ESET Server Security

Manuale dell'utente

Fare clic qui per visualizzare la versione della Guida di questo documento

Digital Security
Progress. Protected.

Copyright ©2024 ESET, spol. s r.o.

ESET Server Security è stato sviluppato da ESET, spol. s r.o.

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

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

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

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

REV. 30/04/2024

1 Panoramica ... 1
1.1 Funzioni principali ... 1
1.2 Novità ... 2
1.3 Tipi di protezione ... 3
1.4 Gestione tramite ESET PROTECT ... 3
2 Requisiti di sistema ... 4
3 Installazione/aggiornamento ... 5
3.1 Preparazione dell’installazione ... 5
3.2 Passaggi di installazione di ESET Server Security ... 6
3.2 Esporta impostazioni o rimuovi installazione ... 10
3.2 Aggiornamento iniziale moduli ... 10
3.3 Installazione silenziosa/senza l'intervento dell'utente ... 11
3.3 Installazione riga di comando ... 12
3.4 Installazione della versione più aggiornata ... 15
3.4 Aggiornamento mediante ESET Cluster ... 16
3.4 Aggiornamento tramite ESET PROTECT ... 19
3.5 Installazione in un ambiente cluster ... 20
3.6 Terminal Server ... 20
3.7 Aggiornamenti di protezione e stabilità ... 21
4 Attiva ESET Server Security ... 21
4.1 Attivazione avvenuta con successo ... 22
4.2 Account ESET PROTECT HUB ... 22
4.3 Errore di attivazione ... 23
4.4 Licenza ... 23
5 L'utilizzo di ESET Server Security ... 23
5.1 Monitoraggio ... 24
5.1 Aggiornamento Windows disponibile ... 25
5.1 Isolamento rete ... 26
5.2 File di rapporto ... 27
5.2 Filtraggio rapporti ... 30
5.3 Controllo ... 32
5.3 Finestra del controllo e rapporto del controllo ... 34
5.4 Aggiornamento ... 37
5.5 Configurazione ... 38
5.5 Server ... 39
5.5 Cluster ... 40
5.5 Procedura guidata cluster - Seleziona nodi ... 41
5.5 Procedura guidata cluster - Impostazioni del cluster ... 43
5.5 Procedura guidata cluster - Impostazioni di configurazione del cluster ... 43
5.5 Procedura guidata cluster - Controllo dei nodi ... 44
5.5 Procedura guidata cluster - Installazione dei nodi ... 45
5.5 Computer ... 47
5.5 Rete ... 49
5.5 Connessioni di rete ... 50
5.5 Risolvi comunicazione bloccata ... 50
5.5 Web e e-mail ... 51
5.5 Strumenti - Registrazione diagnostica ... 52
5.5 Importa ed esporta impostazioni ... 53
5.6 Strumenti ... 54
5.6 Processi in esecuzione ... 55

5.6 Statistiche di protezione ... 57
5.6 ESET Shell ... 58
5.6 Utilizzo ... 60
5.6 Comandi ... 65
5.6 Scelte rapide da tastiera ... 68
5.6 File batch/scripting ... 69
5.6 ESET SysInspector ... 70
5.6 Pianificazione attività ... 71
5.6 Pianificazione attività: aggiungi attività ... 72
5.6 Tipo di attività ... 74
5.6 Esecuzione attività ... 75
5.6 Quando si verifica un evento ... 76
5.6 Esegui applicazione ... 76
5.6 Attività ignorata ... 76
5.6 Panoramica attività pianificata ... 77
5.6 Invia campioni per analisi ... 77
5.6 File sospetto ... 78
5.6 Sito sospetto ... 78
5.6 File falso positivo ... 79
5.6 Sito falso positivo ... 79
5.6 Altro ... 79
5.6 Quarantena ... 80
5.7 Configurazione controllo OneDrive ... 81
5.7 Registra ESET OneDrive Scanner ... 83
5.7 Annulla la registrazione di ESET OneDrive Scanner ... 87
6 Configurazione avanzata ... 90
6.1 Detection engine ... 91
6.1 Protezione riconoscimento automatico ... 93
6.1 Esclusioni ... 96
6.1 Esclusioni dal controllo ... 96
6.1 Esclusioni rilevamento ... 97
6.1 Procedura guidata di creazione di un’esclusione ... 99
6.1 Opzioni avanzate ... 99
6.1 Esclusioni automatiche ... 100
6.1 Rilevamento di un'infiltrazione ... 101
6.1 Protezione file system in tempo reale ... 102
6.1 Parametri di ThreatSense ... 103
6.1 Parametri ThreatSense aggiuntivi ... 107
6.1 Estensioni file esclusi dal controllo ... 108
6.1 Esclusioni processi ... 108
6.1 Protezione basata sul cloud ... 109
6.1 Filtro esclusione ... 111
6.1 Controlli malware ... 111
6.1 Gestione profili ... 112
6.1 Destinazioni profilo ... 113
6.1 Destinazioni di controllo ... 114
6.1 Controllo stato inattivo ... 116
6.1 Controllo all'avvio ... 117
6.1 Controllo automatico file di avvio ... 117
6.1 Supporti rimovibili ... 119
6.1 Protezione documenti ... 119

6.1 Controllo Hyper-V 120
6.1 Controllo OneDrive 122
6.1 HIPS 123
6.1 Impostazioni regole HIPS 125
6.1 Impostazioni avanzate HIPS 128
6.2 Aggiorna configurazione 128
6.2 Rollback aggiornamento 132
6.2 Attività pianificata - Aggiornamento 133
6.2 Mirror di aggiornamento 134
6.3 Protezione accesso alla rete 136
6.3 Profilo della connessione di rete 136
6.3 Aggiungi rete 137
6.3 Firewall 139
6.3 Regole firewall 141
6.3 Impostazioni modalità riconoscimento 142
6.3 Termina la modalità riconoscimento 142
6.3 Rilevamento modifica applicazione 142
6.3 Set di IP 143
6.3 Protezione attacchi di rete 143
6.3 Eccezioni IDS 145
6.3 Minaccia sospetta bloccata 145
6.3 Blacklist temporanea indirizzi IP 146
6.3 Protezione attacchi di forza bruta 146
6.3 Regole di Protezione attacchi di forza bruta 147
6.3 Esclusioni della protezione attacchi di forza bruta 147
6.4 Web ed e-mail 147
6.4 Filtraggio protocolli 148
6.4 Web e client di posta 149
6.4 SSL/TLS 149
6.4 Elenco di certificati noti 151
6.4 Comunicazioni SSL crittografate 151
6.4 Protezione client di posta 152
6.4 Protocolli e-mail 153
6.4 Contrassegni e-mail 154
6.4 Barra degli strumenti di Microsoft Outlook 155
6.4 Barra degli strumenti di Outlook Express e Windows Mail 155
6.4 Finestra di dialogo di conferma 156
6.4 Ripeti controllo messaggi 156
6.4 Protezione accesso Web 156
6.4 Gestione indirizzi URL 157
6.4 Crea nuovo elenco 158
6.4 Protezione Web Anti-Phishing 160
6.5 Controllo dispositivi 161
6.5 Regole dispositivi 162
6.5 Gruppi dispositivi 164
6.6 Configurazione degli strumenti 166
6.6 Fasce orarie 166
6.6 Aggiornamento Microsoft Windows 167
6.6 Scanner riga di comando 167
6.6 ESET CMD 169
6.6 ESET RMM 171

6.6 Licenza ... 172
6.6 Provider WMI ... 173
6.6 Dati forniti ... 173
6.6 Accesso ai dati forniti ... 183
6.6 Destinazioni di controllo della console di gestione ESET ... 184
6.6 Modalità override ... 184
6.6 File di rapporto ... 187
6.6 Modalità presentazione ... 189
6.6 Diagnostica ... 190
6.6 Supporto tecnico ... 191
6.6 Cluster ... 192
6.7 Connettività ... 193
6.8 Interfaccia utente ... 194
6.8 Configurazione dell'accesso ... 195
6.8 ESET Shell ... 196
6.8 Disattiva l'interfaccia utente grafica su Terminal Server ... 196
6.8 Icona nell’area di notifica di Windows ... 197
6.9 Notifiche ... 198
6.9 Stati dell'applicazione ... 198
6.9 Messaggi e stati disattivati ... 199
6.9 Notifiche desktop ... 199
6.9 Personalizzazione ... 200
6.9 Notifiche desktop ... 201
6.9 Avvisi interattivi ... 201
6.9 Riavvio necessario ... 202
6.9 Inoltro ... 202
6.10 Ripristina impostazioni predefinite ... 204
6.11 Guida e supporto tecnico ... 205
6.11 Invia richiesta di assistenza ... 206
6.11 Informazioni su ESET Server Security ... 206
6.12 Glossario ... 207
7 Documenti legali ... 207
7.1 Accordo di licenza per l'utente finale ... 207
7.2 Informativa sulla privacy ... 214

Panoramica

ESET Server Security è una soluzione integrata sviluppata specificamente per l'ambiente Microsoft Windows Server. ESET Server Security garantisce una protezione efficace e valida contro vari tipi di malware e offre due principali tipi di protezione: Anti-malware e antispyware.

Inoltre, ESET Server Security fornisce ulteriori funzioni e caratteristiche utili. Per informazioni dettagliate, consultare Funzionalità principali e Novità.

Funzioni principali

Nella tabella che segue vengono illustrate le funzioni disponibili in ESET Server Security. Nelle reti di maggiori dimensioni, è possibile utilizzare ESET PROTECT per la gestione di ESET Server Security da remoto.

Prodotto chiave a 64 bit	Viene aggiunta maggiore stabilità e prestazioni elevate ai componenti principali del prodotto.
Anti-Malware	Una premiata e innovativa difesa da malware. Questa tecnologia all'avanguardia impedisce attacchi ed elimina qualsiasi tipo di minaccia, compresi virus, ransomware, rootkit, worm e spyware con un controllo basato sul cloud per ottenere tassi di rilevamento persino migliori. Con un "ingombro" minimo, non appesantisce le risorse di sistema e non ne riduce le prestazioni. Utilizza il modello di protezione su più livelli e ciascun livello, o fase, prevede una serie di tecnologie core. La fase di pre-esecuzione prevede tecnologie quali Scanner UEFI, Protezione attacchi di rete, Reputazione e memorizzazione nella cache, Sandbox interna al prodotto, Rilevamenti DNA. Le tecnologie della fase Esecuzione sono Exploit Blocker, Protezione ransomware, Scanner memoria avanzato e Scanner script (AMSI). La fase Post-esecuzione utilizza la Protezione botnet, il Sistema di protezione malware cloud e il Sandboxing. Questa serie ricca di funzionalità basata su tecnologie core offre una protezione senza rivali.
Controllo OneDrive	Nuova funzione che consente di controllare file posizionati nello spazio di archiviazione cloud OneDrive. Solo per account aziendali Office 365.
Controllo Hyper-V	È una tecnologia che abilita il controllo dei dischi della macchina virtuale (Virtual Machine, VM) su Microsoft Hyper-V Server senza la necessità di avere un "Agente" sulla VM specifica.
Cluster ESET	Consente la gestione di server multipli da un'unica posizione. Il collegamento delle workstation ai nodi offre un maggior livello di automazione in termini di gestione, grazie alla sua capacità di distribuire un criterio di configurazione tra tutti i membri del cluster. La creazione degli stessi cluster può essere effettuata mediante l'utilizzo del nodo installato, che può quindi installare e avviare tutti i nodi da remoto. I prodotti ESET Server sono in grado di comunicare tra loro e scambiare dati quali configurazioni e notifiche, nonché sincronizzare i dati necessari per il corretto funzionamento di un gruppo di istanze del prodotto. Ciò consente la stessa configurazione del prodotto per tutti i membri del cluster. I cluster di failover Windows e i cluster Network Load Balancing (NLB) sono supportati da ESET Server Security. È inoltre possibile aggiungere manualmente i membri di ESET Cluster senza il bisogno di utilizzare un cluster Windows specifico. Gli ESET Cluster funzionano sia in ambienti di dominio sia in ambienti di gruppo di lavoro.
Esclusioni automatiche	Rilevamento ed esclusione automatici di applicazioni e di file server critici per un funzionamento e prestazioni ottimali.

Prodotto chiave a 64 bit	Viene aggiunta maggiore stabilità e prestazioni elevate ai componenti principali del prodotto.
Esclusioni processi	Esclude processi specifici dal controllo anti-malware all'accesso. In alcune situazioni, il controllo anti-malware all'accesso può causare conflitti, ad esempio durante un processo di backup o migrazioni in tempo reale di macchine virtuali. Le esclusioni dei processi aiutano a ridurre al minimo il rischio di tali potenziali conflitti e a migliorare le prestazioni delle applicazioni escluse. Tale condizione registra, a sua volta, un effetto positivo sulle prestazioni e sulla stabilità generali del sistema. L'esclusione di un processo/un'applicazione corrisponde all'esclusione del relativo file eseguibile (.exe).
eShell ESET Shell	È un'interfaccia della riga di comando che offre agli utenti avanzati e agli amministratori opzioni più complete per la gestione dei prodotti server ESET.
ESET PROTECT	Offre una migliore integrazione con ESET PROTECT, compresa la pianificazione di un Controllo su richiesta. Per ulteriori informazioni, consultare la Guida online di ESET PROTECT.
Installazione basata sui componenti	Consente di personalizzare l'installazione in modo da contenere solo le parti del prodotto selezionate.
Firewall	Il firewall controlla l'intero traffico di rete in entrata e in uscita sul computer in uso in base alle regole interne e alle regole definite dall'utente. A tal fine vengono consentite o bloccate singole connessioni di rete. Il firewall fornisce protezione contro gli attacchi provenienti da dispositivi remoti e blocca servizi potenzialmente pericolosi.
Gestione delle vulnerabilità e delle patch	Funzione disponibile in ESET PROTECT che consente di impostare un controllo periodico sul server con ESET Server Security per rilevare eventuali software installati vulnerabili ai rischi per la sicurezza. La funzione Gestione delle patch aiuta a garantire che i sistemi e le applicazioni siano protetti da vulnerabilità ed exploit noti. L'applicazione effettiva delle patch è manuale, in modo da fornire all'utente il pieno controllo del momento in cui viene eseguita l'applicazione delle patch. Tutto ciò nell'ottica di garantire la protezione e di ottimizzare i tempi di attività, eliminando potenziali interruzioni di servizio causate dagli aggiornamenti delle applicazioni e dal comportamento indotto dagli aggiornamenti. La tecnologia ESET Server Security è stata adattata nelle seguenti aree rispetto a ESET Endpoint Security: • La gestione delle patch può essere eseguita solo manualmente • L'esecuzione del processo di applicazione termina 60 secondi dopo la ricezione dell'attività di aggiornamento • Nessuna risoluzione automatica delle richieste di riavvio del dispositivo per completare l'applicazione delle patch

Novità

Nuove funzioni e miglioramenti in ESET Server Security:

- Il firewall consente di definire facilmente le regole con più opzioni di configurazione. Se si ha familiarità con i concetti di firewall in Endpoint Security, l'utilizzo non sarà diverso da quello già noto. Il firewall è disponibile solo se si possiede un abbonamento attivo a ESET PROTECT di livello base o superiore.

- **Gestione delle vulnerabilità e delle patch**: ESET PROTECT fornisce una funzione in cui è possibile eseguire un controllo periodico sul server con ESET Server Security per rilevare eventuali software installati vulnerabili ai rischi per la sicurezza. La funzione Gestione delle patch aiuta a garantire che i sistemi e le applicazioni siano protetti da vulnerabilità ed exploit noti. L'applicazione effettiva delle patch è manuale, in modo da fornire all'utente il pieno controllo del momento in cui viene eseguita l'applicazione delle patch.

- **Modifiche del layout dell'interfaccia utente**: la sezione Rete dell'opzione Configurazione è stata migliorata e resa visivamente più gradevole.

- ESET PROTECT HUB Supporto.
- Supporto per l'hash del file SHA-256.
- Supporto per Azure Code Signing.
- Rapporto di controllo: la rimozione di qualsiasi sezione del rapporto verrà ora rilevata nel rapporto di controllo. Si tratta di una pratica di controllo standard che impedisce la copertura delle tracce in seguito ad attacchi di tipo "insider" e migliora l'analisi forense in generale.
- Esclusioni automatiche con l'utilizzo di credenziali arbitrarie.
- ESET Cluster: la procedura guidata di ESET Cluster fornisce informazioni sul risultato dell'attivazione del prodotto sui singoli nodi. Registrazione dei miglioramenti relativi a ESET Cluster e ai feedback provenienti dai nodi principalmente per garantire una maggiore chiarezza.
- **Supporto eShell .CSV**: consente a eShell di esportare i rapporti direttamente in un file . CSV. Questa funzionalità consente ora di aggregare i dati da più server su base periodica, in modo più efficiente e senza dover riformattare manualmente l'output da eShell.
- Supporto per il controllo forzato degli aggiornamenti automatici dei prodotti tramite ESET PROTECT Console.
- Altri miglioramenti minori e correzioni di bug.

Consultare i rapporti delle modifiche dettagliati per ESET Server Security.

Tipi di protezione

Esistono due tipi di protezione:

- Protezione Anti-Malware
- Protezione antispyware

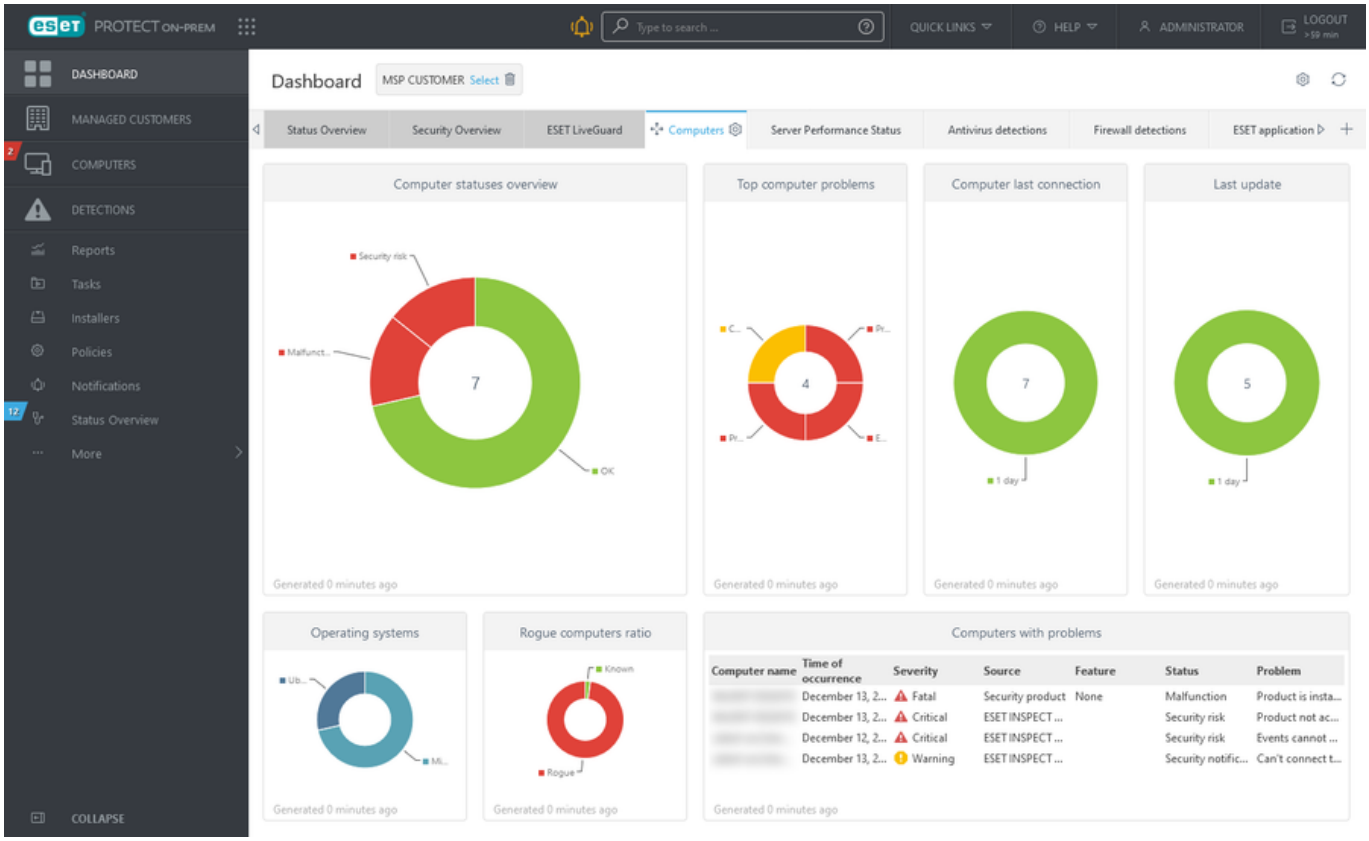
La protezione anti-malware e antispyware rappresenta una funzione di base del prodotto ESET Server Security. La protezione antivirus difende il sistema da attacchi dannosi controllando file, e-mail e comunicazioni su Internet. In caso di rilevamento di una minaccia, il modulo di rilevamento provvede a eliminarla. Il processo prevede le seguenti fasi: blocco, pulizia ed eliminazione o spostamento in Quarantena.

Gestione tramite ESET PROTECT

ESET PROTECT 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 di ESET PROTECT offre l'installazione di soluzioni ESET Security su computer remoti e una risposta rapida ai nuovi problemi e alle nuove minacce.

ESET PROTECT non garantisce protezione contro codice dannoso, ma si affida alla presenza di soluzioni di protezione ESET su ciascun client.

Le soluzioni ESET Security supportano reti che includono vari tipi di piattaforme. Una rete può integrare una combinazione degli attuali sistemi operativi Microsoft, Linux, macOS e mobili.



Per ulteriori informazioni, consultare la Guida online di ESET PROTECT.

Requisiti di sistema

Sistemi operativi supportati:

- Microsoft Windows Server 2022 (Server Core e Desktop Experience)
- Microsoft Windows Server 2019 (Server Core e Desktop Experience)
- Microsoft Windows Server 2016 (Server Core e Desktop Experience)
- Microsoft Windows Server 2012 R2

> Per installare o aggiornare i prodotti ESET rilasciati dopo luglio 2023, il supporto per Azure Code Signing deve essere installato su tutti i sistemi operativi Windows. Ulteriori informazioni.

Storage, Small Business e MultiPoint server:

- Microsoft Windows Storage Server 2016
- Microsoft Windows Storage Server 2012 R2
- Microsoft Windows Server 2019 Essentials
- Microsoft Windows Server 2016 Essentials
- Microsoft Windows Server 2012 R2 Essentials

Sistemi operativi host supportati con ruolo Hyper-V:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2

I requisiti hardware dipendono dalla versione del sistema operativo in uso. Per informazioni dettagliate sui requisiti hardware, si consiglia di consultare la documentazione del prodotto Microsoft Windows Server.

> Prima di installare il prodotto ESET Security, si consiglia vivamente di installare la versione più recente del service pack del sistema operativo Microsoft Server e dell'applicazione server. Se disponibili, si consiglia di installare gli aggiornamenti di Windows e gli aggiornamenti rapidi più recenti.

Requisiti hardware minimi:

Componente	Requisito
Processore	Intel o AMD single core x64
Memoria	256 MB di memoria disponibile
Disco rigido	700 MB di spazio disponibile su disco
Risoluzione schermo	800 x 600 pixel o superiore

Installazione/aggiornamento

Di seguito sono riportati i dettagli sull'installazione e sull'aggiornamento del prodotto insieme a ulteriori informazioni correlate:

- Preparazione dell'installazione
- Passaggi di installazione di ESET Server Security
- Installazione silenziosa/senza l'intervento dell'utente
- Installazione della versione più aggiornata
- Installazione in un ambiente cluster
- Terminal Server
- Aggiornamenti di protezione e stabilità

Preparazione dell'installazione

Si consiglia di eseguire alcune operazioni prima di installare il prodotto:

- Dopo aver acquistato ESET Server Security, scaricare il pacchetto di installazione *.msi* dal sito Web di ESET.

- Verificare che il server sul quale si prevede di installare ESET Server Security soddisfi i requisiti di sistema.

- Eseguire l'autenticazione al server utilizzando un account amministratore.

- In caso di esecuzione di un aggiornamento su un'installazione di ESET Server Security esistente, si consiglia di eseguire il backup della configurazione corrente utilizzando la funzione Esporta impostazioni.

- Rimuovere/disinstallare dal sistema eventuali software antivirus di terze parti. Si consiglia di utilizzare ESET AV Remover . Per consultare un elenco di software antivirus di terze parti che è possibile rimuovere utilizzando ESET AV Remover, consultare questo articolo della knowledge base.

- Se si esegue l'installazione ESET Server Security su Windows Server 2016, Microsoft consiglia di disinstallare le funzionalità di Windows Defender (Microsoft Defender Antivirus) e annullare la registrazione la servizio Windows Defender ATP per evitare problemi dovuti alla presenza di più prodotti antivirus installati in un computer.

- Se si esegue l'installazione di ESET Server Security su Windows Server 2019 o Windows Server 2022, Microsoft consiglia di disabilitare manualmente Microsoft Defender Antivirus per evitare problemi dovuti alla presenza di più prodotti antivirus installati su una macchina.

È possibile eseguire il programma di installazione ESET Server Security nelle seguenti modalità di installazione:

- Finestra principale del programma – L'installazione consigliata è la Procedura di installazione guidata.

- Installazione invisibile all'utente/automatica – Oltra alla procedura di installazione guidata è possibile installare automaticamente ESET Server Security dalla riga di comando.

- Installazione della versione più aggiornata – In caso di utilizzo di una versione precedente di ESET Server Security, è possibile scegliere un metodo di aggiornamento idoneo.

Dopo aver installato o aggiornato correttamente l'istanza di ESET Server Security, è possibile eseguire le seguenti operazioni:

Attivazione prodotto

La disponibilità di uno scenario di attivazione specifico nella finestra di attivazione potrebbe variare in base al Paese e ai mezzi di distribuzione.

Configurazione delle impostazioni generali

È possibile ottimizzare le impostazioni di ESET Server Security modificando le impostazioni avanzate di ciascuna funzione.

Passaggi di installazione di ESET Server Security

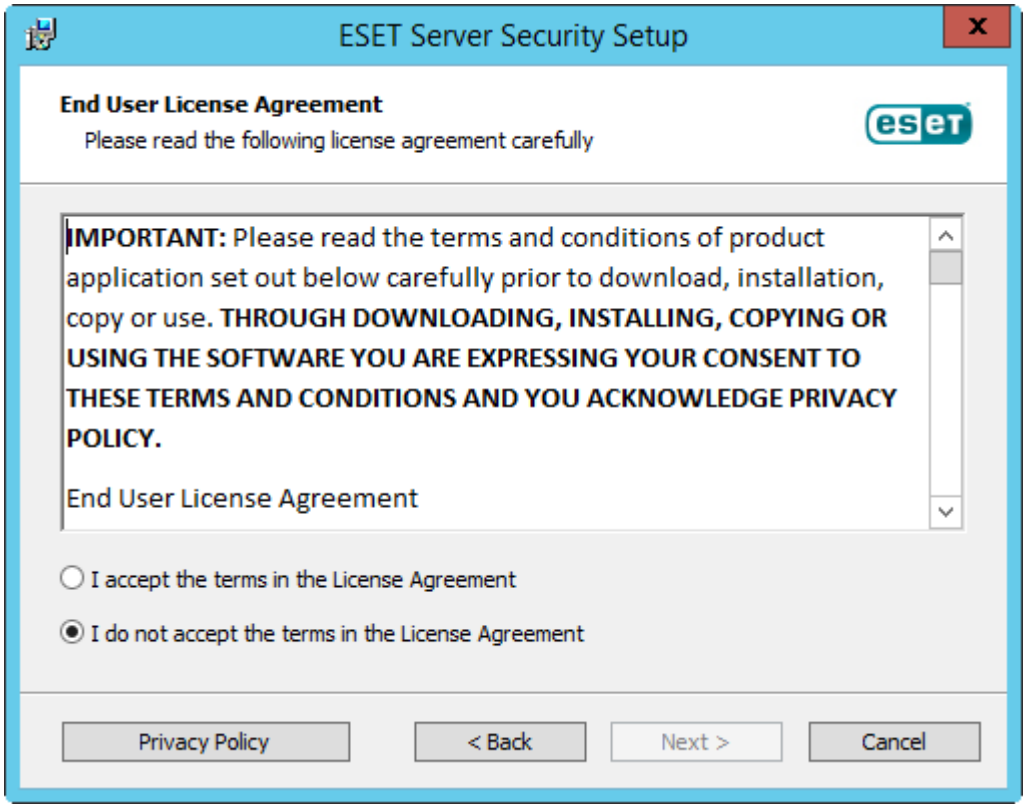
Si tratta di una tipica finestra principale del programma relativa alla procedura di installazione guidata. Fare doppio clic sul pacchetto *.msi* e seguire i passaggi per installare ESET Server Security:

1. Fare clic su **Avanti** per continuare o su **Annulla** per uscire dalla procedura di installazione.

2. La procedura di installazione guidata viene eseguita nella lingua specificata come **Località di residenza** di una **Regione** > impostazione **Posizione** del sistema operativo (o **Posizione corrente** di una **Regione e lingua** >

impostazione **Posizione** nei sistemi meno recenti). Utilizzare il menu a discesa per selezionare la **Lingua del prodotto** preferita. La lingua selezionata per ESET Server Security è indipendente dalla lingua visualizzata nella procedura guidata di installazione.

3. Fare clic su **Avanti** per visualizzare l'Accordo di licenza per l'utente finale. Dopo aver accettato l'Accordo di licenza per l'utente finale e l'Informativa sulla privacy, fare clic su **Avanti**.



4. Scegliere uno dei tipi di installazione disponibili (i tipi di installazione disponibili dipendono dal sistema

operativo in uso):

Completa

Consente di installare tutte le funzioni di ESET Server Security.

> Il programma di installazione contiene solo moduli essenziali. Tutti gli altri moduli verranno scaricati durante l'aggiornamento iniziale del modulo in seguito all'attivazione del prodotto.

Principali

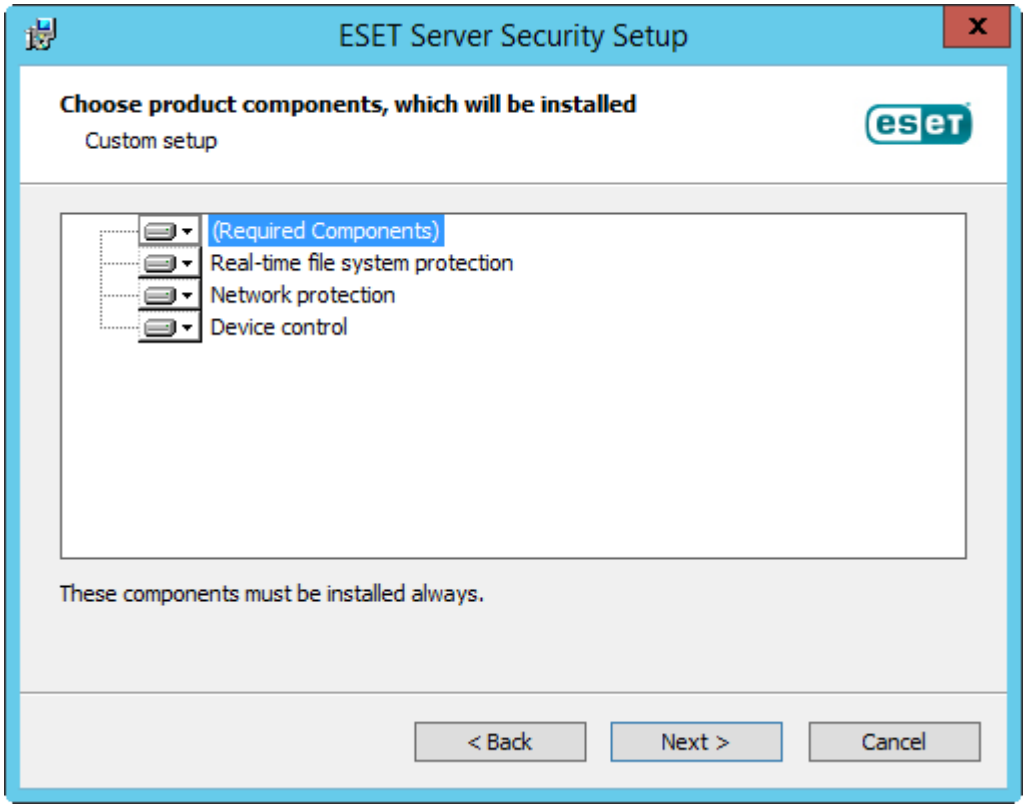
Questo tipo di installazione è destinato alle edizioni Windows Server Core. I passaggi di installazione sono uguali a quelli dell'installazione completa, ma verranno scelte solo le funzioni principali e verrà installata l'interfaccia utente della riga di comando.

Sebbene l'installazione principale sia destinata principalmente all'uso su Windows Server Core, è comunque possibile installarla sui normali Windows Server qualora lo si desideri. I prodotti di protezione ESET installati utilizzando l'installazione di base non dispongono di una finestra principale del programma. Ciò significa che l'utente potrà utilizzare solo l'interfaccia della riga di comando durante l'utilizzo di ESET Server Security. Per maggiori informazioni e per conoscere altri parametri speciali, consultare la sezione Installazione dalla riga di comando.

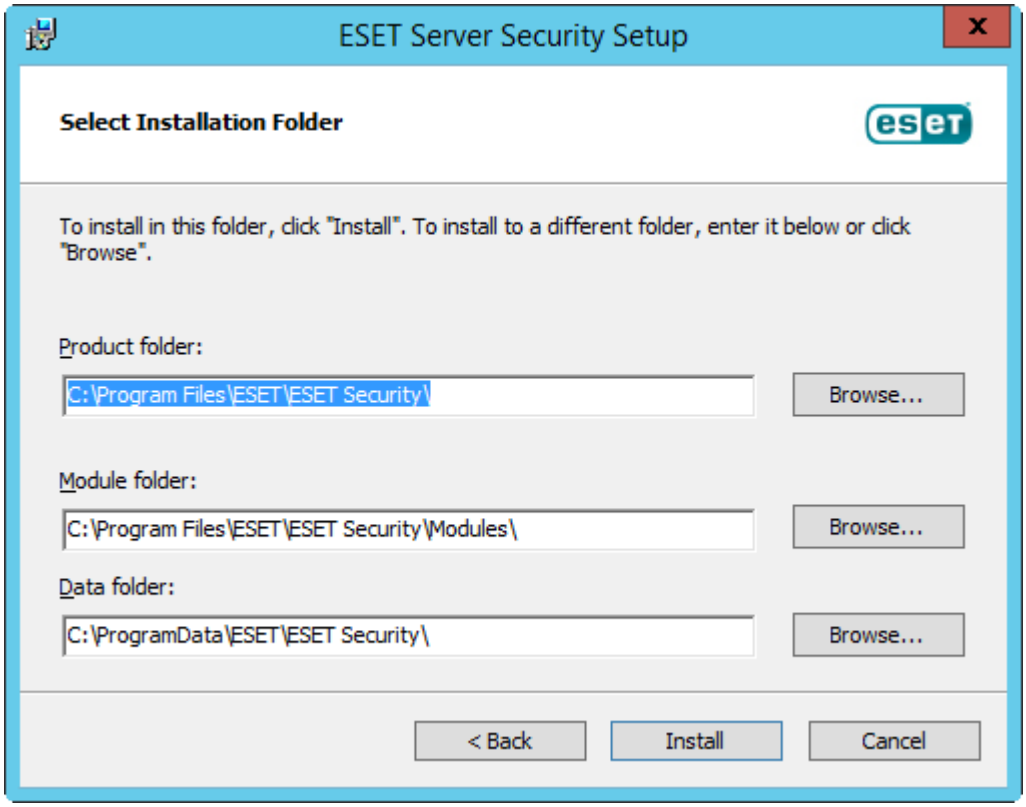
> Per eseguire l'installazione principale mediante la riga di comando, utilizzare il seguente comando fornito come esempio:
> `msiexec /qn /i efsw_nt64.msi ADDLOCAL=_Base`

Personalizzato

L'installazione personalizzata consente all'utente di scegliere le funzioni di ESET Server Security che saranno installate sul sistema. Un elenco di moduli e di funzioni del prodotto comparirà prima dell'avvio dell'installazione. Risulta utile per personalizzare ESET Server Security solo con i componenti necessari all'utente.



5. Verrà richiesto di selezionare il percorso di installazione di ESET Server Security. Per impostazione predefinita, il programma viene installato nel percorso *C:\Program Files\ESET\ESET Server Security*. Fare clic su **Sfoglia** per modificare questo percorso (scelta non consigliata).

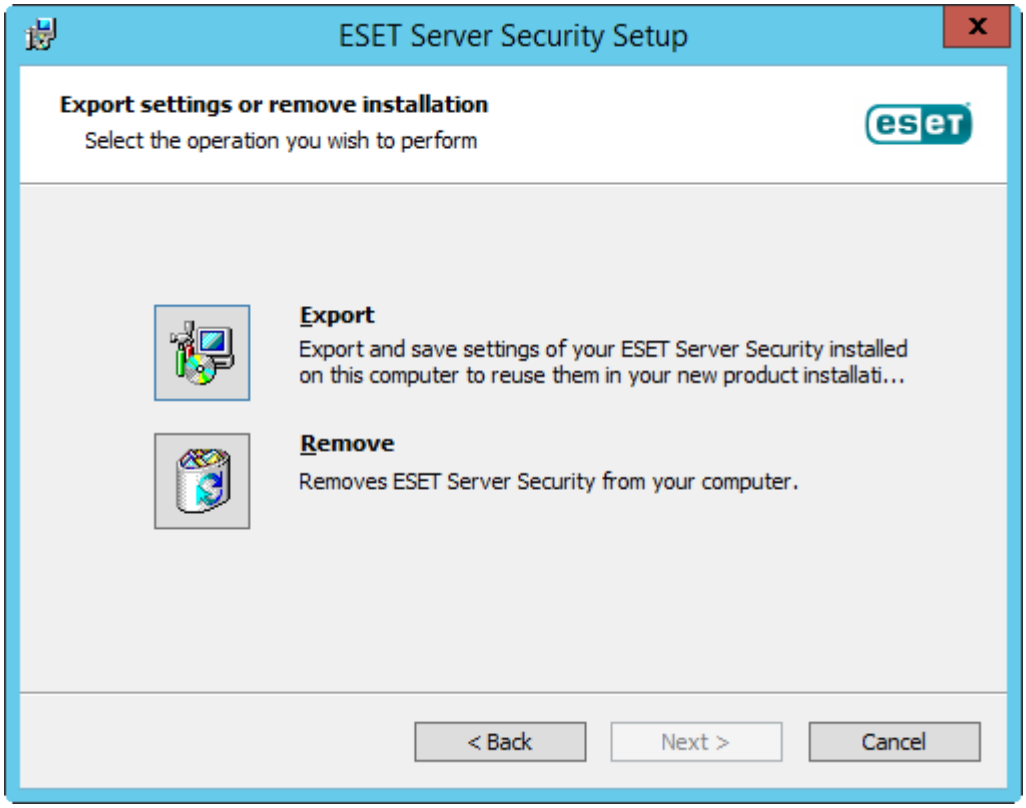


6. Fare clic su **Installa** per avviare l'installazione. Al termine dell'installazione, verrà richiesto di attivare ESET Server Security.

Esporta impostazioni o rimuovi installazione

È possibile esportare e salvare le impostazioni o rimuovere l'installazione. Per compiere tale operazione, eseguire il pacchetto del programma di installazione *.msi* utilizzato durante l'installazione iniziale o portarsi in **Programmi e funzionalità** (opzione accessibile dal Pannello di controllo di Windows), fare clic con il pulsante destro del mouse su ESET Server Security e selezionare **Cambia**.

È possibile **Esportare** le impostazioni di ESET Server Security o **Rimuovere** (disinstallare) completamente ESET Server Security.



Aggiornamento iniziale moduli

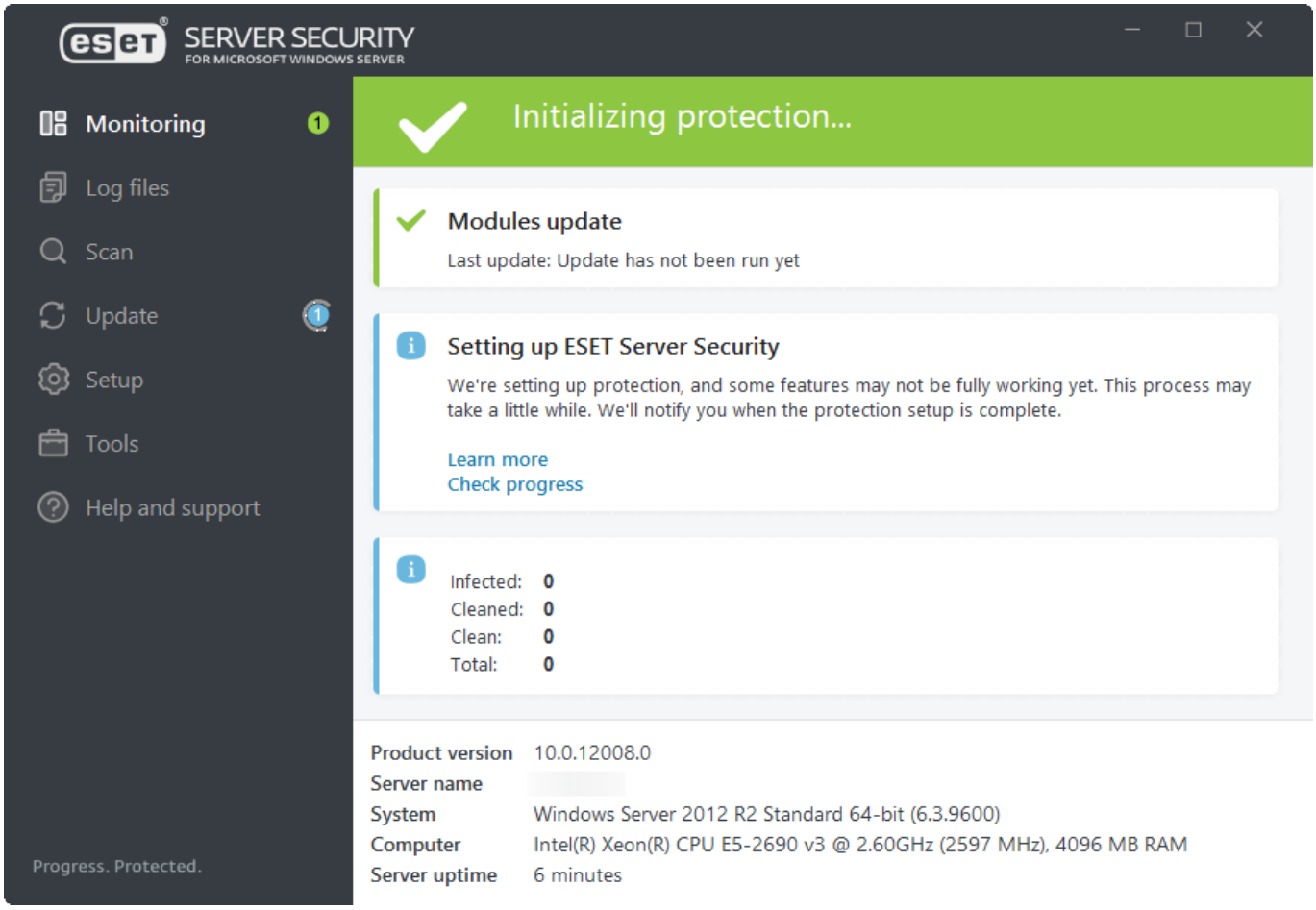
Per ridurre il traffico di rete correlato alle dimensioni del programma di installazione e risparmiare risorse, il programma di installazione contiene solo moduli essenziali. Tutti gli altri moduli verranno scaricati durante l'aggiornamento iniziale del modulo in seguito all'attivazione del prodotto. Il vantaggio principale consiste in un programma di installazione significativamente più piccolo. ESET Server Security consente inoltre di scaricare solo i moduli dell'applicazione più recenti al momento dell'attivazione del prodotto.

Il programma di installazione minimo contiene i seguenti moduli:

- Loaders
- Supporto Anti-Stealth
- Comunicazione Direct Cloud
- Supporto traduzione

- Configurazione
- SSL

In seguito all'attivazione del prodotto, verrà visualizzato lo stato **Inizializzazione della protezione** che informa l'utente dell'inizializzazione delle funzioni.



In caso di problemi durante il download dei moduli (ad esempio assenza di connessione di rete, impostazioni del firewall o del proxy), viene visualizzato l'avviso relativo allo stato dell'applicazione **Attenzione richiesta**. Fare clic su **Aggiorna** > **Ricerca aggiornamenti** nella finestra principale del programma per avviare nuovamente il processo di aggiornamento.
Dopo diversi tentativi non riusciti, viene visualizzato lo stato dell'applicazione di colore rosso **Configurazione della protezione non riuscita**. Se non è possibile aggiornare i moduli, scaricare il programma di installazione di ESET Server Security *.msi* completo.

Se il server non dispone di una connessione a Internet ed è necessario eseguire gli aggiornamenti, utilizzare i seguenti metodi per scaricare i file del modulo di aggiornamento dai server di aggiornamento ESET:

- Aggiornamento dal mirror
- Utilizzo dello strumento Mirror

Installazione invisibile all'utente/automatica

Eseguire il seguente comando per completare l'installazione mediante la riga di comando: `msiexec /i <packagename> /qn /l*xv msi.log`

Utilizzare il visualizzatore eventi di Windows per controllare il **Rapporto dell'applicazione** (ricercare i record da Source: MsiInstaller) per garantire un'installazione corretta o rivedere eventuali problemi di installazione.

Installazione completa su un sistema a 64 bit:

```
msiexec /i efsw_nt64.msi /qn /l*xv msi.log ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,SysInspector,Rmm,eula
```

Installazione del prodotto in una **lingua specificata** (ad esempio tedesco):

```
msiexec /i efsw_nt64.msi /qn ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,^
SysInspector,Rmm,eula PRODUCT_LANG=1031 PRODUCT_LANG_CODE=de-de
```

Per ulteriori informazioni e per visualizzare l'elenco dei codici lingua, consultare **Parametri della lingua** nell'argomento Installazione dalla riga di comando.

Al termine dell'installazione, si avvia la finestra principale del programma di ESET e l'icona viene visualizzata nell'area di notifica di Windows.

Quando si specificano i valori per il parametro `REINSTALL`, è necessario elencare le altre funzioni che non vengono utilizzate come valori per il parametro `ADDLOCAL` o `REMOVE`. Per la corretta esecuzione dell'installazione dalla riga di comando, è necessario elencare tutte le funzioni come valori per i parametri`REINSTALL`, `ADDLOCAL` e `REMOVE`. L'aggiunta o la rimozione potrebbe non riuscire se non si utilizza il parametro `REINSTALL`.
Per un elenco completo delle funzioni, consultare Installazione dalla riga di comando.

Rimozione completa (disinstallazione) su un sistema a 64 bit:

```
msiexec /x efsw_nt64.msi /qn /l*xv msi.log
```

Il server si riavvierà automaticamente al termine di una disinstallazione eseguita correttamente.

Installazione riga di comando

Le impostazioni che seguono sono state concepite per essere utilizzate **esclusivamente con il livello ridotto**, **di base** e **nessuno** dell'interfaccia utente. Consultare la documentazione per la versione `msiexec` utilzizata per i pulsanti della riga di comando appropriati.

Parametri supportati:

APPDIR=<path>

- percorso: percorso di directory valido
- Directory di installazione dell'applicazione
- Ad esempio: `efsw_nt64.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<path>

- percorso: percorso di directory valido
- Directory di installazione dei dati dell'applicazione

MODULEDIR=<path>

- percorso: percorso di directory valido
- Directory di installazione del modulo

ADDLOCAL=<list>

- Installazione dei componenti: elenco di funzioni non obbligatorie da installare localmente.
- Utilizzo con i pacchetti *.msi* ESET: `efsw_nt64.msi /qn ADDLOCAL=<list>`
- Per ulteriori informazioni sulla proprietà `ADDLOCAL`, consultare https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal
- `ADDLOCAL` è un elenco separato da virgole di tutte le funzioni che saranno installate.
- Quando si seleziona una funzione da installare, l'intero percorso (tutte le funzioni correlate) devono essere incluse in maniera esplicita nell'elenco.

REMOVE=<list>

- Installazione dei componenti: funzione principale che non si desidera installare localmente.
- Utilizzo con i pacchetti *.msi* ESET: `efsw_nt64.msi /qn REMOVE=<list>`
- Per ulteriori informazioni sulla proprietà `REMOVE`, consultare https://docs.microsoft.com/en-gb/windows/desktop/Msi/remove
- `REMOVE` è un elenco separato da virgole di tutte le funzioni principali che non saranno installate (o saranno rimosse in presenza dell'installazione).
- Non è sufficiente specificare solo una funzionalità principale. Non è necessario includere in modo esplicito ogni funzionalità secondaria nell'elenco.

ADDEXCLUDE=<list>

- `ADDEXCLUDE` è un elenco separato da virgole di tutti i nomi delle funzioni da non installare.
- Quando si seleziona una funzione da non installare, l'intero percorso (ad es., tutte le relative funzioni secondarie) e le funzioni invisibili correlate devono essere incluse in maniera esplicita nell'elenco.
- Utilizzo con i pacchetti *.msi* ESET: `efsw_nt64.msi /qn ADDEXCLUDE=<list>`

> i `ADDEXCLUDE` non può essere utilizzato con `ADDLOCAL`.

Presenza della funzione

- **Obbligatoria**: la funzione è sempre installata.
- **Facoltativa**: la funzione può essere deselezionata per l'installazione.
- **Invisibile**: funzione logica obbligatoria affinché altre funzioni vengano eseguite correttamente.

Elenco di ESET Server Security funzioni:

> I nomi di tutte le funzioni fanno distinzione tra lettera maiuscola e minuscola, ad esempio `RealtimeProtection` non è uguale a `REALTIMEPROTECTION`.

Nome della funzione	Presenza della funzione
`SERVER`	Obbligatoria
`RealtimeProtection`	Obbligatoria
`WMIProvider`	Obbligatoria
`HIPS`	Obbligatoria
`Updater`	Obbligatoria
`eShell`	Obbligatoria
`UpdateMirror`	Obbligatoria
`DeviceControl`	Facoltativa
`DocumentProtection`	Facoltativa
`WebAndEmail`	Facoltativa
`ProtocolFiltering`	Invisibile
`NetworkProtection`	Facoltativa
`IdsAndBotnetProtection`	Facoltativa
`Rmm`	Facoltativa
`WebAccessProtection`	Facoltativa
`EmailClientProtection`	Facoltativa
`MailPlugins`	Invisibile
`Cluster`	Facoltativa
`_Base`	Obbligatoria
`eula`	Obbligatoria
`ShellExt`	Facoltativa
`_FeaturesCore`	Obbligatoria
`GraphicUserInterface`	Facoltativa
`SysInspector`	Facoltativa
`EnterpriseInspector`	Facoltativa

Se si desidera rimuovere una delle seguenti funzioni è necessario eliminare l'intero gruppo specificando ogni funzione appartenente al gruppo. In caso contrario, la funzionalità non verrà rimossa. Qui sono specificati due gruppi (ciascuna riga rappresenta un gruppo):

```
GraphicUserInterface,ShellExt
```

```
NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,ProtocolFiltering,MailPlugins,EmailClientProtection
```

Escludere la sezione **NetworkProtection** (incluse le funzioni secondarie) dall'installazione utilizzando il parametro `REMOVE` e specificando solo la funzione principale:
```
msiexec /i efsw_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection
```

In alternativa, è possibile utilizzare il parametro `ADDEXCLUDE`, ma è necessario specificare anche tutte le funzioni secondarie:
```
msiexec /i efsw_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,^
ProtocolFiltering,MailPlugins,EmailClientProtection
```

Esempio di installazione **Core**:
```
msiexec /qn /i efsw_nt64.msi /l*xv msi.log ADDLOCAL=RealtimeProtection,Rmm
```

Se si desidera che ESET Server Security sia configurato automaticamente al termine dell'installazione, è possibile specificare i parametri di configurazione di base all'interno del comando di installazione.

Installare ESET Server Security e disattivare ESET LiveGrid®:
```
msiexec /qn /i efsw_nt64.msi ADDLOCAL=RealtimeProtection,Rmm,GraphicUserInterface CFG_LIVEGRID_ENABLED=0
```

Elenco di tutte le proprietà di configurazione:

Pulsante	Valore
`CFG_POTENTIALLYUNWANTED_ENABLED=1/0`	0: disattivata, 1: attivata
`CFG_LIVEGRID_ENABLED=1/0`	0: disattivata, 1: attivata
`FIRSTSCAN_ENABLE=1/0`	0: disattiva, 1: attiva
`CFG_PROXY_ENABLED=0/1`	0: disattivata, 1: attivata
`CFG_PROXY_ADDRESS=<ip>`	Indirizzo IP proxy
`CFG_PROXY_PORT=<port>`	Numero della porta del proxy
`CFG_PROXY_USERNAME=<user>`	Nome utente per l'autenticazione
`CFG_PROXY_PASSWORD=<pass>`	Password per l'autenticazione

Parametri lingua: Lingua del prodotto (è necessario specificare entrambi i parametri)

Pulsante	Valore
`PRODUCT_LANG=`	LCID Decimal (ID locale), ad esempio 1033 per English - United States. Consultare l'elenco di codici lingua.
`PRODUCT_LANG_CODE=`	LCID String (nome delle impostazioni culturali delle lingue) in lettere minuscole, ad esempio en-us per English - United States. Consultare l'elenco di codici lingua.

Installazione della versione più aggiornata

Le nuove versioni di ESET Server Security vengono rilasciate per fornire miglioramenti o risolvere problemi che gli aggiornamenti automatici dei moduli del programma non possono risolvere.

I metodi di aggiornamento includono:

Disinstalla/Installa

Questo metodo consente di rimuovere la versione corrente di ESET Server Security prima di installare quella nuova. Scaricare la versione più recente di ESET Server Security. Esporta impostazioni dall'istanza di ESET Server Security esistente qualora si desideri preservare la configurazione. Disinstallare ESET Server Security e riavviare il server. Eseguire una nuova installazione con il programma di installazione scaricato. Importa impostazioni per caricare la configurazione. Si consiglia di eseguire questa procedura in caso di utilizzo di un unico server su cui è in esecuzione ESET Server Security.

In loco

Si tratta di un metodo aggiornato che consente di installare la nuova versione di ESET Server Security su quella esistente.

> È necessario che sul server non siano presenti aggiornamenti di Windows in sospeso e/o riavvii in sospeso. Se si tenta di eseguire un aggiornamento sul posto con aggiornamenti o riavvii di Windows in sospeso, potrebbe non essere possibile disinstallare correttamente la versione esistente di ESET Server Security. Potrebbero verificarsi problemi anche nel caso in cui si decida successivamente di rimuovere manualmente la vecchia versione di ESET Server Security.

> Durante l'aggiornamento di ESET Server Security è necessario riavviare il server.

Remoto

Questo metodo viene utilizzato in ambienti di rete di grandi dimensioni gestiti da ESET PROTECT ed è un metodo di aggiornamento pulito eseguito da remoto. Risulta utile in presenza di server multipli su cui è in esecuzione ESET Server Security.

Procedura guidata cluster

È inoltre possibile utilizzare la procedura guidata di ESET Cluster per eseguire l'aggiornamento sul posto. Questo metodo è consigliato per due o più server con ESET Server Security. Al termine dell'aggiornamento, è possibile continuare a utilizzare ESET Cluster approfittando dei vantaggi offerti dalle sue funzioni.

> Una volta effettuato l'aggiornamento di ESET Server Security, si consiglia di controllare tutte le impostazioni e di assicurarsi che siano configurate correttamente e conformemente alle proprie esigenze.

Aggiornamento mediante ESET Cluster

La creazione di un'istanza di ESET Cluster consente di aggiornare più server sui quali sono in esecuzione versioni precedenti di ESET Server Security ed è un'alternativa all'aggiornamento di ESET PROTECT. Si consiglia di utilizzare il metodo ESET Cluster in presenza di 2 o più server con ESET Server Security nell'ambiente.

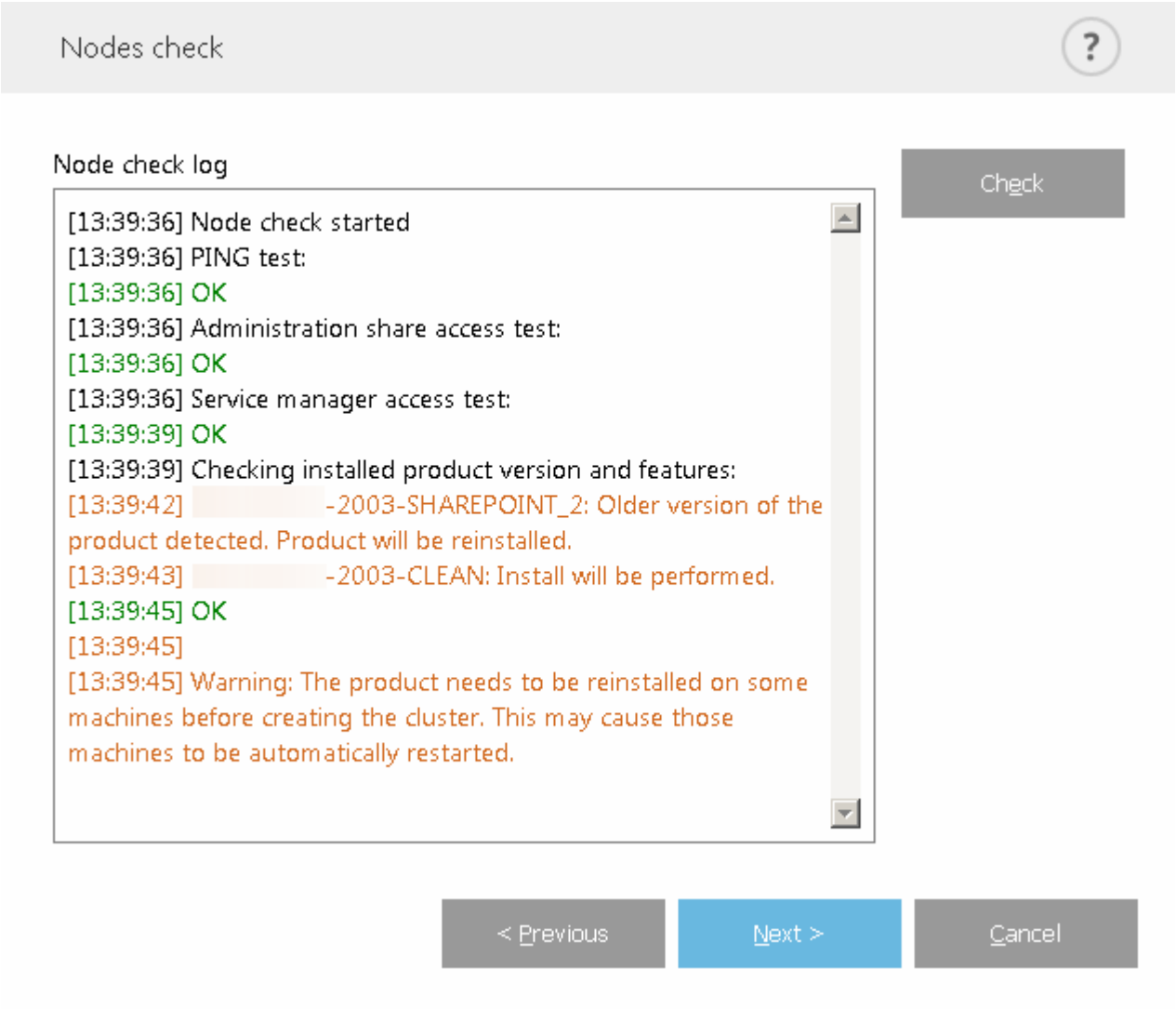
Un altro vantaggio offerto da questo metodo di aggiornamento consiste nella possibilità di continuare a utilizzare ESET Cluster allo scopo di sincronizzare la configurazione di ESET Server Security su tutti i nodi dei membri.

Seguire i passaggi sottostanti per eseguire l'aggiornamento utilizzando ESET Cluster:

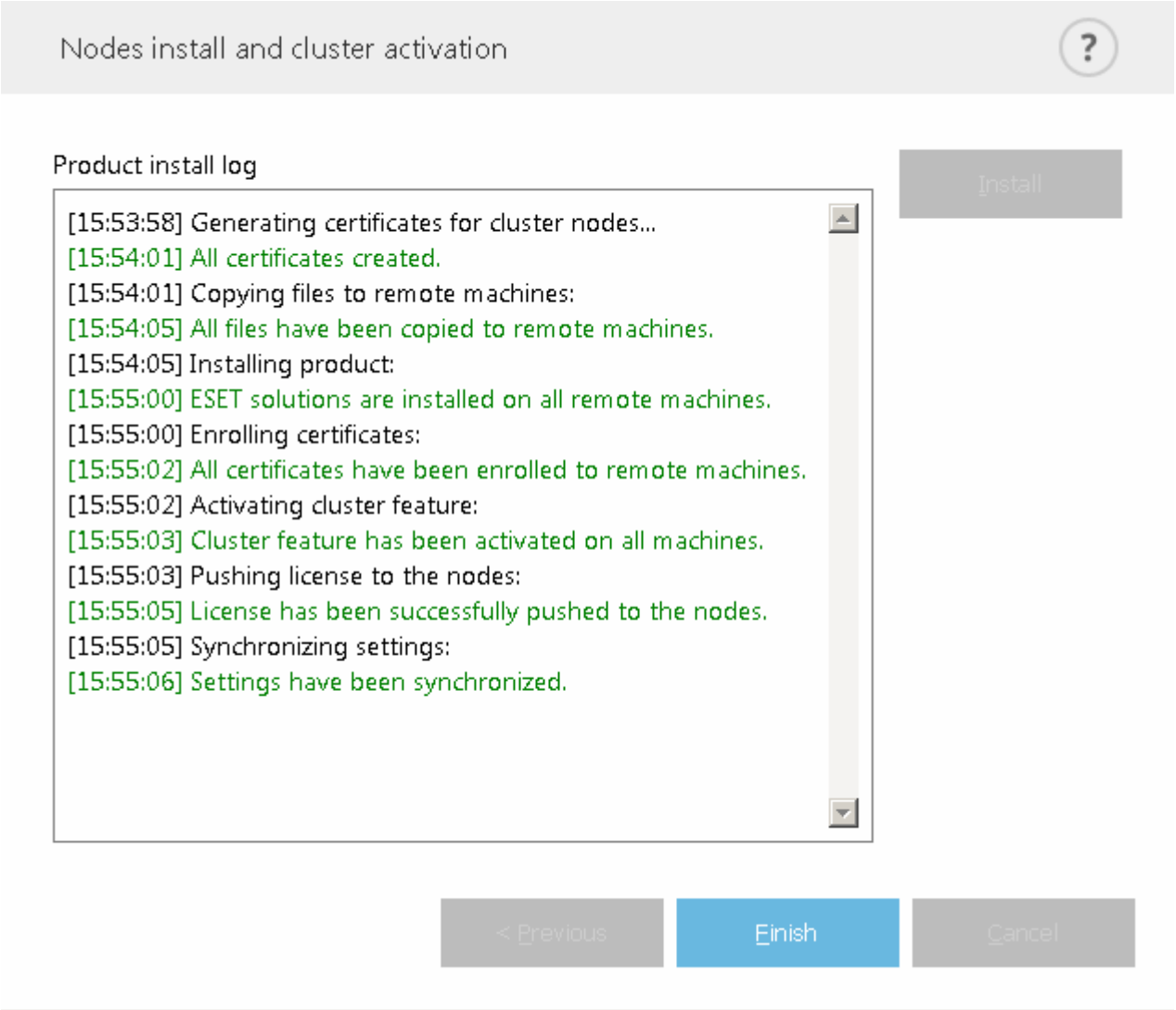
1. Effettuare l'autenticazione a un server sul quale è in esecuzione ESET Server Security ed eseguire l'aggiornamento scaricando e installando la versione più recente su quella esistente. Seguire i passaggi dell'installazione normale. Durante l'installazione la configurazione originale di ESET Server Security viene mantenuta.

2. Eseguire la Procedura guidata di ESET Cluster e aggiungere i nodi del cluster (i server sui quali è necessario che sia in esecuzione una versione aggiornata di ESET Server Security). Se necessario, è possibile aggiungere altri server sui quali non è ancora in esecuzione ESET Server Security (su questi verrà eseguita un'installazione normale). Si consiglia di non modificare le impostazioni predefinite quando si specificano il nome e il tipo di installazione del cluster (assicurarsi di aver selezionato **Esegui il push della licenza sui nodi senza prodotto attivato**).

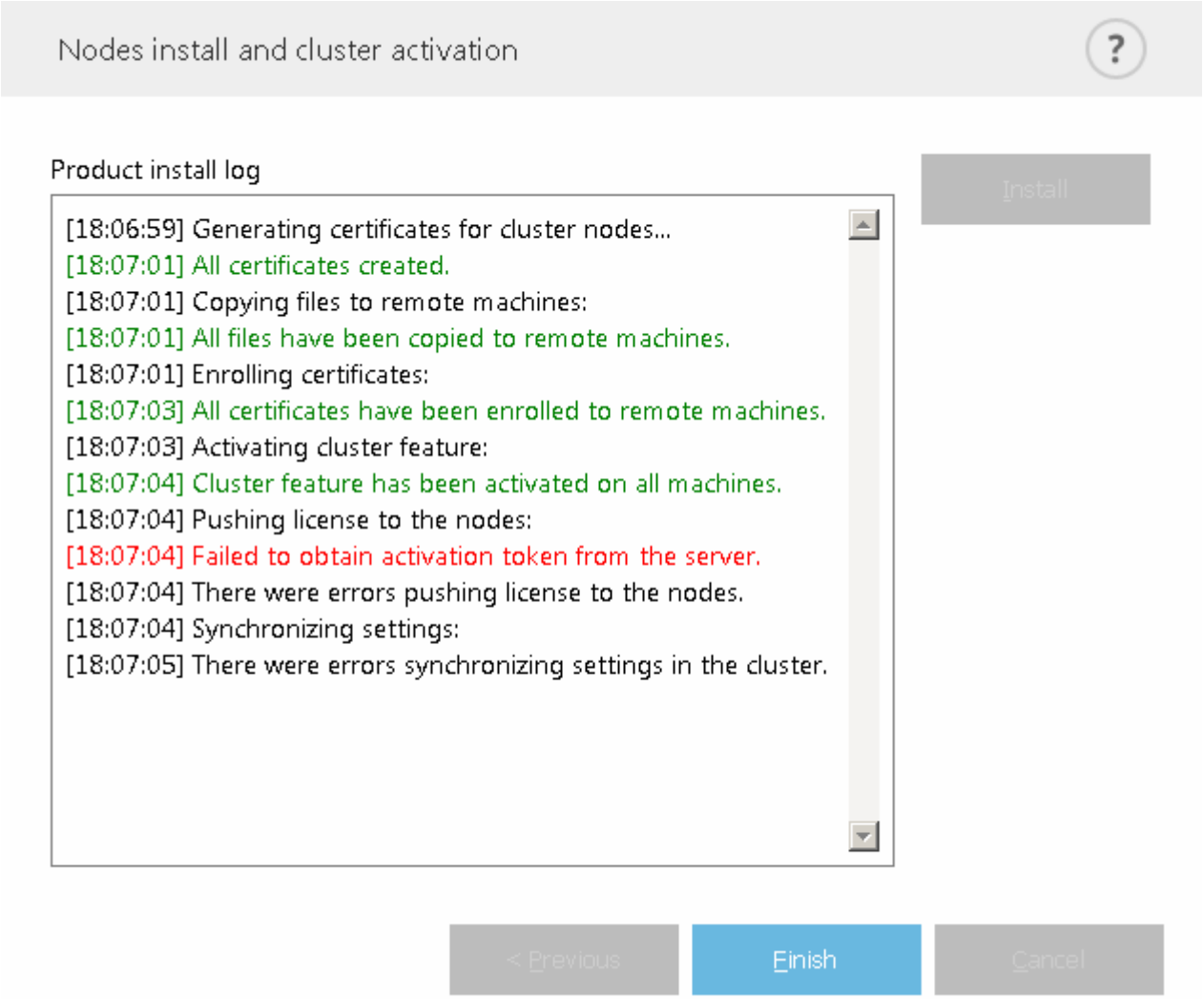
3. Consultare la schermata del **Rapporto di controllo dei nodi**. I server con versioni precedenti del prodotto sono elencati e contrassegnati per l'aggiornamento (reinstallazione). L'applicazione ESET Server Security verrà installata anche sui server sui quali non è ancora stata installata l'applicazione ESET Server Security.



4. La schermata **Installazione nodi e attivazione cluster** consentirà di visualizzare l'avanzamento dell'installazione. Al termine dell'installazione, i risultati visualizzati dovrebbero presentarsi in linea di massima come segue:



In caso di configurazione non corretta della rete o del DNS, l'utente potrebbe ricevere il messaggio di errore **Impossibile ottenere token di attivazione dal server**. Provare a eseguire nuovamente la procedura guidata ESET Cluster. Questa procedura eliminerà il cluster e ne creerà uno nuovo (senza reinstallare il prodotto) e questa volta l'attivazione dovrebbe terminare correttamente. Se il problema persiste, controllare le impostazioni della rete e del DNS.



Aggiornamento tramite ESET PROTECT

ESET PROTECT consente di aggiornare più server su cui è in esecuzione una versione precedente di ESET Server Security. Questo metodo presenta il vantaggio di aggiornare contemporaneamente un numero elevato di server garantendo allo stesso tempo che ciascuna istanza di ESET Server Security sia configurata allo stesso modo (qualora lo si desideri).

La procedura prevede le seguenti fasi:

- **Aggiorna il primo server** manualmente installando la versione più recente di ESET Server Security su quella esistente per preservare la configurazione, incluse le regole e le varie whitelist/blacklist. Questa fase viene eseguita localmente sul server su cui è in esecuzione ESET Server Security.

- **Richiedi configurazione** dell'istanza di ESET Server Security su cui è stata installata la versione 7.x e Converti in criterio in ESET PROTECT. Il criterio verrà applicato in un secondo momento a tutti i server aggiornati. Questa fase, insieme a quelle successive, viene eseguita da remoto tramite ESET PROTECT.

- **Esegui attività di disinstallazione del software** su tutti i server su cui è in esecuzione una vecchia versione di ESET Server Security.

- **Eseguire l'attività di installazione del software** su tutti i server in cui si desidera avere la versione più recente di ESET Server Security.

- **Assegnare un criterio di configurazione** a tutti i server su cui è in esecuzione la versione più recente di ESET Server Security.

Seguire le istruzioni riportate di seguito per eseguire l'aggiornamento tramite ESET PROTECT

1. Accedere a uno dei server su cui è in esecuzione ESET Server Security e aggiornarlo scaricando e installando la versione più recente su quella esistente. Seguire i normali passaggi di installazione. Durante l'installazione le configurazioni originali di ESET Server Security vengono mantenute.

2. Aprire ESET PROTECT **Web Console**, selezionare un computer client da un gruppo statico o dinamico e fare clic su **Mostra dettagli**.

3. Selezionare la scheda Configurazione e fare clic sul pulsante **Richiedi configurazione** per raccogliere le configurazioni del prodotto gestito. Tenere presente che questo processo richiede alcuni minuti. Quando la configurazione più recente compare nell'elenco, fare clic su **Prodotto di protezione** e scegliere **Apri configurazione**.

4. Creare un criterio di configurazione facendo clic sul pulsante **Converti in criterio**. Inserire il **Nome** del nuovo criterio e fare clic su **Fine**.

5. Seleziona **Attività client** e scegliere l'attività Disinstallazione software. Durante la creazione dell'attività di disinstallazione, si consiglia di riavviare il server al termine del processo selezionando la casella di controllo **Riavvia automaticamente se necessario**. Una volta creata l'attività, aggiungere tutti i computer di destinazione desiderati per la disinstallazione.

6. Verificare che ESET Server Security sia disinstallato da tutte le destinazioni.

7. Creare l'attività Installazione software per installare la versione più recente di ESET Server Security su tutte le destinazioni desiderate.

8. **Assegna criterio di configurazione** a tutti i server su cui è in esecuzione ESET Server Security, idealmente a un gruppo.

Installazione in un ambiente cluster

È possibile utilizzare ESET Server Security in un ambiente cluster (ad esempio in un cluster di failover). Installare ESET Server Security su un nodo attivo ed effettuare successivamente una ridistribuzione dell'installazione sul(i) nodo(i) passivo(i) utilizzando la funzione ESET Cluster. Oltre all'installazione, ESET Cluster consentirà di eseguire la replica della configurazione di ESET Server Security al fine di garantire la coerenza tra i nodi del cluster.

Terminal Server

Se ESET Server Security viene installato su un server di Windows che funge da Terminal Server, è possibile disabilitare la finestra principale del programma di ESET Server Security per impedire che venga avviata a ogni autenticazione di un utente. Per informazioni dettagliate su come disabilitare la finestra principale del programma, consultare Disabilita l'interfaccia grafica utente su Terminal Server.

Aggiornamenti di protezione e stabilità

L'aggiornamento di ESET Server Security è essenziale per garantire una protezione costante e completa contro codici dannosi. Le versioni aggiornate di ESET Server Security contengono miglioramenti e correzioni di bug. Si consiglia vivamente di eseguire un aggiornamento periodico di ESET Server Security per evitare vulnerabilità e minacce di protezione.

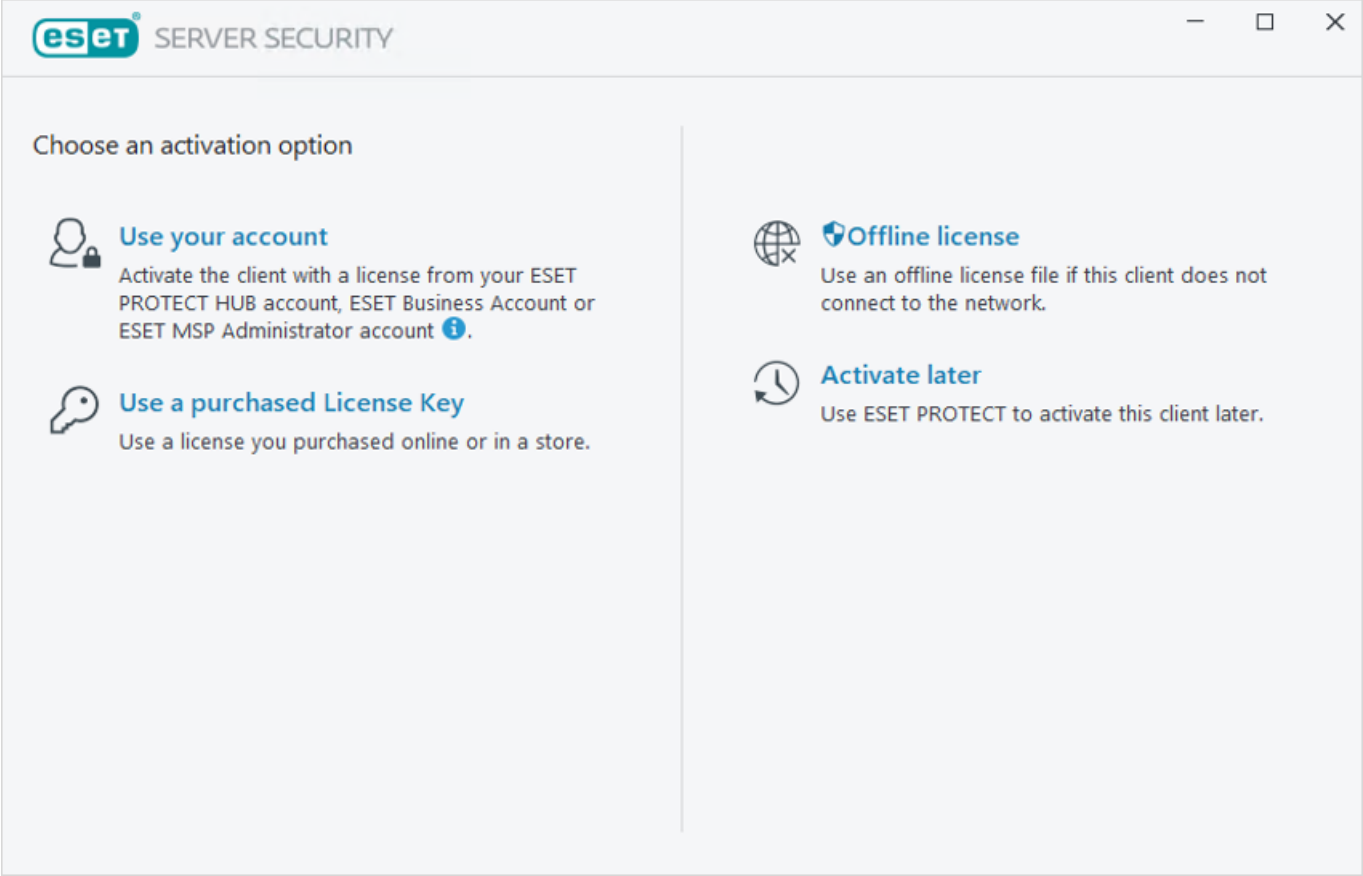
ESET Server Security si inserisce in una fase specifica del ciclo di vita del prodotto, come qualsiasi altro prodotto ESET. Ulteriori informazioni sul Criterio della fine del ciclo di vita (prodotti Business).

Per ulteriori informazioni sulle modifiche apportate, consultare il seguente articolo della Knowledge Base di ESET ESET Server Security.

Gli aggiornamenti automatici garantiscono la massima sicurezza e stabilità del prodotto. Non è possibile disabilitare gli aggiornamenti relativi a protezione e stabilità.

Attiva ESET Server Security

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



Per attivare ESET Server Security, è anche possibile utilizzare uno dei seguenti metodi:

Utilizza il tuo account

Se non si possiede un account ESET PROTECT HUB registrato, crearne uno nuovo. È inoltre possibile utilizzare strumenti di gestione delle licenze meno recenti ESET Business Account o ESET MSP Administrator.

Una chiave di licenza acquistata

Digitare o copiare/incollare la chiave di licenza rilasciata da ESET nel campo **Chiave di licenza** e fare clic su **Continua**. Digitare la chiave di licenza esattamente così come viene fornita, inclusi i trattini. Se si copia/incolla la licenza, assicurarsi di non selezionare accidentalmente uno spazio aggiuntivo attorno al testo.

Tutti i file della licenza off-line

Questo è un file generato automaticamente che viene trasferito al prodotto ESET. Il file della licenza off-line viene generato dal portale della licenza e utilizzato in ambienti in cui l'applicazione non può effettuare la connessione all'autorità che ha concesso la licenza.

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

Selezionare **Guida e supporto tecnico** > **Cambia licenza** nella finestra principale del programma per gestire le informazioni della licenza. Sarà possibile visualizzare l'ID della licenza pubblica per individuare il prodotto e 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 dell'Area di notifica di Windows .

Dopo aver attivato correttamente ESET Server Security, si aprirà la finestra principale del programma e lo stato corrente verrà visualizzato nella pagina Monitoraggio. Inizialmente, potrebbe essere richiesta l'attenzione dell'utente che dovrà, ad esempio, decidere se partecipare o meno a ESET LiveGrid®.

Nella finestra principale del programma verranno inoltre visualizzate le notifiche relative ad altri elementi, come ad esempio gli aggiornamenti di sistema (aggiornamenti di Windows) o gli aggiornamenti del motore di rilevamento. Se tutti i problemi che richiedono attenzione vengono risolti, lo stato di monitoraggio diventa verde e viene visualizzato lo stato **Protezione attiva**.

È inoltre possibile attivare il prodotto dal menu principale in **Guida e supporto tecnico** > **Attiva prodotto** o **Stato di monitoraggio** > **Il prodotto non è attivato**.

> ESET PROTECT è in grado di attivare automaticamente i computer client che utilizzano le licenze messe a disposizione dall'amministratore.

Attivazione avvenuta con successo

Il ESET Server Security non è attivato Da questo punto in poi, ESET Server Security riceverà aggiornamenti periodici che consentiranno di identificare le ultime minacce e garantire la sicurezza del computer.

Fare clic su **Fine** per terminare l'attivazione del prodotto.

Account ESET PROTECT HUB

ESET PROTECT HUB è un gateway centrale per la piattaforma di protezione unificata ESET PROTECT. Fornisce una gestione centralizzata di identità, abbonamenti e utenti per tutti i moduli della piattaforma ESET. ESET PROTECT HUB consente di:

- Ottenere una panoramica degli abbonamenti di protezione

- Controllare l’utilizzo e lo stato degli abbonamenti ai servizi scelti
- Assegna e controlla l’accesso granulare alle singole piattaforme ESET
- Opzione “Single Sign-in” per tutte le piattaforme ESET collegate e accessibili

Se non si possiede un account ESET PROTECT HUB registrato, crearne uno nuovo ed effettuare l’autenticazione con il proprio **indirizzo e-mail** e **la password**.

