

Sophos Compliance Agent Guida alla configurazione

Versione prodotto: 3.9

Data documento: dicembre 2011



Sommario

- 1 Informazioni sulla guida.....3
- 2 Quarantine Agent.....4
- 3 Dissolvable Agent.....10
- 4 Lingue dell'agente.....13
- 5 Supporto tecnico.....14
- 6 Note legali.....15

1 Informazioni sulla guida

Questa guida descrive la configurazione del Compliance Agent gestito da Sophos Enterprise Console. Nello specifico, fornisce informazioni relative a:

- Design, configurazione e impostazione del log per Compliance Agent e Compliance Dissolvable Agent.
- Componenti dell'interfaccia per ogni agente, quali finestre di dialogo.
- Lingue supportate dall'agente.

Questa guida sarà utile se:

- Si utilizza Sophos Enterprise Console.
- Si sta utilizzando la versione di Sophos NAC integrata con Enterprise Console.
- Si desiderano informazioni sulle modalità di progettazione di Compliance Agent e Compliance Dissolvable Agent.
- Si desidera conoscere quali componenti dell'interfaccia vengono visualizzati nei computer.

Prima di consultare questa guida, leggere la Guida di avvio rapido di *Sophos Enterprise Console*.

La documentazione Sophos è reperibile online su www.sophos.it/support/docs/.

1.1 Panoramica

Sophos Compliance Agent è un'applicazione configurabile che verifica e attua la conformità di un computer ai criteri di NAC. L'agente recupera il criterio di NAC, verifica la conformità del computer a tale criterio, può automaticamente correggere le applicazioni fornendo dei messaggi all'utente e crea dei report sullo stato del computer.

Sophos NAC supporta due configurazioni dell'agente. Le aziende possono installare Quarantine Agent nei computer che eseguono Microsoft Windows. Dissolvable Agent è invece progettato per gli utenti ospiti che utilizzano Microsoft Windows.

- **Quarantine Agent:** Quarantine Agent verifica la conformità dei computer al criterio di NAC. Le verifiche vengono svolte prima di e periodicamente dopo aver concesso l'accesso alla rete. L'agente richiede un'interazione dell'utente minima o nulla. Quarantine Agent possiede una funzione di quarantena che consente l'attuazione e limita l'accesso dei computer a specifiche aree della rete qualora non siano conformi al criterio di NAC.
- **Dissolvable Agent:** Dissolvable Agent verifica i computer in modo tale da stabilire se sono conformi al criterio di NAC prima di consentirne l'accesso alla rete. Dissolvable Agent deve venire eseguito da un browser. Dissolvable Agent è concepito per gli utenti che non hanno o non possono avere un agente installato nel computer, ma che devono poter accedere a specifiche risorse di rete in quanto collaboratori esterni o ospiti. Dissolvable Agent non ha funzioni di attuazione in sé, ma può essere utilizzato con l'attuazione di DHCP.

Per ulteriori informazioni relative all'attuazione di DHCP, consultare la *Guida alla configurazione di Sophos NAC DHCP*.

2 Quarantine Agent

Questa sezione contiene informazioni sulla concezione e la configurazione di Quarantine Agent.

2.1 Concezione

Quarantine Agent è un'applicazione dell'area di notifica installata nel computer e che svolge operazioni di elaborazione periodiche, secondo il criterio di NAC definito in NAC Manager. Per installare Quarantine Agent nel computer, sono necessari diritti di amministratore locale.

Impostazioni dell'agente

Quarantine Agent viene visualizzato graficamente da un'icona, che riporta il corrente stato operativo dell'agente. L'icona di Quarantine Agent cambia per indicare quando il computer si trova nello stato di quarantena, quando questo possiede un completo accesso alla rete, o quando sono presenti dei risultati in sospeso. Le impostazioni dell'agente, configurate nei modelli di configurazione di NAC Manager, sono utilizzabili per controllare le opzioni di visualizzazione e le funzioni dell'interfaccia. Dopo l'aggiunta del modello di configurazione dell'agente al criterio, gli agenti possono recuperare il criterio e implementare le impostazioni nel computer.

