

SOPHOS

Sophos Endpoint Security and Control Guida in linea

Versione prodotto: 9.5

Data documento: giugno 2010



Sommario

1	Informazioni su Sophos Endpoint Security and Control.....	3
2	Home page.....	4
3	Gruppi Sophos.....	5
4	Utilizzo di Sophos Anti-Virus.....	8
5	Utilizzo di Sophos Device Control.....	42
6	Utilizzo di Sophos Data Control.....	44
7	Utilizzo di Sophos Client Firewall.....	46
8	Utilizzo di Sophos AutoUpdate.....	72
9	Utilizzo del Blocco rimozione Sophos	75
10	Troubleshooting.....	81
11	Glossario.....	89
12	Supporto tecnico.....	94
13	Note legali.....	95

1 Informazioni su Sophos Endpoint Security and Control

Sophos Endpoint Security and Control, versione 9.5 è una suite di software di sicurezza integrata.

Sophos Anti-Virus rileva e rimuove virus, trojan, worm e spyware, oltre che adware e altre applicazioni potenzialmente indesiderate. La tecnologia Host Intrusion Prevention System (HIPS) protegge il computer da file sospetti e rootkit, virus non identificati e comportamenti sospetti. Protegge anche dalle minacce provenienti da siti web malevoli ed infetti. Sophos Live Protection utilizza la tecnologia “in-the-cloud” per decidere istantaneamente se un file sospetto rappresenta una minaccia, migliorando quindi in maniera significativa il rilevamento di nuovo malware senza il rischio di rilevamenti indesiderati.

Sophos Application Control blocca applicazioni non autorizzate quali Voice over IP, messaggistica istantanea, condivisione file e software di gioco.

Sophos AutoUpdate offre un aggiornamento a prova di errore e il controllo della larghezza di banda quando gli aggiornamenti vengono eseguiti da connessioni di rete a bassa velocità.

Sophos Client Firewall impedisce a worm, trojan e spyware il furto e la distribuzione di informazioni sensibili, oltre che prevenire gli attacchi di pirati informatici.

Sophos Data Control evita la perdita accidentale di dati che possono portare all'identificazione personale da computer gestiti.

Sophos Device Control blocca dispositivi di memorizzazione esterni non autorizzati e tecnologie di connessione wireless.

Il Blocco rimozione Sophos impedisce a malware noto e utenti non autorizzati (utenti con conoscenze tecniche limitate) la disinstallazione del software di sicurezza Sophos o la disabilitazione tramite l'interfaccia Sophos Endpoint Security and Control.

2 Home page

Quando si apre la finestra di **Sophos Endpoint Security and Control**, nel riquadro a destra viene visualizzata la **Home** page. Consente la configurazione e l'utilizzo del software.

Durante l'utilizzo di Sophos Endpoint Security and Control, il contenuto del riquadro a destra cambierà. Per tornare alla **Home** page, cliccare sul pulsante **Home** nella barra degli strumenti.

3 Gruppi Sophos

3.1 Gruppi Sophos

Sophos Endpoint Security and Control limita l'accesso a determinate parti della rete solo ai membri di specifici gruppi Sophos.

Quando viene installato Sophos Endpoint Security and Control, tutti gli utenti del computer vengono inizialmente assegnati a un gruppo Sophos a seconda del gruppo Windows di appartenenza.

Gruppo Windows	Gruppo Sophos
Administrators	SophosAdministrator
Power Users	SophosPowerUser
Utenti	SophosUser

Gli utenti non assegnati ad alcun gruppo Sophos, inclusi gli utenti ospiti, possono svolgere solo le seguenti operazioni:

- Scansione in accesso
- Scansione dal menu del tasto destro del mouse

SophosUsers

I SophosUsers possono svolgere tutte le operazioni elencate qui sopra, oltre a quelle di seguito:

- Apertura della finestra di Sophos Endpoint Security and Control
- Impostazione ed esecuzione delle scansioni su richiesta
- Configurazione della scansione dal menu del tasto destro del mouse
- Gestione, con diritti limitati, degli oggetti in quarantena
- Creazione e configurazione delle regole del firewall

SophosPowerUsers

I SophosPowerUsers hanno gli stessi diritti dei SophosUsers, oltre che i seguenti diritti aggiuntivi:

- Maggiori privilegi nella gestione della quarantena
- Accesso al gestore autorizzazioni

SophosAdministrators

I SophosAdministrators possono utilizzare e configurare qualsiasi parte di Sophos Endpoint Security and Control.

Nota: Se il blocco rimozione è abilitato, un SophosAdministrator deve conoscere la password blocco rimozione per effettuare le seguenti operazioni:

- Configurazione della scansione in accesso.
- Rilevamento di comportamento sospetto.
- Disabilitazione blocco rimozione

Per ulteriori informazioni, consultare la sezione [Informazioni sul blocco rimozione su questo computer](#) a pagina 75.

3.2 Aggiunta di utenti al gruppo Sophos

Gli amministratori di dominio o i membri del gruppo Windows Administrators in tale computer possono cambiare il gruppo Sophos a cui appartiene un determinato utente. Solitamente questa operazione viene svolta per modificare i diritti di accesso a Sophos Endpoint Security and Control.

Per aggiungere utenti al gruppo Sophos:

1. Se si utilizza Windows, aprire Gestione computer.
2. Nella struttura ad albero della console, cliccare su **Users**.
3. Cliccare col tasto destro del mouse sull'account utente e poi su **Proprietà**.
4. Nella scheda **Membro di**, cliccare su **Aggiungi**.
5. In **Immettere i nomi degli oggetti da selezionare**, digitare il nome di un gruppo Sophos:
 - SophosAdministrator
 - SophosPowerUser
 - SophosUser
6. Se si desidera validare il nome del gruppo Sophos, cliccare su **Controlla nomi**.

La prossima volta che l'utente accederà al computer, i diritti di accesso a Sophos Endpoint Security and Control saranno cambiati.

Note

- Per aprire Gestione computer, cliccare su **Start** e successivamente su **Pannello di controllo**. Cliccare due volte su **Strumenti di amministrazione** e due volte su **Gestione computer**.
- Per rimuovere un utente da un gruppo utenti Sophos, dalla scheda **Membro di**, selezionare il gruppo da **Membro di** e cliccare su **Rimuovi**.

3.3 Configurazione dei diritti utente per il Gestore quarantena

In quanto membri del gruppo SophosAdministrator, è possibile configurare i diritti utente per il Gestore quarantena.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Diritti utente per Gestore quarantena**.

2. Selezionare il tipo di utente che svolgerà un certo tipo di azione.

Nota: eccezion fatta per l'opzione **Autorizza**, i diritti qui impostati vengono applicati solo al **Gestore quarantena**.

Opzione	Descrizione
Disinfetta settori	Gli utenti possono disinfettare il boot sector del floppy disk.
Disinfetta file	Gli utenti possono disinfettare documenti e programmi.
Cancella file	Gli utenti possono cancellare file infetti.
Sposta file	Gli utenti possono spostare i file infetti in un'altra cartella.
autorizzazione	Gli utenti possono autorizzare oggetti sospetti, adware e PUA, al fine di consentirne l'esecuzione nel computer. Questa opzione è applicabile sia al Gestore autorizzazioni che al Gestore quarantena .

4 Utilizzo di Sophos Anti-Virus

4.1 Differenze fra scansione in accesso e su richiesta

Scansione in accesso

La scansione in accesso rappresenta il principale metodo di protezione contro virus e altre minacce.

Ogni qual volta si copia, sposta o accede a un file, Sophos Anti-Virus ne esegue la scansione e ne consente l'accesso solo se tale file non costituisce una minaccia per il computer o se autorizzato per l'utilizzo.

Gli Amministratori Sophos possono in aggiunta impostare l'esecuzione della scansione dei file quando essi vengono salvati, creati o rinominati. Per ulteriori informazioni, consultare la sezione [Modifica delle opzioni della scansione in accesso](#) a pagina 11.

Scansione su richiesta

Oltre alla scansione in accesso, Sophos Anti-Virus fornisce diversi tipi di scansione su richiesta per garantire protezione aggiuntiva.

La scansione su richiesta è una scansione avviata dall'utente. È possibile eseguire una scansione di tutto, da un file singolo all'intero computer.

Per ulteriori informazioni, consultare la sezione [Tipi di scansione su richiesta](#) a pagina 14.

4.2 Scansione in accesso

4.2.1 Configurazione della scansione in accesso

Per aprire la finestra di dialogo relativa alle impostazioni della scansione in accesso:

- ❖ Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Scansione in accesso.**
- [Scansione dei file di archivio](#) a pagina 21
- [Ricerca di virus di Mac](#) a pagina 22
- [Scansione di tutti i file](#) a pagina 22
- [Ricerca di adware e PUA](#) a pagina 23
- [Ricerca di file sospetti](#) a pagina 23
- [Ripristino dei file checksum scansionati](#) a pagina 8

4.2.2 Ripristino dei file checksum scansionati

L'elenco dei file checksum scansionati viene ripristinato quando viene eseguito un aggiornamento di Sophos Anti-Virus, oppure quando viene riavviato il computer. L'elenco

viene ricostruito con i nuovi dati mano a mano che i file vengono scansionati da Sophos Anti-Virus.

È possibile ripristinare l'elenco di file checksum scansionati da Sophos Endpoint Security and Control, se non si desidera riavviare il computer.

Per ripristinare i file checksum scansionati:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Scansione in accesso**.
2. Nella scheda **Opzioni**, cliccare su **Pulisci cache**.

4.2.3 Specificazione delle estensioni dei file per la scansione in accesso

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

È possibile specificare quali estensioni dei file debbano essere verificate durante la scansione in accesso.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Scansione in accesso**.
2. Cliccare sulla scheda **Estensioni** ed impostare le opzioni secondo quanto descritto di seguito.

Scansione di tutti i file

Cliccare su questa opzione per abilitare la scansione di tutti i file, indipendentemente dall'estensione del file.

Consenti scelta delle estensioni da esaminare

Cliccare su questa opzione per restringere la scansione ai soli file con un'estensione particolare, specificata nella lista delle estensioni.



Attenzione: l'elenco delle estensioni include i tipi di file che Sophos consiglia di esaminare. Fare attenzione se si modifica l'elenco secondo quanto descritto di seguito.

Per aggiungere un'estensione alla lista, cliccare su **Aggiungi**. È possibile utilizzare il carattere jolly "?" al posto di un singolo carattere.

Per rimuovere un'estensione dalla lista, selezionare l'estensione e cliccare su **Rimuovi**.

Per modificare un'estensione nella lista, selezionare l'estensione e cliccare su **Modifica**.

Selezionando **Consenti scelta delle estensioni da esaminare**, l'opzione **Scansione dei file senza estensione** viene selezionata per impostazione predefinita. Per disabilitare la scansione dei file senza estensione, deselezionare **Scansione dei file senza estensione**.

4.2.4 Esclusione dalla scansione in accesso di file, cartelle e unità

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Esclusione dalla scansione in accesso di file, cartelle e unità.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Scansione in accesso.**
2. Cliccare sulla scheda **Estensioni** ed impostare le opzioni secondo quanto descritto di seguito.

Escludi oggetto

Per specificare gli oggetti da escludere dalla scansione, cliccare su **Aggiungi**. Nella finestra di dialogo **Escludi oggetto**, specificare il tipo e il nome dell'oggetto da escludere. Consultare *Specificare gli oggetti esclusi* di seguito.

Per rimuovere gli oggetti dalla lista degli oggetti esclusi, cliccare su **Rimuovi**.

Per modificare gli oggetti nella lista degli oggetti esclusi, cliccare su **Modifica**.

Specificazione degli oggetti esclusi

Nella finestra di dialogo **Escludi oggetto**, selezionare **Tipo di oggetto**.

Specificare il **Nome dell'oggetto** utilizzando il pulsante **Sfoggia** o digitandolo nella casella di testo.

Nota: se si lavora su una piattaforma a 64 bit, nella finestra di dialogo **Escludi oggetto** il pulsante **Sfoggia** non è visibile.

Ulteriori dettagli sulla modalità per specificare i nomi degli oggetti si possono trovare qui di seguito.

■ **Nome file**

È possibile specificare solo il nome di un file e Sophos Anti-Virus escluderà tutti i file con quel nome, ovunque si trovino. Ad esempio

`fred.bmp`

fa sì che Sophos Anti-Virus escluda tutti i file di nome fred.bmp, indipendentemente dalla loro posizione.

■ **Percorso completo**

È possibile specificare l'esatta posizione e il nome preciso di un file, e Sophos Anti-Virus escluderà solo quel particolare file. Il percorso può includere l'unità o la condivisione. Ad esempio

`C:\Miscellaneous\fred.bmp`

fa sì che Sophos Anti-Virus escluda il file fred.bmp contenuto nella cartella Miscellaneous nell'unità C:.

`\\Server1\Users\Fred\Letter.rtf`

fa sì che Sophos Anti-Virus escluda il file Letter.rtf contenuto nella cartella Fred della condivisione Users sul Server1.

Se non si specifica l'unità o la condivisione, Sophos Anti-Virus cercherà il percorso nella root di ogni unità o condivisione.

■ **Percorso parziale**

È possibile specificare un'unità o una condivisione e Sophos Anti-Virus escluderà tutti i file di quell'unità o condivisione e del livello inferiore. Ad esempio

A :

fa sì che Sophos Anti-Virus escluda tutti i file nell'unità A:.

È possibile specificare una cartella e Sophos Anti-Virus escluderà tutti i file di quella cartella e del livello inferiore. Ad esempio

D:\Tools\

fa sì che Sophos Anti-Virus escluda tutti i file della cartella Tools e relative sottocartelle nell'unità D:.

È possibile specificare una cartella e un file e Sophos Anti-Virus escluderà tutte le cartelle e tutti i file corrispondenti. Ad esempio

logs\log.txt

fa sì che Sophos Anti-Virus escluda log.txt in ogni cartella di nome logs, in ogni unità o condivisione.

Caratteri jolly

Il carattere jolly "?" può essere utilizzato soltanto in un nome file o in un'estensione. Di solito sostituisce un singolo carattere. Tuttavia, se utilizzato alla fine di un nome file o di un'estensione, oltre a sostituire qualsiasi carattere indica anche l'assenza di carattere. Per esempio, file?.txt sta per file.txt, file1.txt e file12.txt, ma non per file123.txt.

Il carattere jolly "*" può essere utilizzato soltanto in un nome file o in un'estensione, nella forma [nome file].* oppure *.*[estensione]. Per esempio, file*.txt, file.txt* e file.*txt non sono validi.

Estensioni multiple

Nei nomi file con estensioni multiple, l'ultima estensione viene considerata come estensione e le altre come parte del nome. Ad esempio

[nome file].[estensione1].[estensione2] significa che il nome file è [nome file].[estensione1] e l'estensione è [estensione2].

Convenzioni di nomenclatura standard

Il nome file o il percorso si basa sulle convenzioni di nomenclatura standard (ad esempio, il nome di una cartella può contenere spazi, ma non può contenere soltanto degli spazi).

4.2.5 Modifica delle opzioni della scansione in accesso

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per impostazione predefinita, Sophos Anti-Virus effettua la scansione dei file che vengono copiati, spostati o aperti.

Gli Amministratori Sophos possono in aggiunta impostare l'esecuzione della scansione dei file quando essi vengono salvati, creati o rinominati.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Scansione in accesso.**

2. Cliccare sulla scheda **Scansione** ed impostare le opzioni secondo quanto descritto di seguito.

Quando effettuare la scansione dei file	Opzione
Copia, spostamento o apertura	in lettura
Salvataggio o creazione	in scrittura
Rinomina	se rinominati

4.2.6 Disabilitazione temporanea della scansione in accesso

In quanto membri del gruppo SophosAdministrator, può presentarsi la necessità di disabilitare temporaneamente la scansione in accesso per motivi di manutenzione o per la risoluzione di alcuni problemi e successivamente di riabilitarla. È possibile disabilitare la protezione in accesso, ma continuare ad eseguire scansioni su richiesta del computer.

Sophos Endpoint Security and Control conserva le impostazioni scelte in questa pagina, anche dopo il riavvio del computer. Se si disabilita la scansione in accesso, il computer risulta non protetto finché la scansione in accesso non venga riabilitata.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Scansione in accesso**.
2. Deselezionare la casella di spunta **Consenti scansione in accesso per questo computer**.

4.2.7 Rilevamento di comportamento sospetto e buffer overflow

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Il rilevamento di comportamento sospetto utilizza l'Host Intrusion Prevention System (HIPS) di Sophos per analizzare dinamicamente il comportamento di tutti i programmi in esecuzione sul computer, per rilevare e bloccare qualsiasi attività dall'aspetto malevolo. Per comportamento sospetto si intendono ad esempio le modifiche al registro che potrebbero consentire l'esecuzione automatica di un virus al riavvio del computer;

Il rilevamento di comportamento sospetto include il rilevamento di buffer overflow, che analizza in modo dinamico il comportamento di tutti i programmi in esecuzione sul sistema, al fine di rilevare attacchi caratterizzati da buffer overflow.

Nota: Il rilevamento di buffer overflow non è disponibile per Windows Vista, Windows 2008, Windows 7 e le versioni di Windows a 64 bit. Questi sistemi operativi sono protetti dai buffer overflow dalla funzione Data Execution Prevention (DEP) di Microsoft.

Se membri del gruppo SophosAdministrator, è possibile modificare le impostazioni per il rilevamento di comportamento sospetto e buffer overflow:

1. Per visualizzare, cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Rilevamento di comportamento sospetto**

2. Nella finestra di dialogo **Rilevamento di comportamento sospetto**:

- Per abilitare o disabilitare il rilevamento di comportamento sospetto, selezionare oppure deselezionare la casella di spunta **Rileva comportamento sospetto**.
- Per abilitare o disabilitare il rilevamento di buffer overflow, selezionare oppure deselezionare la casella di spunta **Rileva buffer overflow**.
- Per impostazione predefinita, i comportamenti sospetti ed i buffer overflow vengono *rilevati* ma non *bloccati* (è selezionata la casella di spunta **Notifica solamente**).



Attenzione: nei primi tempi Sophos consiglia di eseguire Sophos Anti-Virus in modalità solo rilevamento e di autorizzare i programmi necessari prima di abilitare il blocco automatico del comportamento sospetto e dei buffer overflow. Questo approccio evita il blocco dei programmi di cui gli utenti potrebbero aver bisogno.

Per abilitare il *blocco* (oltre al *rilevamento*) del comportamento sospetto e dei buffer overflow, deselezionare la casella di spunta **Notifica solamente**.

4.2.8 Scansione alla ricerca di applicazioni controllate

Un'*applicazione controllata* è un'applicazione la cui esecuzione nel computer è impedita dai criteri di sicurezza aziendali.

La scansione alla ricerca di applicazioni controllate viene attivata o disattivata da una console di gestione come parte del criterio di controllo applicazioni e della scansione in accesso.

Per informazioni sulla scansione in accesso, consultare la sezione [Differenze fra scansione in accesso e su richiesta](#) a pagina 8.

4.2.9 Disabilitazione della scansione alla ricerca di applicazioni controllate

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se si attiva la scansione alla ricerca di applicazioni controllate, questa potrebbe impedire la disinstallazione di alcune applicazioni. In quanto membri del gruppo SophosAdministrator, è possibile disabilitare temporaneamente la scansione alla ricerca di applicazioni controllate nel computer.

Per disabilitare la scansione alla ricerca di applicazioni controllate:

1. Nel menu **Configura**, cliccare su **Controllo applicazioni**.
2. Deselezionare la casella **Abilita scansione in accesso**.

4.3 Scansione su richiesta

4.3.1 Tipi di scansione su richiesta

Scansione completa del computer

Esegue in qualsiasi momento la scansione dell'intero computer, incluso il boot sector e la memoria di sistema.

- [Esecuzione della scansione completa del computer](#) a pagina 17

Scansione dal menu del tasto destro del mouse

Esegue in qualsiasi momento la scansione di file, cartelle o unità in Windows Explorer.

- [Esecuzione della scansione dal menu del tasto destro del mouse](#) a pagina 18

Scansione personalizzata

Esegue la scansione di set di file o cartelle specifici. È possibile eseguire una scansione personalizzata sia manualmente che pianificandone un'esecuzione autonoma.

- [Esecuzione di una scansione personalizzata](#) a pagina 20
- [Pianificazione di una scansione personalizzata](#) a pagina 20

4.3.2 Specificazione delle estensioni dei file per la scansione su richiesta

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

È possibile specificare quali estensioni dei file debbano essere verificate durante la scansione su richiesta.

1. Dal menu **Configura**, cliccare su **Estensioni ed esclusioni su richiesta**.

2. Cliccare sulla scheda **Estensioni** ed impostare le opzioni secondo quanto descritto di seguito.

Scansione di tutti i file

Cliccare su questa opzione per abilitare la scansione di tutti i file, indipendentemente dall'estensione del file.

Consenti scelta delle estensioni da esaminare

Cliccare su questa opzione per restringere la scansione ai soli file con un'estensione particolare, specificata nella lista delle estensioni.



Attenzione: l'elenco delle estensioni include i tipi di file che Sophos consiglia di esaminare. Fare attenzione se si modifica l'elenco secondo quanto descritto di seguito.

Per aggiungere un'estensione alla lista, cliccare su **Aggiungi**. È possibile utilizzare il carattere jolly "?" al posto di un singolo carattere.

Per rimuovere un'estensione dalla lista, selezionare l'estensione e cliccare su **Rimuovi**.

Per modificare un'estensione nella lista, selezionare l'estensione e cliccare su **Modifica**.

Selezionando **Consenti scelta delle estensioni da esaminare**, l'opzione **Scansione dei file senza estensione** viene selezionata per impostazione predefinita. Per disabilitare la scansione dei file senza estensione, deselezionare **Scansione dei file senza estensione**.

4.3.3 Esclusione dalla scansione su richiesta di file, cartelle e unità

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Esclusione dalla scansione su richiesta di file, cartelle e unità.

Nota: la procedura descritta qui sotto si riferisce a *tutte* le scansioni su richiesta. Per escludere gli oggetti da una *specifica* scansione su richiesta, consultare [Creazione di una scansione personalizzata](#) a pagina 18 .

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Estensioni ed esclusioni su richiesta**.
2. Cliccare sulla scheda **Esclusioni**. Impostare le opzioni come descritto di seguito.

Escludi oggetto

Per specificare gli oggetti da escludere dalla scansione, cliccare su **Aggiungi**. Nella finestra di dialogo **Escludi oggetto**, specificare il tipo e il nome dell'oggetto da escludere. Consultare *Specificare gli oggetti esclusi* di seguito.

Per rimuovere gli oggetti dalla lista degli oggetti esclusi, cliccare su **Rimuovi**.

Per modificare gli oggetti nella lista degli oggetti esclusi, cliccare su **Modifica**.

Specificazione degli oggetti esclusi

Nella finestra di dialogo **Escludi oggetto**, selezionare **Tipo di oggetto**.

Specificare il **Nome dell'oggetto** utilizzando il pulsante **Sfoglia** o digitandolo nella casella di testo.

Nota: se si lavora su una piattaforma a 64 bit, nella finestra di dialogo **Escludi oggetto** il pulsante **Sfoglia** non è visibile.

Ulteriori dettagli sulla modalità per specificare i nomi degli oggetti si possono trovare qui di seguito.

