

Sophos Endpoint Security and Control

Guida di avvio per computer autonomi

Sophos Endpoint Security and Control per Windows, versione 10.0
Sophos Anti-Virus per Mac OS X, versione 7

Data documento: dicembre 2011



Sommario

- 1 Prima di cominciare.....3
- 2 Protezione dei computer Windows.....4
- 3 Protezione dei computer Mac OS X.....9
- 4 Supporto tecnico.....11
- 5 Note legali.....12

1 Prima di cominciare

1.1 Requisiti di sistema

Per informazioni relative ai requisiti di sistema, consultare la pagina corrispondente 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.

1.2 Informazioni necessarie

Per effettuare l'installazione e la configurazione sono necessarie le seguenti informazioni:

- Indirizzo web e credenziali per il download del programma di installazione su computer autonomo di Sophos Endpoint Security and Control e/o Sophos Anti-Virus per Mac OS X, a seconda di quanto richiesto.
- Indirizzo della fonte degli aggiornamenti, a meno che non si desideri effettuare l'aggiornamento direttamente da Sophos.
- Credenziali richieste per accedere alla fonte degli aggiornamenti.
- Dati relativi al server proxy che verrà utilizzato per accedere alla fonte degli aggiornamenti (indirizzo, numero della porta e credenziali dell'utente).

2 Protezione dei computer Windows

2.1 Installazione di Sophos Endpoint Security and Control

Per poter eseguire l'installazione di Sophos Endpoint Security and Control, è necessario accedere come amministratore.

Se sul proprio computer è installato un software di sicurezza prodotto da terzi:

- Assicurarsi che la relativa interfaccia utente sia chiusa.
 - Assicurarsi che il firewall e il software HIPS prodotto da terzi siano disattivati o configurati per consentire l'esecuzione del programma di installazione Sophos.
1. Utilizzando l'indirizzo web e le credenziali per il download fornite da Sophos o dal proprio amministratore di sistema, andare sul sito web di Sophos e scaricare il programma di installazione per computer autonomi relativo alla propria versione di Windows.
 2. Individuare il programma di installazione nella cartella in cui lo si è scaricato. Cliccare due volte sul programma di installazione. Nella finestra del programma di installazione, cliccare su **Installa** per avviare la procedura guidata di installazione.
 3. Nella prima pagina della **procedura guidata di installazione di Sophos Endpoint Security and Control**, cliccare su **Avanti**.
 4. Nella pagina **Contratto di licenza**, cliccare su **Accetto i termini del contratto di licenza** se si accettano i termini e si desidera continuare. Cliccare su **Avanti**.
 5. Nella pagina **Cartella di destinazione**, è possibile cambiare la cartella in cui Sophos Endpoint Security and Control verrà installato. Cliccare su **Avanti**.
 6. Nella pagina **Fonte degli aggiornamenti**, inserire il percorso dal quale il computer riceverà gli aggiornamenti. Sophos consiglia di inserire i dati subito.
 - a) Nella casella **Indirizzo**, selezionare **Sophos** oppure, se l'amministratore di sistema ha fornito un indirizzo specifico, inserire tale indirizzo.
 - b) Nelle caselle **Nome utente** e **Password**, inserire il nome utente e la password necessari per accedere alla fonte degli aggiornamenti fornita da Sophos o dall'amministratore di sistema.
 - c) Se si accede alla rete o ad Internet tramite proxy, selezionare la casella **Accesso alla fonte degli aggiornamenti tramite proxy**, cliccare poi su **Avanti** per inserire i dati del server proxy.

Nota: per inserire la fonte degli aggiornamenti in un secondo tempo, selezionare la casella **Inserirò questi dati in un secondo momento**. Una volta portata a termine la procedura di installazione, aprire Sophos Endpoint Security and Control e selezionare **Configura AutoUpdate**.

Per impostazione predefinita, Sophos Endpoint Security and Control si aggiornerà ogni 60 minuti, posto che vengano forniti i dati relativi alla fonte degli aggiornamenti e che il computer sia connesso alla rete.

7. Nella pagina **Seleziona componenti aggiuntivi da installare**, selezionare la casella **Installa Sophos Client Firewall**, se si desidera installare il firewall, quindi cliccare su **Avanti**.

8. Nella pagina **Rimuovi il software di sicurezza di terze parti**, selezionare la casella **Rimuovi il software di sicurezza di terze parti**, se in possesso di un software antivirus o firewall prodotto da terzi, quindi cliccare su **Avanti**.
9. Nella pagina **Pronta per l'installazione di Sophos Endpoint Security and Control**, cliccare su **Avanti**.