Errore di attivazione

Nel caso in cui l’attivazione di ESET Server Security non sia stata eseguita correttamente, gli scenari possibili sono i seguenti:

- Chiave di licenza già in uso
- Chiave di licenza non valida: errore modulo di attivazione del prodotto
- Gestire le informazioni mancanti o non valide
- Comunicazione con il database di attivazione non riuscita: riprovare tra 15 minuti
- La connessione ai server di attivazione ESET non è disponibile o è disabilitata

Assicurarsi di aver inserito la **Chiave di licenza** corretta o di aver associato una **Licenza offline** e tentare di eseguire nuovamente l’attivazione.

Se non è possibile eseguire l’attivazione, consultare la procedura guidata per la risoluzione dei problemi di attivazione.

Licenza

Verrà richiesto di selezionare una licenza per ESET Server Security associata al proprio account. Fare clic su **Continua** per procedere con l’attivazione.

L'utilizzo di ESET Server Security

In questa sezione viene riportata una descrizione dettagliata dell’interfaccia utente del programma e viene spiegato come utilizzare ESET Server Security.

L’interfaccia utente consente di accedere rapidamente alle funzionalità utilizzate più di frequente:

- Monitoraggio
- File di rapporto
- Controllo
- Aggiornamento

- Configurazione
- Strumenti

Monitoraggio

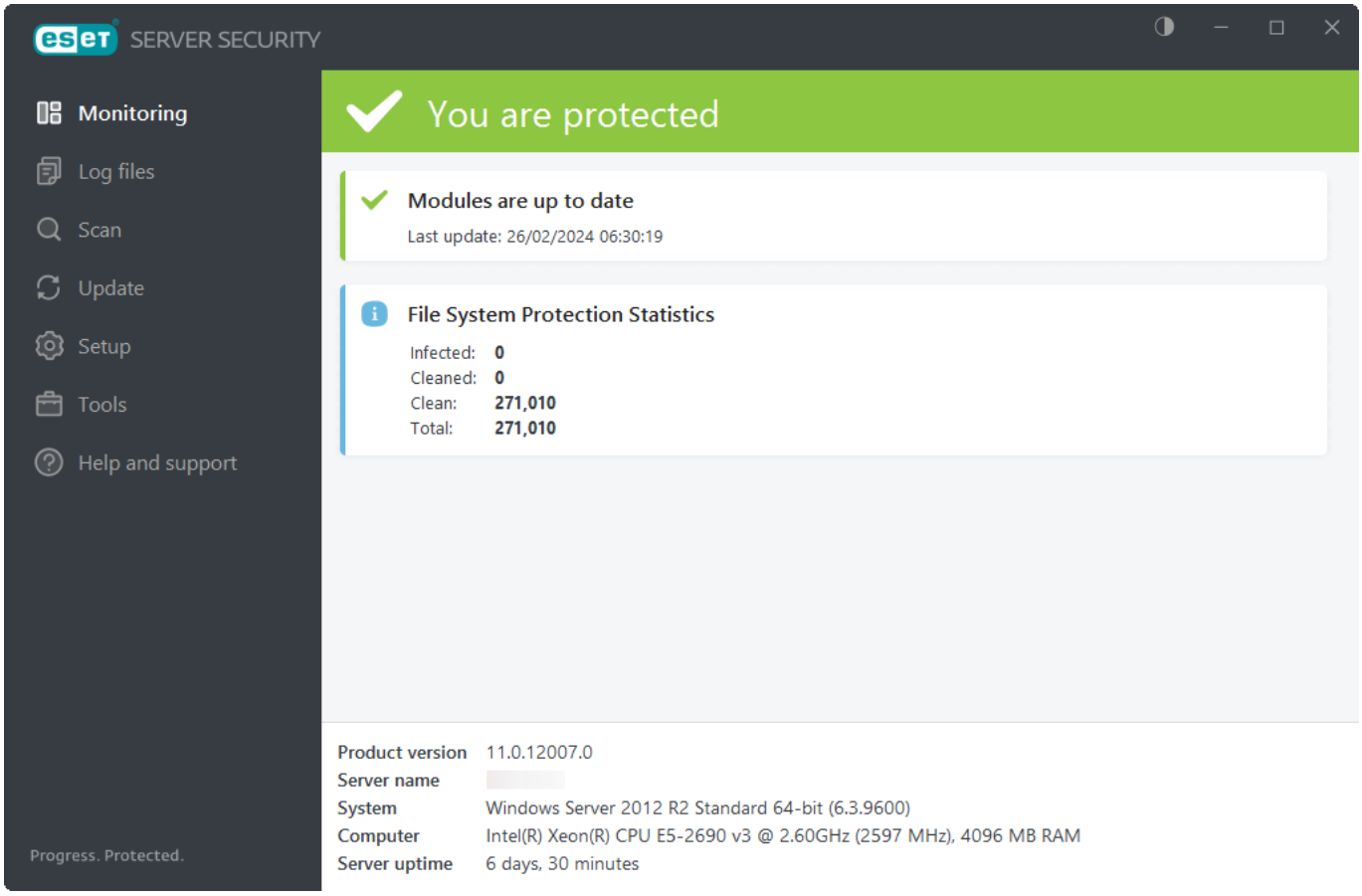
Lo stato di protezione visualizzato nella schermata **Monitoraggio** fornisce all'utente informazioni sull'attuale livello di protezione. Il riepilogo include informazioni dettagliate sul sistema in uso.

Lo stato **La protezione è attiva** (di colore verde) indica che è garantito il livello massimo di protezione.

L'icona di colore rosso indica la presenza di problemi critici ovvero che non è garantito il livello massimo di protezione della sistema. I dettagli del messaggio di errore dovrebbero fornire una migliore comprensione dello stato attuale.

Qualora non si riuscisse a risolvere un problema, effettuare una ricerca nella Knowledge Base di ESET. Nel caso in cui sia necessaria ulteriore assistenza, è possibile selezionare Invia richiesta di assistenza. Il Supporto tecnico di ESET risponderà rapidamente alle domande degli utenti e li aiuterà a trovare una soluzione ai loro problemi. Per un elenco completo degli stati, aprire **Configurazione avanzata** (**F5**) > **Notifiche** > Stati dell'applicazione e fare clic su **Modifica**.

L'icona di colore arancione indica che il prodotto ESET richiede attenzione per un problema non critico.



Ai moduli che funzionano correttamente viene assegnato un segno di spunta di colore verde. Ai moduli che non funzionano correttamente viene assegnato 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.

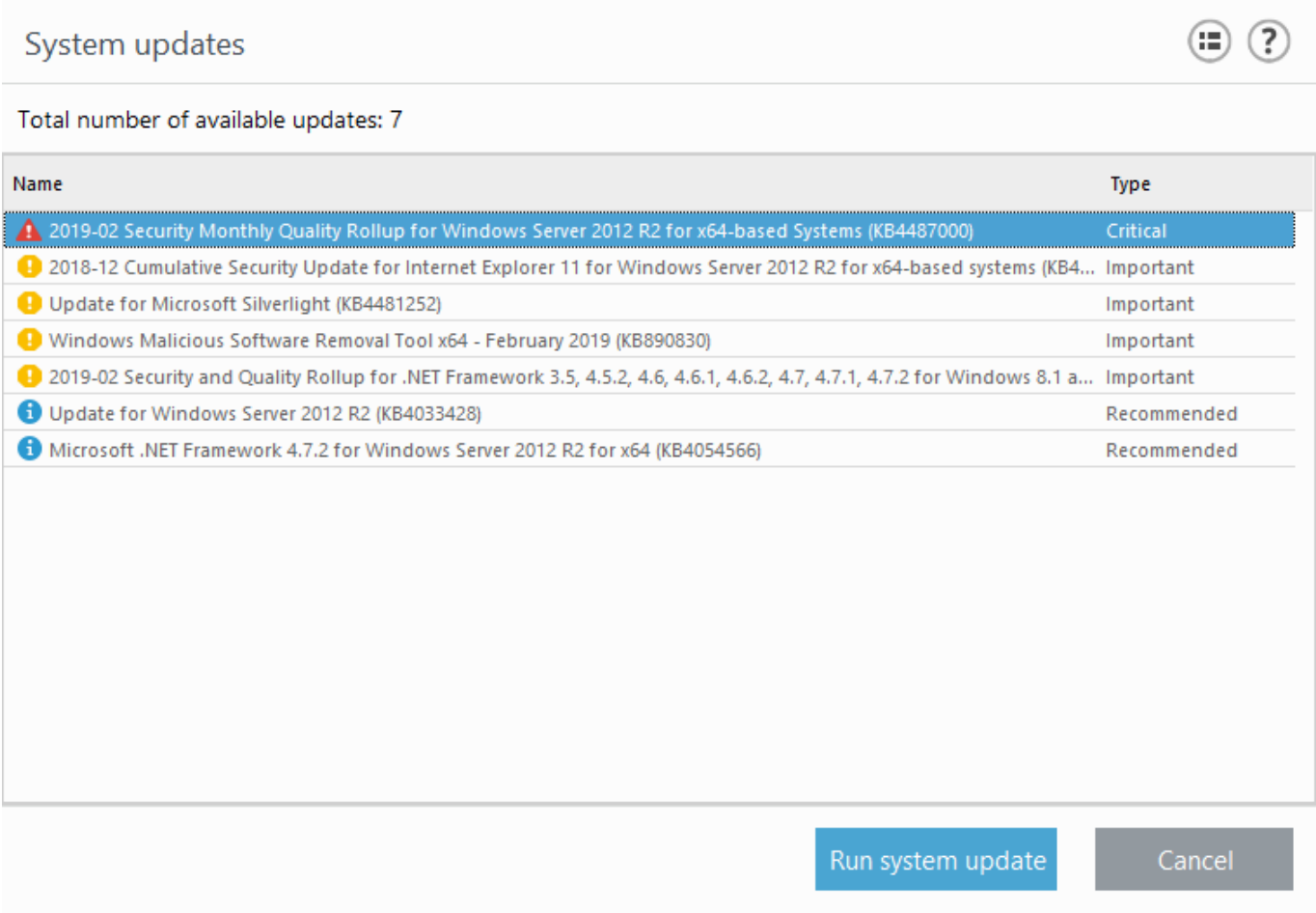
La pagina Monitoraggio contiene anche informazioni sul sistema in uso, tra cui:

- **Versione del prodotto**: numero della versione di ESET Server Security.
- **Nome del server**: nome host della macchina o FQDN.
- **Sistema**: informazioni sul sistema operativo.
- **Computer**: informazioni sull'hardware.
- **Tempo di disponibilità del server**: consente di visualizzare il tempo in cui il sistema è funzionante e in esecuzione ed è fondamentalmente la funzione opposta del tempo di inattività.

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

Aggiornamento Windows disponibile

Nella finestra Aggiornamenti del sistema è visualizzato un elenco di aggiornamenti disponibili per il download e l'installazione. Il livello di priorità compare accanto al nome dell'aggiornamento. Fare clic con il pulsante destro del mouse su qualsiasi riga dell'aggiornamento, quindi selezionare **Ulteriori informazioni** per visualizzare una finestra contenente informazioni aggiuntive:



Fare clic su **Esegui aggiornamento di sistema** per aprire la finestra **Windows Update** e procedere con gli aggiornamenti di sistema.

Isolamento rete

ESET Server Security consente di bloccare la connessione di rete del server con l'isolamento della rete. In alcuni scenari estremi, potrebbe essere necessario isolare un server dalla rete come misura preventiva. Ad esempio, se si scopre che il server è infetto a causa di un attacco malware o che la macchina è altrimenti compromessa.

Attivando l'isolamento di rete, tutto il traffico di rete viene bloccato eccetto le seguenti opzioni:

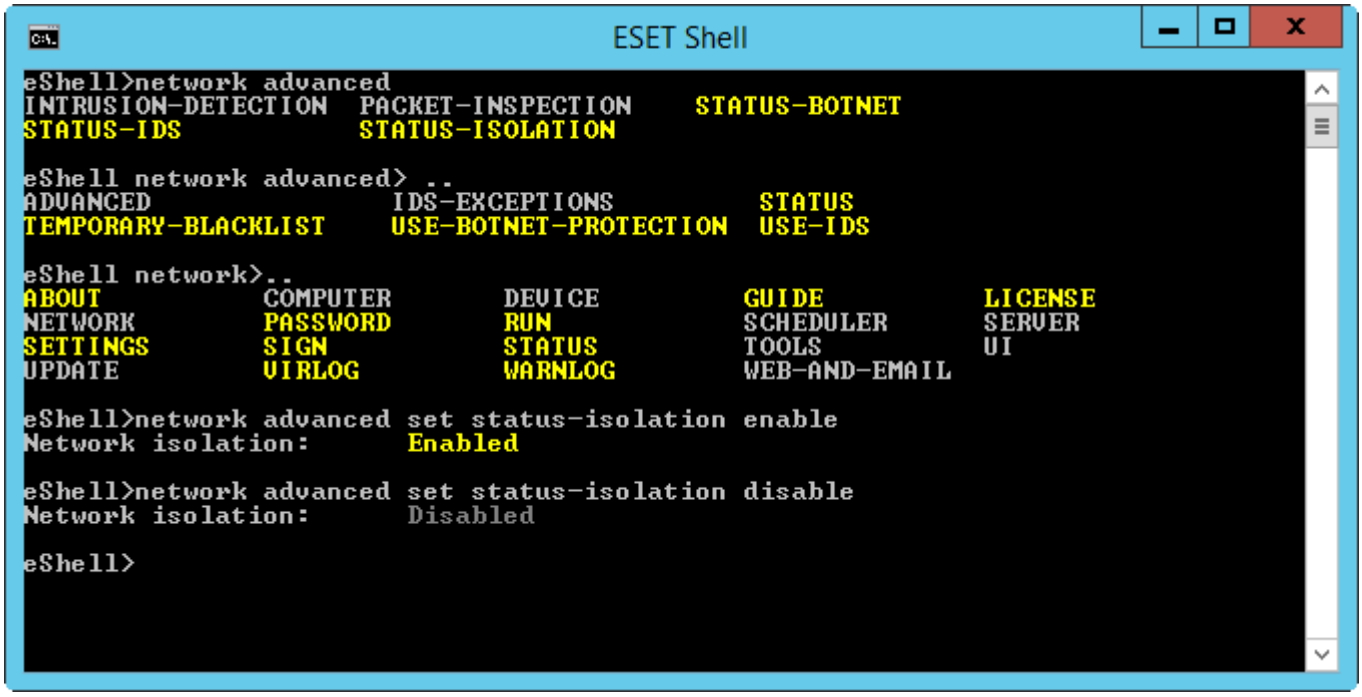
- La connettività al domain controller rimane
- ESET Server Security può ancora comunicare
- Se presenti, ESET Management Agent e ESET Inspect On-Prem Connector possono comunicare sulla rete

Attivare e disattivare l'isolamento di rete utilizzando il comando eShell o l'attività client ESET PROTECT.

eShell

In modalità interattiva:

- Attiva isolamento rete: `network advanced set status-isolation enable`
- Disattiva isolamento rete: `network advanced set status-isolation disable`



In alternativa, è possibile creare ed eseguire un file batch utilizzando la Modalità batch/script.

ESET PROTECT

- Attivare l'isolamento di rete tramite l'attività client.
- Disattivare l'isolamento di rete tramite l'attività client.

Quando l’isolamento della rete è attivato, lo stato di ESET Server Security diventa rosso e viene visualizzato il messaggio **Accesso alla rete bloccato**.

File di rapporto

I file di rapporto contengono informazioni sugli eventi di programma importanti che si sono verificati e forniscono una panoramica dei risultati del controllo, delle minacce rilevate e così via. 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 Server Security, nonché archiviare i file dei rapporti utilizzando la funzione di esportazione.

Scegliere il tipo di rapporto appropriato nel menu a discesa. Sono disponibili i rapporti seguenti:

Rilevamenti

Nel rapporto delle minacce sono contenute informazioni dettagliate sulle infiltrazioni rilevate dai moduli ESET Server 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 i dettagli in una finestra separata. Se richiesto, è possibile creare un'esclusione di rilevamento: fare clic con il pulsante destro del mouse su un record di rapporto (rilevamento) e selezionare **Crea esclusione**. Questa operazione consentirà di aprire la procedura

guidata di esclusione con criteri predefiniti. Se è presente il nome di un rilevamento accanto a un file escluso, ciò significa che il file viene escluso solo per il rilevamento specificato. Se il file si infetta successivamente con altri malware, verrà rilevato.

Eventi

Tutte le azioni importanti eseguite da ESET Server Security vengono registrate nel rapporto eventi. Il rapporto eventi contiene informazioni sugli eventi e gli 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 sono 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.

File bloccati

Contiene i record dei file che sono stati bloccati e ai quali non è possibile accedere. Nel protocollo è possibile visualizzare il motivo e il modulo di origine che ha bloccato il file, oltre all'applicazione e all'utente che hanno eseguito il file.

File inviati

Contiene i record della protezione basata sul cloud dei file, ESET LiveGuard Advanced e ESET LiveGrid®.

Rapporti di controllo

Contiene i record delle modifiche relative alla configurazione o allo stato della protezione e crea snapshot per eventuali consultazioni future. Fare clic con il pulsante destro del mouse su un record qualsiasi appartenente al tipo Modifiche impostazioni e selezionare Mostra modifiche dal menu contestuale per visualizzare informazioni dettagliate sulla modifica eseguita. Se si desidera ripristinare l'impostazione precedente, selezionare Ripristina. È anche possibile utilizzare Elimina tutto per rimuovere i record dei rapporti. Se si desidera attivare la Registrazione dei controlli, accedere a **Configurazione avanzata** > **Strumenti** > **File di rapporto** > Rapporto di 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.

Protezione rete

Contiene i record dei file che sono stati bloccati dalla Protezione botnet e IDS (Protezione attacchi di rete).

Siti Web filtrati

Elenco di siti web bloccati dalla Protezione accesso Web . In questi rapporti è visualizzata l'ora, l'URL, l'utente e l'applicazione che hanno aperto una connessione a un sito Web specifico.

Controllo dispositivi

Contiene record relativi ai supporti rimovibili o ai dispositivi collegati al computer. Nel file di rapporto saranno registrati solo i dispositivi con 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, al numero di serie, al nome del fornitore e alle dimensioni del supporto (laddove disponibili).

Gestione delle vulnerabilità e delle patch

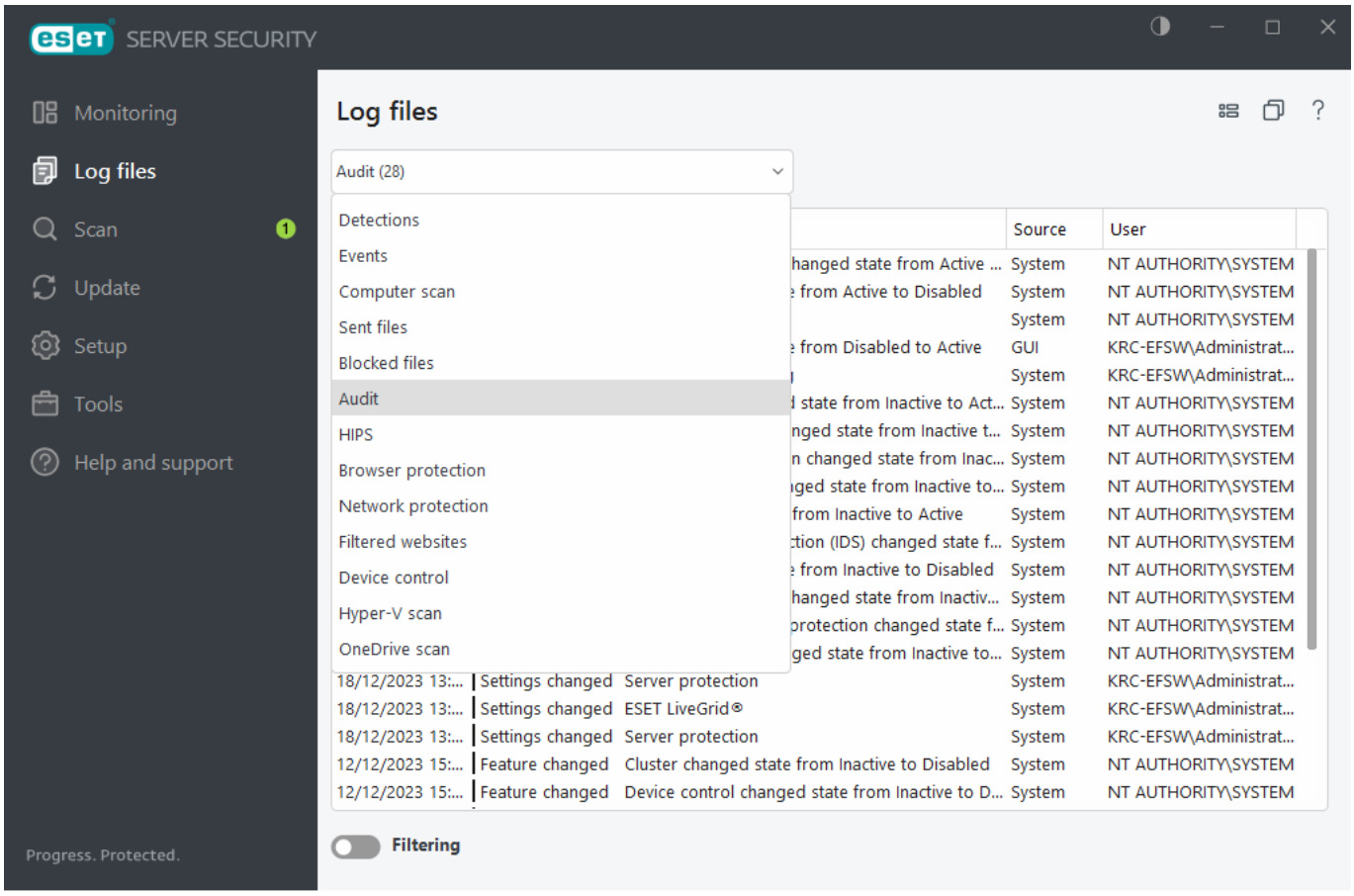
Contiene un elenco dei risultati del controllo relativi ad app di terze parti.

Controllo Hyper-V

Contiene un elenco di risultati del controllo Hyper-V. Fare doppio clic su una voce qualsiasi per visualizzare i dettagli del rispettivo controllo.

Controllo OneDrive

Contiene un elenco dei risultati del controllo OneDrive.



Il menu contestuale (tasto destro) consente di scegliere un’azione con il record del rapporto selezionato:

Azione	Utilizzo	Tasto di scelta rapida	Vedere anche
Mostra	Consente di visualizzare informazioni più dettagliate relative al rapporto selezionato in una nuova finestra (funzione uguale all'esecuzione di un doppio clic).		
Filtra gli stessi record	Questa opzione attiva il filtraggio dei rapporti, consentendo di visualizzare esclusivamente i record dello stesso tipo di quello selezionato.	Ctrl + Maiusc + F	

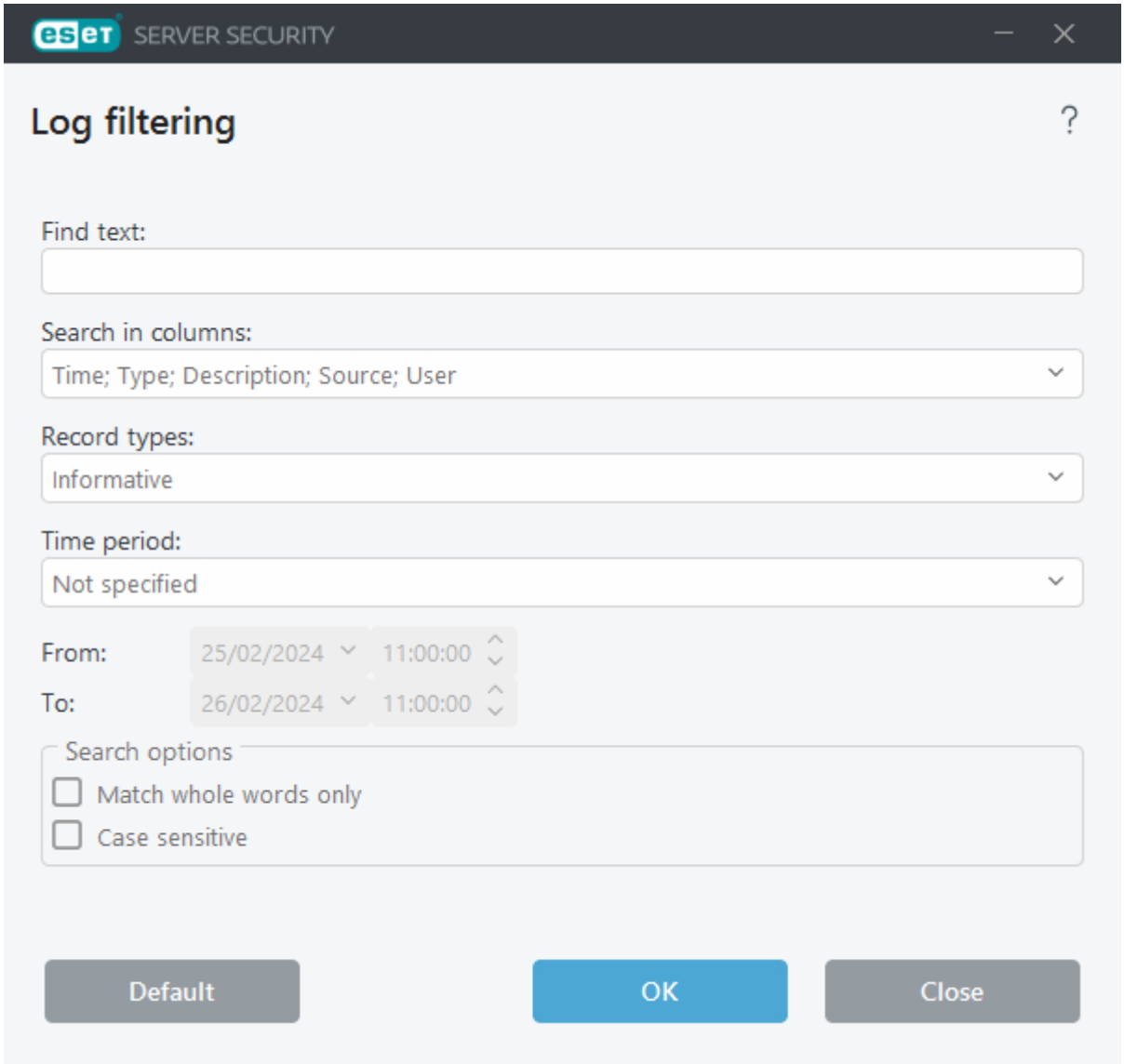
Azione	Utilizzo	Tasto di scelta rapida	Vedere anche
Filtra...	Dopo aver selezionato questa opzione, la finestra Filtraggio rapporti consentirà all'utente di definire i criteri di filtraggio per specifiche voci dei rapporti.		Filtraggio rapporti
Attiva filtro	Consente di attivare le impostazioni del filtro. In caso di prima attivazione del filtraggio, è necessario definirne le impostazioni.		
Disattiva filtro	Consente di disattivare il filtraggio (funzione simile alla selezione del pulsante nella parte inferiore).		
Copia	Consente di copiare le informazioni dei record selezionati/evidenziati negli Appunti.	Ctrl + C	
Copia tutto	Consente di copiare le informazioni da tutti i record presenti nella finestra.		
Elimina	Consente di eliminare i record selezionati/evidenziati. Per poter eseguire questa operazione è necessario disporre dei privilegi amministrativi.	Del	
Rimuovi tutto	Consente di eliminare tutti i record presenti nella finestra. Per poter eseguire questa operazione è necessario disporre dei privilegi amministrativi.		
Esporta...	Consente di esportare le informazioni del(i) record selezionato(i)/evidenziato(i) in un file XML.		
Esporta tutto...	Consente di esportare tutte le informazioni presenti nella finestra in un file XML.		
Trova...	Apre la finestra Trova nel rapporto e consente all'utente di definire i criteri di ricerca. È possibile utilizzare la funzione Trova per individuare un record specifico anche nel caso in cui il filtraggio sia ancora attivo.	Ctrl + F	Trova nel rapporto
Trova successivo	Trova l'occorrenza successiva dei criteri di ricerca definiti dall'utente.	F3	
Trova precedente	Trova l'occorrenza precedente.	Maiusc + F3	
Crea esclusione	Per escludere gli oggetti dalla pulizia utilizzando il nome del rilevamento, il percorso o il relativo hash.		Crea esclusione

Filtraggio rapporti

La funzione Filtraggio rapporti aiuta l'utente a trovare le informazioni di cui ha bisogno, soprattutto in presenza di numerosi record. Consente infatti di ridurre il numero di record dei rapporti, ad esempio, se si sta ricercando un tipo specifico di evento, stato o periodo.

L'utente può filtrare i record dei rapporti specificando opzioni di ricerca specifiche. In questo caso, nella finestra File di rapporto verranno visualizzati solo i record rilevanti (in base a tali opzioni di ricerca).

Immettere la parola chiave da ricercare nel campo **Trova testo**. Utilizzare il menu a discesa **Cerca nelle colonne** per perfezionare la ricerca. Scegliere uno o più record nel menu a discesa **Tipi di rapporto del record**. Definire il **Periodo** a partire dal quale si desiderano visualizzare i risultati. È anche possibile utilizzare ulteriori opzioni di ricerca, ad esempio **Solo parole intere** o **Maiuscole/minuscole**.



Trova testo

Digitare una stringa (parola o parte di una parola). Verranno trovati solo i record contenenti tale stringa. Gli altri record verranno omessi.

Cerca nelle colonne

Selezionare le colonne in cui eseguire la ricerca. È possibile selezionare una o più colonne da utilizzare per la ricerca.

Tipi di record

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

- **Diagnostica**: registra le informazioni necessarie ai fini dell'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativo**: registra i messaggi informativi, compresi quelli relativi agli aggiornamenti riusciti, e tutti i record indicati in precedenza.
- **Allarmi**: registra errori critici e messaggi di allarme.

- **Errori**: verranno registrati errori quali "Errore durante il download del file" ed errori critici.
- **Critico**: registra solo gli errori critici.

Periodo

Definire il periodo di tempo a partire dal quale si desiderano visualizzare i risultati.

- Non specificato (impostazione predefinita): la ricerca non viene eseguita nel periodo indicato ma nell'intero rapporto.
- Ultimo giorno
- Ultima settimana
- Ultimo mese
- Periodo: è possibile specificare il periodo di tempo esatto (Da: e A:) per filtrare esclusivamente i record appartenenti a uno specifico periodo di tempo.

Solo parole intere

Usare questa casella di controllo per ricercare specifiche parole intere e ottenere risultati più precisi.

Maiuscole/minuscole

Abilitare questa opzione se è importante utilizzare lettere maiuscole o minuscole durante il filtraggio. Durante la configurazione delle opzioni di filtraggio/ricerca, fare clic su **OK** per visualizzare i record dei rapporti filtrati o su **Trova** per avviare la ricerca.

La ricerca dei file di rapporto viene eseguita dall'alto verso il basso, partendo dalla posizione corrente, ovvero dal record evidenziato. La ricerca si interrompe quando viene trovato il primo record corrispondente. Premere **F3** per cercare il record successivo oppure fare clic con il pulsante destro del mouse e selezionare **Trova** per perfezionare le opzioni di ricerca.

Controllo

Il Controllo su richiesta rappresenta un componente importante di ESET Server Security. Viene utilizzato per eseguire il controllo di file e di cartelle sul computer in uso. Per garantire la sicurezza della rete, è essenziale che i controlli del computer non vengano eseguiti semplicemente quando si sospetta un'infezione ma periodicamente, nell'ambito delle misure di sicurezza abituali.

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 in caso di infiltrazione di una minaccia se la protezione file system in tempo reale è disattivata, il motore di rilevamento non è stato aggiornato o il file non è stato rilevato nel momento in cui è stato salvato sul disco.

Selezionare i controlli su richiesta disponibili per ESET Server Security:

Controllo archiviazione

Consente di eseguire il controllo di tutte le cartelle condivise sul server locale. Se il Controllo archiviazione non è

disponibile, non sono presenti cartelle condivise sul server.

Controllo computer

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

> È consigliabile eseguire un controllo del computer almeno una volta al mese. Il controllo può essere configurato come attività pianificata.

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 Controllo personalizzato consente di configurare in dettaglio i parametri di controllo. Le configurazioni possono essere salvate su profili di controllo definiti dall'utente, che possono risultare utili se il controllo viene eseguito ripetutamente utilizzando gli stessi parametri.

Controllo supporti rimovibili

Simile al Controllo intelligente: consente di lanciare velocemente un controllo dei supporti rimovibili (come ad esempio CD/DVD/USB) collegati al computer. Questa opzione può rivelarsi utile in caso di connessione di una memoria USB a un computer e nel caso in cui si desideri ricercare malware e altre potenziali minacce. Questo tipo di controllo può anche essere avviato facendo clic su Controllo personalizzato, quindi selezionando Supporti rimovibili nel menu a discesa Destinazioni di controllo e facendo clic su Controllo.

Controllo Hyper-V

Questa opzione è visibile nel menu solo se Hyper-V Manager è installato sul server su cui è in esecuzione ESET Server Security. Hyper-V consente il controllo dei dischi delle macchine virtuali (VM) sul server Microsoft Hyper-V senza che sia necessario installare alcun "Agente" sulle macchine.

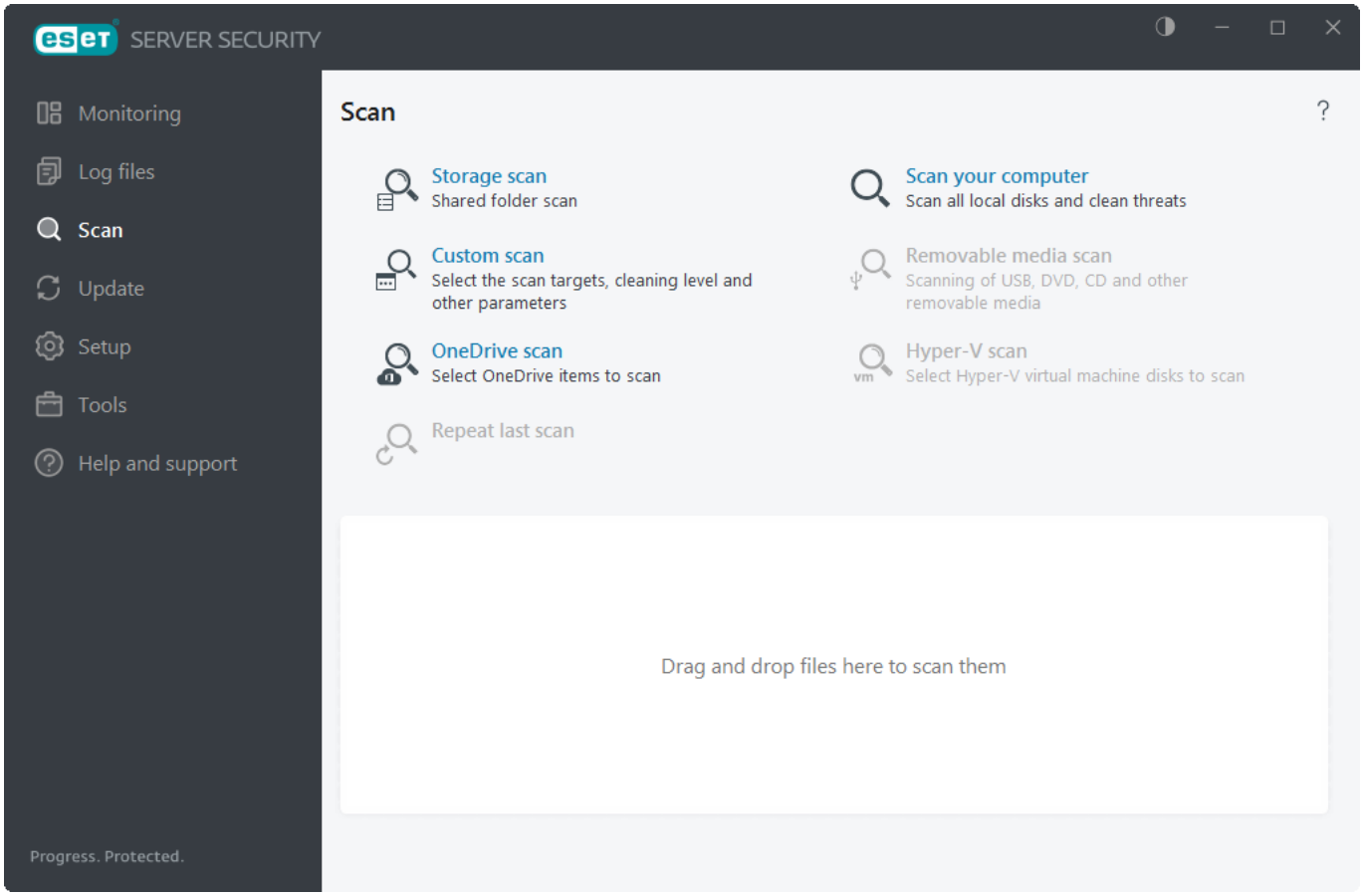
Controllo OneDrive

Consente di controllare i file dell’utente presenti nell’archivio sul cloud OneDrive.

Ripeti ultimo controllo

Ripete il funzionamento dell'ultimo controllo utilizzando esattamente le stesse impostazioni.

> La funzione Ripeti ultimo controllo non è disponibile se è presente il Controllo database su richiesta.



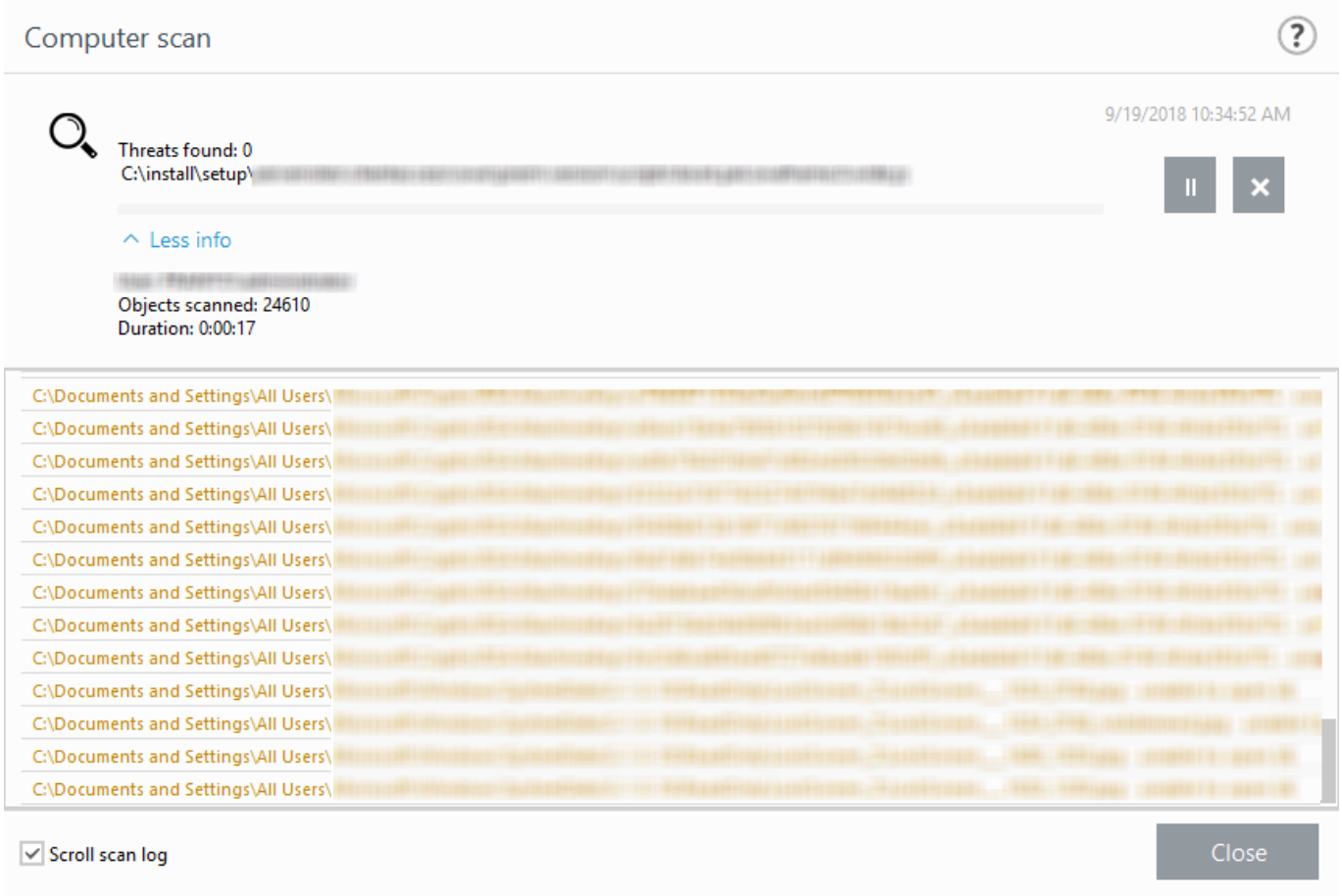
È possibile utilizzare le opzioni e visualizzare ulteriori informazioni sugli stati del controllo:

Trascina file	È anche possibile trascinare i file nella finestra del controllo ESET Server Security. I file saranno controllati immediatamente alla ricerca di virus.
Ignora/Ignora tutto	Consente di ignorare determinati messaggi.
Stati del controllo	Mostra lo stato del controllo iniziale. Questo controllo è stato completato o interrotto dall'utente.
Mostra rapporto	Consente di visualizzare informazioni più dettagliate.
Ulteriori informazioni	Durante un controllo consente di visualizzare alcuni dettagli, tra cui l'Utente che ha eseguito il controllo, il numero di Oggetti controllati e la **Durata** del controllo.
Apri finestre del 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.

Finestra del controllo e rapporto del controllo

Nella finestra del controllo vengono visualizzati gli oggetti attualmente controllati, tra cui la posizione, il numero di eventuali minacce rilevate, il numero di oggetti controllati e la durata del controllo. Nella parte inferiore della finestra è presente un rapporto in cui è indicato il numero di versione del motore di rilevamento, la data e l'ora di avvio del controllo e la selezione delle destinazioni.

Quando è in corso un controllo, è possibile selezionare **Sospendi** per interromperlo provvisoriamente. Quando il processo di controllo è sospeso, è disponibile l'opzione Riprendi.

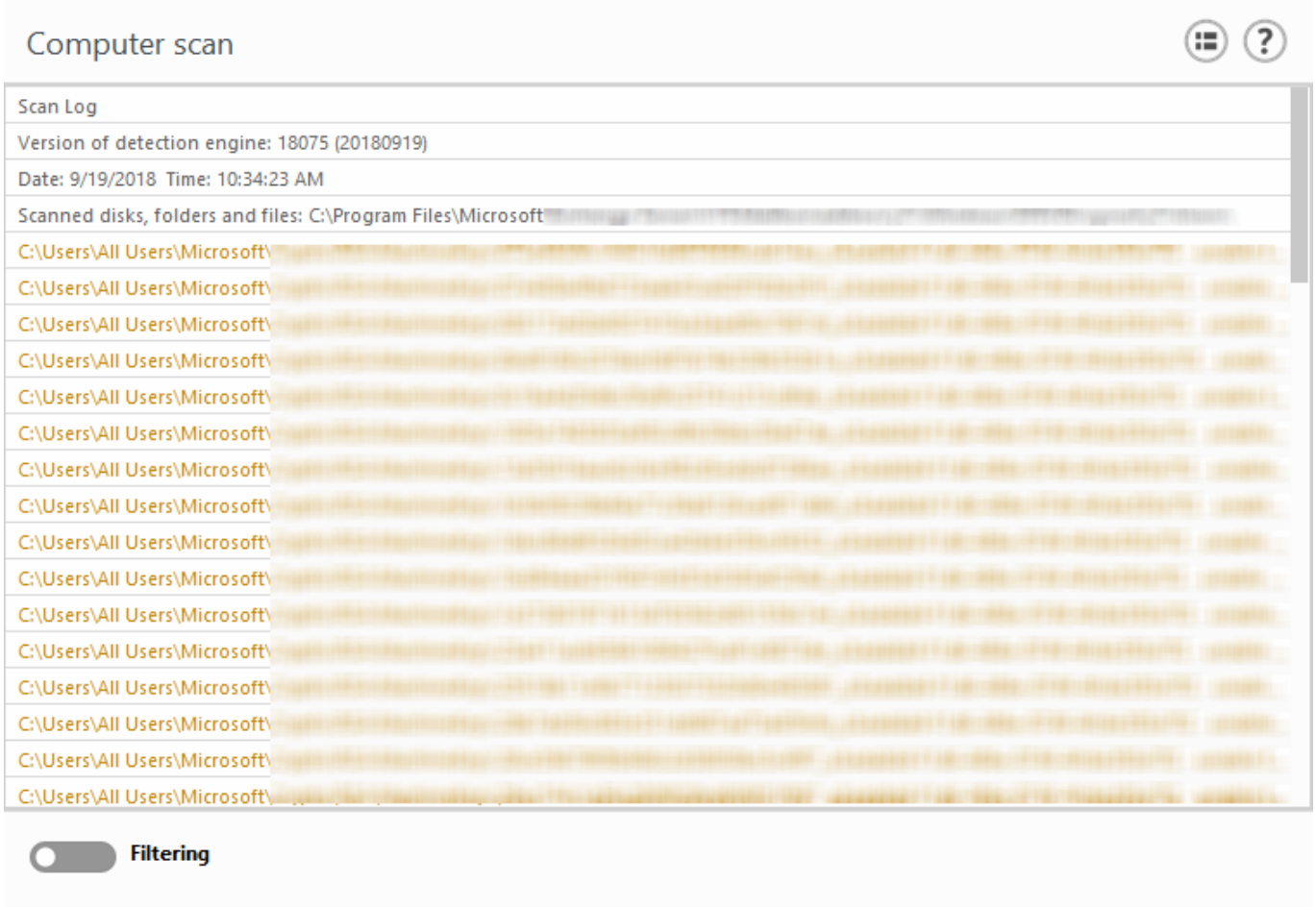


Scorri rapporto di controllo

Lasciare attivata questa opzione per scorrere automaticamente i rapporti meno recenti e visualizzare i rapporti attivi nella finestra File di rapporto.

> 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.

Al termine del controllo, verrà visualizzato il rapporto del controllo contenente tutte le informazioni importanti relative al controllo eseguito.



Fare clic sull'icona del pulsante **Filtraggio** per aprire la finestra Filtraggio rapporti in cui è possibile definire i criteri di filtraggio o di ricerca. Per visualizzare il menu contestuale, fare clic con il pulsante destro del mouse su un elemento specifico del rapporto:

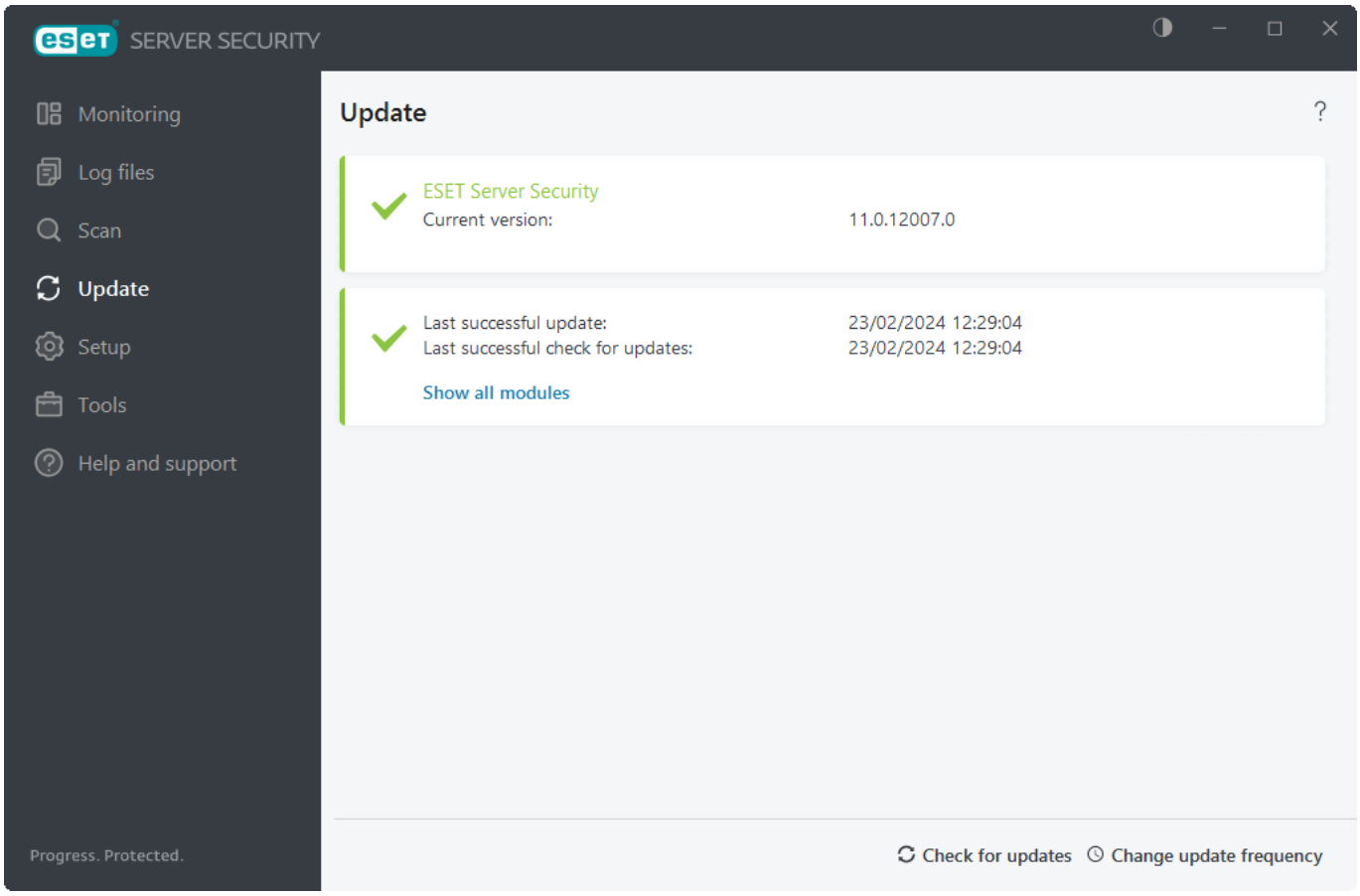
Azione	Utilizzo	Tasto di scelta rapida	Vedere anche
Filtra gli stessi record	Questa opzione attiva il filtraggio dei rapporti, consentendo di visualizzare esclusivamente i record dello stesso tipo di quello selezionato.	Ctrl + Maiusc + F	
Filtra...	Dopo aver selezionato questa opzione, la finestra Filtraggio rapporti consentirà all'utente di definire i criteri di filtraggio per specifiche voci dei rapporti.		Filtraggio rapporti
Attiva filtro	Consente di attivare le impostazioni del filtro. In caso di prima attivazione del filtraggio, è necessario definirne le impostazioni.		
Disattiva filtro	Consente di disattivare il filtraggio (funzione simile alla selezione del pulsante nella parte inferiore).		
Copia	Consente di copiare le informazioni dei record selezionati/evidenziati negli Appunti.	Ctrl + C	
Copia tutto	Consente di copiare le informazioni da tutti i record presenti nella finestra.		
Esporta...	Consente di esportare le informazioni del(i) record selezionato(i)/evidenziato(i) in un file XML.		
Esporta tutto...	Consente di esportare tutte le informazioni presenti nella finestra in un file XML.		

Aggiornamento

Nella sezione Aggiornamento è possibile visualizzare lo stato corrente di aggiornamento di ESET Server Security, compresa la data e l'ora dell'ultimo aggiornamento eseguito correttamente. L'aggiornamento periodico di ESET Server Security rappresenta il metodo migliore per preservare il livello massimo di protezione del server.

Il modulo di aggiornamento garantisce il costante aggiornamento del programma in base a due modalità: attraverso l'aggiornamento del motore di rilevamento e attraverso l'aggiornamento dei componenti del sistema. L'aggiornamento del motore di rilevamento e dei componenti del programma costituisce un aspetto importante per garantire una protezione completa contro codici dannosi.

> Se ancora non è stata inserita la Chiave di licenza, non sarà possibile ricevere gli aggiornamenti e verrà chiesto di attivare il prodotto. Per eseguire tale operazione, accedere a **Guida e supporto tecnico** > **Attiva prodotto**.



- **Versione corrente**: versione della build di ESET Server Security.

- **Ultimo aggiornamento eseguito correttamente**: data dell'ultimo aggiornamento. Accertarsi che la data sia recente: ciò significa che i moduli sono aggiornati.

- **Ultima ricerca di aggiornamenti eseguita correttamente**: data dell'ultimo tentativo di aggiornamento dei moduli.

- **Mostra tutti i moduli**: consente di aprire l'elenco dei moduli installati.

- **Ricerca aggiornamenti**: l'aggiornamento dei moduli costituisce un aspetto importante per garantire il mantenimento di una protezione completa contro codici dannosi.

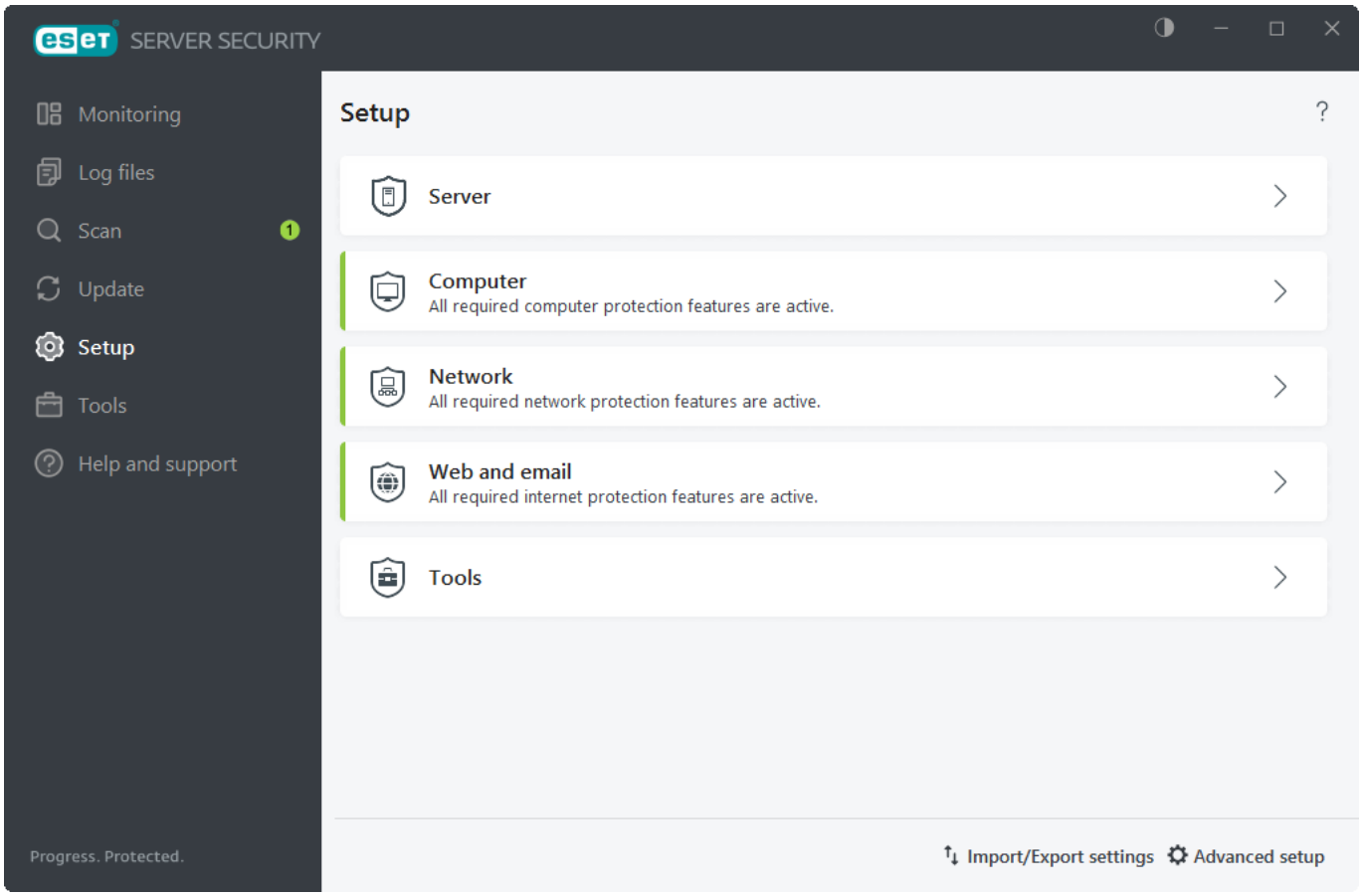
- **Modifica della frequenza degli aggiornamenti**: è possibile modificare la frequenza della pianificazione attività Aggiornamento automatico periodico.

> Le opzioni del server proxy potrebbero essere diverse in base ai vari profili di aggiornamento. In questo caso, configurare i diversi profili di aggiornamento in **Configurazione avanzata** (**F5**) facendo clic su **Aggiornamento** > Profilo.

Configurazione

La finestra del menu Configurazione contiene le seguenti sezioni:

- Server
- Computer
- Rete
- Web e e-mail
- Strumenti - Registrazione diagnostica



Per disattivare temporaneamente i singoli moduli, fare clic sulla barra di scorrimento verde accanto al modulo desiderato. Questo potrebbe ridurre il livello di protezione del server.

Per riattivare la protezione di un componente disattivato, fare clic sulla barra di scorrimento rossa accanto al modulo appropriato. Il componente ritorna allo stato attivo.

Per accedere alle impostazioni dettagliate di un particolare componente di protezione, fare clic sull'icona a forma di ingranaggio ⚙.

Importa/esporta impostazioni

Consente di caricare i parametri di configurazione mediante un file di configurazione *.xml* o salvare i parametri di configurazione correnti su un file di configurazione.

Configurazione avanzata

Impostazioni avanzate di configurazione e opzioni preferite dall'utente. Per accedere alla schermata **Configurazione avanzata** da qualsiasi percorso, premere **F5**.

Server

Sarà possibile visualizzare un elenco di componenti da attivare/disattivare utilizzando la barra di scorrimento. Per configurare le impostazioni di uno specifico elemento, fare clic sull'icona a forma di ingranaggio ⚙.

Esclusioni automatiche

Identifica le applicazioni e i file del sistema operativo del server critici e li aggiunge automaticamente all'elenco di esclusioni. Questa funzionalità riduce al minimo il rischio di potenziali conflitti e migliora le prestazioni generali del server quando è in esecuzione il software di rilevamento minacce.

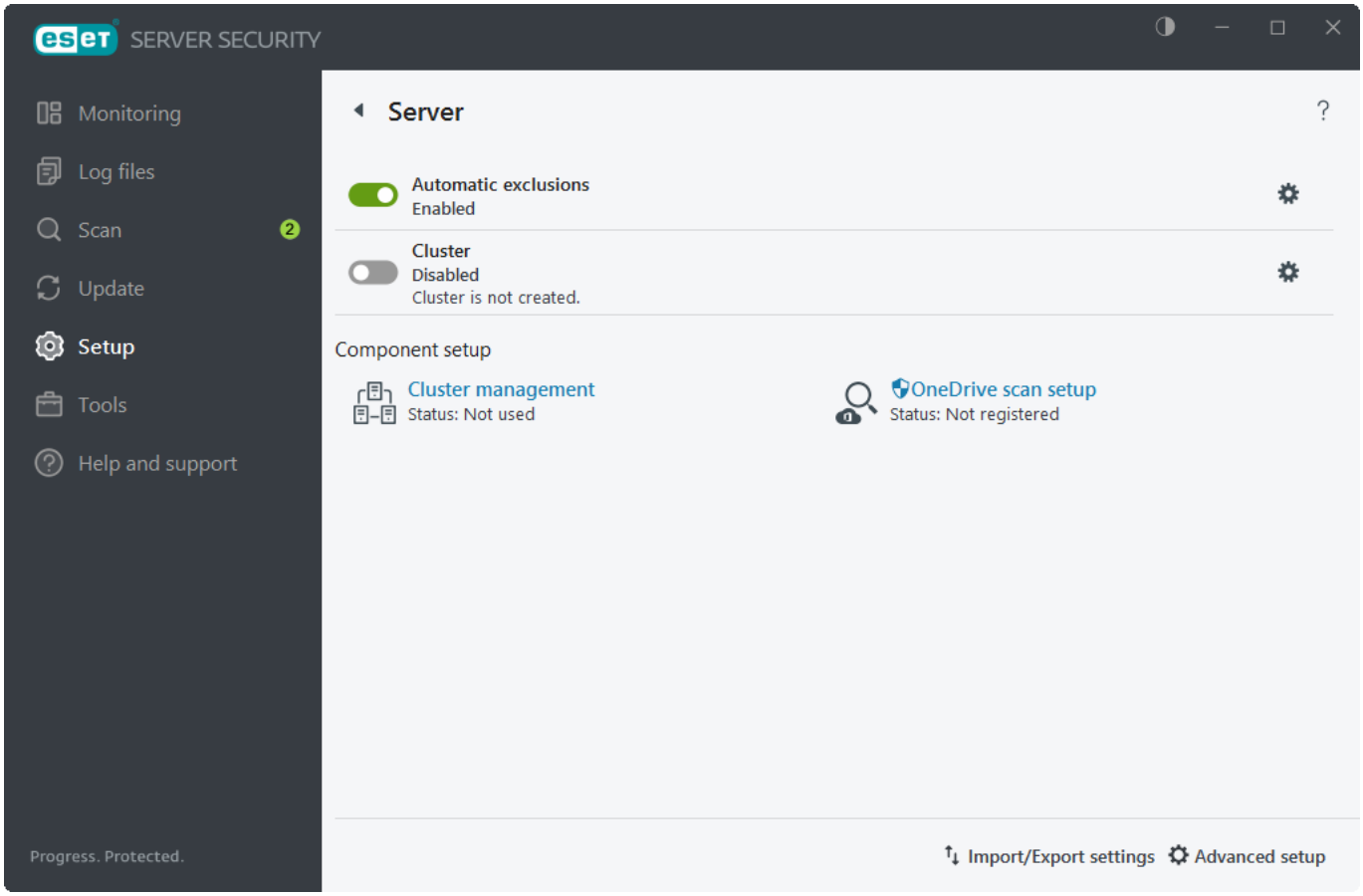
Configurazione dei componenti

Gestione del cluster

È possibile configurare e attivare il cluster ESET.

Configurazione controllo OneDrive

È possibile registrare e annullare la registrazione dell'applicazione scanner ESET OneDrive da Microsoft OneDrive.



Cluster

ESET Cluster è un'infrastruttura di comunicazione P2P della gamma di prodotti ESET per Microsoft Windows Server.

Questa infrastruttura consente ai prodotti server ESET di comunicare tra loro e di scambiare dati quali configurazione e notifiche e può i dati necessari per il corretto funzionamento di un gruppo di istanze del prodotto. Un esempio potrebbe essere un gruppo di nodi in un cluster di failover Windows o cluster Network Load Balancing (NLB) con i prodotti ESET installati dove è richiesta la stessa configurazione del prodotto nell'intero cluster. ESET Cluster assicura questo livello di coerenza tra le istanze.

> Le impostazioni dell'interfaccia utente delle Attività pianificate non sono sincronizzate tra i nodi di ESET Cluster. Questa procedura è voluta.

> La creazione di ESET Cluster tra ESET Server Security ed ESET File Security for Linux non è supportata.

Per configurare ESET Cluster, sono disponibili due metodi di aggiunta dei nodi:

- **Rilevamento automatico** – Se si dispone di un cluster di failover Windows o un cluster NLB, l'opzione Rilevamento automatico consente di aggiungerne automaticamente i nodi membri a ESET Cluster.

- **Sfoglia**: è possibile aggiungere manualmente i nodi digitando i nomi del server (membri dello stesso gruppo di lavoro o membri dello stesso dominio).

In caso di rilascio di un'e-mail dalla quarantena, ESET Server Security ignora l'intestazione MIME `To:` in quanto è un facile oggetto di attacchi di spoofing. Utilizza invece le informazioni del mittente originario dal comando `RCPT TO:` acquisito durante la connessione SMTP. Ciò garantisce la ricezione del messaggio rilasciato dalla quarantena da parte del destinatario corretto dell'e-mail.

Dopo aver aggiunto i nodi in ESET Cluster, è necessario installare ESET Server Security su ciascuno di essi. Questa operazione viene eseguita automaticamente durante la configurazione di ESET Cluster. Le credenziali richieste per l'installazione remota di ESET Server Security su altri nodi cluster sono le seguenti:

- **Scenario dominio**: credenziali amministratore del dominio.
- **Scenario gruppo di lavoro**: è necessario accertarsi che tutti i nodi utilizzino le stesse credenziali dell'account amministratore locale.

In ESET Cluster è inoltre possibile utilizzare una combinazione di nodi aggiunti automaticamente come membri di un cluster di failover Windows/cluster NLB esistente e di nodi aggiunti manualmente (a condizione che si trovino nello stesso dominio).

Non è possibile combinare i nodi dei domini con i nodi dei gruppi di lavoro.

Un altro requisito per l'utilizzo di ESET Cluster consiste nella necessità di attivare **Condivisione file e stampanti** in Windows Firewall prima dell'esecuzione del push ESET Server Security sui nodi di ESET Cluster.

In qualsiasi momento, è possibile aggiungere nuovi nodi a un ESET Cluster esistente eseguendo la Procedura guidata cluster.

Importa certificati

I certificati vengono utilizzati per garantire un'autenticazione efficace da macchina a macchina quando viene utilizzato il protocollo HTTPS. Per ogni ESET Cluster può essere presente una gerarchia dei certificati indipendente. La gerarchia ha un certificato radice e una serie di certificati dei nodi firmati dal certificato radice. La chiave privata del certificato radice viene eliminata dopo che tutti i certificati dei nodi sono stati creati. Quando si aggiunge un nuovo nodo al cluster, viene creata una nuova gerarchia dei certificati. Accedere alla cartella contenente i certificati (generati durante l'utilizzo della Procedura guidata cluster). Selezionare il file del certificato e fare clic su **Apri**.

Elimina cluster

ESET Cluster può essere eliminato. Ciascun nodo scriverà un record nel relativo rapporto eventi sull'ESET Cluster eliminato. Successivamente, tutte le regole del firewall ESET verranno rimosse da Windows Firewall. I primi nodi ritorneranno nello stato precedente e potranno essere nuovamente utilizzati in un'altra istanza di ESET Cluster, se necessario.

Procedura guidata cluster - Seleziona nodi

La prima operazione da eseguire per configurare ESET Cluster consiste nell'aggiunta di nodi. Per aggiungere nodi, è possibile utilizzare l'opzione **Rilevamento automatico** oppure **Sfoglia**. In alternativa, è possibile digitare il nome del server nella casella di testo e fare clic sul pulsante **Aggiungi**.

Rilevamento automatico

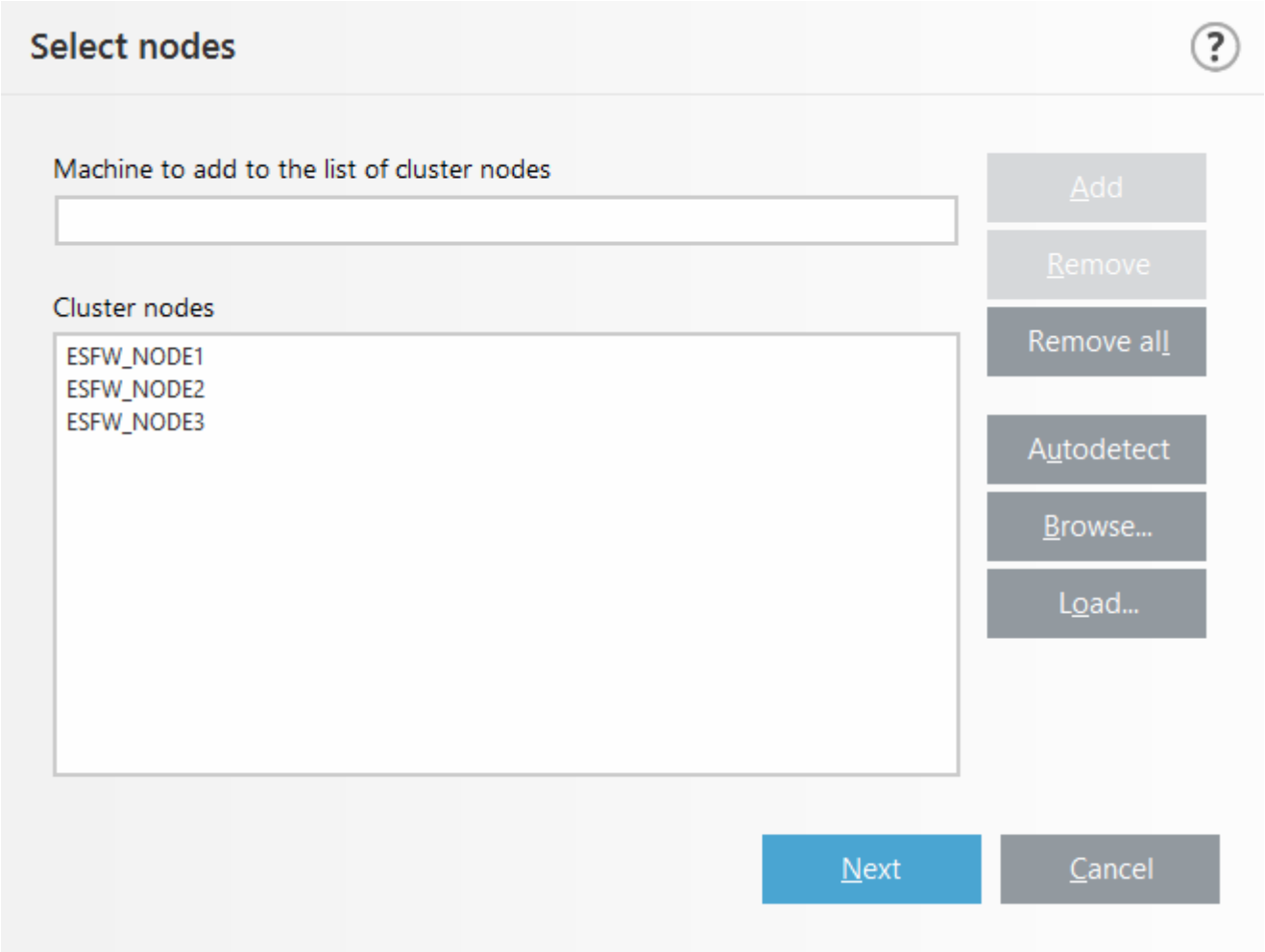
Consente di aggiungere automaticamente nodi da un cluster di Windows Failover Cluster/Network Load Balancing (NLB) Cluster esistente. Per poter aggiungere automaticamente nodi, il server in uso per la creazione di ESET Cluster deve essere un membro di questo cluster di Windows Failover Cluster/NLB Cluster. Affinché possa rilevare correttamente i nodi, è necessario che nelle proprietà del cluster NLB sia attiva la funzione **Consenti controllo remoto**. Dopo aver creato l'elenco dei nuovi nodi.

Sfoglia

Consente di trovare e selezionare i computer all'interno di un Domain o di un Workgroup. Questo metodo consente di aggiungere manualmente nodi a ESET Cluster. Per aggiungere nodi è anche possibile digitare il nome host del server che si desidera aggiungere e fare clic su **Aggiungi**.

Caricamento in corso

Per importare l'elenco di nodi dal file.



Per modificare i **Nodi cluster** nell'elenco, selezionare il nodo che si desidera rimuovere e fare clic su **Rimuovi** oppure fare clic su **Rimuovi tutto** per cancellare completamente l'elenco.

Nel caso in cui sia già presente un'istanza di ESET Cluster, è possibile aggiungere nuovi nodi in qualsiasi momento. Le operazioni da eseguire sono identiche a quelle descritte in precedenza.

> Tutti i nodi che rimangono nell'elenco devono essere on-line e raggiungibili. L'host locale viene aggiunto ai nodi cluster per impostazione predefinita.

Procedura guidata cluster - Impostazioni del cluster

Definire il nome del cluster e le specifiche della rete (se richiesto).

Nome cluster

Immettere un nome per il cluster e fare clic su **Avanti**.

Porta di ascolto (la porta predefinita è 9777)

Se nell'ambiente di rete è già in uso la porta 9777, specificare un numero di porta non in uso.

Apri porta in Windows firewall

Se questa opzione è selezionata, viene creata una regola in Windows Firewall.

Procedura guidata cluster - Impostazioni di configurazione del cluster

Definire la modalità di distribuzione del certificato e decidere se installare o meno il prodotto su altri nodi.

Distribuzione certificato

- **Remota** automatica: il certificato verrà installato automaticamente.
- **Manuale**: fare clic su **Genera** e selezionare la cartella appropriata dove archiviare i certificati. Verrà creato un certificato radice, nonché un certificato per ciascun nodo, compreso quello (macchina locale) dal quale si sta configurando ESET Cluster. Per registrare il certificato sulla macchina locale fare clic su **Sì**.

Installazione prodotto su altri nodi

- **Remota automatica**: ESET Server Security verrà installato automaticamente su ciascun nodo (a condizione che i relativi sistemi operativi abbiano la stessa architettura).
- **Manuale**: consente di installare ESET Server Security manualmente (ad esempio quando su alcuni nodi sono presenti architetture di sistemi operativi differenti).

Esegui il push della licenza sui nodi senza prodotto attivato

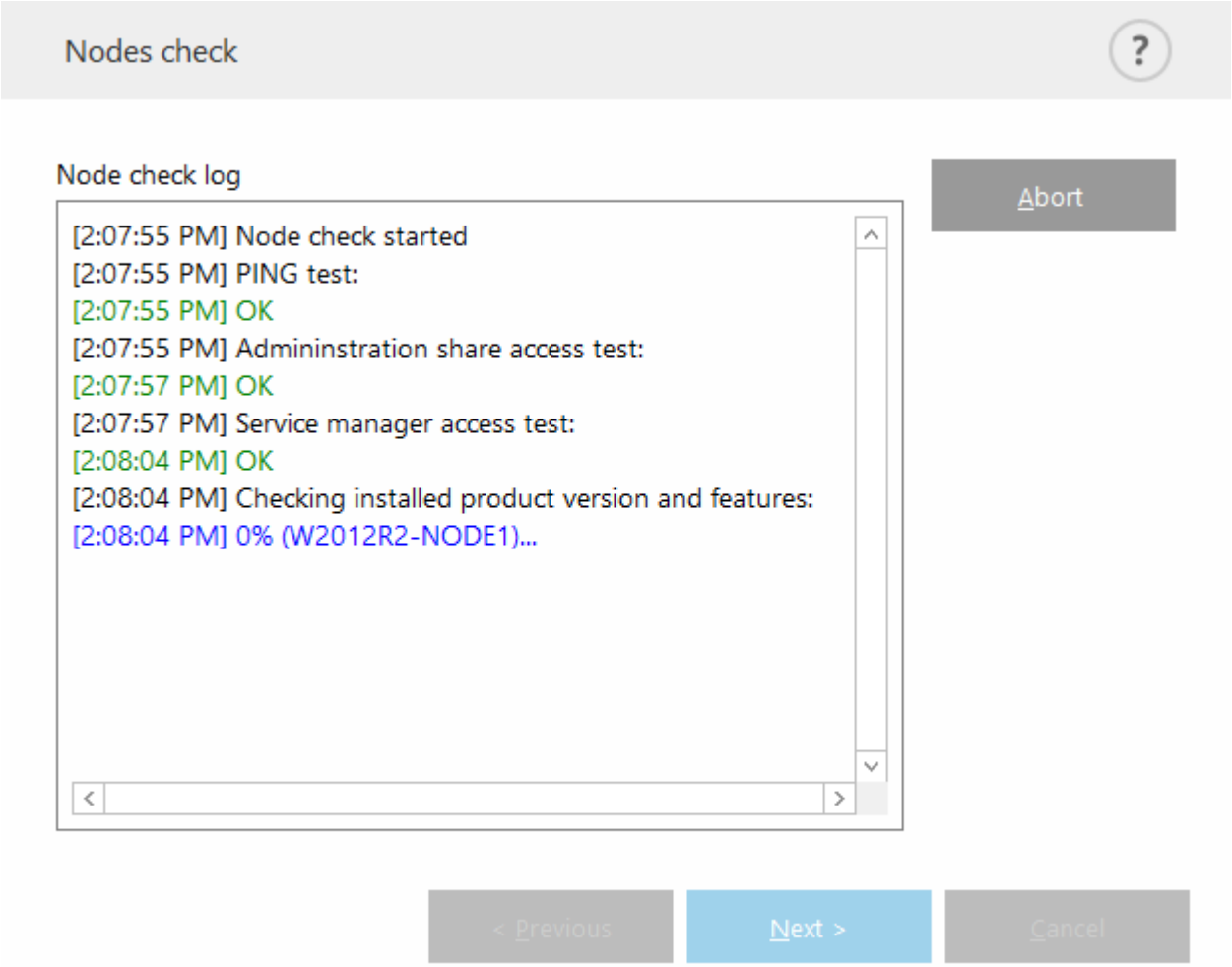
ESET Security attiva automaticamente le soluzioni ESET installate sui nodi senza licenze.

> i Per creare un ESET Cluster con architetture di sistemi operativi miste (a 32 e a 64 bit), installare ESET Server Security manualmente. I sistemi operativi in uso saranno rilevati nei passaggi successivi e le informazioni saranno visualizzate nella finestra del registro.