■ **Nome file**

È possibile specificare solo il nome di un file e Sophos Anti-Virus escluderà tutti i file con quel nome, ovunque si trovino. Ad esempio

`fred.bmp`

fa sì che Sophos Anti-Virus escluda tutti i file di nome fred.bmp, indipendentemente dalla loro posizione.

■ **Percorso completo**

È possibile specificare l'esatta posizione e il nome preciso di un file, e Sophos Anti-Virus escluderà solo quel particolare file. Il percorso può includere l'unità o la condivisione. Ad esempio

`C:\Miscellaneous\fred.bmp`

fa sì che Sophos Anti-Virus escluda il file fred.bmp contenuto nella cartella Miscellaneous nell'unità C:.

`\\Server1\Users\Fred\Letter.rtf`

fa sì che Sophos Anti-Virus escluda il file Letter.rtf contenuto nella cartella Fred della condivisione Users sul Server1.

Se non si specifica l'unità o la condivisione, Sophos Anti-Virus cercherà il percorso nella root di ogni unità o condivisione.

■ **Percorso parziale**

È possibile specificare un'unità o una condivisione e Sophos Anti-Virus escluderà tutti i file di quell'unità o condivisione e del livello inferiore. Ad esempio

`A:`

fa sì che Sophos Anti-Virus escluda tutti i file nell'unità A:.

È possibile specificare una cartella e Sophos Anti-Virus escluderà tutti i file di quella cartella e del livello inferiore. Ad esempio

`D:\Tools\`

fa sì che Sophos Anti-Virus escluda tutti i file della cartella Tools e relative sottocartelle nell'unità D:.

È possibile specificare una cartella e un file e Sophos Anti-Virus escluderà tutte le cartelle e tutti i file corrispondenti. Ad esempio

`logs\log.txt`

fa sì che Sophos Anti-Virus escluda log.txt in ogni cartella di nome logs, in ogni unità o condivisione.

Caratteri jolly

Il carattere jolly "?" può essere utilizzato soltanto in un nome file o in un'estensione. Di solito sostituisce un singolo carattere. Tuttavia, se utilizzato alla fine di un nome file o di un'estensione, oltre a sostituire qualsiasi carattere indica anche l'assenza di carattere. Per esempio, file?.txt sta per file.txt, file1.txt e file12.txt, ma non per file123.txt.

Il carattere jolly "*" può essere utilizzato soltanto in un nome file o in un'estensione, nella forma [nome file].* oppure *. [estensione]. Per esempio, file*.txt, file.txt* e file.*txt non sono validi.

Estensioni multiple

Nei nomi file con estensioni multiple, l'ultima estensione viene considerata come estensione e le altre come parte del nome. Ad esempio

[nome file].[estensione1].[estensione2] significa che il nome file è [nome file].[estensione1] e l'estensione è [estensione2].

Convenzioni di nomenclatura standard

Il nome file o il percorso si basa sulle convenzioni di nomenclatura standard (ad esempio, il nome di una cartella può contenere spazi, ma non può contenere soltanto degli spazi).

4.3.4 Esecuzione della scansione completa del computer

Nota: la **Scansione del computer** non esamina i file di Mac memorizzati nei computer con sistema operativo Windows. Se si desidera che Sophos Anti-Virus esamini i file di Mac, è necessario impostare una scansione su richiesta personalizzata e abilitare la scansione dei file di Mac per quella scansione.

Per ulteriori informazioni sulle scansioni su richiesta personalizzate, consultare la sezione [Creazione di una scansione personalizzata](#) a pagina 18.

Per ulteriori informazioni sulla scansione dei file Mac, consultare la sezione [Ricerca di virus di Mac](#) a pagina 22.

Per eseguire la scansione dell'intero sistema in uso nel computer, inclusi boot sector e memoria di sistema:

- ❖ Nella pagina **Home**, sotto **Antivirus e HIPS**, cliccare su **Scansione del computer**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.

Viene visualizzata una finestra di dialogo che mostra l'avanzamento della scansione e nella finestra **Sophos Endpoint Security and Control** compare il **Riepilogo delle attività**.

Se vengono individuate minacce o applicazioni controllate, cliccare su **Dettagli** e consultare [Gestione degli oggetti in quarantena](#).

4.3.5 Configurazione della scansione dal menu del tasto destro del mouse

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa *non* potrà ignorare le modifiche qui apportate.

- ❖ Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Scansione dal menu del tasto destro del mouse.**

- [Scansione dei file di archivio](#) a pagina 21
- [Ricerca di virus di Mac](#) a pagina 22
- [Scansione di tutti i file](#) a pagina 22
- [Ricerca di adware e PUA](#) a pagina 23
- [Ricerca di file sospetti](#) a pagina 23

4.3.6 Esecuzione della scansione dal menu del tasto destro del mouse

È possibile esaminare file, cartelle e unità da Windows Explorer o dal computer eseguendo la scansione dal menu del tasto destro del mouse.

1. Utilizzando Windows Explorer o nel computer, selezionare il file, la cartella o l'unità disco che si desidera scansionare.
È possibile selezionare file e cartelle multipli.
2. Cliccare col tasto destro del mouse sull'oggetto selezionato e successivamente cliccare su **Scansione con Sophos Anti-Virus.**

Se vengono rilevate minacce o applicazioni controllate, cliccare su **Dettagli** e consultare la sezione *Gestione degli oggetti in quarantena* della Guida in linea.

4.3.7 Scansioni personalizzate

4.3.7.1 Creazione di una scansione personalizzata

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Cliccare su **Imposta una nuova scansione.**
3. Nel campo di testo **Nome scansione**, digitare un nome per la scansione.
4. Nel riquadro **Oggetti da esaminare**, selezionare le unità e le cartelle che si desidera esaminare. A questo scopo, spuntare la casella alla sinistra di ogni unità o cartella. Per informazioni sulle icone visualizzate accanto alle caselle, consultare [Simboli degli oggetti da esaminare](#) a pagina 19.

Nota: le unità o le cartelle non disponibili (perché non sono in linea o sono state cancellate) vengono visualizzate con un carattere barrato. Vengono rimosse dal riquadro **Oggetti da esaminare** se vengono deselezionate o se si apporta una modifica alla selezione della o delle unità o cartelle madri.

5. Per configurare ulteriormente la scansione, cliccare su **Configura scansione** (per ulteriori informazioni, consultare la sezione [Configurazione di una scansione personalizzata](#) a pagina 19).
6. Per pianificare la scansione, cliccare su **Pianifica scansione.** (per ulteriori informazioni, consultare la sezione [Pianificazione di una scansione personalizzata](#) a pagina 20).

7. Cliccare su **Salva** per salvare la scansione oppure **Salva e avvia** per salvare e avviare la scansione.

4.3.7.2 Simboli degli oggetti da esaminare

Nel riquadro **Oggetti da esaminare**, nella casella accanto a ciascun oggetto (unità o cartella) vengono visualizzate diverse icone, a seconda degli oggetti da esaminare. Queste icone sono raffigurate e descritte qui sotto.

Icona	Descrizione
<input type="checkbox"/>	L'oggetto e relativi sotto-oggetti <i>non sono</i> selezionati per la scansione.
<input checked="" type="checkbox"/>	L'oggetto e relativi sotto-oggetti <i>sono</i> selezionati per la scansione.
<input checked="" type="checkbox"/>	L'oggetto è parzialmente selezionato: non l'oggetto in sé ma alcuni suoi sotto-oggetti sono selezionati per la scansione.
<input checked="" type="checkbox"/>	L'oggetto e relativi sotto-oggetti sono esclusi da questa specifica scansione.
<input checked="" type="checkbox"/>	L'oggetto è parzialmente escluso: l'oggetto è selezionato ma alcuni suoi sotto-oggetti sono esclusi da questa particolare scansione.
<input checked="" type="checkbox"/>	L'oggetto e relativi sotto-oggetti sono esclusi da tutte le scansioni su richiesta, perché è stata impostata un'esclusione su richiesta. Per informazioni, consultare la sezione Esclusione dalla scansione in accesso di file, cartelle e unità a pagina 9

4.3.7.3 Configurazione di una scansione personalizzata

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Scansioni disponibili**, selezionare la scansione che si desidera modificare e poi cliccare su **Modifica**.
3. Cliccare su **Configura scansione**.
 - [Scansione dei file di archivio](#) a pagina 21
 - [Ricerca di virus di Mac](#) a pagina 22
 - [Scansione di tutti i file](#) a pagina 22
 - [Ricerca di adware e PUA](#) a pagina 23
 - [Ricerca di file sospetti](#) a pagina 23
 - [Ricerca di rootkit](#) a pagina 19

4.3.7.4 Ricerca di rootkit

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se membri del gruppo SophosAdministrator, la scansione per la ricerca di rootkit viene sempre eseguita ogni qual volta si esegua una scansione completa del computer.

È possibile eseguire la scansione per la ricerca di rootkit come parte di una scansione personalizzata.

Per eseguire la scansione per la ricerca di rootkit:

1. Nella **Home page**, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Scansioni disponibili**, selezionare la scansione che si desidera modificare e poi cliccare su **Modifica**.
3. Cliccare su **Configura scansione**.
4. Nella scheda **Opzioni**, selezionare la casella di spunta **Ricerca di rootkit**.

4.3.7.5 Pianificazione di una scansione personalizzata

Se membri del gruppo SophosAdministrator, è possibile pianificare una scansione personalizzata o visualizzare e modificare le scansioni pianificate create da altri utenti.

1. Nella **Home page**, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Scansioni disponibili**, selezionare la scansione che si desidera modificare e poi cliccare su **Modifica**.
3. Cliccare su **Pianifica scansione**.
4. Nella finestra di dialogo **Pianifica scansione**, selezionare **Abilita operazione pianificata**.

Selezionare il giorno o i giorni nei quali la scansione dovrà essere eseguita.

Aggiungere l'orario (o gli orari) cliccando su **Aggiungi**.

Se necessario, rimuovere o modificare un orario selezionandolo e cliccando rispettivamente su **Rimuovi** o **Modifica**.

5. Digitare *nome utente e password*. Assicurarsi che il campo relativo alla password non sia vuoto.

La scansione pianificata viene eseguita con i diritti di accesso di quell'utente.

4.3.7.6 Esecuzione di una scansione personalizzata

Nota: non è possibile eseguire una scansione personalizzata pianificata manualmente. Le scansioni pianificate sono visualizzate nella lista **Scansioni disponibili** con un'icona a forma di orologio.

1. Nella **Home page**, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.

2. Nell'elenco **Scansioni disponibili**, selezionare la scansione che si desidera eseguire e poi cliccare su **Avvia**.

Viene visualizzata una finestra di dialogo che mostra l'avanzamento della scansione e appare il riquadro **Riepilogo delle attività** nella finestra di Sophos Endpoint Security and Control

Se vengono individuate minacce o applicazioni controllate, cliccare su **Dettagli** e consultare *Gestione degli oggetti in quarantena*.

4.3.7.7 Rinomina di una scansione personalizzata

1. Nella **Home page**, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Scansioni disponibili**, selezionare la scansione che si desidera modificare e poi cliccare su **Modifica**.
3. Nella casella **Nome scansione**, digitare il nuovo nome della scansione.

4.3.7.8 Visualizzazione del log per la scansione personalizzata

1. Nella **Home page**, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Scansioni disponibili**, cliccare su **Riepilogo** per la scansione personalizzata.
3. Nella finestra di dialogo **Riepilogo**, cliccare sul link nella parte inferiore della finestra.

Dalla pagina log, è possibile copiare il log negli appunti, oppure inviarlo per e-mail o stamparlo.

Per trovare un testo specifico all'interno del log, cliccare su **Trova** e inserire il testo desiderato.

4.3.7.9 Visualizzazione del riepilogo di una scansione personalizzata

1. Nella **Home page**, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Scansioni disponibili**, cliccare su **Riepilogo** per la scansione personalizzata.

4.3.7.10 Cancellazione di una scansione personalizzata

1. Nella **Home page**, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Scansioni disponibili**, selezionare la scansione che si desidera cancellare e poi cliccare su **Cancella**.

4.4 Opzioni di scansione

4.4.1 Scansione dei file di archivio

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Nota: Sophos consiglia di non abilitare questa opzione, per le seguenti ragioni:

- La scansione eseguita all'interno dei file di archivio rallenta notevolmente le operazioni di scansione.
- Sia che questa opzione sia abilitata o meno, quando si apre un file estratto dal file di archivio, tale file viene sottoposto a scansione.
- Indipendentemente dall'abilitazione di questa opzione, i file compressi con le utilità di compressione dinamica (PKLite, LZEXE e Diet) vengono comunque esaminati.

Tuttavia, potrebbe essere opportuno abilitare l'opzione in modo tale che il contenuto di un archivio file compresso sia sottoposto a scansione prima che venga scaricato o inviato per e-mail al computer.

Per eseguire la scansione dei file di archivio:

1. Aprire le impostazioni per la scansione che si desidera configurare. Per informazioni su come svolgere questa operazione, consultare una delle seguenti sezioni:
 - [Configurazione della scansione in accesso](#) a pagina 8
 - [Configurazione della scansione dal menu del tasto destro del mouse](#) a pagina 17
 - [Configurazione di una scansione personalizzata](#) a pagina 19
2. Nella scheda **Opzioni**, selezionare la casella di spunta **Scansione dei file di archivio**.

4.4.2 Ricerca di virus di Mac

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

È possibile configurare Sophos Anti-Virus in modo tale che esamini i file di Mac memorizzati nei computer Windows.

1. Aprire le impostazioni per la scansione che si desidera configurare. Per informazioni su come svolgere questa operazione, consultare una delle seguenti sezioni:
 - [Configurazione della scansione in accesso](#) a pagina 8
 - [Configurazione della scansione dal menu del tasto destro del mouse](#) a pagina 17
 - [Configurazione di una scansione personalizzata](#) a pagina 19
2. Nella scheda **Opzioni**, selezionare la casella di spunta **Cerca virus di Macintosh**.

4.4.3 Scansione di tutti i file

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

È possibile abilitare Sophos Anti-Virus perché esegua la scansione di tutti i file, ma ciò influirà sulle prestazioni del computer.

1. Aprire le impostazioni per la scansione che si desidera configurare. Per informazioni su come svolgere questa operazione, consultare una delle seguenti sezioni:
 - [Configurazione della scansione in accesso](#) a pagina 8
 - [Configurazione della scansione dal menu del tasto destro del mouse](#) a pagina 17
 - [Configurazione di una scansione personalizzata](#) a pagina 19
2. Nella scheda **Opzioni**, selezionare la casella di spunta **Scansione di tutti i file**.

4.4.4 Ricerca di adware e PUA

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

1. Aprire le impostazioni per la scansione che si desidera configurare. Per informazioni su come svolgere questa operazione, consultare una delle seguenti sezioni:
 - [Configurazione della scansione in accesso](#) a pagina 8
 - [Configurazione della scansione dal menu del tasto destro del mouse](#) a pagina 17
 - [Configurazione di una scansione personalizzata](#) a pagina 19
2. Nella scheda **Opzioni**, selezionare la casella di spunta **Ricerca di adware e PUA**.

4.4.5 Ricerca di file sospetti

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Un *file sospetto* è un file che presenta una serie di caratteristiche comunemente, ma non esclusivamente, riscontrate in virus.

Per ricercare file sospetti:

1. Aprire le impostazioni per la scansione che si desidera configurare. Per informazioni su come svolgere questa operazione, consultare una delle seguenti sezioni:
 - [Configurazione della scansione in accesso](#) a pagina 8
 - [Configurazione della scansione dal menu del tasto destro del mouse](#) a pagina 17
 - [Configurazione di una scansione personalizzata](#) a pagina 19
2. Nella scheda **Opzioni**, selezionare la casella di spunta **Ricerca di file sospetti (HIPS)**.

4.5 Sophos Live Protection

4.5.1 Sophos Live Protection

Sophos Live Protection decide se un file sospetto rappresenta una minaccia e, quando ciò accade, agisce immediatamente secondo quanto specificato nella configurazione disinfezione di Sophos Anti-Virus.

Sophos Live Protection migliora il rilevamento di nuovo malware, senza il rischio di rilevamenti indesiderati. Questo avviene mediante ricerca istantanea in base alle più aggiornate versioni di malware conosciute. Quando viene identificato un nuovo malware, Sophos è in grado di inviare aggiornamenti entro pochi secondi.

Sophos Live Protection utilizza le seguenti opzioni:

■ **Abilita Live Protection**

Se la scansione antivirus su un computer ha identificato un file come sospetto, ma non riesce poi a determinare se sia pulito o malevolo, in base ai file di identità delle minacce (IDE) memorizzati nel computer, alcuni dati del file (come il checksum e altri attributi) vengono inviati a Sophos per un'ulteriore analisi.

La verifica “in-the-cloud” esegue la ricerca istantanea di un file sospetto nel database di SophosLabs. Se il file viene identificato come pulito o malevolo, la decisione viene inviata al computer e lo stato del file viene automaticamente aggiornato.

■ **Invio automatico dei file campione a Sophos**

Se un file viene considerato sospetto, ma non può essere identificato con certezza come malevolo solo in base ai suoi dati, è possibile permettere la richiesta da parte di Sophos di un campione del file. Se tale opzione è abilitata, e Sophos non detiene ancora un campione del file, il file verrà inviato automaticamente.

L'invio di file campione permette a Sophos di migliorare continuamente il rilevamento del malware senza il rischio di falsi positivi.

4.5.2 Attivazione e disattivazione delle opzioni di Sophos Live Protection

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se si appartiene al gruppo SophosAdministrator, è possibile attivare o disattivare Sophos Live Protection:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Sophos Live Protection.**

2. Nella finestra di dialogo **Sophos Live Protection**:

- Per attivare o disattivare l'invio a Sophos di dati dei file, selezionare o deselezionare la casella di spunta **Abilita Live Protection**.
- Per attivare o disattivare l'invio a Sophos di campioni di file, selezionare o deselezionare la casella di spunta **Invio automatico dei file campione a Sophos**.

Questa opzione è disponibile solamente se **Abilita Live Protection** è già stata selezionata.

Nota

Quando si invia il campione di un file a Sophos per la scansione in linea, insieme al campione vengono sempre inviati i dati del file.

4.5.3 Visualizzazione del log della scansione online di Sophos

Le informazioni sul file inviate a Sophos per la scansione online e gli aggiornamenti sullo stato del file dopo la scansione vengono registrate nel log della scansione per questo computer.

Se la scansione online di Sophos è abilitata, il log visualizzerà:

- Il percorso di ciascun file i cui dati sono stati inviati a Sophos
- L'orario in cui i dati sono stati inviati
- Se l'invio dei dati non è andato a buon fine, il motivo del problema, se conosciuto.
- Lo stato attuale del file (per esempio, "virus/spyware" se il file è stato identificato come malevolo).

Visualizzazione del log della scansione:

- Nella pagina **Home**, sotto **Antivirus ed HIPS**, cliccare su **Visualizza log antivirus e HIPS**. Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.

Dalla pagina log, è possibile copiare il log negli appunti, oppure inviarlo per e-mail o stamparlo.

Per trovare un testo specifico all'interno del log, cliccare su **Trova** e inserire il testo desiderato.

4.6 Web protection

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Sophos Anti-Virus fornisce una protezione avanzata contro le minacce del web, impedendo l'accesso a siti noti per la loro predisposizione ad ospitare malware. Blocca l'accesso dei computer a tali siti, mediante la ricerca dei loro dati in tempo reale all'interno del database online Sophos.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Web protection**.

2. Nella finestra di dialogo **Web protection**, selezionare o deselezionare **Blocca l'accesso ai siti web malevoli**. Per impostazione predefinita, l'accesso ai siti malevoli è bloccato.
Per informazioni su come autorizzare un sito web classificato come malevolo, consultare la sezione [Autorizzazione all'utilizzo di un sito web](#) a pagina 27.

4.7 Autorizzazione all'utilizzo di oggetti

4.7.1 Autorizzazione all'utilizzo di adware e PUA

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se si desidera eseguire adware o un'applicazione che Sophos Anti-Virus ha classificato come potenzialmente indesiderata, è possibile autorizzarla.

Per autorizzare l'utilizzo di adware e PUA:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Autorizzazione**.
2. Nella scheda **Adware o PUA**, nell'elenco **Adware e PUA noti**, selezionare adware o PUA.
3. Cliccare su **Aggiungi**.

L'adware o PUA appare nell'elenco **Adware o PUA autorizzati**.

Nota: è anche possibile autorizzare adware e PUA nel Gestore quarantena. Per informazioni su come svolgere questa operazione, consultare la sezione [Gestione di adware e PUA in quarantena](#) a pagina 30.

4.7.2 Blocco di adware e PUA autorizzati

Per evitare che adware e PUA attualmente autorizzati vengano eseguiti nel computer:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Autorizzazione**.
2. Nella scheda **Adware o PUA**, nell'elenco **Adware o PUA autorizzati**, selezionare adware o PUA che si desidera bloccare.
3. Cliccare su **Rimuovi**.

4.7.3 Autorizzazione all'uso di oggetti sospetti

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se si desidera autorizzare un oggetto che Sophos Anti-Virus ha classificato come sospetto, è possibile autorizzarlo nel modo seguente.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Autorizzazione**.
2. Cliccare sulla scheda relativa al tipo di oggetto rilevato (per es. **Buffer overflow**).

3. Cliccare sull'elenco **Noto** e selezionare l'oggetto sospetto.
4. Cliccare su **Aggiungi**.

L'oggetto sospetto compare nell'elenco **Autorizzato**.

Nota: è anche possibile autorizzare oggetti sospetti nel Gestore quarantena. Per informazioni su come fare ciò, consultare le seguenti sezioni:

- [Gestione di file sospetti in quarantena](#) a pagina 31
- [Gestione di comportamento sospetto in quarantena](#) a pagina 32

4.7.4 Preautorizzazione di oggetti sospetti

Se si desidera autorizzare un oggetto che Sophos Endpoint Security and Control non ha ancora classificato come sospetto, è possibile preautorizzarlo.

Per preautorizzare un oggetto sospetto:

1. Cliccare su **Home** > **Antivirus e HIPS** > **Configura antivirus e HIPS** > **Configura** > **Autorizzazione**.
2. Cliccare sulla scheda relativa al tipo di oggetto rilevato (per es. **Buffer overflow**).
3. Cliccare su **Nuova voce**.
4. Trovare l'oggetto sospetto e cliccarvi due volte.

L'oggetto sospetto compare nell'elenco **Autorizzato**.

4.7.5 Autorizzazione all'utilizzo di un sito web

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se si desidera sbloccare un sito classificato come maligno da Sophos, è possibile aggiungerlo all'elenco dei siti autorizzati. Le URL di un sito web autorizzato non vengono verificate dal filtro web online di Sophos.



Attenzione: Autorizzare un sito web classificato come maligno potrebbe esporre a minacce, assicurarsi che l'accesso al sito sia sicuro prima di autorizzarlo.

Come autorizzare un sito web:

1. Cliccare su **Home** > **Antivirus e HIPS** > **Configura antivirus e HIPS** > **Configura** > **Autorizzazione**.
2. Cliccare sulla scheda **Sito web**.
3. Fare clic su **Aggiungi** per aggiungere un sito web all'elenco dei siti autorizzati, utilizzando uno dei formati disponibili.

E' possibile aggiungere un sito web immettendo il suo dominio, indirizzo IP, o indirizzo IP con maschera di sottorete.

