

**SOPHOS**

---

simple + secure

# Sophos Enterprise Manager

## Guida di avvio

Versione prodotto: 4.7

Data documento: agosto 2011



# Sommario

1	Informazioni sulla guida.....	3
2	Passaggi chiave.....	3
3	Verifica dei requisiti di sistema.....	4
4	Preparazione all'installazione.....	5
5	Download del programma di installazione.....	5
6	Installazione di Enterprise Manager .....	5
7	Download del software di sicurezza.....	6
8	Creazione di gruppi di computer.....	6
9	Impostazione dei criteri di sicurezza.....	7
10	Ricerca dei computer.....	8
11	Protezione dei computer Windows.....	9
12	Protezione dei computer Mac OS X.....	13
13	Protezione dei computer Linux.....	14
14	Verifica dello stato della rete.....	16
15	Risoluzione dei problemi.....	16
16	Aiuto per lo svolgimento di operazioni comuni.....	16
17	Appendice: Passaggio a Enterprise Manager da Enterprise Console.....	17
18	Supporto tecnico.....	20
19	Note legali.....	20

## 1 Informazioni sulla guida

Questa guida spiega come installare Sophos Enterprise Manager versione 4.7 e proteggere la propria rete con il software di sicurezza Sophos.

Sophos Enterprise Manager è una console singola e automatizzata che gestisce e aggiorna i software di sicurezza Sophos su computer con sistemi operativi Windows, Mac e Linux. Enterprise Manager consente di:

- Proteggere la rete da virus, trojan, worm, spyware, siti web malevoli e minacce sconosciute, oltre che da adware ed altre applicazioni potenzialmente indesiderate.
- Gestire nei computer la protezione del client firewall.
- Impedire che gli utenti utilizzino nei computer dispositivi di memorizzazione esterni non autorizzati e tecnologie di connessione wireless.
- Impedire agli utenti di riconfigurare, disabilitare o disinstallare il software di sicurezza Sophos.

Per consultare un elenco di funzioni di Enterprise Manager e per ottenere maggior informazioni sulle differenze fra Enterprise Manager, incluse le relative licenze, e altri prodotti e licenze Sophos, consultare l'articolo 113711 della knowledge base di Sophos (<http://www.sophos.com/support/knowledgebase/article/113711.html>).

### Cambio da Enterprise Console

Descrive anche i passaggi aggiuntivi da eseguire se si desidera disinstallare Enterprise Console per installare Enterprise Manager.

**Importante:** il passaggio da Enterprise Console a Enterprise Manager non è supportato. Sarà necessario disinstallare Enterprise Console per poi installare Enterprise Manager, come descritto in questa guida, quindi eseguirne l'impostazione.

Verranno cancellate tutte le impostazioni di Enterprise Console.

Prima di eseguire l'installazione di Enterprise Console, memorizzare le impostazioni esistenti ed eseguire il backup del database di Enterprise Console, come descritto in [Appendice: Passaggio a Enterprise Manager da Enterprise Console](#) a pagina 17.

## 2 Passaggi chiave

Svolgere i seguenti passaggi chiave:

- Verificare i requisiti di sistema
- Prepararsi all'installazione
- Eseguire il download del programma di installazione
- Installare Enterprise Manager
- Scaricare il software di sicurezza
- Creare i gruppi di computer

- Impostare i criteri di sicurezza
- Ricercare i computer
- Proteggere i computer
- Verificare lo stato della rete.

## 3 Verifica dei requisiti di sistema

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

### 3.1 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>).

### 3.2 Software di sistema Microsoft

Enterprise Manager richiede un software di sistema Microsoft specifico (per es. software di database).

Il programma di installazione di Enterprise Manager cerca di installare tale software di sistema, se non già a disposizione nel server. Tuttavia, in alcuni casi, il software non è compatibile con il server, oppure deve essere installato manualmente.

#### Installazione del SQL Server

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 in 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 gli articoli 65190 e 111220 della knowledge

base del supporto Sophos (<http://www.sophos.com/support/knowledgebase/article/65190.html> e <http://www.sophos.com/support/knowledgebase/article/111220.html>).

## 4 Preparazione all'installazione

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

- Assicurarsi di essere collegati ad Internet.
- Assicurarsi di essere in possesso dei CD relativi ai Service Pack e al sistema operativo Windows. Potrebbero essere richiesti durante l'installazione.
- Se il server esegue Windows Server 2008 o successivo, disattivare il Controllo account utente (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.