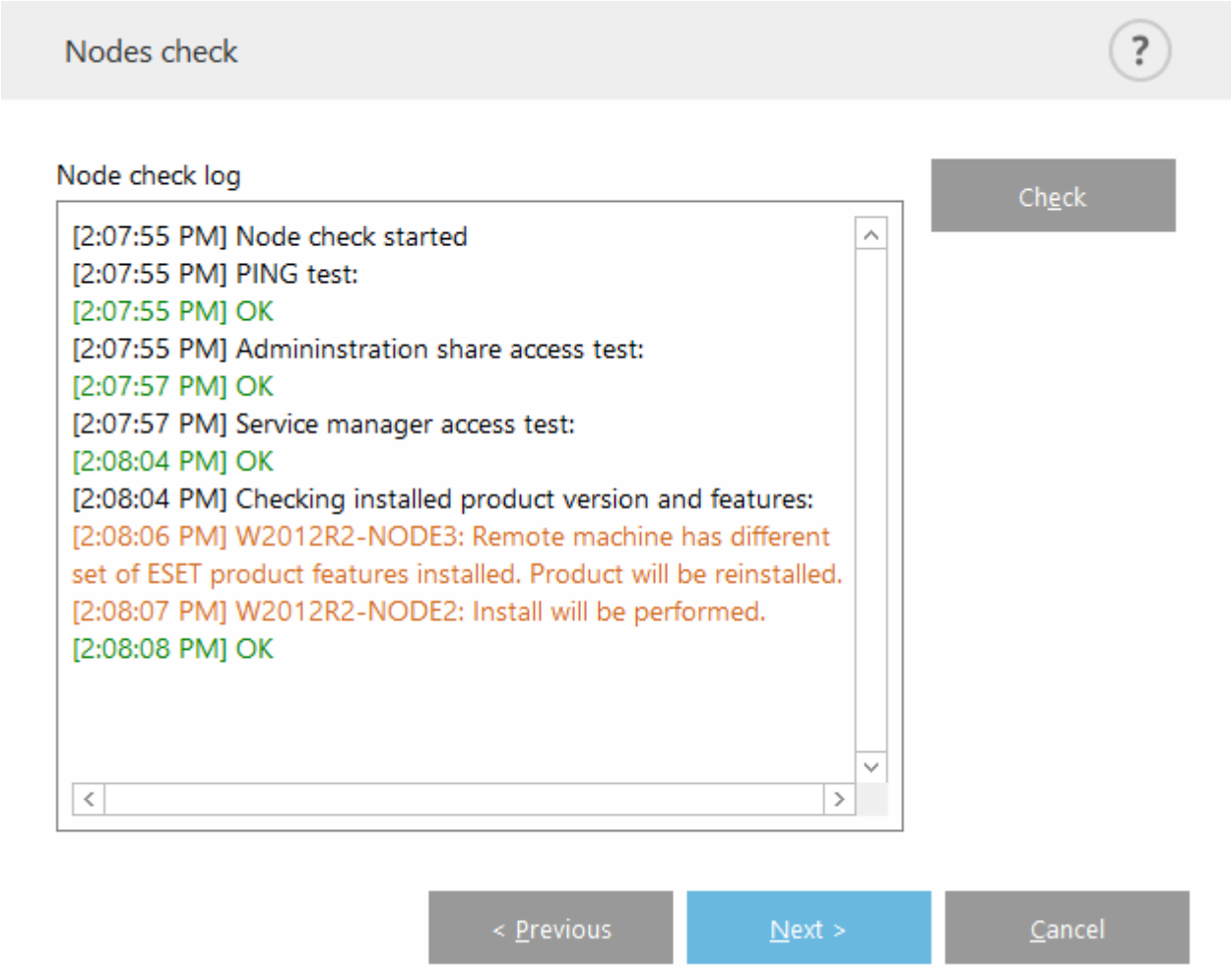
Procedura guidata cluster - Controllo dei nodi

Dopo aver specificato i dettagli di installazione, viene eseguito un controllo del nodo. Le seguenti informazioni saranno visualizzate nel **Rapporto di controllo dei nodi**:

- tutti i nodi esistenti sono on-line
- i nuovi nodi sono accessibili
- il nodo è on-line
- la condivisione admin è accessibile
- l'esecuzione remota è possibile
- sono state installate le versioni corrette dei prodotti (o nessun prodotto)
- sono presenti i nuovi certificati

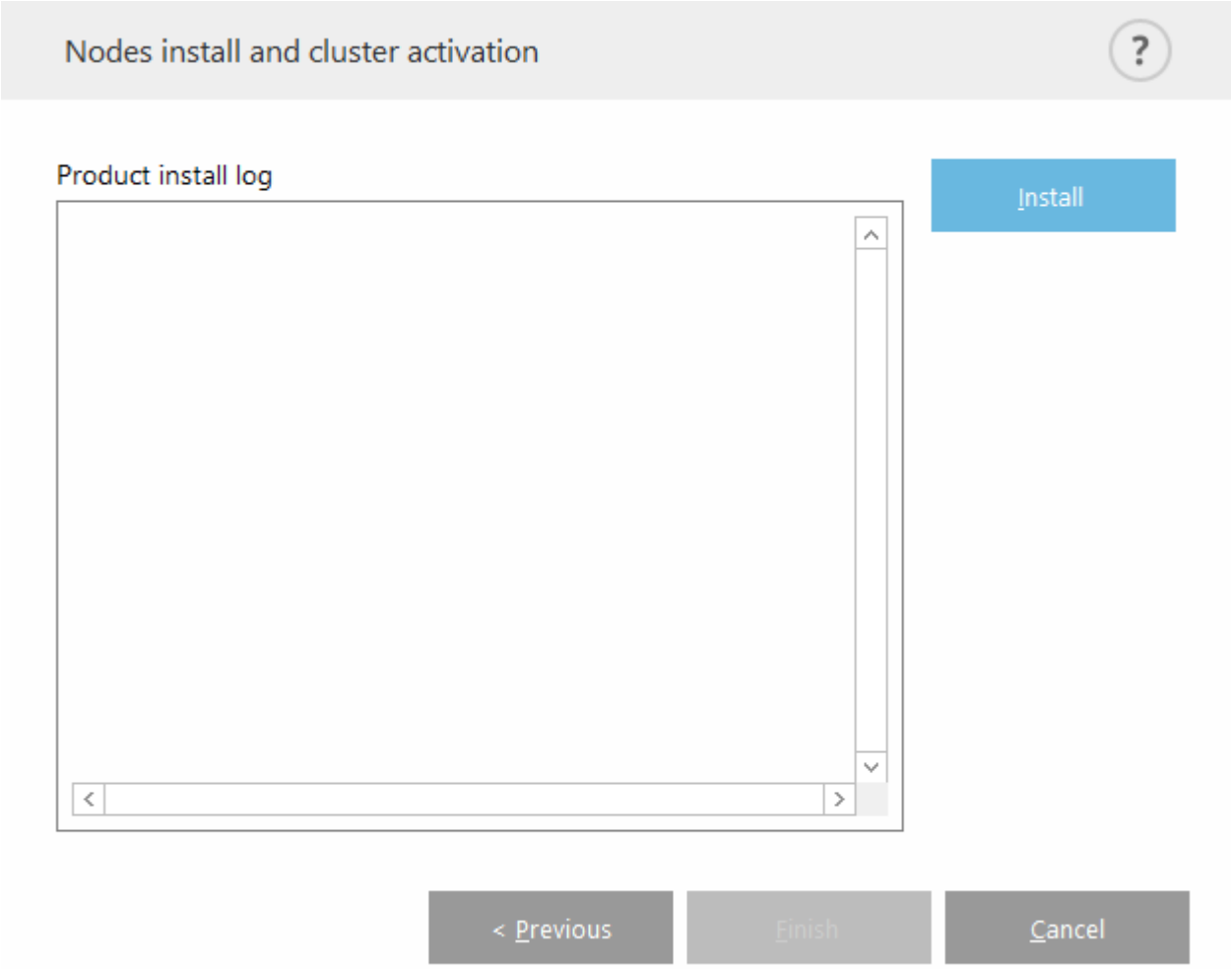


Al termine del controllo del nodo, verrà visualizzato il rapporto:

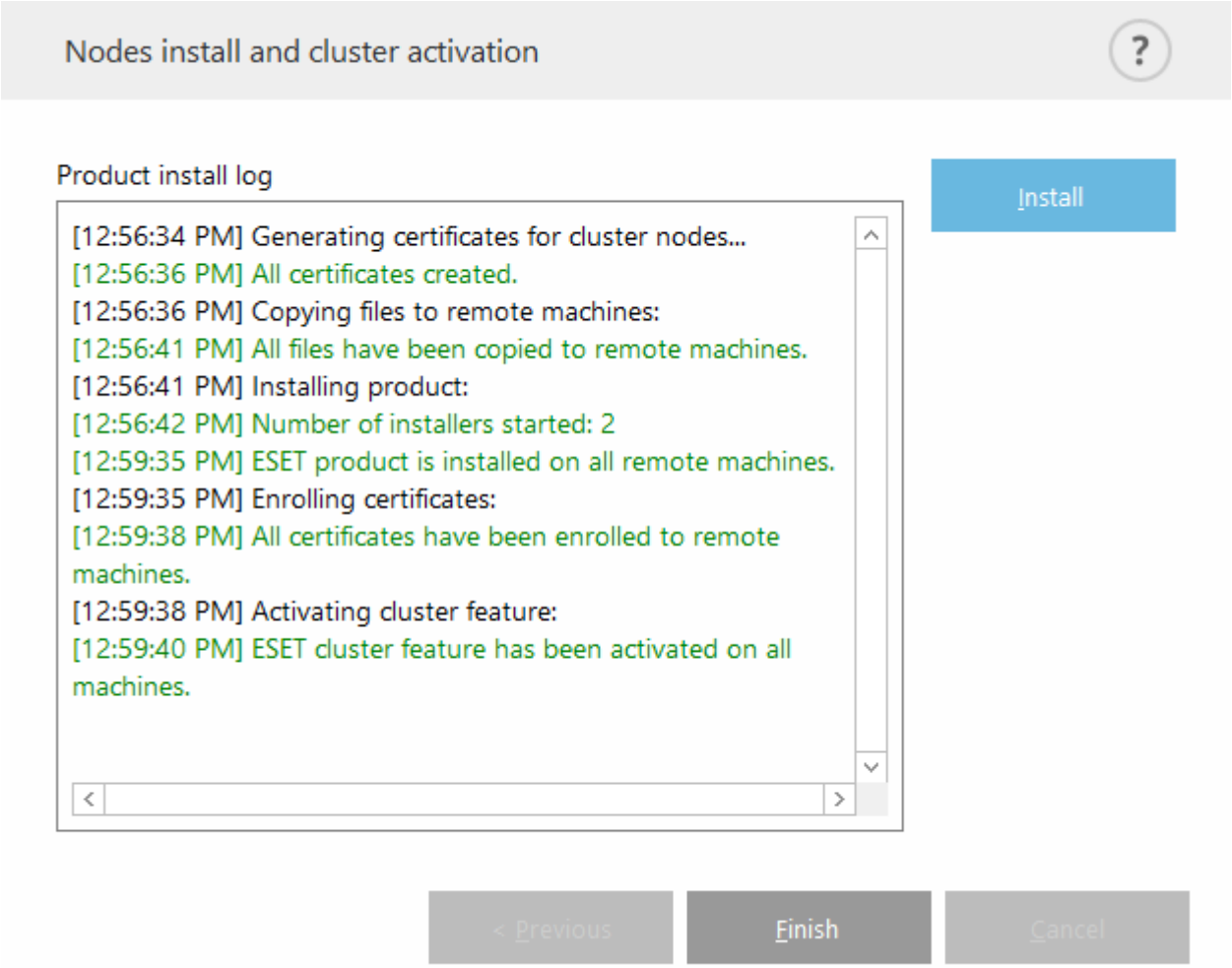


Procedura guidata cluster - Installazione dei nodi

In caso di installazione su una macchina remota durante l'inizializzazione di ESET Cluster, la procedura guidata tenterà di individuare il programma di installazione nella directory *%ProgramData%\ESET\ESET Security\Installer*. Se il pacchetto del programma di installazione non viene trovato in tale percorso, all'utente verrà richiesto di individuare il file del programma di installazione.



Se si tenta di utilizzare l'installazione remota automatica per un nodo con un’architettura differente (a 32 bit invece che a 64 bit), questo verrà rilevato e all'utente verrà richiesto di eseguire l'installazione manuale.



Dopo averlo configurato correttamente, ESET Cluster verrà visualizzato nella pagina **Configurazione** > **Server** come attivato.

> Se su alcuni nodi è già installata una versione precedente di ESET Server Security, l'utente sarà informato della necessità di installare la versione più recente su queste macchine. L'aggiornamento di ESET Server Security potrebbe causare un riavvio automatico.

È inoltre possibile controllarne lo stato corrente dalla pagina Stato cluster (**Configurazione avanzata** (**F5**) > **Strumenti** > **Cluster**).

Computer

In ESET Server Security sono disponibili tutti i componenti necessari per garantire una protezione efficace del server come un computer. Questo modulo consente all'utente di attivare/disattivare e configurare i seguenti componenti:

Protezione file system in tempo reale

Tutti i file vengono sottoposti a controllo per la ricerca di codici dannosi al momento dell'apertura, della creazione o dell'esecuzione sul computer. Per la Protezione file system in tempo reale è inoltre disponibile un'opzione che consente di **Configurare** o **Modificare le esclusioni** e che aprirà la finestra di configurazione delle esclusioni in cui è possibile escludere file e cartelle dal controllo.

Controllo dispositivi

Questo modulo consente all'utente di controllare, bloccare o regolare le estensioni dei filtri o delle autorizzazioni e di definire la propria capacità di accedere e di utilizzare un determinato dispositivo.

Host Intrusion Prevention System (HIPS)

Il sistema monitora gli eventi che si verificano all'interno del sistema operativo e reagisce in base a un set personalizzato di regole.

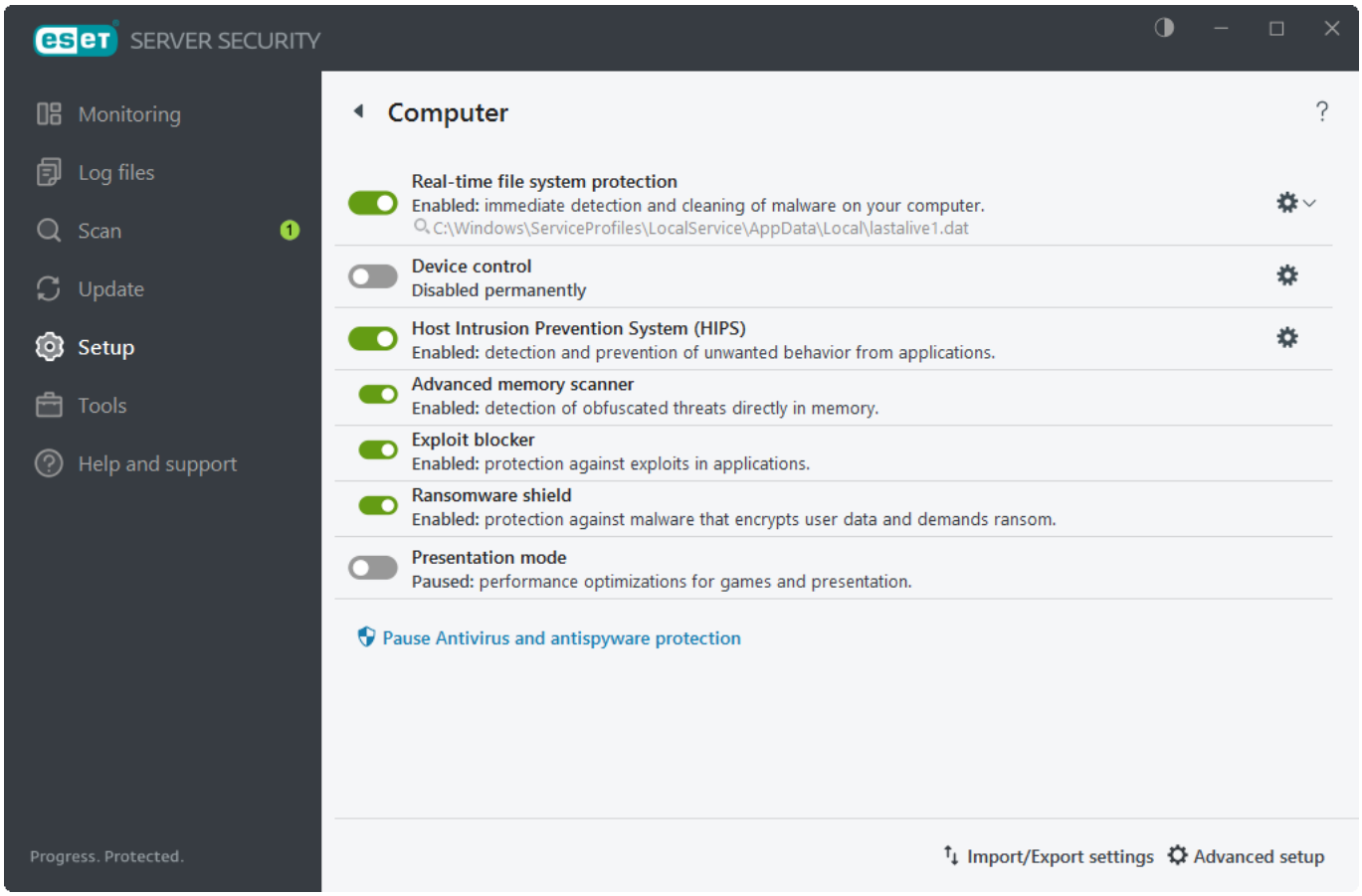
- Scanner memoria avanzato
- Exploit Blocker
- Protezione ransomware

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.

Sospendi la 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**.



Rete

Alcune connessioni individuali di rete vengono consentite o bloccate in base alle regole di filtraggio. Viene offerta la protezione contro gli attacchi dai computer remoti e vengono bloccati alcuni servizi potenzialmente dannosi.

Il modulo Rete consente all'utente di attivare/disattivare e configurare i seguenti componenti:

Firewall

Consente di filtrare tutte le comunicazioni di rete in base alla configurazione di ESET Server Security.

Protezione attacchi di rete (IDS)

Analizza il contenuto del traffico di rete e protegge dagli attacchi alla rete. Il traffico considerato dannoso verrà bloccato.

Protezione Botnet

Rilevamento e blocco di comunicazioni botnet. Identifica in maniera rapida e accurata il malware nel sistema.

Blacklist temporanea indirizzi IP (indirizzi bloccati)

Consente di visualizzare un elenco di indirizzi IP rilevati come la fonte di attacchi e aggiunti alla blacklist per il blocco della connessione per uno specifico periodo di tempo.

Connessioni di rete

Consente di visualizzare le reti a cui sono connesse le schede di rete con informazioni dettagliate.

Risoluzione dei problemi relativi alla protezione accesso di rete

Risolvi comunicazione bloccata

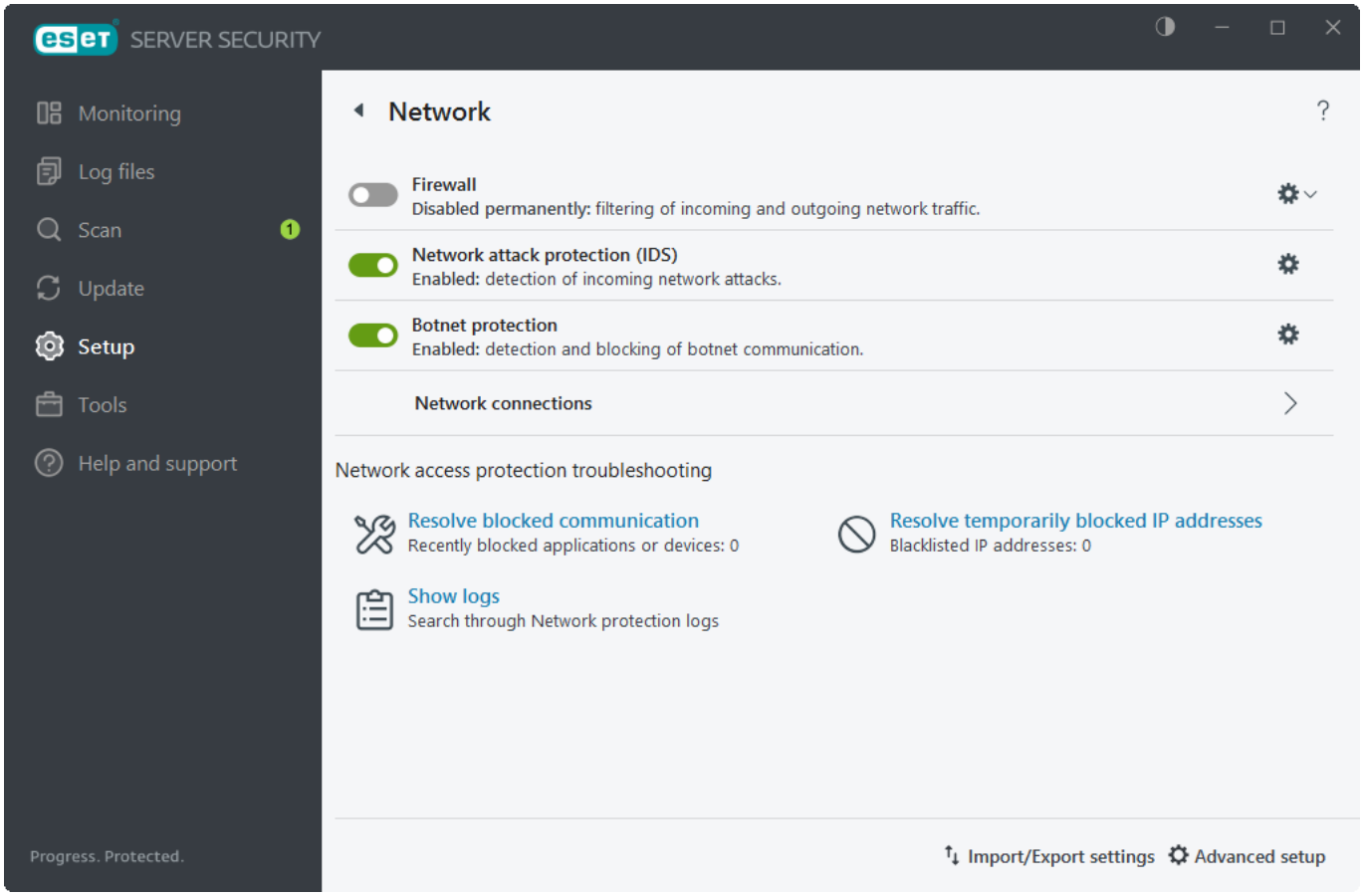
Aiuta l'utente a risolvere problemi di connettività causati dalla protezione attacchi di rete.

Risolvi indirizzi IP temporaneamente bloccati

Consente di visualizzare un elenco di indirizzi IP rilevati come la fonte di attacchi e aggiunti alla blacklist per il blocco della connessione per uno specifico periodo di tempo.

Mostra rapporti

Un’analisi approfondita di questi dati può aiutare a rilevare tentativi di compromissione della sicurezza del sistema. Molti altri fattori indicano potenziali rischi per la sicurezza e consentono di ridurne al minimo l’impatto: connessioni frequenti da posizioni sconosciute, vari tentativi di stabilire connessioni, applicazioni sconosciute che comunicano o numeri di porta utilizzati in modo insolito.



Connessioni di rete

I dettagli della connessione di rete e della scheda di rete consentono di identificare la rete che si sta tentando di configurare in Protezione accesso alla rete. Fare doppio clic su una connessione nell'elenco delle connessioni di rete per visualizzarne i dettagli insieme alle informazioni della scheda di rete.

Passare il puntatore del mouse su una connessione di rete specifica per scegliere una delle seguenti opzioni:

- **Modifica**: consente di aprire la finestra Configura protezione di rete in cui è possibile assegnare un profilo di protezione di rete alla rete specifica.

- **Cancella**: consente di ripristinare le impostazioni predefinite della configurazione della connessione di rete.

Risolvi comunicazione bloccata

La procedura guidata per la risoluzione dei problemi consente di risolvere i problemi di connettività causati dal firewall. Selezionare questa opzione se si desidera visualizzare la comunicazione bloccata per le **Applicazioni locali** o la comunicazione bloccata dai **Dispositivi remoti**.

Dal menu a discesa selezionare un periodo di tempo durante il quale le comunicazioni sono state bloccate. Un elenco delle comunicazioni bloccate di recente offre una panoramica del tipo di applicazione o del dispositivo, della reputazione e del numero totale di applicazioni e di dispositivi bloccati durante tale periodo di tempo. Per ulteriori informazioni sulle comunicazioni bloccate, fare clic su **Dettagli**.

Il passaggio successivo consiste nello sblocco dell'applicazione o del dispositivo su cui si verificano problemi di

connettività.

Facendo clic su **Sblocca**, le comunicazioni precedentemente bloccate saranno consentite. Se si continuano a riscontrare problemi con un'applicazione o il dispositivo in uso non funziona come previsto, fare clic su **Creazione di un'altra regola** per consentire tutte le comunicazioni precedentemente bloccate per il dispositivo interessato. Se il problema persiste, riavviare il computer.

Fare clic su **Apri regole del firewall** per visualizzare le regole create dalla procedura guidata.

Se non è possibile creare la regola, verrà visualizzato un messaggio di errore. Fare clic su **Riprova** e ripetere la procedura per sbloccare la comunicazione o creare un'altra regola dall'elenco delle comunicazioni bloccate.

Web e e-mail

Web e e-mail consente all'utente di attivare/disattivare e configurare i seguenti componenti:

Protezione accesso Web

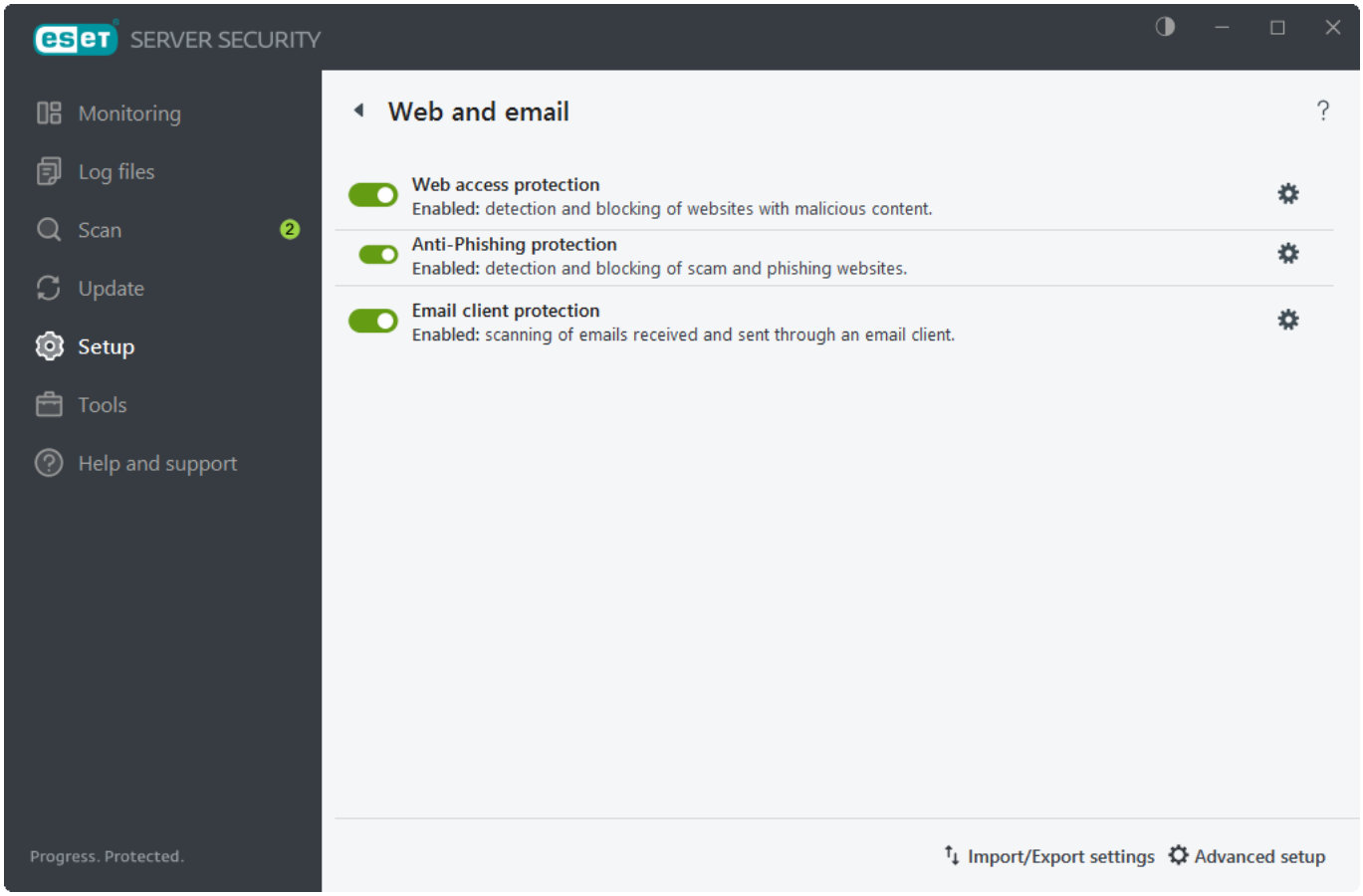
Se questa opzione è attivata, viene eseguito il controllo di tutto il traffico HTTP o HTTPS alla ricerca di software dannoso.

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.

Protezione client di posta

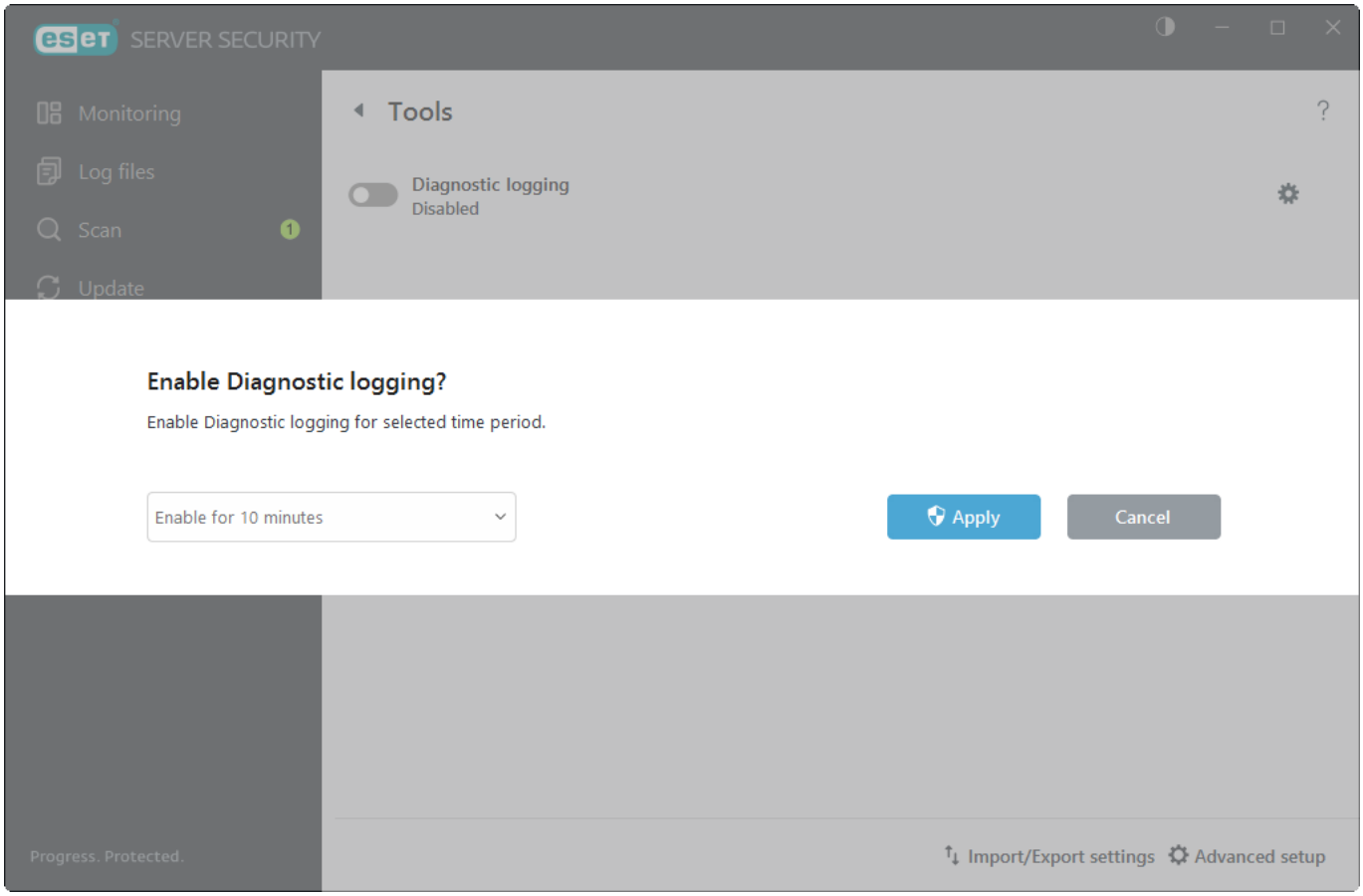
Monitora le comunicazioni ricevute mediante i protocolli POP3 e IMAP.



Strumenti - Registrazione diagnostica

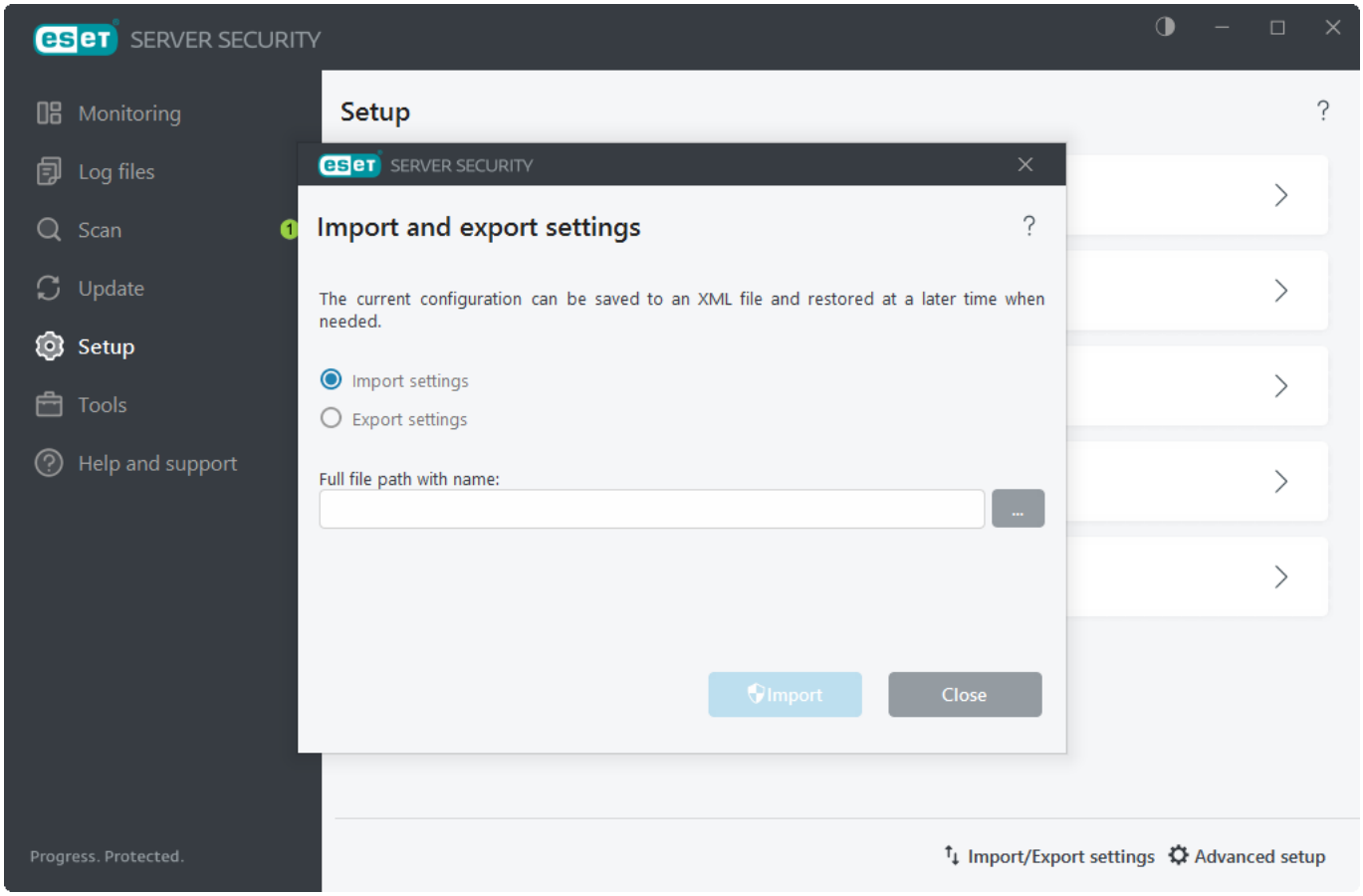
Quando sono necessarie informazioni dettagliate sul comportamento di una funzionalità specifica di ESET Server Security, ad esempio durante la risoluzione dei problemi, è possibile attivare la Registrazione diagnostica. Selezionando l'icona a forma di ingranaggio, è possibile configurare le funzionalità per le quali raccogliere i rapporti di diagnostica.

Scegliere l'intervallo di tempo in cui sarà attivata (10 minuti, 30 minuti, 1 ora, 4 ore, 24 ore, fino al successivo riavvio del server o in modo permanente). Dopo aver attivato la registrazione, ESET Server Security recupererà rapporti dettagliati in base alle funzioni attivate.



Importa ed esporta impostazioni

La funzione di importazione/esportazione delle impostazioni risulta utile se è necessario eseguire il backup della configurazione corrente di ESET Server Security. La funzione di importazione può essere utilizzata anche per distribuire/applicare le stesse impostazioni ad altri server con ESET Server Security. Le impostazioni vengono esportate su un file *.xml*.

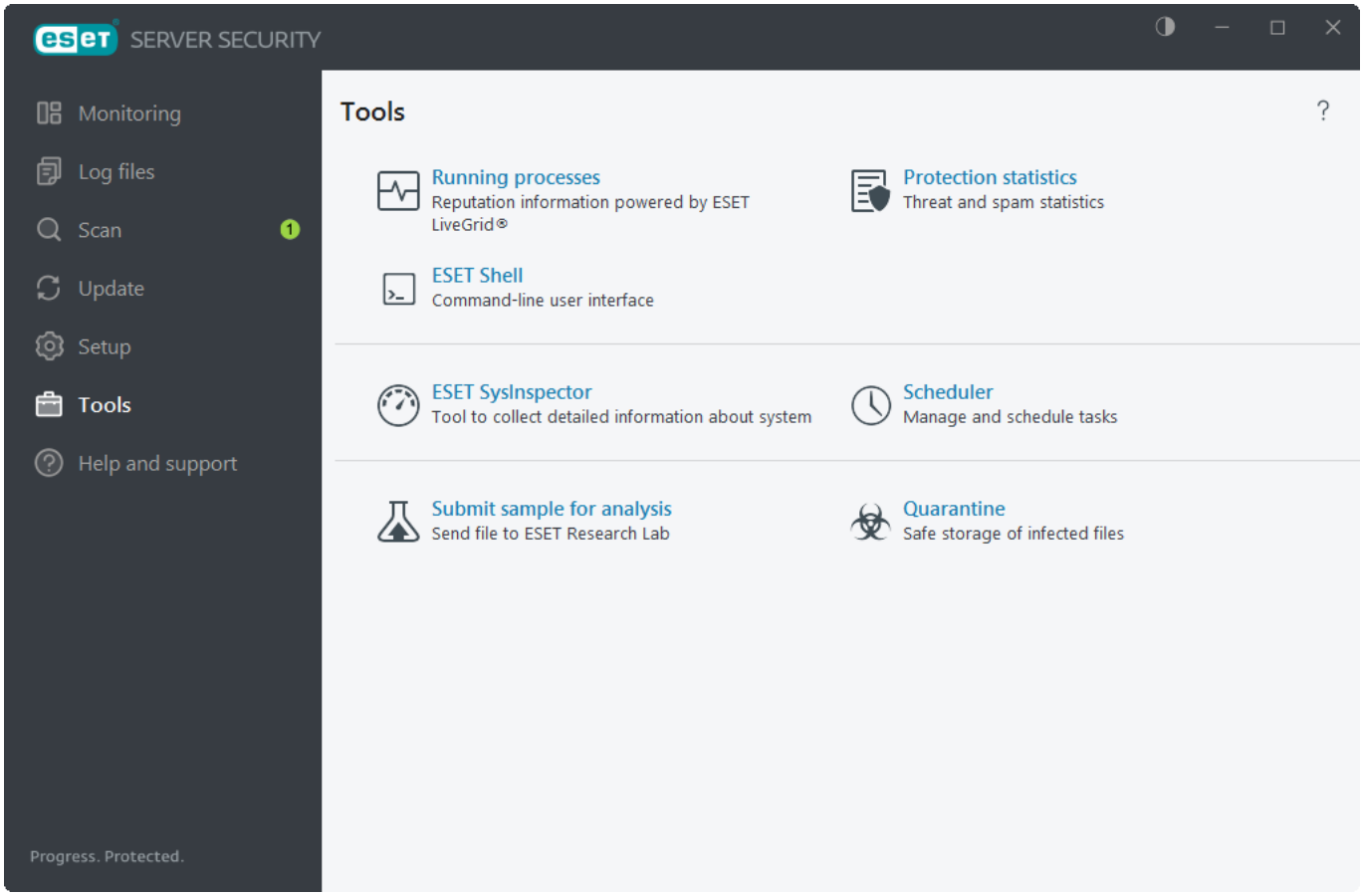


Durante l'esportazione delle impostazioni potrebbe comparire un errore se non si dispone di diritti di scrittura del file esportato nella directory specificata.

Strumenti

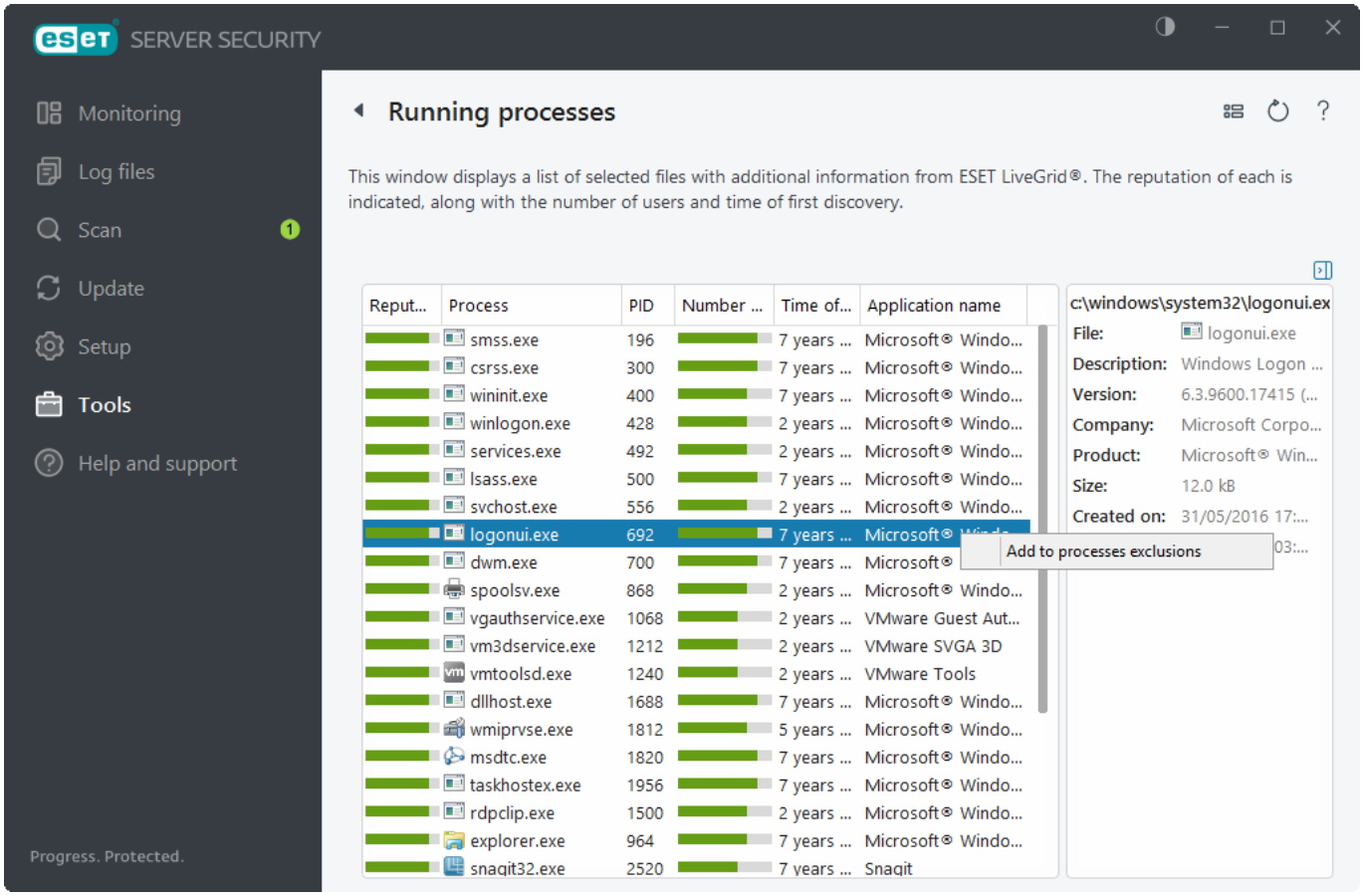
Sono disponibili le seguenti funzionalità per l'amministrazione di ESET Server Security:

- Processi in esecuzione
- Statistiche di protezione
- ESET Shell
- ESET LiveGuard Advanced
- ESET SysInspector
- Pianificazione attività
- Invia file per analisi
- Quarantena



Processi in esecuzione

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



Le applicazioni note contrassegnate come Reputazione massima (verde) sono 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.

Reputazione	**Nella maggior parte dei casi, la tecnologia ESET Server Security e ESET LiveGrid® determina la reputazione degli oggetti in base a una serie di regole euristiche che esaminano le caratteristiche di ciascuno di essi (file, processi, chiavi di registro di sistema e così via) e successivamente ne valutano le potenzialità come attività dannosa. Sulla base di questi dati euristici, agli oggetti viene assegnata una reputazione da 9 - reputazione massima (verde) a 0 - reputazione minima (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 dei processi in esecuzione sui sistemi operativi Windows.
Numero di utenti	Numero di utenti che utilizzano una determinata applicazione. Queste informazioni vengono raccolte mediante la tecnologia ESET LiveGrid®.
Ora del rilevamento	Ora in cui l'applicazione è stata rilevata dalla tecnologia ESET LiveGrid®.
Nome applicazione	Nome specifico di un programma a cui appartiene tale processo.

Se un'applicazione è contrassegnata come "Sconosciuta" (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 campione 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 motore di rilevamento.

Mostra dettagli

Le seguenti informazioni saranno visualizzate nella parte inferiore della finestra:

- **Percorso**: posizione di un'applicazione sul computer.
- **Dimensioni**: dimensione del file in kB (kilobyte) o MB (megabyte).
- **Descrizione**: caratteristiche del file basate sulla descrizione ottenuta dal sistema operativo.
- **Azienda**: 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.

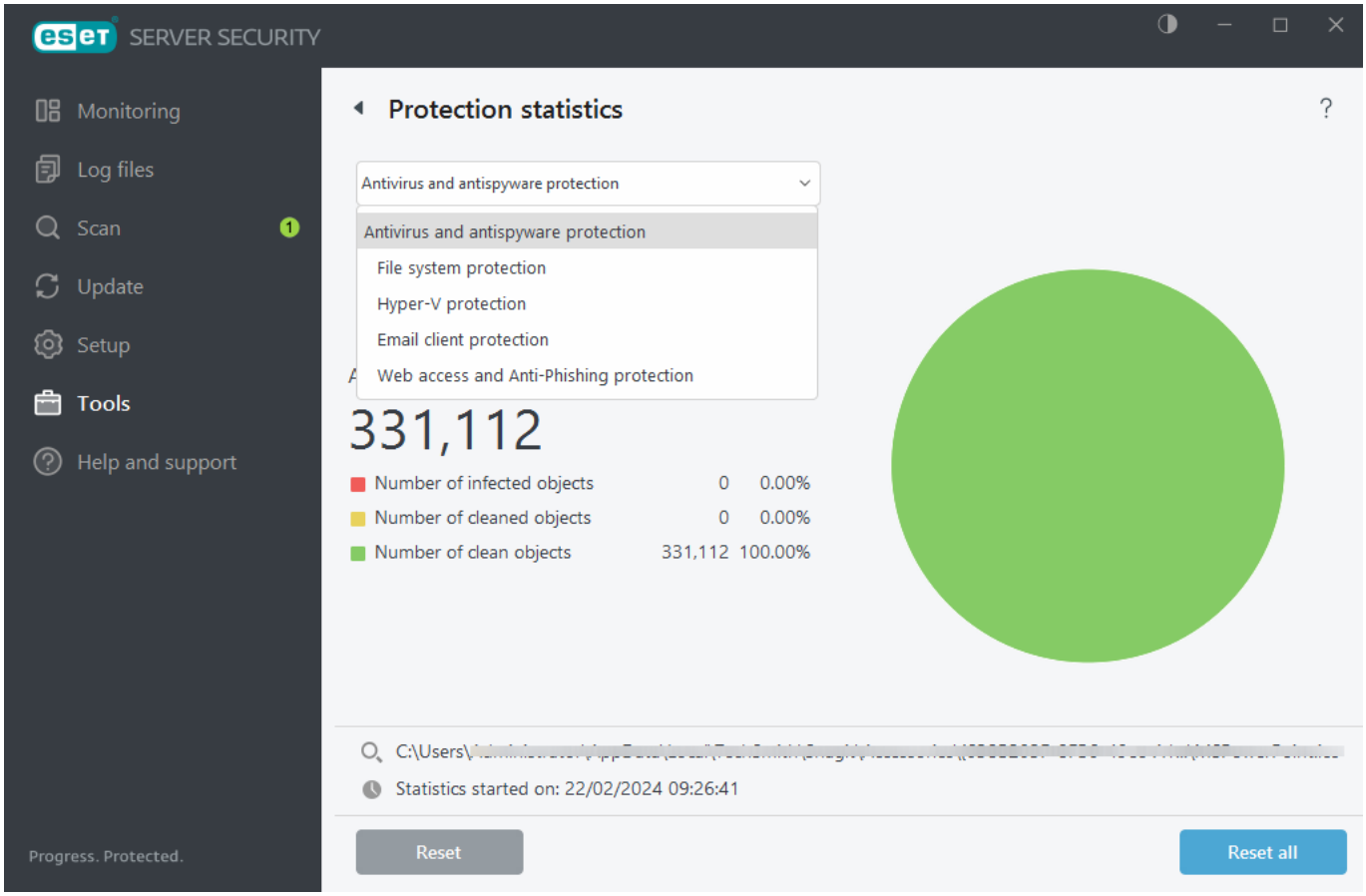
Aggiungi a esclusioni processi

Fare clic con il pulsante destro su un processo nella finestra Processi in esecuzione per escluderlo dal controllo. Il relativo percorso verrà aggiunto all’elenco delle Esclusioni processi.

Statistiche di protezione

Per visualizzare i dati statistici relativi ai moduli di protezione di ESET Server Security, selezionare il modulo di protezione applicabile dal menu a discesa. Le statistiche includono informazioni quali il numero di tutti gli oggetti sottoposti al controllo, numero di oggetti infetti, numero di oggetti puliti e numero di oggetti non infetti.

Spostare il mouse sopra un oggetto accanto al grafico per visualizzare nel grafico solo i dati relativi a tale oggetto specifico. Per cancellare le informazioni statistiche per il modulo di protezione corrente, fare clic su **Azzera**. Per cancellare i dati di tutti i moduli, fare clic su **Azzera tutto**.



In ESET Server Security sono disponibili i seguenti grafici statistici:

Protezione antivirus e antispyware

Consente di visualizzare il numero complessivo di oggetti infetti e puliti.

Protezione file system

Consente di visualizzare solo gli oggetti che sono stati scritti o letti sul file system.

Protezione Hyper-V

Consente di visualizzare il numero complessivo di oggetti infetti, puliti e non infetti (solo sui sistemi con Hyper-V).

Protezione client di posta

Consente di visualizzare solo gli oggetti inviati o ricevuti dai client di posta.

Protezione accesso Web e Anti-Phishing

Consente di visualizzare solo gli oggetti scaricati dai browser Web.

ESET Shell

eShell (abbreviazione di ESET Shell) è un'interfaccia della riga di comando per ESET Server Security. Rappresenta un'alternativa all'interfaccia grafica utente (Graphical User Interface, GUI). eShell include tutte le funzioni e le opzioni generalmente offerte dalla GUI. eShell consente di configurare e amministrare l'intero programma senza utilizzare la GUI.

In aggiunta a tutte le funzionalità disponibili nella GUI, offre anche l'opzione di utilizzo dell'automazione mediante l'esecuzione di script per poter configurare, modificare la configurazione o eseguire un'azione. eShell può inoltre risultare utile per gli utenti che preferiscono utilizzare la riga di comando anziché la GUI.

> Per disporre della funzionalità completa, si consiglia di aprire eShell utilizzando Esegui come amministratore. Lo stesso vale per l'esecuzione di un singolo comando del prompt dei comandi di Windows (cmd). Aprire il prompt utilizzando **Esegui come amministratore**. La mancata esecuzione del prompt dei comandi come amministratore impedirà all'utente di eseguire i comandi per mancanza di autorizzazioni.

eShell può essere eseguito in due modalità:

1. **Modalità interattiva**: risulta utile quando si desidera utilizzare eShell (e non eseguire semplicemente un singolo comando) per attività quali modifica della configurazione, visualizzazione dei rapporti e così via. La modalità interattiva può essere utilizzata se non si ha dimestichezza con tutti i comandi. La modalità interattiva consente lo spostamento all'interno di eShell. Vengono inoltre visualizzati i comandi disponibili che è possibile utilizzare all'interno di un particolare contesto.

2. **Singolo comando/modalità batch**: questa modalità può essere utilizzata se è necessario eseguire solo un comando senza accedere alla modalità interattiva di eShell. Questa operazione può essere eseguita dal prompt dei comandi di Windows digitando `eshell` con i parametri appropriati.

```
eshell get status or eshell computer set real-time status disabled 1h
```

Per eseguire alcuni comandi (come nel secondo esempio indicato in precedenza) in modalità batch/script, sono disponibili due impostazioni che è necessario prima configurare. In caso contrario, verrà visualizzato un messaggio di **Accesso negato**. per motivi di sicurezza.

> Le modifiche alle impostazioni sono necessarie per utilizzare i comandi eShell dal prompt dei comandi di Windows. Ulteriori informazioni sull'esecuzione di file batch.

Esistono due modi per accedere alla modalità interattiva in eShell:

1. Tramite il **menu Start di Windows**: Avvio > Tutti i programmi > ESET > ESET File Security > ESET Shell

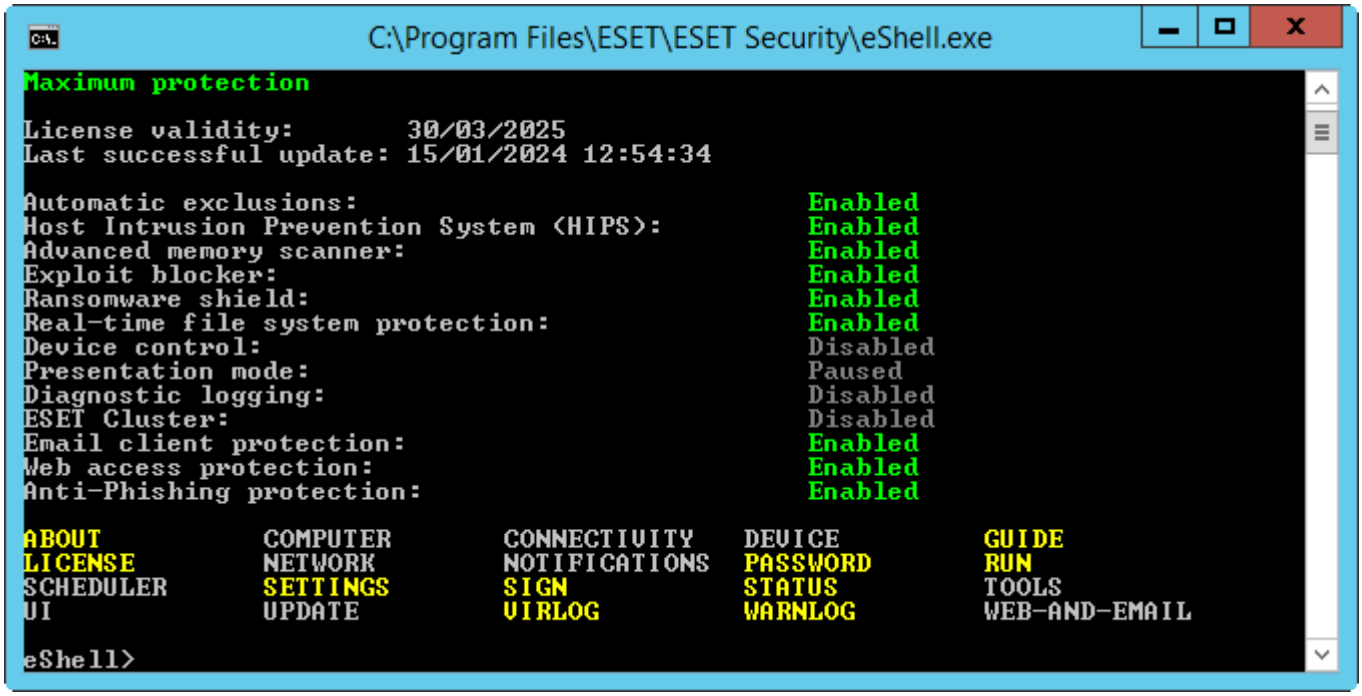
2. Dal **prompt dei comandi di Windows** digitando `eshell` e premendo il tasto Invio

> La comparsa di un errore `'eshell' not recognized as an internal or external command` è dovuta al mancato caricamento delle nuove variabili d'ambiente dal sistema in seguito all'installazione di ESET Server Security.
> Aprire il nuovo prompt dei comandi e tentare di avviare nuovamente eShell. Se continua a comparire un errore o è stata effettuata l'Installazione core di ESET Server Security, avviare eShell utilizzando il percorso assoluto, ad esempio `"%PROGRAMFILES%\ESET\ESET File Security\eShell.exe"` (è necessario utilizzare `""` per consentire il corretto funzionamento del comando).

Quando si esegue per la prima volta eShell in modalità interattiva, viene visualizzata la schermata della prima esecuzione (guide).

> Se in futuro si desidera visualizzare la schermata della prima esecuzione, digitare il comando `guide`. Mostra alcuni esempi di base relativi alle modalità di utilizzo di eShell con sintassi, prefisso, percorso del comando, forme abbreviate, alias, ecc.

Alla successiva esecuzione di eShell, verrà visualizzata questa schermata:



> i I comandi non sono sensibili alle maiuscole e minuscole. I comandi non fanno distinzione tra lettera maiuscola e minuscola per poter essere eseguiti.

Personalizzare eShell

È possibile personalizzare eShell nel contesto `ui eshell`. È possibile configurare alias, colori, lingua, criterio di esecuzione per gli script, impostazioni per i comandi nascosti e altro.

Utilizzo

Sintassi

Per un corretto funzionamento, i comandi devono essere formattati nella sintassi corretta e composti da un prefisso, un contesto, degli argomenti, delle opzioni e così via. Di seguito viene riportata la sintassi generale utilizzata all'interno di eShell:

[<prefix>] [<command path>] <command> [<arguments>]

> ✓ Esempio (verrà attivata la protezione del documento):
> `SET COMPUTER SCANS DOCUMENT REGISTER ENABLED`

`SET`: un prefisso

`COMPUTER SCANS DOCUMENT`: percorso a un particolare comando, un contesto di appartenenza del tale comando

`REGISTER`: il comando stesso

`ENABLED`: un argomento per il comando

Utilizzando `?` come argomento per il comando, è possibile di visualizzare la sintassi di tale comando specifico. Ad esempio, `STATUS ?` mostra all'utente la sintassi del comando `STATUS`:

SINTASSI:

`[get] status`

OPERAZIONI:

`get`: Mostra lo stato di tutti i moduli di protezione

Si noti che `[get]` è posto tra parentesi. Ciò indica che il prefisso `get` è predefinito per il comando `status`. Tale condizione significa che quando si esegue il comando `status` senza specificare un prefisso, verrà utilizzato in realtà il prefisso predefinito (in questo caso `get status`). L'utilizzo di comandi senza un prefisso consente di ridurre i tempi di digitazione. In genere `get` è il prefisso predefinito per la maggior parte dei comandi, ma è necessario accertarsi quale sia il prefisso predefinito per un determinato comando e che sia esattamente quello che si desidera eseguire.

> i I comandi non sono sensibili alle maiuscole e minuscole. I comandi non fanno distinzione tra lettera maiuscola e minuscola per poter essere eseguiti.

Prefisso/operazione

Il prefisso è un'operazione. Il prefisso `GET` fornisce informazioni sulle modalità di configurazione di una determinata funzione di ESET Server Security o ne mostra lo stato (ad esempio `GET COMPUTER REAL-TIME STATUS`, che consente di visualizzare lo stato di protezione corrente). Il prefisso `SET` configura la funzionalità o ne modifica lo stato (`SET COMPUTER REAL-TIME STATUS ENABLED` attiva la protezione).

Questi sono i prefissi abilitati da eShell per l'utilizzo. Un comando può o meno supportare uno dei seguenti prefissi:

GET	ripristina impostazione/stato corrente
SET	imposta valore/stato
SELECT	seleziona una voce
ADD	aggiunge una voce
REMOVE	rimuove una voce
CLEAR	rimuove tutti gli elementi/i file
START	avvia un'azione
STOP	interrompe un'azione
PAUSE	sospende un'azione
RESUME	riprende un'azione
RESTORE	ripristina impostazioni predefinite/oggetto/file
SEND	invia un oggetto/file
IMPORT	importa da un file
EXPORT	esporta in un file

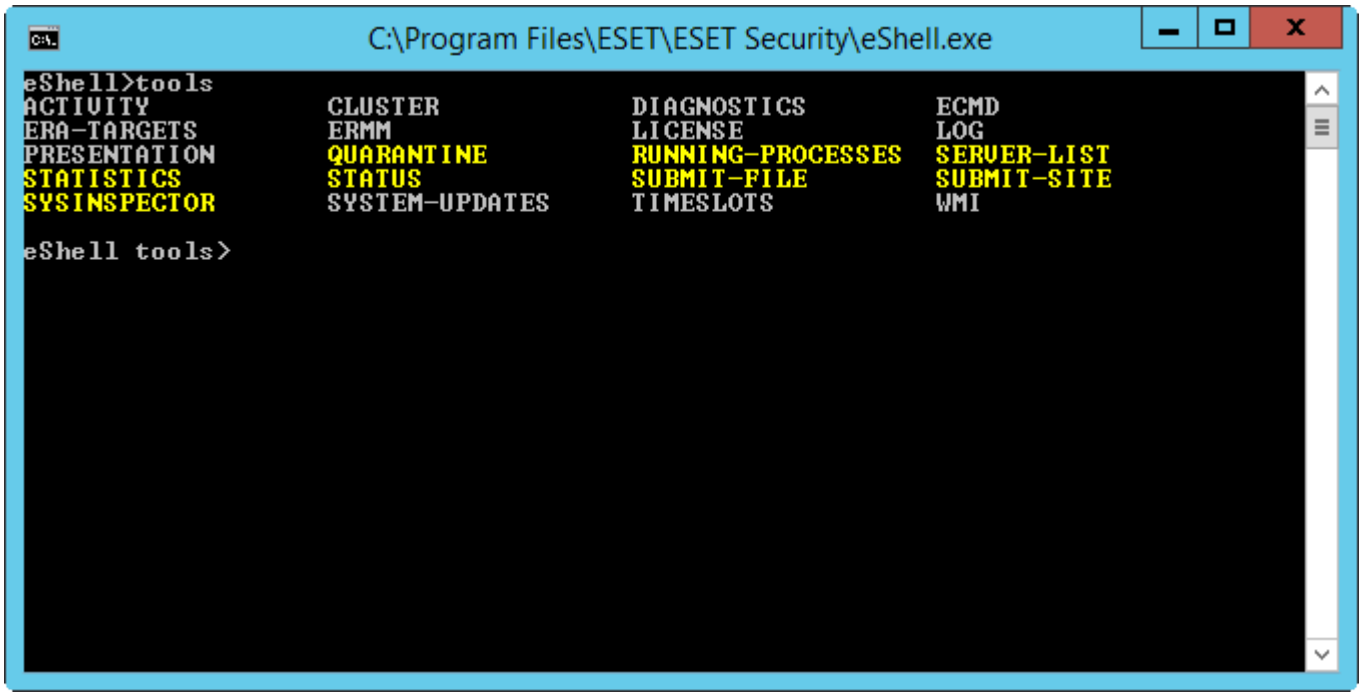
> i Prefissi quali `GET` e `SET` vengono utilizzati con numerosi comandi, ma alcuni di essi (ad esempio `EXIT`) non utilizzano un prefisso.

Percorso del comando/contesto

I comandi sono posizionati in contesti che formano una struttura ad albero. Il livello superiore dell'albero è la radice. Quando si esegue eShell, si è al livello radice:

eShell>

È possibile eseguire un comando da tale posizione oppure immettere il nome del contesto per spostarsi all'interno della struttura ad albero. Ad esempio, quando si immette il contesto TOOLS, verranno elencati tutti i comandi e i sottocontesti disponibili da questa posizione.



Le voci in giallo sono i comandi che è possibile eseguire, mentre quelle in grigio sono i sottocontesti ai quali è possibile accedere. Un sottocontesto contiene ulteriori comandi.

Se è necessario ritornare a un livello superiore, utilizzare . . (due punti).

> Se ci si trova nel contesto:
> eShell computer real-time>
> digitare . . per passare a un livello superiore, ovvero a:
> eShell computer>

Se si desidera ritornare alla radice da eShell computer real-time> (che è inferiore alla radice di due livelli), basta digitare . . . . (due punti e due punti e due punti separati da uno spazio). In questo modo, si passa a due livelli superiori che, in questo caso, corrispondono alla radice. Utilizzare la barra rovesciata \ per ritornare direttamente alla radice da un livello qualsiasi, indipendentemente dalla profondità di quello in cui ci si trova nella struttura dei contesti. Se si desidera ottenere un contesto particolare nei livelli superiori, basta semplicemente utilizzare il numero appropriato di comandi . . per ottenere il livello desiderato, utilizzando lo spazio come separatore. Ad esempio, se si desidera ottenere un valore superiore di tre livelli, utilizzare . . . . . .

Il percorso è relativo al contesto attuale. Se il comando è contenuto nel contesto attuale, non immettere un percorso. Ad esempio, per eseguire GET COMPUTER REAL-TIME STATUS, digitare:

GET COMPUTER STATUS: se ci si trova nel contesto radice (sulla riga di comando è visualizzato eShell>)

GET STATUS: se ci si trova nel contesto COMPUTER (sulla riga di comando è visualizzato eShell computer>)

. . GET STATUS: se ci si trova nel contesto COMPUTER REAL-TIME (sulla riga di comando è visualizzato eShell computer real-time>)

È possibile utilizzare il punto singolo `.` (punto) al posto dei due punti `..`, in quanto il punto singolo è un abbreviazione dei due punti.

> ✔ `. GET STATUS`: se ci si trova nel contesto `COMPUTER REAL-TIME` (sulla riga di comando è visualizzato `eShell computer real-time>`)

Argomento

Un argomento è un'azione eseguita per un comando specifico. Ad esempio, il comando `CLEAN-LEVEL` (posizionato in `COMPUTER REAL-TIME ENGINE`) può essere utilizzato con i seguenti argomenti:

`rigorous`: Correggi sempre il rilevamento

`safe`: Correggi il rilevamento se sicuro; mantienilo in caso contrario

`normal`: Correggi il rilevamento se sicuro; chiedi in caso contrario

`none`: consente di chiedere sempre all'utente finale

Un altro esempio sono gli argomenti `ENABLED` o `DISABLED`, che vengono utilizzati per abilitare o disabilitare una determinata funzione o funzionalità.

Forma abbreviata/comandi abbreviati

eShell consente di abbreviare i contesti, i comandi e gli argomenti (a condizione che l'argomento sia un'opzione oppure un'opzione alternativa). Non è possibile abbreviare un prefisso o un argomento che sia un valore concreto, ad esempio un numero, un nome o un percorso. È possibile utilizzare i numeri `1` e `0` al posto degli argomenti attivati o disattivati.

```
✔ computer set real-time status enabled        =>        com set real stat 1
  computer set real-time status disabled        =>        com set real stat 0
```

Esempi della forma breve:

```
  computer set real-time status enabled        =>        com set real stat en
✔ computer exclusions add detection-excludes object C:\path\file.ext        =>        com excl add det obj C:\path\file.ext
  computer exclusions remove detection-excludes 1        =>        com excl rem det 1
```

Nel caso in cui due comandi o contesti inizino con la stessa lettera (ad esempio `ADVANCED` e `AUTO-EXCLUSIONS` e si immette `A` come contexto abbreviato), eShell non sarà in grado di scegliere quale comando dei due l'utente desidera eseguire. Compare quindi un messaggio di errore e vengono visualizzati i comandi che iniziano con la lettera "`A`" tra i quali scegliere:

`eShell>a`

Il seguente comando non è univoco: `a`

Nel contesto `COMPUTER` sono disponibili i seguenti sottocontesti:

`ADVANCED`

`AUTO-EXCLUSIONS`

Aggiungendo una o più lettere (ad esempio, `AD` anziché solo `A`) eShell inserirà il sottocontesto `ADVANCED` ora diventato univoco. Lo stesso vale per i comandi abbreviati.

> Se si desidera essere certi che i comandi vengano eseguiti come desiderato, si consiglia di non abbreviarli, così come gli argomenti, ecc. e di utilizzare la forma completa. In questo modo, eShell verrà eseguito esattamente come desiderato e si eviteranno errori indesiderati. Ciò è particolarmente utile nel caso dei file/degli script batch.

Completamento automatico

Questa nuova funzionalità è stata introdotta in eShell 2.0 ed è molto simile al completamento automatico nel prompt dei comandi di Windows. Mentre il prompt dei comandi di Windows completa i percorsi dei file, eShell completa i comandi, il contesto e i nomi delle operazioni. Il completamento dell'argomento non è supportato.

Durante la semplice digitazione del comando, premere Tab per completare o scorrere le variazioni disponibili.

Premere Maiusc + Tab per tornare indietro. L'utilizzo contestuale di forme abbreviate e del completamento automatico non è supportato. È infatti possibile utilizzare solo una funzionalità alla volta.

Ad esempio, se si digita `computer real-time additional` premendo Tab non succede niente. Digitare invece `com` e premere Tab per completare `computer`, continuare a digitare `real` + Tab e `add` + Tab e premere Invio. Digitare `on` + Tab e continuare a premere Tab per scorrere tutte le variazioni disponibili: `on-execute-ah, on-execute-ah-removable, on-write-ah, on-write-archive-default`, ecc.

Alias

Un alias è un nome alternativo che può essere utilizzato per eseguire un comando, a condizione che al comando sia assegnato un alias. Sono disponibili alcuni alias predefiniti:

`(global) close`: esci

`(global) quit`: esci

`(global) bye`: esci

`warnlog`: eventi rapporto strumenti

`virlog`: rilevamenti rapporto strumenti

`(global)`: indica che il comando può essere utilizzato ovunque, indipendentemente dall'attuale contesto. A un comando possono essere assegnati più alias. Ad esempio, al comando `EXIT` sono assegnati gli alias `CLOSE`, `QUIT` e `BYE`. Se si desidera uscire da eShell, è possibile utilizzare il comando `EXIT` stesso oppure uno qualsiasi dei rispettivi alias.

L'alias `VIRLOG` è per il comando `DETECTIONS` che è posizionato nel contesto `TOOLS LOG`. In questo modo il comando dei rilevamenti è disponibile dal contesto `ROOT` e tale condizione ne facilita l'accesso (non è necessario immettere il contesto `TOOLS` e successivamente il contesto `LOG` ed eseguirlo direttamente da `ROOT`).

eShell consente di definire gli alias. Il comando `ALIAS` è disponibile nel contesto `UI ESHELL`.

Impostazioni protette con password

ESET Server Security consente di proteggere le impostazioni con password. È possibile impostare una password utilizzando la GUI o eShell utilizzando `set ui access lock-password`.

A questo punto, è necessario inserire la password in modo interattivo per alcuni comandi (come quelli che

consentono di modificare le impostazioni o i dati). Se si desidera lavorare con eShell per un periodo di tempo più prolungato senza inserire ripetutamente la password, è possibile impostarne la memorizzazione tramite eShell utilizzando il comando `set password` (esecuzione da `root`). La password viene quindi inserita automaticamente per ciascun comando eseguito che richiede una password. Viene memorizzata fino all'uscita da eShell. Ciò significa che è necessario utilizzare nuovamente il comando `set password` quando si avvia una nuova sessione e si desidera che eShell ricordi la password.

Guide / Help

Quando si esegue il comando `GUIDE` o `HELP`, verrà visualizzata una schermata "della prima esecuzione" in cui viene illustrato come utilizzare eShell. Questo comando è disponibile esclusivamente nel contesto `ROOT` (`eShell>`).

Cronologia dei comandi

eShell conserva la cronologia dei comandi eseguiti in precedenza. Ciò è applicabile solo alla sessione eShell interattiva corrente. Quando si esce da eShell, la cronologia dei comandi non sarà più disponibile. Utilizzare i tasti delle frecce Su e Giù della tastiera per navigare nella cronologia. Dopo aver trovato il comando desiderato, è possibile eseguirlo nuovamente o modificarlo senza doverlo digitare nuovamente dall'inizio.

CLS/Cancella schermata

Il comando `CLS` può essere utilizzato per cancellare la schermata. Funziona allo stesso modo del prompt dei comandi di Windows o delle interfacce della riga di comando simili.

EXIT/CLOSE/QUIT/BYE

Per chiudere o uscire da eShell, è possibile utilizzare uno di questi comandi (`EXIT`, `CLOSE`, `QUIT` o `BYE`).

Comandi

In questa sezione sono elencati alcuni comandi eShell di base con le relative descrizioni.

> i I comandi non sono sensibili alle maiuscole e minuscole. I comandi non fanno distinzione tra lettera maiuscola e minuscola per poter essere eseguiti.

Esempi di comandi (contenuti nel contesto `ROOT`):

ABOUT

Mostra informazioni sul programma. Consente di visualizzare le seguenti informazioni:

- Nome e numero della versione del prodotto di protezione ESET installato.
- Dati sul sistema operativo e informazioni di base sull'hardware.
- Nome utente (compreso il dominio), nome completo del computer (FQDN, se il server è membro di un dominio) e nome della postazione.
- Componenti installati del prodotto di protezione ESET, compreso il numero della versione di ciascuno di essi.

PERCORSO CONTESTUALE:

`root`

PASSWORD

In genere, per motivi di sicurezza, per eseguire comandi protetti con password, all'utente viene chiesto di immettere una password. Ciò è applicabile a comandi che disabilitano la protezione o che potrebbero influenzare la configurazione di ESET Server Security. A ogni esecuzione di tale comando, all'utente verrà chiesto di inserire una password. Per evitare di doverla inserire ogni volta, l'utente può definirla in modo che verrà ricordata da eShell e inserita automaticamente a ogni esecuzione di un comando protetto con password.

> La password è valida solo per la sessione eShell interattiva corrente. Quando si esce da eShell, la password impostata non sarà più valida. Al successivo avvio di eShell, sarà necessario definirla nuovamente.

In caso di esecuzione di file o script batch, è anche possibile utilizzare una password definita. Assicurarsi di impostare il criterio di esecuzione ESET Shell su Accesso completo in caso di esecuzione di file batch non firmati. Di seguito viene riportato un esempio di file batch:

```
eshell set password plain <yourpassword> "&" computer set real-time status disabled
```

Il comando concatenato indicato in precedenza definisce una password e disattiva la protezione.

> Se possibile, si consiglia di utilizzare file batch firmati. Ciò consentirà di evitare password come testo non crittografato nel file batch (in caso di utilizzo del metodo descritto in precedenza). Per maggiori informazioni, consultare Scripting/file batch (sezione File batch firmati).

PERCORSO CONTESTUALE:

`root`

SINTASSI:

```
[get] | restore password
```

```
set password [plain <password>]
```

OPERAZIONI:

`get`: mostra la password

`set`: imposta o cancella la password

`restore`: cancella la password

ARGOMENTI:

`plain`: consente di utilizzare l’opzione per digitare la password come parametro

`password`: password

> `set password plain <yourpassword>`: imposta una password che verrà utilizzata per i comandi protetti con password
> `restore password`: cancella la password

`get password`: utilizzare questo comando per verificare se la password è stata o meno configurata (verranno visualizzati solo asterischi `"*"` e non la password). Se non sono visibili asterischi, ciò significa che la password non è stata impostata
`set password plain <yourpassword>`: utilizzare questo comando per impostare una password definita
`restore password`: questo comando cancella la password definita

STATUS

Consente di visualizzare informazioni relative all'attuale stato di protezione in tempo reale di ESET Server Security e di sospendere/riprendere la protezione (funzionamento simile a quello della finestra principale del programma).

PERCORSO CONTESTUALE:

`computer real-time`

SINTASSI:

```
[get] status

set status enabled | disabled  [ 10m | 30m | 1h | 4h | temporary ]

restore status
```

OPERAZIONI:

`get`: ripristina impostazione/stato corrente

`set`: configura valore/stato

`restore`: ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`enabled`: Attiva protezione/funzione

`disabled`: Disattiva protezione/funzione

`10m`: Disattiva per 10 minuti

`30m`: Disattiva per 30 minuti

`1h`: Disattiva per 1 ora

`4h`: Disattiva per 4 ore

`temporary`: Disattiva fino al riavvio

Non è possibile disabilitare tutte le funzionalità di protezione con un singolo comando. È possibile gestire le funzionalità di protezione e i moduli uno alla volta utilizzando il comando `status`. Ciascuna funzionalità o modulo di protezione possiede il proprio comando `status`.

Elenco di funzionalità con il comando `status`:

Funzione	Contesto e comando
Esclusioni automatiche	`COMPUTER AUTO-EXCLUSIONS STATUS`
Host Intrusion Prevention System (HIPS)	`COMPUTER HIPS STATUS`
Protezione file system in tempo reale	`COMPUTER REAL-TIME STATUS`
Controllo dispositivi	`DEVICE STATUS`
Protezione Botnet	`NETWORK ADVANCED STATUS-BOTNET`
Protezione attacchi di rete (IDS)	`NETWORK ADVANCED STATUS-IDS`
Isolamento rete	`NETWORK ADVANCED STATUS-ISOLATION`
Cluster ESET	`TOOLS CLUSTER STATUS`
Registrazione diagnostica	`TOOLS DIAGNOSTICS STATUS`
Modalità presentazione	`TOOLS PRESENTATION STATUS`
Protezione Anti-Phishing	`WEB-AND-EMAIL ANTIPHISHING STATUS`
Protezione client di posta	`WEB-AND-EMAIL MAIL-CLIENT STATUS`
Protezione accesso Web	`WEB-AND-EMAIL WEB-ACCESS STATUS`

VIRLOG

Questo è un alias del comando `DETECTIONS`. Risulta utile per visualizzare le informazioni sulle infiltrazioni rilevate.

WARNLOG

Questo è un alias del comando `EVENTS`. Risulta utile per visualizzare informazioni su vari eventi.

Scelte rapide da tastiera

eShell supporta le scorciatoie da tastiera (simili al prompt dei comandi di Microsoft Windows *cmd.exe*). Utilizzare determinati tasti (combinazioni di tasti) sulla tastiera per eseguire azioni in eShell. Ad esempio, mostra la cronologia dei comandi, ripeti parte del comando cronologia, sposta una parola o cancella una riga.

Scorciatoie disponibili:

F1: stampa i caratteri del comando della cronologia effettiva uno per uno.

F2, X: ripeti parte del comando cronologia fino al carattere X.

F3: comando di scrittura della cronologia effettiva.

F4, X: a partire dalla posizione corrente del cursore sul comando effettivo, elimina fino al carattere X.

F5: stesso effetto della FRECCIA SU.

F7: mostra la cronologia dei comandi.

ALT + F7: cancella la cronologia dei comandi.

F8: spostati all’indietro nella cronologia dei comandi, ma visualizza solo i comandi corrispondenti al testo corrente nel prompt dei comandi.

F9: esegui un comando specifico dalla cronologia dei comandi.

FRECCIA A DESTRA: stesso effetto del pulsante F1.

CTRL + START: cancella la riga a sinistra.

CTRL + FINE: cancella la riga a destra.

CTRL + FRECCIA A SINISTRA: sposta una parola a sinistra.

CTRL + FRECCIA A DESTRA: sposta una parola a destra.

File batch/scripting

È possibile utilizzare eShell come utile strumento di scripting per l'automazione. Per utilizzare un file batch con eShell, crearne uno con un eShell ed eseguire i comandi al suo interno.

```
eshell get computer real-time status
```

È inoltre possibile collegare i comandi. Tale operazione si rivela, ad esempio, necessaria se si desidera ottenere un tipo particolare di attività pianificata. Per far ciò, è necessario inserire il seguente comando:

```
eshell select scheduler task 4 "&" get scheduler action
```

La selezione di un oggetto (in questo caso, numero di attività 4) vale solitamente solo per un'istanza attualmente in esecuzione di eShell. In caso di esecuzione di questi due comandi uno di seguito all'altro, il secondo comando restituirebbe l'errore ""No task selected or selected task no longer exists"".

Per motivi di protezione, il criterio di esecuzione è impostato su **Scripting limitato** per impostazione predefinita. Ciò consente all'utente di utilizzare eShell come strumento di monitoraggio, ma non di apportare modifiche alla configurazione di ESET Server Security attraverso l'esecuzione di uno script. Se si sta tentando di eseguire uno script con comandi che influiscono sulla sicurezza, ad esempio disattivando la protezione, verrà visualizzato un messaggio di **Accesso negato**. Per eseguire comandi in grado di modificare la configurazione, si consiglia di utilizzare file batch firmati.

Per modificare la configurazione utilizzando un singolo comando inserito manualmente nel prompt dei comandi di Windows, è necessario autorizzare eShell a eseguire l'accesso completo (scelta non consigliata). Per concedere l'accesso completo, utilizzare il comando `ui eshell shell-execution-policy` nella modalità interattiva di eShell stesso oppure tramite la GUI in **Configurazione avanzata** (**F5**) > **Interfaccia utente** > ESET Shell.

File batch firmati

eShell consente all’utente di proteggere i comuni file batch (**.bat*) con una firma. Gli script vengono firmati con la stessa password utilizzata per la protezione delle impostazioni. Per firmare uno script, è necessario abilitare dapprima la protezione delle impostazioni. È possibile eseguire questa operazione tramite la finestra principale del programma o in eShell utilizzando il comando `set ui access lock-password`. Dopo aver configurato la password per la protezione, è possibile avviare la firma dei file batch.

> È necessario firmare nuovamente tutti gli script se si modifica la password di protezione delle impostazioni. In caso contrario, gli script non riusciranno a eseguire la seguente modifica della password. La password inserita al momento della firma di uno script deve corrispondere alla password per la protezione delle impostazioni sul sistema di destinazione.

Per firmare un file batch, eseguire `sign <script.bat>` dal contesto radice di eShell, dove *script.bat* è il percorso dello script che si desidera firmare. Inserire e confermare la password che verrà utilizzata per la firma. Questa password deve corrispondere a quella utilizzata per la protezione delle impostazioni. Una firma viene posizionata in calce al file batch sotto forma di commento. Se lo script è già stato firmato, la nuova firma sostituirà quella esistente.

> ℹ In caso di modifica di un file batch precedentemente firmato, è necessario firmarlo nuovamente.

Per eseguire un file batch firmato da un prompt dei comandi di Windows o come attività pianificata, utilizzare il comando seguente:

```
eshell run <script.bat>
```

Dove *script.bat* è il percorso del file batch.

```
eshell run d:\myeshellscript.bat
```

ESET SysInspector

ESET SysInspector è un'applicazione che esamina a fondo il computer, raccoglie informazioni dettagliate sui componenti del sistema, quali i driver e le applicazioni installati, 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.

Fare clic su **Crea** e inserire un breve **Commento** che descrive il rapporto da creare. Attendere il completamento del rapporto di ESET SysInspector (lo stato sarà visualizzato come Creato). La creazione del rapporto potrebbe richiedere alcuni minuti in base alla configurazione hardware e ai dati di sistema.