Il sito web compare nell'elenco **Siti web autorizzati**.

4.8 Gestione degli oggetti in quarantena

4.8.1 Gestore quarantena

Il Gestore quarantena consente di gestire gli oggetti individuati mediante la scansione e non eliminati automaticamente durante la stessa. Ciascun oggetto viene conservato qui per una delle ragioni elencate di seguito.

- Non è stata scelta alcuna opzione di disinfezione (disinfezione, cancellazione, spostamento) per il tipo di scansione durante la quale è stato individuato l'oggetto.
- È stata scelta un'opzione di disinfezione per il tipo di scansione durante la quale è stato individuato l'oggetto, ma l'opzione non ha funzionato correttamente.
- L'oggetto ha un'infezione multipla e contiene ancora altre minacce.
- La minaccia è stata rilevata solo parzialmente. Per rilevarla in maniera completa, è necessaria una scansione completa del computer. Per maggiori informazioni su come effettuare tale operazione, consultare [Esecuzione della scansione completa del computer](#) a pagina 17
- L'oggetto manifesta un comportamento sospetto.
- L'oggetto è un'applicazione controllata.

Nota: adware, PUA e infezioni multicomponente rilevate durante la scansione in accesso sono sempre elencate nel Gestore quarantena. La disinfezione automatica di adware, PUA e infezioni multicomponente non è disponibile per la scansione in accesso.

L'opzione di disinfezione potrebbe non aver funzionato correttamente a causa di diritti di accesso insufficienti. Se si dispone di diritti maggiori, è possibile utilizzare il Gestore quarantena per gestire l'oggetto o gli oggetti.

Le minacce rilevate durante la scansione delle pagine web non sono elencate nel Gestore quarantena perché non vengono scaricate nel computer. Pertanto, in tali casi non è necessaria alcuna azione.

4.8.2 Gestione di virus e spyware in quarantena

Nota: con il termine *virus* ci si riferisce a qualsiasi virus, worm o trojan o ad altro software malevolo.

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Gestisci elementi messi in quarantena**. Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Mostra**, cliccare su **Virus/spyware**.

Informazioni relative a ciascun oggetto visualizzato nelle colonne:

Nome visualizza l'identità rilevata da Sophos Anti-Virus. Per ulteriori informazioni sul virus e spyware, cliccare sull'identità. Sophos Anti-Virus si connette all'analisi del virus o spyware disponibile sul sito web di Sophos.

Dettagli visualizza il nome e la posizione dell'oggetto. Se l'oggetto è associato a un rootkit, viene visualizzato come "Nascosto". Se accanto al nome del file appare il collegamento **dettagli**,

significa che l'oggetto presenta un'infezione multicomponente. Cliccare sul link per visualizzare la lista degli altri componenti che formano l'infezione. Se uno dei componenti è associato a un rootkit, la finestra di dialogo indica che alcuni componenti sono nascosti.

Azioni disponibili visualizza le azioni eseguibili sull'oggetto. A meno che l'oggetto non sia nascosto, sono disponibili tre azioni: Disinfetta, Cancella e Sposta, come descritto sotto. Cliccando su una delle azioni, l'azione viene eseguita sull'oggetto dopo la conferma. I file nascosti possono essere solo disinfettati.

Gestione degli oggetti infetti

Per gestire virus e spyware, utilizzare i pulsanti descritti sotto.

Seleziona tutto/Deseleziona tutto

Cliccare su questi pulsanti per selezionare oppure per deselezionare tutti gli oggetti. Ciò consente di eseguire la stessa azione su un gruppo di oggetti. Per selezionare o deselezionare un determinato oggetto, spuntare la casella alla sinistra del tipo di oggetto.

Cancella dall'elenco

Cliccare su questa opzione per rimuovere dalla lista gli oggetti selezionati, se si è certi che non contengono virus o spyware. Comunque gli oggetti non vengono cancellati dal disco.

Esegui azione

Cliccare su questa opzione per visualizzare un elenco di azioni eseguibili sugli oggetti selezionati.

- Cliccare su **Disinfetta** per rimuovere un virus o spyware dagli oggetti selezionati. La disinfezione dei documenti non annulla le modifiche che il virus può aver apportato al documento.

Nota: per una rimozione completa dal computer di alcuni virus e spyware formati da diversi componenti, sarà necessario riavviare il computer. In questo caso viene data la possibilità di riavviare il computer immediatamente o in un secondo tempo. Le operazioni conclusive di rimozione saranno eseguite dopo il riavvio del computer.

- Cliccare su **Cancella** per cancellare gli oggetti selezionati dal computer. Utilizzare questa funzione con cautela.
- Cliccare su **Sposta** per spostare gli oggetti selezionati in un'altra cartella. Gli oggetti vengono spostati nella cartella che è stata specificata durante l'impostazione della disinfezione. Spostando un file eseguibile si riducono le probabilità che venga eseguito. Utilizzare questa funzione con cautela.



Attenzione: talvolta, se si cancella o si sposta un file infetto, il computer può smettere di funzionare correttamente, perché non riesce a trovare il file. Inoltre, un file infetto può essere solo parte di un'infezione multipla, nel qual caso la sua cancellazione o il suo spostamento non comporterà la disinfezione del computer. In questo caso, rivolgersi al supporto tecnico di Sophos per ricevere assistenza nella gestione degli oggetti.

Per informazioni su come contattare il supporto tecnico, consultare la sezione [Supporto tecnico](#) a pagina 94.

Per configurare quali azioni poter svolgere, consultare la sezione [Configurazione dei diritti utente per il Gestore quarantena](#) a pagina 6

4.8.3 Gestione di adware e PUA in quarantena

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Gestisci elementi messi in quarantena**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Mostra**, cliccare su **Adware o PUA**.

Informazioni relative a ciascun oggetto visualizzato nelle colonne:

Nome visualizza l'identità rilevata da Sophos Anti-Virus. Per ulteriori informazioni sull'adware o PUA, cliccare sull'identità. Sophos Anti-Virus si connette quindi all'analisi dell'adware o PUA disponibile sul sito web di Sophos.

Dettagli visualizza il sottotipo di adware e PUA. Se l'oggetto è associato a un rootkit, viene visualizzato come "Nascosto". Se accanto al sottotipo appare il collegamento **dettagli**, significa che l'oggetto è un adware e PUA multicomponente. Cliccare sul link per visualizzare l'elenco degli altri componenti che formano l'adware o PUA. Se uno dei componenti è associato a un rootkit, la finestra di dialogo indica che alcuni componenti sono nascosti.

Azioni disponibili visualizza le azioni eseguibili sull'oggetto. Sono disponibili due azioni: autorizzazione e rimozione, come descritto sotto. Cliccando su una delle azioni, l'azione viene eseguita sull'oggetto dopo la conferma.

Gestione di adware e PUA

Per gestire adware e PUA, utilizzare i pulsanti descritti sotto.

Seleziona tutto/Deseleziona tutto

Cliccare su questi pulsanti per selezionare oppure per deselezionare tutti gli oggetti. Ciò consente di eseguire la stessa azione su un gruppo di oggetti. Per selezionare o deselezionare un determinato oggetto, spuntare la casella alla sinistra del tipo di oggetto.

Cancella dall'elenco

Cliccare su questa opzione per rimuovere dall'elenco gli oggetti selezionati, se attendibili. Comunque gli oggetti non vengono cancellati dal disco.

Esegui azione

Cliccare su questa opzione per visualizzare un elenco di azioni eseguibili sugli oggetti selezionati.

- Cliccare su **Autorizza** per autorizzare nel computer gli oggetti selezionati, se attendibili. Tale opzione aggiunge gli oggetti all'elenco degli adware e PUA autorizzati in modo che Sophos Anti-Virus non ne impedisca l'esecuzione nel computer.
- Cliccare su **Disinfetta** per rimuovere dal computer, per tutti gli utenti, tutti i componenti noti degli oggetti selezionati. Per rimuovere dal computer adware e PUA, è necessario che l'utente appartenga a entrambi i gruppi Windows Administrators e SophosAdministrator.

Nota: per una rimozione completa dal computer di alcuni adware e PUA formati da diversi componenti, sarà necessario riavviare il computer. In questo caso viene data la possibilità di riavviare il computer immediatamente o in un secondo tempo. Le operazioni conclusive di rimozione saranno eseguite dopo il riavvio del computer.

Per configurare quali azioni poter svolgere, consultare la sezione [Configurazione dei diritti utente per il Gestore quarantena](#) a pagina 6

Per visualizzare la lista degli adware e PUA noti e autorizzati, cliccare su **Configura autorizzazione**.

4.8.4 Gestione di file sospetti in quarantena

Un *file sospetto* è un file che presenta una serie di caratteristiche comunemente, ma non esclusivamente, riscontrate in virus.

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Gestisci elementi messi in quarantena**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Mostra**, cliccare su **File sospetti**.

Informazioni relative a ciascun oggetto visualizzato nelle colonne:

Nome visualizza l'identità rilevata da Sophos Anti-Virus. Per ulteriori informazioni sul file sospetto, cliccare sull'identità. Sophos Anti-Virus si connette all'analisi del file sospetto disponibile sul sito web di Sophos.

Dettagli visualizza il nome e la posizione dell'oggetto. Se l'oggetto è associato a un rootkit, viene visualizzato come "Nascosto".

Azioni disponibili visualizza le azioni eseguibili sull'oggetto. A meno che l'oggetto non sia nascosto, sono disponibili tre azioni: autorizza, cancella e sposta, come descritto sotto. Cliccando su una delle azioni, l'azione viene eseguita sull'oggetto dopo la conferma. I file nascosti possono essere solo autorizzati.

Gestione dei file sospetti

Per gestire i file sospetti, utilizzare i pulsanti descritti sotto.

Seleziona tutto/Deseleziona tutto

Cliccare su questi pulsanti per selezionare oppure per deselezionare tutti gli oggetti. Ciò consente di eseguire la stessa azione su un gruppo di oggetti. Per selezionare o deselezionare un determinato oggetto, spuntare la casella alla sinistra del tipo di oggetto.

Cancella dall'elenco

Cliccare su questa opzione per rimuovere dall'elenco gli oggetti selezionati, se attendibili. Comunque gli oggetti non vengono cancellati dal disco.

Esegui azione

Cliccare su questa opzione per visualizzare un elenco di azioni eseguibili sugli oggetti selezionati.

- Cliccare su **Autorizza** per autorizzare nel computer gli oggetti selezionati, se attendibili. Tale opzione aggiunge gli oggetti alla lista degli oggetti sospetti autorizzati in modo che Sophos Anti-Virus non ne impedisca l'accesso.
- Cliccare su **Cancella** per cancellare gli oggetti selezionati dal computer. Utilizzare questa funzione con cautela.

- Cliccare su **Sposta** per spostare gli oggetti selezionati in un'altra cartella. Gli oggetti vengono spostati nella cartella che è stata specificata durante l'impostazione della disinfezione. Spostando un file eseguibile si riducono le probabilità che venga eseguito. Utilizzare questa funzione con cautela.



Attenzione: talvolta, se si cancella o si sposta un file infetto, il computer può smettere di funzionare correttamente, perché non riesce a trovare il file.

Per configurare quali azioni poter svolgere, consultare la sezione [Configurazione dei diritti utente per il Gestore quarantena](#) a pagina 6

Per visualizzare l'elenco dei file sospetti autorizzati, cliccare su **Configura autorizzazione**.

4.8.5 Gestione di comportamento sospetto in quarantena

Il termine *Comportamento sospetto* indica un'attività apparentemente malevola.

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Gestisci elementi messi in quarantena**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Mostra**, cliccare su **Comportamento sospetto**.

Informazioni relative a ciascun oggetto visualizzato nelle colonne:

Nome visualizza l'identità rilevata da Sophos Anti-Virus. Per ulteriori informazioni sul comportamento, cliccare sull'identità. Sophos Anti-Virus si connette quindi all'analisi del comportamento disponibile sul sito web di Sophos.

Dettagli visualizza il nome e la posizione dell'oggetto.

Azioni disponibili visualizza le azioni eseguibili sull'oggetto. Se è stato abilitato il blocco del comportamento sospetto è disponibile una sola azione: autorizzazione, come spiegato di seguito. Cliccando sull'azione, essa viene eseguita sull'oggetto dopo la conferma.

Gestione del comportamento sospetto

Per gestire il comportamento sospetto, utilizzare i pulsanti descritti sotto.

Seleziona tutto/Deseleziona tutto

Cliccare su questi pulsanti per selezionare oppure per deselezionare tutti gli oggetti. Ciò consente di eseguire la stessa azione su un gruppo di oggetti. Per selezionare o deselezionare un determinato oggetto, spuntare la casella alla sinistra del tipo di oggetto.

Cancella dall'elenco

Cliccare su questa opzione per rimuovere dall'elenco gli oggetti selezionati, se attendibili. Comunque gli oggetti non vengono cancellati dal disco.

Esegui azione

Cliccare su questa opzione per visualizzare un elenco di azioni eseguibili sugli oggetti selezionati.

- Cliccare su **Autorizza** per autorizzare nel computer gli oggetti selezionati, se attendibili. Tale opzione aggiunge gli oggetti all'elenco degli oggetti sospetti autorizzati in modo che Sophos Anti-Virus non ne impedisca l'esecuzione.

Per configurare quali azioni poter svolgere, consultare la sezione [Configurazione dei diritti utente per il Gestore quarantena](#) a pagina 6.

Per visualizzare l'elenco dei comportamenti sospetti autorizzati, cliccare su **Configura autorizzazione**.

4.8.6 Gestione di applicazioni controllate in quarantena

Un'*applicazione controllata* è un'applicazione la cui esecuzione nel computer è impedita dai criteri di sicurezza aziendali.

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Gestisci elementi messi in quarantena**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Mostra**, cliccare su **Applicazioni controllate**.

Informazioni relative a ciascun oggetto visualizzato nelle colonne:

Nome visualizza l'identità rilevata da Sophos Anti-Virus. Per ulteriori informazioni sull'applicazione controllata, cliccare sull'identità. Sophos Anti-Virus si connette quindi all'analisi dell'applicazione controllata disponibile sul sito web di Sophos.

Dettagli visualizza il sottotipo di applicazione controllata. Se accanto al sottotipo appare il collegamento **dettagli**, cliccarvi sopra per visualizzare l'elenco degli altri componenti che formano l'applicazione controllata.

Azioni disponibili visualizza le azioni eseguibili sull'oggetto. Tuttavia, non è disponibile alcuna azione per le applicazioni controllate a parte la cancellazione dell'oggetto dall'elenco, come descritto sotto.

Gestione delle applicazioni controllate

Per gestire le applicazioni controllate, utilizzare i pulsanti descritti sotto.

Seleziona tutto/Deseleziona tutto

Cliccare su questi pulsanti per selezionare oppure per deselezionare tutti gli oggetti. Ciò consente di eseguire la stessa azione su un gruppo di oggetti. Per selezionare o deselezionare un determinato oggetto, spuntare la casella alla sinistra del tipo di oggetto.

Cancella dall'elenco

Cliccare su questa opzione per rimuovere gli oggetti selezionati dall'elenco. Comunque gli oggetti non vengono cancellati dal disco. È necessario che le applicazioni controllate vengano autorizzate dalla console centrale prima di poterle utilizzare.

4.9 Configurazione degli allarmi

4.9.1 Configurazione della messaggistica desktop relativa all'antivirus

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per consentire a Sophos Anti-Virus di visualizzare i messaggi sul desktop quando viene rilevata una minaccia, procedere come segue. Ciò vale soltanto per la scansione in accesso.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Allarmi > Messaggistica**.
2. Nella finestra di dialogo **Messaggistica**, cliccare sulla scheda **Messaggistica desktop**. Impostare le opzioni come descritto di seguito.

Abilitazione della messaggistica desktop

Selezionare questa opzione per consentire a Sophos Anti-Virus di visualizzare i messaggi sul desktop quando viene rilevata una minaccia.

Messaggi da inviare

Selezionare gli eventi per i quali si desidera che Sophos Anti-Virus visualizzi i messaggi sul desktop.

Messaggio definito dall'utente

In questa casella di testo è possibile digitare un messaggio che sarà aggiunto alla fine del messaggio standard.

4.9.2 Configurazione degli allarmi e-mail di antivirus

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per consentire a Sophos Anti-Virus di inviare degli allarmi e-mail quando viene rilevata una minaccia o quando si verifica un errore, procedere nel modo seguente. Ciò vale per la scansione in accesso, per la scansione su richiesta e per la scansione dal menu del tasto destro del mouse.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Allarmi > Messaggistica**.

2. Nella finestra di dialogo **Messaggistica**, cliccare sulla scheda **Allarmi e-mail**. Impostare le opzioni come descritto di seguito.

Abilitazione allarmi e-mail

Selezionare questa opzione per consentire a Sophos Anti-Virus di inviare degli allarmi e-mail.

Messaggi da inviare

Selezionare gli eventi per i quali si desidera che Sophos Anti-Virus invii degli allarmi e-mail. Gli **errori di scansione** sono gli errori che si verificano quando a Sophos Anti-Virus viene negato l'accesso a un oggetto che tenta di esaminare.

Sophos Anti-Virus non invia allarmi e-mail relativi alle minacce rilevate dalla scansione delle pagine web perché tali minacce non vengono scaricate nel computer. Pertanto, in tali casi non è necessaria alcuna azione.

Destinatari

Cliccare su **Aggiungi** o **Rimuovi** per aggiungere o rimuovere, rispettivamente, gli indirizzi e-mail ai quali devono essere inviati gli allarmi e-mail. Cliccare su **Modifica** per modificare un indirizzo e-mail che è stato aggiunto.

Configura SMTP

Cliccare su questa opzione per modificare le impostazioni del server SMTP e la lingua degli allarmi e-mail (v. la tabella di seguito).

Configura impostazioni SMTP	
Server SMTP	Nella casella di testo, digitare il nome host o l'indirizzo IP del server SMTP. Cliccare su Prova per verificare che sia stata stabilita la connessione con il server SMTP (<i>non</i> viene inviata un'e-mail di prova).
Indirizzo SMTP "mittente"	Nella casella di testo, digitare un indirizzo e-mail al quale possono essere inviati bounce e messaggi di mancato recapito.
Indirizzo SMTP "rispondi a"	Poiché gli allarmi e-mail vengono inviati automaticamente dal sistema, è possibile digitare nella casella di testo un indirizzo e-mail al quale inviare gli allarmi stessi.
Lingua	Cliccare sulla freccia del menu a discesa e selezionare la lingua nella quale devono essere inviati gli allarmi e-mail.

4.9.3 Configurazione della messaggistica SNMP relativa all'antivirus

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per consentire a Sophos Anti-Virus di inviare dei messaggi SNMP quando viene rilevata una minaccia o quando si verifica un errore, procedere nel modo seguente. Ciò vale per la scansione in accesso, per la scansione su richiesta e per la scansione dal menu del tasto destro del mouse.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Allarmi > Messaggistica**.
2. Nella finestra di dialogo **Messaggistica**, cliccare sulla scheda **Messaggistica SNMP**. Impostare le opzioni come descritto di seguito.

Abilita messaggistica SNMP

Selezionare questa opzione per consentire a Sophos Anti-Virus di inviare dei messaggi SNMP.

Messaggi da inviare

Selezionare gli eventi per i quali si desidera che Sophos Anti-Virus invii i messaggi SNMP. Gli **errori di scansione** sono gli errori che si verificano quando a Sophos Anti-Virus viene negato l'accesso a un oggetto che tenta di esaminare.

Sophos Anti-Virus non invia messaggi SNMP relativi alla minacce rilevate dalla scansione delle pagine web perché tali minacce non vengono scaricate nel computer. Pertanto, in tali casi non è necessaria alcuna azione.

Destinazione trap SNMP

Nella casella di testo, digitare l'indirizzo IP o il nome del computer al quale vengono inviati gli allarmi.

Nome comunità SNMP

Nella casella di testo, digitare il nome della comunità SNMP.

Prova

Cliccare su questo pulsante per inviare un messaggio SNMP di prova alla destinazione del trap SNMP che è stata specificata.

4.9.4 Configurazione del log eventi dell'antivirus

Per consentire a Sophos Anti-Virus di aggiungere gli allarmi al log degli eventi di Windows 2000 o successivo quando viene rilevata una minaccia o si verifica un errore, procedere nel modo seguente. Ciò vale per la scansione in accesso, per la scansione su richiesta e per la scansione dal menu del tasto destro del mouse.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Allarmi > Messaggistica**.

2. Nella finestra di dialogo **Messaggistica**, cliccare sulla scheda **Log eventi**. Impostare le opzioni come descritto di seguito.

Abilita log eventi

Selezionare questa opzione per consentire a Sophos Anti-Virus di inviare i messaggi al log degli eventi di Windows.

Messaggi da inviare

Selezionare gli eventi per i quali si desidera che Sophos Anti-Virus invii i messaggi. Gli **errori di scansione** sono gli errori che si verificano quando a Sophos Anti-Virus viene negato l'accesso a un oggetto che tenta di esaminare.

Sophos Anti-Virus non invia messaggi relativi alla minacce rilevate dalla scansione delle pagine web perché tali minacce non vengono scaricate nel computer. Pertanto, in tali casi non è necessaria alcuna azione.

4.10 Log scansione

4.10.1 Configurazione del log della scansione

Il log della scansione del computer si trova nel seguente percorso:

```
C:\Documents and Settings\All Users\Dati  
applicazioni\Sophos\Sophos  
Anti-Virus\logs\SAV.txt
```

1. Cliccare su **Home > Antivirus e HIPS > Visualizza log antivirus e HIPS > Configura log**.
2. Nella finestra di dialogo **Configura log del computer**, impostare le opzioni come descritto sotto.

Livello di log

Per evitare che venga creato il log, cliccare su **Nessuno**. Per registrare le informazioni di riepilogo, i messaggi di errore e così via, cliccare su **Normale**. Per registrare la maggior parte delle informazioni, inclusi i file esaminati, le fasi principali di una scansione e così via, cliccare su **Dettagliato**.

Archiviazione del log

Affinché il file di log venga archiviato ogni mese, selezionare **Consenti archiviazione**. I file di archivio sono memorizzati nella stessa cartella del file di log. Selezionare il **Numero dei file di archivio** da memorizzare prima di cancellare il meno recente. Selezionare **Comprimi log** per ridurre le dimensioni del file di log.

4.10.2 Visualizzazione del log della scansione

- ❖ Nella pagina **Home**, sotto **Antivirus ed HIPS**, cliccare su **Visualizza log antivirus e HIPS**. Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.

Dalla pagina log, è possibile copiare il log negli appunti, oppure inviarlo per e-mail o stamparlo.

Per trovare un testo specifico all'interno del log, cliccare su **Trova** e inserire il testo desiderato.

4.11 Disinfezione

4.11.1 Disinfezione

La disinfezione elimina le minacce presenti nel computer tramite una delle seguenti azioni:

- Rimozione di un virus da un file o boot sector
- Spostamento o cancellazione di un file sospetto
- Cancellazione di adware o PUA

La disinfezione non annulla le azioni eventualmente già compiute dalla minaccia.

La disinfezione dei documenti non annulla le modifiche che il virus può aver apportato al documento.

La disinfezione dei programmi deve essere usata soltanto come misura temporanea. È poi necessario sostituire i programmi disinfettati a partire dai dischi originali o da una copia di backup pulita.

