminare il file. Prima di procedere all'eliminazione, assicurarsi che i file siano effettivamente pericolosi o non necessari.

3.9.6.2.2 Navigare in ESET SysInspector

ESET SysInspector divide vari tipi di informazioni in numerose sezioni di base, dette nodi. Se disponibili, ulteriori dettagli saranno visualizzabili espandendo ciascun nodo nei relativi sottonodi. Per espandere o comprimere un nodo, fare doppio clic sul nome del nodo oppure fare clic su ⊞ o ⊟ accanto al nome del nodo. Spostandosi nella struttura ad albero di nodi e sottonodi della finestra di spostamento, sono disponibili vari dettagli su ciascun nodo presente nella finestra Descrizione. Navigando tra gli elementi della finestra Descrizione, è possibile visualizzare ulteriori dettagli per ciascun elemento nella finestra Dettagli.

Di seguito vengono riportate le descrizioni dei nodi principali presenti nella finestra di spostamento e le relative informazioni delle finestre Descrizione e Dettagli.

Processi in esecuzione

Questo nodo contiene informazioni sulle applicazioni e sui processi in esecuzione durante la generazione del rapporto. Nella finestra Descrizione sono disponibili dettagli aggiuntivi su ciascun processo, ad esempio le librerie dinamiche utilizzate dal processo e la loro posizione nel sistema, il nome del produttore dell'applicazione e il livello di rischio del file.

La finestra Dettagli contiene informazioni aggiuntive sugli elementi selezionati nella finestra Descrizione, quali le dimensioni del file o il relativo hash.

NOTA: un sistema operativo è basato su diversi componenti kernel, costantemente in esecuzione, che forniscono funzioni fondamentali e di base per le altre applicazioni utente. In alcuni casi, tali processi sono visualizzati nello strumento ESET SysInspector con il percorso file preceduto da \??\. Quei simboli forniscono un'ottimizzazione per i processi in questione prima di avviarli e risultano sicuri per il sistema.

Connessioni di rete

La finestra Descrizione contiene un elenco di processi e applicazioni che comunicano sulla rete utilizzando il protocollo selezionato nella finestra di spostamento (TCP o UDP), unitamente all'indirizzo remoto a cui è collegata l'applicazione. È inoltre possibile verificare gli indirizzi IP dei server DNS.

La finestra Dettagli contiene informazioni aggiuntive sugli elementi selezionati nella finestra Descrizione, quali le dimensioni del file o il relativo hash.

Voci importanti del Registro di sistema

Contiene un elenco delle voci di registro selezionate che sono spesso correlate a vari problemi del sistema, ad esempio quelle indicano i programmi di avvio, oggetti browser helper (BHO) e così via.

Nella finestra Descrizione è possibile visualizzare i file correlati a voci di registro specifiche. Nella finestra Dettagli è possibile visualizzare maggiori informazioni.

Servizi

La finestra Descrizione contiene un elenco di file registrati come Servizi Windows. Nella finestra Dettagli è possibile controllare il modo in cui è impostato l'avvio del servizio insieme ai dettagli specifici del file.

Driver

Un elenco di driver installati nel sistema.

File critici

Nella finestra Descrizione è visualizzato il contenuto dei file critici relativi al sistema operativo Microsoft Windows.

Attività di pianificazione di sistema

Contiene un elenco delle attività avviate dall'Utilità di pianificazione di Windows a un orario/intervallo specificato.

Informazioni di sistema

Contiene informazioni dettagliate sull'hardware e sul software, oltre a informazioni sulle variabili d'ambiente

impostate, sui diritti utente e sui rapporti eventi di sistema.

Dettagli file

Un elenco di file di sistema importanti e di file presenti nella cartella Programmi. Per maggiori informazioni sui file in questione, fare riferimento alle finestre Descrizione e Dettagli.

Informazioni su

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

3.9.6.2.2.1 Tasti di scelta rapida

I tasti di scelta rapida che possono essere utilizzati con ESET SysInspector includono:

File

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

Genera

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

Filtraggio elementi

1, O	non a rischio, visualizzati gli elementi con livello di rischio 1-9
2	non a rischio, visualizzati gli elementi con livello di rischio 2-9
3	non a rischio, visualizzati gli elementi con livello di rischio 3-9
4, U	sconosciuto, visualizzati gli elementi con livello di rischio 4-9
5	sconosciuto, visualizzati gli elementi con livello di rischio 5-9
6	sconosciuto, visualizzati gli elementi con livello di rischio 6-9
7, B	a rischio, visualizzati gli elementi con livello di rischio 7-9
8	a rischio, visualizzati gli elementi con livello di rischio 8-9
9	a rischio, visualizzati gli elementi con livello di rischio 9
-	diminuisce il livello di rischio
+	aumenta il livello di rischio
Ctrl+9	modalità di filtraggio, livello uguale o più alto
Ctrl+0	modalità di filtraggio, solo livello uguale

Visualizza

Ctrl+5	visualizza per fornitore, tutti i fornitori
Ctrl+6	visualizza per fornitore, solo Microsoft
Ctrl+7	visualizza per fornitore, tutti gli altri fornitori
Ctrl+3	mostra tutti i dettagli
Ctrl+2	livello di dettaglio medio
Ctrl+1	visualizzazione di base
Cancella	indietro di un passaggio
Barra spaziatrice	avanti di un passaggio
Ctrl+W	espande la struttura
Ctrl+Q	comprime la struttura

Altri comandi

Ctrl+T	va alla posizione originale dell'elemento dopo averlo selezionato nei risultati di ricerca
Ctrl+P	visualizza informazioni di base su un elemento
Ctrl+A	visualizza informazioni complete di un elemento
Ctrl+C	copia la struttura dell'elemento attuale
Ctrl+X	copia gli elementi

Ctrl+B	trova su Internet le informazioni sui file selezionati
Ctrl+L	apre la cartella dove si trova il file selezionato
Ctrl+R	apre la voce corrispondente nell'editor del Registro di sistema
Ctrl+Z	copia un percorso di un file (se l'elemento è relativo a un file)
Ctrl+F	passa al campo di ricerca
Ctrl+D	chiude i risultati di ricerca
Ctrl+E	esegue lo script di servizio

Confronto

Ctrl+Alt+O	apre il rapporto originale/comparativo
Ctrl+Alt+R	annulla il confronto
Ctrl+Alt+1	visualizza tutti gli elementi
Ctrl+Alt+2	visualizza solo gli elementi aggiunti, il rapporto mostrerà gli elementi presenti nel rapporto attuale
Ctrl+Alt+3	visualizza solo gli elementi rimossi, il rapporto mostrerà gli elementi presenti nel rapporto precedente
Ctrl+Alt+4	visualizza solo gli elementi sostituiti (compresi i file)
Ctrl+Alt+5	visualizza solo le differenze tra i rapporti
Ctrl+Alt+C	visualizza il confronto
Ctrl+Alt+N	visualizza il rapporto attuale
Ctrl+Alt+P	apre il rapporto precedente

Varie

F1	visualizza la guida
Alt+F4	chiude il programma
Alt+Maiusc+F4	chiude il programma senza chiedere
Ctrl+I	statistiche registro

3.9.6.2.3 Confronta

La funzione Confronta consente di mettere a confronto due rapporti esistenti. Il risultato di questa funzione è una serie di elementi non comuni ai due rapporti. È la soluzione ideale se si desidera individuare le modifiche nel sistema ed è un utile strumento per il rilevamento di codice dannoso.