## 5 Download del programma di installazione

Eseguire il download del programma di installazione di Sophos e collocarlo nel server in cui installare la console di gestione:

1. Visitare la pagina web <http://www.sophos.it/support/updates/>.
2. Digitare il proprio nome utente e password MySophos.
3. Della pagina web **Download e aggiornamenti**, scaricare il programma di installazione di Enterprise Manager.
4. Se necessario, copiare i programmi di installazione scaricati nel server in cui si desidera eseguire l'installazione.

## 6 Installazione di Enterprise Manager

Per installare Enterprise Manager:

1. Nel computer in cui si desidera installare Enterprise 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 Enterprise Manager, scaricato in precedenza.
3. Cliccare due volte sul programma di installazione.
4. Nella finestra di dialogo del programma di installazione di rete, cliccare su **Installa**.

I file di installazione vengono copiati sul computer, ed è avviata la procedura guidata per l'installazione.

5. Nella pagina iniziale della Procedura guidata di installazione di Sophos Enterprise Manager, cliccare su **Avanti**.
6. Una procedura guidata accompagna nei passaggi dell'installazione. Accettare le impostazioni predefinite dove possibile.
7. Al termine dell'installazione, potrebbe essere necessario il riavvio. Cliccare su **Sì** o su **Fine**.

## 7 Download del software di sicurezza

Quando si riaccende o si riavvia la console per la prima volta dopo l'installazione, Enterprise Manager 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 illustrato di seguito:

1. Nella pagina **Dattagli dell'account di download 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 la piattaforma che si desidera proteggere. Quando si clicca su **Avanti**, Enterprise Manager 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 Manager utilizzi i gruppi esistenti di Active Directory.

**Nota:** se uno stesso computer è stato aggiunto a più di un albero di Active Directory, ciò può generare problemi quali il continuo scambio di messaggi fra il computer e Enterprise Manager.

Il software selezionato viene scaricato nella condivisione `\\nome server\SophosUpdate`, in cui il *nome server* è il nome del server nel quale è installato Enterprise Manager.

Se si è disattivato il Controllo account utente prima di eseguire l'installazione, è possibile riattivarlo.

## 8 Creazione di gruppi di computer

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

I gruppi sono utili perché tramite questi è possibile:

- Organizzare i computer in gruppi diversi che vengono aggiornati da diverse fonti o in base a pianificazioni diverse.
- Utilizzare diversi antivirus e HIPS, firewall e altri criteri per gruppi differenti.

- Gestire più facilmente i computer.

Se i gruppi nel computer sono già stati impostati in base alla struttura dei gruppi di Active Directory tramite la **procedura guidata di download del software di sicurezza**, saltare questa sezione. Visitare la pagina web [Impostazione dei criteri di sicurezza](#) a pagina 7.

1. Aprire Enterprise Manager, se non ancora aperto.
2. Nel riquadro **Gruppi** (a 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 cima per creare un gruppo di livello principale. Selezionare un gruppo per creare al suo interno un sottogruppo. Infine, inserirne il nome seguendo la procedura svolta in precedenza.

## 9 Impostazione dei criteri di sicurezza

### Criteri predefiniti

Enterprise Manager 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 creare un criterio firewall. Consultare la sezione [Impostazione di un criterio del firewall](#) a pagina 8.
- Se si desidera utilizzare questa funzione, è necessario modificare i criteri del controllo dispositivi e del blocco rimozione. Questa operazione può essere svolta in qualsiasi momento.

Per informazioni su come abilitare e configurare i criteri del controllo dispositivi e del blocco rimozione, consultare le sezioni *Configurazione del criterio del controllo dispositivi* e *Configurazione del criterio del blocco rimozione* nella *Guida in linea* di *Enterprise Manager*.

### Creazione di nuovi criteri

In Enterprise Manager, è possibile creare al massimo quattro nuovi criteri per ogni tipologia. Una volta raggiunto il limite, vengono disabilitate le opzioni **Crea criterio** e **Duplica criterio**.

Per creare un nuovo criterio:

1. Nella vista **Computer**, nel riquadro **Criteri**, cliccare con il tasto destro del mouse sul tipo di criterio che si desidera creare, ad esempio, "Criterio di aggiornamento" e selezionare **Crea criterio**.  
Un "Nuovo criterio" viene aggiunto all'elenco, con il nome evidenziato.
2. Digitare un nuovo nome per il criterio.
3. Cliccare due volte sul nuovo criterio. Inserire le impostazioni desiderate.

Per istruzioni su come scegliere le impostazioni, consultare la sezione relativa alla configurazione dei criteri.