La disinfezione non è disponibile per le minacce rilevate tramite la scansione della pagina web perché non vengono scaricate nel computer. In questo caso non è necessario intraprendere alcuna azione.

4.11.2 Impostazione della rimozione automatica di virus e spyware

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Quando è attiva la scansione in accesso, oppure quando si esegue una scansione su richiesta o dal menu del tasto destro del mouse, Sophos Anti-Virus è in grado di eseguire automaticamente le seguenti operazioni:

- Disinfezione di molti oggetti infetti
- Neutralizzazione di oggetti infetti in modi diversi dalla disinfezione.

Nota: la rimozione automatica di infezioni multicomponente non è disponibile per la scansione in accesso. Per rimuovere dal computer questo tipo di infezioni, utilizzare il Gestore quarantena. Per informazioni sul Gestore quarantena, consultare la sezione [Gestione di adware e PUA in quarantena](#) a pagina 30.

Tutte le azioni eseguite da Sophos Anti-Virus sugli oggetti infetti vengono registrate nel log del computer o nel log della scansione su richiesta. Per informazioni, consultare la sezione [Visualizzazione del log della scansione](#) a pagina 37 o [Visualizzazione del log per la scansione personalizzata](#) a pagina 21.

Per una rimozione completa dal computer di alcune infezioni multicomponente, sarà necessario riavviare il computer. In questo caso viene data la possibilità di riavviare il computer immediatamente o in un secondo tempo. Le operazioni conclusive di rimozione saranno eseguite dopo il riavvio del computer.

1. Aprire le impostazioni per la scansione che si desidera configurare. Per informazioni su come svolgere questa operazione, consultare una delle seguenti sezioni:
 - [Configurazione della scansione in accesso](#) a pagina 8
 - [Configurazione della scansione dal menu del tasto destro del mouse](#) a pagina 17
 - [Configurazione di una scansione personalizzata](#) a pagina 19
2. Cliccare sulla scheda **Disinfezione**.
3. In **Virus/spyware**, selezionare la casella di spunta **Disinfetta automaticamente gli oggetti contenenti virus o spyware** per consentire a Sophos Anti-Virus di disinfettare settori di avvio dei floppy disk, documenti, programmi e qualsiasi altro oggetto selezionato per la scansione.

La disinfezione dei documenti non annulla le modifiche che il virus può aver apportato al documento. Consultare [Informazioni sulla disinfezione](#) a pagina 41 per sapere come visualizzare, sul sito web di Sophos, i dettagli sugli effetti secondari dei virus.
4. Sophos Anti-Virus può neutralizzare un file infetto in modi diversi dalla disinfezione. Se non si utilizza la disinfezione automatica, o se questa non riesce, è possibile selezionare altre azioni che si desidera far eseguire a Sophos Anti-Virus sui file infetti:
 - Cliccare su **Nega accesso** per impedire che il file venga aperto, copiato, o spostato.
 - Cliccare su **Cancella** per eliminare il file.
 - Cliccare su **Nega accesso e sposta su** per spostare il file in un'altra cartella, selezionabile tramite il pulsante **Sfoggia**.

Spostando un file eseguibile si riducono le probabilità che venga eseguito.

Non è possibile spostare automaticamente i componenti di un'infezione multicomponente.



Attenzione: queste opzioni vanno utilizzate soltanto su consiglio del supporto tecnico di Sophos. Utilizzare altrimenti il Gestore quarantena per disinfettare il computer dai virus e spyware rilevati da Sophos Anti-Virus. Per informazioni sul Gestore quarantena, consultare la sezione [Gestione di adware e PUA in quarantena](#) a pagina 30.

Nota: per sapere come disinfettare il computer da virus/spyware utilizzando il Gestore quarantena, consultare la sezione [Gestione di virus e spyware in quarantena](#) a pagina 28 .

4.11.3 Impostazione della rimozione automatica di adware e PUA

Quando si esegue una scansione su richiesta o dal menu del tasto destro del mouse, Sophos Anti-Virus può rimuovere automaticamente dal computer adware e PUA.

Nota: la rimozione automatica di adware e PUA non è disponibile per la scansione in accesso. Per rimuovere dal computer adware e PUA indesiderati, utilizzare il Gestore quarantena. Per informazioni sul Gestore quarantena, consultare la sezione [Gestione di adware e PUA in quarantena](#) a pagina 30.

Tutte le azioni eseguite da Sophos Anti-Virus su adware e PUA vengono registrate nel log del computer o nel log della scansione su richiesta. Per informazioni, consultare la sezione

[Visualizzazione del log della scansione](#) a pagina 37 o [Visualizzazione del log per la scansione personalizzata](#) a pagina 21.

Per una rimozione completa dal computer di alcuni adware e PUA multicomponente, sarà necessario riavviare il computer. In questo caso viene data la possibilità di riavviare il computer immediatamente o in un secondo tempo. Le operazioni conclusive di rimozione saranno eseguite dopo il riavvio del computer.

1. Aprire le impostazioni per la scansione che si desidera configurare. Per informazioni su come svolgere questa operazione, consultare una delle seguenti sezioni:
 - [Configurazione della scansione in accesso](#) a pagina 8
 - [Configurazione della scansione dal menu del tasto destro del mouse](#) a pagina 17
 - [Configurazione di una scansione personalizzata](#) a pagina 19
2. Cliccare sulla scheda **Disinfezione**.
3. In **Adware e PUA**, selezionare **Disinfetta automaticamente adware e PUA** per consentire a Sophos Anti-Virus di rimuovere dal computer tutti i componenti noti di adware e PUA per tutti gli utenti.

La rimozione non annulla le modifiche già apportate da adware o PUA. (Per scoprire come visualizzare sul sito web di Sophos i dettagli sugli effetti secondari di adware o PUA, consultare la sezione [Informazioni sulla disinfezione](#) a pagina 41).

Nota: per sapere come disinfettare il computer da adware e PUA utilizzando Gestore quarantena, consultare la sezione [Gestione di adware e PUA in quarantena](#) a pagina 30.

4.11.4 Impostazione della rimozione automatica di file sospetti

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Quando è attiva la scansione in accesso, oppure quando si esegue una scansione su richiesta o dal menu del tasto destro del mouse, Sophos Anti-Virus può cancellare o spostare automaticamente i file sospetti.

Un *file sospetto* è un file che presenta una serie di caratteristiche comunemente, ma non esclusivamente, riscontrate in virus.

1. Aprire le impostazioni per la scansione che si desidera configurare. Per informazioni su come svolgere questa operazione, consultare una delle seguenti sezioni:
 - [Configurazione della scansione in accesso](#) a pagina 8
 - [Configurazione della scansione dal menu del tasto destro del mouse](#) a pagina 17
 - [Configurazione di una scansione personalizzata](#) a pagina 19
2. Cliccare sulla scheda **Disinfezione**.

3. In **File sospetti**, impostare le opzioni come descritto di seguito.

- Cliccare su **Nega accesso** per impedire che il file venga aperto, copiato, o spostato.
- Cliccare su **Cancella** per eliminare il file.
- Cliccare su **Nega accesso e sposta su** per spostare il file in un'altra cartella selezionabile tramite il pulsante **Sfoggia**. Spostando un file eseguibile si riducono le probabilità che venga eseguito.



Attenzione: queste opzioni vanno utilizzate soltanto su consiglio del supporto tecnico di Sophos. Utilizzare altrimenti il Gestore quarantena per disinfettare il computer dai virus e spyware rilevati da Sophos Anti-Virus. Per informazioni sul Gestore quarantena, consultare la sezione [Gestione di file sospetti in quarantena](#) a pagina 31.

Nota: per sapere come disinfettare il computer da file sospetti utilizzando il Gestore quarantena, consultare la sezione [Gestione di file sospetti in quarantena](#) a pagina 31.

4.11.5 Informazioni sulla disinfezione

Quando nel computer viene rilevata una minaccia, è molto importante controllarne l'analisi sul sito web di Sophos per avere informazioni e consigli sulla disinfezione. E' possibile effettuare questa operazione da:

- Allarme sul desktop (scansione in accesso)
- Finestra di dialogo che mostra l'avanzamento della scansione (scansione su richiesta e scansione dal menu del tasto destro del mouse)
- Gestore quarantena (tutti i tipi di scansione)

Informazioni tramite l'allarme sul desktop

Se nel computer è abilitata la scansione in accesso, Sophos Anti-Virus visualizza un allarme sul desktop ogni volta che rileva una minaccia. Nella finestra di messaggio, cliccare sul nome della minaccia sulla quale si desidera ottenere informazioni.

Sophos Anti-Virus si collega all'analisi della minaccia sul sito web di Sophos.

Informazioni tramite la finestra di avanzamento della scansione

Per la scansione su richiesta o la scansione dal menu del tasto destro del mouse, nel log visualizzato nella finestra di avanzamento della scansione (o nella finestra di riepilogo della scansione, visualizzata al termine della scansione), cliccare sul nome della minaccia sulla quale si desidera ottenere informazioni.

Sophos Anti-Virus si collega all'analisi della minaccia sul sito web di Sophos.

Informazioni tramite Gestore quarantena

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Gestisci elementi messi in quarantena**. Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nella colonna **Nome**, cliccare sul nome della minaccia sulla quale si desidera ottenere informazioni.

Sophos Anti-Virus si collega all'analisi della minaccia sul sito web di Sophos.

5 Utilizzo di Sophos Device Control

5.1 Controllo dispositivi nel computer

Se non viene utilizzata la console di gestione per amministrare Sophos Endpoint Security and Control sul computer, la funzionalità del controllo dispositivi *non* sarà inclusa.

Il controllo dispositivi viene abilitato o disabilitato dalla console di gestione. Se il controllo dispositivi è abilitato, impedirà la connessione di un dispositivo al computer anche se eseguito per motivi di manutenzione o per la risoluzione di alcuni problemi. Se questo è il caso, in tale computer è possibile disabilitare temporaneamente il controllo dispositivi. Per informazioni, consultare la sezione [Disabilitazione temporanea del controllo dei dispositivi](#) a pagina 42.

5.2 Tipi di dispositivo controllabili

Il controllo dispositivi blocca o consente tre tipi di dispositivi presenti nel computer: *Memorizzazione, rete e short range*.

Memorizzazione

- Dispositivo di memoria rimovibile (per esempio unità flash USB, lettori di schede per PC, unità hard disk esterne)
- Unità disco ottico (unità CD-ROM/DVD/Blu-Ray)
- Unità floppy disk.
- Dispositivi di memorizzazione rimovibili sicuri (per esempio unità flash USB a crittografia basata su hardware)

Rete

- Modem
- Wireless (interfaccia Wi-Fi, 802.11 standard)

Il criterio di controllo del dispositivo per questo computer potrebbe essere nella modalità **Block bridged**, che disattiva le schede di rete wireless o modem quando il computer è collegato a una rete fisica (di solito, attraverso una connessione Ethernet). Quando il computer è scollegato dalla rete fisica, le schede di rete wireless o modem vengono riabilitati direttamente.

Short range

- Interfacce Bluetooth
- Infrarossi (Interfaccia infrarossi IrDA)

5.3 Disabilitazione temporanea del controllo dei dispositivi

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se si è membri del gruppo Sophos Administrator e si desidera connettere un dispositivo al computer per motivi di manutenzione o per la risoluzione di alcuni problemi (per es. per installare un software da CD), è possibile disattivare temporaneamente il controllo dei dispositivi.

Per disabilitare il controllo dei dispositivi nel computer:

1. Nel menu **Configura**, cliccare su **Controllo dispositivi**.
2. Deselezionare la casella di spunta **Abilita Sophos Device Control**.

5.4 Configurazione del log del controllo dispositivi

1. Nel menu **Configura**, cliccare su **Controllo dispositivi**.
2. Sotto **Livello di log**, selezionare una delle seguenti opzioni:
 - Cliccare su **Nessuno** per impedire che venga creato il log.
 - Per registrare le informazioni di riepilogo, i messaggi di errore e così via, cliccare su **Normale**.
 - Cliccare su **Dettagliato** per ottenere informazioni relative a molte più attività del normale. Utilizzare questa impostazione solo quando è richiesto un log dettagliato per la risoluzione dei problemi, dal momento che le dimensioni del log cresceranno rapidamente.
3. Sotto **Archiviazione log**, seguire le istruzioni a schermo.

5.5 Visualizzazione del log del controllo dispositivi

- ❖ Nella **Home page**, sotto **Controllo dispositivi**, cliccare su **Visualizzare log controllo dispositivi**.

Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.

Dalla pagina log, è possibile copiare il log negli appunti, oppure inviarlo per e-mail o stamparlo.

Per trovare un testo specifico all'interno del log, cliccare su **Trova** e inserire il testo desiderato.

6 Utilizzo di Sophos Data Control

6.1 Controllo dati nel computer

Se non viene utilizzata la console di gestione per amministrare Sophos Endpoint Security and Control sul computer, la funzionalità del controllo dati *non* sarà inclusa.

Il controllo dati viene abilitato o disabilitato da un criterio rilasciato da una console di gestione. Tuttavia, in quanto membri del gruppo SophosAdministrator, è possibile disabilitare temporaneamente il controllo dati nel computer per motivi di manutenzione o per la risoluzione di alcuni problemi: Per informazioni, consultare la sezione [Disabilitazione temporanea del controllo dati](#) a pagina 44.

6.2 Disabilitazione temporanea del controllo dati

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

In quanto membri del gruppo SophosAdministrator, è possibile disabilitare temporaneamente il controllo dati nel computer per motivi di manutenzione o per la risoluzione di alcuni problemi.

1. Nel menu **Configura**, cliccare su **Controllo dati**.
2. Deselezionare la casella di spunta **Abilita Sophos Data Control**.

6.3 Aggiunta di un file a un dispositivo di memorizzazione

Se in questo computer è abilitato il controllo dati, il criterio di controllo dati potrebbe bloccare qualsiasi tentativo di aggiunta di un file a un dispositivo di memorizzazione monitorato utilizzando i seguenti metodi:

- Salvataggio di dati all'interno di un programma
- Utilizzo del comando DOS copia
- Creazione di un nuovo file nel dispositivo che esegue Windows Explorer

Se si vede un allarme desktop in merito, è opportuno salvare il file sul disco rigido o su un'unità di rete e quindi utilizzare Esplora risorse per copiarlo sul dispositivo di memorizzazione.

6.4 Configurazione del log del controllo dati

1. Nel menu **Configura**, cliccare su **Controllo dati**.

2. Sotto **Livello di log**, selezionare una delle seguenti opzioni:
 - Cliccare su **Nessuno** per impedire che venga creato il log.
 - Per registrare le informazioni di riepilogo, i messaggi di errore e così via, cliccare su **Normale**.
 - Cliccare su **Dettagliato** per ottenere informazioni relative a molte più attività del normale. Utilizzare questa impostazione solo se si devono testare nuove regole del controllo dati, dal momento che le dimensioni del log cresceranno rapidamente.
3. Sotto **Archiviazione log**, seguire le istruzioni a schermo.

6.5 Visualizzazione del log del controllo dati

- ❖ Nella **Home page**, sotto **Controllo dati**, cliccare su **Visualizza log controllo dati**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.

Dalla pagina log, è possibile copiare il log negli appunti, oppure inviarlo per e-mail o stamparlo.

Per trovare un testo specifico all'interno del log, cliccare su **Trova** e inserire il testo desiderato.

7 Utilizzo di Sophos Client Firewall

7.1 Introduzione al firewall

Quando il firewall viene installato per la prima volta, può essere necessario configurarlo. Se sia necessario farlo o meno dipende dal modo in cui è stato installato. Sono disponibili due tipi di installazione:

- Installato in un computer in rete e gestito da una console di gestione
- Installato in un computer autonomo e gestito dal computer

Firewall gestito da una console di gestione

Se il firewall è installato e gestito da una console di gestione, consente o blocca applicazioni e traffico secondo le regole impostate dal criterio.

A meno che il criterio non abbia posto il firewall in modalità interattiva (v. sotto), l'utente non riceverà alcun messaggio e non dovrà configurare il firewall in alcun modo.

Firewall gestito dal computer

Se il firewall è gestito nel computer, si consiglia di cominciare creando regole che consentano l'accesso alla rete per applicazioni e servizi comuni, quali browser web e client di posta elettronica.

Per informazioni sulla creazione di regole, consultare la sezione [Configurazione firewall](#) a pagina 46.

Inizialmente il firewall sarà in modalità interattiva (v. sotto). Lasciarlo in tale modalità per un periodo di tempo sufficiente a consentire o bloccare altri servizi e applicazioni in uso.

Una volta configurato il firewall e assicuratisi che riconosca le applicazioni comunemente utilizzate, si consiglia di passare a una delle modalità non interattive.

Per informazioni, consultare la sezione [Passaggio alla modalità non interattiva](#) a pagina 53.

Modalità interattiva

Quando in modalità interattiva, il firewall chiede di consentire o bloccare le applicazioni e il traffico per cui non sono state create regole.

Per informazioni su come gestire messaggi dal firewall, consultare la sezione [Modalità interattiva](#) a pagina 52.

7.2 Configurazione firewall

7.2.1 Configurazione firewall

È possibile configurare il firewall in molti modi diversi e poi abilitarlo. Tuttavia, se su questo computer viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control, essa potrebbe ignorare le modifiche qui apportate.

Alcune funzioni comuni sono elencate di seguito:

- [Abilitazione della modalità interattiva](#) a pagina 52
- [Filtraggio dei messaggi ICMP](#) a pagina 51
- [Per consentire tutto il traffico su una LAN](#) a pagina 48
- [Autorizzazione del download del FTP](#) a pagina 48
- [Creazione di una regola globale](#) a pagina 57
- [Autorizzazione di un'applicazione](#) a pagina 50
- [Autorizzazione dell'avvio di processi nascosti](#) a pagina 62
- [Autorizzazione dell'utilizzo di raw socket da parte delle applicazioni](#) a pagina 63
- [Utilizzo di checksum per l'autenticazione delle applicazioni](#) a pagina 63

7.2.2 Disabilitazione temporanea del firewall

In quanto membri del gruppo SophosAdministrator, può presentarsi la necessità di disabilitare temporaneamente il firewall per motivi di manutenzione o per la risoluzione di alcuni problemi e successivamente di riabilitarlo.

Sophos Endpoint Security and Control conserva le impostazioni scelte in questa pagina, anche dopo il riavvio del computer. Se si disabilita il firewall, il computer risulta non protetto finché la scansione in accesso non venga riabilitata.

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, selezionare la casella di spunta **Consenti tutto il traffico** di fianco al percorso primario o secondario.

7.2.3 Autorizzazione e-mail

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Cliccare su **Aggiungi**, trovare l'applicazione di posta elettronica e cliccarvi due volte.

L'applicazione di posta elettronica viene autorizzata in quanto applicazione attendibile.

Alle applicazioni attendibili viene concesso accesso alla rete pieno e incondizionato, oltre che accesso a Internet. Per una maggiore sicurezza, è possibile applicare le regole predefinite fornite da Sophos:

1. Nell'elenco delle applicazioni consentite, cliccare sull'applicazione di posta elettronica.

2. Cliccare su **Applicazione personalizzata > Aggiungi regole da quelle predefinite > Client di posta elettronica**.

7.2.4 Autorizzazione all'utilizzo di un browser web

Nota: se si consente l'utilizzo di un browser web, si consente al tempo stesso l'accesso FTP.

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Cliccare su **Aggiungi**, trovare l'applicazione del browser web e cliccarvi due volte.

L'applicazione del browser web viene autorizzata in quanto applicazione attendibile.

Alle applicazioni attendibili viene concesso accesso alla rete pieno e incondizionato, oltre che accesso a Internet. Per una maggiore sicurezza, è possibile applicare le regole predefinite fornite da Sophos:

1. Nell'elenco delle applicazioni consentite, cliccare sull'applicazione del browser web.
2. Cliccare su **Personalizza > Aggiungi regole da quelle predefinite > Browser**.

7.2.5 Autorizzazione del download del FTP

Nota: se è stato concesso l'utilizzo di un browser web che può accedere ai server FTP, non è necessario autorizzare anche i download del FTP.

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Cliccare su **Aggiungi**, trovare l'applicazione del FTP e cliccarvi due volte.

L'applicazione del FTP viene autorizzata in quanto applicazione attendibile.

Alle applicazioni attendibili viene concesso accesso alla rete pieno e incondizionato, oltre che accesso a Internet. Per una maggiore sicurezza, è possibile applicare le regole predefinite fornite da Sophos:

1. Nell'elenco delle applicazioni consentite, cliccare sull'applicazione del FTP.
2. Cliccare su **Applicazione personalizzata > Aggiungi regole da quelle predefinite > Client FTP**.

7.2.6 Per consentire tutto il traffico su una LAN

Per consentire tutto il traffico tra computer su una LAN (Area di Rete Locale):

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.

2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **LAN**, svolgere una delle seguenti operazioni:
 - Cliccare su **Rileva** per rilevare la LAN in cui si trova il computer ed aggiungerla all'elenco di indirizzi di rete.
 - Cliccare su **Aggiungi**. Nella finestra di dialogo **Seleziona indirizzo**, selezionare **Formato indirizzo**, digitare il nome di dominio o l'indirizzo IP e poi cliccare su **Aggiungi**.
4. Cliccare su **OK** per chiudere la finestra di dialogo **Seleziona indirizzo**.
5. Nell'elenco **Impostazioni LAN**, spuntare la casella **Attendibile** per una rete.

Note

- Se si consente tutto il traffico tra computer su una LAN, si consente anche la condivisione file e stampanti su di essa.

7.2.7 Autorizzazione di tutte le condivisioni file e stampanti su una LAN

Nota: Se è già stato autorizzato tutto il traffico tra computer su una LAN (Rete di Area Locale), non c'è bisogno di autorizzare anche la condivisione file e stampanti.

Autorizzazione di tutte le condivisioni file e stampanti su una LAN:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **LAN**, svolgere una delle seguenti operazioni:
 - Cliccare su **Rileva** per rilevare la LAN in cui si trova il computer ed aggiungerla all'elenco di indirizzi di rete.
 - Cliccare su **Aggiungi**. Nella finestra di dialogo **Seleziona indirizzo**, selezionare **Formato indirizzo**, digitare il nome di dominio o l'indirizzo IP e poi cliccare su **Aggiungi**.
4. Cliccare su **OK** per chiudere la finestra di dialogo **Seleziona indirizzo**.
5. Nell'elenco delle **Impostazioni LAN**, selezionare la casella **NetBIOS** per consentire a una LAN la condivisione file stampanti.

Per informazioni su come bloccare o consentire la condivisione file e stampanti su LAN diverse da quelle presenti nell'elenco **Impostazioni LAN**, consultare i seguenti argomenti:

- [Blocco condivisione file e stampanti indesiderata](#) a pagina 60
- [Autorizzazione al controllo flessibile della condivisione file e stampanti](#) a pagina 49

Per informazioni su come consentire tutto il traffico su una LAN, consultare la sezione [Per consentire tutto il traffico su una LAN](#) a pagina 48.

7.2.8 Autorizzazione al controllo flessibile della condivisione file e stampanti

Se si desidera un controllo più flessibile della condivisione file e stampanti sulla propria rete (ad esempio, traffico NetBIOS unidirezionale), è sufficiente fare come segue:

1. Autorizzazione della condivisione file e stampanti in LAN (reti di area locali) diverse da quelle presenti nell'elenco **Impostazioni LAN**. Ciò consente il traffico NetBIOS sulle LAN sottoposte alle regole del firewall.
2. Creazione di regole con elevata priorità che consentono la comunicazione a/da host tramite gli appropriati protocolli e porte NetBIOS. Si consiglia di creare delle regole che blocchino esplicitamente tutto il traffico di condivisione file e stampanti indesiderato, piuttosto che lasciarlo gestire dalla regola predefinita.