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

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

Sono disponibili le azioni seguenti:

- **Mostra**: apre il rapporto creato. È anche possibile fare clic con il pulsante destro del mouse su un rapporto e selezionare **Mostra** dal menu contestuale.
- **Crea**: consente di creare un nuovo rapporto. Immettere un breve commento per descrivere il rapporto da creare e fare clic su **Crea**. Attendere il completamento del rapporto di ESET SysInspector (lo **Stato** sarà visualizzato come Creato).
- **Elimina**: rimuove dall'elenco i rapporti selezionati.

Fare clic con il pulsante destro del mouse su uno o più rapporti selezionati per visualizzare le opzioni seguenti del

menu contestuale:

- **Mostra**: apre il rapporto selezionato in ESET SysInspector (funzione uguale a un doppio clic su un rapporto).

- **Crea**: consente di creare un nuovo rapporto. Immettere un breve commento per descrivere il rapporto da creare e fare clic su **Crea**. Attendere il completamento del rapporto di ESET SysInspector (lo **Stato** sarà visualizzato come Creato).

- **Elimina**: rimuove dall'elenco i rapporti selezionati.

- **Elimina tutto**: consente di eliminare tutti i rapporti.

- **Esporta**: consente di esportare il rapporto in un file *.esil*. In alternativa, scegliere un file *.xml* o un file *.xml* compresso.

Pianificazione attività

La funzione Pianificazione attività consente di gestire e lanciare attività pianificate in base a parametri definiti. È possibile visualizzare un elenco di tutte le attività pianificate sotto forma di una tabella in cui sono presenti parametri quali tipo e nome dell'attività, ora di avvio e ultima esecuzione. È inoltre possibile pianificare nuove attività facendo clic su Aggiungi attività. Per modificare la configurazione di un'attività pianificata esistente, fare clic sul pulsante **Modifica**. Per ripristinare le impostazioni predefinite dell'elenco di attività pianificate, fare clic su **Predefinito**, quindi su **Ripristina impostazioni predefinite**: tutte le modifiche apportate andranno perse e l'operazione non potrà essere annullata.

Sono disponibili una serie di attività predefinite:

- Manutenzione rapporto

- Aggiornamento automatico periodico (utilizzare questa attività per aggiornare la frequenza)

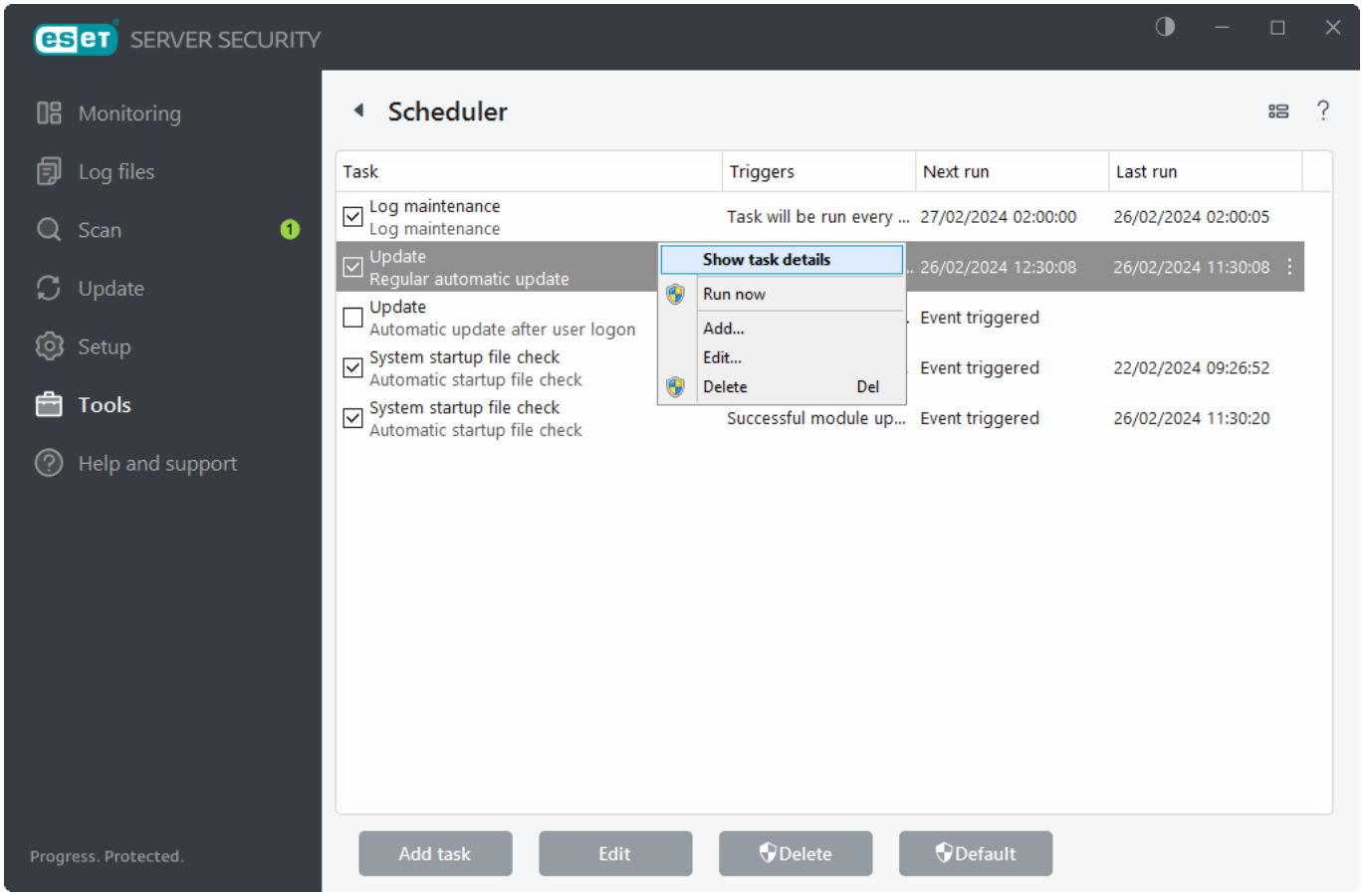
- Aggiornamento automatico dopo la connessione remota

- Aggiornamento automatico dopo l'accesso dell'utente

- Controllo automatico file di avvio (dopo l'accesso utente)

- Controllo automatico file di avvio (dopo il corretto aggiornamento dei moduli)

> Selezionare le caselle di controllo appropriate per attivare o disattivare le attività.



Per eseguire le seguenti azioni, fare clic con il pulsante destro del mouse su un'attività:

Mostra dettagli attività	Consente all'utente di visualizzare informazioni dettagliate su un'attività pianificata facendo doppio clic oppure facendo clic con il pulsante destro del mouse su di essa.
Esegui ora	Consente all'utente di eseguire immediatamente un'attività pianificata selezionata.
Aggiungi...	Consente all'utente di avviare una procedura guidata per creare una nuova attività pianificata.
Modifica...	Consente all'utente di modificare un'attività pianificata esistente (predefinita o definita dall'utente).
Elimina	Consente all'utente di eliminare un'attività esistente.

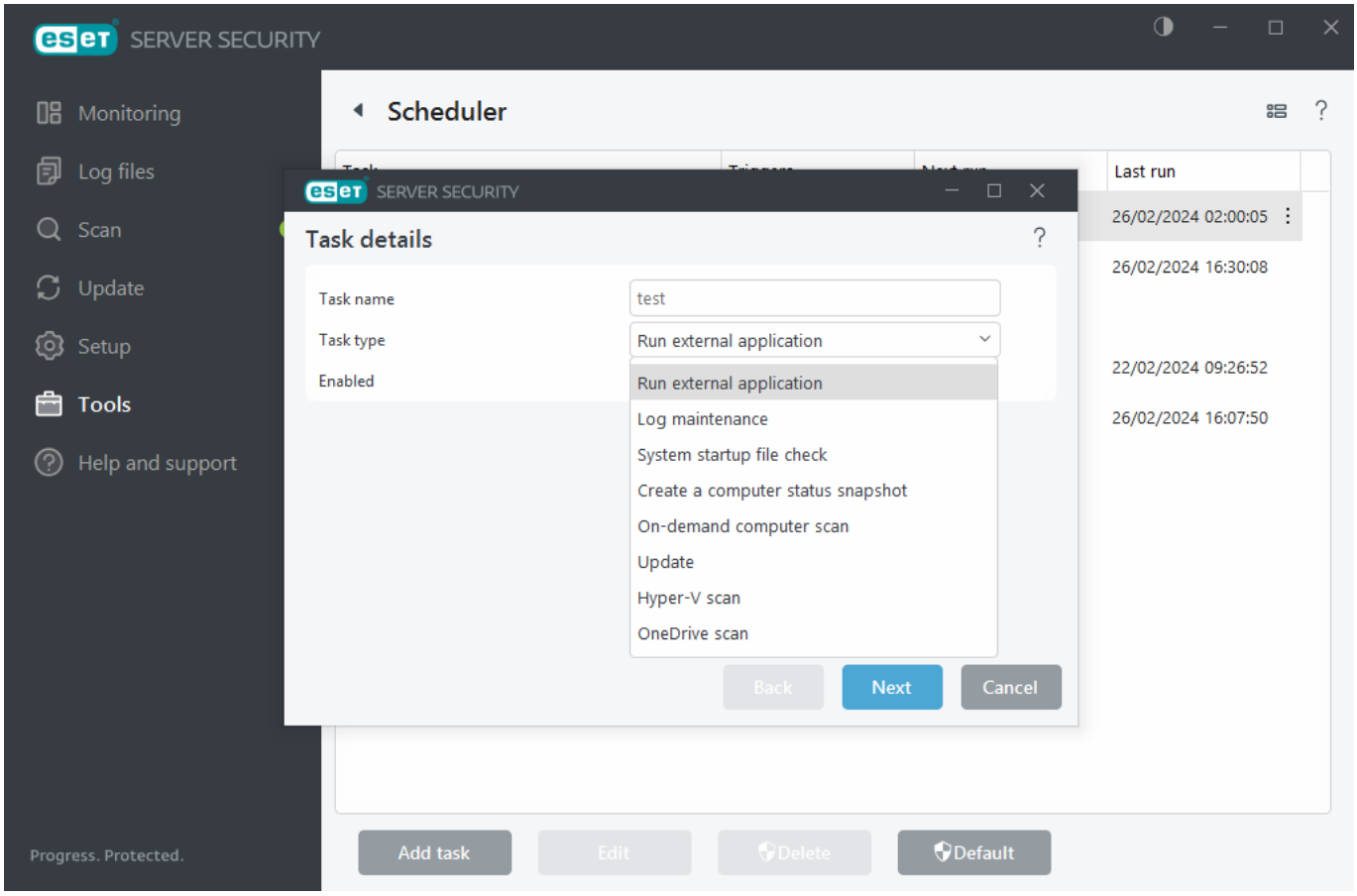
Pianificazione attività: aggiungi attività

Per creare una nuova attività pianificata:

1. Fare clic su **Aggiungi attività**.

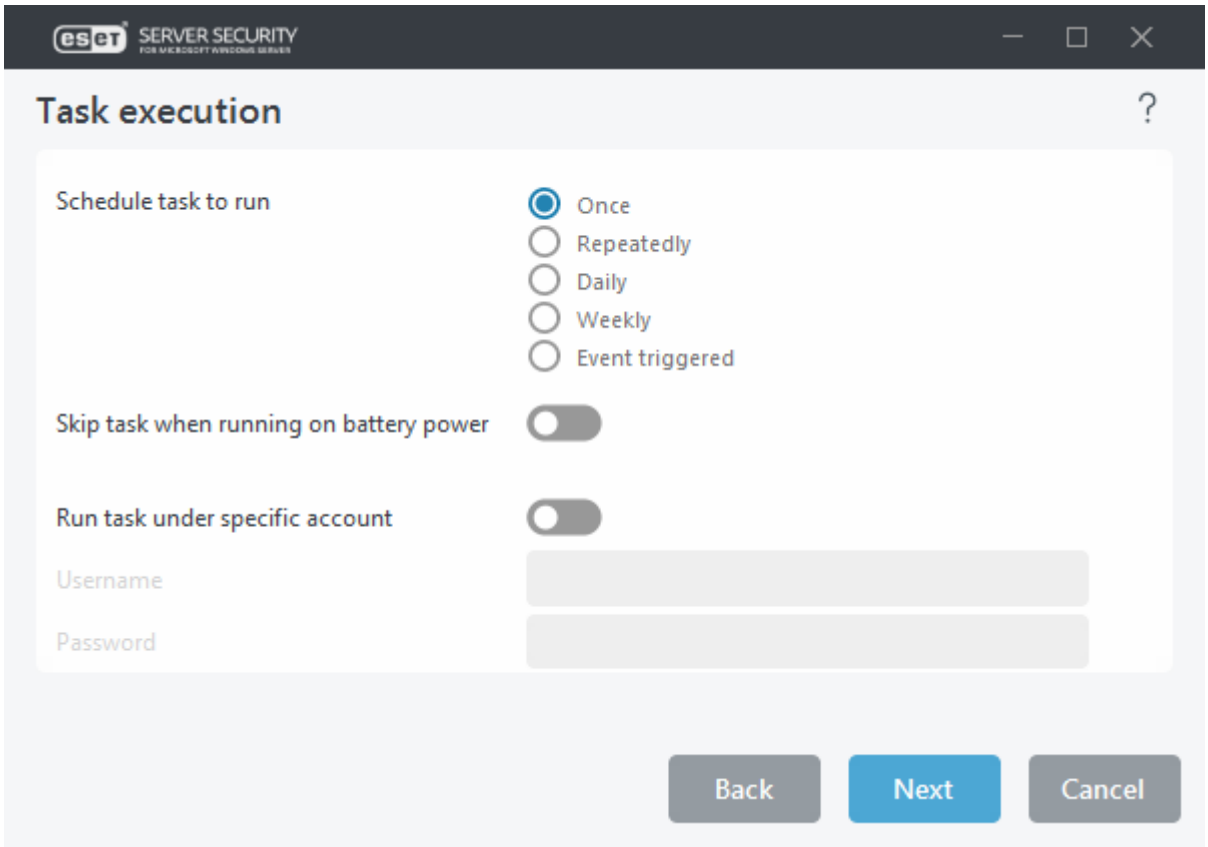
2. Immettere un **Nome attività** e configurare l'attività pianificata personalizzata.

3. Tipo di attività: selezionare il **Tipo di attività** applicabile dal menu a discesa.

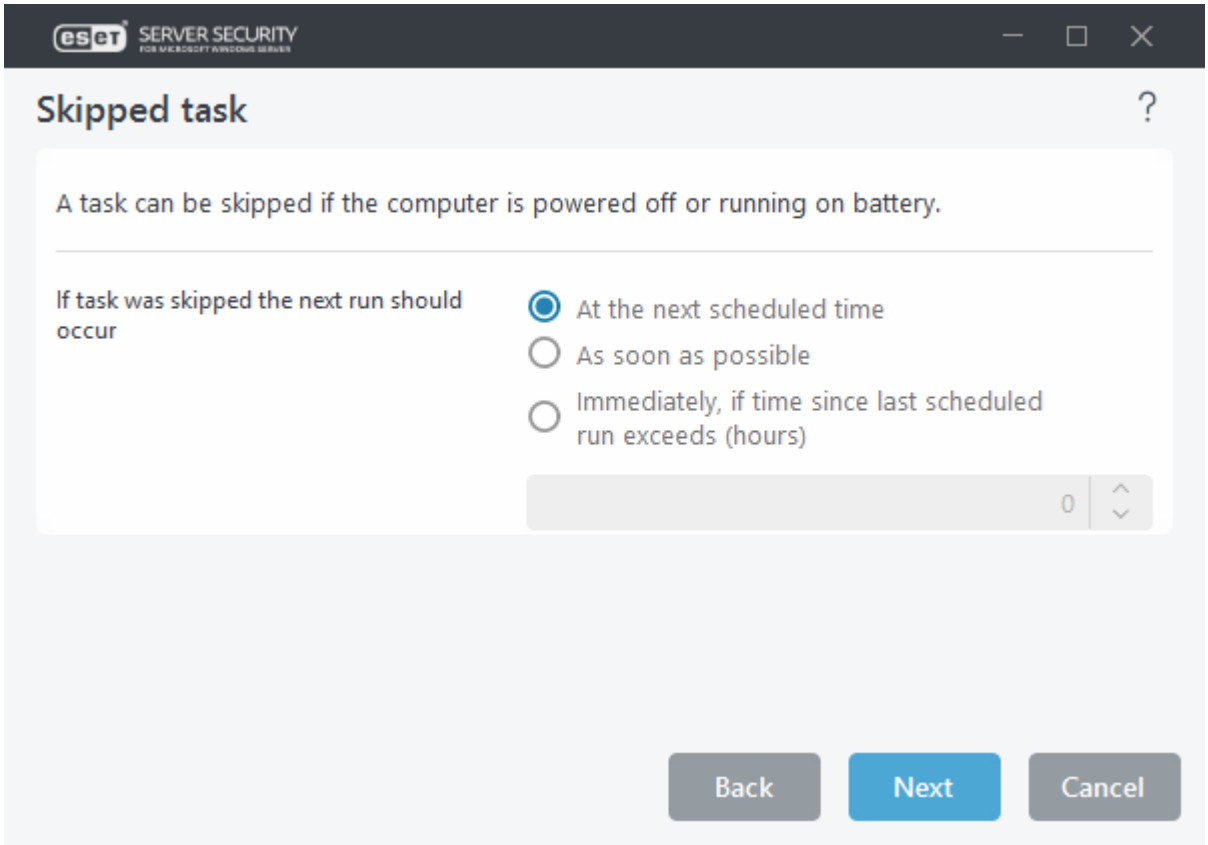


> Per disattivare un'attività, fare clic sulla barra di scorrimento accanto ad **Attivata**. Per attivare l'attività in un secondo momento, utilizzare la casella di controllo nella vista Pianificazione attività.

4. Esecuzione attività: selezionare una delle opzioni per definire quando eseguire l'attività. A seconda della scelta, all'utente verrà chiesto di scegliere un orario, una data, un intervallo o un evento specifico.



5. Attività ignorata: se l’attività non è stata eseguita all’orario predefinito, è possibile specificare il momento in cui dovrà essere eseguita.



6. Esegui applicazione: se l’attività è pianificata per eseguire un’applicazione esterna, scegliere un file eseguibile dalla struttura della directory.

7. Se si desidera apportare modifiche, fare clic su **Indietro** per tornare ai passaggi precedenti e modificare i parametri.

8. Fare clic su **Fine** per creare l’attività o applicare le modifiche.

La nuova attività pianificata comparirà nella vista Pianificazione attività.

Tipo di attività

La procedura di configurazione guidata è diversa per ogni Tipo di attività pianificata. Inserire un **Nome dell’attività** e selezionare il **Tipo di attività** desiderato dal menu a discesa:

- **Esegui applicazione esterna**: consente di pianificare l'esecuzione di un'applicazione esterna. È possibile utilizzare un account specifico per eseguire l’attività pianificata come (opzione Esegui attività con account specifico).

- **Manutenzione rapporto**: i file di rapporto contengono anche gli 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 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 del computer su richiesta**: consente di controllare file e cartelle archiviati localmente o su una condivisione di rete (archiviazione condivisa, come NAS). Utilizzare un account specifico per eseguire l'attività pianificata come (opzione Esegui attività con account specifico).

- **Aggiornamento**: pianifica un'attività di aggiornamento per eseguire un aggiornamento del motore di rilevamento e dei moduli del programma.

- **Controllo Hyper-V**: pianifica un controllo dei dischi virtuali all'interno di Hyper-V.

- **Controllo OneDrive**: consente di pianificare un controllo dei file memorizzati su OneDrive.

Per disattivare un'attività una volta creata, fare clic sul pulsante accanto ad **Attivata**. Per attivare l'attività in un secondo momento, fare clic sulla casella di controllo nella vista Pianificazione attività. Fare clic su **Avanti** per procedere al passaggio successivo.

Esecuzione attività

Selezionare una delle seguenti opzioni relative alla frequenza di esecuzione:

- **Una volta**: l'attività verrà eseguita solo una volta, alla data e all'ora specificate. Per eseguire l'attività solo una volta, in un intervallo di tempo specifico, specificare la data e l'ora di inizio in **Esecuzione attività**.

- **Ripetutamente**: l'attività verrà eseguita in base all'intervallo di tempo specificato (in minuti). Specificare l'ora in cui l'attività verrà eseguita ogni giorno in **Esecuzione attività**.

- **Ogni giorno**: l'attività verrà eseguita ripetutamente ogni giorno all'ora specificata.

- **Ogni settimana**: l'attività verrà eseguita una o più volte alla settimana, nei giorni e nelle ore specificati. Per eseguire l'attività ripetutamente solo in determinati giorni della settimana, a partire dal giorno e dall'orario specificati, specificare l'orario di inizio in Ora di esecuzione attività. Selezionare il giorno o i giorni della settimana in cui eseguire l'attività.

- Quando si verifica un evento: l'attività verrà eseguita quando si verifica un evento specifico.

Salta l'attività in caso di utilizzo dell'alimentazione a batteria

Se si attiva, un'attività non verrà eseguita al momento del lancio se il computer in uso è alimentato dalla batteria, ad esempio per i computer alimentati da gruppi di continuità.

Esegui l'attività con un account specifico

Consente di impostare il nome utente e la password di un account specifico per eseguire l'attività pianificata **Esegui applicazione esterna** o **Controllo del computer su richiesta**. Utilizzare questa funzione per eseguire il **Controllo del computer su richiesta** se si desidera eseguire il controllo della condivisione di rete, ad esempio NAS o altro spazio di archiviazione condiviso.

> Verificare che l’account utente in uso per la funzione **Esegui attività con un account specifico** abbia l’autorizzazione per eseguire l’azione **Accedi come processo batch** (SeBatchLogonRight). È possibile controllare le impostazioni dei criteri utilizzando lo strumento Gestione criteri di gruppo (Impostazioni di protezione > Criteri locali > Assegnazione diritti utente > Effettua l’autenticazione come processo batch).

Quando si verifica un evento

Quando si pianifica un'attività avviata da un evento, è possibile specificare l'intervallo minimo tra il completamento di un'attività e l'altra.

L’attività può essere attivata da uno degli eventi seguenti:

- A ogni avvio del computer
- Al primo avvio del computer ogni giorno
- Connessione remota a Internet/VPN
- In seguito all'esecuzione dell'aggiornamento del modulo
- In seguito all'esecuzione dell'aggiornamento del prodotto
- All’accesso dell’utente: l’attività verrà distribuita quando l’utente esegue l’accesso al sistema. Se si esegue ad esempio l'accesso al computer più volte al giorno, scegliere 24 ore per eseguire l'attività solo al primo accesso del giorno, quindi il giorno successivo.
- Rilevamento delle minacce

Esegui applicazione

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

- **File eseguibile**: scegliere un file eseguibile dalla struttura ad albero della directory, fare clic su Sfoglia... oppure immettere manualmente il percorso.
- **Cartella di lavoro**: specificare la directory di lavoro dell'applicazione esterna. Tutti i file temporanei del File eseguibile selezionato verranno creati all'interno di questa directory.
- **Parametri**: parametri della riga di comando per l'applicazione (facoltativo).

Attività ignorata

Se l'attività non è stata eseguita all'ora predefinita, è possibile specificare il momento in cui dovrà essere eseguita:

- **Al prossimo orario pianificato**: l'attività verrà eseguita all'ora specificata (ad esempio, dopo 24 ore).
- **Prima possibile**: l'attività verrà eseguita il prima possibile, quando le azioni che ne impediscono l'esecuzione non saranno più valide.

- **Immediatamente, se l'ora dall'ultima esecuzione supera un valore specificato** - Ora dall'ultima esecuzione (ore): dopo aver selezionato questa opzione, l'attività verrà sempre ripetuta dopo il periodo di tempo (in ore) specificato.

Panoramica attività pianificata

Questa finestra di dialogo consente di visualizzare informazioni dettagliate su un'attività pianificata facendo doppio clic su di essa nella visualizzazione **Pianificazione attività** oppure facendo clic con il pulsante destro del mouse su di essa e scegliendo **Mostra dettagli attività**.

Invia campioni per analisi

La finestra di dialogo per l'invio dei campioni consente di inviare un file o un sito a ESET 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.

Per inviare il file tramite e-mail, comprimere i(l) file utilizzando un programma come WinRAR o WinZip, proteggere l'archivio utilizzando la password `infected` e inviarlo a samples@eset.com. Inserire una descrizione nel campo dell'oggetto e fornire il maggior numero di informazioni possibile sul file (ad esempio, l'indirizzo del sito Web dal quale è stato scaricato).

> Prima di inviare un campione a ESET, assicurarsi che soddisfi uno o entrambi i criteri seguenti:
> - il file o il sito Web non viene rilevato
> - il file o il sito Web viene erroneamente rilevato come minaccia
> - Non sono accettati file personali (che si sceglie di inviare a ESET per la ricerca di eventuali malware) come campioni (ESET Research Lab non esegue controlli su richiesta per gli utenti)
> - Inserire una descrizione nel campo dell'oggetto e fornire il maggior numero di informazioni possibile sul file (ad esempio, l'indirizzo del sito Web dal quale è stato scaricato).

Se almeno uno dei precedenti requisiti non è soddisfatto, non si riceverà alcuna risposta fino a quando non vengono fornite ulteriori informazioni.

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

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

File/sito

Percorso del file o del sito Web che si intende inviare.

E-mail contatto

E-mail di contatto che viene inviata a ESET insieme ai file sospetti e può essere utilizzata per contattare l'utente 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, pertanto, non è possibile rispondere a tutti.

Invio anonimo

Selezionare la casella di controllo accanto a **Invio anonimo** per inviare il file o il sito Web sospetto senza inserire un indirizzo e-mail.

File sospetto

Segni e sintomi osservati dell'infezione malware

Immettere una descrizione del comportamento del file sospetto osservato sul computer.

Origine file (indirizzo URL o fornitore)

Immettere l'origine e le modalità di ottenimento del file (sorgente).

Note e informazioni aggiuntive

Qui è possibile immettere informazioni aggiuntive o una descrizione utile per individuare il file sospetto.

> Il primo parametro - **Segni e sintomi osservati dell'infezione malware** - è obbligatorio. Tuttavia, l'invio di informazioni aggiuntive aiuterà i laboratori ESET a potenziare notevolmente le capacità di identificazione dei campioni.

Sito sospetto

Selezionare una delle opzioni che seguono dal menu a discesa Problemi del sito:

Infetto

Sito Web che contiene un virus o un altro malware distribuito con vari metodi.

Phishing

Utilizzato solitamente per ottenere l'accesso a dati sensibili, quali numeri di conti bancari, codici PIN e così via. Per ulteriori informazioni su questo tipo di attacco, consultare il glossario.

Scam

Sito Web illegale o fraudolento.

Altro

Utilizzare questa opzione se nessuna delle precedenti opzioni è idonea al sito che si sta per inviare.

Note e informazioni aggiuntive

Qui è possibile inserire informazioni aggiuntive o una descrizione utile ai fini dell'analisi del sito Web sospetto.

File falso positivo

All’utente viene richiesto di inviare file rilevati come infezione, ma che in realtà non lo sono, allo scopo di potenziare il motore di rilevamento e garantire la protezione degli altri utenti. I falsi positivi (FP) possono verificarsi quando la sequenza di un file corrisponde alla sequenza contenuta in un motore di rilevamento.

> i Primi tre parametri sono obbligatori allo scopo di identificare le applicazioni legali e di distinguerle da codice dannoso. L'invio di informazioni aggiuntive aiuterà i laboratori ESET a potenziare notevolmente le capacità di identificazione e di elaborazione dei campioni.

Nome e versione applicazione

Titolo del programma e relativa versione (ad esempio, numero, alias o nome del codice).

Origine file (indirizzo URL o fornitore)

Specificare un'origine e le modalità di ottenimento del file (sorgente).

Scopo dell’applicazione

Descrizione generale dell'applicazione, tipo di applicazione (ad esempio browser, lettore multimediale e così via) e relative funzionalità.

Note e informazioni aggiuntive

Qui è possibile inserire informazioni o descrizioni aggiuntive utili ai fini dell'elaborazione del file sospetto.

Sito falso positivo

Si consiglia di inviare siti rilevati come infetti, scam o phishing ma che in realtà non lo sono. I falsi positivi (FP) possono verificarsi quando la sequenza di un file corrisponde alla sequenza contenuta in un motore di rilevamento. Segnalare questo sito web allo scopo di potenziare il motore di rilevamento e garantire la protezione degli altri utenti.

Note e informazioni aggiuntive

Qui è possibile inserire informazioni o descrizioni aggiuntive utili ai fini dell'elaborazione del file sospetto.

Altro

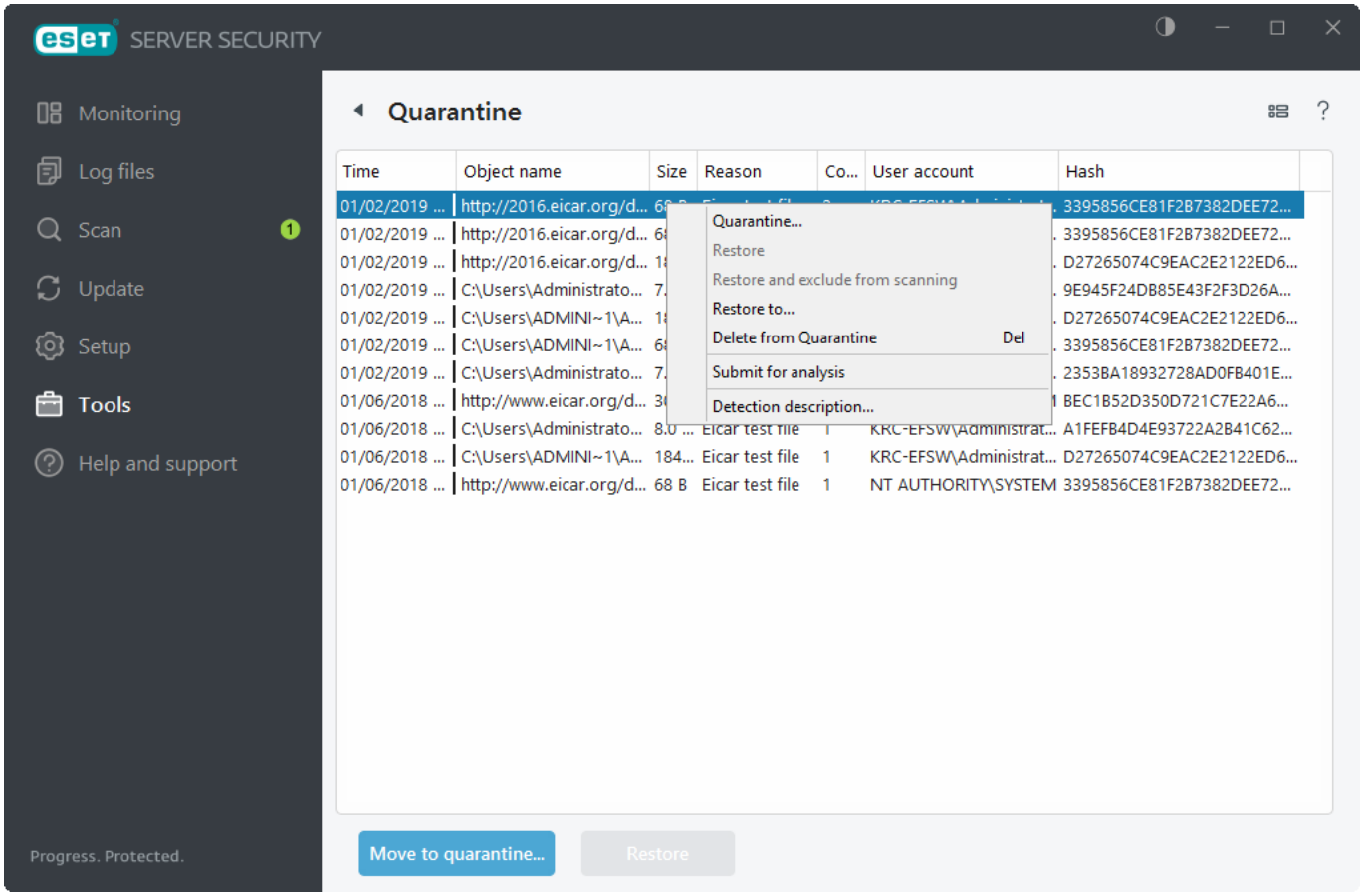
Utilizzare questo modulo se non è possibile classificare il file come File sospetto o Falso positivo.

Motivo per l'invio del file

Immettere una descrizione dettagliata e il motivo dell'invio del file.

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 rimuoverli o, infine, se vengono erroneamente rilevati come minacce da ESET Server 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 anti-malware. 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).

Nel caso in cui gli oggetti di un messaggio di posta elettronica dovessero essere inseriti nel file della quarantena, verrà visualizzato il percorso della casella di posta/cartella/nome file.

Mettere file in quarantena

ESET Server Security mette automaticamente in quarantena i file eliminati (qualora l'utente non abbia provveduto a disattivare questa opzione nella finestra di avviso). Per mettere manualmente in quarantena i file sospetti, fare clic su **Quarantena**. I file della quarantena verranno rimossi dalla loro posizione originale. 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 far ciò, utilizzare la funzione **Ripristina**, disponibile nel menu contestuale, facendo clic con il pulsante destro del mouse sul file desiderato nella

finestra Quarantena. Se un file è contrassegnato come Applicazione potenzialmente indesiderata, sarà disponibile 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 da cui è stato eliminato.

> Se il programma mette 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 Quarantena

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

Elimina dalla quarantena

Fare clic con il pulsante destro del mouse su un oggetto specifico e selezionare **Elimina dalla quarantena** oppure selezionare l'oggetto o gli oggetti di interesse e premere **Elimina** sulla tastiera.

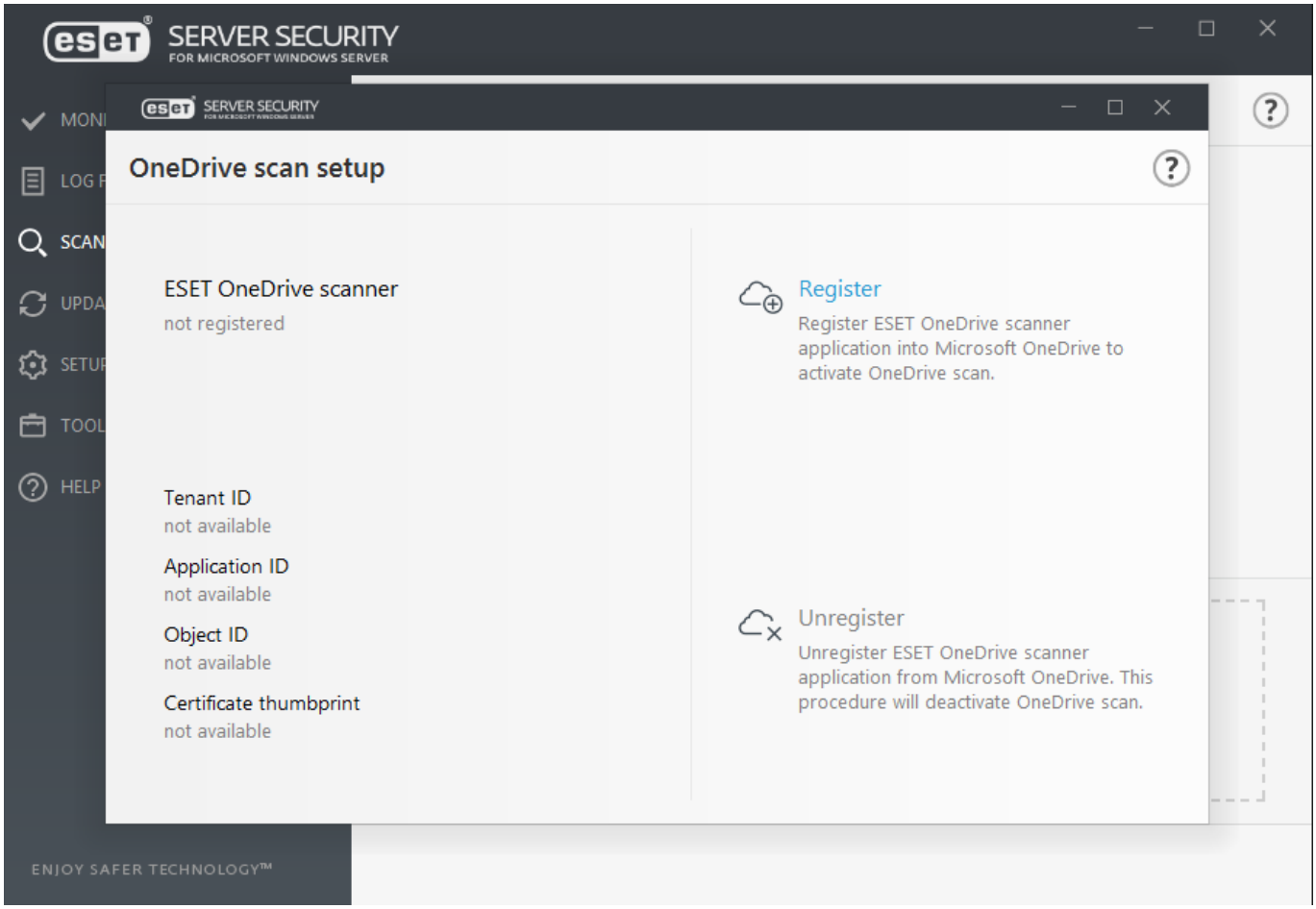
Configurazione controllo OneDrive

Questa funzione consente di controllare i file memorizzati nello spazio di archiviazione cloud Microsoft OneDrive for Business. Il controllo ESET Server Security OneDrive consente di analizzare unicamente i file e le cartelle. Non controlla altri tipi di dati, tra cui e-mail, file di SharePoint, contatti o calendari.

Collegamenti rapidi:

- Registra ESET OneDrive Scanner
- Annulla la registrazione di ESET OneDrive Scanner

Per iniziare a utilizzare il controllo ESET Server Security OneDrive, registrare l'applicazione ESET OneDrive Scanner in Microsoft OneDrive/Microsoft Office 365/Microsoft Azure. Nella pagina di configurazione del controllo OneDrive compaiono lo stato della registrazione (se già eseguita) e i dettagli della registrazione (ID Tenant, ID applicazione, ID oggetto e identificazione personale del certificato). È possibile eseguire o annullare la registrazione di ESET OneDrive Scanner:



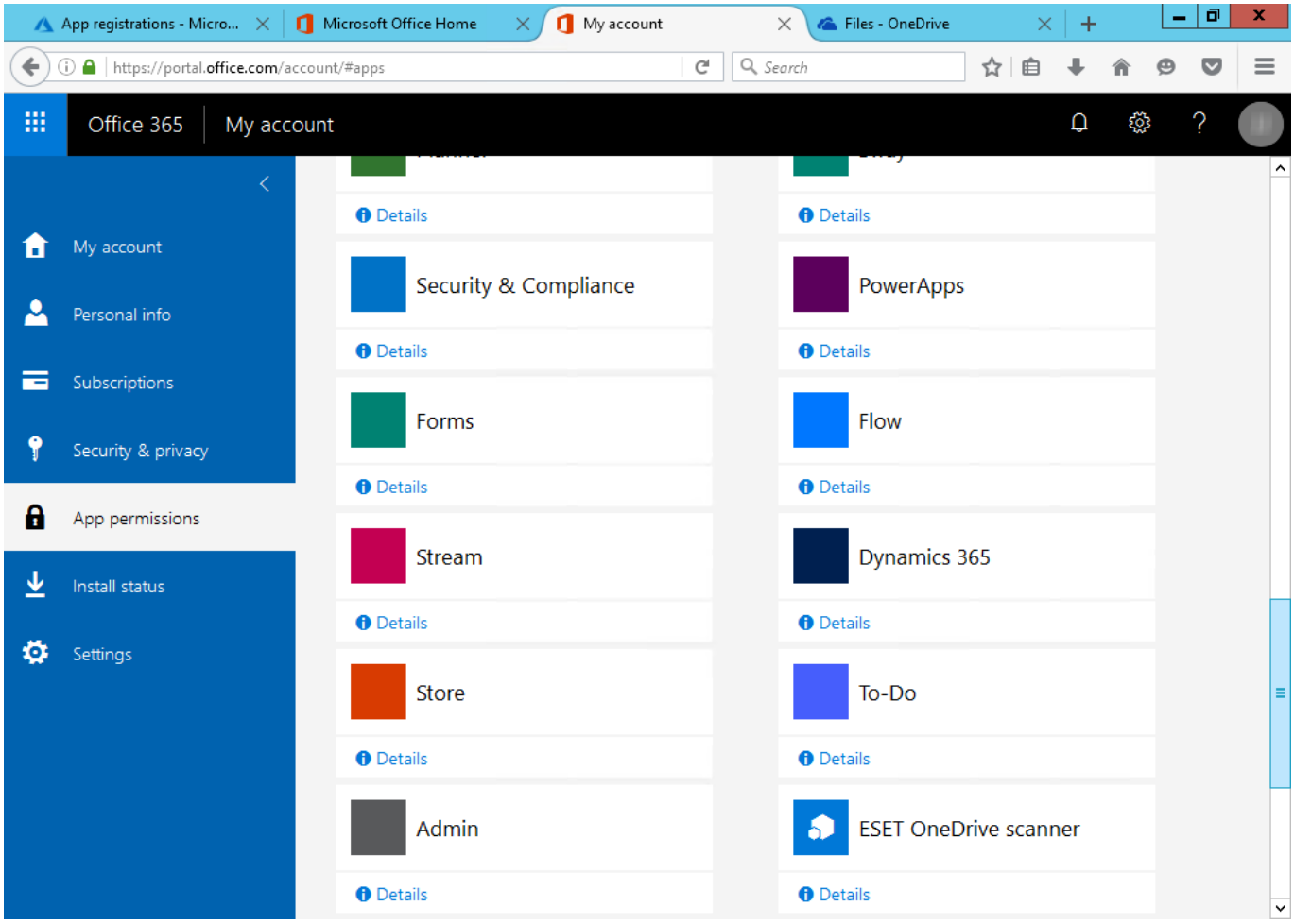
Al termine della registrazione, il controllo OneDrive sarà disponibile nel menu Controllo, nel quale compare un elenco di utenti con la relativa struttura di cartelle e i file che è possibile selezionare per il controllo. Il controllo ESET Server Security OneDrive consente di analizzare i file archiviati dagli utenti su OneDrive for Business.

> Il controllo ESET Server Security OneDrive consente di scaricare i file dallo spazio di archiviazione cloud OneDrive for Business e di eseguire una scansione a livello locale. Al termine del controllo, i file scaricati vengono eliminati. Il download di grandi quantità di dati da OneDrive incide sul traffico di rete.

> Eseguire nuovamente la registrazione con un altro account: Se si desidera registrare ESET Server Security OneDrive Scanner con un nuovo account Microsoft OneDrive for Business/Office 365, è necessario Annullare la registrazione di ESET OneDrive Scanner utilizzata con l'account precedente ed eseguire la registrazione con il nuovo account amministratore Microsoft OneDrive for Business/Office 365.

ESET OneDrive Scanner è registrato come applicazione in Office 365 e Azure:

Portale Office 365: fare clic su **Autorizzazioni app** nella pagina Il mio account per visualizzare l'app ESET OneDrive Scanner.

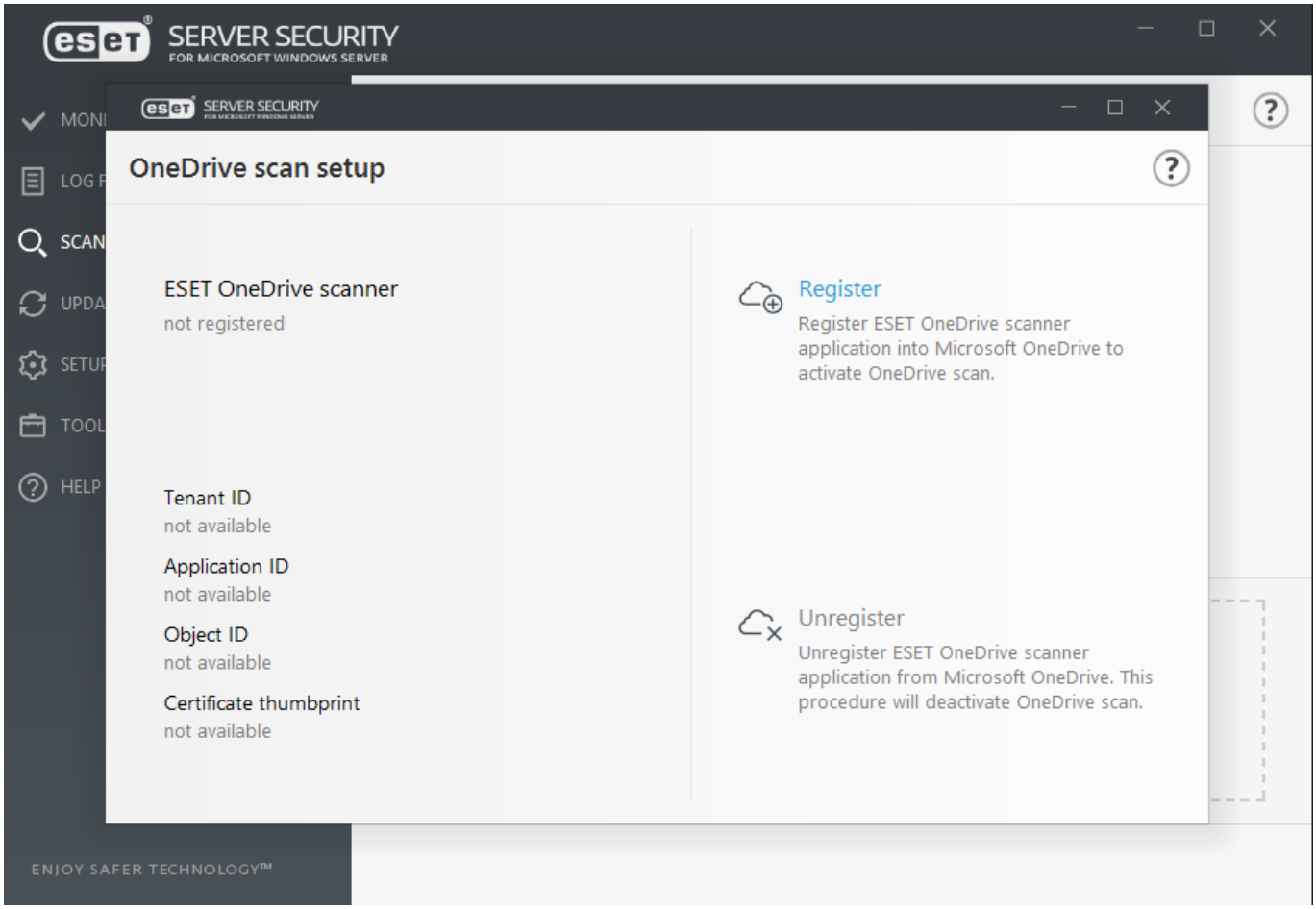


Azure : accedere a **Azure Active Directory** > **Registrazioni app** e fare clic su **Visualizza tutte le applicazioni** per visualizzare l'app ESET OneDrive Scanner. Fare clic sull'app per visualizzarne i dettagli.

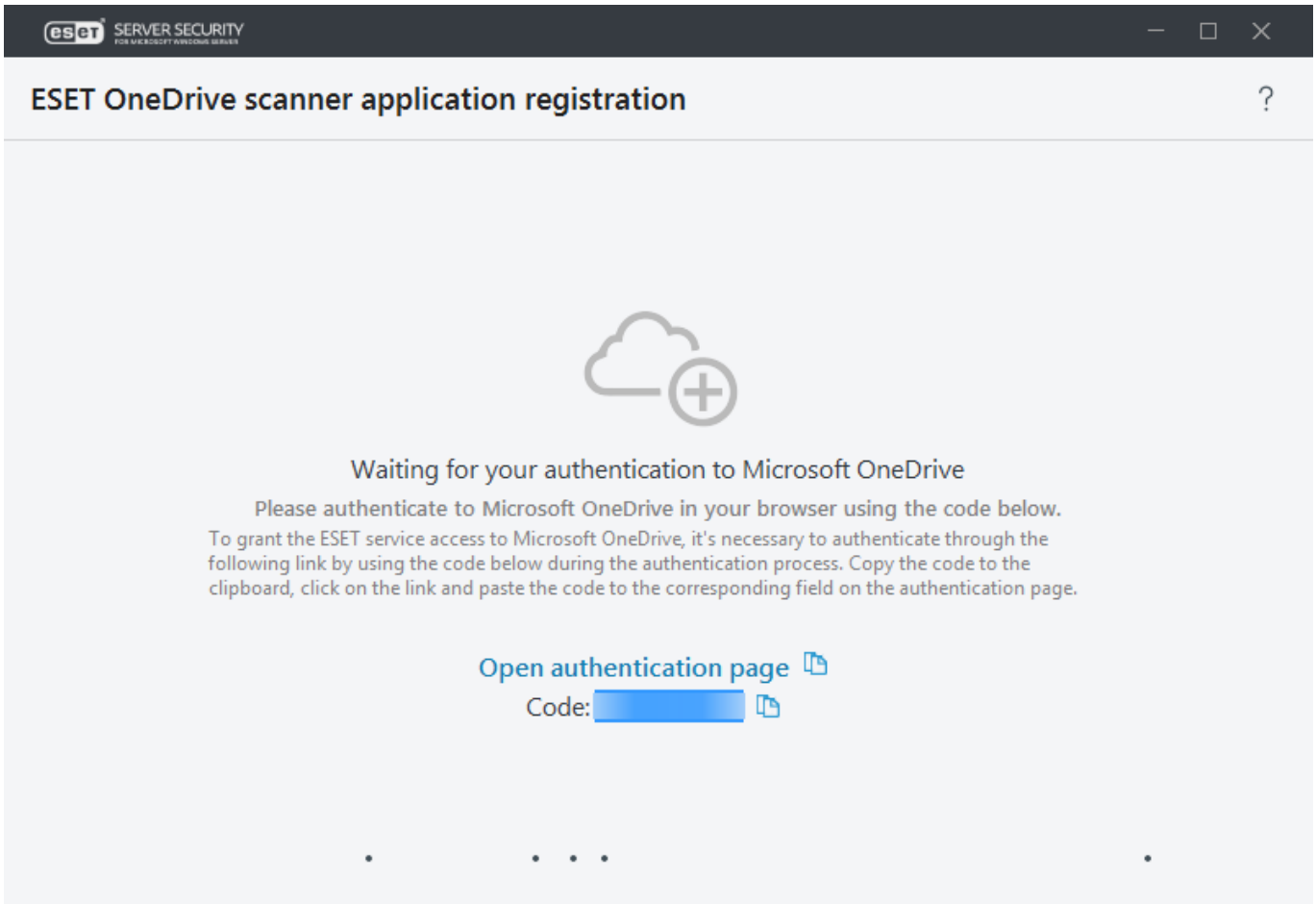
Registra ESET OneDrive Scanner

Utilizzare il seguente processo per registrare l'app ESET OneDrive Scanner per Microsoft OneDrive, Office 365 o Azure:

1. Fare clic su **Registra** per avviare la registrazione dello scanner ESET OneDrive. A questo punto si apre una procedura guidata di registrazione.

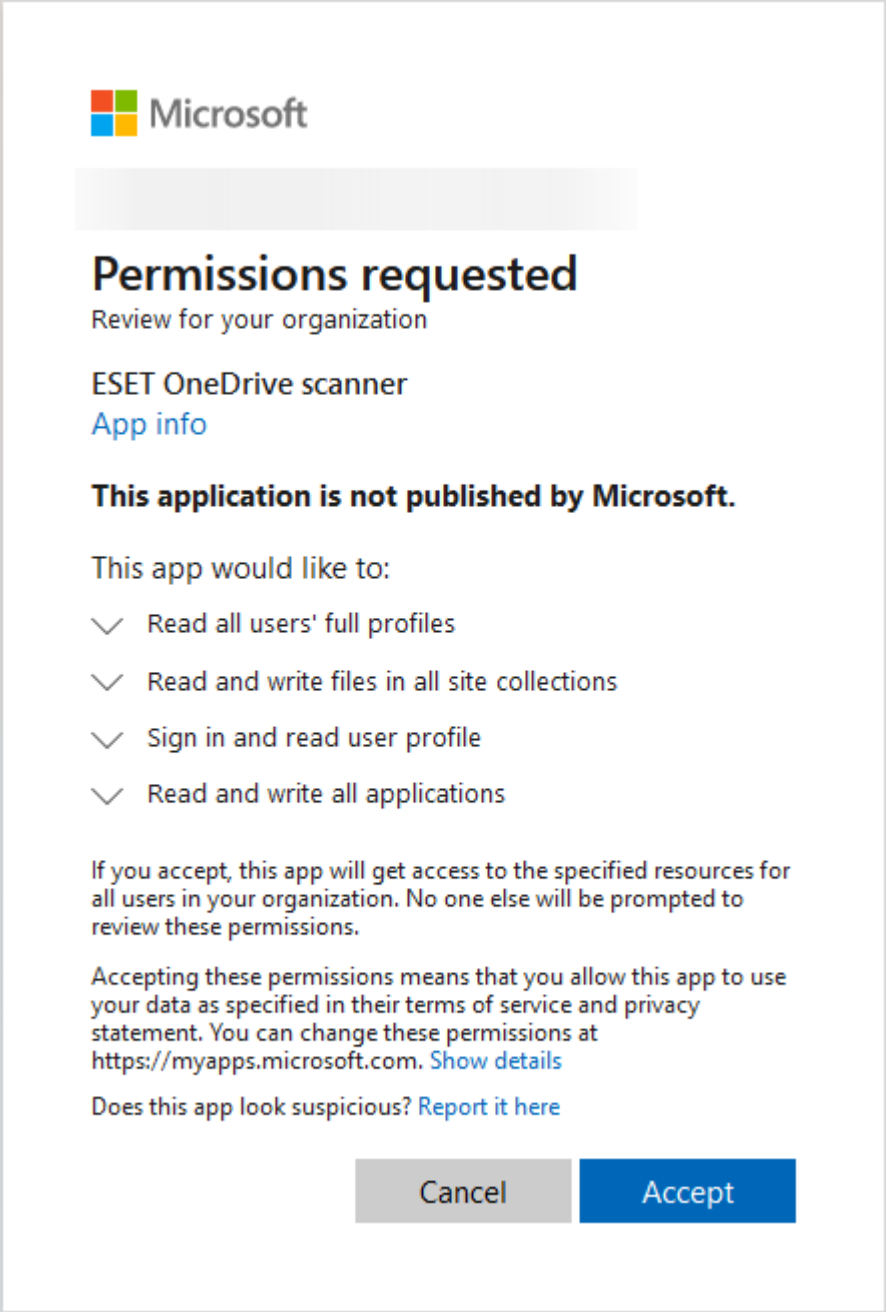


2. Copiare il codice fornito, fare clic su **Apri pagina di autenticazione** e inserire il codice.

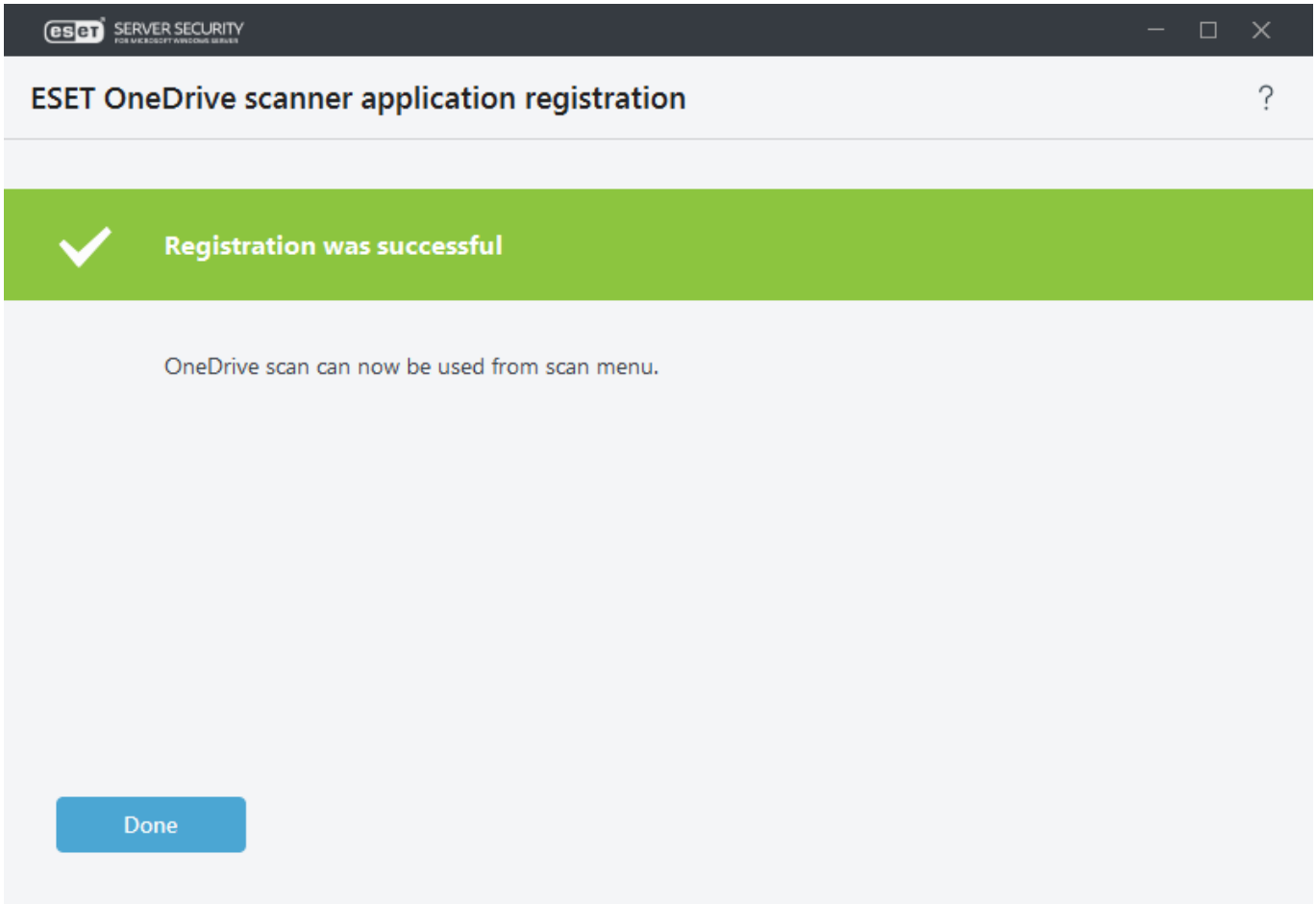


3. Si apre un browser Web contenente la pagina di Microsoft **Seleziona un account**. Fare clic sull'account in uso, se disponibile, oppure inserire le credenziali dell'account amministratore di Microsoft OneDrive/Office 365 e fare clic su **Accedi**.

4. L'app ESET OneDrive Scanner richiede quattro tipi di autorizzazione specificati nel messaggio di accettazione. Fare clic su **Accetto** per consentire a ESET Server Security OneDrive Scanner di accedere ai dati posizionati nello spazio di archiviazione cloud OneDrive.



5. Chiudere il browser web e attendere il completamento della registrazione di ESET OneDrive Scanner. Verrà visualizzato il messaggio **"Registrazione eseguita correttamente"**. Fare clic su **Fine**.



> Il processo di registrazione di ESET OneDrive Scanner potrebbe presentare alcune differenze se è stata eseguita l'autenticazione a un portale Microsoft (OneDrive, Office 365, Azure e così via) con le credenziali dell'account amministratore. Seguire le istruzioni e i messaggi visualizzati sullo schermo della procedura guidata di registrazione.

Se, durante la registrazione di ESET OneDrive Scanner, compare uno degli errori indicati di seguito, fare riferimento alle soluzioni suggerite nei dettagli del messaggio di errore:

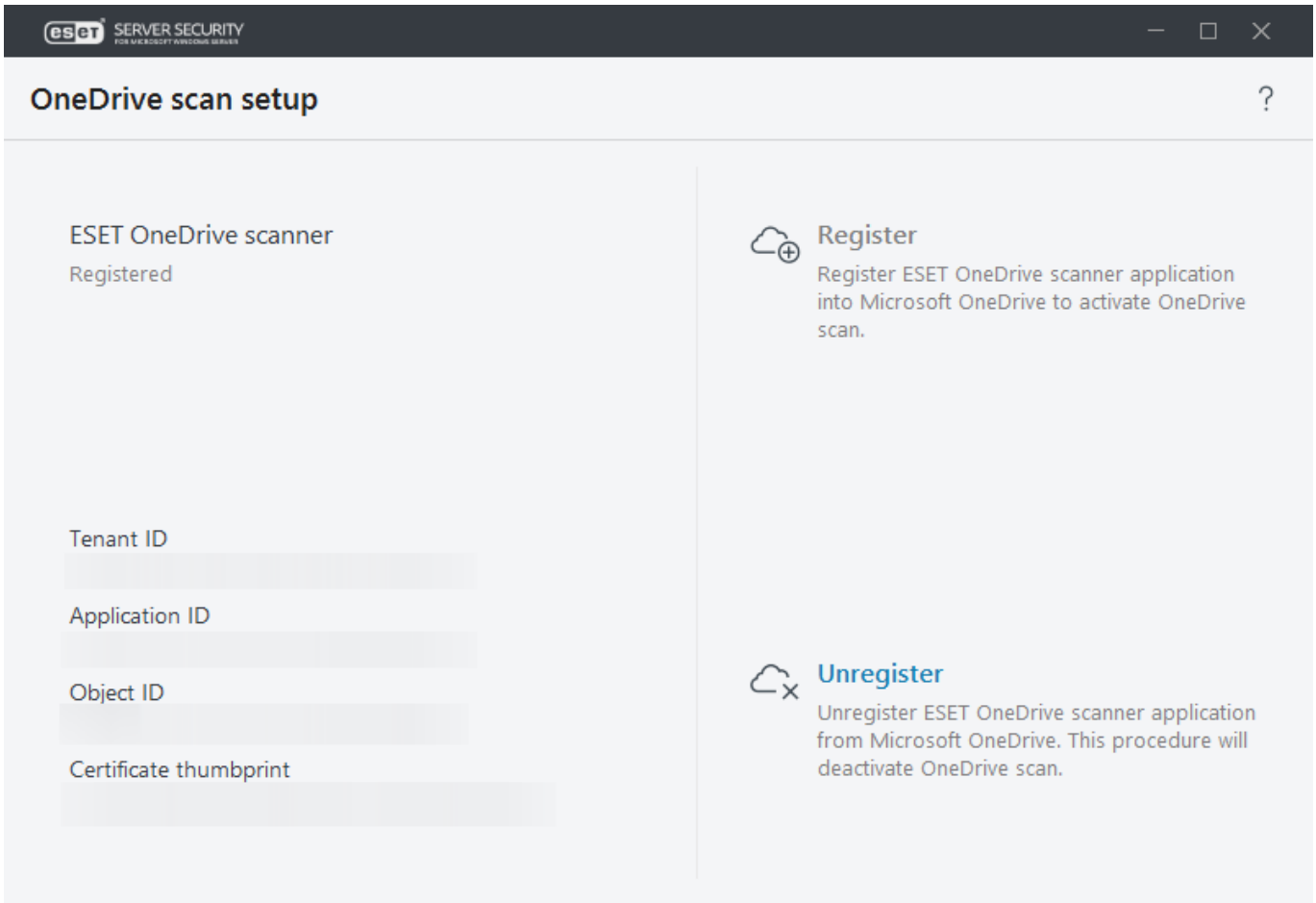
Messaggio di errore	Dettagli del messaggio di errore
Si è verificato un errore imprevisto.	Potrebbe essersi verificato un errore in ESET Server Security. Provare a eseguire nuovamente la registrazione di ESET OneDrive Scanner in un secondo momento. Se il problema persiste, contatta il Supporto tecnico ESET.
Non è stato possibile effettuare la connessione a Microsoft OneDrive.	Controllare la rete e la connessione Internet ed eseguire nuovamente la registrazione di ESET OneDrive Scanner.
È stato ricevuto un errore imprevisto da Microsoft OneDrive.	Nella risposta del messaggio di errore è stato restituito l'errore HTTP 4xx senza soluzione. Se il problema persiste, contattare il Supporto tecnico di ESET.
È stato ricevuto il seguente errore da Microsoft OneDrive.	Il server Microsoft OneDrive ha restituito un errore con un codice/nome specifico. Fare clic su Mostra errore.
L'attività di configurazione è scaduta.	L'attività di configurazione della registrazione di ESET OneDrive Scanner richiede troppo tempo. Provare a eseguire nuovamente la registrazione di ESET OneDrive Scanner in un secondo momento.

Messaggio di errore	Dettagli del messaggio di errore
L'attività di configurazione è stata annullata.	L'utente ha annullato un'attività di registrazione in esecuzione. Eseguire nuovamente la registrazione di ESET OneDrive Scanner se si desidera completare la registrazione.
Un'altra attività di configurazione è già in corso.	È già in esecuzione un'attività di registrazione. Attendere il completamento del primo processo di registrazione ed eseguire nuovamente la registrazione di ESET OneDrive Scanner.

Annulla la registrazione di ESET OneDrive Scanner

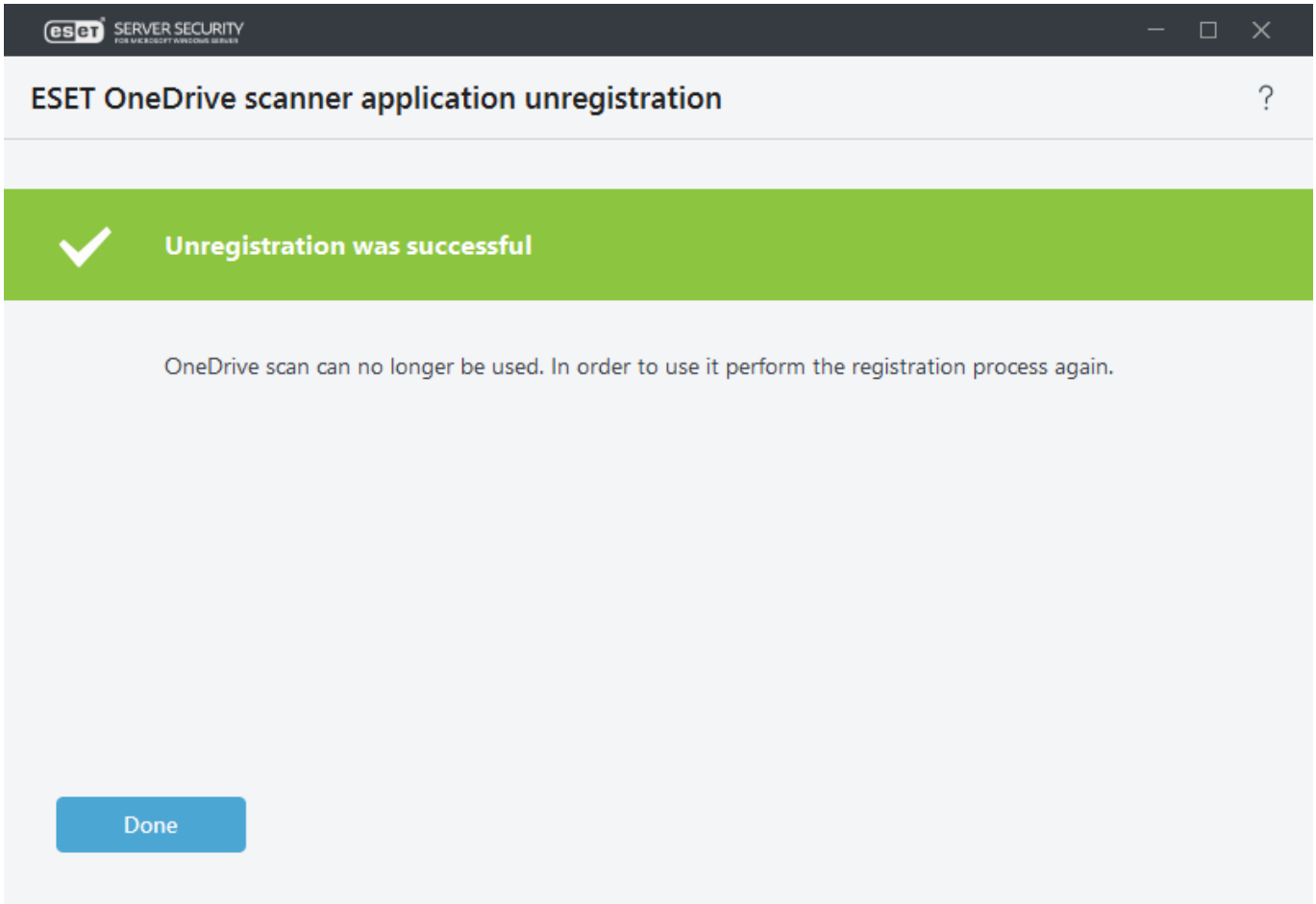
Il processo di annullamento della registrazione consente di rimuovere il certificato e l'app ESET OneDrive Scanner da Microsoft OneDrive, Office 365 o Azure. Questo processo consente inoltre di rimuovere le dipendenze locali e rendere nuovamente disponibile l'opzione Registra.

1. Fare clic su **Configura** > **Server** > **Configurazione del controllo OneDrive** e su **Annulla la registrazione** per avviare il processo di annullamento della registrazione di ESET OneDrive Scanner. A questo punto si apre una procedura guidata di annullamento della registrazione.



2. Fare clic su **Annulla registrazione** per confermare di voler rimuovere ESET OneDrive Scanner. Attendere il completamento del processo di annullamento della registrazione da Microsoft OneDrive.

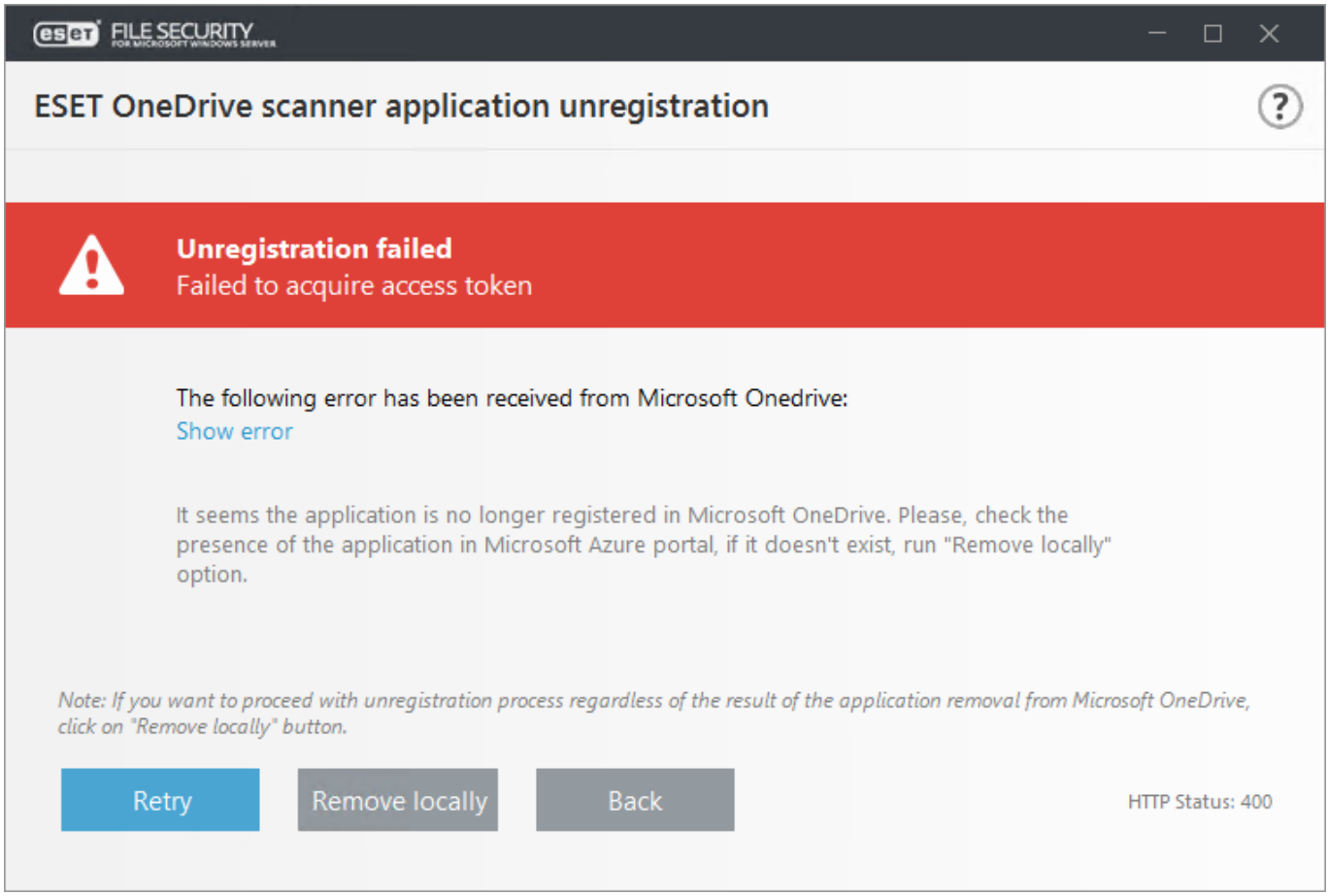
3. Al termine del processo di annullamento della registrazione, nella procedura guidata di annullamento della registrazione verrà visualizzato il messaggio **Annullamento della registrazione eseguito correttamente**.



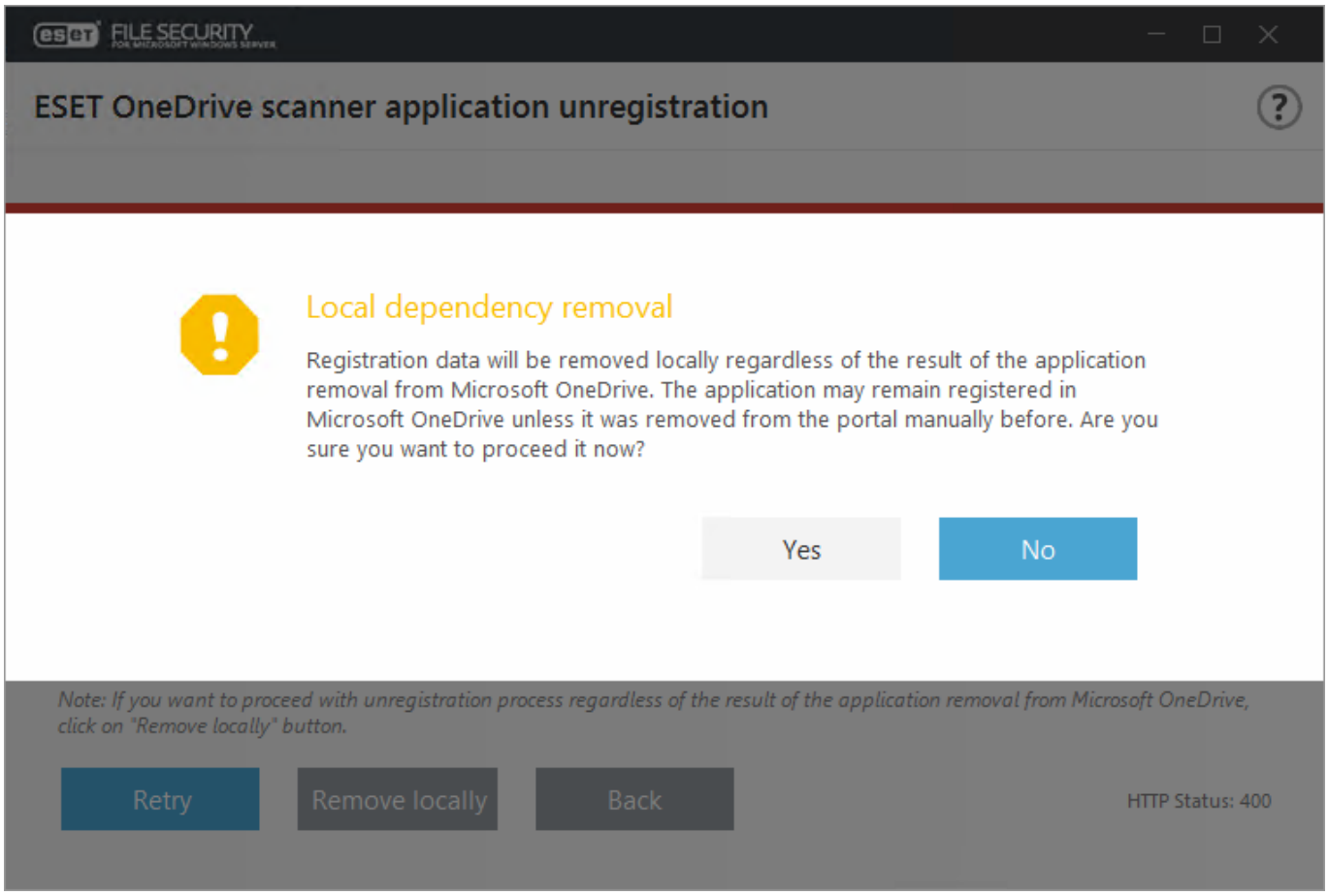
> Se viene visualizzato un messaggio di errore, ad esempio **Annullamento della registrazione non riuscito**, consultare la tabella sottostante per l'elenco dei possibili messaggi di errore e le modalità di risoluzione.

Alcune finestre di dialogo contenenti messaggi di errore consentono all'utente di rimuovere dipendenze locali (problemi di connessione, app inesistenti in Microsoft OneDrive, ecc.). Per rimuovere ESET OneDrive Scanner localmente, seguire la procedura sottostante:

Se il pulsante **Riprova** non funziona e i problemi persistono, fare clic su **Rimuovi localmente** per procedere con il processo di annullamento della registrazione e rimuovere le dipendenze locali di ESET OneDrive Scanner.



5. Fare clic su **Sì** per procedere con la rimozione dell'istanza di ESET OneDrive Scanner locale. ESET OneDrive Scanner non sarà più disponibile e sarà necessario riavviare il processo di registrazione.



La rimozione locale delle dipendenze non incide sulle registrazioni delle app sul portale Azure, né tantomeno sulle autorizzazioni relative alle app sul portale Office 365. In caso di rimozione di ESET OneDrive Scanner in locale per problemi di rete o di connessione con i server Microsoft OneDrive, sarà necessario rimuovere manualmente l'app ESET OneDrive Scanner dalle registrazioni delle app in Azure. Consultare Configurazione del controllo di OneDrive per individuare e rimuovere manualmente ESET OneDrive Scanner dal portale di Azure.

Se, durante l'annullamento della registrazione di ESET OneDrive Scanner, compare uno dei messaggi di errore indicati di seguito, consultare le soluzioni suggerite nei dettagli del messaggio:

Messaggio di errore	Dettagli del messaggio di errore
Il collegamento all'applicazione Azure non è riuscito. Assenza di connessione a Internet.	Controllare la connessione di rete/Internet ed eseguire nuovamente l'annullamento della registrazione. Se si desidera procedere con il processo di annullamento della registrazione senza rimuovere l'app ESET OneDrive Scanner da Microsoft OneDrive, fare clic su **Rimuovi localmente**.
Impossibile acquisire il token di accesso. È stato ricevuto un errore imprevisto da Microsoft OneDrive.	Ci risulta che l'app ESET OneDrive Scanner non sia più registrata con Microsoft OneDrive. L'app ESET OneDrive Scanner potrebbe essere stata eliminata manualmente nel portale Azure. Verificare che l'app ESET OneDrive Scanner sia presente nel portale Microsoft OneDrive o Azure. Se l'app non è disponibile, procedere con il processo di annullamento della registrazione facendo clic su **Rimuovi localmente**.
Impossibile acquisire il token di accesso. È stato ricevuto un errore del server da Microsoft OneDrive.	Microsoft OneDrive ha restituito l'errore HTTP 5xx. Al momento non è possibile completare l'attività di annullamento della registrazione. Provare a eseguire nuovamente l'annullamento della registrazione in un secondo momento.
È stato ricevuto il seguente errore da Microsoft OneDrive.	Il server Microsoft OneDrive ha restituito un errore con un codice/nome specifico. Fare clic su Mostra errore.
Un'altra attività di configurazione è già in corso.	È già in esecuzione un'attività di annullamento della registrazione. Attendere il completamento del primo processo di annullamento della registrazione.

Configurazione avanzata

È possibile configurare le impostazioni e le opzioni in base alle proprie esigenze. Il menu sulla sinistra include le seguenti categorie:

Detection engine

Consente di attivare o disattivare il rilevamento di applicazioni potenzialmente indesiderate, pericolose o sospette e la protezione Anti-Stealth. Specificare le esclusioni di processi o file e cartelle. Configurare la Protezione file system in tempo reale, i parametri di ThreatSense, la protezione basata sul cloud (ESET LiveGrid®), i controlli malware (controllo computer su richiesta e altre opzioni di controllo), controllo Hyper-V e HIPS.

Aggiornamento

Consente di configurare le opzioni di aggiornamento quali profili, età del motore di rilevamento, snapshot per il rollback dei moduli, tipo di aggiornamento, server di aggiornamento personalizzato, server di connessione/proxy, mirror di aggiornamento, accesso ai file di aggiornamento, server HTTP, dettagli account utente per la connessione di rete e così via.