Il software viene così installato nel computer.

Importante: per impostazione predefinita, non vengono rimossi i tool di aggiornamento associati al software di sicurezza in quanto potrebbero essere ancora utilizzati da quest'ultimo. Tuttavia, se non sono utilizzati, è possibile rimuoverli tramite il Pannello di controllo.

10. Nell'ultima pagina della procedura guidata di installazione, scegliere se riavviare il computer e cliccare su **Fine**.

È necessario riavviare il computer per:



- Abilitare il firewall
- Completare la rimozione di software di sicurezza prodotti da terze parti.

L'installazione di Sophos Endpoint Security and Control risulta completata quando nel lato destro dell'area di notifica viene visualizzata l'icona di Sophos Endpoint Security and Control.



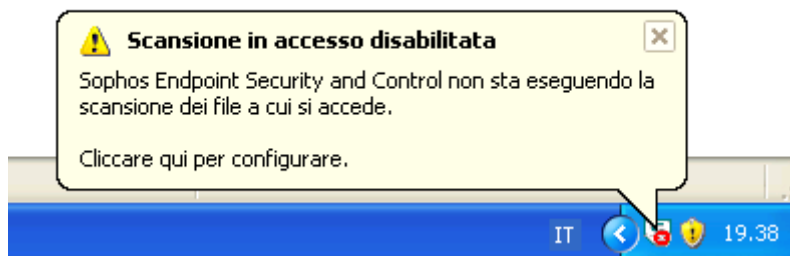
2.1.1 Significato delle icone dell'area di notifica

Le icone dell'area di notifica di Sophos Endpoint Security and Control cambiano nel caso in cui vengano rilevati allarmi in sospeso o si sia verificato un problema relativo alla protezione dalle minacce. La seguente tabella mostra le icone visualizzate nell'area di notifica ed indica la ragione per cui vengono visualizzate.

Icona	Motivo
	<ul style="list-style-type: none"> ■ Quando nel computer non è in esecuzione la scansione in accesso. ■ Quando viene visualizzato un messaggio del firewall. ■ Quando viene visualizzato un messaggio relativo a un'applicazione controllata. ■ Quando viene visualizzato un messaggio relativo al controllo dispositivi. ■ Quando viene visualizzato un messaggio relativo al controllo dati. ■ Quando un sito web è bloccato.
	<ul style="list-style-type: none"> ■ Quando Sophos Endpoint Security and Control non riesce ad autoaggiornarsi. ■ Quando un servizio Sophos non riesce.

Insieme alle icone sopra citate viene visualizzato un fumetto che ne spiega la causa.

Per esempio, se nel computer non è abilitata la scansione in accesso, nell'area di notifica viene visualizzato il fumetto **Scansione in accesso disabilitata** come mostrato di seguito:



2.2 Configurazione del firewall

È necessario configurare il firewall per:

- Gestire i messaggi del firewall
- Consentire ai programmi utilizzati accesso alla rete o a Internet
- Bloccare programmi sconosciuti.

2.2.1 Gestione dei messaggi del firewall

Per impostazione predefinita il firewall è in modalità "interattiva", ciò significa che viene visualizzato un messaggio ogni qual volta venga rilevata un'applicazione o un processo non autorizzati. In entrambi i casi è possibile bloccare o consentire l'attività.

All'inizio bloccare momentaneamente il traffico sconosciuto. Per esempio, se il firewall visualizza un messaggio riguardante un processo nascosto, cliccare su **Blocca il processo questa volta** e successivamente su **OK**.

Se non si riesce a bloccare il traffico in questa specifica occasione, è possibile che l'applicazione che ha generato il traffico non sia stata identificata. In tal caso, scegliere **consenti** o **blocca**, a seconda del caso. È possibile cambiare in seguito modificando la configurazione del firewall. Per ulteriori informazioni, consultare la guida in linea di Sophos Endpoint Security and Control.

In alcuni casi specifici, si consiglia di non bloccare il traffico. Tra questi rientrano i messaggi relativi a checksum e regole delle applicazioni che si riferiscono al proprio browser, al programma di posta e ad altri programmi che devono poter accedere alla rete o a internet.

2.2.2 Consentire ai propri programmi accesso alla rete o ad internet

È necessario abilitare il firewall affinché conceda accesso alla rete ai programmi desiderati.

