

SOPHOS

SMALL BUSINESS EDITION

Sophos Control Center
Guida di avvio



Sommario

1	Informazioni sulla guida.....	3
2	Requisiti di sistema.....	4
3	Installazione.....	5
4	Protezione dei computer in rete.....	8
5	Verifica della protezione dei computer.....	11
6	Impostazione degli allarmi via e-mail.....	12
7	Impostazione della scansione per la ricerca di applicazioni potenzialmente indesiderate.....	13
8	Trattamento dei virus.....	15
9	Impostazione del firewall.....	16
10	Supporto tecnico.....	19
11	Copyright.....	20

1 Informazioni sulla guida

Questa guida spiega come proteggere i computer della rete (sia con sistema operativo Windows che Macintosh) contro virus, (spyware incluso), applicazioni potenzialmente indesiderate e altre minacce alla sicurezza.

Se in possesso di computer che non si connettono mai alla rete, consultare anche la *Guida di avvio per computer autonomi di Sophos Endpoint Security and Control*.

Se si sta eseguendo l'upgrade da una versione precedente di Sophos Control Center, consultare la *guida all'upgrade di Sophos Control Center*.

Per dettagli su tutte le opzioni di configurazione di Sophos Control Center, non incluse in questa guida, consultare la guida in linea di Sophos Control Center.

La documentazione di Sophos è pubblicata in <http://www.sophos.it/support/docs/>.

2 Requisiti di sistema

Per informazioni sui requisiti di sistema, consultare la pagina relativa ai requisiti di sistema del sito web di Sophos <http://www.sophos.it/products/all-sysreqs.html>.

È inoltre necessario avere accesso a Internet per poter scaricare il software dal sito web di Sophos.

Sophos Control Center ed i componenti del server sono in possesso anche dei seguenti requisiti:

- È necessario avere accesso da e a gli altri computer in rete.
- È consigliabile che sia in esecuzione un sistema operativo per server (quale Windows 2000 Server con Service Pack 3 o successivo, Windows Server 2003, Windows Small Business Server 2003 o Windows Small Business Server 2008). In caso contrario, viene compromesso il rendimento di Sophos Control Center.

3 Installazione

3.1 Preparazione all'installazione di Sophos Control Center

Prima di eseguire l'installazione di Sophos Control Center, assicurarsi che:

- Si disponga di nome utente e password forniti da Sophos.
- Si acceda al computer in cui installare Sophos Control Center come amministratore o amministratore di dominio, a seconda del caso.

Nota: per proteggere i computer di un gruppo di lavoro, in tutte le piattaforme Windows, è necessario, per prima cosa, svolgere i passaggi aggiuntivi menzionati nell'articolo: <http://www.sophos.it/support/knowledgebase/article/29728.html>.

3.2 Preparazione dei computer

Prima di installare il software di sicurezza nei computer, assicurarsi che:

- I software antivirus di un altro produttore siano stati rimossi da tutti i computer in cui si desidera installare Sophos Anti-Virus.
- Il sistema operativo sia configurato nel modo richiesto.

3.2.1 Windows Vista

Sophos Anti-Virus possiede requisiti extra nei computer Windows Vista:

- Assicurarsi che il servizio di **Registro Remoto** sia avviato e che la sua modalità di avvio sia impostata su **Automatico**. Su Windows Vista, questo servizio non è attivato per impostazione predefinita. Per accedervi, cliccare su **Start, Pannello di controllo, Strumenti di amministrazione, Servizi**. Scorrere l'elenco dei servizi e cliccare due volte sul servizio **Registro di sistema remoto**. Nella finestra di dialogo delle **Proprietà del Registro Remoto**, nella scheda **Generale**, nel campo **Tipo di avvio**, cliccare sulla freccia del menu a discesa e selezionare **Automatico**. Cliccare su **Applica**. Cliccare su **Start** e poi su **OK**.
- Disabilitare il **Controllo account utente**. Per accedervi, cliccare su **Start, Pannello di controllo, Account utente, Disabilita account utente**. Abilitare nuovamente l'opzione una volta che l'installazione è stata completata.
- Aprire **Windows Firewall con Protezione avanzata**. Per accedervi, cliccare su **Start, Pannello di controllo, Strumenti di amministrazione**. Modificare le **Regole in entrata** al fine di abilitare:

Nome regola	Profilo
Amministrazione remota (NP-In)	Dominio
Amministrazione remota (NP-In)	Privato

Nome regola	Profilo
Amministrazione remota (RPC)	Dominio
Amministrazione remota (RPC)	Privato
Amministrazione remota (RPC-EPMAP)	Dominio
Amministrazione remota (RPC-EPMAP)	Privato

Nota: a installazione completata, tali processi vanno disabilitati nuovamente.