Operazioni di elaborazione

Quarantine Agent esegue un'iniziale verifica della conformità, quindi controlla periodicamente la conformità per assicurare che il computer rimanga conforme al criterio di NAC. Quarantine Agent esegue tutte le operazioni - recupero, verifica e attuazione dei criteri, correzione e reportistica - anche se una delle operazioni non riesce. Se un'operazione non riesce, viene automaticamente ritentata la volta successiva in cui è pianificata la sua esecuzione.

Accesso alla rete

All'utente viene assegnato l'accesso alla rete in base alla conformità o allo stato di accesso del computer e ai modelli di accesso alla rete associati, definiti anch'essi nel criterio. Per esempio, se il computer non è conforme, l'agente mette in quarantena il computer e l'accesso del computer alla rete può venire limitato secondo quanto definito nei modelli di accesso non-compliant. Se l'accesso è limitato, l'agente deve permettere agli utenti di eseguire le operazioni di correzione in modo da riottenere il pieno accesso alla rete, oltre a consentire l'accesso al server proxy, se utilizzato.

Accesso al server proxy

Se è necessaria l'autenticazione attraverso server proxy per consentire all'agente di comunicare col NAC Server, la finestra di dialogo Richiesta credenziali che si visualizza nel computer, prima di procedere al recupero del criterio, richiederà nome utente e password. Se il nome utente e la password di proxy sono stati salvati come impostazioni dell'agente in NAC Manager, quest'ultimo gestirà automaticamente la procedura di autenticazione dei computer senza dover richiedere nuovamente le credenziali dell'utente.

Verifiche di quarantena e conformità

Un computer rimane nello stato di quarantena finché non viene soddisfatta la conformità al criterio. Se consentito dal criterio di NAC, gli utenti possono ignorare lo stato di quarantena durante una sessione dell'agente. La quarantena viene ripristinata quando l'utente la riabilita

oppure si disconnette dal computer. Oltre alle verifiche della conformità continue, gli utenti possono verificare lo stato di conformità dei propri computer endpoint in qualsiasi momento, tramite l'opzione Verifica Conformità del menu associato all'icona di Quarantine Agent posta nell'area di notifica oppure tramite il pulsante Verifica Conformità nella finestra di dialogo Risultati.

Reportistica e messaggi

I dati del report includono informazioni sulle applicazioni del software installate o meno nel computer, lo stato di conformità del computer durante la verifica basata sul criterio di NAC e i messaggi visualizzati all'utente o le azioni eseguite sul computer stesso. Durante il funzionamento, Quarantine Agent visualizza all'utente i messaggi definiti nei profili di NAC Manager e gli errori verificatisi durante il funzionamento.

2.2 Configurazione

Per configurare Quarantine Agent, procedere come segue.

1. In NAC Manager, creare risorse di rete e applicarle ai modelli di accesso di Agent Enforcer utilizzate per i criteri relativi ai computer non conformi.

Le risorse di rete sono applicazioni o dispositivi necessari per la correzione dei computer o responsabili della negazione dell'accesso alla rete dei computer messi in quarantena. I modelli di accesso di Agent Enforcer vengono utilizzati congiuntamente al criterio per individuare le risorse di rete cui i computer possono o non possono accedere quando utilizzano Quarantine Agent per l'attuazione. Le risorse di rete devono essere a disposizione di un computer in quarantena ai fini della correzione, oltre che per dare accesso a un server proxy per la correzione, se utilizzato.

2. Distribuire Sophos Compliance Agent sui computer endpoint, utilizzando Sophos Enterprise Console.

Mediante la procedura guidata per la protezione dei computer di Sophos Enterprise Console, Quarantine Agent viene distribuito sui computer endpoint. Dopo la distribuzione, ogni computer recupera il proprio criterio assegnato e implementa le impostazioni in esso definite. Il criterio associato al gruppo di appartenenza del computer in Sophos Enterprise Console è quello recuperato dall'agente ed utilizzato per la verifica della conformità del computer stesso.

Per ulteriori informazioni sulle risorse di rete, sui modelli di accesso di Agent Enforcer, e sui criteri, consultare la Guida in linea di NAC Manager.

2.3 Registrazione nel log

Per la risoluzione dei problemi, Quarantine Agent supporta file di log multipli che vengono salvati nell'hard disk del computer.