Protezione accesso alla rete

Gestisci protezione di rete: profilo della connessione di rete, firewall, protezione attacchi di rete (IDS), protezione da attacchi di forza bruta e protezione botnet.

Web e e-mail

Consente di configurare il Filtraggio protocolli e le esclusioni (applicazioni e indirizzi IP esclusi) le opzioni di filtraggio del protocollo SSL/TLS, la protezione client di posta (integrazione, protocolli e-mail, avvisi e notifiche), la protezione accesso Web (protocolli Web HTTP/HTTPS e gestione degli indirizzi URL) e la protezione Anti-Phishing client di posta.

Controllo dispositivi

Consente di attivare l'integrazione e configurare le regole e i gruppi del controllo dispositivi.

Configurazione degli strumenti

Consente all'utente di personalizzare strumenti quali ESET CMD, ESET RMM, provider WMI, destinazione del controllo ESET PROTECT, notifiche di Windows Update, file di registro, server proxy, notifiche e-mail, diagnostica, cluster e così via.

Connettività

Se necessario, specificare le impostazioni del server proxy.

Interfaccia utente

Consente di configurare la finestra principale del programma, le informazioni sulla licenza, la protezione con password, il criterio di esecuzione eShell e molto altro ancora.

Notifiche

Consente di configurare le notifiche da visualizzare sul desktop o inviate tramite e-mail per gli stati dell'applicazione, la notifica sul desktop, gli avvisi interattivi e l'inoltro.

Detection engine

Il motore di rilevamento offre protezione dagli attacchi di sistemi dannosi controllando file, e-mail e comunicazioni di rete. In caso di rilevamento di un oggetto classificato come malware, verrà avviata la correzione. Il motore di rilevamento è in grado di eliminarlo bloccandolo in un primo momento, quindi intraprendendo azioni quali pulizia, rimozione o spostamento in quarantena.

Protezione apprendimento automatico e in tempo reale

Il machine learning avanzato, che fa ora parte del motore di rilevamento come livello avanzato di protezione, ne migliora le prestazioni in termini di rilevamento. Per ulteriori informazioni su questo tipo di protezione, consultare il glossario . È possibile configurare i livelli di creazione di report e di protezione delle seguenti categorie:

Malware

Un virus è un frammento di codice dannoso anteposto o allegato ai file esistenti sul computer. Tuttavia, il termine

“virus” è spesso utilizzato in modo non consono. Il “malware” (software dannoso) rappresenta un termine più accurato. Il rilevamento malware viene eseguito dal modulo del motore di rilevamento insieme al componente riconoscimento automatico. Per ulteriori informazioni su questi tipi di applicazione, consultare la relativa voce del glossario.

Applicazioni potenzialmente indesiderate (PUA)

Un'applicazione potenzialmente indesiderata è un software con finalità non necessariamente illecite che, tuttavia, potrebbe installare altri software indesiderati, modificare il comportamento dei dispositivi digitali, eseguire attività non approvate o previste dall'utente o avere altri obiettivi poco chiari.

Questa categoria include: software di annunci pubblicitari, wrapper di download, varie barre degli strumenti dei browser, software con comportamenti ingannevoli, bundleware, trackware, ecc. Per ulteriori informazioni su questi tipi di applicazione, consultare la relativa voce del glossario.

Applicazioni potenzialmente sospette

Software compresso con strumenti di compressione o protettori solitamente utilizzati allo scopo di prevenire tentativi di decodificazione o di offuscamento dei contenuti dei file eseguibili (che nascondono ad esempio la presenza dei malware) attraverso metodi proprietari di compressione e/o crittografia.

Questa categoria include: tutte le applicazioni sconosciute compresse con strumenti di compressione o protettori solitamente utilizzati per la compressione dei malware.

Applicazioni potenzialmente pericolose

Questa classificazione viene utilizzata per software commerciali legittimi che potrebbero essere utilizzati in modo non conforme per scopi illegittimi. Le applicazioni pericolose sono software commerciali legittimi che potrebbero essere utilizzati in modo non corretto per scopi illegittimi.

Questa categoria include: strumenti di cracking, generatori di chiavi di licenza, strumenti di hackeraggio, strumenti di accesso o controllo remoto, applicazioni di password-cracking, keylogger, ecc. (programmi che registrano le battute digitate da un utente). Questa opzione è disattivata per impostazione predefinita.
Per ulteriori informazioni su questi tipi di applicazione, consultare la relativa voce del glossario.

Leggere quanto segue prima di modificare una soglia (o livello) per la categoria Creazione di report o Protezione:

Segnalazione

La creazione di report viene eseguita dal motore di rilevamento e dal componente di machine learning. È possibile impostare la soglia di creazione di report in base alle proprie esigenze e all'ambiente. Non è disponibile una singola configurazione corretta. Pertanto, si consiglia di monitorare il comportamento all'interno dell'ambiente e di stabilire se è più idonea un'impostazione di Creazione di report diversa.
La creazione di report non intraprende alcuna azione con gli oggetti, ma passa le informazioni a un rispettivo livello di protezione e il livello di protezione intraprende azioni di conseguenza.

Aggressivo	**Creazione di report configurata su un livello massimo di sensibilità. Vengono segnalati altri rilevamenti. Sebbene l'impostazione aggressiva possa sembrare più sicura, può essere spesso eccessivamente sensibile, il che potrebbe addirittura essere controproducente.** L'impostazione aggressiva potrebbe falsamente identificare gli oggetti come dannosi e l'azione verrà intrapresa con tali oggetti (in base alle impostazioni di protezione).
Bilanciamento	Questa impostazione rappresenta un bilanciamento ottimale tra le prestazioni e l'accuratezza dei tassi di rilevamento e il numero di oggetti segnalati erroneamente.
Attenzione	Creazione di report configurata per ridurre al minimo gli oggetti identificati erroneamente, mantenendo allo stesso tempo un livello di protezione sufficiente. Gli oggetti vengono segnalati solo in caso di evidenti probabilità e di corrispondenza con il comportamento del malware.
Disattivato	La creazione di report non è attiva. Non sono stati trovati, segnalati o puliti rilevamenti. La segnalazione di malware non può essere disattivata, pertanto, l'impostazione Off non è disponibile per i malware.

Se si desidera Ripristinare i valori predefiniti delle impostazioni in questa sezione, fare clic sulla freccia “a U” accanto all'intestazione della sezione. Tutte le eventuali modifiche apportate in questa sezione andranno perse.

Protezione

Quando un oggetto viene segnalato in base alla configurazione indicata in precedenza e ai risultati del riconoscimento automatico, viene bloccato e viene eseguita un'azione (pulito, rimosso o spostato in quarantena).

Aggressivo	**I rilevamenti dei livelli aggressivi segnalati (o inferiori) vengono bloccati e viene avviata la correzione automatica (ad es. pulizia).**
Bilanciamento	I rilevamenti dei livelli di bilanciamento segnalati (o inferiori) vengono bloccati e viene avviata la correzione automatica (ad es. pulizia).
Attenzione	I rilevamenti di livello “attenzione” segnalati vengono bloccati e viene avviata la correzione automatica (ad es. pulizia).
Disattivato	La creazione di report non è attiva, non è stato trovato, segnalato o pulito alcun rilevamento. La segnalazione di malware non può essere disattivata, pertanto l'impostazione Off non è disponibile per i malware.

Se si desidera Ripristinare le impostazioni predefinite in questa sezione, fare clic sulla freccia “a U” accanto all'intestazione della sezione. Tutte le eventuali modifiche apportate in questa sezione andranno perse.

Per impostazione predefinita, le impostazioni di protezione riconoscimento automatico di cui sopra si applicano anche al controllo del computer su richiesta. Se necessario, è possibile configurare separatamente le impostazioni delle **risposte di rilevamento su richiesta**. Fare clic sull'icona dell’interruttore per disabilitare **Utilizza impostazioni della protezione in tempo reale** e procedere con la configurazione.

Protezione riconoscimento automatico

Il motore di rilevamento offre protezione dagli attacchi di sistemi dannosi controllando file, e-mail e comunicazioni di rete. In caso di rilevamento di un oggetto classificato come malware, verrà avviata la correzione. Il motore di rilevamento è in grado di eliminarlo bloccandolo in un primo momento, quindi intraprendendo azioni quali pulizia, rimozione o spostamento in quarantena.

Protezione apprendimento automatico e in tempo reale

Il machine learning avanzato, che fa ora parte del motore di rilevamento come livello avanzato di protezione, ne migliora le prestazioni in termini di rilevamento. Per ulteriori informazioni su questo tipo di protezione, consultare il glossario . È possibile configurare i livelli di creazione di report e di protezione delle seguenti categorie:

Malware

Un virus è un frammento di codice dannoso anteposto o allegato ai file esistenti sul computer. Tuttavia, il termine “virus” è spesso utilizzato in modo non consono. Il “malware” (software dannoso) rappresenta un termine più accurato. Il rilevamento malware viene eseguito dal modulo del motore di rilevamento insieme al componente riconoscimento automatico. Per ulteriori informazioni su questi tipi di applicazione, consultare la relativa voce del glossario.

Applicazioni potenzialmente indesiderate (PUA)

Un'applicazione potenzialmente indesiderata è un software con finalità non necessariamente illecite che, tuttavia, potrebbe installare altri software indesiderati, modificare il comportamento dei dispositivi digitali, eseguire attività non approvate o previste dall'utente o avere altri obiettivi poco chiari.

Questa categoria include: software di annunci pubblicitari, wrapper di download, varie barre degli strumenti dei browser, software con comportamenti ingannevoli, bundleware, trackware, ecc. Per ulteriori informazioni su questi tipi di applicazione, consultare la relativa voce del glossario.

Applicazioni potenzialmente sospette

Software compresso con strumenti di compressione o protettori solitamente utilizzati allo scopo di prevenire tentativi di decodificazione o di offuscamento dei contenuti dei file eseguibili (che nascondono ad esempio la presenza dei malware) attraverso metodi proprietari di compressione e/o crittografia.

Questa categoria include: tutte le applicazioni sconosciute compresse con strumenti di compressione o protettori solitamente utilizzati per la compressione dei malware.

Applicazioni potenzialmente pericolose

Questa classificazione viene utilizzata per software commerciali legittimi che potrebbero essere utilizzati in modo non conforme per scopi illegittimi. Le applicazioni pericolose sono software commerciali legittimi che potrebbero essere utilizzati in modo non corretto per scopi illegittimi.

Questa categoria include: strumenti di cracking, generatori di chiavi di licenza, strumenti di hackeraggio, strumenti di accesso o controllo remoto, applicazioni di password-cracking, keylogger, ecc. (programmi che registrano le battute digitate da un utente). Questa opzione è disattivata per impostazione predefinita.
Per ulteriori informazioni su questi tipi di applicazione, consultare la relativa voce del glossario.

Leggere quanto segue prima di modificare una soglia (o livello) per la categoria Creazione di report o Protezione:

Segnalazione

La creazione di report viene eseguita dal motore di rilevamento e dal componente di machine learning. È possibile impostare la soglia di creazione di report in base alle proprie esigenze e all'ambiente. Non è disponibile una singola configurazione corretta. Pertanto, si consiglia di monitorare il comportamento all'interno dell'ambiente e di stabilire se è più idonea un'impostazione di Creazione di report diversa.
La creazione di report non intraprende alcuna azione con gli oggetti, ma passa le informazioni a un rispettivo livello di protezione e il livello di protezione intraprende azioni di conseguenza.

Aggressivo	**Creazione di report configurata su un livello massimo di sensibilità. Vengono segnalati altri rilevamenti. Sebbene l'impostazione aggressiva possa sembrare più sicura, può essere spesso eccessivamente sensibile, il che potrebbe addirittura essere controproducente.** L'impostazione aggressiva potrebbe falsamente identificare gli oggetti come dannosi e l'azione verrà intrapresa con tali oggetti (in base alle impostazioni di protezione).
Bilanciamento	Questa impostazione rappresenta un bilanciamento ottimale tra le prestazioni e l'accuratezza dei tassi di rilevamento e il numero di oggetti segnalati erroneamente.
Attenzione	Creazione di report configurata per ridurre al minimo gli oggetti identificati erroneamente, mantenendo allo stesso tempo un livello di protezione sufficiente. Gli oggetti vengono segnalati solo in caso di evidenti probabilità e di corrispondenza con il comportamento del malware.
Disattivato	La creazione di report non è attiva. Non sono stati trovati, segnalati o puliti rilevamenti. La segnalazione di malware non può essere disattivata, pertanto, l'impostazione Off non è disponibile per i malware.

Se si desidera Ripristinare i valori predefiniti delle impostazioni in questa sezione, fare clic sulla freccia “a U” accanto all'intestazione della sezione. Tutte le eventuali modifiche apportate in questa sezione andranno perse.

Protezione OneDrive e riconoscimento automatico

Segnalazione
Eseguito dal motore di rilevamento e dal componente di riconoscimento automatico. La creazione di report non esegue alcuna azione con gli oggetti (questa operazione viene eseguita dal rispettivo livello di protezione).
Protezione
Configurare i parametri nella sezione OneDrive per influenzare l'azione intrapresa con gli oggetti segnalati.
Se si desidera Ripristinare le impostazioni predefinite in questa sezione, fare clic sulla freccia “a U” accanto all'intestazione della sezione. Tutte le eventuali modifiche apportate in questa sezione andranno perse.
Configurare la protezione riconoscimento automatico utilizzando eShell. Il nome del contesto in eShell è **MLP**.
Aprire eShell in modalità interattiva e accedere a MLP:
```
computer onedrive mlp
```
Vedere qual è l'impostazione di creazione dei report corrente per le applicazioni sospette:
```
get suspicious-reporting
```
Se si desidera una creazione di report meno rigorosa, modificare l'impostazione in Prudente:
```
set suspicious-reporting cautious
```

Protezione Hyper-V e riconoscimento automatico

Segnalazione
Eseguito dal motore di rilevamento e dal componente di riconoscimento automatico. La creazione di report non esegue alcuna azione con gli oggetti (questa operazione viene eseguita dal rispettivo livello di protezione).
Protezione
Configurare i parametri nella sezione Controllo Hyper-V per influenzare l'azione intrapresa con gli oggetti segnalati.
Se si desidera Ripristinare le impostazioni predefinite in questa sezione, fare clic sulla freccia “a U” accanto all'intestazione della sezione. Tutte le eventuali modifiche apportate in questa sezione andranno perse.
Configurare la protezione riconoscimento automatico utilizzando eShell. Il nome del contesto in eShell è **MLP**.
Aprire eShell in modalità interattiva e accedere a MLP:
```
computer hyperv mlp
```
Vedere qual è l'impostazione di creazione dei report corrente per le applicazioni sospette:
```
get suspicious-reporting
```
Se si desidera una creazione di report meno rigorosa, modificare l'impostazione in Prudente:
```
set suspicious-reporting cautious
```

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 server durante un controllo o di un software che entra in conflitto con il controllo (ad esempio, software di backup).

Da non confondere con estensioni escluse, esclusioni processi o filtro esclusioni.

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.

Selezionare il tipo di esclusione e fare clic su **Modifica** per aggiungerne una nuova o modificare quelle esistenti:

- Esclusioni prestazioni: escludere file e cartelle dal controllo.
- Esclusioni rilevamento: escludere oggetti dal controllo utilizzando criteri specifici: percorso, hash del file o nome del rilevamento.

Esclusioni dal controllo

Questa funzione consente all'utente di escludere file e cartelle dal controllo. Le esclusioni di prestazioni sono utili per escludere il controllo a livello di file delle applicazioni critiche o nel momento in cui il controllo provoca un comportamento anomalo del sistema o riduce le prestazioni.

Percorso

Esclude un percorso specifico (file o directory) per il computer in uso. Non utilizzare i caratteri jolly - l’asterisco (*) all’interno di un percorso. Per ulteriori informazioni, consultare il seguente articolo della Knowledge Base.

Per escludere contenuti dalla cartella, non dimenticare di aggiungere l'asterisco (*) alla fine del percorso (*C:\Tools**).
C:\Tools non verrà escluso, in quanto dal punto di vista dello scanner, anche gli *Strumenti* possono essere un nome di file.

Commento

Aggiungere un Commento facoltativo per riconoscere facilmente l'esclusione in futuro.

Esclusioni percorso tramite l'utilizzo di un asterisco:
C:\Tools*: il percorso deve terminare con la barra rovesciata (\) e l'asterisco (*) per indicare che si tratta di una cartella e che verranno esclusi tutti i relativi contenuti (file e sottocartelle)
C:\Tools*.*: stesso comportamento di C:\Tools* (ricorsivo)
C:\Tools*.dat: consente di escludere i file dat nella cartella Strumenti
C:\Tools\sg.dat: consente di escludere questo specifico file situato nel percorso esatto

Per escludere tutti i file in una cartella, digitare il percorso alla cartella e utilizzare la maschera *.*. Per escludere solo i file doc, utilizzare la maschera *.doc.
Se il nome di un file eseguibile contiene un certo numero di caratteri (e i caratteri variano) e si conosce con certezza solo il primo carattere (ad esempio "D"), utilizzare il seguente formato:
D????.exe (i punti interrogativi sostituiscono i caratteri mancanti/sconosciuti)

Utilizzare variabili di sistema quali %PROGRAMFILES% per definire le esclusioni del controllo.
Per escludere la cartella File di programma utilizzando la variabile di sistema, utilizzare il percorso %PROGRAMFILES%\ (durante l'aggiunta delle esclusioni, assicurarsi di aggiungere la barra rovesciata alla fine del percorso)
Per escludere tutti i file in una sottodirectory %HOMEDRIVE%, utilizzare il percorso %HOMEDRIVE%\Excluded_Directory*.*
Le seguenti variabili possono essere utilizzate nel formato di esclusione del percorso:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
Le variabili di sistema specifiche dell'utente (come %TEMP% o %USERPROFILE%) o le variabili di ambiente (come %PATH%) non sono supportate.

Esclusioni dalla rilevazione

Si tratta di un altro metodo per escludere gli oggetti dal controllo, utilizzando il nome del rilevamento, il percorso o il relativo hash. Le esclusioni di rilevamento non escludono i file e le cartelle dal controllo (come ad esempio le esclusioni delle prestazioni). Le esclusioni di rilevamento escludono gli oggetti solo se vengono rilevate dal motore di rilevamento e nell'elenco delle esclusioni è presente una regola appropriata.

Il metodo più semplice per creare un'esclusione basata sul rilevamento consiste nell'utilizzo di un rilevamento esistente in **File di rapporto** > Rilevamenti. Fare clic con il pulsante destro del mouse su un record di rapporto

(rilevamento) e selezionare **Crea esclusione**. Questa operazione consentirà di aprire la procedura guidata di esclusione con criteri predefiniti.

Per creare manualmente un'esclusione di rilevamento, fare clic su **Modifica** > **Aggiungi** (o su **Modifica** in caso di modifica di un'esclusione esistente) e specificare uno o più dei seguenti criteri (è possibile combinarli):

Percorso

Esclude un percorso specifico (file o directory). È possibile ricercare uno specifico percorso/file o inserire la stringa manualmente. Non utilizzare i caratteri jolly - l'asterisco (*) all'interno di un percorso. Per ulteriori informazioni, consultare il seguente articolo della Knowledge Base.

> Per escludere contenuti dalla cartella, non dimenticare di aggiungere l'asterisco (*) alla fine del percorso (C:\Tools*).
> *C:\Tools* non verrà escluso, in quanto dal punto di vista dello scanner, anche gli *Strumenti* possono essere un nome di file.

Hash

Esclude un file in base a un hash specificato (SHA1), indipendentemente dal tipo, dalla posizione, dal nome o dalla relativa estensione.

Nome del rilevamento

Inserire un nome di rilevamento (minaccia) valido. La creazione di un'esclusione solo in base al nome del rilevamento potrebbe costituire un rischio per la sicurezza. Si consiglia di combinare il nome del rilevamento con il percorso. Questo criterio di esclusione può essere utilizzato solo per alcuni tipi di rilevamenti.

Commento

Aggiungere un **Commento** facoltativo per riconoscere facilmente l'esclusione in futuro.

ESET PROTECT include la gestione delle esclusioni di rilevamento per creare un'esclusione di rilevamento e applicarla a più computer/gruppi.

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.

> Esclusioni percorso tramite l'utilizzo di un asterisco:
> C:\Tools*: il percorso deve terminare con la barra rovesciata (\) e l'asterisco (*) per indicare che si tratta di una cartella e che verranno esclusi tutti i relativi contenuti (file e sottocartelle)
> C:\Tools*.*: stesso comportamento di C:\Tools* (ricorsivo)
> C:\Tools*.dat: consente di escludere i file dat nella cartella Strumenti
> C:\Tools\sg.dat: consente di escludere questo specifico file situato nel percorso esatto

> Per escludere una minaccia, inserire il nome di un rilevamento valido nel seguente formato:
> @NAME=Win32/Adware.Optmedia
> @NAME=Win32/TrojanDownloader.Delf.QQI
> @NAME=Win32/Bagle.D

Per escludere tutti i file in una cartella, digitare il percorso alla cartella e utilizzare la maschera *.*. Per escludere solo i file doc, utilizzare la maschera *.doc
Se il nome di un file eseguibile contiene un certo numero di caratteri (e i caratteri variano) e si conosce con certezza solo il primo carattere (ad esempio "D"), utilizzare il seguente formato:
D????.exe (i punti interrogativi sostituiscono i caratteri mancanti/sconosciuti)

Utilizzare variabili di sistema quali *%PROGRAMFILES%* per definire le esclusioni del controllo.
Per escludere la cartella File di programma utilizzando la variabile di sistema, utilizzare il percorso %PROGRAMFILES%\ (durante l'aggiunta delle esclusioni, assicurarsi di aggiungere la barra rovesciata alla fine del percorso)
Per escludere tutti i file in una sottodirectory %HOMEDRIVE%, utilizzare il percorso %HOMEDRIVE%\Excluded_Directory*.*
Le seguenti variabili possono essere utilizzate nel formato di esclusione del percorso:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
Le variabili di sistema specifiche dell'utente (come %TEMP% o %USERPROFILE%) o le variabili di ambiente (come %PATH%) non sono supportate.

Procedura guidata di creazione di un'esclusione

L'esclusione consigliata è preselezionata in base al tipo di rilevamento, ma è possibile specificare ulteriori criteri di esclusione per i rilevamenti. Fare clic su **Modifica criteri**:

- **File esatti**: escludere ciascun file in base all'hash SHA-1.
- **Rilevamento**: specificare il nome del rilevamento per escludere ciascun file che contiene tale rilevamento.
- **Percorso + rilevamento**: specificare il nome e il percorso del rilevamento (incluso il nome del file) per escludere ciascun file con un rilevamento posizionato nel percorso specificato.

Aggiungere un **Commento** facoltativo per riconoscere facilmente l'esclusione in futuro.

Opzioni avanzate

Tecnologia Anti-Stealth

Sistema sofisticato che rileva programmi pericolosi, come ad esempio i rootkit, che possono eludere i controlli del sistema operativo. Solitamente, questi tipi di programmi non sono rilevabili mediante l'utilizzo di tecniche standard.

AMSI

Consentire a Microsoft Antimalware Scan Interface (AMSI) di controllare gli script Powershell eseguiti da Windows Script Host.

Esclusioni automatiche

Gli sviluppatori delle applicazioni server e dei sistemi operativi consigliano di escludere i gruppi di file e cartelle di lavoro critici dai controlli anti-malware per la maggior parte dei loro prodotti. I controlli anti-malware possono avere un'influenza negativa sulle prestazioni di un server, creando conflitti e impedendo persino l'esecuzione di alcune applicazioni sul server. Le esclusioni aiutano a ridurre al minimo il rischio di potenziali conflitti e a migliorare le prestazioni generali del server quando è in esecuzione il software anti-malware. Visualizzare l'elenco completo dei file esclusi dal controllo per i prodotti ESET Server.

La funzione “esclusioni automatiche” viene abilitata dopo aver attivato ESET Server Security con una licenza valida ed eseguito l’aggiornamento iniziale per includere i moduli più recenti.

> Le esclusioni automatiche per i file del database di Microsoft SQL Server funzionano per la posizione predefinita. Se i database di Microsoft SQL Server sono presenti in posizioni diverse da quelle predefinite, sono disponibili due opzioni. Aggiungere manualmente le esclusioni o escludere automaticamente i file del database. Per l’esclusione automatica, ESET Server Security necessita di un’autorizzazione per l’accesso in lettura all’istanza di Microsoft SQL Server per trovare i percorsi utilizzati per i file del database. Se in ESET Server Security viene visualizzato un messaggio di errore relativo alla disponibilità di diritti insufficienti, risolverlo concedendo all’account NO_AUTHORITY\SYSTEM l’autorizzazione **Visualizza qualsiasi definizione** per ciascuna istanza di Microsoft SQL Server eseguita sul server con ESET Server Security.
> Per ulteriori informazioni, consultare l’articolo della Knowledge Base su come Aggiungere autorizzazioni per ottenere percorsi dei dati del database per generare esclusioni automatiche per Microsoft SQL Server.

ESET Server Security identifica le applicazioni server e i file del sistema operativo del server critici e li aggiunge automaticamente all'elenco di Esclusioni. Tutte le esclusioni automatiche sono abilitate per impostazione predefinita. È possibile disabilitare/abilitare le esclusioni di ciascuna applicazione server utilizzando la barra di scorrimento con il seguente risultato:

- Quando questa opzione è abilitata, eventuali file e cartelle critici verranno aggiunti all'elenco di file esclusi dal controllo. Ogni volta che il server viene riavviato, il sistema esegue un controllo automatico delle esclusioni e aggiorna l'elenco in caso di modifiche del sistema o dell'applicazione (ad esempio, in caso di installazione di una nuova applicazione server). Questa impostazione garantisce sempre l'applicazione delle Esclusioni automatiche consigliate.

- In caso di disabilitazione, i file e le cartelle esclusi automaticamente saranno rimossi dall'elenco. Tutte le esclusioni definite dall'utente inserite manualmente non saranno influenzate.

Per identificare e generare esclusioni automatiche, ESET Server Security utilizza un'applicazione dedicata, *eAutoExclusions.exe*, posizionata nella cartella di installazione. Non è necessaria alcuna interazione da parte dell'utente, ma è possibile utilizzare la riga di comando per elencare le applicazioni server rilevate sul sistema attraverso l'esecuzione di `eAutoExclusions.exe -servers`. Per visualizzare la sintassi completa, utilizzare `eAutoExclusions.exe -?`.

Account con autorizzazioni elevate

Questa funzione consente a ESET Server Security di generare ulteriori esclusioni di risorse come condivisioni di rete, percorsi di file di database di Microsoft SQL Server o archiviazione di condivisione di file Skype for Business. Per estendere la funzionalità di esclusione automatica, abilitare l’account con autorizzazioni elevate e immettere il nome utente e la password dell’account amministratore locale o di dominio. Se lo si desidera, è possibile creare

un nuovo account dedicato a tale scopo, ma è necessario assicurarsi che l’account sia un membro del dominio built-in Administrators (BA) group o del dominio locale Administrators group.

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 Server 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 di pulire il file infetto per ripristinarne lo stato originale prima della pulizia. 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 un'azione individualmente per ciascuna minaccia nell'elenco oppure utilizzare **Seleziona azione per tutte le minacce specificate** e scegliere un'azione per selezionare tutte le minacce nell'elenco, quindi fare clic su **Fine**.

Eliminazione dei file negli archivi

In modalità 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 anche solo di un file infetto, verrà eliminato l'intero archivio di appartenenza dell'oggetto, indipendentemente dallo stato degli altri file.

Protezione file system in tempo reale

La protezione file system in tempo reale consente di controllare tutti gli eventi correlati ai malware nel sistema. In tutti i file vengono ricercati codici dannosi al momento dell'apertura, della creazione o dell'esecuzione sul computer. Per impostazione predefinita, la protezione file system in tempo reale viene avviata all'avvio del sistema e garantisce un controllo ininterrotto.

In casi particolari (p. es., in caso di conflitto con un altro scanner in tempo reale), la protezione in tempo reale può essere disabilitata deselezionando **Avvia automaticamente protezione file system in tempo reale** in **Configurazione avanzata** (**F5**) in **Protezione file system in tempo reale** > **Di base**.

ESET Server Security è compatibile con le macchine che utilizzano Azure File Sync Agent con il cloud a livelli abilitato. ESET Server Security riconosce i file con l'attributo *FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESS*.

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 file**: controllo in caso di apertura/accesso ai file.
- **Creazione file**: controllo in caso di creazione/modifica dei file.
- **Esecuzione file**: controllo in caso di esecuzione dei file.
- **Accesso ai supporti rimovibili**: controllo durante l'accesso all'archivio rimovibile. In caso di inserimento di un supporto rimovibile che contiene un settore di avvio nel dispositivo, il settore di avvio viene immediatamente controllato. Questa opzione non abilita il controllo dei file dei supporti rimovibili. Il controllo dei file dei supporti rimovibili è posizionato in **Supporti da controllare Supporti rimovibili**. Per garantire un corretto funzionamento del settore di avvio dei supporti rimovibili, mantenere i Settori di avvio/UEFI abilitati nei parametri di ThreatSense.

Esclusioni processi

Consente all'utente di escludere processi specifici. Ad esempio, in caso di esclusione dei processi della soluzione di backup, tutte le operazioni dei file a essi attribuite vengono ignorate e considerate sicure, riducendo in tal modo l'interferenza con il processo di backup.

Parametri di ThreatSense

La protezione file system in tempo reale, che viene attivata da vari eventi di sistema, tra cui l'accesso a un file, controlla tutti i tipi di supporti. Può essere configurata allo scopo di gestire i file di nuova creazione in base a modalità diverse rispetto a quelle utilizzate per i file esistenti. Ad esempio, questa operazione potrebbe essere eseguita 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 **Detection engine** > **Protezione file system in tempo reale**. Fare clic su **Parametri ThreatSense** > **Altro** e selezionare o deselezionare **Abilita ottimizzazione intelligente**.

Parametri ThreatSense aggiuntivi

È possibile modificare le opzioni dettagliate dei **Parametri ThreatSense aggiuntivi per i file di nuova creazione o modifica** o dei **Parametri ThreatSense aggiuntivi per i file eseguiti**.

Parametri di 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.

> Per ulteriori informazioni relative al controllo automatico del file di avvio, consultare Controllo all'avvio.

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** (**F5**) 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:

- Controllo Hyper-V
- Controllo OneDrive
- Protezione file system in tempo reale
- Controlli malware
- Controllo stato di inattività
- Controllo all'avvio
- Protezione documenti
- Protezione client di posta
- Protezione accesso Web

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

Controlla le minacce che attaccano la memoria operativa del sistema.

Settori di avvio/UEFI

Consente all'utente di controllare i settori di avvio alla ricerca di virus nel record di avvio principale ("Master Boot Record", MBR). In caso di una macchina virtuale Hyper-V, il disco MBR viene controllato in modalità di sola lettura.

Database WMI

Consente di eseguire il controllo dell'intero database WMI ricercando riferimenti a file infetti o malware incorporati come dati.

Registro di sistema

Consente di eseguire il controllo del registro di sistema, di tutte le chiavi e le sottochiavi ricercando riferimenti a file infetti o malware incorporati come dati.

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

Opzioni di controllo

Selezionare i metodi utilizzati durante la ricerca di infiltrazioni nel sistema. Sono disponibili le seguenti opzioni:
Euristica
L'euristica è un algoritmo che analizza l'attività (dannosa) dei programmi. Il vantaggio principale offerto da questa tecnologia consiste nella capacità di identificare software dannosi precedentemente inesistenti o non conosciuti dal database del motore di rilevamento precedente.
Euristica avanzata/DNA 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).

Pulizia

Le impostazioni di pulizia determinano il comportamento dello scanner durante la pulizia di file infetti. La protezione in tempo reale e altri moduli di protezione dispongono dei seguenti livelli di correzione (per es. pulizia).
Correggi sempre il rilevamento
Tentativo di correzione del rilevamento durante la pulizia degli oggetti senza alcun intervento da parte dell’utente. I file di sistema sono un’eccezione. Se non è possibile correggere il rilevamento, tali oggetti vengono lasciati nella posizione originale.
Correggi il rilevamento se sicuro; mantienilo in caso contrario
Tentativo di correzione del rilevamento durante la pulizia degli oggetti senza alcun intervento da parte dell’utente. Se non è possibile correggere un rilevamento per i file o gli archivi di sistema (con file puliti e infetti), l’oggetto segnalato viene mantenuto nella posizione originale.
Correggi il rilevamento se sicuro; chiedi in caso contrario
Tentativo di correzione del rilevamento durante la pulizia degli oggetti. In alcuni casi, se ESET Server Security non è in grado di eseguire un’azione automatica, all’utente verrà richiesto di scegliere un’azione (rimuovi o ignora). Questa impostazione è consigliata nella maggior parte dei casi.
Chiedi sempre all'utente finale
Non verrà tentata alcuna azione automatica da parte di ESET Server Security. All’utente verrà richiesto di scegliere un’azione.

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 all'utente di definire i tipi di file da escludere dal 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:

Controllo flussi di dati alternativi (ADS)

I flussi di dati alternativi utilizzati dal file system NTFS sono associazioni di file e cartelle invisibili alle normali tecniche di controllo. Molte infiltrazioni tentano di eludere il rilevamento camuffandosi in flussi di dati alternativi.

Esegui controlli in background con priorità bassa

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

Registra tutti gli oggetti

In caso di selezione di questa opzione, il file del rapporto consentirà di visualizzare tutti i file controllati, anche quelli non infetti.

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 Ottimizzazione intelligente non è attivata, durante il controllo vengono applicate solo le impostazioni definite dall'utente di moduli specifici nell'architettura di ThreatSense.

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 predefinite oggetti

Attivare questa opzione per utilizzare le impostazioni predefinite (nessun limite). ESET Server Security ignorerà le impostazioni personalizzate dell'utente.

Dimensione massima oggetto

Definisce la dimensione massima degli oggetti su cui eseguire il controllo. Il modulo di protezione specifico eseguirà unicamente il controllo degli oggetti di dimensioni inferiori rispetto a quelle specificate. Questa opzione dovrebbe essere modificata solo da utenti esperti con motivi 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 di protezione 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

Per modificare le impostazioni del controllo degli archivi, deselezionare **Impostazioni predefinite controllo degli archivi**.

Livello di nidificazione degli archivi

Consente all'utente di specificare il livello massimo di controllo degli archivi. Valore predefinito: 10. Per gli oggetti rilevati dalla protezione trasporto posta, il livello di annidamento effettivo è +1 in quanto l'archivio allegato in un'e-mail è considerato di primo livello.

> ✓ Se il livello di annidamento è impostato su 3, un file di archivio con livello di annidamento 3 sarà controllato solo a livello di trasporto fino al livello effettivo 2. Di conseguenza, se si desidera controllare gli archivi mediante la protezione trasporto posta fino al livello 3, è necessario impostare il valore del **Livello di annidamento degli archivi** su 4.

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.

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

Parametri ThreatSense aggiuntivi

Parametri ThreatSense aggiuntivi per i file appena creati e modificati

I file appena creati o modificati hanno 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 modulo. 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 dalle loro dimensioni effettive. Per modificare le impostazioni di controllo degli archivi, disabilitare **Impostazioni predefinite di controllo degli archivi**.

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 ed ESET LiveGrid® allo scopo di ridurre l'impatto sulle prestazioni del sistema.

Estensioni file esclusi dal controllo

Un'estensione è la parte del nome di un file delimitata da un punto. L'estensione definisce il tipo di file. Normalmente vengono controllati tutti i file. Tuttavia, se si desidera escludere file con una specifica estensione, la configurazione dei parametri ThreatSense consente di escludere i file dal controllo in base alla relativa estensione. L'esclusione potrebbe rivelarsi utile nel caso in cui il controllo di alcuni tipi di file impedisca il corretto funzionamento di un'applicazione.

Per aggiungere una nuova estensione all'elenco, fare clic su **Aggiungi**. Immettere l'estensione nel campo di testo (ad esempio tmp) e fare clic su **OK**. Se si seleziona **Inserisci valori multipli**, è possibile aggiungere estensioni di file multipli delimitate da righe, virgole o punti e virgola (ad esempio, scegliere **Punto e virgola** dal menu a discesa come separatore e digitare `edb;eml;tmp`).
È possibile utilizzare un simbolo speciale ? (punto interrogativo). Il punto interrogativo rappresenta un simbolo qualsiasi (ad esempio `?db`).

Per visualizzare l'estensione (tipo di file) per tutti i file in un sistema operativo Windows, deselezionare **Nascondi estensioni per i tipi di file noti** sotto a **Pannello di controllo** > **Opzioni cartella** > **Visualizza**.

Esclusioni processi

La funzione "Esclusioni dei processi" consente all'utente di escludere processi di applicazioni solo dal controllo anti-malware all'accesso. Il ruolo critico dei server dedicati (server dell'applicazione, server di archiviazione, ecc.) richiede backup periodici obbligatori allo scopo di garantire un recupero tempestivo da incidenti di qualsiasi tipo.

Per potenziare la velocità del backup, l'integrità del processo e la disponibilità del servizio, durante il backup vengono utilizzate alcune tecniche note per la loro capacità di entrare in conflitto con la protezione anti-malware a livello dei file. Possono verificarsi problemi simili durante un tentativo di esecuzione di migrazioni in tempo reale delle macchine virtuali.

L'unico modo efficace per evitare queste due situazioni consiste nella disattivazione del software anti-malware. Escludendo processi specifici (ad esempio, quelli della soluzione di backup), tutte le operazioni dei file attribuite a tali processi vengono ignorate e considerate sicure, riducendo in tal modo l'interferenza con il processo di backup. Si consiglia di prestare la massima attenzione quando si creano le esclusioni, in quanto uno strumento di backup escluso può accedere a file infetti senza attivare un avviso. È questo il motivo per cui le autorizzazioni estese sono consentite esclusivamente nel modulo della protezione in tempo reale.

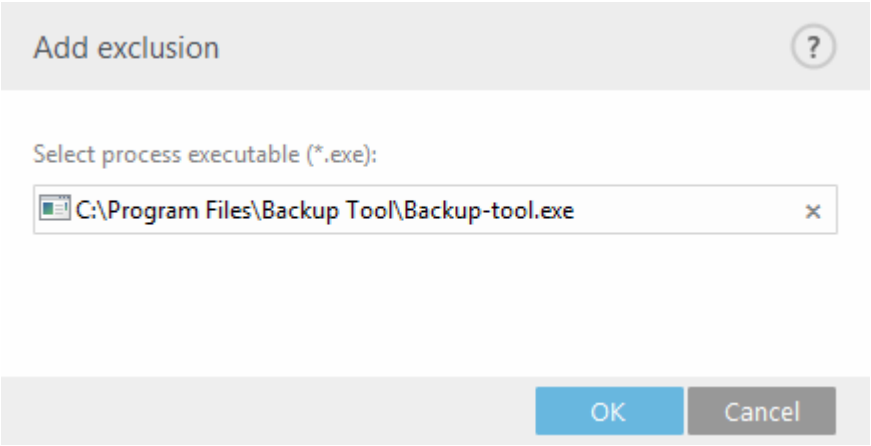
La funzione Esclusioni processi aiuta a ridurre al minimo il rischio di potenziali conflitti e a migliorare le prestazioni delle applicazioni escluse. Tale condizione registra, a sua volta, un effetto positivo sulle prestazioni generali e sulla stabilità del sistema operativo. L'esclusione di un processo/applicazione consiste nell'esclusione del relativo file eseguibile (*.exe*).

È possibile aggiungere file eseguibili all'elenco dei processi esclusi tramite **Configurazione avanzata (F5)** > **Detection engine** > **Protezione file system in tempo reale** > **Di base** > **Esclusioni processi** o utilizzando l'elenco dei processi in esecuzione dal menu principale **Strumenti** > **Processi in esecuzione**.

Questa funzione è stata progettata per escludere gli strumenti di backup. Escludendo il processo dello strumento di backup dal controllo consente di assicurare la stabilità del sistema e non si ripercuote sulle prestazioni del backup che non viene rallentato mentre è in esecuzione.

Fare clic su **Modifica** per aprire la finestra di gestione **Esclusioni processi** dove è possibile **Aggiungere** esclusioni e ricercare il file eseguibile (ad esempio Backup-tool.exe), che verrà escludo dal controllo. Non appena il file *.exe* viene aggiunto alle esclusioni, l'attività di questo processo non è monitorata da ESET Server Security e non viene eseguito alcun controllo sulle operazioni dei file effettuate dal processo.

Se non si utilizza la funzione di ricerca durante la selezione del file eseguibile del processo, sarà necessario inserire manualmente il percorso completo del file eseguibile. In caso contrario, l'esclusione non funzionerà correttamente e HIPS potrebbe segnalare errori.



È inoltre possibile **Modificare** i processi esistenti o **Eliminarli** dalle esclusioni.

La protezione accesso Web non tiene conto di questa esclusione. Di conseguenza, in caso di esclusione del file eseguibile del browser Web in uso, il controllo dei file scaricati continua a essere eseguito. In tal modo, risulta ancora possibile rilevare un'infiltrazione. Poiché lo scenario illustrato è solo un esempio, si sconsiglia di creare esclusioni per i browser Web.

Protezione basata sul cloud

ESET LiveGrid® 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 LiveGrid®.

Durante l'installazione di ESET Server Security, selezionare una delle seguenti opzioni:

- È possibile decidere di non attivare ESET LiveGrid®. Il software non perderà alcuna funzionalità ma, in alcuni casi, ESET Server Security potrebbe rispondere più lentamente alle nuove minacce rispetto all'aggiornamento del database del motore di rilevamento.

- È possibile configurare ESET LiveGrid® 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 LiveGrid® raccoglierà informazioni sul computer dell'utente in relazione alle nuove minacce rilevate. Tali informazioni possono includere un campione o una copia del file in cui è contenuta la minaccia, il percorso 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 Server Security viene configurato per l'invio di file sospetti al laboratorio antivirus ESET per l'analisi. Sono sempre esclusi file con specifiche estensioni, ad esempio .docx o .xlsx. È inoltre possibile aggiungere altre estensioni in presenza di specifici file che l'utente o la società dell'utente non desidera inviare.

Attiva il sistema di reputazione ESET LiveGrid® (scelta consigliata)

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

Attiva il sistema di feedback ESET LiveGrid®

I dati saranno inviati a ESET Research Lab per ulteriori analisi.

Invia report arresti e dati diagnostici

Inviare dati quali report arresti, moduli o dump memoria.

Invia statistiche anonime

Consente a ESET di raccogliere informazioni sulle nuove minacce rilevate, ad esempio nome, data e ora di rilevamento, metodo di rilevamento e metadati associati alla minaccia, sui file controllati (hash, nome del file, origine del file, telemetria), sugli URL bloccati e sospetti, sulla versione e configurazione del prodotto, incluse le informazioni sul sistema in uso.

E-mail contatto (facoltativo)

Il contatto e-mail dell'utente può essere inviato insieme ai file sospetti e potrebbe essere utilizzato per contattare l'utente qualora fossero richieste ulteriori informazioni ai fini dell'analisi. Si tenga presente che l'utente non riceverà una risposta da ESET salvo nel caso in cui siano necessarie ulteriori informazioni.

Invio di campioni

Invio automatico dei campioni infetti
Tutti i campioni infetti saranno inviati a ESET per essere analizzati e per migliorare in futuro il rilevamento.
- Tutti i campioni infetti
- Tutti i campioni tranne i documenti
- Non inviare

Invio automatico dei campioni sospetti
I campioni sospetti simili alle minacce e/o i campioni con caratteristiche o comportamenti insoliti vengono inviati a ESET per l'analisi.
- **Eseguibile**: include i file eseguibili .exe, .dll, .sys
- **Archivi**: include i tipi di file dell'archivio .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- **Script**: include i tipi di file dello script .bat, .cmd, .hta, .js, .vbs, .js, .ps1
- **Altro**: include i tipi di file .jar, .reg, .msi, .swf, .lnk
- **Possibili e-mail indesiderate**: migliora il rilevamento globale di messaggi indesiderati.
- **Documenti**: include documenti di Microsoft Office o PDF con contenuti attivi.

Esclusioni
Fare clic su Modifica accanto a Esclusioni in ESET LiveGrid® per configurare le modalità di invio delle minacce ai laboratori antivirus ESET per l'analisi.
Dimensione massima dei campioni (MB)
Definire le dimensioni massime dei campioni inviati automaticamente.

ESET LiveGuard Advanced

Per abilitare il servizio ESET LiveGuard Advanced su una macchina client utilizzando ESET PROTECT Web Console. In ESET PROTECT Web Console creare un nuovo criterio o modificarne uno esistente e assegnarlo alle macchine sulle quali si desidera utilizzare ESET LiveGuard Advanced.

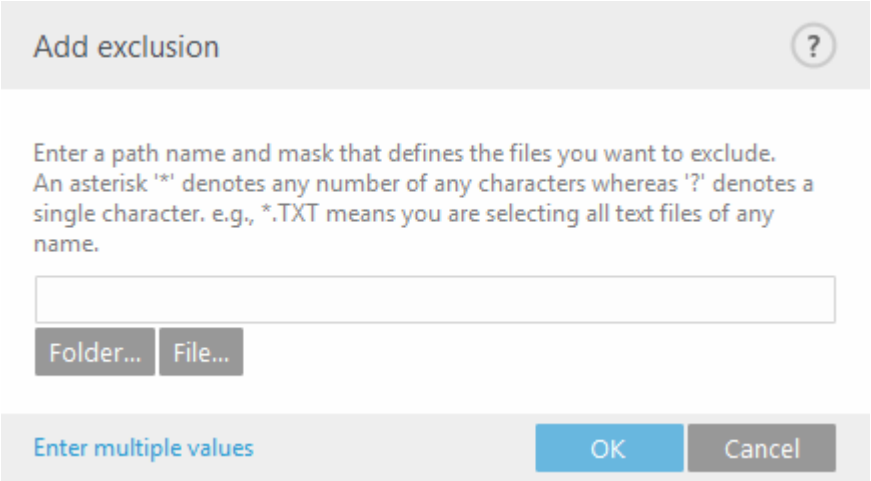
Filtro esclusione

Il Filtro di esclusione consente di escludere dall'invio determinati file/cartelle. È ad esempio utile escludere file che potrebbero contenere informazioni riservate, quali documenti o fogli di calcolo.

I file elencati non saranno mai inviati ai laboratori ESET per l'analisi, anche se contengono codice sospetto.

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



Se si rileva un file sospetto, è possibile inviarlo per l'analisi ai laboratori delle minacce. Se viene individuata un'applicazione dannosa, essa verrà aggiunta al successivo aggiornamento del modulo di rilevamento.

Controlli malware

Questa sezione fornisce opzioni per selezionare i parametri del controllo.

> Questo selettore del profilo di controllo si applica al **Controllo su richiesta**, al Controllo Hyper-V e al Controllo OneDrive.

Profilo selezionato

Serie specifica di parametri utilizzati dal Controllo su richiesta. È possibile utilizzare uno dei profili del controllo predefiniti oppure creare un nuovo profilo. I profili del controllo utilizzano differenti parametri del motore ThreatSense.

Elenco di profili

Per crearne uno nuovo, fare clic su **Modifica**. Immettere il nome del profilo e fare clic su **Aggiungi**. Il nuovo profilo verrà visualizzato nel menu a discesa **Profilo selezionato** in cui sono presenti i profili del controllo esistenti.

Destinazioni di controllo

Per controllare una destinazione specifica, fare clic su **Modifica** e scegliere un'opzione dal menu a discesa oppure selezionare destinazioni specifiche dalla struttura (ad albero) della cartella.

Parametri di ThreatSense

Modificare i parametri del controllo per il controllo del computer su richiesta.

Risposte su richiesta e di rilevamento

La creazione di report viene eseguita dal motore di rilevamento e dal componente di riconoscimento automatico. Se necessario, è possibile configurare separatamente le impostazioni delle **risposte di rilevamento su richiesta**. Fare clic sull'icona dell'interruttore per disabilitare **Utilizza impostazioni della protezione in tempo reale** e procedere con la configurazione.

Gestione profili

Il menu a discesa Profilo di controllo consente all'utente di selezionare profili di controllo predefiniti.

- Controllo intelligente
- Controllo menu contestuale
- Controllo approfondito
- Il mio profilo (si applica al Controllo Hyper-V, ai Profili di aggiornamento e al Controllo OneDrive)

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.

La Gestione profili viene utilizzata in tre posti all'interno di ESET Server Security.

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.

Aggiornamento

L'editor dei profili consente agli utenti di creare nuovi profili di aggiornamento. È necessario solo creare profili di aggiornamento personalizzati se il computer utilizza vari metodi di connessione ai server di aggiornamento.

Controllo Hyper-V

Creare un nuovo profilo, selezionare **Modifica** accanto a **Elenco di profili**. Il nuovo profilo verrà visualizzato nel menu a discesa **Profilo selezionato** in cui sono presenti i profili del controllo esistenti.

Controllo OneDrive

Creare un nuovo profilo, selezionare **Modifica** accanto a **Elenco di profili**. Il nuovo profilo verrà visualizzato nel menu a discesa **Profilo selezionato** in cui sono presenti i profili del controllo esistenti.

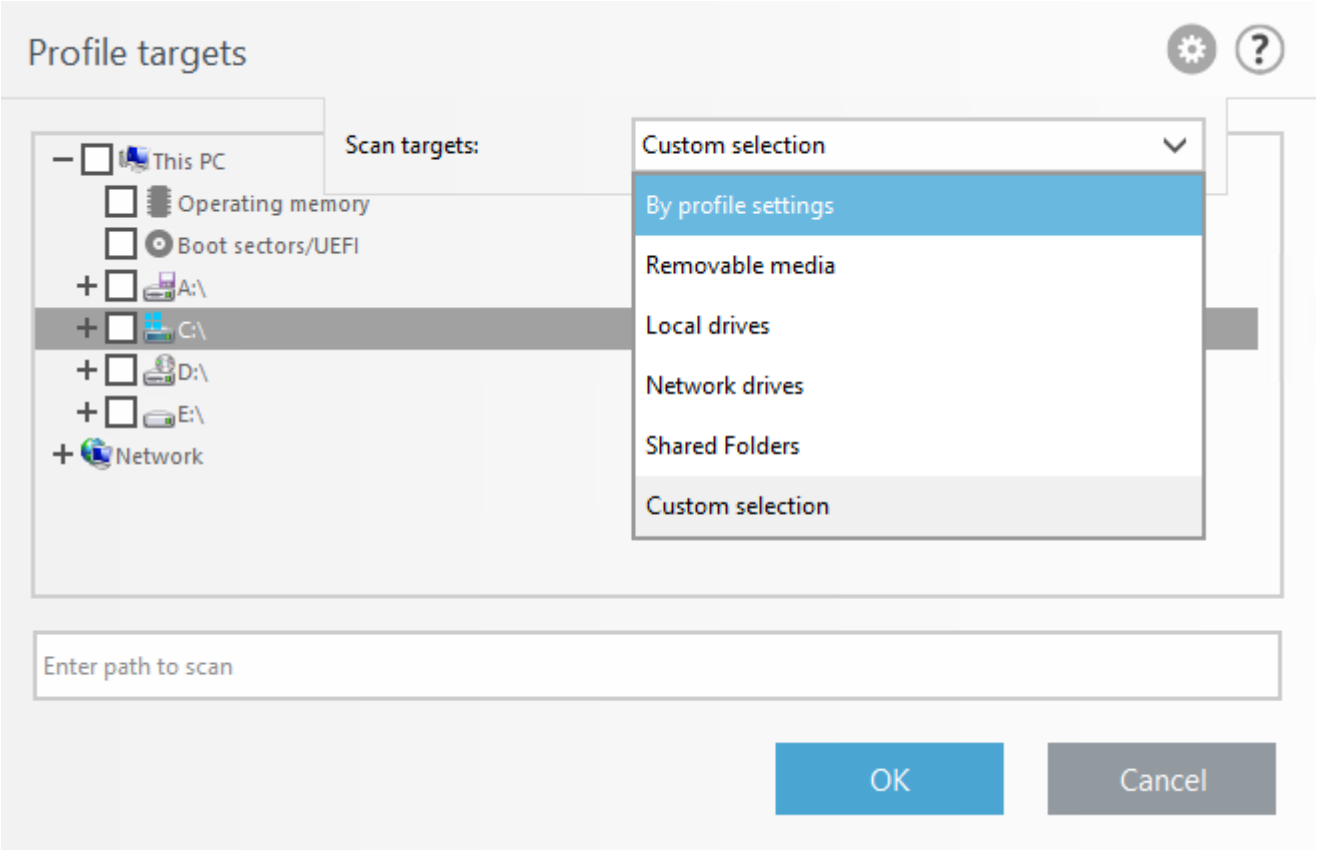
Destinazioni profilo

È possibile specificare gli elementi che saranno controllati alla ricerca di infiltrazioni. Scegliere gli oggetti (memoria, settori di avvio e UEFI, unità, file e cartelle o rete) dalla struttura ad albero in cui sono presenti tutte le destinazioni disponibili sul sistema in uso. Fare clic sull'icona a forma di ingranaggio nell'angolo in alto a sinistra per accedere ai menu a discesa **Destinazioni di controllo** e **Profilo di controllo**.

> Questo selettore del profilo di controllo si applica al Controllo su richiesta, al Controllo Hyper-V e al Controllo OneDrive.

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

Per accedere rapidamente a una destinazione di controllo o aggiungere una cartella o uno o più file di destinazione, inserire la directory di destinazione nel campo vuoto sotto all'elenco delle cartelle.



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

Attraverso le impostazioni di profilo	Consente di selezionare le destinazioni nel profilo di controllo selezionato.
Supporti rimovibili	Consente di selezionare dischi, supporti di archiviazione USB, CD/DVD.
Unità locali	Consente di selezionare tutti gli hard disk del sistema.
Unità di rete	Consente di selezionare tutte le unità di rete mappate.
Cartelle condivise	Consente di selezionare tutte le cartelle condivise sul server locale.
Selezione personalizzata	Cancella tutte le selezioni. Al termine dell'operazione, è possibile effettuare una scelta personalizzata.

Per accedere rapidamente a una destinazione di controllo (file o cartella) in modo da poterla includere per il controllo, immettere il relativo percorso nel campo di testo sotto la struttura ad albero. Il nome del percorso fa distinzione tra lettere maiuscole e minuscole.

Il menu a discesa **Profilo di controllo** consente di selezionare i profili di controllo predefiniti:

- Controllo intelligente
- Controllo menu contestuale
- Controllo approfondito
- Controllo del computer

Questi profili di controllo utilizzano differenti parametri del motore ThreatSense.

Visualizza avanzamento controllo

Se si desidera effettuare solo un controllo del sistema senza azioni di pulizia aggiuntive, selezionare **Controlla senza pulire**. Questa funzione è utile qualora si desideri avere esclusivamente una panoramica di eventuali oggetti infetti e delle relative informazioni. È 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.

Ignora esclusioni

Selezionando Ignora esclusioni, è possibile eseguire un controllo ignorando le esclusioni applicabili.

Destinazioni di controllo

Se si desidera controllare solo una destinazione specifica, è possibile utilizzare **Controllo personalizzato** e selezionare un'opzione dal menu a discesa **Destinazioni di controllo** oppure selezionare destinazioni specifiche dalla struttura (ad albero) della cartella.

Il selettore dei profili delle destinazioni di controllo si applica ai seguenti contrllli:

- Controllo su richiesta
- Controllo Hyper-V

- Controllo OneDrive

Per visualizzare rapidamente una destinazione di controllo o per aggiungere un nuovo file o una nuova cartella di destinazione, 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 **Destinazioni di controllo** è impostato su **Nessuna selezione**.

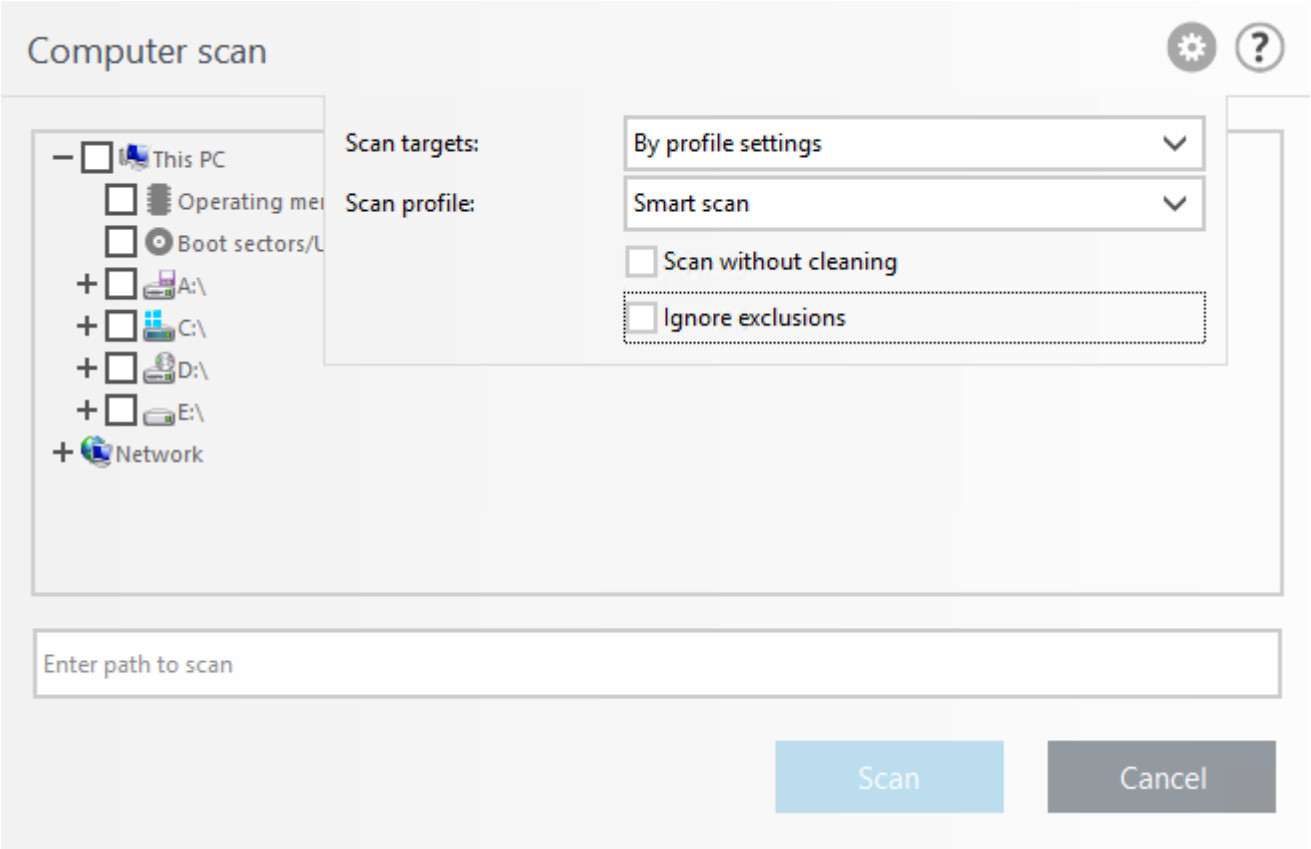
Memoria operativa	Controlla tutti i processi e i dati attualmente utilizzati dalla memoria operativa.
Settori di avvio/UEFI	Controlla i settori di avvio e UEFI alla ricerca di malware. Per ulteriori informazioni sullo scanner UEFI, consultare il glossario.
Database WMI	Controlla l'intero database di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

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.
Cartelle condivise	Consente di selezionare tutte le cartelle condivise sul server locale.
Selezione personalizzata	Cancella tutte le selezioni. Al termine dell'operazione, è possibile effettuare una scelta personalizzata.

È possibile scegliere un profilo dal menu a discesa Profilo di controllo da utilizzare per le destinazioni scelte per il controllo. Il profilo predefinito è Controllo intelligente. Il profilo predefinito è **Controllo intelligente**. Sono disponibili due ulteriori profili di controllo predefiniti: Controllo approfondito e **Controllo menu contestuale**. Questi profili di controllo utilizzano differenti parametri del motore ThreatSense.

La finestra **Controllo personalizzato**:



Controlla senza pulire – Se si desidera effettuare solo un controllo del sistema senza azioni di pulizia aggiuntive, selezionare Controlla senza pulire. Questa funzione è utile qualora si desideri avere esclusivamente una panoramica di eventuali oggetti infetti e delle relative informazioni. È 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.

Ignora esclusioni – È possibile eseguire un controllo ignorando le esclusioni applicabili.

Azione dopo il controllo: scegliere l'azione da eseguire al termine del controllo dal menu a discesa.

Il controllo non può essere interrotto: selezionare questa opzione per impedire agli utenti che non possiedono privilegi di interrompere le azioni intraprese in seguito al controllo.

Il controllo può essere sospeso dall'utente per (min.): consente all'utente con diritti limitati di sospendere il controllo del computer per il periodo di tempo specificato.

Interrompi automaticamente controllo dopo (min.): consente di annullare il controllo se richiede più tempo della soglia temporale specificata.

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.

Controllo stato inattivo

Se il computer si trova nello stato di inattività, verrà eseguito un controllo automatico di tutti i dischi locali. Il **rilevamento dello stato di inattività** verrà eseguito se il computer si trova nei seguenti stati:

- Schermo o screen saver disattivato
- Blocco computer
- Uscita utente

Esegui anche se il computer è alimentato dalla batteria

Per impostazione predefinita, lo scanner dello stato di inattività non verrà eseguito in caso di alimentazione del computer (notebook) a batteria.

Attiva registrazione

Consente di registrare il risultato di un controllo del computer nella sezione File di rapporto (nella finestra principale del programma, fare clic su File di rapporto e selezionare il tipo di rapporto Controllo del computer dal menu a discesa).

Parametri di ThreatSense

Modificare i parametri di controllo per il controllo dello stato di inattività.

Controllo all'avvio

Per impostazione predefinita, all'avvio del sistema (accesso utente) e dopo aver aggiornato automaticamente il modulo, verrà eseguito il controllo automatico del file di avvio. Questo controllo è gestito dalla Configurazione e attività Pianificazione 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**, selezionare una delle attività denominate **Controllo automatico file di avvio** (Accesso utente o aggiornamento del modulo), quindi fare clic su **Modifica**. Seguire le istruzioni fornite nella procedura guidata e nell'ultimo passaggio sarà possibile modificare le opzioni dettagliate del Controllo automatico file di avvio.

Controllo automatico file di avvio

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

Il menu a discesa **Destinazione di controllo** consente di specificare il livello di controllo dei file eseguiti all'avvio del sistema. I file sono visualizzati in ordine crescente 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 della Destinazione di controllo specifici:

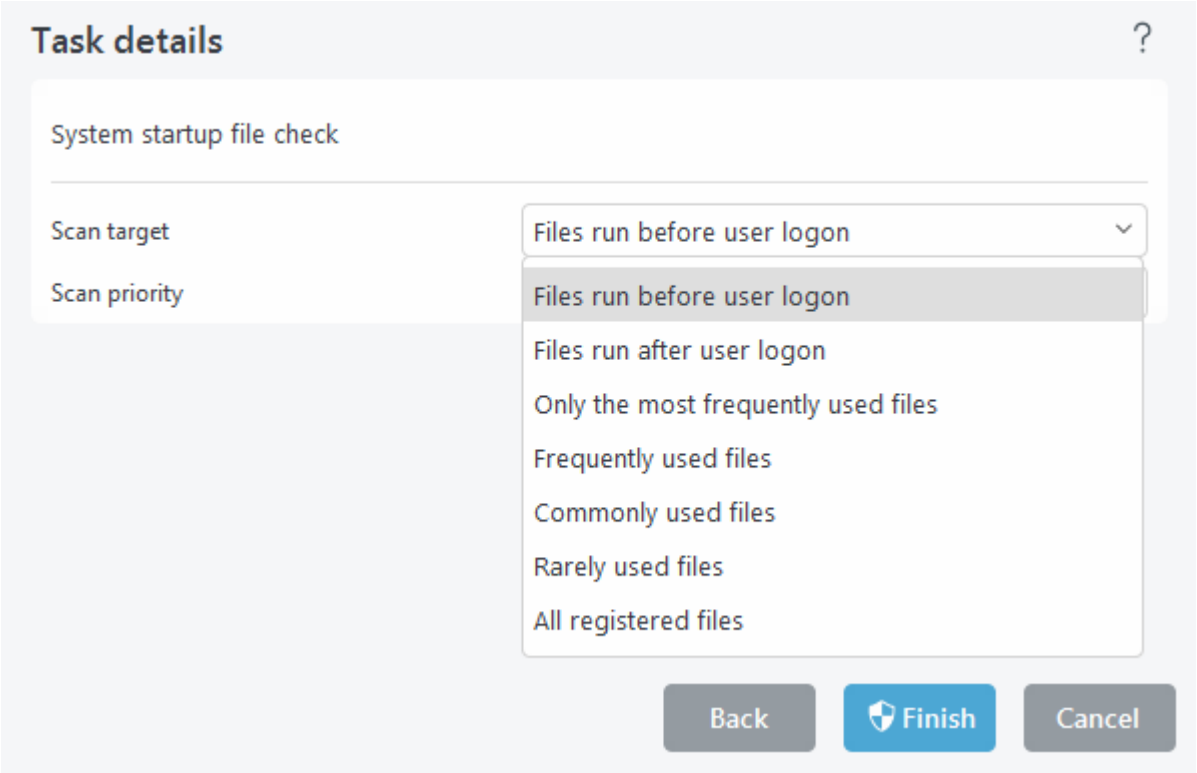
I file vengono eseguiti prima dell'accesso dell'utente

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).

I file vengono eseguiti dopo l'accesso dell'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:

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

Supporti rimovibili

ESET Server Security offre il controllo automatico dei supporti rimovibili (CD/DVD/USB). Questo modulo consente di controllare i supporti inseriti. 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.

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

- **Controlla ora**: avvia il controllo del supporto rimovibile.
- **Non controllare**: i supporti rimovibili non verranno controllati.
- **Configurazione**: consente di aprire la Configurazione avanzata.
- **Usa sempre l'opzione selezionata**: in caso di selezione, verrà eseguita la stessa azione quando viene inserito nuovamente un supporto rimovibile.

In ESET Server Security è inoltre disponibile la funzione Controllo dispositivi che consente all'utente di definire regole per l'utilizzo dei dispositivi esterni su un determinato computer.

Per accedere alle impostazioni per il controllo dei supporti rimovibili, aprire **Configurazione avanzata** (**F5**) > **Notifiche** > **Avvisi interattivi** > **Modifica**. Se l'opzione **Chiedi all'utente** non è selezionata, scegliere l'azione eseguita quando un supporto rimovibile viene inserito nel computer:

- **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.
- **Controllo forzato del dispositivo**: verrà eseguito un controllo del computer del supporto rimovibile inserito e non sarà possibile annullarlo.
- **Mostra opzioni di controllo**: consente di aprire la sezione di configurazione degli **Avvisi interattivi**.

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.

Integra nel sistema

Questa opzione consente di potenziare la protezione dei documenti di Microsoft Office (non necessario in circostanze normali).

Parametri di ThreatSense

Consente di modificare i parametri per la Protezione documenti.

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).

Controllo Hyper-V

La versione corrente del controllo Hyper-V supporta il controllo del sistema virtuale online oppure offline in Hyper-V. I tipi supportati di controllo in base al sistema Windows Hyper-V ospitato e lo stato del sistema virtuale sono visualizzati qui:

Sistemi virtuali con funzione Hyper-V	Machina virtuale on-line	Macchina virtuale off-line
Windows Server 2022 Hyper-V	di sola lettura	di sola lettura/controllo
Windows Server 2019 Hyper-V	di sola lettura	di sola lettura/controllo
Windows Server 2016 Hyper-V	di sola lettura	di sola lettura/controllo
Windows Server 2012 R2 Hyper-V	di sola lettura	di sola lettura/controllo
Windows Server 2012 Hyper-V	di sola lettura	di sola lettura/controllo

Requisiti hardware

Il server non deve presentare problemi di prestazioni nell'esecuzione delle macchine virtuali. L'attività di controllo utilizza principalmente le risorse della CPU. Per controllare le VM on-line, è necessario che vi sia dello spazio libero su disco. Lo spazio su disco deve essere almeno il doppio dello spazio utilizzato dai punti di controllo/dagli snapshot e dai dischi virtuali.

Limitazioni specifiche

- Il controllo dell'archiviazione RAID, i volumi con spanning e i Dischi dinamici non sono supportati a causa della natura dei dischi dinamici. Si consiglia pertanto di evitare di utilizzare il tipo di disco dinamico nelle macchine virtuali.

- Il controllo viene sempre eseguito sulla macchina virtuale corrente e non incide sui punti di controllo o gli snapshot.

- Il controllo Hyper-V sull'host di un cluster non è attualmente supportato da ESET Server Security.

Mentre ESET Security supporta il controllo dei dischi virtuali MBR, il controllo di sola lettura è l'unico metodo supportato per queste destinazioni. È possibile modificare questa impostazione in **Configurazione avanzata** (**F5**) > **Detection engine** > **Controllo Hyper-V** > parametri ThreatSense > **Settori di avvio**.

La macchina virtuale da controllare è "offline": stato "Spenta"

ESET Server Security utilizza gli strumenti di gestione Hyper-V per rilevare ed effettuare la connessione ai dischi virtuali. Ciò consente a ESET Server Security di accedere al contenuto dei dischi virtuali come se accedesse ai dati e ai file su un'unità generica.

La macchina virtuale da controllare è "online": stato "In esecuzione", "Sospesa", "Salvata"

ESET Server Security utilizza gli strumenti di gestione Hyper-V per rilevare i dischi virtuali. Non è possibile effettuare una connessione effettiva a questi dischi. Di conseguenza, ESET Server Security crea un punto di controllo/uno snapshot della macchina virtuale a cui effettuare la connessione. Al termine del controllo, il punto di controllo/lo snapshot viene eliminato. Ciò significa che il controllo in modalità di sola lettura può essere eseguito in quanto l'esecuzione delle macchine virtuali non subisce modifiche a causa dell'attività di controllo.

Consente a ESET Server Security di creare uno snapshot o un punto di controllo durante il controllo in un intervallo di tempo massimo di un minuto. Sarebbe utile se si considerasse questa opzione durante l'esecuzione di un controllo Hyper-V su un maggior numero di macchine virtuali.

Convenzione sulla denominazione

Il modulo di controllo Hyper-V utilizza la seguente convenzione di denominazione:

```
VirtualMachineName\DiskX\VolumeY
```

Dove X è il numero dei dischi e Y è il numero dei volumi. Ad esempio:

```
Computer\Disk0\Volume1
```

Il suffisso del numero viene aggiunto in base all'ordine di rilevamento ed è identico a quello visualizzato in "Gestione disco" della macchina virtuale. Tale convenzione di denominazione viene utilizzata nel menu a discesa strutturato ad albero delle destinazioni da controllare, sulla barra di avanzamento e nei file di rapporto.

Esecuzione di un controllo

- Su richiesta: fare clic su **Controllo Hyper-V** per visualizzare un elenco di macchine virtuali e di volumi disponibili per il controllo. Selezionare una o più macchine virtuali, dischi o volumi che si desidera controllare e fare clic su **Controlla**.

- Per creare una pianificazione attività.

- Tramite ESET PROTECT come attività client denominata Controllo server.

- Il Controllo Hyper-V può essere gestito e avviato tramite eShell.

È possibile eseguire contemporaneamente più controlli Hyper-V. Al termine del controllo, l'utente riceverà una notifica contenente un collegamento ai file del rapporto.

Possibili problemi

- Durante l'esecuzione del controllo di una macchina virtuale online, è necessario creare un punto di controllo/uno snapshot di una macchina virtuale specifica. Durante la creazione di un punto di controllo/uno snapshot, alcune azioni generiche della macchina virtuale potrebbero essere limitate o disabilitate.

- Se una macchina virtuale non in linea viene sottoposta al controllo, non può essere attivata fino al termine dell'operazione.

- Hyper-V Manager consente all'utente di denominare due macchine virtuali differenti in maniera identica e ciò rappresenta un problema quando si tenta di differenziare le macchine durante la consultazione dei rapporti del controllo.

Per creare un nuovo profilo, selezionare **Modifica** accanto a **Elenco di profili**, inserire il proprio **Nome profilo**, quindi fare clic su **Aggiungi**. Il nuovo profilo verrà visualizzato nel menu a discesa **Profilo selezionato** in cui sono presenti i profili del controllo esistenti.

Il menu a discesa **Destinazioni di controllo** per **Hyper -V** consente di selezionare gli oggetti da controllare predefiniti:

Attraverso le impostazioni di profilo	Consente di selezionare le destinazioni nel profilo di controllo selezionato.
Tutte le macchine virtuali	Consente di selezionare tutte le macchine virtuali.
Attivato sulle macchine virtuali	Consente di selezionare tutte le macchine virtuali on-line.
Disattivato sulle macchine virtuali	Consente di selezionare tutte le macchine virtuali off-line.
Nessun elemento selezionato	Cancella tutte le selezioni.

Fare clic sull'icona ⚙ e modificare l'intervallo per **Interrompere il controllo se viene eseguito per più di (minuti)** e impostare l'ora preferita (valore compreso tra 1 e 2880 minuti).

Fare clic su **Controlla** per eseguire il controllo utilizzando i parametri personalizzati configurati dall'utente. Al termine di tutti i controlli, selezionare **File di rapporto** > Controllo Hyper-V.

Protezione Hyper-V e riconoscimento automatico

La creazione di report viene eseguita dal motore di rilevamento e dal componente di riconoscimento automatico.

Parametri di ThreatSense

Consente di modificare i parametri del controllo Hyper-V.

Controllo OneDrive

Standard

È possibile configurare l'azione e la quarantena.
Azione da eseguire se il file è infetto:
- **Nessuna azione**: non verrà applicata alcuna modifica al file.
- **Rimuovi**: i file verranno spostati nella quarantena e rimossi da OneDrive. I file sono ancora tuttavia disponibili nel cestino OneDrive.

Metti file infetti in quarantena
Se attivata, i file contrassegnati per l'eliminazione verranno messi in quarantena. Deselezionare questa impostazione per disattivare la quarantena in modo che non si accumulino file al suo interno.

Avanzate

Questa sezione contiene informazioni sulla registrazione del controllo OneDrive (ID applicazione, ID oggetto su portale Azure, identificazione personale certificato). È possibile configurare i timeout e il limite di download simultanei.

Profili

Per creare un nuovo profilo, selezionare **Modifica** accanto a **Elenco di profili**, inserire il proprio **Nome profilo**, quindi fare clic su **Aggiungi**. Il nuovo profilo verrà visualizzato nel menu a discesa **Profilo selezionato** in cui sono presenti i profili del controllo esistenti.
Il menu a discesa **Destinazione di controllo** consente di selezionare la destinazioni di controllo predefinita:
- **Attraverso il profilo**: consente di selezionare le destinazioni nel profilo di controllo selezionato.
- **Tutti gli utenti**: consente di selezionare tutti gli utenti.
- **Nessuna selezione**: consente di annullare la selezione corrente.

Fare clic sull'icona e modificare l'intervallo per **Interrompere il controllo se viene eseguito per più di (minuti)** e impostare l'ora preferita (valore compreso tra 1 e 2880 minuti).
Fare clic su **Controlla** per eseguire il controllo utilizzando i parametri personalizzati configurati dall'utente. Al termine di tutti i controlli, selezionare **File di rapporto** > Controllo OneDrive.
Parametri di ThreatSense
Modificare i parametri di controllo per lo scanner OneDrive.
Controllo OneDrive e protezione riconoscimento automatico
La creazione di report viene eseguita dal motore di rilevamento e dal componente di riconoscimento automatico.

HIPS

Il Sistema anti-intrusione basato su host (HIPS) protegge il sistema da malware o 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.

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.

Attiva autoprotezione

ESET Server Security integra una tecnologia di Autoprotezione che impedisce a software dannosi di danneggiare o disabilitare la protezione anti-malware, in modo da garantire costantemente la sicurezza del sistema. Le modifiche alle impostazioni Abilita HIPS e Abilita SD (Autoprotezione) avranno effetto solo dopo aver riavviato il sistema operativo Windows. Se si disabilita l'intero sistema HIPS sarà necessario anche riavviare il computer.

Attiva servizio protetto

Con Microsoft Windows Server 2012 R2, Microsoft ha introdotto un concetto di servizi protetti. Impedisce un servizio contro attacchi malware. Per impostazione predefinita, il kernel di ESET Server Security è in esecuzione come un servizio protetto. Questa funzione è disponibile su Microsoft Windows Server 2012 R2 e sistemi operativi server più recenti.

Attiva scanner memoria avanzato

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

Attiva Exploit Blocker

È progettato per rafforzare i tipi di applicazione comunemente utilizzati come browser Web, lettori PDF, client di posta e componenti di Microsoft Office. L'exploit blocker è attivato per impostazione predefinita. Per ulteriori

informazioni su questo tipo di protezione, consultare il glossario.

Attiva protezione ransomware

Per utilizzare questa funzionalità. attivare HIPS ed ESET Live Grid. Per ulteriori informazioni sul Ransomware, consultare il glossario.

Modalità di filtraggio

È possibile scegliere una delle seguenti modalità di filtraggio:

- **Modalità automatica**: le operazioni sono attivate, ad eccezione di quelle bloccate dalle regole predefinite che proteggono il sistema. È consentito tutto ad eccezione delle azioni negate dalla regola.

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

- **Modalità interattiva**: all'utente verrà chiesto di confermare le operazioni. Consenti/nega accesso, Crea regola, Ricorda temporaneamente questa azione.

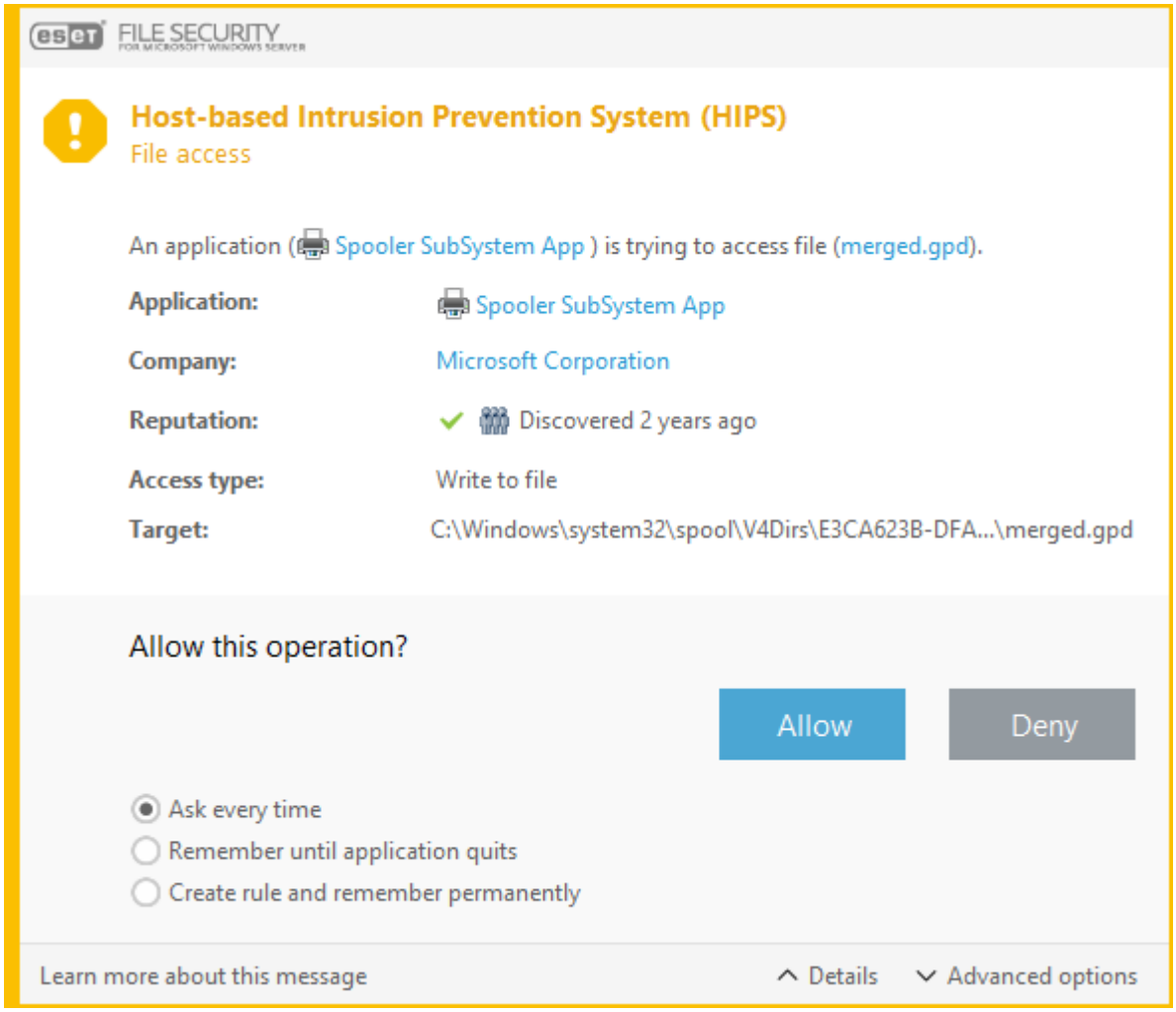
- **Modalità basata su criteri**: le operazioni sono bloccate. Accetta solo regole utente/predefinite.

- **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 (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.

