

SOPHOS

Sophos Control Center Guida in linea

Versione prodotto: 4.1

Data documento: marzo 2010



Sommario

1 Sophos Control Center.....	3
2 Introduzione a Sophos Control Center.....	4
3 Verifica della protezione della rete.....	8
4 Protezione dei nuovi computer.....	10
5 Aggiornamento computer.....	12
6 Risoluzione di allarmi e minacce.....	14
7 Nuova protezione dei computer.....	18
8 Monitoraggio dei computer protetti.....	19
9 Visualizzazione eventi.....	22
10 Configurazione della scansione.....	25
11 Configurazione degli aggiornamenti.....	34
12 Configurazione firewall.....	37
13 Configurazione del controllo applicazioni.....	41
14 Configurazione del controllo dispositivi.....	44
15 Gestione notifiche.....	47
16 Gestione report.....	51
17 Troubleshooting.....	56
18 Supporto tecnico.....	57
19 Copyright.....	58

1 Sophos Control Center

Tramite Sophos Control Center, è possibile:

- Installare software antivirus e firewall nella rete.
Le licenze di Sophos Security Suite e Sophos Computer Security comprendono il firewall, mentre la licenza di Sophos Anti-Virus no.
- Mantenere il software aggiornato automaticamente tramite Internet.
- Configurare centralmente il rilevamento e la rimozione di virus, worm, trojan, spyware e applicazioni potenzialmente indesiderate, quali adware, dialer, strumenti di amministrazione remota e strumenti di hacking.
- Verificare quali applicazioni possono essere eseguite nella rete.
- Evitare che gli utenti utilizzino dispositivi non autorizzati nei computer.
- Configurare centralmente firewall, applicazioni controllate e controllo dispositivi per i computer nella rete.
- Monitorare la rete e verificare che i computer siano protetti e conformi alla configurazione centrale.
- Fornire un riepilogo delle minacce.
- Generare report sulle tendenze delle minacce.

È possibile utilizzare Sophos Control Center per proteggere:

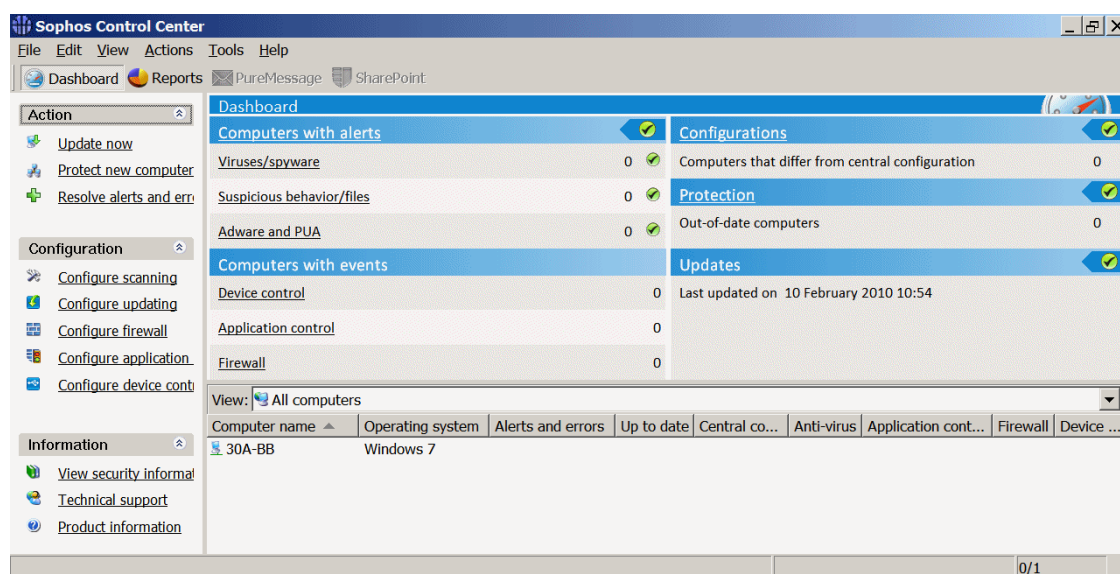
- Computer con sistema operativo Windows 2000 e successivo
- Computer con sistema operativo Windows 98 (SE)
- Computer con sistema operativo Mac OS X

Nota: Sophos Control Center versione 4.1 è compatibile solamente con Windows 7 e Windows Server 2008 R2.

2 Introduzione a Sophos Control Center

2.1 Interfaccia

È possibile utilizzare e configurare i software Sophos Anti-Virus e Sophos Client Firewall tramite l'interfaccia di Sophos Control Center, rappresentata in questa immagine. Le principali funzioni sono descritte di seguito.



Menu Azioni

Questo menu consente di aggiornare i software antivirus e (se compreso nella licenza) firewall, proteggere i computer e risolvere le minacce.

Menu Configurazione

Questo menu consente di configurare i software antivirus e firewall, oltre che di impostare allarmi relativi alle minacce.

Menu Info

Questo menu consente di accedere ai dati relativi alle minacce contenuti nel sito web Sophos, al supporto tecnico e alle informazioni sul prodotto.

Barra degli strumenti

■ Report

Cliccare su questo pulsante per aprire la finestra di dialogo **Report Manager**. Per informazioni su come creare report, consultare la sezione [Creazione di un report](#) a pagina 51.

■ PureMessage

Gli utenti di PureMessage possono avviare la console di PureMessage cliccando su questo pulsante. Il pulsante è attivo solo se la console di PureMessage è installata nello stesso computer di Sophos Control Center.

■ SharePoint

Gli utenti di Sophos per Microsoft SharePoint possono attivare Sophos per Microsoft SharePoint cliccando su questo pulsante. Il pulsante è attivo solo se Sophos per Microsoft SharePoint è installata nello stesso computer di Sophos Control Center.

Pannello di controllo

Il **Pannello di controllo** fornisce una visione d'insieme dello stato della protezione della rete. Per mostrare o nascondere il pannello di controllo, cliccare sul pulsante **Pannello di controllo** nella barra degli strumenti. Per ulteriori informazioni sul pannello di controllo, consultare la sezione [Panoramica del pannello di controllo](#) a pagina 8.

Elenco computer

Consente di visualizzare:

- Se la protezione antivirus e firewall è attiva, inattiva o non è installata.
- Se i computer sono conformi alla configurazione impostata centralmente tramite Sophos Control Center.
- Dove si rilevano allarmi.

Per spiegazioni relative alle icone visualizzate nell'elenco dei computer, consultare la sezione [Significato delle icone](#) a pagina 5.

Per ordinare l'elenco computer in colonne, cliccare sull'intestazione della colonna che si desidera ordinare.


Per visualizzare i dettagli di un computer, quali versione e stato dei software antivirus e firewall, gli allarmi in sospeso e la cronologia del rilevamento delle minacce, cliccare due volte sul computer nell'elenco in modo tale da visualizzare la finestra **Dettagli computer**. In alternativa, evidenziare il computer, cliccarvi col tasto destro del mouse e selezionare **Visualizza dettagli computer**.


2.2 Significato delle icone

Nell'elenco computer, le icone indicano:




- Allarmi
- Protezione disabilitata o non aggiornata
- Stato di ogni computer, ad es. se il software viene installato.

Allarmi







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.

Icona	Descrizione
	<p>Un simbolo d'allarme giallo visualizzato nella colonna Allarmi ed errori indica uno dei seguenti problemi.</p> <ul style="list-style-type: none"> ■ È stato rilevato un file sospetto. ■ È stata rilevata la presenza di adware o altre applicazioni potenzialmente indesiderate. ■ Si è verificato un errore. <p>Un simbolo d'allarme giallo visualizzato nella colonna Configurazione centralizzata indica che il computer non è conforme alla configurazione centrale come gli altri computer in rete.</p>



Protezione disabilitata o scaduta

Icona	Descrizione
	Uno scudo grigio e la parola "Inattivo/a" nella colonna Antivirus dell'elenco computer indica che la scansione in accesso non è attiva.
	Un'icona del firewall grigia e la parola "Inattivo/a" nella colonna Firewall indica che il firewall è disattivato.
	Un'icona a forma di orologio e la parola "No" nella colonna Aggiornato indica che il software è scaduto.

Stato computer

Icona	Descrizione
	Il computer blu indica che il computer è gestito da Sophos Control Center.
	Il computer con la freccia gialla indica che l'installazione del software antivirus e del firewall è in sospeso.
	Il computer con la freccia verde indica che l'installazione è in corso.
	Il computer con la clessidra indica che il componente di aggiornamento di Sophos Anti-Virus è stato installato e sta ora scaricando la versione più recente del prodotto.
	Il computer grigio indica che il computer non è gestito da Sophos Control Center.
	Il computer con la croce rossa a fianco indica che il computer è disconnesso.

Stato Pannello di controllo

Icona	Descrizione
	L'icona verde corrisponde allo stato "normale". Il numero di computer interessati è al di sotto del livello di minaccia.
	Una icona rossa indica che il livello della soglia di minaccia è stato superato per la categoria corrispondente.

2.3 Priorità degli allarmi

In presenza di allarmi multipli sullo stesso computer, nell'elenco computer sarà visualizzata l'icona dell'allarme con la priorità più alta. I tipi di allarme sono elencati qui sotto in ordine decrescente di priorità.

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

3 Verifica della protezione della rete

3.1 Panoramica del pannello di controllo

È possibile utilizzare il pannello di controllo per verificare lo stato di sicurezza della rete. Per mostrare o nascondere il pannello di controllo, cliccare sul pulsante **Pannello di controllo** nella barra degli strumenti.

Dashboard	
Computers with alerts ✓	Configurations ⚠
<u>Viruses/spyware</u> 0 ✓	Computers that differ from central configuration 1
<u>Suspicious behavior/files</u> 0 ✓	Protection ⚠
<u>Adware and PUA</u> 0 ✓	Out-of-date computers 1
Computers over event threshold ✓	Updates ✓
<u>Device control</u> 0 ✓	Last updated at Not available
<u>Application control</u> 0 ✓	
<u>Firewall</u> 0 ✓	

L'interfaccia del pannello di controllo è composta da cinque sezioni aventi indicatori di stato che mostrano lo stato di ogni sezione in base al valore di soglia:

Computer con allarmi

Questa sezione visualizza il numero dei computer gestiti che presentano allarmi su:

- 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 sospenso, cliccare sul titolo della sezione **Computer con allarmi**.

Computer che superano la soglia degli eventi

Questa sezione visualizza il numero di eventi rilevati sotto controllo dispositivi, applicazioni controllate e applicazioni bloccate dal firewall, con indicatori di stato che mostrano lo stato di ogni categoria.

Configurazioni

Questa sezione visualizza il numero di computer gestiti che non corrispondono alla configurazione centrale.

Per visualizzare l'elenco dei computer gestiti che non corrispondono alla configurazione centrale, cliccare sul titolo della sezione **Configurazioni**.

Protezione

Questa sezione visualizza il numero dei computer connessi e gestiti nei quali 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 della sezione **Protezione**.

Aggiornamenti

Questa sezione visualizza la data e l'ora dell'ultimo aggiornamento da Sophos.

3.2 Configurazione pannello di controllo

Il pannello di controllo visualizza indicatori di stato secondo la percentuale dei computer gestiti aventi allarmi o errori in sospenso, oppure secondo il tempo trascorso dall'ultimo aggiornamento da Sophos. Se viene superato un livello, l'indicatore di stato del pannello di controllo cambia.

Per configurare il pannello di controllo in modo da indicare lo stato:

1. Dal menu **Strumenti**, selezionare **Configura pannello**.

Viene visualizzata la finestra di dialogo **Configura pannello**.

2. Cambiare i valori di soglia nei campi di testo relativi al livello secondo necessità.
 - a) Sotto **Computer con allarmi in sospenso**, inserire la percentuale di computer gestiti colpiti da un determinato problema per innescare il cambiamento del relativo indicatore.
 - b) Sotto **Computer con eventi**, inserire il numero di eventi oltre al quale è necessario inviare gli allarmi.
 - c) Sotto **Configurazione e protezione**, inserire la percentuale di computer gestiti interessati in modo tale da innescare il cambiamento dei relativi indicatori.
 - d) Sotto **Ultima protezione da Sophos**, inserire il numero di ore trascorse dalla ricezione dell'ultimo aggiornamento da Sophos. Ciò innescherà il cambiamento dell'indicatore "Aggiornamenti".
 - e) Cliccare su **OK**.