3.2.2 Windows XP

È necessario svolgere i seguenti passaggi su tutti i computer Windows XP, con o senza service pack:

- Rimuovere eventuali firewall di altri produttori, eccetto Windows Firewall, da tutti i computer con sistema operativo Windows XP nei quali si desidera installare Sophos Client Firewall.
- Disabilitare Condivisione file semplice.

Per maggiori informazioni su come effettuare tale operazione, consultare <http://www.sophos.it/support/knowledgebase/article/12837.html>.

Windows XP con Service Pack 2

In un computer Windows XP Service Pack 2, se Windows Firewall è disattivato e **non** si ha intenzione di installarvi Sophos Client Firewall, svolgere le seguenti operazioni:

- Abilitare Condivisione file e stampanti per reti Microsoft.
- Aggiungere la seguente eccezione di programma:

C:\Programmi\Sophos\Remote Management System\RouterNT.exe

Per maggiori informazioni su come effettuare tale operazione, consultare <http://www.sophos.it/support/knowledgebase/article/11075.html>.

3.2.3 Windows Server 2003 con Service Pack 1

Se Windows Firewall è attivato, è necessario procedere come di segue:

- Abilitare Condivisione file e stampanti per reti Microsoft.
- Aggiungere la seguente eccezione di programma:

C:\Programmi\Sophos\Remote Management System\RouterNT.exe

Per maggiori informazioni su come effettuare tale operazione, consultare <http://www.sophos.it/support/knowledgebase/article/11075.html>.

3.2.4 Windows 2000

- Rimuovere eventuali firewall di altri produttori, eccetto Windows Firewall, da tutti i computer con sistema operativo Windows 2000 nei quali si desidera installare Sophos Client Firewall.

3.2.5 Windows 95/98/NT

- Rimuovere tutte le installazioni esistenti di Sophos Anti-Virus. A tal scopo, utilizzare l'utilità Installazione applicazioni dal Pannello di controllo di Windows.

3.3 Installazione di Sophos Control Center

Innanzitutto, installare Sophos Control Center, che permette di scaricare, installare e gestire i software antivirus e firewall.

1. Visitare la pagina relativa al download dei prodotti Sophos <http://www.sophos.it/support/updates> e digitare il nome utente e la password forniti da Sophos.
Seguire i link per scaricare la procedura guidata per il prodotto prescelto della gamma Sophos Small Business Solutions, ed eseguirla.
2. Nella pagina **Benvenuti**, cliccare su **Avanti**.
Una procedura guidata accompagna nei passaggi dell'installazione. Accettare le opzioni predefinite, eccezion fatta per quanto mostrato di seguito.
3. Nella pagina **Tipo di installazione**, selezionare **Completa l'installazione** per installare le funzioni del programma.
Nota: se si desidera gestire il software di sicurezza da un altro computer, è possibile eseguire di nuovo il programma di installazione da quel computer e selezionare **Console di gestione**.
Cliccare su **Avanti** e continuare la procedura guidata mantenendo le opzioni predefinite.
4. Portare a termine l'installazione e cliccare su **Fine** per uscire automaticamente. Se invece si desidera uscire più tardi, deselezionare la casella **Disconnetti ora** prima di cliccare su **Fine**.
Talvolta è necessario riavviare Windows invece di uscire semplicemente. In questo caso, la casella non è visualizzata e un successivo messaggio chiede se si desidera riavviare Windows subito o più tardi.
5. All'accesso successivo, entrare con lo stesso account utente. La Procedura guidata Sophos per la protezione della rete viene avviata automaticamente.
Per informazioni sulla protezione dei computer in rete, consultare la sezione [Protezione dei computer in rete](#) a pagina 8.