Autorizzazione della condivisione file e stampanti in LAN diverse da quelle presenti nell'elenco **Impostazioni LAN**.

1. Nella **Home page**, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **LAN**, deselezionare la casella **Blocca condivisione file e stampanti per altre reti**.

7.2.9 Autorizzazione di un'applicazione

1. Nella **Home page**, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Cliccare su **Aggiungi**, trovare l'applicazione e cliccarvi due volte.

L'applicazione viene consentita in quanto attendibile.

Alle applicazioni attendibili viene concesso accesso alla rete pieno e incondizionato, oltre che accesso a Internet. Per una maggiore sicurezza, è possibile applicare una o più *regole dell'applicazione* per specificare le condizioni in cui un'applicazione può essere eseguita.

- [Creazione di una regola applicazioni](#) a pagina 60
- [Applicazione delle regole applicazioni predefinite](#) a pagina 60

7.2.10 Blocco di un'applicazione

1. Nella **Home page**, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Se l'applicazione non è inclusa nell'elenco, cliccare su **Aggiungi**, trovare l'applicazione e cliccarvi due volte.
5. Selezionare l'applicazione nell'elenco e cliccare su **Blocca**.

7.2.11 Filtraggio dei messaggi ICMP

I messaggi di Internet Control Message Protocol (ICMP) consentono ai computer in rete di condividere informazioni relative ad errori e stato. È possibile consentire o bloccare determinati tipi di messaggi ICMP in entrata o uscita.

Filtrare i messaggi ICMP solo se in possesso di una certa competenza sui protocolli di rete. Per spiegazioni relative ai tipi di messaggi ICM, consultare la sezione [Definizione dei tipi di messaggi ICMP](#) a pagina 51.

Per filtrare i messaggi ICMP:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **ICMP**, selezionare la casella di spunta **Ing.** o **Usc.** per consentire i messaggi in entrata o uscita di un determinato tipo.

7.2.12 Definizione dei tipi di messaggi ICMP

Richiesta Echo, Risposta Echo	Utilizzato per verificare l'accessibilità e lo stato della destinazione. Un host invia una Richiesta Echo e attende la relativa Risposta Echo . Questa operazione viene solitamente svolta tramite il comando <code>ping</code> .
Destinazione irraggiungibile, Risposta Echo	Inviato dal router quando non riesce a recapitare un datagramma IP. Un datagramma è l'unità fondamentale di informazione, o pacchetto, passata attraverso una rete TCP/IP.
Quench sorgente	Inviato da un host o router se riceve dati troppo rapidamente per poterli gestire. Il messaggio è una richiesta di riduzione della velocità con cui la fonte trasmette datagrammi.
Reinstrada	Inviato da un router se riceve datagrammi che dovrebbero essere stati inviati a un router differente. Il messaggio contiene l'indirizzo a cui la fonte deve inviare i futuri datagrammi. Ciò consente di ottimizzare il routing del traffico della rete.
Annuncio del router, Sollecitazione del router	Consente agli host di scoprire l'esistenza di router. I router rendono noti periodicamente i loro indirizzi IP tramite messaggi di tipo Annuncio del router . Gli host possono richiedere l'indirizzo di un router inviando un messaggio Sollecitazione del router a cui il router risponderà con un Annuncio del router .
Tempo scaduto per un datagramma	Inviato da un router quando un datagramma ha raggiunto il livello massimo di router attraverso cui può passare.
Problema di parametro per un datagramma	Inviato da un router se si verifica un problema durante la trasmissione di un datagramma tale da non consentire il

	completamento del processo. Una possibile causa di tale problema è una non valida intestazione del datagramma.
Richiesta data e ora, Risposta data e ora	Utilizzato per sincronizzare gli orologi degli host e per fare stime sulla durata del transito.
Richiesta informazioni, Risposta informazioni	Obsoleto. In passato questi messaggi venivano utilizzati dagli host per determinare i loro indirizzi inter-network; ora sono considerati obsoleti e non dovrebbero essere utilizzati.
Richiesta maschera indirizzo, Risposta maschera indirizzo	Utilizzato per trovare la maschera della sottorete (ovvero quali parti dell'indirizzo definiscono la rete). Un host invia una Richiesta maschera indirizzo a un router e riceve una Risposta maschera indirizzo .

7.2.13 Ripristino delle impostazioni predefinite del firewall

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Gestione configurazione**, cliccare su **Ripristina predefiniti**.

7.3 Lavoro in modalità interattiva

7.3.1 Modalità interattiva

In modalità interattiva, il firewall visualizza una *finestra di apprendimento* ogni qual volta un'applicazione o servizio sconosciuti richiedono accesso alla rete. La finestra di apprendimento chiede se consentire il traffico una volta, bloccarlo una volta o se creare una regola per quel determinato tipo di traffico.

In modalità interattiva, verranno visualizzate le seguenti finestre di apprendimento:

- [Finestre di apprendimento sui processi nascosti](#) a pagina 53
- [Finestre di apprendimento sul protocollo](#) a pagina 54
- [Finestre di apprendimento sulle applicazioni](#) a pagina 54
- [Finestre di apprendimento su raw socket](#) a pagina 54
- [Finestre di apprendimento sui checksum](#) a pagina 54

7.3.2 Abilitazione della modalità interattiva

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **Generale**, sotto **Modalità di funzionamento**, cliccare su **Interattiva**.

7.3.3 Passaggio alla modalità non interattiva

Esistono due tipi di modalità non interattiva:

- Consenti per impostazione predefinita
- Blocca per impostazione predefinita

Nelle modalità non interattive, il firewall gestisce il traffico della rete automaticamente utilizzando le regole impostate dall'utente. Il traffico di rete che non corrisponde ad alcuna regola può essere completamente autorizzato (se in uscita) o completamente bloccato.

Per passare alla modalità interattiva:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **Generale**, sotto **Modalità di funzionamento**, cliccare su **Consenti per impostazione predefinita** o **Blocca per impostazione predefinita**.

7.3.4 Finestre di apprendimento sui processi nascosti

Un processo nascosto avviene quando un'applicazione ne avvia un'altra che svolge delle operazioni di accesso alla rete per lei. Applicazioni malevole possono utilizzare questa tecnica per eludere i firewall: Avviano un'applicazione attendibile che consenta di accedere alla rete, piuttosto che tentare da sole.

La finestra di apprendimento sui processi nascosti visualizza informazioni relative al processo nascosto e all'applicazione che lo ha avviato.

- [Abilitazione delle finestre di apprendimento sui processi nascosti](#) a pagina 53

7.3.5 Abilitazione delle finestre di apprendimento sui processi nascosti

Se si utilizza la modalità interattiva, il firewall può visualizzare una finestra di apprendimento ogni qual volta rilevi una nuova applicazione di questo genere.

Se si utilizza la modalità interattiva e questa opzione non è selezionata, a queste nuove applicazioni viene impedito l'avvio di processi nascosti.

Per abilitare le finestre di apprendimento sui processi nascosti:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Processi**.
4. Selezionare la casella di spunta **Avvisa in caso di nuove applicazioni di questo genere**.

7.3.6 Finestre di apprendimento sul protocollo

Se il firewall rileva attività di rete da parte del sistema che non riesce a relazionare ad alcuna applicazione specifica, richiede la creazione di una regola di protocollo.

La finestra di dialogo sul protocollo visualizza informazioni relative all'attività di rete non riconosciuta, ovvero protocollo e indirizzo remoto.

7.3.7 Finestre di apprendimento sulle applicazioni

Se il firewall rileva che un'applicazione sta tentando di accedere alla rete in una modalità non coperta da alcuna regola esistente, richiede la creazione di una regola dell'applicazione.

La finestra di apprendimento dell'applicazione visualizza informazioni relative all'attività di rete non riconosciuta, ovvero il servizio e l'indirizzo remoti.

7.3.8 Finestre di apprendimento su raw socket

I Rawsocket consentono ai processi di controllare tutti gli aspetti dei dati che inviano in rete e possono essere utilizzati per scopi malevoli.

Se il firewall rileva che un raw socket cerca di accedere alla rete in una modalità che non è coperta da una regola esistente, richiede la creazione di una regola sui raw socket.

La finestra di apprendimento sui raw socket visualizza informazioni relative al raw socket.

■ [Abilitazione delle finestre di apprendimento sui raw socket](#) a pagina 54

7.3.9 Abilitazione delle finestre di apprendimento sui raw socket

Se si utilizza la modalità interattiva, il firewall può visualizzare una finestra di apprendimento ogni qual volta rilevi un raw socket che tenta di accedere alla rete in una modalità non coperta da una regola esistente.

Se si utilizza la modalità interattiva e questa opzione non è selezionata, ai raw socket viene bloccato l'accesso alla rete.

Per abilitare le finestre di apprendimento sui raw socket:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Processi**.
4. Selezionare la casella di spunta **Avvisa sull'utilizzo dei raw socket**.

7.3.10 Finestre di apprendimento sui checksum

Se il firewall rileva un'applicazione nuova o modificata, visualizza una finestra di apprendimento sui checksum.

Se si vuole consentire all'applicazione accesso alla rete, è necessario aggiungere all'elenco di checksum riconosciuti il suo checksum (identificatore unico).

Selezionare una delle seguenti opzioni:

- **Aggiungi il checksum a quelli esistenti per questa applicazione** consente versioni multiple dell'applicazione.
- **Sostituisci qualsiasi checksum esistente per questa applicazione** sostituisce tutti i checksum esistenti per l'applicazione con quello che richiede l'accesso e, di conseguenza, consente l'accesso solo alla versione più recente dell'applicazione.
- **Blocca questa applicazione finché non viene riavviata** in questa occasione blocca l'applicazione.

7.3.11 Abilitazione delle finestre di apprendimento sui checksum

Se si utilizza la modalità interattiva, il firewall può visualizzare una finestra di apprendimento ogni qual volta rilevi un'applicazione nuova o modificata.

Se si utilizza la modalità interattiva e questa opzione non è selezionata, alle applicazioni viene bloccato l'accesso alla rete.

Per abilitare le finestre di apprendimento sui checksum:

1. Nella **Home page**, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Sotto **Blocco**, selezionare la casella di spunta **Utilizzo di checksum per l'autenticazione delle applicazioni**.

7.4 File di configurazione firewall

7.4.1 File di configurazione del firewall

Sophos Client Firewall consente di esportare le impostazioni generali e le regole del firewall come file di configurazione. Utilizzare questa funzione per svolgere le seguenti operazioni:

- Eseguire back up e ripristino di tutte le configurazioni del firewall.
- Salvare la configurazione delle impostazioni generali ed eseguirne l'installazione in computer multipli.
- Creare le regole per le applicazioni in un solo computer ed esportarle per poi utilizzarle in altri computer che eseguono lo stesso set di applicazioni.
- Utilizzare la console di gestione per unire le configurazioni create in diversi computer per poter creare un criterio unico che sia valido per tutti i computer in rete.

7.4.2 Esportazione di un file di configurazione firewall

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Cliccare su **Esporta**.
3. Attribuire al file di configurazione un nome e un percorso e poi cliccare su **Salva**.

7.4.3 Importazione di un file di configurazione firewall

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Cliccare su **Importa**.
3. Selezionare un file di configurazione e cliccare su **Apri**.
4. Seguire le istruzioni sullo schermo.

7.5 Regole firewall

7.5.1 Regole firewall

Regole globali

Le regole globali sono applicate a tutte le comunicazioni di rete e applicazioni anche se in possesso di regole applicazioni.

Regole applicazioni

Un'applicazione può avere una o più regole. È possibile utilizzare sia le regole create da Sophos che creare regole personalizzate per avere pieno controllo sull'accesso consentito a un'applicazione.

7.5.2 Ordine di applicazione delle regole

Per le connessioni che utilizzano raw socket, vengono verificate solo le regole globali.

Per le connessioni che *non* utilizzano raw socket, vengono verificate svariate regole, in base al fatto se la connessione è diretta a un indirizzo di rete elencato nella scheda **LAN** o no.

Se l'indirizzo di rete è elencato nella scheda **LAN**, vengono controllate le seguenti regole:

- Se l'indirizzo è marcato come **Attendibile**, tutto il traffico sulla connessione viene consentito senza ulteriori verifiche.
- Se l'indirizzo è marcato come **NetBIOS**, viene consentita la condivisione file e stampanti su ogni connessione che soddisfa i seguenti requisiti:

Connessione	Porta	Intervallo
TCP	Remoto	137-139 o 445
TCP	Locale	137-139 o 445
UDP	Remoto	137 o 138
UDP	Locale	137 o 138

Se l'indirizzo di rete *non* figura nella scheda **LAN**, vengono verificate altre regole del firewall, nel seguente ordine:

1. Tutto il traffico **NetBIOS** non consentito attraverso la scheda **LAN** viene elaborato in base alle impostazioni della casella **Blocca condivisione file e stampanti per altri network**:
 - Se la casella è spuntata, il traffico viene bloccato.
 - Se la casella non è spuntata, il traffico viene sottoposto alle restanti regole.
 2. Le regole globali ad alta priorità vengono verificate nell'ordine in cui sono elencate.
 3. Se alla connessione non sono ancora state applicate regole, vengono verificate le regole dell'applicazione.
 4. Se la connessione non è stata ancora presa in considerazione, vengono verificate le normali regole globali secondo l'ordine in cui sono elencate.
 5. Se non è stata rilevata alcuna regola per la gestione della connessione:
 - Nella modalità **Consenti per impostazione predefinita** il traffico viene consentito (se si tratta di traffico in uscita).
 - Nella modalità **Blocca per impostazione predefinita**, viene bloccato il traffico.
 - Nella modalità **Interattiva**, viene chiesto all'utente di decidere.
- Nota:** Se la modalità di funzionamento non è stata modificata, il firewall risulterà impostato su **Blocca per impostazione predefinita**.

7.5.3 Regole globali

7.5.3.1 Creazione di una regola globale

Importante: Sophos consiglia di modificare regole globali solo se in possesso di una certa competenza sui protocolli di rete.

Le regole globali vengono applicate a tutte le comunicazioni della rete e a tutte le applicazioni non ancora in possesso di una regola specifica.

Per creare una regola globale:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.

3. Cliccare sulla scheda **Regole globali**.
4. Cliccare su **Aggiungi**.
5. Sotto **Nome della regola**, digitare il nome della regola.
Il nome della regola deve essere unico all'interno dell'elenco delle regole. Due regole globali non possono avere lo stesso nome.
6. Per applicare la regola prima di qualsiasi regola dell'applicazione o del normale ordine di priorità delle regole globali, selezionare la casella di spunta **Regola con elevata priorità**.
Per ulteriori informazioni sull'ordine di applicazione delle regole, consultare la sezione [Ordine di applicazione delle regole](#) a pagina 56.
7. Sotto **Seleziona gli eventi che saranno gestiti dalla regola**, selezionare le condizioni che la connessione deve rispettare affinché la regola venga applicata.
8. Sotto **Seleziona le azioni alle quali la regola reagirà**, selezionare **Consenti** o **Blocca**.
9. Effettuare una delle seguenti operazioni:
 - Per consentire altre connessioni da e verso lo stesso indirizzo remoto mentre la connessione iniziale è ancora attiva, selezionare **Connessioni concorrenti**.
Nota: Questa opzione è disponibile solo per regole TCP, con status per impostazione predefinita.
 - Per consentire risposte intelligenti dal computer remoto in base alla connessione iniziale, selezionare **Ispezione di stato**.
10. Sotto **Descrizione della regola**, cliccare su un valore sottolineato. Per esempio, se si clicca sul link **TCP**, si apre la finestra di dialogo **Seleziona protocollo**.

7.5.3.2 Modifica di una regola globale

Importante: Sophos consiglia di modificare regole globali solo se in possesso di una certa competenza sui protocolli di rete.

Modifica di una regola globale:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Regole globali**.
4. Nell'elenco **Regola**, scegliere la regola che si desidera modificare.
5. Cliccare su **Modifica**.
Per informazioni sulle impostazioni delle regole globali, consultare la sezione [Creazione di una regola globale](#) a pagina 57.

7.5.3.3 Copia di una regola globale

Per copiare una regola globale e aggiungerla all'elenco delle regole:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.

2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Regole globali**.
4. Nell'elenco **Regola**, scegliere la regola che si desidera copiare.
5. Cliccare su **Copia**.

7.5.3.4 Modifica dell'ordine di applicazione delle regole globali

Le regole globali vengono applicate secondo l'ordine in cui appaiono nell'elenco delle regole, dall'alto verso il basso.

Per modificare l'ordine di applicazione delle regole globali:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Regole globali**.
4. Nell'elenco **Regola**, cliccare sulla regola che si desidera spostare in alto o in basso nell'elenco.
5. Cliccare su **Sposta su** o **Sposta giù**.

7.5.3.5 Cancellazione di una regola globale

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Regole globali**.
4. Nell'elenco **Regola**, scegliere la regola che si desidera cancellare.
5. Cliccare su **Rimuovi**.

7.5.4 Blocco

7.5.4.1 Attivazione e disattivazione del blocco di processi modificati

Il malware potrebbe tentare di aggirare il firewall modificando un processo in memoria già iniziato da un programma attendibile, e utilizzare quindi il processo modificato per accedere alla rete in sua vece.

E' possibile configurare il firewall per rilevare e bloccare i processi modificati in memoria.

Attivazione e disattivazione del blocco di processi modificati:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Sulla scheda **Generale**, sotto **Blocco**, deselezionare la casella **Blocca processi se la memoria viene modificata da un'altra applicazione** per rimuovere il blocco dei processi modificati.
Per attivare il blocco di processi modificati, selezionare la relativa casella.

Se il firewall rileva un processo modificato in memoria, aggiunge delle regole per impedire al processo modificato di accedere alla rete.

Note

- Si sconsiglia di disattivare il blocco di processi modificati in maniera permanente. Disattivare il rilevamento solo quando strettamente necessario.
- Il blocco di processi modificati non è supportato sulle versioni 64-bit di Windows.
- Viene bloccato solamente il processo modificato. Al programma che modifica il processo non viene impedito l'accesso alla rete.

7.5.4.2 Blocco condivisione file e stampanti indesiderata

Per bloccare la condivisione di file e stampanti su reti diverse da quelle specificate nell'elenco **Impostazioni LAN** sulla scheda **LAN**:

1. Nella **Home page**, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **LAN**, deselezionare la casella **Blocca condivisione file e stampanti per altre reti**.

7.5.5 Regole applicazioni

7.5.5.1 Applicazione delle regole applicazioni predefinite

Si tratta di un set di regole di applicazione create da Sophos. Per aggiungere regole predefinite all'elenco di regole per un'applicazione:

1. Nella **Home page**, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Selezionare l'applicazione nell'elenco e poi cliccare sulla freccia di fianco a **Personalizza**.
5. Andare a **Aggiungi regole da quelle predefinite** e cliccare sulla regola predefinita.

7.5.5.2 Creazione di una regola applicazioni

Per creare una regola personalizzata che rappresenti un buon meccanismo di controllo sulla concessione dell'accesso a una determinata applicazione:

1. Nella **Home page**, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
È anche possibile cliccare due volte sull'applicazione nell'elenco.

5. Nella finestra di dialogo **Regole applicazioni**, cliccare su **Aggiungi**.
6. Sotto **Nome della regola**, digitare il nome della regola.
Il nome della regola deve essere unico all'interno dell'elenco delle regole. Due regole dell'applicazione non possono avere lo stesso nome, ma due applicazioni possono avere ciascuna una regola con lo stesso nome.
7. Sotto **Seleziona gli eventi che saranno gestiti dalla regola**, selezionare le condizioni che la connessione deve rispettare affinché la regola venga applicata.
8. Sotto **Seleziona le azioni alle quali la regola reagirà**, selezionare **Consenti** o **Blocca**.
9. Per consentire risposte intelligenti dal computer remoto in base alla connessione iniziale, selezionare **Ispezione di stato**.
10. Sotto **Descrizione della regola**, cliccare su un valore sottolineato. Per esempio, se si clicca sul link **TCP**, si apre la finestra di dialogo **Seleziona protocollo**.

7.5.5.3 Modifica di una regola applicazioni

1. Nella **Home page**, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
È anche possibile cliccare due volte sull'applicazione nell'elenco.
5. Nella finestra di dialogo **Regole applicazioni**, cliccare su **Modifica**.
6. Sotto **Nome della regola**, digitare il nome della regola.
Il nome della regola deve essere unico all'interno dell'elenco delle regole. Due regole dell'applicazione non possono avere lo stesso nome, ma due applicazioni possono avere ciascuna una regola con lo stesso nome.
7. Sotto **Seleziona gli eventi che saranno gestiti dalla regola**, selezionare le condizioni che la connessione deve rispettare affinché la regola venga applicata.
8. Sotto **Seleziona le azioni alle quali la regola reagirà**, selezionare **Consenti** o **Blocca**.
9. Per consentire risposte intelligenti dal computer remoto in base alla connessione iniziale, selezionare **Ispezione di stato**.
10. Sotto **Descrizione della regola**, cliccare su un valore sottolineato. Per esempio, se si clicca sul link **TCP**, si apre la finestra di dialogo **Seleziona protocollo**.

7.5.5.4 Copia di una regola applicazioni

Per copiare una regola applicazioni e aggiungerla all'elenco delle regole:

1. Nella **Home page**, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.

4. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
È anche possibile cliccare due volte sull'applicazione nell'elenco.
5. Nella finestra di dialogo **Regole applicazioni**, cliccare su **Copia**.

7.5.5.5 Modifica dell'ordine di applicazione delle regole applicazioni

Le regole applicazioni vengono applicate secondo l'ordine in cui appaiono nell'elenco delle regole, dall'alto verso il basso.

Per modificare l'ordine di applicazione delle regole applicazioni:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
È anche possibile cliccare due volte sull'applicazione nell'elenco.
5. Nell'elenco **Regola**, cliccare sulla regola che si desidera spostare in alto o in basso nell'elenco.
6. Cliccare su **Sposta su** o **Sposta giù**.

7.5.5.6 Cancellazione di una regola applicazioni

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
5. Nella finestra di dialogo **Regole applicazioni**, cliccare su **Rimuovi**.

7.5.5.7 Autorizzazione dell'avvio di processi nascosti

Un'applicazione a volte ne avvia un'altra che svolga delle operazioni di accesso alla rete per lei.

Applicazioni malevole possono utilizzare questa tecnica per eludere i firewall: avviano un'applicazione attendibile che consenta di accedere alla rete, piuttosto che tentare l'accesso esse stesse.

Nel caso ne venga utilizzato uno, il firewall invia un allarme alla console di gestione la prima volta che rileva un processo nascosto.

Per consentire l'avvio di processi nascosti:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Processi**.

4. Nell'area in alto, cliccare sul pulsante **Aggiungi**.
5. Trovare l'applicazione e cliccarvi due volte.

Se si utilizza la modalità interattiva, il firewall può visualizzare una finestra di apprendimento ogni qual volta rilevi una nuova applicazione di questo genere.