Se si imposta un livello su zero, gli avvisi vengono generati non appena viene ricevuto il primo allarme.

È inoltre possibile impostare allarmi e-mail da inviare a destinatari a scelta ogni qual volta il valore di soglia venga superato. Per informazioni, consultare la sezione [Impostazione degli allarmi e-mail sullo stato della rete](#) a pagina 48.

4 Protezione dei nuovi computer

4.1 Protezione dei nuovi computer

Se alla rete vengono aggiunti nuovi computer, è necessario proteggerli con software antivirus e, se compreso nella propria licenza, firewall.

Nota: solo i computer con sistema operativo Windows 2000 e successivo sono destinati all'installazione dal momento che né l'installazione automatica né l'upgrade sono attuabili in computer Windows 95, 98, NT o Mac OS X.

Se si è in possesso di computer che eseguono sistemi operativi diversi (quali Win 95, 98, NT o Mac OS X) da quelli utilizzati in precedenza, consultare la sezione [Protezione di nuovi sistemi operativi](#) a pagina 11.

Per proteggere nuovi computer:

1. In Sophos Control Center, dal menu **Azioni**, cliccare su **Proteggi nuovi computer**.

Viene avviata la **Procedura guidata Sophos per la protezione della rete**.

2. Nella pagina relativa ai **Dati dell'account utente di Windows**, inserire i dettagli relativi all'account amministratore da utilizzare per installare il software nei computer della rete.
3. Nella pagina **Protezione dei computer**, attendere che i computer vengano individuati.

Nella colonna **Proteggi**, selezionare i computer che si desidera proteggere e cliccare su **Avanti**.

4. Nella pagina **Seleziona funzioni**, selezionare le funzioni che si desidera installare nei computer.

- Il software antivirus è selezionato per essere installato per impostazione predefinita in tutti i computer.

- Se si desidera installare il firewall, selezionare la casella di spunta **Firewall**.

Il firewall può essere installato solo nelle workstation con sistema operativo Windows 2000 o successivo; non può essere installato nei computer in cui sono installati sistemi operativi per server. Il firewall richiede Sophos Anti-Virus.

Nota: è necessario riavviare tutti i computer se si sceglie di installare e attivare Sophos Client Firewall.

- Se si desidera rimuovere un qualsiasi software di sicurezza prodotto da terzi, selezionare la casella di spunta **Tool di rimozione del prodotto concorrente**.

5. Se nella pagina **Computer che bisogna proteggere manualmente** sono elencati dei computer, cliccare su **Stampa** per stampare l'elenco dei computer non protetti.

In alternativa, cliccare su **Salva con nome** per salvare una copia dell'elenco, oppure annotare i computer.

6. Nell'ultima pagina della procedura guidata, cliccare su **Fine**.

Dopo aver chiuso la procedura guidata, Sophos Control Center installa automaticamente il software sul maggior numero possibile di computer selezionati. Sarà quindi possibile visualizzare i computer elencati in Sophos Control Center, con informazioni relative al loro stato.

7. Andare a ciascun computer inserito nell'elenco dei computer non protetti ed installare il software manualmente. Per informazioni su come eseguire l'installazione manuale, consultare la Guida di avvio di Sophos Control Center.

4.2 Protezione di nuovi sistemi operativi

Se si aggiungono nuovi tipi di computer alla rete, per esempio se si aggiungono per la prima volta computer con sistema operativo Windows 95, 98, NT o Mac OS X, è necessario abilitare Sophos Control Center per il download del software antivirus per quel determinato tipo di computer.

Sophos Client Firewall può essere installato solo nei computer con sistema operativo Windows 2000 o successivo.

Per proteggere nuovi sistemi operativi:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura aggiornamento**.
2. Nella finestra di dialogo **Configura aggiornamento**, nella scheda **Software**, selezionare il sistema o sistemi operativi che si desidera proteggere.
3. Ritornare alla finestra principale di Sophos Control Center. Nel menu **Azioni**, cliccare su **Aggiorna ora**.
4. Andare a tutti i computer di nuova tipologia e installare il software. Per informazioni su come eseguire l'installazione manuale, consultare la *Guida di avvio di Sophos Control Center*.

5 Aggiornamento computer

5.1 Funzionamento dell'aggiornamento

Sophos Control Center verifica la disponibilità di aggiornamenti da Sophos ogni 60 minuti e, nel caso in cui siano disponibili nuovi aggiornamenti, li scarica.

Questo software è quindi disponibile nel computer in cui si esegue Sophos Control Center. I computer gestiti da Sophos Control Center si autoaggiornano automaticamente dalla copia centrale (per impostazione predefinita, verificano la disponibilità di aggiornamenti ogni 5 minuti).

L'orario dell'ultimo aggiornamento da Sophos viene visualizzato nel pannello di controllo di Sophos Control Center.

5.2 Riuscita degli aggiornamenti

L'aggiornamento del software di sicurezza richiede due passaggi:

1. Sophos Control Center scarica gli aggiornamenti da Sophos.
2. I computer si aggiornano dal server.

Se uno di questi due passaggi non riesce, si viene allertati secondo quanto riportato di seguito:

■ Sophos Control Center non riesce a scaricare gli aggiornamenti

Se il download non riesce, nel pannello di controllo di Sophos Control Center viene visualizzato un messaggio. È possibile scegliere di ricevere un avviso quando il download non riesce. Per informazioni, consultare la sezione [Impostazione degli allarmi e-mail sullo stato della rete](#) a pagina 48.

■ I computer non riescono ad autoaggiornarsi

Nell'elenco di computer, nella colonna **Aggiornato** viene visualizzata la parola "No" al fianco di ogni computer non aggiornato. Per forzare l'aggiornamento di un computer, evidenziare il computer che si desidera aggiornare e cliccarvi col tasto destro del mouse. Nel menu, cliccare su **Aggiorna computer**.

5.3 Ricezione di avvisi sull'ultimo aggiornamento

È possibile configurare Sophos Control Center in modo da ricevere avvisi nel caso si verifichino problemi durante il download degli aggiornamenti da Sophos.

Per ricevere avvisi sull'ultimo aggiornamento:

1. Nel menu **Strumenti**, selezionare **Configura allarmi e-mail**.
2. Nella finestra di dialogo **Configura allarmi e-mail**, cliccare su **Configura** ed inserire i dettagli del server SMTP.

3. Cliccare su **Aggiungi**, digitare l'indirizzo e-mail ed impostare la lingua in cui si desidera inviare gli avvisi.
4. Nella sezione **Sottoscrizioni**, sotto **Livello superato**, assicurarsi che l'opzione **Tempo trascorso dall'ultimo aggiornamento da Sophos** sia selezionata; infine cliccare su **OK**.

5.4 Aggiornamento manuale della rete

È possibile scegliere di aggiornare il software di sicurezza manualmente.

Per aggiornare il software di sicurezza manualmente:

1. Nel menu **Azioni**, cliccare su **Aggiorna ora**.
2. Sophos Control Center visualizza un messaggio che richiede di confermare se si desidera eseguire un aggiornamento. Cliccare su **Sì**.

Sophos Control Center contatta Sophos e scarica la versione più recente dei software antivirus e, se questa opzione è stata selezionata, firewall. La prossima volta in cui si ricercheranno aggiornamenti nel server, tutti i computer della rete verranno aggiornati automaticamente.

5.5 Aggiornamento di un computer singolo

Se un computer risulta non aggiornato (nella colonna **Aggiornato** compare la parola "No"), è possibile spingerlo ad aggiornarsi.

- ❖ Nell'elenco computer, evidenziare il computer che si desidera aggiornare e cliccarvi col tasto destro del mouse. Nel menu, cliccare su **Aggiorna computer**.

6 Risoluzione di allarmi e minacce

6.1 Quando una minaccia viene rilevata

Se nella rete è stata rilevata una minaccia e non è stata automaticamente eliminata:

- Sophos Control Center invierà un allarme, se la scansione degli allarmi è abilitata. Per informazioni, consultare la sezione [Impostazione degli allarmi antivirus e HIPS](#) a pagina 47.
- In Sophos Control Center, nell'elenco computer, sul nome del computer infetto comparirà una icona di allarme. Per scoprire da che cosa è dovuto l'allarme, evidenziare il computer nell'elenco computer, cliccarvi col tasto destro del mouse e selezionare **Visualizza dettagli computer**. Per informazioni sulle icone di allarme, consultare la sezione [Significato delle icone](#) a pagina 5
- In Sophos Control Center, nel riquadro **Pannello di controllo**, verrà visualizzato il numero totale di virus e spyware rilevati nella rete.

6.2 Disinfezione del computer

Per gestire le minacce, i virus e spyware, oltre che i PUA rilevati nei computer, fare quanto segue:

1. Nel menu **Azioni**, cliccare su **Risolvi allarmi ed errori**.
In alternativa, è possibile cliccare sui link relativi al tipo di allarmi presenti nel pannello di controllo.
Viene visualizzata la finestra di dialogo **Risolvi allarmi ed errori**.
2. Nella scheda **Allarmi**, dal menu a discesa **Mostra** selezionare una delle opzioni.
In base a quanto selezionato, nelle colonne verranno visualizzate informazioni relative a tutti i computer infetti, quali il nome del computer infetto, data e ora del primo rilevamento della minaccia nel computer, tipo di allarme, stato dell'allarme ecc.

3. In base a quanto selezionato, la colonna **Stato** visualizza una delle seguenti voci:
- **Rimovibile**
In questo caso, disinfettare gli oggetti infetti tramite il pulsante **Disinfezione**, come descritto di seguito in questa sezione.
 - **Non rimovibile**
Per disinfettare oggetti che risultano "non rimovibili" in Sophos Control Center, andare ai computer infetti ed eseguire la disinfezione manuale. Se la minaccia non è stata rimossa, consultare la sezione [Disinfezione non riuscita](#) a pagina 56.
 - **Rimozione in corso (avviato<orario>)**
Indica che il processo di disinfezione è stato avviato.
 - **Rimozione scaduta (avviato<orario>)**
Indica che il processo di disinfezione è scaduto e che quindi l'allarme potrebbe non essere stato rimosso. Ciò può verificarsi quando il computer non è connesso alla rete. Assicurarsi che il computer sia connesso alla rete e provare ad eseguire la disinfezione nuovamente.
 - **Riavvio necessario**
Indica che l'allarme è stato parzialmente eliminato, ma per completarlo è necessario il riavvio del computer.
 - **Richiesta scansione completa**
Indica che l'allarme può essere eliminato, ma per completare questa operazione sarà necessaria una scansione completa.
 - **Disinfezione non riuscita**
Indica che l'allarme non è stato eliminato. Potrebbe essere necessaria la disinfezione manuale.
 - **Tipo di minaccia non eliminabile**
Indica che l'oggetto non può essere eliminato perché si tratta di un tipo di allarme non eliminabile.

4. Utilizzare le opzioni descritte di seguito per svolgere le relative azioni:

■ **Selezionare/deselezionare tutto**

Cliccare su questi pulsanti per selezionare oppure per deselezionare tutte le voci. Ciò consente di eseguire la stessa azione su un gruppo di voci. Per selezionare o deselezionare una particolare voce, cliccare sulla casella di spunta alla sua destra.

■ **Cancella**

Cliccare qui per rimuovere le voci selezionate dall'elenco, solo se si considera tale operazione sicura. Comunque gli oggetti non vengono cancellati dal disco.

■ **Rimozione**

Cliccare qui per eliminare minacce, virus, spyware o PUA dai computer selezionati.

Nota: È poi necessario sostituire i programmi disinfettati a partire dai dischi originali o da una copia di backup pulita.

Prima di tentare di rimuovere dai computer minacce formate da più componenti, Sophos consiglia di eseguire una scansione completa dei computer, al fine di determinare tutti i componenti che formano tali minacce. Per informazioni sulla scansione di computer ad orari determinati, consultare la sezione [Scansione dei computer a orari prestabiliti](#) a pagina 30.

Per rimuovere completamente da un computer alcune applicazioni composte da numerosi componenti, potrebbe essere necessario il riavvio del computer. In tal caso, sarà visualizzato un messaggio nel computer interessato, in cui si chiede se si desidera riavviare il computer immediatamente o più tardi. Le operazioni conclusive di rimozione saranno eseguite dopo il riavvio del computer.