4 Protezione dei computer in rete

Quando si accede per la prima volta dopo l'installazione, Sophos Control Center si apre automaticamente e viene avviata la procedura guidata di protezione della rete di Sophos. Questa procedura guidata permette di proteggere i computer della rete.

1. Nella pagina **Benvenuti**, cliccare su **Avanti**.
2. Nella pagina **Dati dell'account di download Sophos**, inserire nome utente e password forniti da Sophos e cliccare su **Avanti**.
Per impostazione predefinita, Sophos Control Center scarica il software nella cartella C:\Programmi\Sophos\SCC\Library, nel computer attualmente in uso, e lo distribuisce da qui ad altri computer.
Se ci si connette a Internet tramite server proxy, selezionare **Accedi a Sophos tramite server proxy** e inserire i dettagli del server proxy.
3. Nella pagina **Selezione piattaforma**, selezionare il software relativo al sistema operativo in esecuzione nel computer.
 - L'opzione **Windows 2000 e successivo** viene selezionata per impostazione predefinita.
 - Se sono presenti computer con sistema operativo Mac OS X, selezionare la casella Mac OS X. Ciò consentirà di installare il software antivirus nei computer in un secondo momento.
4. Nella pagina **Download del software**, viene visualizzata una barra di avanzamento. Sophos Control Center scarica il software. Quando il download è completo, cliccare su **Avanti**.
5. Nella pagina **Dati dell'account utente di Windows**, inserire i dati di un account con diritti di amministratore che sia valido in tutti i computer della rete e possa essere utilizzato per installarvi software. Non si tratta dello stesso account Sophos utilizzato in precedenza. In molti casi, è possibile utilizzare l'account con cui si è effettuato l'accesso prima di iniziare l'installazione.
6. Nella pagina **Proteggi computer**, la procedura guidata ricerca i computer nei quali il software può essere installato automaticamente.

In questa pagina sono elencati solo i computer Windows 2000/XP/2003, dal momento che non è possibile eseguire un'installazione automatica nei computer Windows 95/98/NT o Mac.

Per impostazione predefinita, tutti i computer sono selezionati per essere protetti. È possibile deselegionare la casella di spunta di fianco a qualsiasi computer che non si desidera proteggere. Per selezionare o deselegionare tutte le caselle di spunta nell'elenco, selezionare o deselegionare la casella in testa alla colonna **Proteggi**.

7. Nella pagina **Seleziona funzioni**, selezionare le funzioni che si desidera installare:

- Protezione antivirus (selezionata per impostazione predefinita).
- Protezione Sophos Client Firewall (se inclusa nella licenza).

Nota: per attivare il firewall, si dovranno riavviare tutti i computer in cui si è scelto di installare Sophos Client Firewall.

- Tool di rimozione del prodotto concorrente

Cliccare su **Avanti**.

8. Se nella pagina **Computer che bisogna proteggere manualmente** sono elencati dei computer, cliccare su **Stampa** per stampare la lista di tali computer, cliccare su **Salva con nome** per salvare una copia della lista, o prenderne nota. Cliccare su **Avanti**. Cliccare su **Avanti** e completare la procedura guidata.

Sophos Control Center installa il software automaticamente nei computer selezionati.

Poiché la protezione antivirus e firewall è applicata ad ogni computer, viene visualizzata un'icona blu a forma di computer accanto al nome del computer e nella colonna **Aggiornato** è presente la dicitura **Sì**.

Per informazioni su come proteggere i computer manualmente, consultare la sezione [Protezione manuale dei computer in rete](#) a pagina 9.

4.1 Protezione manuale dei computer in rete

È possibile proteggere i computer manualmente.

1. Andare a ciascun computer presente nell'elenco stampato o salvato. Cercare la cartella in cui Sophos Control Center mette a disposizione il software antivirus, il firewall e gli aggiornamenti. Per impostazione predefinita, le cartelle sono:

Sistema operativo	Cartella
Windows 2000/XP/2003	\\[nome server]\Sophos\SAVSCFXP
Windows 95/98/NT	\\[nome server]\Sophos\ES9x
Mac OS X	smb://[nome server]/Sophos/ESOSX

[nome server] è il nome del computer in cui si è installato Sophos Control Center.

2. Cliccare due volte su setup.exe (su Windows) o Sophos Anti-Virus.mpkg (su Mac OS X). Se si effettua l'installazione su Mac OS X 10.2 o successivo, è necessario copiare Sophos Anti-Virus.mpkg nel Mac ed eseguire lì l'installazione.

È anche possibile proteggere computer che non sono sempre collegati alla rete (v. la sezione [Protezione dei computer che si connettono alla rete solo occasionalmente](#) a pagina 10).

4.2 Protezione dei computer che si connettono alla rete solo occasionalmente

I computer che si connettono alla rete solo occasionalmente (per esempio, i portatili utilizzati sia all'esterno che all'interno dell'ufficio) possono essere protetti persino quando non sono connessi alla rete.

Tutti i computer nei quali sono stati installati i software antivirus e firewall sono già configurati per prelevare gli aggiornamenti dei software antivirus e firewall direttamente da Sophos quando non sono connessi alla rete.

Se sono presenti computer che si connettono alla rete occasionalmente, nei quali non si è ancora installato il software antivirus o firewall, si consiglia di installarvi la protezione non appena si connettono alla rete. Questa procedura è descritta nella guida in linea di Sophos Control Center, nella sezione relativa alla protezione di nuovi computer.

5 Verifica della protezione dei computer

È possibile verificare, tramite il pannello di controllo, che i computer in rete siano protetti dalle minacce.

Il pannello di controllo fornisce una visione d'insieme dello stato della protezione della rete. È possibile configurare i valori di soglia in modo tale che il pannello di controllo avverta ed invii messaggi di allarme ogni qual volta tali valori vengano raggiunti.

Per mostrare o nascondere il pannello di controllo, cliccare sul pulsante **Pannello di controllo** nella barra degli strumenti.

Per informazioni su come configurare il pannello di controllo e un elenco completo di icone e del relativo stato, consultare la guida in linea di Sophos Control Center.

6 Impostazione degli allarmi via e-mail

Per impostazione predefinita, gli allarmi del desktop sono visualizzati solo nel computer in cui è stata rilevata la minaccia. Sophos Control Center invia allarmi anche agli utenti o computer prescelti.

1. In Sophos Control Center, nel menu **Configurazione**, cliccare su **Configura scansione**.
2. Nella finestra di dialogo **Configura scansione**, cliccare sulla scheda **Allarmi e-mail**.
Selezionare **Abilita allarmi e-mail** e fare quanto riportato di seguito:
 - a) Selezionare le minacce (per es. virus) per cui si desidera ricevere allarmi.
 - b) Nella cornice **Destinatari**, cliccare su **Aggiungi** ed inserire gli indirizzi.
 - c) Cliccare su **Configura** e inserire i dati del server SMTP e l'indirizzo "mittente" SMTP.

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

7 Impostazione della scansione per la ricerca di applicazioni potenzialmente indesiderate

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

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. In seguito, è possibile abilitare la scansione in accesso per la ricerca di applicazioni potenzialmente indesiderate, al fine di proteggere i computer in futuro.

7.1 Scansione pianificata dei computer

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 **Scansione pianificata**, cliccare su **Configura** (in fondo alla pagina).
4. Nella finestra di dialogo **Impostazioni di scansione e rimozione**, cliccare sulla scheda **Scansione**. Nel riquadro **Opzioni di scansione**, selezionare la casella di spunta **Cerca adware e PUA** e cliccare su **OK**.

A scansione terminata, Sophos Anti-Virus potrebbe segnalare la presenza di alcune applicazioni potenzialmente indesiderate. È possibile autorizzare le applicazioni o rimuoverle dai computer.

7.2 Autorizzazione delle applicazioni che si desidera utilizzare

È possibile scegliere di autorizzare applicazioni rilevate come adware o PUA durante la scansione pianificata.

Per autorizzare un'applicazione:

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**, svolgere una delle seguenti operazioni:
 - Selezionare l'applicazione che si desidera autorizzare. Cliccare su **Aggiungi** per aggiungerla alla lista delle applicazioni autorizzate.
 - Se tale applicazione non viene visualizzata, cliccare su **Nuova voce**. Dalla finestra di dialogo che viene visualizzata, seguire il link all'elenco di Sophos relativo alle applicazioni potenzialmente indesiderate. Individuare l'applicazione che si desidera autorizzare e inserirne il nome nel campo **Nome**.

7.3 Rimozione delle applicazioni che non si desidera utilizzare

È possibile cancellare le applicazioni rilevate come adware o PUA durante la scansione pianificata.

Per cancellare applicazioni:

1. Nel riquadro a sinistra, sotto **Azione**, cliccare su **Risolvi allarmi ed errori**.

Viene visualizzata la finestra di dialogo **Risolvi allarmi ed errori**.

2. Selezionare la casella di spunta relativa ad ogni applicazione che si desidera rimuovere, oppure cliccare su **Seleziona tutti** e poi cliccare su **Disinfetta**.

Ciò rimuove tutti i componenti noti delle applicazioni selezionate dai computer prescelti. La rimozione potrebbe richiedere alcuni minuti.

Nota: alcune applicazioni non possono essere cancellate tramite Sophos Control Center. In questo caso, andare nel computer interessato e rimuovere l'applicazione utilizzando Sophos Anti-Virus.

Per rimuovere completamente da un computer alcune applicazioni composte da numerosi componenti, potrebbe essere necessario il riavvio del computer. In tal caso, viene 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 vengono eseguite dopo il riavvio del computer.

Per trovare maggiori informazioni relative a una specifica applicazione sul sito web di Sophos, nella finestra di dialogo **Risolvi allarmi ed errori**, cliccare sul nome dell'applicazione.

Cliccando su **Cancella dall'elenco**, le applicazioni selezionate verranno rimosse dall'elenco. Tuttavia, non vengono né eliminate del tutto, né autorizzate.

7.4 Abilitazione della scansione in accesso per la ricerca di adware e applicazioni potenzialmente indesiderate

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

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

2. Cliccare su **Scansione in accesso**.

Viene visualizzata la finestra di dialogo **Impostazioni della scansione in accesso**.

3. Nel riquadro **Opzioni di scansione**, selezionare la casella di spunta **Cerca adware e PUA**. Cliccare su **OK**.

Alcune applicazioni monitorano i file tentando frequentemente di accedervi. Se la scansione in accesso è abilitata, essa rileva ogni accesso e invia allarmi multipli.

8 Trattamento dei virus

È possibile rimuovere i virus eseguendo le seguenti operazioni:

1. In Sophos Control Center, nel **Pannello di controllo**, cliccare sul link **Virus/spyware**.

Nella finestra di dialogo **Risolvi allarmi ed errori**, viene visualizzata una lista dei computer infetti, compresi i dati relativi ai virus.

2. Selezionare i virus che si desidera rimuovere e cliccare su **Disinfetta**.

In questo modo si rimuove il virus dal file o dal settore di avvio che è stato infettato. Tuttavia, la disinfezione dei documenti non annulla eventuali modifiche apportate dal virus al documento; la disinfezione dei programmi dovrebbe essere utilizzata solo come misura temporanea: si consiglia di sostituire in seguito i programmi disinfettati utilizzando i dischi originali o copie di backup. La rimozione potrebbe richiedere alcuni minuti.

Alcuni virus non possono essere rimossi tramite Sophos Control Center. In questo caso, andare nel computer interessato e rimuovere il virus utilizzando Sophos Anti-Virus.

Prima di tentare di rimuovere dai computer minacce formate da più componenti, Sophos consiglia di eseguire una scansione pianificata completa dei computer, al fine di determinare tutti i componenti che formano tali minacce.

Per trovare maggiori informazioni su uno specifico virus sul sito web di Sophos, nella finestra di dialogo **Risolvi allarmi ed errori**, cliccare sul nome del virus.

9 Impostazione del firewall

Quando si installa Sophos Client Firewall per la prima volta, risulterà impostato in modo tale da consentire il traffico essenziale in entrata e in uscita.

Nota: Sophos Client Firewall non supporta IPv6. La versione 1 lascia passare i pacchetti IPv6, quelle 1.5 e 2.0 bloccano o lasciano passare tutti i pacchetti IPv6, a seconda della configurazione.