- [Abilitazione della modalità interattiva](#) a pagina 52
- [Abilitazione delle finestre di apprendimento sui processi nascosti](#) a pagina 53

7.5.5.8 Autorizzazione dell'utilizzo di raw socket da parte delle applicazioni

Alcune applicazioni possono accedere alla rete tramite raw socket che forniscono loro controllo su tutti gli aspetti relativi ai dati inviati nella rete.

Alcune applicazioni malevole possono sfruttare i raw socket contraffacendo il loro indirizzo IP o inviando messaggi volutamente corrotti.

Nel caso ne venga utilizzato uno, il firewall invia un allarme alla console di gestione la prima volta che rileva un raw socket.

Per consentire alle applicazioni di accedere alla rete tramite raw socket:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Processi**.
4. Nell'area in basso, cliccare sul pulsante **Aggiungi**.
5. Trovare l'applicazione e cliccarvi due volte.

Se si utilizza la modalità interattiva, il firewall può visualizzare una finestra di apprendimento ogni qual volta rilevi un raw socket.

- [Abilitazione della modalità interattiva](#) a pagina 52
- [Abilitazione delle finestre di apprendimento sui raw socket](#) a pagina 54

7.5.5.9 Utilizzo di checksum per l'autenticazione delle applicazioni

Ogni versione di un'applicazione ha un checksum unico. Il firewall può utilizzare tale checksum per decidere se un'applicazione è consentita o meno.

Per impostazione predefinita, il firewall verifica il checksum di tutte le applicazioni in esecuzione. Se il checksum non è noto o è stato modificato, il firewall lo blocca o (in modalità interattiva) chiede all'utente come procedere.

Nel caso ne venga utilizzato uno, il firewall invia anche un allarme alla console di gestione la prima volta che rileva un'applicazione nuova o modificata.

Per aggiungere un checksum all'elenco di checksum autorizzati:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.

3. Cliccare sulla scheda **Checksum**.
4. Cliccare su **Aggiungi**.
5. Trovare l'applicazione e cliccarvi due volte.

Se si utilizza la modalità interattiva, il firewall può visualizzare una finestra di apprendimento ogni qual volta rilevi un'applicazione nuova o modificata.

- [Abilitazione della modalità interattiva](#) a pagina 52
- [Abilitazione delle finestre di apprendimento sui processi nascosti](#) a pagina 53

7.6 Riconoscimento presenza

7.6.1 Riconoscimento presenza

Il riconoscimento della presenza è una funzione di Sophos Client Firewall che assegna set di regole in base al percorso del computer.

A un laptop, per esempio, può essere assegnato un set di regole del firewall più restrittive quando utilizzato fuori ufficio, dal momento che non potrà godere della protezione aggiuntiva del firewall di rete.

Per utilizzare il riconoscimento della presenza, per prima cosa è necessario definire un elenco dei percorsi primari (per es. le varie reti aziendali). Quando il firewall rileva la connessione a uno dei percorsi primari, utilizza la configurazione primaria.

- [Definizione dei percorsi primari](#) a pagina 64

Successivamente si crea una configurazione secondaria. Quando il firewall rileva che **non** si è connessi a uno dei percorsi primari, utilizza la configurazione secondaria.

- [Creazione di un percorso secondario](#) a pagina 65

7.6.2 Definizione dei percorsi primari

Il firewall utilizza la configurazione primaria quando rileva la presenza in uno dei percorsi primari.

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Cliccare sulla scheda **Rilevamento percorso**.

3. Sotto **Metodo di rilevamento**, cliccare su **Configura** di fianco al metodo che si desidera utilizzare per definire i percorsi primari:

Opzione	Descrizione
Identifica percorso tramite DNS	Creazione di un elenco di nomi di dominio e indirizzi IP previsti, corrispondenti ai percorsi primari.
Identifica percorso tramite indirizzi gateway MAC	Creazione di un elenco di indirizzi gateway MAC corrispondenti ai percorsi primari.

In entrambi i casi, il firewall esamina o risolve l'elenco di percorsi primari. Se trova una corrispondenza, il computer viene inserito in un percorso primario.

4. Seguire le istruzioni sullo schermo.

7.6.3 Creazione di un percorso secondario

Il firewall utilizza la configurazione secondaria quando non si è connessi a un percorso primario.

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Selezionare la casella di spunta **Aggiungi configurazione per percorso secondario**.

Impostare la configurazione secondaria. Per informazioni, consultare la sezione *Configurazione firewall*.

7.7 Reportistica del firewall

7.7.1 Reportistica del firewall

Per impostazione predefinita, i report del firewall comunicano alla console di gestione cambiamenti di stato, eventi ed errori.

Cambiamenti di stato del firewall

Il firewall considera cambiamenti di stato i cambiamenti riportati di seguito:

- Cambiamenti alle modalità di funzionamento
- Cambiamenti della versione del software
- Cambiamenti alla configurazione del firewall per autorizzare tutto il traffico
- Cambiamenti alla conformità del firewall al criterio

Quando si lavora in modalità interattiva, la configurazione firewall potrebbe essere deliberatamente diversa dal criterio applicato dalla console di gestione. Se questo è il caso, è possibile decidere di **non** inviare alla console di gestione allarmi "diverso dal criterio", quando si apportano cambiamenti a determinate parti della configurazione del firewall.

Per ulteriori informazioni, consultare la sezione [Attivazione o disattivazione del rilevamento di modifiche locali](#) a pagina 66.

Eventi firewall

Un *evento* si verifica quando un'applicazione sconosciuta nel computer, o il sistema operativo del computer, prova a comunicare con un altro computer tramite una connessione di rete.

È possibile impedire che il firewall riporti alla console di gestione gli eventi.

Per ulteriori informazioni, consultare la sezione [Disattivazione del rilevamento del traffico di rete sconosciuto](#) a pagina 66

7.7.2 Attivazione o disattivazione del rilevamento di modifiche locali

Se la configurazione del firewall differisce dal criterio, è possibile **disattivare il rilevamento di modifiche locali**.

La disattivazione del rilevamento di modifiche locali fa in modo che il firewall non invii allarmi "diverso dal criterio" alla console di gestione in relazione alle modifiche apportate a regole globali, applicazioni, processi o checksum. Scegliere questa opzione quando si lavora in modalità interattiva, dal momento che si tratta di impostazioni modificabili tramite finestre di apprendimento.

Se nel computer la configurazione del firewall deve essere conforme al criterio, si dovrà **attivare il rilevamento di modifiche locali**.

Per disattivare il rilevamento di modifiche locali:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **Generale**, sotto **Reportistica**, per disattivare il rilevamento di modifiche locali, deselezionare la casella di spunta **Visualizza un allarme nella console di gestione se a regole globali, applicazioni, processi o checksum sono apportate modifiche a livello locale**.

Per attivare il rilevamento di modifiche locali, selezionare la casella di spunta.

7.7.3 Disattivazione del rilevamento del traffico di rete sconosciuto

È possibile impedire che il firewall riporti alla console di gestione il traffico di rete sconosciuto. Il firewall considera il traffico sconosciuto se non rileva regole relative ad esso.

Per impedire che il firewall riporti alla console di gestione il traffico di rete sconosciuto:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **General**, sotto **Blocco**, selezionare la casella di spunta **Utilizzo di checksum per l'autenticazione delle applicazioni**.
4. Sotto **Reportistica**, deselezionare la casella di spunta **Segnala le applicazioni sconosciute e il traffico alla console di gestione**.

7.7.4 Disattivazione del rilevamento degli errori del firewall

Importante: si sconsiglia la disattivazione permanente del rilevamento degli errori del firewall. Disattivare il rilevamento solo quando strettamente necessario.

Per impedire che il firewall riporti errori alla console di gestione:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **Generale**, sotto **Reportistica**, deselezionare la casella di spunta **Segnala errori alla console di gestione**.

7.7.5 Configurazione della messaggistica desktop

È possibile controllare quali messaggi il firewall visualizzi nel desktop tramite l'utilizzo di fumetti.

Fumetti relativi ad applicazioni sconosciute e traffico non vengono mostrati in modalità interattiva dal momento che le stesse informazioni vengono visualizzate nelle finestre di apprendimento.

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **Generale**, sotto **Messaggistica desktop**, svolgere una delle seguenti operazioni:
 - Per visualizzare i fumetti relativi ad allarmi ed errori del firewall, selezionare la casella di spunta **Mostra allarmi ed errori**.
 - Per visualizzare i fumetti relativi ad applicazioni sconosciute e traffico, selezionare la casella di spunta **Mostra applicazioni sconosciute e traffico**.

7.8 Log firewall

7.8.1 Visualizzatore di log firewall

Il visualizzatore di log di Sophos Client Firewall consente di visualizzare, filtrare e salvare dettagli relativi a:

- Tutte le connessioni
- Connessioni che sono state consentite o bloccate
- Eventi firewall
- Log di sistema

7.8.2 Apertura del visualizzatore di log firewall

- ❖ Nella **Home page**, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.

7.8.3 Configurazione log firewall

Per gestire la dimensione e i contenuti del database del log eventi del firewall:

1. Nella **Home page**, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Cliccare sulla scheda **Log**.
3. Per gestire la dimensione del database del log eventi del firewall, selezionare una delle seguenti opzioni:
 - Per consentire al database di crescere senza alcun limite, cliccare su **Mantieni tutti i record**.
 - Per cancellare i vecchi record, cliccare su **Elimina i record vecchi**, e poi configurare le **Impostazioni cancellazione log**.
4. Sotto **Impostazioni cancellazione log**, selezionare una o più delle seguenti opzioni:
 - Cliccare sulla casella di spunta **Elimina i record dopo**, e successivamente inserire o selezionare un numero nella casella **Giorni**.
 - Cliccare sulla casella di spunta **Mantieni non più di**, e successivamente inserire o selezionare un numero nella casella **Record**.
 - Cliccare sulla casella di spunta **Mantieni dimensioni entro**, e successivamente inserire o selezionare un numero nella casella **MB**.

7.8.4 Modifica dell'aspetto del visualizzatore del log del firewall

1. Nella **Home page**, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Dal menu **Visualizza**, cliccare su **Layout**.
3. Nella finestra di dialogo **Visualizza personalizzazione**, selezionare gli oggetti che si desidera nascondere o visualizzare:
 - L'**Albero della console** viene visualizzato nel riquadro a sinistra.
 - La **Barra degli strumenti** viene visualizzata nella parte alta del visualizzatore del log del firewall.
 - La **Barra delle descrizioni** viene visualizzata sopra i dati nel riquadro a destra.
 - La **Barra di stato** viene visualizzata nella parte bassa del visualizzatore del log del firewall.

7.8.5 Personalizzazione del formato dei dati

È possibile cambiare il formato utilizzato per visualizzare i seguenti oggetti relativi ai dati nei log del firewall:

- Visualizzare le porte sotto forma di numero o nome, per es. **HTTP** o **80**.
- Visualizzare le applicazioni come icone, percorsi file o entrambi.
- Specificare l'unità di misura utilizzata per visualizzare i dati relativi alla velocità del trasferimento dei dati, per es. **KByte** o **MByte**.
- Nascondere o visualizzare griglie

Per personalizzare il formato dei dati:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Dal menu **Visualizza**, cliccare su **Personalizza**.
3. Selezionare le opzioni desiderate.

7.8.6 Mostra o nascondi colonne nel visualizzatore di log firewall

1. Nella **Home** page, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Cliccare su un oggetto nell'albero della console che visualizzi colonne nel riquadro dei dettagli.
3. Nel menu **Visualizza**, selezionare **Aggiungi/rimuovi colonne**.
È anche possibile cliccare col tasto destro del mouse su tutte le intestazioni delle colonne.
4. Nella finestra di dialogo **Colonne**, svolgere una delle seguenti operazioni:
 - Per nascondere una colonna, deselezionare la relativa casella di spunta.
 - Per visualizzare una colonna, selezionare la relativa casella di spunta.

7.8.7 Riordinamento delle colonne nel visualizzatore di log firewall

1. Nella **Home** page, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Cliccare su un oggetto nell'albero della console che visualizzi colonne nel riquadro dei dettagli.
3. Nel menu **Visualizza**, selezionare **Aggiungi/rimuovi colonne**.
È anche possibile cliccare col tasto destro del mouse su tutte le intestazioni delle colonne.
4. Nella finestra di dialogo **Colonne**, cliccare sul nome di una colonna e poi su **Sposta su** o **Sposta giù** per cambiare la posizione della colonna.

Note

- È inoltre possibile riordinare le colonne nel riquadro dei dettagli utilizzando il mouse e trascinando l'intestazione della colonna a destra o sinistra della sua posizione originale. Quando si trascina una colonna, parti evidenziate tra le intestazioni delle colonne indicano la nuova posizione della colonna.
- È possibile cambiare le dimensioni delle colonne utilizzando il mouse per trascinare le intestazioni delle colonne.

7.8.8 Filtraggio dei record in un log firewall

È possibile classificare i record del log firewall creando un filtro.

Per filtrare i record del log firewall:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'albero della console, selezionare un log.
3. Nel menu **Azione**, cliccare su **Aggiungi filtro**.
4. Seguire le istruzioni della procedura guidata **Filtro**.

Il filtro appare nell'albero della console immediatamente sotto al nodo che si desiderava filtrare.

7.8.9 Esportazione di tutti i record da un log firewall

Per esportare tutti i record dal log firewall a un file di testo o CSV:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'albero della console, selezionare un log.
3. Cliccare col tasto destro del mouse sull'elenco dei record e poi cliccare su **Esporta tutti i record**.
4. Nel campo di testo **Nome file**, digitare un nome per il file.
5. Nell'elenco **Salva come**, cliccare sul tipo di file desiderato.

7.8.10 Esportazione di record selezionati da un log firewall

Per esportare record selezionati da un log firewall a un file di testo o CSV:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'albero della console, selezionare un log.
3. Selezionare i record che si desidera esportare.
Se i record si aggiornano rapidamente, nel menu **Visualizza**, deselezionare la casella di spunta **Aggiornamento automatico**.
4. Nel menu **Azione**, cliccare su **Esporta record selezionati**.

5. Nel campo di testo **Nome file**, digitare un nome per il file.
6. Nell'elenco **Salva come**, cliccare sul tipo di file desiderato.

8 Utilizzo di Sophos AutoUpdate

8.1 Aggiornamento immediato

Per impostazione predefinita, Sophos AutoUpdate è pianificato in modo da aggiornarsi ogni 5 minuti se si è connessi in maniera permanente alla rete aziendale, oppure ogni 60 minuti se si è connessi in maniera permanente ad internet.

Se si è in possesso di una connessione di tipo dial-up, Sophos AutoUpdate è impostato per eseguire gli aggiornamenti ogni qual volta connessi a Internet o alla rete, dopodiché ogni 60 minuti.

Per eseguire aggiornamenti immediati:

- ❖ Cliccare col tasto destro del mouse sull'icona nell'area di notifica di Sophos Endpoint Security and Control e poi cliccare su **Aggiorna ora**.

8.2 Pianificazione degli aggiornamenti

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

È possibile specificare la modalità o la frequenza degli aggiornamenti di Sophos AutoUpdate.

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Pianificazione**
3. Selezionare **Consenti aggiornamenti automatici** ed inserire la frequenza (in minuti) con la quale Sophos AutoUpdate eseguirà gli aggiornamenti.
Se l'aggiornamento dei file viene scaricato dalla rete aziendale, gli aggiornamenti avvengono ogni 5 minuti per impostazione predefinita. .
Se l'aggiornamento dei file avviene attraverso internet dal server di Sophos, Sophos AutoUpdate può fornire l'aggiornamento solamente ogni 60 minuti.

8.3 Impostazione di una fonte per gli aggiornamenti

Se si desidera che Sophos AutoUpdate esegua l'aggiornamento automatico, è necessario specificare la fonte da cui scaricare gli aggiornamenti.

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Percorso primario**.
3. Nell'elenco **Indirizzo**, inserire il percorso UNC o l'indirizzo web del server di aggiornamento.
Per scaricare gli aggiornamenti direttamente da Sophos tramite Internet, selezionare **Sophos** dall'elenco **Indirizzo**.
4. Nella casella **Nome utente**, digitare il **Nome utente** per l'account utilizzato per accedere al server di aggiornamento.
Se il **Nome utente** deve riportare il dominio, utilizzare la forma *dominio\nome utente*.

5. Nella casella **Password**, digitare e confermare la **Password**.

8.4 Impostazione di una fonte alternativa per gli aggiornamenti

È possibile impostare una fonte alternativa per gli aggiornamenti. Se Sophos AutoUpdate non riesce ad eseguire gli aggiornamenti dalla fonte consueta, tenterà di farlo da quella alternativa.

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Percorso secondario**.
3. Nell'elenco **Indirizzo**, inserire il percorso UNC o l'indirizzo web del server di aggiornamento.

Per scaricare gli aggiornamenti direttamente da Sophos tramite Internet, selezionare **Sophos** dall'elenco **Indirizzo**.

4. Nella casella **Nome utente**, digitare il **Nome utente** per l'account utilizzato per accedere al server di aggiornamento.

Se il **Nome utente** deve riportare il dominio, utilizzare la forma *dominio\nome utente*.

5. Nella casella **Password**, digitare e confermare la **Password**.

8.5 Aggiornamento tramite server proxy

Se Sophos AutoUpdate esegue gli aggiornamenti via Internet, è necessario inserire i dati del server proxy utilizzato per connettersi a Internet.

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Percorso primario** o **Percorso secondario**.
3. Cliccare su **Dati proxy**.
4. Selezionare la casella di spunta **Accedi al percorso tramite proxy**.
5. Inserire l'**Indirizzo** e il numero di **Porta** del server proxy.
6. Inserire il **Nome utente** e la **Password** che danno accesso al server proxy.

Se il Nome utente deve riportare il dominio, utilizzare la forma *dominio\nome utente*.

8.6 Aggiornamento tramite connessione dial-up

Per eseguire gli aggiornamenti tramite connessione dial-up a Internet:

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Pianificazione**
3. Selezionare **Verifica la disponibilità di aggiornamenti in fase di connessione**.

Sophos AutoUpdate esegue l'aggiornamento ogni qual volta ci si connetta a Internet.

8.7 Limitazione della larghezza di banda utilizzata per gli aggiornamenti

Per evitare che Sophos AutoUpdate occupi tutta la larghezza di banda quando è invece necessaria per altri motivi (quali scaricare la posta elettronica), è possibile limitarne la quantità utilizzata.

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Percorso primario** o **Percorso secondario**.
3. Cliccare su **Avanzate**.
4. Selezionare la casella di spunta **Limita occupazione di banda** e spostare l'indicatore in modo tale da indicare la quantità di larghezza di banda che Sophos AutoUpdate potrà utilizzare.

Nota: se si specifica una larghezza di banda superiore alla quantità disponibile, Sophos AutoUpdate utilizzerà tutta la larghezza di banda.

8.8 Log dell'attività di aggiornamento

È possibile configurare Sophos AutoUpdate in modo tale che registri l'attività di aggiornamento in un file di log.

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Log**.
3. Selezionare la casella di spunta **Crea log dell'attività di Sophos AutoUpdate**.
4. Nella casella **Dimensioni massime log**, digitare o selezionare la dimensione massima in MB del log.
5. Nell'elenco **Livello di log**, selezionare un log **Normale** o **Dettagliato**.

Il log dettagliato fornisce informazioni su molte più attività del normale, quindi il log si riempirà più rapidamente. Utilizzare questa opzione solo quando è necessario un log dettagliato per la risoluzione dei problemi.

8.9 Visualizzazione del file di log degli aggiornamenti

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Log**.
3. Cliccare su **Visualizza file di log**.

9 Utilizzo del Blocco rimozione Sophos

9.1 Informazioni sul blocco rimozione su questo computer

Il blocco rimozione consente di impedire a malware noto e utenti non autorizzati (amministratori locali e utenti con conoscenze tecniche limitate), la disinstallazione del software di sicurezza Sophos o la disabilitazione tramite l'interfaccia di Sophos Endpoint Security and Control.

Nota: Il blocco rimozione non è pensato per offrire protezione contro utenti con vaste conoscenze tecniche. Non offre protezione contro malware appositamente studiato per sabotare il rilevamento da parte del sistema operativo. Tale tipo di malware può essere rilevato solamente eseguendo la scansione per minacce e comportamenti sospetti. (Per ulteriori informazioni, consultare la sezione "Utilizzo di Sophos Anti-Virus").

Cosa implica il blocco rimozione per gli utenti del computer?

SophosUsers e SophosPowerUsers

Il blocco rimozione non influisce sui gruppi SophosUser e SophosPowerUser. Quando il blocco rimozione è attivo, essi potranno comunque eseguire tutte le operazioni alle quali sono normalmente autorizzati, senza bisogno di immettere la password blocco rimozione.

I SophosUser o SophosPowerUser non possono attivare o disattivare il blocco rimozione.

Per maggiori informazioni sulle operazioni che ciascun gruppo Sophos è autorizzato ad effettuare, consultare la sezione [Gruppi Sophos](#) a pagina 5.

SophosAdministrators

Se fate parte del gruppo SophosAdministrator siete autorizzati a disabilitare il blocco rimozione.

Se su questo computer viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control, i criteri blocco rimozione impostati sulla console determinano la configurazione e la password blocco rimozione. Se il blocco rimozione viene abilitato dalla console, chiedere la password al proprio amministratore se occorre eseguire qualcuna delle operazioni summenzionate.

I membri del gruppo SophosAdministrator devono conoscere la password blocco rimozione, se il blocco rimozione è abilitato, per effettuare le seguenti operazioni:

- Riconfigurare le impostazioni della scansione in accesso o del rilevamento di comportamenti sospetti in Sophos Endpoint Security and Control. Per ulteriori informazioni, consultare la sezione [Immettere la password blocco rimozione per configurare il software](#) a pagina 78.
- Disabilitazione blocco rimozione Per ulteriori informazioni, consultare la sezione [Disabilitazione blocco rimozione](#) a pagina 76.
- Disinstallare i componenti di Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate, o Sophos Remote Management System) dal Pannello di controllo. Per ulteriori informazioni, consultare la sezione [Disinstallazione del software di sicurezza Sophos](#) a pagina 79.

Un SophosAdministrator che non conosce la password potrà eseguire tutte le altre operazioni, eccetto quelle menzionate sopra.

Se il blocco rimozione non è attivo, ma la password blocco rimozione è già stata impostata, è necessario utilizzare l'opzione **Autentica utente** per autenticarsi prima di poter riattivare il blocco rimozione. Quando il blocco rimozione non è attivo, sono abilitate tutte le altre opzioni di configurazione disponibili per il vostro gruppo utente Sophos. Per ulteriori informazioni sulla riattivazione del blocco rimozione, consultare la sezione [Riattivazione blocco rimozione](#) a pagina 77

9.2 Abilitazione blocco rimozione

Importante: Se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Alla prima installazione di Sophos Endpoint Security and Control, il blocco rimozione è disabilitato. Se fate parte del gruppo SophosAdministrator siete autorizzati ad abilitare il blocco rimozione.

Per abilitare il blocco rimozione:

1. Sulla **Home** page, sotto **Blocco rimozione**, cliccate su **Configura blocco rimozione**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nella finestra di dialogo **Configurazione Blocco rimozione**, mettere la spunta nella casella **Attiva Blocco rimozione**.
3. Cliccare su **Imposta** sotto la casella **Password**. Immettere e confermare una nuova password nella finestra di dialogo **Password Blocco rimozione**.
La password consente agli utenti del computer di riconfigurare, disattivare o disinstallare Sophos Endpoint Security and Control.