Nota: quando si disinfetta un computer da una minaccia, l'azione risulterà non riuscita se dal computer non si riceve alcuna risposta entro un'ora (calcolata dal momento in cui Sophos Control Center ha inviato l'ordine di svolgere l'azione al computer).

6.3 Reperimento di informazioni sulle minacce

Se viene rilevata una minaccia, è possibile reperire informazioni relative ai suoi effetti, oltre che consigli sulle operazioni di disinfezione.

Reperire informazioni sulle minacce:

1. In Sophos Control Center, nell'elenco computer, evidenziare il computer in cui è stata rilevata la minaccia, cliccarvi col tasto destro del mouse e selezionare **Visualizza dettagli computer**.
2. Nella finestra **Dettagli computer**, scorrere fino a **Allarmi ed errori in sospenso** e cliccare sul nome della minaccia.

Sophos Control Center si collegherà all'analisi della minaccia sul sito web di Sophos.

In alternativa, è anche possibile andare al sito web di Sophos e cercare l'analisi della minaccia su cui si desidera reperire informazioni. Per far ciò, dal menu **?**, cliccare su **Informazioni sull'oggetto**.

6.4 Gestione degli allarmi relativi ad errori

Nelle scheda Errori vengono visualizzate informazioni relative a scansioni in sospeso ed errori del firewall verificatisi negli ultimi 30 giorni. È possibile visualizzare il nome del computer in cui è stato rilevato l'errore, la data e l'ora del rilevamento ed il tipo, codice e descrizione dell'errore.

Per gestire errori relativi ad antivirus e firewall:

1. Nel menu **Azioni**, cliccare su **Risolvi allarmi ed errori**.
2. Nella finestra di dialogo **Risolvi allarmi ed errori**, cliccare sulla scheda **Errori**.
3. Utilizzare le opzioni descritte di seguito per svolgere le relative azioni:

- **Selezionare/deselezionare tutto**

Cliccare su questi pulsanti per selezionare oppure per deselezionare tutte le voci. Ciò consente di eseguire la stessa azione su un gruppo di voci. Per selezionare o deselezionare una particolare voce, cliccare sulla casella di spunta alla sua destra.

- **Cancella**

Cliccare qui per marcare gli errori come oggetti trattati. Gli allarmi cancellati non vengono più visualizzati.

7 Nuova protezione dei computer

7.1 Nuova protezione dei computer

È possibile reinstallare i software antivirus e firewall (se compreso nella licenza) che erano inizialmente installati nei computer in rete.

Per proteggere nuovamente i computer:

- ❖ Nell'elenco computer, evidenziare i computer in cui si desidera reinstallare i software. Aprire il menu **Strumenti** e selezionare **Proteggi nuovamente i computer**. Viene avviata la **Procedura guidata per la nuova protezione dei computer**, che accompagna durante il processo di installazione del software.

Per informazioni su come proteggere i computer, consultare la Guida di avvio di Sophos Control Center.

8 Monitoraggio dei computer protetti

8.1 Identificazione dei computer conformi alla configurazione centralizzata

Sophos Control Center consente di creare centralmente un insieme di impostazioni (per es. relative agli aggiornamenti) e di applicarle ai computer; per riferirsi a tale insieme di applicazioni si utilizza il termine configurazione centrale.

Per verificare che tutti i computer siano conformi alla configurazione (impostata centralmente tramite Sophos Control Center) di antivirus, aggiornamenti, firewall, applicazione e controllo dispositivi,

visualizzare l'elenco dei computer. Nella colonna **Configurazione centralizzata**, la parola "Ok" indica che il computer è conforme alla configurazione centralizzata.

- Se un computer non è conforme alla configurazione centralizzata (per es. se la configurazione del computer è stata modificata dal computer stesso, ma tale computer non risulta configurato a livello locale in Sophos Control Center), verrà visualizzato un simbolo di allarme giallo e la parola "Modificato" nella colonna **Configurazione centralizzata**.
- Se nel computer non risulta installato alcun software di sicurezza, la colonna **Configurazione centralizzata** non visualizzerà nessuno stato relativo a tale computer (sarà vuota). Se il software è configurato a livello locale, verrà visualizzata la dicitura "Configurato a livello locale". Se il computer è in attesa della configurazione centralizzata da parte di Sophos Control Center, in questa colonna verrà visualizzata la dicitura "In sospeso".

Per applicare nuovamente la configurazione centralizzata a un computer, evidenziare il computer, cliccarvi col tasto destro del mouse e selezionare **Riapplica configurazione centralizzata**.

8.2 Identificazione di computer configurati a livello locale

È possibile identificare in due modi i computer in cui i software antivirus e firewall sono configurati a livello locale:

❖ **Visualizza solo i computer configurati a livello locale**

È possibile visualizzare solo i computer configurati localmente.

Nel menu a discesa **Visualizza**, selezionare **Computer configurati a livello locale**.

❖ **Verifica computer singoli**

Per verificare se un computer singolo è configurato a livello locale, cliccare col tasto destro del mouse sul nome del computer, se la voce **Utilizza configurazione centralizzata** non è selezionata, il computer è configurato a livello locale.

8.3 Verifica della protezione dei computer

In Sophos Control Center, viene visualizzato un elenco di computer ed il relativo stato.

- Nella colonna **Aggiornato**, la dicitura "Sì" indica che la protezione Sophos nel computer in questione è aggiornata. L'icona a forma di orologio e la parola "No" indicano che non lo è.

Per ordinare i computer secondo lo stato aggiornato o non aggiornato, cliccare sull'intestazione della colonna **Aggiornato**.

- Nella colonna **Antivirus**, la parola "Attiva" indica che il computer è protetto dalla scansione in accesso. Uno scudo non selezionabile e la parola "Inattiva" indicano che non lo è.

Nota: se gli utenti sono protetti dalla scansione in accesso, non è necessario eseguire la scansione in accesso nei file server di Windows 2000 o Windows 2003.

Se il software non è installato nel computer, in questa colonna sarà visualizzata la dicitura "Non installato".

- Nella colonna **Controllo applicazioni**, la parola "Attiva" indica quando nel computer è abilitato il controllo applicazioni. Uno scudo non selezionabile e la parola "Inattiva" indicano che non lo è.
- Nella colonna **Firewall**, la dicitura "Attivo" indica che il computer è protetto dal firewall. Uno scudo non selezionabile e la parola "Inattiva" indicano che non lo è. Se il software non è installato nel computer, la colonna relativa a tale computer non mostrerà alcuno stato (sarà vuota).

8.4 Recupero dei computer eliminati

È possibile recuperare un computer che è stato rimosso dall'elenco dei computer in Sophos Control Center.

Per recuperare un computer che è stato eliminato, è necessario cercare il computer eliminato come se fosse nuovo. Per informazioni su come cercare computer, consultare la sezione [Protezione dei nuovi computer](#) a pagina 10.

8.5 Visualizzazione dei computer in base allo stato

È possibile visualizzare un elenco di computer in base allo stato.

Per visualizzare un computer in base al suo stato:

- ❖ In Sophos Control Center, nel menu a discesa **Visualizza** selezionare uno stato. La seguente tabella mostra l'elenco di stati disponibili:

Opzione	Descrizione
Tutti i computer	Visualizza l'elenco dei computer attualmente connessi alla rete e gestiti da Sophos Control Center.

Opzione	Descrizione
Computer con allarmi ed errori	Visualizza l'elenco dei computer che riportano allarmi. Per scoprire da che cosa è dovuto l'allarme, evidenziare il computer nell'elenco computer, cliccarvi col tasto destro del mouse e selezionare Visualizza dettagli computer .
Computer non gestiti	Visualizza l'elenco dei computer non gestiti da Sophos Control Center.
Computer gestiti non aggiornati	Visualizza l'elenco dei computer gestiti da un software non aggiornato. Per aggiornare un computer singolo, cliccare su di esso nell'elenco computer e selezionare Aggiorna computer .
Computer gestiti	Visualizza l'elenco dei computer attualmente gestiti da Sophos Control Center.
Computer configurati a livello locale	Visualizza l'elenco dei computer configurati a livello locale. Perché il computer utilizzi nuovamente la configurazione centralizzata, cliccare col tasto destro del mouse sul nome del computer e selezionare Utilizza configurazione centralizzata .
Computer connessi	Visualizza l'elenco dei computer gestiti ed attualmente disponibili.
Computer non connessi	Visualizza l'elenco dei computer gestiti, ma attualmente non disponibili (per es. se il computer è spento).

In presenza di allarmi multipli sullo stesso computer, nell'elenco sarà visualizzata l'icona dell'allarme con la priorità più alta. Per informazioni sul livello di priorità delle icone, consultare la sezione [Priorità degli allarmi](#) a pagina 7.

8.6 Stampa del riepilogo delle minacce e dell'elenco computer

È possibile stampare il riepilogo delle minacce presente nei computer e l'elenco computer relativo a una determinata visualizzazione.

Per stampare il riepilogo delle minacce e l'elenco computer:

1. Nella finestra Sophos Control Center, nel menu **File**, cliccare su **Stampa**.

Viene visualizzata la finestra di dialogo **Stampa**.

2. Impostare le opzioni di stampa e cliccare su **OK**. Il documento risultante includerà le seguenti informazioni:

- Nome azienda
- Data e ora della stampa
- Informazioni visualizzate nel riquadro riepilogativo
- Dati visualizzati nell'elenco computer relativi alla visualizzazione selezionata

9 Visualizzazione eventi

9.1 Eventi

Quando si verifica un evento di controllo applicazioni, firewall o controllo dispositivi nel computer, per es. un'applicazione è stata bloccata dal firewall, tale evento viene inviato a Sophos Control Center 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 di applicazioni controllate generati da un determinato utente nelle ultime 24 ore.

Il numero di computer con eventi che hanno superato una determinata soglia entro le 24 ore viene visualizzato nel pannello di controllo. Per informazioni sull'impostazione del livello di soglia, consultare la sezione [Configurazione pannello di controllo](#) a pagina 9.

È inoltre possibile impostare allarmi da inviare a destinatari prescelti ogni qual volta si verifichi un evento. Per ulteriori informazioni, consultare la sezione [Impostazione degli allarmi antivirus e HIPS](#) a pagina 47.

9.2 Visualizzazione degli eventi del controllo applicazioni

Per visualizzare gli eventi del controllo applicazioni:

1. Dal menu **Visualizza**, cliccare su **Eventi controllo applicazioni**.
In alternativa, cliccare sul link **Eventi controllo applicazioni** nel pannello di controllo.
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. Cliccare su **Cerca** per visualizzare un elenco di eventi.

È possibile esportare in un file l'elenco di eventi del controllo applicazioni. Per informazioni, consultare la sezione [Esportazione dell'elenco eventi in un file](#) a pagina 24.

È inoltre possibile copiare gli eventi negli Appunti. Per informazioni, consultare la sezione [Copia degli eventi negli Appunti](#) a pagina 24.

9.3 Visualizzazione degli eventi del controllo dispositivi

Per visualizzare gli eventi del controllo dispositivi:

1. Nel menu **Visualizza**, cliccare su **Eventi controllo dispositivi**.
In alternativa, cliccare sul link **Controllo dispositivi** nel pannello di controllo.
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.
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.
5. Cliccare su **Cerca** per visualizzare un elenco di eventi.

Nella finestra di dialogo **Device Control - Visualizzatore eventi**, è possibile esentare un particolare dispositivo dai criteri relativi al controllo dispositivi. Per informazioni, consultare la sezione [Esenzione di un dispositivo](#) a pagina 46.

È possibile esportare in un file l'elenco di eventi del controllo dispositivi. Per informazioni, consultare la sezione [Esportazione dell'elenco eventi in un file](#) a pagina 24.

È inoltre possibile copiare gli eventi negli Appunti. Per informazioni, consultare la sezione [Copia degli eventi negli Appunti](#) a pagina 24.

9.4 Visualizzazione degli eventi del firewall

Per visualizzare gli eventi del firewall:

1. Nel menu **Visualizza**, cliccare su **Eventi Firewall**.
In alternativa, cliccare sul link **Eventi firewall** nel pannello di controllo.
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. Cliccare su **Cerca** per visualizzare un elenco di eventi.

Nella finestra di dialogo **Firewall - Visualizzatore eventi**, è possibile personalizzare le regole del firewall secondo quanto descritto in [Impostazione del firewall](#) a pagina 37.

È possibile esportare in un file nell'elenco di eventi del controllo dispositivi. Per informazioni, consultare la sezione [Esportazione dell'elenco eventi in un file](#) a pagina 24.

È inoltre possibile copiare gli eventi negli Appunti. Per informazioni, consultare la sezione [Copia degli eventi negli Appunti](#) a pagina 24.

9.5 Esportazione dell'elenco eventi in un file

È possibile esportare l'elenco degli eventi relativi a controllo applicazioni, firewall, controllo dati o dispositivi in un file in formato valore separato da virgola (csv).

1. Nel menu **Visualizza**, 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 **Cerca criteri**, impostare i filtri adeguati e cliccare su **Cerca** per visualizzare tali eventi.

Per ulteriori informazioni, consultare la sezione [Visualizzazione degli eventi del controllo applicazioni](#) a pagina 22, [Visualizzazione degli eventi del controllo dispositivi](#) a pagina 22, o [Visualizzazione degli eventi del firewall](#) a pagina 23.

3. Cliccare su **Esporta**.
4. Nella finestra di dialogo **Salva con nome**, inserire il nome file e cercare una destinazione per tale file.

9.6 Copia degli eventi negli Appunti

È possibile copiare negli Appunti gli eventi relativi a controllo applicazioni, firewall, controllo dati o dispositivi e successivamente incollarli in un altro documento nel formato valore separato da tabulazione. È possibile copiare da uno a tutti gli eventi contenuti nell'elenco.

1. Nel menu **Visualizza**, 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 **Cerca criteri**, impostare i filtri adeguati e cliccare su **Cerca** per visualizzare tali eventi.

Per ulteriori informazioni, consultare la sezione [Visualizzazione degli eventi del controllo applicazioni](#) a pagina 22, [Visualizzazione degli eventi del controllo dispositivi](#) a pagina 22, o [Visualizzazione degli eventi del firewall](#) a pagina 23.

3. Nella finestra di dialogo **Visualizzatore eventi**, cliccare su **Copia** per copiare l'elenco di eventi negli Appunti.

Se si desidera copiare solo un evento, selezionare l'evento e cliccare su **Copia**.

10 Configurazione della scansione

10.1 Ricerca di virus, trojan, spyware e worm

Per impostazione predefinita, Sophos Anti-Virus rileva virus, trojan, spyware e worm automaticamente, non appena un utente cerca di accedere ai file che li contengono.

Per eseguire la scansione del proprio computer:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura scansione**.
2. Nella finestra di dialogo **Configura scansione**, nel riquadro **Configura Sophos antivirus e HIPS**, assicurarsi che la casella di spunta **Abilita scansione in accesso** sia selezionata.

10.2 Ricerca di applicazioni potenzialmente indesiderate

Per impostazione predefinita, Sophos Anti-Virus rileva virus, trojan, spyware e worm. Inoltre, è possibile configurarlo affinché rilevi applicazioni potenzialmente indesiderate.

Nota: questa opzione è valida soltanto per Sophos Anti-Virus su Windows 2000 o successivo.

Per rilevare le applicazioni potenzialmente indesiderate, Sophos consiglia di iniziare utilizzando una scansione pianificata. In tal modo è possibile trattare in sicurezza le applicazioni che sono già in esecuzione nella rete. Quindi, sarà possibile abilitare il rilevamento in accesso per proteggere i computer in futuro.

Per ricercare applicazioni potenzialmente indesiderate:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura scansione**.
2. Nella finestra di dialogo **Configura scansione**, nel pannello **Scansione pianificata**, cliccare su **Aggiungi** per creare una nuova scansione, oppure selezionare una scansione nella lista e cliccare su **Modifica** per modificarla.
3. Nella finestra di dialogo **Impostazioni scansione pianificata**, cliccare su **Configura** (in fondo).
4. Nella finestra di dialogo **Impostazioni di scansione e rimozione**, cliccare sulla scheda **Scansione**. Nel pannello **Altre opzioni di scansione**, accertarsi che l'opzione **Ricerca di applicazioni potenzialmente indesiderate** sia selezionata. Cliccare su **OK**.
5. A scansione terminata, Sophos Anti-Virus potrebbe segnalare la presenza di alcune "applicazioni potenzialmente indesiderate".

Se si desidera che i computer eseguano le applicazioni, è necessario autorizzarle. Per informazioni su come autorizzare le applicazioni, consultare la sezione [Autorizzazione all'utilizzo di applicazioni](#) a pagina 30.

6. Se si desidera abilitare il rilevamento in accesso, nella finestra di dialogo **Configura scansione**, cliccare su **Scansione in accesso**.

Nella finestra di dialogo **Impostazioni della scansione in accesso** che si trova sotto **Altre opzioni di scansione**, selezionare **Cerca adware e PUA**.

Alcune applicazioni "monitorano" i file e tentano frequentemente di accedere ad essi. Se la scansione in accesso è abilitata, essa rileva ogni accesso e invia allarmi multipli. Consultare la sezione [Allarmi frequenti relativi alle applicazioni potenzialmente indesiderate](#) a pagina 56.

10.3 Impostazione delle opzioni della scansione in accesso

Per impostare le opzioni della scansione in accesso:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura scansione**.
2. Nella finestra di dialogo **Configura scansione**, cliccare su **In accesso**.
3. Andare alla finestra di dialogo **Impostazioni della scansione in accesso** e selezionare le opzioni secondo necessità.

■ Scansione dei file di archivio

È possibile eseguire la scansione dei file di archivio. Prima di abilitare questa opzione però prendere in considerazione quanto riportato di seguito:

- La scansione in accesso verifica automaticamente i file di archivio non appena vi si accede. La scansione degli archivi risulta quindi opzionale.
- La scansione dei file di archivio influisce sulle prestazioni del computer ed il suo utilizzo, in concomitanza con la scansione in accesso, non è consigliato.

■ Selezionare Includi virus di Macintosh

Selezionare la scansione dei file Macintosh memorizzati nel computer Windows durante la scansione in accesso.

■ Ricerca di adware e PUA

Per impostazione predefinita, Sophos Endpoint Security and Control rileva virus, trojan e worm. Inoltre, è possibile configurarlo affinché rilevi applicazioni potenzialmente indesiderate.

■ Selezionare Ricerca di file sospetti (HIPS)

Selezionare la ricerca di file sospetti durante la scansione in accesso.

4. Sotto **Comportamento scansione in accesso**, selezionare i file di cui si desidera eseguire la scansione quando l'utente svolge determinate operazioni.

- **In lettura**, il software Sophos Anti-Virus esegue automaticamente la scansione dei file "in accesso". Per impostazione predefinita, ciò significa che la scansione viene eseguita all'apertura del file da parte dell'utente ("in lettura").
- **In scrittura**, se si desidera controllare i file al momento della chiusura.
- **Se rinominati**, se si desidera controllare i file quando vengono rinominati.

Queste opzioni garantiscono maggiore protezione contro i virus che scrivono nell'hard drive del computer e/o rinominano i file. La maggiore attività può però influire sulle prestazioni del computer.

5. Sotto **Supporti rimovibili**, selezionare **Consenti accesso alle unità con boot sector infetti** per poter consentire l'accesso (per esempio, per poter copiare file da un floppy disk infetto da un virus del settore di avvio).

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

10.4 Modifica dei tipi di file da esaminare

I tipi di file da esaminare per impostazione predefinita variano a seconda del sistema operativo e degli aggiornamenti via via apportati al prodotto.

■ Mac

Tramite Sophos Update Manager è possibile apportare cambiamenti sui computer con sistema operativo Mac OS X; si tratta di un'utilità che fa parte di Sophos Anti-Virus per Mac OS X. Per aprire Sophos Update Manager nei computer con sistema operativo Mac OS X, dalla finestra **Finder**, cercare la cartella di Sophos Anti-Virus:ESOSX. Cliccare due volte su **Sophos Update Manager**. Per ulteriori dettagli, consultare la guida in linea di Sophos Update Manager.

■ Windows

Per impostazione predefinita, Sophos Anti-Virus esamina i tipi di file che sono vulnerabili ai virus. È possibile esaminare tipi aggiuntivi di file, oppure scegliere di escludere alcuni tipi di file dalla scansione. Per visualizzare l'elenco dei tipi di file, sul computer con il sistema operativo che interessa, aprire la finestra Sophos Anti-Virus e cercare la pagina di configurazione "Estensioni".

Nota: nei computer con sistema operativo Windows 95, 98 e NT, le modifiche apportate alle impostazioni della scansione pianificata vengono applicate anche alla scansione in accesso.

Per modificare i tipi di file da esaminare, procedere come segue.

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura scansione**. Viene visualizzata la finestra di dialogo **Configura scansione**.
 - Per configurare la scansione in accesso, sotto Configura Sophos Anti-Virus e HIPS, cliccare su **Scansione in accesso**.
 - Per configurare scansioni pianificate, sotto Scansione pianificata, cliccare su **Estensioni ed esclusioni**.
2. Nella scheda **Estensioni**:
 - Per eseguire la scansione di tipi di file aggiuntivi, cliccare su **Aggiungi** e digitare, nel campo Estensione, l'estensione del file quale PDF.
 - **Scansione dei file senza estensione** Per impostazione predefinita, nella scansione sono inclusi i file senza estensione.
 - Per escludere alcuni dei tipi di file che vengono esaminati per impostazione predefinita, cliccare su **Escludi**. Ciò consente di aprire la finestra di dialogo **Escludi estensioni**. Inserire l'estensione del file.

10.5 Abilitazione della scansione web

La scansione web esegue la scansione dei dati e dei file scaricati da Internet Explorer. Per impostazione predefinita, la scansione web è disabilitata.

Per abilitare la scansione web:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura scansione**.
2. Nella finestra di dialogo **Configura scansione**, di fianco a **La scansione web** è, selezionare **Attiva**.

È anche possibile selezionare **Come in accesso**, se si desidera abilitare e disabilitare simultaneamente la scansione in accesso e web.

10.6 Esclusione di oggetti dalla scansione in accesso

Questa sezione spiega come escludere oggetti (quali unità, cartelle o file) dalla scansione in accesso.

È possibile escludere dalla scansione alcuni tipi di file aggiungendo l'estensione del file all'**Elenco delle estensioni escluse**. Per informazioni su come svolgere questa operazione, consultare la sezione [Modifica dei tipi di file da esaminare](#) a pagina 27.

- Le opzioni di "esclusione oggetti" sono applicabili solo a computer Windows 2000 o successivo e Mac OS X.
- Per escludere oggetti da computer Windows 95, 98 e NT, consultare la sezione [Esclusione di oggetti dalla scansione pianificata](#) a pagina 32.

Queste esclusioni sono applicabili anche alla scansione in accesso.

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura scansione**.
2. Nella finestra di dialogo **Configura scansione**, cliccare su **In accesso**.
3. Nella finestra di dialogo **Impostazioni della scansione in accesso**, cliccare sulla scheda **Esclusioni Windows** o **Esclusioni Mac**.
 - Cliccare su **Aggiungi** per aggiungere oggetti all'elenco inserendo il percorso completo nella finestra di dialogo **Escludi oggetto**.
 - Selezionare **Escludi file remoti**, se si desidera evitare che Sophos Anti-Virus esegua la scansione dei file installati in unità di rete.

10.7 Impostazione della disinfezione automatica

10.7.1 Disinfezione automatica

È possibile disinfettare automaticamente i computer non appena viene rilevato un virus. Per far ciò, è necessario cambiare le impostazioni della scansione secondo quanto descritto.

Nota: La scansione in accesso non può eseguire la disinfezione delle applicazioni potenzialmente indesiderate; è però possibile abilitare la disinfezione automatica delle applicazioni non autorizzate durante la scansione pianificata, secondo quanto descritto più avanti in questa sezione.

10.7.2 Disinfezione automatica dei virus

È possibile eseguire la disinfezione automatica dei virus durante le scansioni in accesso e pianificate.

Per eseguire la disinfezione automatica dei virus:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura scansione**.
2. Per cambiare le impostazioni della scansione in accesso, nella finestra di dialogo **Configura scansione**, cliccare sul pulsante **Scansione in accesso**. Nella finestra di dialogo **Impostazioni di scansione in accesso**, cliccare sulla scheda **Disinfezione**.
3. Per cambiare le impostazioni della scansione pianificata, nella finestra di dialogo **Configura scansione**, sotto **Scansione pianificata**, selezionare una scansione e cliccare su **Modifica**.

Nella finestra di dialogo **Impostazioni scansione pianificata**, cliccare su **Configura**. Nella finestra di dialogo **Impostazioni di scansione e rimozione**, cliccare sulla scheda **Disinfezione**.

4. Selezionare **Disinfetta automaticamente gli oggetti contenenti virus/spyware**.
5. Inoltre, è possibile indicare cosa fare se la disinfezione non riesce: Le opzioni sono:
 - Nega solo l'accesso
 - Cancella
 - Nega solo l'accesso e vai al percorso predefinito
 - Nega solo l'accesso e vai a UNC

Nota: se si seleziona **Sposta in** e si indica un percorso. I computer Mac OS X continueranno a spostare gli oggetti infetti nel percorso predefinito.

10.7.3 Disinfezione automatica delle applicazioni potenzialmente indesiderate

Nota: questa opzione è valida soltanto per Sophos Endpoint Security and Control su Windows 2000 o successivo.

È possibile eseguire la disinfezione automatica delle applicazioni potenzialmente indesiderate solo durante la scansione pianificata.

Per eseguire la disinfezione automatica delle applicazioni potenzialmente indesiderate:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura scansione**.
2. Nella finestra di dialogo **Configura scansione**, sotto **Scansione pianificata**, selezionare una scansione e cliccare su **Modifica**.
3. Nella finestra di dialogo **Impostazioni scansione pianificata**, cliccare su **Configura**.
4. Nella finestra di dialogo **Impostazioni di scansione e rimozione**, cliccare sulla scheda **Disinfezione**.

5. Sotto Adware e PUA, selezionare **Rimuovi automaticamente adware e PUA**.
Ciò consentirà a Sophos Anti-Virus di rimuovere dal computer le applicazioni potenzialmente indesiderate.
6. È inoltre possibile specificare l'operazione da eseguire sui file sospetti. Le opzioni sono:
 - Nega solo l'accesso
 - Cancella
 - Nega solo l'accesso e vai al percorso predefinito
 - Nega solo l'accesso e vai a UNC

Nota: Se si seleziona **Sposta in** e si specifica un percorso, i computer con sistema operativo Mac OS X sposteranno comunque gli oggetti infetti nella posizione predefinita.

10.8 Autorizzazione all'utilizzo di applicazioni

Se Sophos Anti-Virus è stato abilitato per il rilevamento di applicazioni potenzialmente indesiderate, è possibile che impedisca l'utilizzo di un'applicazione che si desidera eseguire.

Per utilizzare applicazioni:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura scansione**.
2. Nella finestra di dialogo **Configura scansione**, cliccare su **Autorizzazione**.
3. Nella finestra di dialogo **Gestore autorizzazioni**, nell'elenco **Adware e PUA noti**, selezionare l'applicazione che si desidera autorizzare. Cliccare su **Aggiungi** per aggiungerla alla lista delle applicazioni autorizzate. Ripetere la procedura per ogni applicazione che si desidera autorizzare. Cliccare su **OK**.
4. Se non si riesce a vedere l'applicazione che si desidera autorizzare, cliccare su **Nuova voce**. Nella finestra di dialogo **Aggiungi nuovi adware e PUA**, inserire il nome dell'applicazione che si desidera autorizzare e cliccare su **OK**.

10.9 Scansione dei computer a orari prestabiliti

È possibile configurare computer in modo che si esegua la scansione a orari prestabiliti.

Per eseguire la scansione dei computer a orari prestabiliti:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura scansione**.
2. Nella finestra di dialogo **Configura scansione**, nella scheda **Scansione pianificata**, cliccare su **Aggiungi**.
3. Nella finestra di dialogo **Impostazioni scansione pianificata**, inserire un nome per la scansione.
4. Selezionare gli oggetti da esaminare:
 - Hard disk locali
 - Unità floppy e unità rimovibili
 - Unità CD-ROM

Per impostazione predefinita, viene eseguita la scansione di tutti gli hard disk locali.

5. Selezionare i giorni e gli orari nei quali si desidera che venga eseguita la scansione.

Se si desidera modificare la scansione predefinita o eliminare alcune opzioni di scansione, cliccare su **Configura** in fondo alla finestra di dialogo **Impostazioni scansione pianificata**. Per ulteriori informazioni, consultare la sezione [Impostazione delle opzioni della scansione pianificata](#) a pagina 31 o [Impostazione della disinfezione automatica](#).

Per sapere come modificare i tipi di file per esaminare o escludere determinati oggetti dalla scansione pianificata, consultare la sezione [Modifica dei tipi di file da esaminare](#) a pagina 27 o [Esclusione di oggetti dalla scansione pianificata](#) a pagina 32.

10.10 Impostazione delle opzioni della scansione pianificata

È possibile scegliere di configurare le opzioni relative alla scansione pianificata. Per impostare le opzioni della scansione pianificata:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura scansione**.
2. Nella finestra di dialogo **Configura scansione**, selezionare una scansione pianificata e cliccare su **Modifica**.
3. Nella finestra di dialogo **Impostazioni scansione pianificata**, cliccare su **Configura**.

4. Nella finestra di dialogo **Impostazioni di scansione e rimozione**, scheda **Scansione**, selezionare le opzioni che si desidera.

- **Scansione dei file di archivio**

È possibile eseguire la scansione dei file di archivio. Prima di abilitare questa opzione però prendere in considerazione quanto riportato di seguito:

- La scansione in accesso verifica automaticamente i file di archivio non appena vi si accede. La scansione degli archivi risulta quindi opzionale.
- La scansione dei file di archivio influisce sulle prestazioni del computer ed il suo utilizzo, in concomitanza con la scansione in accesso, non è consigliato.

- **Selezionare Includi virus di Macintosh**

Selezionare la scansione dei file Macintosh memorizzati nel computer Windows durante una scansione pianificata.

- **Ricerca di adware e PUA**

Per impostazione predefinita, Sophos Endpoint Security and Control rileva virus, trojan e worm. Inoltre, è possibile configurarlo affinché rilevi applicazioni potenzialmente indesiderate. Per impostazione predefinita, l'opzione è selezionata per una scansione pianificata.

- **Selezionare Ricerca di file sospetti (HIPS)**

Per impostazione predefinita, la ricerca di file sospetti durante una scansione pianificata è abilitata.

- **Cerca virus di Macintosh**

La ricerca di rootkit viene sempre condotta quando si esegue la scansione completa del sistema di un computer. L'opzione può essere abilitata anche per una scansione pianificata.

Per informazioni sulle opzioni di rimozione, consultare [Disinfezione automatica](#) a pagina 28 e gli altri argomenti della sezione Impostazione della disinfezione automatica.

10.11 Esclusione di oggetti dalla scansione pianificata

Questa sezione spiega come escludere oggetti (quali unità, cartelle o file) dalla scansione pianificata.

È inoltre possibile escludere dalla scansione alcuni tipi di file aggiungendo l'estensione del file all'**Elenco delle estensioni escluse**. Per informazioni su come svolgere questa operazione, consultare la sezione [Modifica dei tipi di file da esaminare](#) a pagina 27.

Nota: nei computer con sistema operativo Windows 95, 98 e NT, le modifiche apportate alle impostazioni della scansione pianificata vengono applicate anche alla scansione in accesso.

Per escludere oggetti dalla scansione pianificata:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura scansione**. Viene visualizzata la finestra di dialogo **Configura scansione**.

2. Nel riquadro **Scansione pianificata**, cliccare su **Estensioni ed Esclusioni**.
3. Nella finestra di dialogo **Estensioni ed esclusioni per la scansione pianificata**, cliccare sulla scheda **Esclusioni Windows** o **Esclusioni Mac** a seconda dei file del sistema operativo da escludere dalla scansione. Per aggiungere oggetti all'elenco, cliccare su **Aggiungi** e inserire il percorso completo nella finestra di dialogo **Escludi oggetto**.

10.12 Configurazione della scansione su computer singoli

È possibile configurare determinati computer in base a opzioni diverse da quelle impostate centralmente nel Sophos Control Center.

Per configurare la scansione su computer singoli:

1. Nell'elenco dei computer, evidenziare il o i computer. Cliccarvi col tasto destro del mouse e deselezionare **Utilizza configurazione centralizzata**.
2. Andare al/ai computer singoli e configurare le opzioni antivirus.

Per configurare la scansione su computer singolo, cliccare col tasto destro del mouse sull'icona di Sophos Endpoint Security and Control posta sulla barra delle applicazioni .

3. Cliccare su **Apri Sophos Endpoint Security and Control**. Nella finestra **Sophos Endpoint Security and Control**, cliccare su **Configura Sophos antivirus e HIPS**. Sotto **Configura**, cliccare su **Scansione in accesso** e modificare le impostazioni.

Per ulteriori informazioni sulla configurazione della scansione in computer singoli, consultare la guida in linea di Sophos Endpoint Security and Control.

11 Configurazione degli aggiornamenti

11.1 Modifica degli aggiornamenti

È possibile cambiare il software che viene aggiornato. È necessario svolgere questa operazione se:

- Si aggiungono alla rete computer con sistema operativo differente (quale Mac OS X) e per tale sistema è richiesto Sophos Anti-Virus.
- Vengono rimossi dalla rete tutti i computer aventi un determinato sistema operativo.

Per cambiare il software scaricato:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura aggiornamento**.
2. Nella finestra di dialogo **Configura aggiornamento**, cliccare sulla scheda **Software**. Quindi scegliere il o i sistemi operativi per cui è richiesto Sophos Anti-Virus e cliccare su **OK**.
Se si scelgono sistemi operativi mai protetti in precedenza (Windows 95, 98, NT o Mac OS X), andare ai passaggi 3 e 4.
3. Ritornare alla finestra principale di Sophos Control Center. Nel menu **Azioni**, cliccare su **Aggiorna ora** per scaricare il nuovo software.
4. Andare a tutti i computer di nuova tipologia e installare Sophos Anti-Virus. Per informazioni su come eseguire l'installazione manuale, consultare la Guida di avvio di Sophos Control Center.

11.2 Aggiornamento tramite server proxy

Se si utilizza un server proxy per accedere a Internet, è necessario abilitare Sophos Control Center a scaricare gli aggiornamenti tramite proxy.

Per aggiornare tramite server proxy:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura aggiornamento**.
2. Nella finestra di dialogo **Configura aggiornamento**, cliccare sulla scheda **Proxy**. Digitare l'indirizzo del server proxy e il numero di porta. Digitare il nome utente e la password di un account che abbia accesso a proxy (l'amministratore di rete può fornire questi dati).

11.3 Cambio dell'ID utente per gli aggiornamenti

È possibile cambiare l'ID utente utilizzata per scaricare gli aggiornamenti.

Per cambiare l'ID utente per gli aggiornamenti:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura aggiornamento**.
2. Nella finestra di dialogo **Configura aggiornamento**, cliccare sulla scheda **ID utente**. Digitare il nome utente e la password forniti da Sophos.

11.4 Disattivazione degli aggiornamenti automatici

Se si desidera disattivare gli aggiornamenti automatici (per es. una connessione dial-up), fare quanto descritto di seguito:

Nota: se si disattivano gli aggiornamenti automatici, assicurarsi di verificare la disponibilità di aggiornamenti regolarmente. Per informazioni relative alla verifica della disponibilità di aggiornamenti manuale, consultare la sezione [Aggiornamento manuale della rete](#) a pagina 13.

Per disattivare gli aggiornamenti automatici:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura aggiornamento**.
2. Nella finestra di dialogo **Configura aggiornamento**, cliccare sulla scheda **Operazione pianificata**. Deselezionare la casella di spunta **Consenti a computer in rete utilizzo automatico aggiornamenti Sophos**.

11.5 Cambiamento della frequenza degli aggiornamenti dei computer

Per impostazione predefinita, i computer in rete verificano la disponibilità di aggiornamenti al software di sicurezza ogni 10 minuti.

Per cambiare la frequenza degli aggiornamenti:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura aggiornamento**.
2. Nella finestra di dialogo **Configura aggiornamento**, cliccare sulla scheda **Operazione pianificata**. Assicurarsi che la casella di spunta **Consenti a computer in rete utilizzo automatico aggiornamenti Sophos** sia selezionata. Nel campo sotto la casella di spunta inserire un intervallo di tempo in minuti.

11.6 Aggiornamento dei computer non sempre connessi alla rete

Per impostazione predefinita, i computer in rete si autoaggiornano dalla cartella contenente gli aggiornamenti e collocata nel computer in cui viene eseguito Sophos Control Center. Se un computer non può più accedere a questa cartella, per esempio, quando non è connesso alla rete aziendale, ma solo a Internet, tale computer si aggiornerà direttamente da Sophos.

Per aggiornare computer non sempre connessi alla rete:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura aggiornamento**.

2. Nella finestra di dialogo **Configura aggiornamento**, cliccare sulla scheda **Fonte alternativa**; verranno visualizzate le seguenti opzioni:

■ **Da Sophos**

Selezionare questa opzione se in possesso di computer non sempre connessi alla rete aziendale, per es. laptop. Questi computer utilizzeranno le stesse credenziali utilizzate dalla copia di Sophos Control Center.

■ **Nessuno**

Si tratta di un'opzione predefinita. Non indica alcuna fonte alternativa.

■ **Dall'azienda dell'utente**

Selezionare questa opzione se si desidera che i computer della rete si aggiornino da un sito web aziendale o da una directory, nel caso in cui il percorso di aggiornamento primario non sia più disponibile. Inserire l'indirizzo di una cartella della rete (percorso UNC) o un sito web (indirizzo HTTP).

Se necessario, inserire il nome utente e la password di un account che i computer possono utilizzare per accedere alla cartella e al sito web. Questo account deve avere diritti di accesso in lettura alla directory inserita nel campo Indirizzo in alto. Se il nome utente dev'essere completato dal dominio, utilizzare la forma dominio\nomeutente.

Nota: se si specifica una cartella nella rete aziendale o un sito web, è necessario assicurarsi che in tale cartella siano disponibili copie regolarmente aggiornate del software di sicurezza. È possibile far ciò installando Sophos Control Center. È anche possibile pubblicare copie degli aggiornamenti della cartella.

12 Configurazione firewall

12.1 Impostazione del firewall

È possibile configurare il firewall in modo tale che blocchi o consenta il traffico in base ai propri requisiti. Per impostazione predefinita, il firewall blocca tutto il traffico non essenziale.

Per un elenco dettagliato delle impostazioni predefinite del firewall, andare a:

<http://www.sophos.com/support/knowledgebase/article/16608.html>

Per configurare il firewall:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura firewall**.
2. Nella procedura guidata di configurazione del firewall, cliccare su **Avanti**.
3. Nella pagina **Configura firewall**, scegliere una delle seguenti opzioni:
 - Selezionare **Consenti tutto il traffico** se si desidera disattivare il firewall e consentire il traffico.
 - 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. È possibile impostare un percorso doppio per i laptop.

4. Se nella pagina precedente si seleziona **Percorso doppio**, nella pagina **Identificazione di rete** configurare nella rete l'identificazione DNS or Gateway.

Nota: la pagina **Identificazione di rete** viene visualizzata solo se si seleziona **Percorso doppio**.

Sophos Control Center applicherà quindi diverse impostazioni del firewall ai computer a seconda che siano in rete o meno.

5. Nella pagina **Modalità operativa**, selezionare la modalità in cui il firewall deve gestire il traffico in entrata e in uscita.
 - **Modalità di apprendimento**

Consente ai computer di accedere sia alla rete che a Internet e di riportare le informazioni alla console.
 - **Blocco del il traffico in ingresso e consenso del traffico in uscita**

Consente ai computer di accedere sia alla rete che a Internet, ma blocca tutto il traffico in entrata.
 - **Blocco del traffico in entrata e in uscita**

Se si seleziona questa opzione, il firewall bloccherà tutto il traffico in uscita, eccetto le applicazioni specificate cliccando sul pulsante **Attendibile** alla destra di questa opzione. Ad un'applicazione "attendibile" è consentita tutta l'attività di rete.

6. Cliccare su **Avanzate** per aprire la configurazione avanzata del firewall.

Nota: è un'opzione avanzata, che si consiglia di utilizzare soltanto se si è consapevoli degli effetti delle modifiche che si apportano.

Per informazioni sulla configurazione avanzata del firewall, consultare la guida in linea di Sophos Endpoint Security and Control.

7. Nella pagina **Condivisione file e stampanti**, selezionare **Consenti condivisione file e stampanti** se si desidera consentire ad altri computer nella rete locale di accedere a stampanti e cartelle condivise nel computer.
8. Se si è selezionato **Percorso doppio**, verrà richiesto di configurare il traffico in entrata e in uscita, oltre che la condivisione file e stampanti (come indicato nei passaggi 5 e 7) relativi al percorso secondario (non in rete).

Una volta impostato il firewall, è possibile visualizzare gli eventi del firewall (per es. le applicazioni bloccate dal firewall) in **Firewall - Visualizzatore eventi**. Per informazioni, consultare la sezione [Visualizzazione degli eventi del firewall](#) a pagina 23.

È possibile eseguire nuovamente la procedura guidata, se in seguito si decide di modificare un'impostazione.

Il numero di computer con eventi che hanno superato una determinata soglia entro le 24 ore viene visualizzato anche nel pannello di controllo.

12.2 Disattivazione del firewall

12.2.1 Disattivazione del firewall dal Sophos Control Center

È possibile scegliere di disattivare il firewall in tutti i computer gestiti da Sophos Control Center.

Per un utilizzo quotidiano, Sophos consiglia di mantenere il firewall attivo.

Per disattivare il firewall dal Sophos Control Center

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura firewall**.
Viene avviata la **Procedura guidata di configurazione del firewall**.
2. Nella **Procedura guidata di configurazione del firewall**, andare alla pagina **Configura firewall** e selezionare **Consenti tutto il traffico**.

12.2.2 Disattivazione del firewall in un computer singolo

È possibile disattivare il firewall solo in determinati computer.

Per disattivare il firewall in un computer singolo:

1. Nell'elenco dei computer, evidenziare il o i computer. Cliccarvi col tasto destro del mouse e deselezionare **Utilizza configurazione centralizzata**.

Nota: se i computer sono impostati in modo da non utilizzare la configurazione centrale insieme al firewall, è anche possibile configurare Sophos Anti-Virus localmente.

2. Andare al o ai computer singoli e disattivare il firewall localizzando l'icona a forma di scudo di Sophos Endpoint Security and Control.
 - a) Cliccare col tasto destro del mouse su tale icona per visualizzare il menu e selezionare **Apri Sophos Endpoint Security and Control**.
 - b) Nella sezione **Firewall**, cliccare su **Configura**.
Viene visualizzata la finestra di configurazione del firewall.
 - c) Cliccare sulla scheda **Generale** e selezionare **Consenti tutto il traffico**. Cliccare su **OK**.

12.3 Ammissione di applicazioni bloccate

Se il firewall blocca un'applicazione nei computer in rete, nel log del firewall viene registrato un evento.

Per trovare dettagli relativi alle applicazioni bloccate e ammetterle, oppure creare appositamente nuove regole:

1. Nel menu **Visualizza**, andare a **Eventi** e poi cliccare su **Eventi firewall**.
2. Nella finestra di dialogo **Firewall - Visualizzatore eventi**, selezionare la voce relativa all'applicazione che si desidera permettere per cui si desidera creare una regola. Cliccare su **Crea regola**.
3. Nella finestra di dialogo che viene visualizzata, scegliere se permettere l'applicazione o se creare una regola per esse 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**.

12.4 Configurazione del firewall in computer singoli

Se si desidera che determinati computer utilizzino opzioni differenti da quelle impostate centralmente in Sophos Control Center, fare quanto descritto di seguito:

1. Nell'elenco dei computer, evidenziare il o i computer. Cliccarvi col tasto destro del mouse e deselezionare **Utilizza configurazione centralizzata**.

2. Andare al o ai computer singoli e li configurare le opzioni del firewall secondo quanto descritto di seguito:
 - a) Nel computer, trovare l'icona a forma di scudo di Sophos Endpoint Security and Control.
 - b) Cliccare col tasto destro del mouse su tale icona per visualizzare il menu e selezionare **Apri Sophos Endpoint Security and Control**.
 - c) Nella sezione **Firewall**, cliccare su **Configura firewall**.
Viene visualizzata la finestra di configurazione del firewall.

13 Configurazione del controllo applicazioni

13.1 Controllo applicazioni

Sophos Control Center 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.

Nota: questa opzione è valida soltanto per Sophos Endpoint Security and Control per Windows 2000 e successivo.

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, consultare l'articolo della knowledge base 35330 (<http://www.sophos.com/support/knowledgebase/article/35330.html>)

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 Sophos Control Center. Per informazioni, consultare la sezione [Visualizzazione degli eventi del controllo applicazioni](#) a pagina 22.

Per impostazione predefinita, il numero di computer con eventi che hanno superato una determinata soglia entro le 24 ore 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 informazioni, consultare la sezione [Impostazione degli allarmi del controllo applicazioni](#) a pagina 49.

13.2 Impostazione del controllo applicazioni

È possibile configurare Sophos Control Center in modo che ricerchi in accesso le applicazioni che si desidera controllare sulla rete.

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura controllo applicazioni**. Viene visualizzata la finestra di dialogo **Configura controllo applicazioni**.
2. 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, ma non si desidera bloccarle in accesso, selezionare la casella **Rileva ma consenti l'esecuzione**.
 - Per abilitare la scansione su richiesta, spuntare la casella **Abilita scansione su richiesta e pianificata**.

Nota: le impostazioni antivirus e HIPS dell'utente determinano quali file vengono esaminati (vale a dire le estensioni e le esclusioni).

3. Cliccare sulla scheda **Autorizzazione** e selezionare l'applicazione che si desidera controllare.

Per informazioni su come selezionare applicazioni, consultare la sezione [Selezione delle applicazioni da controllare](#) a pagina 42.

Se si desidera rimuovere le applicazioni controllate trovate sui computer in rete, seguire le istruzioni della sezione [Disinstallazione applicazioni controllate](#) a pagina 42

Nel caso che in un computer di un gruppo venga rilevata un'applicazione controllata, è possibile inviare allarmi a determinati utenti. Per informazioni, consultare la sezione [Impostazione degli allarmi del controllo applicazioni](#) a pagina 49.

13.3 Selezione delle applicazioni da controllare

Per impostazione predefinita, tutte le applicazioni sono consentite. Per selezionare le applicazioni che si desidera controllare, procedere come segue.

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura controllo applicazioni**.
2. Nella finestra di dialogo **Configura controllo applicazioni**, cliccare sulla scheda **Autorizzazioni**.
3. Selezionare **Tipo applicazione**, per esempio **Condivisione file**.

L'elenco completo delle applicazioni incluse nel gruppo è visualizzata nell'elenco **Autorizzate**.

- Per bloccare un'applicazione, selezionarla e spostarla nella lista **Applicazioni bloccate** cliccare sul pulsante "Aggiungi".



- Per bloccare qualsiasi nuova applicazione che Sophos aggiungerà a quel tipo 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".



13.4 Disinstallazione applicazioni controllate

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.

14 Configurazione del controllo dispositivi

14.1 Controllo dispositivi

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.

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, Sophos consiglia di:

- Selezionare i tipi di dispositivo da controllare.
- Rilevare i dispositivi senza bloccarli.
- Impostare degli allarmi del controllo dispositivi.
- Rilevare e bloccare i dispositivi o consentire l'accesso in sola lettura ai dispositivi di memorizzazione.

Eventi del controllo dispositivi

Quando si verifica un evento del controllo dispositivi, per es. un dispositivo di memorizzazione removibile è stato bloccato, l'evento viene trascritto nel log eventi di Device control e può essere visualizzato da Sophos Control Center. Per informazioni, consultare la sezione [Visualizzazione degli eventi del controllo dispositivi](#) a pagina 22.

Per impostazione predefinita, il numero di computer con eventi che hanno superato una determinata soglia entro le 24 ore 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 dispositivi. Per informazioni, consultare la sezione [Impostazione degli allarmi del controllo dispositivi](#) a pagina 49.

14.2 Tipi di dispositivi che possono essere controllati

Device Control consente di bloccare tre tipi di dispositivo: di *memorizzazione*, *rete* e *short range*.

Memorizzazione

- Dispositivo di memoria rimovibile (per esempio unità flash USB, lettori di schede per PC, unità hard disk esterne)
- Unità disco ottico (unità CD-ROM/DVD/Blu-ray)

- Unità floppy disk.
- Dispositivi di memorizzazione rimovibili sicuri (per es. SanDisk Cruzer Enterprise, SanDisk Cruzer Enterprise FIPS Edition, Kingston Data Traveler Vault - Privacy Edition, Kingston Data Traveler BlackBox e IronKey Enterprise Basic Edition USB flash con cifratura dell'hardware)

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. Un elenco aggiornato dei dispositivi di memoria rimovibile sicuri supportati è disponibile sul sito web di Sophos (www.sophos.it).

Rete

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

Per le interfacce di rete, è possibile impostare un livello di accesso aggiuntivo per la modalità Block Bridged. Esso consente di abilitare un dispositivo di rete (per es. adattatori Wi-Fi) quando il computer è fisicamente disconnesso dalla rete, selezionare l'opzione Blocca bridging quando si impostano i livelli di accesso per i dispositivi di rete.

Nota: La modalità Blocca bridging impedisce il bridging di rete, ad esempio, tra una rete aziendale e una rete non aziendale. La modalità 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 riabilitati direttamente.

Short range

- Interfacce bluetooth
- Infrarossi (Interfaccia infrarossi IrDA)

Device Control blocca interfacce e dispositivi, sia interni che esterni. Per es. il blocco delle interfacce bluetooth porterà al blocco di entrambe:

- L'interfaccia Bluetooth incorporata in computer
- Qualsiasi scheda Bluetooth USB inserita nel computer.

14.3 Impostazione del controllo dispositivi

È possibile configurare Sophos Control Center in modo che esegua la scansione in accesso dei dispositivi che si desidera controllare sulla rete.

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura controllo dispositivi**.
Viene visualizzata la finestra di dialogo **Configura controllo dispositivi**.

2. Nella scheda **Configurazione**, impostare le opzioni come segue.
 - Per abilitare il controllo dispositivi, selezionare la casella di spunta **Abilita la scansione del controllo dispositivi**. Se si desidera rilevare dispositivi ma non bloccarli, selezionare la casella di spunta **Rileva ma non bloccare i dispositivi**.
 - Per impostare il livello di accesso per tutti i tipi di dispositivo, cliccare sulla colonna **Stato** di fianco al tipo di dispositivo e successivamente sul menu a discesa che compare. 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 quanto riguarda i dispositivi di memorizzazione rimovibili sicuri, è possibile cambiare il tipo di accesso e selezionare “Bloccato”.

14.4 Esenzione di un dispositivo

È possibile esentare un dispositivo dai criteri del controllo dispositivi.

È possibile esentare un'istanza di dispositivo (“Solo questo dispositivo”) o un modello di dispositivo (“Tutti i dispositivi di questo modello”). Non impostare le esenzioni sia al livello del modello che dell'istanza del dispositivo. Se vengono definite entrambe le esenzioni, il livello dell'istanza del dispositivo avrà priorità.

Per esentare un dispositivo:

1. Nel menu **Visualizza**, cliccare su **Eventi controllo dispositivi**.

Viene visualizzata la finestra di dialogo **Eventi del dispositivo**.
2. Se si desidera visualizzare solo determinati eventi, nel riquadro **Cerca criteri**, impostare i filtri adeguati e cliccare su **Cerca** per visualizzare tali eventi.

Per ulteriori informazioni, consultare la sezione [Visualizzazione degli eventi del controllo dispositivi](#) a pagina 22.
3. Selezionare la voce del dispositivo che si desidera esentare e cliccare su **Esporta dispositivo**.

Viene visualizzata la finestra di dialogo **Esenta dispositivo**. Sotto **Dettagli dispositivo**, vengono visualizzati tipo, modello e ID del dispositivo.

15 Gestione notifiche

15.1 Configurazione notifiche

È possibile configurare Sophos Control Center per inviare allarmi ogni qual volta vengano rilevate minacce nella rete e/o quando cambia lo stato della rete. Sophos Control Center consente anche di gestire liberamente i vecchi avvisi.

In Sophos Control Center, gli allarmi e-mail sono divisi in due categorie:

- Allarme inviato ai destinatari prescelti se in uno dei computer della rete viene rilevato un virus, un comportamento sospetto, un'applicazione indesiderata o un errore. Questi allarmi vengono configurati tramite le opzioni **Configura scansione > Messaggistica**. Per informazioni, consultare la sezione [Impostazione degli allarmi antivirus e HIPS](#) a pagina 47.
- Allarme inviato ai destinatari prescelti quando si supera un livello impostato nel Pannello di controllo. Viene configurato in due modi:
 - **Strumenti > Configura allarmi e-mail**
 - **Strumenti > Configura pannello di controllo > Allarmi e-mail**

Per informazioni, consultare la sezione [Impostazione degli allarmi e-mail sullo stato della rete](#) a pagina 48.

15.2 Impostazione degli allarmi antivirus e HIPS

Sophos Control Center può visualizzare un allarme nel computer o inviarne uno via e-mail se un virus o un'applicazione potenzialmente indesiderata vengono rilevati in uno dei computer della rete.

Per impostare gli allarmi della scansione:

1. Nel riquadro di sinistra, sotto **Configurazione**, cliccare su **Configura scansione**.
2. Nella finestra di dialogo **Configura scansione**, cliccare su **Messaggistica**.
3. Nel riquadro **Messaggistica**, per impostazione predefinita sono selezionate **Abilita messaggistica desktop** e tutte le opzioni del riquadro **Messaggi da inviare**. È possibile modificare queste impostazioni, se necessario.

Nella casella Messaggio definito dall'utente, è possibile digitare un messaggio che sarà aggiunto alla fine del messaggio standard.

4. Nella scheda **Allarmi e-mail**, per ricevere allarmi via e-mail selezionare **Abilita allarmi e-mail**.

Nota: per gli oggetti bloccati dal firewall non viene inviato alcun allarme via e-mail.

5. 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 e Rilevamento e rimozione di adware e PUA sono applicabili solo a Windows 2000 e successivo. L'impostazione Altri errori è valida soltanto per Windows.

6. 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.

Nota: i computer con sistema operativo Mac OS X invieranno i messaggi solo al primo destinatario dell'elenco.

7. Cliccare su **Configura SMTP** per modificare le impostazioni del server SMTP e la lingua degli allarmi e-mail.

8. 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 Test per inviare un allarme e-mail di prova.

- Nella casella di testo **SMTP sender address**, 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.

Nota: i computer con sistema operativo Linux e UNIX ignoreranno il mittente SMTP e gli indirizzi "rispondi a" e utilizzeranno l'indirizzo root@<nomehost>.

- Nel riquadro **Lingua**, cliccare sulla freccia dell'elenco a discesa e selezionare la lingua in cui inviare gli allarmi e-mail.

15.3 Impostazione degli allarmi e-mail sullo stato della rete

È possibile impostare allarmi e-mail da inviare a destinatari prescelti ogni qual volta venga raggiunto un livello di soglia nel Pannello di controllo.

Per impostare gli allarmi e-mail:

1. Nel 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 le opzioni da inviare al destinatario sotto forma di allarme e-mail quando il livello viene superato.

Per informazioni su come modificare i valori del livello di soglia, consultare la sezione [Configurazione pannello di controllo](#) a pagina 9.

15.4 Impostazione degli allarmi del controllo applicazioni

È possibile inviare allarmi a specifici utenti quando viene rilevata un'applicazione controllata.

1. Nel riquadro di sinistra, sotto **Configurazine**, cliccare su **Configura controllo applicazioni**.
Viene visualizzata la finestra di dialogo **Configura controllo applicazioni**.
2. Nella scheda **Messaggistica**, imposta le opzioni come descritto di seguito:
 - a) 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.
 - b) Nella casella **Testo del messaggio**, digitare il messaggio che si desidera aggiungere alla fine del testo standard.
 - c) Selezionare la casella **Abilita allarmi e-mail** per abilitare Sophos Anti-Virus all'invio di allarmi e-mail. Per ulteriori informazioni sulla configurazione degli allarmi e-mail, consultare la sezione [Impostazione degli allarmi antivirus e HIPS](#) a pagina 47.

15.5 Impostazione degli allarmi del controllo dispositivi

È possibile inviare allarmi a determinati utenti ogni qual volta venga rilevato un evento del controllo dispositivi.

1. Nel riquadro di sinistra, sotto **Configurazine**, cliccare su **Configura controllo dispositivi**.
Viene visualizzata la finestra di dialogo **Configura controllo dispositivi**.
2. Nella scheda **Messaggistica**, imposta le opzioni come descritto di seguito:
 - a) Nel riquadro **Messaggistica**, la casella di spunta **Abilita messaggistica desktop** è selezionata per impostazione predefinita.
Quando un dispositivo non autorizzato viene rilevato dalla scansione in accesso e bloccato, sul desktop dell'utente sarà visualizzato un messaggio che lo informa che l'applicazione è stata bloccata.
 - b) Nella casella **Testo del messaggio**, digitare il messaggio che si desidera aggiungere alla fine del testo standard.
 - c) Selezionare la casella **Abilita allarmi e-mail** per abilitare Sophos Control Center all'invio di allarmi e-mail.
Nella casella **Destinatari di posta**, inserire gli indirizzi e-mail a cui inviare gli allarmi.

15.6 Cancellazione di vecchi allarmi

È possibile impostare Sophos Control Center in modo tale da cancellare automaticamente i vecchi allarmi. Per impostazione predefinita, gli allarmi vengono archiviati nel database per 12 mesi e successivamente cancellati.

Nota: gli allarmi in sospeso non vengono cancellati.

Per cancellare vecchi allarmi:

1. Nel menu **Strumenti** selezionare **Configura reportistica**.
Viene visualizzata la finestra di dialogo **Configura reportistica**.
2. Cliccare sulla scheda **Cancella**.
A seconda dei requisiti della reportistica, scegliere come gestire i vecchi allarmi.
 - **Non cancellare gli allarmi vecchi.**
 - **Cancellare gli allarmi più vecchi di n mesi** (dove n sta per un numero da specificare).

16 Gestione report

16.1 Creazione di un report

È possibile creare un report esistente tramite il gestore reportistica.

Per creare un report:

1. Nella finestra di dialogo Sophos Control Center nella barra degli strumenti, cliccare su **Report**.

Viene visualizzata la finestra di dialogo **Gestore reportistica**.

2. Selezionare il tipo di report che si desidera creare.

Per informazioni su come creare un nuovo report, consultare la sezione [Creazione di un nuovo report](#) a pagina 51.

3. Cliccare su **Esegui**.

Viene visualizzato un report che riassume tutti i criteri utilizzati per la creazione di report.

4. Scegliere una delle seguenti schede per visualizzare il report nel formato desiderato:

Nota: in base ai criteri del report, alcuni report potrebbero avere a disposizione solo un formato per la visualizzazione dei dati.

- **Grafico**
- **Tabella**

16.2 Creazione di un nuovo report

È possibile creare un nuovo report tramite il gestore reportistica.

Per creare un nuovo report:

1. Nella finestra di dialogo Sophos Control Center nella barra degli strumenti, cliccare su **Report**.

Viene visualizzata la finestra di dialogo **Gestore reportistica**.

2. Cliccare su **Crea**.

Viene visualizzata la finestra di dialogo **Crea un nuovo report**.

- Se si utilizza la procedura guidata, nel menu a discesa, selezionare il modello di report che si desidera utilizzare e cliccare su **OK**.

La procedura guidata accompagna l'utente nel processo di creazione di un report in base al modello prescelto.

- Se si utilizza la finestra Proprietà, cancellare **Utilizza la procedura guidata per creare report** e cliccare su **OK**.

Viene visualizzata la finestra **Proprietà** contenente le opzioni per la creazione di un report.

16.3 Impostazione di report pianificati

Sophos Control Center può inviare report contenenti il numero e i dati relativi alle minacce rilevate durante il periodo specificato.

I destinatari riceveranno un report via e-mail contenente le seguenti informazioni:

- Data del report
- Nome dell'azienda (per impostare il nome dell'azienda cliccare su **Strumenti >Configura reportistica**)
- Numero di file/comportamenti sospetti
- Numero di adware/applicazioni potenzialmente indesiderate rilevate
- Numero di virus/spyware rilevati.
- Elenco delle minacce rilevate in ordine cronologico, riportante il nome delle minacce e il numero di infezioni
- Elenco delle applicazioni bloccate in ordine cronologico, riportante il nome delle applicazioni e il numero dei computer infetti. È possibile includere allarmi di tipo Bloccato dal firewall, Applicazioni controllate e Dispositivi controllati.

