

SOPHOS

simple + secure

Sophos Endpoint Security and Control 9.7

Guida di avvio rapido

Data documento: aprile 2011



Sommario

1	Informazioni sulla guida.....	3
2	Cosa installare.....	3
3	Passaggi chiave.....	3
4	Verifica dei requisiti di sistema.....	4
5	Preparazione all'installazione.....	4
6	Download dei programmi di installazione.....	5
7	Installazione di Enterprise Console	5
8	Download del software di sicurezza.....	6
9	Installazione di NAC Manager	6
10	Creazione di gruppi di computer.....	6
11	Impostazione dei criteri di sicurezza.....	7
12	Ricerca dei computer.....	8
13	Protezione dei computer.....	8
14	Verifica dello stato della rete.....	10
15	Troubleshooting.....	10
16	Aiuto per lo svolgimento di operazioni comuni.....	10
17	Supporto tecnico.....	11
18	Note legali.....	12

1 Informazioni sulla guida

Questa guida spiega come proteggere la propria rete con il software di sicurezza Sophos.

Leggere questa guida, se si installa il software Sophos per la prima volta.

Se si sta effettuando un upgrade, visitare il **Centro Upgrade di Endpoint Security and Control** su <http://www.sophos.it/support/upgrades/>

Nota: se in possesso di una rete molto estesa, può essere utile prendere in considerazione le opzioni di installazione descritte nella *Guida di avvio avanzata di Sophos Endpoint Security and Control*.

2 Cosa installare

Installare due tool di gestione:

- **Sophos Enterprise Console.** Consente di installare e gestire il software di sicurezza sui propri computer.
- **Sophos NAC Manager.** Consente di utilizzare il “controllo di accesso alla rete”, che impedisce l'accesso da parte di computer non autorizzati o non conformi agli standard di sicurezza.

L'installazione di NAC Manager è opzionale.

Nota: installare i tool individualmente utilizzando i due rispettivi programmi di installazione.

Nota: è possibile installare entrambi i tool nello stesso server. Tuttavia, se si possiedono più di 1000 computer, si consiglia di installare i tool su server separati. La procedura è la stessa.

3 Passaggi chiave

Svolgere i seguenti passaggi chiave:

- Verificare i requisiti di sistema
- Prepararsi all'installazione
- Scaricare i programmi di installazione
- Installare Enterprise Console
- Scaricare il software di sicurezza
- Installare NAC Manager
- Creare i gruppi di computer
- Impostare i criteri di sicurezza
- Ricercare i computer
- Proteggere i computer
- Verificare lo stato della rete

4 Verifica dei requisiti di sistema

Verificare hardware, sistema operativo e requisiti del software di sistema prima di cominciare l'installazione.

4.1 Hardware e sistema operativo

Per i requisiti di hardware e sistema operativo, consultare la pagina corrispondente del sito web di Sophos (<http://www.sophos.it/products/all-sysreqs.html>).

4.2 Software di sistema Microsoft

Enterprise Console richiede un software di sistema Microsoft specifico (ad esempio, software database).

Il programma di installazione di Enterprise Console cerca di installare tale software di sistema, se non già a disposizione nel server. In alcuni casi però, il software non è compatibile con il server o deve essere installato manualmente.

Installazione del server SQL

Il programma di installazione tenterà di installare SQL Server 2008 Express, a meno che non si sia già in possesso di SQL Server 2005 Express o versioni successive. Notare che:

- Si raccomanda di non installare SQL Server 2008 su un controller di dominio.
- SQL Server 2008 Express non è compatibile con Windows Server 2003 SP1, Windows XP a 64 bit SP1, o Windows Essential Business Server 2008.
- Con Windows Server 2008 R2 Datacenter, è necessario aumentare il livello di funzionalità del dominio a Windows Server 2003, come descritto nella pagina web <http://support.microsoft.com/kb/322692>

Installazione di .NET Framework

Il programma di installazione cerca di installare .NET Framework 3.5, a meno che non sia già stato installato. Notare che:

- Il programma di installazione non può installare .NET Framework 3.5 su un computer che utilizza Windows Server 2008 R2. Deve essere aggiunto dalla sezione Funzioni del Server Manager.

