

SOPHOS

simple + secure

Sophos Endpoint Security and Control 9.7

startup guide for Linux, NetWare, and UNIX

Document date: April 2011



Contents

1 About this guide.....	3
2 System requirements.....	4
3 Protecting Linux computers.....	5
4 Protecting NetWare servers.....	7
5 Deciding how to protect UNIX computers.....	9
6 Protecting UNIX computers with Sophos Anti-Virus version 4.....	10
7 Protecting UNIX computers with Sophos Anti-Virus version 7.....	12
8 Check the health of your network.....	16
9 Technical support.....	17
10 Legal notices.....	18

1 About this guide

This guide describes the procedure for installing Sophos Anti-Virus on Linux, NetWare, and UNIX computers, so that it is managed by Sophos Enterprise Console. The guide assumes that you have installed the management tools, as explained in the *Sophos Endpoint Security and Control advanced startup guide*.

To upgrade, go to the **Endpoint Security and Control Upgrade Center** at <http://www.sophos.com/support/upgrades/>, instead of reading this guide.

Sophos documentation is published at <http://www.sophos.com/support/docs/>.

2 System requirements

For system requirements, go to the system requirements page of the Sophos website (<http://www.sophos.com/products/all-sysreqs.html>).

You must have internet access in order to download the installation software from the Sophos website.

3 Protecting Linux computers

To protect Linux computers, you must:

- Create a deployment package.
- Install Sophos Anti-Virus on the Linux computers.

3.1 Create a deployment package

This section assumes that you have downloaded Sophos Anti-Virus, as explained in the *Sophos Endpoint Security and Control advanced startup guide*.

You can use the **mkinstpkg** script to create a deployment package for your end-users. This script prompts you for information about how Sophos Anti-Virus will be installed on your Linux computers, and the answers gathered are inserted into the deployment package. When the end-user installs from this deployment package, it will not prompt for any information and will set up both the update location and credentials correctly. You can create a package in tar or RPM format.

Note: The **mkinstpkg** script is for use within your organization only. Please read the license agreement and legal notice displayed by the **mkinstpkg** script.

To create a deployment package:

1. To find out the path of the shared folder to which Sophos Anti-Virus has been downloaded, known as the bootstrap location:
 - a) In Enterprise Console, on the **View** menu, click **Bootstrap Locations**.

In the **Bootstrap Locations** dialog box, the **Location** column displays the path of the bootstrap location for each platform.
 - b) Make a note of the relevant path.
2. Log on to your Linux server as root.
3. Mount the bootstrap location.
To enable this folder to be mounted automatically on system boot, use distribution-specific tools for doing so, or edit `fstab`.
4. Change to the bootstrap location.
5. To create a deployment package in tar format, called `savinstpkg.tgz`, type:
./mkinstpkg.sh

To create a deployment package in RPM format, called `savinstpkg-0.0-1.i586.rpm`, type:
./mkinstpkg.sh -r

Note: The filename might differ depending on the RPM setup.
6. When prompted, choose to have the computers managed by Enterprise Console.

7. When prompted for the location, enter the bootstrap location (as seen from the Linux computers).

Now you are ready to install Sophos Anti-Virus using this deployment package.

3.2 Installing Sophos Anti-Virus using the deployment package

You use the package to install Sophos Anti-Virus in one of two ways:

- Manually on each computer. This approach can be used with a package in RPM or tar format.
- Automatically across the network. This approach can be used only with a package in RPM format.

Note: On Red Hat Enterprise Linux version 6 64 bit, the following packages must be installed so that the installation of Sophos Anti-Virus succeeds:

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

3.2.1 Install Sophos Anti-Virus manually

1. Use your own tools to copy the deployment package to the computers where you want to install Sophos Anti-Virus.
2. Go to each computer and log in as root.
3. Place the deployment package in a temporary directory and change to that directory.
4. To install from the tar package, type:

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

To install from the RPM package, type:

```
rpm -i RPM package
```

The necessary files are copied from the server and Sophos Anti-Virus is installed. From now on, Sophos Anti-Virus will be updated automatically whenever the bootstrap location is updated.