Regole

Le regole determinano a quali applicazioni verrà concesso l'accesso a file specifici, parti del registro o altre applicazioni. 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. Se l’azione predefinita di una regola è impostata su **Chiedi**, verrà visualizzata una finestra di dialogo ogni volta che la regola viene attivata. È possibile selezionare **Blocca** o **Consenti** l’operazione. Se l'utente non sceglie un'azione nell'intervallo di tempo specifico, verrà selezionata una nuova azione in base alle regolere.

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 **Bloccare** l'azione. Fare clic su **Dettagli** per visualizzare ulteriori 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.



Chiedi sempre

La finestra di dialogo comparirà a ogni attivazione della regola. È possibile scegliere di **Negare** o **Consentire** l'operazione.

Memorizza fino all'uscita dell'applicazione

Dopo aver scelto un'azione tra **Nega** o **Consenti**, verrà creata una regola HIPS temporanea che verrà utilizzata fino alla chiusura dell'applicazione in questione. Inoltre, in caso di modifica della modalità di filtraggio, modificare anche le regole oppure, in caso di aggiornamento del modulo HIPS e di riavvio del sistema da parte dell'utente, le regole temporanee verranno eliminate.

Crea regola e memorizzala in modo permanente

Creare una nuova regola HIPS. È possibile modificare questa regola in un secondo momento nella sezione di gestione delle regole HIPS.

Impostazioni regole HIPS

La finestra offre una panoramica delle regole HIPS esistenti.

Regola	Nome della regola scelto automaticamente o definito dall'utente.
Attivazione eseguita	Disattivare questo pulsante se si desidera mantenere la regola nell'elenco ma non utilizzarla.

Regola	Nome della regola scelto automaticamente o definito dall'utente.
Azione	La regola specifica un'azione (Consenti, Blocca o Chiedi) che deve essere eseguita se sono soddisfatte le condizioni specificate.
Origini	La regola verrà utilizzata solo se l'evento viene attivato da una o più applicazioni.
Destinazioni	La regola verrà utilizzata esclusivamente se l'operazione è correlata a un file, un'applicazione o una voce di registro specifici.
Gravità del rapporto	Se si attiva questa opzione, le informazioni sulla regola verranno scritte nel Rapporto HIPS.
Notifica	Se viene attivato un evento, nell'area di notifica di Windows viene visualizzata una finestra di piccole dimensioni.

Creare una nuova regola, fare clic su **Aggiungi** nuove regole HIPS o **Modifica** voci selezionate.

Nome regola

Nome della regola scelto automaticamente o definito dall'utente.

Azione

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

Operazioni che influiscono

È necessario selezionare il tipo di operazione alla quale la regola verrà applicata. La regola verrà utilizzata solo per questo tipo di operazione e per la destinazione selezionata. La regola è formata da varie parti che illustrano le condizioni che la attivano.

Applicazioni di origine

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

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

Descrizione delle operazioni importanti:

Operazioni del file

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

La regola sarà utilizzata solo se l'operazione è correlata a questa destinazione. Selezionare **File specifici** dal menu a discesa e fare clic su **Aggiungi** per aggiungere nuovi file o nuove cartelle. In alternativa, è possibile selezionare **Tutti i file** dal menu a discesa per aggiungere tutte le applicazioni.

Operazioni dell'applicazione

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

La regola sarà utilizzata solo se l'operazione è correlata a questa destinazione. Selezionare **Applicazioni specifiche** dal menu a discesa e fare clic su **Aggiungi** per aggiungere nuovi file o nuove cartelle. In alternativa, è possibile selezionare **Tutte le applicazioni** dal menu a discesa per aggiungere tutte le applicazioni.

Operazioni del registro

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

La regola sarà utilizzata solo se l'operazione è correlata a questa destinazione. Selezionare **Voci specifiche** dal menu a discesa e fare clic su **Aggiungi** per aggiungere nuovi file o nuove cartelle. In alternativa, è possibile selezionare **Tutte le voci** dal menu a discesa per aggiungere tutte le applicazioni.

Quando si inserisce una destinazione, è possibile utilizzare i caratteri jolly con alcune limitazioni. Al posto di una chiave particolare, nei percorsi dei registri di sistema è possibile utilizzare il simbolo * (asterisco). Ad esempio *HKEY_USERS*\software can mean HKEY_USER\.default\software*, ma non *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** non è un percorso valido della chiave di registro del sistema. Un percorso della chiave del registro di sistema contenente * indica "questo percorso o qualsiasi percorso a qualsiasi livello dopo tale simbolo". Nelle destinazioni dei file, i caratteri jolly possono essere utilizzati solo in questo modo. Viene innanzitutto valutata la parte specifica di un percorso, quindi esaminato il percorso dopo il carattere jolly (*).

In caso di creazione di una regola eccessivamente generica, l'utente potrebbe ricevere una notifica.

Impostazioni avanzate HIPS

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

Caricamento driver sempre consentito

I driver selezionati sono sempre autorizzati a caricare indipendentemente dalla modalità di filtraggio configurata, eccetto nel caso in cui vengano bloccati esplicitamente da una regola dell'utente. I driver visualizzati in questo elenco sono sempre autorizzati a caricare indipendentemente dalla modalità di filtraggio dell'HIPS, eccetto nel caso in cui vengano bloccati esplicitamente da una regola dell'utente. È possibile selezionare **Aggiungi** nuovo driver, **Modifica** o **Elimina** driver selezionato dall'elenco.

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

Registra tutte le operazioni bloccate

Tutte le operazioni bloccate verranno scritte sul registro HIPS. Utilizzare questa funzione solo durante la risoluzione dei problemi o se richiesto dal Supporto tecnico di ESET, in quanto potrebbe generare un file di rapporto di grandi dimensioni e rallentare il sistema.

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.

Aggiorna configurazione

Questa sezione specifica informazioni sorgente di aggiornamento come i server di aggiornamento e i dati di autenticazione per questi server.

> 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).

Standard

Seleziona profilo di aggiornamento predefinito
Scegliere un profilo esistente o crearne uno nuovo che verrà applicato per impostazione predefinita per gli aggiornamenti.
Commutazione automatica profilo
Assegnare un profilo di aggiornamento in base alle reti note nel firewall. La commutazione automatica del profilo consente di modificare il profilo di una rete specifica in base all'impostazione in "Pianificazione attività". Per ulteriori informazioni, consultare le pagine della guida
Configura notifiche aggiornamento
Fare clic su **Modifica** per selezionare le notifiche dell'applicazione da visualizzare. È possibile scegliere tra le notifiche "Mostra su un desktop" o "Inoltra a e-mail".
Cancella cache aggiornamenti
In caso di problemi con un aggiornamento, fare clic su **Cancella** per eliminare la cache dei file di aggiornamento temporanei.

Aggiornamenti prodotto

Aggiornamenti automatici
Funzione abilitata per impostazione predefinita. Utilizzare il dispositivo di scorrimento per disabilitare gli aggiornamenti automatici qualora si desideri interrompere temporaneamente l'aggiornamento di ESET Server Security. Si consiglia di mantenere questa impostazione abilitata per assicurarsi che su ESET Server Security siano applicati gli aggiornamenti dei componenti di programma (Program Component Updates, PCU) e gli aggiornamenti dei componenti di programma micro (µPCU) più recenti in caso di disponibilità di un nuovo aggiornamento.

> Gli aggiornamenti vengono applicati al successivo riavvio del server.

Avvisi motore di rilevamento obsoleto

Imposta automaticamente età massima motore di rilevamento/Età massima motore di rilevamento (giorni)
Utilizzare il dispositivo di scorrimento per disabilitare l'età automatica del motore di rilevamento e impostare manualmente il tempo massimo (in giorni) dopo il quale l'età del motore di rilevamento verrà segnalata come obsoleta. Il valore predefinito è 7.

Rollback modulo

Se si sospetta che un nuovo aggiornamento del motore di rilevamento e/o dei moduli del programma possa essere instabile o danneggiato, è possibile ripristinare la versione precedente e disattivare gli aggiornamenti per un determinato periodo di tempo. In alternativa, è possibile attivare gli aggiornamenti disattivati in precedenza che erano stati posticipati in modo indefinito. ESET Server Security registra gli snapshot del motore di rilevamento e dei moduli del programma da utilizzare con la funzione Rollback. Per creare snapshot del motore di rilevamento, lasciare abilitato **Crea snapshot dei moduli**.
Numero di snapshot archiviati localmente
Definisce il numero di snapshot del modulo archiviato in precedenza.
Rollback dei moduli precedenti
Fare clic su Ripristino dello stato precedente per ripristinare la versione precedente dei moduli del programma e disabilitare temporaneamente gli aggiornamenti.

Profili

Per creare un profilo di aggiornamento personalizzato, selezionare **Modifica** accanto a **Elenco di profili**. Inserire il proprio **Nome profilo** e fare clic su **Aggiungi**. Selezionare il profilo da modificare e modificare i parametri per i tipi di aggiornamenti dei moduli oppure creare un **Mirror di aggiornamento**.

Aggiornamenti

Selezionare il tipo di aggiornamento da utilizzare dal menu a discesa:

• **Aggiornamento periodico**: 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 con un livello minimo di traffico di rete.

• **Aggiornamenti pre-rilascio**: sono aggiornamenti che sono stati sottoposti ad approfonditi test interni e 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 dei virus con un ritardo di almeno X ore (ovvero, database testati in un ambiente reale e considerati, pertanto, stabili).

Attiva ottimizzazione consegna aggiornamento

Abilitando questa opzione, i file di aggiornamento vengono scaricati dalla CDN (Content Delivery Network). La disabilitazione di questa impostazione potrebbe causare interruzioni del download e rallentamenti in caso di sovraccarico dei server di aggiornamento ESET dedicati. La disabilitazione è utile nel caso in cui un firewall possa accedere esclusivamente agli Indirizzi IP del server di aggiornamento ESET o una connessione ai servizi CDN non funzioni.

Chiedi prima di scaricare l'aggiornamento

Quando è disponibile un nuovo aggiornamento, all'utente verrà chiesto di scaricarlo.

Chiedi se le dimensioni di un file di aggiornamento sono maggiori di (kB)

Se la dimensione del file di aggiornamento supera il valore specificato nel campo, verrà visualizzata una notifica.

Aggiornamenti moduli

Per impostazione predefinita, gli aggiornamenti dei moduli sono impostati su **Scegli automaticamente**. 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://computer_name_or_its_IP_address:2221
Quando si utilizza un server HTTP locale con SSL, il server di aggiornamento deve essere impostato come riportato di seguito: https://computer_name_or_its_IP_address:2221
Quando si utilizza una cartella locale condivisa, il server di aggiornamento deve essere impostato come riportato di seguito: \\computer_name_or_its_IP_address\shared_folder

Attiva aggiornamenti più frequenti delle firme di rilevamento

Il motore di rilevamento sarà aggiornato a intervalli più brevi. Se si disabilita questa impostazione si potrebbe influenzare negativamente la frequenza di rilevamento.

Consenti aggiornamenti modulo da supporti rimovibili

Consente all'utente di effettuare l'aggiornamento dai supporti rimovibili in presenza del mirror creato. Selezionando **Automatico**, gli aggiornamenti verranno eseguiti in background. Se si desidera visualizzare le finestre di dialogo dell'aggiornamento, selezionare **Chiedi sempre**.

Aggiornamenti prodotto

La sospensione degli aggiornamenti automatici per specifici profili di aggiornamento disabilita temporaneamente gli aggiornamenti automatici del prodotto, per esempio quando ci si collega a Internet utilizzando altre reti o connessioni a consumo. Mantenere questa impostazione abilitata per accedere costantemente alle funzioni più recenti e ottenere la massima protezione possibile.

> i In alcuni casi, potrebbe essere necessario riavviare il server per rendere effettivi gli aggiornamenti.

Opzioni connessione

Server proxy

Per accedere alle opzioni di configurazione del server proxy per un dato profilo di aggiornamento. Fare clic su Modalità proxy e selezionare una delle tre seguenti opzioni:

- **Non utilizzare server proxy**: durante l'esecuzione degli aggiornamenti, ESET Server Security non utilizzerà alcun server proxy.

- **Utilizza impostazioni del server proxy globali**: verrà utilizzata la configurazione del server proxy specificata nella Configurazione avanzata (F5) > Strumenti > Server proxy.

- **Connessione tramite un server proxy**: utilizzare questa opzione nei casi seguenti:

È necessario utilizzare un server proxy per aggiornare ESET Server 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 Server 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.

> i 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 di ESET Server Security, devono essere compilati solo se è richiesta una password di accesso a Internet mediante un server proxy.

Usa la connessione diretta in caso di mancata disponibilità del proxy

Se un prodotto è configurato per utilizzare il proxy HTTP e questo non è raggiungibile, il prodotto disabiliterà il proxy e comunicherà direttamente con i server ESET.

Condivisioni Windows

Durante l'aggiornamento da un server locale su cui è in esecuzione Windows, per impostazione predefinita è richiesta l'autenticazione per ciascuna connessione di rete.

Connetti a LAN come

Per configurare l'account, selezionare una delle seguenti opzioni:

- **Account di sistema (predefinito)**: 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.

- **Utente corrente**: selezionare questa opzione per verificare che il programma esegua l'autenticazione utilizzando l'account utente che ha eseguito correntemente l'autenticazione. 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.

- **Utente specificato**: selezionare questa opzione per utilizzare 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. Nel caso in cui l’utente non disponga di tale accesso, il programma non sarà in grado di stabilire una connessione o scaricare gli aggiornamenti.

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: domain_name\user (se si tratta di un gruppo di lavoro, immettere workgroup_name\name) e la password utente. Per l'aggiornamento dalla versione HTTP del server locale, non è richiesta alcuna autenticazione.

Disconnetti dal server dopo l'aggiornamento

Consente di forzare una disconnessione nel caso in cui una connessione al server dovesse rimanere attiva anche dopo aver scaricato gli aggiornamenti.

Mirror di aggiornamento

Le opzioni di configurazione per il server mirror locale sono disponibili in **Configurazione avanzata** (F5) in **Aggiornamento** > **Profili** > scheda Mirror di aggiornamento.

Rollback aggiornamento

Se si sospetta che un nuovo aggiornamento del motore di rilevamento o dei moduli del programma possa essere instabile o danneggiato, è possibile ripristinare la versione precedente e disabilitare temporaneamente gli aggiornamenti. In alternativa, è possibile abilitare gli aggiornamenti precedentemente disabilitati in caso di rimandi indefiniti da parte dell’utente.

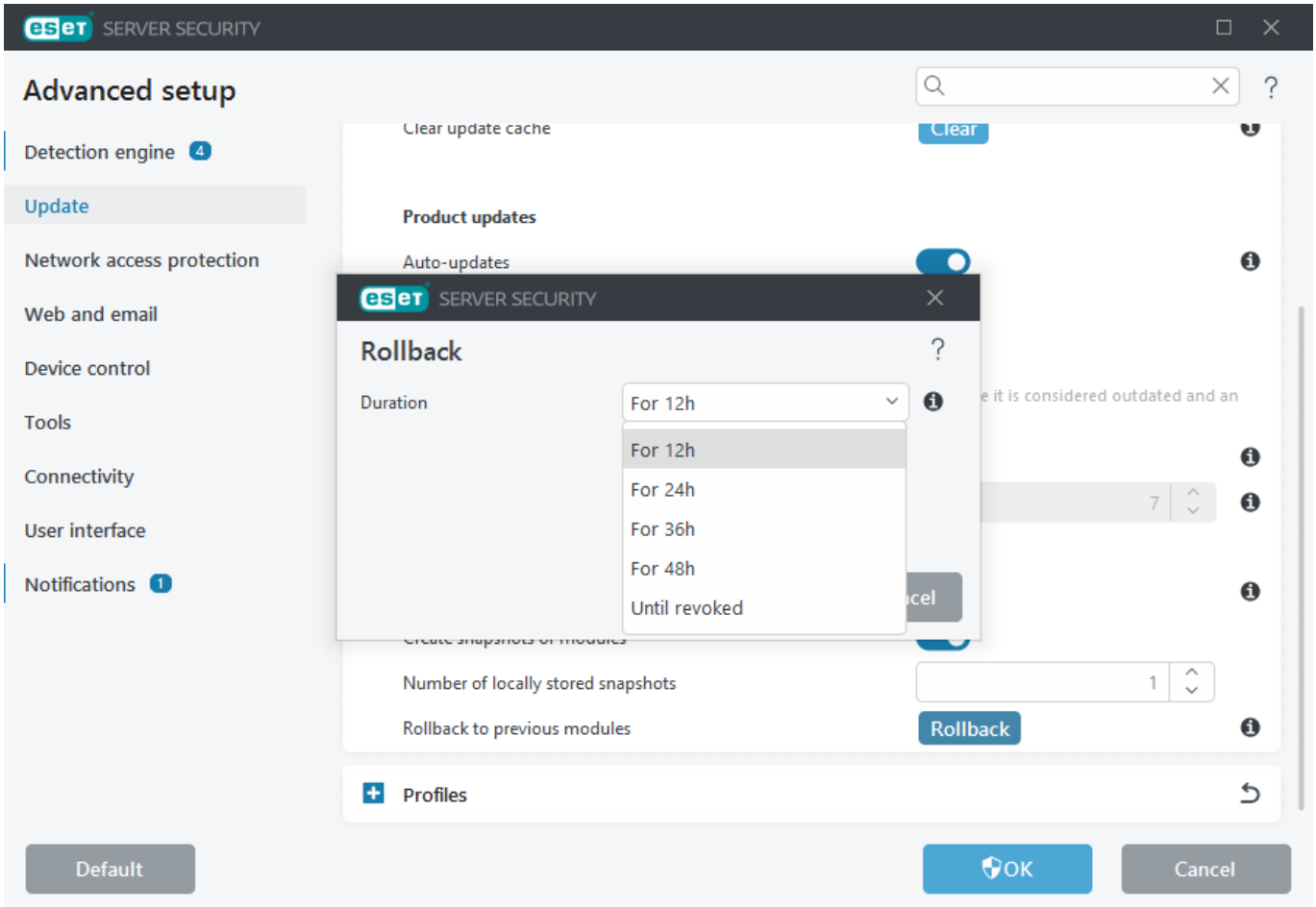
ESET Server Security registra gli snapshot del motore di rilevamento e dei moduli del programma da utilizzare con la funzione di rollback. Per creare snapshot del database dei virus, mantenere abilitato **Crea snapshot dei moduli**.

In caso di abilitazione dell’opzione **Crea snapshot dei moduli**, durante il primo aggiornamento viene creato il primo snapshot. Quello successivo viene creato dopo 48 ore.

Il campo **Numero di snapshot archiviati localmente** definisce il numero di snapshot del motore di rilevamento archiviati.

Quando viene raggiunto il numero massimo di snapshot (ad esempio tre), lo snapshot meno recente viene sostituito con un nuovo snapshot ogni 48 ore. ESET Server Security esegue il rollback delle versioni dell’aggiornamento del motore di rilevamento e del modulo del programma ripristinando quella più vecchia.

Facendo clic su **Rollback**, è necessario scegliere un intervallo temporale dal menu a discesa che indica il periodo di tempo nel quale gli aggiornamenti del database del motore di rilevamento e del modulo del 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. Poiché rappresenta un potenziale rischio per la protezione, si consiglia di non selezionare questa opzione.

In caso di esecuzione di un rollback, il pulsante **Rollback** cambia in **Consenti aggiornamenti**. Gli aggiornamenti non sono consentiti per l'intervallo di tempo selezionato dal menu a discesa **Sospendi aggiornamenti**.

Il database del motore di rilevamento viene ripristinato alla versione più vecchia disponibile e memorizzato come snapshot nel file system del computer locale.

Attività pianificata - Aggiornamento

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

I passaggi sottostanti guidano l'utente attraverso un'attività di modifica dell'**Aggiornamento automatico periodico** esistente.
1. Nella finestra principale di **Pianificazione attività**, selezionare l'attività **Aggiornamento** con il nome **Aggiornamento automatico periodico** e fare clic su **Modifica**. Verrà visualizzata la procedura di configurazione guidata.
2. Configurare l'attività pianificata da eseguire, selezionare una delle seguenti opzioni temporali per definire quando eseguire l'attività pianificata:
3. Se si desidera impedire l'esecuzione dell'attività su un sistema alimentato dalla batteria (ad esempio, gruppi di continuità), fare clic sul pulsante accanto a **Ignora attività se in esecuzione su un computer alimentato dalla batteria**.
4. Selezionare il profilo di aggiornamento da utilizzare per l'aggiornamento. Selezionare un'azione da eseguire nel caso in cui, per qualsiasi motivo, non fosse possibile completare l'esecuzione dell'attività.
5. Fare clic su **Fine** per confermare l'attività.

Mirror di aggiornamento

ESET Server 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.

Per ridurre al minimo il traffico Internet sulle reti in cui l'applicazione ESET PROTECT viene utilizzata per la gestione di numerosi client, si consiglia di utilizzare ESET Bridge anziché configurare un client come mirror. ESET Bridge può essere installato con ESET PROTECT utilizzando il programma di installazione integrato o come componente autonomo. Per ulteriori informazioni e differenze tra ESET Bridge, Apache HTTP Proxy, Mirror Tool e connettività diretta, consultare la pagina della Guida online di ESET PROTECT.

Mirror di aggiornamento

Crea mirror di aggiornamento: consente di attivare le opzioni di configurazione del mirror.

Accesso ai file di aggiornamento

Attiva server HTTP: in caso di abilitazione, è possibile accedere ai file di aggiornamento tramite HTTP senza che vengano richieste le credenziali.

Cartella di archiviazione: fare clic su **Modifica** per ricercare una cartella sul computer locale o la 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.

Fare clic su **Cancella** se si desidera modificare una cartella predefinita indicata per l'archiviazione dei file con mirroring *C:\ProgramData\ESET\ESET Security\mirror*.

Server HTTP

Porta server: la porta predefinita è 2221. Se si utilizza una porta differente, modificare questo valore.

Autenticazione

Consente all’utente di definire il metodo di autenticazione utilizzato per l'accesso ai file di aggiornamento. Sono disponibili le seguenti opzioni: **Nessuna**, **Di base** e **NTLM**.

- Selezionare **Di base** per utilizzare la codifica base64 con l'autenticazione di base con 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 consentire l'accesso ai file di aggiornamento tramite il server HTTP, la cartella Mirror deve essere posizionata nello stesso computer dell'istanza di ESET Server Security che la crea.

SSL per server HTTP

Aggiungere il **File della catena di certificati** o generare un certificato autofirmato se si desidera eseguire il server HTTP con il supporto HTTPS (SSL). 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.

Per impostazione predefinita, il **Tipo di chiave privata** è impostato su **Integrato** (e, di conseguenza, sempre 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.

Opzioni connessione

Condivisioni Windows: durante l'aggiornamento da un server locale su cui è in esecuzione Windows, per impostazione predefinita è richiesta l'autenticazione per ciascuna connessione di rete.

Connetti a LAN come

Per configurare l’account, selezionare una delle seguenti opzioni:

- **Account di sistema (predefinito)**: 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.

- **Utente corrente**: selezionare questa opzione per verificare che il programma esegua l’autenticazione utilizzando l’account utente che ha eseguito correntemente l’autenticazione. 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’autenticazione in quel momento.

- **Utente specificato**: selezionare questa opzione per utilizzare 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. Nel caso in cui l’utente non disponga di tale accesso, il programma non sarà in grado di stabilire una connessione e di scaricare gli aggiornamenti.

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: *domain_name\user* (se si tratta di un gruppo di lavoro, immettere *workgroup_name\name*) e la password utente. Per l'aggiornamento dalla versione HTTP del server locale, non è richiesta alcuna autenticazione.

Disconnetti dal server dopo l'aggiornamento: donsente di forzare una disconnessione nel caso in cui una connessione al server dovesse rimanere attiva anche dopo aver scaricato gli aggiornamenti.

Protezione accesso alla rete

Gestire la protezione di rete e fare clic su **Modifica** per aggiungerne una nuova o modificare quella esistente:

- Profilo della connessione di rete
- Set di IP
- Firewall

Profilo della connessione di rete

In caso di utilizzo di un computer che si connette frequentemente a reti pubbliche o a reti esterne alla normale rete di lavoro, si consiglia di verificare la credibilità delle nuove reti alle quali si effettua la connessione. Dopo aver definito le reti, ESET Server Security può riconoscere le reti attendibili (domestiche/aziendali) utilizzando vari parametri di rete configurati in Identificazione della rete.

I computer accedono spesso a reti con indirizzi IP simili a quelli della rete attendibile. In questi casi, ESET Server Security potrebbe considerare attendibile una rete sconosciuta (domestica/aziendale). Per evitare questo tipo di situazione, si consiglia di utilizzare l'Autenticazione della rete.

Quando una scheda di rete è connessa a una rete o le relative impostazioni di rete vengono riconfigurate, ESET Server Security ricercherà nell'elenco di reti note un record che corrisponde alla nuova rete. Se l'identificazione della rete e l'autenticazione della rete (facoltativo) corrispondono, la rete sarà contrassegnata come connessa in questa interfaccia.

Se non viene trovata alcuna rete nota, la configurazione dell'identificazione della rete creerà una nuova connessione di rete per identificare la rete alla successiva connessione. Per impostazione predefinita, la nuova connessione di rete utilizza il tipo di protezione Rete pubblica.

La finestra di dialogo Nuova connessione di rete rilevata chiederà all'utente di scegliere tra la rete pubblica, la rete domestica o aziendale e il tipo di protezione delle impostazioni di Utilizzo di Windows. Se una scheda di rete è connessa a una rete nota e tale rete è contrassegnata come Rete domestica o aziendale, le subnet locali della scheda verranno aggiunte nell'area attendibile.

Tipo di protezione delle nuove reti

Selezionare quale tra le opzioni: **Utilizza l'impostazione di Windows**, **Chiedi all'utente** e **Contrassegna come pubblica** viene utilizzata per impostazione predefinita per le nuove reti. Se si seleziona **Utilizza l'impostazione di Windows**, non comparirà una finestra di dialogo e la rete alla quale si è connessi verrà automaticamente

contrassegnata in base alle impostazioni di Windows. Ciò causerà l'accessibilità di alcune funzioni (per esempio, la condivisione di file e il desktop remoto) dalle nuove reti.

Le reti note possono essere configurate manualmente nella finestra dell'Editor delle reti note.

Aggiungi rete

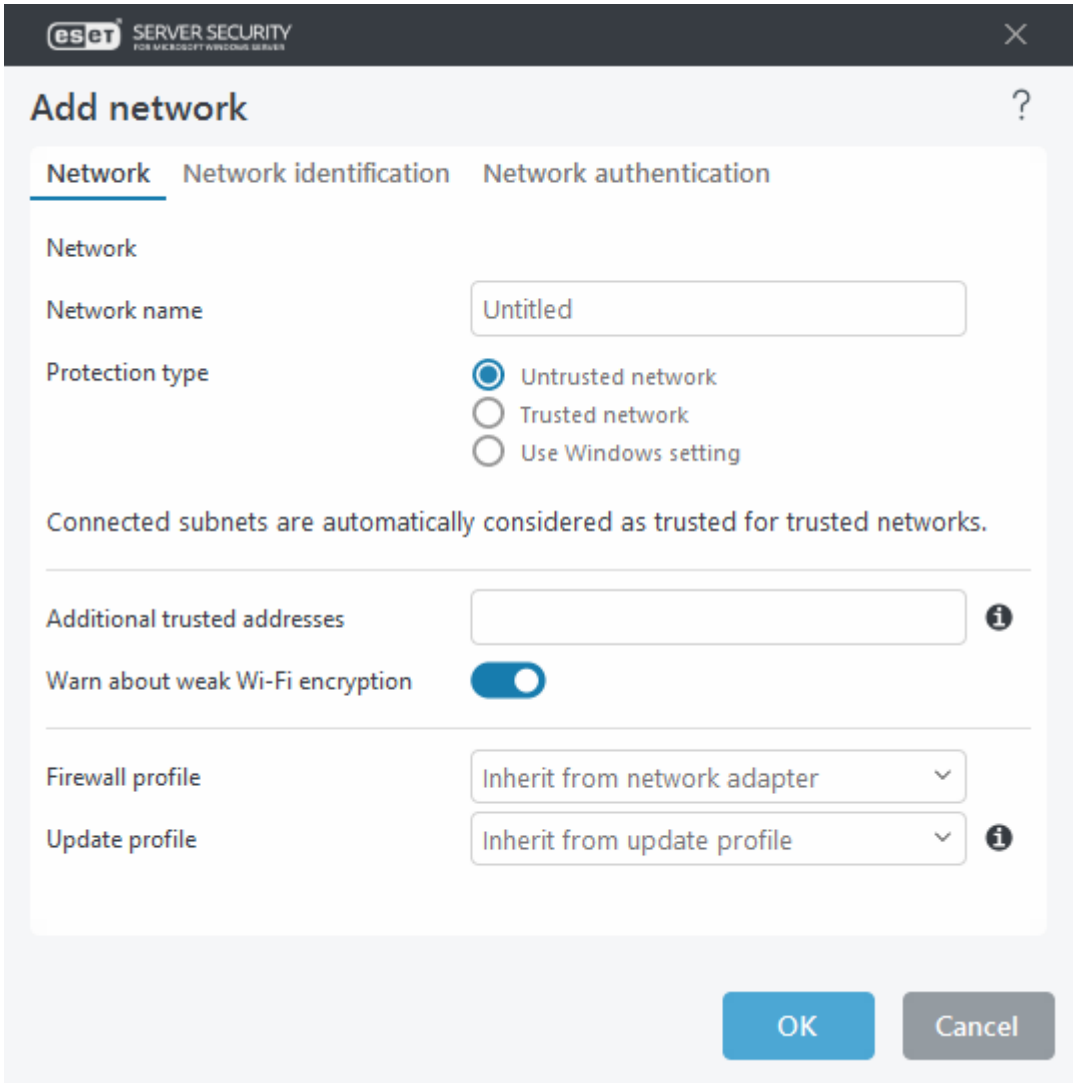
Le impostazioni di configurazione della rete sono organizzate nelle seguenti schede:

Rete

È possibile definire il **Nome della rete** e selezionare il **Tipo di protezione** per la rete. Consente di visualizzare se la rete è impostata su **Rete attendibile**, **Rete non attendibile** o **Utilizza l'impostazione di Windows**.

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

- **Avvisa in caso di crittografia Wi-Fi vulnerabile**: ESET Server Security informa l'utente in caso di connessione a una rete wireless non protetta o a una rete con protezione vulnerabile.
- Il **Profilo firewall** sarà ereditato dalla scheda di rete.
- **Profilo di aggiornamento**: selezionare il profilo di aggiornamento che verrà utilizzato in caso di connessione a questa rete.



Identificazione rete

Viene eseguito in base ai parametri della scheda di rete locale. Tutti i parametri selezionati vengono confrontati con i parametri effettivi delle connessioni di rete attive. Gli indirizzi IPv4 e IPv6 sono consentiti.

Autenticazione di rete

Ricerca uno specifico server nella rete e utilizza la crittografia asimmetrica (RSA) per autenticare tale server. Il nome della rete autenticata deve corrispondere al nome dell'area specificato nelle impostazioni del server di autenticazione. Il nome fa distinzione tra maiuscole e minuscole. Specificare il nome del server, la porta di ascolto del server e una chiave pubblica corrispondente alla chiave privata del server. Il nome del server può essere inserito sotto forma di indirizzo IP, DNS o nome NetBios e seguito da un percorso che specifica la posizione della chiave sul server (per esempio, *server_name_/directory1/directory2/authentication*). È possibile specificare i server alternativi da utilizzare aggiungendoli al percorso, separati da punti e virgola.

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

- Chiave pubblica crittografata PEM (*.pem*), che può essere generata utilizzando ESET Authentication Server.
- Chiave pubblica crittografata
- File del certificato della chiave pubblica (*.crt*)

Fare clic su **Esegui test** per eseguire un test sulle impostazioni. Se l'autenticazione viene eseguita correttamente, verrà visualizzato il messaggio "L'autenticazione del server è stata eseguita correttamente". Se l'autenticazione non viene configurata correttamente, verranno visualizzati i seguenti messaggi di errore:

Autenticazione del server non riuscita. Firma non valida o senza corrispondenza.	La firma del server non corrisponde alla chiave pubblica inserita.
Autenticazione del server non riuscita. Il nome della rete non corrisponde.	Disattivare questo pulsante se si desidera mantenere la regola nell'elenco ma non utilizzarla.
Autenticazione del server non riuscita. Risposta non valida o inesistente dal server.	Se il server non è in esecuzione o è inaccessibile, non viene ricevuta alcuna risposta. Se è in esecuzione un altro server HTTP sull'indirizzo specificato, si potrebbe ricevere una risposta non valida.
È stata inserita una chiave pubblica non valida.	Verificare che il file della chiave pubblica inserito non sia danneggiato.

Firewall

Il firewall controlla l'intero traffico di rete in entrata e in uscita da e verso il sistema. A tal fine vengono consentite o bloccate singole connessioni di rete in base a specifiche regole di filtraggio. Il firewall fornisce protezione contro gli attacchi provenienti da dispositivi remoti e blocca servizi potenzialmente pericolosi.

Il firewall è disabilitato per impostazione predefinita. Prima di abilitarlo, esaminare le regole del firewall e, se necessario, modificarle per assicurarsi che soddisfino le proprie esigenze.

Il firewall è disponibile solo se si possiede un abbonamento attivo a ESET PROTECT di livello base o superiore.

Attiva firewall

Prima di abilitarlo, esaminare le regole del firewall e modificarle se necessario. Con il firewall abilitato, il traffico di rete viene controllato in base alle regole configurate.

Regole

La configurazione delle regole consente di visualizzare e modificare tutte le regole del firewall applicate al traffico generato da singole applicazioni all'interno di connessioni attendibili e Internet.

Le regole di Windows Firewall configurate tramite i Criteri di gruppo (Group Policy, GPO) non vengono valutate.

È possibile creare una regola IDS in caso di attacco del computer in uso da parte di una botnet. È possibile modificare una regola in **Configurazione avanzata** > **Protezione accesso alla rete** > **Protezione attacchi di rete** > **Regole IDS** facendo clic su **Modifica**.

Valuta anche le regole di Windows Firewall

In modalità filtraggio automatico, il traffico in entrata consentito dalle regole di Windows Firewall viene valutato ed elaborato, a meno che non sia esplicitamente bloccato dalle regole ESET.

Modalità di filtraggio

È possibile scegliere una delle seguenti modalità di filtraggio:

- **Modalità automatica**: modalità predefinita. Questa modalità è adatta agli utenti che preferiscono un utilizzo semplice e pratico facile del firewall senza la necessità di definire regole. Sebbene non sia necessario, in modalità automatica è possibile creare regole personalizzate definite dall'utente. La modalità automatica consente tutto il traffico in uscita per un determinato sistema e blocca la maggior parte del traffico in entrata, ad eccezione di parte del traffico proveniente dall'area attendibile (come specificato in IDS e opzioni avanzate/Servizi consentiti) e delle risposte alle comunicazioni in uscita recenti.

- **Modalità interattiva**: consente di creare una configurazione personalizzata per il firewall. Quando viene rilevata una comunicazione alla quale non si applicano regole esistenti, verrà visualizzata una finestra di dialogo che segnala una connessione sconosciuta. La finestra di dialogo offre la possibilità di consentire o negare la comunicazione e la decisione di consentire o negare può essere salvata come nuova regola per il firewall. Se si sceglie di creare una nuova regola, tutte le connessioni future di questo tipo saranno consentite o bloccate in base a tale regola.

- **Modalità basata su criteri**: consente di bloccare tutte le connessioni non definite da una regola specifica che le consente. Questa modalità permette agli utenti avanzati di definire regole che consentono solo le connessioni desiderate e sicure. Tutte le altre connessioni non specificate verranno bloccate dal firewall.

- **Modalità riconoscimento**: consente di creare e di salvare automaticamente le regole. Questa modalità è utilizzata soprattutto per la configurazione iniziale del firewall, ma non deve essere lasciata attiva per periodi di tempo prolungati. Non è richiesta alcuna interazione da parte dell'utente, perché le regole vengono salvate da ESET Server Security in base a parametri predefiniti. La modalità riconoscimento deve essere utilizzata solo fino a quando non sono state create tutte le regole per le comunicazioni richieste allo scopo di prevenire rischi per la sicurezza.

La modalità riconoscimento terminerà alle ore

Impostare la data e l'ora di disattivazione automatica della modalità riconoscimento. È anche possibile disattivare la modalità riconoscimento manualmente ogni volta che lo si desideri.

Modalità impostata dopo la scadenza della modalità di riconoscimento

Definire la modalità di filtraggio ripristinata dal firewall al termine del periodo di attivazione della modalità riconoscimento. Per ulteriori informazioni sulle modalità di filtraggio, fare riferimento alla tabella precedente. Al termine dell'operazione, l'opzione **Chiedi all'utente** richiede privilegi amministrativi per apportare modifiche alla modalità di filtraggio del firewall.

Impostazioni modalità riconoscimento

Fare clic su **Modifica** per configurare i parametri di salvataggio delle regole create in modalità riconoscimento.

Rilevamento modifica applicazione

La funzione di rilevamento delle modifiche dell'applicazione consente di visualizzare notifiche se le applicazioni modificate, per le quali esiste una regola del firewall, tentano di stabilire connessioni. La modifica dell'applicazione è un meccanismo di sostituzione temporanea o permanente di un'applicazione originale con un'altra applicazione con eseguibile diverso (per garantire protezione da utilizzi non corretti delle regole del firewall).

Questa funzione non è stata concepita allo scopo di rilevare le modifiche apportate a qualsiasi tipo di applicazione. L'obiettivo consiste nell'evitare utilizzi non corretti delle regole del firewall esistenti e nel

monitorare solo le applicazioni per le quali esistono regole firewall specifiche.

Attiva rilevamento delle modifiche alle applicazioni

In caso di selezione, il programma monitora le applicazioni per verificare l'eventuale presenza di modifiche (aggiornamenti, infezioni, altre modifiche). Quando un'applicazione modificata tenta di stabilire una connessione, l'utente riceve una notifica dal firewall.

Consenti modifica delle applicazioni firmate (attendibili)

Non inviare notifiche se l'applicazione presenta la stessa firma digitale valida prima e dopo la modifica.

Elenco di applicazioni escluse dal rilevamento

Aggiungere o rimuovere singole applicazioni per le quali sono consentite modifiche senza notifica.

Regole firewall

Le regole del firewall rappresentano un insieme di condizioni utilizzate per testare in modo significativo tutte le connessioni di rete e tutte le azioni assegnate a tali condizioni. Utilizzando le regole del firewall, è possibile definire l'azione da intraprendere quando vengono stabiliti diversi tipi di connessioni di rete.

Le regole vengono valutate dall'alto verso il basso ed è possibile visualizzarne la priorità nella prima colonna. L'azione della prima regola di corrispondenza viene utilizzata per ciascuna connessione di rete in fase di valutazione.

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

Se viene rilevata una nuova comunicazione sconosciuta, è necessario valutare attentamente se consentirla o negarla. Connessioni non richieste, non protette o sconosciute rappresentano un rischio per la sicurezza del sistema. Se viene stabilita una connessione di questo tipo, si consiglia di prestare attenzione al dispositivo remoto e all'applicazione che tenta di connettersi al computer. Numerose infiltrazioni tentano di ottenere e inviare dati privati o di scaricare altre applicazioni dannose per ospitare workstation. Il firewall consente di rilevare e terminare tali connessioni.

Se si dispone di numerose regole del firewall, è possibile utilizzare un filtro per visualizzare solo regole specifiche. Per filtrare le regole del firewall, fare clic su Altri filtri sopra l'elenco Regole del firewall. È possibile filtrare le regole in base ai seguenti criteri:

- Origine
- Direzione
- Azione
- Disponibilità

Per impostazione predefinita, le regole predefinite del firewall sono nascoste. Per visualizzare tutte le regole predefinite, disabilitare il tasto di alternanza accanto a Nascondi regole integrate (predefinite). È possibile

disabilitare queste regole, ma non rimuovere una regola predefinita.

Impostazioni 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 in quanto le regole vengono salvate da ESET Server Security in base ai parametri predefiniti. È possibile modificare questi parametri in base alle proprie esigenze.

> i Si consiglia di utilizzare la modalità riconoscimento solo per la configurazione iniziale del firewall perché la comunicazione non viene filtrata da ESET Server Security durante il riconoscimento.

- **Traffico in entrata dall'area attendibile**: un esempio di connessione in entrata all'interno dell'area attendibile è un dispositivo remoto dall'area attendibile che tenta di stabilire una comunicazione con un'applicazione locale in esecuzione sul server.

- **Traffico in uscita verso l'area attendibile**: applicazione locale sul server che tenta di stabilire una connessione a un altro dispositivo all'interno della rete locale o all'interno di una rete nell'area attendibile.

- **Traffico Internet in entrata**: dispositivo remoto che tenta di comunicare con un'applicazione in esecuzione sul server.

- **Traffico Internet in uscita**: applicazione locale in esecuzione sul server che tenta di stabilire una connessione a un altro dispositivo.

Termina la modalità riconoscimento

Al termine del periodo di utilizzo della modalità riconoscimento, verrà richiesto di passare alla modalità di filtraggio **Interattiva** o **Basata su criteri**. Quando il firewall è in modalità riconoscimento, le nuove regole vengono create senza interazione da parte dell'utente.

Per ulteriori informazioni su ciascuna modalità di filtraggio, consultare Modalità di filtraggio.

> i Si consiglia di rivedere le regole create durante la modalità riconoscimento. Fare clic su **Modifica** per aprire l'elenco delle regole.

Rilevamento modifica applicazione

Le notifiche vengono visualizzate se le applicazioni modificate per le quali esiste una regola del firewall tentano di stabilire connessioni. La modifica dell'applicazione consiste nella sostituzione temporanea o permanente di un'applicazione originale con un'altra applicazione con un eseguibile diverso (per garantire protezione da utilizzi non corrette delle regole del firewall).

Questa funzione non è stata concepita allo scopo di rilevare le modifiche apportate a qualsiasi tipo di applicazione. L'obiettivo consiste nell'evitare utilizzi non corretti delle regole del firewall esistenti e nel monitorare solo le applicazioni per le quali esistono regole firewall specifiche.

Abilita il rilevamento delle modifiche dell'applicazione: in caso di selezione, il programma monitora le modifiche apportate alle applicazioni (aggiornamenti, infezioni, altre modifiche). Quando un'applicazione modificata tenta di stabilire una connessione, l'utente riceve una notifica dal firewall.

Consenti la modifica di applicazioni firmate (attendibili): non inviare notifiche se l'applicazione dispone della stessa firma digitale valida prima e dopo la modifica.

Elenco delle applicazioni escluse dal rilevamento: fare clic su **Modifica** e **Aggiungi** o modificare le singole applicazioni per le quali sono consentite modifiche senza notifica.

Set di IP

Un set di IP rappresenta una raccolta di indirizzi di rete che creano un gruppo logico di indirizzi IP che si rivela utile quando è necessario riutilizzare lo stesso set di indirizzi in regole multiple. A ciascun indirizzo in un dato gruppo vengono assegnate regole simili definite centralmente per l'intero gruppo. Un esempio di questo genere di gruppo è un'**Area attendibile**. L'area attendibile rappresenta un gruppo di indirizzi di rete che non sono in alcun modo bloccati dal firewall. I set di IP predefiniti non possono essere rimossi.

Quando si aggiunge o si modifica un set di IP, sono disponibili i seguenti campi:

- **Nome**: nome di un gruppo di computer remoti.
- **Descrizione**: descrizione generale del gruppo.
- **Indirizzo computer remoto (IPv4, IPv6, intervallo, maschera):** indirizzo remoto, intervallo di indirizzi o subnet.
- **Rimuovi**: consente di rimuovere un'area dall'elenco.

Aggiungi indirizzo IPv4:
Indirizzo singolo: consente di aggiungere l'indirizzo IP di un singolo computer (ad esempio, 192.168.0.10).
Intervallo di indirizzi: digitare gli indirizzi IP iniziali e finali per specificare l'intervallo di IP di vari computer (ad esempio, 192.168.0.1-192.168.0.99).
Subnet: subnet (un gruppo di computer) definita da un indirizzo IP e da una maschera. Ad esempio, 255.255.255.0 è la maschera di rete per la subnet 192.168.1.0. Per escludere l'intero tipo di subnet in 192.168.1.0/24.
Aggiungi indirizzo IPv6:
Indirizzo singolo: consente di aggiungere l'indirizzo IP di un singolo computer (ad esempio, 2001:718:1c01:16:214:22ff:fec9:ca5).
Subnet: la subnet (un gruppo di computer) è definita da un indirizzo IP e da una maschera (ad esempio, 2002:c0a8:6301:1::1/64).

Protezione attacchi di rete

Attiva protezione attacchi di rete (IDS)

Consente all'utente di configurare l'accesso ad alcuni dei servizi in esecuzione sul computer dall'Area attendibile e di attivare o disattivare il rilevamento di vari tipi di attacchi ed exploit che potrebbero essere utilizzati per arrecare danni al computer in uso.

Attiva protezione botnet

Consente all'utente di rilevare e bloccare la comunicazione con comandi o server di controllo dannosi in base a modelli tipici quando il computer è infetto e un bot sta tentando di comunicare.

Eccezioni IDS

È possibile immaginare le eccezioni Intrusion Detection System (IDS) come regole di protezione di rete. Fare clic su Modifica per definire le eccezioni IDS.

> Se nell'ambiente è in esecuzione una rete ad alta velocità (10 GbE e superiori), consultare l'articolo della Knowledge Base per informazioni sulle prestazioni relative alla velocità di rete e ESET Server Security.

Protezione attacchi di forza bruta

ESET Server Security controlla il contenuto del traffico di rete e blocca i tentativi di individuazione delle password.

Opzioni avanzate

Configurare le opzioni di filtraggio avanzate per rilevare i vari tipi di attacchi e di vulnerabilità che potrebbero essere eseguiti sul computer in uso.

Rilevamento intrusioni

Protocollo SMB: rileva e blocca vari problemi di protezione nel protocollo SMB
Protocollo RPC: rileva e blocca vari CVE nel sistema di chiamata procedura remota sviluppato per il DCE (Distributed Computing Environment).
Protocollo RDP: rileva e blocca vari CVE nel protocollo RDP (vedere sopra).
Blocca indirizzo non sicuro dopo il rilevamento di un attacco: gli indirizzi IP rilevati come origine degli attacchi vengono aggiunti alla blacklist per impedire la connessione per uno specifico periodo di tempo.
Visualizza notifica dopo il rilevamento di un attacco: consente di attivare l'area di notifica di Windows nell'angolo in basso a destra della schermata.
Visualizza notifiche anche per gli attacchi in ingresso contro problemi di sicurezza: avvisa l'utente in caso di rilevamento di attacchi contro problemi di sicurezza o se viene effettuato un tentativo di accesso al sistema in questo modo.

Ispezione pacchetto

Consenti connessione in entrata alle condivisioni admin nel protocollo SMB: le condivisioni amministrative (condivisioni admin) sono le condivisioni di rete predefinite che condividono le partizioni dell'hard disk (C$, D$, ...) nel sistema insieme alla cartella di sistema (ADMIN$). Se si disattiva la connessione alle condivisioni admin, si dovrebbero ridurre molti rischi per la protezione. Ad esempio, il worm Conficker esegue attacchi a dizionario per potersi connettere alle condivisioni admin.
Nega vecchi (non supportati) dialetti SMB: consente di negare le sessioni SMB che utilizzano un vecchio dialetto SMB non supportato da IDS. I moderni sistemi operativi Windows supportano i vecchi dialetti SMB grazie alla compatibilità con i vecchi sistemi operativi quali Windows 95. L'autore dell'attacco può utilizzare un vecchio dialetto in una sessione SMB per poter eludere l'ispezione sul traffico. Negare i vecchi dialetti SMB se il computer in uso non deve condividere file (o utilizzare in generale la comunicazione SMB) con un computer sul quale è in esecuzione una vecchia vrsione di Windows.
Nega sessioni SMB in assenza di estensioni di protezione: le estensioni di protezione possono essere utilizzate durante la negoziazione delle sessioni SMB al fine di offrire un meccanismo di autenticazione più sicuro rispetto all'autenticazione LAN Manager Challenge/Response (LM). La protezione di tipo LM è considerata debole e se ne sconsiglia l'utilizzo.

Consenti connessione in entrata alle condivisioni admin nel protocollo SMB: le condivisioni amministrative (condivisioni admin) sono le condivisioni di rete predefinite che condividono le partizioni dell'hard disk (C$, D$, ...) nel sistema insieme alla cartella di sistema (ADMIN$). Se si disattiva la connessione alle condivisioni admin, si dovrebbero ridurre molti rischi per la protezione. Ad esempio, il worm Conficker esegue attacchi a dizionario per potersi connettere alle condivisioni admin.
Consenti comunicazione con il servizio Security Account Manager: per ulteriori informazioni su questo servizio, vedere [MS-SAMR].
Consenti comunicazione con il servizio Local Security Authority: per ulteriori informazioni su questo servizio, vedere [MS-LSAD] e [MS-LSAT].
Consenti comunicazione con il servizio Remote Registry: per ulteriori informazioni su questo servizio, vedere [MS-RRP].
Consenti comunicazione con il servizio Service Control Manager: per ulteriori informazioni su questo servizio, vedere [MS-SCMR].
Consenti comunicazione con il servizio Server: per ulteriori informazioni su questo servizio, vedere [MS-SRVS].
Consenti comunicazione con gli altri servizi: altri servizi MSRPC.

Eccezioni IDS

Le eccezioni Intrusion Detection System (IDS) rappresentano essenzialmente regole di protezione della rete. Sono valutate dall'alto verso il basso. L'editor delle eccezioni IDS consente all'utente di personalizzazione il comportamento della protezione di rete in base a varie eccezioni IDS. Viene applicata l'eccezione della prima corrispondenza, per ciascun tipo di azione (Blocca, Notifica, Registra) in modo separato. **Primo/Su/Giù/Ultimo** consentono di modificare il livello di priorità delle eccezioni. Per creare una nuova eccezione IDS, fare clic su **Aggiungi**. Fare clic su **Modifica** per modificare un'eccezione IDS esistente o su **Elimina** per rimuoverla.

Scegliere il tipo di **Avviso** dall'elenco a discesa. Specificare il **Nome della minaccia** e la **Direzione**. Ricercare un'**Applicazione** per la quale si desidera creare l'eccezione. Specificare un elenco di indirizzi IP (IPv4 o IPv6) o subnet. Per le voci multiple, utilizzare la virgola come separatore.

Configurare l'**Azione** per l'eccezione IDS selezionando una delle opzioni dal menu a discesa (**Predefinita**, **Sì**, **No**). Eseguire questa operazione per ciascun tipo di azione (**Blocca**, **Notifica**, **Registra**).

> ✔ Se si desidera visualizzare una notifica in caso di comparsa di un avviso relativo a un'eccezione IDS, nonché la durata dell'evento registrato, lasciare il tipo di azione **Blocca** impostato su **Predefinita** e per gli altri due tipi (**Notifica** e **Registra**) scegliere **Sì** dal menu a discesa.

Minaccia sospetta bloccata

Questa situazione può verificarsi quando un'applicazione sul computer in uso tenta di trasmettere traffico dannoso a un altro computer presente nella rete sfruttando un problema di sicurezza o nel caso in cui qualcuno tenti di eseguire il controllo delle porte sulla rete in uso.

- Minaccia: nome della minaccia.
- Origine: indirizzo di rete di origine.
- Destinazione: indirizzo di rete di destinazione.
- Smetti di bloccare: consente di creare una regola IDS per la minaccia sospetta con le impostazioni per

consentire la comunicazione.

- Continua a bloccare: consente di bloccare la minaccia rilevata. Per creare una regola IDS con le impostazioni per bloccare le comunicazioni per questa minaccia, selezionare Non visualizzare più questo messaggio.

> Le informazioni visualizzate in questa finestra di notifica possono variare in base al tipo di minaccia rilevata. Per ulteriori informazioni sulle minacce e altri termini correlati, consultare Tipi di attacchi remoti o Tipi di rilevamenti.

Blacklist temporanea indirizzi IP

Consente di visualizzare un elenco di indirizzi IP rilevati come origine degli attacchi e aggiunti alla blacklist per il blocco delle connessioni per uno specifico periodo di tempo (fino a un massimo di un'ora). Consente di visualizzare l'**Indirizzo IP** che è stato bloccato.

Motivo del blocco

Consente di visualizzare il tipo di attacco che è stato bloccato dall'indirizzo (ad esempio, un tentativo di sfruttamento della vulnerabilità della sicurezza).

Timeout

Mostra la data e l'ora di scadenza dell'indirizzo nella blacklist.

Rimuovi/Rimuovi tutto

Consente di rimuovere l'indirizzo IP selezionato dalla blacklist temporanea prima che scada o rimuove immediatamente tutti gli indirizzi dalla blacklist.

Aggiungi eccezione

Consente di aggiungere un'eccezione firewall nel filtraggio IDS per l'indirizzo IP selezionato.

Protezione attacchi di forza bruta

La protezione attacchi di forza bruta blocca i tentativi di individuazione delle password per i servizi RDP ed SMB. Un attacco di forza bruta è un metodo che consente di individuare una specifica password tentando in modo sistematico ogni possibile combinazione di lettere, numeri e simboli.

- **Abilita protezione attacchi di forza bruta**: ESET Server Security ispeziona il contenuto del traffico di rete e blocca i tentativi di attacchi finalizzati all'individuazione di password.

- Regole: questa opzione consente di creare, modificare e visualizzare le regole per le connessioni di rete in entrata e in uscita.

- Esclusioni – Elenco di rilevamenti esclusi definiti da un indirizzo IP o percorso dell'applicazione. È possibile creare e modificare le esclusioni nella Console Web di ESET PROTECT.

Regole di Protezione attacchi di forza bruta

Regole della protezione attacchi di forza bruta che consentono di creare, modificare e visualizzare le regole per le connessioni di rete in entrata e in uscita. Non è possibile modificare o rimuovere le regole predefinite.

Creare una nuova regola e fare clic su **Aggiungi** nuove regole protezione attacchi di forza bruta o su **Modifica** voci selezionate.

Questa finestra fornisce una panoramica delle regole della protezione attacchi di forza bruta.

Nome	Nome della regola scelto automaticamente o definito dall'utente.
Attivazione eseguita	Disattivare questo pulsante se si desidera mantenere la regola nell'elenco ma non utilizzarla.
Azione	La regola specifica un'azione (Consenti o Nega) che deve essere eseguita se vengono soddisfatte le condizioni specificate.
Protocollo	Protocollo di comunicazione che verrà controllato da questa regola.
Profilo	È possibile impostare e applicare regole personalizzate per profili specifici.
Numero massimo di tentativi	Numero massimo di tentativi consentiti di ripetizione dell'attacco fino a quando l'indirizzo IP non viene bloccato e aggiunto alla blacklist.
Periodo di conservazione blacklist (min)	Consente di impostare l'ora della scadenza dell'indirizzo della blacklist. Il periodo di tempo predefinito per il conteggio del numero di tentativi è 30 minuti.
IP di origine	Elenco di indirizzi IP/intervalli/subnet. Gli indirizzi multipli devono essere separati da una virgola.
Aree di origine	Consente all'utente di aggiungere un'area predefinita o creata con un intervallo di indirizzi IP qui facendo clic su Aggiungi.

Esclusioni della protezione attacchi di forza bruta

Le esclusioni di forza bruta possono essere utilizzate per eliminare il rilevamento di attacchi di forza bruta per criteri specifici. Queste esclusioni vengono create da ESET PROTECT in base al rilevamento di attacchi di forza bruta. Le esclusioni saranno visualizzate se un amministratore crea esclusioni di forza bruta in ESET PROTECT Web Console. Le esclusioni possono contenere solo regole di autorizzazione e vengono valutate prima delle regole IDS.

- **Rilevamento**: tipo di rilevamento.
- **Applicazione**: selezionare il percorso del file di un'applicazione esclusa facendo clic su ... (per esempio *C:\Program Files\Firefox\Firefox.exe*). Non digitare il nome dell'applicazione.
- **IP remoto**: elenco di indirizzi/intervalli/subnet IPv4 o IPv6 remoti. Gli indirizzi multipli devono essere separati da una virgola.

Web e e-mail

È possibile configurare il filtraggio protocolli, la protezione client di posta, la protezione accesso web e la protezione Anti-Phishing per proteggere il server durante la comunicazione su Internet.

Protezione client di posta

Controlla tutte le comunicazioni tramite posta elettronica, protegge da codice dannoso e consente all'utente di scegliere l'azione da eseguire quando viene rilevata un'infezione.

Protezione accesso Web

Monitora la comunicazione tra i browser Web e i server remoti ed è conforme alle regole HTTP e HTTPS. Questa funzionalità consente inoltre di bloccare, consentire o escludere alcuni Indirizzi URL.

Filtraggio protocolli

Offre una protezione avanzata per i protocolli delle applicazioni che viene fornita dal motore di controllo ThreatSense. Questo controllo funziona automaticamente, indipendentemente dal browser Web o dal client di posta in uso. Funziona anche per la comunicazione crittografata (SSL/TLS).

Protezione Anti-Phishing

Consente all'utente di bloccare le pagine Web note per la distribuzione di contenuto di phishing.

Filtraggio protocolli

La protezione anti-malware per i protocolli delle applicazioni viene offerta dal motore di controllo ThreatSense, che integra molteplici tecniche di controllo avanzato dei malware. Il filtraggio protocolli funziona automaticamente, indipendentemente dal browser Internet o dal client di posta in uso. In caso di abilitazione del filtraggio protocolli, ESET Server Security controllerà le comunicazioni che utilizzano il protocollo SSL/TLS; portarsi su **Web ed e-mail** > SSL/TLS.

Attiva filtraggio contenuto protocollo applicazione

Se si disattiva il filtraggio protocolli, tenere presente che molti componenti di ESET Server Security (Protezione accesso Web, Protezione protocolli e-mail e Protezione Anti-Phishing) dipendono da questa funzione e che non saranno disponibili tutte le relative funzionalità.

Applicazioni escluse

Per escludere la comunicazione di specifiche applicazioni di rete dal filtraggio dei contenuti, selezionarle nell'elenco. Sulla comunicazione HTTP/POP3 delle applicazioni selezionate non verrà eseguito il rilevamento delle minacce. Questa opzione consente all'utente di escludere applicazioni specifiche dal filtraggio protocolli. Fare clic su **Modifica** e su **Aggiungi** per selezionare un file eseguibile dall'elenco di applicazioni per escluderlo dal filtraggio protocolli.

È consigliabile usare questa opzione solo per le applicazioni che non funzionano correttamente se la rispettiva comunicazione viene sottoposta a controllo.

Indirizzi IP esclusi

Consente all'utente di escludere indirizzi remoti specifici dal filtraggio protocolli. 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.

Fare clic su **Modifica** e su **Aggiungi** per specificare l’indirizzo IP, l’intervallo di indirizzi o la subnet sui quali applicare l’esclusione. Dopo aver selezionato **Inserisci valori multipli**, è possibile aggiungere indirizzi IP multipli delimitati da nuove righe, virgole o punti e virgola. Attivando selezioni multiple, sarà possibile visualizzare gli indirizzi IP nell'elenco di indirizzi IP esclusi.

> Le esclusioni sono utili in caso di problemi di compatibilità causati dal filtraggio protocolli.

Web e client di posta

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 Server 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 aggiungere le applicazioni che utilizzano già protocolli di comunicazione o applicazioni provenienti dai percorsi selezionati.

SSL/TLS

ESET Server Security è in grado di ricercare le minacce contenute nelle comunicazioni che utilizzano il protocollo Secure Sockets Layer (SSL)/Transport Layer Security (TLS).

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 sul protocollo SSL/TLS. La modalità di filtraggio del protocollo Secure Sockets Layer (SSL)/Transport Layer Security (TLS) è disponibile nelle seguenti opzioni:

- **Modalità automatica**: selezionare questa opzione per controllare tutte le comunicazioni protette dal protocollo SSL/TLS 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 dal protocollo SSL/TLS (con un certificato sconosciuto), viene visualizzata una finestra di dialogo per la scelta dell'azione. Questa modalità consente all'utente di creare un elenco di certificati SSL/TLS che saranno esclusi dal controllo.

- **Modalità criteri**: tutte le connessioni SSL/TLS vengono filtrate, ad eccezione delle esclusioni configurate.

Elenco di applicazioni filtrate tramite SSL/TLS

Aggiungere l’applicazione filtrata e impostare una delle azioni del controllo. L'elenco delle applicazioni filtrate tramite il protocollo SSL/TLS può essere utilizzato per la personalizzazione del comportamento di ESET Server Security per applicazioni specifiche e per ricordare le azioni scelte qualora in **Modalità filtraggio protocollo**

SSL/TLS venga selezionata la **Modalità interattiva**.

Elenco di certificati noti

Consente all’utente di personalizzare il comportamento di ESET Server Security per specifici certificati SSL. L’elenco può essere visualizzato e gestito facendo clic su Modifica accanto a **Elenco di certificati noti**.

Escludi comunicazione con domini attendibili

Consente di escludere la comunicazione utilizzando le Estensioni dei certificati di convalida dal controllo del protocollo (Internet Banking).

Blocca comunicazione crittografata che utilizza il protocollo obsoleto SSL v2

Le comunicazioni che utilizzano questa versione precedente del protocollo SSL verranno automaticamente bloccate.

Certificato radice

Affinché la comunicazione SSL/TLS 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 conosciuti (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 il 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 grandi dimensioni (ad esempio, le banche) utilizza un certificato firmato dal TRCA.

Dopo aver selezionato **Chiedi conferma della validità dei certificati** (impostazione predefinita), all'utente verrà richiesto di selezionare un'azione da eseguire in caso di comunicazione crittografata. È possibile selezionare **Blocca comunicazioni che utilizzano il certificato** per terminare sempre le connessioni crittografate ai siti con certificati non verificati.

Se il certificato è danneggiato o non valido

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

Elenco di certificati noti

Consente di personalizzare il comportamento di ESET Server Security per certificati Secure Sockets Layer (SSL)/Transport Layer Security (TLS) specifici e ricordare le azioni scelte se nella modalità di filtraggio con protocollo SSL/TLS è selezionata la **Modalità interattiva**. È possibile configurare il certificato selezionato o **Aggiungere** un certificato da un URL o un File.

Nella finestra **Aggiungi certificato**, fare clic sull'**URL** o sul **File** e specificare l'URL del certificato o ricercare un file del certificato. I seguenti campi saranno riempiti automaticamente utilizzando i dati del certificato:

- **Nome certificato**: 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.

Azione di accesso

- **Auto**: consente i certificati attendibili e chiede conferma all’utente per quelli non attendibili.
- **Consenti o Blocca**: consente/blocca la comunicazione protetta da questo certificato indipendentemente dalla sua attendibilità.
- **Chiedi**: consente di ricevere un prompt relativo alla presenza di un certificato specifico.

Azione di controllo

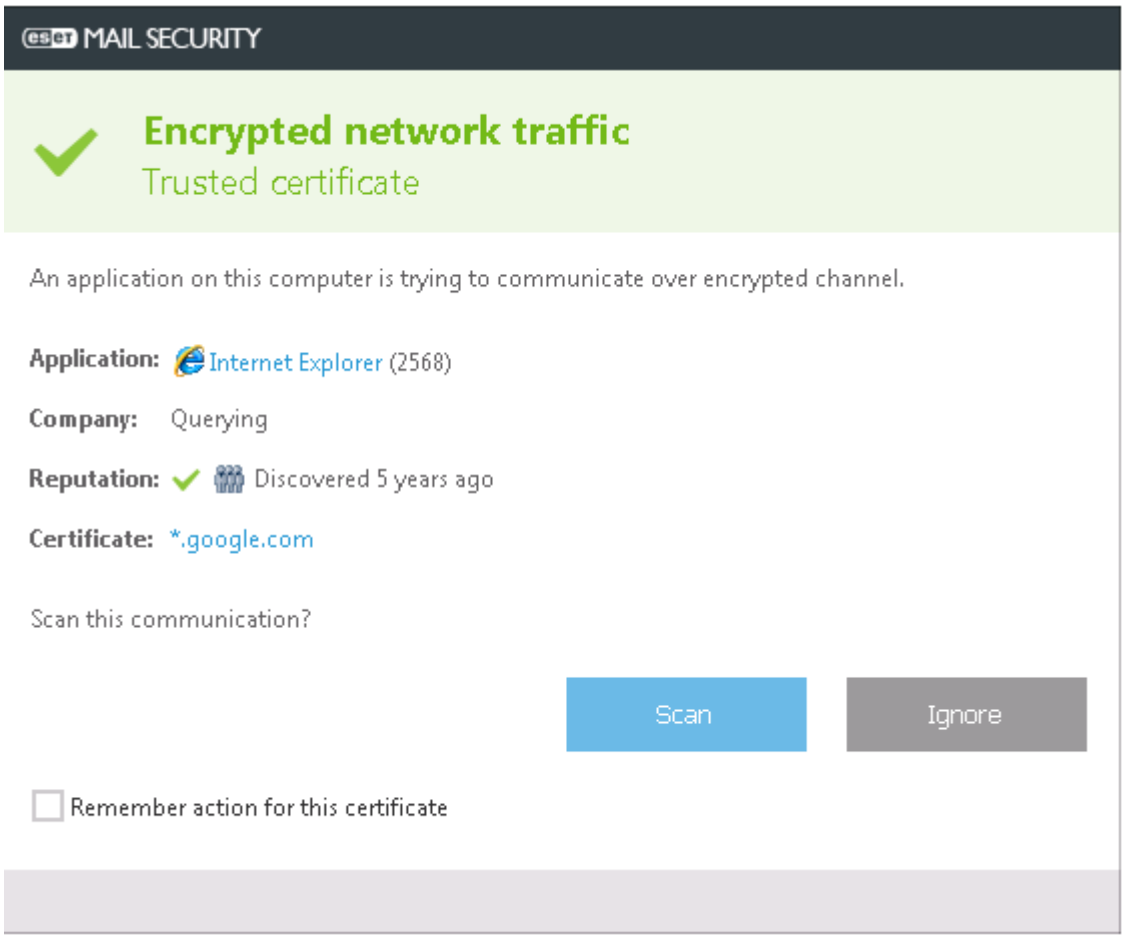
- **Auto**: consente di eseguire il controllo nella modalità automatica e di chiedere all’utente nella modalità interattiva.
- **Controlla o Ignora**: consente di eseguire il controllo o di ignorare la comunicazione protetta da questo certificato.
- **Chiedi**: consente di ricevere un prompt relativo alla presenza di un certificato specifico.

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 Server 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 Server 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.

Protezione client di posta

L'integrazione di ESET Server 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 Server Security. In caso di attivazione dell'integrazione, la barra degli strumenti di ESET Server Security viene inserita direttamente nel client di posta allo scopo di garantire una protezione più efficace delle e-mail. Le impostazioni di integrazione sono disponibili in **Configurazione avanzata** (**F5**) > **Web ed e-mail** > **Protezione client di posta** > **Integrazione client di posta**.

Integrazione client di posta

Microsoft Outlook è attualmente l'unico client di posta supportato. La protezione e-mail funziona come un plug-in. Il vantaggio principale offerto dal plug-in consiste nella sua indipendenza dal protocollo utilizzato. Quando il client di posta riceve un messaggio crittografato, questo viene decodificato e inviato allo scanner antivirus. Per un elenco completo dei client di posta supportati e delle relative versioni, fare riferimento al seguente articolo della Knowledge Base.

Ottimizzazione della gestione degli allegati: se l'ottimizzazione è disabilitata, tutti gli allegati vengono controllati immediatamente. In caso di disabilitazione, le prestazioni del client di posta possono subire un rallentamento.

Elaborazione avanzata client di posta: disabilitare questa opzione in caso di rallentamenti del sistema durante l'utilizzo del 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. Anche se l'integrazione non è attivata, la comunicazione e-mail rimane comunque protetta tramite il modulo di protezione client di posta (POP3, IMAP).

Attiva protezione e-mail con plug-in client

Consente all'utente di disattivare la protezione client di posta senza rimuovere l'integrazione nel client di posta. È possibile disattivare contemporaneamente tutti i plug-in o disattivare in maniera selettiva i seguenti elementi:

- 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.
- E-mail modificata: attiva/disattiva il controllo dei messaggi modificati.

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.

Protocolli e-mail

Attiva protezione e-mail con filtraggio protocollo

I protocolli IMAP e POP3 sono quelli più diffusi per la ricezione di comunicazioni e-mail in un'applicazione client di posta. ESET Server Security offre protezione per questi protocolli, indipendentemente dal client di posta in uso.

ESET Server Security supporta anche il controllo dei protocolli IMAPS e POP3S che utilizzano un canale crittografato per trasferire le informazioni tra server e client. ESET Server 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 IMAPS/POP3S**, indipendentemente dalla versione del sistema operativo.

Configurazione scanner IMAPS/POP3S

Le comunicazioni crittografate non verranno controllate durante l'utilizzo delle impostazioni predefinite. Per

attivare il controllo delle comunicazioni crittografate, accedere a Verifica protocollo SSL/TLS.

Il numero di porta ne identifica la tipologia. Segue un elenco delle porte per le comunicazioni e-mail predefinite:

Nome della porta	Numeri delle porte	Descrizione
POP3	110	Porta predefinita POP3 non crittografata.
IMAP	143	Porta predefinita IMAP non crittografata.
Secure IMAP (IMAP4-SSL)	585	Attiva filtraggio protocollo SSL/TLS. I numeri delle porte devono essere separati da una virgola.
IMAP4 over SSL (IMAPS)	993	Attiva filtraggio protocollo SSL/TLS. I numeri delle porte devono essere separati da una virgola.
Secure POP3 (SSL-POP)	995	Attiva filtraggio protocollo SSL/TLS. I numeri delle porte devono essere separati da una virgola.

Contrassegni e-mail

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 Server 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 di rilevamento di virus. Il controllo delle comunicazioni mediante i protocolli POP3 e IMAP non dipende dal client di posta in uso.

Dopo che un messaggio e-mail è stato controllato, è possibile aggiungere una notifica contenente i risultati del controllo. È possibile selezionare **Aggiungi messaggi per il tag alla posta ricevuta e letta** o **Aggiungi messaggi per il tag ai messaggi di posta elettronica inviati**.

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.
- **Quando si verifica un rilevamento**: vengono contrassegnati come controllati (impostazione predefinita) solo i messaggi contenenti software dannoso.
- **Per tutte le e-mail durante il controllo**: il programma aggiunge i messaggi a tutte le e-mail controllate.

Testo da aggiungere all'oggetto dell'e-mail rilevata

Modificare questo template se si desidera cambiare il formato predefinito dell'oggetto di un'e-mail infetta. Questa funzione sostituirà l'oggetto del messaggio `Hello` nel seguente formato: "`[rilevamento %DETECTIONNAME%] Ciao`. La variabile `%DETECTIONNAME%` rappresenta il rilevamento.

Barra degli strumenti di Microsoft Outlook

La protezione di Microsoft Outlook ha la stessa funzione di un modulo plug-in. Dopo aver installato ESET Server Security, la barra degli strumenti contenente le opzioni della protezione anti-malware verrà aggiunta a Microsoft Outlook:

ESET Server Security

Fare clic sull'icona per aprire la finestra principale del programma di ESET Server Security.

Ripeti controllo messaggi

Consente di avviare manualmente il controllo delle e-mail. È possibile specificare i messaggi da controllare e attivare un nuovo controllo dei messaggi e-mail ricevuti. Per ulteriori informazioni, consultare Protezione client di posta.

Configurazione scanner

Consente di visualizzare le opzioni per la configurazione della Protezione client di posta.

Barra degli strumenti di Outlook Express e Windows Mail

La protezione per Outlook Express e Windows Mail funziona come un modulo plug-in. Dopo aver installato ESET Server Security, la barra degli strumenti contenente le opzioni della protezione anti-malware verrà aggiunta a Outlook Express o Windows Mail:

ESET Server Security

Fare clic sull'icona per aprire la finestra principale del programma di ESET Server Security.

Ripeti controllo messaggi

Consente di avviare manualmente il controllo delle e-mail. È possibile specificare i messaggi da controllare e attivare un nuovo controllo dei messaggi e-mail ricevuti. Per ulteriori informazioni, consultare Protezione client di posta.

Configurazione scanner

Consente di visualizzare le opzioni per la configurazione della Protezione client di posta.

Personalizza aspetto

È possibile modificare l'aspetto della barra degli strumenti del client di posta. Deselezionare l'opzione per personalizzare l'aspetto indipendentemente dai parametri del client di posta.

- **Visualizza testo**: consente di visualizzare le descrizioni delle icone.
- **Testo a destra**: le descrizioni delle opzioni vengono spostate dal basso a destra delle icone.

- **Icone grandi**: consente di visualizzare icone grandi per le opzioni dei menu.

Finestra di dialogo di conferma

Questo messaggio di notifica serve a verificare che l'utente intenda davvero effettuare l'azione selezionata, evitando in questo modo possibili errori. In questa finestra di dialogo è anche possibile disattivare le richieste di conferma tramite l'apposita opzione.

Ripeti controllo messaggi

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

- **Tutti i messaggi nella cartella corrente**: esegue il controllo dei messaggi nella cartella visualizzata al momento.
- **Solo messaggi selezionati**: esegue il controllo dei soli messaggi contrassegnati dall'utente.
- **Ripeti controllo sui messaggi già controllati**: consente all'utente di eseguire un altro controllo sui messaggi che sono stati già controllati.

Protezione accesso Web

La protezione accesso Web monitora la comunicazione tra i browser Web e i server remoti per proteggere l'utente da minacce on-line 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.

Standard

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

Attiva controllo avanzato degli script del browser

Per impostazione predefinita, tutti i programmi JavaScript eseguiti dai browser Web saranno controllati dal motore di rilevamento.

Protocolli Web

Consente all'utente di configurare il monitoraggio di questi protocolli standard utilizzati dalla maggior parte dei browser Internet. Per impostazione predefinita, ESET Server Security è configurato per monitorare il protocollo HTTP utilizzato dalla maggior parte dei browser Internet.
ESET Server Security supporta anche il controllo del protocollo HTTPS. La comunicazione HTTPS utilizza un canale crittografato per trasferire le informazioni tra server e client. ESET Server 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 **Configurazione avanzata** (**F5**) > **Web ed e-mail** > SSL/TLS.

Parametri di ThreatSense

Consente all'utente di configurare impostazioni quali i tipi di controlli (e-mail, archivi, esclusioni, limiti e così via) e i metodi di rilevamento della protezione accesso Web.

Gestione indirizzi URL

La gestione degli 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 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. È necessario attivare Filtraggio protocolli SSL/TLS se si desidera filtrare gli indirizzi HTTPS oltre alle pagine Web HTTP. In caso contrario, verranno aggiunti solo i domini dei siti HTTPS visitati e non l'URL completo.

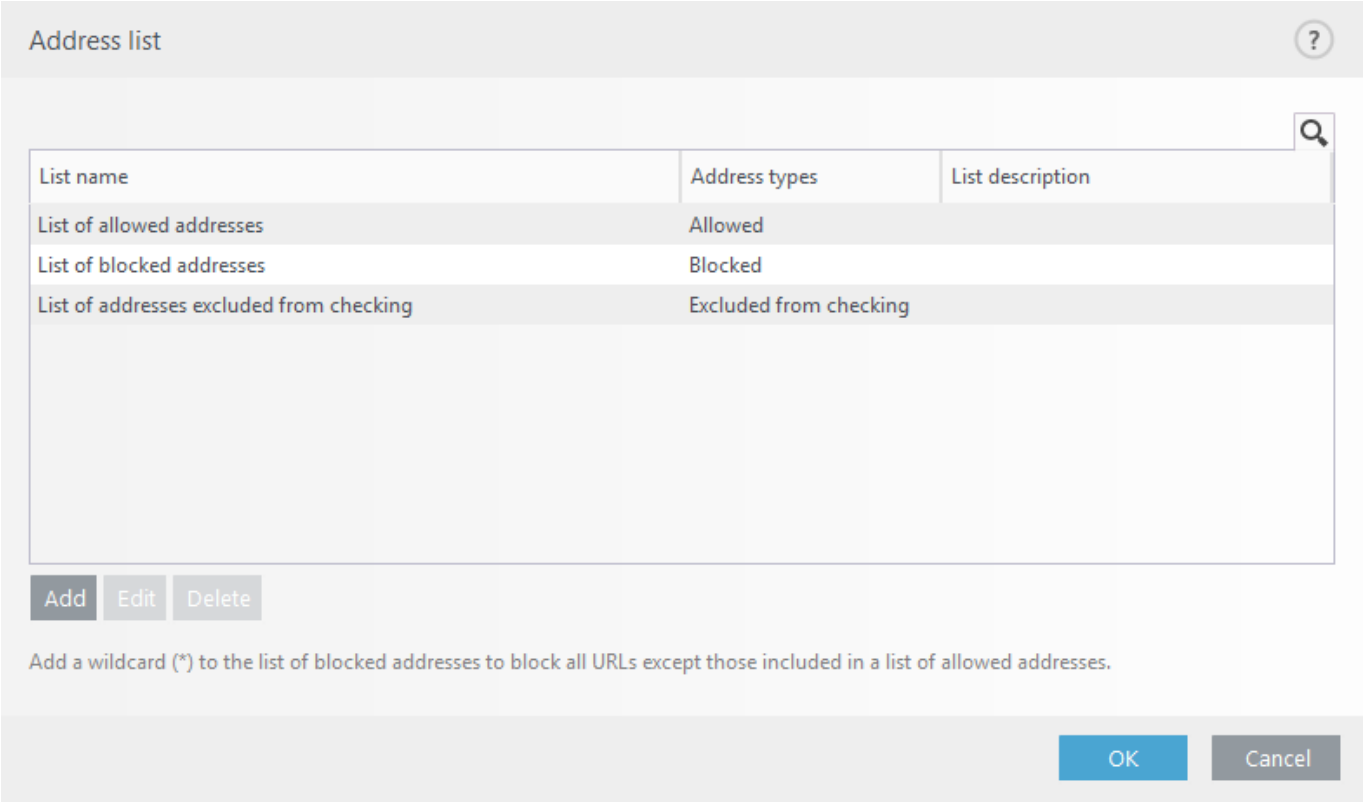
Un elenco di indirizzi bloccati potrebbe contenere indirizzi provenienti da blacklist pubbliche esterne e un altro la blacklist dell'utente. In tal modo, si facilita l'aggiornamento dell'elenco esterno mantenendo nel contempo intatto quello dell'utente.

Fare clic su **Modifica** e su **Aggiungi** per creare un nuovo elenco di indirizzi oltre a quelli predefiniti. Questa opzione è utile se si desidera suddividere vari gruppi di indirizzi in base a criteri logici. Per impostazione predefinita, sono disponibili i tre elenchi riportati di seguito:

- **Elenco indirizzi esclusi dal controllo**: per gli indirizzi aggiunti a questo elenco non verrà eseguita la ricerca di codice dannoso.

- **Elenco di indirizzi consentiti**: se è attivato Consenti accesso solo agli indirizzi HTTP dell'elenco di indirizzi consentiti e l'elenco di indirizzi bloccati contiene * (ricerca tutto), l'utente potrà accedere solo agli indirizzi specificati in questo elenco. Gli indirizzi in questo elenco sono consentiti anche se inclusi nell'elenco di indirizzi bloccati.

- **Elenco di indirizzi bloccati**: all'utente non sarà consentito di accedere agli indirizzi indicati in questo elenco a meno che non siano anche presenti nell'elenco di indirizzi consentiti.



È possibile **Aggiungere** un nuovo indirizzo URL all'elenco. È anche possibile immettere valori multipli con separatore. Fare clic su **Modifica** per modificare un indirizzo esistente nell'elenco, oppure su **Rimuovi** per eliminarlo. È possibile eliminare solo gli indirizzi creati con l'opzione **Aggiungi** e non quelli importati.

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.

> 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.

Crea nuovo elenco

L'elenco includerà gli indirizzi URL/le maschere di dominio desiderati che verranno bloccati, consentiti o esclusi dal controllo. Quando si crea un nuovo elenco, specificare i seguenti valori:

- **Tipo di elenco degli indirizzi**: scegliere il tipo (Escluso dal controllo, Bloccato o Consentito) dall'elenco a discesa.
- **Nome elenco**: specificare il nome dell'elenco. Il campo verrà disattivato durante la modifica di uno dei tre elenchi predefiniti.
- **Descrizione elenco**: digitare una breve descrizione per l'elenco (facoltativo). Verrà disattivato durante la modifica di uno dei tre elenchi predefiniti.
- **Elenco attivo**: utilizzare il pulsante per disattivare l'elenco. Se necessario, è possibile attivarlo in un secondo momento.

- **Avvisa in caso di applicazione**: utilizzare questa opzione se, in caso di utilizzo di un elenco specifico, si desidera ricevere una notifica contenente la valutazione di un sito HTTP/HTTPS visitato. Verrà inviata una notifica se un sito Web viene bloccato o consentito perché incluso nell'elenco di indirizzi rispettivamente bloccati o consentiti. La notifica conterrà il nome dell'elenco che include il sito Web specifico.

- **Gravità registrazione**: scegliere il livello di gravità della registrazione (Nessuno, Diagnostica, Informazioni o Avvertenza) nell'elenco a discesa. I record con un livello di dettaglio Avvertenza possono essere raccolti da ESET PROTECT.