Nota: dopo l'installazione del software di sistema richiesto potrebbe essere necessario riavviare il computer. Per ulteriori informazioni, consultare l'articolo 65190 in inglese della knowledge base del supporto Sophos (<http://www.sophos.com/support/knowledgebase/article/65190.html>).

5 Preparazione all'installazione

Selezionare un server che soddisfi i requisiti di sistema e procedere come indicato qui di seguito:

- Assicurarsi di essere collegati ad Internet.
- Assicurarsi di essere in possesso dei CD di Service Pack e del sistema operativo Windows. Potrebbero essere richiesti durante l'installazione.

- Se il server esegue Windows Server 2008 o successivo, disattivare lo User Account Control (UAC) e riavviare il server.

Nota: è possibile riattivare lo UAC dopo aver completato l'installazione e dopo aver eseguito il download del software di sicurezza.

6 Download dei programmi di installazione

Scaricare i programmi di installazione Sophos sul server in cui si intende installare i tool di gestione:

1. Visitare la pagina web <http://www.sophos.it/support/updates/>.
2. Digitare il proprio nome utente e password MySophos.
3. Nella pagina relativa ai download di **Enterprise**:
 - Scaricare il programma di installazione di Enterprise Console.
 - Se si desidera utilizzare NAC Manager, scaricare il programma di installazione di Sophos NAC.
4. Se necessario, copiare i programmi di installazione scaricati nel server in cui si desidera eseguire l'installazione.

Se si desidera installare NAC Manager in un server diverso da quello di Enterprise Console, copiare il programma di installazione su tale server.

7 Installazione di Enterprise Console

Per installare Enterprise Console:

1. Nel computer dove si desidera installare Enterprise Console, accedere come amministratore:
 - Se il computer si trova in un dominio, accedere come amministratore di dominio.
 - Se il computer si trova in un gruppo di lavoro, accedere come amministratore locale.
2. Trovare il programma di installazione di Enterprise Console scaricato in precedenza.

Suggerimento: il nome del programma di installazione contiene l'adicitura "sec".
3. Cliccare due volte sul programma di installazione.
4. Nella finestra di dialogo **Programma di installazione in rete di Sophos Endpoint Security and Control**, cliccare su **Installa**.

I file di installazione vengono copiati sul computer, ed è avviata la procedura guidata per l'installazione.
5. Nella finestra di dialogo **Sophos Enterprise Console**, cliccare su **Avanti**.
6. Una procedura guidata accompagna nei passaggi dell'installazione. È necessario procedere come segue:
 - a) Accettare le impostazioni predefinite dove possibile.
 - b) Selezionare un'installazione **Completa**.
7. Al termine dell'installazione, potrebbe essere necessario il riavvio. Cliccare su **Sì** o su **Fine**.

8 Download del software di sicurezza

Quando si riaccende o si riavvia la console per la prima volta dopo l'installazione, Enterprise Console si apre automaticamente e ha inizio una procedura guidata.

Nota: se per l'installazione si è utilizzato Remote Desktop, la console non si aprirà automaticamente. Aprirla dal menu Start.

La procedura guidata accompagna nella scelta e nel download del software di sicurezza. È necessario procedere come segue:

1. Nella pagina **Dettagli dell'account di download di Sophos**, inserire il nome utente e la password stampati nell'allegato alla licenza. Se si accede a Internet tramite server proxy, selezionare la casella di spunta **Accedi a Sophos tramite server proxy**.
2. Nella pagina **Selezione piattaforma**, selezionare solo le piattaforme che si desidera proteggere subito.

Quando si clicca su **Avanti**, Enterprise Console comincia a scaricare il software.

3. Nella pagina **Download del software**, viene visualizzato l'avanzamento del download. Cliccare su **Avanti** in qualsiasi momento.
4. Nella pagina **Importa computer da Active Directory**, selezionare **Imposta gruppi per i computer**, se si desidera che Enterprise Console utilizzi i gruppi esistenti di Active Directory.

Se, prima di eseguire l'installazione, si è disattivato lo User Account Control è possibile riattivarlo.

9 Installazione di NAC Manager

Assicurarsi di essere in possesso dei CD di Service Pack e del sistema operativo Windows. Potrebbero essere richiesti durante l'installazione.

Nota: se si installa NAC Manager in un server diverso da Enterprise Console, per prima cosa è necessario eseguire l'installazione manuale del database di SQL Server 2005 o successivo.

1. Sul computer dove si desidera installare NAC Manager, accedere come amministratore:
 - Se il computer si trova in un dominio, accedere come amministratore di dominio.
 - Se il computer si trova in un gruppo di lavoro, accedere come amministratore locale.

2. Trovare il programma di installazione di Sophos NAC, scaricato in precedenza.

Suggerimento: il nome del programma di installazione contiene la dicitura "nac".

3. Cliccare due volte sul programma di installazione.
4. Nella finestra di dialogo di **Sophos NAC Manager**, cliccare su **Install**.
5. Una procedura guidata accompagna nei passaggi dell'installazione.

10 Creazione di gruppi di computer

Se, per configurare i gruppi di computer (basati sui gruppi di Active Directory), è stata utilizzata la **procedura guidata di download del software di sicurezza**, saltare questa sezione. Andare direttamente alla sezione [Impostazione dei criteri di sicurezza](#) a pagina 7.

Prima di proteggere e gestire i computer, è necessario organizzarli in gruppi.

1. Aprire Enterprise Console, se non ancora aperta.
2. Nel riquadro **Gruppi** (nella parte sinistra della console), assicurarsi che il nome del server visualizzato in alto sia selezionato.
3. Cliccare sull'icona **Crea gruppo** posta sulla barra degli strumenti.
Un "Nuovo Gruppo" viene aggiunto alla lista, con il nome evidenziato.
4. Digitare il nome del gruppo.

Per creare ulteriori gruppi, andare nel riquadro di sinistra. Selezionare il server visualizzato in alto per creare un altro gruppo al livello più alto. Selezionare invece un gruppo per creare al suo interno un sottogruppo. Creare e scegliere il nome per tale sottogruppo seguendo la procedura svolta in precedenza.

11 Impostazione dei criteri di sicurezza

Enterprise Console applica criteri di sicurezza "predefiniti" ai gruppi di computer. Non è necessario modificare tali criteri se non lo si desidera, fatta eccezione per i casi in cui:

- Si deve impostare subito un criterio firewall.
- Si devono modificare i criteri di accesso alla rete, controllo applicazioni, controllo dati o controllo dispositivi, per poter utilizzare tali funzioni. Questa operazione può essere svolta in qualsiasi momento.

11.1 Impostazione di un criterio del firewall

Nota: durante l'installazione del firewall, si verificherà una temporanea interruzione della connessione delle schede di rete. Tale interruzione può provocare la sconnessione di applicazioni di rete quali Remote Desktop.

Per impostazione predefinita, il firewall blocca tutte le applicazioni non essenziali. È quindi necessario configurare il firewall prima di proteggere i computer.

1. Nel riquadro **Criteri**, cliccare due volte su **Firewall**.
2. Cliccare due volte sul criterio **Predefinito** per modificarlo. Viene avviata una procedura guidata.
3. Nella **procedura guidata di configurazione dei criteri del Firewall** si consiglia di selezionare quanto elencato qui di seguito.
 - a) Nella pagina **Configura firewall**, selezionare **Percorso singolo**, a meno che non si desideri che il firewall utilizzi impostazioni diverse a seconda del percorso in cui lo si utilizza.
 - b) Nella pagina **Modalità operativa**, selezionare **Blocca il traffico in ingresso e consenti il traffico in uscita**.
 - c) Nella pagina **Condivisione file e stampanti**, selezionare **Consenti condivisione file e stampanti**.

12 Ricerca dei computer

Affinché Enterprise Console possa proteggere e gestire i computer in rete, è necessario innanzitutto localizzarli.

1. Cliccare sull'icona **Cerca nuovi computer** nella barra degli strumenti.
2. Selezionare il metodo che si desidera utilizzare per cercare i computer.
3. Inserire i dati relativi all'account e, se necessario, indicare dove si desidera effettuare la ricerca.

Se si utilizza una delle opzioni **Cerca**, i computer vengono posizionati nella cartella **Nessun gruppo**.

13 Protezione dei computer

Per proteggere i computer, occorre:

- Preparare i computer
- Proteggere i computer Windows automaticamente.
- Proteggere i computer Windows o Mac OS X manualmente.

13.1 Preparazione della protezione dei computer

Prima di proteggere i computer, fare quanto segue:

Prepararsi alla rimozione del software di sicurezza di terze parti

Se si desidera che il programma di installazione di Sophos rimuova tutti i software di sicurezza precedentemente installati, svolgere le seguenti operazioni:

- Se i computer utilizzano un software antivirus di altro produttore, assicurarsi che la relativa interfaccia utente sia chiusa.
- Se i computer eseguono un prodotto firewall o HIPS di terzi, accertarsi che sia disattivato o configurato per consentire l'esecuzione del programma di installazione di Sophos.

Se i computer eseguono un tool di aggiornamento di terzi, sarà necessario rimuoverlo. Leggere il paragrafo "Rimozione del software di sicurezza prodotto da terzi", nella sezione "Protezione dei computer" della Guida in linea di Enterprise Console.

Verifica del possesso di un account utilizzabile per l'installazione di software

Verrà richiesto di inserire dati relativi a un account che possa essere utilizzato per l'installazione del software di sicurezza. Si tratta solitamente dell'account di un amministratore di dominio. Deve:

- Avere diritti di amministratore locale sui computer che si desidera proteggere.
- Essere in grado di aprire una sessione sul computer nel quale è stata installata Enterprise Console

- Avere accesso in lettura al percorso posizione dalla quale i computer si aggiorneranno. Per verificarlo, nel riquadro **Criteri**, cliccare due volte su **Aggiornamento**, quindi due volte su **Predefinito**.

Preparazione dell'installazione del controllo di accesso alla rete

Prima di poter installare il controllo di accesso alla rete nei computer, è necessario:

- Specificare l'URL del computer su cui è stato installato NAC Manager. In Enterprise Console, selezionare **Strumenti > Configura URL NAC**.

13.2 Protezione automatica dei computer Windows

Per proteggere i computer, fare quanto descritto di seguito:

1. Selezionare i computer che si desidera proteggere.
2. Cliccare con il tasto destro del mouse e selezionare **Proteggi computer**.

Nota: se i computer si trovano nel gruppo **Nessun gruppo**, basta semplicemente trascinarli nel gruppo prescelto.

3. Una procedura guidata accompagna nei passaggi dell'installazione. È necessario procedere come segue:
 - a) Sulla pagina **Seleziona funzioni** è possibile installare funzioni opzionali. Selezionare **Compliance Control** se si desidera il controllo di accesso alla rete.
 - b) Sulla pagina **Riepilogo protezione** verificare eventuali problemi di installazione. Per ulteriore assistenza, consultare la sezione [Troubleshooting](#) a pagina 10.
 - c) Nella pagina **Credenziali**, inserire i dati di un account utilizzabile per installare il software.

L'installazione avviene in più fasi, quindi il processo potrebbe richiedere del tempo per essere completato su tutti i computer.

Al termine dell'installazione, osservare nuovamente l'elenco dei computer. Nella colonna **In accesso**, la parola **Attivo/a** indica che sul computer è in esecuzione la scansione dei virus in accesso.

13.3 Protezione manuale dei computer Windows o Mac OS X

Se in possesso di computer che non possono essere protetti automaticamente, proteggerli eseguendo il programma di installazione dalla directory centrale.

Per sapere in quale directory si trova il programma di installazione, aprire Enterprise Console e selezionare **Visualizza > Percorsi Bootstrap**.

1. Accedere a ciascun computer con diritti di amministratore locale.

2. Posizionare il programma di installazione nella directory centrale e cliccarvi sopra due volte.
 - Per i computer Windows, il programma è denominato setup.exe.
 - Per i computer Mac OS X, il programma è denominato Sophos Anti-Virus.mpkg
3. Una procedura guidata accompagna nei passaggi dell'installazione.

14 Verifica dello stato della rete

Per verificare lo stato della rete da Enterprise Console, fare quanto segue.

1. Nella barra dei menu, cliccare sull'icona **Pannello di controllo** (se il Pannello di controllo non è già visualizzato).

Il Pannello di controllo mostra quanti computer:

- Presentano minacce
 - Non sono aggiornati
 - Non sono conformi ai criteri
2. Se si utilizza NAC, è inoltre possibile:
 - a) Selezionare **File > Apri > NAC** .
 - b) In NAC Manager, selezionare **Report > Compliance** .Ciò mostra se i computer sono conformi al criterio NAC.

15 Troubleshooting

Quando si esegue la procedura guidata per la Protezione dei computer, l'installazione del software di sicurezza può non riuscire per diversi motivi:

- L'installazione automatica non è attuabile nel sistema operativo in questione. Eseguire l'installazione manualmente. Consultare la sezione [Protezione manuale dei computer Windows o Mac OS X](#) a pagina 9. Per altri sistemi operativi, consultare la *Guida di avvio avanzata di Sophos Endpoint Security and Control*.
- È stato impossibile determinare il sistema operativo. Ciò può essere dovuto al fatto che, durante la ricerca dei computer, il nome utente non è stato inserito nel formato dominio\nome utente.
- I computer eseguono il firewall.

16 Aiuto per lo svolgimento di operazioni comuni

Questa sezione indica dove reperire informazioni relative allo svolgimento di operazioni comuni.

SESC = Sophos Endpoint Security and Control

Operazione	Documento
Protezione dei computer Linux	Guida di avvio di SESC 9.7 per Linux, NetWare e UNIX: "Protezione dei computer con sistema operativo Linux"
Protezione dei computer autonomi	Guida di avvio avanzata di SESC 9.7: "Protezione dei computer autonomi"
Configurazione di antivirus e HIPS	Enterprise Console Guida in linea: "Configurazione dei criteri antivirus e HIPS"
Configurazione del controllo applicazioni	Enterprise Console Guida in linea: "Configurazione del criterio del controllo applicazioni"
Configurazione del controllo dati	Enterprise Console Guida in linea: "Configurazione del criterio del controllo dati"
Configurazione del controllo dispositivi	Enterprise Console Guida in linea: "Configurazione del criterio del controllo dispositivi"
Configurazione del blocco rimozione	Enterprise Console Guida in linea: "Configurazione del criterio del blocco rimozione"
Configurazione di NAC	NAC Manager Guida in linea: "Panoramica dell'area Manage"
Concessione dell'accesso alla rete a utenti ospiti	Guida alla configurazione di Sophos Compliance Agent: "Dissolvable Agent"
Gestione allarmi	Enterprise Console Guida in linea: "Come gestire computer con allarmi ed errori"
Disinfezione dei computer	Enterprise Console Guida in linea: "Disinfezione dei computer"
Creazione di report di SEC	Enterprise Console Guida in linea: "Creazione dei report"
Creazione di report di NAC	NAC Manager Guida in linea: "Panoramica dell'area Report"

17 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.com/support/>.
- Scaricando la documentazione del prodotto su <http://www.sophos.com/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.

18 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.

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

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

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

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