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

Il confronto tra due rapporti offre il vantaggio di visualizzare un rapporto attualmente attivo e uno salvato in un file. Per confrontare i rapporti, fare clic su **File** > **Confronta rapporto** e scegliere **Seleziona file**. Il rapporto selezionato verrà confrontato con quello attivo nelle finestre principali del programma. Nel rapporto comparativo saranno visualizzate solo le differenze tra i due.

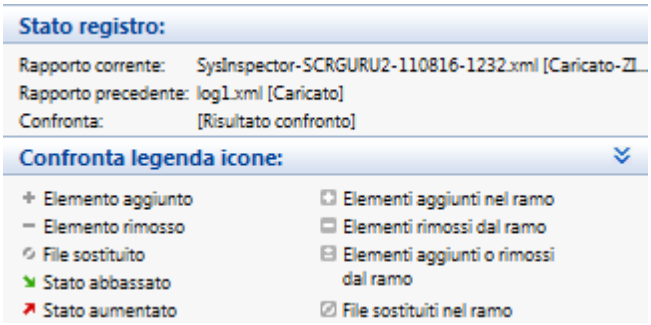
NOTA: se si mettono a confronto due file di rapporto, facendo clic su **File** > **Salva rapporto** e salvandoli in un file ZIP, verranno salvati entrambi i file. Se si apre il file in un secondo momento, i rapporti contenuti verranno automaticamente messi a confronto.

Accanto agli elementi visualizzati, ESET SysInspector mostra i simboli che identificano le differenze tra i rapporti confrontati.

Descrizione di tutti i simboli che possono essere visualizzati accanto agli elementi:

- + nuovo valore, non presente nel rapporto precedente
- la sezione della struttura contiene nuovi valori
- – valore rimosso, presente solo nel rapporto precedente
- la sezione della struttura contiene i valori rimossi
- il valore/file è stato modificato
- la sezione della struttura contiene valori/file modificati
- il livello di rischio è diminuito/era più alto nel precedente rapporto
- il livello di rischio è aumentato/era più basso nel precedente rapporto

Nella sezione di descrizione visualizzata nell'angolo in basso a sinistra vengono descritti tutti i simboli e mostrati i nomi dei rapporti confrontati.



Qualsiasi rapporto comparativo può essere salvato in un file e aperto successivamente.

Esempio

Generare e salvare un rapporto, registrando le informazioni originali sul sistema, in un file denominato previous.xml. Dopo aver effettuato le modifiche al sistema, aprire ESET SysInspector e attendere che venga eseguito un nuovo rapporto. Salvarlo in un file denominato *current.xml*.

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

È possibile ottenere lo stesso risultato utilizzando la seguente opzione della riga di comando:

SysIsnpector.exe current.xml previous.xml

3.9.6.3 Parametri della riga di comando

ESET SysInspector supporta la generazione di rapporti dalla riga di comando con i seguenti parametri:

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

Esempi

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

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

NOTA: Se il nome di un file/cartella contiene uno spazio vuoto, è necessario inserirlo tra virgolette.

3.9.6.4 Script di servizio

Lo script di servizio è uno strumento utile per i clienti che utilizzano ESET SysInspector in quanto consente di rimuovere facilmente gli oggetti indesiderati dal sistema.

Lo script di servizio consente all'utente di esportare l'intero rapporto di ESET SysInspector o le parti selezionate. Al termine dell'esportazione, è possibile selezionare gli oggetti indesiderati da eliminare. È quindi possibile eseguire il rapporto modificato per eliminare gli oggetti contrassegnati.

Lo script di servizio è adatto agli utenti avanzati che hanno già esperienza nella diagnostica dei problemi del sistema. Le modifiche effettuate da persone non qualificate potrebbero causare danni al sistema operativo.

Esempio

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

1. Eseguire ESET SysInspector per generare un nuovo snapshot del sistema.
2. Selezionare il primo elemento della sezione a sinistra (nella struttura ad albero), premere Shift ed evidenziare l'ultimo elemento per selezionarli tutti.
3. Fare clic con il pulsante destro del mouse sugli oggetti selezionati e scegliere **Esporta sezioni selezionate a script di servizio**.
4. Gli oggetti selezionati verranno esportati in un nuovo rapporto.
5. Questo è il passaggio più importante dell'intera procedura: aprire il nuovo rapporto e cambiare l'attributo - in + per tutti gli oggetti che si desidera rimuovere. Fare attenzione a non contrassegnare file/oggetti importanti del sistema operativo.
6. Aprire ESET SysInspector, fare clic su **File** > **Esegui script di servizio** e immettere il percorso dello script.
7. Fare clic su **OK** per eseguire lo script.

3.9.6.4.1 Generazione dello script di servizio

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

NOTA: non è possibile esportare lo script di servizio quando vengono confrontati due rapporti.

3.9.6.4.2 Struttura dello script di servizio

Nella prima riga dell'intestazione dello script sono disponibili informazioni sulla versione del motore (ev), sulla versione dell'interfaccia utente (gv) e sulla versione del rapporto (lv). Questi dati possono essere utilizzati per tenere traccia delle possibili variazioni nel file XML che genera lo script e prevenire eventuali incoerenze durante l'esecuzione. Non modificare questa parte dello script.

La restante parte del file è suddivisa in sezioni in cui è possibile modificare gli elementi (indicare quelli che saranno elaborati dallo script). È possibile contrassegnare gli elementi da elaborare sostituendo il carattere "-" davanti a un elemento con il carattere "+". Le sezioni dello script sono separate tra loro mediante una riga vuota. A ogni sezione viene assegnato un numero e un titolo.

01) Processi in esecuzione

Questa sezione contiene un elenco di tutti i processi in esecuzione nel sistema. Ogni processo è identificato mediante il proprio percorso UNC e, successivamente, dal rispettivo codice hash CRC16 tra asterischi (*).

Esempio:

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

Nell'esempio, è stato selezionato un processo, module32.exe (contrassegnato dal carattere "+"). Il processo

terminerà all'esecuzione dello script.

02) Moduli caricati

In questa sezione sono contenuti i moduli di sistema attualmente in uso.

Esempio:

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

Nell'esempio, il modulo khbekhb.dll è stato contrassegnato con "+". All'esecuzione dello script, i processi che eseguono tale modulo specifico verranno riconosciuti e interrotti.

03) Connessioni TCP

Questa sezione contiene informazioni sulle connessioni TCP esistenti.

Esempio:

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

All'esecuzione dello script, verrà individuato il proprietario del socket nelle connessioni TCP contrassegnate e il socket verrà interrotto, liberando le risorse del sistema.

04) Endpoint UDP

Questa sezione contiene informazioni sugli endpoint UDP esistenti.

Esempio:

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

All'esecuzione dello script, verrà isolato il proprietario del socket sugli endpoint UDP contrassegnati e il socket verrà interrotto.

05) Voci server DNS

Questa sezione contiene informazioni sulla configurazione del server DNS corrente.

Esempio:

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

All'esecuzione dello script, le voci del server DNS contrassegnate verranno rimosse.

06) Voci importanti del Registro di sistema

Questa sezione contiene informazioni su importanti voci del Registro di sistema.

Esempio:

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

All'esecuzione dello script, le voci contrassegnate verranno eliminate, ridotte a valori a 0 byte o ripristinate sui valori predefiniti. L'azione da eseguire su una particolare voce dipende dalla categoria della voce stessa e dal valore principale nel Registro di sistema specifico.

07) Servizi

In questa sezione sono riportati i servizi registrati all'interno del sistema.

Esempio:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

All'esecuzione dello script, i servizi contrassegnati e i relativi servizi dipendenti verranno interrotti e disinstallati.

08) Driver

In questa sezione sono riportati i driver installati.