3.2.2 Install Sophos Anti-Virus automatically

- To install Sophos Anti-Virus automatically from the deployment package, use one of the operating system administration tools that support remote deployment.

For more information, see the documentation for that tool.

Once Sophos Anti-Virus is installed, it will be started and will be updated automatically whenever the bootstrap location is updated.

4 Protecting NetWare servers

To protect NetWare servers, you must perform the following for each NetWare server:

- Install Sophos Anti-Virus.
- Load Sophos Anti-Virus.

4.1 Install Sophos Anti-Virus

This section assumes that you have created a directory on each NetWare server that you want to protect and have downloaded Sophos Anti-Virus to it, as explained in the *Sophos Endpoint Security and Control advanced startup guide*.

To install Sophos Anti-Virus, perform the following for each NetWare server:

1. To find out the path of the shared folder to which Sophos Anti-Virus has been downloaded, known as the bootstrap location:
 - a) In Enterprise Console, on the **View** menu, click **Bootstrap Locations**.
In the **Bootstrap Locations** dialog box, the **Location** column displays the path of the bootstrap location for each platform.
 - b) Make a note of the relevant path.
2. At a Windows computer that is running NetWare administrator software, log on to the NetWare server with write access rights equivalent to ADMIN.
3. Go to the bootstrap location.
4. Copy all the files there to \\NetWare server\SYS\SWEEP

4.2 Load Sophos Anti-Virus

To load Sophos Anti-Virus, perform the following for each NetWare server:

1. At a Windows computer that is running NetWare administrator software:
 - a) Add the default installation directory to the search path:
SEARCH
The number of strings in the search path is displayed. Type:
SEARCH ADD next string number SYS:\SWEEP
where *next string number* is the number of strings + 1.
 - b) Load Sophos Anti-Virus:
LOAD SWEEP

Sophos recommends that you add these commands in the same order to the AUTOEXEC.NCF file, so that Sophos Anti-Virus is restarted if the server is restarted.

The first time that you load Sophos Anti-Virus, it prompts you to enter administrator details.

2. Press any key.
3. At the login prompt, type the fully qualified distinguished name of an administrator and press ENTER.
4. Type the administrator password and press ENTER.

Make a note of the fully qualified distinguished name of the administrator and (in a secure place) the password. Sophos Anti-Virus will log in as this user every time it is started, enabling it to see the complete eDirectory tree.

The **Sophos Anti-Virus** screen is displayed.

You have loaded Sophos Anti-Virus. From now on Sophos Anti-Virus will be updated automatically whenever the bootstrap location is updated.

5 Deciding how to protect UNIX computers

To protect UNIX computers, you must install one of two versions of Sophos Anti-Virus.

Sophos Anti-Virus version 4

This version:

- Supports a wide range of platforms, as listed on the system requirements page of the Sophos website (<http://www.sophos.com/products/all-sysreqs.html>).
- Cannot be managed using Enterprise Console.
- Cannot be automatically updated.
- Cannot be scheduled to scan (apart from using crontab).

To protect UNIX computers with version 4, go to [Protecting UNIX computers with Sophos Anti-Virus version 4](#) (page 10).

Sophos Anti-Virus version 7

This version:

- Supports a narrow range of platforms, as listed on the system requirements page of the Sophos website (<http://www.sophos.com/products/all-sysreqs.html>).
- Can be managed using Enterprise Console.
- Can be automatically updated.
- Can be scheduled to scan.

To protect UNIX computers with version 7, go to [Protecting UNIX computers with Sophos Anti-Virus version 7](#) (page 12).

6 Protecting UNIX computers with Sophos Anti-Virus version 4

To protect UNIX computers with version 4, you must:

- Publish Sophos Anti-Virus for UNIX on a web server.
- Install Sophos Anti-Virus on the UNIX computers.

6.1 Publish Sophos Anti-Virus on a web server

This step assumes that you have downloaded Sophos Anti-Virus, as explained in the *Sophos Endpoint Security and Control advanced startup guide*.

You must publish Sophos Anti-Virus on a web server for computers to access via HTTP. If you have already done this, you can skip this step.

- To publish Sophos Anti-Virus on a web server, see Sophos support knowledgebase article 12134 (<http://www.sophos.com/support/knowledgebase/article/12134.html>).