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

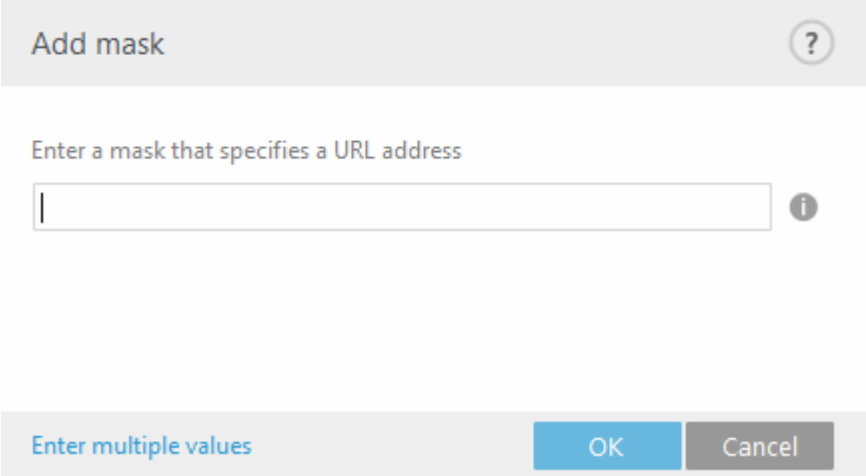
Le maschere includono i simboli ? e *:

- utilizzare ? per sostituire un simbolo

- utilizzare * per sostituire una stringa di testo

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

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

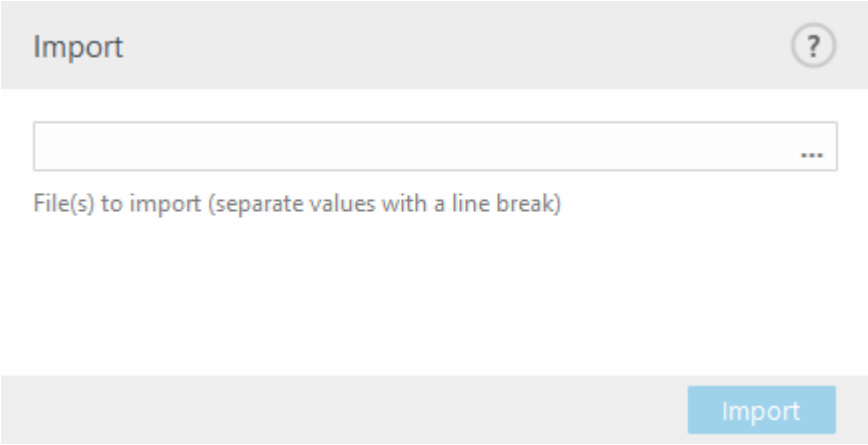


Inserisci valori multipli

Aggiungere indirizzi URL multipli delimitati da nuove righe, virgole o punti e virgola. Attivando selezioni multiple, sarà possibile visualizzare gli indirizzi nell'elenco.

Importa

File di testo con gli indirizzi URL da importare (separare i valori con un'interruzione di riga, ad esempio `*.txt` utilizzando la codifica UTF-8).

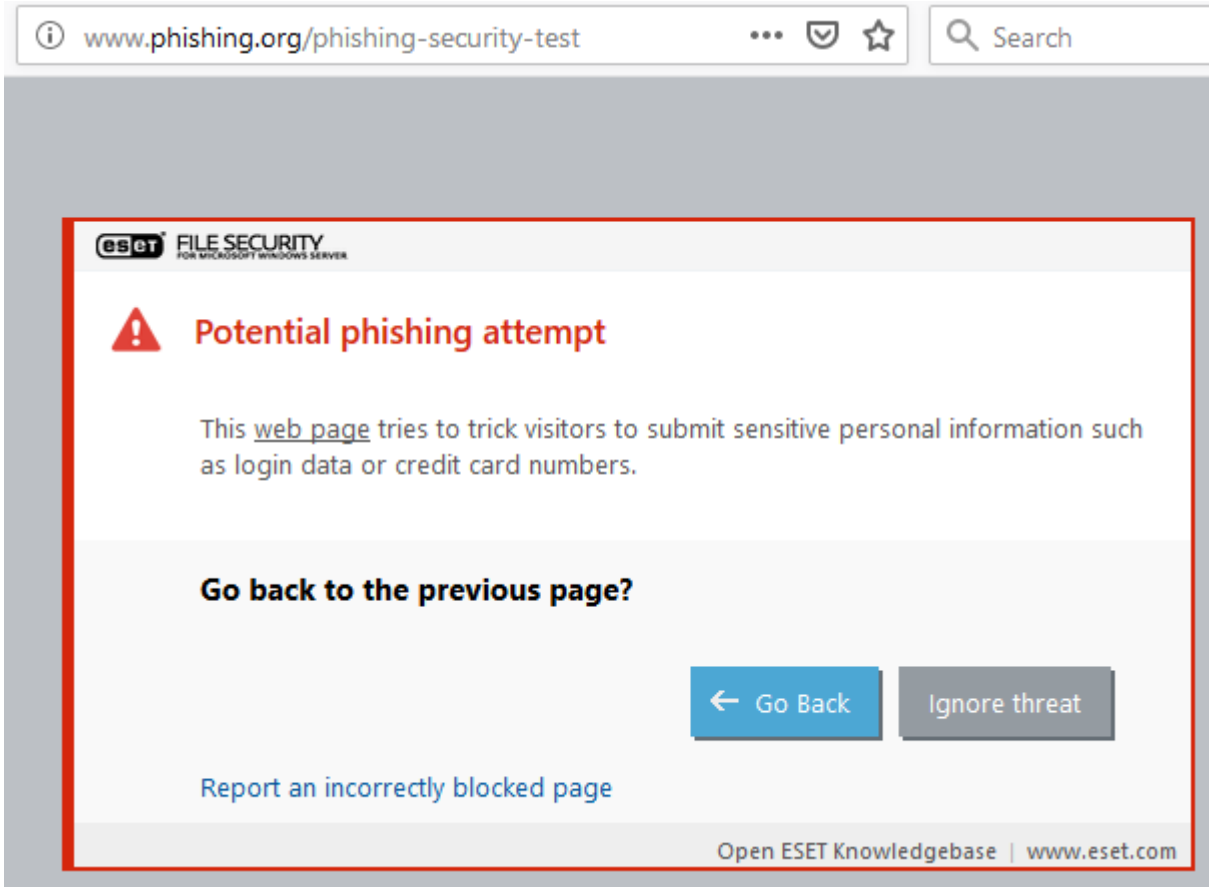


Protezione Web Anti-Phishing

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.

ESET Server Security include la protezione Anti-Phishing che blocca le pagine Web note per distribuire questo tipo di contenuto. Si consiglia vivamente di attivare la protezione Anti-Phishing in ESET Server Security. Consultare questo articolo della Knowledge Base per ulteriori informazioni sulla protezione Anti-Phishing in ESET Server Security.

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



> 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.

Segnala un sito phishing

Se si visita un sito Web sospetto che sembra essere phishing o in altro modo dannoso, è possibile segnalarlo a ESET ai fini dell'analisi. Prima di inviare un sito Web a ESET, assicurarsi che soddisfi uno o più dei criteri seguenti:

- il sito Web non viene rilevato
- il sito Web viene erroneamente rilevato come una minaccia. In questo caso, è possibile Segnalare 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.).

Controllo dispositivi

ESET Server Security include un controllo automatico dei dispositivi (CD/DVD/USB). Questo modulo consente all'utente di controllare, bloccare o regolare le estensioni dei filtri o delle autorizzazioni e di definire la propria capacità 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.

> Quando si attiva il controllo dispositivi tramite l’opzione **Integra nel sistema**, verrà attivata la funzionalità Controllo dispositivi di ESET Server Security. Tuttavia, per rendere effettiva questa modifica, è necessario riavviare il sistema.

Il Controllo dispositivi diventerà attivo, consentendo all’utente di modificarne le impostazioni. In caso di rilevamento di un dispositivo bloccato mediante una regola esistente, verrà visualizzata una finestra di notifica e l'accesso al dispositivo non sarà garantito.

Regole

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.

Gruppi

Quando si seleziona Modifica, è possibile gestire i Gruppi dispositivi. Creare un nuovo Gruppo dispositivi o selezionarne uno esistente per aggiungere o rimuovere i dispositivi dall’elenco.

> È possibile visualizzare le voci del rapporto Controllo dispositivi in File di rapporto.

Regole dispositivi

È possibile consentire o bloccare specifici dispositivi in base all'utente, al gruppo di utenti o a un qualsiasi parametro aggiuntivo da specificare nella configurazione delle regole. L'elenco di regole contiene varie descrizioni di una regola, ad esempio, il nome, il tipo di dispositivo esterno, l'azione da eseguire in seguito al rilevamento di un dispositivo e la gravità del rapporto.

È possibile selezionare **Aggiungi** per aggiungere un nuova regola oppure modificare le impostazioni di una regola esistente. 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.

Applica durante

Le regole possono essere limitate tramite le Fasce orarie. Creare prima la fascia oraria, che sarà quindi visualizzata nel menu a discesa.

Tipo di dispositivo

Scegliere il tipo di dispositivo esterno dal menu a discesa (Archiviazione su disco/Dispositivo portatile/Bluetooth/FireWire/...). I tipi di dispositivi vengono ereditati dal sistema operativo e possono essere visualizzati in Gestione dispositivi del sistema, ipotizzando che un dispositivo sia 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, che non forniscono informazioni sugli utenti, ma solo sulle azioni. Ciò implica che i dispositivi di acquisizione immagini 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.

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

Tipo di criterio

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

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

> i In caso di mancata definizione dei parametri, la regola ignorerà questi campi durante la ricerca delle corrispondenze. I parametri di filtraggio in tutti i campi di testo fanno distinzione tra maiuscolo e minuscolo e supportano i caratteri jolly (un punto interrogativo (?) rappresenta un carattere singolo, mentre un asterisco (*) rappresenta una stringa di zero o più caratteri).

Per trovare i parametri di un dispositivo, creare una regola che autorizzi il tipo di dispositivo, collegare il dispositivo al computer in uso, quindi rivedere i dettagli del dispositivo in Rapporto controllo dispositivi.

Scegliere la **Gravità registrazione** nell’elenco a discesa:

- **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. Fare clic su

Modifica per gestire **l'elenco di utenti**.

- **Aggiungi**: apre la finestra di dialogo Tipi di oggetto: Utenti o Gruppi, che consente di selezionare gli utenti desiderati.

- **Rimuovi**: rimuove l'utente selezionato dal filtro.

> 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 richiamate).

Sono disponibili le seguenti funzioni:

Modifica

Consente all'utente di modificare il nome di una regola selezionata o dei parametri dei dispositivi in esso contenuti (fornitore, modello, numero di serie).

Copia

Crea una nuova regola in base ai parametri della regola selezionata.

Elimina

Consente di eliminare la regola selezionata. In alternativa, è possibile utilizzare la casella di controllo accanto a una regola specifica per disattivarla. Questa opzione è utile se non si desidera eliminare definitivamente una regola in modo da poterla utilizzare in futuro.

Popola

Fornisce una panoramica di tutti i dispositivi attualmente connessi contenenti le seguenti informazioni: tipo di dispositivo, fornitore del dispositivo, modello e numero di serie (se disponibili). Dopo aver selezionato un dispositivo (dall'elenco di dispositivi rilevati) e aver fatto clic su **OK**, si aprirà una finestra di editor regole contenente le informazioni predefinite (è possibile modificare tutte le impostazioni).

Le regole sono disposte in ordine di priorità e quelle con priorità più elevata sono posizionate in alto. È possibile selezionare regole multiple e applicare azioni, ad esempio l'eliminazione o lo spostamento in alto o in basso nell'elenco, facendo clic su **In alto**/**Su**/**Giù**/**In basso** (pulsanti freccia).

Gruppi dispositivi

La finestra Gruppi dispositivi è suddivisa in due parti. La parte destra contiene un elenco di dispositivi appartenenti al gruppo di riferimento e la parte sinistra un elenco di gruppi esistenti. Selezionare il gruppo contenente i dispositivi che si desidera visualizzare nel riquadro di destra.

È possibile creare vari gruppi di dispositivi ai quali verranno applicate regole diverse. È anche possibile creare un singolo gruppo di dispositivi impostati su **Lettura**/**Scrittura** o **Di sola lettura**. Ciò consente al Controllo dispositivi di bloccare i dispositivi non riconosciuti che si connettono al computer in uso.

> La presenza di un dispositivo esterno connesso al computer in uso potrebbe rappresentare un rischio per la sicurezza.

Sono disponibili le seguenti funzioni:

Aggiungi

È possibile aggiungere un nuovo gruppo di dispositivi inserendone il nome o un dispositivo a un gruppo esistente (facoltativamente, è possibile specificare informazioni quali il nome del fornitore, il modello e il numero di serie) in base al punto della finestra in cui è stato premuto il pulsante.

Modifica

Consente all'utente di modificare il nome di un gruppo selezionato o i parametri dei dispositivi in esso contenuti (fornitore, modello, numero di serie).

Elimina

Consente di eliminare il gruppo o il dispositivo scelto in base al punto della finestra selezionato dall'utente. In alternativa, è possibile utilizzare la casella di controllo accanto a una regola specifica per disattivarla. Questa opzione è utile se non si desidera eliminare definitivamente una regola in modo da poterla utilizzare in futuro.

Importa

Consente di importare un elenco di numeri di serie di dispositivi da un file. Ciascun dispositivo inizia dalla nuova riga.

Per ciascun dispositivo devono essere presenti le informazioni relative al **Fornitore**, al **Modello** e al **Numero di serie**, separati da una virgola.

✔ Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101

Popola

Fornisce una panoramica di tutti i dispositivi attualmente connessi contenenti le seguenti informazioni: tipo di dispositivo, fornitore del dispositivo, modello e numero di serie (se disponibili). Dopo aver selezionato un dispositivo (dall'elenco di dispositivi rilevati) e aver fatto clic su **OK**, si aprirà una finestra di editor regole contenente le informazioni predefinite (è possibile modificare tutte le impostazioni).

Aggiungi dispositivo

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

- **Fornitore**: filtraggio in base al nome o all'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.
- **Descrizione**: descrizione del dispositivo fornita dall’utente per una migliore organizzazione.

> In caso di mancata definizione dei parametri, la regola ignorerà questi campi durante la ricerca delle corrispondenze. I parametri di filtraggio in tutti i campi di testo fanno distinzione tra maiuscolo e minuscolo e supportano i caratteri jolly (un punto interrogativo (?) rappresenta un carattere singolo, mentre un asterisco (*) rappresenta una stringa di zero o più caratteri).

Dopo aver creato un gruppo di dispositivi, è necessario aggiungere una nuova regola di controllo dei dispositivi per il gruppo di dispositivi creato e scegliere l'azione da eseguire.

Una volta completata la personalizzazione, fare clic su **OK**. Fare clic su **Annulla** per abbandonare la finestra **Gruppi dispositivi** senza salvare le modifiche.

> Tenere presente che non sono disponibili tutti i diritti (Azioni) per tutti i tipi di dispositivi. Se su un dispositivo è presente spazio di archiviazione, saranno disponibili tutte e quattro le azioni. Per i dispositivi non di archiviazione, sono disponibili solo due azioni (ad esempio, l'azione Solo lettura non è disponibile per il sistema Bluetooth. Ciò significa che i dispositivi Bluetooth possono essere solo consentiti o bloccati).

Configurazione degli strumenti

È possibile personalizzare le seguenti impostazioni avanzate:

- Fasce orarie
- Microsoft Windows® Update
- ESET CMD
- ESET RMM
- Licenza
- Provider WMI
- Destinazioni di controllo della console di gestione ESET
- File di rapporto
- Modalità presentazione
- Diagnostica
- Cluster

Fasce orarie

Le fasce orarie sono utilizzate all'interno delle Regole controllo dispositivi per limitare le regole in fase di applicazione. Creare una fascia oraria e selezionarla quando si aggiungono regole o si modificano quelle esistenti (parametro **Applica durante**). Questa funzione consente all'utente di definire fasce orarie utilizzate comunemente (orario di lavoro, fine settimana e così via) e di riutilizzarle facilmente senza dover definire l'intervallo orario per ogni regola. Una fascia oraria dovrebbe essere applicabile a qualsiasi tipo di regola che supporta il controllo basato sul tempo.

Aggiornamento Microsoft Windows

Gli aggiornamenti di Windows offrono importanti correzioni a pericolose vulnerabilità potenziali e migliorano il livello di protezione generale del computer dell'utente. Per questo motivo, è fondamentale installare gli aggiornamenti di Microsoft Windows non appena disponibili. ESET Server 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 potrebbero non essere disponibili subito dopo il salvataggio delle modifiche.

Scanner riga di comando

In alternativa a eShell, è possibile eseguire lo Scanner su richiesta ESET Server Security tramite la riga di comando utilizzando `ecls.exe` posizionato nella cartella di installazione.

Segue un elenco di parametri e opzioni:

Opzioni:

`/base-dir=FOLDER`	carica moduli da CARTELLA
`/quar-dir=FOLDER`	CARTELLA di quarantena
`/exclude=MASK`	escludi dal controllo i file corrispondenti a MASCHERA
`/subdir`	eseguire 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 il controllo
`/symlink`	segui i collegamenti simbolici (impostazione predefinita)
`/no-symlink`	ignora collegamenti simbolici
`/ads`	esegui il controllo di ADS (impostazione predefinita)
`/no-ads`	non eseguire il controllo 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	eseguire controllo dei file (impostazione predefinita)
/no-files	non eseguire controllo dei file
/memory	esegui controllo della memoria
/boots	esegui il controllo dei settori di avvio
/no-boots	non eseguire il controllo 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 il controllo 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 il controllo
/scan-timeout=LIMIT	eseguire controllo degli archivi per LIMITE secondi al massimo
/max-arch-size=SIZE	esegui il controllo dei file di un archivio solo se inferiori a DIMENSIONE (impostazione predefinita 0 = illimitato)
/max-sfx-size=SIZE	esegui il controllo dei file di un archivio autoestraente solo se inferiori a DIMENSIONE megabyte (impostazione predefinita 0 = illimitato)
/mail	esegui il controllo dei file di e-mail (impostazione predefinita)
/no-mail	non eseguire controllo dei file di e-mail
/mailbox	esegui il controllo delle caselle di posta (impostazione predefinita)
/no-mailbox	non eseguire il controllo delle caselle di posta
/sfx	esegui il controllo degli archivi autoestraenti (impostazione predefinita)
/no-sfx	non eseguire controllo degli archivi autoestraenti
/rtp	esegui il controllo degli eseguibili compressi (impostazione predefinita)
/no-rtp	non eseguire controllo degli eseguibili compressi
/unsafe	eseguire controllo delle applicazioni potenzialmente pericolose
/no-unsafe	non eseguire il controllo delle applicazioni potenzialmente pericolose (impostazione predefinita)
/unwanted	eseguire controllo delle applicazioni potenzialmente indesiderate
/no-unwanted	non eseguire il controllo delle applicazioni potenzialmente indesiderate (impostazione predefinita)
/suspicious	ricerca applicazioni sospette (impostazione predefinita)
/no-suspicious	non ricercare applicazioni sospette
/pattern	utilizza le firme digitali (impostazione predefinita)
/no-pattern	non utilizzare le firme digitali
/heur	attiva l'euristica (impostazione predefinita)

/no-heur	disattiva l'euristica
/adv-heur	attiva l'euristica avanzata (impostazione predefinita)
/no-adv-heur	disattiva Euristica avanzata
/ext-exclude=EXTENSIONS	escludi dal controllo il file ESTENSIONI delimitato da due punti
/clean-mode=MODE	utilizza la MODALITÀ pulizia per gli oggetti infetti Sono disponibili le seguenti opzioni: • none (impostazione predefinita): non verrà eseguita alcuna pulizia automatica. • standard: ecls.exe tenterà di pulire o rimuovere automaticamente i file infetti. • strict: ecls.exe tenterà di pulire o rimuovere automaticamente i file infetti senza l'intervento dell'utente (all'utente non verrà richiesto di confermare la rimozione dei file). • rigorous: ecls.exe rimuoverà i file senza tentare di eseguire la pulizia indipendentemente dalla tipologia. • delete: ecls.exe rimuoverà i file senza tentare di eseguire la pulizia, ma non rimuoverà file sensibili come i file di sistema di Windows.
/quarantine	copia i file infetti (se puliti) in Quarantena (integra l'azione eseguita durante la pulizia)
/no-quarantine	non copiare file infettati in Quarantena

Opzioni generali:

/help	mostra Guida ed esci
/version	mostra informazioni sulla versione ed esci
/preserve-time	mantieni indicatore data e ora dell'ultimo accesso

Codici di uscita:

0	nessuna minaccia trovata
1	minacce trovate e pulite
10	non è possibile controllare alcuni file (potrebbe trattarsi di minacce)
50	minaccia trovata
100	errore (i codici di uscita superiori a 100 significano che il file non è stato controllato e non può essere considerato pulito)

ESET CMD

Questa funzione consente di attivare i comandi ecmd avanzati. Consente all'utente di esportare e importare impostazioni utilizzando la riga di comando (ecmd.exe). Finora era possibile esportare solo le importazioni utilizzando la configurazione dell'interfaccia grafica utente Graphical User Interface, GUI. La configurazione di ESET Server Security può essere esportata in un file *.xml*.

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

- **Nessuna**: nessuna autorizzazione. Si sconsiglia di utilizzare questo metodo in quanto consente di importare configurazioni non firmate che rappresentano un rischio potenziale.

- **Password configurazione avanzata**: è richiesta una password per l'importazione di una configurazione da

un file .xml, che deve essere firmato (consultare Firma del file di configurazione .xml di seguito). La password specificata in Configurazione dell'accesso deve essere fornita prima dell'importazione di una nuova configurazione. Se la configurazione dell'accesso non è stata attivata, la password non corrisponde o il file di configurazione .xml non è stato firmato, la configurazione non sarà importata.

Dopo aver attivato ESET CMD, è possibile utilizzare la riga di comando per importare o esportare le configurazioni di ESET Server Security. È possibile eseguire questa operazione manualmente o creare uno script per l'automazione.

Per utilizzare i comandi ecmd avanzati, è necessario eseguirli con privilegi di amministratore o aprire un prompt dei comandi di Windows (cmd) utilizzando **Esegui come amministratore**. In caso contrario, verrà visualizzato il messaggio **Errore durante l'esecuzione del comando**. Inoltre, durante l'esportazione di una configurazione, la cartella di destinazione deve essere esistente. Il comando Esporta continua a funzionare anche in caso di disattivazione dell'impostazione ESET CMD.

Comando Esporta impostazioni:
`ecmd /getcfg c:\config\settings.xml`

Comando Importa impostazioni:
`ecmd /setcfg c:\config\settings.xml`

I comandi ecmd avanzati possono essere eseguiti solo localmente. L'esecuzione dell'attività client **Esegui comando** con ESET PROTECT non funzionerà.

Firma di un file di configurazione *.xml*:

1. Scaricare l'eseguibile XmlSignTool.

2. Aprire un prompt dei comandi di Windows (cmd) utilizzando **Esegui come amministratore**.

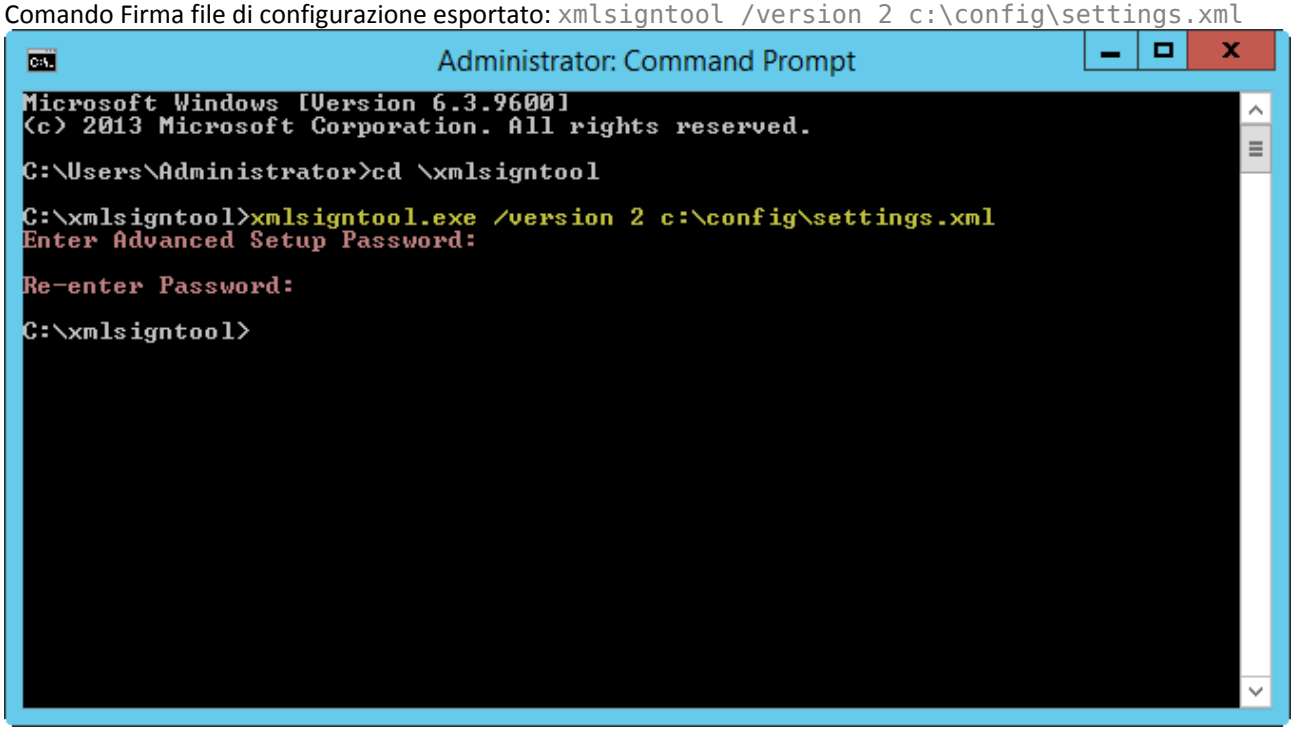
3. Individuare il file `xmlsigntool.exe`

4. Eseguire un comando per firmare il file di configurazione *.xml*, utilizzo: `xmlsigntool /version 1|2 <xml_file_path>`

Il valore del parametro `/version` dipende dalla versione di ESET Server Security. Utilizzare `/version 2` per ESET Server Security 7 e versioni successive.

5. Inserire e reinserire la password della configurazione avanzata richiesta da XmlSignTool. Il file di configurazione *.xml* è ora firmato e può essere utilizzato per l'importazione su un'altra istanza di ESET Server Security con ESET CMD mediante il metodo di autorizzazione con password.

Comando Firma file di configurazione esportato: `xmlsigntool /version 2 c:\config\settings.xml`



Se la password della configurazione dell'accesso viene modificata e si desidera importare una configurazione firmata in precedenza con una vecchia password, è possibile firmare nuovamente il file di configurazione *.xml* utilizzando la password corrente. Ciò consente all'utente di utilizzare un file di configurazione precedente senza doverlo esportare su un'altra macchina su cui è in esecuzione ESET Server Security prima dell'importazione.

ESET RMM

RMM (Remote Monitoring and Management) è un processo di supervisione e controllo dei sistemi software (ad esempio quelli su desktop, server e dispositivi mobili) mediante un agente installato a livello locale al quale è possibile accedere tramite un fornitore di servizi di gestione.

Attiva RMM

Consente di rendere operativi i comandi di RMM. Per poter utilizzare l'attività RMM, è necessario disporre dei privilegi di amministratore.

Modalità operativa

Selezionare la modalità operativa di RMM nel menu a discesa:

- **Solo separazione sicura**: se si desidera abilitare l'interfaccia RMM per le operazioni sicure e di sola lettura
- **Tutte le operazioni**: se si desidera abilitare l'interfaccia RMM per tutte le operazioni

Metodo di autorizzazione

Impostare il metodo di autorizzazione RMM nel menu a discesa:

- **Nessuno**: non verrà eseguito alcun controllo del percorso dell'applicazione e sarà possibile eseguire ermm.exe da qualsiasi applicazione

- **Percorso applicazione**: è possibile specificare l'applicazione autorizzata ad eseguire ermm.exe

L'installazione ESET Server Security predefinita contiene il file ermm.exe posizionato in ESET Server Security (percorso predefinito c:\Program Files\ESET\ESET Server Security). ermm.exe scambia dati con il plug-in RMM, che comunica con l'agente RMM, collegato a un server RMM.

- ermm.exe: Utilità della riga di comando sviluppata da ESET che consente di gestire i prodotti Endpoint e di comunicare con qualsiasi plug-in RMM.

- **Plug-in RMM**: applicazione di terze parti che viene eseguita a livello locale sul sistema Endpoint Windows. Il plug-in è stato sviluppato per comunicare con l'agente RMM specifico (ad esempio solo Kaseya) e con *ermm.exe*.

- **Agente RMM**: applicazione di terze parti (ad esempio di Kaseya) che viene eseguita a livello locale sul sistema Endpoint Windows. L'agente comunica con il plug-in RMM e con il server RMM.

- **Server RMM**: eseguito come un servizio su un server di terze parti. I sistemi RMM supportati sono Kaseya, Labtech, Autotask, Max Focus e Solarwinds N-able.

Consultare questo articolo della Knowledge Base per ulteriori informazioni su ESET RMM in ESET Server Security.

Plug-in ESET Direct Endpoint Management per soluzioni RMM di terze parti

Il server RMM è in esecuzione come servizio su un server di terze parti. Per ulteriori informazioni, consultare le seguenti guide per l'utente di ESET Direct Endpoint Management online:

- Plug-in ESET Direct Endpoint Management per ConnectWise Automate

- Plug-in ESET Direct Endpoint Management per DattoRMM

- ESET Direct Endpoint Management per Solarwinds N-Central

- ESET Direct Endpoint Management per NinjaRMM

Licenza

ESET Server Security si connette a ESET License Server alcune volte ogni ora per i controlli di preforma. Per impostazione predefinita, il parametro **Controllo intervallo** è impostato su **Automatico**. Se si desidera ridurre il traffico di rete causato dai controlli delle licenze, modificare il Controllo intervallo in **Limitato** e il controllo della licenza verrà eseguito solo una volta al giorno (anche dopo il riavvio del server).

Con il Controllo intervallo impostato su **Limitato**, tutte le modifiche relative alla licenza eseguite su ESET Server Security tramite ESET Business Account e a ESET MSP Administrator potrebbero richiedere fino a un giorno per l'applicazione.

ESET Server Security si connette al server delle licenze di ESET più volte in un'ora per eseguire controlli. Per impostazione predefinita, il parametro **Controllo intervallo** è impostato su **Automatico**. Se si desidera ridurre il traffico di rete causato dai controlli delle licenze, modificare il Controllo intervallo in Limitato e il controllo della licenza verrà eseguito solo una volta al giorno (anche dopo il riavvio del server).

Con il Controllo intervallo impostato su **Limitato**, tutte le modifiche relative alla licenza eseguite su ESET Server Security tramite ESET Business Account e a ESET MSP Administrator potrebbero richiedere fino a un giorno per l'applicazione.

Provider WMI

Windows Management Instrumentation (WMI) è l'implementazione Microsoft di Web-Based Enterprise Management (WBEM), ovvero un'iniziativa industriale basata sullo sviluppo di una tecnologia standard per l'accesso alle informazioni di gestione in un ambiente aziendale.

Per ulteriori informazioni su WMI, consultare
http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx

ESET WMI Provider

ESET WMI Provider è stato concepito allo scopo di garantire il monitoraggio remoto dei prodotti ESET in un ambiente aziendale senza la necessità di utilizzare software o strumenti ESET. L'offerta di informazioni di base sul prodotto, sullo stato e sulele statistiche attraverso WMI consente a ESET di ampliare notevolmente le possibilità degli amministratori aziendali durante il monitoraggio dei prodotti ESET.

Gli amministratori possono usufruire dei numerosi metodi di accesso offerti da WMI (riga di comando, script e strumenti di monitoraggio aziendali di terze parti) per monitorare lo stato dei propri prodotti ESET.

L'implementazione corrente offre un accesso di sola lettura alle informazioni di base sul prodotto, alle funzioni installate e al relativo stato di protezione, alle statistiche dei singoli scanner e ai file dei rapporti dei prodotti.

Il fornitore WMI consente di utilizzare l'infrastruttura e gli strumenti Windows WMI standard per la lettura dello stato e dei rapporti del prodotto.

Dati forniti

Tutte le classi WMI correlate al prodotto ESET sono posizionate nello spazio dei nomi "root\ESET". Le seguenti classi, descritte in modo più approfondito nello spazio sottostante, sono attualmente implementate:

Generale

- ESET_Product
- ESET_Features
- ESET_Statistics

Rapporti

- ESET_ThreatLog
- ESET_EventLog
- ESET_ODFileScanLogs
- ESET_ODFileScanLogRecords

- ESET_ODServerScanLogs
- ESET_ODServerScanLogRecords
- ESET_HIPSLog
- ESET_URLLog
- ESET_DevCtrlLog
- ESET_GreylistLog
- ESET_MailServeg
- ESET_HyperVScanLogs
- ESET_HyperVScanLogRecords

Classe ESET_Product

Esiste solo un'istanza della classe ESET_Product. Le proprietà di questa classe fanno riferimento alle informazioni di base sul prodotto ESET installato:

- ID: identificatore del tipo di prodotto, ad esempio, "emsl"
- Name: nome del prodotto, ad esempio, "ESET Mail Security"
- FullName: nome completo del prodotto, ad esempio, "ESET Mail Security for IBM Domino"
- Version: versione del prodotto, ad esempio, "6.5.14003.0"
- VirusDBVersion: versione del database delle firme antivirali, ad esempio, "14533 (20161201)"
- VirusDBLastUpdate: indicatore della data e dell'ora dell'ultimo aggiornamento del database delle firme antivirali. La stringa contiene il timestamp nel formato DataOra WMI, ad esempio, "20161201095245.000000+060"
- LicenseExpiration: data di scadenza della licenza. La stringa contiene il timestamp nel formato DataOra WMI
- KernelRunning: valore booleano che indica se il servizio ekrn è in esecuzione sulla macchina, ad esempio “VERO”
- StatusCode: numero che indica lo stato di protezione del prodotto: 0: verde (OK), 1: giallo (avviso), 2: rosso (errore)
- StatusText: messaggio che descrive il motivo alla base di un codice di stato diverso da zero; in caso contrario, il valore è null

Classe ESET_Features

La classe ESET_Features presenta istanze multiple, in base al numero delle funzioni del prodotto. Ciascuna istanza della classe contiene:

- Name: nome della funzione (l'elenco dei nomi è fornito nella sezione sottostante)
- Status: stato della funzione: 0: inattiva, 1: disattivata, 2: attivata

Elenco di stringhe che rappresentano le funzioni del prodotto attualmente riconosciute:

- CLIENT_FILE_AV: protezione antivirus file system in tempo reale
- CLIENT_WEB_AV: protezione antivirus del client di posta
- CLIENT_DOC_AV: protezione antivirus dei documenti del client
- CLIENT_NET_FW: rapporto del Personal Firewall del client
- CLIENT_EMAIL_AV: protezione antivirus del client di posta
- CLIENT_EMAIL_AS: protezione antispam delle e-mail del client
- SERVER_FILE_AV: protezione antivirus in tempo reale dei file sul server dei file protetti, ad esempio, file presenti nel database dei contenuti di SharePoint nel caso di ESET Server Security
- SERVER_EMAIL_AV: protezione antivirus delle e-mail del prodotto server, per esempio, e-mail in Microsoft Exchange o IBM Lotus Domino
- SERVER_EMAIL_AS: protezione antispam delle e-mail del prodotto server, per esempio, e-mail in Microsoft Exchange o IBM Lotus Domino
- SERVER_GATEWAY_AV: protezione antivirus dei protocolli delle reti protette sul gateway
- SERVER_GATEWAY_AS: protezione antispam dei protocolli delle reti protette sul gateway

Classe ESET_Statistics

La classe ESET_Statistics presenta istanze multiple, in base al numero di scanner presenti nel prodotto. Ciascuna istanza della classe contiene:

- Scanner: codice della stringa per lo scanner specifico, ad esempio, “CLIENT_FILE”
- Total: numero totale di file controllati
- Infected: numero di file infetti trovati
- Cleaned: numero di file puliti
- Timestamp: indicatore della data e dell'ora dell'ultima modifica di questa statistica. Espresso nel formato dataora WMI, ad esempio, "20130118115511.000000+060"
- ResetTime: indicatore della data e dell'ora dell'ultimo azzeramento del contatore di statistiche. Espresso nel formato dataora WMI, ad esempio, "20130118115511.000000+060"

Elenco di stringhe che rappresentano gli scanner attualmente riconosciuti:

- CLIENT_FILE

- CLIENT_EMAIL
- CLIENT_WEB
- SERVER_FILE
- SERVER_EMAIL
- SERVER_WEB

Classe ESET_ThreatLog

La classe ESET_ThreatLog presenta istanze multiple e ciascuna di esse rappresenta un record del rapporto "Minacce rilevate". Ciascuna istanza della classe contiene:

- ID: ID univoco di questo record di rapporto del controllo
- Timestamp: creazione dell'indicatore della data e dell'ora del rapporto (nel formato data/ora WMI)
- LogLevel: livello di gravità del record di rapporto espresso come numero nell'intervallo [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- Scanner: nome dello scanner che ha creato questo evento del rapporto
- ObjectType: tipo di oggetto che ha prodotto questo evento del rapporto
- ObjectName: nome dell'oggetto che ha prodotto questo evento del rapporto
- Threat: nome della minaccia che è stata trovata nell'oggetto descritto dalle proprietà ObjectName e ObjectType
- Action: azione eseguita in seguito all'identificazione della minaccia
- User: account utente che ha causato la generazione di questo evento di rapporto
- Information: descrizione aggiuntiva dell'evento
- Hash: hash dell'oggetto che ha prodotto questo evento del rapporto

ESET_EventLog

La classe ESET_EventLog presenta istanze multiple e ciascuna di esse rappresenta un record del rapporto "Eventi". Ciascuna istanza della classe contiene:

- ID: ID univoco di questo record di rapporto del controllo
- Timestamp: creazione dell'indicatore della data e dell'ora del rapporto (nel formato data/ora WMI)
- LogLevel: livello di gravità del record di rapporto espresso come numero nell'intervallo [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- Module: nome del modulo che ha creato questo evento del rapporto

- Event: descrizione dell'evento
- User: account utente che ha causato la generazione di questo evento di rapporto

ESET_ODFileScanLogs

La classe ESET_ODFileScanLogs presenta istanze multiple e ciascuna di esse rappresenta un record di controllo dei file su richiesta. Tale funzione equivale all'elenco di rapporti "Controllo computer su richiesta" della GUI. Ciascuna istanza della classe contiene:

- ID: ID univoco di questo record di rapporto del controllo
- Timestamp: creazione dell'indicatore della data e dell'ora del rapporto (nel formato data/ora WMI)
- Targets: cartelle/oggetti di destinazione del controllo
- TotalScanned: numero totale di oggetti controllati
- Infected: numero di oggetti infetti trovati
- Cleaned: numero di oggetti puliti
- Status: stato del processo di controllo

ESET_ODFileScanLogRecords

La classe ESET_ODFileScanLogRecords presenta istanze multiple e ciascuna di esse rappresenta un record di uno dei rapporti di controllo rappresentati dalle istanze della classe ESET_ODFileScanLogs. Le istanze di questa classe offrono record di rapporto di tutti i controlli/rapporti su richiesta. Se sono richieste solo le istanze di uno specifico rapporto di controllo, è necessario filtrarle in base alla proprietà LogID. Ciascuna istanza della classe contiene:

- LogID: ID del rapporto di controllo a cui appartiene questo record (ID di una delle istanze della classe ESET_ODFileScanLogs)
- ID: ID univoco di questo record di rapporto del controllo
- Timestamp: creazione dell'indicatore della data e dell'ora del rapporto (nel formato data/ora WMI)
- LogLevel: livello di gravità del record di rapporto espresso come numero [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- Log: messaggio del rapporto effettivo

ESET_ODServerScanLogs

La classe ESET_ODServerScanLogs presenta istanze multiple e ciascuna di esse rappresenta un'esecuzione del controllo del server su richiesta. Ciascuna istanza della classe contiene:

- ID: ID univoco di questo record di rapporto del controllo
- Timestamp: creazione dell'indicatore della data e dell'ora del rapporto (nel formato data/ora WMI)
- Targets: cartelle/oggetti di destinazione del controllo

- TotalScanned: numero totale di oggetti controllati
- Infected: numero di oggetti infetti trovati
- Cleaned: numero di oggetti puliti
- RuleHits: numero totale di attivazioni della regola
- Status: stato del processo di controllo

ESET_ODServerScanLogRecords

La classe ESET_ODServerScanLogRecords presenta istanze multiple e ciascuna di esse rappresenta un record di uno dei rapporti di controllo rappresentati dalle istanze della classe ESET_ODServerScanLogs. Le istanze di questa classe offrono record di rapporto di tutti i controlli/rapporti su richiesta. Se sono richieste solo le istanze di uno specifico rapporto di controllo, è necessario filtrarle in base alla proprietà LogID. Ciascuna istanza della classe contiene:

- LogID: ID del rapporto di controllo a cui appartiene questo record (ID di una delle istanze della classe ESET_ ODServerScanLogs)
- ID: ID univoco di questo record di rapporto del controllo
- Timestamp: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)
- LogLevel: livello di gravità del record di rapporto espresso come numero nell'intervallo [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- Log: messaggio del rapporto effettivo

ESET_SmtpProtectionLog

La classe ESET_SmtpProtectionLog presenta istanze multiple e ciascuna di esse rappresenta un record del rapporto “Protezione Smtp". Ciascuna istanza della classe contiene:

- ID: ID univoco di questo record di rapporto del controllo
- Timestamp: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)
- LogLevel: livello di gravità del record di rapporto espresso come numero [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- HELODomain: nome del dominio HELO
- IP: indirizzo IP di origine
- Sender: mittente dell'e-mail
- Recipient: destinatario dell'e-mail

- ProtectionType: tipo di protezione utilizzata
- Action: azione eseguita
- Motivo: motivo alla base dell’azione
- TimeToAccept: numero di minuti in seguito ai quali l'e-mail verrà accettata

ESET_HIPSLog

La classe ESET_HIPSLog presenta istanze multiple e ciascuna di esse rappresenta un record del rapporto “HIPS". Ciascuna istanza della classe contiene:

- ID: ID univoco di questo record di rapporto
- Timestamp: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)
- LogLevel: livello di gravità del record di rapporto espresso come numero nell'intervallo [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- Application: applicazione di origine
- Target: tipo di operazione
- Action: azione intrapresa da HIPS, ad esempio consenti, nega e così via
- Rule: nome della regola responsabile dell’azione
- AdditionalInfo

ESET_URLLog

La classe ESET_URLLog presenta istanze multiple e ciascuna di esse rappresenta un record del rapporto “Siti Web filtrati". Ciascuna istanza della classe contiene:

- ID: ID univoco di questo record di rapporto
- Timestamp: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)
- LogLevel: livello di gravità del record di rapporto espresso come numero [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- URL: l’URL
- Status: cosa è successo all’URL, ad esempio “Bloccato dal Controllo Web”
- Application: applicazione che ha cercato di accedere all’URL
- User: account utente sul quale era in esecuzione l’applicazione

ESET_DevCtrlLog

La classe ESET_DevCtrlLog presenta istanze multiple e ciascuna di esse rappresenta un record del rapporto “Controllo dispositivi". Ciascuna istanza della classe contiene:

- ID: ID univoco di questo record di rapporto
- Timestamp: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)
- LogLevel: livello di gravità del record di rapporto espresso come numero [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- Device: nome del dispositivo
- User: nome dell’account utente
- UserSID: SID dell’account utente
- Group: nome del gruppo utente
- GroupSID: SID del gruppo utente
- Status: cosa è successo al dispositivo, ad esempio “Scrittura bloccata”
- DeviceDetails: ulteriori informazioni sul dispositivo
- EventDetails: ulteriori informazioni sull’evento

ESET_MailServerLog

La classe ESET_MailServerLog presenta istanze multiple e ciascuna di esse rappresenta un record del rapporto “Server di posta". Ciascuna istanza della classe contiene:

- ID: ID univoco di questo record di rapporto
- Timestamp: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)
- LogLevel: livello di gravità del record di rapporto espresso come numero [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- IPAddr: indirizzo IP di origine
- HELODomain: nome del dominio HELO
- Sender: mittente dell'e-mail
- Recipient: destinatario dell'e-mail
- Subject: oggetto dell’e-mail

- Tipo di protezione: tipo di protezione che ha eseguito l’azione descritta dal record del rapporto attuale, ad esempio anti-malware, antispam o regole.

- Action: azione eseguita

- Reason: motivo per il quale l’azione è stata eseguita sull’oggetto dal determinato ProtectionType.

ESET_HyperVScanLogs

La classe ESET_HyperVScanLogs presenta istanze multiple e ciascuna di esse rappresenta un’esecuzione del controllo del file Hyper-V. Tale funzione equivale all'elenco di rapporti "Controllo Hyper-V" della GUI. Ciascuna istanza della classe contiene:

- ID: ID univoco di questo record di rapporto

- Timestamp: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)

- Targets: macchine/dischi/volumi di destinazione del controllo

- TotalScanned: numero totale di oggetti controllati

- Infected: numero di oggetti infetti trovati

- Cleaned: numero di oggetti puliti

- Status: stato del processo di controllo

ESET_HyperVScanLogRecords

La classe ESET_HyperVScanLogRecords presenta istanze multiple e ciascuna di esse rappresenta un record di uno dei rapporti di controllo rappresentati dalle istanze della classe ESET_HyperVScanLogs. Le istanze di questa classe offrono record di rapporto di tutti i controlli/rapporti Hyper-V. Se sono richieste solo le istanze di uno specifico rapporto di controllo, è necessario filtrarle in base alla proprietà LogID. Ciascuna istanza della classe contiene:

- LogID: ID del rapporto di controllo a cui appartiene questo record (ID di una delle istanze della classe ESET_HyperVScanLogs)

- ID: ID univoco di questo record di rapporto

- Timestamp: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)

- LogLevel: livello di gravità del record di rapporto espresso come numero [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico

- Log: messaggio del rapporto effettivo

ESET_NetworkProtectionLog

La classe ESET_NetworkProtectionLog presenta istanze multiple e ciascuna di esse rappresenta un record del rapporto “Protezione di rete". Ciascuna istanza della classe contiene:

- ID: ID univoco di questo record di rapporto
- Timestamp: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)
- LogLevel: livello di gravità del record di rapporto espresso come numero [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- Evento: evento che ha attivato l'azione di protezione della rete
- Action: azione eseguita dalla protezione di rete
- Origine: indirizzo di origine del dispositivo di rete
- Destinazione: indirizzo di destinazione del dispositivo di rete
- Protocollo: protocollo di comunicazione della rete
- RuleOrWormName: regola o nome del worm correlato all'evento
- Applicazione: applicazione che ha iniziato la comunicazione di rete
- User: account utente che ha causato la generazione di questo evento di rapporto

ESET_SentFilesLog

La classe ESET_SentFilesLog presenta istanze multiple e ciascuna di esse rappresenta un record del rapporto "File inviati". Ciascuna istanza della classe contiene:

- ID: ID univoco di questo record di rapporto
- Timestamp: creazione dell'indicatore della data e dell'ora del record di rapporto (nel formato data/ora WMI)
- LogLevel: livello di gravità del record di rapporto espresso come numero [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- Sha1: hash Sha-1 del file inviato
- File: file inviato
- Dimensione: dimensione del file inviato
- Categoria: categoria del file inviato
- Motivo: motivo alla base dell'invio del file
- SentTo: reparto ESET al quale è stato inviato il file
- User: account utente che ha causato la generazione di questo evento di rapporto

ESET_OneDriveScanLogs

La classe ESET_OneDriveScanLogs presenta istanze multiple e ciascuna di esse rappresenta un’esecuzione del controllo OneDrive. Tale funzione equivale all'elenco di rapporti "Controllo OneDrive" della GUI. Ciascuna istanza della classe contiene:

- ID: ID univoco di questo rapporto OneDrive
- Timestamp: creazione dell'indicatore della data e dell'ora del rapporto (nel formato data/ora WMI)
- Targets: cartelle/oggetti di destinazione del controllo
- TotalScanned: numero totale di oggetti controllati
- Infected: numero di oggetti infetti trovati
- Cleaned: numero di oggetti puliti
- Status: stato del processo di controllo

ESET_OneDriveScanLogRecords

La classe ESET_OneDriveScanLogRecords presenta istanze multiple e ciascuna di esse rappresenta un record di uno dei rapporti di controllo rappresentati dalle istanze della classe ESET_OneDriveScanLogs. Le istanze di questa classe offrono record di rapporto di tutti i controlli/rapporti OneDrive. Se sono richieste solo le istanze di uno specifico rapporto di controllo, è necessario filtrarle in base alla proprietà LogID. Ciascuna istanza della classe contiene:

- LogID: ID del rapporto di controllo a cui appartiene questo record (ID di una delle istanze della classe ESET_OneDriveScanLogs)
- ID: ID univoco di questo rapporto OneDrive
- Timestamp: creazione dell'indicatore della data e dell'ora del rapporto (nel formato data/ora WMI)
- LogLevel: livello di gravità del record di rapporto espresso come numero [0-8]. I valori corrispondono ai seguenti livelli con nome: Debug, Informazioni-Nota a piè di pagina, Informazioni, Informazioni-Importanti, Avviso, Errore, AvvisoProtezione, Errore-Critico, AvvisoProtezione-Critico
- Log: messaggio del rapporto effettivo

Accesso ai dati forniti

Seguono alcuni esempi delle modalità di accesso ai dati ESET WMI dalla riga di comando Windows e PowerShell, che dovrebbero funzionare da qualsiasi sistema operativo Windows attualmente disponibile. Esistono, tuttavia, numerosi altri modi per accedere ai dati a partire da altri linguaggi e strumenti di scripting.

Riga di comando senza script

Lo strumento della riga di comando `wmic` può essere utilizzato per accedere a varie classi predefinite o WMI personalizzate.

Per visualizzare informazioni complete sul prodotto sulla macchina locale:

```
wmic /namespace:\\root\ESET Path ESET_Product
```

Per visualizzare solo il numero della versione del prodotto sulla macchina locale:

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

Per visualizzare informazioni complete sul prodotto su una macchina remota con IP 10.1.118.180:

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Per ottenere e visualizzare informazioni complete sul prodotto sulla macchina locale:

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

Per ottenere e visualizzare informazioni complete sul prodotto su una macchina remota con IP 10.1.118.180:

```
$cred = Get-
Credential # promts the user for credentials and stores it in the variable
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -
cred $cred
```

Destinazioni di controllo della console di gestione ESET

Questa funzionalità consente a ESET PROTECT di utilizzare la destinazione di controllo (controllo database casella di posta su richiesta e controllo Hyper-V) quando è in esecuzione l'attività client Controllo del server su un server con ESET Server Security. L'impostazione delle destinazioni di controllo ESET PROTECT è disponibile solo in caso di installazione di ESET Management Agent. In caso contrario, sarà disattivata.

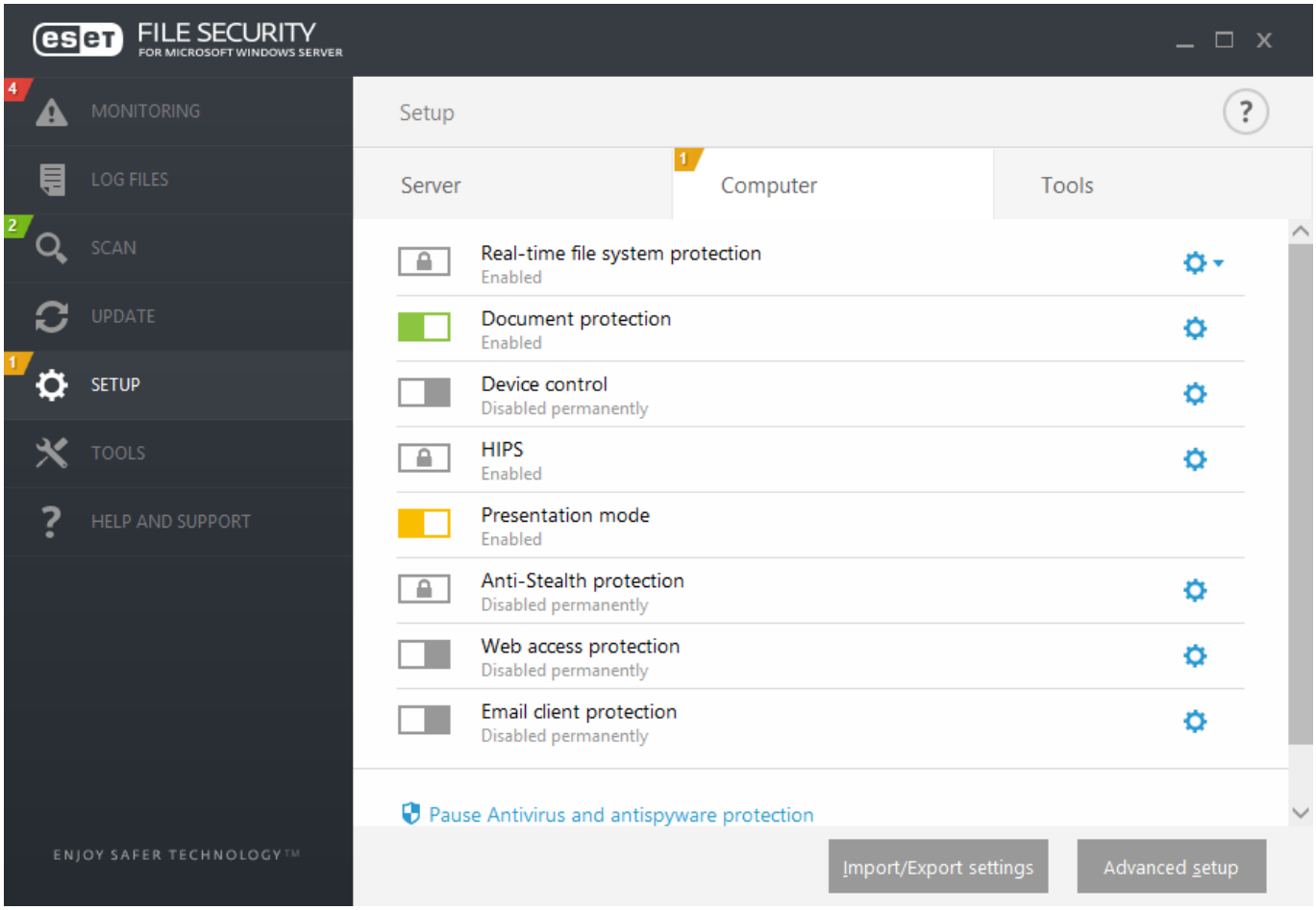
Quando si abilita l'opzione **Genera elenco destinazioni**, crea un elenco di destinazioni di controllo su richiesta disponibili. Se necessario, impostare il **Periodo di aggiornamento**.

> Se si attiva **Genera elenco destinazioni** per la prima volta, ESET PROTECT impiegherà all'incirca metà del **Periodo di aggiornamento** specificato per selezionarlo. Di conseguenza, se il **Periodo di aggiornamento** è impostato su 60 minuti, ESET PROTECT impiegherà all'incirca 30 minuti per ricevere l'elenco di destinazioni di controllo. Se si desidera che ESET PROTECT recuperi più rapidamente l'elenco, è necessario impostare il periodo di aggiornamento su un valore inferiore. È sempre possibile aumentare questo valore in un secondo momento.

Durante un'attività client di **Controllo server**, ESET PROTECT recupera l'elenco e chiede all'utente di selezionare le destinazioni di controllo per il Controllo Hyper-V sul server in questione.

Modalità override

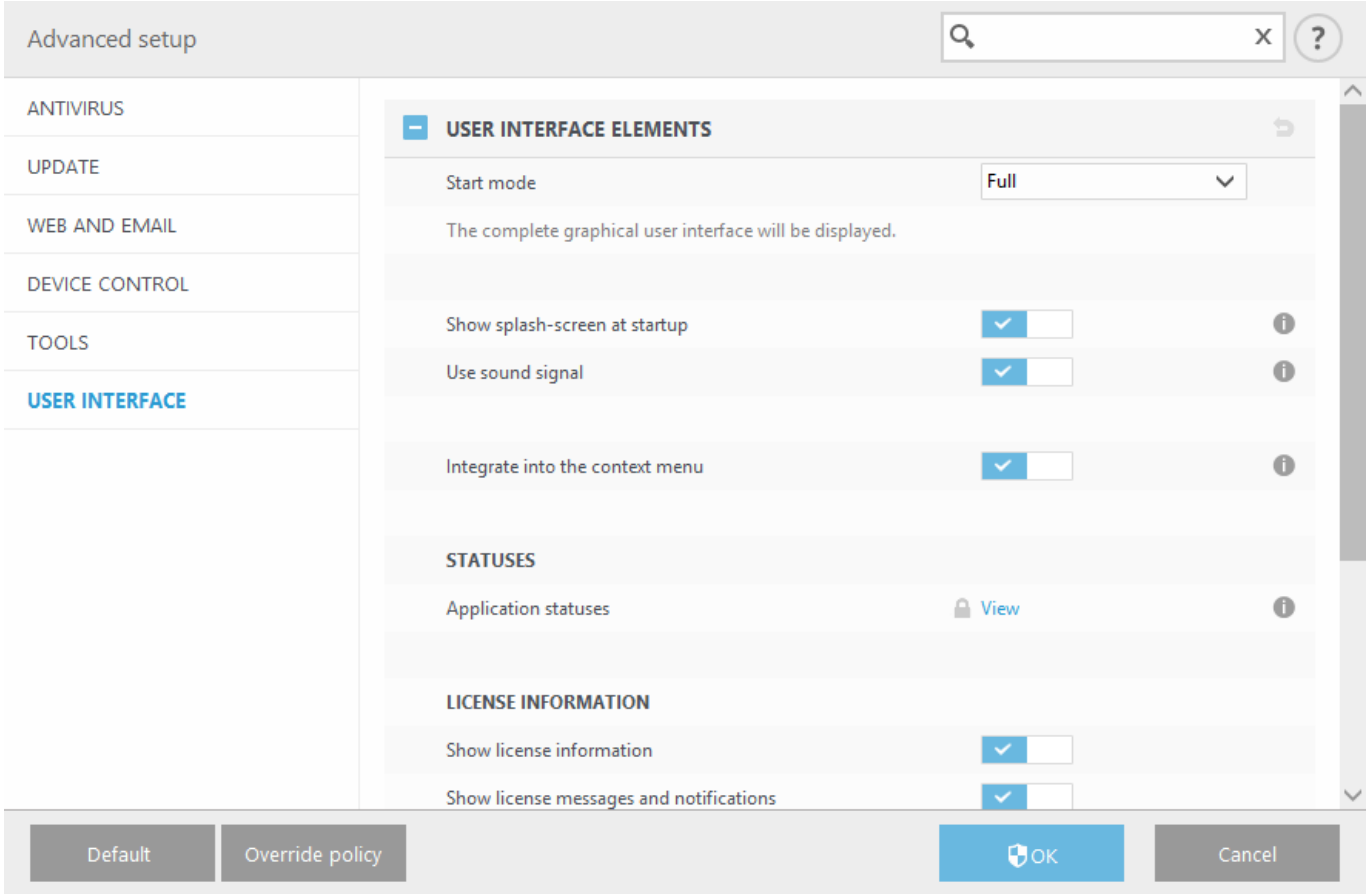
Se il criterio ESET PROTECT è stato applicato a ESET Server Security, compariranno un'icona a forma di lucchetto al posto del pulsante Attiva/Disattiva nella pagina di configurazione e un'icona a forma di lucchetto accanto al pulsante nella finestra **Configurazione avanzata**.



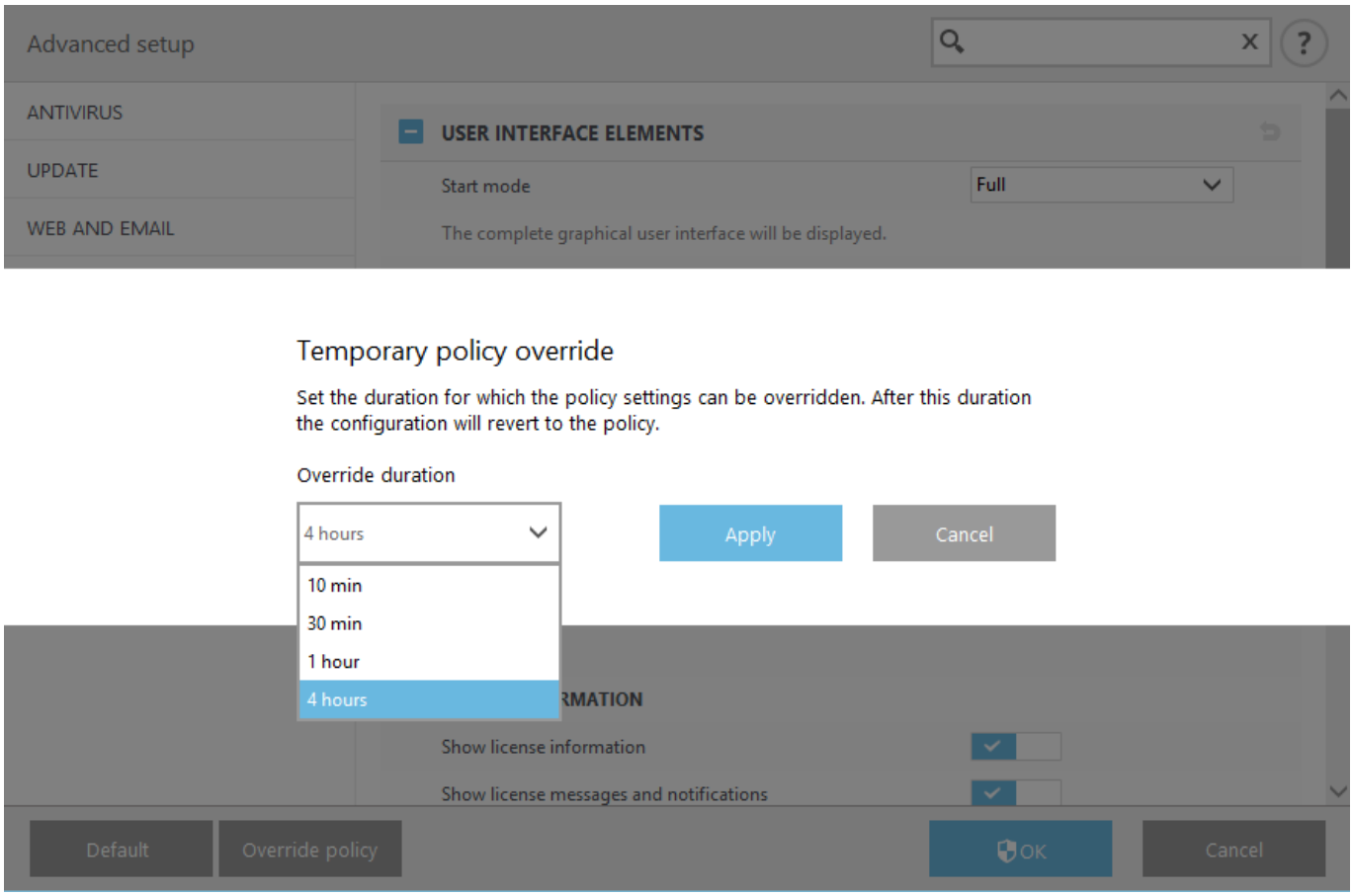
Normalmente, non è possibile modificare le impostazioni configurate mediante il criterio ESET PROTECT. La modalità override consente di sbloccare temporaneamente queste impostazioni. Tuttavia, la **Modalità override** deve essere attivata utilizzando il criterio ESET PROTECT.

Accedere a ESET PROTECT Web Console, aprire **Criteri** e selezionare e modificare il criterio esistente applicato a ESET Server Security o crearne uno nuovo. In **Impostazioni**, fare clic su **Modalità override**, attivarla e configurare il resto delle impostazioni, tra cui il tipo di autenticazione (Utente Active Directory o Password).

Dopo aver modificato il criterio esistente o applicato il nuovo criterio a ESET Server Security, comparirà il pulsante Criterio di override nella finestra **Configurazione avanzata**.

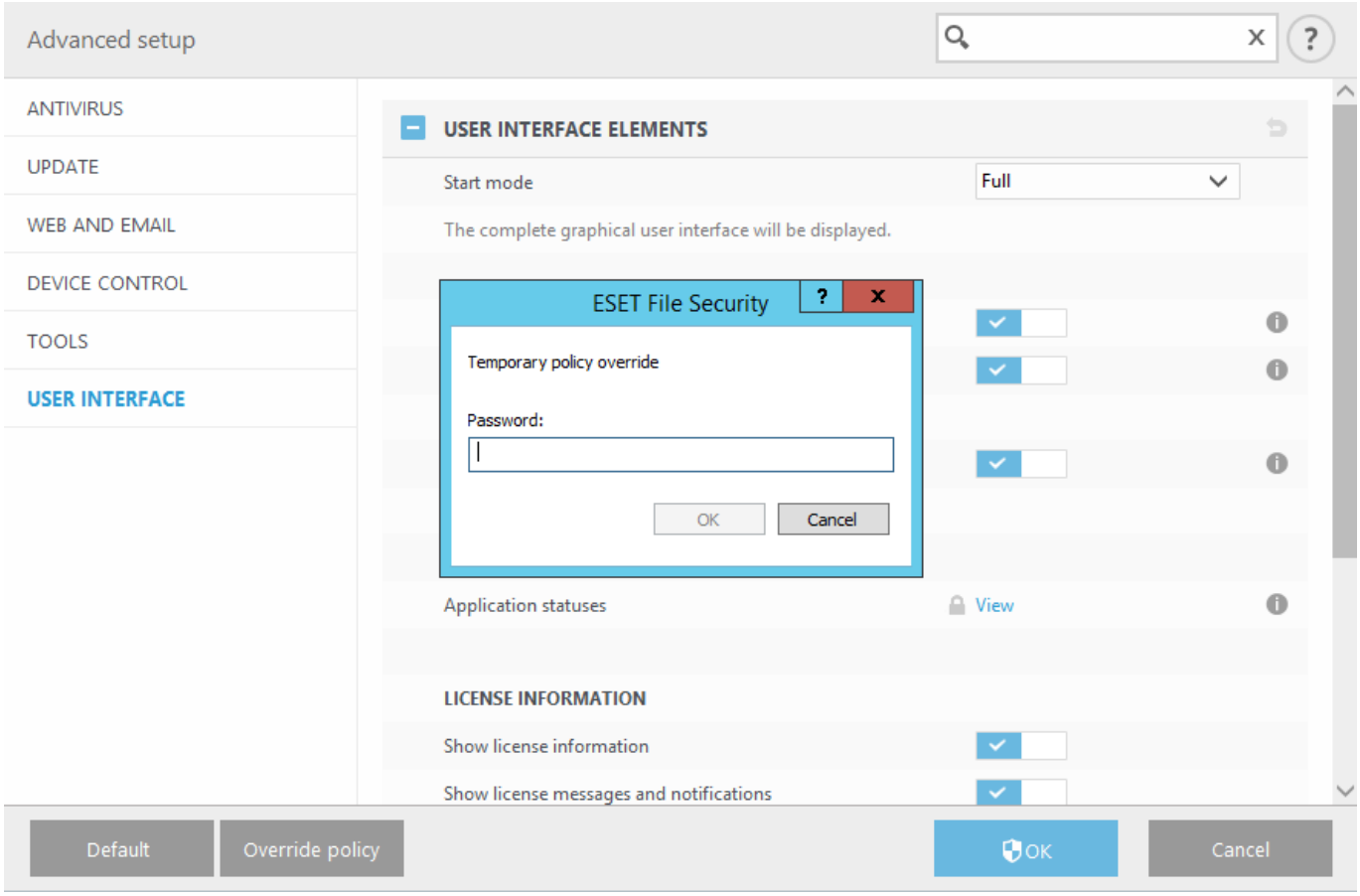


Fare clic sul pulsante **Criterio di override**, impostare la durata e fare clic su **Applica**.



Dopo aver selezionato **Password** come tipo di autenticazione, inserire la password della modalità override del

criterio.



In seguito alla scadenza della modalità override, la configurazione eventualmente modificata dall'utente verrà ripristinata in base alle impostazioni originali del criterio di ESET PROTECT. Prima della scadenza della modalità override, verrà visualizzata una notifica.

Prima della scadenza è possibile **Terminare la modalità override** in qualsiasi momento nella pagina Monitoraggio o nella finestra Configurazione avanzata.

File di rapporto

Questa sezione consente all'utente di modificare la configurazione della registrazione di ESET Server Security.

Filtro registrazione

Viene generata una quantità significativa di dati poiché tutte le opzioni di registrazione sono attivate per impostazione predefinita. Si consiglia di disattivare in maniera selettiva la registrazione dei componenti che non sono interessanti o correlati al problema.

> Per avviare la registrazione effettiva, è necessario attivare la **Registrazione diagnostica** generale a livello di prodotto nel menu principale **Configurazione** > Strumenti. Se è stata attivata la registrazione, ESET Server Security raccoglierà rapporti dettagliati in base alle funzioni attivate in questa sezione.

Utilizzare i pulsanti per attivare o disattivare funzioni specifiche. È anche possibile combinare questa opzione a seconda della disponibilità dei singoli componenti in ESET Server Security.

- **Registrazione diagnostica cluster**: la registrazione del cluster sarà inclusa nella registrazione diagnostica generale.
- **Registrazione diagnostica di OneDrive**: la registrazione di OneDrive sarà inclusa nella registrazione diagnostica generale.

File di rapporto

Definisce le modalità di gestione dei rapporti. Questa risorsa è importante soprattutto per prevenire un utilizzo eccessivo dello spazio sul disco. Le impostazioni predefinite consentono la cancellazione automatica dei rapporti meno recenti per liberare spazio sul disco.

Elimina record automaticamente

Le voci del rapporto precedenti al numero specificato di giorni (sotto) verranno rimosse.

Elimina record più vecchi di (giorni)

Specificare il numero di giorni.

Elimina automaticamente i vecchi record in caso di superamento delle dimensioni previste per i rapporti

Se la dimensione del rapporto supera la **Dimensione massima rapporto** [MB], i vecchi record del rapporto verranno eliminati fino al raggiungimento della **Dimensione ridotta rapporto** [MB].

Esegui il backup dei record eliminati automaticamente

Verrà eseguito il backup dei record e dei file di rapporto eliminati automaticamente nella directory specificata e, facoltativamente, la compressione in file ZIP.

Esegui il backup dei rapporti di diagnostica

Eseguirà il backup automatico dei rapporti di diagnostica eliminati. Se questa opzione non è attivata, non verrà eseguito il backup dei record dei rapporti di diagnostica.

Esegui backup cartella

Cartella in cui verranno archiviati i backup dei rapporti. È possibile attivare i backup dei rapporti compressi utilizzando un file ZIP.

Ottimizza automaticamente file di rapporto

Selezionando questa opzione, i file di rapporto verranno automaticamente deframmentati se la percentuale di frammentazione è superiore al valore specificato nel campo **Se il numero di record inutilizzati supera (%)**. Fare clic su **Ottimizza** per avviare la deframmentazione dei file di rapporto. Tutte le voci vuote del rapporto vengono rimosse allo scopo di migliorare le prestazioni e la velocità di elaborazione dei rapporti. Tale miglioramento può essere rilevato soprattutto nel caso in cui i rapporti contengano un numero elevato di voci.

Attiva protocollo di testo

Per attivare l'archiviazione dei rapporti in un altro formato di file separato da File di rapporto:

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

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

Rapporto di controllo

Monitora le modifiche apportate alla configurazione o alla protezione. Dal momento che la modifica della configurazione del prodotto potrebbe incidere in modo determinante sul suo funzionamento, è possibile monitorare le modifiche per scopi di controllo. I record dei rapporti delle modifiche sono disponibili nella sezione **File di rapporto** > Rapporto di controllo.

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 intendono ridurre al minimo l'utilizzo della CPU. La modalità presentazione può essere utilizzata anche durante le presentazioni che non possono essere interrotte dall'attività di ESET Server Security. Se abilitata, tutte le finestre di notifica verranno disabilitate e le attività pianificate non verranno eseguite. La protezione del sistema è ancora in esecuzione in background, ma non

richiede l'interazione dell'utente.

Attiva automaticamente modalità presentazione quando vengono eseguite applicazioni in modalità a schermo intero

La Modalità presentazione viene attivata automaticamente ogni volta che si esegue un’operazione a schermo intero. Quando è attiva, non sarà possibile visualizzare le notifiche o un cambiamento di stato di ESET Server Security.

Disattiva automaticamente modalità presentazione

Consente di definire l'intervallo di tempo espresso in minuti dopo il quale la Modalità presentazione verrà automaticamente disattivata.

Diagnostica

La diagnostica offre all'applicazione i dump di arresto anomalo dei processi ESET (ad esempio, *ekrn*). Se un'applicazione si arresta in modo anomalo, verrà generato un dump che aiuta gli sviluppatori a eseguire il debug e a risolvere vari ESET Server Security problemi.

Fare clic sul menu a discesa accanto a **Tipo di dump** e selezionare una delle tre opzioni disponibili:

- **Disattiva**: per disattivare questa funzionalità.
- **Mini**: (impostazione predefinita) 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. A causa delle informazioni limitate incluse, gli errori che non sono stati causati direttamente dal thread in esecuzione quando si è verificato il problema potrebbero tuttavia 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 in modo inaspettato. Un dump di memoria completo può contenere dati estrapolati dai processi in esecuzione al momento del recupero.

Directory di destinazione

Directory nella quale verrà generato il dump durante l'arresto anomalo.

Apri cartella diagnostica

Fare clic su **Apri** per aprire questa directory in una nuova finestra di Windows Explorer.

Crea dump di diagnostica

Fare clic su **Crea** per creare file dump di diagnostica nella directory Destinazione.

Registrazione avanzata

Abilita registrazione avanzata scanner computer – Registra tutti gli eventi che si verificano durante il controllo di file e cartelle da parte del controllo computer o della protezione file system in tempo reale.

Attiva registrazione avanzata Controllo dispositivi – Registra tutti gli eventi che si verificano nel Controllo

dispositivi per consentire la diagnosi e la risoluzione dei problemi.

Abilita registrazione avanzata Direct Cloud – Registra tutte le comunicazioni tra il prodotto e i server di Direct Cloud.

Attiva registrazione avanzata Protezione documenti – Registrare tutti gli eventi che si verificano nella Protezione documenti per consentire la diagnosi e la risoluzione dei problemi.

Abilita registrazione avanzata kernel – Registrare tutti gli eventi che si verificano nel servizio kernel ESET (ekrn) per consentire la diagnosi e la risoluzione dei problemi.

Abilita registrazione avanzata delle licenze: consente di registrare tutte le comunicazioni del prodotto con il server della licenza.

Abilita tracciatura memoria – Registra tutti gli eventi che aiuteranno gli sviluppatori a diagnosticare le perdite di memoria.

Attiva la registrazione avanzata protezione di rete – Registra tutti i dati di rete che attraversano la protezione di rete in formato PCAP. Tale operazione consente agli sviluppatori di diagnosticare e risolvere problemi correlati alla protezione di rete.

Attiva registrazione sistema operativo – Saranno raccolte informazioni aggiuntive sul sistema operativo, tra cui i processi in esecuzione, l'attività della CPU e le operazioni del disco. Questo funzionamento aiuta gli sviluppatori a diagnosticare e a risolvere problemi correlati al prodotto ESET in esecuzione sul sistema operativo in uso.

Attiva registrazione avanzata filtraggio protocolli – Registra tutti i dati che attraversano il motore di filtraggio protocolli in formato PCAP per consentire agli sviluppatori di diagnosticare e di correggere problemi correlati al filtraggio protocolli.

Abilita registrazione avanzata messaggistica push – Registra tutti gli eventi durante la messaggistica push per consentire la diagnosi e la risoluzione dei problemi.

Abilita registrazione avanzata della protezione file system in tempo reale: consente di registrare tutti gli eventi nella protezione file system in tempo reale ai fini della diagnosi e della risoluzione dei problemi.

Attiva registrazione avanzata motore aggiornamenti – Registra tutti gli eventi che si verificano durante il processo di aggiornamento. Tale operazione consente agli sviluppatori di facilitare la diagnosi e la correzione di eventuali problemi legati al motore degli aggiornamenti.

Percorso file di rapporto

C:\ProgramData\ESET\ESET Security\Diagnostics

Supporto tecnico

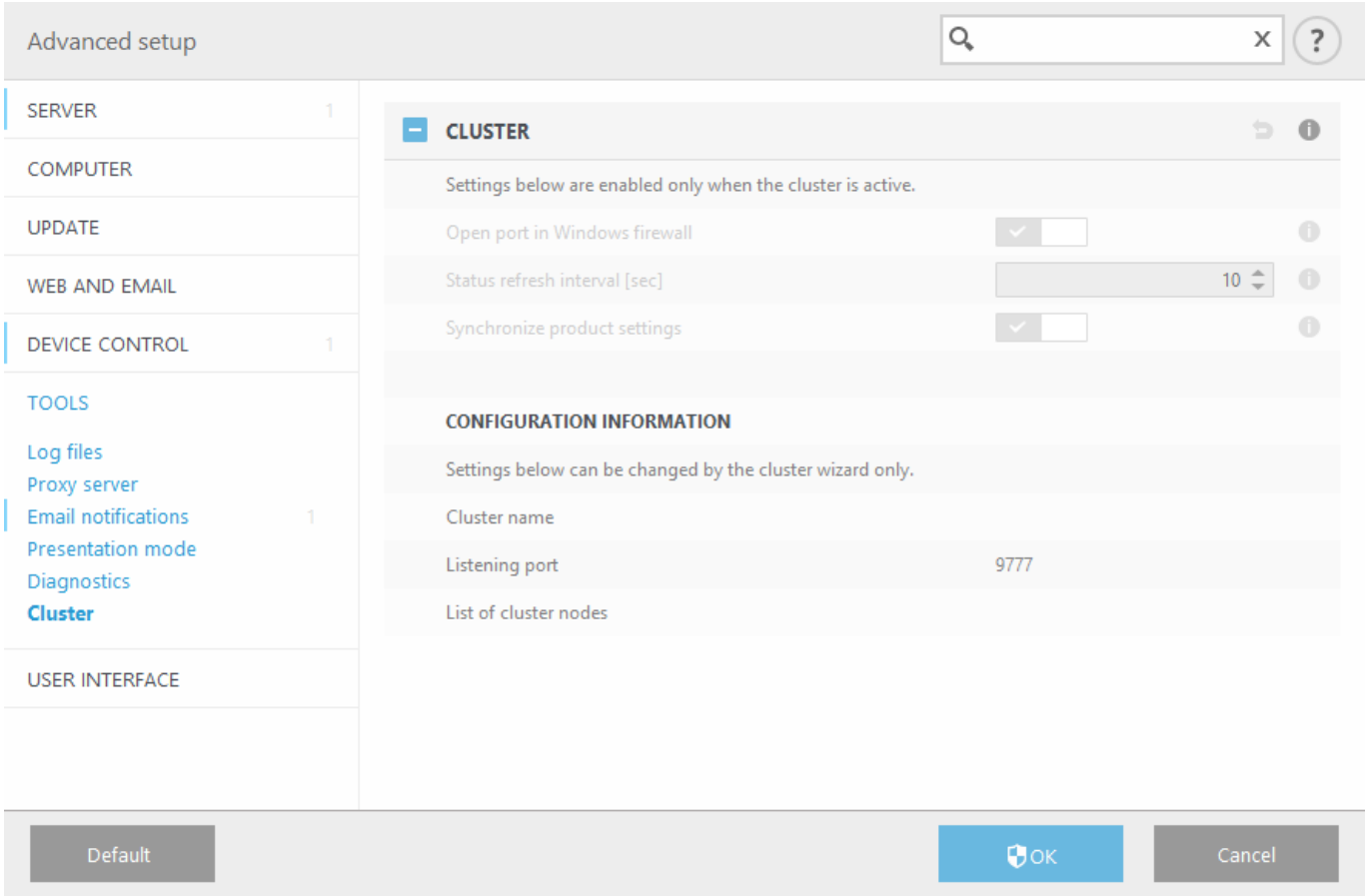
Invia dati configurazione sistema

Selezionare **Invia sempre** per non ricevere una richiesta di conferma prima di inviare i dati di configurazione ESET Server Security al Supporto tecnico oppure utilizzare **Chiedi prima di inviare**.