Esempio:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Quando si esegue lo script, i driver selezionati verranno arrestati. Tenere presente che alcuni driver non possono essere arrestati.

09) File critici

Questa sezione contiene informazioni sui file critici per il corretto funzionamento del sistema operativo.

Esempio:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Gli elementi selezionati saranno eliminati o ripristinati sui valori originali.

3.9.6.4.3 Esecuzione degli script di servizio

Contrassegnare tutti gli elementi desiderati, quindi salvare e chiudere lo script. Eseguire lo script modificato direttamente dalla finestra principale di ESET SysInspector selezionando l'opzione **Esegui script di servizio** dal menu File. All'apertura di uno script, verrà visualizzato il seguente messaggio: **Eseguire lo script di servizio "%Scriptname %"?** Dopo aver confermato, verrà visualizzato un altro messaggio per segnalare che lo script di servizio che si sta cercando di eseguire non è stato firmato. Fare clic su **Esegui** per avviare lo script.

Verrà visualizzata una finestra di dialogo per confermare la corretta esecuzione dello script.

Se lo script è stato eseguito solo parzialmente, verrà visualizzata una finestra di dialogo contenente il seguente messaggio: **Lo script di servizio è stato eseguito parzialmente. Visualizzare il rapporto degli errori?** Selezionare **Sì** per visualizzare un rapporto completo degli errori in cui sono indicate le operazioni non eseguite.

Se lo script non viene riconosciuto, verrà visualizzata una finestra di dialogo contenente il seguente messaggio: **Lo script di servizio selezionato non è firmato. L'esecuzione di script sconosciuti o non firmati potrebbe causare seri danni ai dati nel computer. Eseguire lo script e le azioni?** Ciò potrebbe essere causato da incoerenze all'interno dello script (intestazione danneggiata, titolo della sezione danneggiato, linea vuota tra le sezioni e così via). È possibile riaprire il file script e correggere gli errori all'interno dello script o creare un nuovo script di servizio.

3.9.6.5 Domande frequenti

ESET SysInspector richiede privilegi di amministratore per l'esecuzione?

Anche se per eseguire ESET SysInspector non sono necessari privilegi di amministratore, alcune informazioni raccolte possono essere visualizzate solo da un account amministratore. Eseguendo il programma come utente standard o utente con restrizioni, si raccoglieranno meno informazioni sull'ambiente operativo in uso.

ESET SysInspector crea un file di rapporto?

ESET SysInspector può creare un file di rapporto della configurazione del proprio computer. Per salvarne uno, fare clic su **File** > **Salva rapporto** nella finestra principale del programma. I rapporti vengono salvati nel formato XML. Per impostazione predefinita, i file vengono salvati nella directory *%USERPROFILE%\Documenti*, con una convenzione di denominazione file "SysInpsector-%COMPUTERNAME%-AAMMGG-HHMM.XML". Se preferibile, è possibile modificare la posizione e il nome del file di rapporto prima di salvarlo.

Come si visualizza il file di rapporto di ESET SysInspector?

Per visualizzare un file di rapporto creato da ESET SysInspector, eseguire il programma e fare clic su **File** > **Apri rapporto** nella finestra principale del programma. È anche possibile trascinare i file di rapporto all'interno dell'applicazione ESET SysInspector. Se è necessario consultare frequentemente i file di rapporto di ESET SysInspector, è consigliabile creare un collegamento sul Desktop al file SYSINSPECTOR.EXE, quindi sarà sufficiente trascinare i file di rapporto sopra di esso per poterli visualizzare. Per motivi di protezione, in Windows Vista/7 la funzione di trascinamento della selezione tra finestre con differenti autorizzazioni di protezione potrebbe non

essere disponibile.

È disponibile una specifica per il formato del file di rapporto? E per quanto riguarda un SDK?

Attualmente non è disponibile né una specifica per il file di rapporto né un SDK, in quanto il programma è ancora in fase di sviluppo. Dopo il rilascio del programma, potrebbero essere forniti sulla base dei commenti e delle richieste dei clienti.

In che modo ESET SysInspector valuta il rischio di un determinato oggetto?

Nella maggior parte dei casi, ESET SysInspector assegna livelli di rischio agli oggetti (file, processi, chiavi di registro, ecc.), utilizzando una serie di regole euristiche che esaminano le caratteristiche di ogni oggetto e quindi ne valutano le potenzialità come attività dannosa. Sulla base di tali euristiche, agli oggetti viene assegnato un livello di rischio da 1 - Non a rischio (verde) a 9 - A rischio (rosso). Nel riquadro di spostamento a sinistra, le sezioni sono colorate sulla base del livello di rischio più elevato di un oggetto al loro interno.

Un livello di rischio "6 - Sconosciuto (rosso)" significa che un oggetto è pericoloso?

Le valutazioni di ESET SysInspector non garantiscono che un oggetto sia dannoso. Questa affermazione dovrebbe essere eseguita da un esperto di sicurezza. ESET SysInspector è progettato per fornire una rapida valutazione agli esperti di sicurezza, in modo da informarli su quali oggetti del sistema potrebbero richiedere una loro ulteriore analisi in presenza di comportamento anomalo.

Perché ESET SysInspector si collega a Internet quando viene avviato?

Al pari di molte applicazioni, ESET SysInspector è provvisto di firma digitale, un certificato che garantisce la pubblicazione del software da parte di ESET e l'assenza di alterazione dello stesso. Al fine di verificare il certificato, il sistema operativo contatta un'autorità di certificazione per verificare l'identità dell'autore del software. Si tratta di una procedura comune eseguita su tutti i programmi con firma digitale eseguiti in Microsoft Windows.

Cos'è la tecnologia Anti-Stealth?

La tecnologia Anti-Stealth assicura un efficace rilevamento di rootkit.

Se il sistema viene attaccato da codice dannoso che si comporta come un rootkit, l'utente può essere esposto al rischio di perdita o furto dei dati. In assenza di uno strumento speciale anti-rootkit, è quasi impossibile rilevarli.

Perché a volte i file contrassegnati come "Firmati da MS", hanno contemporaneamente un "Nome aziendale" differente?

Quando si cerca di identificare la firma digitale di un file eseguibile, ESET SysInspector verifica innanzitutto se nel file è incorporata una firma digitale. Se viene trovata una firma digitale, il file verrà convalidato usando tali informazioni. Se la firma digitale non viene trovata, ESI inizia a ricercare il file CAT corrispondente (Catalogo di protezione - *%systemroot%\system32\catroot*) contenente informazioni sul file eseguibile elaborato. Nel caso in cui dovesse trovare il file CAT appropriato, nel processo di convalida del file eseguibile verrà applicata la firma digitale di tale file CAT.

Per tale motivo, a volte i file contrassegnati come "Firmati da MS", hanno contemporaneamente un "Nome aziendale" differente.

3.9.6.6 ESET SysInspector come componente di ESET Endpoint Security

Per aprire la sezione ESET SysInspector in ESET Endpoint Security, fare clic su **Strumenti** > **ESET SysInspector**. Il sistema di gestione della finestra di ESET SysInspector è simile a quello dei rapporti di scansione del computer o delle attività pianificate. Tutte le operazioni con gli snapshot del sistema (crea, visualizza, confronta, rimuovi ed esporta) sono accessibili con pochi clic.

La finestra di ESET SysInspector contiene informazioni di base sugli snapshot creati, quali data e ora di creazione, breve commento, nome dell'utente che ha creato lo snapshot e stato dello snapshot.

Per eseguire il confronto, la creazione o l'eliminazione degli snapshot, utilizzare i pulsanti corrispondenti nella parte inferiore della finestra di ESET SysInspector. Quelle opzioni sono disponibili anche dal menu contestuale. Per visualizzare lo snapshot di sistema selezionato, scegliere **Mostra** dal menu contestuale. Per esportare lo snapshot

selezionato in un file, fare clic con il pulsante destro del mouse, quindi selezionare **Esporta...**.

Di seguito viene fornita una descrizione dettagliata delle opzioni disponibili:

- **Confronta** - Consente di confrontare due rapporti esistenti. È idonea se si desidera rilevare le modifiche tra il rapporto attuale e uno precedente. Per utilizzare questa opzione, selezionare due snapshot da mettere a confronto.
- **Crea...** - Consente di creare un nuovo record. È prima necessario inserire un breve commento sul record. Per visualizzare lo stato di avanzamento della procedura di creazione dello snapshot (relativamente allo snapshot in corso di generazione), fare riferimento alla colonna **Stato**. Tutti gli snapshot completati sono contrassegnati dallo stato **Creato**.
- **Elimina/Elimina tutto** - Consente di rimuovere le voci dall'elenco.
- **Esporta...** - Salva la voce selezionata in un file XML (anche in una versione compressa).

3.10 Glossario

3.10.1 Tipi di minacce

Un'infiltrazione è una parte di software dannoso che tenta di entrare e/o danneggiare il computer di un utente.

3.10.1.1 Virus

Un virus è un pezzo di codice dannoso che è pre-incorporato o viene aggiunto ai file esistenti nel computer. I virus prendono il nome dai virus biologici, poiché utilizzano tecniche simili per diffondersi da un computer all'altro. Il termine "virus" viene spesso utilizzato in maniera errata per indicare qualsiasi tipo di minaccia. Attualmente, l'utilizzo di questo termine è stato superato e sostituito dalla nuova e più accurata definizione di "malware" (software dannoso).

I virus attaccano principalmente i file eseguibili e i documenti. In breve, un virus funziona nel seguente modo: dopo aver eseguito un file infetto, il codice dannoso viene chiamato ed eseguito prima dell'esecuzione dell'applicazione originale. Un virus può infettare qualsiasi file sul quale l'utente corrente dispone dei diritti di scrittura.

I virus possono essere classificati in base agli scopi e ai diversi livelli di gravità. Alcuni di essi sono estremamente dannosi poiché sono in grado di eliminare deliberatamente i file da un disco rigido. Altri, invece, non causano veri e propri danni, poiché il loro scopo consiste esclusivamente nell'infastidire l'utente e dimostrare le competenze tecniche dei rispettivi autori.

Se il computer è stato infettato da un virus e non è possibile rimuoverlo, inviarlo ai laboratori ESET ai fini di un esame accurato. In alcuni casi, i file infetti possono essere modificati a un livello tale da impedirne la pulizia. In questo caso, è necessario sostituire i file con una copia non infetta.

3.10.1.2 Worm

Un worm è un programma contenente codice dannoso che attacca i computer host e si diffonde tramite la rete. La differenza fondamentale tra un virus e un worm è che i worm hanno la capacità di propagarsi autonomamente, in quanto non dipendono da file host (o settori di avvio). I worm si diffondono attraverso indirizzi e-mail all'interno della lista dei contatti degli utenti oppure sfruttano le vulnerabilità delle applicazioni di rete.

I worm sono pertanto molto più attivi rispetto ai virus. Grazie all'ampia disponibilità di connessioni Internet, possono espandersi in tutto il mondo entro poche ore o persino pochi minuti dal rilascio. Questa capacità di replicarsi in modo indipendente e rapido li rende molto più pericolosi rispetto ad altri tipi di malware.

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

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

3.10.1.3 Trojan horse

Storicamente, i trojan horse sono stati definiti come una classe di minacce che tentano di presentarsi come programmi utili per ingannare gli utenti e indurli così a eseguirli.

Poiché si tratta di una categoria molto ampia, è spesso suddivisa in diverse sottocategorie:

- **Downloader** - Programmi dannosi in grado di scaricare altre minacce da Internet.
- **Dropper** - Programmi dannosi in grado di installare sui computer compromessi altri tipi di malware.
- **Backdoor** - Programmi dannosi che comunicano con gli autori degli attacchi remoti, consentendo loro di ottenere l'accesso al computer e assumerne il controllo.
- **Keylogger** (registratore delle battute dei tasti) - Un programma che registra ogni battuta di tasto effettuata da un utente e che invia le informazioni agli autori degli attacchi remoti.
- **Dialer** - Programmi dannosi progettati per connettersi a numeri con tariffe telefoniche molto elevate anziché ai provider dei servizi Internet dell'utente. È quasi impossibile che un utente noti la creazione di una nuova connessione. I dialer possono causare danni solo agli utenti con connessione remota che ormai viene utilizzata sempre meno frequentemente.

Se sul computer in uso viene rilevato un trojan horse, si consiglia di eliminarlo, poiché probabilmente contiene codice dannoso.

3.10.1.4 Rootkit

I rootkit sono programmi dannosi che forniscono agli autori degli attacchi su Internet l'accesso illimitato a un sistema, nascondendo tuttavia la loro presenza. I rootkit, dopo aver effettuato l'accesso a un sistema (di norma, sfruttando una vulnerabilità del sistema), utilizzano le funzioni del sistema operativo per non essere rilevate dal software antivirus: nascondono i processi, i file e i dati del Registro di sistema di Windows. Per tale motivo, è quasi impossibile rilevarli utilizzando le tradizionali tecniche di testing.

Per bloccare i rootkit, sono disponibili due livelli di rilevamento:

1. Quando tentano di accedere 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 dal normale testing: ESET Endpoint Security gli utenti hanno il vantaggio di poter utilizzare la tecnologia Anti-Stealth che è in grado di rilevare ed eliminare anche i rootkit attivi.

3.10.1.5 Adware

Adware è l'abbreviazione di software con supporto della pubblicità (advertising-supported software). Rientrano in questa categoria i programmi che consentono di visualizzare materiale pubblicitario. Le applicazioni adware spesso aprono automaticamente una nuova finestra popup contenenti pubblicità all'interno di un browser Internet oppure ne modificano la pagina iniziale. I programmi adware vengono spesso caricati insieme a programmi freeware, che consentono ai loro sviluppatori di coprire i costi di sviluppo delle applicazioni che, in genere, si rivelano molto utili.

L'adware non è di per sé pericoloso, anche se gli utenti possono essere infastiditi dai messaggi pubblicitari. Il pericolo sta nel fatto che l'adware può svolgere anche funzioni di rilevamento, al pari dei programmi spyware.

Se si decide di utilizzare un prodotto freeware, è opportuno prestare particolare attenzione al programma di installazione. Nei programmi di installazione viene in genere visualizzata una notifica dell'installazione di un programma adware aggiuntivo. Spesso è possibile annullarla e installare il programma senza adware.

Alcuni programmi non verranno installati senza l'installazione dell'adware. In caso contrario, le rispettive funzionalità saranno limitate. Ciò significa che l'adware potrebbe accedere di frequente al sistema in modo "legale", poiché l'utente ne ha dato il consenso. In questi casi, vale il proverbio secondo il quale la prudenza non è mai troppa. Se in un computer viene rilevato un file adware, si consiglia di eliminarlo, in quanto esistono elevate probabilità che contenga codice dannoso.

3.10.1.6 Spyware

Questa categoria include tutte le applicazioni che inviano informazioni riservate senza il consenso o la consapevolezza dell'utente. Gli spyware si avvalgono di funzioni di monitoraggio per inviare dati statistici di vario tipo, tra cui un elenco dei siti Web visitati, indirizzi e-mail della rubrica dell'utente o un elenco dei tasti digitati.

Gli autori di spyware affermano che lo scopo di tali tecniche è raccogliere informazioni aggiuntive sulle esigenze e sugli interessi degli utenti per l'invio di pubblicità più mirate. Il problema è legato al fatto che non esiste una distinzione chiara tra applicazioni utili e dannose e che nessuno può essere sicuro del fatto che le informazioni raccolte verranno utilizzate correttamente. I dati ottenuti dalle applicazioni spyware possono contenere codici di sicurezza, PIN, numeri di conti bancari e così via. I programmi spyware sono frequentemente accoppiati a versioni gratuite di un programma creato dal relativo autore per generare profitti o per offrire un incentivo all'acquisto del software. Spesso, gli utenti sono informati della presenza di un'applicazione spyware durante l'installazione di un programma che li esorta a eseguire l'aggiornamento a una versione a pagamento che non lo contiene.

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

Se in un computer viene rilevato un file spyware, è consigliabile eliminarlo in quanto è molto probabile che contenga codice dannoso.

3.10.1.7 Programmi di compressione

Un programma di compressione è un eseguibile compresso autoestraente che riunisce vari tipi di malware in un unico pacchetto.

I programmi di compressione più comuni sono UPX, PE_Compact, PKLite e ASPack. Se compresso, lo stesso malware può essere rilevato in modo diverso, mediante l'utilizzo di un programma di compressione diverso. I programmi di compressione sono anche in grado di mutare le proprie "firme" nel tempo, rendendo più complessi il rilevamento e la rimozione dei malware.

3.10.1.8 Applicazioni potenzialmente pericolose

Esistono molti programmi legali utili per semplificare l'amministrazione dei computer in rete. Tuttavia, nelle mani sbagliate, possono essere utilizzati per scopi illegittimi. ESET Endpoint Security offre la possibilità di rilevare tali minacce.

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

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

3.10.1.9 Applicazioni potenzialmente indesiderate

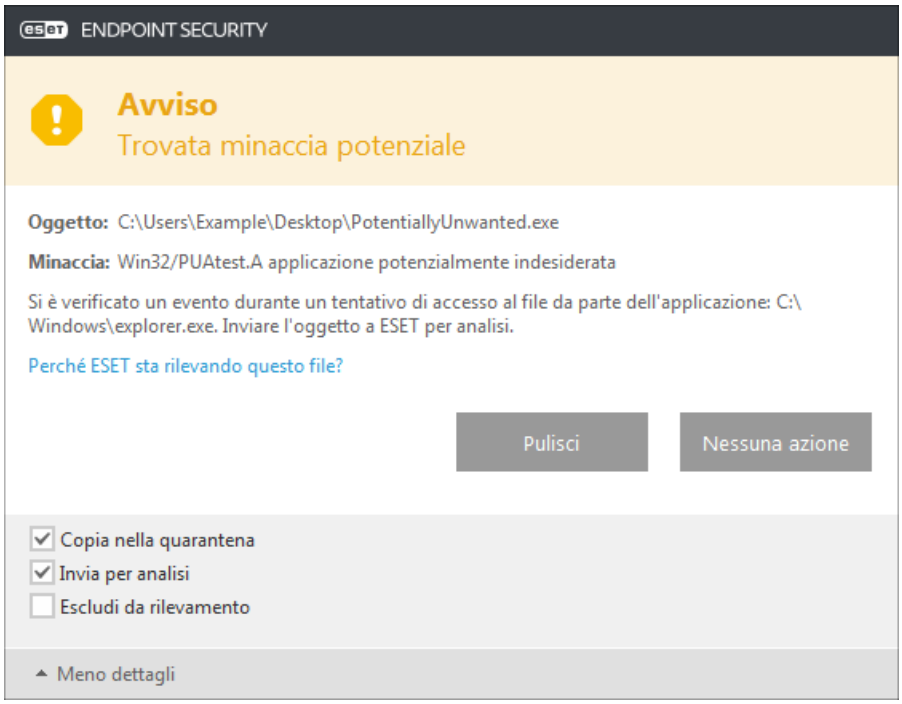
Un'applicazione potenzialmente indesiderata è un programma che contiene adware, installa barre degli strumenti o si prefigge altri obiettivi poco chiari. Esistono alcune situazioni in cui un utente potrebbe percepire che i vantaggi di un'applicazione potenzialmente indesiderata superano i rischi. Per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

Avviso: trovata minaccia potenziale

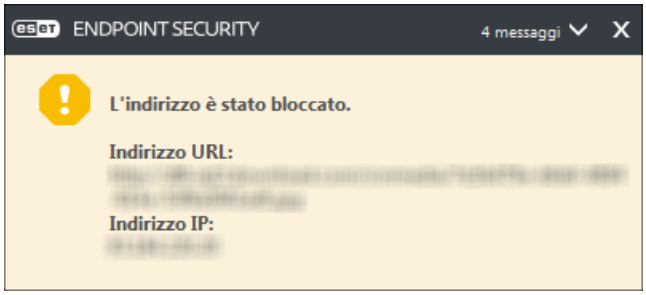
In caso di rilevamento di un'applicazione potenzialmente indesiderata, l'utente potrà scegliere l'azione da intraprendere:

1. **Pulisci/Disconnetti**: questa opzione termina l'azione e impedisce alla minaccia potenziale di entrare nel sistema in uso.
2. **Nessuna azione**: questa opzione consente a una minaccia potenziale di entrare nel sistema in uso.
3. Per consentire l'esecuzione futura dell'applicazione sul computer in uso senza interruzioni, fare clic su **Maggiori**

informazioni/Mostra opzioni avanzate e selezionare la casella di controllo accanto a **Escludi dal rilevamento**.

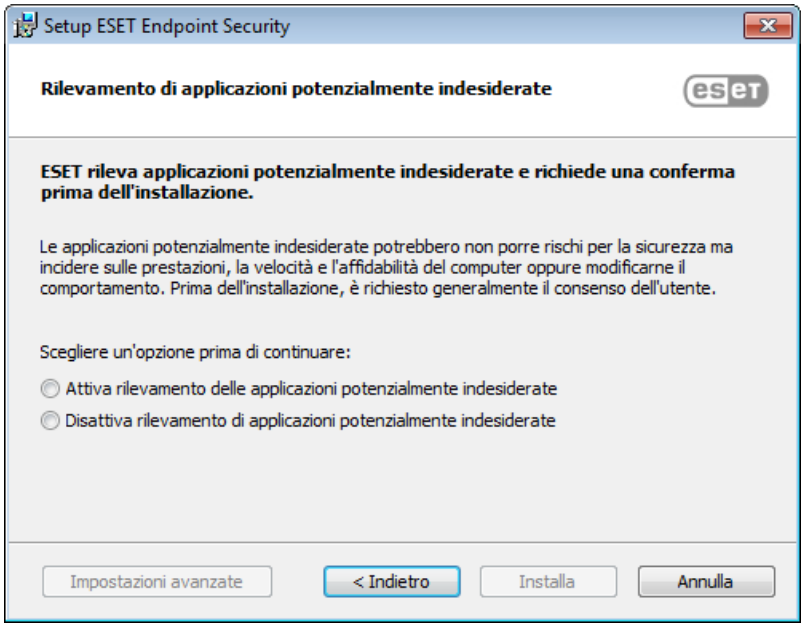


Se un'applicazione potenzialmente indesiderata viene rilevata e non può essere pulita, verrà visualizzata la finestra di notifica **L'indirizzo è stato bloccato** nell'angolo in basso a destra della scherma. Per ulteriori informazioni su questo evento, accedere a **Strumenti** > **File di rapporto** > **Siti Web filtrati** dal menu principale.



Applicazioni potenzialmente indesiderate: impostazioni

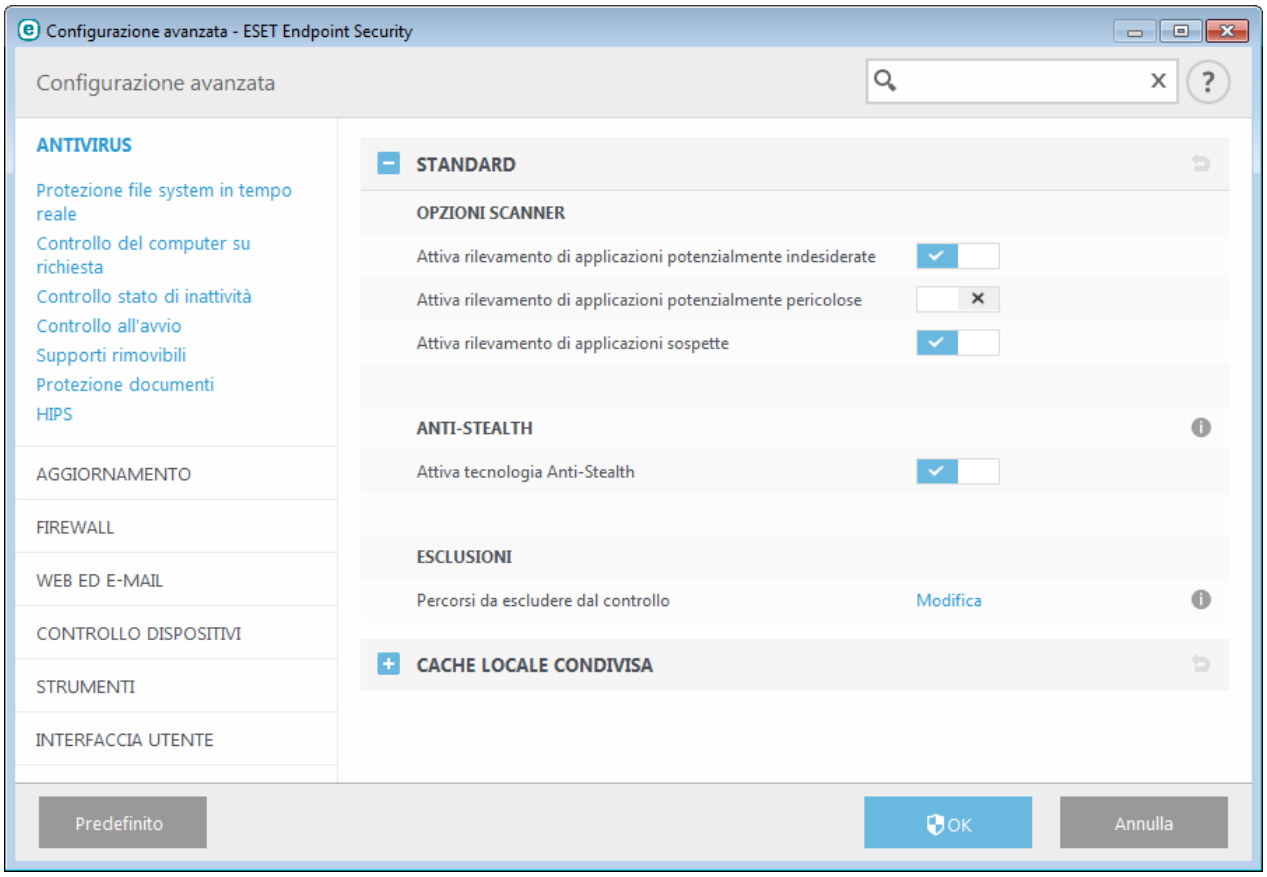
Durante l'installazione di un prodotto ESET, l'utente può decidere di attivare il rilevamento di applicazioni potenzialmente indesiderate, come illustrato di seguito:



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

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

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



Applicazioni potenzialmente indesiderate: wrapper di software

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

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

3.10.1.10 Botnet

Un bot o robot Web è un programma malware automatizzato che ricerca blocchi di indirizzi di rete e infetta computer vulnerabili. Questo tipo di programma consente agli hacker di assumere il controllo di più di un computer contemporaneamente e di trasformarli in bot (noti anche come zombie). Solitamente, gli hacker utilizzano i bot per infettare un gran numero di computer che prendono il nome di botnet. Se il computer in uso è infetto ed entra a far parte di una botnet, esso può essere utilizzato negli attacchi DDoS (Distributed Denial of Service), oltre che per eseguire attività automatizzate su Internet all'insaputa dell'utente (ad esempio, per l'invio di messaggi di spam o virus o per impossessarsi di informazioni personali e private come dati bancari o numeri di carte di credito).

3.10.2 Tipi di attacchi remoti

Esistono molte tecniche particolari che consentono agli autori degli attacchi di compromettere i sistemi remoti. Tali tecniche sono suddivise in diverse categorie.

3.10.2.1 Attacchi worm

Un worm è un programma contenente codice dannoso che attacca i computer host e si diffonde tramite una rete. I worm di rete sfruttano le vulnerabilità di protezione di diverse applicazioni. Grazie alla disponibilità di Internet, possono diffondersi in tutto il mondo entro poche ore dal loro rilascio,

La maggior parte degli attacchi worm può essere evitata utilizzando le impostazioni di protezione predefinite del firewall. È inoltre importante scegliere il tipo di protezione **Rete pubblica** tra le reti pubbliche e mantenere il sistema operativo e i programmi aggiornati con le patch di protezione più recenti.

3.10.2.2 Attacchi DoS (Denial of Service)

DoS, acronimo di *Denial of Service* (ovvero negazione del servizio), è un tentativo di rendere un computer o una rete non disponibile agli utenti destinati. Le comunicazioni fra utenti con tale problema vengono bloccate e non possono più essere eseguite in modo efficace. In genere, è necessario riavviare i computer esposti ad attacchi DoS. In caso contrario, potrebbero non funzionare correttamente.

Nella maggior parte dei casi, gli obiettivi sono i server Web, allo scopo di renderli non disponibili agli utenti per un determinato periodo di tempo.

3.10.2.3 Scansione porta

La scansione porta può essere utilizzata per individuare le porte del computer aperte su un host di rete. Uno scanner di porte è un software progettato per rilevare tali porte.

La porta di un computer è un punto virtuale che gestisce i dati in entrata e in uscita: un elemento strategico dal punto di vista della sicurezza. In una rete di grandi dimensioni, le informazioni raccolte dagli scanner di porta possono contribuire a identificare le potenziali vulnerabilità. Tale uso è legittimo.

Tuttavia, la scansione delle porte viene spesso utilizzata dagli hacker nel tentativo di compromettere la sicurezza. Per prima cosa, gli hacker inviano pacchetti a ogni porta. A seconda del tipo di risposta, è possibile stabilire quali sono le porte in uso. La scansione in sé non causa danni, ma occorre tenere presente che questa attività può rivelare le potenziali vulnerabilità e consente agli autori degli attacchi di assumere il controllo dei computer remoti.

Si consiglia agli amministratori di rete di bloccare tutte le porte inutilizzate e proteggere quelle in uso dagli accessi non autorizzati.

3.10.2.4 Poisoning del DNS

Attraverso il poisoning DNS (Domain Name Server), gli hacker possono ingannare il server DNS di qualsiasi computer facendo credere che i dati fasulli forniti siano legittimi e autentici. Le false informazioni vengono memorizzate nella cache per un determinato periodi di tempo, consentendo agli autori degli attacchi informatici di riscrivere le risposte DNS degli indirizzi IP. Di conseguenza, gli utenti che tentano di accedere a siti Web su Internet scaricheranno virus o worm nel computer, anziché i contenuti originali.

3.10.3 E-mail

L'e-mail o electronic mail è una moderna forma di comunicazione che presenta numerosi vantaggi. È flessibile, veloce e diretta e ha svolto un ruolo cruciale nella proliferazione di Internet all'inizio degli anni novanta.

Purtroppo, a causa dell'elevato livello di anonimità, i messaggi e-mail e Internet lasciano ampio spazio ad attività illegali come lo spam. Lo spamming include annunci pubblicitari non desiderati, hoax e proliferazione di software dannoso o malware. Ad aumentare ulteriormente i disagi e i pericoli è il fatto che i costi di invio dello spamming sono minimi e gli autori dispongono di numerosi strumenti per acquisire nuovi indirizzi e-mail. Il volume e la varietà dello spamming ne rende inoltre estremamente difficoltoso il monitoraggio. Maggiore è il periodo di utilizzo dell'indirizzo e-mail, più elevata sarà la possibilità che finisca in un database per motori di spamming. Di seguito sono riportati alcuni suggerimenti per la prevenzione di messaggi e-mail indesiderati:

- Se possibile, evitare di pubblicare il proprio indirizzo e-mail su Internet
- Fornire il proprio indirizzo e-mail solo a utenti considerati attendibili
- Se possibile, non utilizzare alias comuni. Maggiore è la complessità degli alias, minore sarà la probabilità che vengano rilevati
- Non rispondere a messaggi di spam già recapitati nella posta in arrivo
- Quando si compilano moduli su Internet, prestare particolare attenzione a selezionare opzioni quali "Sì, desidero ricevere informazioni".
- Utilizzare indirizzi e-mail "specializzati", ad esempio, uno per l'ufficio, uno per comunicare con gli amici e così via.
- Cambiare di tanto in tanto l'indirizzo e-mail
- Utilizzare una soluzione antispam

3.10.3.1 Pubblicità

La pubblicità su Internet è una delle forme di pubblicità in maggior crescita. I vantaggi principali dal punto di vista del marketing sono i costi ridotti e un livello elevato di immediatezza. I messaggi vengono inoltre recapitati quasi immediatamente. Molte società utilizzano strumenti di marketing via e-mail per comunicare in modo efficace con i clienti attuali e potenziali.

Questo tipo di pubblicità è legittimo, perché si potrebbe essere interessati a ricevere informazioni commerciali su determinati prodotti. Molte società inviano tuttavia messaggi di contenuto commerciale non desiderati. In questi casi, la pubblicità tramite e-mail supera il limite e diventa spam.

La quantità di messaggi e-mail non desiderati diventa così un problema e non sembra diminuire. Gli autori di messaggi e-mail non desiderati tentano spesso di mascherare i messaggi spam come messaggi legittimi.

3.10.3.2 Hoax: truffe e bufale

Un hoax è un messaggio contenente informazioni non veritiere diffuso su Internet che viene in genere inviato via e-mail e tramite strumenti di comunicazione come ICQ e Skype. Il messaggio stesso è in genere una burla o una leggenda metropolitana.

Gli hoax virus tentano di generare paura, incertezza e dubbio (FUD, Fear, Uncertainty and Doubt) nei destinatari, inducendoli a credere che nei relativi sistemi è presente un "virus non rilevabile" in grado di eliminare file e recuperare password o di eseguire altre attività dannose.

Alcuni hoax richiedono ai destinatari di inoltrare messaggi ai loro contatti, aumentandone così la diffusione. Esistono hoax via cellulare, richieste di aiuto, offerte di denaro dall'estero e così via. Spesso è impossibile determinare l'intento dell'autore del messaggio.

È molto prababile che i messaggi che invitano a essere inoltrati a tutti i propri conoscenti siano hoax. Su Internet sono presenti molti siti Web in grado di verificare l'autenticità di un messaggio e-mail. Prima di inoltrarlo, effettuare una ricerca in Internet per qualsiasi messaggio si sospetti essere hoax.

3.10.3.3 Phishing

Il termine phishing definisce un'attività illegale che si avvale di tecniche di ingegneria sociale (ovvero di manipolazione degli utenti al fine di ottenere informazioni confidenziali). Lo scopo è quello di ottenere l'accesso a dati sensibili quali numeri di conti bancari, codici PIN e così via.

Di norma, l'accesso viene ricavato tramite l'invio di messaggi e-mail che imitano quelli di una persona o società affidabile (ad esempio, istituto finanziario, compagnia di assicurazioni). Il messaggio e-mail sembra autentico e presenta immagini e contenuti che possono indurre a credere che provenga effettivamente da un mittente affidabile. Tali messaggi chiedono all'utente, con vari pretesti (verifica dati, operazioni finanziarie), di immettere alcuni dati personali: numeri di conto bancario o nomi utente e password. Tali dati, se inviati, possono essere rubati e utilizzati in modo illegale.

Le banche, le compagnie di assicurazioni e altre società legittime non chiederanno mai di rivelare nomi utente e password in messaggi e-mail non desiderati.

3.10.3.4 Riconoscimento messaggi indesiderati di spam

In genere, esistono alcuni indicatori che consentono di identificare i messaggi spam (e-mail indesiderate) nella casella di posta. Un messaggio può essere considerato un messaggio spamming se soddisfa almeno alcuni dei criteri riportati di seguito.

- L'indirizzo del mittente non appartiene a nessuno degli utenti presenti nell'elenco dei contatti.
- Agli utenti viene offerta una grossa somma di denaro, purché si impegnino tuttavia ad anticipare una piccola somma di denaro.
- Viene chiesto di immettere con vari pretesti (verifica di dati, operazioni finanziarie) alcuni dati personali, tra cui numeri di conti bancari, nomi utente, password e così via
- È scritto in una lingua straniera.
- Viene chiesto di acquistare un prodotto a cui non si è interessati. Se tuttavia si decide di acquistarlo, è consigliabile verificare che il mittente del messaggio sia un fornitore attendibile (contattare il produttore originale).
- Alcuni termini contengono errori di ortografia nel tentativo di aggirare il filtro di spamming, ad esempio "vaigra" invece di "viagra" e così via

3.10.3.4.1 Regole

Nell'ambito delle soluzioni antispam e dei client di posta, le regole sono strumenti per manipolare le funzioni e-mail. Sono composte da due parti logiche:

1. Condizione (ad esempio, messaggio in arrivo da un determinato indirizzo)

2. Azione (ad esempio, eliminazione del messaggio, spostamento in una cartella specificata)

Il numero e la combinazione di regole varia a seconda della soluzione antispam. Queste regole rappresentano misure contro i messaggi di spam (e-mail indesiderate). Esempi tipici:

- 1. Condizione: un messaggio e-mail in arrivo contiene alcune parole generalmente inserite nei messaggi di spam
  2. Azione: eliminare il messaggio

- 1. Condizione: un messaggio e-mail in arrivo contiene un allegato con estensione .exe
  2. Azione: eliminare l'allegato e recapitare il messaggio alla casella di posta

- 1. Condizione: un messaggio e-mail in arrivo è stato inviato dal datore di lavoro dell'utente
  2. Azione: spostare il messaggio nella cartella "Lavoro"

Si consiglia di utilizzare una combinazione di regole nei programmi antispam per semplificare l'amministrazione e filtrare più efficacemente i messaggi di spam.

