SOPHOS

Cybersecurity made simple.

Sophos Enterprise Console

Guida in linea

Versione prodotto: 5.5

Sommario

Info su Sophos Enterprise Console....1
Guida all'interfaccia di Enterprise Console....2
- Layout dell'interfaccia utente....2
- Pulsanti della barra degli strumenti....2
- Pannello di controllo....4
- Icone dello stato di sicurezza....5
- Spostamenti all'interno della vista computer....6
- Icone elenco computer....7
- Filtraggio dei computer in base agli oggetti rilevati....8
- Ricerca di un computer in Enterprise Console....9
- Spostamenti nella vista Update Manager (gestore aggiornamenti)....10

Introduzione a Sophos Enterprise Console....11
Impostazione di Enterprise Console....13
- Gestione dei ruoli e dei sottoambienti....13
- Creazione e utilizzo dei gruppi....23
- Creazione e utilizzo dei criteri....26
- Individuazione dei computer nella rete....33
- Sincronizzazione con Active Directory....36
- Configurazione dell'URL di Sophos Mobile....43

Protezione dei computer....44
- Preparazione per l'installazione del software di sicurezza....44
- Rimozione del software di sicurezza prodotto da terzi....44
- Protezione automatica dei computer....45
- Localizzazione dei programmi di installazione per la protezione manuale dei computer....47
- Verifica della protezione della rete....47
- Come gestire computer con allarmi ed errori....50
- Immediata scansione e disinfezione dei computer....53

Aggiornamento dei computer....56
- Configurazione del gestore aggiornamenti....56
- Configurazione delle sottoscrizioni ai software....64
- Configurazione del criterio di aggiornamento....68
- Monitoraggio del gestore aggiornamenti....77
- Aggiornamento dei computer non aggiornati....78

Configurazione dei criteri....80
- Criterio antivirus e HIPS....80
- Criterio firewall....113
- Criterio del controllo applicazioni....144
- Criterio del controllo dati....147
- Criterio del controllo dispositivi....161
- Criteri blocco rimozione....169
- Criterio patch....172
- Criterio del controllo web....174
- Criterio di prevenzione degli exploit....182

Impostazione di allarmi e messaggi....186
- Impostazione degli allarmi relativi alle sottoscrizioni software....186
- Impostazione degli allarmi e-mail di antivirus e HIPS....187
- Impostazione della messaggistica SNMP di antivirus e HIPS....188
- Configurazione della messaggistica desktop di antivirus e HIPS....189
- Impostazione di allarmi e messaggi del controllo applicazioni....190
- Impostazione di allarmi e messaggi del controllo dati....190
- Impostazione di allarmi e messaggi per il controllo dispositivi....192
- Impostazione degli allarmi e-mail sullo stato della rete....193

Impostazione del pannello di controllo e degli allarmi e-mail relativi alla sincronizzazione con Active Directory.... 194
Configurazione del log eventi di Windows.... 194
Attivazione e disattivazione dei feedback a Sophos.... 195
Visualizzazione eventi.... 196
Visualizzazione degli eventi del controllo applicazioni.... 196
Visualizzazione di eventi del controllo dati.... 197
Visualizzazione degli eventi del controllo dispositivi.... 197
Visualizzazione degli eventi del firewall.... 198
Visualizzazione degli eventi del blocco rimozione.... 199
Eventi verifica patch.... 199
Visualizzazione degli eventi web.... 203
Eventi della prevenzione degli exploit.... 204
Esportazione dell'elenco eventi in un file.... 205
Esclusione di eventi dalla prevenzione degli exploit.... 205
Creazione dei report.... 207
Creazione di un nuovo report.... 207
Configurazione del report Cronologia allarmi ed eventi.... 208
Configurazione del report Riepilogo allarmi.... 209
Configurazione del report Allarmi ed eventi per nome oggetto.... 209
Configurazione del report Allarmi ed eventi per orario.... 210
Configurazione del report Allarmi ed eventi per percorso.... 211
Configurazione del report Criterio del computer non conforme.... 212
Configurazione del report Eventi in base all'utente.... 213
Configurazione del report Protezione dei computer gestiti.... 214
Report della gerarchia degli aggiornamenti.... 214
Pianificazione di un report.... 214
Esecuzione di un report.... 215
Visualizzazione di un report sotto forma di tabella o grafico.... 215
Stampa di un report.... 215
Esportazione del report in un file.... 215
Modifica del layout del report.... 216
Controllo.... 217
Abilitazione o disabilitazione del Controllo.... 218
Copia e stampa di dati da Enterprise Console.... 219
Copia dei dati dall'elenco dei computer.... 219
Stampa dei dati dall'elenco dei computer.... 219
Copia dei dettagli del computer.... 219
Stampa dei dettagli del computer.... 220
Risoluzione dei problemi.... 221
Mancata esecuzione da parte dei computer della scansione in accesso.... 221
Firewall disabilitato.... 221
Firewall non installato.... 221
Computer con allarmi in sospeso.... 222
Computer non gestiti dalla console.... 222
Impossibile proteggere i computer nel gruppo Nessun gruppo.... 223
Installazione di Sophos Endpoint Security and Control non riuscita.... 223
I computer non sono aggiornati.... 224
Impostazioni antivirus non applicate ai computer Mac.... 224
Le impostazioni antivirus non vengono applicate nei computer Linux e UNIX.... 224
Computer Linux o UNIX non conformi ai criteri.... 224
Una nuova scansione compare inaspettatamente in un computer Windows.... 225
Problemi di connettività e scadenza del tempo di attesa.... 225
Adware e PUA non vengono rilevati.... 225
Oggetto parzialmente rilevato.... 225
Allarmi frequenti relativi alle applicazioni potenzialmente indesiderate.... 226

Disinfezione non riuscita..... 226
Rimozione degli effetti secondari dei virus..... 227
Rimozione degli effetti secondari delle applicazioni.....227
Il controllo dati non rileva i file caricati tramite browser incorporati..... 228
Il controllo dati non esegue la scansione dei file caricati o allegati..... 228
Visualizzazione nella console di un gestore aggiornamenti disinstallato..... 228
Glossario.....229
Supporto tecnico..... 235
Note legali..... 236

Indice analitico.....237

1 Informazioni su Sophos Enterprise Console

Sophos Enterprise Console è una console singola e automatizzata che gestisce e aggiorna i software di sicurezza Sophos in computer con sistemi operativi Windows, Mac OS X, Linux e UNIX, oltre che ambienti virtuali VMware vShield.

Enterprise Console consente di:

- Protegge la rete contro attacchi di malware, tipi file e siti Web a rischio, traffico di rete malevolo, oltre che adware ed altre applicazioni potenzialmente indesiderate.
- Stabilire a quali siti web possano accedere i propri utenti, oltre che proteggere la rete da malware e impedire l'accesso a siti web inappropriati.
- Verificare quali applicazioni possano essere eseguite nella rete.
- Gestire nei computer la protezione del client firewall.
- Controllare i computer alla ricerca di patch mancanti.
- Ridurre la perdita accidentale di informazioni, come il trasferimento non intenzionale di dati sensibili da un computer all'altro.
- Impedire che gli utenti utilizzino nei computer dispositivi di memorizzazione esterni non autorizzati e tecnologie di connessione wireless.
- Impedire agli utenti di riconfigurare, disabilitare o disinstallare il software di sicurezza Sophos.

Nota
Alcune delle funzioni presentate qui sopra non saranno incluse in tutte le licenze. Se la si desidera utilizzare potrebbe essere necessario cambiare la propria licenza. Per maggiori informazioni sulle licenze disponibili, consultare le pagine Web www.sophos.com/it-it/products/enduser-protection-suites/how-to-buy.aspx e www.sophos.com/it-it/products/server-security/how-to-buy.aspx.

Copyright © Sophos Limited

2 Guida all'interfaccia di Enterprise Console

2.1 Layout dell'interfaccia utente

L'interfaccia utente di Enterprise Console è composta dalle seguenti aree:

Barra degli strumenti

La barra degli strumenti include opzioni di scelta rapida valide per i comandi più comuni che consentono l'esecuzione e la configurazione del software di sicurezza Sophos.

Per ulteriori informazioni, consultare la sezione Pulsanti della barra degli strumenti (pagina 2).

Pannello di controllo

Il **pannello di controllo** fornisce una visione d'insieme dello stato della protezione della rete.

Per ulteriori informazioni, consultare la sezione Pannello di controllo (pagina 4).

Elenco computer

L'elenco dei computer viene visualizzato in basso a destra. Ha due viste:

- La vista **Computer** visualizza i computer appartenenti al gruppo selezionato nel riquadro **Gruppi**, in basso a sinistra. Per ulteriori informazioni, consultare la sezione Spostamenti all'interno della vista computer (pagina 6).
- La vista **Update manager** visualizza i computer in cui è installato Sophos Update Manager. Per ulteriori informazioni, consultare la sezione Spostamenti nella vista Update Manager (gestore aggiornamenti) (pagina 10).

2.2 Pulsanti della barra degli strumenti

La seguente tabella descrive i pulsanti della barra degli strumenti. Alcuni pulsanti della barra degli strumenti sono disponibili solo in determinate circostanze. Per esempio, il pulsante **Proteggi** per installare software anti-virus e firewall, è disponibile solo se, nel riquadro **Gruppi** della vista **Computer**, viene selezionato un gruppo di computer.

Copyright © Sophos Limited

Pulsant barra degli strumen	Descrizione	Note
	Individuazione dei computer	Cerca i computer nella rete e li aggiunge alla console. Per ulteriori informazioni, consultare la sezione Individuazione dei computer nella rete (pagina 33).
	Crea gruppo	Crea un nuovo gruppo di computer. Per ulteriori informazioni, consultare la sezione Creazione di un gruppo (pagina 24).
	Visualizza/ Modifica criterio	Nel riquadro **Criteri**, apre il criterio selezionato per modificarlo. Per ulteriori informazioni, consultare la sezione Modifica di un criterio (pagina 31).
	Proteggi	Installa i software anti-virus e firewall nei computer selezionati dall'elenco dei computer. Per ulteriori informazioni, consultare la sezione Protezione automatica dei computer (pagina 45).
	Endpoint	Passa alla vista **Computer** nell'elenco dei computer. La vista **Computer** visualizza i computer del gruppo selezionato nel riquadro **Gruppi**. Per ulteriori informazioni, consultare la sezione Spostamenti all'interno della vista computer (pagina 6).
	Gestori aggiornamenti	Passa alla vista **Gestori aggiornamenti** nell'elenco dei computer. La vista **Gestori aggiornamenti** visualizza i computer in cui è installato Sophos Update Manager. Per ulteriori informazioni, consultare la sezione Spostamenti nella vista Update Manager (gestore aggiornamenti) (pagina 10).
	Panello di controllo	Mostra o nasconde il **Pannello di controllo**. Il **pannello di controllo** fornisce una visione d'insieme dello stato della protezione della rete. Per ulteriori informazioni, consultare la sezione Pannello di controllo (pagina 4).
	Report	Avvia **Update Manager** per poter creare report relativi ad allarmi ed eventi nella rete. Per ulteriori informazioni, consultare la sezione Creazione dei report (pagina 207).
	Sophos Central	Apre Sophos Central. Per informazioni su Sophos Central, consultare l'articolo 119598 della knowledge base. Per informazioni sulla migrazione a Sophos Central, consultare l'articolo 122264 della knowledge base.

Pulsant barra degli strumen	Descrizione	Note
	Sophos Mobile	Configurando l'URL di Sophos Mobile viene aperta la console Web di Sophos Mobile. Si tratta di una soluzione per la gestione dei dispositivi mobili (quali smartphone e tablet) che aiuta a gestire le app e le impostazioni di sicurezza. Per ulteriori informazioni, consultare la sezione Configurazione dell'URL di Sophos Mobile (pagina 43).

2.3 Pannello di controllo

Il **Pannello di controllo** include i seguenti riquadri:

Pannello di controllo	Descrizione
Computer	Mostra il numero totale di computer in rete e il numero di computer connessi, gestiti e non gestiti. Per visualizzare l'elenco dei computer gestiti, non gestiti, connessi o di tutti i computer, cliccare su uno dei collegamenti nell'area **Computer**.
Aggiornamenti	Mostra lo stato dei gestori degli aggiornamenti.
Computer con allarmi	Mostra il numero e la percentuale dei computer gestiti che presentano allarmi relativi a: • Virus e spyware noti e sconosciuti • File e comportamenti sospetti • Adware e altre applicazioni potenzialmente indesiderate Per visualizzare l'elenco dei computer gestiti aventi allarmi in sospeso, cliccare sul titolo del riquadro **Computer con allarmi**.
Computer oltre la soglia di evento	Mostra il numero di computer che presentano eventi che hanno superato la soglia negli ultimi sette giorni. Per visualizzare un elenco di computer con controllo dei dispositivi, dei dati, applicazioni controllate o eventi del firewall, cliccare su un link nella sezione **Computer oltre la soglia di evento**. **Nota** A seconda del tipo di licenza in possesso, alcuni dei tipi di eventi potrebbero non venire visualizzati.

Copyright © Sophos Limited

Pannello di controllo	Descrizione
Criteri	Visualizza il numero e la percentuale dei computer gestiti che presentano violazioni dei criteri di gruppo o errori di confronto dei criteri. Inoltre, visualizza i computer che non hanno ancora risposto ai nuovi criteri inviati loro dalla console. Per visualizzare l'elenco dei computer gestiti non conformi ai criteri, cliccare sul titolo del riquadro **Criteri**.
Protezione	Visualizza il numero e la percentuale dei computer connessi e gestiti nei quali Sophos Endpoint Security and Control o Sophos Anti-Virus non è aggiornato o utilizza file dati sconosciuti per la rilevazione delle minacce. Per visualizzare l'elenco dei computer gestiti e non aggiornati, cliccare sul titolo del riquadro **Protezione**.
Errori	Visualizza il numero e la percentuale dei computer gestiti che presentano errori in sospeso della scansione, dell'aggiornamento o del firewall. Per visualizzare l'elenco dei computer gestiti con allarmi del prodotto Sophos in sospeso, cliccare sul titolo del riquadro **Errori**.

2.4 Icone dello stato di sicurezza

La seguente tabella descrive le icone dello stato di sicurezza visualizzate nel **Pannello di controllo** e nella barra di stato di Enterprise Console.

Icona stato di sicurezza	Descrizione
	Normale Il numero di computer interessati è al di sotto del livello di avviso.
	Avviso È stato superato il livello di avviso.
	Critico È stato superato il livello critico.

Icone di stato del Pannello di controllo

Viene visualizzata un'icona di stato nel **Pannello di controllo**, situata nell'angolo in alto a destra. Mostra lo stato dell'area di sicurezza rappresentata dal pannello.

L'icona di stato di una sezione del **Pannello di controllo** mostra lo stato più grave tra quelli visualizzati, ossia:

- L'indicatore di stato di una sezione passa da **Normale** ad **Avviso** quando viene superato il livello di avviso per almeno un indicatore all'interno della sezione.
- L'indicatore di stato di una sezione passa da **Avviso** a **Critico** quando viene superato il livello critico per almeno un indicatore all'interno della sezione.

Icona dello stato della rete

L'icona dello stato della rete viene visualizzata a destra della barra di stato di Enterprise Console. Mostra lo stato di sicurezza generale della rete.

L'indicatore di stato della rete mostra lo stato più grave tra quelli delle varie sezioni del **Pannello di controllo**, ossia:

- L'icona dello stato della rete passa da **Normale** ad **Avviso** quando viene superato il livello di avviso per almeno un indicatore all'interno del pannello di controllo.
- L'icona dello stato della rete passa da **Avviso** a **Critico** quando viene superato il livello critico per almeno un indicatore all'interno del pannello di controllo.

Alla prima installazione o al primo upgrade di Enterprise Console, il **Pannello di controllo** utilizza i livelli critico e di avviso predefiniti. Per configurare i livelli di avviso e critico, consultare la sezione Pannello di controllo (pagina 4).

È inoltre possibile impostare l'invio di allarmi e-mail a destinatari prescelti, nel caso in cui venga superato il livello di avviso o il livello critico per una sezione del **Pannello di controllo**. Per istruzioni consultare la sezione Impostazione degli allarmi e-mail sullo stato della rete (pagina 193).

2.5 Spostamenti all'interno della vista computer

Elenco computer

Nella **Vista computer**, l'elenco dei computer è formato dai computer endpoint facenti parte del gruppo selezionato nel riquadro **Gruppi**.

Questa vista include diverse schede. La scheda di **Stato** mostra se i computer sono protetti dalla scansione in accesso, se sono conformi ai criteri di gruppo, quali funzioni sono abilitate e se il software è aggiornato. Questa scheda visualizza anche eventuali allarmi. Le restanti schede forniscono maggiori dettagli su ciascuno degli argomenti sopra citati.

È possibile filtrare l'elenco di computer utilizzando il filtro **Visualizza**. Nell'elenco a discesa **Visualizza**, selezionare quale computer si desidera visionare. Per esempio, selezionare **Computer con potenziali problemi** per visualizzare i computer che presentano problemi.

È inoltre possibile filtrare l'elenco dei computer in base al nome degli oggetti rilevati, quali malware, applicazioni potenzialmente indesiderate, file sospetti. Per ulteriori informazioni, consultare la sezione Filtraggio dei computer in base agli oggetti rilevati (pagina 8).

È possibile eseguire cercare computer in base al loro nome, descrizione o indirizzo IP. Per ulteriori informazioni, consultare la sezione Ricerca di un computer in Enterprise Console (pagina 9).

Per spiegazioni relative alle icone visualizzate nell'elenco dei computer, consultare la sezione Icone elenco computer (pagina 7).

È possibile copiare o stampare i dati visualizzati nell'elenco dei computer. Per ulteriori informazioni, vedere Copia dei dati dall'elenco dei computer (pagina 219) e Stampa dei dati dall'elenco dei computer (pagina 219).

 Copyright © Sophos Limited

Riquadro Gruppi

Nel riquadro **Gruppi**, è possibile creare gruppi

e inserire i computer della rete in tali gruppi. È possibile creare propri gruppi o importare alberi di Active Directory, con o senza computer, per utilizzarli come gruppi di computer in Enterprise Console.

Per ulteriori informazioni, consultare la sezione Creazione e utilizzo dei gruppi (pagina 23).

Nessun gruppo

è riservato ai computer non ancora assegnati a un gruppo creato.

Riquadro Criteri

Nel riquadro **Criteri** è possibile creare o modificare i criteri applicati a gruppi di computer. Per ulteriori informazioni, consultare la sezione Creazione e utilizzo dei criteri (pagina 26).

2.6 Icone elenco computer

Allarmi

Icona	Descrizione
	Un simbolo d'allarme rosso visualizzato nella colonna **Allarmi ed errori**, nella scheda di **Stato**, indica che è stato rilevato un virus, worm, trojan, spyware o comportamento sospetto.
	Un simbolo d'allarme giallo visualizzato nella colonna **Allarmi ed errori**, nella scheda di **Stato**, indica uno dei seguenti problemi. • È stato rilevato un file sospetto. • È stata rilevata la presenza di adware o altre applicazioni potenzialmente indesiderate. • Si è verificato un errore. Un simbolo d'allarme giallo visualizzato nella colonna **Conformità al criterio** indica che il computer non sta utilizzando lo stesso criterio/criteri degli altri computer del gruppo.

In presenza di allarmi o errori multipli sullo stesso computer, nella colonna **Allarmi ed errori** sarà visualizzata l'icona d'allarme con priorità più alta. I tipi di allarme sono elencati qui sotto in ordine decrescente di priorità.

1. Allarmi virus e spyware
2. Allarmi da comportamento sospetto
3. Allarmi da file sospetti

4. Allarmi adware e PUA
5. Errori dell'applicazione del software (ad esempio, errori di installazione)

Se si ricevono più allarmi aventi il medesimo livello di priorità dallo stesso computer, l'allarme più recente verrà visualizzato nell'elenco dei computer.

Protezione disabilitata o non aggiornata

Un'icona grigia nella colonna di stato della funzione, nella scheda **Stato**, indica che la funzione è disabilitata. Per esempio, un'icona grigia a forma di scudo

nella colonna **In accesso**, indica che la scansione in accesso è disabilitata.

Un'icona a forma di orologio

nella colonna **Aggiornato** indica che il software è scaduto.

Stato computer

Icona	Descrizione
	Un computer con connettore verde indica che il computer è gestito da Enterprise Console.
	Un computer con clessidra gialla indica che l'installazione del software di sicurezza è in sospeso.
	Un computer con freccia gialla rivolta verso il basso indica che l'installazione del software di sicurezza è in corso.
	Il computer grigio indica che il computer non è gestito da Enterprise Console.
	Il computer con la croce rossa a fianco indica che il computer solitamente gestito da Enterprise Console è disconnesso dalla rete (i computer non connessi e non gestiti dalla console, non vengono visualizzati).

2.7 Filtraggio dei computer in base agli oggetti rilevati

È possibile filtrare l'elenco dei computer in base al nome degli oggetti rilevati, quali malware, applicazioni potenzialmente indesiderate, file sospetti. Far ciò configurando il filtro su "Computer gestiti interessati da...". Il filtro viene visualizzato nell'elenco a discesa **Visualizza** insieme ad altri filtri per computer.

Per configurare il filtro:

1. Nel menu **Strumenti**, cliccare su **Configura filtri**.
2. Nella finestra di dialogo **Consente di configurare filtri per elenchi di computer**, inserire il nome dell'oggetto rilevato in base a cui si desidera filtrare l'elenco. È possibile trovare i nomi degli oggetti rilevati nella rete:

Copyright © Sophos Limited

- Vista dell'elenco computer, scheda **Dettagli di allarmi ed errori**, colonna **Oggetto rilevato**.

  Ricordare che se il computer rileva più oggetti, la colonna **Oggetto rilevato** visualizzerà solo l'oggetto più recente e avente la priorità più elevata; tale oggetto potrebbe non essere quello in base a cui si desidera filtrare l'elenco.
- Finestra di dialogo **Risolvi allarmi ed errori**. Per aprire la finestra di dialogo, selezionare il/i computer dall'elenco computer o un gruppo di computer dal pannello **Gruppi**, cliccarvi col tasto destro del mouse, quindi cliccare su **Risolvi allarmi ed errori**.
- Finestra di dialogo **Dettagli del computer**. Per aprire la finestra di dialogo, cliccare due volte sul computer interessato. Quindi scorrere in giù fino alla sezione **Allarmi ed errori in sospeso**.
- **Report** (per es. **Riepilogo allarmi** o **Allarmi ed eventi per nome dell'oggetto**). Per aprire **Report Manager**, dal menu**Strumenti**, cliccare su **Gestisci report**.

È possibile utilizzare i caratteri jolly. Utilizzare ? per ogni singolo carattere e * per ogni stringa di caratteri. Per esempio, se si inserisce il testo "Mal*" e si applica il filtro, la vista dell'elenco dei computer visualizzerà solo i computer colpiti da malware il cui nome inizia per "Mal", quali "Mal/Conficker-A" e "Mal/Packer".

2.8 Ricerca di un computer in Enterprise Console

È possibile cercare uno o più computer in Enterprise Console in base a:

- Nome computer
- Descrizione computer
- Indirizzo IP

1. Per trovare un computer, svolgere una delle seguenti operazioni:
   - Premere CTRL+F.
   - Nel menu **Modifica**, cliccare su **Cerca computer**.
   - Cliccare all'interno dell'elenco dei computer, cliccare col tasto destro del mouse e quindi cliccare su **Cerca computer**.
2. Nella finestra di dialogo **Trova**, inserire i criteri della ricerca.

   Il campo **Oggetto ricerca** non distingue fra maiuscole e minuscole. I caratterre jolly all'inizio sono impliciti.

   È possibile utilizzare i caratteri jolly * e ?.

   Per esempio:

Criteri della ricerca	Risultati della ricerca
UKlapt	Cerca tutte le stringhe che iniziano per “uklapt”, per es. UKlaptop-011, UKlaptop-155, uklaptop132.
Ukla*	Cerca tutte le stringhe che iniziano per "ukla". Il carattere jolly è necessario in quanto presente implicitamete; la ricerca avrà gli stessi risultati di quella precedente, vale a dire UKlaptop-011, UKlaptop-155, uklaptop132.
***ukla**	Cerca tutte le stringhe che comprendono la dicitura “ukla”, per es. UKlaptop-011, 055uklax, 056-Dukla-sales.

Criteri della ricerca	Risultati della ricerca
Ukl*t	Cerca tutte le stringht che iniziano per “ukl”, comprendono una “t” e che terminano con un carattere qualsiasi, per es. UKlaptop-011, ukLite55.
?klap	Cerca tutte le stringhe che iniziano per un qualsiasi carattere singolo seguito da “klap” e terminanti per un carattere qualsiasi, per es. UKlaptop-011, uklapland33.
UKl??t	Cerca tutte le strinche che iniziano per “ukl”, seguito da due due caratteri, seguiti da “t” e terminate per un carattere qualsiasi, per es. UKlaptop-011, uklist101.

2.9 Spostamenti nella vista Update Manager (gestore aggiornamenti)

Elenco computer

Nella vista **Gestori aggiornamenti** è possibile impostare l'aggiornamento automatico del software di sicurezza Sophos dal sito web Sophos e visualizzare lo stato e i dettagli relativi ai gestori aggiornamenti.

L'elenco dei computer mostra i computer in cui è installato Sophos Update Manager.

Sottoscrizioni software

Utilizzare il riquadro **Sottoscrizioni software** per creare o modificare sottoscrizioni software che specifichino le versioni del software scaricate da Sophos per ogni piattaforma.

Copyright © Sophos Limited

3 Introduzione a Sophos Enterprise Console

Questa è una panoramica dei compiti da svolgere per proteggere la rete dopo avere installato Enterprise Console e completato la Procedura guidata di **download del software di sicurezza**. Per ulteriori informazioni sull'utilizzo di Enterprise Console, consultare il materiale e le sezioni citate.

Si consiglia di consultare la *Guida all'impostazione dei criteri di Sophos Enterprise Console* per informazioni sulle migliori pratiche per l'utilizzo e la gestione del software di sicurezza Sophos. La documentazione di Sophos è pubblicata alla pagina web http://www.sophos.com/it-it/support/documentation.

Se dopo l'installazione di Enterprise Console non è stata portata a termine la **procedura guidata di download del software di sicurezza**, consultare la sezione Esecuzione della procedura guidata di download del software di sicurezza (pagina 68).

Per proteggere la rete, seguire questi passaggi:

1. **Creare gruppi.**

   È possibile creare propri gruppi, uno per volta, o importare alberi di Active Directory, con o senza computer, per utilizzarli come gruppi di computer di Enterprise Console.

   Se si desidera importare gli alberi di Active Directory, consultare la sezione Importazione alberi e computer da Active Directory (pagina 33). Si consiglia, per prima cosa, di importare gli alberi da Active Directory senza i computer, assegnare poi i criteri di gruppo ai gruppi ed infine assegnare i computer ai gruppi, per es. sincronizzando i gruppi con Active Directory.

   Per informazioni su come creare gruppi manualmente, consultare la sezione Creazione e utilizzo dei gruppi (pagina 23).

2. **Impostare i criteri**

   Enterprise Console possiede un set di criteri predefiniti essenziali per mantenere la rete protetta. È possibile utilizzare, senza apportare modifiche, i criteri predefiniti di **Aggiornamento** e **Antivirus e HIPS**. Per configurare il criterio del firewall, eseguire la procedura guidata di **Configurazione dei criteri del Firewall**: Vedere Impostazione di un criterio del firewall di base (pagina 113).

3. **Individuare i computer nella rete e aggiungerli alla console.**

   Se sono stati importati alberi e computer da Active Directory, come descritto al passaggio 1, non è necessario fare altro. Altrimenti vedere la sezione Individuazione dei computer nella rete (pagina 33).

4. **Proteggere i computer.**

   È possibile scegliere quello preferito fra i due metodi di protezione dei computer in rete.

   - **Utilizzo della Procedura guidata per la protezione dei computer**

     Quando si trascina un computer dal gruppo **Nessun gruppo** in un altro gruppo, viene avviata una procedura guidata per la protezione dei computer. Vedere Protezione automatica dei computer (pagina 45).

   - **Protezione automatica del computer durante la sincronizzazione con Active Directory**

     Se si è scelto di effettuare la sincronizzazione con Active Directory è anche possibile proteggere i computer con sistema operativo Windows automaticamente. A tale scopo, utilizzare la **Procedura guidata di sincronizzazione con Active Directory** o la finestra di

dialogo **Proprietà della sincronizzazione**. Per istruzioni consultare la sezione Utilizzo della sincronizzazione per proteggere i computer automaticamente (pagina 40).

5. **Verificare che i computer siano protetti.**

   Quando l'installazione è terminata, controllare di nuovo l'elenco dei computer presenti nel nuovo gruppo. Nella colonna **Scansione in accesso** dovrebbe essere riportata l'indicazione "*Attivo/a*": ciò significa che il computer è protetto dalla scansione in accesso e che ora è gestito da Enterprise Console. Per ulteriori informazioni, consultare la sezione Verifica della protezione della rete (pagina 47).

6. **Disinfettare i computer.**

   Se sulla rete è stato rilevato un virus, un'applicazione indesiderata, o un altro problema, disinfettare i computer interessati come spiegato nella sezione Disinfezione immediata dei computer (pagina 54).

Opzioni aggiuntive di protezione

Per impostazione predefinita, Sophos Endpoint Security and Control rileva malware (virus, trojan, worm e spyware), adware, altre applicazioni potenzialmente indesiderate e traffico di rete malevolo. Può inoltre bloccare l'accesso a siti web noti per ospitare malware ed effettuare la scansione dei contenuti scaricati da Internet. È possibile abilitare ulteriori funzioni di protezione e funzioni utili per potenziare la produttività, secondo quanto descritto nella sezione Creazione e utilizzo dei gruppi (pagina 23).

Opzioni amministrative

In Enterprise Console è possibile impostare *ruoli* diversi, aggiungere diritti ai ruoli e assegnare utenti e gruppi di Windows ai ruoli. Il ruolo di Amministratore di sistema, comprendente il gruppo Sophos Full Administrators Windows, ha pieni diritti e non richiede impostazione. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile dividere il proprio ambiente IT in *sottoambienti* a cui assegnare i gruppi di computer di Enterprise Console. È quindi possibile controllare l'accesso ai sottoambienti assegnando loro utenti e gruppi Windows. Il sottoambiente **predefinito** comprende tutti i gruppi di Enterprise Console che include il gruppo **Nessun gruppo**. Per ulteriori informazioni sui sottoambienti, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Consiglio
Si consiglia anche di vedere i nostri video sull'impostazione e l'uso di Enterprise Console nel canale YouTube SophosGlobalSupport, sezione Sophos Enduser Protection.

Copyright © Sophos Limited

4 Impostazione di Enterprise Console

4.1 Gestione dei ruoli e dei sottoambienti

Importante
Se si utilizza l'amministrazione basata sui ruoli, è necessario possedere i diritti di **Amministrazione basata sui ruoli** per poter impostare ruoli e sottoambienti. Il ruolo di Amministratore di sistema, comprendente il gruppo Sophos Full Administrators Windows, ha pieni diritti e non richiede impostazione. Per ulteriori informazioni, vedere Ruoli preconfigurati (pagina 14) e Operazioni autorizzate dai diritti (pagina 17).

È possibile scegliere un accesso alla console basato sui ruoli impostando ruoli, aggiungendo diritti ai ruoli e assegnando loro utenti e gruppi Windows. Per esempio, un ingegnere di Help Desk può aggiornare e disinfettare i computer, ma non può configurare i criteri; responsabilità di un amministratore.

Per aprire Enterprise Console, un utente deve essere membro del gruppo Sophos Console Administrators ed essere assegnato ad almeno un ruolo e sottoambiente di Enterprise Console. I membri del gruppo Sophos Full Administrators hanno accesso completo ad Enterprise Console.

Nota
Se si desidera consentire all'utente l'utilizzo di un'Enterprise Console remota o aggiuntiva, consultare la sezione Utilizzo di Enterprise Console da parte di un altro utente (pagina 22).

È possibile creare ruoli personalizzati o utilizzare quelli preconfigurati.

È possibile assegnare lo stesso utente a più ruoli, aggiungendo ai ruoli un singolo utente o il gruppo di Windows a cui tale utente appartiene.

Se un utente non è in possesso dei diritti adeguati per svolgere una determinata operazione all'interno della console, potrà comunque visualizzare le impostazioni della configurazione relative a tale operazione. Un utente a cui non è assegnato alcun ruolo non può aprire Enterprise Console.

È inoltre possibile limitare i computer e i gruppi su cui l'utente può operare. È possibile dividere il proprio ambiente IT in sottoambienti a cui assegnare i gruppi di computer di Enterprise Console. È quindi possibile controllare l'accesso ai sottoambienti assegnando loro utenti e gruppi Windows. Il sottoambiente **predefinito** comprende tutti i gruppi di Enterprise Console che include il gruppo **Nessun gruppo**.

Un utente può visualizzare solo il sottoambiente a cui è assegnato. Se a uno stesso utente è stato assegnato più di un sottoambiente, tale utente può scegliere quale sottoambiente visualizzare (può visualizzare un sottoambiente alla volta). Il sottoambiente aperto in Enterprise Console è il *sottoambiente attivo*. Un utente non può modificare un criterio applicato al di fuori del proprio sottoambiente attivo.

Copyright © Sophos Limited

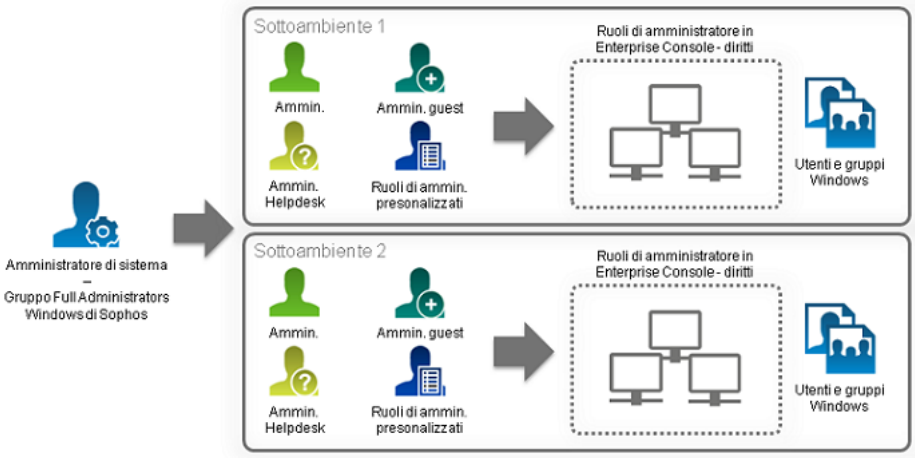


Figura 1: Ruoli e sottoambienti

4.1.1 Ruoli preconfigurati

In Enterprise Console esistono quattro ruoli preconfigurati:

Ruolo	Descrizione
Amministratore di sistema	Ruolo preconfigurato con pieni diritti di gestione del software di sicurezza Sophos nella rete e dei ruoli in Enterprise Console. Il ruolo Amministratore di sistema non può essere modificato e cancellato.
Amministratore	Ruolo preconfigurato con diritti di gestione del software di sicurezza Sophos nella rete, ma non dei ruoli in Enterprise Console. Il ruolo di Amministratore di sistema può essere rinominato, modificato o cancellato.
Helpdesk	Ruolo preconfigurato con soli diritti di correzione, per esempio di disinfezione e aggiornamento dei computer. Il ruolo di Helpdesk può essere rinominato, modificato o cancellato.
Ospite	Ruolo preconfigurato avente accesso in sola lettura a Enterprise Console. Il ruolo di Ospite può essere rinominato, modificato o cancellato.

È possibile modificare i ruoli di Amministratore, Helpdesk e Ospite o creare propri ruoli, secondo quanto descritto in Creazione di un ruolo (pagina 14).

4.1.2 Creazione di un ruolo

Se si sta già utilizzando l'amministrazione basata sui ruoli, per svolgere questa operazione, è necessario possedere i diritti di **Amministrazione basata sui ruoli**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Nel menu **Strumenti**, cliccare su **Gestisci ruoli e sottoambienti**.

Copyright © Sophos Limited

2. Nella finestra di dialogo **Gestisci ruoli e sottoambienti**, nel riquadro **Gestisci ruoli**, cliccare su **Crea**.
   Viene visualizzata la finestra di dialogo **Crea ruolo**.
3. Nel campo **Nome Ruolo**, inserire il nome del ruolo.
4. Nel riquadro **Diritti**, selezionare il diritto o i diritti che si desidera assegnare al ruolo e cliccare **Aggiungi**.
5. Nel riquadro **Utenti/Gruppi**, cliccare su **Aggiungi**.
6. Nella finestra di dialogo **Seleziona utente/gruppo**, inserire il nome di un utente o gruppo Windows da assegnare al ruolo. Cliccare su **OK**.

   Se necessario, assegnare allo stesso ruolo più utenti o gruppi, secondo quanto descritto ai punti 5 e 6.

4.1.3 Cancellazione di un ruolo

Se si sta già utilizzando l'amministrazione basata sui ruoli, per svolgere questa operazione, è necessario possedere i diritti di **Amministrazione basata sui ruoli**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Nel menu **Strumenti**, cliccare su **Gestisci ruoli e sottoambienti**.
2. Nella finestra di dialogo **Gestisci ruoli e sottoambienti**, nella scheda **Gestisci ruoli**, selezionare il ruolo che si desidera cancellare e cliccare su **Cancella**.

Nota
il ruolo preconfigurato di Amministratore di sistema non può essere cancellato.

4.1.4 Modifica di un ruolo

Se si sta già utilizzando l'amministrazione basata sui ruoli, per svolgere questa operazione, è necessario possedere i diritti di **Amministrazione basata sui ruoli**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Nel menu **Strumenti**, cliccare su **Gestisci ruoli e sottoambienti**.
2. Nella finestra di dialogo **Gestisci ruoli e sottoambienti**, nella scheda **Gestisci ruoli**, selezionare il ruolo che si desidera modificare e cliccare su **Modifica**.
   Viene visualizzata la finestra di dialogo **Modifica ruolo**.
3. Nel riquadro **Diritti**, assegnare diritti al ruolo o rimuovere i diritti esistenti a seconda della necessità.
4. Nel riquadro **Utenti/gruppi**, aggiungere al o rimuovere dal ruolo gli utenti e gruppi di Windows, a seconda della necessità.

4.1.5 Assegnazione di diritti a un ruolo

Se si sta già utilizzando l'amministrazione basata sui ruoli, per svolgere questa operazione, è necessario possedere i diritti di **Amministrazione basata sui ruoli**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Nel menu **Strumenti**, cliccare su **Gestisci ruoli e sottoambienti**.
2. Nella finestra di dialogo **Gestisci ruoli e sottoambienti**, nella scheda **Gestisci ruoli**, selezionare il ruolo a cui si desidera assegnare diritti e cliccare su **Modifica**.
   Viene visualizzata la finestra di dialogo **Modifica ruolo**.

3. Nel riquadro **Diritti**, nell'elenco **Diritti disponibili**, selezionare un diritto e cliccare su **Aggiungi**.

4.1.6 Creazione di un sottoambiente

Se si sta già utilizzando l'amministrazione basata sui ruoli, per svolgere questa operazione, è necessario possedere i diritti di **Amministrazione basata sui ruoli**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Nel menu **Strumenti**, cliccare su **Gestisci ruoli e sottoambienti**.
2. Nella finestra di dialogo **Gestisci ruoli e sottoambienti**, nel riquadro **Gestisci sottoambienti**, cliccare su **Crea**.
   Viene visualizzata la finestra di dialogo **Crea sottoambiente**.
3. Nel campo **Nome sottoambiente**, inserire il nome del sottoambiente.
4. Nel riquadro **Gruppi di Enterprise Console**, selezionare i gruppi che si desidera aggiungere al sottoambiente.
5. Nel riquadro **Utenti/gruppi**, cliccare su **Aggiungi** per aggiungere al sottoambiente utenti e gruppi di Windows.

4.1.7 Modifica di un sottoambiente attivo

Se assegnati a più di un sottoambiente, è possibile scegliere quale sottoambiente si desidera visualizzare all'apertura di Enterprise Console; è anche possibile passare da un sottoambiente all'altro in Enterprise Console.

È possibile visualizzare solo un sottoambiente alla volta. Quando si modifica il sottoambiente attivo, Enterprise Console viene ricaricata con un nuovo sottoambiente.

Per modificare il sottoambiente attivo:

1. Nel menu **Strumenti**, cliccare su **Seleziona sottoambiente attivo**.
2. Nella finestra di dialogo **Seleziona sottoambiente attivo**, selezionare il sottoambiente che si desidera aprire e cliccare su **OK**.

4.1.8 Modifica di un sottoambiente

Se si sta già utilizzando l'amministrazione basata sui ruoli, per svolgere questa operazione, è necessario possedere i diritti di **Amministrazione basata sui ruoli**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Nel menu **Strumenti**, cliccare su **Gestisci ruoli e sottoambienti**.
2. Nella finestra di dialogo **Gestisci ruoli e sottoambienti**, nella scheda **Gestisci sottoambienti**, selezionare il sottoambiente che si desidera modificare e cliccare su **Modifica**.
3. Nella finestra di dialogo **Modifica sottoambiente**, modificare il nome del sottoambiente, i gruppi di Enterprise Console inclusi nel sottoambiente o gli utenti e i gruppi di Windows con accesso al sottoambiente, secondo necessità. Cliccare su **OK**.

4.1.9 Copiatura di un sottoambiente

Se si sta già utilizzando l'amministrazione basata sui ruoli, per svolgere questa operazione, è necessario possedere i diritti di **Amministrazione basata sui ruoli**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

 Copyright © Sophos Limited

1. Nel menu **Strumenti**, cliccare su **Gestisci ruoli e sottoambienti**.
2. Nella finestra di dialogo **Gestisci ruoli e sottoambienti**, nella scheda **Gestisci sottoambienti**, selezionare il sottoambiente che si desidera copiare e cliccare su **Copia**.
   Nell'elenco dei sottoambienti compare una copia del sottoambiente.
3. Selezionare il sottoambiente appena creato e cliccare su **Modifica**. Rinominare il sottoambiente. Modificare i gruppi inclusi nel sottoambiente e/o gli utenti e i gruppi di Windows che vi possono accedere, se lo si desidera.

4.1.10 Eliminazione di un sottoambiente

Se si sta già utilizzando l'amministrazione basata sui ruoli, per svolgere questa operazione, è necessario possedere i diritti di **Amministrazione basata sui ruoli**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Nel menu **Strumenti**, cliccare su **Gestisci ruoli e sottoambienti**.
2. Nella finestra di dialogo **Gestisci ruoli e sottoambienti**, nella scheda **Gestisci sottoambienti**, selezionare il sottoambiente che si desidera cancellare e cliccare su **Cancella**.

   Non è possibile cancellare il sottoambiente **predefinito**.

4.1.11 Visualizzazione di ruoli di utenti o gruppi e sottoambienti

Per visualizzare i ruoli e i sottoambienti a cui è stato assegnato un utente o gruppo di Windows:

1. Nel menu **Strumenti**, cliccare su **Gestisci ruoli e sottoambienti**.
2. Nella finestra di dialogo **Gestisci ruoli e sottoambienti**, andare alla scheda **Visualizza utenti/gruppi** e cliccare sul pulsante **Seleziona utente/gruppo**.
3. Nella finestra di dialogo **Seleziona utente o gruppo**, selezionare un utente o gruppo di cui si desidera visualizzare ruolo e sottoambiente, quindi cliccare su **OK**.

4.1.12 Operazioni autorizzate dai diritti

Nota
A seconda del tipo di licenza in possesso, alcuni diritti potrebbero non essere applicabili.

Diritto	Operazioni
Controllo	Abilitazione del Controllo, disabilitazione del Controllo

Diritto	Operazioni
Ricerca computer, protezione e gruppo	Avvio della ricerca, blocco della ricerca e reperimento domini per la ricerca nella rete, ricerca per intervallo IP e Active Directory Importazione di computer e gruppi da Active Directory; importazione di gruppi da Active Directory Importazione nomi computer da file Cancellazione di un computer Protezione di un computer Sincronizzazione gruppo con Active Directory Modifica delle proprietà di sincronizzazione del gruppo Rimozione della sincronizzazione del gruppo Spostamento di un computer Creazione di un gruppo Rinomina di un gruppo Spostamento di un gruppo Cancellazione di un gruppo Assegnazione di un criterio a un gruppo
Personalizzazione del controllo dati	Creazione della regola del controllo dati Modifica della regola del controllo dati Copia della regola del controllo dati Cancellazione della regola del controllo dati Esclusione di file dalla scansione del controllo dati Creazione di una Content Control List Modifica di una Content Control List Copia di una Content Control List Cancellazione di una Content Control List
Eventi del controllo dati	Visualizzazione del visualizzatore eventi del controllo dati Visualizzazione degli eventi del controllo dati in dettagli computer

Copyright © Sophos Limited

Diritto	Operazioni
Impostazione criterio - antivirus e HIPS	Creazione di un criterio antivirus e HIPS Duplicazione di un criterio antivirus e HIPS Rinomina di un criterio antivirus e HIPS Modifica di un criterio antivirus e HIPS Ripristino delle impostazioni predefinite antivirus e HIPS Cancellazione di un criterio antivirus e HIPS Aggiunta o rimozione di una voce dall'elenco del master delle minacce
Impostazione criterio - controllo applicazioni	Creazione del criterio di controllo applicazioni Duplicazione del criterio di controllo applicazioni Rinomina del criterio di controllo applicazioni Modifica del criterio di controllo applicazioni Ripristino delle impostazioni predefinite del controllo delle applicazioni Cancellazione del criterio di controllo applicazioni
Impostazione criterio - controllo dati	Creazione del criterio del controllo dati Duplicazione del criterio del controllo dati Rinomina del criterio del controllo dati Modifica del criterio del controllo dati Ripristino delle impostazioni predefinite del controllo dati Cancellazione del criterio del controllo dati
Impostazione criterio - controllo dispositivi	Creazione del criterio del controllo dispositivi Duplicazione del criterio del controllo dispositivi Rinomina del criterio del controllo dispositivi Modifica del criterio del controllo dispositivi Ripristino delle impostazioni predefinite del controllo dispositivi Cancellazione del criterio del controllo dispositivi
Impostazione criterio - firewall	Creazione di un criterio firewall Duplicazione di un criterio firewall Rinomina di un criterio firewall Modifica di un criterio firewall Ripristino delle impostazioni predefinite del firewall Cancellazione di un criterio firewall

Copyright © Sophos Limited

Diritto	Operazioni
Impostazione criterio - patch	Creazione di un criterio patch Duplicazione di un criterio patch Rinomina di un criterio patch Modificare un criterio patch Ripristino delle impostazioni patch predefinite Cancellazione di un criterio patch
Impostazione dei criteri - Blocco rimozione	Creazione di un criterio del blocco rimozione Duplicazione di un criterio del blocco rimozione Rinomina di un criterio del blocco rimozione Modifica di un criterio del blocco rimozione Ripristino di impostazioni predefinite del blocco rimozione Cancellazione di un criterio del blocco rimozione
Impostazione criteri - aggiornamento	Creazione di un criterio di aggiornamento Duplicazione di un criterio di aggiornamento Rinomina di un criterio di aggiornamento Modifica di un criterio di aggiornamento Ripristino delle impostazioni predefinite di aggiornamento Cancellazione di un criterio di aggiornamento Creazione di una sottoscrizione Modifica di una sottoscrizione Rinomina di una sottoscrizione Duplicazione di una sottoscrizione Cancellazione di una sottoscrizione Configurazione dei gestori aggiornamenti
Impostazione criterio - controllo web	Creazione del criterio del controllo web Duplicazione del criterio del controllo web Rinomina del criterio del controllo web Modifica del criterio del controllo web Reimpostazione di un criterio del controllo web predefinito Cancellazione del criterio del controllo web

Copyright © Sophos Limited

Diritto	Operazioni
Impostazione criterio - prevenzione degli exploit	Creazione di un criterio di prevenzione degli exploit Duplicazione di un criterio di prevenzione degli exploit Rinomina di un criterio di prevenzione degli exploit Modifica di un criterio di prevenzione degli exploit Aggiunta di un'esclusione da attenuazione exploit Eliminazione di un'esclusione da attenuazione exploit Reimpostazione di un criterio di prevenzione degli exploit Eliminazione di un criterio di prevenzione degli exploit
Correzione - disinfezione	Rimozione oggetti rilevati Cancellazione allarmi Cancellazione errori
Azione correttiva - aggiornamento e scansione	Aggiornamento computer ora Esecuzione della scansione completa del sistema di un computer Computer conformi al criterio di gruppo Allineamento del gestore aggiornamenti alla configurazione Esecuzione immediata dell'aggiornamento da parte del gestore aggiornamenti
Riavvio della configurazione	Creazione, modifica o cancellazione di un report
Amministrazione basata sui ruoli	Creazione di un ruolo Rinomina di un ruolo Cancellazione di un ruolo Modifica dei criteri di un ruolo Aggiunta di un utente o gruppo a un ruolo Rimozione di un utente o gruppo da un ruolo Gestione sottoambiente: creazione di un sottoambiente; rinomina di un sottoambiente; cancellazione di un sottoambiente; aggiunta di un gruppo radice di un sottoambiente; rimozione di un gruppo radice di un sottoambiente; aggiunta di un utente o gruppo a un sottoambiente; rimozione di un utente o gruppo da un sottoambiente

Copyright © Sophos Limited

Diritto	Operazioni
Configurazione del sistema	Modifica delle impostazioni del server SMTP; test delle impostazioni del server SMTP; modifica dei destinatari di allarmi e-mail Configurazione degli avvisi del pannello di controllo e dei livelli critici Configurazione reportistica: configurazione della cancellazione di allarmi del database; impostazione del nome dell'azienda da visualizzare nei report Configurazione reportistica a Sophos: abilitazione o visualizzazione della reportistica a Sophos; modifica del nome utente; modifica dell'indirizzo e-mail di contatto Configurazione dell’uso delle versioni fisse di pacchetti software
Eventi web	Visualizzazione del visualizzatore eventi web Visualizzazione degli eventi web nella finestra di dialogo dei dettagli computer

4.1.13 Utilizzo di Enterprise Console da parte di un altro utente

I membri del gruppo Sophos Full Administrators hanno accesso completo ad Enterprise Console.

È possibile autorizzare all'uso di Enterprise Console anche altri utenti. Per aprire Enterprise Console, un utente deve:

- Essere membro del gruppo Sophos Console Administrators.
- Essere assegnato ad almeno un ruolo di Enterprise Console.
- Essere assegnato ad almeno un sottoambiente di Enterprise Console.

Se si desidera assegnare un utente al gruppo Sophos Console Administrators, usare i tool di Windows per aggiungerlo al gruppo.

Per assegnare un utente a un ruolo o sottoambiente di Enterprise Console, nel menu **Strumenti**, cliccare su **Gestisci ruoli e sottoambienti**. Per ulteriori informazioni su ruoli e sottoambienti, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per usare un'Enterprise Console remota o aggiuntiva, l'utente deve essere:

- Membro del gruppo Sophos Console Administrators sul server in cui è installato il server di gestione di Enterprise Console.
- Membro del gruppo Distributed COM Users sul server in cui è installato il server di gestione di Enterprise Console (il gruppo Distributed COM Users si trova nel contenitore Builtin del tool Active Directory Users and Computers).
- Assegnato ad almeno un ruolo di Enterprise Console.
- Assegnato ad almeno un sottoambiente di Enterprise Console.

Copyright © Sophos Limited

4.2 Creazione e utilizzo dei gruppi

Per proteggere e gestire i computer, è necessario, per prima cosa creare gruppi in cui collocare i computer stessi.

4.2.1 Utilità dei gruppi

I gruppi sono utili perché consentono di:

- Organizzare i computer in gruppi diversi che vengono aggiornati da diverse fonti o in base a pianificazioni diverse.
- Utilizzare diversi antivirus e HIPS, controllo applicazioni, firewall e altri criteri per gruppi differenti.
- Gestire più facilmente i computer.

Consiglio
è possibile creare gruppi all'interno di gruppi e applicare uno specifico insieme di criteri ad ogni gruppo e sottogruppo.

4.2.2 Gruppo

Un gruppo

è una cartella che contiene un certo numero di computer.

È possibile creare propri gruppi o importare alberi di Active Directory, con o senza computer, per utilizzarli come gruppi di computer in Enterprise Console. È possibile anche impostare la sincronizzazione con Active Directory in modo che i nuovi computer e alberi, oltre che le altre modifiche effettuate in Active Directory, vengano copiati automaticamente in Enterprise Console.

Ogni gruppo ha le proprie impostazioni relative ad aggiornamento, protezione antivirus e HIPS, protezione del firewall ecc. Tutti i computer di un gruppo dovrebbero utilizzare di regola le stesse impostazioni, chiamate "criterio".

Un gruppo può contenere sottogruppi.

4.2.3 Nessun gruppo

Nessun gruppo è il gruppo in cui Enterprise Console inserisce i computer prima che vengano assegnati ai gruppi.

Non è possibile:

- Applicare criteri al gruppo **Nessun gruppo**.
- Creare sotto gruppi all'interno del gruppo **Nessun gruppo**.
- Spostare o cancellare il gruppo **Nessun gruppo**.

Copyright © Sophos Limited

4.2.4 Creazione di un gruppo

Se si utilizza un'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per creare un nuovo gruppo di computer:

1. Nella vista **Computer,** nel riquadro **Gruppi** (lato sinistro della console), scegliere dove si desidera creare il gruppo.

   Se si desidera creare un nuovo gruppo al livello superiore, cliccare sul nome del computer in alto. Se si desidera creare un sottogruppo, cliccare su un gruppo esistente.
2. Cliccare sull'icona **Crea gruppo** posta sulla barra degli strumenti.
   Un "Nuovo Gruppo" viene aggiunto all'elenco, con il nome evidenziato.
3. Digitare il nome del gruppo.

I criteri di aggiornamento, antivirus e HIPS, di controllo applicazioni, firewall, patch, di controllo dati, di controllo dispositivi, blocco rimozione e web vengono applicati automaticamente al nuovo gruppo. È possibile modificare tali criteri oppure applicare criteri differenti. Vedere Modifica di un criterio (pagina 31) o Assegnazione di un criterio a un gruppo (pagina 30).

Nota
Se il nuovo gruppo è un sottogruppo, inizialmente utilizzerà le stesse impostazioni del gruppo nel quale si trova.

4.2.5 Aggiunta di computer a un gruppo

Se si utilizza un'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Selezionare i computer che si desidera aggiungere al gruppo. Per esempio, cliccare sul gruppo **Nessun gruppo** e selezionare i computer ivi contenuti.
2. Trascinare i computer e rilasciarli nel nuovo gruppo.

   Se i computer non protetti vengono spostati dal gruppo **Nessun gruppo** a un gruppo nel quale è impostato l'aggiornamento automatico, viene avviata una procedura guidata che accompagna durante l'installazione della protezione antivirus su questi computer.

   Se i computer vengono spostati da un gruppo all'altro, utilizzeranno gli stessi criteri dei computer già presenti nel nuovo gruppo.

4.2.6 Cancellazione di computer da un gruppo

Se si utilizza un'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile eliminare computer da un gruppo, per esempio se si desidera rimuovere voci relative a computer che non sono più in rete.

 Copyright © Sophos Limited

Importante
se si cancellano dei computer che sono ancora in rete, questi non compariranno più nell'elenco, né verranno gestiti dalla console.

Se si è effettuato l'upgrade da una versione precedente di Enterprise Console e sono presenti computer cifrati con una versione legacy della cifratura completa del disco gestita da Enterprise Console, non eliminare questi computer dalla console. In caso contrario potrebbe essere impossibile effettuare il recupero dei computer cifrati.

Per cancellare i computer, procedere come segue.

1. Selezionare i computer che si desidera cancellare.
2. Cliccarvi sopra con il tasto destro del mouse e selezionare **Cancella**.

Se si desidera visualizzare di nuovo i computer, cliccare sull'icona **Individuazione dei computer** posta sulla barra degli strumenti. Questi computer non risulteranno gestiti, fino al loro riavvio.

4.2.7 Tagliare e incollare un gruppo

Se si utilizza un'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Selezionare il gruppo che si desidera tagliare e incollare. Dal menu **Modifica**, cliccare su **Taglia**.
2. Selezionare il gruppo nel quale si desidera inserire quello tagliato. Dal menu **Modifica**, cliccare su **Incolla**.

4.2.8 Cancellazione di un gruppo

Se si utilizza un'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

I computer che si trovavano nel gruppo cancellato verranno posti nel gruppo **Nessun gruppo**.

1. Selezionare il gruppo che si desidera cancellare.
2. Cliccarvi sopra con il tasto destro del mouse e selezionare **Cancella**. Quando richiesto, confermare la cancellazione del gruppo e, nel caso che questo li possieda, anche dei relativi sottogruppi.

4.2.9 Rinomina di un gruppo

Se si utilizza un'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Selezionare il gruppo che si desidera rinominare.
2. Cliccarvi sopra con il tasto destro del mouse e selezionare **Rinomina**.

4.2.10 Criteri utilizzati da un dato gruppo

Per verificare quali criteri siano stati assegnati a un gruppo:

- Nel riquadro **Gruppi**, cliccare con il tasto destro del mouse sul gruppo. Selezionare **Visualizza/ Modifica dati dei criteri di gruppo**.

  Nella finestra di dialogo Dati del gruppo è possibile consultare i criteri attualmente in uso.

4.3 Creazione e utilizzo dei criteri

I criteri riuniscono le impostazioni applicate a tutti i computer di un gruppo.

Durante l'installazione di Enterprise Console, vengono creati criteri predefiniti che forniscono un livello di sicurezza di base. Tali criteri vengono applicati a tutti i gruppi creati dall'utente. È possibile modificare questi criteri predefiniti oppure crearne di nuovi.

Nota
Se non incluse nella licenza, alcune funzioni potrebbero non essere disponibili.

Per ogni tipo di gruppo è possibile creare più di un criterio.

È possibile inoltre applicare lo stesso criterio a più di un gruppo.

4.3.1 Criteri disponibili

Nota
Se non incluse nella licenza, alcune funzioni potrebbero non essere disponibili.

- I criteri di **Aggiornamento** stabiliscono la modalità in cui i computer vengono aggiornati con il nuovo software di sicurezza.
- Il criterio **Antivirus e HIPS** stabilisce come il software di sicurezza effettui la scansione dei computer alla ricerca di virus, trojan, worm, spyware, adware, applicazioni potenzialmente indesiderate, comportamenti e file sospetti e come li rimuova.
- I criteri del **Controllo applicazioni** stabiliscono quali applicazioni vengono bloccate e quali consentite nei computer.
- I criteri **Firewall** stabiliscono la modalità con la quale il firewall protegge i computer.
- Il criterio del **Controllo dati** specifica le regole per il monitoraggio o la restrizione del trasferimento di file, in base a contenuto, nome o tipo di file.
- Il criterio del **Controllo dispositivi** specifica quali dispositivi di archiviazione e di rete non sono autorizzati nelle workstation.
- Il criterio **Patch** indica se la verifica patch è abilitata e con quale frequenza i computer vengono sottoposti a verifica per rilevare eventuali patch mancanti.
- Il criterio del **Blocco rimozione** specifica la password che consente agli utenti autorizzati di riconfigurare, disabilitare o disinstallare il software di sicurezza di Sophos.
- Il criterio del **Controllo web** indica a quali siti web gli utenti possano accedere. Gli utenti riceveranno una notifica se tenteranno di accedere a siti configurati come "blocca" o "avvisa".
- Il criterio **Prevenzione degli exploit** specifica quali applicazioni, funzionalità e processi vengono protetti contro gli exploit, come ad esempio quando si proteggono file di documento contro il ransomware (CryptoGuard), oppure funzioni critiche nei browser web (Safe Browsing).

 Copyright © Sophos Limited

4.3.2 Criteri predefiniti

Dopo l'installazione di Enterprise Console, vengono creati criteri predefiniti.

Nota
Se non incluse nella licenza, alcune funzioni potrebbero non essere disponibili.

Criterio di aggiornamento

In una nuova installazione di Enterprise Console, il criterio di aggiornamento predefinito fornisce:

- L'aggiornamento automatico dei computer ogni 10 minuti dal percorso predefinito. Il percorso predefinito è una condivisione UNC `\\<NomeComputer>\SophosUpdate`, in cui NomeComputer è il nome del computer dove il gestore aggiornamenti è installato.

Criterio antivirus e HIPS

In una nuova installazione di Enterprise Console, il criterio antivirus e HIPS predefinito fornisce:

- La scansione in accesso alla ricerca do virus, trojan, worm, spyware e adware, oltre che altre applicazioni potenzialmente indesiderate (ma non file sospetti).
- Rilevamento di buffer overflow, comportamenti sospetti o malevoli di programmi in esecuzione nel sistema, oltre che traffico di rete malevole.
- Blocco dell'accesso a siti Web noti per ospitare malware.
- Scansione dei contenuti scaricati da Internet.
- La visualizzazione degli allarmi di sicurezza nell desktop del computer interessato e la loro aggiunta al log degli eventi.

Per un elenco completo di tutte le impostazioni predefinite relative ai criteri antivirus e HIPS presenti in una nuova installazione di Enterprise Console, consultare l'articolo 27267 della knowledge base.

Criteri di controllo applicazioni

Per impostazione predefinita, sono consentite tutte le applicazioni e i tipi di applicazione. La scansione in accesso per le applicazioni che si desidera controllare sulla rete è disabilitata.

Criteri firewall

Per impostazione predefinita Sophos Client Firewall è attivato e blocca tutto il traffico non essenziale. Dopo averlo utilizzato in tutta la rete, è necessario configurarlo per poter consentire le applicazioni che si desidera utilizzare. Vedere Impostazione di un criterio del firewall di base (pagina 113).

Per l'elenco completo di tutte le impostazioni predefinite del firewall, consultare l'articolo 57757 della knowledge base.

Criterio del controllo dati

Per impostazione predefinita, il controllo dati è disattivato e non è specificata alcuna regola che monitori o limiti il trasferimento di file su Internet o su dispositivi di memorizzazione.

Criterio del controllo dispositivi

Per impostazione predefinita, il controllo dispositivi è disattivato e tutti i dispositivi sono consentiti.

Criterio Patch

Per impostazione predefinita la verifica delle patch è disattivata, mentre la verifica dei nuovi criteri delle patch è attiva. Una volta che la verifica delle patch è attiva, i computer vengono controllati giornalmente alla ricerca di patch mancanti (a meno che non si siano apportate modifiche all'intervallo della verifica delle patch).

Criterio del blocco rimozione

Per impostazione predefinita, il blocco rimozione è disattivato e non viene richiesta alcuna password per consentire agli utenti autorizzati di riconfigurare, disattivare o disinstallare il software di sicurezza Sophos.

Criterio del controllo web

Per impostazione predefinita, il controllo web è disattivato e gli utenti possono consultare tutti i siti web il cui accesso non sia stato interdetto nella parte di Enterprise Console relativa alla Protezione web. Vedere Protezione web (pagina 102).

Criterio di prevenzione degli exploit

Per impostazione predefinita, la prevenzione degli exploit è attivata. Vedere Criterio di prevenzione degli exploit (pagina 182).

4.3.3 È necessario creare criteri personali?

Dopo l'installazione di Enterprise Console, vengono creati dei criteri "predefiniti". Tali criteri vengono applicati a tutti i gruppi creati dall'utente.

I criteri predefiniti offrono un livello di protezione di base, ma è necessario che gli utenti creino nuovi criteri o modifichino quelli predefiniti se desiderano utilizzare funzionalità quali il controllo dell'accesso alla rete o delle applicazioni.

Nota
quando si cambiano i criteri predefiniti, il cambiamento apportato verrà applicato a tutti i nuovi criteri creati.

Copyright © Sophos Limited

Nota
se si utilizza l'amministrazione basata sui ruoli, è necessario essere in possesso dei diritti di **Impostazione criterio** per poter creare o modificare un criterio. Per esempio, per creare o modificare un criterio antivirus e HIPS è necessario possedere i diritti di **Impostazione criterio - antivirus e HIPS**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Criterio di aggiornamento

I criteri di aggiornamento predefiniti fanno in modo che i computer controllino ogni 10 minuti la disponibilità di aggiornamenti per la sottoscrizione consigliata nella condivisione UNC del software di distribuzione. Per modificare sottoscrizioni, aggiornare percorsi e altre impostazioni, configurare i criteri di aggiornamento come descritto nella sezione Configurazione del criterio di aggiornamento (pagina 68).

Antivirus e HIPS

Il criterio predefinito antivirus e HIPS protegge i computer da virus e altro malware. Tuttavia, per abilitare il rilevamento di altre applicazioni o comportamenti non desiderati o sospetti, è consigliabile creare nuovi criteri, o modificare il criterio predefinito. Vedere Criterio antivirus e HIPS (pagina 80).

Controllo applicazioni

Per specificare e bloccare applicazioni non autorizzate, configurare i criteri del controllo applicazioni come indicato nella sezione Criterio del controllo applicazioni (pagina 144).

Criteri firewall

Per consentire l'accesso alla rete ad applicazioni attendibili, configurare i criteri del firewall come descritto nella sezione Criterio firewall (pagina 113).

Controllo dati

Per impostazione predefinita il controllo dati è disattivato. Per limitare il rischio di fuga di dati, configurare i criteri del controllo dati come descritto nella sezione Criterio del controllo dati (pagina 147).

Controllo dispositivi

Per impostazione predefinita il controllo dispositivi è disattivato. Per limitare i dispositivi hardware autorizzati, configurare i criteri del controllo dispositivi come indicato nella sezione Criterio del controllo dispositivi (pagina 161).

Copyright © Sophos Limited

Patch

Per impostazione predefinita la verifica delle patch è disattivata, mentre la verifica dei nuovi criteri delle patch è attiva. Una volta che la verifica delle patch è attiva, i computer vengono controllati giornalmente alla ricerca di patch mancanti (a meno che non si siano apportate modifiche all'intervallo della verifica delle patch). Per attivare o disattivare la verifica delle patch o modificare l'intervallo di verifica, configurare i criteri delle patch secondo quanto descritto nella sezione Criterio patch (pagina 172).

Blocco rimozione

Per impostazione predefinita, il blocco rimozione è disattivato. Per attivare il blocco rimozione, configurare i criteri del blocco rimozione come indicato nella sezione Criteri blocco rimozione (pagina 169).

Controllo web

Per impostazione predefinita, il controllo web è disattivato. Per attivare il controllo web e configurarne i criteri, consultare la sezione Criterio del controllo web (pagina 174).

Prevenzione degli exploit

Per impostazione predefinita, la prevenzione degli exploit è attivata. Per configurare criteri di prevenzione degli exploit, vedere Criterio di prevenzione degli exploit (pagina 182).

4.3.4 Creazione di un criterio

Se si utilizza l'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei relativi diritti di **Impostazione criteri**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per creare un criterio:

1. Nella vista **Computer**, nel riquadro **Criteri,** cliccare con il tasto destro del mouse sul tipo di criterio che si desidera creare, ad esempio, "Criterio di aggiornamento" e selezionare **Crea criterio**. Un "Nuovo criterio" viene aggiunto all'elenco, con il nome evidenziato.
2. Digitare un nuovo nome per il criterio.
3. Cliccare due volte sul nuovo criterio. Inserire le impostazioni desiderate.

   Per istruzioni su come scegliere le impostazioni, consultare la sezione relativa alla configurazione dei criteri.

Il criterio appena creato può ora essere applicato ai gruppi.

4.3.5 Assegnazione di un criterio a un gruppo

Se si utilizza un'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

 Copyright © Sophos Limited

1. Nel riquadro **Criteri**, evidenziare il criterio.
2. Cliccare sul criterio e trascinarlo sul gruppo al quale lo si desidera applicare. Quando richiesto, continuare con la procedura.

Nota
in alternativa, è possibile cliccare col tasto destro del mouse su un gruppo e selezionare **Visualizza/Modifica dati dei criteri di gruppo**. È quindi possibile scegliere i criteri per quel gruppo dai menu a discesa.

4.3.6 Modifica di un criterio

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei relativi diritti di **Impostazione criteri** per svolgere questa operazione.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per modificare un criterio per uno o più gruppi di computer:

1. Nel riquadro **Criteri**, cliccare due volte sul criterio che si desidera modificare.
2. Modificare le impostazioni.

Per istruzioni su come configurare criteri diversi, consultare le relative sezioni.

4.3.7 Rinomina di un criterio

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei relativi diritti di **Impostazione criteri** per svolgere questa operazione.
- Non è possibile rinominare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Nota
non è possibile rinominare un criterio "predefinito".

Per rinominare un criterio:

1. Nel riquadro **Criteri**, selezionare il criterio che si desidera rinominare.
2. Cliccarvi sopra con il tasto destro del mouse e selezionare **Rinomina criterio**.

4.3.8 Cancellazione di un criterio

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei relativi diritti di **Impostazione criteri** per svolgere questa operazione.
- Non è possibile cancellare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Nota
non è possibile cancellare un criterio "predefinito".

Per cancellare un criterio:

1. Nel riquadro **Criteri**, cliccare con il tasto destro del mouse sul criterio che si desidera cancellare e selezionare **Cancella criterio**.
2. Qualsiasi gruppo che utilizza il criterio cancellato tornerà a utilizzare quello predefinito.

4.3.9 Gruppi che utilizzano un dato criterio

Per sapere quali siano i gruppi ai quali è stato applicato un criterio in particolare:

- Nel riquadro **Criteri**, cliccare con il tasto destro del mouse sul criterio e selezionare **Visualizza gruppi che utilizzano il criterio**.

  Viene visualizzato l'elenco dei gruppi che utilizzano tale criterio.

4.3.10 Verifica che i computer utilizzino i criteri di gruppo

È possibile verificare se tutti i computer in un gruppo sono conformi ai criteri di tale gruppo.

1. Selezionare il gruppo che si desidera verificare.
2. Nell'elenco computer, vista **Computer** e scheda **Stato**, cercare nella colonna **Conformità al criterio**.
   - Se compare la dicitura "Come nel criterio", il computer è conforme ai criteri del gruppo di appartenenza.
   - Se vengono visualizzati un simbolo d'allarme giallo e la dicitura "Diverso dal criterio", il computer non sta utilizzando lo stesso o stessi criteri utilizzati dagli altri computer nel gruppo.

   Per maggiori informazioni relative allo stato delle funzioni di sicurezza nel computer e ai criteri applicati al computer, consultare le relative schede presenti nella vista **Computer**, per es. la scheda **Dettagli dell'antivirus**.

Se si desidera che i computer siano conformi ai criteri del gruppo a cui appartengono, consultare Allineamento dei computer ai criteri di gruppo (pagina 32).

4.3.11 Allineamento dei computer ai criteri di gruppo

Se si utilizza l'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Correzione - aggiornamento e scansione**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Se vengono rilevati computer non conformi ai criteri del gruppo di appartenenza, è possibile applicare i criteri del gruppo a tali computer.

1. Selezionare il o i computer non conformi ai criteri di gruppo.
2. Cliccarvi sopra con il tasto destro del mouse e selezionare **Allinea con**. Quindi selezionare il tipo di criterio adeguato, per es. **Criteri antivirus e HIPS di gruppo**.

 Copyright © Sophos Limited

4.4 Individuazione dei computer nella rete

Per poter gestire i computer in Enterprise Console, è per prima cosa necessario aggiungerli a Enterprise Console. È possibile utilizzare la funzione "Individuazione dei computer" e scegliere tra numerose opzioni che consentono di trovare i computer nella rete e di aggiungerli a Enterprise Console. Le opzioni sono le seguenti:

- Importazione alberi e computer da Active Directory (pagina 33)
- Individuazione dei computer tramite Active Directory (pagina 34)
- Individuazione dei computer cercando in rete (pagina 34)
- Individuazione dei computer per intervallo IP (pagina 35)
- Importazione nomi computer da file (pagina 35)

Se si utilizza un'amministrazione basata sui ruoli, per poter aggiungere computer alla console, è necessario essere in possesso dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

4.4.1 Importazione alberi e computer da Active Directory

Se si utilizza un'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

L'importazione di gruppi da Active Directory recupera la struttura ad albero di Active Directory e la copia in Enterprise Console come struttura di gruppi di computer. È possibile importare la sola struttura dei gruppi oppure gruppi e computer. Scegliendo la seconda opzione, i computer individuati in Active Directory vengono collocati nel rispettivo gruppo anziché nel gruppo **Nessun gruppo**.

È possibile disporre sia di gruppi "normali" da creare e gestire autonomamente, sia di gruppi importati da Active Directory. Inoltre, è possibile sincronizzare i gruppi importati con Active Directory.

Per importare gruppi da Active Directory, procedere come segue.

1. Nella barra degli strumenti, cliccare sull'icona **Individuazione dei computer**.
2. Nella finestra di dialogo **Individuazione dei computer**, nel riquadro **Importa da Active Directory**, selezionare **Importa** e cliccare su **OK**.

   In alternativa, selezionare un gruppo nel quale si desidera importare il o gli alberi di Active Directory, cliccarvi sopra con il tasto destro del mouse e selezionare **Importa da Active Directory**.

   Viene avviata la **Procedura guidata di importazione da Active Directory**.
3. Seguire le istruzioni della procedura guidata. Quando richiesto cosa importare, selezionare **Computer e alberi** o **Solo alberi**, a seconda di ciò che si desidera importare.

Dopo aver importato gli alberi da Active Directory, applicare i criteri ai gruppi. Vedere Criteri disponibili (pagina 26).

Dopo avervi applicato i criteri di gruppo, è possibile sincronizzare i gruppi con Active Directory, se lo si desidera. Per istruzioni consultare la sezione Sincronizzazione con Active Directory (pagina 36).

4.4.2 Individuazione dei computer tramite Active Directory

Se si utilizza un'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile utilizzare Active Directory per individuare i computer in rete ed aggiungerli nel gruppo **Nessun gruppo**.

1. Nella barra degli strumenti, cliccare sull'icona **Individuazione dei computer**.
2. Nella finestra di dialogo **Individuazione dei computer**, selezionare **Cerca con Active Directory** e cliccare su **OK**.
3. Viene richiesto di inserire nome utente e password. Questa operazione è necessaria se si possiedono computer (per es. Windows XP Service Pack 2) ai quali non si può accedere senza i dettagli dell'account.

   L'account deve appartenere all'amministratore di dominio, oppure deve disporre di diritti completi di amministrazione sui computer di destinazione con sistema operativo XP.

   Se si utilizza un account di dominio, *è necessario* inserire il nome utente nella forma dominio \utente.
4. Nella finestra **Individuazione dei computer**, selezionare i domini o gruppi di lavoro nei quali si desidera cercare i computer. Cliccare su **OK**.
5. Cliccare sul gruppo **Nessun gruppo** per visualizzare i computer trovati.

Per iniziare la gestione dei computer, selezionarli e trascinarli in un gruppo.

4.4.3 Individuazione dei computer cercando in rete

Se si utilizza un'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per aggiungere un elenco dei computer individuati nei domini e nei gruppi di lavoro Windows nel gruppo **Nessun gruppo**:

1. Nella barra degli strumenti, cliccare sull'icona **Individuazione dei computer**.
2. Nella finestra di dialogo **Individuazione dei computer**, selezionare **Cerca nella rete** e cliccare su **OK**.
3. Nella finestra di dialogo **Credenziali**, inserire il nome utente e la password di un account che possieda diritti sufficienti per recuperare le informazioni del computer.

   L'account deve appartenere all'amministratore di dominio, oppure deve disporre di diritti completi di amministrazione sui computer di destinazione. Se si utilizza un account di dominio, *è necessario* inserire il nome utente nella forma dominio\utente.

   È possibile saltare questo passaggio se si può accedere ai computer di destinazione senza fornire dettagli dell'account.
4. Nella finestra **Individuazione dei computer**, selezionare i domini o gruppi di lavoro nei quali si desidera cercare i computer. Cliccare su **OK**.
5. Cliccare sul gruppo **Nessun gruppo** per visualizzare i computer trovati.

Per iniziare la gestione dei computer, selezionarli e trascinarli in un gruppo.

 Copyright © Sophos Limited

4.4.4 Individuazione dei computer per intervallo IP

Se si utilizza un'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile utilizzare un intervallo di indirizzi IP per individuare i computer in rete ed aggiungerli al gruppo **Nessun gruppo**.

Nota
Non è possibile utilizzare gli indirizzi IPv6.

1. Nella barra degli strumenti, cliccare sull'icona **Individuazione dei computer**.
2. Nella finestra di dialogo **Individuazione dei computer**, selezionare **Cerca per intervallo IP** e cliccare su **OK**.
3. Nella finestra di dialogo **Credenziali**, viene richiesto di inserire nome utente e password. Questa operazione è necessaria se si possiedono computer (per es. Windows XP Service Pack 2) ai quali non si può accedere senza i dettagli dell'account.

   L'account deve appartenere all'amministratore di dominio, oppure deve disporre di diritti completi di amministrazione sui computer di destinazione con sistema operativo XP.

   Se si utilizza un account di dominio, *è necessario* inserire il nome utente nella forma dominio \utente.

   Nel riquadro **SNMP**, è possibile inserire il nome comunità SNMP.
4. Nella finestra di dialogo **Individuazione dei computer**, inserire **Inizio intervallo IP** e **Fine intervallo IP**. Cliccare su **OK**.
5. Cliccare sul gruppo **Nessun gruppo** per visualizzare i computer trovati.

Per iniziare la gestione dei computer, selezionarli e trascinarli in un gruppo.

4.4.5 Importazione nomi computer da file

Se si utilizza un'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per abilitare Enterprise Console alla creazione di un elenco dei propri computer, è possibile importare i nomi dei computer da un file. È possibile creare tale file utilizzando voci come queste:

```
[GroupName1]
 Domain1|Windows7|ComputerName1
 Domain1|Windows2008ServerR2|ComputerName2
```

Nota
non è necessario specificare in quale gruppo verranno collocati i computer. Se si inserisce `[]` (senza spazi fra le parentesi) per il nome del gruppo, i computer verranno collocati nel gruppo **Nessun gruppo**.

I nomi dei sistemi operativi validi sono: WindowsXP, Windows2003, WindowsVista, Windows7, WindowsServer2008, Windows2008ServerR2, Windows8, WindowsServer2012, Windows81, WindowsServer2012R2, Windows10, WindowsServer2016, MACOSX, Linux e Unix.

Il nome di dominio e il sistema operativo sono entrambi facoltativi. Quindi, una voce può avere questo formato:

```
[GroupName1]
 ComputerName1
```

Importare i nomi dei computer come segue.

1. Nel menù **File**, cliccare su **Importa computer dal file**.
2. Nella finestra del browser, selezionare il file.
3. Cliccare sul gruppo **Nessun gruppo** per visualizzare i computer trovati.
4. Per iniziare la gestione dei computer, selezionarli e trascinarli in un gruppo.

4.5 Sincronizzazione con Active Directory

Questa sezione fornisce una panoramica sulla sincronizzazione di Active Directory.

Utilità di Active Directory

Mediante la sincronizzazione con Active Directory, è possibile sincronizzare i gruppi di Enterprise Console con gli alberi di Active Directory. I nuovi computer e gli alberi di Active Directory verranno copiati automaticamente in Enterprise Console. È possibile scegliere di proteggere automaticamente i computer con sistema operativo Windows, aggiunti nell'albero di Active Directory in un secondo momento. Ciò consentirà di ridurre al minimo il tempo di esposizione dei computer alle infezioni e di ridurre la quantità di lavoro necessario per organizzare e proteggere i computer.

Nota
i computer con sistema operativo Windows per server, Mac OS, Linux o UNIX non saranno protetti automaticamente. Questi computer devono essere protetti manualmente.

Dopo aver impostato la sincronizzazione, è possibile impostare l'invio via e-mail ai destinatari prescelti di allarmi relativi ai nuovi computer e agli alberi individuati durante le sincronizzazioni future. Se si sceglie di proteggere automaticamente i computer dei gruppi sincronizzati di Enterprise Console, è possibile anche impostare allarmi relativi ai problemi della protezione automatica.

Funzionamento della sincronizzazione con Active Directory

In Enterprise Console, è possibile disporre sia di gruppi "normali" non sincronizzati da gestire autonomamente, sia di gruppi sincronizzati con Active Directory.

Durante l'impostazione della sincronizzazione, selezionare o creare un punto di sincronizzazione, un gruppo di Enterprise Console che sarà sincronizzato con un albero di Active Directory. Tutti i sottogruppi e i computer contenuti in Active Directory saranno copiati in Enterprise Console e mantenuti sincronizzati da Active Directory.

Nota
Per maggiori informazioni sui punti di sincronizzazione, v. Punto di sincronizzazione (pagina 38) Per maggiori informazioni sui gruppi sincronizzati, v. Gruppo sincronizzato (pagina 38)

 Copyright © Sophos Limited

Dopo aver impostato la sincronizzazione con Active Directory, la parte sincronizzata dei gruppi di Enterprise Console corrisponde esattamente con l'albero di Active Directory con cui è sincronizzata. Ciò significa che:

- Se un computer viene aggiunto all'albero di Active Directory, sarà visualizzato anche in Enterprise Console.
- Se un computer viene rimosso da Active Directory o spostato in un albero non sincronizzato, il computer viene spostato nel gruppo **Nessun gruppo** in Enterprise Console.

  Nota
  quando un computer viene spostato nel gruppo **Nessun gruppo**, non riceve più i nuovi criteri.

- Se un computer viene spostato da un albero sincronizzato all'altro, il computer stesso viene anche spostato da un gruppo di Enterprise Console all'altro.
- Se un computer esiste già in un gruppo di Enterprise Console quando viene sincronizzato per la prima volta, viene spostato da quel gruppo al gruppo sincronizzato che corrisponde alla sua posizione in Active Directory.
- Quando un computer viene spostato in un nuovo gruppo con criteri diversi, i nuovi criteri vengono inviati al computer.

Per impostazione predefinita, la sincronizzazione ha luogo ogni 60 minuti. È possibile modificare l'intervallo di sincronizzazione, se necessario.

Gestione della sincronizzazione

È a completa discrezione dell'utente decidere quali gruppi sincronizzare con Active Directory e quanti punti di sincronizzazione impostare; oltre che stabilire se le dimensioni dei gruppi che saranno creati siano gestibili. L'utente deve essere in grado di installare il software, esaminare e disinfettare i computer con facilità. Ciò riveste particolare importanza per l'installazione iniziale.

Nota
Se avete una struttura di Active Directory piuttosto complessa e desiderate sincronizzare i gruppi di dominio locali, oppure i gruppi di Active Directory inseriti in altri gruppi, si consiglia di consultare l'articolo 122529 della knowledge base per informazioni relative a come abilitare questa funzionalità.

Si consiglia di procedere come segue.

1. Importare la struttura dei gruppi (senza computer), utilizzando la funzione **Importa da Active Directory**. Per istruzioni consultare la sezione Importazione alberi e computer da Active Directory (pagina 33).
2. Rivedere la struttura dei gruppi importati e scegliere i punti di sincronizzazione.
3. Impostare criteri di gruppo e applicarli ai gruppi e sottogruppi. Per istruzioni consultare le sezioni Creazione di un criterio (pagina 30) e Assegnazione di un criterio a un gruppo (pagina 30).
4. Sincronizzare i punti prescelti di sincronizzazione, uno alla volta, con Active Directory. Per istruzioni consultare la sezione Sincronizzazione con Active Directory (pagina 38).

4.5.1 Punto di sincronizzazione

Un *punto di sincronizzazione* è un gruppo di Enterprise Console che punta a un albero (o sottoalbero) in Active Directory. Un punto di sincronizzazione può contenere gruppi sincronizzati importati da Active Directory.

Nel riquadro **Gruppi**, un punto di sincronizzazione apparirà nel modo seguente:

È possibile spostare, rinominare o cancellare un punto di sincronizzazione. Inoltre, è possibile modificare i criteri e le impostazioni della sincronizzazione, incluse le impostazioni della protezione automatica, per un punto di sincronizzazione.

Non è possibile creare o cancellare sottogruppi in un punto di sincronizzazione o spostare altri gruppi all'interno di esso. Non è possibile spostare i computer nel o dal punto di sincronizzazione.

4.5.2 Gruppo sincronizzato

Un *gruppo sincronizzato* è un sottogruppo di un punto di sincronizzazione, importato da Active Directory.

Nel riquadro **Gruppi**, un gruppo sincronizzato apparirà nel modo seguente:

È possibile modificare i criteri assegnati a un gruppo sincronizzato.

Non è possibile modificare le impostazioni di un gruppo sincronizzato se non i criteri di gruppo. Non è possibile rinominare, spostare o cancellare un gruppo sincronizzato. Non è possibile spostare computer o gruppi nel o dal gruppo. Non è possibile creare o cancellare sottogruppi nel gruppo. Non è possibile modificare le impostazioni della sincronizzazione per il gruppo.

4.5.3 Sincronizzazione con Active Directory

Prima di eseguire questa operazione:

- Se si utilizza un'amministrazione basata sui ruoli, è necessario disporre dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).
- Se si desidera proteggere automaticamente i computer che si trovano in gruppi sincronizzati, assicurarsi che i computer siano stati predisposti a tale scopo, secondo quanto descritto nella sezione Preparazione per l'installazione del software di sicurezza (pagina 44).
- Se avete una struttura di Active Directory piuttosto complessa e desiderate sincronizzare i gruppi di dominio locali, oppure i gruppi di Active Directory inseriti in altri gruppi, abilitare questa funzionalità secondo le istruzioni fornite nell'articolo 122529 della knowledge base.

Per effettuare la sincronizzazione con Active Directory procedere come riportato qui di seguito:

1. Selezionare un gruppo che fungerà da punto di sincronizzazione, cliccarvi sopra con il tasto destro del mouse e selezionare **Sincronizza con Active Directory**.
   Viene avviata la procedura guidata di **sincronizzazione con Active Directory**.

 Copyright © Sophos Limited

2. Nella pagina di **Panoramica** della procedura guidata, cliccare su **Avanti**.
3. Nella pagina **Scegliere un gruppo di Enterprise Console**, selezionare o creare il gruppo di Enterprise Console che si desidera sincronizzare con Active Directory (punto di sincronizzazione). Cliccare su **Avanti**.
4. Nella pagina **Scegliere un albero di Active Directory**, selezionare l'albero di Active Directory con il quale si desidera sincronizzare il gruppo. Inserire il nome dell'albero (per esempio, LDAP://CN=Computers,DC=domain_name,DC=local) oppure cliccare su **Sfoglia** per cercare l'albero in Active Directory. Cliccare su **Avanti**.

   Importante
   se un computer si trova in più di un albero di Active Directory sincronizzato, ciò può generare problemi quali il continuo scambio di messaggi fra il computer e Enterprise Console. I computer dovrebbero essere elencati solo una volta in Enterprise Console.

5. Se si desidera proteggere automaticamente le workstation con sistema operativo Windows, nella pagina **Protezione automatica dei computer**, selezionare la casella di spunta **Installa automaticamente il software di sicurezza Sophos** e poi il software che si desidera installare.

   Nota
   Per un elenco dei requisiti di sistema per il software, consultare la pagina corrispondente del sito web di Sophos (http://www.sophos.com/it-it/products/all-system-requirements.aspx).

   - Prima d'installare il **Firewall** nei computer, assicurarsi di averlo configurato in modo tale da consentire il traffico, le applicazioni e i processi che si desidera utilizzare. Per impostazione predefinita il firewall è attivato e blocca tutto il traffico non essenziale. Vedere Criterio firewall (pagina 113).
   - Per rimuovere automaticamente un software di sicurezza di altro fornitore, lasciare selezionata l'opzione **Third-Party Security Software Detection**. Se è necessario rimuovere il tool di aggiornamento di un altro produttore, consultare la sezione Rimozione del software di sicurezza prodotto da terzi (pagina 44).

   Tutte le workstation con sistema operativo Windows, individuate durante questa sincronizzazione e le sincronizzazioni future, saranno protette automaticamente, in conformità con i rispettivi criteri di gruppo.

   Importante
   i computer con sistema operativo Windows per server, Mac OS, Linux o UNIX non saranno protetti automaticamente. Tali computer dovranno essere protetti manualmente, come descritto nella *Guida di avvio avanzata di* Sophos Enterprise Console.

   Nota
   è possibile abilitare o disabilitare la protezione automatica in un secondo tempo, dalla finestra di dialogo **Proprietà della sincronizzazione**. Per istruzioni consultare la sezione Visualizzazione e modifica delle proprietà della sincronizzazione (pagina 41).

   Cliccare su **Avanti**.
6. Se si è scelto di proteggere i computer automaticamente, nella pagina **Inserisci le credenziali di Active Directory**, inserire i dati dell'account amministratore che sarà utilizzato per installare il software nei computer. Cliccare su **Avanti**.

7. Nella pagina **Scegli l'intervallo di sincronizzazione**, scegliere la frequenza con la quale si desidera sincronizzare il gruppo di Enterprise Console con l'albero di Active Directory. Il valore predefinito è 60 minuti.

   Nota
   è possibile modificare l'intervallo di sincronizzazione in un secondo tempo, dalla finestra di dialogo **Proprietà della sincronizzazione**. Per istruzioni consultare la sezione Visualizzazione e modifica delle proprietà della sincronizzazione (pagina 41).

8. Nella pagina **Conferma le scelte**, verificare i dati e cliccare su **Avanti** per continuare.
9. Nell'ultima pagina della procedura guidata, è possibile visualizzare i dati dei gruppi e dei computer sincronizzati.

   Inoltre, è possibile impostare l'invio via e-mail, ai destinatari prescelti, di allarmi sui nuovi computer e gruppi individuati durante le future sincronizzazioni. Se si è scelto di proteggere automaticamente i computer nei gruppi sincronizzati, è inoltre possibile impostare allarmi sul malfunzionamento della protezione automatica. Per aprire la finestra di dialogo **Configura allarmi e-mail** dopo aver cliccato su **Fine**, selezionare la casella nell'ultima pagina della procedura guidata. Per istruzioni consultare la sezione Impostazione del pannello di controllo e degli allarmi e-mail relativi alla sincronizzazione con Active Directory (pagina 194).

   Per chiudere la procedura guidata, cliccare su **Fine**.

4.5.4 Utilizzo della sincronizzazione per proteggere i computer automaticamente

Prima di eseguire questa operazione:

- Se si utilizza un'amministrazione basata sui ruoli, è necessario disporre dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).
- Accertarsi che i computer siano stati predisposti per l'installazione automatica del software di sicurezza, secondo quanto descritto nella sezione Preparazione per l'installazione del software di sicurezza (pagina 44).

È possibile proteggere automaticamente le workstation con sistema operativo Windows quando vengono individuate durante la sincronizzazione con Active Directory.

Importante
i computer con sistema operativo Windows per server, Mac OS, Linux o UNIX non saranno protetti automaticamente. Tali computer dovranno essere protetti manualmente, come descritto nella *Guida di avvio avanzata di* Sophos Enterprise Console.

È possibile proteggere automaticamente i computer nei gruppi sincronizzati sia al momento dell'impostazione della sincronizzazione (v. Sincronizzazione con Active Directory (pagina 38)), che modificando in un secondo tempo le proprietà della sincronizzazione.

Le istruzioni di seguito indicano come proteggere i computer modificando le proprietà di sincronizzazione.

1. Nel riquadro **Gruppi**, selezionare il gruppo (punto di sincronizzazione) per il quale si desidera abilitare la protezione automatica. Cliccare con il tasto destro del mouse sul gruppo e selezionare **Proprietà della sincronizzazione**.

 Copyright © Sophos Limited

2. Nella finestra di dialogo **Proprietà della sincronizzazione**, selezionare la casella di spunta **Installa automaticamente il software di sicurezza Sophos** e poi il software che si desidera installare.
   - Prima d'installare il **Firewall** nei computer, assicurarsi di averlo configurato in modo tale da consentire il traffico, le applicazioni e i processi che si desidera utilizzare. Per impostazione predefinita il firewall è attivato e blocca tutto il traffico non essenziale. Vedere Criterio firewall (pagina 113).
   - Per rimuovere automaticamente un software di sicurezza di altro fornitore, lasciare selezionata l'opzione **Third-Party Security Software Detection**. Se è necessario rimuovere il tool di aggiornamento di un altro produttore, consultare la sezione Rimozione del software di sicurezza prodotto da terzi (pagina 44).
3. Inserire il nome utente e la password dell'account amministratore che sarà utilizzato per installare il software nei computer. Cliccare su **OK**.

Se in seguito si desidera disabilitare la protezione automatica, nella finestra di dialogo **Proprietà della sincronizzazione**, deselezionare la casella **Installa automaticamente il software di sicurezza Sophos**.

4.5.5 Visualizzazione e modifica delle proprietà della sincronizzazione

Prima di eseguire questa operazione:

- Se si utilizza un'amministrazione basata sui ruoli, è necessario disporre dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).
- Se si desidera proteggere automaticamente i computer che si trovano in gruppi sincronizzati, assicurarsi che i computer siano stati predisposti a tale scopo, secondo quanto descritto nella sezione Preparazione per l'installazione del software di sicurezza (pagina 44).
- Se avete una struttura di Active Directory piuttosto complessa e desiderate sincronizzare i gruppi di dominio locali, oppure i gruppi di Active Directory inseriti in altri gruppi, abilitare questa funzionalità secondo le istruzioni fornite nell'articolo 122529 della knowledge base.

Per visualizzare e modificare le proprietà della sincronizzazione:

1. Nel riquadro **Gruppi**, selezionare il gruppo (punto di sincronizzazione) per il quale si desidera modificare le proprietà della sincronizzazione. Cliccare con il tasto destro del mouse sul gruppo e selezionare **Proprietà della sincronizzazione**.
   Viene visualizzata la finestra di dialogo **Proprietà della sincronizzazione**.
2. Nel campo **Albero di Active Directory**, è possibile visualizzare l'albero a cui è sincronizzato il gruppo. Se si desidera sincronizzare il gruppo con un albero diverso, **Rimuovere la sincronizzazione** ed eseguire nuovamente la procedura guidata di Sincronizzazione con Active Directory. Vedere Attivazione e disattivazione della sincronizzazione (pagina 42) e Sincronizzazione con Active Directory (pagina 38).
3. Nel campo **Intervallo di sincronizzazione**, impostare la frequenza di sincronizzazione. Il valore predefinito è 60 minuti. Il valore minimo è 5 minuti.
4. Spuntare la casella **Installa automaticamente il software di sicurezza Sophos** se si desidera proteggere automaticamente tutte le nuove workstation con sistema operativo Windows individuate, in conformità con i rispettivi criteri di gruppo. Sotto **Funzioni**, la protezione antivirus viene selezionata per impostazione predefinita. Se si desidera installare altri software di sicurezza Sophos, selezionare le relative caselle di spunta. Inserire il nome utente e la password dell'account amministratore che sarà utilizzato per installare il software nei computer.

Nota
Potranno essere protette automaticamente le sole workstation con sistema operativo Windows. i computer con sistema operativo Windows per server, Mac OS, Linux o UNIX non possono essere protetti automaticamente. Tali computer dovranno essere protetti manualmente, come descritto nella *Guida di avvio avanzata di* Sophos Enterprise Console.

4.5.6 Sincronizzazione con Active Directory

Prima di eseguire questa operazione:

- Se si utilizza un'amministrazione basata sui ruoli, è necessario disporre dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).
- Se si desidera proteggere automaticamente i computer che si trovano in gruppi sincronizzati, assicurarsi che i computer siano stati predisposti a tale scopo, secondo quanto descritto nella sezione Preparazione per l'installazione del software di sicurezza (pagina 44).
- Se avete una struttura di Active Directory piuttosto complessa e desiderate sincronizzare i gruppi di dominio locali, oppure i gruppi di Active Directory inseriti in altri gruppi, abilitare questa funzionalità secondo le istruzioni fornite nell'articolo 122529 della knowledge base.

È possibile sincronizzare immediatamente i gruppi di Enterprise Console (punti di sincronizzazione) con gli alberi di Active Directory, senza dover attendere la prossima sincronizzazione programmata.

Per effettuare immediatamente la sincronizzazione con Active Directory procedere come segue.

1. Nel riquadro **Gruppi**, selezionare il gruppo (punto di sincronizzazione) che si desidera sincronizzare con Active Directory. Cliccare con il tasto destro del mouse sul gruppo e selezionare **Proprietà della sincronizzazione**.
2. Nella finestra di dialogo **Proprietà della sincronizzazione**, apportare le adeguate modifiche e cliccare su **OK**.

4.5.7 Attivazione e disattivazione della sincronizzazione

Prima di eseguire questa operazione:

- Se si utilizza un'amministrazione basata sui ruoli, è necessario disporre dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).
- Se si desidera proteggere automaticamente i computer che si trovano in gruppi sincronizzati, assicurarsi che i computer siano stati predisposti a tale scopo, secondo quanto descritto nella sezione Preparazione per l'installazione del software di sicurezza (pagina 44).
- Se avete una struttura di Active Directory piuttosto complessa e desiderate sincronizzare i gruppi di dominio locali, oppure i gruppi di Active Directory inseriti in altri gruppi, abilitare questa funzionalità secondo le istruzioni fornite nell'articolo 122529 della knowledge base.

Per eseguire la sincronizzazione, sia che Active Directory sia attiva o meno:

- Per attivare la sincronizzazione, eseguire la **Procedura guidata di sincronizzazione con Active Directory**, come descritto in Sincronizzazione con Active Directory (pagina 38).
- Per disattivare la sincronizzazione, selezionare il gruppo (punto di sincronizzazione) che non si desidera più sincronizzare con Active Directory, cliccarvi sopra con il tasto destro del mouse e selezionare **Rimuovi sincronizzazione**. Cliccare su **Sì** per confermare.

 Copyright © Sophos Limited

4.6 Configurazione dell'URL di Sophos Mobile

Sophos Mobile è una soluzione di gestione per dispositivi mobili quali smartphone e tablet. Sophos Mobile consente di proteggere i dati aziendali grazie alla gestione di app e impostazioni di sicurezza.

È possibile aprire la console Web di Sophos Mobile da Enterprise Console cliccando sul pulsante **Sophos Mobile** della barra degli strumenti. Per far ciò, è per prima cosa necessario configurare l'URL di Sophos Mobile.

1. Nel menu **Strumenti**, cliccare su **Configura URL Sophos Mobile**.
2. Nella finestra dialogo **URL Sophos Mobile**, inserire l'URL della console Web di Sophos Mobile, quindi cliccare su **OK**.

5 Protezione dei computer

Il software di protezione Sophos può essere installato nei seguneti modi:

- Per proteggere i computer automaticamente, utilizzare la Procedura guidata di protezione dei computer in Enterprise Console; consultare la sezione Protezione automatica dei computer (pagina 45).
- In alternativa, è possibile proteggere i computer automaticamente utilizzando la sincronizzazione di Active Directory; consultare la sezione Sincronizzazione con Active Directory (pagina 36).
- Per proteggere i computer manualmente, Enterprise Console consente di individuare il software necessario, consultare la sezione Localizzazione dei programmi di installazione per la protezione manuale dei computer (pagina 47). Una volta individuato, installare manualmente il software di sicurezza nei computer.

5.1 Preparazione per l'installazione del software di sicurezza

Oltre ad assicurarsi che i computer rispondano ai requisiti di sistema generali, è necessario svolgere ulteriori passaggi prima di poter installare il software automaticamente.

Nota
L'installazione automatica non è possibile nei computer con sistema operativo Mac, Linux e UNIX.

Se si utilizza Active Directory, è possibile preparare i computer tramite l'Oggetto Criteri di gruppo (GPO). Se si utilizzano gruppi di lavoro, i computer dovranno essere configurati localmente.

Per istruzioni, consultare la *Guida alla distribuzione di Sophos Endpoint*. Per video sulla distribuzione, consultare l'articolo 111180 della knowledge base.

5.2 Rimozione del software di sicurezza prodotto da terzi

Se si desidera rimuovere un qualsiasi software di sicurezza precedentemente installato, è necessario fare quanto riportato di seguito PRIMA di selezionare il **Third-Party Security Software Detection** nella procedura guidata di **Procedura guidata per la protezione dei computer** e di installarlo:

- Se i computer utilizzano un software antivirus di altro fornitore, assicurarsi che la relativa interfaccia utente sia chiusa.
- Se i computer eseguono un prodotto firewall o HIPS di terzi, accertarsi che sia disattivato o configurato per consentire l'esecuzione del programma di installazione di Sophos.
- Se si desidera rimuovere non solo il software ma anche il tool di aggiornamento prodotto da terzi (per prevenire la reinstallazione automatica del software), procedere come segue. Se i computer non hanno il tool di aggiornamento installato, ignorare i punti seguenti.

Copyright © Sophos Limited

Nota
è necessario riavviare localmente ciascun computer dal quale è stato rimosso il software antivirus prodotto da terzi.

Nota
HitmanPro.Alert potrebbe essere già stato installato come prodotto standalone oppure da Sophos Central. Occorre rimuovere HitmanPro.Alert prima di applicare la gestione on-premise da Sophos Enterprise Console.

Se nei computer è installato un tool di aggiornamento di terzi e lo si vuole rimuovere, è necessario modificare il file di configurazione prima di selezionare l'opzione **Third-Party Security Software Detection** nella procedura guidata di **Procedura guidata per la protezione dei computer**.

Nota
Se i computer eseguono un prodotto firewall o HIPS di terzi, potrebbe essere necessario lasciare il relativo tool di aggiornamento intatto. Per chiarimenti, consultare la documentazione fornita dal produttore.

Per modificare il file di configurazione:

1. Nella directory di installazione centrale cercare il file data.zip.
2. Estrarre da data.zip il file di configurazione crt.cfg.
3. Modificare il file crt.cfg cambiando la riga "RemoveUpdateTools=0" in "RemoveUpdateTools=1".
4. Salvare le modifiche, quindi salvare il file crt.cfg nella stessa directory contenente data.zip. Non reinserire crt.cfg in data.zip, altrimenti verrà sovrascritto al prossimo aggiornamento del file data.zip.

Quando si esegue la **Procedura guidata per la protezione dei computer** e si sceglie l'opzione **Third-Party Security Software Detection**, il file di configurazione modificato rimuoverà qualsiasi tool di aggiornamento prodotto da terzi, oltre che il relativo software di sicurezza.

5.3 Protezione automatica dei computer

Prima di proteggere i computer dalla console:

- Applicare un criterio di aggiornamento al gruppo prima di poter proteggere i computer in tale gruppo.
- Accertarsi che i computer siano stati predisposti per l'installazione automatica del software di sicurezza, secondo quanto descritto nella sezione Preparazione per l'installazione del software di sicurezza (pagina 44).
- Se si utilizza un'amministrazione basata sui ruoli, per poter proteggere i computer, è necessario essere in possesso dei diritti di **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

L'installazione automatica non è possibile nei computer con sistema operativo Mac, Linux e UNIX. Eseguire invece l'installazione manuale. Per le istruzioni, consultare la *Guida di avvio avanzata di Sophos Enterprise Console*.

Se si è scelto di effettuare la sincronizzazione con Active Directory e di proteggere i computer automaticamente, *non è* necessario seguire le istruzioni riportate qui sotto. Per informazioni più

dettagliate, consultare la sezione Sincronizzazione con Active Directory (pagina 36) e altri argomenti pertinenti.

Per proteggere i computer automaticamente:

1. Se i computer che si desidera proteggere appartengono già a un gruppo, svolgere una delle seguenti operazioni:
   - Se i computer che si desidera proteggere si trovano nel gruppo **Nessun gruppo**, trascinare i computer in un gruppo.
   - Se i computer che si desidera proteggere appartengono già a un gruppo, selezionare i computer, cliccarvi col tasto destro del mouse e poi cliccare su **Proteggi computer**.

   Viene avviata la **Procedura guidata per la protezione dei computer**. Seguire le istruzioni della procedura guidata.
2. Nella pagina **Seleziona funzioni**, selezionare le funzioni desiderate.

   Nota
   Per un elenco dei requisiti di sistema relativi alle funzioni, consultare la pagina corrispondente del sito web di Sophos (http://www.sophos.com/it-it/products/all-system-requirements).

   Alcune funzioni, fra cui la protezione antivirus, sono sempre selezionate e devono essere installate. È inoltre possibile scegliere di installare le funzioni elencate qui di seguito: Alcune funzioni sono disponibili solo se incluse nella licenza in possesso.

   - **Firewall**

     Prima d'installare il firewall nei computer, assicurarsi di averlo configurato in modo tale da consentire il traffico, le applicazioni e i processi che si desidera utilizzare. Per impostazione predefinita il firewall è attivato e blocca tutto il traffico non essenziale. Vedere Criterio firewall (pagina 113).
   - **Patch**
   - **Exploit Prevention, Sophos Clean**

     Questa funzionalità protegge i sistemi da ransomware ed exploit. Se è inclusa nella licenza, viene selezionata per impostazione predefinita.

     Nota
     Se si effettua l'upgrade della licenza in modo da includere Exploit Prevention (con Sophos Clean), questa funzionalità non viene installata automaticamente sui computer che sono già gestiti. Occorrerà proteggere nuovamente i computer per installarla.

   - **Third-Party Security Software Detection**

     Per rimuovere automaticamente un software di sicurezza di altro fornitore, lasciare selezionata l'opzione **Third-Party Security Software Detection**. Il Software di sicurezza di terze parti disinstalla solo i prodotti con le stesse funzionalità di quelli che si desidera installare al loro posto. Se è necessario rimuovere il tool di aggiornamento di un altro produttore, consultare la sezione Rimozione del software di sicurezza prodotto da terzi (pagina 44).
3. Nella pagina **Riepilogo protezione**, qualsiasi problema relativo all'installazione viene segnalato nella colonna **Problemi di protezione**. Risolvere i problemi dell'installazione (v. Installazione di Sophos Endpoint Security and Control non riuscita (pagina 223)) o, in tali computer, eseguire l'installazione manuale (v. la *Guida di avvio avanzata di Sophos Enterprise Console*). Cliccare su **Avanti**.
4. Nella pagina **Credenziali**, inserire i dati dell'account che si utilizzerà per installare il software.

 Copyright © Sophos Limited

Si tratta di solito di un account amministratore di dominio. Deve:

- Avere diritti di amministratore locale sui computer che si desidera proteggere.
- Essere in grado di aprire una sessione nel computer sul quale è stato installato il server di gestione.
- Avere accesso in lettura al percorso del server primario specificato nel criterio di **Aggiornamento**. Vedere Configurazione dei server di aggiornamento (pagina 70).

Nota
Se si utilizza un account di dominio, è *imperativo* inserire il nome utente nella forma `dominio\utente`.

Se i computer si trovano su domini diversi coperti dallo stesso schema di Active Directory, usare l'account di Enterprise Administrator in Active Directory.

5.4 Localizzazione dei programmi di installazione per la protezione manuale dei computer

Se in alcuni computer Enterprise Console non riesce a eseguire l'installazione automatica delle funzioni antivirus, firewall o patch, è possibile eseguire l'installazione manuale.

Per trovare il programma di installazione:

1. Nel menu **Visualizza**, cliccare su **Percorsi Bootstrap**.
2. Nella finestra di dialogo **Percorsi Bootstrap**, per ciascuna sottoscrizione al software, visualizzare i percorsi che contengono i programmi di installazione del software, oltre che le piattaforme che supportano il software e le versioni del software. Memorizzare il percorso del programma di installazione a cui si è interessati.

Per ulteriori informazioni su come installare manualmente i software di sicurezza in diversi sistemi operativi, consultare la *Guida di avvio avanzata di* Sophos Enterprise Console.

5.5 Verifica della protezione della rete

Per una panoramica sullo stato di sicurezza della rete, utilizzare il Pannello di controllo. Per ulteriori informazioni, vedere Pannello di controllo (pagina 4) e Configurazione del pannello di controllo (pagina 48).

È possibile identificare i computer che presentano un problema tramite l'elenco dei computer e i filtri dell'elenco dei computer. Per esempio, è possibile visualizzare i computer che non hanno il firewall o le funzioni delle patch installati, oppure allarmi a cui è necessario prestare attenzione. Per ulteriori informazioni, vedere Verifica che i computer siano protetti (pagina 48), Verifica dello stato di aggiornamento dei computer (pagina 49), e Rilevamento di computer con problemi (pagina 49).

È inoltre possibile verificare se tutti i computer di un gruppo siano conformi ai criteri di tale gruppo, come descritto in Verifica che i computer utilizzino i criteri di gruppo (pagina 32).

5.5.1 Configurazione del pannello di controllo

Se si utilizza l'amministrazione basata sui ruoli, per poter configurare il pannello di controllo, è necessario essere in possesso dei diritti di **Configurazione del sistema**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Il pannello di controllo visualizza indicatori di stato che sono critici o di avviso secondo la percentuale dei computer gestiti aventi allarmi o errori in sospeso, oppure secondo il tempo trascorso dall'ultimo aggiornamento da Sophos.

È possibile impostare i livelli critico e di avviso che si desidera utilizzare.

1. Nel menu **Strumenti**, cliccare su **Configura pannello di controllo**.
2. Nella finestra di dialogo **Configura pannello di controllo**, modificare i valori di soglia nelle caselle di testo **Livello di avviso** e **Livello critico** secondo quanto descritto di seguito.

   a) Sotto **Computer con allarmi in sospeso**, **Computer con errori di un prodotto Sophos** e **Criterio e protezione**, inserire la percentuale di computer gestiti interessati da uno specifico problema; tale percentuale determinerà il passaggio del rispettivo indicatore ad "avviso" o "critico".

   b) Sotto **Computer con eventi**, inserire il numero di eventi verificatisi in un periodo di sette giorni e che portano alla visualizzazione di un allarme nel pannello di controllo.

   c) Sotto **Protezione aggiornata da Sophos**, inserire il tempo in ore trascorso dall'ultimo aggiornamento da Sophos; tale valore determinerà il passaggio dell'indicatore "aggiornamenti" ad "avviso" o "critico". Cliccare su **OK**.

   Se si imposta uno dei livelli su zero, gli avvisi vengono generati non appena viene ricevuto il primo allarme.

Inoltre, è possibile impostare l'invio di allarmi via e-mail a destinatari prescelti nel caso in cui venga superato il livello di avviso o il livello critico. Per istruzioni consultare la sezione Impostazione di allarmi e messaggi (pagina 186).

5.5.2 Verifica che i computer siano protetti

I computer sono protetti se eseguono la scansione in accesso e il firewall (se installato). Perché la protezione sia completa, anche il software deve essere aggiornato.

Nota
È possibile aver scelto l'opzione di non utilizzare la scansione in accesso su certi tipi di computer, ad esempio i file server. In tal caso, accertarsi che i computer utilizzino le scansioni pianificate e che siano aggiornati.

Per verificare che i computer siano protetti:

1. Selezionare il gruppo di computer che si desidera controllare.
2. Se si desidera controllare i computer nei sottogruppi del gruppo, selezionare **A questo livello e al livello inferiore** nell'elenco a discesa.
3. Nell'elenco dei computer, nella scheda **Stato**, cercare nella colonna **In accesso**.
   Se appare la scritta "Attiva", il computer esegue la scansione in accesso. Se presenta uno scudo grigio, la scansione in accesso non viene eseguita.
4. Se il firewall è installato, guardare la colonna **Firewall attivato**.

Copyright © Sophos Limited

Se appare la scritta "Sì", il firewall è abilitato. Se appare il simbolo del firewall di colore grigio e la scritta "No" il firewall è disabilitato.

5. Se si utilizzano altre funzioni, quali controllo applicazioni, dati o patch, verificarne lo stato nelle rispettive colonne.

Per informazioni su come verificare che i computer siano aggiornati, consultare la sezione Verifica dello stato di aggiornamento dei computer (pagina 49).

Per informazioni su come reperire i computer che presentano problemi tramite i filtri dell'elenco computer, consultare la sezione Rilevamento di computer con problemi (pagina 49).

5.5.3 Verifica dello stato di aggiornamento dei computer

Se si imposta Enterprise Console secondo le raccomandazioni fornite, i computer riceveranno automaticamente gli aggiornamenti.

Per verificare lo stato di aggiornamento dei computer:

1. Selezionare il gruppo di computer che si desidera controllare.
2. Se si desidera controllare i computer in uno dei sottogruppi, selezionare nell'elenco a discesa **A questo livello e al livello inferiore**.
3. Nella scheda **Stato**, cercare nella colonna **Aggiornato**, oppure passare alla scheda **Dettagli degli aggiornamenti**.
   - Se compare la dicitura “Sì” nella colonna **Aggiornato**, il computer è aggiornato.
   - Se riporta l'icona a forma di orologio, il computer non è aggiornato. Il testo indica da quanto tempo il computer non è stato aggiornato.

Per informazioni su come aggiornare i suddetti computer non aggiornati, vedere Aggiornamento dei computer non aggiornati (pagina 78).

5.5.4 Rilevamento di computer con problemi

Per visualizzare un elenco di computer che non sono protetti in maniera adeguata oppure che hanno altri problemi connessi alla protezione:

1. Selezionare il gruppo di computer che si desidera controllare.
2. Nel menu a discesa **Visualizza**, selezionare quali computer si desidera trovare, per es. **Computer con potenziali problemi**.

   È anche possibile selezionare una sottovoce di una voce, per visualizzare i computer affetti da problemi specifici (per es. i computer che si allontanano dal criterio del gruppo, con allarmi in sospeso o in cui si è verificato un errore di installazione).
3. Se il gruppo contiene dei sottogruppi, selezionare anche l'opzione **Solo a questo livello** oppure **A questo livello e al livello inferiore**.
   Verranno elencati tutti i computer che presentano problemi di protezione.

È inoltre possibile filtrare l'elenco dei computer in base al nome degli oggetti rilevati, quali malware, applicazioni potenzialmente indesiderate, file sospetti. Per ulteriori informazioni, consultare la sezione Filtraggio dei computer in base agli oggetti rilevati (pagina 8).

Per informazioni relative a problemi di protezione, consultare Mancata esecuzione da parte dei computer della scansione in accesso (pagina 221) e gli altri argomenti della sezione Risoluzione dei problemi (pagina 221).

5.6 Come gestire computer con allarmi ed errori

Se viene rilevata la presenza di virus, spyware, oggetti sospetti, adware o altre applicazioni potenzialmente indesiderate, vengono visualizzate delle icone di allarme nella scheda **Stato**, vista **Computer**.

Per una legenda delle icone di allarme, vedere la sezione Significato delle icone di allarme (pagina 50) Negli altri argomenti di questa sezione vengono forniti consigli sulla gestione degli allarmi.

Nota
nella console vengono visualizzati avvisi anche se il software è disabilitato o obsoleto. Per le relative informazioni, consultare la sezione Verifica della protezione della rete (pagina 47).

Per ulteriori informazioni su un allarme, ad esempio il nome dell'elemento rilevato, cliccare sulla scheda **Dati di allarmi ed errori**.

Per informazioni sugli allarmi del gestore aggiornamenti, consultare la sezione Monitoraggio del gestore aggiornamenti (pagina 77).

5.6.1 Significato delle icone di allarme

Icona	Descrizione
	Un simbolo d'allarme rosso visualizzato nella colonna **Allarmi ed errori** indica che è stato rilevato un virus, worm, trojan, spyware o comportamento sospetto.
	Un simbolo d'allarme giallo visualizzato nella colonna **Allarmi ed errori** indica uno dei seguenti problemi. • È stato rilevato un file sospetto. • È stata rilevata la presenza di adware o altre applicazioni potenzialmente indesiderate. • Si è verificato un errore. Un simbolo d'allarme giallo visualizzato nella colonna **Conformità al criterio** indica che il computer non sta utilizzando lo stesso criterio/criteri degli altri computer del gruppo.

In presenza di allarmi o errori multipli sullo stesso computer, nella colonna **Allarmi ed errori** sarà visualizzata l'icona d'allarme con priorità più alta. I tipi di allarme sono elencati qui sotto in ordine decrescente di priorità.

1. Allarmi virus e spyware
2. Allarmi da comportamento sospetto
3. Allarmi da file sospetti
4. Allarmi adware e PUA
5. Errori dell'applicazione del software (ad esempio, errori di installazione)

Copyright © Sophos Limited

5.6.2 Trattamento degli allarmi su oggetti rilevati

Se si utilizza l'amministrazione basata sui ruoli, è necessario essere in possesso dei diritti di **Correzione - disinfezione** per disinfettare gli oggetti rilevati o cancellare allarmi dalla console. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per intervenire contro gli allarmi visualizzati nella console:

1. Nella vista **Computer**, selezionare il/i computer per cui si desidera visualizzare gli allarmi. Cliccarvi sopra con il tasto destro del mouse e selezionare **Risolvi allarmi ed errori**.
   Viene visualizzata la finestra di dialogo **Risolvi allarmi ed errori**.
2. L'azione che si può intraprendere contro un allarme dipende dallo stato di disinfezione dell'allarme. Cercare nella colonna **Stato disinfezione** e decidere quale azione si desidera intraprendere.

Consiglio
è possibile ordinare gli allarmi cliccando su una delle intestazioni di colonna. Ad esempio, per ordinare gli allarmi in base allo stato di disinfezione, cliccare sull'intestazione di colonna **Stato disinfezione**.

stato disinfezione	Descrizione e azioni da intraprendere
Rimovibile	È possibile rimuovere l'oggetto. A tal fine, selezionare l'allarme o gli allarmi e cliccare su **Rimozione**.
Tipo di minaccia non eliminabile	Questo tipo di oggetto rilevato, ad esempio file sospetto, comportamento sospetto o traffico di rete malevolo, non può essere disinfettato dalla console. È necessario decidere se si desidera consentire o bloccare l'oggetto. Se non si considera affidabile l'oggetto, è possibile inviarlo a Sophos per farlo analizzare. Per ulteriori informazioni, consultare la sezione Reperimento di informazioni sugli oggetti rilevati (pagina 52).
Non rimovibile	Questo oggetto non può essere disinfettato dalla console. Per ulteriori informazioni sull'oggetto e le azioni che si possono intraprendere contro di esso, consultare Reperimento di informazioni sugli oggetti rilevati (pagina 52).
Richiesta scansione completa	Questo oggetto potrebbe essere disinfettabile, ma prima dell'esecuzione della disinfezione è necessario eseguire una scansione completa del computer. Per istruzioni consultare la sezione Scansione immediata dei computer (pagina 53).
Riavvio necessario	L'oggetto è stato parzialmente rimosso, ma è necessario riavviare il computer per completare la disinfezione. **Nota** Gli endpoint devono essere riavviati localmente, e non da Enterprise Console.
Disinfezione non riuscita	Non è stato possibile rimuovere l'oggetto. Potrebbe essere necessaria la disinfezione manuale. Per ulteriori informazioni, consultare la sezione Disinfezione immediata dei computer (pagina 54).

stato disinfezione	Descrizione e azioni da intraprendere
Rimozione in corso (avviato<orario>)	Disinfezione in corso.
Rimozione scaduta (avviato<orario>)	La disinfezione è scaduta. È possibile che l'oggetto non sia stato disinfettato. Questo può accadere, ad esempio, quando il computer è scollegato dalla rete o quando la rete è occupata. È possibile provare a ripulire l'oggetto in un secondo momento.

Se si decide di consentire un oggetto, consultare la sezione Autorizzazione di adware e PUA (pagina 109) o Autorizzazione di oggetti sospetti (pagina 111).

5.6.3 Reperimento di informazioni sugli oggetti rilevati

Se si desidera saperne di più su una minaccia o un altro oggetto rilevato su un computer e segnalato nella console, oppure se si ha bisogno di consigli su quale azione intraprendere contro l'oggetto, procedere come segue:

1. Nella modalità di visualizzazione **Computer**, nell'elenco dei computer, cliccare due volte sul computer desiderato.
2. Nella finestra di dialogo **Dettagli computer**, scorrere in giù fino alla sezione **Allarmi ed errori in sospeso**. Nell'elenco degli oggetti rilevati, cliccare sul nome dell'oggetto al quale si è interessati. Così facendo, ci si collega al sito Web Sophos, in cui è possibile leggere una descrizione dell'oggetto e ricevere consigli sulle azioni da intraprendere contro di esso.

Nota
In alternativa, è possibile visitare la pagina **Analisi di sicurezza** sul sito web di Sophos (http://www.sophos.com/it-it/threat-center/threat-analyses/viruses-and-spyware.aspx), selezionare il tipo di oggetto che si desidera individuare, e digitare il nome dell'oggetto nella casella di ricerca.

5.6.4 Gestione degli allarmi relativi al ransomware

Se si utilizza l'amministrazione basata sui ruoli, è necessario essere in possesso dei diritti di **Correzione - disinfezione** per disinfettare gli oggetti rilevati o cancellare allarmi dalla console. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

CryptoGuard blocca il processo sull’endpoint che ha generato l'allarme di ransomware. Il blocco viene rimosso solamente quando l’allarme viene cancellato.

Nota
Se si riavvia l’endpoint, il blocco viene rimosso. Se il processo infetto si riavvia, viene generato un nuovo allarme di ransomware.

Copyright © Sophos Limited

Ricordare
Sophos Clean deve essere eseguito manualmente sul computer per cui è stato segnalato il rilevamento, altrimenti il computer continuerà ad attivare l'allarme, e il processo sarà bloccato ogni volta che viene eseguito.

Per intervenire sugli allarmi di ransomware visualizzati nella console:

1. Nella vista **Computer**, selezionare il/i computer per cui si desidera visualizzare gli allarmi. Cliccarvi sopra con il tasto destro del mouse e selezionare **Risolvi allarmi ed errori**.
   Viene visualizzata la finestra di dialogo **Risolvi allarmi ed errori**.
2. Selezionare l'allarme di ransomware che si desidera eliminare, e cliccare su **Cancella**.
   Gli allarmi già esaminati (cancellati) non sono più visualizzati nella console. In questo modo viene rimosso il blocco imposto sul processo.

5.6.5 Cancellazione di allarmi ed errori dei computer dalla console

Se si utilizza l'amministrazione basata sui ruoli, è necessario essere in possesso dei diritti **Correzione - disinfezione** per cancellare allarmi o errori dalla console. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Se sono già stati presi dei provvedimenti riguardo a un allarme, o se si è certi che un computer sia sicuro, è possibile cancellare i simboli d'allarme visualizzati nella console.

Nota
non è possibile cancellare gli allarmi riguardanti errori di installazione. Verranno cancellati solo quando l'installazione di Sophos Endpoint Security and Control nel computer è portata a termine.

1. Nella vista **Computer**, selezionare il/i computer per cui si desidera cancellare gli allarmi. Cliccarvi sopra con il tasto destro del mouse e selezionare **Risolvi allarmi ed errori**.
   Viene visualizzata la finestra di dialogo **Risolvi allarmi ed errori**.
2. Per cancellare allarmi o errori relativi a prodotti Sophos dalla console, andare alla scheda Allarmi ed errori, scegliere gli allarmi o gli errori che si desidera cancellare e cliccare su **Cancella**.
   Gli allarmi già esaminati (cancellati) non sono più visualizzati nella console.

Per informazioni su come cancellare allarmi del gestore aggiornamenti dalla console, consultare la sezione Cancellazione degli allarmi del gestore aggiornamenti dalla console (pagina 78).

5.7 Immediata scansione e disinfezione dei computer

5.7.1 Scansione immediata dei computer

È possibile esaminare uno o più computer immediatamente, senza dover attendere la prossima scansione pianificata.

Se si utilizza l'amministrazione basata sui ruoli, per eseguire la scansione dei computer, è necessario essere in possesso dei diritti **Correzione - aggiornamento e scansione**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Nota
solo i computer con sistema operativo Windows, Linux e UNIX possono eseguire immediatamente la scansione completa del sistema lanciata dalla console.

Per eseguire la scansione completa dei computer:

1. Selezionare i computer dall'elenco dei computer o un gruppo dal riquadro **Gruppi**. Cliccarvi sopra con il tasto destro del mouse e selezionare **Scansione completa del sistema**.

   In alternativa, nel menu **Azioni**, selezionare **Scansione completa del sistema**.
2. Nella finestra di dialogo **Scansione completa del sistema**, controllare i dati dei computer da esaminare e cliccare su **OK** per avviare la scansione.

Nota
Se la scansione rileva componenti di una minaccia nella memoria, la scansione si arresta e viene inviato un allarme a Enterprise Console. Ciò avviene poiché procedere con la scansione potrebbe consentire la diffusione di questa minaccia. Occorre effettuare la disinfezione della minaccia, prima di poter eseguire nuovamente la scansione.

5.7.2 Disinfezione immediata dei computer

È possibile disinfettare immediatamente i computer Windows 2000 o Mac che sono stati colpiti da un virus o nei quali sono installate applicazioni indesiderate.

Se si utilizza l'amministrazione basata sui ruoli, è necessario essere in possesso dei diritti di **Correzione - disinfezione** per disinfettare i computer. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Nota
Per disinfettare i computer con sistema operativo Linux o UNIX, è possibile impostare una disinfezione automatica dalla console (v. Impostazione della disinfezione automatica per la scansione in accesso (pagina 85)) o disinfettare ogni computer individualmente, come descritto in Trattamento degli oggetti rilevati se la disinfezione non riesce (pagina 55).

Se un oggetto (per es. un trojan o un'applicazione potenzialmente indesiderata) è stato "parzialmente rilevato", prima di disinfettarlo sarà necessario eseguire una scansione completa del sistema di tale computer al fine di rilevare i componenti dell'oggetto parzialmente rilevato. Nell'elenco dei computer, vista **Computer**, cliccare col tasto destro del mouse sul computer colpito e cliccare su **Scansione completa del sistema**. Per ulteriori informazioni, consultare la sezione Oggetto parzialmente rilevato (pagina 225).

Per disinfettare immediatamente i computer:

1. Nell'elenco computer, vista **Computer**, cliccare col tasto destro del mouse sul/i computer che si desidera disinfettare e successivamente cliccare su **Risolvi allarmi ed errori**.
2. Nella finestra di dialogo **Risolvi allarmi ed errori**, nella scheda **Allarmi**, selezionare la casella di spunta relativa a ciascun oggetto che si desidera disinfettare, oppure cliccare su **Seleziona tutti**. Cliccare su **Disinfetta**.

Se la disinfezione riesce, gli allarmi visualizzati nella lista dei computer scompaiono.

Se alcuni allarmi permangono, i computer devono essere disinfettati manualmente. Vedere Trattamento degli oggetti rilevati se la disinfezione non riesce (pagina 55).

 Copyright © Sophos Limited

Nota
la disinfezione di alcuni virus provoca l'esecuzione di una scansione completa del sistema nei computer interessati, la quale cerca di effettuare la disinfezione di *tutti* i virus. Ciò potrebbe richiedere molto tempo. Gli allarmi vengono aggiornati al termine della scansione.

5.7.3 Trattamento degli oggetti rilevati se la disinfezione non riesce

Se non è possibile disinfettare i computer dalla console è possibile eseguire tale operazione manualmente.

1. Nell'elenco computer, cliccare due volte sul computer infetto.
2. Nella finestra di dialogo **Dettagli computer**, scorrere in giù fino alla sezione **Allarmi ed errori in sospeso**. Nell'elenco degli oggetti rilevati, cliccare sul nome dell'oggetto che si desidera rimuovere dal computer.
   Questa operazione collega al sito web di Sophos, in cui sono contenuti consigli su come disinfettare i computer.
3. Andare al computer e procedere alla disinfezione manuale.

Nota
dal sito web di Sophos è possibile scaricare speciali programmi di rimozione per determinati virus e worm.

6 Aggiornamento dei computer

6.1 Configurazione del gestore aggiornamenti

Un gestore degli aggiornamenti consente di impostare aggiornamenti automatici del software di sicurezza Sophos da un sito web di Sophos. Il gestore degli aggiornamenti viene installato con e gestito da Enterprise Console.

È possibile installare gestori degli aggiornamenti aggiuntivi. Per esempio, se in possesso di una rete complessa con diversi percorsi, è possibile installare un gestore aggiornamenti aggiuntivo in un percorso remoto. Per informazioni, consultare la sezione Aggiunta di un gestore aggiornamenti addizionale (pagina 62).

6.1.1 Funzionamento del gestore aggiornamenti

Una volta configurato un gestore aggiornamenti, questo:

- Si connette, a una frequenza pianificata, alla warehouse di distribuzione dei dati di Sophos o della rete.
- Scarica gli aggiornamenti ai dati della rilevazione delle minacce e ai software di sicurezza a cui è sottoscritto l'amministratore.
- Posiziona i software aggiornati in una o più condivisioni di rete, in un formato compatibile per l'installazione nei computer.

I computer si aggiornano automaticamente dalle condivisioni solo se il software Sophos installato è stato configurato per svolgere questa operazione, per esempio tramite l'applicazione di un criterio di aggiornamento.

6.1.2 Visualizzazione o modifica della configurazione del gestore aggiornamenti

Se si utilizza l'amministrazione basata sui ruoli, per poter configurare un gestore degli aggiornamenti, è necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Se si è nella vista **Computer**, per poter accedere alla vista **Gestori aggiornamenti**, cliccare sul pulsante **Gestori aggiornamenti** che si trova nella barra degli strumenti,.
2. Nell'elenco dei gestori degli aggiornamenti, selezionare quello la cui configurazione si desidera visualizzare o modificare. Cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza/ Modifica configurazione**.

   Nota
   in alternativa, selezionare il gestore aggiornamenti, andare al menu **Azioni**, andare a **Update manager** e successivamente cliccare su **Visualizza/Modifica configurazione**.

   Viene visualizzata la finestra di dialogo **Configura il gestore aggiornamenti**.
3. Modificare la configurazione secondo quanto descritto nei seguenti argomenti:

 Copyright © Sophos Limited

- Scelta di una fonte degli aggiornamenti per un gestore aggiornamenti (pagina 57).
- Scelta del software da scaricare (pagina 58).
- Indicazioni circa la collocazione del software (pagina 59).
- Creazione o modifica di una pianificazione aggiornamento (pagina 60).
- Configurazione del log del gestore aggiornamenti (pagina 61).
- Configurazione dell'autoaggiornamento di un gestore aggiornamenti (pagina 61).

Per informazioni su come cancellare allarmi del gestore aggiornamenti dalla console, consultare la sezione Cancellazione degli allarmi del gestore aggiornamenti dalla console (pagina 78).

Dopo avere configurato il gestore aggiornamenti, è possibile configurare i propri criteri di aggiornamento e applicarli ai computer.

6.1.3 Scelta di una fonte degli aggiornamenti per un gestore aggiornamenti

Se si utilizza l'amministrazione basata sui ruoli, per poter configurare un gestore degli aggiornamenti, è necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È necessario selezionare una fonte da cui il gestore aggiornamenti scaricherà il software di sicurezza ed i relativi aggiornamenti da distribuire nella rete.

È possibile selezionare diverse fonti. La prima fonte dell'elenco è quella primaria. Le altre fonti inserite nell'elenco sono percorsi alternativi opzionali che il gestore aggiornamenti utilizzerà nel caso in cui non riesca a reperire un aggiornamento dalla fonte primaria.

1. Se si è nella vista **Computer**, per poter accedere alla vista **Gestori aggiornamenti**, cliccare sul pulsante **Gestori aggiornamenti** che si trova nella barra degli strumenti,.
2. Nell'elenco dei gestori degli aggiornamenti, selezionare quello per cui si desidera selezionare una fonte degli aggiornamenti. Cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza/ Modifica configurazione**.
3. Nella finestra di dialogo **Configura il gestore aggiornamenti**, nella scheda **Fonti**, cliccare su **Aggiungi**.
4. Nella finestra di dialogo **Dettagli fonte**, nel campo **Indirizzo**, inserire l'indirizzo della fonte. L'indirizzo può essere sia un percorso UNC che HTTP.

   Se si desidera scaricare il software e gli aggiornamenti direttamente da Sophos, selezionare **Sophos**.
5. Se necessario, nei campi **Nome utente** e **Password**, inserire il nome utente e la password dell'account utilizzato per accedere alla fonte degli aggiornamenti.

   - Se la fonte di aggiornamento è Sophos, inserire le credenziali di download fornite da Sophos.
   - Se la fonte di aggiornamento è la condivisione di aggiornamento predefinita creata da un gestore aggiornamenti avente una posizione più elevata nella gerarchia degli aggiornamenti, i campi **Nome utente** e **Password** saranno prepopolati.

     La condivisione di aggiornamento predefinita è una condivisione UNC `\\<NomeComputer>\SophosUpdate`, in cui NomeComputer è il nome del computer in cui il gestore aggiornamenti è installato.
   - Se la fonte di aggiornamento è una condivisione degli aggiornamenti non predefinita nella rete, inserire le credenziali dell'account che ha diritti di lettura per la condivisione. Se il **Nome utente** deve riportare il dominio, utilizzare la forma dominio\nome utente.

6. Se si accede alla fonte di aggiornamento tramite server proxy, selezionare **Utilizza server proxy per la connessione** . Quindi inserire l'**Indirizzo** e il numero di **Porta** del server proxy. 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. Cliccare su OK.
   La nuova fonte viene inclusa nell'elenco presente nella finestra di dialogo **Configura il gestore aggiornamenti**.

Se è già stato installato un gestore aggiornamenti in un computer differente, la condivisione da cui tale gestore scarica il software e gli aggiornamenti comparirà nell'elenco degli indirizzi. È possibile scegliere tale condivisione come fonte per il gestore aggiornamenti che si sta configurando. È poi possibile spostare in cima all'elenco l'indirizzo che si desidera considerare primario tramite i pulsanti **Sposta su** e **Sposta giù** che si trovano a destra dell'elenco.

6.1.4 Scelta del software da scaricare

Se si utilizza l'amministrazione basata sui ruoli, per poter configurare un gestore degli aggiornamenti, è necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

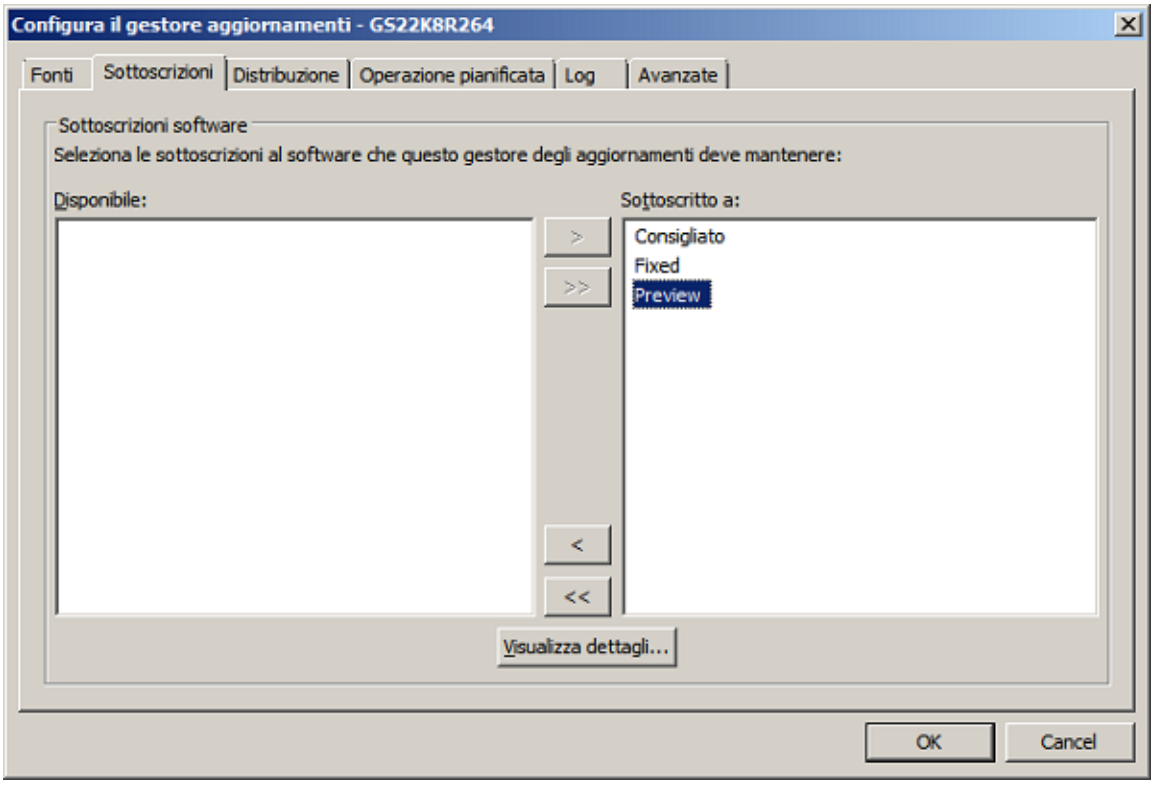
È necessario selezionare le sottoscrizioni che il gestore aggiornamenti manterrà aggiornate.

1. Se si è nella vista **Computer**, per poter accedere alla vista **Gestori aggiornamenti**, cliccare sul pulsante **Gestori aggiornamenti** che si trova nella barra degli strumenti,.
2. Nell'elenco dei gestori degli aggiornamenti, selezionare quello per cui si desidera scegliere il software da scaricare. Cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza/Modifica configurazione**.
3. Nella finestra di dialogo **Configura il gestore aggiornamenti**, nella scheda **Sottoscrizioni**, selezionarne una dall'elenco delle sottoscrizioni disponibili.

   Per visualizzare i dettagli della sottoscrizione, per esempio quali software sono inclusi nella sottoscrizione, cliccare su **Visualizza dettagli**.
4. Per spostare la sottoscrizione selezionata nell'elenco "Sottoscritto a", cliccare sul pulsante "Aggiungi".

   Per spostare tutte le sottoscrizioni nell'elenco "Sottoscritto a", cliccare sul pulsante "Aggiungi".

 Copyright © Sophos Limited



6.1.5 Indicazioni circa la collocazione del software

Se si utilizza l'amministrazione basata sui ruoli, per poter configurare un gestore degli aggiornamenti, è necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Una volta scelto quale software scaricare, è possibile indicare dove collocarlo nella rete. Per impostazione predefinita, il software è collocato in una condivisione UNC `\\<NomeComputer>\SophosUpdate`, in cui NomeComputer è il nome del computer in cui è installato il gestore aggiornamenti.

È possibile distribuire i software scaricati a condivisioni aggiuntive nella rete. Per far ciò, aggiungere all'elenco delle condivisioni disponibili una condivisione di rete esistente e poi spostarla nell'elenco delle condivisioni di aggiornamento secondo quanto descritto di seguito. Assicurarsi che l'account utente di Update Manager (**SophosUpdateMgr**) abbia diritti di lettura per le condivisioni.

Nota
L'account utente di Update Manager deve essere creato prima di eseguire l'installazione di Enterprise Console. Per ulteriori informazioni sull'account, consultare la documentazione relativa all'avvio di Enterprise Console.

Per specificare dove è collocato il software:

1. Se si è nella vista **Computer**, per poter accedere alla vista **Gestori aggiornamenti**, cliccare sul pulsante **Gestori aggiornamenti** che si trova nella barra degli strumenti,.
2. Nell'elenco dei gestori degli aggiornamenti, selezionare quello per cui si desidera scegliere le condivisioni di rete per la distribuzione del software. Cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza/Modifica configurazione**.

3. Nella finestra di dialogo **Configura il gestore aggiornamenti**, nella scheda **Distribuzione**, selezionare dall'elenco la sottoscrizione al software.
4. Selezionare una condivisione dall'elenco delle condivisioni "Disponibile" e spostarla nell'elenco "Aggiorna a" cliccando sul pulsante "Aggiungi" (>).

   La condivisione predefinita `\\<NomeComputer>\SophosUpdate` è sempre presente nell'elenco "Aggiorna a". Non è possibile rimuovere tale condivisione dall'elenco.

   L'elenco delle condivisioni "Disponibile" comprende tutte le condivisioni di cui Enterprise Console è al corrente e non ancora utilizzate da un altro gestore aggiornamenti.

   È possibile aggiungere o rimuovere condivisioni dall'elenco "Disponibile" tramite il pulsante "Aggiungi" (>) o "Rimuovi" (<).
5. Se si desidera inserire una descrizione per la condivisione o le credenziali necessarie per scrivere nella condivisione, selezionare la condivisione e cliccare su **Configura**. Nella finestra di dialogo **Gestione condivisione**, inserire la descrizione e le credenziali.

   Se si desidera immettere le stesse credenziali per più condivisioni, selezionare le condivisioni nell'elenco “Aggiorna a” e cliccare su **Configura**. Nella finestra di dialogo **Configura condivisioni multiple**, immettere le credenziali che verranno usate per scrivere sulle condivisioni.

6.1.6 Creazione o modifica di una pianificazione aggiornamento

Se si utilizza l'amministrazione basata sui ruoli, per poter configurare un gestore degli aggiornamenti, è necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per impostazione predefinita, un gestore aggiornamenti verificherà ogni 10 minuti la disponibilità, nella banca dati Sophos, di aggiornamenti relativi ai **dati sul rilevamento delle minacce**.

È possibile modificare questo intervallo di aggiornamento. Il tempo minimo è 5 minuti e quello massimo 1440 (24 ore). Si consiglia un intervallo di aggiornamento di 10 minuti per i dati relativi al rilevamento delle minacce, in modo tale da ottenere la protezione dalle minacce più recenti, non appena Sophos pubblichi i dati del rilevamento.

Per impostazione predefinita, un gestore aggiornamenti verificherà ogni 60 minuti la disponibilità, nella banca dati Sophos, di aggiornamenti **software**.

È possibile modificare questo intervallo di aggiornamento. Il tempo minimo è 10 minuti e quello massimo 1440 (24 ore).

Per gli aggiornamenti software, è possibile specificare un intervallo di aggiornamento che avvenga ogni ora tutti i giorni, oppure creare pianificazioni più sofisticate in cui ogni giorno può essere organizzato in modo autonomo e suddiviso in periodi aventi intervalli di aggiornamento differenti.

Nota
è possibile creare diverse pianificazioni per differenti giorni della settimana. Una sola pianificazione può essere associata a un determinato giorno della settimana.

1. Se si è nella vista **Computer**, per poter accedere alla vista **Gestori aggiornamenti**, cliccare sul pulsante **Gestori aggiornamenti** che si trova nella barra degli strumenti,.
2. Nell'elenco dei gestori degli aggiornamenti, selezionare quello per cui si desidera creare una pianificazione degli aggiornamenti. Cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza/Modifica configurazione**.
3. Nella finestra di dialogo **Configura il gestore aggiornamenti**, nella scheda **Operazione pianificata**, inserire l'intervallo tra gli aggiornamenti dei dati sul rilevamento delle minacce.
4. Inserire l'intervallo tra gli aggiornamenti software.

 Copyright © Sophos Limited

- È necessario indicare un intervallo di aggiornamento utilizzato giornalmente ogni ora, selezionare l'opzione **Verifica disponibilità aggiornamenti ogni n minuti** ed inserire l'intervallo in minuti.
- Se si desidera creare pianificazioni più sofisticate o diverse per ciascun giorno della settimana, selezionare l'opzione **Imposta e gestisci gli aggiornamenti pianificati** e cliccare su **Aggiungi**.

  Nella finestra di dialogo **Aggiorna operazione pianificata**, inserire il nome della pianificazione, i giorni della settimana e gli intervalli di aggiornamento.

6.1.7 Configurazione del log del gestore aggiornamenti

Se si utilizza l'amministrazione basata sui ruoli, per poter configurare un gestore degli aggiornamenti, è necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Se si è nella vista **Computer**, per poter accedere alla vista **Gestori aggiornamenti**, cliccare sul pulsante **Gestori aggiornamenti** che si trova nella barra degli strumenti,.
2. Nell'elenco dei gestori degli aggiornamenti, selezionare quello per cui si desidera configurare il file di log. Cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza/Modifica configurazione**.
3. Nella finestra di dialogo **Configura il gestore aggiornamenti**, nella scheda **Log**, selezionare il numero di giorni entro cui si desidera conservare il log e la sua dimensione massima.

6.1.8 Configurazione dell'autoaggiornamento di un gestore aggiornamenti

Se si utilizza l'amministrazione basata sui ruoli, per poter configurare un gestore degli aggiornamenti, è necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Se si è nella vista **Computer**, per poter accedere alla vista **Gestori aggiornamenti**, cliccare sul pulsante **Gestori aggiornamenti** che si trova nella barra degli strumenti,.
2. Nell'elenco dei gestori degli aggiornamenti, selezionare quello per cui si desidera configurare l'autoaggiornamento. Cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza/Modifica configurazione**.
3. Nella finestra di dialogo **Configura il gestore aggiornamenti**, nella scheda **Avanzate**, selezionare la versione del gestore aggiornamenti che si desidera mantenere aggiornata.
   Per esempio, se si seleziona "consigliata", il gestore aggiornamenti eseguirà sempre l'upgrade alla versione considerata più recente da Sophos. L'attuale versione del gestore aggiornamenti cambierà.

6.1.9 Verifica immediata degli aggiornamenti da parte del gestore degli aggiornamenti

Se si utilizza l'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Correzione - aggiornamento e scansione**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Dopo aver configurato un gestore degli aggiornamenti, quest'ultimo verifica gli aggiornamenti e li scarica dalle fonte degli aggiornamenti alle condivisioni degli aggiornamenti che gestisce automaticamente, secondo una pianificazione specifica. Se si desidera che il gestore degli

aggiornamenti ricerchi e scarichi immediatamente gli aggiornamenti relativi ai dati sul rilevamento delle minacce, gli aggiornamenti dei software per computer e quelli per lo stesso gestore degli aggiornamenti, seguire i passaggi riportati di seguito:

1. Se si è nella vista **Computer**, per poter accedere alla vista **Gestori aggiornamenti**, cliccare sul pulsante **Gestori aggiornamenti** che si trova nella barra degli strumenti,.
2. Nell'elenco dei gestori degli aggiornamenti, selezionare quello che si desidera aggiornare. Cliccarvi col tasto destro del mouse e cliccare su **Aggiorna ora**.

6.1.10 Allineamento del gestore aggiornamenti alle impostazioni della configurazione

Se si utilizza l'amministrazione basata sui ruoli, per poter configurare un gestore degli aggiornamenti, è necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Se si è nella vista **Computer**, per poter accedere alla vista **Gestori aggiornamenti**, cliccare sul pulsante **Gestori aggiornamenti** che si trova nella barra degli strumenti,.
2. Nell'elenco dei gestori degli aggiornamenti, selezionare quello che si desidera allineare alle impostazioni della configurazione. Cliccarvi col tasto destro del mouse e successivamente cliccare su **Allinea con la configurazione**.

6.1.11 Aggiunta di un gestore aggiornamenti addizionale

Sophos Update Manager (SUM) viene sempre installato nel computer in cui viene installata Enterprise Console. Se durante l'installazione è stato selezionato **Installazione personalizzata**, questo sarà il computer in cui verrà installato il server di gestione.

È possibile aggiungere alla rete uno o più gestori degli aggiornamenti addizionali. Ciò riduce il carico sul gestore aggiornamenti già installato e distribuisce gli aggiornamenti in modo più efficace. È possibile installare un gestore aggiornamenti addizionale in un computer non ancora in possesso di gestore aggiornamenti installato.

Importante
non rimuovere il gestore aggiornamenti installato nello stesso computer in cui è installato il server di gestione di Enterprise Console. Finché questo gestore degli aggiornamenti non è configurato con una fonte per gli aggiornamenti, Enterprise Console non può proteggere completamente la rete. Ciò consentirà a Enterprise Console di ricevere gli aggiornamenti necessari (per es. informazioni relative ai software di sicurezza che i computer dovrebbero eseguire, Content Control List nuove e aggiornati per il controllo dati o l'elenco di nuovi dispositivi o applicazioni controllati).

Per consentire a un gestore aggiornamenti addizionale di scaricare il software di sicurezza da Sophos o da un gestore aggiornamenti tramite HTTP, aprire la porta 80 (in uscita) nel computer sul quale si desidera installare il gestore aggiornamenti addizionale. Per consentire al gestore degli aggiornamenti di scaricare il software di sicurezza da un altro gestore aggiornamenti tramite percorso UNC, aprire le seguenti porte in uscita del computer: porta UDP 137, porta UDP 138, porta TCP 139 e porta TCP 445.

Se nel computer è in esecuzione una versione di Windows che include la funzione Individuazione rete e la funzione è disattivata, attivarla e riavviare il computer.

Se il Controllo dell'account utente (UAC) è abilitato nel computer, disabilitarlo e riavviare il computer. Potrà essere riattivato una volta installato il gestore degli aggiornamenti e sottoscritto gli aggiornamenti Sophos.

 Copyright © Sophos Limited

Se il computer si trova in un dominio, accedere come amministratore di dominio.

Se il computer si trova in un gruppo di lavoro, accedere come amministratore locale.

Il programma di installazione del gestore aggiornamenti è posizionato nel computer in cui è installato il server di gestione di Enterprise Console, nella cartella condivisa `\\Nomeserver\SUMInstallSet`. Per visualizzare il percorso del programma di installazione, andare al menu **Visualizza** e cliccare su **Percorso del programma di installazione di Update Manager**.

È possibile installare Sophos Update Manager tramite Windows Remote Desktop.

Per installare una gestione di aggiornamenti supplementare:

1. Eseguire il programma di installazione di Update Manager **Setup.exe**.
   Viene avviata la procedura guidata di installazione.
2. Nella pagina **Benvenuti** della procedura guidata, cliccare su **Avanti**.
3. **Nella pagina Contratto di licenza**, leggere il contratto e cliccare su Accetto i termini del contratto di licenza se se ne accettano i termini. Cliccare su **Avanti**.
4. Nella pagina **Cartella di destinazione**, accettare l'impostazione predefinita o cliccare su **Cambia** e inserire una nuova cartella di destinazione. Cliccare su **Avanti**.
5. Dalla pagina **Distribuzione dati non gestita**, selezionare un account che i computer utilizzeranno per accedere alla condivisione predefinita degli aggiornamenti creata dal gestore aggiornamenti (Il percorso predefinito per la condivisione degli aggiornamenti è `\\<NomeComputer>\SophosUpdate`, ove NomeComputer è il nome del computer su cui è installato il gestore aggiornamenti). Questo account deve essere possesso di diritti di lettura per la condivisione, e non è necessario che abbia anche diritti di amministrazione.

   È possibile selezionare un utente predefinito, esistente o crearne uno nuovo.

   Per impostazione predefinita, il programma di installazione crea l'account **SophosUpdateMgr** con diritti di lettura per la condivisione degli aggiornamenti predefinita, ma con nessun diritto di accesso interattivo.

   Se, in un secondo tempo, si desiderano aggiungere ulteriori condivisioni degli aggiornamenti, selezionare un account esistente o crearne uno nuovo che abbia diritti di lettura per tali condivisioni. In alternativa, assicurarsi che l'account di **SophosUpdateMgr** abbia diritti di lettura per le condivisioni.
6. Nella pagina **Dettagli dell'account di Sophos Update Manager**, a seconda dell'opzione selezionata nella pagina precedente, inserire una password per l'utente predefinito, dettagli relativi al nuovo utente o selezionare account esistenti.

   La password per l'account deve essere conforme al criterio password.
7. Nella pagina **Pronta per l'installazione del programma**, cliccare su **Installa**.
8. Una volta portata a termine l'installazione, cliccare su **Fine**.

Il computer in cui è stato installato Sophos Update Manager dovrebbe ora apparire in Enterprise Console, visualizzare **Update manager** (Dal menu **Visualizza**, cliccare su **Update Manager**.)

Per configurare il gestore aggiornamenti, selezionarlo, cliccarvi col tasto destro del mouse e poi cliccare **Visualizza/Modifica configurazione**.

6.1.12 Pubblicazione del software di sicurezza in un server web

È possibile pubblicare il software di sicurezza Sophos su un server web, in modo tale che i computer vi accedano tramite HTTP.

Per pubblicare il software di sicurezza in un server web:

1. Trovare il percorso della cartella condivisa in cui è stato scaricato il software di sicurezza; tale percorso è conosciuto come percorso bootstrap:

a) In Enterprise Console, dal menu **Visualizza**, cliccare su **Percorsi Bootstrap**.
Nella finestra di dialogo **Percorsi Bootstrap**, nella colonna **Percorso** vengono visualizzati i percorsi bootstrap per tutte le piattaforme.

b) Annotare il percorso fino alla cartella delle `CID`, senza includerla. Per esempio:
`\\nome server\SophosUpdate`

2. Rendere disponibile nel server web il percorso bootstrap, comprese le sottocartelle. Per istruzioni, consultare l'articolo 38238 della knowledge base Sophos.

6.2 Configurazione delle sottoscrizioni ai software

La sottoscrizione a un software specifica quali versioni del software del computer vengono scaricate da Sophos per ciascuna piattaforma.

La **procedura guidata per il download del software di sicurezza** imposta una sottoscrizione predefinita che specifica le versioni consigliate per tutti i software selezionati.

Se si desidera aggiungere un software alla propria sottoscrizione o sottoscrivere una versione diversa da quella consigliata, configurare la sottoscrizione secondo quanto descritto in Sottoscrizione al software di sicurezza (pagina 66).

Se dopo l'installazione di Enterprise Console non è stata portata a termine la procedura guidata, consultare la sezione Esecuzione della procedura guidata di download del software di sicurezza (pagina 68).

6.2.1 Tipi di aggiornamento disponibili

Per ciascuna piattaforma (per es. Windows), sono disponibili diversi pacchetti software rappresentanti diversi tipi di aggiornamento e diversi versioni di software per endpoint. È possibile scegliere il pacchetto software da scaricare da Sophos per ulteriori distribuzioni ai computer endpoint, selezionando uno dei seguenti tipi di aggiornamento nella sottoscrizione.

Tipo di aggiornamento	Descrizione
Consigliato	Si tratta di un pacchetto predefinito. Se si utilizza questo pacchetto, Sophos aggiorna il software regolarmente (solitamente con cadenza mensile) con: • Risoluzioni a problemi rilevati da clienti. • Nuove funzioni disponibili. Se si sta installando Enterprise Console per la prima volta e si accettano le impostazioni predefinite, questo è il tipo di pacchetto che si utilizzerà.

Copyright © Sophos Limited

Tipo di aggiornamento	Descrizione
Panoramica	Questo pacchetto è stato pensato per amministratori IT e della sicurezza. Se si utilizza questa versione, si potranno utilizzare nuove funzioni prima del loro rilascio nel pacchetto di aggiornamento Consigliato. Ciò consentirà di testare e valutare le novità a disposizione (n reti di test) prima che siano a disposizione nelle altre versioni. **Nota** A volte il pacchetto Panoramica fornisce le stesse funzioni di quello Consigliato. Ciò si verifica quando le nuove funzioni sono pronte per essere testate in ambienti cliente.
Esteso	Il pacchetto degli aggiornamenti Esteso è pensato per clienti con processi di installazione nella rete rigidi o conservativi. Se si utilizza questa versione, si riceveranno gli stessi aggiornamenti a disposizione dei pacchetti Consigliati con un ritardo di diversi mesi. Ciò significa che gli eventuali problemi identificati nel prodotto saranno stati già risolti una volta si proceda all'installazione nella rete.
Precedentemente consigliato	La versione precedente dell'attuale pacchetto consigliato. Questa versione è utile se si desidera più tempo per testare il nuovo software prima di effettuare la distribuzione nella rete.
Precedentemente esteso	La versione precedente dell'attuale pacchetto esteso. Questa versione è utile se si desidera più tempo per testare il nuovo software prima di effettuare la distribuzione nella rete.
Versioni fisse	Vedere Versioni fisse di pacchetti software (pagina 65).

Nota
Questi pacchetti potrebbero essere modificati nel tempo. Per ulteriori informazioni sui pacchetti software attualmente disponibili, consultare l'articolo 119216 della knowledge base Sophos.

La **Procedura guidata per il download del software di sicurezza** imposta una sottoscrizione che specifica le versioni consigliate di tutti i software selezionati.

Le versioni scaricate ogni mese cambieranno ogni mese. Per verificare quali versioni software siano disponibili per il download, nella finestra di dialogo **Sottoscrizioni software**, scegliere il pacchetto che si desidera visionare e cliccare su **Dettagli**.

6.2.2 Versioni fisse di pacchetti software

Una versione fissa è una versione fissa aggiornata mensilmente con i nuovi dati relativi al rilevamento delle minacce, ma non con la versione più recente del software. Un esempio di versione fissa di Sophos Endpoint Security and Control per Windows è "10.3.15 VE3.60.0". Si tratta di un identificatore di versione composto da tre parti (identificatore del rilascio principale [10], identificatore del rilascio minore [3], identificatore del rilascio di manutenzione [15]), più la versione del motore di rilevamento delle minacce (VE3.60.0).

Uso di pacchetti fissi

Per impostazione predefinita, l'uso di versioni fisse di pacchetti software è disattivato (vedere sotto **Strumenti > Configura l'uso di pacchetti fissi**). Non sono visualizzati nella casella di dialogo **Sottoscrizioni software**, e non è possibile effettuarne la sottoscrizione.

Consiglio
Se si è sottoscritti a una versione fissa del software, per garantire la migliore protezione passare alla sottoscrizione di un pacchetto "Recommended". Per ulteriori informazioni sui pacchetti software, consultare la sezione Tipi di aggiornamento disponibili (pagina 64).

Se in precedenza non si è mai fatto uso di versioni fisse di pacchetti software ma si desidera cominciare a utilizzarle, è possibile abilitare l'uso di pacchetti fissi sotto **Strumenti > Configura l'uso di pacchetti fissi**. Una volta abilitato l'uso di pacchetti fissi, tali pacchetti vengono visualizzati nella casella di dialogo **Sottoscrizioni software**, dove è possibile effettuare la sottoscrizione ad essi.

Nota
Se si utilizza l'amministrazione basata sui ruoli, è necessario essere in possesso di diritti di **Configurazione del sistema** per poter configurare l'uso di pacchetti fissi.

Se si disattiva l'uso di pacchetti fissi mentre si è in possesso di una sottoscrizione in corso di validità a un pacchetto fisso, verrà mantenuta la sottoscrizione a tale pacchetto, che continuerà a essere scaricato sino a quando non ne venga cancellata la sottoscrizione. Non si sarà tuttavia in grado di visualizzare o di effettuare nuovamente la sottoscrizione a un pacchetto fisso diverso.

In presenza di console remote, la modifica di questa configurazione in una di esse verrà implementata su tutte le console. Se l'uso di pacchetti fissi è stato abilitato nel registro di sistema (come indicato nell'articolo 117348 della knowledge base Sophos), le impostazioni del registro di sistema verranno applicate solamente al computer che è stato utilizzato per la configurazione, e assumeranno la precedenza rispetto all'opzione di configurazione della console.

Ciclo di vita dei pacchetti fissi

Le versioni fisse vengono scaricate fino a che sono rese disponibili da Sophos. Se una versione fissa verrà ritirata, nella vista **Update manager** comparirà un allarme di fianco a tutti i gestori degli aggiornamenti che hanno sottoscritto quella versione. Se gli allarmi e-mail sono attivi, anche l'amministratore riceverà un allarme e-mail.

Quando viene ritirata una versione fissa per la quale si era in possesso di una sottoscrizione, verrà automaticamente effettuata la sottoscrizione a un pacchetto esteso fisso più recente, a meno che non sia stata modificata la sottoscrizione prima del termine del supporto. Per ulteriori informazioni, consultare l'articolo 121139 della knowledge base Sophos.

Per maggiori informazioni sui criteri applicati al ciclo di vita dei prodotti Sophos, consultare l'articolo 112580 della knowledge base Sophos .

6.2.3 Sottoscrizione al software di sicurezza

Se si utilizza l'amministrazione basata sui ruoli:

Copyright © Sophos Limited

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento** per modificare la sottoscrizione a un software.
- È impossibile modificare una sottoscrizione se quest'ultima è applicata a un criterio di aggiornamento applicato al di fuori del sottoambiente attivo.

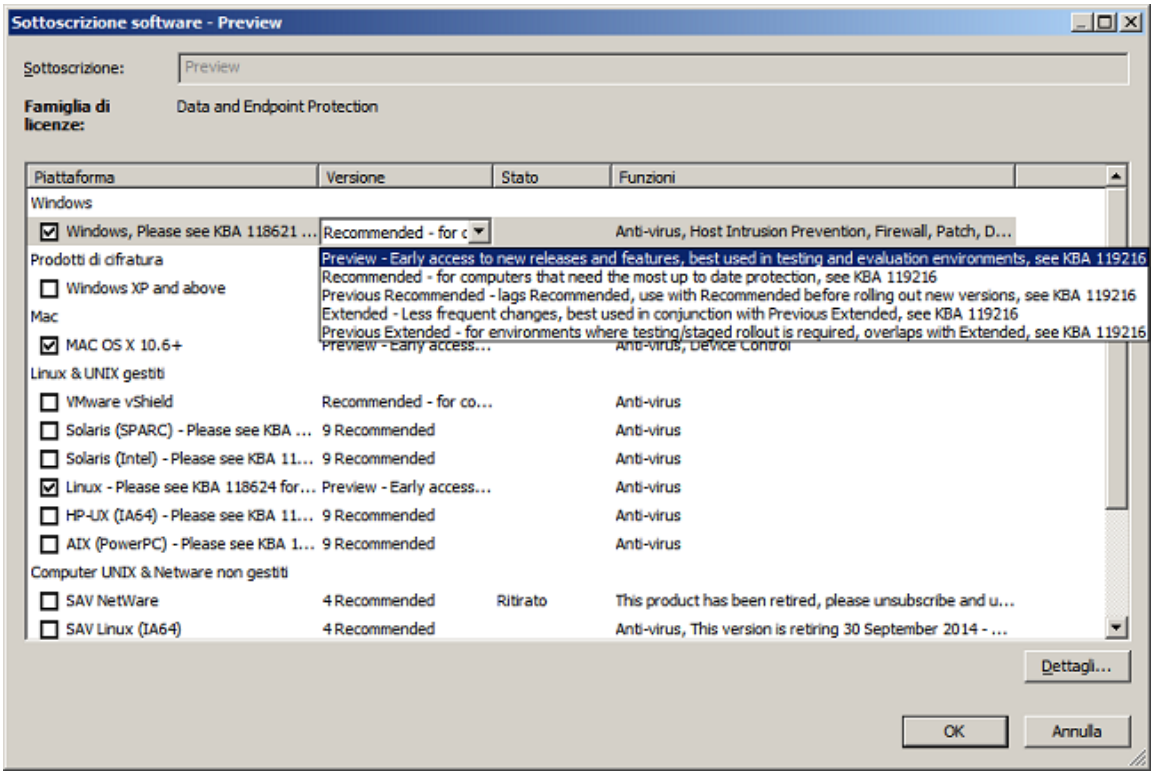
Per ulteriori informazioni sull'amministrazione basata sui ruoli, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per eseguire la sottoscrizione a un software di sicurezza:

1. Dal menu **Visualizza**, cliccare su **Update Manager**.
2. Nel riquadro **Sottoscrizioni software**, cliccare due volte sulla sottoscrizione che si desidera modificare oppure cliccare sul pulsante **Aggiungi**, nella parte alta del riquadro, per creare una nuova sottoscrizione.

   Viene visualizzata la finestra di dialogo **Sottoscrizione al software**.

   In alternativa, se si desidera creare una copia di una sottoscrizione esistente, selezionare tale sottoscrizione, cliccarvi col tasto destro del mouse e quindi cliccare su **Duplica sottoscrizione**. Digitare un nuovo nome per la sottoscrizione e cliccarvi due volte per aprire la finestra di dialogo **Sottoscrizione software**.
3. Nella finestra di dialogo **Sottoscrizione software**, se lo si desidera, modificare il nome della sottoscrizione.
4. Selezionare le piattaforme per cui scaricare il software.
5. Per impostazione predefinita si è sottoscritti a un pacchetto "Recommended". È comunque possibile scegliere un pacchetto che non predefinito (per es. nel caso si desideri vedere l'anteprima di alcune funzioni). Per far ciò, cliccare nel campo **Versione** di fianco alla piattaforma per cui si desidera cambiare il pacchetto, quindi cliccare di nuovo. Dal menu a discesa relativo alle versioni disponibili, scegliere la versione che si desidera scaricare (per es. "Anteprima").



Per informazioni su quali altri pacchetti siano disponibili, consultare la sezione Tipi di aggiornamento disponibili (pagina 64).

Portata a termine la sottoscrizione a un software di sicurezza, è possibile impostare gli allarmi e-mail relativi a tale sottoscrizione. Per ulteriori informazioni, consultare la sezione Impostazione degli allarmi relativi alle sottoscrizioni software (pagina 186).

Se si è creata una nuova sottoscrizione al software, configurare il gestore degli aggiornamenti in modo tale che la mantenga, secondo quanto descritto in Visualizzazione o modifica della configurazione del gestore aggiornamenti (pagina 56).

6.2.4 Esecuzione della procedura guidata di download del software di sicurezza

Se si utilizza l'amministrazione basata sui ruoli, per poter eseguire la **Procedura guidata di download del software di sicurezza**, è necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento** . Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Se, dopo l'installazione di Enterprise Console, non è stata portata a termine la **Procedura guidata di download del software di sicurezza**, fare quanto riportato di seguito:

- Nel menu **Azioni**, cliccare su **Esegui la Procedura guidata di download del software di sicurezza**.

  La **procedura guidata di download del software di sicurezza** accompagna durante la scelta ed il download di un software.

Nota
Una volta completata la procedura guidata, l'opzione **Esegui la Procedura guidata di download del software di sicurezza** scomparirà dal menu **Azioni**.

6.2.5 Verifica di quali criteri di aggiornamento utilizzino la sottoscrizione al software

Per verificare quali criteri di aggiornamento utilizzino la sottoscrizione al software:

- Selezionare la sottoscrizione, cliccarvi col tasto destro del mouse e poi cliccare su **Visualizza utilizzo sottoscrizione**.

  Nella finestra di dialogo **Utilizzo delle sottoscrizioni al software**, viene visualizzato un elenco di criteri di aggiornamento che utilizzano tale sottoscrizione.

6.3 Configurazione del criterio di aggiornamento

Un criterio di aggiornamento consente di mantenere i computer aggiornati con i più recenti software di sicurezza. Enterprise Console verificherà la disponibilità di aggiornamenti e aggiornerà i computer, se necessario a intervalli regolari.

Il criterio di aggiornamento predefinito consente di installare e aggiornare il software specificato nella sottoscrizione "consigliata".

 Copyright © Sophos Limited

Se si desidera modificare il criterio di aggiornamento predefinito o crearne uno nuovo, seguire le istruzioni riportate nel seguente argomento.

- Scelta di una sottoscrizione (pagina 69)
- Configurazione dei server di aggiornamento (pagina 70)
- Pianificazione degli aggiornamenti (pagina 75)
- Selezione di una fonte differente per l'installazione iniziale (pagina 76)
- Log degli aggiornamenti (pagina 76)

Nota

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento** per confermare un criterio di aggiornamento.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni sull'amministrazione basata sui ruoli, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

6.3.1 Scelta di una sottoscrizione

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento** per confermare un criterio di aggiornamento.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

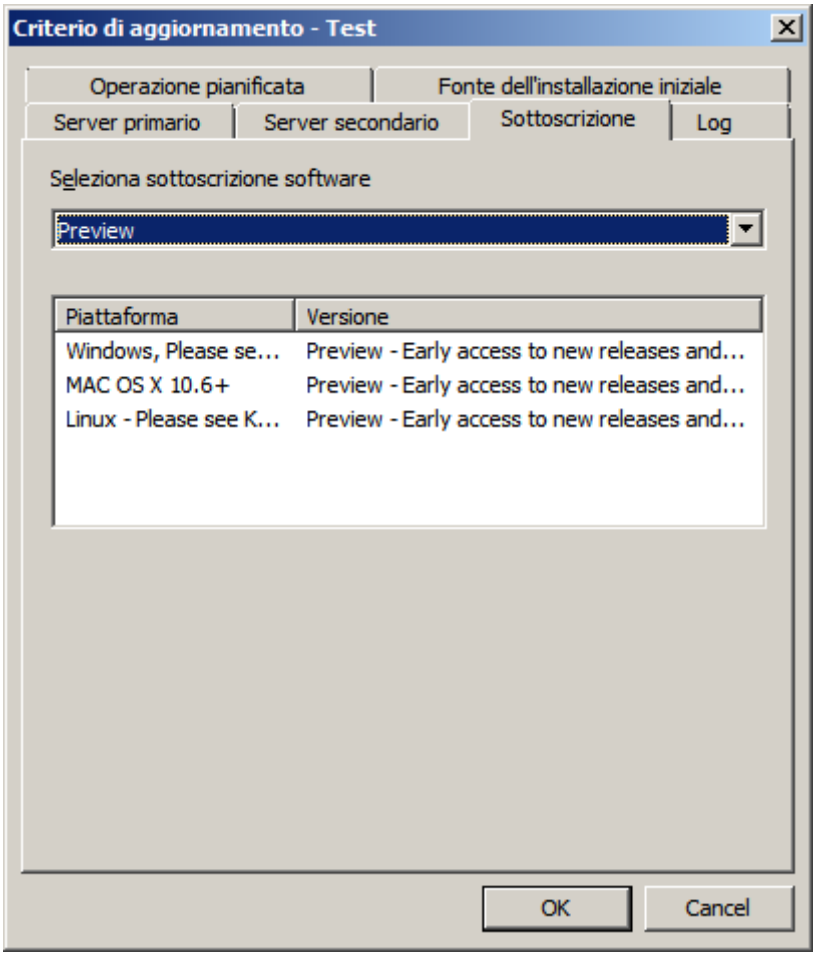
Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Una sottoscrizione specifica quali versioni del software del computer vengono scaricate da Sophos per ciascuna piattaforma. La sottoscrizione predefinita include il software più recente per Windows.

Per selezionare una sottoscrizione:

1. Controllare quale criterio di aggiornamento è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri,** cliccare due volte su **Aggiornamento**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criterio di aggiornamento**, cliccare sulla scheda **Sottoscrizioni** e selezionare la sottoscrizione per il software che si desidera mantenere aggiornato.



6.3.2 Configurazione dei server di aggiornamento

Per impostazione predefinita, i computer si aggiornano da una singola condivisione primaria UNC di origine, `\\<NomeComputer>\SophosUpdate`, dove `<NomeComputer>` è il nome del computer dell'Update Manager. È inoltre possibile specificare una fonte secondaria alternativa per gli aggiornamenti, abilitare la ricerca automatica di un percorso, e attivare la regolazione della larghezza di banda.

Se i computer endpoint non riescono a contattare la propria fonte primaria, cercheranno di aggiornarsi dalla fonte secondaria (se ne è stata indicata una). Si consiglia di specificare sempre una fonte secondaria.

I percorsi primari e secondari del server per gli aggiornamenti possono essere condivisioni UNC, oppure URL HTTP accessibili da qualsiasi Update Manager sulla propria rete. In alternativa, il percorso secondario del server per gli aggiornamenti può venire impostato in modo che ottenga aggiornamenti direttamente da Sophos su internet, tramite HTTP.

Nota
Gli Update Manager possono avere a disposizione condivisioni di distribuzione multiple, a seconda di come sono stati impostati.

Copyright © Sophos Limited

Server primario

Il server primario viene automaticamente impostato con il percorso del server primario predefinito. Per impostazione predefinita, i computer si aggiornano da una singola condivisione primaria UNC di origine, `\\<NomeComputer>\SophosUpdate`, ove `<NomeComputer>` è il nome del computer su cui è installato Sophos Update Manager.

Per accedere alla condivisione, i computer utilizzano le credenziali di Sophos Update Manager inserite durante l'installazione di Enterprise Console. Se si sono seguite le raccomandazioni indicate nella Guida di avvio di Enterprise Console, il nome dell'account sarà "SophosUpdateMgr".

Se si desidera modificare le credenziali, consultare la sezione Modifica delle credenziali del server primario (pagina 73).

Se si accede alla fonte degli aggiornamenti tramite server proxy, cliccare su **Dettagli proxy** e inserire i dettagli del server proxy.

Se si desidera abilitare la ricerca automatica di un percorso, vedere Ricerca automatica di un percorso nei laptop (pagina 71).

È anche possibile abilitare la regolazione della larghezza di banda, per limitare la quantità di larghezza di banda che possono utilizzare i computer durante gli aggiornamenti. Nella scheda **Server primario** del criterio di aggiornamento, cliccare sul pulsante **Avanzate**. Nella finestra di dialogo **Impostazioni avanzate**, spuntare la casella **Limita occupazione di banda**, e utilizzare l'indicatore di scorrimento per specificare la larghezza di banda limite, in Kbit al secondo.

Ricerca automatica di un percorso nei laptop

All'interno di un'organizzazione alcuni utenti con un laptop in dotazione possono spostarsi frequentemente e trovarsi in diversi paesi. Se è abilitata la ricerca automatica di un percorso (in un criterio di aggiornamento per laptop in roaming), i laptop in roaming cercheranno di trovare e di aggiornarsi dal server degli aggiornamenti a loro più vicino; tale server verrà identificato tramite richiesta ad altri computer endpoint (fissi) nella rete locale a cui i laptop sono connessi, riducendo al minimo i ritardi negli aggiornamenti e i costi legati alla larghezza di banda.

Un laptop in roaming riceve i percorsi e le credenziali del server di aggiornamento, facendone richiesta ai computer fissi all'interno della stessa rete locale. Se vengono restituiti percorsi multipli, il laptop determina quale sia quello più vicino e lo utilizza. Se nessuno di essi funziona, il laptop utilizzerà il o i percorsi primari (e successivamente quelli secondari) indicati nei criteri di aggiornamento.

Nota
quando i computer fissi inviano percorsi e credenziali di aggiornamento al laptop, le password sono occultate sia in fase di trasmissione, sia di memorizzazione. Tuttavia, è buona norma rendere il più restrittivi possibile gli account impostati per la lettura dei percorsi del server di aggiornamento, consentendo esclusivamente un accesso di sola lettura. Vedere Indicazioni circa la collocazione del software (pagina 59).

Per ulteriori informazioni sul funzionamento della ricerca automatica di un percorso, consultare la sezione Funzionamento della ricerca automatica di un percorso (pagina 72).

La ricerca automatica di un percorso è utilizzabile esclusivamente se:

- È presente un'unica Enterprise Console in comune per i computer endpoint fissi e quelli in roaming.
- I computer fissi utilizzano la stessa sottoscrizione software dei laptop in roaming.

- I laptop in roaming utilizzano il percorso di aggiornamento primario indicato nel criterio di aggiornamento.
- Gli eventuali firewall di terze parti sono configurati per consentire richieste e risposte relative al percorso degli aggiornamenti. Solitamente viene utilizzata la porta UDP 51235, ma si tratta di un elemento configurabile; per informazioni dettagliate, consultare l'articolo 110371 della knowledge base Sophos.

Si abilita la ricerca automatica di un percorso, come parte della specificazione delle fonti degli aggiornamenti. La ricerca automatica di un percorso dovrebbe essere abilitata solo per gruppi di computer che vengono spostati spesso da un ufficio all'altro. Per informazioni su come abilitare la ricerca automatica di un percorso, consultare la sezione Modifica delle credenziali del server primario (pagina 73).

Per le domande più frequenti relative alla ricerca automatica di un percorso, leggere l'articolo 112830 della knowledge base Sophos.

Funzionamento della ricerca automatica di un percorso

La ricerca automatica di un percorso è un tipo di aggiornamento intelligente per computer laptop in roaming, in cui gli aggiornamenti vengono eseguiti dal "miglior" percorso di aggiornamento disponibile, e non esclusivamente dai percorsi di aggiornamento primari e secondari indicati nel criterio di aggiornamento del computer laptop.

Quando è abilitata la ricerca automatica di un percorso, si verifica quanto riportato qui di seguito:

1. Quando un computer laptop cambia percorso, il componente Sophos AutoUpdate, facente parte di Endpoint Security and Control e installato nel computer laptop, rileva che l'indirizzo MAC del gateway predefinito, nella rete a cui si è connessi, è diverso da quello dell'ultimo aggiornamento. Invia un broadcast ICMP, attraverso la sottorete locale, alle installazioni di AutoUpdate più vicine, utilizzando la porta UDP predefinita 51235.
2. Tali installazioni di AutoUpdate rispondono utilizzando la stessa porta e comunicando il loro criterio di aggiornamento. La risposta inviata include solo il percorso di aggiornamento primario.

   Tutte le installazioni di Endpoint Security and Control restano in ascolto in attesa di broadcast, sia che la ricerca automatica del percorso sia abilitata o meno.

   Nelle risposte le informazioni sensibili vengono offuscate e i campi protetti con hash.

   I messaggi di risposta hanno un tempo di risposta impostato in modo casuale, per evitare tempeste di messaggi Anche le risposte sono boradcast ICMP, in modo tale che tutti i computer che avrebbero risposto fornendo gli stessi dettagli riceveranno il broadcast e sapranno di non dover rispondere.
3. AutoUpdate sceglie il percorso "migliore" tra quelli ricevuti, verifica se il mittente è gestito dalla stessa Enterprise Console e se l'ID di sottoscrizione corrisponde a quello utilizzato da AutoUpdate nel laptop.

   Il percorso di aggiornamento "migliore" viene scelto in base al numero di hop necessari per raggiungere il percorso di aggiornamento.
4. Viene quindi tentato un aggiornamento e, nel caso riesca, il percorso viene memorizzato nella cache.

   Nel computer laptop vengono memorizzati al massimo quattro percorsi di aggiornamento accessibili, aventi la medesima ID di sottoscrizione e il numero più basso di hop (nel file `iustatus.xml`, in questo percorso: `C:\Program Files\Sophos\AutoUpdate\data\status\iustatus.xml`).

   Questi percorsi di aggiornamento vengono verificati ogni volta che AutoUpdate esegue un aggiornamento.

 Copyright © Sophos Limited

Nota
Se si desidera tornare ad utilizzare i percorsi di aggiornamento primari e secondari indicati nel criterio di aggiornamento (per es. se si desidera distribuire personalizzazioni dal percorso di aggiornamento indicato nel criterio), sarà necessario disabilitare la ricerca automatica di un percorso.

Abilitazione della ricerca automatica di un percorso

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento** per confermare un criterio di aggiornamento.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Abilitare la ricerca automatica di un percorso solo per gruppi di computer che vengono spesso spostati da un ufficio all'altro.

Per abilitare la ricerca automatica di un percorso:

1. Nel riquadro **Criteri,** cliccare due volte su **Aggiornamento**. Quindi cliccare due volte sul criterio di aggiornamento che si desidera modificare.
2. Nella finestra di dialogo **Criterio di aggiornamento**, nella scheda **Server primario**, selezionare la casella di spunta **Consenti ricerca di un percorso**.
3. Nel riquadro **Gruppi**, selezionare un gruppo che utilizza i criteri di aggiornamento appena modificati. Cliccare con il tasto destro del mouse e selezionare **Allinea con**, **Criteri di aggiornamento di gruppo**.

   Ripetere questa procedura per ciascun gruppo a cui applicare questo criterio di aggiornamento.

Nota
Se in seguito sarà necessario tornare a utilizzare i percorsi di aggiornamento primari e secondari indicati nel criterio di aggiornamento, disabilitare la ricerca automatica di un percorso.

Modifica delle credenziali del server primario

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento** per confermare un criterio di aggiornamento.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Per modificare le credenziali del server primario:

1. Nel riquadro **Criteri,** cliccare due volte su **Aggiornamento**. Quindi cliccare due volte sul criterio di aggiornamento che si desidera modificare.
2. Nella finestra di dialogo **Criterio di aggiornamento**, nella scheda **Server primario**, inserire le nuovi credenziali che verranno usate per accedere al server. Modificare gli altri dettagli, se lo si desidera.

Copyright © Sophos Limited

Nota
Se la fonte primaria di aggiornamento è una cartella nel proprio sito web e si sta utilizzando Internet Information Services (IIS) con autenticazione anonima, sarà comunque necessario inserire le credenziali nella scheda **Server primario**. Utilizzare le credenziali della condivisione UNC per la "Fonte di installazione iniziale", anche se non sono necessarie per accedere al server web. Se, nella scheda **Server primario**, i campi **Nome utente** e **Password** vengono lasciati vuoti, non sarà possibile proteggere i computer endpoint dalla console.

3. Nel riquadro **Gruppi**, selezionare un gruppo che utilizza i criteri di aggiornamento appena modificati. Cliccare con il tasto destro del mouse e selezionare **Allinea con**, **Criteri di aggiornamento di gruppo**.

   Ripetere questa procedura per ciascun gruppo a cui applicare questo criterio di aggiornamento.

Impostazione del server di aggiornamento secondario

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento** per confermare un criterio di aggiornamento.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Per impostare il percorso secondario del server per gli aggiornamenti:

1. Controllare quale criterio di aggiornamento è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Aggiornamento**, e successivamente sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criterio di aggiornamento**, cliccare sulla scheda **Server secondario**, e spuntare la casella **Specifica dettagli del server secondario**.
4. Nella casella **Indirizzo (HTTP o UNC)**, svolgere una delle seguenti operazioni:
   - Inserire l'URL HTTP o il percorso UNC di rete della condivisione del server di aggiornamento.
   - Selezionare **Sophos**.

   Importante
   Se si opta per un URL HTTP o per una condivisione che non è mantenuta da un gestore degli aggiornamenti gestito, Enterprise Console non è in grado di controllare se la sottoscrizione al software specificata sia disponibile. È necessario assicurarsi manualmente che la condivisione contenga la sottoscrizione al software specificata, altrimenti i computer non verranno aggiornati.

5. Se il criterio comprende computer Mac e se nel campo **Indirizzo** si è specificato un percorso UNC, è necessario selezionare in **Seleziona un protocollo di condivisione file per Mac OS X** un protocollo con cui i Mac possano accedere alla condivisione di aggiornamento.
6. Se necessario, nel campo **Nome utente**, inserire il nome utente dell'account che sarà utilizzato per accedere al server, quindi inserire e confermare la password. Per gli HTTP Sophos, si intendono le credenziali di sottoscrizione.

   Questo account dovrebbe avere diritti di accesso di sola lettura (esplorazione) alla condivisione precedentemente inserita nel campo "indirizzo".

 Copyright © Sophos Limited

Nota
se il nome utente deve riportare il dominio, utilizzare la forma dominio\nome utente. Per informazioni su come verificare un account utente Windows, consultare l'articolo 11637 della knowledge base Sophos.

7. Per porre un limite alla larghezza di banda, cliccare su **Avanzate**. Nella finestra di dialogo **Impostazioni avanzate**, spuntare la casella **Limita occupazione di banda**, e utilizzare l'indicatore di scorrimento per specificare la larghezza di banda limite, in Kbit al secondo.
8. Se si accede alla fonte degli aggiornamenti tramite proxy, cliccare su **Proxy**. Nella finestra di dialogo **Dati proxy**, spuntare la casella **Accedi al server tramite proxy**, e successivamente inserire l'**Indirizzo** ed il numero di **Porta** del server proxy. 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.

   Nota
   Alcuni Internet Service Provider impongono che le richieste HTTP vengano inviate a un server proxy.

9. Cliccare su **OK** per chiudere la finestra di dialogo **Criterio di aggiornamento**.
10. Nel riquadro **Gruppi**, cliccare con il tasto destro del mouse su un gruppo che utilizza il criterio di aggiornamento appena modificato, e successivamente cliccare su **Allinea con > Criterio di aggiornamento del gruppo**.

    Ripetere questa procedura per ciascun gruppo a cui applicare questo criterio di aggiornamento.

6.3.3 Pianificazione degli aggiornamenti

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento** per confermare un criterio di aggiornamento.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Per impostazione predefinita, i computer verificano ogni 5 minuti la disponibilità di aggiornamenti nella condivisione di rete.

Nota
se i computer scaricano gli aggiornamenti direttamente da Sophos, l'intervallo di aggiornamento non viene applicato. I computer che eseguono Sophos PureMessage sono in grado di verificare la disponibilità degli aggiornamenti ogni 15 minuti. I computer che non eseguono Sophos PureMessage si aggiorneranno ogni 60 minuti.

Per specificare l'intervallo di aggiornamento:

1. Controllare quale criterio di aggiornamento è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri,** cliccare due volte su **Aggiornamento**. Quindi cliccare due volte sul criterio che si desidera modificare.

3. Nella finestra di dialogo **Criterio di aggiornamento**, scheda **Pianificato**, lasciare selezionata l'opzione **Consenti a computer in rete utilizzo automatico aggiornamenti Sophos**. Inserire l'intervallo fra gli aggiornamenti software (in minuti).
4. Se i computer eseguono l'aggiornamento tramite una connessione Internet via modem, selezionare **Verifica la disponibilità di aggiornamenti in fase di connessione**.
   In questo caso i computer tenteranno di eseguire l'aggiornamento non appena connessi a Internet.

6.3.4 Selezione di una fonte differente per l'installazione iniziale

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento** per confermare un criterio di aggiornamento.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Per impostazione predefinita, il software di sicurezza è installato nei computer e aggiornato dalla fonte indicata nella scheda **Server primario**. È possibile indicare una fonte differente per l'installazione iniziale.

Nota
impostazione valide solo per Windows.

Se il server primario è un indirizzo HTTP (ossia un indirizzo web), e si desidera eseguire l'installazione sui computer dalla console, è necessario specificare una fonte per l'installazione iniziale.

Per eseguire l'installazione iniziale da una fonte differente:

1. Controllare quale criterio di aggiornamento è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri,** cliccare due volte su **Aggiornamento**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criterio di aggiornamento**, nella scheda **Fonte dell'installazione iniziale**, deselezionare la casella di spunta **Utilizza indirizzo del server primario**. Inserire quindi l'indirizzo della fonte che si desidera utilizzare.

6.3.5 Log degli aggiornamenti

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - aggiornamento** per confermare un criterio di aggiornamento.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Per impostazione predefinita, i computer registrano le relative attività di aggiornamento. La dimensione massima di log predefinita è 1 MB. Il livello di log predefinito è normale.

Per modificare le impostazioni di log:

 Copyright © Sophos Limited

1. Controllare quale criterio di aggiornamento è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri,** cliccare due volte su **Aggiornamento**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criteri di aggiornamento**, nella scheda **Log**, lasciare selezionata l'opzione **Crea log dell'attività di Sophos AutoUpdate**. Nel campo **Dimensioni massime log**, indicare la dimensione massima del log in MB.
4. Nel campo **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 impostazione soltanto se il log dettagliato è necessario per la risoluzione di eventuali problemi.

6.4 Monitoraggio del gestore aggiornamenti

Verifica dello stato del gestore aggiornamenti nel pannello di controllo

Lo stato dei gestori aggiornamenti viene visualizzato nel pannello **Aggiornamenti** del **Pannello di controllo**. Viene indicato quando sia avvenuto il download dell'ultimo aggiornamento da Sophos e visualizzato un avviso nel caso in cui la data dell'ultimo aggiornamento superi il livello di allarme o critico.

Nota
la sezione **Aggiornamenti** del pannello di controllo non rileva alcun allarme o errore se il gestore aggiornamenti non riesce ad aggiornarsi. Gli allarmi ed errori vengono generati se il tempo trascorso dall'ultimo aggiornamento del gestore aggiornamenti supera il livello di avviso o critico impostato in Configurazione del pannello di controllo (pagina 48).

Verifica degli allarmi ed errori del gestore aggiornamenti

Allarmi ed errori relativi al gestore aggiornamenti vengono visualizzati nella vista **Gestori aggiornamenti**, rispettivamente nelle colonne **Allarmi** ed **Errori**.

Se si è eseguita la sottoscrizione a una versione fissa di un software, quando tale versione sarà vicina al ritiro o verrà ritirata si visualizzerà un allarme. Anche nel caso di modifiche apportate alla licenza del prodotto verrà visualizzato un allarme.

Per visionare allarmi ed errori del gestore aggiornamenti:

1. Se si è nella vista **Computer**, per poter accedere alla vista **Gestori aggiornamenti**, cliccare sul pulsante **Gestori aggiornamenti** che si trova nella barra degli strumenti,.
2. Nell'elenco relativo ai gestori aggiornamenti, sotto **Allarmi** ed **Errori** verranno visualizzati eventuali problemi.
3. Se di fianco a un gestore aggiornamenti viene visualizzato un allarme o un errore, cliccare col tasto destro del mouse su tale gestore, quindi su **Visualizza dettagli di Update Manager**.

   Nella finestra di dialogo **Dettagli sul gestore aggiornamenti**, è possibile visualizzare l'orario degli ultimi dati relativi al rilevamento delle minacce e all'aggiornamento del software, lo stato della sottoscrizione o sottoscrizioni che il gestore mantiene aggiornate e lo stato del gestore aggiornamenti.

4. Per maggiori informazioni sullo stato di un determinato gestore aggiornamenti e su come intervenire, seguire il link nella colonna **Descrizione computer**.

Per controllare o modificare la propria sottoscrizione, per esempio nel caso in cui il prodotto che si è sottoscritto sia vicino al ritiro o la licenza sia stata modificata e non includa più quel determinato prodotto, consultare la sezione Sottoscrizione al software di sicurezza (pagina 66).

Se con la modifica della licenza vengono messe a disposizione nuove funzioni, prima di poterle eseguire potrebbe essere necessario configurare nuovi criteri.

Sottoscrizione agli allarmi e-mail

È possibile impostare l'invio di allarmi e-mail a destinatari prescelti quando la versione del prodotto a cui si è sottoscritti sia vicina al ritiro o sia stata ritirata; oppure in caso di modifica delle funzioni del prodotto Sophos in esecuzione dovuta a cambiamenti apportati alla relativa licenza. Per ulteriori informazioni, consultare la sezione Impostazione degli allarmi relativi alle sottoscrizioni software (pagina 186).

6.4.1 Cancellazione degli allarmi del gestore aggiornamenti dalla console

Se si utilizza l'amministrazione basata sui ruoli, è necessario essere in possesso dei diritti di **Correzione - disinfezione** per cancellare allarmi dalla console. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Per cancellare gli allarmi del gestore aggiornamenti dalla console:

1. Nella vista **Update manager**, selezionare il/i gestori aggiornamenti per cui cancellare gli allarmi. Cliccarvi col tasto destro del mouse e selezionare **Cancella allarmi**.
   Viene visualizzata la finestra di dialogo **Allarmi di Update Manager** .
2. Per cancellare gli allarmi dalla console, selezionare gli allarmi che si desidera cancellare e cliccare su **Cancella**.
   Gli allarmi già esaminati (cancellati) non sono più visualizzati nella console.

6.5 Aggiornamento dei computer non aggiornati

Se si utilizza l'amministrazione basata sui ruoli, per aggiornare i computer, è necessario essere in possesso dei diritti di **Correzione - aggiornamento e scansione**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Dopo avere impostato i criteri di aggiornamento ed averli applicati ai computer nella rete, tali computer verranno aggiornati automaticamente. Non è necessario aggiornare i computer manualmente, a meno che non si sia verificato un problema relativo agli aggiornamenti.

Se nella vista **Computer**, all'interno dell'elenco dei computer, di fianco a un computer viene visualizzata un'icona a forma di orologio, sotto la colonna **Aggiornato** della scheda **Stato**, tale computer è in possesso di un software di sicurezza non aggiornato. Il testo indica da quanto tempo il computer non è stato aggiornato.

Un computer può non essere aggiornato per una delle due seguenti ragioni:

- Il computer non è riuscito a prelevare un aggiornamento dal server.
- Il server stesso non contiene il software Sophos più recente.

Per diagnosticare un problema e aggiornare i computer:

 Copyright © Sophos Limited

1. Nella vista **Computer**, selezionare il gruppo contenente computer non aggiornati.
2. Nella scheda **Stato**, cliccare sull'intestazione della colonna **Aggiornato** per ordinare i computer in base al relativo livello di aggiornamento.
3. Cliccare sulla scheda **Dati aggiornamento** e controllare la colonna **Server primario**. Questa mostra la directory dalla quale ogni computer esegue l'aggiornamento.
4. Ora controllare i computer che eseguono l'aggiornamento da una directory specifica.
   - *Se alcuni computer risultano non aggiornati, mentre altri lo sono*, il problema riguarda i singoli computer. Selezionarli, cliccarvi sopra con il tasto destro del mouse e selezionare **Aggiorna computer**.
   - *Se tutti i computer risultano non aggiornati*, il problema potrebbe riguardare la directory. Dal menu **Visualizza**, cliccare su **Update Manager**. Selezionare il gestore aggiornamenti che mantiene la directory che si sospetta non essere aggiornata, cliccarvi col tasto destro del mouse e poi cliccare su **Aggiorna ora**. Successivamente, dal menu **Visualizza**, cliccare su **Computer**. Selezionare i computer non aggiornati, cliccarvi col tasto destro del mouse e poi cliccare su **Aggiorna computer**.

Se in possesso di diversi gestori degli aggiornamenti e non certi di quale di questi mantenga la directory non aggiornata, utilizzare il report Gerarchia aggiornamenti per poter visualizzare quali condivisioni siano mantenute da ciascun gestore aggiornamenti. Per visualizzare il report Gerarchia aggiornamenti, nel menu **Strumenti**, cliccare su **Gestisci report**. Nella finestra di dialogo **Report Manager**, selezionare **Gerarchia aggiornamenti** e cliccare su **Esegui**. Selezionare la sezione del report "Condivisioni gestite dai gestori degli aggiornamenti".

7 Configurazione dei criteri

7.1 Criterio antivirus e HIPS

Un criterio antivirus e HIPS consente di:

- Rilevare automaticamente virus, trojan, worm e spyware, noti e sconosciuti, non appena l'utente tenta l'accesso ai file che li contengono.
- Ricercare adware e altre applicazioni potenzialmente indesiderate.
- Cercare file sospetti e rootkit nei computer.
- Rilevare il traffico di rete malevolo, ovvero le comunicazioni tra computer endpoint e server di comando e controllo coinvolti in attacchi sferrati tramite botnet o altri tipi di malware.
- Disinfettare automaticamente i computer non appena venga rilevato un virus o altra minaccia.

  Per informazioni su come cambiare le impostazioni per la disinfezione automatica, consultare la sezione Impostazione della disinfezione automatica per la scansione in accesso (pagina 85).
- Analizzare il comportamento del programma in esecuzione nel sistema.

  Per ulteriori informazioni, consultare la sezione Monitoraggio del comportamento (pagina 95).
- Eseguire la scansione dei computer a orari prestabiliti.

  Per ulteriori informazioni, consultare la sezione Creazione di una scansione pianificata (pagina 89).

Utilizzare impostazioni differenti per la scansione di ogni gruppo di computer. Per informazioni dettagliate sulla configurazione delle impostazioni di scansione, consultare i seguenti argomenti:

- Configurazione della scansione in accesso (pagina 82)
- Configurazione delle impostazioni di scansione per la scansione pianificata (pagina 90)

Nota
I Sophos Labs sono in grado di controllare in maniera indipendente i file che vengono sottoposti a scansione. Potrebbero aggiungere o rimuovere la scansione di tipi di file specifici, al fine di garantire i massimi livelli di protezione.

Per informazioni sulle opzioni di scansione e disinfezione che non riguardano i computer Mac, Linux o UNIX, consultare la sezione Impostazioni non valide per computer Mac, Linux o UNIX (pagina 81).

Per informazioni sulle opzioni di scansione e rimozione che non sono applicabili a Sophos Anti-Virus per VMware vShield, consultare l'articolo 121745 della knowledge base Sophos. Per Sophos Anti-Virus per VMware vShield, versione 2.x, vedere anche la Guida alla configurazione di Sophos Anti-Virus per VMware vShield, disponibile su questo link: www.sophos.com/it-it/support/documentation/sophos-anti-virus-for-vmware-vshield.

Copyright © Sophos Limited

7.1.1 Impostazioni non valide per computer Mac, Linux o UNIX

Se tutti i tipi di scansione e disinfezione nei computer Windows possono essere interamente gestiti da Enterprise Console, esistono, al contrario, impostazioni non utilizzabili nei computer Mac, Linux o UNIX.

Mac OS X

Per informazioni sulle impostazioni dei criteri antivirus e HIPS applicabili ai computer MAC, consultare l'articolo 118859 della knowledge base Sophos.

Linux

Le seguenti opzioni opzioni di disinfezione automatica non sono applicabili ai computer Linux che le ignoreranno.

Opzioni della disinfezione automatica per la scansione in accesso:

- **Nega l'accesso e sposta in percorso predefinito**
- **Nega l'accesso e sposta in**

Impostazioni della disinfezione automatica per la scansione pianificata:

- **Sposta in percorso predefinito**
- **Sposta in**

Per ulteriori informazione sull'esportazione di dispositivi, vedere Impostazione della rimozione automatica per la scansione pianificata (pagina 92) e Impostazioni della disinfezione automatica per la scansione predefinita (pagina 92).

Per ulteriori informazioni sulle impostazioni dei criteri antivirus e HIPS applicabili ai computer Linux, consultare l'articolo 117344 della knowledge base Sophos.

UNIX

- Enterprise Console non può eseguire la scansione in accesso nei computer UNIX.

  È possibile configurare scansioni pianificate, allarmi, log e aggiornamenti centralmente da Enterprise Console.

  Nota
  queste funzioni comprendono anche alcuni parametri che non possono essere impostati tramite Enterprise Console. Per impostarli localmente utilizzare l'interfaccia della riga di comando di Sophos Anti-Virus in ciascun computer UNIX. Enterprise Console li ignora.

  È possibile configurare la scansione su richiesta localmente, dall'interfaccia della riga di comando di Sophos Anti-Virus in ciascun computer UNIX.

  Per informazioni su come impostare parametri aggiuntivi o configurare Sophos Anti-Virus per UNIX localmente, consultare la *Guida alla configurazione di Sophos Anti-Virus per UNIX*.

- Le seguenti opzioni opzioni di disinfezione automatica non sono applicabili ai computer UNIX che le ignoreranno.

— **Sposta in percorso predefinito**

— **Sposta in**

Per ulteriori informazioni sulle opzioni di disinfezione automatica per la scansione pianificata, consultare la sezione Impostazioni della disinfezione automatica per la scansione predefinita (pagina 92).

Per ulteriori informazioni sulle impostazioni dei criteri antivirus e HIPS applicabili ai computer UNIX, consultare l'articolo 117344 della knowledge base Sophos.

7.1.2 Scansione in accesso

Migliore protezione con la scansione in accesso

Questa sezione offre consigli per poter utilizzare la scansione in accesso al meglio.

Si consiglia l'utilizzo delle impostazioni predefinite per la scansione in accesso, per ottenere il giusto equilibrio fra la protezione dei computer dalle minacce e la resa del sistema. Per informazioni sulle impostazioni consigliate per la scansione in accesso, consultare l'articolo 114345 della knowledge base del supporto Sophos (http://www.sophos.com/it-it/support/knowledgebase/114345.aspx).

Si consiglia di consultare la *Guida all'impostazione dei criteri di* Sophos Enterprise Console per informazioni sulle migliori pratiche per l'utilizzo e la gestione del software di sicurezza Sophos. La documentazione di Sophos è pubblicata alla pagina web http://www.sophos.com/it-it/support/documentation.

Configurazione della scansione in accesso

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Attenzione
La scansione in accesso potrebbe non rilevare i virus, se sono installati determinati software di cifratura. Modificare i processi di avvio per assicurarsi che i file vengano decifrati quando inizia la scansione in accesso. Per ulteriori informazioni su come utilizzare criteri antivirus e HIPS con software di cifratura, consultare l'articolo 12790 della knowledge base del supporto Sophos.

Per configurare la scansione in accesso:

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Nel pannello **Scansione in accesso**, di fianco a **Abilita scansione in accesso**, cliccare su **Configura**.

 Copyright © Sophos Limited

5. Per apportare modifiche alla tempistica in cui viene eseguita la scansione in accesso, in **Verifica file in**, impostare le opzioni secondo quanto descritto qui di seguito.

Opzione	Descrizione
Lettura	• Scansione dei file quando copiati, spostati o aperti. • Scansione dei programmi quando riavviati.
Rinomina	Scansione dei file quando rinominati.
Scrittura	Scansione dei file quando salvati o creati.

6. In **Esegui scansione alla ricerca di**, impostare le opzioni come descritto di seguito.

Opzione	Descrizione
Adware e PUA	• L'adware visualizza messaggi pubblicitari, quali messaggi pop up, che possono incidere sulla produttività degli utenti e sull'efficienza del sistema. • I PUA (Potentially Unwanted Applications) non sono malevoli, ma inappropriati per reti aziendali e ambienti lavorativi.
File sospetti	I file sospetti presentano determinate caratteristiche comuni, ma non esclusive, del malware (per es. il codice di decompressione dinamica). Queste caratteristiche non sono però così rilevanti da poter identificare il file come nuovo malware. **Nota** questa opzione è valida soltanto per Sophos Endpoint Security and Control per Windows.

7. In **Altre opzioni di scansione**, impostare le opzioni come descritto di seguito.

Opzione	Descrizione
Accesso alle unità con settori di avvio infetti	Consentire l'accesso a uno mezzo o dispositivo rimovibile infetto, quale CD di avvio, floppy disk o unità flash USB. Utilizzate questa opzione soltanto su consiglio del supporto tecnico di Sophos.
Scansione dei file di archivio	Eseguire la scansione del contenuto dei file di archivio o compressi prima che vengano scaricati o inviati per e-mail dai computer gestiti.

Opzione	Descrizione
	Si consiglia di lasciare questa opzione **disabilitata**, dal momento che rallenta notevolmente la scansione. Gli utenti saranno comunque protetti da eventuali minacce presenti nei file di archivio o compressi, dal momento che tutti i componenti dei file di archivio o compressi che potrebbero contenere malware verranno bloccati dalla scansione in accesso: • Quando si apre un file estratto dal file di archivio, tale file viene sottoposto a scansione. • I file compressi tramite utilità di compressione dinamiche, quali PKLite, LZEXE e Diet, vengono sottoposti a scansione.
Scansione della memoria di sistema	Eseguire una scansione di background a cadenza oraria per rilevare malware nascosti nella memoria di sistema del computer (la memoria utilizzata dal sistema operativo).

Attivazione e disattivazione della scansione in accesso

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per impostazione predefinita, Sophos Endpoint Security and Control esamina i file non appena l'utente tenta di accedervi, negando l'accesso a meno che i file non siano puliti.

Se si decide di disattivare la scansione in accesso sui server Exchange o su altri server, perché si teme che la scansione possa influire sulle prestazioni, Inserire i server in un gruppo speciale e modificare i criteri antivirus e HIPS utilizzati per quel gruppo, come illustrato di seguito.

Per attivare e disattivare la scansione in accesso:

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**. Quindi cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criteri antivirus e HIPS**.
3. Nel pannello **Scansione in accesso**, selezionare o deselezionare la casella di spunta **Abilita scansione in accesso**.

Copyright © Sophos Limited

Importante
Se si disattiva la scansione in accesso su un server, si consiglia di impostare le scansioni pianificate nei relativi computer. Per istruzioni sull'impostazione delle scansioni pianificate, consultare la sezione Creazione di una scansione pianificata (pagina 89).

Impostazione della disinfezione automatica per la scansione in accesso

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per impostazione predefinita Sophos Endpoint Security and Control disinfetta automaticamente i computer non appena venga rilevato un virus o altra minaccia. È possibile modificare le impostazioni per la disinfezione automatica secondo quanto descritto qui di seguito.

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Nel pannello **Scansione in accesso**, di fianco a **Abilita scansione in accesso**, cliccare su **Configura**.
5. Nella finestra di dialogo **Impostazioni della scansione in accesso**, cliccare sulla scheda **Disinfezione**.
6. Impostare le opzioni secondo quanto descritto nella sezione Impostazioni della disinfezione automatica per la scansione in accesso (pagina 85).

Impostazioni della disinfezione automatica per la scansione in accesso

Virus/spyware

Selezionare o deselezionare la casella di spunta **Disinfetta automaticamente gli oggetti contenenti virus/spyware**.

È inoltre possibile specificare come trattare gli oggetti se la disinfezione non riesce:

- **Nega solo l'accesso**
- **Elimina**
- **Nega l'accesso e sposta in percorso predefinito**
- **Nega l'accesso e sposta in (inserire percorso UNC completo)**

Nota
Le impostazioni **Nega l'accesso e sposta in posizione predefinita** e **Nega l'accesso e sposta in** non sono applicabili ai computer Linux o UNIX che le ignoreranno.

File sospetti

Nota
impostazioni valide solo per Windows.

È possibile specificare l'azione da eseguire sui file sospetti rilevati:

- **Nega solo l'accesso**
- **Elimina**
- **Nega l'accesso e sposta in percorso predefinito**
- **Nega l'accesso e sposta in (inserire percorso UNC completo)**

Specificazione delle estensioni dei file per la scansione in accesso

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

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

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.
   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Nel pannello **Scansione in accesso**, di fianco a **Abilita scansione in accesso**, cliccare su **Configura**.
5. Cliccare sulla scheda **Estensioni** e configurare le opzioni secondo quanto descritto di seguito.

Opzione	Descrizione
Scansione di tutti i file	Eseguire la scansione di tutti i file, indipendentemente dal nome del file. Se si attiva questa opzione, le altre opzioni presenti nella scheda **Estensioni** verranno disattivate. La scansione di tutti i file limita le prestazioni del computer, si consiglia quindi di attivare questa opzione solo per la scansione pianificata settimanale.
Scansiona solo eseguibili e altri tipi di file vulnerabili	• Esegue la scansione di tutte le estensioni di file eseguibili (per es. .exe, .bat, .pif) o di tutti i file potenzialmente infetti (per es. .doc, .chm, .pdf).

Copyright © Sophos Limited

Opzione	Descrizione
	• Verificare rapidamente la struttura di tutti i file, quindi sottoporre a scansione quelli in formato eseguibile.
Estensioni di tipi file aggiuntive da sottoporre a scansione	Per esaminare tipi aggiuntivi di file, cliccare su **Aggiungi**, quindi digitare l'estensione del file, per esempio PDF, nella finestra **Estensione**. È possibile utilizzare il carattere jolly "?" al posto di un singolo carattere. Per non sottoporre a scansione un determinato tipo di file, selezionare la relativa estensione dall'elenco, quindi cliccare su **Rimuovi**. Per modificare un determinato tipo di file, selezionare la relativa estensione dall'elenco, quindi cliccare su **Modifica**.
Scansione dei file senza estensione	I file privi di estensione potrebbero essere malware, si consiglia quindi di lasciare sempre attiva questa opzione.
Escludi	Per escludere determinati tipi di file dalla scansione in accesso, cliccare su **Aggiungi**, quindi digitare l'estensione del file, per esempio PDF, nella finestra **Estensione**. Per sottoporre a scansione un determinato tipo di file, selezionare la relativa estensione dall'elenco, quindi cliccare su **Rimuovi**. Per modificare un determinato tipo di file, selezionare la relativa estensione dall'elenco, quindi cliccare su **Rinomina**.

Esclusione di oggetti dalla scansione in accesso

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile escludere oggetti dalla scansione in accesso.

Nota
Queste opzioni sono valide soltanto per Windows, Mac OS X e Linux.

Enterprise Console non può eseguire la scansione in accesso nei computer UNIX.

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

Vedere Criteri utilizzati da un dato gruppo (pagina 25).

2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**. Quindi cliccare due volte sul criterio che si desidera modificare.

   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.

3. Nel riquadro **Scansione in accesso**, cliccare sul pulsante **Configura**.
4. Cliccare sulla scheda **Esclusioni Windows**, **Esclusioni Mac** o **Esclusioni Linux/Unix**. Per aggiungere oggetti all'elenco, cliccare su **Aggiungi** e inserire il percorso completo nella finestra di dialogo **Escludi oggetto**.

   Gli oggetti che è possibile escludere dalla scansione variano a seconda del tipo di computer. Vedere Oggetti che possono essere esclusi dalla scansione (pagina 105).

   Per escludere i file non archiviati in unità locali, selezionare la casella di spunta **Escludi file remoti**. Selezionare questa opzione se si desidera aumentare la velocità di accesso a questi file e si ritiene affidabile il loro percorso remoto.

Importante
Se nella scheda **Esclusioni Windows** si seleziona la casella **Escludi file remoti**, il controllo dati non eseguirà la scansione dei file scaricati o allegati da un percorso di rete utilizzando un'applicazione monitorata; per esempio, un client e-mail, un browser web o un client di messaggistica istantanea (IM). Ciò avviene perché il controllo dati utilizza le stesse esclusioni applicate alla scansione in accesso di Sophos Anti-Virus (InterCheck ™). Se la scansione dei file remoti è disabilitata, nessuno di tali file sarà sottoposto a verifica del controllo dati. Questa limitazione non si applica al monitoraggio dei dispositivi di memorizzazione.

È possibile importare l'elenco di esclusioni Windows in un file per poi importarlo in un altro criterio. Per ulteriori informazioni, consultare la sezione Importazione o esportazione delle esclusioni di scansione (pagina 88).

Importazione o esportazione delle esclusioni di scansione

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile importare l'elenco di esclusioni Windows per la scansione in entrata in un file e quindi importarlo in un altro criterio.

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).

2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Nel pannello **Scansione in accesso**, di fianco a **Abilita scansione in accesso**, cliccare su **Configura**.
5. Nella scheda **Esclusioni Windows**, cliccare su **Esporta** o **Importa**.

Copyright © Sophos Limited

7.1.3 Scansione su richiesta e pianificata

Nel riquadro **Scansione pianificata** del criterio **Antivirus e HIPS**, è possibile:

- Impostare scansioni pianificate.
- Configurare opzioni di scansione quali estensioni ed esclusioni per tutti i tipi di scansione su richiesta — scansioni pianificate, scansione completa del sistema, e scansioni su richiesta predefinite sui singoli computer.

Creazione di una scansione pianificata

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Creando scansioni pianificate sarà possibile eseguire la scansione dei computer tramite Sophos Endpoint Security and Control a orari predefiniti.

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Nel riquadro **Scansione su richiesta**, sotto **Impostare e gestire scansioni pianificate**, cliccare su **Aggiungi**.
   Viene visualizzata la finestra di dialogo **Impostazioni scansione pianificata**.
5. Nel campo di testo **Nome scansione**, digitare un nome per la scansione.
6. Sotto **Cosa scansionare**, selezionare la casella di spunta relativa agli oggetti che si desidera sottoporre a scansione. Per impostazione predefinita, viene eseguita la scansione di tutti i dischi rigidi e i file system UNIX montati.
7. Sotto **Cosa scansionare**, selezionare la casella di spunta relativa ai giorni in cui eseguire la scansione.
8. Per indicare gli orari in cui eseguire la scansione, cliccare su **Aggiungi**.
   - Per modificare un orario, dall'elenco **Orari in cui sarà eseguita la scansione** selezionare un orario e cliccare su **Modifica**.
   - Per cancellare un orario, dall'elenco **Orari in cui sarà eseguita la scansione** selezionare un orario e cliccare su **Rimouvi**.

Nota
Se la scansione rileva componenti di una minaccia nella memoria, e non si è impostata la disinfezione automatica, la scansione si arresta e viene inviato un allarme a Enterprise Console. Ciò avviene poiché procedere con la scansione potrebbe consentire la diffusione di questa minaccia. Occorre effettuare la disinfezione della minaccia, prima di poter eseguire nuovamente la scansione.

Per modificare le opzioni di scansione e disinfezione, consultare i seguenti argomenti:

- Configurazione delle impostazioni di scansione per la scansione pianificata (pagina 90)
- Impostazione della disinfezione automatica per la scansione in accesso (pagina 85)

Configurazione delle impostazioni di scansione per la scansione pianificata

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per configurare le impostazioni di scansione per la scansione pianificata:

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Nell'elenco **Impostare e gestire scansioni pianificate**, selezionare la scansione, quindi cliccare su **Modifica**.
5. Nella finestra di dialogo **Impostazioni scansione pianificat**a, cliccare su **Configura**.
6. In **Scansione dei file alla ricerca di**, configurare le impostazioni come descritto di seguito.

Opzione	Descrizione
Adware e PUA	• L'adware visualizza messaggi pubblicitari, quali messaggi pop up, che possono incidere sulla produttività degli utenti e sull'efficienza del sistema. • I PUA (Potentially Unwanted Applications) non sono malevoli, ma inappropriati per reti aziendali e ambienti lavorativi.
File sospetti	I file sospetti presentano determinate caratteristiche comuni, ma non esclusive, del malware (per es. il codice di decompressione dinamica). Queste caratteristiche non sono però così rilevanti da poter identificare il file come nuovo malware. **Nota** Questa impostazione è valida soltanto per Sophos Endpoint Security and Control per Windows.
Rootkit	Un rootkit è un trojan o tecnologia utilizzata per nascondere la presenza di un oggetto malevolo (processo, file, chiave di registro

Copyright © Sophos Limited

Opzione	Descrizione
	o porta di rete) all'utente del computer o all'amministratore.

7. In **Altre opzioni di scansione**, impostare le opzioni come descritto di seguito.

Opzione	Descrizione
Scansione dei file di archivio	Eseguire la scansione del contenuto di archivi e altri file compressi. Si sconsiglia l'esecuzione della scansione dei file contenuti negli archivi durante la scansione pianificata, perché ciò allungherebbe notevolmente i tempi di esecuzione. Si consiglia invece l'utilizzo della scansione in accesso (in lettura e scrittura) per garantire la protezione della rete. Qualsiasi componente del malware presente in un archivio non compresso verrà bloccato dalla scansione in lettura e scrittura una volta vi si acceda. Se si desidera eseguire la scansione completa di tutti gli archivi per un numero limitato di computer tramite scansione pianificata, si consiglia di: • Creare una scansione pianificata aggiuntiva. • Nella casella di dialogo **Configura > Impostazioni della scansione in accesso**, sotto la scheda **Estensioni**, aggiungere solamente le estensioni per i file di archivio all'elenco di estensioni da sottoporre a scansione. • Accertarsi che l'opzione **Scansiona tutti i file** sia disabilitata. Ciò consentirà di eseguire la scansione dei file di archivio limitandone il più possibile la durata.
Scansione della memoria di sistema	Rilevare il malware nascosto nella memoria di sistema del computer (la memoria utilizzata dal sistema operativo).
Esegui scansione a priorità più bassa	In Windows Vista e superiore, eseguire la scansione pianificata con priorità più bassa in modo tale da avere un impatto minimo sulle applicazioni per gli utenti.

Per consigli dettagliati su come regolare le impostazioni di scansione predefinite per una scansione pianificata, consultare l'articolo 63985 della knowledge base Sophos.

Impostazione della rimozione automatica per la scansione pianificata

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per impostazione predefinita Sophos Endpoint Security and Control disinfetta automaticamente i computer non appena venga rilevato un virus o altra minaccia. È possibile modificare le impostazioni per la disinfezione automatica secondo quanto descritto qui di seguito.

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Nell'elenco **Impostare e gestire scansioni pianificate**, selezionare la scansione, quindi cliccare su **Modifica**.
5. Di fianco a **Modifica impostazioni di scansione e disinfezione**, cliccare su **Configura**.
   Viene visualizzata la finestra di dialogo **Impostazioni di scansione e disinfezione**.
6. Cliccare sulla scheda **Disinfezione**.
7. Impostare le opzioni secondo quanto descritto nella sezione Impostazioni della disinfezione automatica per la scansione in accesso (pagina 85).

Impostazioni della disinfezione automatica per la scansione predefinita

Virus/spyware

Selezionare o deselezionare la casella di spunta **Disinfetta automaticamente gli oggetti contenenti virus/spyware**.

È inoltre possibile specificare come trattare gli oggetti se la disinfezione non riesce:

- **Registra solo**
- **Elimina**
- **Sposta in percorso predefinito**
- **Sposta in (inserire percorso UNC completo)**

Note

- Spostando un file eseguibile si riducono le probabilità che venga eseguito.
- Non è possibile spostare automaticamente i componenti di un'infezione multicomponente.

Adware e PUA

Selezionare **Disinfetta automaticamente adware e PUA**.

Nota

Copyright © Sophos Limited

- impostazione valide solo per Windows.

File sospetti

È possibile specificare l'azione da eseguire sui file sospetti rilevati:

- **Registra solo**
- **Elimina**
- **Sposta in percorso predefinito**
- **Sposta in (inserire percorso UNC completo)**

Note

- impostazioni valide solo per Windows.
- Spostando un file eseguibile si riducono le probabilità che venga eseguito.
- Non è possibile spostare automaticamente i componenti di un'infezione multicomponente.

Specificazione delle estensioni dei file per la scansione su richiesta e pianificata

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile specificare le estensioni dei file da sottoporre a scansione durante le scansioni su richiesta e pianificate.

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Nel riquadro **Scansione su richiesta**, cliccare su **Configura**.
   Viene visualizzata la finestra di dialogo **Impostazioni della scansione su richiesta**.
5. Nella scheda **Estensioni**, configurare le opzioni secondo quanto descritto qui sotto.

Opzione	Descrizione
Scansione di tutti i file	Eseguire la scansione di tutti i file, indipendentemente dal nome del file. Se si attiva questa opzione, le altre opzioni presenti nella scheda **Estensioni** verranno disattivate. La scansione di tutti i file limita le prestazioni del computer, si consiglia quindi di attivare questa opzione solo per la scansione pianificata settimanale.

Opzione	Descrizione
Scansiona solo eseguibili e altri tipi di file vulnerabili	• Esegue la scansione di tutte le estensioni di file eseguibili (per es. .exe, .bat, .pif) o di tutti i file potenzialmente infetti (per es. .doc, .chm, .pdf). • Verificare rapidamente la struttura di tutti i file, quindi sottoporre a scansione quelli in formato eseguibile.
Estensioni di tipi file aggiuntive da sottoporre a scansione	Per esaminare tipi aggiuntivi di file, cliccare su **Aggiungi**, quindi digitare l'estensione del file, per esempio PDF, nella finestra **Estensione**. È possibile utilizzare il carattere jolly "?" al posto di un singolo carattere. Per non sottoporre a scansione un determinato tipo di file, selezionare la relativa estensione dall'elenco, quindi cliccare su **Rimuovi**. Per modificare un determinato tipo di file, selezionare la relativa estensione dall'elenco, quindi cliccare su **Modifica**.
Scansione dei file senza estensione	I file privi di estensione potrebbero essere malware, si consiglia quindi di lasciare sempre attiva questa opzione.
Escludi	Per escludere determinati tipi di file dalla scansione pianificata, cliccare su **Aggiungi**, quindi digitare l'estensione del file, per esempio PDF, nella finestra **Estensione**. Per sottoporre a scansione un determinato tipo di file, selezionare la relativa estensione dall'elenco, quindi cliccare su **Rimuovi**. Per modificare un determinato tipo di file, selezionare la relativa estensione dall'elenco, quindi cliccare su **Rinomina**.

Per consigli dettagliati sulla configurazione delle impostazioni relative alle estensioni per la scansione pianificata, consultare l'articolo 63985 della knowledge base Sophos .

Esclusione di oggetti dalla scansione su richiesta e pianificata

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile escludere oggetti dalle scansioni su richiesta e pianificate.

 Copyright © Sophos Limited

Nota
Oltre che per le scansioni pianificate, l'impostazione "oggetti esclusi" è valida anche per le scansioni complete del sistema eseguite tramite la console e per le "scansioni del computer" eseguite sui computer collegati in rete. Vedere Scansione immediata dei computer (pagina 53).

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**. Nel riquadro **Scansione su richiesta**, cliccare su **Configura**.
4. Cliccare sulla scheda **Esclusioni Windows**, **Esclusioni Linux/Unix** o **Esclusioni Mac**. Per aggiungere oggetti all'elenco, cliccare su **Aggiungi** e inserire il percorso completo nella finestra di dialogo **Escludi oggetto**.

   Gli oggetti che è possibile escludere dalla scansione variano a seconda del tipo di computer. Vedere Oggetti che possono essere esclusi dalla scansione (pagina 105).

È possibile importare l'elenco di esclusioni Windows in un file per poi importarlo in un altro criterio. Per ulteriori informazioni, consultare la sezione Importazione o esportazione delle esclusioni di scansione (pagina 88).

Importazione o esportazione delle esclusioni Windows per la scansione su richiesta e pianificata

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile esportare l'elenco di esclusioni Windows per la scansione su richiesta e pianificata in un file, per poi importarlo in un altro criterio.

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Nel riquadro **Scansione su richiesta**, cliccare su **Configura**.
5. Nella scheda **Esclusioni Windows**, cliccare su **Esporta** o **Importa**.

7.1.4 Monitoraggio del comportamento

In quanto parte della scansione in accesso, Sophos Behavior Monitoring protegge i computer con sistema operativo Windows dalle minacce non identificate o del giorno zero, oltre che da comportamento sospetto.

Il rilevamento in fase di esecuzione può rilevare minacce che non possono essere identificate prima dell'esecuzione. Il monitoraggio del comportamento utilizza i seguenti metodi di rilevamento in fase di esecuzione per identificare eventuali minacce:

- Rilevamento di comportamento malevolo e sospetto
- Rilevamento del traffico malevolo
- Rilevamento di buffer overflow

Rilevamento di comportamento malevolo e sospetto

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 controlla tutti i processi di sistema alla ricerca di segni che indichino la presenza di malware attivo, quali scritture sospette nel registro o azioni di copiatura file. Può essere impostato in modo tale da avvertire l'amministratore e/o bloccare il processo.

Il rilevamento di comportamento malevolo coincide con l'analisi dinamica di tutti i programmi in esecuzione nel computer e ha lo scopo di rilevare e bloccare attività apparentemente malevoli.

Rilevamento del traffico malevolo

Il rilevamento del traffico malevolo consente di rilevare le comunicazioni tra computer endpoint e server di comando e controllo coinvolti in attacchi sferrati tramite botnet o altri tipi di malware.

Nota
Per il rilevamento del traffico malevolo occorre abilitare Sophos Live Protection, che consente di effettuare le ricerche e ottenere i dati. (Sophos Live Protection è abilitata per impostazione predefinita).

Rilevamento di buffer overflow

Il rilevamento di buffer overflow è fondamentale nel trattamento delle minacce del giorno zero.

Analizza dinamicamente il comportamento dei programmi in esecuzione nel sistema per poter rilevare eventuali tentativi di sfruttare un processo in esecuzione tramite tecniche di buffer overflow. Intercetta attacchi che puntano a vulnerabilità della sicurezza nei software e applicazioni del sistema operativo.

Attivazione e disattivazione del monitoraggio del comportamento

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Il monitoraggio del comportamento è abilittato per impostazione predefinita.

 Copyright © Sophos Limited

Per attivare o disattivare il monitoraggio del comportamento:

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Nel pannello **Scansione in accesso**, selezionare o deselezionare la casella di spunta **Abilita il monitoraggio del comportamento**.

Rilevamento di comportamento malevolo

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Il rilevamento di comportamento malevolo coincide con l'analisi dinamica di tutti i programmi in esecuzione nel computer e ha lo scopo di rilevare e bloccare attività apparentemente malevoli.

Il rilevamento del comportamento malevolo è abilitato per impostazione predefinita.

Per modificare le impostazioni di rilevamento e reportistica relative a comportamento malevolo:

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Nel pannello **Scansione in accesso**, verificare che la casella di spunta **Abilita il monitoraggio del comportamento** sia selezionata.
5. Di fianco a **Abilita il monitoraggio del comportamento**, cliccare su **Configura**.
6. Nella finestra di dialogo **Configura monitoraggio del comportamento**:
   - Per allertare l'amministratore e bloccare gli episodi di comportamento malevolo, selezionare la casella di spunta **Rileva comportamento malevolo**.
   - Per disabilitare il rilevamento del comportamento malevolo, deselezionare la casella di spunta **Rileva comportamento malevolo**.

   Nota
   Se si disabilita il rilevamento del comportamento malevolo, verrà disattivato anche il rilevamento del comportamento sospetto. Si noti che il rilevamento del traffico malevolo **non** verrà disabilitato.

Rilevamento di traffico malevolo

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

  Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).
- Per il rilevamento del traffico malevolo, occorre che Sophos Live Protection sia abilitata. (Sophos Live Protection è abilitata per impostazione predefinita).

Il rilevamento del traffico malevolo consente di rilevare le comunicazioni tra computer endpoint e server di comando e controllo coinvolti in attacchi sferrati tramite botnet o altri tipi di malware.

Nota
il rilevamento del traffico malevolo utilizza le stesse esclusioni della scansione in accesso di Sophos Anti-Virus (InterCheck ™). Per informazioni sulla configurazione di esclusioni per la scansione in accesso, consultare la sezione Esclusione di oggetti dalla scansione in accesso (pagina 87).

Il rilevamento del traffico malevolo è abilitato per impostazione predefinita nelle nuove installazioni di Enterprise Console versione 5.3 o successive. Se si è effettuato l'upgrade da una versione precedente di Enterprise Console, sarà necessario abilitare il rilevamento del traffico malevolo per poter usufruire di tale funzionalità.

Per modificare le impostazioni di rilevamento del traffico malevolo:

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Nel pannello **Scansione in accesso**, verificare che la casella di spunta **Abilita il monitoraggio del comportamento** sia selezionata.
5. Di fianco a **Abilita il monitoraggio del comportamento**, cliccare su **Configura**.
6. Nella finestra di dialogo **Configura monitoraggio del comportamento**, verificare che la casella di spunta **Rileva comportamento malevolo** sia selezionata.
7. Per abilitare/disabilitare il rilevamento del traffico malevolo, selezionare o deselezionare la casella di spunta **Rilevamento di traffico malevolo**.

Rilevamento di comportamento sospetto

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Il rilevamento di comportamento sospetto controlla tutti i processi di sistema alla ricerca di segni che indichino la presenza di malware attivo, quali scritture sospette nel registro o azioni di copiatura file. Può essere impostato in modo tale da avvertire l'amministratore e/o bloccare il processo.

Per impostazione perdefinita, i comportamenti sospetti vengono individuati e riportati, ma non bloccati.

 Copyright © Sophos Limited

Per modificare le impostazioni di rilevamento e la reportistica relative a comportamento sospetto:

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Nel pannello **Scansione in accesso**, verificare che la casella di spunta **Abilita il monitoraggio del comportamento** sia selezionata.
5. Di fianco a **Abilita il monitoraggio del comportamento**, cliccare su **Configura**.
6. Nella finestra di dialogo **Configura monitoraggio del comportamento**, verificare che la casella di spunta **Rileva comportamento malevolo** sia selezionata.
   - Per avvisare l'amministratore e bloccare eventuali processi sospetti, selezionare la casella di spunta **Rileva comportamento malevolo** e deselezionare quella **Avvisa solo, non bloccare comportamento sospetto**.
   - Per avvisare l'amministratore, ma non bloccare eventuali processi sospetti, selezionare sia la casella di spunta **Rileva comportamento malevolo** che quella **Avvisa solo, non bloccare comportamento sospetto**.

Per avere protezione massima, si consiglia di abilitare il rilevamento di file sospetti. Vedere Configurazione della scansione in accesso (pagina 82).

Rileva buffer overflow

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Il rilevamento di buffer overflow analizza dinamicamente il comportamento dei programmi in esecuzione nel sistema per poter rilevare eventuali tentativi di sfruttare un processo in esecuzione tramite tecniche di buffer overflow.

Per impostazione predefinita, i buffer overflow vengono rilevati e bloccati.

Per modificare le impostazioni di rilevamento e reportistica relative ad attacchi di buffer overflow:

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Nel pannello **Scansione in accesso**, verificare che la casella di spunta **Abilita il monitoraggio del comportamento** sia selezionata.
5. Di fianco a **Abilita il monitoraggio del comportamento**, cliccare su **Configura** Nella finestra di dialogo **Configura monitoraggio del comportamento**:
   - Per avvisare l'amministratore e bloccare episodi di buffer overflow, selezionare la casella di spunta **Rileva buffer overflow** e deselezionare quella **Avvisa solo, non bloccare**.

- Per avvisare l'amministratore, ma non bloccare episodi di buffer overflow, selezionare le caselle di spunta **Rileva buffer overflow** e **Avvisa solo, non bloccare**.

7.1.5 Sophos Live Protection

Sophos Live Protection utilizza la tecnologia "in-the-cloud" per decidere all'istante se un file sospetto è una minaccia, e intraprende l'azione specificata nei criteri antivirus e HIPS.

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 file malevoli. Quando viene identificato un nuovo malware, Sophos è in grado di inviare aggiornamenti entro pochi secondi.

Per sfruttare appieno Live Protection, è necessario assicurarsi che le seguenti opzioni siano abilitate.

- **Abilita Live Protection**

  Se la scansione in accesso di un computer ha identificato un file come sospetto, ma non riesce poi a determinare se sia pulito o malevolo in base ai dati dei file di identità delle minacce (IDE) memorizzati nel computer, alcune caratteristiche del file, quali ad esempio il checksum, vengono inviate a Sophos per 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.

  Importante
  Per le funzionalità Rilevamento del traffico malevolo e Reputazione del download, occorre che Live Protection sia abilitata; ciò consente di effettuare ricerche immediate nel database on-line dei SophosLabs, e ottenere i dati più recenti sulle minacce e sulla reputazione.

- **Abilita Live Protection per la scansione su richiesta**

  Selezionare questa opzione se si desidera che le scansioni su richiesta utilizzino la stessa modalità di verifica in-the-cloud delle scansioni in accesso.

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

  Se un file viene stimato potenzialmente malevolo, ma non può essere identificato con certezza come malevolo solo in base alle sue caratteristiche, Live Protection consente a Sophos di richiedere un campione del file. Quando Live Protection è abilitata, se questa opzione è attivata e Sophos non detiene ancora un campione del file, il file verrà automaticamente inviato per ulteriori analisi.

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

  Nota
  La dimensione massima del campione è 10 MB. Il timeout per l'upload del campione è di 30 secondi. Si sconsiglia di abilitare l'invio automatico di campioni attraverso una connessione lenta (meno di 56Kbps).

Copyright © Sophos Limited

Importante
Occorre assicurarsi che il dominio Sophos a cui i dati del file vengono inviati sia considerato fidato nella vostra soluzione di filtraggio web. Per informazioni, consultare l'articolo 62637 della knowledge base (http://www.sophos.com/it-it/support/knowledgebase/62637.aspx).

Se si utilizza una soluzione di filtraggio web Sophos, come ad esempio la Web Appliance WS1000, non è richiesta nessun'altra azione - domini Sophos sono già considerati attendibili.

Attivazione e disattivazione di Sophos Live Protection

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Sophos Live Protection analizza i file sospetti utilizzando le informazioni più aggiornate presenti nel database dei SophosLabs.

Per impostazione predefinita, Live Protection invia a Sophos dati di file quali ad esempio i checksum a scopo di analisi, ma non invia file campione. Per poter usufruire di tutti i vantaggi di Live Protection, si consiglia di selezionare l'opzione che prevede l'invio di file campione.

Per attivare e disattivare le opzioni di Sophos Live Protection:

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criteri antivirus e HIPS**, cliccare sul pulsante **Sophos Live Protection**.
4. Nella finestra di dialogo **Sophos Live Protection**:
   - Selezionare o deselezionare la casella di spunta **Abilita Live Protection**. Questa opzione attiva o disattiva Live Protection per le scansioni in accesso.

     Importante
     Per le funzionalità Rilevamento del traffico malevolo e Reputazione del download, occorre che Live Protection sia abilitata; ciò consente di effettuare ricerche immediate nel database on-line dei SophosLabs, e ottenere i dati più recenti sulle minacce e sulla reputazione.

   - Selezionare o deselezionare la casella di spunta **Abilita Live Protection per la scansione su richiesta**. Questa opzione attiva o disattiva Live Protection per le scansioni su richiesta.
   - Selezionare o deselezionare la casella di spunta **Invio automatico dei file campione a Sophos**.

     È possibile inviare campioni solamente quando Live Protection è abilitata.

Nota
Quando si invia il campione di un file a Sophos per la scansione on-line, insieme al campione vengono sempre inviati i dati del file (il checksum, ecc).

7.1.6 Protezione web

La protezione web offre una protezione ancora più efficace contro le minacce web. Include le seguenti funzioni:

- Filtraggio URL in tempo reale
- Scansione dei contenuti scaricati
- Verifica della reputazione dei file scaricati

Filtraggio URL in tempo reale

Il filtraggio URL in tempo reale consente di bloccare l'accesso a siti web noti per ospitare malware. Questa funzione opera una ricerca in tempo reale all'interno del database online di Sophos in cui vengono raccolti i siti web infetti.

Nota
Per esercitare un maggior controllo sui siti web a cui si può accedere, per esempio se si desidera evitare che gli utenti visitino siti web per cui l'organizzazione può essere perseguibile legalmente, utilizzare la funzione Web Control (controllo web). Per ulteriori informazioni, consultare la sezione Criterio del controllo web (pagina 174).

Scansione dei contenuti

La scansione dei contenuti esegue la scansione dei dati e dei file scaricati da Internet (o Intranet) e rileva contenuto malevolo in modo proattivo. Questa funzione esegue la scansione di contenuti ospitati in qualsiasi percorso, compresi quelli non facenti parte del database dei siti web infetti.

Reputazione del download

La reputazione del download viene definita in base all'età dei file, alle loro fonti e prevalenza, oltre che a un'approfondita analisi dei contenuti e ad altre caratteristiche specifiche.

Nota
l'analisi della reputazione del download è solo supportata in computer Windows 7 o successivi.

Per impostazione predefinita, viene visualizzato un avviso ogniqualvolta venga effettuato il tentativo di scaricare un file con reputazione bassa o sconosciuta. Sophos consiglia di non effettuare il download di tali file. Se si ritiene la fonte e l'entità di pubblicazione attendibili, è possibile scegliere di effettuare comunque il download. Le azioni intraprese e le URL dei file vengono registrati nel log di scansione.

Nota
la reputazione del download viene definita in base ai dati raccolti nel database in-the-cloud dei SophosLabs e richiede l'abilitazione di Sophos Live Protection per poter effettuare ricerche ed ottenere dati (Sophos Live Protection è abilitata per impostazione predefinita).

 Copyright © Sophos Limited

Per maggiori informazione sulla reputazione del download, consultare l'articolo 121319 della knowledge base.

Impostazioni di configurazione della Protezione Web

La funzionalità di Protezione Web è abilitata per impostazione predefinita e consente di bloccare l'accesso a siti Web malevoli, effettuare la scansione dei contenuti scaricati, oltre che di verificare la reputazione dei file scaricati.

Per maggiori informazioni sulle impostazioni relative alla Protezione web e su come modificarle, consultare la sezione Configurazione delle opzioni della protezione web (pagina 103).

Browser Web supportati

I seguenti browser Web supportano la funzionalità di protezione Web:

- Internet Explorer
- Edge
- Google Chrome
- Firefox (esclusa la funzionalità per il rilevamento della reputazione dei download)
- Safari (esclusa la funzionalità per il rilevamento della reputazione dei download)
- Opera

I contenuti web a cui si accede non utilizzando un browser supportato non verranno filtrati e quindi non potranno essere bloccati.

Eventi della protezione web

Quando viene bloccato l'accesso a un sito web malevolo, viene registrato un evento nel Visualizzatore eventi web e nella voce **Dettagli del computer**, riferita al computer endpoint in cui si è verificato l'evento. Se si utilizza la funzione Web Control, sia gli eventi di protezione web, sia quelli di controllo web vengono visualizzati nel Visualizzatore eventi web e in **Dettagli del computer**. Vedere Visualizzazione degli eventi web (pagina 203) e Visualizzazione nel computer degli eventi web più recenti (pagina 204).

Configurazione delle opzioni della protezione web

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per attivare e disattivare la protezione web:

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.

4. Nella finestra di dialogo **Criteri antivirus e HIPS**, cliccare sul pulsante **Protezione web**.
5. Nella finestra di dialogo **Protezione web**, sotto **Protezione antimalware**, accanto a **Blocca l'accesso ai siti malevoli**, selezionare**Attivato** o **Disattivato** per bloccare o sbloccare l'accesso ai siti web malevoli. Questa opzione è abilitata per impostazione predefinita.
   Per informazioni su come autorizzare determinati siti web, consultare la sezione Autorizzazione di siti web (pagina 112).
6. Per attivare o disattivare la scansione dei dati e file scaricati, di fianco all'opzione **Scansione dei contenuti**, selezionare **Scansione in accesso**, **Attivato** o **Disattivato**.

   Per impostazione predefinita è selezionata l'opzione **Scansione in accesso**, vale a dire, la scansione dei contenuti viene disattivata o attivata contemporaneamente alla scansione in accesso.
7. Per modificare le azioni intraprese quando un utente cerca di scaricare un file con reputazione bassa o sconosciuta, sotto **Reputazione del download**, di fianco all'opzione **Azione**, selezionare **Richiedi conferma all'utente** (impostazione predefinita) oppure **Solo log**.

   Nota
   Per la reputazione del download, occorre che Sophos Live Protection sia abilitata. (Sophos Live Protection è abilitata per impostazione predefinita).

   - Se si seleziona l'opzione **Richiedi conferma all'utente**, ogni volta che un utente cerca di scaricare un file a bassa reputazione, verrà visualizzato un avviso informativo in cui si chiede se bloccare o autorizzare il download. Sophos consiglia agli utenti di non effettuare il download di tali file. Se gli utenti ritengono che fonte ed entità di pubblicazione sono attendibili, potranno scegliere di effettuare comunque il download. La scelta effettuata in merito al blocco o all'autorizzazione del download, insieme all'URL del file, verrà inserita nel log di scansione e inclusa tra gli eventi web in Enterprise Console.
   - Se si seleziona l'opzione **Solo log**, non verrà visualizzato alcun avviso; il download verrà autorizzato, registrato nel log di scansione, e incluso tra gli eventi web in Enterprise Console.
8. Per stabilire quanto rigido debba essere il rilevamento della reputazione, di fianco all'opzione **Soglia**, selezionare **Consigliata** (impostazione predefinita) o **Rigida**.
   - Se si seleziona l'opzione **Consigliata**, verrà visualizzato un allarme e/o creata una nuova voce nel file di log e un nuovo evento ogniqualvolta un utente cerchi di scaricare un file con reputazione bassa o sconosciuta.
   - Se si seleziona l'opzione **Rigida**, verrà visualizzato un allarme e/o creata una nuova voce nel file di log e un nuovo evento ogniqualvolta un utente cerchi di scaricare un file con reputazione media, bassa o sconosciuta.

7.1.7 Tipi di file ed esclusioni sottoposti a scansione

Per impostazione predefinita, Sophos Endpoint Security and Control esegue la scansione dei tipi di file vulnerabili ai virus. I tipi di file esaminati per impostazione predefinita non solo variano a seconda del sistema operativo, ma anche degli aggiornamenti via via apportati al prodotto.

Per visualizzare l'elenco dei tipi di file esaminati per impostazione predefinita, sul computer con il sistema operativo che interessa, aprire la finestra Sophos Endpoint Security and Control o Sophos Anti-Virus e cercare la pagina di configurazione "Estensioni".

È inoltre possibile esaminare tipi di file aggiuntivi o escluderne altri.

 Copyright © Sophos Limited

Windows

Per consultare un elenco dei file esaminati per impostazione predefinita nei computer Windows:

1. Apri Sophos Endpoint Security and Control.
2. Sotto **Anti-virus e HIPS**, cliccare su **Configura Sophos antivirus e HIPS** e quindi su **Estensioni ed esclusioni su richiesta**.

Per informazioni sulla scansione di tipi di file aggiuntivi o dell'esclusione di altri nei computer Windows, consultare i seguenti argomenti:

- Specificazione delle estensioni dei file per la scansione in accesso (pagina 86)
- Specificazione delle estensioni dei file per la scansione su richiesta e pianificata (pagina 93)

Mac OS X

Sophos Anti-Virus per Mac OS X, durante le operazioni di scansione in accesso, sottopone a scansione tutte le estensioni file. Per modificare le impostazioni relative alla scansione pianificata, consultare la sezione Specificazione delle estensioni dei file per la scansione su richiesta e pianificata (pagina 93).

Linux o UNIX

Per apportare modifiche a computer Linux, utilizzare i comandi `savconfig` e `savscan` come descritto nella *Guida alla configurazione di Sophos Anti-Virus per Linux*.

Per apportare modifiche a computer UNIX, utilizzare il comando `savscan` descritto nella *Guida alla configurazione di Sophos Anti-Virus per UNIX*.

Oggetti che possono essere esclusi dalla scansione

Su ogni tipo di computer esistono diverse limitazioni riguardo agli oggetti che è possibile escludere dalla scansione.

Windows

Su Windows, è possibile escludere unità, cartelle, file e processi.

È possibile utilizzare i caratteri jolly * e ?.

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.

Mac OS X

Sui computer con sistema operativo Mac OS X, è possibile escludere file, cartelle e volumi.

È possibile specificare quali oggetti escludere aggiungendo una barra singola come prefisso o suffisso, oppure una barra doppia solo come suffisso dell'esclusione.

Per ulteriori informazioni, consultare la *Guida in linea di Sophos Anti-Virus per Mac OS X* (in inglese).

Linux o UNIX

Su Linux e Unix, è possibile escludere unità, cartelle e file.

È possibile indicare qualsiasi percorso POSIX, costituito sia da file che da directory, ad es. /cartella/file È possibile utilizzare i caratteri jolly ? e *.

Nota
Enterprise Console supporta solo esclusioni Linux e UNIX basate sul percorso. È anche possibile impostare altri tipi di esclusioni direttamente nei computer gestiti. Quindi, è possibile utilizzare espressioni regolari, escludere tipi di file e file system. Per informazioni su come svolgere queste operazioni, consultare la *Guida alla configurazione di Sophos Anti-Virus per Linux* o la *Guida alla configurazione di Sophos Anti-Virus per UNIX.*

Se, in un computer Linux o UNIX gestito, si è impostata un'altra esclusione basata sul percorso, questo computer sarà segnalato alla console come non conforme ai criteri di gruppo.

Per informazioni sull'esclusione di oggetti dalla scansione, consultare le seguenti sezioni:

- Esclusione di oggetti dalla scansione in accesso (pagina 87)
- Esclusione di oggetti dalla scansione su richiesta e pianificata (pagina 94)

Specificazione delle esclusioni di scansione per Windows

Convenzioni di nomenclatura standard

Sophos Anti-Virus convalida percorsi e nomi file degli oggetti che si desidera escludere dalla scansione, in base alla convenzioni di denominazione di Windows. Per esempio, il nome di una cartella può contenere spazi, ma non solo.

Estensioni file multiple

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

`MySample.txt.doc` = nome file `MySample.txt` + estensione `.doc`.

 Copyright © Sophos Limited

Esclusione di file, cartelle o unità specifiche

Tipo di esclusione	Descrizione	Esempi	Commenti

File specifico	Specificare sia il percorso che il nome per poter escludere un determinato file. Il percorso può includere una lettera di unità o il nome di una condivisione di rete.	`C:\Documents\CV.doc`
		`\\Server\Users\Documents\CV.doc`
			Per assicurarsi che le esclusioni vengano applicate correttamente, aggiungere nome file e cartella sia nella versione estesa che conforme alla 8.3:
			`C:\Programmi\Sophos\Sophos Anti-Virus`
			`C:\Progra~1\Sophos\Sophos~1`
			Per ulteriori informazioni, consultare l'articolo 13045 della knowledge base.

Tutti i file con lo stesso nome	Indicare il nome di un file senza percorso per escludere tutti i file aventi lo stesso nome ovunque si trovino nel file system.	`spacer.gif`	
Tutti gli oggetti di un'unità o condivisione di rete	Specificare la lettera dell'unità o il nome della condivisione per escludere tutti gli oggetti contenuti in un'unità o condivisione di rete	`D:` `\\Server\<nomecondivisione>\`	Quando viene specificata una condivisione di rete, includere una barra finale dopo il nome della condivisione.

Tipo di esclusione	Descrizione	Esempi	Commenti
Cartella specifica	Indicare il percorso di una cartella che comprenda una lettera di unità o il nome di una condivisione di rete, per escludere tutti gli oggetti presenti in quella cartella e nelle relative sottocartelle.	`D:\Tools\logs\`	Includere una barra finale dopo il nome della cartella.
Tutte le cartelle con lo stesso nome	Indicare il percorso di una cartella senza alcuna lettere di unità o nome di condivisione di rete, per escludere qualsiasi oggetto presente in quella cartella e nelle relative sottocartelle in ***tutte*** le unità o condivisioni di rete.	`\Tools\logs\` (esclude le seguenti cartelle: `C:\Tools\logs\`, `\\Server\Tools\logs\`)	È necessario indicare tutto il percorso fino alla lettera di unità o al nome della condivisione di rete. In questo esempio, specificando `\logs\` non verrebbe escluso alcun file.

Caratteri jolly

È possibile utilizzare i caratteri jolly ? e *.

Utilizzare il carattere jolly ? nel nome file o estensione al posto di un singolo carattere.

Alla fine di un nome file o estensione, il carattere jolly ? sostituisce un singolo carattere o nessun carattere. per esempio `file??.txt` corriponde a `file.txt`, `file1.txt`, e `file12.txt`, ma non a `file123.txt`.

Utilizzare il carattere jolly * in un nome file o estensione, nel formato `[nome file].*` o `*.[estensione]`:

Corretto

`file.*`

`*.txt`

Errato

`file.txt*`

`file.*txt`

È anche possibile escludere file aventi un'estensione e caratteri iniziali specifici:

`file*.txt`

Nell'esempio di cui sopra, vengono esclusi dalla scansione i seguenti file:

Copyright © Sophos Limited

```
file.txt
file1.txt
file12.txt
file.1.txt
file.12.txt
file12.12.txt
```

I seguenti file non sono esclusi, se si applica l'esclusione definita nell'esempio di cui sopra:

```
file.1txt
file.12txt
file.txt1
file.txt12
1file.txt
1file.txt1
```

7.1.8 Autorizzazione all'utilizzo di oggetti

Autorizzazione di adware e PUA

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Se Sophos Endpoint Security and Control è stato abilitato al rilevamento di adware e altre applicazioni potenzialmente indesiderate (PUA), potrebbe impedire l'utilizzo di un'applicazione che invece è necessaria.

Per autorizzare un'applicazione adware o PUA:

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Cliccare su **Autorizzazioni**.
   Viene visualizzata la finestra di dialogo **Gestore autorizzazioni**.
5. Nella scheda **Adware e PUA**, nell'elenco **Adware e PUA noti**, selezionare l'applicazione che si desidera autorizzare.

   Se non si riesce a trovare l'applicazione desiderata, aggiungerla all'elenco di adware e PUA. Per informazioni su come svolgere questa operazione, vedere Preautorizzazione di adware e PUA (pagina 110).
6. Cliccare su **Aggiungi**.

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

Preautorizzazione di adware e PUA

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Se si desidera autorizzare l'utilizzo di un'applicazione che Sophos Endpoint Security and Control non ha ancora classificato come adware o PUA, è possibile preautorizzarla aggiungendola direttamente all'elenco di adware e PUA autorizzati.

1. Visitare la pagina dedicata ad **Adware e PUA** del sito web di Sophos (http://www.sophos.com/it-it/threat-center/threat-analyses/adware-and-puas.aspx).
2. Trovare e quindi copiare il nome dell'applicazione che si desidera preautorizzare.
3. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
4. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
5. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
6. Cliccare su **Autorizzazioni**.
   Viene visualizzata la finestra di dialogo **Gestore autorizzazioni**.
7. Nella scheda **Adware e PUA**, cliccare su **Nuova voce**.
8. Nella finestra di dialogo **Aggiungi nuovi adware e PUA**, copiare il nome dell'applicazione copiato al passaggio 2.

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

Nel caso si siano verificati errori o semplicemente si desideri rimuovere un'applicazione da **Gestore autorizzazioni**, sarà possibile cancellarlo direttamente dall'elenco degli adware e PUA noti:

1. Nell'elenco **Adware e PUA autorizzati**, selezionare l'applicazione.
2. Cliccare su **Rimuovi**.
3. Nell'elenco **Adware o PUA noti**, selezionare l'applicazione.
4. Cliccare su **Cancella voce**.

Blocco di adware e PUA autorizzati

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

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

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).

 Copyright © Sophos Limited

2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criteri antivirus e HIPS**, cliccare sul pulsante **Autorizzazioni**.
4. Nella scheda **Adware o PUA**, nell'elenco **Adware e PUA autorizzati**, selezionare l'applicazione che si desidera bloccare.
5. Cliccare su **Rimuovi**.

Autorizzazione di oggetti sospetti

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Se sono state abilitate una o più opzioni HIPS (ad es. rilevamento di comportamento sospetto, rilevamento di buffer overflow o rilevamento di file sospetti), ma si desidera utilizzare alcuni degli oggetti rilevati, è possibile autorizzarli eseguendo la procedura riportata qui di seguito.

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Cliccare su **Autorizzazioni**.
   Viene visualizzata la finestra di dialogo **Gestore autorizzazioni**.
5. Cliccare sulla scheda relativa al tipo di comportamento rilevato.

   In questo esempio ci si riferirà a **Buffer Overflow**.
6. Nel riquadro **Applicazioni note**, selezionare il criterio che si desidera rinominare.

   Se non si riesce a trovare l'applicazione desiderata, aggiungerla all'elenco delle applicazioni autorizzate. Per informazioni su come svolgere questa operazione, vedere Preautorizzazione di adware e PUA (pagina 110).
7. Cliccare su **Aggiungi**.

L'applicazione sospetta compare nell'elenco **Applicazioni autorizzate**.

Preautorizzazione di oggetti potenzialmente sospetti

Se si desidera autorizzare l'utilizzo di un'applicazione o file che Sophos Endpoint Security and Control non ha ancora classificato come sospetto, è possibile preautorizzarlo aggiungendolo direttamente all'elenco degli oggetti autorizzati.

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Cliccare su **Autorizzazioni**.
   Viene visualizzata la finestra di dialogo **Gestore autorizzazioni**.

5. Cliccare sulla scheda relativa al tipo di comportamento rilevato.

   In questo esempio ci si riferirà a **Buffer Overflow**.
6. Cliccare su **Nuova voce**.
   Viene visualizzata la finestra di dialogo di **apertura**.
7. Trovare l'applicazione e cliccarvi due volte.

L'applicazione sospetta compare nell'elenco **Applicazioni autorizzate**.

Nel caso si siano verificati errori o semplicemente si desideri rimuovere un'applicazione da **Gestore autorizzazioni**, sarà possibile cancellarlo direttamente dall'elenco dei file noti:

1. Nella finestra di dialogo **Gestore autorizzazioni**, cliccare sulla scheda relativa al tipo di comportamento rilevato.

   In questo esempio ci si riferirà a **File sospetti**.
2. Nell'elenco **File autorizzati**, selezionare il file.
3. Cliccare su **Rimuovi**.
4. Nell'elenco **File noti**, selezionare il file.
5. Cliccare su **Cancella voce**.

Autorizzazione di siti web

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Se si desidera autorizzare un sito classificato come malevolo da Sophos, è possibile aggiungerlo all'elenco dei siti autorizzati. Gli URL di un sito web autorizzato non vengono verificati dal filtro web online di Sophos.

Attenzione
Autorizzare un sito web classificato come malevolo da Sophos potrebbe esporre i propri utenti a minacce. Verificare che l'accesso al sito sia sicuro prima di autorizzarlo.

Come autorizzare un sito web:

1. Controllare quale criterio antivirus e HIPS è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Anti-virus e HIPS**.
3. Cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio antivirus e HIPS**.
4. Cliccare su **Autorizzazioni**.
   Viene visualizzata la finestra di dialogo **Gestore autorizzazioni**.
5. Nella scheda **Siti web**, cliccare su **Aggiungi**.
   - Per modificare la voce relativa a un determinato sito web, selezionarla dall'elenco **Siti web autorizzati**, quindi cliccare su **Modifica**.
   - Per cancellare la voce relativa a un determinato sito web, selezionarla dall'elenco **Siti web autorizzati**, quindi cliccare su **Rimuovi**.

 Copyright © Sophos Limited

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

Note

- se la scansione dei download è abilitata e un utente visita un sito web che contiene una minaccia, l'accesso al sito verrà bloccato anche se questo appartiene all'elenco dei siti autorizzati.
- se si utilizza una funzione di Web Control (controllo web), quando si autorizza l'accesso a un sito web bloccato dal proprio criterio di **Controllo web**, l'accesso a tale sito web continuerà ad essere bloccato. Per consentire l'accesso a tale sito web, sarà necessario escluderlo dalle operazioni di filtro condotte dal controllo web; oltre che autorizzarlo nel criterio antivirus e HIPS. Per maggiori informazioni sul controllo web, consultare la sezione Criterio del controllo web (pagina 174).

7.2 Criterio firewall

Il criterio **Firewall** stabilisce la modalità con la quale il firewall protegge i computer.

Per impostazione predefinita Sophos Client Firewall è attivato e blocca tutto il traffico non essenziale. Dopo averlo utilizzato in tutta la rete, è necessario configurarlo per poter consentire le applicazioni che si desidera utilizzare. Vedere Impostazione di un criterio del firewall di base (pagina 113).

Per l'elenco completo di tutte le impostazioni predefinite del firewall, consultare l'articolo 57757 della knowledge base.

Nota
Sono presenti varie funzionalità che sono state rimosse da Sophos Client Firewall 3.0 per Windows 8 e versioni successive, e che sono disponibili solamente per i computer che eseguono Windows 7 o versioni precedenti. Tali funzionalità sono le seguenti:

- Modalità interattiva
- Rilevamento di processi nascosti
- Rilevamento delle modifiche della memoria
- Applicazioni rawsocket (i rawsocket vengono considerati esattamente come qualsiasi altra connessione)
- Regole senza stato
- Opzione **Connessioni simultanee** per le regole TCP
- Opzione **Dove la porta locale è uguale alla porta remota**

7.2.1 Configurazione di base del firewall

Impostazione di un criterio del firewall di base

Per impostazione predefinita il firewall è attivato e blocca tutto il traffico non essenziale. È quindi necessario configurarlo in modo tale da poter consentire le applicazioni che si desidera utilizzare e testarlo prima di eseguirne l'installazione in tutti i computer. Per informazioni dettagliate, consultare la *Guida all'impostazione dei criteri di* Sophos Enterprise Console.

Per ulteriori informazioni sulle impostazioni predefinite del firewall, consultare l'articolo 57757 della knowledge base Sophos.

Per informazioni su come impedire il bridging di rete, vedere Criterio del controllo dispositivi (pagina 161).

Importante
quando si desidera applicare ai computer un criterio nuovo o aggiornato, le applicazioni in precedenza consentite potranno essere bloccate per un breve periodo di tempo, fin tanto che il nuovo criterio non venga completamente applicato. Informare gli utenti prima di applicare nuovi criteri.

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni sull'amministrazione basata sui ruoli, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per impostare un criterio di base per il firewall:

1. Nel riquadro **Criteri**, cliccare due volte su **Firewall**.
2. Cliccare due volte sul criterio **Predefinito** per modificarlo.
   Si avvia la procedura guidata di **configurazione dei criteri del Firewall**. Seguire le istruzioni sullo schermo. Alcune delle opzioni qui di seguito riportano informazioni aggiuntive.
3. Nella pagina **Configura firewall**, selezionare il tipo di percorso:
   - Selezionare **Percorso singolo** per i computer che sono sempre in rete, per es. i desktop.
   - Selezionare **Percorso doppio** se si desidera che il firewall utilizzi impostazioni diverse a seconda del percorso da cui vengono eseguiti i computer, per es. in ufficio (in rete) e fuori ufficio (fuori rete). È possibile impostare un percorso doppio per i laptop.
4. Nella pagina **Modalità operativa**, selezionare la modalità in cui il firewall deve gestire il traffico in entrata e in uscita.

Mode	Descrizione
Blocco del traffico in entrata e in uscita	• Livello predefinito. Offre la massima sicurezza. • Consente attraverso il firewall solo il traffico essenziale ed autentica l'identità delle applicazioni mediante i checksum. • Per consentire alle applicazioni normalmente utilizzate nella vostra azienda di comunicare attraverso il firewall, cliccare su **Attendibile**. Per ulteriori informazioni, consultare la sezione Attendibilità delle applicazioni (pagina 122).
Blocca il traffico in ingresso e consenti il traffico in uscita	• Offre un livello sicurezza più basso rispetto a **Blocca il traffico in entrata e in uscita**. • Consente ai computer di accedere alla rete e ad Internet senza bisogno di creare regole speciali.

 Copyright © Sophos Limited

Mode	Descrizione
	• A tutte le applicazioni viene consentito di comunicare attraverso il firewall.
Monitora	• Applica al traffico di rete le regole che sono state impostate. Se non esiste una regola soddisfacente per il traffico, il fatto viene segnalato alla console, e viene consentito solo il traffico in uscita. • Consente di raccogliere informazioni relative alla rete e di creare regole adeguate prima di eseguire la distribuzione del firewall su tutti i computer. Per ulteriori informazioni, consultare la sezione Utilizzo della modalità monitor (pagina 115).

5. Nella pagina **Condivisione file e stampanti**, selezionare **Consenti condivisione file e stampanti** se si desidera consentire ai computer di condividere nella rete stampanti e cartelle locali.

Una volta impostato il firewall, è possibile visualizzare gli eventi del firewall (per es. le applicazioni bloccate dal firewall) in **Firewall - Visualizzatore eventi**. Per ulteriori informazioni, vedere Visualizzazione degli eventi del firewall (pagina 198).

Il numero di computer con eventi che hanno superato una determinata soglia entro gli ultimi 7 giorni viene visualizzato anche nel pannello di controllo.

Utilizzo della modalità monitor

È possibile scegliere di utilizzare questa modalità su computer di prova e di utilizzare il visualizzatore eventi del Firewall per visualizzare quale traffico, applicazioni e processi siano in esecuzione.

È quindi possibile utilizzare l'Event Viewer per creare regole che consentano o blocchino il traffico, le applicazioni e i processi rilevati, secondo quanto descritto nella sezione Creazione di una regola per gli eventi del firewall (pagina 118).

Nota
quando si crea una regola tramite il Firewall Event Viewer e questa regola viene aggiunta al criterio del firewall, la modalità del firewall passa da **Monitora** a **Personalizza**.

Se non si desidera permettere, come impostazione predefinita, il traffico sconosciuto, è possibile utilizzare la *modalità interattiva*.

Quando in modalità interattiva, il firewall chiede all'utente di consentire o bloccare le applicazioni e il traffico per cui non sono state create regole. Per ulteriori informazioni, vedere Modalità interattiva (pagina 120).

Aggiungere e dichiarare attendibile un'applicazione

Alle applicazioni attendibili viene concesso accesso alla rete pieno e incondizionato, oltre che accesso a Internet.

Per aggiungere un'applicazione ai criteri del firewall, e per dichiararla attendibile:

1. Sulla pagina **Modalità operativa** della procedura guidata per il **criterio del firewall**, cliccare su **Attendibile**.

Viene visualizzata la finestra di dialogo **Criterio firewall**.

2. Cliccare su **Aggiungi**.
   Viene visualizzata la finestra di dialogo **Criterio firewall - Aggiungi applicazione attendibile**.
3. Nel campo **Periodo ricerca**, cliccare sulla freccia dell'elenco a discesa e selezionare il periodo in cui si desidera visualizzare gli eventi delle applicazioni.

   È possibile selezionare un periodo fisso, per es. **Entro 24 ore**, oppure l'opzione **Personalizzato** e indicare il periodo prescelto selezionando l'orario e la data di inizio e fine.
4. Se si desidera visualizzare un certo tipo di eventi delle applicazioni, nel campo **Tipo di evento**, cliccare sulla freccia dell'elenco a discesa e selezionare il tipo di evento.
5. Se si desidera visualizzare gli eventi delle applicazioni per un certo file, nel campo **Nome file**, inserire il nome del file.

   Se questo campo viene lasciato vuoto, verranno visualizzati gli eventi delle applicazioni per tutti i file.

   In questo campo si possono utilizzare caratteri jolly. Utilizzare ? per ogni singolo carattere e * per ogni stringa di caratteri.
6. Cliccare su **Cerca** per visualizzare un elenco di eventi delle applicazioni.
7. Selezionare un evento delle applicazioni, e cliccare su **OK**.

L'applicazione viene aggiunta ai criteri firewall e contrassegnata come **Attendibile**.

Amministrazione basata sui ruoli

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Autorizzazione di tutto il traffico su una LAN

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

1. Controllare quale criterio firewall è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Firewall** e poi sul criterio che si desidera modificare.
3. Sulla pagina **Condivisione file e stampanti** della procedura guidata per i **Criteri firewall**, selezionare **Utilizza impostazioni personalizzate**, e cliccare su **Personalizza**.
4. Nell'elenco **Impostazioni LAN**, spuntare la casella **Attendibile** per una rete.

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

 Copyright © Sophos Limited

Amministrazione basata sui ruoli

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Consenso alla condivisione file e stampanti

Per consentire ai computer di condividere nella rete stampanti e cartelle locali:

1. Controllare quale criterio firewall è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Firewall** e poi sul criterio che si desidera modificare.
3. Nella pagina **Condivisione file e stampanti** della procedura guidata per i **Criteri firewall**, selezionare **Consenti condivisione file e stampanti**.

Amministrazione basata sui ruoli

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Autorizzazione del controllo flessibile di 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:

- Autorizzare la 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.
- Creare regole con elevata priorità che consentano la comunicazione a/da host tramite gli adeguati 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.

Per autorizzare la condivisione file e stampanti in LAN diverse da quelle presenti nell'elenco **Impostazioni LAN**:

1. Controllare quale criterio firewall è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Firewall** e poi sul criterio che si desidera modificare.
3. Sulla pagina **Condivisione file e stampanti** della procedura guidata per i **Criteri firewall**, selezionare **Utilizza impostazioni personalizzate**, e cliccare su **Personalizza**.

4. Deselezionare la casella **Blocca condivisione file e stampanti per altre reti**.

Amministrazione basata sui ruoli

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Blocco di condivisioni file e stampanti indesiderate

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

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

1. Controllare quale criterio firewall è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Firewall** e poi sul criterio che si desidera modificare.
3. Sulla pagina **Condivisione file e stampanti** della procedura guidata per i **Criteri firewall**, selezionare **Utilizza impostazioni personalizzate**, e cliccare su **Personalizza**.
4. Selezionare la casella **Blocca condivisione file e stampanti per altre reti**.

Creazione di una regola per gli eventi del firewall

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile creare regole per tutti gli eventi del firewall, eccezion fatta per gli eventi di "memoria modificata".

Per creare una regola per gli eventi del firewall:

1. Dal menu **Eventi**, cliccare su **Eventi firewall**.
2. Nella finestra di dialogo **Firewall - Visualizzatore eventi**, selezionare un evento relativo all'applicazione per cui si desidera creare una regola e cliccare su **Crea regola**.

 Copyright © Sophos Limited

3. Nella finestra di dialogo che viene visualizzata, selezionare l'opzione che si desidera applicare all'applicazione.
4. Scegliere a quale percorso applicare la regola (primario, secondario o entrambi). Se si sceglie di applicare la regola al percorso secondario o a entrambi, la regola verrà aggiunta solo ai criteri che hanno configurato un percorso secondario. Cliccare su **OK**.

   Nota
   gli eventi relativi a "nuova applicazione" e "applicazione modificata" sono percorsi indipendenti (aggiungono i checksum condivisi da entrambi i percorsi). È impossibile scegliere un percorso per questi eventi.

5. Dall'elenco dei criteri firewall, selezionare un criterio o criteri a cui si desidera applicare il criterio. Cliccare su **OK**.

   Nota
   è impossibile aggiungere una regola a un criterio applicato al di fuori del proprio sottoambiente attivo.

Nota
se si desidera creare una regola delle applicazioni direttamente da un criterio del firewall, tramite le pagine di configurazione avanzata del criterio firewall, consultare la sezione Creazione di una regola delle applicazioni da un criterio firewall (pagina 136).

Disabilitazione temporanea del firewall

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per impostazione predefinita, il firewall è abilitato. Talvolta può essere necessario disabilitarlo temporaneamente per svolgere operazioni di manutenzione o risoluzione di problemi per poi riabilitarlo.

Per disattivare il firewall in un gruppo di computer:

1. Controllare quale criterio firewall è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Firewall**. Quindi cliccare due volte sul criterio che si desidera modificare.
   Si avvia la procedura guidata di **configurazione dei criteri del Firewall**.
3. Nella pagina di Benvenuto della procedura guidata, svolgere una delle seguenti operazioni:
   - Se si desidera disabilitare il firewall per tutti i percorsi impostati (primario e secondario, se configurato), cliccare su **Avanti**. Nella pagina **Configura firewall**, selezionare **Consenti tutto il traffico (firewall disattivato)**. Completare la procedura guidata.

- Se si desidera disabilitare il firewall solo per uno dei percorsi (primario o secondario), cliccare sul pulsante **Criteri avanzati firewall**. Nella finestra di dialogo **Criterio firewall** che viene visualizzata, selezionare **Consenti tutto il traffico** di fianco a **Percorso primario** o **Percorso secondario**. Cliccare su **OK**. Portare a termine la procedura guidata di **configurazione dei criteri del Firewall**.

Se si disabilita il firewall, i computer risultano non protetti finché la scansione in accesso non venga riabilitata. Per abilitare il firewall, deselezionare la casella di spunta **Consenti tutto il traffico**.

7.2.2 Configurazione avanzata del firewall

Apertura delle pagine di configurazione avanzata

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Se si desidera avere maggiore controllo delle impostazioni del firewall e la possibilità di regolarle, utilizzare le pagine di configurazione avanzata del criterio firewall per configurarlo.

Per aprire le pagine di configurazione avanzata del firewall:

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.

Modalità interattiva

Nei computer che eseguono Windows 7 o versioni precedenti, è possibile abilitare la modalità interattiva. Il firewall visualizza nel computer endpoint una finestra di apprendimento ogni volta che un'applicazione o un servizio sconosciuto richiede accesso alla rete. La finestra di apprendimento chiede all'utente se consentire o bloccare il traffico, oppure se creare una regola per quel particolare tipo di traffico.

Nota
In Windows 8 e versioni successive, la modalità interattiva non è disponibile. È necessario aggiungere criteri specifici per consentire o bloccare applicazioni. È possibile utilizzare **Firewall - Visualizzatore eventi** per gestire le regole delle applicazioni in maniera interattiva, come indicato nella sezione Creazione di una regola per gli eventi del firewall (pagina 118).

 Copyright © Sophos Limited

Abilitazione della modalità interattiva

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Il firewall può lavorare in modalità interattiva, chiedendo all'utente come gestire il traffico rilevato. Per ulteriori informazioni, consultare la sezione Modalità interattiva (pagina 120).

Per mettere il firewall in modalità interattiva in un gruppo di computer:

1. Controllare quale criterio firewall è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
4. Nella scheda **Generale**, sotto **Modalità di funzionamento**, cliccare su **Interattiva**.

Passaggio alla modalità non interattiva

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

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 non interattiva in un gruppo di computer:

1. Nel riquadro **Criteri**, cliccare due volte su **Firewall** e poi sul criterio che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
4. Cliccare sulla scheda **Generale**.
5. Sotto **Modalità di funzionamento**, cliccare su **Consenti per impostazione predefinita** o **Blocca per impostazione predefinita**.

Copyright © Sophos Limited

Configurazione del firewall

Attendibilità delle applicazioni

Per aiutare a rendere i computer più sicuri, il firewall blocca il traffico proveniente da applicazioni non riconosciute nei computer. Alcune applicazioni comunemente utilizzate dalla propria organizzazione, potrebbero essere comunque bloccate, impedendo così agli utenti di svolgere i loro incarichi quotidiani.

È possibile *dichiarare attendibili* queste applicazioni, in modo che possano comunicare attraverso il firewall. Alle applicazioni attendibili viene concesso pieno e incondizionato accesso alla rete e a Internet.

Nota
Per un maggior livello di sicurezza, è possibile applicare una o più *regole dell'applicazione* per specificare le condizioni in cui un'applicazione può essere eseguita. Per informazioni su come svolgere questa operazione, vedere Creazione di una regola delle applicazioni da un criterio firewall (pagina 136).

Aggiunta di un'applicazione ad un criterio del firewall

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per aggiungere un'applicazione ad un criterio del firewall:

1. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
2. Cliccare sulla scheda **Applicazioni**.
3. Cliccare su **Aggiungi**.
   Viene visualizzata la finestra di dialogo **Criterio firewall - Aggiungi applicazione**.
4. Nel campo **Periodo ricerca**, cliccare sulla freccia dell'elenco a discesa e selezionare il periodo in cui si desidera visualizzare gli eventi delle applicazioni.

   È possibile selezionare un periodo fisso, per es. **Entro 24 ore**, oppure l'opzione **Personalizzato** e indicare il periodo prescelto selezionando l'orario e la data di inizio e fine.
5. Se si desidera visualizzare un certo tipo di eventi delle applicazioni, nel campo **Tipo di evento**, cliccare sulla freccia dell'elenco a discesa e selezionare il tipo di evento.
6. Se si desidera visualizzare gli eventi delle applicazioni per un certo file, nel campo **Nome file**, inserire il nome del file.

   Se questo campo viene lasciato vuoto, verranno visualizzati gli eventi delle applicazioni per tutti i file.

   In questo campo si possono utilizzare caratteri jolly. Utilizzare ? per ogni singolo carattere e * per ogni stringa di caratteri.
7. Cliccare su **Cerca** per visualizzare un elenco di eventi delle applicazioni.
8. Selezionare un evento delle applicazioni, e cliccare su **OK**.

- L'applicazione viene aggiunta ai criteri firewall e contrassegnata come **Attendibile**.

 Copyright © Sophos Limited

- Il checksum dell'applicazione viene aggiunto all'elenco dei checksum consentiti.

Rimuovere un'applicazione da un criterio del firewall

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per rimuovere un'applicazione da un criterio del firewall:

1. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
2. Cliccare sulla scheda **Applicazioni**.
3. Selezionare l'applicazione nell'elenco e cliccare su **Rimuovi**.

Attendibilità delle applicazioni

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per dichiarare attendibile un'applicazione in un gruppo di computer:

1. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
2. Cliccare sulla scheda **Applicazioni**.

   Se l'applicazione non è nell'elenco, seguire le istruzioni nella sezione Aggiunta di un'applicazione ad un criterio del firewall (pagina 122) per aggiungerla.
3. Selezionare l'applicazione nell'elenco e cliccare su **Attendibile**.

- L'applicazione viene aggiunta ai criteri firewall e contrassegnata come **Attendibile**.
- Il checksum dell'applicazione viene aggiunto all'elenco dei checksum consentiti.

Alle applicazioni attendibili viene concesso accesso alla rete pieno e incondizionato, oltre che accesso a Internet. per un maggior livello di 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 dell'applicazione (pagina 135)
- Applicazione delle regole delle applicazioni predefinite (pagina 138)

Dichiarare un'applicazione attendibile mediante il Visualizzatore eventi firewall

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Se il firewall rileva un'applicazione sconosciuta o blocca un'applicazione nei computer in rete, comparirà un evento nel Visualizzatore eventi firewall. Questa sezione descrive come dichiarare attendibile un'applicazione del Visualizzatore eventi firewall e come applicare la nuova regola ai criteri firewall prescelti.

Per reperire dati relativi alle applicazioni rilevate o bloccate nel Visualizzatore eventi firewall e dichiararle attendibili, oppure per creare nuove regole per tali applicazioni:

1. Dal menu **Eventi**, cliccare su **Eventi firewall**.
2. Nella finestra di dialogo **Firewall - Visualizzatore eventi**, selezionare la voce relativa all'applicazione che si desidera considerare affidabile o per cui si desidera creare una regola, e cliccare su **Crea regola**.
3. Nella finestra di dialogo che viene visualizzata, scegliere se dichiarare l'applicazione attendibile o se creare una regola tramite impostazioni predefinite esistenti.
4. Dall'elenco dei criteri firewall, selezionare i criteri firewall a cui applicare la regola. Per applicare la regola a tutti i criteri, cliccare su **Seleziona tutto** e successivamente su **OK**.

- Se si utilizzano checksum, potrebbe essere necessario aggiungere il checksum dell'applicazione all'elenco dei checksum autorizzati. Vedere Aggiunta di checksum dell'applicazione (pagina 127).
- È inoltre possibile aggiungere direttamente a un criterio del firewall un'applicazione dichiarata attendibile, tramite le pagine relative alla configurazione avanzata del criterio del firewall. Vedere Creazione di una regola delle applicazioni da un criterio firewall (pagina 136).

Blocco di un'applicazione

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per bloccare un'applicazione in un gruppo di computer:

1. Controllare quale criterio firewall è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Firewall** e poi sul criterio che si desidera modificare.
3. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
4. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
5. Cliccare sulla scheda **Applicazioni**.

 Copyright © Sophos Limited

Se l'applicazione non è nell'elenco, seguire le istruzioni nella sezione Aggiunta di un'applicazione ad un criterio del firewall (pagina 122) per aggiungerla.

6. Selezionare l'applicazione nell'elenco e cliccare su **Blocca**.

Autorizzazione dell'avvio di processi nascosti

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

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 aggirare i firewall; possono infatti lanciare un'applicazione ritenuta affidabile per accedere alla rete invece che tentare da sole.

Per consentire alle applicazioni di avviare processi nascosti, procedere come indicato qui di seguito.

Nota
Questa opzione non è disponibile in Windows 8 e versioni successive, dal momento che l'operazione viene gestita automaticamente dalla tecnologia HIPS di Sophos Anti-Virus.

1. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
2. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
3. Cliccare sulla scheda **Processi**.
4. Nella parte in alto, cliccare su **Aggiungi**.
   Viene visualizzata la finestra di dialogo **Criterio firewall - Aggiungi applicazione**.
5. Nel campo **Periodo ricerca**, cliccare sulla freccia dell'elenco a discesa e selezionare il periodo in cui si desidera visualizzare gli eventi delle applicazioni.

   È possibile selezionare un periodo fisso, per es. **Entro 24 ore**, oppure l'opzione **Personalizzato** e indicare il periodo prescelto selezionando l'orario e la data di inizio e fine.
6. Se si desidera visualizzare gli eventi delle applicazioni per un certo file, nel campo **Nome file**, inserire il nome del file.

   Se questo campo viene lasciato vuoto, verranno visualizzati gli eventi delle applicazioni per tutti i file.

   In questo campo si possono utilizzare caratteri jolly. Utilizzare ? per ogni singolo carattere e * per ogni stringa di caratteri.
7. Cliccare su **Cerca** per visualizzare un elenco di eventi delle applicazioni.
8. Selezionare un evento delle applicazioni, e cliccare su **OK**.

Se si utilizza la modalità interattiva, il firewall può visualizzare sul computer una finestra di apprendimento ogni qual volta rilevi un nuovo programma di avvio. Per ulteriori informazioni, vedere Abilitazione della modalità interattiva (pagina 121). La modalità interattiva non è disponibile in Windows 8 e versioni successive.

Autorizzazione dell'utilizzo di raw socket da parte di applicazioni

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

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.

Per consentire alle applicazioni di accedere alla rete tramite raw socket, procedere come indicato di seguito.

Nota
Questa opzione non è disponibile in Windows 8 e versioni successive. Il firewall tratterà i rawsocket nello stesso modo in cui vengono trattati i socket ordinari.

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Processi**.
5. Nella parte in basso, cliccare su **Aggiungi**.
   Viene visualizzata la finestra di dialogo **Criterio firewall - Aggiungi applicazione**.
6. Nel campo **Periodo ricerca**, cliccare sulla freccia dell'elenco a discesa e selezionare il periodo in cui si desidera visualizzare gli eventi delle applicazioni.

   È possibile selezionare un periodo fisso, per es. **Entro 24 ore**, oppure l'opzione **Personalizzato** e indicare il periodo prescelto selezionando l'orario e la data di inizio e fine.
7. Se si desidera visualizzare gli eventi delle applicazioni per un certo file, nel campo **Nome file**, inserire il nome del file.

   Se questo campo viene lasciato vuoto, verranno visualizzati gli eventi delle applicazioni per tutti i file.

   In questo campo si possono utilizzare caratteri jolly. Utilizzare ? per ogni singolo carattere e * per ogni stringa di caratteri.
8. Cliccare su **Cerca** per visualizzare un elenco di eventi delle applicazioni.
9. Selezionare un evento delle applicazioni, e cliccare su **OK**.

Se si utilizza la modalità interattiva, il firewall può visualizzare sul computer una finestra di apprendimento ogni qual volta venga rilevato un raw socket. Per ulteriori informazioni, vedere Abilitazione della modalità interattiva (pagina 121).

 Copyright © Sophos Limited

Aggiunta di checksum dell'applicazione

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

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 è sconosciuto o è stato modificato, il firewall lo bloccherà.

Per aggiungere un checksum all'elenco di checksum autorizzati:

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Cliccare sulla scheda **Checksum**.
4. Cliccare su **Aggiungi**.
   Viene visualizzata la finestra di dialogo **Criterio firewall - Aggiungi checksum dell'applicazione**.
5. Nel campo **Periodo ricerca**, cliccare sulla freccia dell'elenco a discesa e selezionare il periodo in cui si desidera visualizzare gli eventi delle applicazioni.

   È possibile selezionare un periodo fisso, per es. **Entro 24 ore**, oppure l'opzione **Personalizzato** e indicare il periodo prescelto selezionando l'orario e la data di inizio e fine.
6. Nel campo **Tipo di evento**, cliccare sulla freccia dell'elenco a discesa e selezionare se si desidera aggiungere un checksum per un'applicazione modificata o una nuova applicazione.
7. Se si desidera visualizzare gli eventi delle applicazioni per un certo file, nel campo **Nome file**, inserire il nome del file.

   Se questo campo viene lasciato vuoto, verranno visualizzati gli eventi delle applicazioni per tutti i file.

   In questo campo si possono utilizzare caratteri jolly. Utilizzare ? per ogni singolo carattere e * per ogni stringa di caratteri.
8. Cliccare su **Cerca** per visualizzare un elenco di eventi delle applicazioni.
9. Selezionare l'evento dell'applicazione al quale si desidera aggiungere un checksum, e cliccare su **OK**.

Il checksum dell'applicazione viene aggiunto all'elenco di checksum consentiti nella finestra di dialogo **Criterio firewall**.

Se si utilizza la modalità interattiva, il firewall può visualizzare sul computer una finestra di apprendimento ogni qual volta rilevi un'applicazione nuova o modificata. Per ulteriori informazioni, vedere Abilitazione della modalità interattiva (pagina 121).

Attivazione e disattivazione del blocco di processi modificati

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

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.

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

Per attivare e disattivare il blocco di processi modificati:

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. 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 nelle versioni di Windows a 64 bit e in Windows 8 e versioni successive. In Windows 8 e versioni successive questa operazione viene gestita automaticamente dalla tecnologia HIPS di Sophos Anti-Virus.
- Viene bloccato solamente il processo modificato. Al programma che modifica il processo non viene impedito l'accesso alla rete.

Attivare o disattivare i checksum

Per impostazione predefinita, il firewall utilizza i checksum per autenticare le applicazioni. Quando si autorizzano o bloccano applicazioni, queste ultime vengono automaticamente identificate dai loro checksum (i checksum possono anche essere aggiunti manualmente). Se un'applicazione non corrisponde a nessun checksum, viene bloccata.

Se questa opzione viene disabilitata, le applicazioni verranno riconosciute in base al loro nome file.

Per attivare o disattivare l'utilizzo dei checksum per l'autenticazione delle applicazioni:

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Nella scheda **Generale**, sotto **Blocco**, selezionare la casella di spunta **Utilizzo di checksum per l'autenticazione di applicazioni**.

 Copyright © Sophos Limited

Autorizzazione o blocco dei pacchetti IPv6

Per autorizzare o bloccare i pacchetti IPv6:

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Nella scheda **Generale**, sotto **Blocco**, selezionare o deselezionare la casella di spunta **Blocca pacchetti IPv6**.

Filtraggio dei messaggi ICMP

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

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 informazioni sui tipi di messaggi ICMP, consultare la sezione Definizione dei tipi di messaggi ICMP (pagina 129).

Per filtrare i messaggi ICMP:

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Nella scheda **ICMP**, selezionare la casella di spunta **Ing.** o **Usc.** per consentire i messaggi in entrata o uscita di un determinato tipo.

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 `ping`.
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.
Richiesta di rallentamento dell'origine	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.
Reindirizza messaggio	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	Inviato da un router quando un datagramma ha raggiunto il livello massimo di router attraverso cui può passare.
Problema di parametro	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**.

Regole del firewall

Regole globali

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

Regole delle 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.

Per informazioni sulle impostazioni relative alle regole predefinite globali e delle applicazioni, consultare l'articolo 57757 della knowledge base Sophos.

Ordine di applicazione delle regole

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

Per connessioni che *non* utilizzano raw socket, vengono verificate svariate regole, a seconda che la connessione sia verso un indirizzo di rete elencato nella scheda **LAN** o meno.

 Copyright © Sophos Limited

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

- Se l'indirizzo è stato contrassegnato come **Attendibile**, viene permesso tutto il traffico su tale connessione, senza ulteriori verifiche.
- Se l'indirizzo è stato contrassegnato come **NetBIOS**, viene permessa la condivisione di file e stampanti su qualsiasi connessione che rispetti i seguenti criteri:

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* è elencato nella scheda **LAN**, altre regole del firewall vengono verificate nel seguente ordine:

1. Tutto il traffico **NetBIOS** non consentito tramite la scheda **LAN** viene sottoposto alle seguenti procedure, a seconda delle impostazioni della casella di spunta **Blocca condivisione file e stampanti per altre reti**:
   - Se la casella è spuntata, il traffico è 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 di priorità 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**, l'utente deve decidere. Questa modalità non è disponibile in Windows 8 e versioni successive.

Nota
Se la modalità di funzionamento non è stata modificata, il firewall sarà in modalità **Blocca per impostazione predefinita**.

Rilevamento della rete locale

Nota
Questa funzionalità non è disponibile in Windows 8 e versioni successive.

È possibile assegnare regole del firewall alla rete locale di un computer.

All'avvio del firewall, questo definisce la rete locale del computer, e durante la sua esecuzione ne monitora gli eventuali cambiamenti. Se viene rilevata una qualsiasi modifica, il firewall aggiorna le regole della rete locale con l'intervallo di indirizzi della nuova rete locale.

Attenzione
si consiglia vivamente di procedere con cautela quando si utilizzano le regole di rete locale come parte di configurazioni secondarie. Se il computer è un laptop, e viene utilizzato all'esterno dell'ufficio, esiste la possibilità che si colleghi ad una rete sconosciuta. In tal caso, le regole del firewall nella configurazione secondaria che utilizzano la rete locale come indirizzo possono inavvertitamente consentire traffico sconosciuto.

Regole globali

Creazione di una regola globale

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

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 soggette a una regola specifica.

Per creare una regola globale:

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Regole globali**.
5. 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 globali non possono avere lo stesso nome.
7. Per applicare la regola prima delle regole dell'applicazione o del normale ordine di priorità delle regole globali, selezionare la casella di spunta **Regola con elevata priorità**.

   Per informazioni sull'ordine di priorità con cui vengono applicate le regole, consultare la sezione Ordine di applicazione delle regole (pagina 130).
8. Sotto **Selezionare gli eventi che saranno gestiti dalla regola**, selezionare le condizioni che la connessione deve rispettare affinché la regola venga applicata.
9. Sotto **Selezionare le azioni alle quali la regola reagirà**, selezionare **Consenti** o **Blocca**.
10. Effettuare una delle seguenti operazioni:

 Copyright © Sophos Limited

- 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 le regole TCP, che sono di stato per impostazione predefinita.

- Per consentire risposte intelligenti dal computer remoto in base alla connessione iniziale, selezionare **Ispezione di stato**.

  Nota
  Questa opzione è disponibile solo per le regole UDP e IP.

Nota
In Windows 8 e versioni successive, queste opzioni non sono applicabili, dal momento che viene sempre utilizzata la funzione **Ispezione di stato** e le **Connessioni concorrenti** non sono supportate.

11. Sotto **Descrizione della regola**, cliccare su un valore sottolineato. Per esempio, se si clicca sul link **TCP con stato** si apre la finestra di dialogo **Seleziona protocollo**.

Modifica di una regola globale

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

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

Per modifica una regola globale:

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Regole globali**.
5. Nell'elenco **Regola**, scegliere la regola che si desidera modificare.
6. Cliccare su **Modifica**.

   Per informazioni sulle impostazioni delle regole globali, consultare l'articolo 57757 della knowledge base.

Copia di una regola globale

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

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

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Regole globali**.
5. Nell'elenco **Regola**, scegliere la regola che si desidera copiare.
6. Cliccare su **Copia**.

Cancellazione di una regola globale

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Regole globali**.
5. Nell'elenco **Regola**, scegliere la regola che si desidera cancellare.
6. Cliccare su **Rimuovi**.

Modifica dell'ordine di applicazione delle regole globali

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

 Copyright © Sophos Limited

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. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Regole globali**.
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**.

Regole delle applicazioni

Creazione di una regola dell'applicazione

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

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

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Applicazioni**.
5. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
6. Nella finestra di dialogo **Regole applicazioni**, cliccare su **Aggiungi**.
7. Sotto **Nome della regola**, digitare il nome della regola.

   Il nome della regola deve essere unico all'interno dell'elenco delle regole. Due regole delle applicazioni non possono avere lo stesso nome, ma due applicazioni possono avere ciascuna una regola con lo stesso nome.
8. Sotto **Selezionare gli eventi che saranno gestiti dalla regola**, selezionare le condizioni che la connessione deve rispettare affinché la regola venga applicata.
9. Sotto **Selezionare le azioni alle quali la regola reagirà**, selezionare **Consenti** o **Blocca**.
10. 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 le regole TCP, che sono di stato per impostazione predefinita.

- Per consentire risposte intelligenti dal computer remoto in base alla connessione iniziale, selezionare **Ispezione di stato**.

  Nota
  Questa opzione è disponibile solo per le regole UDP e IP.

Nota
In Windows 8 e versioni successive, queste opzioni non sono applicabili, dal momento che viene sempre utilizzata la funzione **Ispezione di stato** e le **Connessioni concorrenti** non sono supportate.

11. Sotto **Descrizione della regola**, cliccare su un valore sottolineato. Per esempio, se si clicca sul link **TCP con stato** si apre la finestra di dialogo **Seleziona protocollo**.

Creazione di una regola delle applicazioni da un criterio firewall

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile creare una regola delle applicazioni direttamente da un criterio del firewall tramite le pagine di configurazione avanzata del criterio firewall.

Per creare una regola delle applicazioni da un criterio firewall:

1. Cliccare due volte sul criterio che si desidera modificare.
2. Nella pagina Benvenuti della procedura guidata per la **configurazione del criterio firewall**, cliccare sul pulsante **Criteri avanzati firewall**.
3. Nella finestra di dialogo **Criterio firewall**, cliccare su **Configura** di fianco al percorso per cui si desidera configurare il firewall.
4. Effettuare una delle seguenti operazioni:
   - Se si desidera aggiungere un'applicazione al criterio del firewall, nella finestra di dialogo che viene visualizzata, andare alla scheda **Applicazioni** e cliccare su **Aggiungi**.
   - Se si desidera consentire a un'applicazione di lanciare processi nascosti, andare alla scheda **Processi** e cliccare su **Aggiungi** nella parte in alto.
   - Se si desidera consentire a un'applicazione di accedere alla rete tramite raw socket, andare alla scheda **Processi** e cliccare su **Aggiungi** nella parte bassa.

   Viene visualizzata la finestra di dialogo **Criterio firewall - Aggiungi applicazione**.
5. Se si sta aggiungendo un'applicazione, nella casella **Tipo di evento**, scegliere se aggiungere un'applicazione modificata, nuova o un'applicazione per cui non è stata impostata alcuna regola delle applicazioni nel criterio del firewall.
6. Selezionare una voce per l'applicazione che si desidera aggiungere o a cui si desidera consentire il lancio di processi nascosti oppure l'utilizzo di raw socket, quindi cliccare su **OK**.
   L'applicazione viene aggiunta al criterio del firewall.

 Copyright © Sophos Limited

Se si è aggiunta un'applicazione nella scheda **Applicazioni**, tale applicazione viene aggiunta come affidabile. Se lo si desidera è possibile bloccarla o crearle una regola personalizzata.

Modifica di una regola delle applicazioni

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Applicazioni**.
5. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
6. Nella finestra di dialogo **Regole applicazioni**, cliccare su **Modifica**.
7. Sotto **Nome della regola**, digitare il nome della regola.

   Il nome della regola deve essere unico all'interno dell'elenco delle regole. Due regole delle applicazioni non possono avere lo stesso nome, ma due applicazioni possono avere ciascuna una regola con lo stesso nome.
8. Sotto **Selezionare gli eventi che saranno gestiti dalla regola**, selezionare le condizioni che la connessione deve rispettare affinché la regola venga applicata.
9. Sotto **Selezionare le azioni alle quali la regola reagirà**, selezionare **Consenti** o **Blocca**.
10. 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 le regole TCP, che sono di stato per impostazione predefinita.

    - Per consentire risposte intelligenti dal computer remoto in base alla connessione iniziale, selezionare **Ispezione di stato**.

      Nota
      Questa opzione è disponibile solo per le regole UDP e IP.

Nota
In Windows 8 e versioni successive, queste opzioni non sono applicabili, dal momento che viene sempre utilizzata la funzione **Ispezione di stato** e le **Connessioni concorrenti** non sono supportate.

11. Sotto **Descrizione della regola**, cliccare su un valore sottolineato. Per esempio, se si clicca sul link **TCP con stato** si apre la finestra di dialogo **Seleziona protocollo**.

Applicazione delle regole delle applicazioni predefinite

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Si tratta di una serie di regole delle applicazioni create da Sophos. Per aggiungere regole predefinite all'elenco di regole per un'applicazione:

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Applicazioni**.
5. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
6. Andare a **Aggiungi regole da quelle predefinite** e cliccare sulla regola predefinita.

Copia di una regola delle applicazioni

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

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

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Applicazioni**.
5. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
6. Nella finestra di dialogo **Regole applicazioni**, selezionare la regola che si desidera copiare e cliccare su **Copia**.

Copyright © Sophos Limited

Cancellazione di una regola delle applicazioni

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Applicazioni**.
5. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
6. Nella finestra di dialogo **Regole applicazioni**, selezionare la regola che si desidera rimuovere e cliccare su **Rimuovi**.

Modifica dell'ordine di applicazione delle regole delle applicazioni

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Le regole dell'applicazione 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 delle applicazioni:

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Applicazioni**.
5. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
6. Nella finestra di dialogo **Regole applicazioni**, all'interno dell'elenco **Regola**, cliccare sulla regola che si desidera spostare in alto o in basso nell'elenco.
7. Cliccare su **Sposta su** o **Sposta giù**.

Riconoscimento presenza

Il riconoscimento della presenza in rete è una funzionalità di Sophos Client Firewall che attribuisce una configurazione del firewall a ciascuna scheda di rete presente sul computer, a seconda dell'attuale posizione della scheda di rete stessa.

Lo scenario più consueto per l'utilizzo di tale funzionalità si presenta quando l'utente è in possesso di un laptop aziendale, e lavora dalla propria abitazione. Utilizza così due connessioni di rete allo stesso momento:

- Per il lavoro, si connette alla rete aziendale mediante un client VPN ed una **scheda di rete virtuale**.
- Per uso personale, si connette al proprio provider di servizi internet tramite un cavo di rete ed una **scheda di rete fisica**.

In questo scenario, occorre che la configurazione lavorativa venga applicata alla connessione aziendale virtuale, e che la configurazione non lavorativa (di solito più restrittiva) venga applicata alla connessione del provider di servizi Internet non lavorativo.

Nota
la configurazione non lavorativa richiederà che siano presenti abbastanza regole per consentire che venga stabilita la connessione aziendale "virtuale".

Impostazione del riconoscimento della presenza in rete

1. Definire l'elenco di indirizzi o domini gateway MAC dei propri percorsi primari. Di norma, si tratta delle proprie reti aziendali.
2. Creare la configurazione del firewall che verrà utilizzata per i propri percorsi primari. Di solito tale configurazione è meno restrittiva.
3. Creare una configurazione del firewall secondaria. Di solito tale configurazione è più restrittiva.
4. Selezionare una configurazione da applicare.

A seconda del metodo di rilevamento utilizzato, il firewall ottiene l'indirizzo DNS o gateway per ciascuna scheda di rete del computer, e le paragona all'elenco di indirizzi fornito.

- Se si verifica una corrispondenza fra uno degli indirizzi nell'elenco e l'indirizzo di una scheda di rete, a tale scheda viene assegnata la configurazione per il **percorso primario**.
- Se non si rileva alcuna corrispondenza fra gli indirizzi nell'elenco e quelli delle schede di rete, alla scheda viene assegnato il criterio per il **percorso secondario**.

Importante
La configurazione secondaria in un computer passa dalla modalità **Interattiva** a quella **Blocca per impostazione predefinita** quando si verificano entrambe le seguenti condizioni:

- Entrambi i percorsi sono attivi.
- La configurazione primaria *non è* interattiva.

Definizione dei percorsi primari

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Rilevamento percorso**.
5. Sotto **Metodo di rilevamento**, cliccare su **Configura** di fianco al metodo che si desidera utilizzare per definire i percorsi primari:

 Copyright © Sophos Limited

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.

6. Seguire le istruzioni sullo schermo.

Creazione di una configurazione secondaria

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Selezionare la casella di spunta **Aggiungi configurazione per percorso secondario**.

Impostare la configurazione secondaria. Per informazioni su come svolgere questa operazione, vedere Apertura delle pagine di configurazione avanzata (pagina 120).

Attenzione
Si consiglia vivamente di esercitare cautela quando si utilizzano le regole di sottorete locale come parte di configurazioni secondarie. Se il computer è un laptop, e viene utilizzato all'esterno dell'ufficio, esiste la possibilità che si colleghi ad una rete locale sconosciuta. In tale evenienza, le regole del firewall nella configurazione secondaria che utilizzano la rete locale come indirizzo possono inavvertitamente consentire traffico sconosciuto.

Selezione di una configurazione da applicare

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Nella scheda **Generale**, sotto **Percorso applicato**, cliccare su una delle seguenti opzioni:

Opzione	**Descrizione**
Applica la configurazione per il percorso rilevato	Il firewall applica la configurazione primaria o secondaria a ciascuna connessione di rete, a seconda delle impostazioni di rilevamento per il riconoscimento della presenza in rete (come descritto nella sezione Impostazione del riconoscimento della presenza in rete (pagina 140)).
Applica la configurazione per il percorso primario	Il firewall applica la configurazione primaria a tutte le connessioni di rete.
Applica la configurazione per il percorso secondario	Il firewall applica la configurazione secondaria a tutte le connessioni di rete.

Reportistica del firewall

Per impostazione predefinita, il firewall di un computer notifica cambiamenti di stato, eventi ed errori a Enterprise Console.

Cambiamenti di stato del firewall

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

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

Quando si lavora in modalità interattiva, la configurazione firewall potrebbe essere deliberatamente diversa dal criterio applicato da Enterprise Console. È quindi possibile decidere di **non** inviare la notifica di allarme "Diverso dal criterio" a Enterprise Console 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 (pagina 142).

Eventi firewall

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

È possibile evitare che il firewall riporti a Enterprise Console gli eventi.

Per ulteriori informazioni, consultare la sezione Disattivazione del rilevamento del traffico di rete sconosciuto (pagina 143).

Attivazione o disattivazione del rilevamento di modifiche locali

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

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

Nota
Questa opzione non è supportata in Windows 8 e versioni successive.

La disattivazione del rilevamento di modifiche locali blocca l'invio da parte del firewall di allarmi "diverso dal criterio" a Enterprise Console, in relazione a eventuali modifiche apportate a regole globali, applicazioni, processi o checksum. Si può scegliere questa opzione quando, ad esempio,

 Copyright © Sophos Limited

i computer operano in modalità interattiva, dal momento che si tratta di impostazioni modificabili tramite finestre di apprendimento.

Se nei 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. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Generale**.
5. Sotto **Reportistica**, effettuare una delle seguenti operazioni:
   - Per attivare il rilevamento di modifiche locali, selezionare 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 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**.

Disattivazione del rilevamento del traffico di rete sconosciuto

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile impedire che il firewall nei computer riporti traffico di rete sconosciuto a Enterprise Console. Il firewall considera il traffico sconosciuto se non rileva regole relative ad esso.

Per impedire che il firewall presente nei computer riporti traffico di rete sconosciuto a Enterprise Console.

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Generale**.
5. Sotto **Blocco**, selezionare la casella di spunta **Utilizzo di checksum per l'autenticazione delle applicazioni**.
6. Sotto **Reportistica**, deselezionare la casella di spunta **Segnala le applicazioni sconosciute e il traffico alla console di gestione**.

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 evitare che il firewall nei computer endpoint riporti errori a Enterprise Console:

1. Cliccare due volte sul criterio firewall che si desidera modificare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Under **Configurazioni**, cliccare su **Configura**, di fianco al percorso per cui si desidera configurare il firewall.
4. Cliccare sulla scheda **Generale**.
5. Sotto **Reportistica**, deselezionare la casella di spunta **Segnala errori alla console di gestione**.

Importazione o esportazione della configurazione del firewall

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazioni del criterio - firewall** per configurare i criteri del firewall.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Consente di importare o esportare le impostazioni generali e le regole del firewall come file di configurazione (*.conf). Utilizzare questa funzione per svolgere le seguenti operazioni:

- Eseguire backup e ripristino le configurazioni del firewall.
- Importare le regole di applicazione create in un computer ed utilizzarle per la creazione di un criterio per altri computer che eseguono le stesse applicazioni.
- Raccogliere le configurazioni create in diversi computer per la creazione di un criterio valido per uno o più gruppi di computer nella rete.

Per importare o esportare la configurazione del firewall:

1. Controllare quale criterio firewall è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Firewall** e poi ancora sul criterio che si desidera importare o esportare.
3. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
4. Nella finestra di dialogo **Criterio firewall**, nella scheda **Generale**, sotto **Gestione configurazione**, cliccare su **Importa** o **Esporta**.

7.3 Criterio del controllo applicazioni

Enterprise Console consente di rilevare e bloccare le "applicazioni controllate", ovvero applicazioni legittime che non rappresentano una minaccia per la sicurezza, ma il cui utilizzo sul posto di lavoro è ritenuto inappropriato. A tali applicazioni appartengono i client di messaggistica istantanea (IM), i client per il Voice over Internet Protocol (VoIP), i software per imaging digitale, i riproduttori multimediali o i plug-in dei browser.

 Copyright © Sophos Limited

Nota
questa opzione è valida soltanto per Sophos Endpoint Security and Control per Windows.

Le applicazioni possono essere bloccate o autorizzate per gruppi diversi di computer con grande flessibilità. Per esempio, il VoIP può essere disattivato per i computer desktop utilizzati in ufficio, ma autorizzato per i computer che si collegano in remoto.

L'elenco di applicazioni controllate viene fornito e aggiornato regolarmente da Sophos. Non è possibile aggiungere nuove applicazioni all'elenco, ma è possibile inviare a Sophos la richiesta di includere una nuova applicazione legittima che si desidera controllare all'interno della propria rete.

Per informazioni più dettagliate, consultare l'articolo 63656 della knowledge base.

Questa sezione spiega come selezionare le applicazioni da controllare nella rete e come impostare la scansione per la ricerca delle applicazioni controllate.

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- Per configurare un criterio di controllo delle applicazioni è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni sull'amministrazione basata sui ruoli, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Eventi del controllo applicazioni

Quando si verifica un evento di controllo applicazioni, per es. nella rete viene rilevata un'applicazione controllata, tale evento viene trascritto nel log eventi dell'applicazione controllata visibile da Enterprise Console. Per ulteriori informazioni, vedere Visualizzazione degli eventi del controllo applicazioni (pagina 196).

Il numero di computer con eventi che hanno superato una determinata soglia entro gli ultimi 7 giorni viene visualizzato nel pannello di controllo.

È inoltre possibile impostare allarmi da inviare a destinatari prescelti ogni qual volta si verifichi un evento di controllo applicazioni. Per ulteriori informazioni, vedere Impostazione di allarmi e messaggi del controllo applicazioni (pagina 190).

7.3.1 Selezione delle applicazioni che si desidera controllare

Se si utilizza l'amministrazione basata sui ruoli:

- Per configurare un criterio di controllo delle applicazioni è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per impostazione predefinita, tutte le applicazioni sono consentite. Per selezionare le applicazioni che si desidera controllare, procedere come segue.

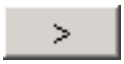
1. Controllare quale criterio di controllo applicazioni è utilizzato dal o dai gruppi di computer che si desidera configurare.

Vedere Criteri utilizzati da un dato gruppo (pagina 25).

2. Nel riquadro **Criteri**, cliccare due volte su **Controllo applicazioni**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criterio di controllo applicazioni**, cliccare sulla scheda **Autorizzazione**.
4. Selezionare un **Tipo applicazione**, per esempio **Condivisione file**.

   L'elenco completo delle applicazioni incluse nel gruppo è visualizzata nell'elenco **Autorizzate** sottostante.

   - Per bloccare un'applicazione, selezionarla e spostarla nell'elenco **Applicazioni bloccate** cliccare sul pulsante "Aggiungi".

   - Per bloccare qualsiasi nuova applicazione di quel tipo che Sophos aggiungerà in futuro, spostare **Tutte quelle aggiunte da Sophos in futuro** nell'elenco **Applicazioni bloccate**.
   - Per bloccare qualsiasi nuova applicazione di quel tipo in futuro, spostarle tutte dalla lista **Autorizzate** a quella **Bloccate**, cliccando sul pulsante "Aggiungi tutte".

5. Nella scheda **Scansione** della finestra di dialogo **Criterio di controllo applicazioni**, accertarsi che sia abilitata la scansione per la ricerca delle applicazioni controllate (Vedere Ricerca delle applicazioni che si desidera controllare (pagina 146) per informazioni dettagliate.) Cliccare su **OK**.

7.3.2 Ricerca delle applicazioni che si desidera controllare

Se si utilizza l'amministrazione basata sui ruoli:

- Per configurare un criterio di controllo delle applicazioni è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile configurare Sophos Endpoint Security and Control in modo che ricerchi in accesso le applicazioni che si desidera controllare sulla rete.

1. Controllare quale criterio di controllo applicazioni è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Controllo applicazioni**. Quindi cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo Criterio **di controllo applicazioni**.
3. Nella scheda **Scansione**, impostare le opzioni come segue.

   - Per abilitare la scansione in accesso, spuntare la casella **Abilita scansione in accesso**. Se si desidera rilevare le applicazioni senza bloccare l'accesso alle stesse, spuntare la casella **Rileva ma consenti l'esecuzione**.
   - Per abilitare la scansione su richiesta, spuntare la casella **Abilita scansione su richiesta e pianificata**.

Copyright © Sophos Limited

Nota
le impostazioni antivirus e HIPS dell'utente determinano quali file vengono esaminati (vale a dire le estensioni e le esclusioni).

Se si desidera rimuovere le applicazioni controllate individuate nei propri computer in rete, seguire le istruzioni in Disinstallazione delle applicazioni controllate che non si desidera utilizzare (pagina 147).

Nel caso che in un computer di un gruppo venga rilevata un'applicazione controllata, è possibile inviare allarmi a determinati utenti. Per istruzioni consultare la sezione Impostazione di allarmi e messaggi del controllo applicazioni (pagina 190).

7.3.3 Disinstallazione delle applicazioni controllate che non si desidera utilizzare

Prima di disinstallare le applicazioni controllate, accertarsi che la scansione in accesso per la ricerca di applicazioni controllate sia disabilitata. Questo tipo di scansione blocca i programmi utilizzati per installare e disinstallare le applicazioni, quindi potrebbe interferire con la disinstallazione.

È possibile rimuovere un'applicazione in due modi diversi:

- in ogni computer eseguire il programma di disinstallazione per il prodotto in questione. Di solito lo si può eseguire dal Pannello di controllo di Windows mediante Installazione applicazioni.
- Sul server, utilizzare il consueto script o tool di amministrazione per eseguire il programma di disinstallazione relativo a quel prodotto nei computer della rete.

Ora è possibile abilitare la scansione in accesso per la ricerca delle applicazioni controllate.

7.4 Criterio del controllo dati

Nota
Questa funzione non è inclusa in tutte le licenze. Se la si desidera utilizzare potrebbe essere necessario cambiare la propria licenza. Per ulteriori informazioni, vedere http://www.sophos.com/it-it/products/complete/comparison.aspx.

Il controllo dati consente di ridurre il rischio di perdita di dati accidentale dalle workstation monitorando e limitando il trasferimento di file contenenti dati sensibili. Ciò è possibile tramite la creazione di regole del controllo dei dati da aggiungere ai criteri del Controllo dati.

È possibile monitorare e controllare il trasferimento di file in determinati dispositivi di memorizzazione (per es. dispositivi di memorizzazione rimovibili o unità ottica) o tramite specifiche applicazioni (per es. e-mail client o browser web).

Per consentire di definire e distribuire rapidamente un criterio del controllo dei dati, SophosLabs mantiene aggiornata una libreria di definizioni di dati sensibili (Content Control List). Maggiore attenzione da parte di questa libreria è rivolta ai dati che possono portare all'identificazione personale, fermo restando l'interesse rivolto ad altre strutture di dati comuni. È possibile utilizzare Content Control List in Enterprise Console, come descritto in questa sezione.

7.4.1 Funzionamento del controllo dati

Il controllo dati identifica la perdita di informazioni accidentale, generalmente causata dall'impiego errato di dati sensibili da parte dei dipendenti. Per esempio, un utente invia un file contenente dati sensibili tramite e-mail basata sul web.

Il controllo dati consente di monitorare e controllare il trasferimento di file da computer a dispositivi di memorizzazione e applicazioni connesse a Internet.

- **Dispositivi di memorizzazione** il controllo dati intercetta tutti i file copiati su dispositivi di memorizzazione monitorati utilizzando Esplora risorse (incluso il desktop di Windows). Tuttavia, i salvataggi diretti effettuati dall'interno di applicazioni come Microsoft Word, o i trasferimenti eseguiti utilizzando il prompt di comando, non sono intercettati.

  È possibile forzare tutti i trasferimenti su dispositivi di memorizzazione monitorati da eseguire usando Esplora risorse, mediante l'azione **Consenti il trasferimento se l'utente ha accettato e registra evento** o l'azione **Blocca trasferimento e registra evento**. In ogni caso, qualsiasi tentativo di salvare direttamente dall'interno di un'applicazione o di trasferire i file utilizzando il prompt di comando viene bloccato dal controllo dati e sul desktop è visualizzato un allarme per l'utente, in cui si richiede l'utilizzo di Esplora risorse per completare il trasferimento.

  Quando un criterio del controllo dati contiene solo regole con l'azione **Consenti trasferimento file e registra evento**, i salvataggi diretti dall'interno delle applicazioni e i trasferimenti mediante il prompt di comando non sono intercettati. Questo comportamento consente agli utenti di utilizzare dispositivi di memorizzazione senza limitazioni. Tuttavia, gli eventi di controllo dati sono comunque registrati per i trasferimenti effettuati utilizzando Esplora risorse.

  Nota
  Questa limitazione non si applica al monitoraggio dell'applicazione.

- **Applicazioni:** Per assicurarsi che vengano monitorati solo i file caricati dagli utenti, alcuni percorsi dei file di sistema vengono esclusi dal monitoraggio del controllo dati. Ciò consente di ridurre in modo rilevante il rischio che si generino eventi del controllo dati dovuti ad applicazioni che aprono file di configurazione, piuttosto che a utenti che caricano file.

  Importante
  se si verificano eventi errati generati da un'applicazione che apre file di configurazione, tale problema può essere risolto aggiungendo esclusioni di percorsi personalizzate o configurando una regola del controllo dati. Per ulteriori informazioni, consultare l'articolo 113024 della knowledge base Sophos.

  Nota
  Le esclusioni di scansione in accesso non sono sempre applicabili al controllo dati.

In quali occasioni il controllo dati utilizza le esclusioni di scansione in accesso?

A seconda di dove vengano copiati o trasferiti i file, il controllo dati può tenere in considerazione o meno le esclusioni di scansione in accesso che sono state impostate nel criterio antivirus e HIPS.

Copyright © Sophos Limited

Il controllo dati **adopera** le esclusioni di scansione in accesso quando i file vengono caricati o allegati con un'applicazione monitorata, ad esempio un client di posta, un browser web, oppure un client di messaggistica istantanea (IM). Per informazioni sulla configurazione di esclusioni per la scansione in accesso, consultare la sezione Esclusione di oggetti dalla scansione in accesso (pagina 87).

Importante
Se dalla scansione in accesso sono stati esclusi i file remoti, il controllo dati non sottoporrà a scansione i dati che provengono da un percorso di rete e che sono allegati o caricati su un'applicazione monitorata, come ad es. e-mail o browser web. Vedere anche Il controllo dati non esegue la scansione dei file caricati o allegati (pagina 228).

Il controllo dati **non adopera** le esclusioni di scansione in accesso quando i file vengono copiati o trasferiti usando Esplora risorse. Per cui le esclusioni non verranno applicate se, ad esempio, vengono copiati file su un dispositivo di archiviazione, ad es. una chiave USB, oppure se vengono copiati o trasferiti file su un percorso di rete. Tutti i file verranno sottoposti a scansione, anche se i file remoti sono stati esclusi dalla scansione in accesso.

Nota
Se vengono copiati o trasferiti file di **archivio** su un percorso di rete, il processo potrebbe richiedere diverso tempo, ad esempio più di un minuto per 100 MB di dati, a seconda della connessione di rete. Ciò è dovuto al fatto che la scansione dei file di archivio richiede più tempo della scansione dei file non compressi.

Criteri del controllo dati

Il controllo dati consente di monitorare e controllare il trasferimento di file tramite la definizione di criteri del controllo dati e la loro applicazione ai gruppi di computer nella rete.

Importante
Il controllo dati non è supportato in Windows 2008 Server Core e deve essere disabilitato nei computer che eseguono tale sistema operativo. Per escludere dalla scansione del controllo dati i computer Windows 2008 Server Core, collocarli in un gruppo che possieda un criterio del controllo dati avente la scansione del controllo dati disabilitata. Per ulteriori informazioni, vedere Attivazione o disattivazione del controllo dati (pagina 153).

I criteri del controllo dati comprendono una o più regole indicanti le condizioni che verranno rilevate e le azioni che saranno svolte se la regola è soddisfatta. Una regola del controllo dati può essere inclusa in più criteri.

Quando un criterio del controllo dati contiene più regole, un file che soddisfa *una* di tali regole viola il criterio.

Condizioni della regola del controllo dati

Le condizioni della regola del controllo dati comprendono: destinazione, nome file ed estensione, tipo di file o contenuto del file.

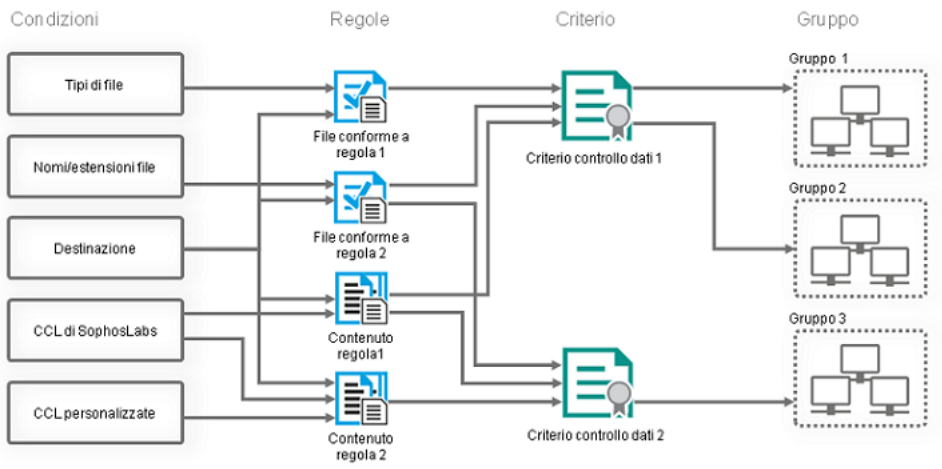
La destinazione comprende i dispositivi (per es. dispositivi di memorizzazione rimovibili, quali unità USB flash) e le applicazioni (per es. browser Internet e client e-mail).

La corrispondenza del contenuto del file viene definita tramite Content Control List. Si tratta della descrizione di dati strutturati basata su XML . SophosLabs fornisce un ricco set di Content Control List utilizzabile all'interno delle regole del controllo dati.

Per ulteriori informazioni sulle regole del controllo dati e sulle condizioni applicate ai file, consultare la sezione Regole del controllo dati (pagina 151).

Per ulteriori informazioni su Content Control List (CCL) che definiscono il contenuto dei file, consultare la sezione Content Control List (pagina 151).

Controllo dati



Azioni delle regole del controllo dati

Quando il controllo dati rileva tutte le condizioni specificate nella regola, tale regola risulta soddisfatta e il controllo dati svolge l'azione indicata nella regola e registra l'evento. È possibile specificare una delle seguenti azioni:

- Consenti il trasferimento del file e l'accesso all'evento
- Consenti il trasferimento se l'utente ha accettato e accedi all'evento
- Blocca trasferimento e l'accesso all'evento

Se un file soddisfa due regole del controllo dati che specificano due diverse azioni, viene applicata quella più restrittiva. Le regole del controllo dati che bloccano il trasferimento di file hanno priorità su quelle che consentono il trasferimento previo consenso dell'utente. Le regole che consentono il trasferimento previo consenso dell'utente hanno priorità su quelle che consentono il trasferimento della rete.

Per impostazione predefinita, quando la regola è soddisfatta e il trasferimento del file viene bloccato o è richiesta conferma da parte dell'utente, viene visualizzato un messaggio nel desktop del computer. La regola che viene soddisfatta è inclusa nel messaggio. Ai messaggi standard relativi al consenso dell'utente o al blocco del trasferimento dati è possibile aggiungere messaggi personalizzati. Per ulteriori informazioni, consultare la sezione Impostazione di allarmi e messaggi del controllo dati (pagina 190).

Copyright © Sophos Limited

7.4.2 Regole del controllo dati

Le regole del controllo dati indicano le condizioni che il controllo dei dati rileverà, le azioni da intraprendere ogni volta venga soddisfatta una regola e i file da escludere dalla scansione per il controllo dati.

È possibile creare le proprie regole o utilizzare il modello di regole del controllo dati fornito. Sophos fornisce un numero di regole del controllo dati preconfigurate da utilizzare senza modificarle o adattandole alle proprie esigenze. Tali regole sono fornite solo come esempio e non vengono aggiornate.

Esistono due tipi di regole del controllo dati: *regola di corrispondenza file* e *regola dei contenuti*.

regole di corrispondenza file

Una *regola di corrispondenza file* specifica quale azione intraprendere se un utente cerca di trasferire un file avente il nome o tipo di file specificato (categoria tipo file true, per es. foglio elettronico) a una destinazione specificata; per es. viene bloccato il trasferimento di database su dispositivi di memorizzazione rimovibili.

Il controllo dati include le definizioni del tipo file true per oltre 150 diversi formati di file. Di tanto in tanto potrebbero venire aggiunti nuovi tipi di file true. I tipi appena aggiunti verranno automaticamente inseriti nelle regole di controllo dati che utilizzano la relativa categoria di tipo file true.

I tipi di file non coperti dalla definizione "tipo file true" possono essere identificati tramite le estensioni del file.

Regole dei contenuti

Una *regola dei contenuti* è una 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 tutti le Content Control List presenti nella regola.

7.4.3 Content Control List

Content Control List (CCL) è un set di condizioni che descrivono il contenuto di file strutturati. Content Control List può descrivere un solo tipo di dati (per es. un indirizzo postale o numero di codice fiscale) o una combinazione di vari tipi di dati (per es. il nome di un progetto simile al termine "confidenziale").

È possibile utilizzare i *Content Control List di SophosLabs* forniti da Sophos o creare i propri Content Control List.

I Content Control List di SophosLabs forniscono definizioni specifiche per comuni tipi di dati finanziari o che possono portare all'identificazione personale, per esempio numeri di carte di credito, codici fiscali, indirizzi postali o di posta elettronica. I Content Control List di SophosLabs utilizzano tecniche avanzate, quali checksum, per aumentare il livello di precisione con cui vengono rilevati i dati sensibili.

Non è possibile modificare i Content Control List di SophosLabs; è invece possibile inviare una richiesta a Sophos di creare un nuovo Content Control List da parte di SophosLabs. Per informazioni dettagliate, consultare l'articolo 51976 della knowledge base del supporto Sophos.

Nota
i caratteri a byte doppio (per es. i caratteri giapponesi o cinesi) non sono ufficialmente supportati dalla versione corrente delle Content Control List. È comunque possibile inserire caratteri a byte doppio nell'editor di Content Control List.

Impostazione della quantità per i Content Control List di SophosLabs

La maggior parte dei Content Control List di SophosLabs sono in possesso di una *quantità* assegnata.

Una *quantità* rappresenta il volume di informazioni chiave da reperire nel file prima di eseguire il match con il Content Control List. È possibile modificare la quantità relativa a un Content Control List di SophosLabs all'interno di una regola di contenuto che comprende un determinato Content Control List.

Utilizzando la quantità, è possibile calibrare le regole del controllo dei dati ed evitare il blocco di documenti che non contengono informazioni sensibili (ad es. un documento contenente un indirizzo postale o uno o due numeri di telefono, magari nell'intestazione, nella firma o nel piè di pagina). Se si utilizza come criterio della ricerca un solo indirizzo di posta, migliaia di documenti potrebbero soddisfare questa regola ed innescare un evento del controllo dati. Tuttavia, se si desidera evitare la perdita di un elenco clienti, si vorrà rilevare il trasferimento solo di documenti contenenti, per es., più di 50 indirizzi di posta. Possono invece sussistere casi in cui è consigliabile ricercare una sola istanza di contenuto, per es. il numero di una carta di credito.

7.4.4 Eventi del controllo dei dati

Quando si verifica un evento del controllo dati, per esempio se si esegue la copia di un file contenente dati sensibili in un'unità USB flash, l'evento viene inviato a Enterprise Console e può essere visualizzato in **Controllo dati - Visualizzatore eventi**. Se l'evento è registrato anche a livello locale nel computer, può essere visualizzato, se in possesso delle autorizzazioni adeguate, in Sophos Endpoint Security and Control.

Nota
un computer può inviare a Enterprise Console un massimo di 50 eventi del controllo dati all'ora. Tutti gli eventi vengono registrati a livello locale nel computer.

Nella finestra di dialogo **Data Control - Visualizzatore eventi**, è possibile utilizzare filtri per visualizzare solo gli eventi a cui si è interessati. È inoltre possibile esportare in un file l'elenco di eventi del controllo dati. Per dettagli, consultare le sezioni Eventi del controllo dei dati (pagina 152) e Esportazione dell'elenco eventi in un file (pagina 205).

Il numero di computer con eventi del controllo dati che hanno superato una determinata soglia negli ultimi 7 giorni viene visualizzato nel pannello di controllo. Per informazioni sull'impostazione del livello di soglia, consultare la sezione Pannello di controllo (pagina 4).

È inoltre possibile impostare allarmi da inviare a destinatari prescelti ogni qual volta si verifichi un evento del controllo dati. Per ulteriori informazioni, vedere Impostazione di allarmi e messaggi del controllo dati (pagina 190).

 Copyright © Sophos Limited

7.4.5 Attivazione o disattivazione del controllo dati

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - controllo dati** per configurare il criterio del controllo dati.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Per impostazione predefinita, il controllo dati è disattivato e non è specificata alcuna regola che monitori o limiti il trasferimento di file nella rete.

Per attivare il controllo dati:

1. Controllare quale criterio del controllo dati è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Controllo dati**. Quindi cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio di controllo dati**.
3. Nella scheda **Regole criteri**, selezionare la casella di spunta **Abilita la scansione del controllo dati**.
4. Cliccare sul pulsante **Aggiungi regola**. Nella finestra di dialogo **Gestione regole del controllo dati**, selezionare le regole che si desidera aggiungere al criterio e cliccare su **OK**.

> **Importante**
> Se non vengono aggiunti criteri sul controllo dati, il controllo dati non esegue il monitoraggio o la restrizione al trasferimento dei file finché ciò non viene effettuato.

Se, in un secondo tempo, si desidera disabilitare la scansione del controllo dati, deselezionare la casella di spunta **Abilita la scansione del controllo dati**.

7.4.6 Creazione di una regola "file che soddisfa la regola"

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Personalizzazione del controllo dati** per poter creare o modificare le regole di controllo dati.
- È necessario essere in possesso dei diritti di **Impostazione criterio - controllo dati** per poter impostare i criteri del controllo dati.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per una panoramica sulle regole "file che soddisfa la regola", consultare la sezione Regole del controllo dati (pagina 151).

Per creare una regola "file che soddisfa la regola" ed aggiungerla al criterio del controllo dati:

1. Controllare quale criterio del controllo dati è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).

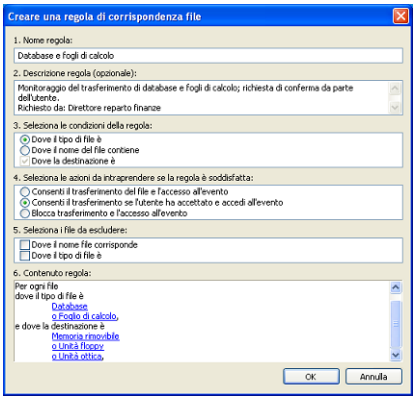
In alternativa, è possibile creare una regola dal menu **Strumenti** per poi aggiungerla al criterio o ai criteri. Nel menu **Strumenti**, andare a **Gestisci controllo dati**, cliccare poi su **Regole controllo dati** e svolgere i passaggi da 4 a 10.

2. Nel riquadro **Criteri**, cliccare due volte su **Controllo dati**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criterio del controllo dati**, nella scheda **Regole criteri**, assicurarsi che la casella di spunta **Abilita la scansione del controllo dati** sia selezionata, e cliccare su **Aggiungi regola**.
4. Nella finestra di dialogo **Gestione regole del controllo dati**, cliccare sul pulsante **Aggiungi regola "file che soddisfa la regola"**.
5. Nella finestra di dialogo **Creare una regola di corrispondenza file** , sotto **Nome regola**, digitare il nome della regola.
6. Sotto **Descrizione regola (opzionale)**, inserire, se lo si desidera, la descrizione della regola.
7. Sotto **Seleziona le condizioni della regola**, selezionare le condizioni per la regola.

   La condizione di destinazione è preselezionata e deve essere inclusa nella regola.

   Per impostazione predefinita, tutti i tipi di file vengono scansionati. Se si desidera scansionare solo determinati tipi di file, selezionare **Dove il tipo di file è**. È poi possibile impostare questa condizione secondo quanto descritto al passaggio 10.
8. Sotto **Seleziona le azioni da intraprendere se la regola è soddisfatta**, selezionare l'azione.
9. Se si desidera escludere alcuni file dalla scansione per il controllo dati, sotto **Seleziona i file da escludere**, selezionare la casella di spunta **Dove il nome file corrisponde** o **Dove il tipo di file è**.
10. Sotto **Contenuto regola**, cliccare su ogni valore sottolineato ed impostare le condizioni della regola.
    Per esempio, se si clicca su **Seleziona la destinazione**, viene visualizzata la finestra di dialogo **Soddisfa la condizione tipo di destinazione** in cui è possibile selezionare dispositivi e/o applicazioni a cui si desidera limitare il trasferimento dei dati.

    Selezionare o inserire le credenziali per ciascun valore sottolineato.



    Cliccare su **OK**.

    La nuova regola viene visualizzata nella finestra di dialogo **Gestione regole del controllo dati**.
11. Per aggiungere la regola a un criterio, selezionare la casella di spunta di fianco al nome della regola e cliccare su **OK**.
    La regola viene aggiunta al criterio del controllo dati.

È possibile impostare allarmi e messaggi da inviare all'utente ogni qual volta una regola del criterio del controllo dati venga soddisfatta. Vedere Impostazione di allarmi e messaggi del controllo dati (pagina 190).

 Copyright © Sophos Limited

7.4.7 Creazione di una regola dei contenuti

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Personalizzazione del controllo dati** per poter creare o modificare le regole di controllo dati e i Content Control List.
- È necessario essere in possesso dei diritti di **Impostazione criterio - controllo dati** per poter impostare i criteri del controllo dati.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per una panoramica relativa alle regole dei contenuti e alle Content Control List, consultare la sezione Regole del controllo dati (pagina 151).

Per creare una regola dei contenuti ed aggiungerla al criterio del controllo dati:

1. Controllare quale criterio del controllo dati è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).

   In alternativa, è possibile creare una regola dal menu **Strumenti** per poi aggiungerla al criterio o ai criteri. Nel menu **Strumenti**, andare a **Gestisci controllo dati**, cliccare poi su **Regole controllo dati** e svolgere i passaggi da 4 a 13.
2. Nel riquadro **Criteri**, cliccare due volte su **Controllo dati**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criterio del controllo dati**, nella scheda **Regole criteri**, assicurarsi che la casella di spunta **Abilita la scansione del controllo dati** sia selezionata, e cliccare su **Aggiungi regola**.
4. Nella finestra di dialogo **Gestione regole del controllo dati**, cliccare sul pulsante **Aggiungi regola contenuti**.
5. Nella finestra di dialogo **Crea una regola di contenuto**, sotto **Nome regola**, digitare il nome della regola.
6. Sotto **Descrizione regola (opzionale)**, inserire, se lo si desidera, la descrizione della regola.
7. Sotto **Seleziona le condizioni della regola**, il contenuto e la destinazione del file sono già selezionati. Per le regole di contenuto è necessario impostare entrambe le condizioni.
8. Sotto **Seleziona le azioni da intraprendere se la regola è soddisfatta**, selezionare l'azione.
9. Se si desidera escludere alcuni file dalla scansione per il controllo dati, sotto **Seleziona i file da escludere**, selezionare la casella di spunta **Dove il nome file corrisponde** o **Dove il tipo di file è**.
10. Sotto **Contenuto regola**, cliccare sul valore sottolineato "seleziona il contenuto del file".
11. Nella finestra di dialogo **Gestione Content Control List**, selezionare i Content Control List da includere nel criterio.

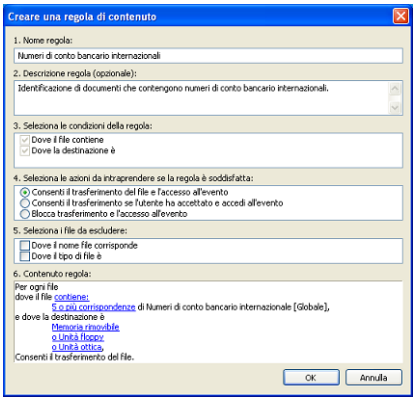
    Se si desidera aggiungere i Content Control List dei SophosLabs, selezionarne uno per ciascun paese richiesto.

    Consiglio
    Evitare di selezionare un Content Control List globale, se non si richiede supporto per tutti i paesi. Procedere piuttosto selezionando solamente i Content Control List corrispondenti ai paesi desiderati. Così facendo si diminuiranno significativamente i tempi di scansione, e si ridurrà il rischio di riscontri indesiderati e involontari.

Se si desidera creare una nuova Content Control List, consultare la sezione Creazione e modifica di un semplice Content Control List (pagina 158) o Creazione o modifica di un Content Control List avanzato (pagina 159).

Cliccare su **OK**.

12. Se si desidera modificare la quantità assegnata a un Content Control List di SophosLabs, sotto **Contenuto regola**, cliccare sul valore "quantità" ("*n* o più corrispondenze") sottolineato che si desidera modificare. Nella finestra di dialogo **Editor quantità**, inserire una nuova quantità. Per ulteriori informazioni, consultare la sezione Content Control List (pagina 151).
13. Sotto **Contenuto regola**, selezionare o inserire condizioni per i restanti valori sottolineati.



Cliccare su **OK**.

La nuova regola viene visualizzata nella finestra di dialogo **Gestione regole del controllo dati**.

14. Per aggiungere la regola a un criterio, selezionare la casella di spunta di fianco al nome della regola e cliccare su **OK**.
La regola viene aggiunta al criterio del controllo dati.

È possibile impostare allarmi e messaggi da inviare all'utente ogni qual volta una regola del criterio del controllo dati venga soddisfatta. Vedere Impostazione di allarmi e messaggi del controllo dati (pagina 190).

7.4.8 Aggiunta di una regola del controllo dati al criterio

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criteri - controllo dati** per svolgere questa operazione.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per aggiungere una regola del controllo dati a un criterio:

1. Controllare quale criterio del controllo dati è utilizzato dal o dai gruppi di computer che si desidera configurare.
Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Controllo dati**. Quindi cliccare due volte sul criterio che si desidera modificare.
Viene visualizzata la finestra di dialogo **Criterio di controllo dati**.
3. Nella scheda **Regole criteri**, cliccare su **Aggiungi regola**.
Viene visualizzata la finestra di dialogo **Gestione regole del controllo dati**.
4. Selezionare le regole che si desidera aggiungere al criterio e cliccare su **OK**.

 Copyright © Sophos Limited

7.4.9 Rimozione di una regola del controllo dati da un criterio

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criteri - controllo dati** per svolgere questa operazione.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per rimuovere una regola del controllo dati da un criterio:

1. Controllare quale criterio del controllo dati è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Controllo dati**. Quindi cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio di controllo dati**.
3. Nella scheda **Operazione pianificata**, selezionare la regola che si desidera rimuovere e cliccare su **Rimuovi regola**.

7.4.10 Esclusione di file o tipi di file dal controllo dati

Se si utilizza un'amministrazione basata sui ruoli, per poter escludere file dal controllo dati, è necessario essere in possesso dei diritti di **Personalizzazione controllo dati**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile escludere file e tipi di file impostando esclusioni all'interno di una regola del controllo dati.

Per escludere un file o tipo di file dal controllo dati, escluderlo all'interno di una regola che abbia la priorità più alta (vale a dire, che indica l'azione più restrittiva).

Per escludere file o tipi di file dal controllo dati:

1. Nel menu **Strumenti**, andare a **Gestisci controllo dati** e poi cliccare su **Regole controllo dati**.
2. Nella finestra di dialogo **Gestione regole del controllo dati**, selezionare la regola che si desidera modificare e cliccare su **Modifica**, oppure creare una nuova regola cliccando sul pulsante **Aggiungi file soddisfacenti regola** o **Aggiungi regola contenuti**.
3. Per escludere file dal controllo dati, nella finestra di dialogo **Editor regola**, sotto **Seleziona i file da escludere**, selezionare la casella di spunta **Dove il nome file corrisponde**.
4. Sotto **Contenuto regola**, cliccare sul valore sottolineato per specificare i nomi dei file esclusi.
5. Nella finestra di dialogo **Escludi la condizione nome file**, cliccare su **Aggiungi** e specificare i nomi dei file che si desidera escludere.

   È possibile utilizzare i caratteri jolly * e ?.

   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.
6. Per escludere i tipi di file dal controllo dati, nella finestra di dialogo **Editor regola**, sotto **Seleziona i file da escludere**, selezionare la casella di spumta **Dove il tipo di file è**.

7. Sotto **Contenuto regola**, cliccare sul valore sottolineato per specificare i tipi dei file esclusi.
8. Nella finestra di dialogo **Escludi la condizione nome file**, selezionare i tipi di file che si desidera escludere e cliccare su **OK**.

7.4.11 Importazione o esportazione di una regola del controllo dati

Se si utilizza l'amministrazione basata sui ruoli, per poter importare o esportare una regola del controllo dati, è necessario possedere i diritti di **Personalizzazione controllo dati**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Le regole del controllo dati possono essere importate in o esportate da Enterprise Console sotto forma di file XML.

Per importare o esportare una regola del controllo dati:

1. Nel menu **Strumenti**, andare a **Gestisci controllo dati** e poi cliccare su **Regole controllo dati**.
2. Nella finestra di dialogo **Gestione regole del controllo dati**, cliccare su **Importa** o **Esporta**.
   - Se si desidera importare una regola, nella finestra di dialogo **Importa**, andare alla regola che si desidera importare, selezionarla e cliccare su **Apri**.
   - Se si desidera esportare una regola, nella finestra di dialogo **Esporta**, selezionare la destinazione del file, digitare il nome file e cliccare su **Salva**.

7.4.12 Creazione e modifica di un semplice Content Control List

Se si utilizza un'amministrazione basata sui ruoli, per poter creare una Content Control List, è necessario essere in possesso dei diritti di **Personalizzazione controllo dati**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per una panoramica relativa alle Content Control List, consultare la sezione Content Control List (pagina 151).

Per creare e modificare una Content Control List:

1. Nel menu **Strumenti**, andare a **Gestisci controllo dati** e poi cliccare su **Elenchi controllo contenuti di controllo dati**.
2. Nella finestra di dialogo **Gestione Content Control List** cliccare su **Aggiungi** per creare un nuovo Content Control List, oppure selezionare il Content Control List esistente e cliccare su **Modifica**.
3. Nella finestra di dialogo **Aggiungi Content Control List**, nel campo **Nome**, inserire il nome del Content Control List.
4. Nel campo **Descrizione**, inserire, se lo si desidera, una descrizione del Content Control List.
5. Se si desidera aggiungere tag o modificare quelli già assegnati al Content Control List, cliccare su **Cambia** di fianco al campo **Tag**.

   È possibile assegnare tag per definire il tipo e la regione di appartenenza del Content Control List, qualora applicabili.
6. Nella finestra di dialogo **Modifica i tag della Content Control List**, nell'elenco **Tag disponibili**, selezionare i tag che si desidera assegnare e spostarli nell'elenco **Tag selezionati**. Cliccare su **OK**.
7. Nella sezione **Cerca contenuto corrispondente**, selezionare una condizione di ricerca (“Uno di questi termini”, “Tutti questi termini” oppure “Questa frase”) ed inserire i termini della ricerca che si desidera applicare al documento, separati da uno spazio. Cliccare su **OK**.

 Copyright © Sophos Limited

Nota
la ricerca non fa distinzione tra maiuscole e minuscole.

Nelle Content Control List semplici non sono supportate le virgolette. Utilizzare la condizione “Questa frase” per cercare una frase esatta.

Per creare espressioni più complesse, utilizzare l'editor avanzato di Content Control List, secondo quanto descritto in Creazione o modifica di un Content Control List avanzato (pagina 159).

Il nuovo content control list viene visualizzato nella finestra di dialogo **Gestione Content Control List**.

Esempi

Condizione di ricerca	Esempio	Descrizione
Soddisfa almeno un termine	segreto confidenziale	Corrisponde ai documenti che contengono "confidenziale" o "segreto".
Soddisfa tutti i termini	progetto confidenziale	Corrisponde ai documenti che contengono sia "progetto" che "confidenziale".
Corrispondenza esatta	solo per uso interno	Corrisponde ai documenti che contengono la frase "solo per uso interno".

È ora possibile aggiungere la nuova Content Control List a una regola di contenuto.

7.4.13 Creazione o modifica di un Content Control List avanzato

Se si utilizza un'amministrazione basata sui ruoli, per poter creare una Content Control List, è necessario essere in possesso dei diritti di **Personalizzazione controllo dati**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Per una panoramica relativa alle Content Control List, consultare la sezione Content Control List (pagina 151).

È possibile creare una Content Control List comprensiva di una o più espressioni regolari e di trigger score. Per far ciò, utilizzare l'editor avanzato.

Per creare o modificare un Content Control List tramite l'editor avanzato:

1. Nel menu **Strumenti**, andare a **Gestisci controllo dati** e poi cliccare su **Elenchi controllo contenuti di controllo dati**.
2. Nella finestra di dialogo **Gestione Content Control List** cliccare su **Aggiungi** per creare un nuovo Content Control List, oppure selezionare il Content Control List esistente e cliccare su **Modifica**.
3. Nella finestra di dialogo **Aggiungi Content Control List**, nel campo **Nome**, inserire il nome del Content Control List.
4. Nel campo **Descrizione**, inserire, se lo si desidera, una descrizione del Content Control List.

5. Se si desidera aggiungere tag o modificare quelli già assegnati al Content Control List, cliccare su **Cambia** di fianco al campo **Tag**.

   È possibile assegnare tag per definire il tipo e la regione di appartenenza del Content Control List, qualora applicabili.
6. Nella finestra di dialogo **Modifica i tag della Content Control List**, nell'elenco **Tag disponibili**, selezionare i tag che si desidera assegnare e spostarli nell'elenco **Tag selezionati**. Cliccare su **OK**.
7. Cliccare sul pulsante **Avanzate**.
8. Nella scheda **Avanzate**, cliccare su **Crea** per creare una nuova espressione, oppure selezionare un'espressione esistente e cliccare su **Modifica**.
9. Nella finestra di dialogo **Content Control List - Avanzate**, inserire un'espressione regolare di Perl 5.

   Per la descrizione delle espressioni regolari di Perl 5, consultare la documentazione Perl o visitare il sito http://www.boost.org/doc/libs/1_34_1/libs/regex/doc/syntax_perl.html.
10. Nel campo **Score espressione**, inserire il numero che verrà aggiunto allo score totale per una Content Control List ogni qual volta venga soddisfatta l'espressione regolare.
11. Nel campo **Conteggio massimo**, inserire un numero massimo di corrispondenze per le espressioni regolari da conteggiare per raggiungere lo score totale.
    Per esempio, un'espressione regolare avente score di 5 e il conteggio massimo di 2 può essere aggiunta al valore massimo di 10 allo score totale del Content Control List. Se un'espressione viene rilevata 3 volte, aggiunge comunque 10 allo score totale.

    Cliccare su **OK**.
12. Ripetere i passaggi da 5 a 11, se si desiderano aggiungere più espressioni regolari al Content Control List.
13. Nel campo **Trigger score**, inserire il numero di volte in cui si deve verificare la corrispondenza di un'espressione regolare prima che il Content Control List venga soddisfatto.

    Per esempio, un Content Control List che ha il trigger score di 8 e consiste di 3 espressioni (A, B e C) aventi i seguenti score e conteggi massimi:

Espressione	Score	Conteggio massimo
Espressione A	5	2
Espressione B	3	1
Espressione C	1	5

    Questo Content Control List risulta soddisfatto se il controllo dati rileva 2 corrispondenze dell'espressione A o 1 dell'espressione A e 1 dell'espressione B oppure una dell'espressione B e 5 dell'espressione C.

    Cliccare su **OK**.

Il nuovo content control list viene visualizzato nella finestra di dialogo **Gestione Content Control List**.

Esempio espressione regolare

```
(?i)\b[a-ceghj-pr-tw-z][a-ceghj-npr-tw-z]\s?\d{2}\s?\d{2}\s?\d{2}\s?
[abcd]?\b
```


Copyright © Sophos Limited

Questa espressione regolare corrisponde a numeri di codice fiscale (National Insurance) per il Regno Unito, come ad esempio AA 11 11 11 A.

(?i)	Fa in modo che la corrispondenza non distingua tra maiuscole e minuscole.
\b	Corrisponde al limite tra carattere alfanumerico e non.
[a-ceghj-npr-tw-z]	Corrisponde a un qualsiasi carattere nella gamma di caratteri (da A a C, E, G, H, da J a P, da N R a T, da W a Z).
?	Corrisponde all'elemento precedente nessuna o una volta.
\s?	Corrisponde a uno spazio bianco nessuna o una volta.
\d{2}	Corrisponde a due caratteri.
[abcd]	Corrisponde a un qualsiasi carattere singolo dell'elenco (A, B, C o D).

È ora possibile aggiungere la nuova Content Control List a una regola di contenuto.

7.4.14 Importazione o esportazione di un Content Control List

Se si utilizza l'amministrazione basata sui ruoli, per poter importare o esportare una Content Control List, è necessario possedere i diritti di **Personalizzazione controllo dati**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Le Content Control List possono essere importate in o esportata da Enterprise Console sotto forma di file XML. È possibile condividere le Content Control List fra i prodotti Sophos che le supportano.

Nota
Le Content Control List di SophosLabs non possono essere esportate.

Per importare o esportare una Content Control List:

1. Nel menu **Strumenti**, andare a **Gestisci controllo dati** e poi cliccare su **Elenchi controllo contenuti di controllo dati**.
2. Nella finestra di dialogo **Gestione Content Control List**, cliccare su **Importa** o **Esporta**.
   - Se si desidera importare un Content Control List, nella finestra di dialogo **Importa**, andare al Content Control List che si desidera importare, selezionarlo e cliccare su **Apri**.
   - Se si desidera esportare un Content Control List, nella finestra di dialogo **Esporta**, selezionare la destinazione del file, digitare il nome file e cliccare su **Salva**.

7.5 Criterio del controllo dispositivi

Nota
Questa funzione non è inclusa in tutte le licenze. Se la si desidera utilizzare potrebbe essere necessario cambiare la propria licenza. Per ulteriori informazioni, vedere http://www.sophos.com/it-it/products/complete/comparison.aspx.

Importante
Sophos Device Control non va installato insieme a un eventuale software di controllo dei dispositivi prodotto da terzi.

Device control consente di impedire agli utenti l'utilizzo nei loro computer di dispositivi hardware esterni non autorizzati, strumenti di memorizzazione rimovibili e tecnologie di connessione wireless. Ciò riduce in modo significativo il rischio di perdite accidentali di dati e limita le possibilità degli utenti di introdurre software dall'esterno dell'ambiente di rete.

I dispositivi di memorizzazione rimovibili, le unità disco ottico e le unità floppy disk possono essere impostate per fornire accesso in sola lettura.

Utilizzando il controllo dispositivi è inoltre possibile ridurre notevolmente il rischio di bridging di rete tra una rete aziendale e una rete non aziendale. La modalità **Block Bridged** è disponibile sia per i dispositivi wireless che per i modem. La modalità funziona disabilitando le schede di rete wireless o modem quando un computer è collegato a una rete fisica (solitamente, mediante una connessione Ethernet). Quando il computer è scollegato dalla rete fisica, le schede di rete wireless o modem vengono riabilitate direttamente.

Per impostazione predefinita, il controllo dispositivi è disattivato e tutti i dispositivi sono consentiti.

Se si desidera attivare il controllo dispositivi per la prima volta, si consiglia di:

- Selezionare i tipi di dispositivo da controllare.
- Rilevare i dispositivi senza bloccarli.
- Utilizzare gli eventi del controllo dispositivi per stabilire quali tipi di dispositivo bloccare e quali, se del caso, rendere esenti.
- Rilevare e bloccare i dispositivi o consentire l'accesso in sola lettura ai dispositivi di memorizzazione.

Per ulteriori informazioni sulle impostazioni consigliate per il controllo dispositivi, consultare la *Guida all'impostazione dei criteri di Sophos Enterprise Console*.

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - controllo dispositivo** per configurare il criterio del controllo dispositivi.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

7.5.1 Eventi del controllo dispositivi

Quando si verifica un evento del controllo dispositivi, per esempio viene bloccato un dispositivo di memorizzazione rimovibile, tale evento viene inviato a Enterprise Console e può essere visualizzato nella finestra di dialogo **Device Control - Visualizzatore eventi**.

Nota
Se le unità disco ottico vengono impostate su "Sola lettura", gli eventi di queste unità disco non verranno inviati a Enterprise Console e non saranno registrati localmente nei log. Questa opzione previene la compilazione di report di eventi indesiderati.

 Copyright © Sophos Limited

Nella finestra di dialogo **Controllo dispositivi - Visualizzatore eventi**, è possibile utilizzare filtri per visualizzare solo gli eventi a cui si è interessati. Vi è anche l'opzione di esportare in un file l'elenco di eventi del controllo dispositivi. Per dettagli, consultare le sezioni Eventi del controllo dispositivi (pagina 162) e Esportazione dell'elenco eventi in un file (pagina 205).

È possibile utilizzare gli eventi del controllo dispositivi per aggiungere esenzioni relative a determinati dispositivi o modelli di dispositivo ai criteri del controllo dispositivi. Per ulteriori informazione sull'esportazione di dispositivi, consultare la sezione Esenzione di un dispositivo da un singolo criterio (pagina 167) o Esenzione di un dispositivo da tutti i criteri (pagina 166).

Il numero di computer con eventi del controllo dispositivi che hanno superato una determinata soglia negli ultimi 7 giorni viene visualizzato nel pannello di controllo. Per informazioni sull'impostazione del livello di soglia, consultare la sezione Configurazione del pannello di controllo (pagina 48).

È inoltre possibile impostare allarmi da inviare a destinatari prescelti ogni qual volta si verifichi un evento di controllo dispositivi. Per ulteriori informazioni, vedere Impostazione di allarmi e messaggi per il controllo dispositivi (pagina 192).

7.5.2 Tipi di dispositivi che possono essere controllati

Device Control consente di bloccare i seguenti tipi di dispositivi: *memorizzazione*, *rete*, *short range e media*.

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 cifratura basata su hardware)

Per un elenco dei dispositivi di memoria rimovibili sicuri supportati, consultare l'articolo 63102 della knowledge base Sophos .

Consiglio
Utilizzando la categoria dispositivo di memoria rimovibile sicuro, è possibile utilizzare facilmente i dispositivi di memoria rimovibile sicuri supportati, mentre vengono bloccati quelli non sicuri.

Rete

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

Per le interfacce di rete, è anche possibile selezionare la modalità **Block bridged**, che consente di ridurre significativamente il rischio di bridging di rete tra una rete aziendale e una rete non aziendale. La modalità funziona disabilitando le schede di rete wireless o modem quando un computer è collegato a una rete fisica (solitamente, mediante una connessione Ethernet). Quando il computer è scollegato dalla rete fisica, le schede di rete wireless o modem vengono riabilitate direttamente.

Short range

- Interfacce Bluetooth
- Infrarossi (Interfaccia infrarossi IrDA)

Device Control blocca interfacce e dispositivi, sia interni che esterni. Per esempio, un criterio che blocca le interfacce Bluetooth bloccherà:

- L'interfaccia Bluetooth incorporata in un computer
- Qualsiasi scheda Bluetooth USB inserita nel computer.

Supporti

- MTP/PTP

  Sono inclusi telefoni cellulari, tablet, fotocamere digitali, lettori multimediali ed altri dispositivi che possono essere collegati a computer tramite Media Transfer Protocol (MTP) o Picture Transfer Protocol (PTP).

7.5.3 Selezione dei tipi di dispositivo da controllare

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - controllo dispositivo** per modificare il criterio del controllo dispositivi.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Importante
le connessioni Wi-Fi non vanno bloccate nei computer che sono gestiti da Enterprise Console tramite Wi-Fi.

1. Controllare quale criterio del controllo dispositivi è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Controllo dispositivi**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criterio del controllo dei dispositivi**, nella scheda **Configurazione**, sotto **Memorizzazione**, selezionare il tipo di dispositivo di memorizzazione che si desidera controllare.
4. Cliccare sulla colonna **Stato** di fianco al tipo di dispositivo e successivamente cliccare sulla freccia dell'elenco a discesa che viene visualizzato. Selezionare il tipo di accesso che si desidera consentire.

   Per impostazione predefinita, i dispositivi hanno accesso completo. Per quanto riguarda i dispositivi di memorizzazione rimovibili, le unità disco ottico e le unità floppy disk, è possibile cambiare il tipo di accesso e selezionare “Bloccato” o “Sola lettura”. Per i dispositivi di memorizzazione rimovibili selezionare "Bloccato".
5. Sotto **Rete**, selezionare il tipo di dispositivo di rete che si desidera bloccare.
6. Cliccare sulla colonna **Stato** di fianco al tipo di dispositivo di rete e successivamente cliccare sulla freccia dell'elenco a discesa che viene visualizzato.

 Copyright © Sophos Limited

- Selezionare “Bloccato” se si desidera bloccare il tipo di dispositivo.
- Selezionare “Blocca bridging” se si desidera impedire il bridging di rete tra una rete aziendale e una rete non aziendale. Il tipo di dispositivo viene bloccato quando un computer è collegato a una rete fisica (solitamente, mediante una connessione Ethernet). Quando il computer è scollegato dalla rete fisica, il dispositivo viene riabilitato.

7. Sotto **Short range**, selezionare il tipo di dispositivo short range che si desidera bloccare. Nella colonna **Stato** accanto al tipo di dispositivo, selezionare “Bloccato”.

   Cliccare su **OK**.
8. Per bloccare i supporti che si collegano al computer tramite Media Transfer Protocol (MTP) o Picture Transfer Protocol (PTP), come per esempio telefonini, tablet, fotocamere digitali o lettori multimediali, sotto **Media**, selezionare **MTP/PTP**. Nella colonna **Stato** selezionare “Bloccato”.

7.5.4 Rilevamento dei dispositivi senza bloccarli

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - controllo dispositivo** per modificare il criterio del controllo dispositivi.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile rilevare dispositivi senza bloccarli. Ciò risulta utile se in futuro si desidera eseguire il blocco di dispositivi, ma per prima cosa si vuole rilevare ed esentare i dispositivi utili.

Per rilevare dispositivi senza bloccarli, abilitare la scansione del controllo dispositivi in un criterio del controllo dispositivi e attivare la modalità *solo rilevamento*. Cambiare lo stato dei dispositivi da rilevare impostandolo su “Bloccato”. Ciò genererà eventi relativi ai dispositivi utilizzati nel computer nel caso in cui il criterio venga violato, ma i dispositivi non verranno bloccati.

Per informazioni sulla visualizzazione di eventi del controllo dispositivi, consultare la sezione Eventi del controllo dispositivi (pagina 162).

Per rilevare i dispositivi senza bloccarli:

1. Controllare quale criterio del controllo dispositivi è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Controllo dispositivi**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criterio del controllo dei dispositivi**, nella scheda **Configurazione**, selezionare **Abilita la scansione del controllo dispositivi**.
4. Selezionare **Rileva, ma non bloccare i dispositivi**.
5. Se non è stato ancora fatto, cambiare lo stato dei dispositivi da rilevare impostandolo su “Bloccato” (Per ulteriori informazioni, vedere Selezione dei tipi di dispositivo da controllare (pagina 164).)

   Cliccare su **OK**.

7.5.5 Rilevamento e blocco dei dispositivi

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - controllo dispositivo** per modificare il criterio del controllo dispositivi.

- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

1. Controllare quale criterio del controllo dispositivi è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Controllo dispositivi**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criterio del controllo dei dispositivi**, nella scheda **Configurazione**, selezionare la casella di spunta **Abilita la scansione del controllo dispositivi**.
4. Deselezionare la casella di spunta **Rileva, ma non bloccare i dispositivi**.
5. Se non è stato ancora fatto, cambiare lo stato dei dispositivi da bloccare impostandolo su “Bloccato”. (Per ulteriori informazioni, vedere Selezione delle applicazioni che si desidera controllare (pagina 145).)

   Cliccare su **OK**.

7.5.6 Esenzione di un dispositivo da tutti i criteri

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - controllo dispositivo** per modificare il criterio del controllo dispositivi.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile esentare un dispositivo da tutti i criteri, compreso quello predefinito. L'esenzione verrà quindi aggiunta a tutti i nuovi criteri che verranno creati.

È possibile esentare un'istanza di dispositivo (“Solo questo dispositivo”) o un modello di dispositivo specifico (“Tutti i dispositivi con ID modello”). È imperativo non impostare più esenzioni per lo stesso modello a livello di ID modello e istanza del dispositivo. Se vengono definite entrambe le esenzioni, il livello dell'istanza del dispositivo avrà priorità.

Per esentare un dispositivo da tutti i criteri del controllo dispositivi:

1. Dal menu **Eventi**, cliccare su **Eventi controllo dispositivi**.
   Si apre la finestra di dialogo **Controllo dispositivi - Visualizzatore eventi**.
2. Se si desidera visualizzare solo determinati eventi, nel riquadro **Criteri di ricerca**, impostare i filtri adeguati e cliccare su **Cerca** per visualizzare tali eventi.

   Per ulteriori informazioni, consultare la sezione Eventi del controllo dispositivi (pagina 162).
3. Selezionare la voce del dispositivo che si desidera esentare dai criteri e cliccare su **Esporta dispositivo**.

   Viene visualizzata la finestra di dialogo **Esenta dispositivo**. Sotto **Dettagli dispositivo**, vengono visualizzati tipo, ID modello e ID dispositivo. Sotto **Dettagli dell'esenzione**, **Ambito**, viene visualizzata la dicitura "Tutti i criteri".

 Copyright © Sophos Limited

Nota
se non è presente alcun evento per il dispositivo che si desidera esentare, per es. l'unità CD o DVD integrale del computer, andare al computer che contiene il dispositivo e, in Gestione periferiche, abilitare il dispositivo (per accedere a Device Manager, cliccare col tasto destro del mouse su **Risorse del computer**, cliccare su **Gestione** e successivamente su **Gestione periferiche**.) Ciò genererà un nuovo evento “blocco” che apparirà nella finestra di dialogo **Device Control - Visualizzatore eventi**. È poi possibile esentare il dispositivo secondo quanto descritto in precedenza.

4. Scegliere se si desidera esentare solo tale dispositivo o tutti i dispositivi presenti nell'ID modello.
5. Scegliere se si desidera consentire al dispositivo pieno accesso o accesso solo in lettura.
6. Nel campo **Commento**, se lo si desidera inserire un commento. Per esempio, è possibile indicare chi ha richiesto l'esenzione.
7. Cliccare su **OK**.

7.5.7 Esenzione di un dispositivo da un singolo criterio

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - controllo dispositivo** per modificare il criterio del controllo dispositivi.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile esentare un determinato dispositivo da un criterio del controllo dispositivi.

È possibile esentare un'istanza di dispositivo (“Solo questo dispositivo”) o un modello di dispositivo specifico (“Tutti i dispositivi con ID modello”). È imperativo non impostare più esenzioni per lo stesso modello a livello di ID modello e istanza del dispositivo. Se vengono definite entrambe le esenzioni, il livello dell'istanza del dispositivo avrà priorità.

Per esentare un dispositivo da un singolo criterio:

1. Controllare quale criterio del controllo dispositivi è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Controllo dispositivi**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criterio del controllo dei dispositivi**, nella scheda **Configurazione**, cliccare su **Aggiungi esenzione**.
   Si apre la finestra di dialogo **Controllo dispositivi - Visualizzatore eventi**.
4. Se si desidera visualizzare solo determinati eventi, nel riquadro **Criteri di ricerca**, impostare i filtri adeguati e cliccare su **Cerca** per visualizzare tali eventi.

   Per ulteriori informazioni, consultare la sezione Eventi del controllo dispositivi (pagina 162).
5. Selezionare la voce del dispositivo che si desidera esentare dal criterio e cliccare su **Esporta dispositivo**.

   Viene visualizzata la finestra di dialogo **Esenta dispositivo**. Sotto **Dettagli dispositivo**, vengono visualizzati tipo, ID modello e ID dispositivo. Sotto **Dettagli dell'esenzione**, **Ambito**, viene visualizzata la dicitura “Solo questo dispositivo”.

Nota
se non è presente alcun evento per il dispositivo che si desidera esentare, per es. l'unità CD o DVD integrale del computer, andare al computer che contiene il dispositivo e, in Gestione periferiche, abilitare il dispositivo (per accedere a Device Manager, cliccare col tasto destro del mouse su **Risorse del computer**, cliccare su **Gestione** e successivamente su **Gestione periferiche**.) Ciò genererà un nuovo evento “blocco” che apparirà nella finestra di dialogo **Device Control - Visualizzatore eventi**. È poi possibile esentare il dispositivo secondo quanto descritto in precedenza.

6. Scegliere se si desidera esentare solo tale dispositivo o tutti i dispositivi presenti nell'ID modello.
7. Scegliere se si desidera consentire al dispositivo pieno accesso o accesso solo in lettura.
8. Nel campo **Commento**, se lo si desidera inserire un commento. Per esempio, è possibile indicare chi ha richiesto l'esenzione.
9. Cliccare su **OK**.

7.5.8 Visualizzazione o modifica dell'elenco dei dispositivi da esentare

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - controllo dispositivo** per modificare il criterio del controllo dispositivi.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per visualizzare o modificare l'elenco dei dispositivi da esentare:

1. Controllare quale criterio del controllo dispositivi è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Controllo dispositivi**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criterio del controllo dei dispositivi**, nella scheda **Configurazione**, selezionare il tipo di dispositivo per cui si desidera visualizzare le esenzioni, per es. unità ottica. Cliccare su **Visualizza esenzione**.
   Viene visualizzata la finestra di dialogo **Esenzioni di <tipo di dispositivo>**. Se un'esenzione è valida per tutti i dispositivi aventi una determinata ID modello, il campo **ID dispositivo** è vuoto.
4. Se si desidera modificare l'elenco dei dispositivi da esentare, svolgere una delle seguenti operazioni:
   - Se si desidera aggiungere un'esenzione, cliccare su **Aggiungi**. Per ulteriori informazioni, consultare la sezione Esenzione di un dispositivo da un singolo criterio (pagina 167).
   - Se si desidera modificare un'esenzione, selezionare l'esenzione e cliccare su **Modifica**. Modificare le impostazioni nella finestra di dialogo **Esenta dispositivo** secondo necessità.
   - Se si desidera rimuovere un'esenzione, selezionare il dispositivo da esentare e cliccare su **Rimuovi**.

     Ciò consentirà di rimuovere tutti i dispositivi da esentare dal criterio che si sta modificando. Se si desidera rimuovere il dispositivo da altri criteri, ripetere i passaggi qui descritti per ogni criterio.

 Copyright © Sophos Limited

7.6 Criteri blocco rimozione

Il blocco rimozione consente di impedire a malware noto e a utenti non autorizzati (amministratori locali e utenti con conoscenze tecniche limitate) la disinstallazione del software di sicurezza Sophos o la sua disabilitazione attraverso 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 una scansione alla ricerca di minacce e comportamenti sospetti (Per ulteriori informazioni, vedere Criterio antivirus e HIPS (pagina 80).)

Dopo aver abilitato la protezione e aver creato una password del blocco rimozione, un membro del gruppo SophosAdministrator che non conosce la password non sarà in grado di:

- Riconfigurare le impostazioni della scansione in accesso o del rilevamento di comportamenti sospetti in Sophos Endpoint Security and Control.
- Disabilitazione del blocco rimozione
- Disinstallare i componenti di Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate, o Sophos Remote Management System).

Se si desidera che SophosAdministrators svolga queste operazioni, è necessario fornire la password blocco rimozione, in modo tale che possano, per prima cosa, essere autenticate col blocco rimozione .

Il blocco rimozione non ha alcuna ripercussione sui gruppi SophosUsers e SophosPowerUsers. Quando il blocco rimozione è attivo, sarà comunque possibile eseguire tutte le operazioni normalmente autorizzate, senza bisogno di immettere la password del blocco rimozione.

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- Per configurare un criterio blocco rimozione occorre avere il diritto **Impostazione dei criteri - blocco rimozione.**
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Eventi del blocco rimozione

Quando si verifica un evento del blocco rimozione, per esempio viene impedito un tentativo non autorizzato di disinstallare Sophos Anti-Virus da un computer, l'evento viene trascritto nel log eventi visualizzabile tramite Enterprise Console. Per ulteriori informazioni, vedere Visualizzazione degli eventi del blocco rimozione (pagina 199).

Esistono due tipi di eventi del blocco rimozione:

- Per gli eventi di autenticazione del blocco rimozione riusciti, viene riportato il nome dell'utente autenticato e l'orario dell'autenticazione.
- Nel caso si tentativi di sabotaggio falliti vengono riportati i nomi dei componenti o dei prodotti Sophos oggetto di attacco, l'orario del tentativo e i dettagli dell'utente responsabile di tale tentativo.

Copyright © Sophos Limited

7.6.1 Attivare e disattivare il blocco rimozione

Se si utilizza l'amministrazione basata sui ruoli:

- Per configurare un criterio blocco rimozione occorre avere il diritto **Impostazione dei criteri - blocco rimozione.**
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Per attivare e disattivare il blocco rimozione

1. Controllare quale criterio relativo al blocco rimozione è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri,** cliccare due volte su **blocco rimozione**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criteri del blocco rimozione**, mettere o togliere la spunta nella casella **Attiva blocco rimozione**.

   Se si desidera attivare il blocco rimozione per la prima volta, cliccare su **Imposta** sotto la casella **Password**. Immettere e confermare una nuova password nella finestra di dialogo **Password del blocco rimozione**.

   Consiglio
   Si consiglia di utilizzare una password di almeno otto caratteri, che contenga numeri e lettere maiuscole e minuscole.

7.6.2 Cambiamento della password del blocco rimozione

Per cambiare la password del blocco rimozione

1. Controllare quale criterio relativo al blocco rimozione è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri,** cliccare due volte su **blocco rimozione**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criterio del blocco rimozione**, cliccare su **Cambia** sotto la casella **Password**. Immettere e confermare una nuova password nella finestra di dialogo **Password blocco rimozione**.

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

Copyright © Sophos Limited

7.6.3 Informazioni sul blocco rimozione avanzato

Il blocco rimozione avanzato si basa sulle funzionalità del blocco rimozione. Abilitando il blocco rimozione avanzato, le seguenti azioni risulteranno bloccate per Sophos Anti-Virus, Sophos AutoUpdate, Sophos Management Communication System, Sophos Remote Management System e Sophos Endpoint Defense:

- Arresto dei servizi dall'interfaccia utente Servizi
- Terminazione dei servizi dall'interfaccia utente Gestione attività
- Modifica della configurazione dei servizi dall'interfaccia utente Servizi
- Arresto dei servizi/modifica della configurazione dei servizi dalla riga di comando
- Disinstallazione
- Reinstallazione
- Terminazione dei processi dall'interfaccia utente Gestione attività
- Eliminazione o modifica di file o cartelle protetti
- Eliminazione o modifica di chiavi di registro di sistema protette

Importante
Per attivare il blocco rimozione avanzato, il blocco rimozione deve essere abilitato. Se il blocco rimozione non è abilitato, il blocco rimozione avanzato sarà automaticamente disattivato.

7.6.4 Impostazioni del blocco rimozione avanzato

1. Nel riquadro **Criteri,** cliccare due volte su **blocco rimozione**. Quindi cliccare due volte sul criterio che si desidera modificare.
2. Nella finestra di dialogo **Criterio blocco rimozione**, verificare che la casella di spunta **Attiva blocco rimozione** sia selezionata e successivamente cliccare sulla casella di spunta **Attiva blocco rimozione avanzato**.
3. Se si sta effettuando una nuova installazione o un upgrade, nella finestra di dialogo **Criterio del blocco rimozione**, cliccare su **Imposta** nel riquadro **Password**.

   Se il blocco rimozione è già attivato, cliccare su **Modifica** nel riquadro **Password**. Immettere e confermare una nuova password nella finestra di dialogo **Password del blocco rimozione**.

   Nota
   Questa password sarà identica sia per il blocco rimozione che per il blocco rimozione avanzato. Quando è abilitato, il blocco rimozione avanzato sostituisce le azioni del blocco rimozione. È per questo motivo che occorre modificare la password quando la password del blocco rimozione è già stata impostata.

   Si consiglia di utilizzare una password diversa per ciascun criterio.

7.7 Criterio patch

Nota
Questa funzione non è inclusa in tutte le licenze. Se la si desidera utilizzare potrebbe essere necessario cambiare la propria licenza. Per ulteriori informazioni, vedere http://www.sophos.com/it-it/products/complete/comparison.aspx.

Enterprise Console consente di verificare che i computer abbiano sempre installate le patch di protezione più recenti.

SophosLabs fornisce livelli di valutazione delle minacce che consentono di determinare i problemi critici relativi alle patch, per poterli risolvere il più rapidamente possibile. I livelli di minaccia forniti da SophosLabs prendono in considerazione i fenomeni più recenti e possono quindi non corrispondere ai livelli di pericolosità stabiliti dai fornitori.

Prima di utilizzare le patch, è necessario installare l'agente delle patch nei computer in rete in modo tale che questi possano eseguire la verifica delle patch e comunicare informazioni relative al loro stato a Enterprise Console. È possibile installarlo utilizzando la **Procedura guidata per la protezione dei computer**. Vedere Protezione automatica dei computer (pagina 45).

Le informazioni contenute in questa sezione presuppongono che l'agente delle patch sia installato.

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - patch** per configurare i criteri relativi alle patch.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni sull'amministrazione basata sui ruoli, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

7.7.1 Funzionamento della verifica patch

Nel criterio predefinito la verifica patch è disabilitata. Una volta abilitata la verifica delle patch, i computer daranno inizio a tale operazione. Possono essere necessari diversi minuti. Le verifiche successive verranno eseguite in base all'intervallo impostato nel criterio, per impostazione predefinita con cadenza giornaliera.

Nota
Se i computer eseguono una verifica prima che Enterprise Console abbia scaricato per la prima volta i dati sulle patch da Sophos, il Visualizzatore eventi patch non restituirà alcun risultato. Il download può richiedere molte ore. Per verificare che sia concluso, controllare il campo relativo agli **aggiornamenti delle patch** nel **Eventi > Eventi verifica patch**.

Se, per qualsiasi motivo, l'agente delle patch non riesce ad aggiornarsi da Enterprise Console, continuerà comunque a verificare i computer facendo riferimento ai rilevamenti delle patch scaricati in precedenza.

 Copyright © Sophos Limited

La verifica delle patch di protezione riguarda solo il software installato nei computer. Se viene rilasciata una nuova patch in sostituzione di un precedente, la verifica delle patch non cercherà più quella precedente. Solo quella nuova verrà vaultata e verificata.

Cosa si intende per patch di sostituzione

Se un fornitore rilascia una patch che sostituisca quella già esistente, la patch nuova viene denominata patch di sostituzione. La patch precedente viene invece denominata patch sostituita.

Sophos consiglia di installare la patch di sostituzione per mantenere i computer aggiornati.

Esempio: se si cerca un "virusX" e si scopre che nella patch P01 è disponibile la soluzione per tale tipo di virus, ma tale patch è sostituita dalla patch P02, Sophos consiglia di installare la P02.

7.7.2 Eventi relativi alla verifica delle patch

Nel caso di evento della verifica delle patch, per esempio un computer non è in possesso di una determinata patch, tale evento viene inviato a Enterprise Console e può essere visualizzato in **Verifica patch- Visualizzatore eventi**.

In **Verifica patch - Visualizzatore eventi**, è possibile applicare filtri per visualizzare solo gli eventi a cui si è interessati. È inoltre possibile esportare in un file l'elenco di eventi di verifica patch. Per dettagli, consultare le sezioni Eventi verifica patch (pagina 199) e Esportazione dell'elenco eventi in un file (pagina 205).

7.7.3 Attivazione e disattivazione della verifica delle patch

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - patch** per configurare i criteri relativi alle patch.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per attivare o disattivare la verifica delle patch:

1. Verificare quale criterio delle patch è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri,** cliccare due volte su **Patch**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criterio patch**, selezionare o meno la casella **Attiva blocco rimozione** e cliccare su **OK**.

7.7.4 Selezione dell'intervallo di verifica delle patch

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - patch** per configurare i criteri relativi alle patch.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per impostare l'intervallo di verifica delle patch:

1. Verificare quale criterio delle patch è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri,** cliccare due volte su **Patch**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criterio patch**, cliccare sulla freccia del menu a discesa relativo al campo **Ricerca patch mancanti** e selezionare l'intervallo adeguato. Cliccare su **OK**.

   Per eseguire la verifica in base all'intervallo prescelto, nel criterio deve essere abilitata la verifica delle patch.

7.8 Criterio del controllo web

Nota
Questa funzione non è inclusa in tutte le licenze. Se la si desidera utilizzare potrebbe essere necessario cambiare la propria licenza. Per ulteriori informazioni, vedere http://www.sophos.com/it-it/products/complete/comparison.aspx.

Per impostazione predefinita, il criterio del controllo web è disattivato in Enterprise Console Selezionando **Abilita il controllo web** è possibile scegliere una delle seguenti opzioni del criterio:

- **Controllo siti web inappropriati**: opzione del controllo web di base che include 14 categorie di siti web essenziali. Pensata per bloccare l'accesso degli utenti a siti web per cui si può essere perseguibili legalmente. Per ulteriori informazioni, consultare la sezione Controllo siti web inappropriati (pagina 175).
- **Controllo web completo**: Questa opzione consente di applicare un criterio globale a più di 50 categorie di siti web. È richiesta la presenza di una Sophos Web Appliance, Sophos Management Appliance o di un'appliance Sophos UTM (versione 9.2 o successiva) per poter effettuare la sincronizzazione degli endpoint che consente di distribuire gli aggiornamenti dei criteri e raccogliere i dati sull'attività Web. Per ulteriori informazioni, consultare la sezione Controllo web completo (pagina 180).

Quando si utilizza l'opzione Controllo di siti web inappropriati, è possibile modificare i criteri del controllo web esistenti o crearne di nuovi. Per ulteriori informazioni, consultare la sezione Creazione di un criterio (pagina 30). È possibile impostare le diverse categorie di siti web in modo tale che se ne esegua il «blocco», vengano inviati «avvisi» o ne venga «consentito» l'accesso. Lo stato del controllo web e gli eventi web vengono visualizzati in Enterprise Console. Per ulteriori informazioni sull'evento web, consultare Visualizzazione degli eventi web (pagina 203).

Se invece si utilizza l'opzione Controllo web completo, Enterprise Console richiede il percorso della Web Appliance, appliance UTM o della Management Appliance da cui viene configurato il filtro del controllo web completo, oltre alla chiave condivisa che consente la comunicazione tra appliance e Enterprise Console. Quando il criterio completo del controllo web è selezionato, la maggior parte delle operazioni di reportistica e monitoraggio vengono trasferite all'appliance; mentre la scansione e verifica dei siti web viene eseguita dal filtro URL di Sophos Endpoint Security and Control (Protezione web (pagina 102)) e i risultati vengono visualizzati come eventi web in Enterprise Console.

Per ulteriori informazioni sul controllo web, consultare la *Panoramica sul controllo web per endpoint*.

 Copyright © Sophos Limited

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - controllo web** per modificare il criterio del controllo web.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni sull'amministrazione basata sui ruoli, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

7.8.1 Controllo siti web inappropriati

Nota
Questa funzione non è inclusa in tutte le licenze. Se la si desidera utilizzare potrebbe essere necessario personalizzare la propria licenza. Per ulteriori informazioni, vedere http://www.sophos.com/it-it/products/complete/comparison.aspx.

Applicando ai siti web questo controllo di base, è possibile filtrare l'attività web degli utenti in base a 14 categorie di siti web. A ogni categoria è applicata un'azione predefinita (v. descrizione Categorie dei siti web (pagina 176)), ma, se necessario, è possibile selezionarne una differente, secondo quanto descritto nella sezione Selezione di un'azione da applicare a una categoria di siti web (pagina 178).

È possibile bloccare l'accesso da parte degli utenti a siti web soggetti a restrizioni. Si genera un evento che viene mostrato all'utente e inviato a Enterprise Console.

In alternativa, avvisare gli utenti tramite notifica qualora cerchino di accedere a siti web controllati; anche se l'utente non accede effettivamente al sito, viene generato un evento di avviso. Se l'utente non tiene conto dell'avviso ricevuto e procede nell'accedere al sito, si genera un secondo evento che viene inviato a Enterprise Console.

Nota
sebbene entrambi i siti HTTP e HTTPS siano soggetti a filtro in tutti i browser web supportati, le notifiche inviate all'utente sono differenti se l'URL del sito web è HTTP o HTTPS. Nel caso di siti HTTP, gli utenti ricevono notifica per i siti soggetti all'azione «Blocca» o «Avvisa». Nel caso di siti HTTPS, gli utenti ricevono notifica solo per i siti soggetti all'azione «Blocca»; tali notifiche vengono visualizzate nell'area di notifica di Windows e nel formato di fumetto suggerimento. Le azioni «Avvisa» per i siti HTTPS non vengono né visualizzate all'utente né registrate. Gli utenti possono quindi accedere alla pagina web desiderata e l'evento viene registrato come soggetto all'azione «Procedi» in Enterprise Console.

Se si sceglie l'azione «Consenti» per una determinata categoria di siti web, gli utenti potranno accedere a tutti i siti appartenenti a questa categoria, a meno che non siano state impostate delle eccezioni. Gli eventi legati all'azione «Consenti» non vengono registrate se l'opzione **Controllo siti web inappropriati** è selezionata.

Nota
i siti web consentiti sono comunque sottoposti a scansione e verifica grazie alla funzione filtro URL (protezione web) di Sophos Endpoint Security and Control.

Attivazione del controllo siti web inappropriati

Per attivare il controllo web in Enterprise Console eseguire i seguenti passaggi e utilizzare l'opzione Controllo siti web inappropriati.

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - controllo web** per modificare il criterio del controllo web.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni sull'amministrazione basata sui ruoli, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per attivare del controllo siti web inappropriati:

1. Verificare quale criterio del controllo web è utilizzato dal o dai gruppi di computer che si desidera configurare. Per ulteriori informazioni, consultare la sezione Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel pannello **Criteri**, cliccare due volte su **Controllo web**. Quindi cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio di controllo web**.
3. Nel riquadro **Generale**, selezionare **Abilita controllo web**.
   Viene visualizzato il criterio **Controllo siti web inappropriati**. Sebbene a ciascuna delle 14 categorie di siti web sia abbinata un'azione predefinita, è possibile modificarla. Per ulteriori informazioni, consultare la sezione Selezione di un'azione da applicare a una categoria di siti web (pagina 178).

Categorie dei siti web

Selezionando **Controllo siti web inappropriati**, è possibile configurare 14 categorie di siti web, consentendo in questo modo di controllare i contenuti Internet a cui gli utenti possono accedere utilizzando un browser web. Per ulteriori informazioni, consultare la sezione Controllo siti web inappropriati (pagina 175).

Le categorie di siti web elencate qui di seguito sono sottoposte a filtro. L'azione predefinita relativa a ciascuna categoria è riportata tra parentesi. Ogni categoria può essere configurata come **Blocca**, **Avvisa** o **Consenti**. La categoria **Consenti** autorizza l'accesso a tutti i siti che ne fanno parte. Per cambiare azione, consultare la sezione Selezione di un'azione da applicare a una categoria di siti web (pagina 178).

- **Adulti/Sessualmente esplicito (Blocca)**: in questa categoria sono inclusi siti web relativi a prodotti per adulti tra i quali strumenti erotici, CD-ROM e video, oltre che pornografia minorile e pedofilia (compreso l'elenco di URL e pagine web della IWF, Internet Watch Foundation); servizi per adulti tra cui servizi di video conferenza, escort e informazioni su locali per spogliarelli; racconti a sfondo erotico e descrizioni grafiche di atti sessuali; animazioni e cartoni animati espliciti, gruppi online riguardanti tematiche sessuali (newsgroup e forum di natura sessuale) o siti erotici contenenti immagini di corpi completamente o parzialmente nudi; descrizioni o immagini di atti sessuali (anche riguardanti animali e oggetti inanimati); immagini o testi che promuovono lo sfruttamento o la violenza sessuale; bondage, feticismo, piercing ai genitali; siti per nudisti che mostrino nudità e fotografie erotiche o feticiste che rappresentano nudità.

 Copyright © Sophos Limited

Nota
non sono inclusi siti web di natura medica riguardanti tematiche sessuali, cancro al seno o malattie trasmesse sessualmente (eccezion fatta per quelli che forniscono esempi grafici).

- **Alcool e tabacco (Avvisa)**: in questa categoria sono inclusi siti web che promuovono o distribuiscono bevande alcoliche o prodotti derivati dal tabacco gratuitamente o a pagamento.
- **Anonimizzatore Proxy (Blocca)**: in questa categoria sono inclusi siti web per proxy remoti o per la navigazione anonima, oltre che cache di motori di ricerca e siti di traduzione basati sul web che evitano il blocco applicato dai filtri.
- **Attività criminali (Blocca)**: in questa categoria sono inclusi siti web che difendono e forniscono istruzioni o consigli su come intraprendere azioni illegali; dispensano suggerimenti su come aggirare l'applicazione della legge e su tecniche di scassinamento e furto con scasso.
- **Azzardo (Avvisa)**: in questa categoria sono inclusi siti web in cui vengono svolte attività di gioco d'azzardo on-line o lotterie che invitano all'utilizzo di denaro virtuale o reale; vengono fornite informazioni o consigli su come piazzare scommesse, partecipare a lotterie, a giochi d'azzardo o scegliere numeri; casinò virtuali e società di gioco d'azzardo offshore; scommesse sportive e pronostici; oltre che sport virtuali e fantatornei che offrono ricchi premi o richiedono quote di partecipazione elevate.
- **Pirateria informatica (Blocca)**: in questa categoria sono inclusi siti web che promuovono e forniscono istruzioni o consigli sull'utilizzo discutibile o addirittura illegale di apparecchiature e software, al fine di decodificare password, creare virus, accedere a computer di altri e inserirsi in sistemi di comunicazione computerizzati; oltre che siti che contengono istruzioni o modalità per aggirare i software per il filtraggio; software e siti d'informazione craccati, warez, software piratati, siti di download multimediali e siti di criminalità informatica.
- **Sostanze illecite (Blocca)**: in questa categoria sono inclusi siti web che forniscono ricette, istruzioni o kit per realizzare o coltivare sostanze illecite a scopi diversi dall'utilizzo industriale; incoraggiano o consigliano il consumo o come nascondere il consumo di tabacco, sostanze illecite o altre sostanze il cui consumo è illegale per minorenni; forniscono informazioni sullo "sballo legale", tra cui sniffare colla, utilizzare in modo errato farmaci o abusare di sostanze legali; distribuiscono gratuitamente o a pagamento droghe e mostrano o vendono strumentazione legata al consumo di droghe.
- **Intolleranza e razzismo (Blocca)**: in questa categoria sono inclusi siti web che sostengono e incitano alla degradazione o all'attacco di determinate popolazioni o istituzioni in base a principi religiosi, razziali, di nazionalità, genere, età, disabilità o orientamenti sessuali; siti che promuovono un'agenda politica e sociale orientata alla supremazia di un gruppi e all'esclusione degli altri in base a razza, religione, nazionalità, genere, età, disabilità o orientamento sessuale; con idee revisioniste o negazioniste sull'olocausto e altri siti revisionisti che promuovono l'odio; siti di coercizione o reclutamento dei membri di gang[1] o sette [2]; siti militanti ed estremisti; oltre che contenenti materiale apertamente scorretto e offensivo, fra cui quelli in cui non vengono ammesse o riconosciute posizioni e credi opposti.

Nota
non sono inclusi siti web di notizie, di natura storica o casi giornalistici in cui si ritrovano i criteri citati qui sopra (eccezion fatta per esempi grafici).

[1]Per gang si intende un gruppo che svolge attività criminali, con un nome proprio e segni o simboli che ne identificano l'appartenenza; i suoi membri commettono crimini sia individualmente che collettivamente in nome dell'appartenenza a tale gruppo.

[2] Per setta si intende un gruppo i cui membri sono stati raccolti con l'inganno e la manipolazione e trattenuti sotto un'influenza negativa che altera la personalità e il comportamento dei suoi seguaci; si tratta di un gruppo in cui chi è al comando dispone di potere assoluto, basato sul totalitarismo e in cui la volontà del singolo è subordinata a quella del gruppo. È un gruppo che si colloca al di fuori della società.

- **Phishing e truffe (Blocca):** in questa categoria sono inclusi siti web coinvolti in campagne di phishing e scherzi telefonici, siti d'informazione sul furto di servizi e plagio e che mettono in vendita materiale di ricerca.
- **URL di spam (Blocca):** in questa categoria sono incluse le URL di spam, in particolare quelle che si riferiscono ai seguenti argomenti: informatica, finanza e borse, intrattenimento, giochi, salute e medicina, umorismo, personale e dating, prodotti e servizi, shopping e viaggi.
- **Spyware (Blocca)**: in questa categoria sono inclusi i siti web che forniscono o promuovono la raccolta o la ricostruzione di informazioni all'insaputa o senza il consenso esplicito dell'utente finale o dell'organizzazione; sono inclusi siti con eseguibili malevoli o virus, monitoraggio di terzi e altri software commerciali non desiderati, oltre che spyware e malware.
- **Cattivo gusto/Offensivo (Avvisa)**: in questa categoria sono inclusi i siti web che utilizzano un linguaggio offensivo o violento, sia che si tratti di barzellette, fumetti o satira, oltre che un uso eccessivo di blasfemie o gesti osceni.
- **Violenza (Avvisa)**: in questa categoria sono inclusi i siti web che mostrano, descrivono o inneggiano alla violenza fisica contro altri essere umani, animali o istituzioni; che descrivono atti di tortura, mutilazione, sangue o morti cruente; descrivono o promuovono l'auto-violenza o il suicidio, sia che trattino di disturbi alimentari che di dipendenze; istruzioni o kit per la costruzione di bombe o altri dispositivi che possano causare danni o distruzione a cose o persone; siti che promuovono terrorismo e sport o giochi troppo violenti, compresi videogiochi e giochi online.

  Nota
  non sono inclusi siti web di notizie, di natura storica o casi giornalistici in cui si ritrovano i criteri citati qui sopra (eccezion fatta per esempi grafici).

- **Armi (Avvisa)**: in questa categoria sono inclusi i siti web che forniscono informazioni su come ordinare e acquistare armi on-line, completi di listino prezzi e indirizzi; qualsiasi sito o pagina che contiene o fornisce link a contenuti inerenti alla vendita di pistole, armi, munizioni o sostanze velenose; mostrano o descrivono l'utilizzo di pistole, armi, munizioni o sostanze velenose; o che promuove club che offrono addestramento per l'utilizzo di mitragliatrici, armi automatiche e altre armi d'assalto, oltre che addestramento per cecchini.

  Nota
  per armi si ritengono oggetti (quali mazze, coltelli o pistole) utilizzati per causare offese e distruzione.

Selezione di un'azione da applicare a una categoria di siti web

Una volta abilitato il controllo web e selezionato il criterio **Controllo siti web inappropriati**, è possibile configurare l'azione da applicare a ogni categoria di siti web. È anche possibile creare un nuovo criterio che si basi su quello predefinito. Per ulteriori informazioni, consultare la sezione Creazione di un criterio (pagina 30).

Per selezionare l'azione da applicare a una Categoria di siti web:

 Copyright © Sophos Limited

1. Nella scheda **Generale**, dall'elenco a discesa, di fianco alla o alle categorie che si desidera configurare, selezionare una delle seguenti opzioni:
   - **Blocca**: Blocca l'accesso degli utenti ai siti che appartengono a questa categoria. Se si tratta di una pagina web HTTP, l'utente riceve notifica del blocco e le motivazioni per cui questa azione è stata intrapresa. Se si tratta di una pagina web HTTPS, nell'area di notifica di Windows viene visualizzato un fumetto di suggerimento.
   - **Avvisa**: Avvisa gli utenti del rischio di stare per violare il criterio di utilizzo del web della propria organizzazione, ma consente di procedere. Se si tratta di una pagina web HTTP, gli utenti ricevono notifica dell'avviso e vengono messi in guardia sul procedere nella navigazione. Se si tratta di una pagina web HTTPS, gli utenti non ricevono alcuna notifica e possono procedere ad accedere al sito web. L'evento viene registrato come soggetto all'azione «Procedi» in Enterprise Console.
   - **Consenti**: Gli utenti possono accedere liberamente ai siti che appartengono a questa categoria. L'evento non viene registrato.
2. Cliccare su **OK**.

Gestione delle eccezioni applicate ai siti web

Se si seleziona il criterio **Controllo siti web inappropriati**, è possibile creare eccezioni per le azioni «Blocca» e «Avvisa». È possibile escludere alcuni siti web dall'azione di filtro aggiungendoli all'elenco «Siti web da consentire» o «Siti web da bloccare». Gli elemento dell'elenco possono essere sotto forma di indirizzi IP o nomi dominio. È anche possibile modificare voci già incluse negli elenchi di siti web, oltre che rimuovere siti web da tali elenchi.

Nota
Nel caso di elementi in conflitto o sovrapponibili, presenti sia nell'elenco "Blocca" sia nell'elenco "Consenti", quelli presenti nell'elenco Blocca avranno sempre priorità. Per esempio, se lo stesso indirizzo IP è incluso sia nell'elenco Blocca che Consenti, il sito web viene bloccato. Inoltre, se nell'elenco Blocca è incluso un dominio, mentre un sottodominio di quello stesso dominio fa parte dell'elenco Consenti, la voce presente nell'elenco Consenti viene ignorata e tutto il dominio, inclusi i sottodomini, viene bloccato.

Per aggiungere eccezioni:

1. Nella scheda **Esenzioni per site web**, cliccare sul pulsante **Aggiungi**, di fianco alla casella di testo **Siti web da consentire** o **Siti web da bloccare**.
2. Nella finestra di dialogo **Aggiungi siti web da consentire**, cliccare su **Nome dominio**, **Indirizzo IP con maschera di sottorete** o **Indirizzo IP**. Sopra ogni casella di testo vengono visualizzati i relativi esempi di formato.
3. Nella casella di testo, inserire il nome di dominio o indirizzo IP relativo al sito web che si desidera bloccare o consentire.
4. Cliccare su **OK**.

Se si desidera modificare o rimuovere un sito web dall'elenco, selezionare il sito in questione e cliccare su **Modifica** o **Rimuovi** a seconda del caso.

7.8.2 Controllo web completo

Nota
Questa funzione non è inclusa in tutte le licenze. Se la si desidera utilizzare potrebbe essere necessario personalizzare la propria licenza. Per ulteriori informazioni, vedere http://www.sophos.com/it-it/products/complete/comparison.aspx.

Se in possesso di una Sophos Web Appliance, Security Management Appliance o appliance UTM (versione 9.2 o successiva), è possibile distribuire ai propri clienti un criterio basato sull'appliance tramite Enterprise Console.

I computer endpoint comunicano con Enterprise Console nello stesso modo in cui comunicherebbero se il criterio di controllo delle applicazioni potenzialmente indesiderate fosse selezionato; tuttavia le regole relative al filtro web e ai log sull'attività web vengono sincronizzate con l'appliance prescelta. Il criterio viene archiviato nel computer endpoint e applicato in base ai dati Sophos più recenti.

A seconda del criterio del controllo web applicato gli utenti possono essere bloccati, avvisati, o può essere loro consentito l'accesso a un determinato sito web. È possibile visualizzare i dati relativi all'attività degli utenti utilizzando le funzioni di **Report** e **Ricerca** dell'Web Appliance, della Management Appliance oppure selezionando l'opzione **Accesso & Reportistica > Web Protection** dell'appliance UTM. Gli eventi del controllo Web vengono tutte registrate nell'appliance. I siti scansionati e verificati in tempo reale dal filtro URL di Sophos Endpoint Security and Control vengono invece registrati come eventi web in Enterprise Console.

Nota
sebbene entrambi i siti HTTP e HTTPS siano soggetti a filtro in tutti i browser web supportati, nella Web Appliance o Management Appliance le notifiche inviate all'utente sono differenti se l'URL del sito web è HTTP o HTTPS. Nel caso di siti HTTP, gli utenti ricevono notifica per i siti soggetti all'azione «Blocca» o «Avvisa». Nel caso di siti HTTPS, gli utenti ricevono notifica solo per i siti soggetti all'azione «Blocca»; tali notifiche vengono visualizzate nell'area di notifica di Windows e nel formato di fumetto suggerimento. Le azioni «Avvisa» dei siti HTTPS non vengono né visualizzate agli utenti, né registrate. Gli utenti possono quindi accedere alla pagina web desiderata e l'evento viene registrato come soggetto all'azione «Procedi» nella Web Appliance o nella Management Appliance.

Gli utenti dell'appliance UTM utilizzano un servizio basato sul cloud denominato Sophos LiveConnect che consente di proteggere e monitorare i computer endpoint. LiveConnect consente di gestire tutti gli endpoint sempre, sia che facciano parte della rete locale sia che si trovino in località remote; inoltre, per gli utenti in viaggio, gli aggiornamenti dei criteri verranno distribuiti e i dati dei report sugli endpoint verranno caricati, anche quando gli utenti non sono collegati alla rete.

Quando si utilizza la Management Appliance o la Web Appliance, gli endpoint possono comunicare con l'appliance sia direttamente che tramite Sophos LiveConnect.

Se si seleziona l'opzione **Controllo web completo**, viene applicato un criterio completo. Full Web Control fornisce i seguenti benefici rispetto al controllo Web di base, a seconda del tipo di appliance in uso:

- Le azioni di avviso o blocco si basano su 50 categorie di URL.
- Possono essere applicati criteri diversificati relativi a «Fasce orarie specifiche».
- Criteri aggiuntivi possono essere utilizzati come eccezioni (per determinati utenti o gruppi) ai criteri di accesso web predefiniti o a quelli relativi a fasce orarie specifiche.

 Copyright © Sophos Limited

- Log e report dettagliati sono disponibili nella Web Appliance o nella Management Appliance.
- LiveConnect consente la distribuzione degli aggiornamenti dei criteri e il caricamento dei dati sulla reportistica, anche quando gli utenti sono collegati in remoto.
- Gli utenti possono fornire feedback sulla gestione delle URL bloccate.
- Gli utenti possono accedere a pagine di notifica personalizzate che riportano il logo dell'azienda, oltre che testi specifici per la propria organizzazione. Per ulteriori informazioni, consultare la documentazione relativa alla Sophos Web Appliance.
- Quando l'opzione SafeSearch è abilitata l'accesso a siti inappropriati è automaticamente bloccato al livello del motore di ricerca.

Per ulteriori informazioni sulla configurazione di un criterio completo per Web Appliance, consultare la documentazione relativa alla Sophos Web Appliance e reperibile cliccando su questo link http://wsa.sophos.it/docs/wsa/.

La documentazione sull'appliance UTM è disponibile alla pagina http://www.sophos.com/it-it/support/documentation/sophos-utm.aspx.

Attivazione del controllo web completo

Nota
La seguente procedura presuppone che la Sophos Web Appliance, Sophos Management Appliance o l'appliance di Sophos UTM (versione 9.2 o successiva) sia configurata, funzionante e che utilizzi Endpoint Web Control.

Per impostazione predefinita, il criterio del controllo web è disattivato. Eseguire i seguenti passaggi per abilitare il controllo web ed eseguire il criterio del controllo web completo.

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - controllo web** per modificare il criterio del controllo web.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni sull'amministrazione basata sui ruoli, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per abilitare il controllo web completo:

1. Verificare quale criterio del controllo web è utilizzato dal o dai gruppi di computer che si desidera configurare. Per ulteriori informazioni, consultare la sezione Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel pannello **Criteri**, cliccare due volte su **Controllo web**. Quindi cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio di controllo web**.
3. Nella scheda **Generale**, cliccare su **Abilita il controllo web**.
4. Selezionare **Controllo web completo**.
5. Nel riquadro **Impostazioni**, inserire il **Nome host dell'appliance** e la **Chiave di sicurezza per lo scambio di criteri**.
   - Nel caso si disponga di una Web Appliance o di una Management Appliance, è necessario fornire un nome host valido. La chiave di sicurezza deve corrispondere a quella visualizzata nella pagina **Endpoint Web Control** dell'appliance.

- Nel caso si disponga di un'appliance UTM, inserire il nome host e la chiave condivisa del broker di Sophos LiveConnect utilizzata dall'appliance UTM. Sia il nome host che la chiave condivisa sono reperibili nell'interfaccia amministrativa WebAdmin di UTM, nella scheda **Endpoint Protection** > **Gestione computer** > **Avanzate**, nella sezione **Sophos LiveConnect – Registrazione** sotto **Informazioni SEC**.

Per ulteriori informazioni, consultare la documentazione sulla Sophos Web Appliance disponibile alla pagina Web http://wsa.sophos.it/docs/wsa/ o quella sull'appliance UTM disponibile alla pagina Web http://www.sophos.com/it-it/support/documentation/sophos-utm.aspx.

6. Opzionalmente, selezionare **Blocca navigazione se non può essere determinata alcuna categoria web**. Se il computer endpoint è abilitato al recupero di dati relativi alle categorie dei siti web, le URL non riconducibili ad alcuna categoria vengono bloccate fino al ripristino del servizio.

   Questa casella di spunta non viene selezionata per impostazione predefinita, consentendo agli utenti di continuare nella navigazione se il servizio viene interrotto.

7. Cliccare su **OK**.
   Enterprise Console riconfigura i computer endpoint in modo da consentire la comunicazione con la Web Appliance, Management Appliance, o col broker di Sophos LiveConnect utilizzato dall'appliance UTM.

7.9 Criterio di prevenzione degli exploit

Nota
Questa funzione non è inclusa in tutte le licenze. Se la si desidera utilizzare potrebbe essere necessario cambiare la propria licenza. Per ulteriori informazioni, vedere http://www.sophos.com/it-it/products/complete/comparison.aspx.

La prevenzione degli exploit consente di:

- Proteggere i file di documento dal ransomware (CryptoGuard).
- Proteggere i sistemi dagli attacchi contro il settore di avvio (WipeGuard).

  Importante
  Al momento, questa funzionalità non è disponibile per i server.

- Proteggere le funzioni critiche nei browser web (Safe Browsing).
- Attenuare gli exploit. Questa opzione difende le applicazioni più vulnerabili agli exploit da parte del malware, come ad es. le applicazioni Java.
- Proteggere i sistemi dagli attacchi di process hollowing.
- Proteggere i sistemi dal caricamento di file .DLL da cartelle non attendibili.
- Proteggere i sistemi contro il branch tracing del processore.

Per impostazione predefinita, la prevenzione degli exploit e tutte le opzioni di prevenzione degli exploit sono attivate.

Importante
Se si effettua l'upgrade della licenza in modo da includere Exploit Prevention, questa funzionalità non viene installata automaticamente sui computer che sono già gestiti. Occorrerà proteggere nuovamente i computer per installarla. Vedere Protezione automatica dei computer (pagina 45).

 Copyright © Sophos Limited

È possibile escludere applicazioni dalla prevenzione degli exploit. Si noti che continueranno pur sempre a essere protette da CryptoGuard e Safe Browsing (Navigazione sicura).

Per ulteriori informazioni sulle impostazioni consigliate per la prevenzione degli exploit, consultare la Guida all'impostazione dei criteri di Sophos Enterprise Console.

Nota
Se si utilizza l'amministrazione basata sui ruoli:

- È necessario possedere il diritto **Impostazione criterio - prevenzione degli exploit** per configurare un criterio di prevenzione degli exploit.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

HitmanPro.Alert e gli aggiornamenti dei criteri

HitmanPro.Alert rileva, negli endpoint, le applicazioni che hanno bisogno di essere protette. Segnala al server di Sophos Enterprise Console le applicazioni rilevate. Il server confronta le applicazioni che richiedono protezione, e ogni 120 minuti include nel criterio i nuovi dati sulle applicazioni. Il server distribuisce il criterio aggiornato sugli endpoint, fornendo l'elenco di applicazioni da proteggere.

7.9.1 Attivazione e disattivazione della prevenzione degli exploit

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario possedere il diritto **Impostazione criterio - prevenzione degli exploit** per configurare un criterio di prevenzione degli exploit.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Nota
Per impostazione predefinita, la prevenzione degli exploit è attivata, e sono attivate anche tutte le opzioni di prevenzione degli exploit.

Per attivare o disattivare la prevenzione degli exploit:

1. Controllare quale criterio di prevenzione degli exploit è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Prevenzione degli exploit**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella scheda **Impostazioni di protezione** della finestra di dialogo **Criterio di prevenzione degli exploit**, selezionare o deselezionare la casella di spunta **Abilita prevenzione degli exploit**.
4. Selezionare o deselezionare la casella di spunta **Proteggi i file di documento contro il ransomware (CryptoGuard)**.

   È anche possibile selezionare se attivare la protezione contro il ransomware eseguito in remoto (solo su endpoint a 64 bit).
5. Selezionare o deselezionare la casella di spunta **Protezione del disco e del record di avvio (WipeGuard)**.

6. Selezionare o deselezionare la casella di spunta **Proteggi funzioni critiche nei browser web (Safe Browsing)**.
7. Selezionare o deselezionare la casella di spunta **Attenua exploit in applicazioni vulnerabili**.

   È anche possibile selezionare i tipi di applicazioni da proteggere contro gli exploit, come ad esempio le applicazioni Microsoft Office.
8. Selezionare o deselezionare la casella di spunta **Impedisci attacchi di process hollowing**.
9. Selezionare o deselezionare la casella di spunta **Impedisci il caricamento di DLL da cartelle non attendibili**.
10. Selezionare o deselezionare la casella di spunta **Abilita branch tracing della CPU**.
11. Cliccare su **OK**.

È possibile escludere applicazioni dalla prevenzione degli exploit. Si noti che continueranno pur sempre a essere protette da CryptoGuard e Safe Browsing (Navigazione sicura), se sono state selezionate queste opzioni. Vedere Esclusione di applicazioni dalla prevenzione degli exploit (pagina 184).

È anche possibile escludere eventi di exploit dalla prevenzione degli exploit. Vedere Esclusione di eventi di exploit dalla prevenzione degli exploit (pagina 185).

7.9.2 Esclusione di applicazioni dalla prevenzione degli exploit

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario possedere il diritto **Impostazione criterio - prevenzione degli exploit** per configurare un criterio di prevenzione degli exploit.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Importante
Le applicazioni vulnerabili sono protette per impostazione predefinita. Occorre esercitare la dovuta cautela quando si escludono applicazioni dalla prevenzione degli exploit. Continueranno infatti a essere protette da CryptoGuard e Safe Browsing (Navigazione sicura), vedere Attivazione e disattivazione della prevenzione degli exploit (pagina 183).

È possibile escludere applicazioni dalla prevenzione degli exploit. È anche possibile proteggere applicazioni precedentemente escluse.

Per escludere applicazioni:

1. Controllare quale criterio di prevenzione degli exploit è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Prevenzione degli exploit**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella scheda **Esclusioni delle applicazioni** della finestra di dialogo **Criterio di prevenzione degli exploit**, selezionare le applicazioni che si desidera escludere nell'elenco **Applicazioni protette**, e cliccare su **Escludi**.
   Questa azione trasferisce le applicazioni selezionate nell'elenco **Applicazioni escluse**.
4. Per proteggere le applicazioni che sono attualmente escluse dai controlli, caricare l'elenco **Applicazioni escluse**, selezionare le applicazioni e cliccare su **Includi**.
5. Cliccare su **OK**.

 Copyright © Sophos Limited

7.9.3 Esclusione di eventi di exploit dalla prevenzione degli exploit

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario possedere il diritto **Impostazione criterio - prevenzione degli exploit** per configurare un criterio di prevenzione degli exploit.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Importante

- Quando si esclude un evento di exploit, verrà escluso solamente l'exploit specifico, e non l'applicazione intera.
- Se un evento di exploit fa parte di un'applicazione che è già stata esclusa, non occorrerà escludere l'evento di exploit.

È possibile escludere eventi di exploit dalla prevenzione degli exploit. È anche possibile proteggere eventi di exploit precedentemente esclusi.

Per escludere eventi di exploit:

1. Controllare quale criterio di prevenzione degli exploit è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Prevenzione degli exploit**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella scheda **Esclusioni degli exploit** della finestra di dialogo **Criterio di prevenzione degli exploit**, selezionare gli eventi di exploit che si desidera escludere dall'elenco **Eventi relativi agli exploit rilevati** e cliccare su **Escludi**.
   Questa azione trasferisce gli eventi di exploit selezionati nell'elenco **Eventi relativi agli exploit esclusi**
4. Per proteggere gli eventi di exploit che sono attualmente esclusi dai controlli, caricare l'elenco **Eventi relativi agli exploit esclusi**, selezionare gli eventi e cliccare su **Includi**.
5. Cliccare su **OK**.

Copyright © Sophos Limited

8 Impostazione di allarmi e messaggi

In Enterprise Console sono presenti diversi tipi di allarmi.

- **Allarmi visualizzati nella console**

  Se in un computer viene rilevato un oggetto che richiede attenzione oppure si verifica un errore, Sophos Endpoint Security and Control invia un allarme a Enterprise Console. L'allarme viene visualizzato nell'elenco dei computer. Per ulteriori informazioni sulla gestione di tali allarmi, consultare la sezione Trattamento degli allarmi su oggetti rilevati (pagina 51).

  Questi allarmi vengono sempre visualizzati. Non è necessario impostarli.

- **Eventi visualizzati nella console**

  Quando si verifica un evento di controllo applicazioni, dati e dispositivi, firewall, verifica patch, blocco rimozione o di controllo web in un computer endpoint, per esempio un'applicazione è stata bloccata dal firewall, tale evento viene inviato a Enterprise Console e può essere visualizzato nel relativo visualizzatore eventi.

- **Allarmi e messaggi inviati dalla console ai destinatari prescelti**

  Per impostazione predefinita, quando nel computer viene rilevato un oggetto, sul desktop viene visualizzato un messaggio e viene aggiunta una voce al log degli eventi di Windows. Quando si verifica un evento di controllo applicazioni, dati o dispositivi, viene visualizzato un messaggio sul computer.

  Nota
  I messaggi desktop opzionali definiti dall'utente non vengono visualizzati nei computer che eseguono Windows 8 o versioni successive.

  È inoltre possibile configurare allarmi e-mail o messaggi SNMP da inviare agli amministratori.

  Nota
  Se si desidera utilizzare SMTP autenticato per gli allarmi e-mail, consultare l'articolo 113780 della knowledge base Sophos.

Questa sezione spiega come impostare gli allarmi che verranno inviati ai destinatari prescelti.

8.1 Impostazione degli allarmi relativi alle sottoscrizioni software

Se si utilizza l'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Configurazione del sistema**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Enterprise Console visualizza gli allarmi rilevati dal gestore degli aggiornamenti nella colonna **Allarmi**, presente nella vista **Update manager**. Se si è eseguita la sottoscrizione a una versione fissa di un software, quando tale versione sarà vicina al ritiro o verrà ritirata si visualizzerà un allarme. Anche nel caso di modifiche apportate alla licenza del prodotto verrà visualizzato un allarme.

 Copyright © Sophos Limited

Se si è eseguita la sottoscrizione a una versione fissa del software e si è scelto di **Eseguire l'upgrade automatico delle sottoscrizioni a versioni fisse quando non più supportate da Sophos**, l'upgrade della sottoscrizione verrà eseguito automaticamente.

Se, al contrario, si è scelto di non eseguire l'upgrade automatico, verrà richiesto di cambiare la sottoscrizione.

Importante
L'esecuzione di un software non supportato espone al rischio di nuove minacce per la sicurezza. Si consiglia di eseguire l'upgrade a una versione supportata il più presto possibile.

È inoltre possibile impostare allarmi e-mail da inviare ai destinatari prescelti quando la versione del prodotto sottoscritta si avvicina al ritiro o è stata ritirata.

1. Dal menu **Strumenti,** selezionare **Configura allarmi e-mail**.
   Viene visualizzata la finestra di dialogo **Configura allarmi e-mail**.
2. Se le impostazioni SMTP non sono state configurate oppure si desidera visualizzarle o modificarle, cliccare su **Configura.**

   Nella finestra di dialogo **Configura impostazioni SMTP**, inserire i dati come descritto sotto.

   a) Nella casella di testo **Indirizzo server**, digitare il nome dell'host o l'indirizzo IP del server SMTP.

   b) Nella casella di testo **Mittente**, digitare un indirizzo e-mail al quale possono essere inviati i "bounce" e i messaggi di mancato recapito.

   c) Cliccare su **Prova** per effettuare il test della connessione.
3. Nel riquadro **Destinatari**, cliccare su **Aggiungi**.
   Viene visualizzata la finestra di dialogo **Aggiungi un nuovo destinatario degli allarmi e-mail**.
4. Nel campo **Indirizzo e-mail**, inserire l'indirizzo del destinatario.
5. Nel campo **Lingua,** selezionare la lingua in cui saranno inviati gli allarmi e-mail.
6. Nel riquadro **Sottoscrizioni**, selezionare gli allarmi e-mail di tipo "Sottoscrizioni software"che si desidera inviare a questo destinatario. È possibile sottoscrivere tre tipi di allarmi:

   - La sottoscrizione al software comprende la versione di un prodotto che presto Sophos ritirerà.
   - La sottoscrizione al software comprende la versione di un prodotto non più disponibile.

     Questo tipo di allarme viene inviato se il prodotto che si è sottoscritto è stato ritirato, oppure se la licenza è stata modificata e non include più tale prodotto.
   - Le informazioni relative alla licenza Sophos sono state aggiornate. Le funzioni del prodotto potrebbero essere cambiate.

8.2 Impostazione degli allarmi e-mail di antivirus e HIPS

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile inviare gli allarmi e-mail a determinati utenti nel caso in cui venga riscontrato un virus, un comportamento sospetto, un'applicazione indesiderata o un errore su uno dei computer di un gruppo.

Importante
i computer con sistema operativo Mac OS X possono inviare gli allarmi e-mail a un solo indirizzo.

1. Nel riquadro **Criteri**, cliccare due volte sul criterio antivirus e HIPS che si desidera modificare.
2. Nella finestra di dialogo **Criterio antivirus e HIPS**, cliccare su **Messaggistica**.
3. Nella finestra di dialogo **Messaggistica**, andare alla scheda **Allarmi e-mail** e selezionare **Abilita allarmi e-mail**.
4. Nel riquadro **Messaggi da inviare**, selezionare gli eventi per cui si desidera inviare allarmi e-mail.

   Nota
   le impostazioni **Rilevamento di comportamento sospetto**, **Rilevamento di file sospetti**, **Rilevamento e disinfezione di adware e PUA** e **Altri errori** sono applicabili solo ai computer Windows.

5. Nel riquadro **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 **Rinomina** per modificare un indirizzo e-mail che è stato aggiunto.

   Importante
   i computer con sistema operativo Mac OS X invieranno i messaggi solo al primo destinatario dell'elenco.

6. Cliccare su **Configura SMTP** per modificare le impostazioni del server SMTP e la lingua degli allarmi e-mail.
7. Nella finestra di dialogo **Configura impostazioni SMTP**, inserire i dati come descritto sotto.
   - Nella casella di testo **Server SMTP**, digitare il nome dell'host o l'indirizzo IP del server SMTP. Cliccare su **Prova** per inviare un allarme e-mail di prova.
   - Nella casella di testo **Indirizzo SMTP mittente**, digitare un indirizzo e-mail al quale possono essere inviati i "bounce" e i messaggi di mancato recapito.
   - Nella casella di testo **Indirizzo SMTP rispondi a**, è possibile inserire l'indirizzo e-mail a cui inviare le risposte agli allarmi e-mail. Gli allarmi e-mail vengono inviati automaticamente dal sistema.
   - Nel riquadro **Lingua**, cliccare sulla freccia dell'elenco a discesa e selezionare la lingua in cui inviare gli allarmi e-mail.

8.3 Impostazione della messaggistica SNMP di antivirus e HIPS

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

 Copyright © Sophos Limited

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Nel caso in cui venga rilevato un virus o venga riscontrato un errore su uno dei computer di un gruppo è possibile inviare messaggi SNMP a determinati utenti.

Nota
impostazioni valide solo per Windows.

1. Nel riquadro **Criteri**, cliccare due volte sul criterio antivirus e HIPS che si desidera modificare.
2. Nella finestra di dialogo **Criterio antivirus e HIPS**, cliccare su **Messaggistica**.
3. Nella finestra di dialogo **Messaggistica**, andare alla scheda **Messaggistica SNMP** e selezionare **Abilita messaggistica SNMP**.
4. Nel riquadro **Messaggi da inviare**, selezionare i tipi di evento per cui si desidera che Sophos Endpoint Security and Control invii i messaggi SNMP.
5. Nella casella di testo **Destinazione trap SNMP**, inserire l'indirizzo IP del destinatario.
6. Nella casella di testo **Nome comunità SNMP**, inserire il nome comunità SNMP.

8.4 Configurazione della messaggistica desktop di antivirus e HIPS

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per impostazione predefinita, i messaggi sul desktop vengono visualizzati sul computer in cui è stato rilevato un virus, un oggetto sospetto o un'applicazione potenzialmente indesiderata. L'utente può configurare questi messaggi a proprio piacimento.

1. Nel riquadro **Criteri**, cliccare due volte sul criterio antivirus e HIPS che si desidera modificare.
2. Nella finestra di dialogo **Criterio antivirus e HIPS**, cliccare su **Messaggistica**.
3. Nella finestra di dialogo **Messaggistica**, cliccare sulla scheda **Messaggistica desktop**.

   Per impostazione predefinita, **Abilita messaggistica desktop** e tutte le opzioni del riquadro **Messaggi da inviare** sono selezionate. Se necessario modificare queste impostazioni.

   Nota
   le impostazioni **Rilevamento di comportamento sospetto**, **Rilevamento di file sospetti** e **Rilevamento di adware e PUA** sono applicabili solo ai computer Windows.

4. Nella casella **Messaggio definito dall'utente**, è possibile digitare un messaggio che sarà aggiunto alla fine del messaggio standard.

   Nota
   I messaggi desktop definiti dall'utente non vengono visualizzati nei computer che eseguono Windows 8 o versioni successive.

8.5 Impostazione di allarmi e messaggi del controllo applicazioni

Se si utilizza l'amministrazione basata sui ruoli:

- Per configurare un criterio di controllo delle applicazioni è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile inviare messaggi a specifici utenti quando viene rilevata un'applicazione controllata.

1. Nel riquadro **Criteri**, cliccare due volte sul criterio di controllo applicazioni che si desidera modificare.
2. Nella finestra di dialogo **Criteri di controllo applicazioni**, andare alla scheda **Messaggistica**.

   Nel riquadro **Messaggistica**, la casella di spunta **Abilita messaggistica desktop** è selezionata per impostazione predefinita. Quando un'applicazione controllata non autorizzata viene rilevata dalla scansione in accesso e bloccata, sul desktop dell'utente sarà visualizzato un messaggio che lo informa che l'applicazione è stata bloccata.
3. Nella casella **Testo del messaggio**, digitare un messaggio che sarà aggiunto alla fine del testo standard.

   Nota
   I messaggi desktop definiti dall'utente non vengono visualizzati nei computer che eseguono Windows 8 o versioni successive.

4. Se si desidera inviare allarmi e-mail relativi alle applicazioni controllate rilevate, selezionare la casella di spunta **Abilita allarmi e-mail**.
5. Selezionare la casella di spunta **Abilita messaggistica SNMP**, se si desidera inviare, messaggi SNMP.

   Nota
   le impostazioni utente dei criteri antivirus e HIPS determinano la configurazione e i destinatari della messaggistica e-mail ed SNMP. Per ulteriori informazioni, vedere Impostazione della messaggistica SNMP di antivirus e HIPS (pagina 188).

8.6 Impostazione di allarmi e messaggi del controllo dati

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - controllo dati** per configurare il criterio del controllo dati.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

 Copyright © Sophos Limited

Enterprise Console utilizza eventi e messaggi per segnalare quando viene rilevato o bloccato il trasferimento di dati sensibili.

Per informazioni su criteri ed eventi del controllo dati, consultare la sezione Criterio del controllo dati (pagina 147).

Quando il controllo dati è abilitato, per impostazione predefinita vengono connessi o visualizzati i seguenti eventi o messaggi:

- Gli eventi del controllo dati vengono connessi alla workstation.
- Gli eventi del controllo dati vengono inviati a Enterprise Console e possono essere visualizzati in **Data Control - Visualizzatore eventi** (per aprire il visualizzatore eventi, nel menu **Eventi**, cliccare su **Eventi controllo dati**).

  Nota
  ogni computer può inviare a Enterprise Console un massimo di 50 eventi del controllo dati all'ora.

- Il numero di computer con eventi del controllo dati che hanno superato una determinata soglia negli ultimi 7 giorni viene visualizzato nel pannello di controllo.
- Nella workstation vengono visualizzati messaggi desktop.

È inoltre possibile configurare Enterprise Console per inviare i seguenti messaggi:

Allarmi e-mail	Un messaggio e-mail viene inviato ai destinatari specificati.
Messaggi SNMP	Un messaggio SNMP viene inviato ai destinatari specificati nelle impostazioni del criterio antivirus e HIPS.

Per impostare la messaggistica del controllo dati:

1. Controllare quale criterio del controllo dati è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Controllo dati**. Quindi cliccare due volte sul criterio che si desidera modificare.
   Viene visualizzata la finestra di dialogo **Criterio di controllo dati**.
3. Nella finestra di dialogo **Criteri di controllo dati**, andare alla scheda **Messaggistica**. La messaggistica desktop è abilitata per impostazione predefinita ed è selezionato **Includi nei messaggi le regole soddisfatte**.
4. Se lo si desidera, digitare messaggi che verranno aggiunti a quelli standard per richiedere conferma da parte dell'utente del trasferimento o blocco di un file.

   È possibile inserire al massimo 100 caratteri e aggiungere al messaggio un link HTML, per esempio About Sophos.

   Nota
   I messaggi desktop definiti dall'utente non vengono visualizzati nei computer che eseguono Windows 8 o versioni successive.

5. Per abilitare gli allarmi e-mail, selezionare la casella di spunta **Abilitazione degli allarmi e-mail**. Nel campo **Destinatari e-mail**, inserire gli indirizzi e-mail dei destinatari. Separare ogni indirizzo da punto e virgola (;).

6. Per abilitare la messaggistica SNMP, selezionare la casella di spunta **Abilita messaggistica SNMP**.

   Le impostazioni del server e-mail e del trap SNMP sono configurate tramite il criterio antivirus e HIPS.

8.7 Impostazione di allarmi e messaggi per il controllo dispositivi

Se si utilizza l'amministrazione basata sui ruoli:

- È necessario essere in possesso dei diritti di **Impostazione criterio - controllo dispositivo** per modificare il criterio del controllo dispositivi.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Enterprise Console utilizza eventi e messaggi per segnalare il rilevamento o blocco di un dispositivo controllato.

Per informazioni sulla visualizzazione di eventi del controllo dispositivi, consultare la sezione Criterio del controllo dispositivi (pagina 161).

Quando il controllo dispositivi è abilitato, per impostazione predefinita vengono connessi o visualizzati i seguenti eventi o messaggi:

- Gli eventi del controllo dispositivi vengono connessi alla workstation.
- Gli eventi del controllo dispositivi vengono inviati a Enterprise Console e possono essere visualizzati in **Device Control - Visualizzatore eventi** (per aprire il visualizzatore eventi, nel menu **Eventi**, cliccare su **Eventi controllo dispositivi**).
- Il numero di computer con eventi del controllo dispositivi che hanno superato una determinata soglia negli ultimi 7 giorni viene visualizzato nel pannello di controllo.
- Nella workstation vengono visualizzati messaggi desktop.

È inoltre possibile configurare Enterprise Console per inviare i seguenti messaggi:

Allarmi e-mail	Un messaggio e-mail viene inviato ai destinatari specificati.
Messaggi SNMP	Un messaggio SNMP viene inviato ai destinatari specificati nelle impostazioni del criterio antivirus e HIPS.

Per impostare la messaggistica del controllo dispositivi:

1. Controllare quale criterio del controllo dispositivi è utilizzato dal o dai gruppi di computer che si desidera configurare.

   Vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Nel riquadro **Criteri**, cliccare due volte su **Controllo dispositivi**. Quindi cliccare due volte sul criterio che si desidera modificare.
3. Nella finestra di dialogo **Criterio del controllo dispositivi**, nella scheda **Messaggi**, la messaggistica desktop è abilitata per impostazione predefinita. Per configurare ulteriormente la messaggistica, svolgere le seguenti operazioni:
   - *Per inserire un messaggio di testo per la messaggistica desktop*, nella casella **Testo messaggio**, digitare un messaggio che verrà aggiunto alla fine del messaggio standard.

 Copyright © Sophos Limited

È possibile inserire al massimo 100 caratteri e aggiungere al messaggio un link HTML, per esempio About Sophos.

Nota
I messaggi desktop definiti dall'utente non vengono visualizzati nei computer che eseguono Windows 8 o versioni successive.

- *Per abilitare gli allarmi e-mail*, selezionare la casella di spunta **Abilitazione degli allarmi e-mail**. Nel campo **Destinatari e-mail**, inserire gli indirizzi e-mail dei destinatari. Separare ogni indirizzo da punto e virgola (;).
- *Per abilitare la messaggistica SNMP*, selezionare la casella di spunta **Abilita messaggistica SNMP**.

Le impostazioni del server e-mail e del trap SNMP sono configurate tramite il criterio antivirus e HIPS.

8.8 Impostazione degli allarmi e-mail sullo stato della rete

Se si utilizza l'amministrazione basata sui ruoli, per poter configurare gli allarmi e-mail relativi allo stato della rete, è necessario essere in possesso dei diritti di **Configurazione del sistema**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile impostare l'invio di allarmi via e-mail ai destinatari prescelti nel caso in cui venga superato il livello di avviso o il livello critico per una sezione del pannello di controllo.

1. Dal menu **Strumenti,** selezionare **Configura allarmi e-mail**.
   Viene visualizzata la finestra di dialogo **Configura allarmi e-mail**.
2. Se le impostazioni SMTP non sono state configurate oppure si desidera visualizzarle o modificarle, cliccare su **Configura.** Nella finestra di dialogo **Configura impostazioni SMTP**, inserire i dati come descritto sotto.
   a) Nella casella di testo **Indirizzo server**, digitare il nome dell'host o l'indirizzo IP del server SMTP.
   b) Nella casella di testo **Mittente**, digitare un indirizzo e-mail al quale possono essere inviati i "bounce" e i messaggi di mancato recapito.
   c) Cliccare su **Prova** per effettuare il test della connessione.
3. Nel riquadro **Destinatari**, cliccare su **Aggiungi**.
   Viene visualizzata la finestra di dialogo **Aggiungi un nuovo destinatario degli allarmi e-mail**.
4. Nel campo **Indirizzo e-mail**, inserire l'indirizzo del destinatario.
5. Nel campo **Lingua,** selezionare la lingua in cui saranno inviati gli allarmi e-mail.
6. Nel riquadro **Sottoscrizioni**, selezionare gli allarmi e-mail di tipo "Livello di avviso superato" e "Livello critico superato" che si desidera inviare a questo destinatario.

8.9 Impostazione del pannello di controllo e degli allarmi e-mail relativi alla sincronizzazione con Active Directory

Se si utilizza l'amministrazione basata sui ruoli, per poter configurare gli allarmi e-mail relativi alla sincronizzazione con Active Directory, è necessario essere in possesso dei diritti di **Configurazione del sistema**. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile impostare l'invio via e-mail ai destinatari prescelti di allarmi relativi ai nuovi computer e gruppi individuati durante le sincronizzazioni con Active Directory. Se si sceglie di proteggere automaticamente i computer dei gruppi sincronizzati, è possibile anche impostare allarmi sui problemi della protezione automatica.

1. Dal menu **Strumenti,** selezionare **Configura allarmi e-mail**.
   Viene visualizzata la finestra di dialogo **Configura allarmi e-mail**.
2. Se le impostazioni SMTP non sono state configurate oppure si desidera visualizzarle o modificarle, cliccare su **Configura.**

   Nella finestra di dialogo **Configura impostazioni SMTP**, inserire i dati come descritto sotto.

   a) Nella casella di testo **Indirizzo server**, digitare il nome dell'host o l'indirizzo IP del server SMTP.

   b) Nella casella di testo **Mittente**, digitare un indirizzo e-mail al quale possono essere inviati i "bounce" e i messaggi di mancato recapito.

   c) Cliccare su **Prova** per effettuare il test della connessione.
3. Nel riquadro **Destinatari**, cliccare su **Aggiungi**.
   Viene visualizzata la finestra di dialogo **Aggiungi un nuovo destinatario degli allarmi e-mail**.
4. Nel campo **Indirizzo e-mail**, inserire l'indirizzo del destinatario.
5. Nel campo **Lingua,** selezionare la lingua in cui saranno inviati gli allarmi e-mail.
6. Nel riquadro **Sottoscrizioni**, selezionare gli allarmi e-mail di tipo "Sincronizzazione di Active Directory" che si desidera inviare a questo destinatario.

   Allarmi e-mail di tipo "Sincronizzazione di Active Directory":

   - Trovati nuovi gruppi
   - Trovati nuovi computer
   - Protezione automatica dei computer non riuscita

8.10 Configurazione del log eventi di Windows

Se si utilizza l'amministrazione basata sui ruoli:

- Per svolgere questa operazione è necessario possedere i diritti di **Impostazioni del criterio - antivirus e HIPS**.
- Non è possibile modificare un criterio se applicato al di fuori del proprio sottoambiente attivo.

Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

 Copyright © Sophos Limited

Per impostazione predefinita, ogni qual volta un virus o spyware viene rilevato o rimosso, comportamenti o file sospetti vengono rilevati oppure PUA sono rilevate o rimosse, Sophos Endpoint Security and Control aggiunge allarmi al log eventi di Windows.

Per modificare queste impostazioni:

1. Nel riquadro **Criteri**, cliccare due volte sul criterio antivirus e HIPS che si desidera modificare.
2. Nella finestra di dialogo **Criterio antivirus e HIPS**, cliccare su **Messaggistica**.
3. Nella finestra di dialogo **Messaggistica**, andare alla scheda **Log eventi**.

   Per impostazione predefinita, il log eventi è abilitato. Se necessario modificare le impostazioni.

   Gli **errori di scansione** sono gli errori che si verificano quando a Sophos Endpoint Security and Control viene negato l'accesso a un oggetto che tenta di esaminare.

8.11 Attivazione e disattivazione dei feedback a Sophos

Se si utilizza l'amministrazione basata sui ruoli, è necessario essere in possesso dei diritti di **Configurazione del sistema** per attivare o disattivare i feedback a Sophos. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Enterprise Console invierà a Sophos report a cadenza regolare. Questi report aiutano Sophos a capire come vengono utilizzati i propri prodotti e contribuiscono a migliorare i nostri prodotti e servizi. Per informazioni dettagliate sul tipo di informazioni raccolte e su come vengano utilizzate, consultare il Sophos End User License Agreement (Contratto di licenza Sophos per l'utente finale) e il Sophos Privacy Policy (Politica Sophos sulla privacy) reperibili su questo link: http://www.sophos.com/it-it/legal.

Alcune delle informazioni riportate sono opzionali, mentre altre sono obbligatorie, come descritto in maniera più dettagliata nell'EULA (End User License Agreement, Contratto di licenza per l'utente finale) e nella Privacy Policy (Politica sulla privacy). È possibile ritirare il proprio consenso per l'inserimento delle informazioni facoltative nei report, modificando l'impostazione **Feedback a Sophos**.

Per impostazione predefinita, l'opzione Feedback a Sophos è abilitata. È possibile disabilitare questa opzione durante l'installazione o l'upgrade della console, nella procedura guidata di installazione di Sophos Enterprise Console.

Se si desidera attivare o disattivare l'invio di feedback a Sophos, procedere come segue:

1. Nel menu **Strumenti**, cliccare su **Feedback a Sophos**.
2. Nella finestra di dialogo **Feedback a Sophos**, è possibile abilitare o disabilitare l'invio di feedback a Sophos.
   - *Se si desidera abilitare il'invio di feedback a Sophos,* leggere il contratto di licenza e selezionare la casella **Do il consenso** se ne accettano i termini.
   - *Se si desidera disabilitare l'invio di feedbacka Sophos,* deselezionare la casella di controllo **Do il consenso**.

9 Visualizzazione eventi

Quando si verifica un evento di controllo applicazioni, dati e dispositivi, firewall, verifica delle patch, blocco rimozione, controllo web o evento della prevenzione degli exploit in un computer endpoint (ad esempio se un'applicazione è stata bloccata dal firewall), tale evento viene inviato a Enterprise Console e può essere visionato nel relativo visualizzatore eventi.

Tramite il visualizzatore eventi è possibile analizzare gli eventi che si sono verificati nella rete. È inoltre possibile creare un elenco di eventi basato su un filtro a propria scelta, per es. un elenco di tutti gli eventi del controllo dati generati da un determinato utente negli ultimi sette giorni.

Il numero di computer con eventi che hanno superato una determinata soglia entro gli ultimi 7 giorni viene visualizzato nel pannello di controllo (esclusi gli eventi del blocco rimozione). Per informazioni sull'impostazione del livello di soglia, consultare la sezione Configurazione del pannello di controllo (pagina 48).

È inoltre possibile impostare allarmi da inviare a destinatari prescelti ogni qual volta si verifichi un evento. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

9.1 Visualizzazione degli eventi del controllo applicazioni

Per visualizzare gli eventi del controllo applicazioni:

1. Dal menu **Eventi**, cliccare su **Eventi controllo applicazioni**.
   Si apre la finestra di dialogo **Controllo applicazioni - Visualizzatore eventi**.
2. Nel campo **Periodo ricerca**, cliccare sulla freccia dell'elenco a discesa e selezionare il periodo in cui si desidera visualizzare gli eventi.

   È possibile selezionare un periodo fisso, per es. **Entro 24 ore**, oppure l'opzione **Personalizzato** e indicare il periodo prescelto selezionando l'orario e la data di inizio e fine.
3. Se si desidera visualizzare gli eventi relativi a un determinato tipo di utente o computer, inserirne il nome nel campo relativo.

   Se i campi vengono lasciati vuoti, verranno visualizzati gli eventi relativi a tutti gli utenti e i computer.

   In questi campi possono essere utilizzati caratteri jolly. Utilizzare ? per ogni singolo carattere e * per ogni stringa di caratteri.
4. Se si desidera visualizzare gli eventi per un determinato tipo di applicazione, nel campo **Tipo applicazione**, cliccare sulla freccia dell'elenco a discesa e selezionare il tipo di applicazione.

   Per impostazione predefinita, il visualizzatore eventi mostra gli eventi relativi a tutti i tipi di applicazione.
5. Cliccare su **Cerca** per visualizzare un elenco di eventi.

È possibile esportare in un file l'elenco di eventi del controllo applicazioni. Per ulteriori informazioni, vedere Esportazione dell'elenco eventi in un file (pagina 205).

 Copyright © Sophos Limited

9.2 Visualizzazione di eventi del controllo dati

Nota
Questa funzione non sarà disponibile se la licenza non include il Controllo dati.

Se si utilizza l'amministrazione basata sui ruoli, è necessario essere in possesso dei diritti per **Eventi del controllo dati** al fine di poterli visionare in Enterprise Console. Per ulteriori informazioni sull'amministrazione basata sui ruoli, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per visualizzare gli eventi del controllo dati:

1. Dal menu **Eventi**, cliccare su **Eventi controllo dati**.
   Si apre la finestra di dialogo **Controllo dati - Visualizzatore eventi**.
2. Nel campo **Periodo ricerca**, cliccare sulla freccia dell'elenco a discesa e selezionare il periodo in cui si desidera visualizzare gli eventi.

   È possibile selezionare un periodo fisso, per es. **Entro 24 ore**, oppure l'opzione **Personalizzato** e indicare il periodo prescelto selezionando l'orario e la data di inizio e fine.
3. Se si desidera visualizzare gli eventi relativi a un determinato tipo di utente, computer o file, inserirne il nome nel campo relativo.

   Se i campi vengono lasciati vuoti, verranno visualizzati gli eventi relativi a tutti gli utenti, i computer ed i file.

   In questi campi possono essere utilizzati caratteri jolly. Utilizzare ? per ogni singolo carattere e * per ogni stringa di caratteri.
4. Se si desidera visualizzare eventi relativi a determinate regole, nel campo **Nome regola**, cliccare sulla freccia dell'elenco a discesa e selezionare il nome della regola.

   Per impostazione predefinita, il visualizzatore eventi mostra gli eventi relativi a tutte le regole.
5. Se si desidera visualizzare gli eventi per un determinato tipo di file, nel campo **Tipo file**, cliccare sulla freccia dell'elenco a discesa e selezionare il tipo di file.

   Per impostazione predefinita, il visualizzatore eventi mostra gli eventi relativi a tutti i tipi di file.
6. Cliccare su **Cerca** per visualizzare un elenco di eventi.

È possibile esportare in un file l'elenco di eventi del controllo dati. Per ulteriori informazioni, vedere Esportazione dell'elenco eventi in un file (pagina 205).

9.3 Visualizzazione degli eventi del controllo dispositivi

Per visualizzare gli eventi del controllo dispositivi:

1. Dal menu **Eventi**, cliccare su **Eventi controllo dispositivi**.
   Si apre la finestra di dialogo **Controllo dispositivi - Visualizzatore eventi**.
2. Nel campo **Periodo ricerca**, cliccare sulla freccia dell'elenco a discesa e selezionare il periodo in cui si desidera visualizzare gli eventi.

   È possibile selezionare un periodo fisso, per es. **Entro 24 ore**, oppure l'opzione **Personalizzato** e indicare il periodo prescelto selezionando l'orario e la data di inizio e fine.
3. Se si desidera visualizzare gli eventi relativi a un determinato tipo di dispositivo, nel campo **Tipi di dispositivo**, cliccare sulla freccia dell'elenco a discesa e selezionare il tipo di dispositivo.

Per impostazione predefinita, il visualizzatore eventi mostra gli eventi relativi a tutti i tipi di dispositivo.

Nota
Se le unità disco ottico vengono impostate su "Sola lettura", gli eventi di questi dispositivi non verranno visualizzati nel visualizzatore eventi.

4. Se si desidera visualizzare gli eventi relativi a un determinato tipo di utente o computer, inserirne il nome nel campo relativo.

   Se i campi vengono lasciati vuoti, verranno visualizzati gli eventi relativi a tutti gli utenti e i computer.

   In questi campi possono essere utilizzati caratteri jolly. Utilizzare ? per ogni singolo carattere e * per ogni stringa di caratteri.
5. Cliccare su **Cerca** per visualizzare un elenco di eventi.

Nella finestra di dialogo **Controllo dispositivi - Visualizzatore eventi**, è possibile esentare un particolare dispositivo dai criteri relativi al controllo dispositivi. Per ulteriori informazioni, vedere Esenzione di un dispositivo da tutti i criteri (pagina 166).

È possibile esportare in un file l'elenco di eventi del controllo dispositivi. Per ulteriori informazioni, vedere Esportazione dell'elenco eventi in un file (pagina 205).

9.4 Visualizzazione degli eventi del firewall

Gli eventi del firewall vengono inviati solo una volta dal computer alla console. Eventi identici provenienti da diversi computer vengono raggruppati insieme nel **Firewall - Visualizzatore eventi**. Nella colonna **Conteggio**, viene visualizzato il numero totale di volte in cui un evento è stato inviato da diversi computer.

Per visualizzare gli eventi del firewall:

1. Dal menu **Eventi**, cliccare su **Eventi firewall**.
   Viene visualizzata la finestra di dialogo **Firewall - Visualizzatore eventi**.
2. Nel campo **Periodo ricerca**, cliccare sulla freccia dell'elenco a discesa e selezionare il periodo in cui si desidera visualizzare gli eventi.

   È possibile selezionare un periodo fisso, per es. **Entro 24 ore**, oppure l'opzione **Personalizzato** e indicare il periodo prescelto selezionando l'orario e la data di inizio e fine.
3. Se si desidera visualizzare gli eventi di un certo tipo, nel campo **Tipo di evento**, cliccare sulla freccia dell'elenco a discesa e selezionare il tipo di evento.

   Per impostazione predefinita il visualizzatore eventi visualizza tutti i tipi di evento.
4. Se si desidera visualizzare gli eventi per un certo file, nel campo **Nome file**, inserire il nome del file.

   Se questo campo viene lasciato vuoto, verranno visualizzati gli eventi per tutti i file.

   In questo campo si possono utilizzare caratteri jolly. Utilizzare ? per ogni singolo carattere e * per ogni stringa di caratteri.
5. Cliccare su **Cerca** per visualizzare un elenco di eventi.

Nella finestra di dialogo **Firewall - Visualizzatore eventi**, è possibile creare una regola del firewall come descritto nella sezione Creazione di una regola per gli eventi del firewall (pagina 118).

È possibile esportare in un file l'elenco di eventi del controllo dispositivi. Per ulteriori informazioni, vedere Esportazione dell'elenco eventi in un file (pagina 205).

 Copyright © Sophos Limited

9.5 Visualizzazione degli eventi del blocco rimozione

Esistono due tipi di eventi del blocco rimozione:

- Per gli eventi di autenticazione del blocco rimozione riusciti, viene riportato il nome dell'utente autenticato e l'orario dell'autenticazione.
- Nel caso si tentativi di sabotaggio falliti vengono riportati i nomi dei componenti o dei prodotti Sophos oggetto di attacco, l'orario del tentativo e i dettagli dell'utente responsabile di tale tentativo.

Visualizzazione degli eventi del blocco rimozione:

1. Dal menu **Eventi**, cliccare su **Eventi blocco rimozione**.
   Si apre la finestra di dialogo **Blocco rimozione - Visualizzatore eventi**.
2. Nel campo **Periodo ricerca**, cliccare sulla freccia dell'elenco a discesa e selezionare il periodo in cui si desidera visualizzare gli eventi.

   È possibile selezionare un periodo fisso, per es. **Entro 24 ore**, oppure l'opzione **Personalizzato** e indicare il periodo prescelto selezionando l'orario e la data di inizio e fine.
3. Se si desidera visualizzare eventi di un certo tipo, nel campo **Tipo di evento**, cliccare sulla freccia dell'elenco a discesa e selezionare il tipo di evento.

   Per impostazione predefinita, il visualizzatore eventi mostra gli eventi relativi a tutti i tipi di file.
4. Se si desidera visualizzare gli eventi relativi a un determinato tipo di utente o computer, inserirne il nome nel campo relativo.

   Se i campi vengono lasciati vuoti, verranno visualizzati gli eventi relativi a tutti gli utenti e i computer.

   In questi campi possono essere utilizzati caratteri jolly. Utilizzare ? per ogni singolo carattere e * per ogni stringa di caratteri.
5. Cliccare su **Cerca** per visualizzare un elenco di eventi.

È possibile esportare l'elenco degli eventi in un file. Per ulteriori informazioni, vedere Esportazione dell'elenco eventi in un file (pagina 205).

9.6 Eventi verifica patch

Nota
Questa funzione non sarà disponibile se la licenza non include la Verifica patch.

La **Verifica Patch - Visualizzatore eventi** offre informazioni sulle patch di protezione e i risultati relativi alla verifica delle patch.

Il campo **Aggiornamenti patch** visualizza lo stato di download della patch e mostra i seguenti messaggi di stato:

- **Non scaricata** indica che la patch non è stata scaricata o che non si possiede la licenza per l'utilizzo della funzione Patch.
- **Download** indica che il primo download, dopo l'installazione, è ancora in esecuzione.
- **OK** indica che la patch è aggiornata.
- **Scaduta** indica che nelle ultime 72 ore non è avvenuto un aggiornamento completo dei dati della patch. Solitamente questo messaggio di stato viene visualizzato quando SEC non è aggiornata a

causa di problemi relativi alla connettività di rete, oppure se si modifica la licenza da una SEC con funzione Patch a una sprovvista di tale funzione. Quando viene visualizzato questo messaggio di stato, è possibile che si sia verificato un aggiornamento solo parziale.

La **Verifica patch - Visualizzatore eventi** include le seguenti schede:

Patch per livello di minaccia

Per impostazione predefinita questa scheda visualizza le patch mancanti. Insieme alla patch viene visualizzato il numero di computer in cui manca, oltre che le minacce e vulnerabilità collegate a tale patch. È possibile utilizzare filtri per ottenere un elenco completo di tutte le patch supportate e il numero di computer in cui mancano.

Computer con patch mancanti

Questa scheda visualizza lo stato della verifica per computer. Vengono visualizzati tutti i computer e le relative patch mancanti. I computer con più di una patch mancante vengono citati più volte all'interno dell'elenco.

9.6.1 Visualizzazione degli eventi relativi alla verifica delle patch

Per visualizzare gli eventi relativi alla verifica delle patch:

1. Nel menu **Eventi**, cliccare su **Eventi verifica patch**.
   Si apre la finestra di dialogo **Verifica patch - Visualizzatore eventi**.
2. Cliccare su una delle schede **Patch per livello di minaccia** o **Computer con patch mancanti**.
   Per ulteriori informazioni sulle schede, consultare la sezione Eventi verifica patch (pagina 199).
3. Nel pannello di ricerca, se si desidera visualizzare gli eventi per patch, nome, computer, minaccia o vulnerabilità inserire le informazioni necessarie nei campi adeguati. I criteri a disposizione si basano sulle informazioni visualizzate nella scheda.

   Se i campi vengono lasciati vuoti, verranno visualizzati gli eventi relativi a tutti i nomi delle patch, ID delle patch e nomi dei computer.

   In questi campi possono essere utilizzati caratteri jolly. Utilizzare ? per ogni singolo carattere e * per ogni stringa di caratteri.
4. Se si desidera visualizzare eventi relativi ad un determinato stato della patch, livello di minaccia, fornitore, gruppo o data di rilascio, cliccare sulla freccia del menu a discesa nei rispettivi campi e selezionare le opzioni adeguate. I criteri a disposizione si basano sulle informazioni visualizzate nella scheda.

   Per impostazione predefinita, il visualizzatore eventi visualizza gli eventi relativi ai livelli di minaccia, fornitori, gruppi, minacce e il nome delle patch.
5. Cliccare su **Cerca** per visualizzare un elenco di eventi di verifica delle patch.
   Per informazioni sui risultati visualizzati, consultare la sezione Categorie dei risultati della ricerca (pagina 201).

È possibile cliccare col tasto destro del mouse su ciascun collegamento ipertestuale per copiarne il nome, oppure, per copiare un evento della verifica petch sugli Appunti, premere Ctrl+C.

È possibile esportare l'elenco di eventi di verifica delle patch. Per ulteriori informazioni, vedere Esportazione dell'elenco eventi in un file (pagina 205).

È possibile visualizzare i dati relativi a una determinata patch cliccando sul link a disposizione.
Per ulteriori informazioni, consultare la sezione Visualizzazione dei dati relativi a patch, minacce o vulnerabilità (pagina 201).

 Copyright © Sophos Limited

9.6.2 Visualizzazione dei dati relativi a patch, minacce o vulnerabilità

Per visualizzare i dati relativi a patch, minacce o vulnerabilità:

1. Nel menu **Eventi**, cliccare su **Eventi verifica patch**.
   Si apre la finestra di dialogo **Verifica patch - Visualizzatore eventi**.
2. Cliccare sulle schede **Patch per livello di minaccia** o **Computer con patch mancanti**, selezionare l'opzine desiderata e cliccare su **Cerca** per visualizzare l'elenco eventi.
   Per informazioni sui risultati visualizzati, consultare la sezione Categorie dei risultati della ricerca (pagina 201).
3. Se si desidera visionare ulteriori dati relativi a una patch, cliccare sul nome di tale patch.
4. Nella finestra di dialogo **Dati patch**, è possibile visionare una descrizione della patch, oltre che informazioni sulle minacce e vulnerabilità da cui protegge i computer. Se disponibile, è possibile:
   - Cliccare sul nome della patch per aprire un browser web in cui vengono visualizzate informazioni del fornitore su quella determinata patch.
   - Cliccare sul nome della minaccia per aprire un browser web e visualizzare l'analisi di tale minaccia ed eventuali consigli forniti da Sophos.
   - Cliccare sul nome della vulnerabilità per aprire un browser web e visualizzare informazioni relative a vulnerabilità ed esposizioni comuni (CVE).
   - Cliccare sul nome della patch nella colonna **In precedenza trattata da** per aprire il browser web e visualizzare le informazioni del fornitore sulla patch sostituita.

L'elenco è organizzato in ordine alfabetico, prima per minaccia e poi per vulnerabilità.

9.6.3 Categorie dei risultati della ricerca

I risultati della ricerca vengono visualizzati secondo le categorie:

- Patch per livello di minaccia (pagina 201)
- Computer con patch mancanti (pagina 202)

Patch per livello di minaccia

I risultati di questa ricerca vengono visualizzati in base alle seguenti categorie:

- **Minacce**: per minaccia si intende un virus, trojan, worm, spyware, sito web malevolo, oltre che adware e altre applicazioni potenzialmente indesiderate. Cliccando sul nome della minaccia è possibile visualizzare, in un browser web, analisi della minaccia e consigli di Sophos.
- **Vulnerabilità**: per vulnerabilità si intende una pecca del software che può essere sfruttata dagli autori di attacchi informatici. Il danno potenziale causato dallo sfruttamento di eventuali vulnerabilità dipende dalla loro natura e dal software coinvolto. Le patch vengono fornite per risolvere le vulnerabilità, in modo tale da neutralizzarle. Cliccando sul nome della vulnerabilità è possibile visualizzare, in un browser web, informazioni relative a vulnerabilità comuni ed esposizioni (CVE).
- **Livello della minaccia**: SophosLabs attribuisce alle patch un determinato livello di minaccia.

Copyright © Sophos Limited

Nota
Si consiglia di applicare tutte le patch mancanti a prescindere dal livello di minaccia attribuito loro.

— **Critico**: è quasi certo che una delle vulnerabilità a cui si riferisce la patch venga utilizzata.

— **Alto**: è molto probabile che una delle vulnerabilità a cui si riferisce la patch venga utilizzata.

— **Medio**: è possibile che una delle vulnerabilità a cui si riferisce la patch venga utilizzata.

— **Basso**: è poco probabile che una delle vulnerabilità a cui si riferisce la patch venga utilizzata.

- **Nome patch**: visualizza il nome della patch. È possibile cliccare sul nome della patch per aprire un browser web in cui vengono visualizzate informazioni del fornitore su quella determinata patch.
- **Fornitore**: visualizza il nome del fornitore che ha pubblicato la patch.
- **Computer**: visualizza il numero di computer coinvolti. Se si tratta di uno o più computer, è possibile cliccare sul numero per visualizzare maggiori dettagli nella scheda **Computer con patch mancanti**. Se vine visualizzato questo simbolo "-", la patch non è stata verificata.
- **Sostituita da**: visualizza il nome o i nomi di tutte le patch sosituite. È possibile cliccare sul nome della patch per aprire la finestra di dialogo **Dettagli patch**e visualizzare informazioni relative alle patch di sostituzione.
- **Data di rilascio**: visualizza la data di rilascio della patch.

Computer con patch mancanti

I risultati di questa ricerca vengono visualizzati in base alle seguenti categorie:

- **Computer**: visualizza il nome del computer coinvolto.
- **Livello della minaccia**: SophosLabs attribuisce alle patch un determinato livello di minaccia.

Nota
Si consiglia di applicare tutte le patch mancanti a prescindere dal livello di minaccia attribuito loro.

— **Critico**: è quasi certo che una delle vulnerabilità a cui si riferisce la patch venga utilizzata.

— **Alto**: è molto probabile che una delle vulnerabilità a cui si riferisce la patch venga utilizzata.

— **Medio**: è possibile che una delle vulnerabilità a cui si riferisce la patch venga utilizzata.

— **Basso**: è poco probabile che una delle vulnerabilità a cui si riferisce la patch venga utilizzata.

- **Nome patch**: visualizza il nome della patch. È possibile cliccare sul nome della patch per aprire un browser web in cui vengono visualizzate informazioni del fornitore su quella determinata patch.
- **Sostituita da**: visualizza il nome o i nomi di tutte le patch sosituite. È possibile cliccare sul nome della patch per aprire la finestra di dialogo **Dettagli patch**e visualizzare informazioni relative alle patch di sostituzione.
- **Ultima verifica**: visualizza la data dell'ultima verifica del computer alla ricerca delle patch mancanti.
- **Fornitore**: visualizza il nome del fornitore che ha pubblicato la patch.
- **Data di rilascio**: visualizza la data di rilascio della patch.
- **Gruppo**: visualizza il nome del gruppo a cui appartiene il computer.

 Copyright © Sophos Limited

9.7 Visualizzazione degli eventi web

Nota
Questa funzione non sarà disponibile se la licenza non include il Controllo web.

Se si utilizza l'amministrazione basata sui ruoli, è necessario essere in possesso dei diritti per **Eventi web** per poterli visionare in Enterprise Console. Per ulteriori informazioni sull'amministrazione basata sui ruoli, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

È possibile visualizzare i seguenti eventi web nel Visualizzatore eventi web:

- Siti web malevoli, bloccati dalla funzione di Protezione web nel criterio **Anti-virus e HIPS**.
- Eventi di controllo web, se si utilizza la funzione di Web Control (controllo web).

Gli eventi di controllo web vengono visualizzati in modo differente, a seconda del criterio di controllo web selezionato. Anche sa il Visualizzatore eventi web può essere utilizzato in entrambe le modalità del criterio, il contenuto è differente.

Se l'opzione del criterio **Controllo siti web inappropriati** è selezionata, è possibile visualizzare tutte le azioni «blocca» e «avvisa». Quando si visitano siti HTTPS soggetti all'azione «Avvisa», questi vengono registrati come eventi a cui applicare l'azione «Procedi» dal momento che Sophos Endpoint Security and Control tratta in modo differente i siti HTTPS (v. note nella sezione Controllo siti web inappropriati (pagina 175)).

Se si è selezionata l'opzione **Controllo web completo**, gli eventi vengono visualizzati nell'appliance.

- Per la Sophos Web Appliance o Management Appliance, è possibile visionare le attività di utilizzo del web utilizzando le funzioni di **Report** e **Ricerca**. Le azioni «blocca», «avvisa» e «consenti» vengono tutte visualizzate. Quando si visitano siti HTTPS soggetti all'azione «Avvisa», questi vengono visualizzati come eventi a cui applicare l'azione «Procedi» dal momento che Sophos Endpoint Security and Control tratta in modo differente i siti HTTPS (v. note nella sezione Controllo web completo (pagina 180)).
- Per UTM, utilizzare l'opzione **Accesso & Reportistica** > **Web Protection** > **Report sull'utilizzo del Web**. Qui è possibile visionare le azioni che confermano il delivery del sito Web al client (passato), se il sito sia stato bloccato da una regola del controllo delle applicazioni, oppure se l'utente sia riuscito ad accedere alla pagina bloccata utilizzando la funzione di bypass del blocco (sovrascritto), oltre che altre informazioni utili.

Nota
A prescindere dal criterio prescelto, i siti web, scansionati e verificati in tempo reale dal filtro URL di Sophos Endpoint Security and Control (Protezione web (pagina 102)), vengono visualizzati come eventi web in Enterprise Console.

Per visualizzare gli eventi web:

1. Dal menu **Eventi**, cliccare su **Eventi web**.
   Viene visualizzata la finestra di dialogo **Web - Visualizzatore eventi**.
2. Nella casella **Periodo ricerca**, cliccare sulla freccia dell'elenco a discesa e selezionare il periodo in cui si desidera visualizzare gli eventi.

   È possibile selezionare un periodo fisso, per es. **Entro 24 ore**, oppure l'opzione **Personalizzato** e indicare il periodo prescelto selezionando l'orario e la data di inizio e fine.
3. Se si desidera visualizzare gli eventi riguardanti un determinato **Utente** o **Computer**, compilare i campi relativi a queste voci.

Se i campi vengono lasciati vuoti, verranno visualizzati gli eventi relativi a tutti gli utenti e i computer.

In questi campi possono essere utilizzati caratteri jolly. Utilizzare ? per ogni singolo carattere e * per ogni stringa di caratteri.

4. Se si desidera visualizzare eventi relativi a determinate azioni, nel campo **Azione**, cliccare sulla freccia dell'elenco a discesa e selezionare il nome dell'azione.
5. Se si desidera visualizzare eventi riguardanti un determinato dominio, inserirlo nel campo **Dominio**.
6. Se si desidera visualizzare eventi generati per un determinato **Motivo**, cliccare sulla freccia dell'elenco a discesa e selezionare il motivo.
7. Cliccare su **Cerca** per visualizzare un elenco di eventi.

È possibile esportare in un file l'elenco di eventi web. Per ulteriori informazioni, vedere Esportazione dell'elenco eventi in un file (pagina 205).

9.7.1 Visualizzazione nel computer degli eventi web più recenti

È possibile visualizzare gli ultimi 10 eventi che hanno richiesto l'esecuzione di un'azione nel computer endpoint, per esempio gli ultimi siti web bloccati.

Per visualizzare gli eventi web più recenti:

1. Nella vista **Computer**, nell'elenco dei computer, cliccare due volte sul computer la cui attività si desidera visionare.
2. Nella finestra di dialogo **Dettagli computer**, scorrere giù fino alla sezione **Eventi web recenti**.

È anche possibile visionare il numero di eventi per utente generando un report. Per ulteriori informazioni, consultare la sezione Configurazione del report Eventi in base all'utente (pagina 213).

9.8 Eventi della prevenzione degli exploit

Nota
Questa funzionalità non sarà disponibile se la licenza non include la Prevenzione degli exploit.

Se si utilizza l'amministrazione basata sui ruoli, occorre avere il diritto **Prevenzione degli exploit** per visualizzare gli eventi di prevenzione degli exploit in Enterprise Console. Per ulteriori informazioni sull'amministrazione basata sui ruoli, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per visualizzare gli eventi della prevenzione degli exploit:

1. Dal menù **Eventi**, cliccare su **Prevenzione degli exploit**.
   Si apre la finestra di dialogo **Prevenzione degli exploit - Visualizzatore eventi**.
2. Nella casella **Periodo ricerca**, cliccare sulla freccia dell'elenco a discesa e selezionare il periodo in cui si desidera visualizzare gli eventi.

   È possibile selezionare un periodo fisso, per es. **Entro 24 ore**, oppure l'opzione **Personalizzato** e indicare il periodo prescelto selezionando l'orario e la data di inizio e fine.
3. Se si desidera visualizzare gli eventi riguardanti un determinato **Utente** o **Computer**, compilare i campi relativi a queste voci.

   Se i campi vengono lasciati vuoti, verranno visualizzati gli eventi relativi a tutti gli utenti e i computer.

 Copyright © Sophos Limited

In questi campi possono essere utilizzati caratteri jolly. Utilizzare ? per ogni singolo carattere e * per ogni stringa di caratteri.

4. Se si desidera visualizzare eventi associati a un tipo in particolare, nel campo **Tipo**, cliccare sulla freccia dell'elenco a discesa e selezionare il tipo desiderato.
5. Cliccare su **Cerca** per visualizzare un elenco di eventi.

- È possibile esportare in un file l'elenco di eventi di prevenzione degli exploit. Per ulteriori informazioni, vedere Esportazione dell'elenco eventi in un file (pagina 205).
- È possibile escludere eventi di prevenzione degli exploit dalla prevenzione degli exploit. Vedere Esclusione di eventi dalla prevenzione degli exploit (pagina 205).

9.9 Esportazione dell'elenco eventi in un file

È possibile esportare l'elenco degli eventi relativi a controllo di applicazioni, dati e dispositivi, firewall, verifica delle patch, blocco rimozione, eventi web o eventi di prevenzione degli exploit, creando un file con valori delimitati da virgole (CSV). È inoltre possibile esportare l'elenco di eventi relativi alla verifica delle patch in un file PDF.

1. Nel menu **Eventi**, cliccare su una delle opzioni "eventi", a seconda dell'elenco eventi che si desidera esportare.
   Viene visualizzata la finestra di dialogo **Visualizzatore eventi**.
2. Se si desidera visualizzare solo determinati eventi, nel riquadro **Criteri di ricerca**, impostare i filtri adeguati e cliccare su **Cerca** per visualizzare tali eventi.

   Per maggiori informazioni, consultare:

   - Visualizzazione degli eventi del controllo applicazioni (pagina 196)
   - Eventi del controllo dei dati (pagina 152)
   - Eventi del controllo dispositivi (pagina 162)
   - Visualizzazione degli eventi del firewall (pagina 198)
   - Eventi verifica patch (pagina 199)
   - Visualizzazione degli eventi del blocco rimozione (pagina 199)
   - Visualizzazione degli eventi web (pagina 203)
   - Eventi della prevenzione degli exploit (pagina 204)
3. Cliccare su **Esporta**.
4. Nella finestra **Salva con nome**, selezionare un percorso in cui salvare il file, inserire il nome del file nel campo **Nome file** e scegliere un tipo di file nel campo **Salva come**.
5. Cliccare su **Salva**.

9.10 Esclusione di eventi dalla prevenzione degli exploit

È possibile escludere applicazioni ed eventi della prevenzione degli exploit dalla prevenzione degli exploit: basta selezionare eventi specifici dal visualizzatore eventi.

1. Dal menù **Eventi**, cliccare su **Eventi prevenzione degli exploit**.
   Viene visualizzata la finestra di dialogo **Visualizzatore eventi**.

2. Se si desidera visualizzare solo determinati eventi, nel riquadro **Criteri di ricerca**, impostare i filtri adeguati e cliccare su **Cerca** per visualizzare tali eventi.

   Per ulteriori informazioni, consultare la sezione Eventi della prevenzione degli exploit (pagina 204).
3. Selezionare un evento e cliccare su **Escludi**.
   Si apre la finestra di dialogo **Esclusioni della prevenzione degli exploit**.
4. Cliccare sul criterio che si desidera modificare. Per modificare le impostazioni in tutti i criteri, cliccare su **Seleziona tutto**.
5. Nella sezione **Evento di exploit** o **Applicazione**, cliccare su **Escludi**
6. Cliccare su **OK**.

L'evento della prevenzione degli exploit o l'applicazione verrà escluso dalla prevenzione degli exploit per i criteri selezionati.

 Copyright © Sophos Limited

10 Creazione dei report

I report forniscono informazioni testuali e grafiche su una varietà di aspetti relativi allo stato di sicurezza della rete.

I report sono disponibili tramite **Report Manager**. Tramite **Report Manager**, è possibile creare rapidamente un report basato su modelli esistenti, cambiare la configurazione di un report esistente e pianificare un report perché venga eseguito a intervalli regolari ed i risultati inviati al destinatario prescelto sotto forma di allegato di posta elettronica. È inoltre possibile stampare report ed esportarli in diversi formati.

Sophos fornisce un numero di report da utilizzare senza modificarli o adattandoli alle proprie esigenze. Tali report sono:

- Cronologia allarmi ed eventi
- Riepilogo allarmi
- Allarmi ed eventi per nome dell'oggetto
- Allarmi ed eventi per orario
- Allarmi ed eventi per percorso
- Non conforme al criterio del computer
- Eventi per utente
- Protezione dei computer gestiti
- Gerarchia aggiornamenti

Report e amministrazione basata sul ruolo

Se si utilizza un'amministrazione basata sui ruoli, è necessario essere in possesso dei diritti di **Configurazione report** per creare, modificare o cancellare un report. Se non si è in possesso di tali diritti, è unicamente possibile eseguire un report. Per ulteriori informazioni sull'amministrazione basata sui ruoli, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Un report può includere dati provenienti solo da sottoambienti attivi. Non è possibile condividere report tra diversi sottoambienti. I report predefiniti non vengono copiati dal sottoambiente **Predefinito** ai nuovi sottoambienti creati.

Quando si cancella un sottoambiente, anche tutti i report in tale sottoambiente vengono cancellati.

10.1 Creazione di un nuovo report

Se si utilizza l'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Configurazione report**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Per creare un report:

1. Cliccare sull'icona **Report** posta sulla barra degli strumenti.
2. Nella finestra di dialogo **Report Manager**, cliccare su **Crea**.
3. Nella finestra di dialogo **Crea nuovo report**, selezionare un modello di report e cliccare su **OK**.

Una procedura guidata accompagnerà durante le operazioni di creazione di report basati modelli prescelti.

Se non si desidera utilizzare la procedura guidata, nella finestra di dialogo **Crea nuovo report**, deselezionare la casella di spunta **Utilizza la procedura guidata per creare report**. È quindi possibile configurare il nuovo report nella finestra di dialogo relativa alle proprietà dei report. Per ulteriori informazioni, riferirsi all'argomento relativo alla configurazione di report rilevanti.

10.2 Configurazione del report Cronologia allarmi ed eventi

Se si utilizza l'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Configurazione report**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Il rapporto **Cronologia allarmi ed eventi** mostra gli allarmi e gli eventi per un periodo del report specificato.

1. Cliccare sull'icona **Report** posta sulla barra degli strumenti.
2. Nella finestra di dialogo **Report Manager**, selezionare **Cronologia allarmi ed eventi** e cliccare su **Proprietà**.
3. Nella finestra di dialogo **Proprietà cronologia allarmi ed eventi**, nella scheda **Configurazione**, impostare le opzioni desiderate.
   a) Nel riquadro **Dettagli del report**, modificare il nome e la descrizione del report, se lo si desidera.
   b) Nel riquadro **Periodo del report**, nella casella di testo **Periodo**, cliccare sulla freccia dell'elenco a discesa e selezionare un periodo di tempo.

      È possibile selezionare un periodo fisso, per es. **Mese scorso**, oppure **Personalizzato** specificando il periodo di tempo desiderato nei campi **Inizio** e **Fine**.
   c) Nel riquadro **Percorso del report**, cliccare su **Gruppo di computer** o **Computer singolo**. Quindi cliccare sulla freccia del menu a discesa per specificare un gruppo o un computer.
   d) Nel riquadro **Allarmi e tipi di evento da includere**, selezionare i tipi di allarmi che si desidera includere nel report.

      Per impostazione predefinita, il report mostra tutti i tipi di allarme e di evento.

      In alternativa, è possibile configurare il report in modo tale che visualizzi soltanto le posizioni in cui è stato segnalato un particolare allarme o evento. Per specificare un singolo allarme o evento, cliccare su **Avanzate** e quindi su un nome di allarme o evento nell'elenco. Per specificare più di un allarme o evento, digitare un nome nella casella di testo utilizzando i caratteri jolly. Utilizzare ? per ogni singolo carattere nel nome, e * per ogni stringa di caratteri. Per esempio, W32/* si riferisce a tutti i virus i cui nomi iniziano per W32/.
4. Nella scheda **Mostra opzioni**, selezionare come si desidera ordinare gli allarmi e eventi.

   Per impostazione predefinita, i dettagli di allarmi ed eventi sono ordinati in base a **Nome allarme ed evento**. Tuttavia, i report possono essere ordinati anche per **Nome computer**, **Nome gruppo** del computer, oppure per **Data e ora**.
5. Nel riquadro **Operazione pianificata**, selezionare **Pianifica questo report** se si desidera eseguire i report ad intervalli regolari ed inviarne i risultati sotto forma di allegati e-mail ai destinatari prescelti. Inserire la data e l'ora di inizio, oltre che la frequenza con cui verranno generati i report, specificare il formato e la lingua del file di output ed inserire gli indirizzi e-mail dei destinatari dei report.

 Copyright © Sophos Limited

10.3 Configurazione del report Riepilogo allarmi

Se si utilizza l'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Configurazione report**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Il report **Riepilogo allarmi** fornisce dati statistici relativi alla salute e allo stato di tutta la rete.

1. Cliccare sull'icona **Report** posta sulla barra degli strumenti.
2. Nella finestra di dialogo **Report Manager**, selezionare **Riepilogo allarmi** e cliccare su **Proprietà**.
3. Nella finestra di dialogo **Proprietà riepilogo allarmi**, nella scheda **Configurazione**, impostare le opzioni desiderate.
   a) Nel riquadro **Dettagli del report**, modificare il nome e la descrizione del report, se lo si desidera.
   b) Nel riquadro **Periodo del report**, nella casella di testo **Periodo**, cliccare sulla freccia dell'elenco a discesa e selezionare un periodo di tempo.

      È possibile selezionare un periodo fisso, per es. **Mese scorso**, oppure **Personalizzato** specificando il periodo di tempo desiderato nei campi **Inizio** e **Fine**.
4. Nel riquadro **Mostra opzioni**, sotto **Mostra risultati per**, specificare gli intervalli di tempo in cui viene misurata la non conformità, per es. ogni ora o giorno, cliccare sulla freccia dell'elenco a discesa e selezionare un intervallo.
5. Nel riquadro **Operazione pianificata**, selezionare **Pianifica questo report** se si desidera eseguire i report ad intervalli regolari ed inviarne i risultati sotto forma di allegati e-mail ai destinatari prescelti. Inserire la data e l'ora di inizio, oltre che la frequenza con cui verranno generati i report, specificare il formato e la lingua del file di output ed inserire gli indirizzi e-mail dei destinatari dei report.

10.4 Configurazione del report Allarmi ed eventi per nome oggetto

Se si utilizza l'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Configurazione report**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Il report **Allarmi ed eventi per nome dell'oggetto** fornisce dati statistici su tutti gli allarmi provenienti da tutti i computer in un determinato periodo di tempo, ordinati per nome dell'oggetto.

Per configurare il report:

1. Cliccare sull'icona **Report** posta sulla barra degli strumenti.
2. Nella finestra di dialogo **Report Manager**, selezionare **Allarmi ed eventi per nome dell'oggetto** e cliccare su **Proprietà**.
3. Nella finestra di dialogo **Proprietà allarmi ed eventi per nome dell'oggetto**, nella scheda **Configurazione**, impostare le opzioni desiderate.
   a) Nel riquadro **Dettagli del report**, modificare il nome e la descrizione del report, se lo si desidera.
   b) Nel riquadro **Periodo del report**, nella casella di testo **Periodo**, cliccare sulla freccia dell'elenco a discesa e selezionare un periodo di tempo.

È possibile selezionare un periodo fisso, per es. **Mese scorso**, oppure **Personalizzato** specificando il periodo di tempo desiderato nei campi **Inizio** e **Fine**.

c) Nel riquadro **Percorso del report**, cliccare su **Gruppo di computer** o **Computer singolo**. Quindi cliccare sulla freccia del menu a discesa per specificare un gruppo o un computer.

d) Nel riquadro **Allarmi e tipi di evento da includere**, selezionare i tipi di allarmi che si desidera includere nel report.

Per impostazione predefinita, il report mostra tutti i tipi di allarme e di evento.

4. Nel riquadro **Mostra opzioni**, sotto **Mostra**, scegliere quali allarmi ed eventi si desidera visualizzare nel report.

Per impostazione predefinita, il report mostra tutti gli allarmi ed eventi e il numero delle occorrenze per ognuno di essi.

Inoltre, è possibile configurare il report in modo da mostrare soltanto:

- I primi *x* allarmi ed eventi (*x* è il numero specificato dall'utente), oppure
- gli allarmi ed eventi con *y* o più occorrenze (*y* è il numero specificato dall'utente).

5. Sotto **Ordina per**, scegliere se si desidera ordinare gli allarmi ed eventi per numero o nome.

Per impostazione predefinita, il report elenca gli allarmi ed eventi in ordine decrescente di occorrenze.

6. Nel riquadro **Operazione pianificata**, selezionare **Pianifica questo report** se si desidera eseguire i report ad intervalli regolari ed inviarne i risultati sotto forma di allegati e-mail ai destinatari prescelti. Inserire la data e l'ora di inizio, oltre che la frequenza con cui verranno generati i report, specificare il formato e la lingua del file di output ed inserire gli indirizzi e-mail dei destinatari dei report.

10.5 Configurazione del report Allarmi ed eventi per orario

Se si utilizza l'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Configurazione report**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Il report **Allarmi ed eventi per orario** mostra gli allarmi e gli eventi riepilogati secondo intervalli specifici.

1. Cliccare sull'icona **Report** posta sulla barra degli strumenti.
2. Nella finestra di dialogo **Report Manager**, selezionare **Allarmi ed eventi per orario** e cliccare su **Proprietà**.
3. Nella finestra di dialogo **Proprietà allarmi ed eventi per orario**, nella scheda **Configurazione**, impostare le opzioni desiderate.

a) Nel riquadro **Dettagli del report**, modificare il nome e la descrizione del report, se lo si desidera.

b) Nel riquadro **Periodo del report**, nella casella di testo **Periodo**, cliccare sulla freccia dell'elenco a discesa e selezionare un periodo di tempo.

È possibile selezionare un periodo fisso, per es. **Mese scorso**, oppure **Personalizzato** specificando il periodo di tempo desiderato nei campi **Inizio** e **Fine**.

c) Nel riquadro **Percorso del report**, cliccare su **Gruppo di computer** o **Computer singolo**. Quindi cliccare sulla freccia del menu a discesa per specificare un gruppo o un computer.

 Copyright © Sophos Limited

d) Nel riquadro **Allarmi e tipi di evento da includere**, selezionare i tipi di allarmi che si desidera includere nel report.

Per impostazione predefinita, il report mostra tutti i tipi di allarme e di evento.

In alternativa, è possibile configurare il report in modo tale che visualizzi soltanto le posizioni in cui è stato segnalato un particolare allarme o evento. Per specificare un singolo allarme o evento, cliccare su **Avanzate** e quindi su un nome di allarme o evento nell'elenco. Per specificare più di un allarme o evento, digitare un nome nella casella di testo utilizzando i caratteri jolly. Utilizzare ? per ogni singolo carattere nel nome, e * per ogni stringa di caratteri. Per esempio, W32/* si riferisce a tutti i virus i cui nomi iniziano per W32/.

4. Nella scheda **Mostra opzioni**, per specificare gli intervalli di tempo nei quali viene calcolato il tasso di allarmi e eventi, per esempio ogni ora oppure ogni giorno, cliccare sulla freccia dell'elenco a discesa e selezionare un intervallo.
5. Nel riquadro **Operazione pianificata**, selezionare **Pianifica questo report** se si desidera eseguire i report ad intervalli regolari ed inviarne i risultati sotto forma di allegati e-mail ai destinatari prescelti. Inserire la data e l'ora di inizio, oltre che la frequenza con cui verranno generati i report, specificare il formato e la lingua del file di output ed inserire gli indirizzi e-mail dei destinatari dei report.

10.6 Configurazione del report Allarmi ed eventi per percorso

Se si utilizza l'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Configurazione report**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Il report **Allarmi ed eventi per percorso** fornisce dati statistici su tutti gli allarmi provenienti da tutti i computer in un determinato periodo di tempo, ordinati per percorso.

1. Cliccare sull'icona **Report** posta sulla barra degli strumenti.
2. Nella finestra di dialogo **Report Manager**, selezionare **Allarmi ed eventi per percorso** e cliccare su **Proprietà**.
3. Nella finestra di dialogo **Proprietà allarmi ed eventi per percorso**, nella scheda **Configurazione**, impostare le opzioni desiderate.

a) Nel riquadro **Dettagli del report**, modificare il nome e la descrizione del report, se lo si desidera.

b) Nel riquadro **Periodo del report**, nella casella di testo **Periodo**, cliccare sulla freccia dell'elenco a discesa e selezionare un periodo di tempo.

È possibile selezionare un periodo fisso, per es. **Mese scorso**, oppure **Personalizzato** specificando il periodo di tempo desiderato nei campi **Inizio** e **Fine**.

c) Nel riquadro **Percorso del report**, cliccare su **Computer** per visualizzare gli allarmi ordinati per computer o **Gruppo** per visualizzare gli allarmi ordinati per gruppi di computer.

d) Nel riquadro **Allarmi e tipi di evento da includere**, selezionare i tipi di allarmi che si desidera includere nel report.

Per impostazione predefinita, il report mostra tutti i tipi di allarme e di evento.

In alternativa, è possibile configurare il report in modo tale che visualizzi soltanto le posizioni in cui è stato segnalato un particolare allarme o evento. Per specificare un singolo allarme o evento, cliccare su **Avanzate** e quindi su un nome di allarme o evento nell'elenco. Per specificare più di un allarme o evento, digitare un nome nella casella di testo utilizzando i caratteri jolly. Utilizzare ? per ogni singolo carattere nel nome, e * per ogni stringa di caratteri. Per esempio, W32/* si riferisce a tutti i virus i cui nomi iniziano per W32/.

4. Nel riquadro **Mostra opzioni**, sotto **Mostra**, scegliere quali percorsi si desidera visualizzare nel report.

   Per impostazione predefinita, il report mostra tutti i computer, gruppi e il numero delle occorrenze per ognuno di essi. È possibile configurarlo in modo tale da mostrare soltanto:

   - le prime *x* posizioni nelle quali è stata registrata la maggior parte degli allarmi e eventi (*x* è il numero specificato dall'utente), oppure
   - le posizioni con *y* o più allarmi e eventi (*y* è il numero specificato dall'utente).
5. Sotto **Ordina per**, scegliere se si desidera ordinare i percorsi per numero di oggetti rilevati o nomi.

   Per impostazione predefinita, il report elenca i percorsi in ordine decrescente di numero di allarmi ed eventi per percorso. Selezionare **Percorso** se si desidera che vengano elencati per nome, in ordine alfabetico.
6. Nel riquadro **Operazione pianificata**, selezionare **Pianifica questo report** se si desidera eseguire i report ad intervalli regolari ed inviarne i risultati sotto forma di allegati e-mail ai destinatari prescelti. Inserire la data e l'ora di inizio, oltre che la frequenza con cui verranno generati i report, specificare il formato e la lingua del file di output ed inserire gli indirizzi e-mail dei destinatari dei report.

10.7 Configurazione del report Criterio del computer non conforme

Se si utilizza l'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Configurazione report**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Il report **Criterio del computer non conforme** mostra la percentuale e il numero di computer non conformi al criterio del gruppo di appartenenza, riepilogati secondo intervalli specifici.

1. Cliccare sull'icona **Report** posta sulla barra degli strumenti.
2. Nella finestra di dialogo **Report Manager**, selezionare **Criterio del computer non conforme** e cliccare su **Proprietà**.
3. Nella finestra di dialogo **Proprietà del criterio del computer non conforme**, nella scheda **Configurazione**, impostare le opzioni desiderate.

   a) Nel riquadro **Dettagli del report**, modificare il nome e la descrizione del report, se lo si desidera.

   b) Nel riquadro **Periodo del report**, nella casella di testo **Periodo**, cliccare sulla freccia dell'elenco a discesa e selezionare un periodo di tempo.

      È possibile selezionare un periodo fisso, per es. **Mese scorso**, oppure **Personalizzato** specificando il periodo di tempo desiderato nei campi **Inizio** e **Fine**.

   c) Nel riquadro **Mostra**, selezionare i criteri che si desidera visualizzare nel report. Per impostazione predefinita, è selezionato solo il criterio **Anti-virus e HIPS**.
4. Nel riquadro **Mostra opzioni**, sotto **Mostra risultati per**, specificare gli intervalli di tempo in cui viene misurata la non conformità, per es. ogni ora o giorno, cliccare sulla freccia dell'elenco a discesa e selezionare un intervallo.
5. Sotto **Mostra risultati come**, scegliere se si desidera visualizzare i risultati in percentuale o numero.
6. Nel riquadro **Operazione pianificata**, selezionare **Pianifica questo report** se si desidera eseguire i report ad intervalli regolari ed inviarne i risultati sotto forma di allegati e-mail ai destinatari prescelti. Inserire la data e l'ora di inizio, oltre che la frequenza con cui verranno generati i report,

 Copyright © Sophos Limited

specificare il formato e la lingua del file di output ed inserire gli indirizzi e-mail dei destinatari dei report.

10.8 Configurazione del report Eventi in base all'utente

Se si utilizza l'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Configurazione report**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Il report **Eventi per utente** visualizza gli eventi web e gli eventi del controllo applicazioni, firewall, controllo dati e controllo dispositivi, ordinati per utente.

1. Cliccare sull'icona **Report** posta sulla barra degli strumenti.
2. Nella finestra di dialogo **Report Manager**, selezionare **Eventi in base all'utente** e cliccare su **Proprietà**.
3. Nella finestra di dialogo **Proprietà eventi in base all'utente**, nella scheda **Configurazione**, impostare le opzioni desiderate.
   a) Nel riquadro **Dettagli del report**, modificare il nome e la descrizione del report, se lo si desidera.
   b) Nel riquadro **Periodo del report**, nella casella di testo **Periodo**, cliccare sulla freccia dell'elenco a discesa e selezionare un periodo di tempo.

      È possibile selezionare un periodo fisso, per es. **Mese scorso**, oppure **Personalizzato** specificando il periodo di tempo desiderato nei campi **Inizio** e **Fine**.
   c) Sotto **Tipi di evento da includere**, selezionare le funzioni per cui si desidera visualizzare eventi.
4. Nel riquadro **Mostra opzioni**, sotto **Mostra**, scegliere quali utenti si desidera visualizzare nel report.

   Per impostazione predefinita, il report mostra tutti gli utenti e il numero degli eventi per ognuno di essi. È possibile configurarlo in modo tale da mostrare soltanto:
   - I primi *x* utenti nei quali è stata registrata la maggior parte degli eventi (*x* è il numero specificato dall'utente), oppure
   - gli utenti con *y* o più eventi (*y* è il numero specificato dall'utente).
5. Sotto **Ordina per**, scegliere se si desidera ordinare gli utenti per numero di eventi o nomi.

   Per impostazione predefinita, il report elenca gli utenti in ordine decrescente di numero di eventi per utente. Selezionare **Utente** se si desidera che vengano elencati per nome, in ordine alfabetico.
6. Nel riquadro **Operazione pianificata**, selezionare **Pianifica questo report** se si desidera eseguire i report ad intervalli regolari ed inviarne i risultati sotto forma di allegati e-mail ai destinatari prescelti. Inserire la data e l'ora di inizio, oltre che la frequenza con cui verranno generati i report, specificare il formato e la lingua del file di output ed inserire gli indirizzi e-mail dei destinatari dei report.

10.9 Configurazione del report Protezione dei computer gestiti

Se si utilizza l'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Configurazione report**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Il report **Protezione dei computer gestiti** mostra la percentuale o il numero di computer protetti, riepilogati secondo intervalli specifici.

1. Cliccare sull'icona **Report** posta sulla barra degli strumenti.
2. Nella finestra di dialogo **Report Manager**, selezionare **Protezione dei computer gestiti** e cliccare su **Proprietà**.
3. Nella finestra di dialogo **Proprietà protezione dei computer gestiti**, nella scheda **Configurazione**, impostare le opzioni desiderate.
   a) Nel riquadro **Identità del report**, modificare il nome e la descrizione del report, se lo si desidera.
   b) Nel riquadro **Periodo del report**, nella casella di testo **Periodo**, cliccare sulla freccia dell'elenco a discesa e selezionare un periodo di tempo.

      È possibile selezionare un periodo fisso, per es. **Mese scorso**, oppure **Personalizzato** specificando il periodo di tempo desiderato nei campi **Inizio** e **Fine**.
   c) Nel riquadro **Mostra**, selezionare le funzioni che si desidera visualizzare nel report.
4. Nel riquadro **Mostra opzioni**, sotto **Mostra risultati per**, specificare gli intervalli di tempo in cui viene misurata la non conformità, per es. ogni ora o giorno, cliccare sulla freccia dell'elenco a discesa e selezionare un intervallo.
5. Sotto **Mostra risultati come**, scegliere se si desidera visualizzare i risultati in percentuale o numero.
6. Nel riquadro **Operazione pianificata**, selezionare **Pianifica questo report** se si desidera eseguire i report ad intervalli regolari ed inviarne i risultati sotto forma di allegati e-mail ai destinatari prescelti. Inserire la data e l'ora di inizio, oltre che la frequenza con cui verranno generati i report, specificare il formato e la lingua del file di output ed inserire gli indirizzi e-mail dei destinatari dei report.

10.10 Report della gerarchia degli aggiornamenti

Il report **Gerarchia aggiornamenti** mostra i gestori degli aggiornamenti nella rete, le condivisioni degli aggiornamenti che gestiscono e il numero di computer che si aggiornano dalle condivisioni.

Non è possibile configurare il report **Gerarchia aggiornamenti** . È possibile eseguire il report secondo quanto descritto in Esecuzione di un report (pagina 215).

10.11 Pianificazione di un report

Se si utilizza l'amministrazione basata sui ruoli, per poter svolgere questa operazione, è necessario essere in possesso dei diritti di **Configurazione report**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

 Copyright © Sophos Limited

È possibile pianificare l'esecuzione di report ad intervalli regolari ed inviare i risultati ai destinatari prescelti sotto forma di allegato e-mail.

1. Cliccare sull'icona **Report** posta sulla barra degli strumenti.
2. Nella finestra di dialogo **Report Manager**, selezionare il report che si desidera pianificare e cliccare su **Operazione pianificata**.
3. Nella finestra di dialogo che viene visualizzata, nel riquadro **Operazione pianificata**, selezionare **Pianifica questo report**.
4. Inserire la data e l'ora di inizio, oltre che la frequenza con cui verranno generati i report.
5. Specificare il formato e la lingua del file di output.
6. Inserire gli indirizzi e-mail dei destinatari dei report.

10.12 Esecuzione di un report

1. Cliccare sull'icona **Report** posta sulla barra degli strumenti.
2. Nella finestra di dialogo **Report Manager**, selezionare il report che si desidera eseguire e cliccare su **Esegui**.
   Viene visualizzata la finestra **Reportistica** che mostra il report.

È possibile modificare il layout del report, stamparlo o esportarlo in un file.

10.13 Visualizzazione di un report sotto forma di tabella o grafico

Alcuni report possono essere visualizzati sia come tabella che come grafico. In questo caso saranno disponibili due schede (**Tabella** e **Grafico**) nella finestra **Reportistica** in cui viene visualizzato il report.

1. Cliccare sull'icona **Report** posta sulla barra degli strumenti.
2. Nella finestra di dialogo **Report Manager**, selezionare il report che si desidera eseguire, ad es. **Allarmi ed eventi per percorso** , e cliccare su **Esegui**.
   Viene visualizzata la finestra **Reportistica** che mostra il report.
3. Per visualizzare il report come tabella oppure come grafico, selezionare la rispettiva scheda.

10.14 Stampa di un report

Per stampare un report, cliccare sull'icona **Stampa** posta nella barra degli strumenti sopra il report.

10.15 Esportazione del report in un file

Per esportare il report in un file:

1. Cliccare sull'icona **Esporta** posta sulla barra degli strumenti sopra il report.

2. Nella finestra di dialogo **Esporta report**, selezionare il tipo di documento o di foglio elettronico nel quale si desidera esportare il report.

   Le opzioni sono:

   - PDF (Acrobat)
   - HTML
   - Microsoft Excel
   - Microsoft Word
   - Rich Text Format (RTF)
   - Valori separati (CSV)
   - XML
3. Cliccare sul pulsante Sfoglia del campo **Nome file** per selezionare un percorso. Quindi inserire un nome. Cliccare su **OK**.

10.16 Modifica del layout del report

È possibile modificare il layout della pagina utilizzata per i report. Per esempio, è possibile visualizzare un report in formato orizzontale.

1. Cliccare sull'icona del layout di pagina posta sulla barra degli strumenti sopra il report.

2. Nella finestra di dialogo **Imposta pagina**, specificare le dimensioni della pagina, l'orientamento e i margini. Cliccare su **OK**.
   Il report viene quindi visualizzato con queste impostazioni di pagina.

Le stesse impostazioni vengono utilizzate anche quando si stampa o si esporta il report.

 Copyright © Sophos Limited

11 Controllo

L'opzione di Controllo consente di monitorare le modifiche apportate alla configurazione di Enterprise Console, oltre che altre azioni condotte da utenti o sistema. Queste informazioni sono utili per la conformità alle normative e la risoluzione dei problemi, oppure, in caso di attività malevoli, per azioni di analisi e indagine.

Per impostazione predefinita, il controllo è disabilitato. Quando lo si abilitata, nel database di controllo viene scritta una voce di Controllo ogni qualvolta determinate impostazioni di configurazioni vengono modificate o azioni specifiche vengono eseguite.

Nota
Se si utilizza l'amministrazione basata sui ruoli, è necessario essere in possesso dei diritti di **Controllo**, per poterlo abilitare o disabilitare. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Tale voce di controllo includerà le seguenti informazioni:

- Azione eseguita
- Utente che ha eseguito l'azione
- Computer dell'utente
- Sottoambiente dell'utente
- Data e ora dell'azione

Vengono sottoposte a controllo sia le azioni che hanno esito positivo sia quelle con esito negativo; in questo modo le voci di controllo potranno mostrare chi ha eseguito in modo efficace determinate azioni all'interno del sistema e chi ne ha intraprese altre che non hanno invece avuto successo.

Le azioni di controllo includono:

Categoria	Azioni
Azioni del computer	Cancellare/risolvere allarmi ed errori, proteggere, aggiornare e cancellare computer, eseguire scansioni complete del sistema
Gestione di gruppi di computer	Creare, cancellare, spostare o rinominare un gruppo, oltre che assegnare un computer a un gruppo
Gestione criteri	Creare, rinominare, copiare o modificare un criterio, oltre che assegnare un criterio a un computer, ripristina impostazioni predefinite o cancellare un criterio
Gestione dei ruoli	Creare, rinominare, copiare o modificare un ruolo, oltre che aggiungere o rimuovere un utente a/da un ruolo, aggiungere o rimuovere diritti a/da un ruolo
Gestione di Update Manager	Aggiornare un gestore degli aggiornamenti, renderlo conforme alla configurazione, cancellare allarmi, eliminare un gestore aggiornamenti, configurare un gestore aggiornamenti, aggiungere o cancellare una nuova sottoscrizione software, oltre che rinominare, modificare o copiare una sottoscrizione software

Copyright © Sophos Limited

Categoria	Azioni
Eventi di sistema	Abilitazione del Controllo, disabilitazione del Controllo

È possibile utilizzare programmi prodotti da terzi, quali Microsoft Excel, Microsoft Access, Microsoft SQL Server Reporting Services o Crystal Reports, per accedere e analizzare i dati archiviati nel database di controllo. Per informazioni su come visualizzare le voci di controllo, consultare il *Manuale utente sulla funzione di Controllo di* Sophos Enterprise Console.

11.1 Abilitazione o disabilitazione del Controllo

Se si utilizza l'amministrazione basata sui ruoli, è necessario essere in possesso del diritto **Controllo**, per poter abilitare o disabilitare il Controllo. Per ulteriori informazioni, consultare la sezione Gestione dei ruoli e dei sottoambienti (pagina 13).

Per abilitare o disabilitare l'opzione di controllo

1. Dal menu **Strumenti**, cliccare su **Gestione controllo**.
2. Nella finestra di dialogo **Gestione controllo**, selezionare o deselezionare la casella di spunta **Attiva controllo** per abilitare o disabilitare l'opzione di contollo. Questa opzione è disabilitata per impostazione predefinita.

Copyright © Sophos Limited

12 Copia e stampa di dati da Enterprise Console

12.1 Copia dei dati dall'elenco dei computer

È possibile copiare informazioni visualizzate nell'elenco dei computer, dalla visualizzazione **Computer** negli Appunti e poi incollarle in un altro documento nel formato valore separato da tabulazione.

1. Nella vista **Computer**, nel riquadro **Gruppi**, selezionare il gruppo di computer da cui si desidera copiare dati.
2. Nel menu a discesa **Visualizza**, selezionare quali computer si desidera visualizzare, per es. **Computer con potenziali problemi**.
3. Se il gruppo contiene dei sottogruppi, selezionare anche l'opzione **Solo a questo livello** oppure **A questo livello e al livello inferiore**.
4. Nell'elenco dei computer, andare alla scheda che si desidera visualizzare, per es. **Dettagli dell'antivirus**.
5. Cliccare ovunque nell'elenco dei computer per metterlo in rilievo.
6. Nel menu **Modifica**, cliccare su **Copia** per copiare i dati negli Appunti.

12.2 Stampa dei dati dall'elenco dei computer

È possibile stampare le informazioni visualizzate nell'elenco dei computer, nella vista **Computer**.

1. Nella vista **Computer**, nel riquadro **Gruppi**, selezionare il gruppo di computer i cui dati si desidera stampare.
2. Nel menu a discesa **Visualizza**, selezionare quali computer si desidera visualizzare, per es. **Computer con potenziali problemi**.
3. Se il gruppo contiene dei sottogruppi, selezionare anche l'opzione **Solo a questo livello** oppure **A questo livello e al livello inferiore**.
4. Nell'elenco dei computer, andare alla scheda che si desidera visualizzare, per es. **Dettagli dell'antivirus**.
5. Cliccare ovunque nell'elenco dei computer per metterlo in rilievo.
6. Nel menu **File**, cliccare su **Stampa**.

12.3 Copia dei dettagli del computer

È possibile copiare le informazioni dalla finestra di dialogo **Dettagli computer** agli Appunti e quindi incollarle in un altro documento. Le informazioni includono nome e sistema operativo del computer, versioni del software di sicurezza installato nel computer, eventuali allarmi ed errori di rilievo, stato di aggiornamento e così via.

1. Nella vista **Computer**, nell'elenco di computer, cliccare due volte sul computer per il quale si desidera copiare i dati.
2. Nella finestra di dialogo **Dettagli computer**, cliccare su **Copia** per copiare i dati negli Appunti.

Copyright © Sophos Limited

12.4 Stampa dei dettagli del computer

È possibile stampare informazioni dalla finestra di dialogo **Dettagli computer**. Le informazioni includono nome e sistema operativo del computer, versioni del software di sicurezza installato nel computer, eventuali allarmi ed errori di rilievo, stato di aggiornamento e così via.

1. Nella vista **Computer**, nell'elenco di computer, cliccare due volte sul computer per il quale si desidera stampare i dati.
2. Nella finestra di dialogo **Dettagli computer**, cliccare su **Stampa**.

Copyright © Sophos Limited

13 Risoluzione dei problemi

Quando si esegue la procedura guidata per la protezione dei computer, l'installazione del software di sicurezza può non riuscire per svariate ragioni:

- L'installazione automatica non è attuabile sul sistema operativo in questione. Eseguire l'installazione manualmente. Per altri sistemi operativi (se la licenza a disposizione lo consente), consultare la Guida di avvio di per Linux e UNIX.
- È stato impossibile determinare il sistema operativo. Ciò può essere dovuto al fatto che, durante la ricerca dei computer, il nome utente non è stato inserito nel formato dominio\nomeutente.
- Le regole del Firewall bloccano l'acesso, necessario per distribuire il software di sicurezza.

13.1 Mancata esecuzione da parte dei computer della scansione in accesso

Se sono presenti computer che non eseguono la scansione in accesso:

1. Verificare quale antivirus e criterio HIPS viene utilizzato da tali computer.

   Per ulteriori informazioni, vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Assicurarsi che la scansione in accesso sia abilitata nel criterio e che i computer siano conformi a tale criterio.

   Per dettagli, consultare le sezioni Attivazione e disattivazione della scansione in accesso (pagina 84) e Allineamento dei computer ai criteri di gruppo (pagina 32).

13.2 Firewall disabilitato

Se sono presenti computer col firewall disabilitato:

1. Verificare quale criterio del firewall viene eseguito da tali computer.

   Per ulteriori informazioni, vedere Criteri utilizzati da un dato gruppo (pagina 25).
2. Assicurarsi che il firewall sia abilitato nel criterio e che i computer siano conformi al criterio.

   Per dettagli, consultare le sezioni Disabilitazione temporanea del firewall (pagina 119) e Allineamento dei computer ai criteri di gruppo (pagina 32).

13.3 Firewall non installato

Nota
Se si utilizza un'amministrazione basata sui ruoli, per poter installare il firewall, è necessario essere in possesso dei diritti per **Ricerca computer, protezione e gruppo**. Per ulteriori informazioni, vedere Gestione dei ruoli e dei sottoambienti (pagina 13).

Prima di cercare di installare il client firewall nei computer endpoint, verificare che stiano eseguendo un sistema operativo client di Windows.

Nota
Non è possibile installare il firewall nei computer che eseguono sistemi operativi per server o Windows Vista Starter.

Se ci sono computer nei quali si desidera installare il firewall:

1. Selezionare i computer, cliccarvi col tasto destro del mouse e selezionare **Proteggi computer**.
   Viene visualizzata la **Procedura guidata per la protezione dei computer**. Cliccare su **Avanti**.
2. Quando richiesto di selezionare le funzioni, selezionare **Firewall**. Completare la procedura guidata.

Se il problema persiste, contattare il supporto tecnico di Sophos.

13.4 Computer con allarmi in sospeso

- Se in alcuni computer è presente un virus o un'applicazione indesiderata, consultare la sezione Disinfezione immediata dei computer (pagina 54).
- Se in alcuni computer è presente adware o altra applicazione potenzialmente indesiderata che *si desidera* utilizzare, consultare la sezione Autorizzazione di adware e PUA (pagina 109).
- In caso di computer non aggiornati, consultare la sezione Aggiornamento dei computer non aggiornati (pagina 78), per istruzioni su come individuare e risolvere il problema.

Nota
Se non è necessario che l'allarme continui ad essere visualizzato, è possibile cancellarlo. Selezionare il o i computer con allarmi, cliccarvi sopra con il tasto destro del mouse e selezionare **Risolvi allarmi ed errori**. Per cancellare allarmi ed errori è necessario essere in possesso dei diritti di **Correzione - disinfezione**.

13.5 Computer non gestiti dalla console

I computer Windows, Mac, Linux e UNIX devono essere gestiti da Enterprise Console, in modo tale che possano essere aggiornati e monitorati.

Nota
A meno che si utilizzi la Sincronizzazione con Active Directory (vedere Gestione dei ruoli e dei sottoambienti (pagina 13)), i nuovi computer aggiunti alla rete non vengono né visualizzati né gestiti automaticamente dalla console. Cliccare su **Individuazione dei computer** nella barra degli strumenti per cercarli e inserirli nel gruppo **Nessun gruppo**.

Se un computer non è gestito, i relativi dati nella scheda **Stato** sono visualizzati in grigio.

Per cominciare a gestire i computer non gestiti:

1. Nel menu a discesa **Visualizza**, selezionare **Computer non gestiti**.
2. Effettuare una delle seguenti operazioni:
   - Se i computer non gestiti si trovano nel gruppo **Nessun gruppo**, selezionare i computer e trascinarli nel gruppo a cui si desidera attribuirli. Viene avviata la **Procedura guidata per la protezione dei computer**.

 Copyright © Sophos Limited

- Se i computer fanno già parte di un gruppo, selezionarli, cliccarvi col tasto destro del mouse e selezionare la voce **Proteggi computer** per installare una versione gestita di Sophos Endpoint Security and Control.

3. Se sono presenti dei computer nei quali Enterprise Console non può installare automaticamente Sophos Endpoint Security and Control, eseguire un'installazione manuale.

   L'installazione automatica tramite **procedura guidata per la protezione dei computer** è disponibile solo per computer Windows. Nel caso si desideri proteggere computer Mac, Linux o UNIX, installare il software manualmente.

   Per informazioni su come proteggere manualmente i computer Mac o Windows, consultare la *Guida di avvio avanzato di* Sophos Enterprise Console.

   Per informazioni su come proteggere Linux o UNIX, consultare la *Guida di avvio per Linux e UNIX di* Sophos Enterprise Console.

13.6 Impossibile proteggere i computer nel gruppo Nessun gruppo

Il gruppo **Nessun gruppo** ha la sola funzione di riunire tutti i computer che non si trovano ancora in alcun gruppo creato dall'utente, a cui possono essere applicati criteri. Non è possibile proteggere i computer finché non vengono inseriti in tale gruppo.

13.7 Installazione di Sophos Endpoint Security and Control non riuscita

Se la **Procedura guidata per la protezione dei computer** non riesce a installare Sophos Endpoint Security and Control sui computer, ciò potrebbe essere dovuto a una delle seguenti cause.

- Enterprise Console non riconosce il sistema operativo installato nei computer. L'utente potrebbe non aver inserito il nome utente nel formato dominio\utente durante la ricerca dei computer.
- L'installazione automatica non è attuabile sul sistema operativo in questione. Eseguire l'installazione manualmente. Per le istruzioni, consultare la *Guida di avvio avanzata di* Sophos Enterprise Console.
- I computer eseguono il firewall.
- La "Condivisione file semplice" non è stata disattivata sui computer con sistema operativo Windows XP.
- L'opzione “Usa procedura guidata condivisione” non è stata disattivata sui computer Windows Vista.
- È stato scelto di installare una funzione non supportata dai sistemi operativi dei computer.

Per un elenco completo dei requisiti per le funzioni di Sophos Endpoint Security and Control, consultare la pagina dei requisiti di sistema sul sito web di Sophos (http://www.sophos.com/it-it/products/all-system-requirements).

13.8 I computer non sono aggiornati

Per supporto sulla diagnostica e la risoluzione del problema, consultare Aggiornamento dei computer non aggiornati (pagina 78).

13.9 Impostazioni antivirus non applicate ai computer Mac

Alcune impostazioni antivirus non possono essere applicate ai computer con sistema operativo Macintosh. In questo caso, appare un avviso nella relativa pagina delle impostazioni.

Per ulteriori informazioni sulle impostazioni dei criteri antivirus e HIPS applicabili ai Mac, consultare l'articolo 118859 della knowledge base.

13.10 Le impostazioni antivirus non vengono applicate nei computer Linux e UNIX

Alcune impostazioni antivirus non possono essere applicate ai computer con sistema operativo Linux e UNIX. In questo caso, appare un avviso nella relativa pagina delle impostazioni.

È possibile modificare le impostazioni antivirus nei computer con sistema operativo Linux utilizzando i comandi `savconfig` e `savscan`, come spiegato nella *Guida alla configurazione di Sophos Anti-Virus per Linux*.

È possibile modificare le impostazioni antivirus nei computer con sistema operativo UNIX utilizzando il comando `savscan` come spiegato nella *Guida alla configurazione di Sophos Anti-Virus per UNIX*.

13.11 Computer Linux o UNIX non conformi ai criteri

Se nella CID si utilizza un file di configurazione aziendale e tale file contiene un valore di configurazione in conflitto con il criterio, il computer verrà indicato come non conforme al criterio stesso.

Selezionando l'opzione **Allinea con**, il computer sarà conforme al criterio solo temporaneamente, finché la configurazione basata sulla CID non verrà riapplicata.

Per risolvere il problema, rivedere il file di configurazione aziendale e, dove possibile, sostituirlo con una configurazione basata sulla console.

Copyright © Sophos Limited

13.12 Una nuova scansione compare inaspettatamente in un computer Windows

Se si controlla la copia locale di Sophos Endpoint Security and Control sui computer con sistema operativo Windows, può accadere di vedere elencata una nuova "Scansione disponibile", anche se l'utente non l'ha creata.

Questa nuova scansione è una scansione pianificata impostata dall'utente all'interno della console. Non va cancellata.

13.13 Problemi di connettività e scadenza del tempo di attesa

Se le comunicazioni tra Enterprise Console e un computer della rete diventano lente o il computer non risponde più, potrebbe sussistere un problema di connettività.

Verificare il report sulle comunicazioni di rete Sophos, che presenta una panoramica dell'attuale stato delle comunicazioni tra un computer ed Enterprise Console. Per visualizzare il report, andare al computer in cui si è verificato il problema. Nella barra delle applicazioni, cliccare sul pulsante **Start**, selezionare **Programmi > Sophos > Sophos Endpoint Security and Control** e quindi cliccare su **Visualizza Report comunicazioni di rete Sophos**.

Il report mostra le aree con potenziali problemi e, nel caso sia stato riscontrato un problema, anche le possibili soluzioni.

13.14 Adware e PUA non vengono rilevati

Se adware e altre applicazioni potenzialmente indesiderate (PUA) non vengono rilevati, è necessario verificare che:

- Il rilevamento sia stato abilitato. Vedere Configurazione della scansione in accesso (pagina 82).
- Le applicazioni si trovano in un computer che esegue Windows.

13.15 Oggetto parzialmente rilevato

Sophos Endpoint Security and Control può rilevare che un oggetto (per es. un trojan o un'applicazione potenzialmente indesiderata) è stato "parzialmente rilevato". Ciò significa che non tutti i componenti dell'applicazione sono stati trovati.

Per trovare gli altri componenti è necessario eseguire la scansione completa del sistema del o dei computer interessati. A tale scopo, sui computer che eseguono Windows, selezionare i computer, cliccarvi con il tasto destro del mouse e selezionare **Scansione completa del sistema**. È anche possibile impostare una ricerca pianificata di adware e altre applicazioni potenzialmente indesiderate. Vedere Configurazione della scansione in accesso (pagina 82) e Creazione di una scansione pianificata (pagina 89).

Se l'applicazione non è stata ancora completamente rilevata, ciò può dipendere dalle seguenti ragioni:

- I diritti di accesso non sono sufficienti.
- Alcune unità o cartelle presenti nel computer e contenenti i componenti dell'applicazione, sono escluse dalla scansione.

In quest'ultimo caso, controllare l'elenco degli oggetti esclusi dalla scansione (v. Esclusione di oggetti dalla scansione in accesso (pagina 87)). Se nell'elenco compaiono degli oggetti, rimuoverli e sottoporre di nuovo il computer a scansione.

Sophos Endpoint Security and Control potrebbe non essere in grado di rilevare o rimuovere completamente adware e altre applicazioni potenzialmente indesiderate i cui componenti sono installati sulle unità di rete.

Per ricevere assistenza, contattare il supporto tecnico di Sophos.

13.16 Allarmi frequenti relativi alle applicazioni potenzialmente indesiderate

È possibile che si ricevano molti allarmi riguardanti applicazioni potenzialmente indesiderate, compresi più report della stessa applicazione.

Ciò può verificarsi perché alcuni tipi di applicazioni potenzialmente indesiderate "monitorano" i file, provando ad accedervi di frequente. Se la scansione in accesso è abilitata, Sophos Endpoint Security and Control rileva ogni accesso a un file e invia un allarme.

È quindi necessario effettuare una delle seguenti operazioni:

- Disabilitare la scansione in accesso per la ricerca di adware e PUA. In alternativa si può utilizzare una scansione pianificata.
- Autorizzare l'applicazione (se si desidera eseguirla sui computer). Vedere Autorizzazione di adware e PUA (pagina 109).
- Disinfettare il o i computer, rimuovendo le applicazioni non autorizzate. Vedere Disinfezione immediata dei computer (pagina 54).

13.17 Disinfezione non riuscita

Se Sophos Endpoint Security and Control non riesce a rimuovere gli oggetti ("Disinfezione non riuscita"), può essere dovuto a una delle seguenti ragioni.

- Non ha trovato tutti i componenti di un oggetto multicomponente. Eseguire una scansione completa del sistema del o dei computer per trovare gli altri componenti. Vedere Scansione immediata dei computer (pagina 53).
- Alcune unità o cartelle, contenenti i componenti dell'oggetto, sono escluse dalla scansione. Controllare gli oggeti esclusi dalla scansione (v. Esclusione di oggetti dalla scansione in accesso (pagina 87)). Se l'elenco contiene alcuni oggetti, rimuoverli.
- Non si possiedono diritti di accesso sufficienti.
- Non è possibile rimuovere quel tipo di oggetto.
- È stato rilevato un frammento di virus, piuttosto che una corrispondenza esatta con un virus.
- L'oggetto è contenuto in un floppy disk o CD protetto da scrittura.
- L'oggetto è contenuto in un volume NTFS protetto da scrittura (Windows).

 Copyright © Sophos Limited

13.18 Rimozione degli effetti secondari dei virus

La disinfezione è in grado di rimuovere un virus dai computer, ma non è sempre in grado di annullarne gli effetti secondari.

Alcuni virus non lasciano effetti secondari. Altri possono apportare modifiche oppure danneggiare i dati in modi che siano difficili da rilevare. Per rimediare, procedere come segue.

- Nel menu **?**, cliccare su **Visualizza informazioni sulla sicurezza**. In questo modo ci si collega al sito web di Sophos, in cui è disponibile l'analisi del virus.
- Utilizzare gli originali o le copie di backup dei programmi infetti per sostituirli. Se non si disponeva di copie di backup prima dell'infezione, è necessario crearle ora 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.

13.19 Rimozione degli effetti secondari delle applicazioni

Anche se si rimuovono le applicazioni indesiderate, non è sempre possibile annullarne anche gli effetti secondari.

Alcune applicazioni modificano il sistema operativo, ad es., cambiando le impostazioni della connessione a Internet. Sophos Endpoint Security and Control non riesce sempre a ripristinare tutte le impostazioni. Per esempio, se un'applicazione ha cambiato la pagina iniziale del browser, Sophos Endpoint Security and Control non può sapere qual era la pagina iniziale precedentemente impostata.

Alcune applicazioni installano sul computer utilità, quali i file .dll o .ocx. Se un'utilità è innocua (vale a dire che non possiede le caratteristiche di un'applicazione potenzialmente indesiderata), come ad es. una libreria della lingua, e non è integrata in un'applicazione, Sophos Endpoint Security and Control può non rilevarla come parte dell'applicazione stessa. In tal caso il file non verrà rimosso dal computer.

A volte un'applicazione, quale l'adware, fa parte di un programma installato volontariamente dall'utente e pertanto la sua presenza è necessaria affinché il programma possa essere eseguito. Se l'applicazione viene rimossa dal computer, il programma potrebbe smettere di funzionare.

È necessario:

- Nel menu **?**, cliccare su **Visualizza informazioni sulla sicurezza**. In questo modo ci si collega al sito web di Sophos, in cui è disponibile l'analisi dell'applicazione.
- Utilizzare le copie di backup per ripristinare le impostazioni di sistema oppure i programmi che si desidera utilizzare. Se non si disponeva in precedenza di copie di backup, è necessario crearle ora in caso di problemi futuri.

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

Copyright © Sophos Limited

13.20 Il controllo dati non rileva i file caricati tramite browser incorporati

Il controllo dati intercetta i documenti caricati tramite browser web autonomi. Non intercetta i documenti caricati tramite browser incorporati in applicazioni prodotte da terzi (per es. Lotus Notes). Se in possesso di un'applicazione prodotta da terzi con browser incorporato e si desidera monitorare tutti i documenti caricati, sarà necessario configurare tale applicazione in modo tale che lanci un browser esterno.

13.21 Il controllo dati non esegue la scansione dei file caricati o allegati

Se il controllo dati non esegue la scansione dei file scaricati o allegati da un percorso di rete utilizzando un'applicazione monitorata (per es. un client e-mail, un browser web o un client di messaggistica istantanea (IM)), nel criterio antivirus e HIPS i file remoti potrebbero essere stati esclusi dalla scansione in accesso. In tale eventualità, il controllo dati utilizza le stesse esclusioni applicate alla scansione in accesso di Sophos Anti-Virus (InterCheck ™); di conseguenza, se la scansione dei file remoti è disattivata, nessuno di tali file sarà sottoposto a verifica da parte del controllo dati.

Per informazioni sulla configurazione di esclusioni per la scansione in accesso, consultare la sezione Esclusione di oggetti dalla scansione in accesso (pagina 87).

Nota
Il controllo dati non adopera le esclusioni di scansione in accesso quando i file vengono copiati o trasferiti usando Esplora risorse. In tale eventualità, il controllo dati riuscirà a intercettare il trasferimento di file da un percorso di rete a dispositivi di memorizzazione monitorati; per esempio, quando si copiano file su un dispositivo di memorizzazione removibile o li si masterizzano su un supporto ottico.

13.22 Visualizzazione nella console di un gestore aggiornamenti disinstallato

Dopo avere disinstallato un gestore aggiornamenti addizionale, tale gestore potrebbe essere ancora visualizzato in Enterprise Console, vista **Update manager**.

Per rimuovere il gestore aggiornamenti dalla console, selezionarlo, cliccarvi col tasto destro del mouse e cliccare su **Cancella**.

Copyright © Sophos Limited

14 Glossario

evento di sincronizzazione di Active Directory	Evento che si verifica durante la sincronizzazione con Active Directory.
sottoambiente attivo	Sottoambiente visualizzato nel riquadro Gruppi.
editor di Content Control List avanzato	Editor che consente all'utente di creare una Content Control List personalizzata comprendente score, conteggio massimo, espressioni regolari e trigger score da ottenere prima di eseguire il match con la Content Control List.
gestore applicazioni	Finestra di dialogo che consente la creazione di nuove regole per le applicazioni bloccate da Sophos Client Firewall.
controllo	Una funzione che consente di monitorare le modifiche apportate alla configurazione di Enterprise Console, oltre che altre azioni condotte da utenti e sistema.
protezione automatica	Distribuzione del software di sicurezza (attuazione dell'installazione e dei criteri) in tutti i computer presenti nel contenitore di Active Directory, non appena portata a termine la loro sincronizzazione con Enterprise Console.
categoria	Tag specifico utilizzato per classificare le Content Control List di SophosLabs in base alla loro tipologia, alle norme che ne definiscono i contenuti o alla regione in cui sono applicate.
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: SophosLabs Content Control List e Content Control List personalizzata.
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.
applicazione controllata	Applicazione non malevola che un'azienda può decidere di rilevare o bloccare perché minante alla produttività e alle prestazioni della rete.
dati controllati	File che soddisfano le condizioni di controllo dei dati.
dispositivo controllato	Dispositivo soggetto a controllo.
livello critico	Valore che determina il cambiamento dello stato di sicurezza di un elemento a Critico.

Copyright © Sophos Limited

Content Control List personalizzata	Content Control List creata da un cliente Sophos. È possibile creare una Content Control List in due modi,creando un semplice elenco di termini della ricerca aventi condizioni di ricerca specifiche, quali “uno qualsiasi di questi termini”, oppure utilizzando un editor di Content Control List avanzato.
Pannello di controllo	Panoramica immediata dello stato di sicurezza della rete.
evento del pannello di controllo	Evento in cui l'indicatore di stato del pannello di controllo supera il livello critico. Quando si verifica un evento del pannello di controllo viene generato un allarme e-mail.
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.
prevenzione della perdita di dati (DLP)	V. *controllo dati*.
database	Il componente di Sophos Enterprise Console che memorizza i dati relativi ai computer in rete.
sottoambiente predefinito	**Sottoambiente avente come radice il nodo del server della struttura ad albero del gruppo e il gruppo Nessun gruppo** Per impostazione predefinita viene visualizzata quando si apre Enterprise Console per la prima volta.
controllo 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.
reputazione del download	Reputazione dei file scaricati da Internet. La reputazione viene definita in base all'età dei file, alle loro fonti e prevalenza, oltre che a un'approfondita analisi dei contenuti e ad altre caratteristiche specifiche. È un utile supporto per stabilire se i file siano sicuri o se il loro download rappresenti un potenziale rischio per i computer.
ambiente	Vedere *ambiente IT*.
dispositivo esente	Dispositivo esplicitamente escluso dal controllo dei dispositivi.

Copyright © Sophos Limited

espressione	Vedere *espressione regolare*.
file soddisfacente la regola	Regola che stabilisce l'azione da intraprendere se l'utente cerca di trasferire in una destinazione specificata un file avente nome o tipo specifico; per esempio blocco del trasferimento dei database in dispositivi di memorizzazione removibili.
gruppo	Gruppo di computer gestiti definito in Sophos Enterprise Console.
indicatore di stato	Termine generico riferito alle icone indicanti lo stato di sicurezza della sezione del pannello di controllo, di un elemento o di tutta la rete.
Host Intrusion Prevention System (HIPS)	Tecnologia per la sicurezza che protegge i computer dai virus non identificati e dai file e comportamenti sospetti.
ambiente IT	L'infrastruttura informatica aziendale, comprendente computer, rete ecc.
Malicious Traffic Detection (Rilevamento del traffico malevolo)	Una funzionalità che consente di rilevare le comunicazioni fra computer compromessi e server command and control degli hacker.
computer gestito	Computer in cui è installato Remote Management System (RMS) ed in cui Sophos Enterprise Console può rilevare, installare e aggiornare un software.
console di gestione	Il componente di Sophos Enterprise Console che consente di proteggere e gestire i computer.
server di gestione	Il componente di Sophos Enterprise Console che gestisce gli aggiornamenti e la comunicazione con i computer della rete.
conteggio massimo	Il numero massimo di corrispondenze di un'espressione regolare conteggiate per raggiungere il punteggio totale.
computer non aggiornato	Computer non in possesso della versione aggiornata del software Sophos.
verifica patch	Esegue una valutazione dei computer in base alle patch installate e identifica quelle mancanti.
criterio	Insieme di impostazioni, per esempio relative all'aggiornamento, applicate a un gruppo o gruppi di computer.
applicazione potenzialmente indesiderata	Un'applicazione non intrinsecamente dannosa, ma che in genere viene considerata inadatta per la maggior parte delle reti aziendali.
quantità	Il volume del tipo di informazioni chiave da reperire nel file prima di eseguire il match con la Content Control List.
quantità chiave	La tipologia chiave dei dati definita nella Content Control List, a cui viene applicata l'impostazione relativa alla quantità. Per esempio, nel caso di

	una Content Control List contenente numeri di carte di credito o debito (bancomat), si tratta della quantità di numeri di carte di credito o debito da reperire in un file prima di eseguirne il match con la Content Control List.
regione	L'ambito di una SophosLabs Content Control List. Può specificare la nazione in cui si applica la Content Control List (Content Control List specifica di una nazione) oppure essere “globale” (Content Control List globali, applicabili a tutte le nazioni).
espressione regolare	Stringa di ricerca utilizzante caratteri speciali che devono corrispondere a un pattern di testo presente nel file. Il controllo dei dati utilizza la sintassi delle espressioni regolari di Perl 5.
diritto	Insieme di autorizzazioni che consentono di svolgere determinate operazioni in Enterprise Console.
ruolo	Insieme di diritti che permette di accedere a Enterprise Console.
Amministrazione basata sui ruoli	Funzione che consente di specificare a quali computer l'utente possa accedere e quali operazioni possa svolgere, a seconda del suo ruolo all'interno dell'azienda.
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.
regola	Indica le azioni da intraprendere se un file soddisfa determinate condizioni. Esistono due tipi di regole del controllo dati: file soddisfacente la regola e regola del contenuto.
score	Numero aggiunto al punteggio totale di una Content Control List quando si esegue il match di un'espressione regolare.
nodo radice del server	Nel riquadro **Gruppi** è il nodo di livello più alto della struttura ad albero del gruppo e comprendente il gruppo **Nessun gruppo**.
Sophos Live Protection	Funzione che utilizza la tecnologia "in-the-cloud" per decidere all'istante se un file sospetto rappresenta una minaccia e intraprendere l'azione specificata nella configurazione di disinfezione di Sophos Anti-Virus.
Sophos Update Manager (SUM)	Programma che scarica il software di sicurezza Sophos e i relativi aggiornamenti da Sophos o da altro server di aggiornamento nelle posizioni di aggiornamento condivise.
regola definita da Sophos	Regola fornita da Sophos come esempio. Le regole definite da Sophos non vengono però aggiornate da Sophos.

Copyright © Sophos Limited

Content Control List di SophosLabs	Content Control List fornita e gestita da Sophos. Sophos può aggiornare le Content Control List di SophosLabs o crearne di nuove e metterle a disposizione in Enterprise Console. I contenuti delle Content Control List di SophosLabs non possono essere modificati, mentre la quantità può esserlo.
sottoambiente	Una parte dell'ambiente IT comprendente un determinato sottoinsieme di computer e gruppi.
sottoambiente amministrativo	Funzione che limita i computer e i gruppi in cui è possibile svolgere determinate operazioni.
sottoscrizione al software	Versioni di un software per piattaforme diverse scelte dall'utente e che Update Manager scaricherà e manterrà aggiornate. Ogni versione può essere specifica per ciascuna piattaforma supportata (per es. “Recommended” per Windows).
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 malevole.
file sospetto	File che presenta una serie di caratteristiche comunemente, ma non esclusivamente, riscontrate in virus.
intervallo di sincronizzazione	Periodo di tempo entro cui un punto di sincronizzazione in Enterprise Console viene sincronizzato con il contenitore di Active Directory prescelto.
punto di sincronizzazione (per un albero di Active Directory)	Gruppo di Sophos Enterprise Console in cui verranno aggiunti per la sincronizzazione i contenuti di un determinato contenitore di Active Directory (gruppi e computer o solo gruppi), mentre la loro struttura non verrà alterata.
sincronizzazione con Active Directory	Sincronizzazione unidirezionale dei gruppi di Sophos Enterprise Console con le unità organizzative o i contenitori di Active Directory.
gruppo sincronizzato	Qualsiasi gruppo al di sotto del punto di sincronizzazione.
Amministratore di sistema	Ruolo preconfigurato con pieni diritti di gestione del software di sicurezza Sophos nella rete e dei ruoli in Enterprise Console. Il ruolo di System Administrator (amministratore di sistema) non può essere eliminato o vedere modificati i suoi diritti o nome, inoltre il gruppo Sophos Full Administrators Windows non può essere rimosso da tale ruolo. Altri utenti e gruppi possono essere aggiunti o rimossi dal ruolo.
tag	Descrittore applicato alla Content Control List di SophosLabs per definirne i contenuti o l'ambito. Esistono tre tipi di tag: tipo, norma e regione.

blocco rimozione	Una funzione che impedisce 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 interfaccia .
livello minaccia	Valore che determina il cambiamento dello stato di sicurezza di un elemento a Livello di avviso o Critico.
score totale	La somma dei punteggi di una Content Control List, secondo il contenuto per cui è stato eseguito il match.
trigger score	Il numero di volte in cui viene eseguito il match di un'espressione regolare prima che lo si esegua con la Content Control List.
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.
tipo	I parametri secondo cui vengono classificate le Content Control List di SophosLabs; per esempio una Content Control List che definisce dati di passaporti, indirizzi postali o indirizzi e-mail appartiene alla tipologia Personally Identifiable Information (dati che possono portare all'identificazione personale).
gestore degli aggiornamenti	Consultare la sezione *Sophos Update Manager*.
livello di avviso	Valore che determina il cambiamento dello stato di sicurezza di un elemento a Livello di avviso.
controllo web	Una funzione che consente di impostare e distribuire criteri di accesso al web per la propria organizzazione; consente anche di visualizzare report sull'utilizzo del web. È possibile consentire o bloccare l'accesso a determinate categorie di siti web e avvisare gli utenti che l'accesso a un determinato sito web costituisce violazione dei criteri.
protezione web	Una funzione che rileva le eventuali minacce presenti nelle pagine web. Questa funzione consente il blocco di pagine web che hanno, in passato, ospitato contenuti malevoli, oltre che di download malevoli. La protezione web è parte del criterio antivirus e HIPS.

Copyright © Sophos Limited

15 Supporto tecnico

È possibile ricevere supporto tecnico per i prodotti Sophos in ciascuno dei seguenti modi:

- Visitando la Sophos Community su community.sophos.com/ e cercando altri utenti che hanno riscontrato lo stesso problema.
- Visitando la knowledge base del supporto Sophos su www.sophos.com/it-it/support.aspx.
- Scaricando la documentazione del prodotto da www.sophos.com/it-it/support/documentation.aspx.
- Aprendo un ticket col team di supporto su https://secure2.sophos.com/it-it/support/contact-support/support-query.aspx.

Copyright © Sophos Limited

16 Note legali

Copyright © 2018 . Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero informazioni, o trasmessa, in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, inclusi le fotocopie, la 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.

, e sono marchi registrati di , e , qualora applicabile. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.

Indice analitico

A

abilitazione della protezione web 103
abilitazione della ricerca automatica di un percorso 73
accesso ad Enterprise Console 22, 22
accesso ai dischi 82
Active Directory
    allarmi sincronizzazione 194
    importazione da 33
    sincronizzazione con 38
adware
    ricerca di 82
adware autorizzati, blocco 110
adware e PUA
    autorizzazione 109
adware e PUA, preautorizzazione 110
aggiornamento
    aggiornamento intelligente 71, 72
    aggiornamento intelligente, abilitazione 73
    automatico 68
    computer non aggiornati 78
    dati proxy 70, 71, 74
    fonte degli aggiornamenti primaria 70, 71
    fonte degli aggiornamenti secondaria 70, 74
    fonte per l'installazione iniziale 76
    immediato 78
    limitazione della larghezza di banda 70, 71, 74
    log 76
    manuale 78
    pacchetti software 64
    pianificazione 75
    pubblicazione del software in un server web 63
    ricerca automatica di un percorso 71, 72
    ricerca automatica di un percorso, abilitazione 73
    server primario 70, 71
    server secondario 70, 74
    tipi 64
    versioni fisse 65
aggiornamento automatico 68
aggiornamento immediato 78
aggiornamento intelligente
    abilitazione 73
aggiornamento manuale 78
aggiunta di applicazioni 115, 122
aggiunta di computer 33
aggiunta di computer a gruppi 24
aggiunta diritti 15
allarmi
    cancellazione 53
    e-mail 187
    gestione 51, 52
    gestore degli aggiornamenti 78
    informazioni sugli oggetti rilevati 52
    risoluzione 51, 52
    Sincronizzazione di Active Directory 194
    sottoscrizioni 186
    stato della rete 193
allarmi e-mail
    antivirus e HIPS 187
    Sincronizzazione di Active Directory 194
    stato della rete 193
allarmi HIPS
    e-mail 187
allarmi relativi alla sottoscrizione 186
allarmi sullo stato della rete 193
allarmi virus
    e-mail 187
analisi del comportamento in fase di esecuzione 96
antivirus 80
applicazione criteri 30
applicazioni
    aggiunta 115, 122
    attendibilità 115, 122, 123, 124
    blocco 124
applicazioni controllate
    blocca 145
    ricerca di 146
applicazioni controllate, disinstallazione 147
assegnazione criteri 30
assegnazione diritti 15
Attendibilità delle applicazioni 115, 122, 123, 124
autorizzazione
    adware e PUA 109
    condivisione stampanti 117
    oggetti sospetti 111
    processi nascosti 125
    raw socket 126
    Sito web 112
    traffico LAN 116
avvisa 178

B

blocca
    applicazioni controllate 145
blocco
    adware autorizzati 110
    applicazioni 124
    condivisione stampanti 118
    PUA autorizzate 110
blocco rimozione
    abilitazione 170
    attivazione 170
    come cambiare la password 170
    disabilitazione 170
    disattivazione 170
    eventi 169, 199
    panoramica 169
blocco rimozione avanzato
    impostazioni 171
    Informazioni su 171
boot sector infetto 82
buffer overflow
    rilevamento 99

C

cancellazione allarmi 53
cancellazione criteri 31
cancellazione di un gruppo 25
cancellazione errori 53
cancellazione ruoli 15
Cartella Nessun gruppo 23
categorie dei siti web 176, 178
checksum 127
come gestire gli allarmi 51, 52
comportamento malevolo
    rilevamento 97
comportamento sospetto
    rilevamento 98
computer aggiornati
    verifica 49
computer con problemi 49
computer disconnessi 7
computer gestiti 7
computer non aggiornati
    aggiornamento 78
    ricerca 49
computer non gestiti 222
computer non protetti 49
computer protetti 47, 48
condivisione file e stampanti, autorizzazione 117
condivisione file e stampanti, blocco 118
condivisione file, autorizzazione 117
condivisione file, blocco 118
condivisione stampanti
    autorizzazione 117
condivisione stampanti, autorizzazione 117
condivisione stampanti, blocco 118
configurazione
    criteri 28
    filtri elenco computer 8
    gestore aggiornamenti 56
    Pannello di controllo 48
    reportistica centrale 142
    scansione in accesso 82
configurazione firewall
    esportazione 144
    importazione 144
configurazione, applicazione di 141
configurazioni secondarie, creazione di 141
consenso alla condivisione file e stampanti 117
consenti 178
Content Control List
    creazione 158
    creazione tramite editor avanzato 159
    modifica 158
    modifica tramite editor avanzato 159
controllo
    abilitazione 218
    disabilitazione 218
controllo applicazioni
    eventi 196
    messaggistica 190
controllo dati
    abilitazione 153
    aggiunta di regole a un criterio 156
    Attivazione o disattivazione 153
    azioni 148
    CCL 151
    come abilitare il controllo dati 153
    condizioni della regola 148
    Content Control List 151
    creazione di Content Control List 158
    editor di Content Control List avanzato 159
    esclusione file 157
    esportazione di Content Control List 161
    esportazione regole 158
    eventi 152, 197
    importazione di Content Control List 161
    importazione regole 158
    messaggistica 190
    modifica di Content Control List 158
    panoramica 147
    regole 151
    regole "file che soddisfa la regola" 153
    regole dei contenuti 155
    rimozione regole da un criterio 157
controllo dispositivi
    eventi 162, 197
    panoramica 161
Controllo dispositivi
    blocco bridging di rete 163
    blocco dispositivi 165
    dispositivi controllati 163
    elenco di dispositivi 168
    esenzione di un dispositivo da tutti i criteri 166
    esenzione di un dispositivo da un criterio 167
    messaggistica 192
    rilevamento dispositivi senza bloccarli 165
    rilevamento e blocco dei dispositivi 165
    selezione dei tipi di dispositivo 164
controllo web 174
Controllo web 175, 176, 178, 180
controllo web di base 176, 178
copia
    dati elenco computer 219
    dettagli computer 219
creazione dei criteri 30
creazione dei gruppi 24
creazione di report 207
creazione di sottoambienti 16
Creazione di una scansione pianificata 89
creazione ruolo 14
criteri
    antivirus e HIPS 80
    applicazione 30
    assegnazione 30
    configurazione 28
    creazione 30
    enforcing (attuazione dei criteri) 32
    gruppi che utilizzano 32
    modifica 31
    panoramica 26
    predefiniti 27
    rimozione 31
    rinomina 31
    verifica 32
criteri antivirus e HIPS 80
criteri del controllo applicazioni 144

Copyright © Sophos Limited

criterio 180
criterio controllo web 174

D

dettagli computer
    copia 219
    stampa 220
di base 175
diritti
    aggiunta 15
    assegnazione 15
disinfezione
    automatico 85, 85, 92, 92
    manuale 55, 55
    non riuscita 226
disinfezione automatica 85, 85, 92, 92
disinfezione manuale 55, 55
disinfezione non riuscita 226
disinstallazione applicazioni controllate 147
distribuzione software 59
Due schede di rete
    utilizzo 139

E

eccezioni per siti web 179
elenco computer
    copia dei dati da 219
    stampa dei dati da 219
Enterprise Console
    copia dei dati da 219
    stampa dei dati da 219
errori
    cancellazione 53
esclusioni
    importazione o esportazione 88, 95
    scansione in accesso 87
    scansione pianificata 94
esecuzione dei report 215
esportazione report 215
estensioni 104
eventi
    blocco rimozione 199
    controllo applicazioni 196
    controllo dati 197
    controllo dispositivi 197
    esclusione dalla prevenzione degli exploit 205
    esportazione in un file 205
    firewall 198
    Previeni exploit 204
    verifica patch 200
    web 203, 204

F

Feedback a Sophos 195
file che soddisfa le regole del controllo dati
    creazione 153
file di archivio, scansione 82
file sospetti
    ricerca di 82
filtraggio dei messaggi ICMP 129
filtraggio elenco computer
    in base agli oggetti rilevati 8
filtraggio URL 102
firewall
    abilitazione 119
    aggiunta di applicazioni 115, 122
    aggiunta di checksum 127
    Attendibilità delle applicazioni 115, 122, 123, 124
    configurazione avanzata 120
    consenso alla condivisione file e stampanti 117
    creazione di una regola 118, 136
    disabilitazione 119
    eventi 198
    impostazione 113
    opzioni avanzate 120
fonte degli aggiornamenti
    alternativa 71
    primaria 70, 71
    secondaria 70, 74
    server web 63
fonte di aggiornamento alternativa 71
fonte per l'installazione iniziale 76

G

gestore aggiornamenti
    addizionale 62
    aggiornamento 61
    aggiunta 62
    allarmi 77
    Allineamento con la configurazione 62
    configurazione 56
    errori 77
    monitoraggio 77
    scelta di una fonte degli aggiornamenti 57
    stato 77
    visualizzazione della configurazione 56
gestore degli aggiornamenti
    allarmi
        cancellazione 78
    autoaggiornamento 61
    distribuzione software 59
    log 61
    pianificazione 60
Glossario 229
gruppi
    aggiunta di computer 24
    creazione 24
    criteri utilizzati 25
    importazione dei gruppi da Active Directory 33
    Nessun gruppo 23
    rimozione 25
    rimozione computer 24
    rinomina 25
    sincronizzazione con Active Directory 38
    tagliare e incollare 25
gruppo sincronizzato 38

H

HIPS (Sistema di prevenzione delle intrusioni su host) 80, 95
Host Intrusion Prevention System (Sistema di prevenzione delle intrusioni su host) 95

I

icone 7
icone di allarme 50
importazione computer
    dal file 35
impostazione delle regole globali 132, 134, 139
impostazione di una regola 133, 134, 134
individuazione dei computer
    con Active Directory 34
    importazione da file 35
    importazione dei gruppi da Active Directory 33
    nella rete 34
    per intervallo IP 35
Installazione 11
interfaccia
    Vista computer 6
    Vista dei gestori degli aggiornamenti 10
Interfaccia di Enterprise Console
    Vista computer 6
    Vista dei gestori degli aggiornamenti 10
Introduzione 11

L

larghezza di banda
    limitazione 70, 71, 74
    regolazione 70, 71, 74
log eventi 194

M

mancata installazione
    Sophos Endpoint Security and Control 223
Mancata installazione di Sophos Endpoint Security and Control 223
memoria di sistema, scansione 82
messaggi ICMP
    filtraggio 129
    informazioni su 129
messaggistica
    controllo applicazioni 190
    desktop 189
    SNMP 188
Messaggistica desktop 189
messaggistica HIPS
    desktop 189
    SNMP 188
Messaggistica SNMP 188
messaggistica virus
    desktop 189
    SNMP 188
modalità di funzionamento, cambia a interattiva 121
modalità interattiva, abilitazione 121
modalità interattiva, info su 120
modalità monitor 115
modalità non interattiva, cambia con 121
modifica criteri 31
modifica ruoli 15
monitoraggio del comportamento
    abilitazione 96
    attivazione 96
    disabilitazione 96
    disattivazione 96

N

Nessun gruppo 23, 223
nuovo utente 22

O

oggetti potenzialmente sospetti, preautorizzazione 111
oggetti sospetti
    autorizzazione 111
    consenti 111
oggetti sospetti, cancellazione dall'elenco degli oggetti autorizzati 111
Oggetto parzialmente rilevato 225
organizzazione elenco computer
    computer con problemi 49
    computer non protetti 49

P

Pannello di controllo
    configurazione 48
    icone dello stato di sicurezza 5
    pannelli 4
percorsi bootstrap 47
percorsi primari, definizione di 140
Percorso doppio 113, 139
pianificazione aggiornamento 60
pianificazione degli aggiornamenti 75
pianificazione dei report 214
preautorizzazione
    Sito web 112
preautorizzazione di adware e PUA 110
preautorizzazione di oggetti potenzialmente sospetti 111
Prevenzione degli exploit
    abilitazione 183, 184, 185
    attivazione 183, 184, 185
    disabilitazione 183, 184, 185
    disattivazione 183, 184, 185
    eventi 204
    panoramica 182
priorità regole 130
problemi di connettività 225
Procedura guidata per la protezione dei computer
    Credenziali 45
    Selezione delle funzioni 45
processi nascosti, autorizzazione 125
protezione automatica
    durante la sincronizzazione con Active Directory 40
Protezione dei computer
    Credenziali 45
    preparazione per l'installazione 44

Copyright © Sophos Limited

prerequisiti, antivirus 44
Procedura guidata per la protezione dei computer 45
Selezione delle funzioni 45
protezione web
abilitazione 103
disabilitazione 103
panoramica 102
protezione, verifica 47
PUA
allarmi frequenti 226
effetti secondari 227
non rilevati 225
ricerca di 82
PUA autorizzate, blocco 110
pubblicazione del software in un server web
Internet Information Services (IIS) 63
pulsanti barra degli strumenti 2
punto di sincronizzazione 38

R

raw socket, autorizzazione 126
Regola
impostazione 133, 134, 134
regole dei contenuti del controllo dati
creazione 155
regole del controllo dati
aggiunta a un criterio 156
regole globali
impostazione 132, 134, 139
report
allarmi ed eventi per nome dell'oggetto 209
allarmi ed eventi per orario 210
allarmi ed eventi per percorso 211
creazione 207
criterio del computer non conforme 212
cronologia allarmi ed eventi 208
esecuzione 215
esportazione 215
eventi per utente 213
gerarchia aggiornamenti 214
layout 216
non conformità del criterio in base all'ora 212
panoramica 207
pianificazione 214
protezione dei computer gestiti 214
protezione dei computer in base all'ora 214
riepilogo allarmi 209
stampa 215
visualizza come tabella 215
reportistica centrale, configurazione 142
reputazione del download 102, 103
rete protetta 47
ricerca automatica di un percorso
abilitazione 73
ricerca computer
in Enterprise Console 9
ricerca di adware e PUA 82
ricerca di file sospetti 82
ricerca di virus di Mac 82
riconoscimento presenza
impostazione 140
Informazioni su 139
Utilizzo di due schede di rete 139
Rilevamento del traffico malevolo 95
rilevamento di buffer overflow 99
rilevamento di comportamento malevolo 97
rilevamento di comportamento sospetto 98
rilevamento di traffico malevolo 97
rimozione computer da gruppo 24
rinomina criteri 31
rinomina gruppi 25
risoluzione allarmi
azioni da intraprendere 51, 52, 52
informazioni sugli oggetti rilevati 52
stato disinfezione 51, 52
Risoluzione dei problemi
allarmi in sospeso 222
computer non aggiornati 224
computer non gestiti 222
controllo dati 228
controllo dati, browser incorporati 228
disinfezione 226
disinstallazione di Update Manager 228
firewall disabilitato 221
firewall non installato 221
Linux 224, 224
Mac 224
Mancata installazione di Sophos Endpoint Security and Control 223
Nessun gruppo 223
Oggetto parzialmente rilevato 225
problemi di connettività 225
PUA, allarmi frequenti 226
PUA, effetti secondari 227
PUA, non rilevati 225
scansione in accesso 221
timeout 225
UNIX 224, 224
virus, effetti secondari 227
Windows 225
ruoli
assegnazione di diritti a 15
creazione 14
modifica 15
preconfigurati 14
rimozione 15
rinomina 15
ruoli preconfigurati 14
ruoli utenti
visualizzazione 17

S

scansione
pianificato 90
Scansione
esclusioni 105
scansione completa del sistema 53
scansione dei computer
immediatamente 53
scansione dei contenuti
abilitazione 103
disabilitazione 103

scansione dei file di archivio 82
scansione del download
abilitazione 103
disabilitazione 103
scansione della memoria di sistema 82
scansione di tutti i file 82
scansione immediata 53, 53
scansione in accesso
abilitazione 84
attivazione 84
configurazione 82
disabilitazione 84
disattivazione 84
disinfezione 85
esclusione di oggetti dalla 87
importazione o esportazione di esclusioni 88
in lettura 82
in scrittura 82
migliori pratiche 82
se rinominati 82
software di cifratura 82
specificazione delle estensioni dei file 86
scansione pianificata
disinfezione 92
esclusione di oggetti dalla 94
importazione o esportazione di esclusioni 95
specificazione delle estensioni dei file 93
scansioni pianificate
creazione 89
impostazioni di scansione 90
scansioni su richiesta 89
scelta del software 58
scelta sottoscrizioni 69
server di aggiornamento 56
server primario
modifica delle credenziali 73
server secondario 70, 74
simboli di allarme 7
Sincronizzazione con Active Directory
abilita 42
disabilita 42
proprietà, modifica 41
protezione automatica 40
Sincronizzazione di Active Directory 36
Sito web
autorizzazione 112
consenti 112
preautorizzazione 112
software
selezione 58
sottoscrizione a 66
Sophos Central 2
Sophos Enterprise Console 10
Sophos Live Protection
abilitazione 101
attivazione 101
disabilitazione 101
disattivazione 101
panoramica 100
tecnologia in-the-cloud 100
Sophos Mobile 2, 43
Sophos Update Manager 56
sottoambiente dell'utente
visualizzazione 17
sottoambienti
attivo 16
copia 16
creazione 16
modifica 16, 16
rimozione 17
rinomina 16
selezione 16
sottoscrizione al software 66
sottoscrizioni
aggiunta 66
selezione 69
specificazione delle estensioni dei file per la scansione in accesso 86
specificazione delle estensioni dei file per la scansione pianificata 93
spyware 80
stampa
dati elenco computer 219
dettagli computer 220
stampa dei report 215
stato disinfezione 51, 52

T

tecnologia in-the-cloud 100
timeout 225
tipi di aggiornamento 64
Tipi di file da esaminare 104
tool di rimozione
rimozione del software di sicurezza prodotto da terzi 44
Tool di rimozione del software di sicurezza prodotto da terzi 44
traffico LAN, autorizzazione 116
traffico malevolo
rilevamento 97
trojan 80
tutti i file, scansione 82

U

utilizzo della sottoscrizione 68

V

verifica patch
abilitazione 173
attivazione 173
dati patch 201
disabilitazione 173
disattivazione 173
eventi 173, 200
impostazioni predefinite 172
intervallo 173
panoramica 172
viste eventi 199
versioni fisse, aggiornamenti 65
virus
effetti secondari 227

Copyright © Sophos Limited

virus di Mac, ricerca 82
Vista computer
    copia dei dati da 219
    stampa dei dati da 219
Vista dei gestori degli aggiornamenti 10

W

web
    eventi 203, 204
web appliance 180
worm 80