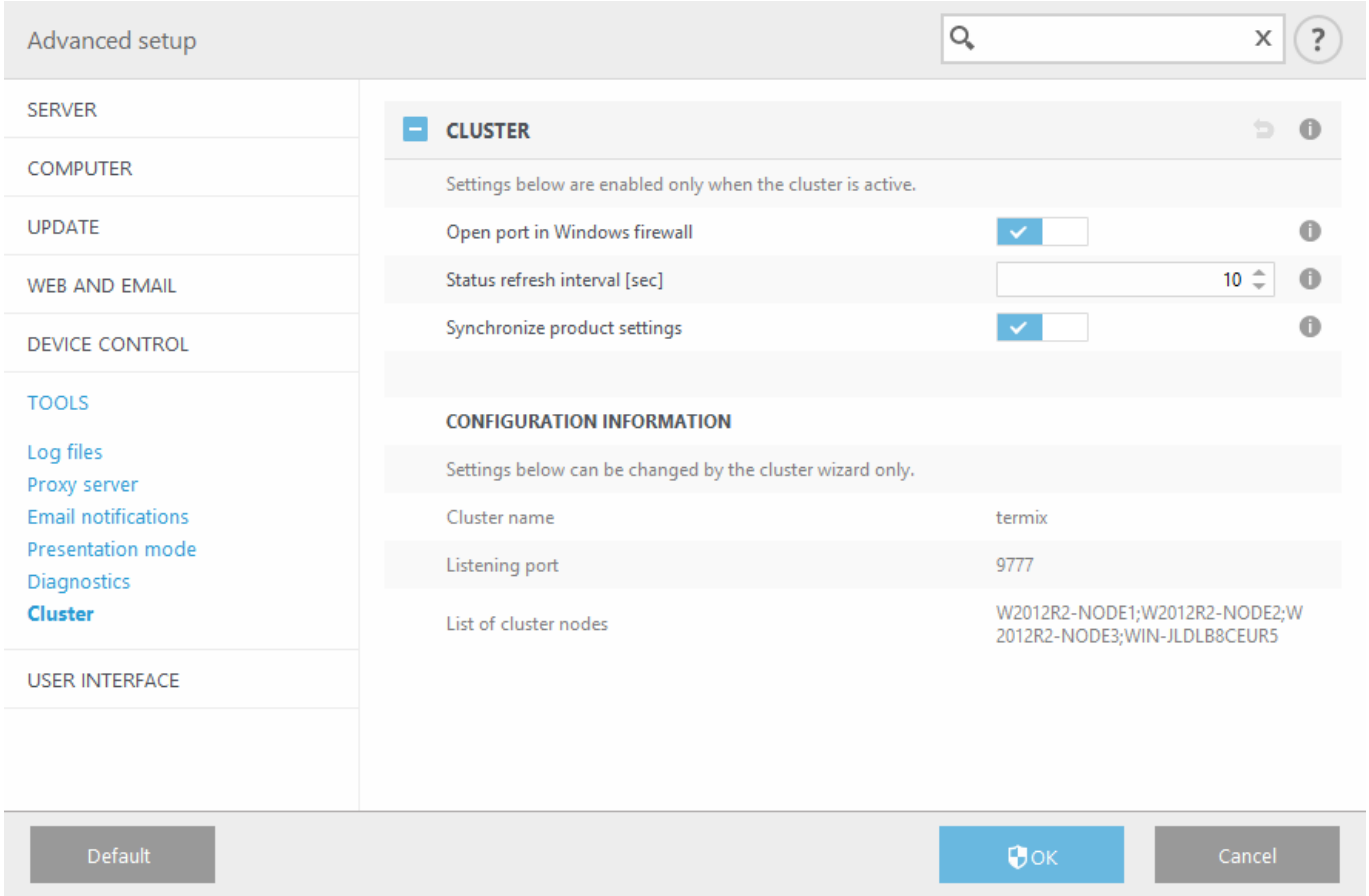
Cluster

Quando ESET Cluster è configurato, la funzione Attiva cluster è attiva automaticamente. È possibile disattivarla manualmente nella finestra **Configurazione avanzata** (F5) facendo clic sull'icona del pulsante (ad esempio quando è necessario modificare la configurazione senza influenzare altri nodi in ESET Cluster). Questo pulsante consente solo di attivare o disattivare le funzionalità di ESET Cluster. Per configurare o eliminare il cluster, utilizzare la Procedura guidata cluster o selezionare l'opzione **Elimina** per eliminare il cluster disponibile nella sezione Strumenti >Cluster della finestra principale del programma.

ESET Cluster non configurato e disattivato:



ESET Cluster correttamente configurato con relativi dettagli e opzioni:



Connettività

Nelle reti LAN di grandi dimensioni la connessione del computer dell'utente a Internet può essere mediata da un server proxy. In questo caso, occorre definire le impostazioni seguenti. Se non si definiscono le impostazioni, il programma non può aggiornarsi automaticamente.

Specificando il server proxy a questo livello, si definiscono le impostazioni globali del server proxy per l'intera applicazione ESET Server Security. Questi parametri saranno utilizzati da tutti i moduli che si connettono a Internet.

Attivare l'interruttore **Utilizza server proxy** e successivamente immettere l'indirizzo del server proxy nel campo **Server proxy** insieme al **Numero di porta** del server proxy.

Il server proxy richiede l'autenticazione

Se la comunicazione di rete tramite il server proxy server richiede l'autenticazione, attivare questa opzione e specificare il **Nome utente** e la **Password**.

Rileva server proxy

Fare clic su **Rileva** per rilevare e inserire automaticamente le impostazioni del server proxy. Verranno copiati i parametri specificati in Internet Explorer.

> Questa funzione non consente di recuperare i dati sull'autenticazione (nome utente e password). Tali informazioni devono quindi essere immesse dall'utente.

Usa la connessione diretta in caso di mancata disponibilità del proxy

Se un prodotto è configurato per utilizzare il proxy HTTP e questo non è raggiungibile, il prodotto disabiliterà il proxy e comunicherà direttamente con i server ESET.

Interfaccia utente

Configurare il comportamento dell'interfaccia utente grafica (GUI) di ESET Server Security. È possibile modificare l'aspetto e gli effetti visivi del programma.

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 utente completa.
- **Terminal**: non verranno visualizzati avvisi o notifiche. L'interfaccia utente grafica può essere avviata solo dall'amministratore. L'interfaccia utente deve essere impostata su Terminal qualora gli elementi grafici rallentino le prestazioni del computer o causino altri problemi. L'utente potrebbe anche decidere di disattivare l'interfaccia utente grafica su un Terminal server. Per ulteriori informazioni su ESET Server Security installato su Terminal Server, consultare l'argomento Disattiva l'interfaccia utente grafica su Terminal Server.

Modalità colore

Selezionare la combinazione di colori dell’interfaccia utente grafica (Graphical User Interface, GUI) di ESET Server Security dal menu a discesa:

- **Uguale al colore del sistema**: la combinazione di colori di ESET Server Security si basa sulle impostazioni del sistema operativo in uso.
- **Scura**: ESET Server Security utilizzerà una combinazione di colori scuri (modalità scura).
- **Chiara**: ESET Server Security utilizzerà una combinazione di colori chiari (standard).

Mostra schermata iniziale all'avvio

Disabilitare questa opzione se si preferisce non visualizzare la schermata iniziale all’avvio della finestra principale del programma di ESET Server Security, ad esempio quando si esegue l’autenticazione al sistema.

Utilizza segnale audio

ESET Server Security emette un segnale acustico al verificarsi di eventi importanti durante un controllo, ad esempio in caso di rilevamento di una minaccia o al termine del controllo.

Integra nel menu contestuale

In caso di abilitazione, gli elementi di controllo di ESET Server Security sono integrati nel 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.

Informazioni sulla licenza

In caso di attivazione, verranno visualizzati i messaggi e le notifiche sulla licenza.

Mostra informazioni sulla licenza

In caso di disabilitazione, la data di scadenza della licenza nella schermata **Stato protezione** e **Guida e supporto tecnico** non verrà visualizzata.

Configura gli stati dell'applicazione correlata alla licenza

Consente di aprire l'elenco di stati dell'applicazione correlati alla licenza.

Configura notifiche licenza

In caso di disabilitazione, le notifiche e i messaggi verranno visualizzati solo alla scadenza della licenza.

Configurazione dell'accesso

È possibile prevenire modifiche non autorizzate utilizzando lo strumento **Configurazione dell'accesso** per garantire il mantenimento di un livello di protezione elevato.

ESET Shell

Modificando il Criterio di esecuzione ESET Shell, è possibile configurare i diritti di accesso alle impostazioni, alle funzioni e ai dati del prodotto mediante eShell.

Icona nell'area di notifica di Windows

Ripristina tutte le impostazioni in questa sezione

Configurazione dell'accesso

Per garantire un livello di protezione massimo del sistema, è fondamentale che ESET Server Security sia configurato correttamente. Qualsiasi modifica non appropriata potrebbe causare problemi o la perdita di dati importanti. Per evitare modifiche non autorizzate, i parametri di configurazione di ESET Server Security possono essere protetti con password.

> Se si disinstalla ESET Server Security mentre è in uso la protezione con password per la configurazione degli accessi, all'utente verrà chiesto di immettere la password. In caso contrario, non sarà possibile disinstallare ESET Server Security.

Impostazioni protezione con password

Blocca/sblocca i parametri di impostazione del programma. Fare clic per aprire la finestra **Configurazione password**.

Imposta password

Per impostare o modificare una password per proteggere i parametri di configurazione, fare clic su **Imposta**. Per proteggere i parametri di configurazione di ESET Server Security al fine di evitare una modifica non autorizzata, è necessario impostare una nuova password. Se si desidera modificare una password esistente, è necessario digitare la vecchia password nel campo **Vecchia password**, inserire la nuova nel campo **Nuova password**, selezionare **Conferma password** e fare clic su **OK**. La password verrà richiesta per apportare future modifiche a ESET Server Security.

Richiedi diritti di amministratore completi per gli account amministratore con diritti limitati

Selezionare questa opzione per richiedere all'utente corrente (nel caso in cui non disponga di diritti di amministratore) di immettere le credenziali dell'account amministratore per la modifica di alcuni parametri, ad esempio la disattivazione dei moduli di protezione.

> Se la password della configurazione dell'accesso viene modificata e si desidera importare un file di configurazione .xml esistente (che è stato firmato prima della modifica della password) utilizzando la riga di comando ESET CMD, assicurarsi di firmarlo nuovamente utilizzando la password corrente. Ciò consente all'utente di utilizzare un file di configurazione precedente senza la necessità di esportarlo su un'altra macchina su cui è in esecuzione ESET Server Security prima dell'importazione.

ESET Shell

Modificando il **Criterio di esecuzione ESET Shell**, è possibile configurare i diritti di accesso alle impostazioni, alle funzioni e ai dati del prodotto mediante eShell. L'impostazione predefinita è **Scripting limitato**. Tuttavia, se necessario, è possibile modificarla scegliendo tra Disattivato, Di sola lettura o Accesso completo.

Disattivato

eShell non può essere assolutamente utilizzato. È consentita solo la configurazione di eShell stesso nel contesto ui eshell. È possibile personalizzare l'aspetto di eShell ma non accedere alle impostazioni o ai dati del prodotto.

Di sola lettura

eShell può essere utilizzato come strumento di monitoraggio. È possibile visualizzare tutte le impostazioni sia in modalità interattiva sia in modalità batch, ma non modificare le impostazioni, le funzioni o i dati.

Scripting limitato

Nella Modalità interattiva, è possibile visualizzare e modificare tutte le impostazioni, le funzioni e i dati. In modalità batch, eShell funzionerà come in modalità di sola lettura. Tuttavia, in caso di utilizzo di file batch firmati, l'utente potrà modificare le impostazioni e i dati.

Accesso completo

Accesso illimitato a tutte le impostazioni sia in modalità interattiva sia in modalità batch (in caso di esecuzione di file batch). È possibile visualizzare e modificare qualsiasi impostazione. Per eseguire eShell in modalità accesso completo, è necessario utilizzare un account amministratore. In caso di attivazione del Controllo dell'account utente (UAC), è richiesta anche l'elevazione.

Disattiva l'interfaccia utente grafica su Terminal Server

In questo capitolo viene illustrato come disattivare l'interfaccia utente grafica (Graphical User Interface, GUI) di ESET Server Security in esecuzione su Windows Terminal Server per le sessioni utente.

In genere l'interfaccia utente grafica (GUI) di ESET Server Security viene avviata ogni volta che un utente remoto accede al server e crea una sessione terminal. Ciò non è di norma auspicabile sui Terminal Server. Per disattivare l'interfaccia utente grafica per le sessioni terminal, utilizzare eShell eseguendo il comando `set ui ui gui-start-mode none`. Questa operazione imposterà l'interfaccia utente grafica in modalità terminal. Le due

modalità disponibili per l'avvio dell'interfaccia utente grafica sono:

```
set ui ui gui-start-mode full
```

```
set ui ui gui-start-mode none
```

Per scoprire la modalità attualmente in uso, eseguire il comando `get ui ui gui-start-mode`.

> In caso di installazione di ESET Server Security su un server Citrix, si consiglia di utilizzare le impostazioni descritte in questo articolo della Knowledge Base .

Icona nell'area di notifica di Windows

Le principali opzioni di configurazione e funzioni sono disponibili facendo clic con il pulsante destro del mouse sull'icona della barra delle applicazioni (area delle notifiche di Windows) .

> Per accedere all'area di notifica di Windows, assicurarsi che la modalità di avvio degli Elementi dell'interfaccia utente sia impostata su "Completa".

Ulteriori informazioni

Consente all'utente di aprire la pagina Monitoraggio per visualizzare lo stato corrente della protezione e i messaggi.

Sospendi protezione

Consente di visualizzare il riquadro della finestra di dialogo di conferma del prodotto per disabilitare la Protezione antivirus e antispyware che protegge da attacchi controllando file e comunicazioni web e e-mail. Il menu a discesa **Intervallo di tempo** consente all'utente di specificare l'intervallo di tempo durante il quale la protezione verrà disabilitata.

Configurazione avanzata

Consente di aprire la Configurazione avanzata di ESET Server Security.

File di rapporto

Contiene informazioni relative a tutti gli eventi di programma importanti che si sono verificati e fornisce una panoramica delle minacce rilevate.

Ripristina layout finestra

Ripristina le dimensioni predefinite e la posizione sullo schermo della finestra di ESET Server Security.

Modalità colore

Consente di aprire le impostazioni dell'interfaccia utente in cui è possibile modificare il colore dell'interfaccia utente grafica.

Ricerca aggiornamenti

Avvia l'aggiornamento dei moduli per garantire il livello di protezione stabilito dall'utente contro codice dannoso.

Informazioni su

Fornisce informazioni sul sistema, dettagli sulla versione installata di ESET Server 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.

Notifiche

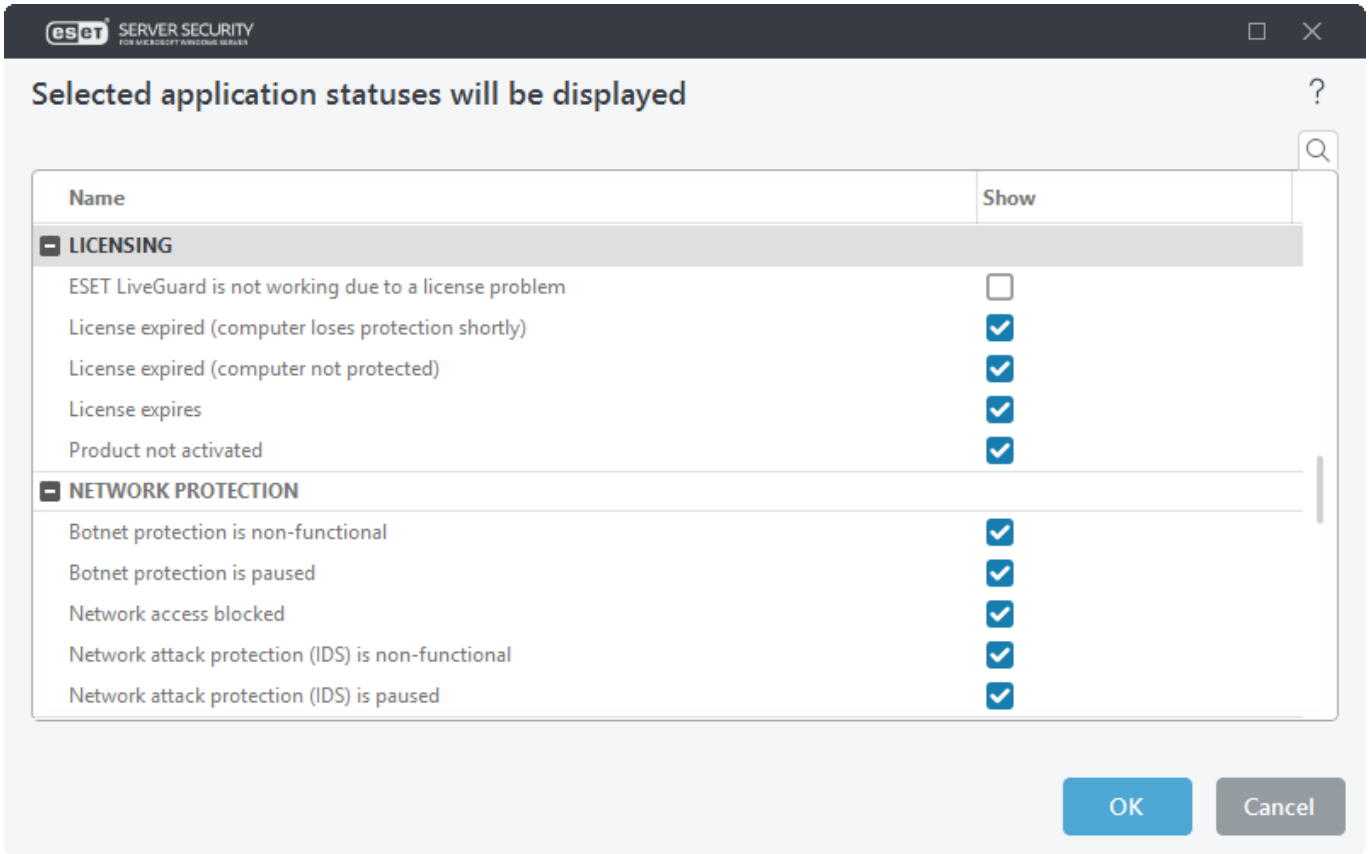
Le notifiche visualizzate sul desktop e i suggerimenti sono forniti esclusivamente a titolo informativo e non richiedono l'interazione dell'utente. Vengono visualizzate nell'area di notifica posta nell'angolo in basso a destra della schermata. È possibile modificare opzioni più dettagliate, ad esempio l'orario di visualizzazione della notifica e la trasparenza della finestra seguendo le istruzioni fornite di seguito.

Gestire le notifiche di ESET Server Security, aprire la **Configurazione avanzata** (**F5**) > **Notifiche**. È possibile configurare i seguenti tipi:

- Stati dell'applicazione: fare clic su Modifica per selezionare gli stati dell'applicazione che saranno visualizzati nella sezione "Home" della finestra principale del programma.
- Notifiche desktop: piccole finestre a comparsa accanto alla barra delle applicazioni del sistema.
- Avvisi interattivi: finestre di avviso e finestre di messaggio che richiedono l'interazione dell'utente.
- Inoltro (notifiche tramite e-mail): le notifiche vengono inviate a un indirizzo e-mail specificato.

Stati dell'applicazione

In questa finestra di dialogo è possibile selezionare o deselezionare gli stati dell'applicazione che verranno visualizzati e quelli che non verranno visualizzati. Ad esempio, la sospensione della protezione antivirus e antispyware determinerà una modifica dello stato di protezione che comparirà nella pagina Monitoraggio. Lo stato di un'applicazione sarà visualizzato anche se il prodotto non è attivato o se la licenza è scaduta. Gli stati dell'applicazione possono essere gestiti mediante i criteri ESET PROTECT.



Messaggi e stati disattivati

Messaggi di conferma

Consente all'utente di visualizzare un elenco di messaggi di conferma che è possibile decidere di visualizzare o meno.

Stati dell'applicazione

Abilitare o disabilitare lo stato di visualizzazione nella pagina Monitoraggio del menu principale.

Notifiche desktop

La notifica desktop è rappresentata da una piccola finestra di notifica accanto alla barra delle applicazioni del sistema. Per impostazione predefinita viene mostrata per 10 secondi, per poi scomparire lentamente. ESET Server Security comunica con l'utente inviando una notifica sugli aggiornamenti del prodotto eseguiti correttamente, sui nuovi dispositivi connessi, sui controlli antivirus, sul completamento delle attività o sui nuovi rilevamenti trovati.

Visualizza notifiche desktop

Si consiglia di mantenere questa opzione abilitata in modo che il prodotto informi l'utente quando si verifica un nuovo evento.

Notifiche desktop

Fare clic su **Modifica** per selezionare le Notifiche desktop per la comunicazione dei vari eventi.

Attivare l’opzione **Non visualizzare le notifiche quando vengono eseguite applicazioni in modalità a schermo intero** per eliminare tutte le notifiche non interattive.

Visualizza tempo in secondi

Impostare la durata della visibilità della notifica. Il valore deve essere compreso tra 3 e 30 secondi.

Trasparenza

Impostare la percentuale di trasparenza della notifica. L’intervallo supportato è compreso tra 0 (nessuna trasparenza) e 80 (trasparenza molto elevata).

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. Sono disponibili le seguenti opzioni:

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

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.

Consenti l’attivazione delle notifiche sullo schermo: le notifiche saranno attive sullo schermo e accessibili mediante la combinazione di tasti Alt+Tab.

Personalizzazione

In questa finestra è possibile personalizzare il servizio di messaggistica utilizzato nelle notifiche.

Messaggio di notifica – Messaggio predefinito che verrà visualizzato nel piè di pagina delle notifiche.

Rilevamento

Non chiudere automaticamente le notifiche di rilevamento

Consente la visualizzazione delle notifiche rilevamento sullo schermo fino a quando non vengono chiuse manualmente dall’utente.

Usa messaggio predefinito

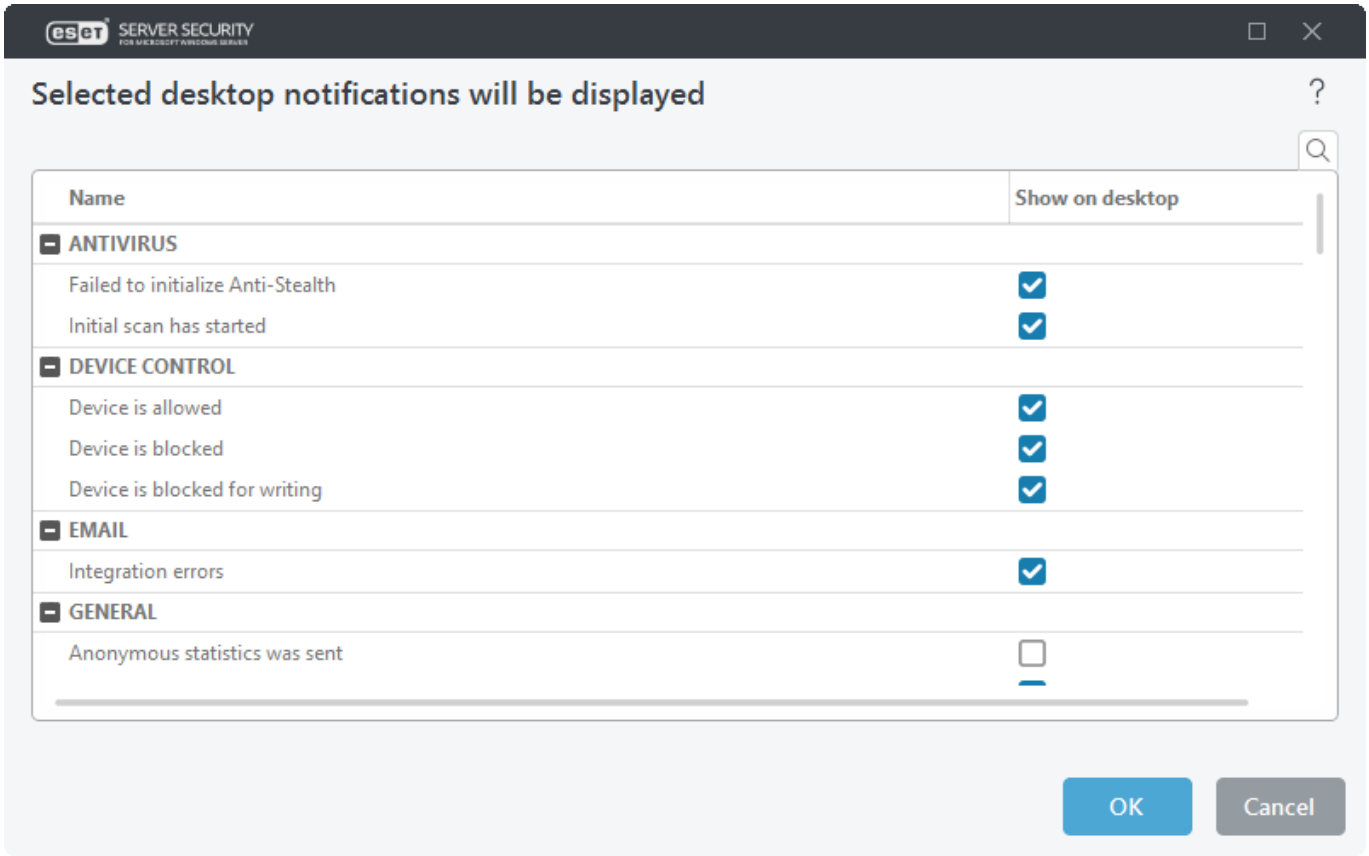
È possibile disattivare il messaggio predefinito e specificare il messaggio di notifica sui rilevamenti personalizzato che verrà visualizzato in caso di blocco di un rilevamento.

Messaggio notifica rilevamento

Inserire un messaggio personalizzato da visualizzare nel momento in cui un rilevamento viene bloccato.

Notifiche desktop

È possibile configurare le notifiche di ESET Server Security da visualizzare sul desktop.



Avvisi interattivi

È possibile configurare le modalità di gestione dei messaggi di avviso relativi alle minacce e delle notifiche di sistema (p. es. messaggi di aggiornamenti eseguiti correttamente) da parte di ESET Server Security. Ad esempio, la **Durata** e la **Trasparenza** dell'ora di visualizzazione nell'area di notifica di Windows (applicabile solo ai sistemi che supportano le notifiche).

Visualizza avvisi interattivi

Disabilitare questa funzione se si desidera impedire a ESET Server Security di mostrare avvisi nell'area delle notifiche di Windows.

Elenco di avvisi interattivi

Utile per l'automazione. Deselezionare **Chiedi all'utente** per le voci che si desidera automatizzare e scegliere l'azione che verrà intrapresa al posto della finestra di avviso in attesa di interazione.

Le finestre di messaggio vengono utilizzate per visualizzare brevi messaggi di testo o domande.

Chiudi automaticamente finestre di messaggio

Questa opzione consente di chiudere automaticamente le finestre di notifica dopo un determinato periodo di tempo. Se non viene eseguita manualmente, la chiusura delle finestre di avviso avviene automaticamente una volta trascorso il periodo di tempo specificato.

Messaggi di conferma

Se l'utente fa clic su **Modifica**, verrà visualizzata una finestra popup contenente un elenco dei messaggi di conferma visualizzati da ESET Server Security prima che venga eseguita un'azione. Utilizzare le caselle di controllo per personalizzare le preferenze dei messaggi di conferma.

Riavvio necessario

È necessario riavviare il computer dopo il passaggio di app di terze parti alla nuova versione o l'applicazione di patch tramite la funzione Gestione delle vulnerabilità e delle patch.

> Potrebbe essere necessario chiudere alcune app di terze parti prima dell'aggiornamento. In questo caso, verrà visualizzata una notifica per 60 secondi prima che l'app e i processi in background in esecuzione vengano interrotti. È possibile pianificare l'aggiornamento o l'applicazione di patch di conseguenza, poiché le app di terze parti non saranno disponibili per l'intera durata dell'aggiornamento.

Inoltro

ESET Server Security invia automaticamente e-mail di notifica nel caso in cui si verifichi un evento con il livello di dettaglio selezionato.

Inoltra all'e-mail

Abilitare "Inoltra notifiche all'e-mail" per attivare le notifiche tramite e-mail.

Notifiche inoltrate

Selezionare le notifiche desktop da inoltrare all'e-mail.

Impostazioni e-mail

Livello di dettaglio minimo per le notifiche: specifica il livello di dettaglio minimo delle notifiche da inviare.

- **Diagnostico**: consente di registrare le informazioni necessarie ai fini dell'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativo**: consente di registrare i messaggi informativi, compresi quelli correlati a eventi di rete non standard, tra cui messaggi di aggiornamenti riusciti, e tutti i record indicati in precedenza.
- **Avvisi**: consente di registrare messaggi di errori critici e di allarme (la funzione Anti-Stealth non funziona correttamente o l'aggiornamento non è riuscito).
- **Errori**: verranno registrati errori quali "Errore durante il download del file" ed errori critici.

- **Critico**: registra solo gli errori critici.

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.

Intervallo in seguito al quale verranno inviate nuove e-mail di notifica (min.)

Intervallo in minuti in seguito al quale verrà inviata una nuova notifica tramite e-mail. Impostare il valore su 0 se si desidera inviare immediatamente queste notifiche.

Indirizzo mittente

Inserire l'indirizzo del mittente che comparirà nell'intestazione delle e-mail di notifica. Questo è ciò che il destinatario visualizzerà nel campo **Da**.

Indirizzo destinatario

Specificare l'indirizzo e-mail del destinatario che verrà visualizzato nell'intestazione delle e-mail di notifica. Utilizzare un punto e virgola ";" per separare indirizzi e-mail multipli.

Server SMTP

Nome del server SMTP utilizzato per l'invio di avvisi e notifiche. Si tratta tipicamente del nome di Microsoft Exchange Server.

ESET Server 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 password validi per l'accesso al server SMTP.

Attiva TLS

Attiva messaggi di avviso e notifiche supportati dalla crittografia TLS.

Connessione di prova SMTP

Verrà inviata un'e-mail di prova all'indirizzo e-mail del destinatario.

Formato del messaggio

Le comunicazioni tra il programma e un utente remoto o un amministratore di sistema avvengono tramite e-mail o messaggi LAN (utilizzando il servizio Messenger di Windows). I messaggi di avviso predefiniti e il formato delle notifiche saranno ottimali per la maggior parte delle situazioni. In alcune circostanze, potrebbe essere necessario modificare il formato dei messaggi di evento.

Formato dei messaggi di evento

Specificare il formato dei messaggi di notifica degli eventi di posta elettronica.

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.

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

- %TimeStamp%: data e ora dell'evento.
- %Scanner%: modulo interessato.
- %ComputerName%: nome del computer sul quale è stato visualizzato l'avviso.
- %ProgramName%: programma che ha generato l'avviso.
- %DetectionObject%: nome del file, del messaggio, ecc. infetto.
- %DetectionName%: identificazione dell'infezione.
- %ErrorDescription%: descrizione di un evento non correlato a virus.

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

Set di caratteri

È possibile scegliere la codifica dal menu a discesa. Il messaggio e-mail sarà convertito in base alla codifica di caratteri selezionata. Consente di convertire un messaggio e-mail nella codifica dei caratteri ANSI in base alle impostazioni regionali di Windows (ad esempio, windows-1250, Unicode (UTF-8), ACSII 7-bit o Japanese (ISO-2022-JP)). Di conseguenza, la lettera "á" verrà modificata in "a" e un simbolo sconosciuto verrà modificato in "?".

Usa codifica Quoted-printable

L'origine del messaggio di posta elettronica 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).

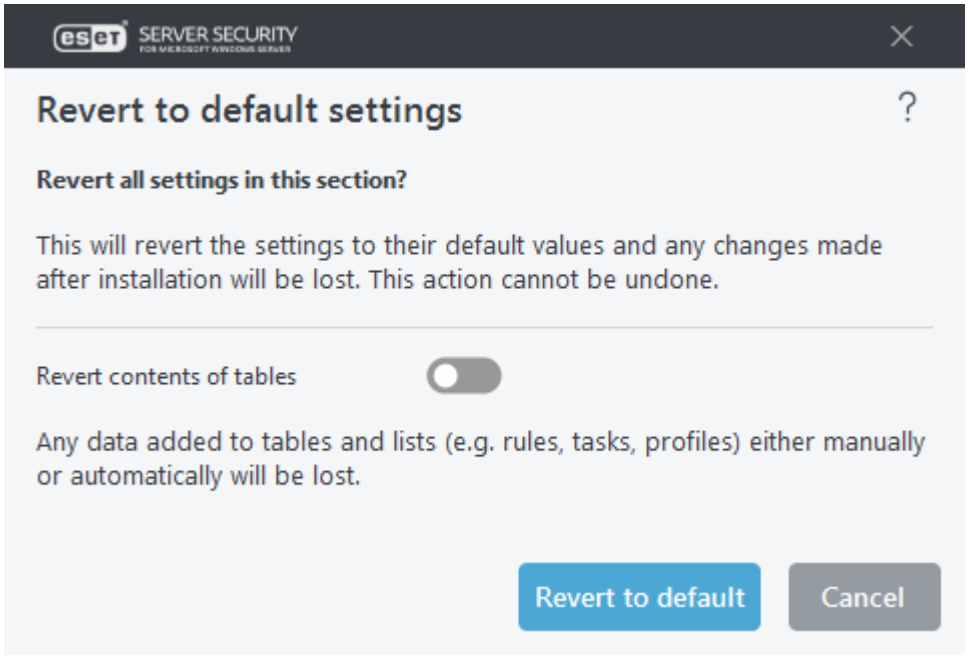
Ripristina impostazioni predefinite

È possibile ripristinare le impostazioni predefinite all'interno di **Configurazione avanzata**. Sono disponibili due opzioni. È possibile ripristinare tutte le impostazioni predefinite oppure ripristinare le impostazioni solo per una sezione specifica (le impostazioni delle altre sezioni rimarranno invariate).

Ripristina tutte le impostazioni – Tutte le impostazioni in tutte le sezioni della configurazione avanzata verranno ripristinate nello stato in cui si trovavano dopo aver installato ESET Server Security. È una sorta di Ripristino impostazioni predefinite.

> i Quando si seleziona **Ripristina impostazioni predefinite**, tutte le modifiche apportate andranno perse. L'operazione non potrà essere annullata.

Ripristina tutte le impostazioni in questa sezione: consente di ripristinare i valori predefiniti delle impostazioni del modulo nella sezione selezionata. Tutte le eventuali modifiche apportate in questa sezione andranno perse.



Ripristina contenuti tabelle – Attivando questa opzione, le regole, le attività o i profili aggiunti manualmente o automaticamente andranno persi.

Guida e supporto tecnico

ESET Server Security contiene strumenti di individuazione e risoluzione dei problemi e informazioni di supporto in grado di assistere l'utente nella risoluzione di eventuali problemi che potrebbero insorgere.

Prodotto installato

Informazioni sul prodotto e sulla licenza

- Informazioni su ESET Server Security: consente di visualizzare le informazioni sulla copia di ESET Server Security.
- Risoluzione dei problemi relativi al prodotto – Selezionare questa opzione per trovare le soluzioni ai problemi riscontrati con maggiore frequenza. Si consiglia di leggere questa sezione prima di contattare il Supporto tecnico.
- Risoluzione dei problemi relativi alla licenza: consente di trovare le soluzioni ai problemi relativi all’attivazione o alla modifica della licenza.
- Modifica licenza: fare clic per avviare la finestra di attivazione e attivare il prodotto.

Pagine della guida

Consente all’utente di visualizzare le pagine della guida on-line di ESET Server Security.

Knowledge Base

Cerca nella Knowledge Base ESET: la Knowledge Base ESET contiene le risposte alle domande frequenti, nonché le

soluzioni consigliate per i vari problemi. Grazie all'aggiornamento periodico effettuato dagli esperti del supporto tecnico di ESET, la Knowledge Base rappresenta lo strumento più potente per risolvere diversi tipi di problemi.

Supporto tecnico

- Registrazione avanzata – Crea rapporti avanzati per tutte le funzioni disponibili per aiutare gli sviluppatori a diagnosticare e risolvere i problemi.

- Richiedi assistenza: se non è possibile trovare una risposta al problema, contattare il reparto del Supporto tecnico.

- Informazioni per il Supporto tecnico – Consente di visualizzare le informazioni dettagliate (nome prodotto, versione prodotto, e così via) per il Supporto tecnico.

- ESET Log Collector – ESET Log Collector è un'applicazione che raccoglie automaticamente informazioni, come i dati sulle configurazioni e i rapporti dal server allo scopo di garantire una più rapida risoluzione dei problemi.

Invia richiesta di assistenza

Per offrire un servizio di assistenza il più rapido e accurato possibile, ESET richiede informazioni sulla configurazione di ESET Server Security, informazioni dettagliate sul sistema, i processi in esecuzione (File di rapporto ESET SysInspector) e i dati di registro. ESET utilizzerà questi dati esclusivamente per offrire assistenza tecnica ai propri clienti. Questa impostazione può essere configurata anche in **Configurazione avanzata** (**F5**) > **Strumenti** > **Diagnostica** > **Supporto tecnico**.

> Se si decide di inviare i dati del sistema, è necessario compilare e inviare il modulo Web. La mancata osservanza di tale istruzione impedirà la creazione della richiesta di assistenza causando la perdita dei dati del sistema.

In caso di invio del modulo Web, i dati relativi alla configurazione del sistema verranno inviati a ESET. Selezionare **Invia sempre queste informazioni** per ricordare questa azione per il processo.

Non inviare i dati: Usare questa opzione se non si desidera inviare i dati. SI verrà reindirizzati alla pagina Web del Supporto tecnico ESET.

Informazioni su ESET Server Security

Questa finestra fornisce dettagli relativi alla versione installata di ESET Server Security. La parte superiore della finestra contiene informazioni sul sistema operativo e sulle risorse di sistema, sull'utente corrente e sul nome del computer completo.

Componenti installati

Contiene informazioni sui moduli. Fare clic su Componenti installati per visualizzare un elenco dei componenti installati e dei relativi dettagli. Fare clic su **Copia** per copiare l'elenco negli Appunti. Tali informazioni potrebbero essere utili per la risoluzione dei problemi o per contattare il Supporto tecnico.

Glossario

Per ulteriori informazioni sui termini tecnici, le minacce e la sicurezza su Internet, consultare il Glossario.

Documenti legali

Quella che segue è una raccolta di documenti legali:

Accordo di licenza per l'utente finale

Informativa sulla privacy

Accordo di licenza per l'utente finale

Con decorrenza a partire dal 19 ottobre 2021.

IMPORTANTE: Leggere attentamente i termini e le condizioni delineati di seguito prima di scaricare, installare, duplicare o utilizzare il prodotto. **SCARICANDO, INSTALLANDO, DUPLICANDO O UTILIZZANDO IL SOFTWARE, L'UTENTE SI IMPEGNA AD ACCETTARE I TERMINI E LE CONDIZIONI DEL PRESENTE CONTRATTO E DELL'INFORMATIVA SULLA PRIVACY.**

Accordo di licenza per l'utente finale

Ai sensi del presente Accordo di licenza per l'utente finale ("Accordo"), stipulato da e tra ESET, spol. s r. o., con sede legale presso Einsteinova 24, 85101 Bratislava, Slovak Republic, iscritta nel registro delle imprese di competenza del tribunale circoscrizionale Bratislava I, Sezione Sro, numero di registro 3586/B, numero di identificazione commerciale 31333532 ("ESET" o "il Fornitore") e l'utente, persona fisica o giuridica ("l'Utente" o "l'Utente finale") autorizzano l'Utente a utilizzare il Software specificato nell'Articolo 1 del presente Contratto. Il Software specificato nell'Articolo 1 del presente Accordo può essere memorizzato su un supporto informatico, inviato tramite posta elettronica, scaricato da Internet, scaricato dai server del Fornitore od ottenuto da altre fonti secondo i termini e le condizioni specificati di seguito.

IL PRESENTE CONTRATTO HA PER OGGETTO I DIRITTI DELL'UTENTE FINALE E NON COSTITUISCE UN CONTRATTO DI VENDITA. Il Fornitore conserva la proprietà della copia del Software e dei supporti fisici contenuti nella confezione di vendita, nonché di ogni altra copia che l'Utente finale è autorizzato a effettuare in conformità al presente Contratto.

Facendo clic su "Accetto" o "Accetto..." durante l'installazione, il download, la copia o l'utilizzo del Software, l'Utente accetta i termini e le condizioni del presente Accordo e dell'Informativa sulla privacy. Qualora non intenda accettare integralmente i termini e le condizioni del presente Accordo e/o dell'Informativa sulla privacy, l'Utente dovrà prontamente fare clic sull'opzione di annullamento, interrompere l'installazione o il download oppure eliminare o restituire il Software, i supporti di installazione, la documentazione di accompagnamento e la prova di acquisto al Fornitore o presso il punto vendita in cui l'Utente ha acquistato il Software.

L'UTENTE CONVIENE CHE IL SUO UTILIZZO DEL SOFTWARE COSTITUISCE CONFERMA DELL'AVVENUTA LETTURA, COMPRENSIONE E ACCETTAZIONE DEL PRESENTE CONTRATTO E ACCETTA DI RISPETTARE I TERMINI E LE CONDIZIONI INDICATI.

1. **Software.** Ai sensi del presente Accordo, il termine "Software" indica: (i) il programma accompagnato dal

presente Accordo e tutti i suoi componenti; (ii) tutti i contenuti dei dischi, CD-ROM, DVD, e-mail ed eventuali allegati o altri supporti medianti i quali viene fornito il presente Contratto, compreso il formato del codice oggetto del Software fornito su un supporto informativo, tramite posta elettronica o scaricato da Internet; (iii) qualsiasi materiale cartaceo illustrativo correlato e qualsiasi altra possibile documentazione correlata al Software, soprattutto qualsiasi descrizione del Software, relative specifiche, qualsiasi descrizione delle proprietà o del funzionamento del Software, qualsiasi descrizione dell'ambiente operativo in cui il Software viene utilizzato, istruzioni di utilizzo o installazione del Software o qualsiasi descrizione delle modalità di utilizzo del Software ("Documentazione"); (iv) copie del Software, correzioni di possibili errori nel Software, aggiunte al Software, estensioni al Software, versioni modificate del Software ed eventuali aggiornamenti dei componenti del Software, concesso in licenza all'Utente dal Fornitore ai sensi dell'Articolo 3 del presente Contratto. Il Software deve essere fornito esclusivamente sotto forma di codice oggetto eseguibile.

2. **Installazione, Computer e Chiave di licenza**. Il Software fornito su un supporto informatico, inviato tramite posta elettronica, scaricato da Internet o dai server del Fornitore od ottenuto da altre fonti richiede una procedura di installazione. L'Utente finale è tenuto a installare il Software su un Computer correttamente configurato, conformemente ai requisiti minimi specificati nella Documentazione fornita. Il metodo di installazione è illustrato nella Documentazione. È vietato installare programmi per computer o componenti hardware che possano influire negativamente sul Software sullo stesso Computer su cui si installa il Software medesimo. Per Computer si intende qualsiasi componente hardware, compresi, a mero titolo esemplificativo e non limitativo, personal computer, computer portatili, workstation, computer palmari, smartphone, dispositivi elettronici portatili o altri dispositivi elettronici per i quali è stato concepito il Software e sui quali sarà installato e/o utilizzato. Per Chiave di licenza si intende una sequenza univoca di simboli, lettere, numeri o segni speciali forniti all’Utente finale per consentire un utilizzo legale del Software, la sua versione specifica o l’estensione della durata della Licenza in conformità del presente Accordo.

3. **Licenza**. Subordinatamente alla condizione che l'Utente abbia accettato i termini del presente Contratto e rispettato tutti i termini e le condizioni qui indicati, il Fornitore deve garantire all'Utente i seguenti diritti ("la Licenza"):

a) **Installazione e utilizzo.** L'Utente deve avere il diritto non esclusivo e non trasferibile che consente l'installazione del Software sul disco rigido di un computer o su altri supporti permanenti per la memorizzazione dei dati, l'installazione e la memorizzazione del Software sulla memoria di un computer e di implementare, memorizzare e visualizzare il Software.

b) **Indicazione del numero di licenze.** Il diritto di utilizzo del Software deve essere legato al numero di Utenti finali. Quanto segue fa riferimento a un Utente finale: (i) installazione del Software su un computer, o (ii) se una licenza è legata al numero di caselle di posta, un Utente finale corrisponderà a un utente che accetta la posta elettronica tramite un Mail User Agent ("MUA"). Se un MUA accetta la posta elettronica e successivamente la distribuisce automaticamente a diversi utenti, il numero di Utenti finali sarà determinato in base al numero effettivo di utenti a cui viene distribuita la posta elettronica. Se un server di posta svolge la funzione di Mailgate, il numero di Utenti finali dovrà essere pari al numero di utenti del server di posta per cui tale gate fornisce i servizi. Se un numero non specificato di indirizzi di posta elettronica è diretto a e accettato da un utente (ad es., inclusi gli alias) e i messaggi non sono automaticamente distribuiti dal client a un numero maggiore di utenti, è richiesta una Licenza per un computer soltanto. L'Utente non deve utilizzare la stessa Licenza contemporaneamente su più di un computer. L’Utente finale ha facoltà di inserire la Chiave di licenza del Software unicamente nella misura in cui sia autorizzato a utilizzare il Software in conformità delle limitazioni derivanti dal numero di Licenze fornite dal Fornitore. La Chiave di licenza è considerata un contenuto riservato che non dovrà essere condiviso con terzi o utilizzato da terzi salvo quanto consentito dal presente Accordo o dal Fornitore. In caso di compromissione della Chiave di licenza, è necessario darne immediata comunicazione al Fornitore.

c) **Home/Business Edition.** Il diritto di utilizzo della versione Home Edition del Software sarà limitato esclusivamente ad ambienti privati e/o non commerciali per scopi domestici e familiari. Ai fini dell’utilizzo del

Software in ambienti commerciali nonché su server di posta, mail relay, gateway di posta o gateway Internet, occorre procurarsi una versione Business Edition.

d) **Termine della Licenza.** Il diritto di utilizzo del Software deve essere limitato nel tempo.

e) **Software OEM.** L'utilizzo di software classificati come "OEM" sarà limitato al Computer con il quale sono stati ottenuti. Non è possibile trasferirlo su un computer diverso.

f) **Software di valutazione o di prova.** Non è possibile vendere il software classificato come "Not-for-resale" (versione di valutazione), NFR o TRIAL e deve essere utilizzato esclusivamente ai fini della verifica e della valutazione delle funzioni del Software.

g) **Risoluzione della Licenza.** La Licenza deve scadere automaticamente al termine del periodo stabilito. In caso di mancato rispetto di qualsiasi clausola del presente Contratto, il Fornitore è autorizzato a recedere dal Contratto, senza pregiudizio per i diritti o i rimedi legali disponibili al Fornitore in tali eventualità. In caso di annullamento della Licenza, l'Utente è tenuto a cancellare, distruggere o restituire immediatamente, a proprie spese, A fronte della risoluzione della Licenza, il Fornitore avrà facoltà di annullare il diritto dell'Utente finale di utilizzare le funzioni del Software, che richiedono la connessione ai server del Fornitore o a server di terzi.

4. **Funzioni che prevedono requisiti di raccolta di dati e di connessione a Internet.** Ai fini di un corretto funzionamento, il Software richiede una connessione a Internet, deve essere collegato a intervalli regolari ai server del Fornitore o di terzi e conforme ai requisiti applicabili in materia di raccolta di dati previsti dalla Politica sulla privacy. La connessione a Internet e la raccolta di dati sono requisiti necessari per le seguenti funzioni del Software:

a) **Aggiornamenti del Software.** Il Fornitore è autorizzato a rilasciare di tanto in tanto aggiornamenti o upgrade del Software ("Aggiornamenti") ma non è tenuto a fornirli. Questa funzione è abilitata nelle impostazioni standard del Software e gli Aggiornamenti vengono pertanto installati automaticamente, eccetto se l'Utente finale ha disabilitato l'installazione automatica degli Aggiornamenti. Ai fini del rilascio degli Aggiornamenti, è richiesta una verifica dell'autenticità della Licenza, comprese le informazioni sul Computer e/o sulla piattaforma di installazione del Software ai sensi dell'Informativa sulla privacy.

Il rilascio di eventuali Aggiornamenti potrebbe essere soggetto al Criterio di fine del ciclo di vita ("Criterio EOL"), disponibile alla pagina https://go.eset.com/eol. In seguito al raggiungimento della data di fine del ciclo di vita definita nel Criterio EOL per il Software o le relative funzioni, non verranno rilasciati aggiornamenti.

b) **Inoltro di infiltrazioni e di informazioni al Fornitore.** Il Software prevede funzioni in grado di raccogliere campioni di virus e di altri programmi dannosi per il computer, nonché oggetti sospetti, problematici, potenzialmente indesiderati o potenzialmente pericolosi, come file, URL, pacchetti IP e frame Ethernet ("Infiltrazioni") e di inviarli al Fornitore, incluse, a titolo esemplificativo ma non esaustivo, informazioni relative al processo di installazione, al Computer e/o alla piattaforma su cui è installato il Software e informazioni relative alle operazioni e alle funzionalità del Software ("Informazioni"). Le Informazioni e le Infiltrazioni possono contenere dati (compresi dati personali ottenuti in modo casuale o accidentale) sull'Utente finale o altri utenti del computer sul quale è installato il Software, nonché file colpiti da Infiltrazioni con i metadati associati.

Le Informazioni e le Infiltrazioni possono essere raccolte mediante le seguenti funzioni del Software:

i. La funzione del sistema di reputazione LiveGrid, che prevede la raccolta e l'invio al Fornitore di hash unidirezionali correlati alle Infiltrazioni. Questa funzione è attivata nelle impostazioni standard del Software.

ii. La funzione del sistema di feedback LiveGrid, che prevede la raccolta e l'invio di Infiltrazioni al Fornitore con i metadati e le Informazioni associati. Questa funzione potrebbe essere attivata dall'Utente finale durante il processo di installazione del Software.

Il Fornitore dovrà utilizzare esclusivamente le Informazioni e le Infiltrazioni ricevute ai fini dell'analisi e della ricerca di Infiltrazioni, il miglioramento del Software e la verifica dell'autenticità della Licenza, e dovrà adottare misure appropriate per garantire la sicurezza delle Infiltrazioni e delle Informazioni ricevute. L'attivazione di questa funzione del Software consente al Fornitore di raccogliere ed elaborare Infiltrazioni e Informazioni in base a quanto specificato nella Politica sulla privacy e in conformità delle norme vigenti in materia. È possibile disattivare queste funzioni in qualsiasi momento.

Per le finalità previste dal presente Accordo, è necessario raccogliere, elaborare e conservare i dati che consentono al Fornitore di identificare l'Utente in conformità della Politica sulla privacy. L'Utente ivi accetta che il Fornitore verifichi con mezzi propri se l'utilizzo del Software da parte dell'Utente sia conforme alle disposizioni previste dal presente Accordo. Per le finalità del presente Accordo, l'Utente accetta il trasferimento dei propri dati, attraverso la comunicazione del Software con i sistemi informatici del Fornitore o dei relativi partner commerciali, nell'ambito della rete di distribuzione e di supporto del Fornitore, ai fini della garanzia della funzionalità e dell'autorizzazione all'utilizzo del Software, nonché della protezione dei diritti del Fornitore.

Alla risoluzione del presente Accordo, il Fornitore o qualsiasi suo partner commerciale nell'ambito della rete di distribuzione e di supporto del Fornitore deve essere autorizzato al trasferimento, all'elaborazione e alla memorizzazione dei dati fondamentali che identificano l'Utente, a scopo di fatturazione e ai fini dell'esecuzione del presente Accordo, e alla trasmissione delle notifiche sul proprio Computer.

Ulteriori informazioni sulla tutela della privacy, sulla protezione dei dati personali e sui diritti dell'Utente in qualità di persona interessata sono disponibili nella Politica sulla privacy sul sito Web del Fornitore e accessibili direttamente dal processo di installazione. È ALTRESÌ DISPONIBILE LA SEZIONE "GUIDA" DEL SOFTWARE.

5. **Esercizio dei diritti dell'Utente finale**. L'Utente è tenuto a esercitare i diritti dell'Utente finale di persona o attraverso i propri dipendenti. L'Utente è autorizzato a utilizzare il Software al solo scopo di salvaguardare le proprie operazioni e di proteggere i(l) Computer per cui è stata ottenuta una Licenza.

6. **Limitazioni dei diritti.** È vietata la copia, la distribuzione, la separazione dei componenti o la creazione di prodotti derivati del Software. Durante l'utilizzo del Software, l'Utente è tenuto ad attenersi alle seguenti limitazioni:

a) È autorizzata una copia del Software su supporto per l'archivio permanente come copia di backup, a condizione che quest'ultima non venga installata o utilizzata su altri computer. Ogni altra copia del Software effettuata dall'Utente rappresenta una violazione del presente Contratto.

b) L'Utente non può utilizzare, modificare, tradurre o riprodurre il Software, né trasferire i diritti all'utilizzo del Software, né copiare il Software, eccetto laddove espressamente indicato nel presente Contratto.

c) La rivendita, la sublicenza, il noleggio, il prestito del Software o l'utilizzo del Software per la fornitura di servizi commerciali non sono consentiti.

d) Sono vietate la decodificazione, la decomposizione o il disassemblaggio del Software o qualsivoglia tentativo di determinazione del codice sorgente del software, fatto salvo laddove tale divieto è espressamente proibito per legge.

e) L'Utente accetta di utilizzare il Software esclusivamente secondo modalità conformi a tutte le leggi applicabili nella giurisdizione in cui avviene l'utilizzo dello stesso, incluse, a titolo esemplificativo ma non esaustivo, le limitazioni relative al copyright e ad altri diritti sulla proprietà intellettuale.

f) L'Utente accetta di utilizzare esclusivamente il Software e le relative funzioni in base a modalità che non limitino le possibilità dell'Utente finale di accedere a questi servizi. Il Fornitore si riserva il diritto di limitare l'ambito dei servizi forniti ai singoli Utenti finali e di attivare l'utilizzo dei servizi da parte del maggior numero possibile di

Utenti finali. La limitazione dell'ambito dei servizi potrà altresì significare l'interruzione completa della possibilità di utilizzo di qualsiasi funzione del Software e l'eliminazione dei Dati e delle informazioni sui server del Fornitore o sui server di terze parti correlati ad una specifica funzione del Software.

g) L'Utente accetta di non eseguire alcuna attività basata sull'utilizzo della Chiave di licenza, in violazione dei termini del presente Accordo e di non fornire la Chiave di licenza a soggetti non autorizzati a utilizzare il Software, tra cui il trasferimento di Chiavi di licenza utilizzate o non utilizzate in qualsiasi forma, nonché la riproduzione o la distribuzione non autorizzata di Chiavi di licenza duplicate o generate o l'utilizzo del Software in conseguenza dell'uso di una Chiave di licenza ottenuta da una fonte diversa dal Fornitore.

7. **Copyright**. Il Software e tutti i relativi diritti, inclusi, a titolo esemplificativo ma non esaustivo, i diritti di esclusiva e i diritti di proprietà intellettuale associati, appartengono a ESET e/o ai suoi licenziatari. Sono protetti dalle disposizioni dei trattati internazionali, nonché da ogni altra legge nazionale applicabile nel paese di utilizzo del Software. La struttura, l'organizzazione e il codice del Software costituiscono preziosi segreti industriali e dati sensibili di proprietà di ESET e/o dei suoi licenziatari. È vietata la copia del Software, fatta eccezione per i casi previsti all'Articolo 6 (a). Ogni copia autorizzata ai sensi del presente Contratto deve contenere le stesse note sul copyright e sulla proprietà riportate sul Software. Se l'utente effettua la decodificazione, la decompilazione, il disassemblaggio o qualsivoglia tentativo di determinazione del codice sorgente in violazione delle disposizioni del presente Contratto, qualsiasi informazione in tal modo ottenuta sarà irrevocabilmente e automaticamente ritenuta trasferita al Fornitore e di completa proprietà del Fornitore dal momento della sua origine, nonostante i diritti del Fornitore relativi alla violazione del presente Contratto.

8. **Riserva di diritti**. Il Fornitore si riserva tutti i diritti correlati al Software, ad eccezione dei diritti espressamente concessi all'Utente finale del Software nel presente Contratto.

9. **Versioni in più lingue, software su due supporti, duplicati**. Se il Software supporta più piattaforme o lingue o se l'Utente ha ricevuto più copie del Software, questi è autorizzato a utilizzare il Software unicamente per il numero di computer e per le versioni per i quali ha ottenuto una Licenza. La vendita, il noleggio, l'affitto, la sublicenza, il prestito o il trasferimento di versioni o copie del Software non utilizzato dall'Utente non sono consentiti.

10. **Entrata in vigore e risoluzione del Contratto.** Il presente Contratto entra in vigore alla data dell'accettazione dei termini del presente Contratto da parte dell'Utente. Quest'ultimo potrà recedere dal Contratto in qualsiasi momento disinstallando, distruggendo e restituendo in modo permanente, a sue spese, il Software, tutte le copie di backup e tutto il materiale correlato ricevuto dal Fornitore o dai suoi Business Partner. Il diritto di utilizzo del Software e di qualsiasi altra funzione potrebbe essere soggetto alle disposizioni di cui al Criterio EOL. In seguito al raggiungimento della data di fine del ciclo di vita definita nel Criterio EOL per il Software o una delle relative funzioni, decade il diritto di utilizzo del Software da parte dell’Utente. Indipendentemente dalla modalità di risoluzione del presente Contratto, le disposizioni previste agli Articoli 7, 8, 11, 13, 19 e 21 resteranno valide senza limiti di tempo.

11. **DICHIARAZIONI DELL'UTENTE FINALE**. L'UTENTE FINALE RICONOSCE CHE IL SOFTWARE VIENE FORNITO "COSÌ COM'È" SENZA GARANZIE DI ALCUN TIPO, NÉ ESPLICITE NÉ IMPLICITE, E CHE, SALVO QUANTO INDEROGABILMENTE PREVISTO DALLA LEGGE. IL FORNITORE, I SUOI LICENZIATARI O AFFILIATI COME ANCHE I TITOLARI DEL COPYRIGHT, NON RILASCIANO ALCUNA DICHIARAZIONE O GARANZIA ESPLICITA O IMPLICITA, COMPRESE, A MERO TITOLO ESEMPLIFICATIVO MA NON LIMITATIVO, GARANZIE DI COMMERCIABILITÀ O IDONEITÀ PER UNO SCOPO SPECIFICO O LA GARANZIA CHE IL SOFTWARE NON VIOLI BREVETTI, COPYRIGHT, MARCHI O ALTRI DIRITTI DI TERZE PARTI. IL FORNITORE O ALTRE PARTI NON GARANTISCONO CHE LE FUNZIONI CONTENUTE NEL SOFTWARE SODDISFERANNO I REQUISITI DELL'UTENTE, NÉ CHE L'USO DEL SOFTWARE NON SUBIRÀ INTERRUZIONI O CHE LO STESSO SIA ESENTE DA ERRORI. L'UTENTE SI ASSUME TUTTE LE RESPONSABILITÀ E I RISCHI INERENTI LA SCELTA DEL SOFTWARE AL FINE DI OTTENERE I RISULTATI DESIDERATI, NONCHÉ L'INSTALLAZIONE, L'UTILIZZO E I RISULTATI OTTENUTI DALL'UTILIZZO DEL SOFTWARE.

12. **Assenza di altri obblighi**. Il presente Contratto non pone in essere altri obblighi a carico del Fornitore e dei suoi licenziatari oltre a quanto qui specificamente stabilito.

13. **LIMITAZIONE DI RESPONSABILITÀ**. SALVO QUANTO INDEROGABILMENTE PREVISTO DALLA LEGGE, IN NESSUNA CIRCOSTANZA IL FORNITORE, I SUOI DIPENDENTI O LICENZIATARI POTRANNO ESSERE RITENUTI RESPONSABILI PER LUCRO CESSANTE, PERDITA DI RICAVI, VENDITE, DATI O PER COSTI DERIVANTI DALLA SOSTITUZIONE DI BENI O SERVIZI, DANNI ALLA PROPRIETÀ, LESIONI PERSONALI, INTERRUZIONE DELL'ATTIVITÀ COMMERCIALE, SMARRIMENTO DI INFORMAZIONI COMMERCIALI, O PER QUALSIASI DANNO SPECIALE, DIRETTO, INDIRETTO, ACCIDENTALE, ECONOMICO, ESEMPLARE, PUNITIVO O CONSEQUENZIALE, INDIPENDENTEMENTE DALLA CAUSA E DAL FATTO CHE TALE EVENTO DERIVI DA CONTRATTO, FATTO ILLECITO, NEGLIGENZA O ALTRA INTERPRETAZIONE DI RESPONSABILITÀ DERIVANTE DALL'INSTALLAZIONE, DALL'UTILIZZO OPPURE DALL'IMPOSSIBILITÀ DI UTILIZZARE IL SOFTWARE, ANCHE QUALORA IL FORNITORE O I SUOI LICENZIATARI O AFFILIATI SIANO STATI AVVISATI DELLA POSSIBILITÀ DI TALI DANNI. POICHÉ ALCUNI PAESI E GIURISDIZIONI NON AMMETTONO L'ESCLUSIONE DI RESPONSABILITÀ DI CUI SOPRA, MA POTREBBERO CONSENTIRE DI LIMITARE LA RESPONSABILITÀ, IN QUESTI CASI LA RESPONSABILITÀ DEL FORNITORE, DEI SUOI DIPENDENTI O DEI SUOI LICENZIATARI O AFFILIATI SARÀ LIMITATA AL PREZZO CORRISPOSTO PER LA LICENZA.

14. Nessuna disposizione contenuta nel presente Contratto costituirà pregiudizio per i diritti legali di qualsiasi parte in veste di consumatore in caso di funzionamento contrario a quanto esposto.

15. **Supporto tecnico**. ESET o terze parti commissionate da ESET forniranno supporto tecnico a propria discrezione, senza garanzie né dichiarazioni. In seguito al raggiungimento della data di fine del ciclo di vita definita nel Criterio EOL per il Software o le relative funzioni, non verrà offerta alcuna forma di supporto tecnico. Verrà richiesto all'Utente finale di salvare tutti i dati, i software e i programmi prima della fornitura del supporto tecnico. ESET e/o terze parti commissionate da ESET non possono accettare la responsabilità per danni o perdite di dati, proprietà, software o hardware o perdita di profitti legati alla fornitura del supporto tecnico. ESET e/o terze parti commissionate da ESET si riservano il diritto di decidere che la risoluzione del problema va al di là della pertinenza del supporto tecnico. ESET si riserva il diritto di rifiutare, interrompere o concludere la fornitura del supporto tecnico a sua discrezione. Per le finalità legate all'offerta di un servizio di assistenza tecnica, potrebbero essere richieste informazioni sulla Licenza, le Informazioni e altri dati in conformità dell'Informativa sulla privacy.

16. **Trasferimento della Licenza**. È possibile trasferire il software da un computer a un altro, eccetto se in contrasto con i termini del Contratto. Se non in contrasto con i termini del Contratto, l'Utente finale sarà autorizzato a trasferire permanentemente la Licenza e tutti i diritti derivanti dal presente Contratto a un altro Utente finale solo con il consenso del Fornitore, secondo la condizione che (i) l'Utente finale originale non conservi copie del Software; (ii) il trasferimento dei diritti deve essere diretto, ossia dall'Utente finale originale al nuovo Utente finale; (iii) il nuovo Utente finale deve assumersi tutti i diritti e gli obblighi incombenti sull'Utente finale originale secondo i termini del presente Contratto; (iv) l'Utente finale originale deve fornire al nuovo Utente finale la documentazione che consente la verifica dell'autenticità del Software, come specificato all'Articolo 17.

17. **Verifica dell'autenticità del Software.** L'Utente finale può dimostrare il diritto a utilizzare il Software in uno dei modi seguenti: (i) tramite un certificato di licenza emesso dal Fornitore o da terzi designati dal Fornitore; (ii) tramite un contratto di licenza scritto, qualora sia stato stipulato; (iii) tramite l'invio di un'e-mail inviata dal Fornitore contenente i dettagli della licenza (nome utente e password). Per le finalità legate alla verifica dell'autenticità del Software, potrebbero essere richieste informazioni sulla Licenza e dati di identificazione dell'Utente finale in conformità dell'Informativa sulla privacy.

18. **Licenze per enti pubblici e governo degli Stati Uniti**. Il Software sarà fornito agli enti pubblici, incluso il governo degli Stati Uniti, con i diritti e le limitazioni della licenza descritti nel presente Contratto.

19. **Conformità alle disposizioni in materia di controllo del commercio**.

a) L’utente non esporterà, riesporterà, trasferirà o cederà, in modo diretto o indiretto, il Software a terzi e non lo utilizzerà in alcun modo ovvero si asterrà dal compimento di azioni che potrebbero spingere ESET o le relative società controllanti, le relative sussidiarie e le sussidiarie di una società controllante, nonché le entità controllate dalle relative società controllanti (“Affiliate”) ad agire in violazione di o a essere esposte alle eventuali conseguenze negative previste dalle Leggi in materia di controllo del commercio che comprendono

i. leggi che controllano, limitano o impongono requisiti di licenza sulle esportazioni, le riesportazioni o il trasferimento di merci, software, tecnologie o servizi, emanate o adottate da governi, Stati o autorità di regolamentazione degli Stati Uniti d’America, di Singapore, del Regno Unito, dell’Unione europea o dei relativi Stati membri ovvero di un paese che impone il rispetto degli obblighi ai sensi del presente Contratto o in cui ESET o le relative Affiliate sono costituite o operano (“Leggi in materia di controllo delle esportazioni”) e

ii. leggi in materia economica, finanziaria, commerciale o di altra natura, sanzioni, restrizioni, embarghi, divieti di importazione o esportazione, divieti sul trasferimento di fondi o beni o sull’esecuzione di servizi o misure equivalenti imposte da governi, Stati o autorità di regolamentazione degli Stati Uniti d’America, di Singapore, del Regno Unito, dell’Unione europea o dei relativi Stati membri ovvero di un paese che impone il rispetto degli obblighi ai sensi del presente Contratto o in cui ESET o le relative Affiliate sono costituite o operano.

(gli atti legali di cui ai punti i e ii. sopra sono denominati “Leggi sul controllo del commercio”).

b) ESET avrà facoltà di sospendere i propri obblighi ai sensi o a fronte della risoluzione dei presenti Termini con effetto immediato nei casi di seguito specificati:

i. ESET stabilisce, a sua ragionevole discrezione, che l’Utente abbia violato o abbia commesso una possibile violazione delle disposizioni di cui all’Articolo 19 a) del presente Contratto; oppure

ii. l’Utente finale e/o il Software diventino soggetti alle disposizioni di cui alle Leggi in materia di controllo del commercio e, conseguentemente, ESET stabilisca, a sua ragionevole discrezione, che l’adempimento in forma continuativa dei propri obblighi ai sensi del presente Contratto potrebbe causare la violazione o l’esposizione di ESET o delle relative Affiliate alle eventuali conseguenze negative previste dalle Leggi in materia di controllo del commercio.

c) Nessuna disposizione di cui al presente Contratto è intesa e dovrebbe essere concepita o interpretata allo scopo di indurre o richiedere a una delle parti di agire o astenersi dall’agire (o di accettare di agire o astenersi dall’agire) in base a modalità incompatibili con, penalizzate o vietate ai sensi delle Leggi in materia di controllo del commercio applicabili.

20. **Avvisi**. Tutti gli avvisi e i resi del Software e della Documentazione devono essere inviati a: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, fatto salvo il diritto di ESET di comunicare all’Utente eventuali modifiche al presente Accordo, alle Informative sulla privacy, al Criterio EOL e alla Documentazione ai sensi dell’art. 22 dell’Accordo. ESET potrebbe inviare all’Utente e-mail o notifiche in-app tramite il Software ovvero pubblicare le comunicazioni sul proprio sito web. L’Utente accetta di ricevere comunicazioni legali da ESET in formato elettronico, comprese eventuali comunicazioni in caso di modifica dei Termini, dei Termini speciali o delle Informative sulla privacy, eventuali proposte/accettazioni di contratti o inviti a trattare, avvisi o altre comunicazioni legali. Tali comunicazioni elettroniche saranno considerate ricevute per iscritto, fatto salvo il caso in cui le leggi applicabili non richiedano specificamente un tipo di comunicazione differente.

21. **Legge applicabile**. Il presente Accordo è disciplinato e interpretato in base alle leggi in vigore nella Repubblica Slovacca. L'Utente finale e il Fornitore accettano che gli eventuali conflitti con la Convenzione delle Nazioni Unite sui contratti per la compravendita internazionale di merci non sono applicabili. L'Utente accetta espressamente che qualsiasi reclamo o disputa derivante dal presente Contratto con il Fornitore o correlata all'utilizzo del Software sia di competenza del Tribunale di Bratislava I e accetta espressamente l'esercizio della giurisdizione da parte del suddetto tribunale.

22. **Disposizioni generali**. Qualora alcune disposizioni del presente Contratto fossero giudicate non valide o non applicabili, ciò non avrà alcun effetto sulla parte restante del Contratto, che resterà valido e applicabile nei termini e nelle condizioni qui indicati. Il presente Accordo è stato sottoscritto in lingua inglese. In caso di traduzione dell'Accordo per motivi di praticità di fruizione o altri scopi ovvero in caso di discrepanza tra le versioni nelle varie lingue del presente Accordo, prevarrà la versione in lingua inglese.

ESET si riserva il diritto di apportare modifiche al Software nonché di rivedere i termini del presente Accordo, gli Allegati, gli Addendum, l'Informativa sulla privacy, il Criterio EOL e la Documentazione o parti degli stessi in qualsiasi momento, attraverso l'aggiornamento dei relativi documenti (i) allo scopo di integrare le modifiche apportate al Software o alle modalità di conduzione delle attività aziendali da parte di ESET, (ii) per motivi legali, normativi o di sicurezza o (iii) per prevenire situazioni di abuso o danno. Eventuali revisioni dell'Accordo verranno segnalate all'Utente tramite e-mail, notifiche in-app o con altri mezzi elettronici. Qualora l'Utente non esprima il suo consenso alle modifiche all'Accordo proposte, avrà facoltà di recedere in base a quanto previsto dall'Art. 10 entro 30 giorni dalla ricezione di un avviso relativo a dette modifiche. Fatto salvo il caso in cui l'Utente receda dall'Accordo entro questo limite di tempo, le modifiche proposte saranno considerate accettate e diventeranno effettive a far data dalla ricezione di un avviso relativo a dette modifiche.

Il presente Contratto costituisce il Contratto completo tra il Fornitore e l'Utente in relazione al Software e sostituisce qualsiasi precedente dichiarazione, intesa, impegno, comunicazione o avviso relativo al Software.

EULAID: EULA-PRODUCT-LG; 3537.0

Informativa sulla privacy

La protezione dei dati personali rappresenta un aspetto particolarmente importante per ESET, spol. s r. o., con sede legale presso Einsteinova 24, 851 01 Bratislava, Slovak Republic, registrata presso il registro delle imprese di competenza del tribunale circoscrizionale Bratislava I, Sezione Sro, numero di registro 3586/B, numero di identificazione commerciale 31333532 in qualità di titolare del trattamento dei dati ("ESET" o "la Società"). ESET desidera attenersi ai requisiti in materia di trasparenza legalmente standardizzati ai sensi del Regolamento generale sulla protezione dei dati dell'UE ("GDPR"). Per raggiungere tale obiettivo, la Società pubblica la presente Informativa sulla privacy al solo scopo di informare il cliente ("Utente finale" o "Utente") in qualità di soggetto interessato relativamente agli argomenti in materia di protezione dei dati personali:

- Base legale dell'elaborazione dei dati personali,
- Condivisione e riservatezza dei dati,
- Protezione dei dati,
- Diritti dell'Utente finale in qualità di soggetto interessato,
- Elaborazione dei dati personali dell'Utente
- Informazioni di contatto.

Elaborazione dei dati personali dell'Utente

I servizi offerti da ESET integrati nei relativi prodotti sono forniti ai sensi dell' EULA. Tuttavia, alcuni di essi potrebbero richiedere un'attenzione particolare. Con la presente la Società desidera fornire all'Utente ulteriori informazioni relative alla raccolta dei dati relativamente alla fornitura dei propri servizi. La Società offre vari servizi descritti nell'Accordo di licenza per l'utente finale e nella documentazione. Per garantire un funzionamento corretto delle varie applicazioni, la Società richiede all'Utente di fornire le informazioni di seguito indicate:

- Aggiornamenti e altre informazioni statistiche, tra cui dati concernenti i processi di installazione e i computer degli Utenti finali, come ad esempio le piattaforme di installazione dei prodotti e le informazioni sulle operazioni e le funzionalità degli stessi, come i sistemi operativi, le informazioni sui dispositivi

hardware, gli ID di installazione, gli ID delle licenze, gli indirizzi IP, gli indirizzi MAC e le impostazioni di configurazione dei prodotti.

- Hash unidirezionali correlati alle infiltrazioni previsti dal sistema di reputazione ESET LiveGrid® che garantisce un potenziamento delle prestazioni delle soluzioni anti-malware proposte eseguendo un confronto tra i file controllati e un database di oggetti inseriti nelle whitelist o nelle blacklist all'interno del cloud.
- I campioni sospetti e i metadati “from the wild” prodotti da ESET LiveGrid® Feedback System che consente a ESET di fornire una risposta tempestiva alle esigenze degli Utenti finali e alle minacce più recenti. Le attività della Società dipendono strettamente dall’invio, da parte degli Utenti finali, di
    - infiltrazioni, quali campioni potenziali di virus e altri programmi dannosi e sospetti; oggetti problematici, potenzialmente indesiderati o pericolosi, come file eseguibili, messaggi di posta elettronica segnalati dagli Utenti finali come spam o contrassegnati dal prodotto;
    - informazioni sui dispositivi all'interno di reti locali, tra cui tipo, fornitore, modello e/o nome dei dispositivi;
    - informazioni relative all'uso di Internet, tra cui indirizzi IP e dati geografici, pacchetti IP, URL e frame Ethernet;
    - file di arresti anomali e le informazioni in essi contenute.

Non è volontà di ESET raccogliere dati personali al di fuori di tale ambito ma, a volte, risulta impossibile. Accidentalmente i dati raccolti potrebbero essere inclusi negli stessi malware (a insaputa di ESET e senza la sua previa autorizzazione) o all’interno di nomi di file o URL ed ESET non desidera che diventino parte dei propri sistemi o che siano elaborati per le finalità di cui alla presente Informativa sulla privacy.

- Le informazioni sulla licenza, tra cui ID e dati personali come nomi, cognomi, indirizzi e indirizzi di posta elettronica sono necessari per scopi di fatturazione, ai fini della verifica dell’autenticità delle licenze e per la fornitura dei servizi.
- Le informazioni di contatto e i dati contenuti nelle richieste di assistenza potrebbero essere necessari ai fini dell’offerta dei servizi di assistenza. In base al canale scelto dall’Utente finale per contattare ESET, quest’ultima potrebbe raccogliere l’indirizzo e-mail, il numero di telefono, informazioni sulle licenze, dettagli sui prodotti e descrizione della richiesta di assistenza. La Società potrebbe richiedere all’Utente di fornire altre informazioni al fine di facilitare la gestione delle richieste di assistenza.

Condivisione e riservatezza dei dati

La Società non condivide i dati dell’Utente con terze parti. Tuttavia, ESET è un’azienda che opera in tutto il mondo tramite società affiliate o partner che fanno parte della rete di distribuzione, assistenza e supporto. Le informazioni relative alla gestione delle licenze, alla fatturazione e al supporto tecnico elaborate da ESET potrebbero essere trasferite da e verso le società affiliate o i partner ai fini dell’esecuzione dei termini dell’Accordo di licenza per l’utente finale, tra cui l’erogazione dei servizi o l’assistenza.

ESET preferisce elaborare i propri dati all’interno dell’Unione europea (UE). Tuttavia, in base alla posizione dell’Utente (utilizzo dei prodotti e/o servizi della Società al di fuori dell’UE) e/o del servizio scelto dall’Utente, potrebbe essere necessario trasferire i dati dell’Utente in un paese al di fuori dell’UE. Ad esempio, in relazione al cloud computing, la Società utilizza servizi di terze parti. In questi casi, la Società seleziona attentamente i fornitori di servizi e garantisce un livello adeguato di protezione dei dati attraverso misure contrattuali, tecniche e organizzative. Di norma, se necessario, la Società conviene sulle clausole contrattuali tipo dell’UE con le normative contrattuali supplementari.

Per alcuni paesi al di fuori dell’UE, tra cui il Regno Unito e la Svizzera, l’UE ha già stabilito un livello comparabile di protezione dei dati. Grazie al sistema del livello comparabile di protezione dei dati, il trasferimento dei dati verso questi paesi non richiede particolari autorizzazioni o accordi.

Diritti dei soggetti titolari dei dati

Data la centralità dei diritti di ogni Utente finale, la Società desidera informare l'Utente che tutti gli Utenti finali (provenienti da qualsiasi paese UE o extra-UE) hanno i seguenti diritti garantiti in ESET. Per esercitare i diritti del soggetto interessato, l'Utente può contattare la Società tramite il modulo di supporto o tramite e-mail all'indirizzo dpo@eset.sk. Ai fini dell'identificazione, l'Utente dovrà fornire le seguenti informazioni: Nome, indirizzo e-mail e, se disponibile, chiave di licenza o numero cliente e affiliazione aziendale. Non inviare altri dati personali, tra cui la data di nascita. Tenere presente che, per poter elaborare la richiesta dell'Utente, oltre che per scopi di identificazione, la Società provvederà al trattamento dei dati personali dello stesso.

Diritto di revoca del consenso. Il diritto di revoca del consenso è valido in caso di un'elaborazione basata solo sul consenso. Nel caso in cui la Società elabori i dati personali dell'Utente in base al consenso, quest'ultimo ha facoltà di recedere dal consenso in qualsiasi momento senza fornire la motivazione. La revoca del consenso dell'Utente ha effetto futuro e non incide sulla legalità dei dati elaborati in precedenza.

Diritto di opposizione. Il diritto di opporsi all'elaborazione è valido in caso di trattamento basato sul legittimo interesse di ESET o di terze parti. Nel caso in cui la Società elabori i dati personali dell'Utente al fine di tutelare un interesse legittimo, in quanto soggetto interessato, l'Utente ha il diritto di opporsi in qualsiasi momento all'interesse legittimo invocato dalla Società e all'elaborazione dei propri dati personali. Il diritto di opposizione dell'Utente ha effetto futuro e non incide sulla legalità dei dati elaborati prima dell'opposizione. Nel caso in cui la Società elabori i dati personali dell'Utente per finalità di marketing diretto, non è necessario fornire le motivazioni dell'opposizione. Ciò vale anche per la profilazione, nella misura in cui è collegata a tali attività di marketing diretto. In tutti gli altri casi, la Società richiede all'Utente di informarla brevemente in relazione ai propri reclami contro l'interesse legittimo di ESET a elaborare i suoi dati personali.

Tenere presente che, in alcuni casi, nonostante la revoca del consenso da parte dell'Utente, la Società ha facoltà di elaborare ulteriormente i suoi dati personali sulla base di altri requisiti legali, ad esempio ai fini dell'esecuzione di un contratto.

Diritto di accesso. In quanto soggetto interessato, l'Utente ha diritto a ottenere in qualsiasi momento e gratuitamente da ESET informazioni sui propri dati memorizzati.

Diritto di rettifica. In caso di trattamento non intenzionale di dati personali non corretti sull'Utente, quest'ultimo ha il diritto di correggere il problema.

Diritto di cancellazione e diritto di limitazione dell'elaborazione. In qualità di soggetto interessato, l'Utente ha il diritto di richiedere la cancellazione o la limitazione dell'elaborazione dei propri dati personali. Se la Società elabora i dati personali dell'Utente (ad esempio, con il suo consenso) quest'ultimo ha il diritto di recedere e, se non sussistono altre basi legali (ad esempio, un contratto), i dati personali vengono rimossi immediatamente. I dati personali dell'Utente verranno rimossi anche nel momento in cui non saranno più richiesti per gli scopi indicati al termine del periodo di conservazione.

Se la Società utilizza i dati personali dell'Utente al solo scopo di eseguire attività di marketing diretto e l'Utente ha revocato il proprio consenso o si è opposto all'interesse legittimo sottostante di ESET, la Società limiterà l'elaborazione dei suoi dati personali nella misura in cui i dati di contatto dell'Utente sono inclusi nella blacklist interna al fine di evitare contatti indesiderati. In caso contrario, i dati personali dell'Utente verranno rimossi.

Tenere presente che la Società potrebbe richiedere la memorizzazione dei dati dell'Utente fino alla scadenza degli obblighi di conservazione e dei periodi stabiliti dal legislatore o dalle autorità di supervisione. Gli obblighi e i periodi di conservazione potrebbero anche essere stabiliti dalla legislazione della Repubblica Slovacca. Successivamente, i dati corrispondenti verranno sistematicamente rimossi.

Diritto di portabilità dei dati. ESET è lieta di fornire all'Utente, in quanto soggetto interessato, i dati personali elaborati in formato xls.

Diritto di presentazione di un reclamo. In qualità di soggetto interessato, l'Utente ha facoltà di presentare un reclamo in qualsiasi momento dinanzi a un'autorità di supervisione. ESET è subordinata alla normativa delle leggi vigenti in Slovacchia e come membro dell'Unione Europea è vincolata alla legislazione inerente la protezione dei dati. L'autorità responsabile della supervisione dei dati competente è l'Office for Personal Data Protection della Repubblica Slovacca, con sede al seguente indirizzo: Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Informazioni di contatto

Qualora desideri esercitare i propri diritti in qualità di soggetto titolare dei dati o in caso di domande o dubbi, l'Utente potrà inviare un messaggio ai seguenti recapiti:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk