

# SOPHOS

## Sophos Endpoint Security and Control 9.5 Guida di avvio per Linux, NetWare, e UNIX

Data documento: giugno 2010



# Sommario

1	Informazioni sulla guida.....	3
2	Requisiti di sistema.....	4
3	Protezione dei computer con sistema operativo Linux.....	5
4	Protezione dei server NetWare.....	7
5	Come proteggere computer UNIX.....	9
6	Protezione dei computer UNIX tramite Sophos Anti-Virus versione 4.....	10
7	Protezione dei computer UNIX tramite Sophos Anti-Virus versione 7.....	12
8	Verifica dello stato della rete.....	16
9	Supporto tecnico.....	17
10	Note legali.....	18

## 1 Informazioni sulla guida

Questa guida descrive la procedura per installare Sophos Anti-Virus sui computer Linux, NetWare e UNIX, in modo che la gestione sia affidata a Sophos Enterprise Console. Questa guida presume che i tool di gestione siano già installati, come spiegato nella *Guida di avvio avanzata di Sophos Endpoint Security and Control*.

Per eseguire l'upgrade, consultare la *Guida all'upgrade rapido di Sophos Endpoint Security and Control* oppure la *Guida all'upgrade avanzata di Sophos Endpoint Security and Control* invece di questa guida.

La documentazione Sophos è pubblicata nel link <http://www.sophos.it/support/docs/> e nei CD Sophos.

## **2 Requisiti di sistema**

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

È necessario disporre della connessione Internet al fine di scaricare il software di installazione dal sito web di Sophos.

## 3 Protezione dei computer con sistema operativo Linux

Per proteggere i computer con sistema operativo Linux, occorre:

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

### 3.1 Creazione di un pacchetto di distribuzione

In questa sezione si presuppone che si sia eseguito il download di Sophos Anti-Virus, secondo quanto spiegato nella *Guida all'avvio avanzato di Sophos Endpoint Security and Control*

È possibile utilizzare lo script **mkinstpkg** per creare un pacchetto di distribuzione per i propri utenti finali. Questo script richiede informazioni sulle modalità di installazione di Sophos Anti-Virus sui computer con sistema operativo Linux, e le risposte ottenute vengono 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 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 in cui è stato scaricato Sophos Anti-Virus, conosciuto come percorso bootstrap:
  - a) In Enterprise Console, dal menu **Visualizza**, cliccare su **Percorsi Bootstrap**.  
Nella finestra di dialogo **Percorsi Bootstrap**, la colonna **Percorso** visualizza il percorso del 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 directory nel boot di sistema, utilizzare i tool specifici della distribuzione oppure modificare fstab.
4. Passare al percorso bootstrap.
5. Per creare un pacchetto di distribuzione nel formato tar, chiamato savinstpkg.tgz, digitare:  

```
./mkinstpkg.sh
```

  
Per creare un pacchetto di distribuzione nel formato RPM, chiamato 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 far gestire i computer da Enterprise Console.

7. Quando richiesto, inserire il percorso bootstrap (come visualizzato dai computer con sistema operativo Linux).

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

## 3.2 Installazione di Sophos Anti-Virus tramite pacchetto di distribuzione

Utilizzare il pacchetto per installare Sophos Anti-Virus in due modi:

- Manualmente su 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.

### 3.2.1 Installazione manuale di Sophos Anti-Virus

1. Utilizzare i propri tool per copiare il pacchetto di distribuzione nei computer sui quali si desidera installare Sophos Anti-Virus.
2. Quindi, accedere a ciascun computer come utente root.
3. Collocare il pacchetto di distribuzione in una directory temporanea e passare a questa cartella.
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 RPM package
```

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

### 3.2.2 Installazione automatica di Sophos Anti-Virus

- ❖ 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 si avvierà e sarà aggiornato automaticamente ad ogni aggiornamento del percorso del bootstrap.

## 4 Protezione dei server NetWare

Per proteggere i server NetWare, è necessario svolgere le seguenti operazioni per ciascun server:

- Installare Sophos Anti-Virus
- Caricare Sophos Anti-Virus.

### 4.1 Installazione di Sophos Anti-Virus

In questa sezione si presuppone che sia stata creata una directory in tutti i server NetWare che si desidera proteggere e che si sia eseguito il download di Sophos Anti-Virus in tale directory, secondo quanto spiegato in precedenza nella *Guida all'avvio avanzato di Sophos Endpoint Security and Control*.

Per installare Sophos Anti-Virus, svolgere la seguente procedura su tutti i server NetWare:

1. Per trovare il percorso della cartella condivisa in cui è stato scaricato Sophos Anti-Virus, conosciuto come percorso bootstrap:
  - a) In Enterprise Console, dal menu **Visualizza**, cliccare su **Percorsi Bootstrap**.  
Nella finestra di dialogo **Percorsi Bootstrap**, la colonna **Percorso** visualizza il percorso del bootstrap di tutte le piattaforme.
  - b) Annotare il percorso rilevante.
2. In un computer Windows che esegue il software di amministrazione di NetWare, accedere al server NetWare con diritti di accesso in scrittura equivalenti ad ADMIN.
3. Cambiare il percorso bootstrap.
4. Copiare tutti i file presenti in `\\NetWare server\SYS\SWEET`

### 4.2 Caricamento di Sophos Anti-Virus

Per caricare Sophos Anti-Virus, svolgere la seguente procedura su tutti i server NetWare:

1. In un computer Windows che esegue il software di amministrazione NetWare:

a) Aggiungere la directory di installazione predefinita al percorso di ricerca:

```
SEARCH
```

Viene visualizzato il numero di stringhe del percorso di ricerca. Tipo:

```
SEARCH ADD numero di stringhe successivo SYS:\SWEEP\
```

in cui il *numero di stringhe successivo* è il numero di stringhe + 1.

b) Caricamento di Sophos Anti-Virus:

```
LOAD SWEEP
```

Sophos consiglia di aggiungere al file AUTOEXEC.NCF questi comandi rispettandone l'ordine, in modo tale che Sophos Anti-Virus venga riavviato quando il server è riavviato.

Al primo caricamento di Sophos Anti-Virus, questo richiede di inserire i dati dell'amministratore.

2. Premere un tasto qualsiasi.

3. Nel prompt di accesso, digitare il nome distinto pienamente qualificato di un amministratore e premere INVIO.

4. Digitare la password dell'amministratore e premere INVIO.

Annotare il nome distinto pienamente qualificato dell'amministratore e (in un posto sicuro) la password. Sophos Anti-Virus accederà in qualità di tale utente tutte le volte che verrà avviato, consentendo di visualizzare l'albero completo di eDirectory.

Viene visualizzata la schermata **Sophos Anti-Virus**.

Sophos Anti-Virus è stato caricato. D'ora in poi, Sophos Anti-Virus verrà aggiornato automaticamente ogni volta che il percorso del bootstrap verrà aggiornato.

## 5 Come proteggere computer UNIX

Per proteggere i computer UNIX, è necessario installare una delle versioni di Sophos Anti-Virus.

### Sophos Anti-Virus versione 4

Questa versione:

- Supporta un'ampia gamma di piattaforme, come indicato nella pagina relativa ai requisiti di sistema del sito web di Sophos (<http://www.sophos.it/products/all-sysreqs.html>).
- Non può essere gestita tramite Enterprise Console.
- Non può essere aggiornata automaticamente.
- Non può essere pianificata per eseguire la scansione (eccezion fatta se si utilizza crontab).

Per proteggere i computer UNIX con la versione 4, andare alla sezione *Protezione dei computer UNIX tramite Sophos Anti-Virus versione 4* a pagina 10.

### Sophos Anti-Virus versione 7

Questa versione:

- Supporta una gamma limitata di piattaforme, come indicato nella pagina relativa ai requisiti di sistema del sito web di Sophos (<http://www.sophos.it/products/all-sysreqs.html>).
- Può essere gestita tramite Enterprise Console.
- Può essere aggiornata automaticamente.
- Può pianificare la scansione.

Per proteggere i computer UNIX con la versione 7, andare alla sezione *Protezione dei computer UNIX tramite Sophos Anti-Virus versione 7* a pagina 12.

## 6 Protezione dei computer UNIX tramite Sophos Anti-Virus versione 4

Per proteggere i computer UNIX con la versione 4, è necessario:

- Pubblicare Sophos Anti-Virus per UNIX su un server web.
- Installare Sophos Anti-Virus sui computer UNIX.

### 6.1 Pubblicazione di Sophos Anti-Virus su un server web

In questa sezione si presuppone che si sia eseguito il download di Sophos Anti-Virus, secondo quanto spiegato nella *Guida all'avvio avanzato di Sophos Endpoint Security and Control*

Si deve pubblicare Sophos Anti-Virus su un server web perché i computer possano accedervi tramite HTTP. Se ciò è già stato fatto, saltare questa sezione.

Per pubblicare Sophos Anti-Virus su un server web:

1. Per trovare il percorso della cartella condivisa in cui è stato scaricato Sophos Anti-Virus, conosciuto come percorso bootstrap:
  - a) In Enterprise Console, dal menu **Visualizza**, cliccare su **Percorsi Bootstrap**.  
Nella finestra di dialogo **Percorsi Bootstrap**, la colonna **Percorso** visualizza il percorso del bootstrap di tutte le piattaforme.
  - b) Annotare il percorso rilevante.
2. Rendere disponibile nel server web il percorso bootstrap, comprese le sottocartelle.
3. Specificare i nomi utente e le password per evitare l'accesso non autorizzato a questa cartella dal server web.

**Nota:** la documentazione del vostro server web descrive la modalità per la condivisione di una cartella sul web e per l'impostazione dei relativi nomi utente e password. Per ulteriori informazioni su come svolgere questa procedura, contattare il fornitore del server web.

Ora installare Sophos Anti-Virus.

### 6.2 Installazione di Sophos Anti-Virus

Per installare Sophos Anti-Virus, svolgere la seguente procedura su tutti i computer UNIX:

1. Andare al percorso della root del bootstrap pubblicata nel server web.
2. Copiare il file `emininstall.sh` in un percorso eseguibile quale `/etc`.  
Come riepilogo delle istruzioni, questo percorso viene visualizzato come *percorso*.
3. Tipo:  

```
cd percorso
```

4. Tipo:

```
chmod +x eminstall.sh
```

5. Nella directory /etc, creare un file chiamato eminstall.conf.

6. Aggiungere le seguenti righe a eminstall.conf:

```
EM install CID=percorso bootstrap
EM cache dir=percorso cache
SAV install dir=percorso di installazione
```

in cui:

- *Percorso bootstrap* è il percorso del bootstrap pubblicato nel server web.
- *Percorso cache* è il percorso della cache nella quale viene collocata una copia dei file di installazione quando viene eseguito un aggiornamento.
- *Percorso di installazione* è il percorso in cui verrà installato Sophos Anti-Virus.

**Nota:** i file contenuti in *percorso cache* non devono essere cancellati, altrimenti saranno scaricati di nuovo. Per questa ragione, si consiglia di non collocare i file nella directory /tmp, che qualche volta viene ripulita dal sistema UNIX.

7. Eseguire

```
eminstall.sh
```

Sophos Anti-Virus è installato.

8. Creare un'operazione cron per eseguire periodicamente eminstall.sh. In questo modo si controllerà la presenza degli aggiornamenti, che verranno installati automaticamente. Per ulteriori informazioni su come creare un'operazione cron, consultare l'articolo 12176 (in inglese) del knowledge base di Sophos (<http://www.sophos.com/support/knowledgebase/article/12176.html>).

## 7 Protezione dei computer UNIX tramite Sophos Anti-Virus versione 7

Per proteggere i computer UNIX con la versione 7, è necessario applicare uno dei seguenti metodi:

- Utilizzare un pacchetto di distribuzione.
- Utilizzare una tarball.

### 7.1 Protezione dei computer UNIX tramite un pacchetto di distribuzione

Per proteggere i computer UNIX tramite un pacchetto di distribuzione, è necessario:

- Eseguire la prima installazione di Sophos Anti-Virus in un server UNIX manualmente.
- Creare un pacchetto di distribuzione.
- Installare Sophos Anti-Virus sugli altri computer UNIX.

#### 7.1.1 Prima installazione manuale di Sophos Anti-Virus

In questa sezione si presuppone che si sia eseguito il download di Sophos Anti-Virus, secondo quanto spiegato nella *Guida all'avvio avanzato di Sophos Endpoint Security and Control*

Se Sophos Anti-Virus versione 4 è già installato nel server UNIX e lo si vuole sostituire con la versione 7, si deve prima disinstallarlo. Per informazioni su come svolgere tale operazione, consultare la *Guida di avvio di Sophos Anti-Virus UNIX* per la versione 4.

1. Per trovare il percorso della cartella condivisa in cui è stato scaricato Sophos Anti-Virus, conosciuto come percorso bootstrap:
  - a) In Enterprise Console, dal menu **Visualizza**, cliccare su **Percorsi Bootstrap**.  
Nella finestra di dialogo **Percorsi Bootstrap**, la colonna **Percorso** visualizza il percorso del bootstrap di tutte le piattaforme.
  - b) Annotare il percorso rilevante.
2. Accedere al server UNIX come utente root.
3. Montare il percorso bootstrap.
4. Passare al percorso bootstrap.
5. Eseguire lo script di installazione:

```
./install.sh
```

Quando richiesto, scegliere di abilitare la gestione remota.

Portata a termine l'installazione, in Enterprise Console, il server UNIX compare nel gruppo **Nessun gruppo**.

6. Se non si è già proceduto in tal senso, creare in Enterprise Console un nuovo gruppo nel quale inserire il server UNIX.
7. Trascinare il server dal gruppo **Nessun gruppo** a questo gruppo.
8. Per impostazione predefinita, questo gruppo ha già applicato un criterio di aggiornamento predefinito. Se è necessario modificare tale criterio, consultare la Guida in linea di Enterprise Console.
9. Nel server UNIX, avviare il primo aggiornamento:

```
/opt/sophos-av/bin/savupdate
```

Ora creare un pacchetto di distribuzione.

## 7.1.2 Creazione di un pacchetto di distribuzione

È possibile utilizzare lo script **mkinstpkg** per creare un pacchetto di distribuzione per i propri utenti finali. Questo script richiede informazioni sulle modalità di installazione di Sophos Anti-Virus sui computer con sistema operativo UNIX, e le risposte ottenute vengono 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 possibile creare un pacchetto in formato tar.

**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. Nel server UNIX in cui è installato Sophos Anti-Virus, cambiare la directory `/opt/sophosav/update/cache/Primary-unpacked`.
2. Per creare un pacchetto di distribuzione nel formato tar, chiamato `savinstpkg.tar`, digitare:  

```
./mkinstpkg.sh
```
3. Quando richiesto, scegliere di far gestire i computer da Enterprise Console.
4. Quando richiesto, inserire il percorso della cartella condivisa (come visualizzato dai computer con sistema operativo UNIX).

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

## 7.1.3 Installazione di Sophos Anti-Virus tramite pacchetto di distribuzione

Utilizzare il pacchetto per installare Sophos Anti-Virus in due modi:

- Manualmente su ciascun computer.
- Automaticamente su tutta la rete.

### 7.1.3.1 Installazione manuale di Sophos Anti-Virus

1. Utilizzare i propri tool per copiare il pacchetto di distribuzione nei computer sui quali si desidera installare Sophos Anti-Virus.
2. Quindi, accedere a ciascun computer come utente root.

3. Collocare il pacchetto di distribuzione in una directory temporanea e passare a questa cartella.
4. Per eseguire l'installazione dal pacchetto tar, digitare:

```
tar -xvf savinstpkg.tar
./sophos-av/install.sh
```

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

### 7.1.3.2 Installazione automatica di Sophos Anti-Virus

- ❖ 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 si avvierà e sarà aggiornato automaticamente ad ogni aggiornamento del percorso del bootstrap.

## 7.2 Protezione dei computer UNIX tramite una tarball

### 7.2.1 Download della tarball di Sophos Anti-Virus

1. Andare alla sezione <http://www.sophos.it/support/updates/>.
2. Digitare il nome utente e la password di MySophos.
3. Andare alla pagina web relativa ai download di Sophos Anti-Virus per UNIX e scaricare la tarball di Sophos Anti-Virus per UNIX.
4. Assicurarsi che la tarball si trovi in un percorso a cui si possa accedere dai computer UNIX da proteggere.

In alternativa, copiarlo su CD o DVD.

### 7.2.2 Installazione di Sophos Anti-Virus tramite tarball

Oltre alla tarball, questa sezione presuppone che Sophos Anti-Virus sia stato scaricato in una cartella condivisa, secondo quanto spiegato nella *Guida all'avvio avanzato di Sophos Endpoint Security and Control*.

Se Sophos Anti-Virus versione 4 è già installato nel computer UNIX e lo si vuole sostituire con la versione 7, per prima cosa è necessario disinstallarlo. Per informazioni su come svolgere tale operazione, consultare la *Guida di avvio di Sophos Anti-Virus UNIX* per la versione 4.

1. Per trovare il percorso della cartella condivisa in cui è stato scaricato Sophos Anti-Virus, conosciuto come percorso bootstrap:
  - a) In Enterprise Console, dal menu **Visualizza**, cliccare su **Percorsi Bootstrap**.  
Nella finestra di dialogo **Percorsi Bootstrap**, la colonna **Percorso** visualizza il percorso del bootstrap di tutte le piattaforme.
  - b) Annotare il percorso rilevante.
2. Accedere al computer UNIX come utente root.
3. Trovare la tarball scaricata in precedenza e decomprimerla:

```
tar -xvf tarball
```
4. Eseguire lo script di installazione:

```
./sophos-av/install.sh
```

Quando viene richiesto un percorso aggiornato, inserire l'indirizzo del percorso bootstrap.
5. Dare inizio al primo aggiornamento:

```
/opt/sophos-av/bin/savupdate
```

Portato a termine l'aggiornamento, in Enterprise Console, il computer UNIX compare nel gruppo **Nessun gruppo**.
6. Se non si è già proceduto in tal senso, creare in Enterprise Console un nuovo gruppo nel quale inserire il computer UNIX.
7. Trascinare il computer dal gruppo **Nessun gruppo** a questo gruppo.
8. Per impostazione predefinita, questo gruppo ha già applicato un criterio di aggiornamento predefinito. Se è necessario modificare tale criterio, consultare la Guida in linea di Enterprise Console.

Il computer UNIX è ora protetto. D'ora in poi, Sophos Anti-Virus verrà aggiornato automaticamente ogni volta che il percorso del bootstrap verrà aggiornato. Ripetere i passaggi dal 2 al 8 per tutti gli altri computer UNIX che si desidera proteggere.

## 8 Verifica dello stato della rete

Per verificare lo stato di salute della rete da Enterprise Console:

- ❖ Visualizzare il Pannello di controllo.

Se non già visualizzato, dal menu **Visualizza**, cliccare su **Pannello di controllo**.

Nel Pannello di controllo vengono visualizzati quanti computer:

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

## 9 Supporto tecnico

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

- Visitando il forum 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.

## 10 Note legali

Copyright © 2010 Sophos Group. Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere riprodotta, archiviata in un sistema di recupero, o trasmessa, in alcuna forma o in alcun mezzo, elettronico o meccanico, inclusi fotocopie, registrazione e altri mezzi, salvo che da un licenziatario autorizzato a riprodurre la documentazione in conformità con i termini della licenza, oppure previa autorizzazione scritta del titolare dei diritti d'autore.

Sophos e Sophos Anti-Virus sono marchi registrati di Sophos Plc e Sophos Group. Tutti gli altri nomi 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](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>

### **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<sup>10</sup>, 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>11</sup> know so we can promote your project in the DOC software success stories<sup>12</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>13</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>14</sup>, TAO<sup>15</sup>, CIAO<sup>16</sup>, and CoSMIC<sup>17</sup> web sites are maintained by the DOC Group<sup>18</sup> at the Institute for Software Integrated Systems (ISIS)<sup>19</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>20</sup> for the development of open-source software as part of the open-source software community<sup>21</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>22</sup> know.

Douglas C. Schmidt<sup>23</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. <http://www.the-it-resource.com/Open-Source/Licenses.html>
11. [mailto:doc\\_group@cs.wustl.edu](mailto:doc_group@cs.wustl.edu)
12. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
13. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
14. <http://www.cs.wustl.edu/~schmidt/ACE.html>
15. <http://www.cs.wustl.edu/~schmidt/TAO.html>
16. <http://www.dre.vanderbilt.edu/CIAO/>
17. <http://www.dre.vanderbilt.edu/cosmic/>
18. <http://www.dre.vanderbilt.edu/>
19. <http://www.isis.vanderbilt.edu/>

20. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
21. <http://www.opensource.org/>
22. <mailto:d.schmidt@vanderbilt.edu>
23. <http://www.dre.vanderbilt.edu/~schmidt/>

## **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.

## **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 © 1998–2006 The OpenSSL Project. All rights reserved.

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 licence [including the GNU Public Licence.]

**iMatix SFL**

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