Per impostare i report pianificati:

1. Nella finestra di dialogo Sophos Control Center nella barra degli strumenti, cliccare su **Report**.
Viene visualizzata la finestra di dialogo **Gestore reportistica**.
2. Selezionare il report esistente e cliccare su **Operazione pianificata**.
Viene visualizzata la finestra di dialogo **Proprietà Nome report** (dove *Nome report* sta per il nome di uno specifico report).
3. Nella scheda **Operazione pianificata**, impostare le opzioni come descritto qui sotto:
 - a) Selezionare **Pianifica questo report**.
 - b) Nella sezione Operazione pianificata, impostare i campi **Inizio** e **Il**, indicare l'ora e la data in cui si desidera creare il report.
Nel menu a discesa **Ripeti** impostare la frequenza con cui si desidera generare report.
 - c) Nella sezione **Output**, impostare il **Formato** in cui si desidera inviare l'allegato di posta elettronica.
 - d) Impostare la **Lingua** in cui si desidera ricevere il report.
 - e) Selezionare l'indirizzo e-mail a cui inviare l'e-mail e aggiungerlo all'elenco dei destinatari.
Per inviare e-mail è necessario configurare le impostazioni del server SMTP. Per informazioni su come configurare le impostazioni, consultare la sezione [Impostazione degli allarmi e-mail sullo stato della rete](#) a pagina 48.

16.4 Modifica dei report

È possibile modificare un report esistente e generare dati.

Per modificare un report esistente:

1. Nella finestra di dialogo Sophos Control Center nella barra degli strumenti, cliccare su **Report**.
2. Nella finestra di dialogo **Gestore reportistica**, selezionare il report che si desidera modificare e cliccare su **Proprietà**.

Nota: in base ai criteri selezionati, solo alcuni o tutti i campi appariranno nelle schede.

3. Nella scheda **Configurazione** scegliere di modificare una delle seguenti opzioni:

- **Dettagli del report**

Inserire il **Nome** per salvare il report in base al nome. Per impostazione predefinita, la casella **Descrizione report** contiene una descrizione che si basa sulle scelte fatte.

- **Periodo del report**

Nel menu a discesa **Periodo**, selezionare un periodo di tempo definito. Selezionare **Personalizzato** per specificare un periodo di tempo utilizzando le caselle **Inizio** e **Fine**.

- **Percorso del report**

Selezionare il menu a discesa **Tutti i computer** o **Computer singolo** per specificare il nome di un computer.

- **Tipi di allarmi da comprendere**

Selezionare il tipo di allarme che si desidera includere.

È inoltre possibile configurare il report in modo tale che visualizzi soltanto i computer in cui è stata segnalata una particolare minaccia. Per specificare una singola minaccia, cliccare su **Avanzata**.

Nella finestra **Configurazione avanzata**, scegliere quale allarme includere nel report. Nella casella di testo **Espressione** è possibile inserire il nome di una particolare minaccia, oppure, per specificare più di una minaccia, digitare il nome nella casella di testo utilizzando caratteri jolly. Utilizzare il ? 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** scegliere di modificare una delle seguenti opzioni:
 - Per impostazione predefinita, **Mostra opzioni** elenca tutti gli oggetti selezionati. È però possibile configurare il report in modo che mostri:
 - Solo primi x allarmi (x è il numero specificato dall'utente).
 - Solo gli allarmi con n o più occorrenze.
 - **Mostra i risultati per**
Per impostazione predefinita, i risultati vengono visualizzati in base al **Giorno**. È anche possibile ordinarli per **Ora**, **Settimana** o **Mese**.
 - **Visualizza i risultati come**
Per impostazione predefinita i risultati vengono visualizzati in **Percentuali**. È anche possibile visualizzarli in **Numeri**.
 - **Ordina per**
Per impostazione predefinita, il report elenca le minacce in ordine decrescente di numero di allarmi per minaccia. È anche possibile ordinarle per **Nome allarme**, **Nome computer** o **Data e ora**.
5. Nella scheda Operazione pianificata, selezionare le opzioni per modificare la pianificazione:
 - a) Selezionare **Pianifica questo report**.
 - b) Nella sezione Operazione pianificata, impostare i campi **Inizio** e **Il**, indicare l'ora e la data in cui si desidera creare il report.

Il menu a discesa **Ripeti** consente di selezionare la frequenza a cui si desidera ripetere l'operazione.
 - c) Nella sezione **Output**, selezionare il **Formato** in cui si desidera inviare l'allegato di posta elettronica.
 - d) Impostare la **Lingua** in cui si desidera ricevere il report.
 - e) Selezionare l'indirizzo e-mail a cui inviare l'e-mail e aggiungerlo all'elenco dei destinatari. Per informazioni su come configurare o aggiungere un indirizzo e-mail, consultare la sezione [Impostazione degli allarmi e-mail sullo stato della rete](#) a pagina 48.


16.5 Esportazione del report in un file

Dopo che il report è stato creato, è possibile esportarlo in diversi formati.

Per esportare il report in un file:

1. Nella finestra di dialogo Sophos Control Center nella barra degli strumenti, cliccare su **Report**.


Viene visualizzata la finestra di dialogo **Gestore reportistica**.
2. Selezionare il report che si desidera esportare e cliccare su **Esegui**.

3. Nella finestra di dialogo **Reportistica**, nella barra degli strumenti, cliccare sull'icona **Esporta** .
4. Nella finestra di dialogo **Esporta report**, selezionare il tipo di documento o di foglio elettronico nel quale si desidera esportare il report.
5. Cliccare sul pulsante Sfoglia del campo **Nome file** per selezionare un percorso.
6. Nella finestra di dialogo **Salva con nome**, andare al percorso in cui si desidera salvare il report, inserire un nome per il report e cliccare su **Salva**.
7. Nella finestra di dialogo **Esporta report**, cliccare su **OK**.

16.6 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.

Per modificare il layout del report:

1. Nella finestra di dialogo Sophos Control Center, dalla barra degli strumenti, cliccare su **Report**.
Viene visualizzata la finestra di dialogo **Gestore reportistica**.
2. Selezionare un report e cliccare su **Esegui**.
3. Nella finestra di dialogo **Reportistica**, dalla barra degli strumenti cliccare sull'icona del layout di pagina .
4. 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.
5. Le stesse impostazioni vengono utilizzate anche quando si stampa o si esporta il report.

17 Troubleshooting

17.1 Disinfezione non riuscita

Se non si riesce a rimuovere centralmente una minaccia, andare al computer infetto ed eseguire la disinfezione manualmente.

Se la minaccia non è stata rimossa e si richiede assistenza, si consiglia di:

1. Annotare il nome della minaccia.
2. Nel riquadro a sinistra, sotto **Informazioni**, cliccare su **Info sulle minacce** per collegarsi alla pagina del sito web Sophos relativa all'analisi delle minacce.
3. Nella pagina relativa all'analisi delle minacce, cercare la minaccia. Seguire i collegamenti per consigli sulla disinfezione.

Se non si riesce ad eliminare la minaccia, sotto **Informazioni**, cliccare su **Supporto tecnico**.

Inserire il nome della minaccia, i dettagli del o dei computer infettati e inviare un'e-mail.

17.2 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 Anti-Virus 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 applicazioni potenzialmente indesiderate. In alternativa si può utilizzare una scansione pianificata.
- Autorizzare l'applicazione, se si desidera eseguirla sui computer. Per informazioni, consultare la sezione [Autorizzazione all'utilizzo di applicazioni](#) a pagina 30.
- Cancellare le applicazioni non autorizzate. Per informazioni, consultare la sezione [Disinfezione del computer](#) a pagina 14.

18 Supporto tecnico

Per ricevere assistenza tecnica relativa a questa versione beta:

1. Visualizzare il modulo di invio personalizzato (allegato all'email inviata da Sophos contenente le istruzioni per il download), completare i campi pertinenti, ed inviarlo al nostro team di supporto.
2. Accedere al forum Beta Sophos (utilizzando i dati inclusi nell'email inviata da Sophos contenente le istruzioni per il download) e cercare altri utenti beta con lo stesso problema.
3. Se si riscontrano problemi con quanto citato sopra, si prega di inviare un'e-mail a betaprogram@sophos.com, al cui indirizzo risponderà un membro del nostro Team Beta.

19 Copyright

Copyright © 2010 Sophos Group. 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.

Sophos e Sophos Anti-Virus sono marchi registrati di Sophos Plc e Sophos Group. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as "DOC software") are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source¹⁰, free software, you are free to use, modify, copy, and distribute--perpetually and irrevocably--the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us¹¹ know so we can promote your project in the DOC software success stories¹².

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies¹³ around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE¹⁴, TAO¹⁵, CIAO¹⁶, and CoSMIC¹⁷ web sites are maintained by the DOC Group¹⁸ at the Institute for Software Integrated Systems (ISIS)¹⁹ and the Center for Distributed Object Computing of Washington University, St. Louis²⁰ for the development of open-source software as part of the open-source software community²¹. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge

that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

Sono graditi eventuali suggerimenti, aggiunte, commenti o domande²².

Douglas C. Schmidt²³

The ACE home page is <http://www.cs.wustl.edu/ACE.html>

References

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. <http://www.the-it-resource.com/Open-Source/Licenses.html>
11. mailto:doc_group@cs.wustl.edu
12. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
13. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
14. <http://www.cs.wustl.edu/~schmidt/ACE.html>
15. <http://www.cs.wustl.edu/~schmidt/TAO.html>
16. <http://www.dre.vanderbilt.edu/CIAO/>
17. <http://www.dre.vanderbilt.edu/cosmic/>
18. <http://www.dre.vanderbilt.edu/>
19. <http://www.isis.vanderbilt.edu/>
20. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
21. <http://www.opensource.org/>
22. <mailto:d.schmidt@vanderbilt.edu>
23. <http://www.dre.vanderbilt.edu/~schmidt/>

Indice

A

- aggiornamento
 - selezionare applicazioni 34
- aggiornamento della rete 13
- aggiornamento immediato 13
- aggiornamento manuale 13
- allarmi
 - antivirus 47
 - cancella 50
 - configura 47
 - controllo applicazioni 49
 - controllo dei dispositivi 49
 - HIPS 47
 - pannello di controllo 48
 - stato della rete 48
- allineamento alla configurazione 19
- Applicare nuovamente la configurazione centralizzata 19
- autorizza applicazioni 30

C

- cancellazione
 - allarmi 17
 - errori 17
- computer non aggiornati
 - aggiornamento 13
- computer protetti 20
- Configurazione centralizzata 19
- configurazione scansione 33
- controllo applicazioni
 - allarmi 49
- controllo dei dispositivi
 - allarmi 49
 - block bridge 44
 - eventi 22
 - memorizzazione 44
 - rete
 - short range 44
 - tipi di dispositivi 44
- creazione
 - report 51

D

- disattivazione
 - firewall
 - Sophos Control Center 38
- disinfezione 14
- Disinfezione automatica 28
 - PUA 29
 - Virus 29
- disinstallazione
 - applicazioni controllate 42
- disinstallazione applicazioni controllate 42

E

- esclusione dalla scansione 28
- esclusione scansione pianificata 32
- esportazione
 - report 54
- eventi
 - controllo dei dispositivi 22

F

- file sospetti 29
- firewall
 - disattivare da Sophos Control Center 38

I

- interfaccia
 - Vista computer 4
 - Vista dei gestori degli aggiornamenti 4
- Interfaccia di Sophos Control Center 4

L

- layout
 - report 55

M

- Messaggistica desktop 47
- modifica
 - report 53

O

- operazione pianificata
 - report 52

opzioni della scansione in accesso 26
opzioni operazione pianificata 31

P

Pannello di controllo
 panoramica 8
protezione di nuovi sistemi operativi 11
PUA
 allarmi frequenti 56

R

recupero dei computer eliminati 20
report
 creazione 51
 esportazione 54
 layout 55
 modifica 53
 operazione pianificata 52
rete protetta 20

risoluzione dei problemi
 allarmi frequenti 56
 PUA 56
risolvi
 allarmi 17
 errori 17

S

scansione
 in accesso 26
scansione computer singoli 33
scansione web 28
Sophos Control Center 3, 4

V

verifica aggiornamento 12
verifica della rete 20
Vista computer 4