Il criterio appena creato può ora essere assegnato ai gruppi.

### Assegnazione dei criteri ai gruppi

1. Nel riquadro **Criteri**, evidenziare il criterio.
2. Cliccare sul criterio e trascinarlo sul gruppo al quale lo si desidera applicare. Quando richiesto, continuare con la procedura.

## 9.1 Impostazione di un criterio del firewall

Per impostazione predefinita il firewall è attivato e blocca tutto il traffico non essenziale. È quindi necessario configurarlo in modo tale da poter consentire le applicazioni che si desidera utilizzare e testarlo prima di eseguirne l'installazione in tutti i computer. Per informazioni dettagliate, consultare la *Guida all'impostazione dei criteri di Sophos Enterprise Manager*.

È possibile impostare le principali opzioni di configurazione del firewall direttamente nella **procedura guidata per l'impostazione dei criteri Firewall**.

1. Nel riquadro **Criterio**, 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 segue.
  - 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**.

## 10 Ricerca dei computer

Affinché Enterprise Manager possa proteggere e gestire i computer in rete, è necessario innanzitutto cercarli.

Se i gruppi nel computer sono già stati impostati in base alla struttura dei gruppi di Active Directory tramite la **procedura guidata di download del software di sicurezza**, saltare questa sezione. Andare alla sezione *Protezione dei computer Windows* a pagina 9.

1. Cliccare sull'icona **Cerca nuovi computer** nella barra degli strumenti.

2. Selezionare il metodo che si desidera utilizzare per cercare i computer.
  - Se si utilizza l'opzione **Importa da Active Directory** e si sceglie di importare computer e alberi, i computer verranno collocati nei relativi gruppi.
  - Se si utilizza una delle opzioni **Trova**, i computer vengono posizionati nella cartella **Nessun gruppo**.
3. Inserire i dati relativi all'account e, se necessario, indicare dove si desidera effettuare la ricerca.
4. Se si è utilizzata una delle opzioni **Trova**, cliccare sulla cartella **Nessun gruppo** per visualizzare i computer trovati. Per iniziare la gestione dei computer, selezionarli e trascinarli in un gruppo.

## 11 Protezione dei computer Windows

Questa sezione spiega come proteggere automaticamente o manualmente i computer con sistema operativo Windows.

### 11.1 Preparazione della protezione automatica dei computer Windows

Prima di proteggere i computer, è necessario prepararli nel modo seguente:

- Effettuare la preparazione della rimozione del software di sicurezza di terze parti
- Essere in possesso di un account utilizzabile per l'installazione di software
- Prepararsi per l'installazione del software antivirus.

#### 11.1.1 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 fornitore, 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 Manager.

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

Quando si esegue la protezione automatica dei computer, nella **procedura guidata di protezione dei computer**, verranno richiesti i dettagli di un account che possa essere utilizzato

per l'installazione di software di sicurezza. Si tratta di solito 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 in cui è stata installato Enterprise Manager.
- Avere accesso in lettura alla posizione dalla quale i computer si aggiorneranno.

Per impostazione predefinita, i computer si aggiornano da una singola condivisione primaria UNC di origine, \\<NomeComputer>\SophosUpdate, dove è installato Enterprise Manager. Per verificare questo percorso, nel riquadro **Criteri**, cliccare due volte su **Aggiornamento** e poi sul criterio che si desidera aggiornare.

### 11.1.3 Preparazione per l'installazione del software antivirus

È necessario preparare i computer all'installazione del software antivirus. I passaggi da eseguire dipendono dal sistema operativo in esecuzione.

**Nota:** Se qui non si fa riferimento a un determinato sistema operativo, ciò significa che non richiede alcuna preparazione.

#### 11.1.3.1 Preparazione dei computer Windows 7

Per preparare i computer Windows 7 all'installazione del software antivirus, eseguire i passaggi riportati qui di seguito.

In alternativa, se si esegue Active Directory, è possibile preparare i computer Windows 7 tramite un oggetto Criteri di gruppo (GPO) in Windows 2008 e Windows 2008 R2. Consultare l'articolo 111180 della knowledge base del supporto tecnico di Sophos (<http://www.sophos.com/support/knowledgebase/article/111180.html>).

1. Dal Pannello di controllo aprire a il Centro connessioni di rete e condivisione . Per il percorso della **Rete ufficio** , assicurarsi che le opzioni siano configurate nel modo seguente:  
Individuazione rete: Attiva  
Condivisione file e stampanti: Attiva  
Connessioni condivisione file: Abilita condivisione file per dispositivi che utilizzano la crittografia a 40 o 56 bit  
Condivisione protetta da password: Disattiva
2. Accertarsi che il servizio Registro di sistema remoto sia avviato e che l'avvio sia impostato su Automatico.
3. Impostare il Controllo dell'account utente su **Non notificare**. Quando l'installazione è completata, reimpostare su **Predefinito**.
4. Disattivare Usa procedura guidata condivisione.

5. Aprire Windows Firewall con Advanced Security, tramite la voce **Strumenti di amministrazione** nel Pannello di controllo.
  - a) Assicurarsi che le **Connessioni in ingresso** siano consentite.
  - b) Modificare le **Regole in entrata** al fine di abilitare i seguenti processi. Una volta completata l'installazione, disattivarli di nuovo.
    - Amministrazione remota (NP-In) Dominio
    - Amministrazione remota (NP-In) Privato
    - Amministrazione remota (RPC) Dominio
    - Amministrazione remota (RPC) Privato
    - Amministrazione remota (RPC-EPMAP) Dominio
    - Amministrazione remota (RPC-EPMAP) Privato

### 11.1.3.2 Preparazione dei computer Windows Vista

1. Dal Pannello di controllo aprire a il Centro connessioni di rete e condivisione . Assicurarsi che le opzioni siano configurate nel modo seguente:
  - Individuazione rete: Attiva
  - Condivisione file: Attiva
  - Condivisione stampanti: Attiva
  - Condivisione protetta da password: Disattiva
2. Accertarsi che il servizio Registro di sistema remoto sia avviato e che l'avvio sia impostato su Automatico.
3. Disabilitare il Controllo account utente. Quando l'installazione è completata, è necessario riattivarlo.
4. Disattivare Usa procedura guidata condivisione.
5. Aprire Windows Firewall con Advanced Security, tramite la voce **Strumenti di amministrazione** nel Pannello di controllo.
  - a) Assicurarsi che le **Connessioni in ingresso** siano consentite.
  - b) Modificare le **Regole in entrata** al fine di abilitare i seguenti processi. Una volta completata l'installazione, disattivarli di nuovo.
    - Amministrazione remota (NP-In) Dominio
    - Amministrazione remota (NP-In) Privato
    - Amministrazione remota (RPC) Dominio
    - Amministrazione remota (RPC) Privato
    - Amministrazione remota (RPC-EPMAP) Dominio
    - Amministrazione remota (RPC-EPMAP) Privato

### 11.1.3.3 Preparazione dei computer Windows 2003/XP Pro/2000

1. Assicurarsi che siano stati avviati i servizi Registro di sistema remoto, Server, Computer Browser e Utilità di pianificazione.
2. Assicurarsi che la condivisione C\$ admin sia abilitata.
3. Assicurarsi che la Condivisione file semplice sia disattivata (solo XP Pro).

### 11.1.3.4 Preparazione dei computer Windows XP (SP2 o successivi)

**Nota:** Per i computer Windows XP Pro, consultare la sezione [Preparazione dei computer Windows 2003/XP Pro/2000](#) a pagina 12.

1. Assicurarsi che siano stati avviati i servizi Registro di sistema remoto, Server, Computer Browser e Utilità di pianificazione.
2. Assicurarsi che la condivisione C\$ admin sia abilitata.
3. Assicurarsi che la Condivisione file semplice sia disattivata.
4. Abilitare Condivisione file e stampanti per reti Microsoft.
5. Accertarsi che le porte TCP 8192, 8193 e 8194 siano aperte.
6. Riavviare il computer per rendere effettive le modifiche.

## 11.2 Protezione automatica dei computer Windows

Per proteggere i computer, fare quanto segue:

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 del software di sicurezza Sophos. È necessario procedere come illustrato di seguito:

- a) Nella pagina **Seleziona funzioni**, selezionare tutte le funzioni opzionali desiderate.  
La funzione antivirus è sempre installata.

Sophos Client Firewall non è supportato dal sistema operativo del server.

**Importante:** Assicurarsi che il firewall sia stato configurato e consenta il traffico, le applicazioni e i processi che si desidera utilizzare; si consiglia inoltre di testarlo prima di installarlo ed eseguirlo su tutti i computer. Consultare la sezione [Impostazione di un criterio del firewall](#) a pagina 8.

- b) Sulla pagina **Riepilogo protezione** verificare eventuali problemi di installazione. Per ulteriore assistenza, consultare la sezione [Risoluzione dei problemi](#) a pagina 16.
- 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.

**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 verificare lo stato della protezione dei computer, selezionare il gruppo in cui sono stati collocati i computer, o selezionare il server visualizzato in alto per vedere tutti i computer. Una volta portata a termine l'installazione, nell'elenco computer, nella colonna **In accesso**, la parola **Attivo/a** indica che sul computer è in esecuzione la scansione dei virus in accesso.

### 11.3 Protezione manuale dei computer Windows

Se in possesso di computer che non possono essere protetti automaticamente, è possibile proteggerli eseguendo un programma di installazione dalla cartella condivisa in cui è stato scaricato il software di sicurezza. Tale cartella corrisponde al percorso bootstrap.

1. Per scoprire in quale directory si trovi il programma di installazione, aprire Enterprise Manager. Nel menu **Visualizza**, cliccare su **Percorsi Bootstrap**.

Nella finestra di dialogo **Percorsi Bootstrap**, la colonna **Percorso** mostra il percorso bootstrap di tutte le piattaforme.

2. Recarsi presso ciascun computer e accedere con diritti di amministratore locale.
3. Posizionare il programma di installazione nella percorso bootstrap e cliccarvi due volte. Per i computer Windows, il programma è chiamato setup.exe.
4. Una procedura guidata accompagna nei passaggi dell'installazione.

## 12 Protezione dei computer Mac OS X

L'installazione automatica non è possibile nei computer con sistema operativo Mac. È possibile proteggerli eseguendo un programma di installazione dalla cartella condivisa in cui è stato scaricato il software di sicurezza. Tale cartella corrisponde al percorso bootstrap.

1. Per scoprire in quale directory si trovi il programma di installazione, aprire Enterprise Manager. Nel menu **Visualizza**, cliccare su **Percorsi Bootstrap**.

Nella finestra di dialogo **Percorsi Bootstrap**, la colonna **Percorso** mostra il percorso bootstrap di tutte le piattaforme.

2. Recarsi presso ciascun computer e accedere con diritti di amministratore locale.
3. Posizionare il programma di installazione nella percorso bootstrap e cliccarvi due volte. Per i computer Mac OS X, il programma è chiamato Sophos Anti-Virus.mpkg
4. Una procedura guidata accompagna nei passaggi dell'installazione.

## 13 Protezione dei computer Linux

Per proteggere i computer con sistema operativo Linux, occorre:

- Creare un pacchetto di distribuzione.
- Installare Sophos Anti-Virus nei computer Linux.

### 13.1 Creazione di un pacchetto di distribuzione

In questa sezione si presuppone che sia già stato eseguito il download di Sophos Anti-Virus per Linux, secondo quanto spiegato alla sezione [Download del software di sicurezza](#) a pagina 6.

Utilizzare lo script **mkinstpkg** per creare un pacchetto di distribuzione per gli utenti finali. Questo script richiede informazioni sulle modalità di installazione di Sophos Anti-Virus nei computer con sistema operativo Linux; le risposte ottenute vengono quindi inserite nel pacchetto di distribuzione. Quando l'utente finale esegue l'installazione dal pacchetto di distribuzione, sia la posizione di aggiornamento che le credenziali vengono impostate correttamente, senza l'intervento dell'utente. È inoltre possibile creare un pacchetto in formato tar o RPM.

**Nota:** lo script **mkinstpkg** va utilizzato solo all'interno della propria organizzazione. Leggere il contratto di licenza e la nota legale visualizzati dallo script **mkinstpkg**.

Per creare un pacchetto di distribuzione:

1. Per trovare il percorso della cartella condivisa (percorso bootstrap) in cui è stato scaricato Sophos Anti-Virus:
  - a) In Enterprise Manager, dal menu **Visualizza**, cliccare su **Percorsi Bootstrap**.  
Nella finestra di dialogo **Percorsi Bootstrap**, la colonna **Percorso** mostra il percorso bootstrap di tutte le piattaforme.
  - b) Annotare il percorso rilevante.
2. Accedere al server Linux come utente root.
3. Montare il percorso bootstrap.  
Per consentire il montaggio automatico di questa cartella nel boot di sistema, utilizzare i tool di distribuzione oppure modificare fstab.
4. Passare al percorso bootstrap.
5. Per creare un pacchetto di distribuzione in formato tar, denominato savinstpkg.tgz, digitare:  
**./mkinstpkg.sh**

Per creare un pacchetto di distribuzione in formato RPM, denominato savinstpkg-0.0-1.i586.rpm, digitare:

**./mkinstpkg.sh -r**

**Nota:** il nome del file potrebbe variare a seconda dell'installazione RPM.

6. Quando richiesto, scegliere di abilitare la gestione remota.
7. Quando richiesto, inserire il percorso bootstrap (come visualizzato nei computer con sistema operativo Linux).

È ora possibile installare Sophos Anti-Virus tramite pacchetto di distribuzione.

## 13.2 Installazione di Sophos Anti-Virus per Linux tramite pacchetto di distribuzione

Utilizzare il pacchetto per installare Sophos Anti-Virus scegliendo una delle due modalità riportate qui di seguito:

- Manualmente in ciascun computer. Questo metodo è utilizzabile con un pacchetto in formato RPM o tar.
- Automaticamente su tutta la rete. Questo metodo è utilizzabile solo con un pacchetto in formato RPM.

**Nota:** in Linux Red Hat Enterprise versione 6 a 64 bit, per poter eseguire l'installazione di Sophos Anti-Virus è necessario installare i seguenti pacchetti:

- glibc-2.11.1-1.i686
- nss-softokn-freebl i686 3.12.4-10.fc12

### 13.2.1 Installazione manuale di Sophos Anti-Virus per Linux

1. Utilizzare i tool di cui si è in possesso per copiare il pacchetto di distribuzione nei computer sui quali si desidera installare Sophos Anti-Virus.
2. Accedere a ciascun computer come utente root.
3. Collocare il pacchetto di distribuzione in una directory temporanea e selezionarla.
4. Per eseguire l'installazione dal pacchetto tar, digitare:

```
tar -zxvf savinstpkg.tgz  
./sophos-av/install.sh
```

Per eseguire l'installazione dal pacchetto RPM, digitare:

```
rpm -i pacchetto RPM
```

Dal server vengono copiati i file necessari e viene installato Sophos Anti-Virus. D'ora in poi, Sophos Anti-Virus verrà aggiornato automaticamente ogni volta che il percorso del bootstrap verrà aggiornato.

### 13.2.2 Installazione automatica di Sophos Anti-Virus per Linux

- ❖ Per installare Sophos Anti-Virus automaticamente dal pacchetto di distribuzione, utilizzare uno dei tool di amministrazione del sistema operativo che supporta la distribuzione remota. Per ulteriori informazioni, consultare la documentazione relativa a tale tool.

Dopo l'installazione, Sophos Anti-Virus verrà riavviato e sarà aggiornato automaticamente ad ogni aggiornamento del percorso del bootstrap.

## 14 Verifica dello stato della rete

Per verificare lo stato di salute della rete da Enterprise Manager, nella barra dei menu, cliccare sull'icona del **Pannello di controllo** (se non ancora visualizzato).

Il Pannello di controllo mostra quanti computer:

- Presentano minacce
- Non sono aggiornati
- Non sono conformi ai criteri

## 15 Risoluzione dei problemi

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

- Nei computer Mac e Linux non è possibile eseguire l'installazione automatica tramite Enterprise Manager. Per informazioni su come proteggere questi sistemi operativi, consultare le sezioni [Protezione dei computer Mac OS X](#) a pagina 13 e [Protezione dei computer Linux](#) a pagina 14.
- 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\nomeutente.
- I computer eseguono il firewall.

## 16 Aiuto per lo svolgimento di operazioni comuni

Per informazioni su come svolgere operazioni ordinarie, consultare le seguenti sezioni della *Guida in linea* di *Enterprise Manager*:

- *Configurazione dei criteri*
  - *Configurazione dei criteri antivirus e HIPS*
  - *Configurazione del criterio del firewall*
  - *Configurazione del criterio del controllo dispositivi*
  - *Configurazione del criterio del blocco rimozione*
- *Protezione dei computer*
  - *Come gestire computer con allarmi ed errori*
  - *Disinfezione dei computer*

### ■ Creazione dei report

Per le linee guida e le migliori pratiche sull'impostazione dei criteri, consultare anche la *Guida all'impostazione dei criteri di Sophos Enterprise Manager*.

## 17 Appendice: Passaggio a Enterprise Manager da Enterprise Console

Quando si disinstalla Enterprise Console per installare Enterprise Manager, tutte le impostazioni di Enterprise Console verranno perse. I computer verranno spostati nel gruppo **Nessun gruppo** e verranno ripristinati i criteri predefiniti.

Memorizzare le impostazioni esistenti per rendere più facile la creazione creazione dei gruppi e la configurazione dei criteri in Enterprise Manager.

È possibile esportare le impostazioni della configurazione dei criteri firewall da Enterprise Console versione 4.5 o 4.7 per importarle in Enterprise Manager. Le istruzioni su come svolgere questa operazione sono disponibili nelle seguenti sezioni:

Se si utilizza Sophos NAC (Network Access Control), è necessario rimuoverlo dalla propria rete. Se si utilizzano le funzioni del controllo dati e applicazioni, è inoltre consigliabile disabilitarle prima di eseguire la disinstallazione di Enterprise Console.

**Importante:** prima di disinstallare Enterprise Console, eseguire il back up del database di Enterprise Console, secondo quanto descritto nella sezione [Backup del database di Enterprise Console](#) a pagina 19.

### 17.1 Esportazione e importazione delle impostazioni di configurazione del firewall

Per esportare le impostazioni di configurazione dei criteri firewall da Enterprise Console e importarle in Enterprise Manager:

1. In Enterprise Console, nel riquadro **Criteri**, cliccare due volte su **Firewall** e quindi sul criterio che si desidera esportare.
2. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
3. Nella finestra di dialogo **Criteri firewall**, nella scheda **Generale**, sotto **Gestione configurazione**, cliccare su **Esporta** per esportare le impostazioni del firewall come file di configurazione (\*.conf).
4. Ripetere i passaggi 1-3 per tutti i criteri firewall di Enterprise Console, fino a un massimo di 5 (Enterprise Manager supporta un massimo di 5 criteri).
5. Per importare le impostazioni in Enterprise Manager, da Enterprise Manager, nel riquadro **Criteri**, cliccare due volte su **Firewall** e quindi sul criterio in cui importare le impostazioni.
6. Nella pagina **Benvenuti** della procedura guidata **Criteri firewall**, cliccare su **Criteri avanzati firewall**.
7. Nella finestra di dialogo **Criteri firewall**, nella scheda **Generale**, sotto **Gestione configurazione**, cliccare su **Importa** per importare le impostazioni di configurazione del firewall.

8. Ripetere i passaggi 5-7 per altri cirteri firewall di Enterprise Manager.

## 17.2 Rimozione di Sophos NAC

Se si utilizza Sophos NAC (Network Access Control), è necessario rimuoverlo dalla propria rete.

I componenti di Sophos NAC vanno rimossi come segue:

- Rimuovere Sophos Compliance Agent dai computer endpoint.
- Rimuovere NAC Manager dal server.
- Rimuovere i database NAC dal server.

**Nota:** se i componenti non vengono rimossi in questo ordine, si potrebbero generare messaggi di errore per gli utenti.

### 17.2.1 Rimozione di Sophos Compliance Agent

Per rimuovere Sophos Compliance Agent, è necessario recarsi fisicamente presso ciascun computer endpoint e rimuovere l'agente manualmente.

**Nota:** prima di rimuovere l'agente, può venire richiesta la chiusura di determinate applicazioni.

**Nota:** dopo la rimozione dell'agente, è necessario riavviare il computer.

1. Andare al computer endpoint.
2. Dal menu **Start**, selezionare **Pannello di controllo > Installazione applicazioni**.
3. Selezionare **Sophos Network Access Control**, e cliccare su **Rimuovi**.
4. Cliccare su **Sì** per confermarne la rimozione.

### 17.2.2 Rimozione di NAC Manager

Per rimuovere NAC Manager:

1. Andare al server su cui è installato NAC Manager. Solitamente, si tratta dello stesso server su cui è installata Enterprise Console.
2. Dal menu **Start**, cliccare su **Pannello di controllo > Installazione applicazioni**.
3. Selezionare **Sophos NAC Application Server** e cliccare su **Rimuovi**.
4. Cliccare su **Sì** per confermarne la rimozione.

Viene rimosso NAC Manager.

### 17.2.3 Rimozione dei database di NAC

**Nota:** questa procedura rimuove solo i file utilizzati per creare i database e non i database veri e propri.

Sul server in cui è installato il database di NAC:

1. Dal menu **Start**, cliccare su **Pannello di controllo > Installazione applicazioni**.
2. Selezionare **Sophos NAC Databases** e cliccare su **Rimuovi**.
3. Cliccare su **Sì** per confermarne la rimozione.

## 17.3 Backup del database di Enterprise Console

Prima di installare Enterprise Console, assicurarsi di avere eseguito un backup completo dell'installazione di Enterprise Console. Accertarsi di poter ripristinare il sistema tramite il backup. Ciò sarà di aiuto se in seguito si deciderà di reinstallare Enterprise Console e ripristinare le sue impostazioni.