Suggerimento: La password deve essere lunga almeno otto caratteri, e deve contenere numeri e lettere maiuscole e minuscole.

9.3 Disabilitazione blocco rimozione

Importante: Se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se fate parte del gruppo SophosAdministrator siete autorizzati a disabilitare il blocco rimozione.

Disabilitazione blocco rimozione:

1. Se non vi siete ancora autenticati, e l'opzione **Configura blocco rimozione** sulla **Home** page non è disponibile, seguite le istruzioni riportate in [Immettere la password blocco rimozione per configurare il software](#) a pagina 78 prima di passare alla fase 2.
2. Sulla **Home** page, sotto **Blocco rimozione**, cliccate su **Configura blocco rimozione**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
3. Nella finestra di dialogo **Configurazione Blocco rimozione**, mettere o togliere la spunta nella casella **Attiva Blocco rimozione** e fare clic su **OK**.

9.4 Riattivazione blocco rimozione

Importante: Se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per abilitare il blocco rimozione è necessario immetterne la password, se:

- In precedenza si è abilitato il blocco rimozione, creata una password per esso, e poi lo si è disabilitato.
- Una password blocco rimozione è stata creata nella console di gestione, ma il blocco rimozione non è attivo.

E' necessario essere membri del gruppo SophosAdministrator per attivare la password blocco rimozione.

Per riattivare il blocco rimozione:

1. Sulla **Home** page, sotto **Blocco rimozione**, cliccare su **Autenticare utente**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nella finestra di dialogo **Autenticazione Blocco rimozione**, immettere la password blocco rimozione e fare clic su **OK**.
3. Sulla **Home** page, sotto **Blocco rimozione**, cliccate su **Configura blocco rimozione**.
4. Nella finestra di dialogo **Configurazione Blocco rimozione**, mettere la spunta nella casella **Attiva blocco rimozione**.

Se si desidera cambiare la password blocco rimozione, cliccare su **Cambia** sotto la casella **Password**. Immettere e confermare una nuova password nella finestra di dialogo **Password Blocco rimozione**.

9.5 Informazioni sulla password blocco rimozione

Quando il blocco rimozione è attivo, è necessario immettere la password blocco rimozione se si desidera configurare la scansione in accesso, il rilevamento di comportamenti sospetti, o disattivare il blocco rimozione. E' necessario essere membri del gruppo SophosAdministrator per fare ciò.

La password blocco rimozione deve essere immessa solo dopo aver aperto Sophos Endpoint Security and Control. Se si chiude e poi si riapre Sophos Endpoint Security and Control, è necessario immettere nuovamente la password blocco rimozione.

Se si desidera disinstallare qualcuno dei componenti di Sophos Endpoint Security and Control, è necessario immettere la password blocco rimozione prima di poter disabilitare il blocco rimozione e disinstallare quindi il software.

Se il blocco rimozione è disattivato, ma la password blocco rimozione è stata impostata in precedenza, è necessario inserire la password prima di riattivare il blocco rimozione.

Per abilitare il blocco rimozione è necessario immetterne la password, se:

- In precedenza si è abilitato il blocco rimozione, creata una password per esso, e poi lo si è disabilitato.

- Una password blocco rimozione è stata creata nella console di gestione, ma il blocco rimozione non è attivo.

9.6 Immettere la password blocco rimozione per configurare il software

Quando il blocco rimozione è attivo, è necessario immettere la password blocco rimozione se si desidera configurare la scansione in accesso, il rilevamento di comportamenti sospetti, o disattivare il blocco rimozione. E' necessario essere membri del gruppo SophosAdministrator per fare ciò.

La password blocco rimozione deve essere immessa solo dopo aver aperto Sophos Endpoint Security and Control. Se si chiude e poi si riapre Sophos Endpoint Security and Control, è necessario immettere nuovamente la password blocco rimozione.

Se si desidera disinstallare qualcuno dei componenti di Sophos Endpoint Security and Control, è necessario immettere la password blocco rimozione prima di poter disabilitare il blocco rimozione e disinstallare quindi il software.

Se il blocco rimozione è disattivato, ma la password blocco rimozione è stata impostata in precedenza, è necessario inserire la password prima di riattivare il blocco rimozione.

Per immettere la password blocco rimozione ed autenticarsi:

1. Sulla **Home** page, sotto **Blocco rimozione**, cliccare su **Autenticare utente**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nella finestra di dialogo **Autenticazione Blocco rimozione**, immettere la password blocco rimozione e fare clic su **OK**.

9.7 Cambiare la password blocco rimozione

Importante: Se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

E' necessario essere membri del gruppo SophosAdministrator per cambiare la password blocco rimozione.

Per cambiare la password blocco rimozione

1. Se non vi siete ancora autenticati, e l'opzione **Configura blocco rimozione** sulla **Home** page non è disponibile, seguite le istruzioni riportate in [Immettere la password blocco rimozione per configurare il software](#) a pagina 78 prima di passare alla fase 2.
2. Sulla **Home** page, sotto **Blocco rimozione**, cliccate su **Configura blocco rimozione**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
3. Nella finestra di dialogo dei **Configurazione Blocco rimozione**, cliccare su **Cambia** sotto la casella **Password**.

4. Immettere e confermare una nuova password nella finestra di dialogo **Password Blocco rimozione**.

Suggerimento: La password deve essere lunga almeno otto caratteri, e deve contenere numeri e lettere maiuscole e minuscole.

9.8 Disinstallazione del software di sicurezza Sophos

Se il blocco rimozione è abilitato e si desidera disinstallare qualcuno dei componenti di Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate, o Sophos Remote Management System), è necessario immettere la password blocco rimozione per disabilitare il blocco rimozione e quindi disinstallare il software. Per disinstallare il software è necessario essere membri del gruppo SophosAdministrator.



Attenzione: Il software di sicurezza va disinstallato solo dietro consiglio del supporto tecnico di Sophos. Se si disinstalla il software, il computer resta senza protezione finché esso non viene installato di nuovo.

Per disinstallare il software di sicurezza Sophos quando il blocco rimozione è abilitato:

1. Sulla **Home** page, sotto **Blocco rimozione**, cliccare su **Autenticare utente**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nella finestra di dialogo **Autenticazione Blocco rimozione**, immettere la password blocco rimozione e fare clic su **OK**.
3. Sulla **Home** page, sotto **Blocco rimozione**, cliccate su **Configura blocco rimozione**.
4. Nella finestra di dialogo **Configurazione Blocco rimozione**, togliere la spunta nella casella **Attiva blocco rimozione** e fare clic su **OK**.

Il blocco rimozione è disattivato.

5. Nel **Pannello di controllo**, aprire **Installazione applicazioni**, individuare il software che si desidera rimuovere e fare clic su **Cambia/Rimuovi** or **Rimuovi**. Seguire le istruzioni per la disinstallazione del software.

9.9 Visualizzazione del log blocco rimozione:

Il log blocco rimozione mostra due tipi di evento:

- Eventi di autenticazione blocco rimozione riuscita, dove viene riportato il nome dell'utente autenticato e l'orario della autenticazione.
- Tentativi di sabotaggio falliti, dove vengono riportati i nomi dei componenti o dei prodotti Sophos oggetto di attacco, l'orario del tentativo e i dettagli dell'utente responsabile del tentativo.

E' necessario essere membri del gruppo SophosAdministrator per visualizzare il log blocco rimozione.

Visualizzazione del log blocco rimozione:

- ❖ Sulla **Home** page, sotto **Blocco rimozione**, cliccare su **Visualizza log blocco rimozione**.

Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.

Dalla pagina log, è possibile copiare il log negli appunti, oppure inviarlo per e-mail o stamparlo.

Per trovare un testo specifico all'interno del log, cliccare su **Trova** e inserire il testo desiderato.

10 Troubleshooting

10.1 Aggiornamento non riuscito

10.1.1 Mancato funzionamento di un aggiornamento

Per ulteriori informazioni sul mancato funzionamento di un aggiornamento, guardare il log dell'aggiornamento. Per informazioni su come svolgere questa operazione, consultare la sezione [Visualizzazione del file di log degli aggiornamenti](#) a pagina 74.

Le sezioni seguenti spiegano la ragione per cui l'aggiornamento può non riuscire, e come modificare le impostazioni per risolvere il problema.

- [Sophos Endpoint Security and Control contatta la fonte sbagliata per gli aggiornamenti](#) a pagina 81
- [Sophos Endpoint Security and Control non riesce ad utilizzare il server proxy](#) a pagina 81
- [L'aggiornamento automatico non è pianificato in modo corretto](#) a pagina 82
- [Il mantenimento della fonte degli aggiornamenti non viene curato](#) a pagina 82

10.1.2 Sophos Endpoint Security and Control contatta la fonte sbagliata per gli aggiornamenti

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Nella scheda **Percorso primario**, verificare che i dati relativi all'indirizzo e all'account siano quelli forniti dall'amministratore.
Per informazioni sulla configurazione del **Percorso primario**, consultare la sezione [Impostazione di una fonte per gli aggiornamenti](#) a pagina 72.

10.1.3 Sophos Endpoint Security and Control non riesce ad utilizzare il server proxy

Se Sophos Endpoint Security and Control esegue l'aggiornamento via Internet, è necessario accertarsi che possa utilizzare un eventuale server proxy.

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Nella scheda **Percorso primario**, cliccare su **Dati proxy**.
3. Assicurarsi che l'indirizzo del server proxy, il numero della porta e i dati dell'account siano corretti.
Per informazioni su come inserire dati proxy, consultare la sezione [Aggiornamento tramite server proxy](#) a pagina 73

10.1.4 L'aggiornamento automatico non è pianificato in modo corretto

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Pianificazione** (per informazioni sulla scheda **Operazione pianificata**, consultare la sezione [Pianificazione degli aggiornamenti](#) a pagina 72).
3. Se il computer è collegato alla rete, oppure se si esegue l'aggiornamento tramite una connessione Internet a banda larga, selezionare **Consenti aggiornamenti automatici** e inserire la frequenza di aggiornamento. Se si esegue l'aggiornamento tramite una connessione via modem, selezionare **Verifica la disponibilità di aggiornamenti in fase di connessione**.

10.1.5 Il mantenimento della fonte degli aggiornamenti non viene curato

L'azienda potrebbe aver spostato la directory (sulla rete o su un server web) dalla quale si eseguono gli aggiornamenti. In alternativa, è possibile che l'azienda non curi affatto il mantenimento della directory.

Se si ritiene che sia proprio questo il caso, contattare l'amministratore di rete.

10.2 Minaccia non rimossa

Se Sophos Anti-Virus non ha rimosso una minaccia dal computer, la causa può essere una delle seguenti.

La disinfezione automatica è disabilitata

Se Sophos Anti-Virus non ha tentato la disinfezione, verificare che la disinfezione automatica sia stata abilitata. Per abilitare la disinfezione automatica, consultare la sezione [Disinfezione](#) a pagina 38 e gli altri argomenti inclusi nella sezione [Disinfezione](#). la rimozione automatica di adware e PUA non è disponibile per la scansione in accesso.

Disinfezione non riuscita

Se Sophos Anti-Virus non è riuscito a rimuovere una minaccia ("Disinfezione non riuscita"), è possibile che non riesca a rimuovere quel tipo di minaccia o che l'utente non possieda diritti di accesso sufficienti.

È necessaria una scansione completa del computer

Prima che Sophos Anti-Virus rimuova una minaccia multicomponente dal computer, o rilevi una minaccia nei file precedentemente nascosti, potrebbe essere necessario eseguire una scansione completa del computer per determinare tutti i componenti della minaccia.

1. Per eseguire una scansione di tutte le unità disco, inclusi i settori di avvio, eseguire la **Scansione del computer**. Per informazioni, consultare la sezione [Esecuzione della scansione completa del computer](#) a pagina 17.
2. Se la minaccia non è stata totalmente rilevata, la causa può risiedere in diritti di accesso dell'utente insufficienti o nel fatto che alcune unità o cartelle del computer, contenenti i componenti della minaccia, sono escluse dalla scansione. Per informazioni, consultare la sezione [Esclusione dalla scansione in accesso di file, cartelle e unità](#) a pagina 9. Controllare

la lista degli oggetti esclusi dalla scansione. Se l'elenco contiene degli oggetti, rimuoverli e sottoporre di nuovo il computer a scansione.

L'unità rimovibile è protetta da scrittura

Se si tratta di un supporto rimovibile (per esempio un floppy disk o un CD), accertarsi che non sia protetto da scrittura.

Il volume NTFS è protetto da scrittura

In caso di file su un volume NTFS (Windows 2000 o successivo), accertarsi che questo non sia protetto da scrittura.

È stato segnalato un frammento di virus o spyware

Sophos Anti-Virus non rimuove i frammenti di virus/spyware perché non trova un'esatta corrispondenza con il virus/spyware. Consultare la sezione [Segnalato frammento di virus o spyware](#) a pagina 83.

10.3 Segnalato frammento di virus o spyware

Se viene segnalato un frammento di virus o spyware, fare quanto indicato di seguito:

1. Aggiornare immediatamente la protezione, in modo tale che Sophos Anti-Virus possieda i file di identità dei virus più recenti.
2. Eseguire la scansione completa del computer

■ [Aggiornamento immediato](#) a pagina 72

■ [Esecuzione della scansione completa del computer](#) a pagina 17

Se vengono segnalati ancora frammenti di virus o spyware, rivolgersi al supporto tecnico di Sophos per ricevere assistenza:

■ [Supporto tecnico](#) a pagina 94

La segnalazione di un frammento di virus o spyware indica che parte di un file corrisponde a parte di un virus o spyware. Le cause possibili sono tre.

Variante di un virus o spyware noto

Molti virus o spyware nuovi poggiano su esemplari esistenti, quindi frammenti di codice tipici di un virus o spyware noto possono sembrare parte di un nuovo codice. Se viene segnalato un frammento di virus o spyware, è possibile che Sophos Anti-Virus abbia rilevato un nuovo virus o spyware che potrebbe diventare attivo.

Virus danneggiato

Molti virus contengono bug nelle loro routine di replicazione che fanno sì che questi virus infettino i file in modo non corretto. Una parte inattiva del virus (anche considerevole) potrebbe apparire all'interno del file che la ospita e venire rilevata da Sophos Anti-Virus. Un virus danneggiato non riesce a diffondersi.

Database contenente un virus o spyware

Quando si esegue una scansione completa, Sophos Anti-Virus può segnalare la presenza di un frammento di virus o spyware all'interno di un file di database. In questo caso, non cancellare il database. Rivolgersi al supporto tecnico di Sophos per ricevere assistenza.

Per informazioni su come contattare il supporto tecnico, consultare la sezione [Supporto tecnico](#) a pagina 94.

10.4 Minaccia parzialmente rilevata

Per eseguire la scansione nel computer di unità disco, inclusi boot sector, eseguire la scansione completa del computer.

- [Esecuzione della scansione completa del computer](#) a pagina 17

Se la minaccia non è stata totalmente rilevata, la causa può risiedere nel fatto che alcune unità o cartelle del computer, contenenti i componenti della minaccia, sono escluse dalla scansione. Se nell'elenco delle esclusioni sono compresi alcuni di questi oggetti, rimuoverli ed eseguire nuovamente la scansione del computer.

- [Esclusione dalla scansione su richiesta di file, cartelle e unità](#) a pagina 15

Se la minaccia non viene ancora completamente rilevata, la causa può risiedere in diritti di accesso dell'utente insufficienti.

Sophos Anti-Virus può non essere in grado di rilevare completamente o rimuovere le minacce i cui componenti sono installati in unità di rete.

10.5 Adware o PUA scomparsi dalla quarantena

Se un adware o PUA rilevato da Sophos Anti-Virus è scomparso dal Gestore quarantena, senza che sia stata prima eseguita un'azione su di esso, l'adware o PUA potrebbe essere stato autorizzato o rimosso dalla console di gestione o da un altro utente. Controllare la lista degli adware e PUA autorizzati per verificare se l'applicazione è stata autorizzata. Per maggiori informazioni su come effettuare tale operazione, consultare [Autorizzazione all'utilizzo di adware e PUA](#) a pagina 26.

10.6 Il computer diventa lento

Se il computer è diventato molto lento, è possibile che un'applicazione potenzialmente indesiderata (PUA) sia in esecuzione nel computer e lo stia monitorando. Se nel computer è abilitata la scansione in accesso, è possibile inoltre che compaiano molti allarmi sul desktop relativi a un'applicazione potenzialmente indesiderata (PUA). Per risolvere il problema, procedere nel modo seguente.

1. Eseguire la **Scansione del computer** per rilevare tutti i componenti dell'applicazione indesiderata (PUA). Per informazioni, consultare la sezione [Esecuzione della scansione completa del computer](#) a pagina 17.

Nota: Se, dopo la scansione, l'applicazione (PUA) viene rilevata parzialmente, consultare [Minaccia parzialmente rilevata](#) a pagina 84, punto 2.

2. Rimuovere l'adware o PUA dal computer. Per maggiori informazioni su come effettuare tale operazione, consultare [Gestione di adware e PUA in quarantena](#) a pagina 30.

10.7 Impossibile accedere al disco con boot sector infetto

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per impostazione predefinita, Sophos Anti-Virus impedisce l'accesso ai supporti rimovibili i cui boot sector sono infetti.

Per consentire l'accesso (per es. per copiare file da un floppy infetto da un virus del boot sector):

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Scansione in accesso.**
2. Nella scheda **Scansione**, selezionare la casella di spunta **Consenti accesso alle unità con boot sector infetti.**

Importante: appena terminato l'accesso al disco, deselezionare la casella di spunta e rimuovere il disco dal computer, in modo tale che non provi a infettare nuovamente il computer al momento del riavvio.

10.8 Impossibile accedere ad alcune aree di Sophos Endpoint Security and Control

Se non si riesce a utilizzare o a configurare determinate aree di Sophos Endpoint Security and Control, ciò può essere dovuto al fatto che l'accesso a queste aree sia riservato ai membri di particolari gruppi di utenti Sophos.

Per ulteriori informazioni sui gruppi di utenti Sophos, consultare la sezione [Gruppi Sophos](#) a pagina 5.

10.9 Rimozione degli effetti secondari dei virus

La rimozione degli effetti secondari del virus dipende dal modo in cui il virus ha infettato il computer.

Effetti secondari dei virus

Alcuni virus non provocano effetti secondari, altri possono averne di così gravi da comportare il ripristino dell'hard disk.

Alcuni virus alterano i dati gradualmente. Questo tipo di alterazione può essere difficile da rilevare.

Cosa fare

È molto importante leggere l'analisi del virus sul sito web di Sophos e verificare con attenzione i documenti dopo aver effettuato la disinfezione. Consultare [Informazioni sulla disinfezione](#) a

pagina 41 per sapere come visualizzare, sul sito web di Sophos, i dettagli sugli effetti secondari dei virus.

È essenziale disporre di copie di backup attendibili. Se non si disponeva di tali copie prima dell'infezione, è necessario cominciare a crearle e conservarle in caso di future infezioni.

Talvolta è possibile recuperare i dati dai dischi danneggiati da un virus. Sophos fornisce delle utilità per la riparazione dei danni causati da alcuni virus.

Rivolgersi al supporto tecnico di Sophos per ricevere assistenza.

Per informazioni su come contattare il supporto tecnico, consultare la sezione [Supporto tecnico](#) a pagina 94.

10.10 Rimozione degli effetti secondari di adware e PUA

La rimozione di adware e PUA può comportare alcuni effetti secondari che non possono essere eliminati durante la disinfezione.

Il sistema operativo è stato modificato

Alcuni adware e PUA possono modificare il sistema operativo Windows, per esempio le impostazioni della connessione a Internet. Sophos Anti-Virus non sempre riesce a ripristinare le impostazioni con i valori precedenti all'installazione degli adware o PUA. Se, per esempio, un adware o PUA ha modificato la pagina iniziale del browser, Sophos Anti-Virus non può conoscere la pagina iniziale impostata in precedenza.

Utilità non rimosse

Alcuni adware e PUA possono installare nel computer delle utilità come i file .dll o .ocx. Se un'utilità è innocua (vale a dire, se non possiede le caratteristiche di adware e PUA), per esempio una libreria della lingua, e non è integrata nell'adware o PUA, Sophos Anti-Virus può non rilevarla come componente dell'adware o PUA stesso. In questo caso, il file non viene rimosso dal computer neanche dopo la rimozione dell'adware o PUA che l'ha installato.

L'adware o PUA fa parte di un programma necessario

Talvolta un oggetto, adware o PUA, fa parte di un programma installato intenzionalmente, ed è necessario affinché il programma funzioni correttamente. Se si rimuove l'adware o PUA, il programma potrebbe non venire più eseguito nel computer.

Cosa fare

È molto importante leggere l'analisi della minaccia sul sito web di Sophos. Per scoprire come visualizzare sul sito web di Sophos i dettagli sugli effetti secondari di adware o PUA, consultare la sezione . a pagina 41

Per poter ripristinare il sistema e le sue impostazioni allo stato preesistente, è necessario eseguire periodicamente il backup del sistema. È inoltre necessario eseguire copie di backup dei file eseguibili originali dei programmi che si desidera utilizzare.

Per ulteriori informazioni o consigli sulla rimozione degli effetti secondari di adware e PUA, rivolgersi al supporto tecnico di Sophos.

Per informazioni su come contattare il supporto tecnico, consultare la sezione [Supporto tecnico](#) a pagina 94.

10.11 Segnalato errore della password

Se si cerca di pianificare una scansione personalizzata e viene visualizzato un messaggio di errore relativo alla password, assicurarsi che:

- La password sia quella relativa all'account utente
- La password non sia vuota

Per assicurarsi che la password sia corretta, verificare le proprietà dell'account utente in **Account utente**, nel **Pannello di controllo**.

10.12 Messaggio di errore "Service failure"

Sintomi

Nell'area di notifica viene visualizzato uno dei seguenti messaggi di errore:

- Anti-virus and HIPS: service failure
- Firewall: service failure

Cause

Uno dei servizi di Sophos Endpoint Security and Control nel computer non è riuscito e deve essere riavviato.

Risoluzione del problema

1. Tramite Windows, aprire Servizi.
2. Effettuare una delle seguenti operazioni:
 - Se viene visualizzato un messaggio di errore `Anti-virus and HIPS: service failure`, cliccare col tasto destro del mouse su **Sophos Anti-Virus** e successivamente su **Riavvia**.
 - Se viene visualizzato un messaggio di errore `Firewall: service failure`, cliccare col tasto destro del mouse su **Sophos Client Firewall Manager** e successivamente su **Riavvia**.

Note

- Per aprire Servizi, cliccare su **Start**, successivamente su **Pannello di controllo**, cliccare due volte su **Strumenti di amministrazione** e poi due volte su **Servizi**.

10.13 Il database del log firewall è danneggiato

Sintomi

Mentre si utilizza il visualizzatore del log firewall, compare il messaggio di errore: "L'attuale database del log di Sophos Client Firewall è danneggiato".

Causa

Il database del log eventi del firewall si è danneggiato, ed ha bisogno di essere ricreato.

Risoluzione del problema

Per svolgere le seguenti operazioni, è necessario essere membri del gruppo Windows Administrators sul computer in questione.

1. Tramite Windows, aprire Servizi.
2. Con il tasto destro del mouse, cliccare su **Sophos Client Firewall** Manager, e successivamente cliccare su **Arresta**.
3. Mediante Windows Explorer, andare su C:\Documents and Settings\All Users\Application Data\Sophos\Sophos Client Firewall\logs.

Per visualizzare questa cartella nascosta, può essere necessario impostare in Windows Explorer la visualizzazione di file e cartelle nascosti.

4. Cancellare op_data.mdb.
5. In "Servizi", cliccare con il tasto destro del mouse su **Sophos Client Firewall** Manager, e poi cliccare su **Riavvia**.

Note

- Per aprire Servizi, cliccare su **Start**, successivamente su **Pannello di controllo**, cliccare due volte su **Strumenti di amministrazione** e poi due volte su **Servizi**.

11 Glossario

Adware e PUA	L'adware prevede la presentazione all'utente di messaggi pubblicitari, quali messaggi popup, che incidono sulla produttività degli utenti e sull'efficienza del sistema. Un'applicazione potenzialmente indesiderata (PUA) è un'applicazione che di per sé non è malevola, ma viene generalmente considerata inadatta per la maggior parte delle reti aziendali.
Analisi del comportamento in fase di esecuzione	Analisi dinamica svolta tramite il rilevamento del comportamento sospetto e del buffer overflow.
Applicazione attendibile	Applicazione a cui è concesso accesso alla rete completo e incondizionato.
Applicazione controllata	Un'applicazione la cui esecuzione nel computer è impedita dai criteri di sicurezza aziendali.
Applicazioni bloccate	Applicazioni controllate che la scansione in accesso "blocca" e di cui non consente l'utilizzo all'utente.
Barra delle descrizioni	Barra del visualizzatore del log che si trova sopra la vista dei dati e che contiene il nome dell'elemento della vista ad albero selezionato.
Checksum	Ogni versione di un'applicazione ha un checksum unico. Il firewall può utilizzare tale checksum per decidere se un'applicazione è consentita o meno.
Configurazione primaria	La configurazione del firewall utilizzata per la rete aziendale a cui l'utente si collega per svolgere il suo lavoro giornaliero.
Configurazione secondaria	La configurazione del firewall utilizzata quando gli utenti non sono connessi alla rete aziendale primaria, ma a una rete differente, quale la rete wireless di un hotel o aeroporto, oppure un'altra rete aziendale.
Content Control List (CCL)	Un set di condizioni che specificano il contenuto di un file, per esempio numeri di carte di credito o debito (bancomat) o conti corrente bancari simili ad altri tipi di dati che possono portare all'identificazione personale. Esistono due tipi di Content Control List: il Content Control List di SophosLabs e quello personalizzato.
Controllo dati	Funzione che riduce il rischio di perdita di dati accidentale dalle workstation. Questa funzione entra in azione quando l'utente di una workstation tenta di trasferire un file che soddisfa i parametri stabiliti da criteri e regole di controllo dei dati. Per esempio quando un utente cerca di copiare in un dispositivo di memorizzazione removibile un foglio elettronico contenente dati relativi ai clienti o cerca di caricare un documento contrassegnato

	come confidenziale in un account di web mail; in questi casi la funzione di controllo dei dati, se configurata in tal senso, bloccherà il trasferimento.
Controllo dei dispositivi	Funzione che riduce la perdita accidentale di informazioni dalle workstation e che limita l'introduzione di software esterni alla rete. Entra in azione quando l'utente di una workstation tenta di utilizzare nella propria workstation dispositivi di memorizzazione o di rete non autorizzati.
Corrispondenza	Equivale al contenuto definito in un Content Control List.
Criteri firewall	Impostazioni volute dalla console di gestione e che il firewall utilizza per monitorare la connessione del computer a Internet e ad altre reti.
disinfezione	La disinfezione elimina le minacce presenti nel computer rimuovendo i virus da file e boot sector, spostando o cancellando un file sospetto, o cancellando un oggetto adware o PUA. Non è tuttavia in grado di annullare le azioni eventualmente già compiute dalla minaccia. Non è disponibile per le minacce rilevate tramite la scansione della pagina web perché le minacce non vengono scaricate nel computer. Pertanto, in tali casi non è necessaria alcuna azione.
Disinfezione automatica	Disinfezione svolta senza l'intervento o il consenso dell'utente.
Disinfezione manuale	Disinfezione svolta tramite utilità di disinfezione specifiche o cancellando i file manualmente.
Dispositivi di memorizzazione	Dispositivi di memorizzazione rimovibili (per es. unità USB flash, lettori di schede per PC e unità hard disk USB), unità CD/DVD, unità floppy disk e dispositivi di memorizzazione rimovibili sicuri (per es. unità SanDisk Cruzer Enterprise, Kingston Data Traveller, IronKey Enterprise e IronKey Basic USB flash con cifratura dell'hardware).
Errore della scansione	Errore verificatosi durante la scansione di un file, per esempio quando viene negato l'accesso.
Evento firewall	Situazione che si verifica nel computer quando un'applicazione sconosciuta, o il sistema operativo, prova a comunicare con un altro computer tramite connessione di rete in una modalità non specificamente richiesta dalle applicazioni in esecuzione nel computer ricevente.
Evento minaccia	Rilevamento o disinfezione di una minaccia.
File di identità del virus (IDE)	File che consente a Sophos Anti-Virus di rilevare e rimuovere un determinato virus, worm, trojan o spyware.

File sospetto	File che presenta una serie di caratteristiche comunemente, ma non esclusivamente, riscontrate in virus.
Finestra di apprendimento	Una finestra di dialogo che chiede all'utente di scegliere se consentire o bloccare l'attività di rete quando un'applicazione sconosciuta richiede l'accesso alla rete.
Gestore autorizzazioni	Il modulo che consente di autorizzare adware e PUA, file sospetti, applicazioni sospette o buffer overflow.
Gestore quarantena	Il modulo che consente di visualizzare e gestire gli elementi messi in quarantena.
Host Intrusion Prevention System (HIPS)	Termine generale che indica l'analisi del comportamento prima dell'esecuzione ed in fase di esecuzione.
ICMP	Acronimo di "Internet Control Message Protocol". Un protocollo del livello di rete che fornisce la correzione di errori e altre informazioni relative all'elaborazione dei pacchetti IP.
Impostazioni cancellazione log	Impostazioni che controllano quando i dati vengono cancellati.
Impostazioni ICMP	Le impostazioni che determinano quali tipi di comunicazione di gestione della rete sono consentiti.
Impostazioni processo	Impostazioni che determinano se a processi modificati o nascosti debba essere concesso accesso alla rete.
Ispezione di stato	Tecnologia firewall che consente di aggiornare la tabella relativa alle connessioni di rete TCP e UDP attive. Il firewall consentirà l'accesso solo ai pacchetti che soddisfano uno stato di connessione noto; tutti gli altri verranno rifiutati.
Messaggistica istantanea	Categoria di applicazioni controllate che comprende applicazioni di messaggistica istantanea (per es. MSN).
Modalità di funzionamento	Impostazione che stabilisce se il firewall agisce in base all'input da parte dell'utente (modalità interattiva) o automaticamente (modalità non interattiva).
Modalità interattiva	La modalità in cui il firewall visualizza una o più finestre di apprendimento quando viene rilevato traffico di rete per cui non esiste alcuna regola.
Modalità non interattiva	Modalità in cui il firewall consente o blocca tutto il traffico di rete per cui non è stata rilevata alcuna regola.
NetBIOS	Acronimo di "Network Basic Input/Output System." Software che fornisce un'interfaccia tra il sistema operativo, il bus di I/O e la rete. Quasi tutte le LAN basate su Windows sono basate su NetBIOS.

Processo nascosto	Un'applicazione a volte ne avvia un'altra che svolga delle operazioni di accesso alla rete per lei. Applicazioni malevole possono utilizzare questa tecnica per eludere i firewall: avviano un'applicazione attendibile che consenta di accedere alla rete, piuttosto che tentare l'accesso esse stesse.
Protocollo di rete	Set di regole o standard progettati per consentire ai computer di connettersi tramite la rete e di scambiare informazioni col minor margine di errore possibile.
Rawsocket	I Rawsocket consentono ai processi di controllare tutti gli aspetti dei dati che inviano in rete e possono essere utilizzati per scopi malevoli.
Regola con elevata priorità	Regola applicata prima di qualsiasi regola globale o di applicazione.
Regola dei contenuti	Regola comprendente una o più Content Control List e indicante l'azione da intraprendere se l'utente cerca di trasferire in una destinazione specificata i dati che soddisfano tutte le Content Control List presenti nella regola.
Regola dell'applicazione	Una regola applicabile solo a pacchetti di dati trasferiti attraverso la rete a o da una particolare applicazione.
Regola di sistema	Regola applicata a tutte le applicazioni che consentirà o bloccherà le attività di rete di livello basso.
Regola personalizzata	Regola creata dall'utente per indicare le circostanze in cui l'esecuzione di un'applicazione è consentita.
Regole globali	Regole applicate a tutte le connessioni di rete e applicazioni non ancora in possesso di regole specifiche. Hanno priorità minore delle regole impostate nella pagina della LAN. Hanno priorità minore anche delle regole delle applicazioni (a meno che non diversamente indicato dall'utente).
Rilevamento di buffer overflow	Rileva attacchi di buffer overflow.
Rilevamento di comportamento sospetto	Analisi dinamica del comportamento di tutti i programmi in esecuzione sul sistema al fine di rilevare e bloccare le attività che appaiono sospette.
Rootkit	Trojan o tecnologia utilizzata per nascondere la presenza di un oggetto malevolo (processo, file, chiave di registro o porta di rete) all'utente del computer o all'amministratore.
Scansione completa	Scansiona tutte le parti di ciascun file.

Scansione dal menu del tasto destro del mouse	Scansione di file in Windows Explorer o nel desktop eseguiti tramite menu.
Scansione in accesso	il vostro principale metodo di protezione contro virus e altre minacce. Ogni qual volta si accede a un file (copia, salva, sposta o apri), Sophos Anti-Virus ne esegue la scansione e ne consente l'accesso solo se tale file non costituisce una minaccia per il computer o se è autorizzato per l'utilizzo.
Scansione normale	Scansiona solo le parti del file con maggiori probabilità di essere infettate da virus.
Scansione pianificata	Scansione del computer, o di parti di esso, eseguita ad orari fissi.
Scansione su richiesta	Scansione avviata dall'utente. È possibile utilizzare la scansione su richiesta per controllare tutto, da un file singolo all'intero computer.
Spyware	Programma che si autoinstalla sul computer di un utente utilizzando sotterfugi o tecniche di ingegneria sociale, per poi inviare informazioni da quel computer a terzi, senza il consenso dell'utente o a sua insaputa.
Tipo file true	Il tipo di file che viene verificato tramite l'analisi della sua struttura piuttosto che dell'estensione del nome. Si tratta di un metodo più affidabile.
Traffico sconosciuto	Forma di accesso alla rete da parte di un'applicazione o servizio per cui il firewall non ha rilevato alcuna regola.
Virus non identificato	Virus per il quale non esiste uno specifico file di identità.
Vista ad albero	Vista che controlla quali dati il visualizzatore di log mostra nella propria vista dei dati.
Vista dati	Vista che mostra dati diversi a seconda dell'elemento della vista ad albero selezionato.
Vista di log	Visualizzazione dei dati relativi agli eventi del database quali connessioni consentite o bloccate, il log di sistema e tutti gli allarmi che sono stati generati.
Voice over IP	Categoria di applicazioni controllate che comprende applicazioni di Voice over IP.

12 Supporto tecnico

È possibile ricevere supporto tecnico per i prodotti Sophos in ciascuno dei seguenti modi:

- Visitando il forum SophosTalk su <http://community.sophos.com/> e cercando altri utenti con lo stesso problema.
- Visitando la knowledge base del supporto Sophos su <http://www.sophos.it/support/>
- Scaricando la documentazione del prodotto su <http://www.sophos.it/support/docs/>
- Inviando un'e-mail a support@sophos.com, indicando il o i numeri di versione del software Sophos in vostro possesso, i sistemi operativi e relativi livelli di patch, ed il testo di ogni messaggio di errore.

13 Note legali

Copyright © 2010 Sophos Group. Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere riprodotta, archiviata in un sistema di recupero, o trasmessa, in alcuna forma o in alcun mezzo, elettronico o meccanico, inclusi fotocopie, registrazione e altri mezzi, salvo che da un licenziatario autorizzato a riprodurre la documentazione in conformità con i termini della licenza, oppure previa autorizzazione scritta del titolare dei diritti d'autore.

Sophos e Sophos Anti-Virus sono marchi registrati di Sophos Plc e Sophos Group. Tutti gli altri nomi citati di società e prodotti sono marchi o marchi registrati dei rispettivi titolari.

Il software Sophos descritto in questo documento comprende o può comprendere programmi di software concessi in licenza (o sottolicenza) all'utente secondo i termini della Common Public License (CPL), la quale, tra gli altri diritti, permette all'utente di avere accesso al codice sorgente. La CPL richiede, per qualsiasi software concesso in licenza secondo i termini della stessa, e distribuito in formato codice oggetto, che il codice sorgente di tale software venga messo a disposizione anche degli altri utenti del formato codice oggetto. Per qualsiasi software che rientri nei termini della CPL, il codice sorgente è disponibile tramite ordine postale inviandone richiesta a Sophos; per e-mail a support@sophos.com o tramite internet su <http://www.sophos.com/support/queries/enterprise.html>. Una copia dei termini per tali software è reperibile all'indirizzo <http://opensource.org/licenses/cpl1.0.php>

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

Indice

A

- abilitazione della scansione in accesso 12
- abilitazione finestre di apprendimento su checksum 55
- accesso ai dischi 85
- adware 84, 86
 - autorizzazione 26
 - Disinfezione automatica 39
 - ricerca di 23
- adware autorizzati, blocco 26
- adware in quarantena, gestione 30
- aggiornamento 72, 74, 81
- aggiornamento immediato 72
- aggiornamento tramite connessione dial-up 72
- aggiunta utenti ai gruppi Sophos 6
- Analisi del comportamento in fase di esecuzione 12
- Analisi delle minacce 41
- antivirus
 - configurazione degli allarmi e-mail 34
 - configurazione log eventi 36
 - configurazione messaggistica desktop 33
 - configurazione messaggistica SNMP 36
- applicazioni
 - autorizzazione 50
 - blocco 50
 - utilizzo per l'autenticazione di 63
- applicazioni controllate
 - autorizzazione 33
 - gestione 33
 - ricerca di 13
- autenticazione delle applicazioni, utilizzo di checksum per 63
- autorizzazione
 - adware 26
 - applicazioni 50
 - applicazioni controllate 33
 - browser web 48
 - buffer overflow 26, 32
 - comportamento sospetto 26, 32
 - condivisione stampanti 49
 - download del FTP 48
 - e-mail 47
 - file sospetti 26
 - processi nascosti 62

- autorizzazione (*continua*)

- PUA 26
- raw socket 63
- traffico LAN 48

- Autorizzazione

- Sito web 27

B

- blocco

- adware autorizzati 26
- applicazioni 50
- condivisione stampanti 60
- PUA autorizzate 26
- siti web malevoli 25

- Blocco rimozione

- abilitazione 76
- attivazione 76
- autenticazione utente 78
- come cambiare la password 78
- configurazione software 78
- disabilitazione 76
- disattivazione 76
- Disinstallazione del software di sicurezza Sophos 79
- Disinstallazione di Sophos Endpoint Security and Control 79
- immissione password 78
- Log 79
- panoramica 75
- riattivazione 77

- boot sector infetto 85

- browser web, autorizzazione 48

- buffer overflow

- autorizzazione 26, 32
- rilevamento 12

C

- cancellazione scansioni personalizzate 21

- checksum, utilizzo per l'autenticazione delle applicazioni 63

- comportamento sospetto

- autorizzazione 26, 32
- rilevamento 12

- comportamento sospetto in quarantena, gestione 32

- computer lento, risoluzione dei problemi 84

- condivisione file e stampanti, autorizzazione 49

- condivisione file e stampanti, blocco 60

condivisione file, autorizzazione 49
 condivisione file, blocco 60
 condivisione stampanti, autorizzazione 49
 condivisione stampanti, blocco 60
 configurazione 17

- reportistica centrale 65
- allarmi e-mail di antivirus 34
- diritti utente per Gestore quarantena 6
- log eventi dell'antivirus 36
- Log firewall 68
- log scansione 37
- messaggistica desktop relativa all'antivirus 33
- messaggistica SNMP relativa all'antivirus 36
- scansione in accesso 8
- scansioni personalizzate 19

 controllo dati, disabilitazione temporanea 44
 controllo dei dispositivi 42

- blocco bridging di rete 42
- dispositivi controllati 42

 creazione di scansioni personalizzate 18

D

diritti di accesso 5, 85
 diritti utente 5, 85
 diritti utente per Gestore quarantena, configurazione 6
 disabilitazione del firewall 47
 Disabilitazione della scansione 42
 disabilitazione della scansione alla ricerca di applicazioni controllate 13
 disabilitazione della scansione in accesso 12
 disinfezione 38, 82

- Risoluzione dei problemi 82

 Disinfezione automatica

- adware 39
- file sospetti 40
- PUA 39
- Spyware 38
- Virus 38

 Disinstallazione del software di sicurezza Sophos 79
 download del FTP, autorizzazione 48

E

e-mail, autorizzazione 47
 effetti secondari 86
 errore della password 87
 esclusione di oggetti dalla scansione in accesso 9

esclusione di oggetti dalla scansione su richiesta 15
 esecuzione della scansione dal menu del tasto destro del mouse 18
 esecuzione di scansioni complete di computer 17
 esecuzione di scansioni personalizzate 20
 esportazione di file di configurazione firewall 56
 esportazione di tutti i record dal visualizzatore del log firewall 70

F

file checksum scansionati, ripristino 8
 file di archivio, scansione 21
 file di configurazione firewall

- esportazione 56
- importazione 56

 file sospetti

- autorizzazione 26
- Disinfezione automatica 40
- ricerca di 23

 file sospetti in quarantena, gestione 31
 filtraggio dei messaggi ICMP 51
 filtraggio dei record 70
 finestre di apprendimento sui checksum

- abilitazione 55
- Modalità interattiva 54

 firewall

- disabilitazione 47

 Frammento 82

G

gestione delle applicazioni controllate 33
 gestione di adware in quarantena 30
 gestione di comportamento sospetto in quarantena 32
 gestione di file sospetti in quarantena 31
 gestione di PUA in quarantena 30
 Gestione di spyware in quarantena 28
 gestione di virus in quarantena 28
 Gestore quarantena 28
 gruppi di utenti 5, 85
 Gruppi Sophos 5

- Aggiunta di utenti 6

I

icona nell'area di notifica 81
 icone

- oggetti da esaminare 19

- importazione di file di configurazione firewall 56
- impostazione delle regole globali 57, 59, 62
- impostazione di una regola 58, 59
- informazioni sulla disinfezione 41
- Informazioni sulla disinfezione 41
- Informazioni sulla sicurezza 41
- Introduzione
 - cosa fare per prima cosa 46

L

- larghezza di banda utilizzata per gli aggiornamenti, limitazione 74
- limitazione della larghezza di banda utilizzata per gli aggiornamenti 74
- log degli aggiornamenti 74
- log della scansione personalizzata
 - visualizzazione 21
- Log firewall
 - configurazione 68
- log scansione
 - configurazione 37
 - visualizzazione 37

M

- messaggi ICMP
 - filtraggio 51
 - info su 51
- minaccia parzialmente rilevata 84
- modalità di funzionamento, cambia con interattiva 52
- Modalità interattiva
 - finestre di apprendimento sui checksum 54
 - messaggi su applicazioni 54
 - messaggi su raw socket 54
 - messaggi sui processi nascosti 53
 - messaggi sul protocollo 54
- modalità interattiva, abilitazione 52
- modalità interattiva, info su 52
- modalità non interattiva, cambia con 53

O

- oggetti sospetti, preautorizzazione 27

P

- Pagina iniziale 4
- pianificazione degli aggiornamenti 72

- pianificazione di una scansione 87
- pianificazione di una scansione personalizzata 20
- preautorizzazione di oggetti sospetti 27
- priorità regole 56
- processi nascosti, autorizzazione 62
- PUA 84, 86
 - autorizzazione 26
 - Disinfezione automatica 39
 - ricerca di 23
- PUA autorizzate, blocco 26
- PUA in quarantena, gestione 30

R

- raw socket, autorizzazione 63
- record del log
 - filtraggio 70
- regola
 - imposta 58, 59
- Regole globali
 - impostazione 57, 59, 62
- reportistica centrale, configurazione 65
- ricerca di adware e PUA 23
- ricerca di file sospetti 23
- ricerca di virus di Mac 22
- rilevamento di buffer overflow 12
- rilevamento di comportamento sospetto 12
- rilevamento parziale 84
- Rimozione degli effetti secondari di una minaccia 86
- rinomina scansioni personalizzate 21
- ripristino dei file checksum scansionati 8
- rootkit, ricerca 19

S

- scansione alla ricerca di applicazioni controllate 13
- scansione alla ricerca di applicazioni controllate, disabilitazione 13
- scansione dal menu del tasto destro del mouse 18
- scansione dal menu del tasto destro del mouse, configurazione 17
- scansione dal menu del tasto destro del mouse, esecuzione 18
- scansione dei file di archivio 21
- scansione di singoli oggetti 18
- scansione di tutti i file 22
- scansione di un singolo oggetto 18
- scansione in accesso
 - abilitazione 12

- scansione in accesso (*continua*)
 - configurazione 8
 - disabilitazione 12
 - esclusione di oggetti dalla 9
 - specificazione delle estensioni dei file 9
 - scansione in accesso e su richiesta, differenze 8
 - Scansione online di Sophos
 - Log 25
 - scansione per la ricerca di rootkit 19
 - scansione su richiesta
 - esclusione di oggetti dalla 15
 - specificazione delle estensioni dei file 14
 - scansione su richiesta, tipi di 14
 - scansioni complete di computer, esecuzione 17
 - scansioni personalizzate
 - configurazione 19
 - creazione 18
 - esecuzione 20
 - pianificazione 20
 - rimozione 21
 - rinomina 21
 - Segnalato frammento, risoluzione dei problemi 83
 - server primario 72
 - server proxy 73
 - server secondario 73
 - siti web malevoli
 - Protezione 25
 - Sito web
 - Autorizzazione 27
 - Sophos Endpoint Security and Control 3
 - Sophos Live Protection
 - abilitazione 24
 - attivazione 24
 - disabilitazione 24
 - Sophos Live Protection (*continua*)
 - disattivazione 24
 - panoramica 24
 - tecnologia in-the-cloud 24
 - sospensione della scansione 42
 - specificazione delle estensioni dei file per la scansione in accesso 9
 - Spyware
 - Disinfezione automatica 38
 - spyware in quarantena, gestione 28
 - supporto tecnico 94
- ## T
- tecnologia in-the-cloud 24
 - tipi di scansione su richiesta 14
 - traffico LAN, autorizzazione 48
 - tutti i file, scansione 22
- ## V
- Virus
 - Disinfezione automatica 38
 - Rimozione degli effetti secondari di una minaccia 85
 - virus di Mac, ricerca 22
 - virus in quarantena, gestione 28
 - Vista di log
 - Informazioni su 67
 - visualizzatore del log firewall
 - esportazione record 70
 - visualizzazione
 - log della scansione personalizzata 21
 - log scansione 37