L'installazione di Sophos Compliance Agent crea un log automaticamente. Se l'agente riscontra un errore durante l'installazione, o se questa non riesce, il log fornisce informazioni per la risoluzione del problema. Il log di installazione dell'agente si trova nella directory **%temp%**. A meno che la posizione della directory temp sia stata modificata dall'utente, è possibile accedere a quest'ultima aprendo Windows Explorer, digitando **%temp%** nel campo dell'indirizzo e premendo **Invio**.

In aggiunta a ciò, la registrazione nel log può essere utilizzata per la risoluzione di problemi relativi all'attività dell'agente sul computer in questione. La registrazione nel log incide sulle prestazioni di Quarantine Agent; si consiglia perciò di abilitarla esclusivamente per la risoluzione di un problema, e di disabilitarla a problema risolto. I file di log escludono i dati sensibili per l'utente e contengono livelli di informazione personalizzabili. La registrazione viene abilitata dalla finestra di dialogo About dell'agente, ed il suo livello è personalizzabile come impostazione dell'agente.

I tre file di log sono:

- **Session Log:** fornisce un alto livello di informazioni sull'errore.
 - **Trace Log:** fornisce informazioni dettagliate sull'errore.
 - **Agent Log:** fornisce informazioni sull'errore che riguardano l'applicazione dell'agente.
1. In NAC Manager, accedere alla pagina **Create Agent Configuration Template**.
 2. Aggiungere l'impostazione **Log** nel modello di configurazione dell'agente, quindi selezionare l'adeguato livello di registrazione.
Per ulteriori informazioni relative alle impostazioni dell'agente, consultare la Guida in linea di NAC Manager.
 3. Nel computer, aprire la finestra di dialogo **About** dell'agente e spuntare la casella **Abilita registrazione nel log**.
I file di log per Windows 2000 e Windows XP si trovano nella cartella <unità>:\Documents and Settings\All Users\Application Data\Sophos\Sophos Compliance Agent\Logs. I file di log per Windows Vista e Windows 7 si trovano nella cartella <unità>:\ProgramData\Sophos\Sophos Compliance Agent\Logs.
 4. A problema risolto, nel computer aprire la finestra di dialogo **About** dell'agente e deselezionare la casella **Abilita registrazione nel log**.

2.4 Icone, menu, fumetti con messaggi e finestre di dialogo

La seguente sezione fornisce informazioni su icone dell'area di notifica, descrizioni, opzioni di menu, fumetti e finestre di dialogo a disposizione in Quarantine Agent.

2.4.1 Icone dell'area di notifica e relative descrizioni

Le icone dell'area di notifica indicano lo stato corrente dell'agente nei modi seguenti:

- Le icone mostrano i vari stati dell'agente.
- Passando il puntatore sopra un'icona compare la descrizione associata.

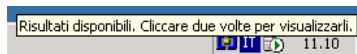





Figura 1: esempio di icona nell'area di notifica e sua descrizione

La seguente tabella fornisce informazioni sulle icone.

Icona	Testo visualizzato	Descrizione
	Risultati disponibili. Cliccare due volte per visualizzarli.	Sono presenti azioni in sospenso che vengono visualizzate nella finestra di dialogo Risultati.
	Sophos Compliance Agent - Inattivo. Computer in quarantena.	Icona che indica che l'agente è in stato di quarantena.
	Sophos Compliance Agent - Inattivo.	Icona visualizzata quando l'agente è in stato di inattività.

2.4.2 Opzioni del menu

Cliccando con il tasto destro del mouse sull'icona posta nell'area di notifica è possibile aprire il menu dell'agente, che dà accesso alle azioni dell'agente disponibili. Per impostazione predefinita, cliccando due volte sull'icona viene eseguita l'azione Mostra risultati (in grassetto nell'esempio).

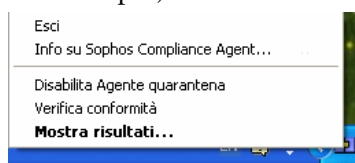


Figura 2: esempio del menu

La tabella seguente riporta testo e descrizioni del menu.

Testo del menu	Descrizione
Esci	Esce dall'agente, rimuove l'icona dall'area di notifica e mette il computer in quarantena, se applicabile. Nota: se l'impostazione Show Exit Agent è Show, questa opzione di menu viene visualizzata. Se l'impostazione è Hide (valore predefinito), non viene visualizzata. Per ulteriori informazioni relative alle impostazioni dell'agente, consultare la Guida in linea di NAC Manager.
Info su Sophos Compliance Agent...	Visualizza la finestra di dialogo About.
Disabilita agente quarantena	Ignora la quarantena del computer. Quando la quarantena è disabilitata, accanto al testo viene visualizzato un segno di spunta. Quando è abilitata, il segno di spunta non viene visualizzato. Nota: Se i criteri non si trovano in modalità Enforce, o se l'opzione Quarantine Override all'interno del criterio è impostata come 'False' (ovvero il computer endpoint non

Testo del menu	Descrizione
	è autorizzato a prevenire le azioni della quarantena), non viene visualizzata questa opzione di menu.
Verifica conformità	Dà inizio, su richiesta dell'utente, alla verifica della conformità che include le operazioni di recupero, verifica e attuazione dei criteri, oltre che correzione e reportistica.
Mostra risultati...	Visualizza la finestra di dialogo Risultati con i messaggi relativi alla verifica di conformità più recente.

2.4.3 Fumetti

I fumetti forniscono informazioni testuali aggiuntive riguardanti le azioni che l'agente ha eseguito o deve eseguire. Il fumetto può venire visualizzato se sono necessarie azioni da parte di un utente, come nel caso di risultati in sospeso, o se lo stato di un agente cambia.

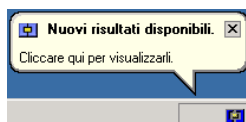


Figura 3: esempio di fumetto

La tabella seguente riporta il testo dei fumetti insieme alla relativa descrizione.

Testo del fumetto	Descrizione
Titolo: nuovi risultati disponibili. Testo: cliccare qui per visualizzarli.	Fumetto visualizzato quando sono presenti azioni in sospeso e visualizzate nella finestra di dialogo Risultati.
Titolo: il computer è stato posto in quarantena. Nessun testo predefinito.	Fumetto visualizzato quando il computer viene messo in quarantena.
Titolo: il computer è stato rimosso dalla quarantena. Nessun testo predefinito.	Fumetto visualizzato quando il computer viene rimosso dalla quarantena.

2.4.4 Finestra di dialogo Richiesta credenziali

La finestra di dialogo Richiesta credenziali indica se è necessaria l'autenticazione attraverso un server proxy per consentire all'agente di comunicare col NAC Server.

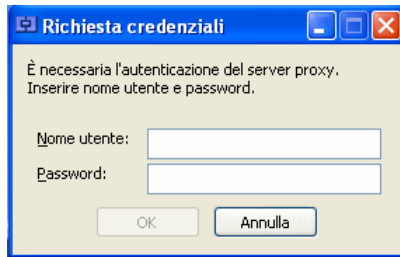


Figura 4: esempio della finestra di dialogo Richiesta credenziali

2.4.5 Finestra di dialogo Risultati

La finestra di dialogo Risultati mostra all'utente i messaggi definiti dal criterio oppure i messaggi di errore visualizzabili dall'utente. È possibile aprire la finestra di dialogo Risultati tramite l'opzione di menu Mostra risultati e visualizzare i messaggi dell'ultima verifica della conformità.



Figura 5: esempio della finestra di dialogo Risultati

2.4.6 Finestra di dialogo About

La finestra di dialogo About riporta le informazioni sull'agente, sul copyright e la casella di spunta Abilita registrazione nel log. La finestra di dialogo About è disponibile dall'opzione About del menu.

3 Dissolvable Agent

Questa sezione contiene informazioni sulla concezione e la configurazione di Dissolvable Agent.

3.1 Concezione

Dissolvable Agent può essere installato su qualsiasi server web basato su Windows, incluso il NAC Server, e fornisce una pagina web accessibile da parte degli utenti ospiti per scaricare Dissolvable Agent. Dissolvable Agent è un'applicazione autonoma che viene eseguita localmente sul computer endpoint senza richiedere diritti di amministratore o di power user. Se è necessaria l'autenticazione attraverso server proxy per consentire a Dissolvable Agent di comunicare col NAC Server, il browser web richiederà nome utente e password.

Operazioni di elaborazione

Una volta scaricato, Dissolvable Agent visualizza una serie di finestre di dialogo che indicano l'avanzamento e le eventuali azioni. Dissolvable Agent svolge le operazioni di elaborazione - recupero, verifica e attuazione del criterio, correzione e reportistica - ogni volta che è richiamato, secondo il criterio di NAC definito in NAC Manager. Quando le operazioni sono completate, Dissolvable Agent si autorimuove dal computer. Dissolvable Agent non ha funzioni di attuazione in sé, ma può essere utilizzato con l'attuazione di DHCP.

Reportistica e messaggi

I dati del report includono informazioni sulle applicazioni del software installate o meno nel computer, lo stato di conformità del computer durante la verifica basata sul criterio di NAC e i messaggi visualizzati all'utente del computer. Durante il funzionamento, Dissolvable Agent visualizza all'utente i messaggi definiti nei profili di NAC Manager e gli errori verificatisi durante il funzionamento.

3.2 Configurazione

Per utilizzare Dissolvable Agent, è necessario innanzitutto installarlo su un server web basato su Windows, che sia accessibile dagli utenti ospiti. Dissolvable Agent può essere installato sullo stesso server di Sophos NAC.

1. Installare Sophos Compliance Dissolvable Agent in un server web basato Windows.

Dissolvable Agent è reperibile online dal sito di Sophos. In alternativa, è possibile installare Dissolvable Agent dal CD di installazione di Sophos. Il file di installazione di Sophos Compliance Dissolvable Agent installa tutti i file che supportano Dissolvable Agent. Per ulteriori informazioni, consultare la *Guida di avvio avanzata di Sophos Endpoint Security and Control*.

2. Se necessario, distribuire l'URL di Sophos Compliance Dissolvable Agent agli utenti ospiti.

Il computer recupera il criterio ad esso assegnato e svolge la verifica della conformità. Se Dissolvable Agent viene installato nella directory predefinita, i computer endpoint possono accedere a Dissolvable Agent utilizzando l'URL seguente: `http://<indirizzo ip/nome DNS>/dissolvableagent`. L'indirizzo IP o il nome DNS rappresenta il server web su cui è stato installato Dissolvable Agent.

3.3 Registrazione nel log

In NAC Manager, non sono presenti impostazioni definite per Dissolvable Agent. L'impostazione della registrazione viene definita nel computer.

Per la risoluzione dei problemi, Dissolvable Agent supporta file di log multipli che, se utilizzati, vengono salvati nell'hard disk del computer. La registrazione nel log incide sulle prestazioni di Dissolvable Agent; si consiglia perciò di abilitarla (dalla finestra di dialogo About) esclusivamente per la risoluzione di un problema e di disabilitarla a problema risolto. I file di log escludono i dati sensibili per l'utente e contengono livelli di informazione personalizzabili.

I tre file di log sono:

- **Session Log:** fornisce un alto livello di informazioni sull'errore.
 - **Trace Log:** fornisce informazioni dettagliate sull'errore.
 - **Agent Log:** fornisce informazioni sull'errore che riguardano l'applicazione dell'agente.
1. Avviare Dissolvable Agent.
 2. Cliccare sull'icona Sophos NAC nella finestra di dialogo **Risultati** e selezionare **Info su Sophos Compliance Agent**.
 3. Nella finestra **About**, selezionare la casella di spunta **Abilita registrazione nel log**.
 4. Eseguire Dissolvable Agent.
 5. Individuare i file di log, reperibili nella directory `%temp%\SDA<numero casuale>\Logs`.
A meno che la posizione della directory temp sia stata cambiata dall'utente, è possibile accedere a quest'ultima aprendo Internet Explorer, digitando `%temp%` nel campo dell'indirizzo e premendo **Invio**.
 6. A problema risolto, eseguire di nuovo Dissolvable Agent, aprire la finestra di dialogo **About** di Dissolvable Agent e deselezionare la casella **Abilita registrazione nel log**.

3.4 Finestre di dialogo

La sezione seguente contiene informazioni sulle finestre di dialogo che sono a disposizione per Dissolvable Agent.

3.4.1 Finestra di dialogo Richiesta credenziali

La finestra di dialogo Richiesta credenziali indica se è necessaria l'autenticazione attraverso un server proxy per consentire a Dissolvable Agent di comunicare con il NAC Server.

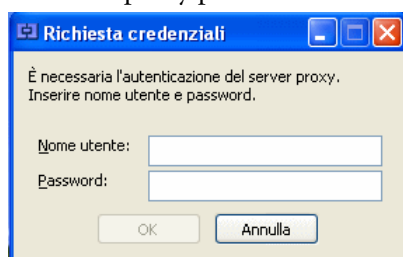


Figura 6: esempio della finestra di dialogo Richiesta credenziali

3.4.2 Finestra di dialogo Avanzamento

La finestra di dialogo Avanzamento viene visualizzata quando Dissolvable Agent sta eseguendo le operazioni di elaborazione: recupero, verifica e attuazione del criterio, correzione e reportistica. La finestra di dialogo Avanzamento riporta: lo stato, l'avanzamento delle singole operazioni e l'avanzamento complessivo.

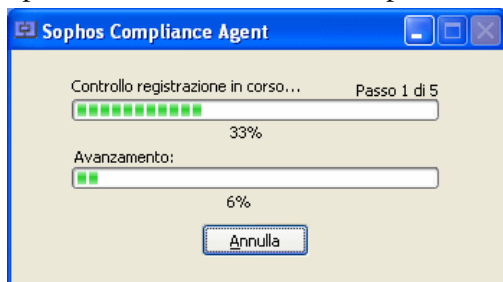


Figura 7: esempio della finestra di dialogo Avanzamento

3.4.3 Finestra di dialogo Risultati

La finestra di dialogo Risultati mostra all'utente i messaggi definiti dal criterio oppure i messaggi di errore disponibili.

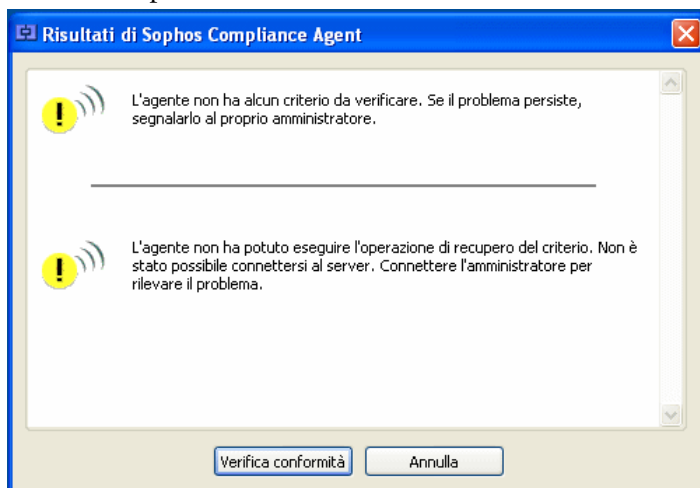


Figura 8: esempio della finestra di dialogo Risultati

3.4.4 Finestra di dialogo About

La finestra di dialogo About riporta le informazioni sull'agente, sul copyright e la casella di spunta Abilita registrazione nel log. La finestra di dialogo About è disponibile cliccando sull'icona Sophos nella finestra di dialogo Risultati.

4 Lingue dell'agente

Per impostazione predefinita, l'agente supporta le seguenti otto lingue: inglese, francese, spagnolo, tedesco, italiano, giapponese, cinese semplificato e cinese tradizionale.

I messaggi per l'utente sono definiti nei profili di NAC Manager. L'agente visualizza i messaggi per l'utente in una lingua specifica solo se definiti.

Si consiglia di creare per un profilo un messaggio in inglese (lingua predefinita), in modo tale che, se non può essere visualizzato in un'altra lingua, all'utente compaia comunque un messaggio.

Per ulteriori informazioni sulla creazione di messaggi per l'utente, consultare la Guida in linea di NAC Manager.

5 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.

6 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.