9.1 Configurazione del firewall

È possibile configurare il firewall per consentire o bloccare il traffico a seconda delle necessità. Per impostazione predefinita, il firewall è impostato per consentire il traffico in entrata essenziale e tutto quello in uscita.

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:
 - **Percorso singolo**
Selezionare i computer che sono sempre in rete, per es. i desktop.
 - **Percorso doppio**
Selezionarlo 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.
 - **Consenti tutto il traffico**
Selezionarlo se si desidera disattivare il firewall e consentire il traffico.
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.
 - **Blocca il traffico in ingresso e consenti il traffico in uscita**

Consente solo al traffico essenziale dei computer di accedere sia alla rete che a Internet, ma blocca tutto il traffico in entrata. In questa modalità le applicazioni non sono autenticate
 - **Blocco del traffico in entrata e in uscita**

Se si seleziona questa modalità, il firewall bloccherà il traffico in uscita, eccezion fatta per le applicazioni specificate. Per aggiungere applicazioni, cliccare su **Attendibile** alla destra di questa opzione. Ad un'applicazione "attendibile" è consentita tutta l'attività di rete.
 - **Monitora**

Questa modalità applica ai computer tutte le regole specificate, oltre che consentire a tutto il traffico sconosciuto di accedere alla rete e a Internet. Riporta poi queste informazioni alla console. Utilizzare questa modalità per raccogliere informazioni sulla rete e creare regole adeguate.
 - **Personalizza**

Consente di applicare una configurazione personalizzata. 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*.
6. 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.
7. Se si seleziona **Percorso doppio**, verrà richiesta la modalità operativa e la condivisione file e stampanti (come citato ai passaggi 5 e 6) per il percorso secondario (esterno alla rete).

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

Una volta impostato il firewall, è possibile visualizzare gli eventi del firewall (per es. le applicazioni bloccate dal firewall) in **Firewall - Visualizzatore eventi**. Per ulteriori informazioni, consultare la guida in linea di Sophos Control Center.

9.2 Trattamento degli oggetti bloccati dal firewall

Sophos Control Center potrebbe bloccare applicazioni o processi che si desidera eseguire. In tal caso, procedere come segue:

1. In Sophos Control Center, nel **Pannello di controllo**, cliccare sul link **Firewall**.
2. Nella finestra di dialogo **Firewall - Visualizzatore eventi**, selezionare la voce relativa all'applicazione che si desidera permettere o 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 tramite impostazioni predefinite esistenti.

10 Supporto tecnico

Per ricevere assistenza tecnica relativa a questa versione beta:

1. reperire i dati del proprio indirizzo web di cliente beta (nell'e-mail inviata da Sophos)
2. visitare quell'indirizzo
3. compilare e inviare il modulo.

11 Copyright

Copyright © 2009 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.

Alcuni programmi software sono concessi in licenza (o in sottolicenza) all'utente secondo i termini della GNU General Public License (GPL) o licenze similari per il software libero che, tra gli altri diritti, permettono all'utente di copiare, modificare e redistribuire determinati programmi, o porzioni di programma, e di accedere al codice sorgente. La GPL richiede, per qualsiasi software concesso in licenza secondo i termini della stessa e distribuito a un utente in formato binario eseguibile, che il codice sorgente venga messo a disposizione anche degli altri utenti. Per qualsiasi di tale software che sia distribuito insieme a questo prodotto Sophos, è possibile ottenere il codice sorgente tramite ordine postale inviandone richiesta a Sophos.

E-mail: savlinuxgpl@sophos.com

Indirizzo: Sophos Plc, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Regno Unito.

Copia dei termini della GPL è reperibile all'indirizzo www.gnu.org/copyleft/gpl.html

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.com or via the web at <http://www.sophos.com/support/queries/enterprise.html>. A copy of the license agreement for any such included software can be found at <http://opensource.org/licenses/cpl1.0.php>

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.

If you have any suggestions, additions, comments, or questions, please let me²² know.

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/>

iMatix SFL

This product uses parts of the iMatix SFL, Copyright © 1991-2000 iMatix Corporation
<<http://www.imatix.com>>.