3.10.3.4.2 Whitelist

In generale, una whitelist è un elenco di voci o di persone accettate a cui è stata concessa l'autorizzazione di accesso. Il termine "whitelist di posta" definisce un elenco di contatti da cui l'utente desidera ricevere messaggi. Tali whitelist sono basate su parole chiave ricercate negli indirizzi e-mail, nei nomi di domini o negli indirizzi IP.

Se una whitelist funziona in "modalità di esclusività", i messaggi provenienti da qualsiasi altro indirizzo, dominio o indirizzo IP non verranno ricevuti. Se una whitelist non è esclusiva, tali messaggi non verranno eliminati ma solo filtrati in altro modo.

Una whitelist si basa sul principio opposto di quello di una blacklist. Le whitelist sono relativamente facili da mantenere, molto di più rispetto alle blacklist. Si consiglia di utilizzare sia la whitelist che la blacklist per filtrare più efficacemente i messaggi di spam.

3.10.3.4.3 Blacklist

In genere, una blacklist è un elenco di persone o elementi non accettati o vietati. Nel mondo virtuale, è una tecnica che consente di accettare messaggi provenienti da tutti gli utenti non presenti in questo elenco.

Esistono due tipi di blacklist: quelle create dall'utente all'interno della propria applicazione antispam e molte blacklist di tipo professionale, aggiornate regolarmente e create da istituzioni specializzate che sono disponibili su Internet.

È essenziale utilizzare le blacklist per bloccare lo spamming in modo efficace. Tali elenchi sono tuttavia difficili da gestire perché ogni giorno si presentano nuovi elementi da bloccare. È pertanto consigliabile utilizzare sia whitelist che blacklist per filtrare in modo più efficace lo spamming.

3.10.3.4.4 Elenco eccezioni

L'elenco di eccezioni contiene solitamente indirizzi di posta elettronica che potrebbero essere contraffatti e utilizzati per l'invio di messaggi di spam. I messaggi e-mail ricevuti da indirizzi presenti nell'elenco Eccezione verranno sempre sottoposti al controllo alla ricerca di spamming. Per impostazione predefinita, l'elenco di eccezioni contiene tutti gli indirizzi di posta elettronica degli account del client di posta esistenti.

3.10.3.4.5 Controllo lato server

Il controllo lato server è una tecnica che consente di identificare spamming di massa in base al numero di messaggi ricevuti e alle reazioni degli utenti. Ogni messaggio lascia una "impronta" digitale univoca in base al suo contenuto. Il numero ID univoco non fornisce alcuna informazione in merito al contenuto del messaggio e-mail. Due messaggi identici avranno impronte identiche, mentre messaggi diversi avranno impronte diverse.

Se un messaggio viene contrassegnato come spam, l'impronta corrispondente viene inviata al server. Se il server riceve più impronte identiche (che corrispondono a un determinato messaggio di spam), l'impronta viene memorizzata nel database di impronte di spam. Durante il controllo dei messaggi in arrivo, il programma invia le impronte dei messaggi al server. Il server restituisce informazioni sulle impronte corrispondenti ai messaggi già contrassegnati dagli utenti come spam.

3.10.4 Tecnologia ESET

3.10.4.1 Exploit Blocker

L'Exploit Blocker è progettato per rafforzare le applicazioni comunemente utilizzate come browser Web, lettori PDF, client di posta o componenti di MS Office. Il sistema monitora il comportamento dei processi ai fini del rilevamento di attività sospette che potrebbero indicare la presenza di un exploit e aggiunge un altro livello di protezione, in grado di rilevare gli autori degli attacchi informatici con un maggior livello di precisione, utilizzando una tecnologia completamente differente rispetto alle comuni tecniche di rilevamento di file dannosi.

Nel momento in cui l'Exploit Blocker identifica un processo sospetto, lo interrompe immediatamente e registra i dati relativi alla minaccia, che vengono quindi inviati al sistema cloud di ESET Live Grid. Le informazioni vengono elaborate dal laboratorio delle minacce ESET e utilizzate ai fini di una maggiore protezione degli utenti contro minacce sconosciute e attacchi zero-day (malware di nuova concezione per i quali non sono disponibili soluzioni preconfigurate).

3.10.4.2 Scanner memoria avanzato

Lo Scanner memoria avanzato lavora congiuntamente all'Exploit Blocker per garantire una maggiore protezione contro malware concepiti allo scopo di eludere il rilevamento dei prodotti antimalware mediante l'utilizzo di pratiche di offuscamento e/o crittografia. Qualora i metodi di emulazione o di euristica ordinari non siano in grado di rilevare una minaccia, lo Scanner memoria avanzato identifica il comportamento sospetto ed effettua un controllo delle minacce presenti nella memoria del sistema. Questa soluzione si rivela efficace persino contro i malware che utilizzano pratiche di offuscamento ottimizzate. Diversamente dall'Exploit Blocker, lo Scanner memoria avanzato rappresenta un metodo post-esecuzione. Ciò implica un rischio di esecuzione di attività dannose prima del rilevamento di una minaccia. Tuttavia, qualora le altre tecniche di rilevamento disponibili non si rivelino efficaci, questo sistema offre un livello di protezione aggiuntivo.

3.10.4.3 ESET Live Grid

Sviluppato sul sistema avanzato di allarme immediato ThreatSense.Net®, ESET Live Grid utilizza i dati inviati dagli utenti ESET di tutto il mondo e li invia al laboratorio antivirus ESET. Grazie all'invio di campioni e metadati "from the wild" sospetti, ESET Live Grid consente a ESET di soddisfare le esigenze dei clienti e gestire le minacce più recenti in modo tempestivo. I ricercatori dei malware ESET utilizzano le informazioni per creare un'istantanea accurata della natura e dell'ambito delle minacce globali, che consente a ESET di puntare il mirino sugli obiettivi appropriati. I dati ESET Live Grid giocano un ruolo importante nella definizione delle priorità nell'ambito dei sistemi di elaborazione automatici.

Questo strumento consente inoltre di implementare un sistema di reputazione che contribuisce al potenziamento dell'efficienza complessiva delle soluzioni anti-malware ESET. Durante l'analisi di un file eseguibile o di un archivio sul sistema di un utente, il relativo hashtag viene dapprima confrontato rispetto a un database di oggetti della whitelist e della blacklist. Se presente nella whitelist, il file analizzato viene considerato pulito e contrassegnato ai fini dell'esclusione da controlli futuri. Se presente nella blacklist, verranno intraprese azioni appropriate in base alla natura della minaccia. In caso di mancata corrispondenza, il file viene sottoposto a un controllo completo. Sulla base dei risultati del controllo, i file vengono categorizzati come minacce o non minacce. Questo approccio registra un impatto positivo importante sulle prestazioni del controllo.

Il sistema di reputazione consente di effettuare un rilevamento efficace di campioni di malware anche prima della distribuzione delle relative firme agli utenti, mediante gli aggiornamenti del database delle firme antivirali più di una volta al giorno.

3.10.4.4 Protezione botnet

La protezione botnet consente di individuare malware tramite l'analisi dei rispettivi protocolli di comunicazione di rete. A differenza dei protocolli di rete, che non hanno subito variazioni negli ultimi anni, il malware botnet cambia con una certa frequenza. Questa nuova tecnologia aiuta ESET a sconfiggere i malware che tentano di connettere il computer dell'utente alle reti botnet.

3.10.4.5 Java Exploit Blocker

Java Exploit Blocker è un'estensione della protezione ESET Exploit Blocker esistente. Monitora Java e ricerca comportamenti simili a quelli degli exploit. I campioni bloccati possono essere segnalati agli analisti di malware i quali possono creare firme per bloccare tentativi di exploit su Java su vari livelli (blocco URL, download di file e così via).