**Nota:** la cartella di installazione predefinita per il database è C:\Programmi\Microsoft SQL Server\MSSQL\$SOPHOS.

Per effettuare il backup del database di Enterprise Console:

1. Andare al computer in cui è installato il server di gestione di Enterprise Console.
2. Bloccare i servizi Sophos Message Router e Sophos Management Service. Per fare ciò:
  - a) Cliccare su **Start**, quindi su **Esegui**, digitare **services.msc** e cliccare su **OK**.
  - b) Nella finestra **Servizi (computer locale)**, cliccare con il tasto destro del mouse sul nome del servizio e quindi su **Arresta**.
  - c) Chiudere la finestra **Servizi (computer locale)**.

Ciò garantisce che non vengano scritte nuove informazioni nel database durante il backup.

3. Creare una cartella per il backup del database, per esempio C:\SophosBackups.
4. Aprire un prompt dei comandi nella directory di installazione del database di Enterprise Console.

La directory predefinita è: C:\Programmi\Sophos\Enterprise Console\DB.

5. Eseguire il backup del database inserendo un comando nel seguente formato:  
**BackupDB C:\SophosBackups\SOPHOS.bak**

Se il nome dell'istanza del server SQL è diverso da SOPHOS, aggiungere il nome dell'istanza del server SQL, per esempio:

**BackupDB C:\SophosBackups\SOPHOS.bak MySQLServerInstance**

6. Esportare la seguente chiave di registro:
  - Per sistemi operativi a 32 bit: HKLM\SOFTWARE\Sophos\Certification Manager
  - Per sistemi operativi a 64 bit:  
HKEY\_LOCAL\_MACHINE\Software\WOW6432Node\Sophos\Certification Manager

È ora possibile disinstallare Enterprise Console.

Per informazioni sul ripristino del database di Enterprise Console, consultare la sezione *Risoluzione dei problemi* qui di seguito.

## 17.4 Risoluzione dei problemi

### Ripristino dei dati di Enterprise Console

Se si desidera riportare l'installazione di Enterprise Console al suo stato precedente, procedere come riportato di seguito:

1. Ripristinare l'istanza del database utilizzata. l'istanza predefinita del server SQL è SOPHOS.
2. Ripristinare la seguente chiave di registro:
  - Per sistemi operativi a 32 bit: HKLM\SOFTWARE\Sophos\Certification Manager
  - Per sistemi operativi a 64 bit:  
HKEY\_LOCAL\_MACHINE\Software\WOW6432Node\Sophos\Certification Manager

Per maggiori informazioni e consigli, contattare il supporto tecnico.

## 18 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](mailto: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.

## 19 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.

### **ACE™, TAO™, CIAO™, and CoSMIC™**

ACE<sup>1</sup>, TAO<sup>2</sup>, CIAO<sup>3</sup>, and CoSMIC<sup>4</sup> (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt<sup>5</sup> and his research group<sup>6</sup> at Washington University<sup>7</sup>, University of California<sup>8</sup>, Irvine, and Vanderbilt University<sup>9</sup>, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source, 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 us<sup>10</sup> know so we can promote your project in the DOC software success stories<sup>11</sup>.

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 companies<sup>12</sup> 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 ACE<sup>13</sup>, TAO<sup>14</sup>, CIAO<sup>15</sup>, and CoSMIC<sup>16</sup> web sites are maintained by the DOC Group<sup>17</sup> at the Institute for Software Integrated Systems (ISIS)<sup>18</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>19</sup> for the development of open-source software as part of the open-source software community<sup>20</sup>. 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 me<sup>21</sup> know.

Douglas C. Schmidt<sup>22</sup>

## 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. [mailto:doc\\_group@cs.wustl.edu](mailto:doc_group@cs.wustl.edu)
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>
16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu/>
18. <http://www.isis.vanderbilt.edu/>
19. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
20. <http://www.opensource.org/>
21. <mailto:d.schmidt@vanderbilt.edu>
22. <http://www.dre.vanderbilt.edu/~schmidt/>

## Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at <http://www.apache.org/licenses/LICENSE-2.0>.

## Common Public License

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](mailto: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.

### **iMatix SFL**

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

### **OpenSSL cryptographic toolkit**

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

### **OpenSSL license**

Copyright © 1998-2011 The OpenSSL Project. Tutti i diritti riservati.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY

OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).  
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### **Original SSLeay license**

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word "cryptographic" can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR

OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]