1. Aprire il programma a cui si desidera concedere accesso alla rete, quale ad esempio un programma browser o di posta elettronica.
2. Il firewall visualizza un messaggio che informa che un'applicazione nuova o modificata ha richiesto l'accesso alla rete. Cliccare su **Aggiungi il checksum a quelli esistenti per questa applicazione** e successivamente su **OK**.
3. Il firewall visualizza un secondo messaggio che informa che un'applicazione (quale programma browser o di posta elettronica) ha richiesto l'accesso alla rete. Cliccare su **Crea regola con le impostazioni predefinite** e accertarsi di avere selezionato nella finestra di dialogo l'impostazione appropriata per il programma (quale **Browser**, **Client e-mail**); quindi cliccare su **OK**.

È inoltre possibile modificare la configurazione firewall per consentire ai programmi accesso alla rete o ad internet in qualsiasi modalità. Per ulteriori informazioni, consultare la guida in linea di Sophos Endpoint Security and Control.

2.2.3 Consentire ad altri programmi accesso alla rete o ad internet

Può essere necessario consentire l'accesso alla rete o a Internet ad altri programmi, per esempio Windows Update. Per fare ciò, utilizzare la modalità interattiva e seguire la stessa procedura descritta nella sezione [Consentire ai propri programmi accesso alla rete o ad internet](#) a pagina 7.

Per abilitare il download di FTP, consultare la Guida in linea di Sophos Endpoint Security and Control.

2.2.4 Blocco di programmi sconosciuti

Abilitare a questo punto il firewall per gestire il traffico automaticamente e bloccare i programmi sconosciuti.

1. Per visualizzare il menu, cliccare col tasto destro del mouse sull'icona di Sophos Endpoint Security and Control nell'area di notifica. Selezionare **Apri Sophos Endpoint Security and Control**.
2. Nella finestra di **Sophos Endpoint Security and Control**, nella sezione **Firewall**, cliccare su **Configura firewall**.

Viene visualizzata la finestra di dialogo **Configurazione Firewall**.

3. Nella scheda **Generale**, sotto **Configurazione**, cliccare su **Configura**.
4. Nella finestra di dialogo di configurazione del percorso, nella sezione **Modalità di lavoro**, selezionare **Blocca per impostazione predefinita - tutto il traffico che non corrisponde ad alcuna regola viene bloccato**.

Da ora in avanti, il firewall non visualizzerà alcun messaggio quando rileva traffico sconosciuto. Tale traffico verrà invece registrato nel file di log del firewall stesso. Per abilitare i fumetti di notifica quando il firewall rileva traffico non autorizzato, è necessario modificare la configurazione del firewall. Per ulteriori informazioni, consultare la Guida in linea di Sophos Endpoint Security and Control.

Nota: talvolta può essere necessario tornare alla modalità interattiva, per esempio nel caso si desideri utilizzare Windows Update. Dopo avere utilizzato il programma desiderato, Sophos consiglia di tornare alla modalità non interattiva.

3 Protezione dei computer Mac OS X

3.1 Installazione di Sophos Anti-Virus

Prima di installare Sophos Anti-Virus è necessario disinstallare eventuali software antivirus di terze parti.

Per prima cosa accedere come amministratore.

1. Utilizzando l'indirizzo web e le credenziali per il download fornite dal proprio amministratore di sistema, andare sul sito web di Sophos e scaricare il programma di installazione di Sophos Anti-Virus per Mac OS X per computer autonomi.
2. Individuare l'immagine del disco di installazione nella cartella in cui lo si è scaricato. Cliccare sull'immagine del disco. Cercare Sophos-Anti-Virus.mpkg e cliccarvi due volte per dare inizio al programma di installazione.
3. Cliccare su **Continua**. Seguire la procedura fino al termine dell'installazione.

L'installazione di Sophos Anti-Virus risulta completata quando l'icona di Sophos Anti-Virus, nel lato destro della barra dei menu, è di colore nero.



Se l'icona è grigia, significa che la scansione in accesso non è attiva e che il Mac non è protetto in accesso dalle minacce. Per assistenza, contattare l'amministratore di sistema.

3.2 Configurazione di Sophos Anti-Virus per l'aggiornamento

Assicurarsi di essersi connessi come amministratori.

1. Cliccare sull'icona Sophos Anti-Virus nel lato destro della barra dei menu e scegliere **Open Preferences** dal menu.
2. Cliccare su **AutoUpdate**.
3. Se qualche opzione non è disponibile, cliccare sull'icona del lucchetto e immettere nome e password dell'amministratore.

4. Cambiare le preferenze secondo quanto descritto di seguito:

- Per consentire a Sophos Anti-Virus di aggiornarsi direttamente da Sophos, selezionare **Sophos** dal menu di scelta rapida **Update from primary location**. Nei campi **Username** e **Password**, inserire le credenziali per l'aggiornamento fornite da Sophos.
- Per consentire a Sophos Anti-Virus di aggiornarsi dal server web aziendale, scegliere **Company web server** dal menu di scelta rapida **Update from primary location**. Nel campo **Address** inserire il percorso dal quale gli aggiornamenti verranno scaricati. Nei campi **User Name** e **Password**, inserire le credenziali per l'aggiornamento necessarie per accedere al server.
- Per consentire a Sophos Anti-Virus di aggiornarsi dal volume di rete, scegliere **Network Volume** dal menu di scelta rapida **Update from primary location**. Nel campo **Address** inserire il percorso dal quale gli aggiornamenti verranno scaricati. Nei campi **User Name** e **Password**, inserire le credenziali per l'aggiornamento necessarie per accedere al volume.

Seguono esempi di indirizzo. Sostituire il testo tra parentesi con i nomi appropriati:

http://<server>/<condivisione web>/Sophos Anti-Virus/ESCOSX

smb://<server>/<condivisione Samba>/Sophos Anti-Virus/ESCOSX

afp://<server>/<condivisione AppleShare>/Sophos Anti-Virus/ESCOSX

È possibile utilizzare un indirizzo IP o un nome NetBIOS, invece un dominio oppure il nome dell'host che riferirsi al server. Si consiglia l'utilizzo di un indirizzo IP, nel caso in cui vengano rilevati problemi di DNS.

5. Per abilitare l'aggiornamento di Sophos Anti-Virus utilizzando il proxy configurato nelle Impostazioni di Sistema, selezionare **Use system proxy settings** dal menu di scelta rapida nella parte inferiore della sezione del **percorso primario**.
6. Per abilitare l'aggiornamento di Sophos Anti-Virus tramite un proxy di cui si desidera specificare le impostazioni:
 - a) Selezionare **Use custom proxy settings** nel menu di scelta rapida in fondo della sezione **Primary location**.
 - b) Nella finestra di dialogo che viene visualizzata, digitare l'indirizzo del server proxy e il numero di porta nei campi **Address**. Nei campi **User Name** e **Password**, inserire le credenziali necessarie per accedere al server proxy.

7. Selezionare **Check for updates on connection to network or internet**.

Sophos Anti-Virus si aggiornerà automaticamente dalla fonte specificata. Per impostazione predefinita ciò avrà luogo ogni 60 minuti, posto che il computer sia connesso alla rete. Se compare una croce bianca sull'icona di Sophos Anti-Virus nel lato destro della barra dei menu, Sophos Anti-Virus non è riuscito ad autoaggiornarsi. Per assistenza, contattare l'amministratore di sistema.

4 Supporto tecnico

È possibile ricevere supporto tecnico per i prodotti Sophos in uno dei seguenti modi:

- Visitando la community SophosTalk su <http://community.sophos.com/> e cercando altri utenti con lo stesso problema.
- Visitando la knowledge base del supporto Sophos su <http://www.sophos.it/support/>.
- Scaricando la documentazione del prodotto su <http://www.sophos.it/support/docs/>.
- Inviando un'e-mail a support@sophos.com, indicando il o i numeri di versione del software Sophos in vostro possesso, i sistemi operativi e relativi livelli di patch, ed il testo di ogni messaggio di errore.

5 Note legali

Copyright © 2011 Sophos Limited. 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 Limited. Tutti gli altri nomi citati di società e prodotti sono marchi o marchi registrati dei rispettivi titolari.

Common Public License

Il software Sophos descritto in questo documento comprende o può comprendere programmi di software concessi in licenza (o sottolicensing) all'utente secondo i termini della Common Public License (CPL), la quale, tra gli altri diritti, permette all'utente di avere accesso al codice sorgente. La CPL richiede, per qualsiasi software concesso in licenza secondo i termini della stessa, e distribuito in formato codice oggetto, che il codice sorgente di tale software venga messo a disposizione anche degli altri utenti del formato codice oggetto. Per qualsiasi software che rientri nei termini della CPL, il codice sorgente è disponibile tramite ordine postale inviandone richiesta a Sophos; per e-mail a support@sophos.com o tramite internet su <http://www.sophos.it/support/queries/enterprise.html>. Una copia dei termini per tali software è reperibile all'indirizzo <http://opensource.org/licenses/cpl1.0.php>

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

iMatix SFL

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