Now install Sophos Anti-Virus.

6.2 Install Sophos Anti-Virus

To install Sophos Anti-Virus, perform the following at each UNIX computer:

1. Go to the root of the bootstrap location that you have published on the web server.
2. Copy the file `emininstall.sh` to an executable path location such as `/etc`.
For the remainder of these instructions, this location is shown as *path*.
3. Type:
`cd path`
4. Type:
`chmod +x emininstall.sh`
5. In the directory `/etc`, create a file called `emininstall.conf`.

6. Add the following lines to `emininstall.conf`:

```
EM install CID=bootstrap location
EM cache dir=cache path
SAV install dir=installation path
```

where:

- *bootstrap location* is the bootstrap location that you have published on the web server.
- *cache path* is the location of the cache where a copy of the installation files is placed when performing an update.
- *installation path* is the location where Sophos Anti-Virus is going to be installed.

Note: The files in *cache path* must not be deleted as this will cause them to be downloaded again. For this reason, you should not place the files in the `/tmp` directory, which is sometimes purged by the UNIX system.

7. Run

emininstall.sh

Sophos Anti-Virus is installed.

8. Create a cron job to run `emininstall.sh` periodically. This will check for updates and install them automatically. For more information on creating a cron job, see Sophos support knowledgebase article 12176 (<http://www.sophos.com/support/knowledgebase/article/12176.html>).

7 Protecting UNIX computers with Sophos Anti-Virus version 7

To protect UNIX computers with version 7, you must use one of the following methods:

- Use a deployment package.
- Use a tarball.

7.1 Protecting UNIX computers using a deployment package

To protect UNIX computers using a deployment package, you must:

- Install Sophos Anti-Virus on a UNIX server for the first time manually.
- Create a deployment package.
- Install Sophos Anti-Virus on the rest of the UNIX computers.

7.1.1 Install Sophos Anti-Virus for the first time manually

This section assumes that you have downloaded Sophos Anti-Virus, as explained in the *Sophos Endpoint Security and Control advanced startup guide*.

If Sophos Anti-Virus version 4 is already installed on your UNIX server, and you want to replace it with version 7, you must uninstall it first. For information about how to do this, see the *Sophos Anti-Virus UNIX startup guide* for version 4.

1. To find out the path of the shared folder to which Sophos Anti-Virus has been downloaded, known as the bootstrap location:
 - a) In Enterprise Console, on the **View** menu, click **Bootstrap Locations**.

In the **Bootstrap Locations** dialog box, the **Location** column displays the path of the bootstrap location for each platform.
 - b) Make a note of the relevant path.
2. Log on to your UNIX server as root.
3. Mount the bootstrap location.
4. Change to the bootstrap location.
5. Run the install script:
./install.sh

When prompted, choose to enable remote management.

When installation has finished, in Enterprise Console the UNIX server appears in the **Unassigned** group.

6. If you have not done so already, in Enterprise Console create a new group where you want to put the UNIX server.
7. Drag the server from the **Unassigned** group to this group.
8. By default, this group already has a default updating policy applied to it. If you need to edit the policy, see the Enterprise Console Help.
9. On the UNIX server, trigger the first update:
/opt/sophos-av/bin/savupdate

Now create a deployment package.

7.1.2 Create a deployment package

You can use the **mkinstpkg** script to create a deployment package for your end-users. This script prompts you for information about how Sophos Anti-Virus will be installed on your UNIX computers, and the answers gathered are inserted into the deployment package. When the end-user installs from this deployment package, it will not prompt for any information and will set up both the update location and credentials correctly. You can create a package in tar format.

Note: The **mkinstpkg** script is for use within your organization only. Please read the license agreement and legal notice displayed by the **mkinstpkg** script.

To create a deployment package:

1. On the UNIX server where you installed Sophos Anti-Virus, change to the directory `/opt/sophosav/update/cache/Primary-unpacked`.
2. To create a deployment package in tar format, called `savinstpkg.tar`, type:
./mkinstpkg.sh
3. When prompted, choose to have the computers managed by Enterprise Console.
4. When prompted for the location, enter the location of the shared folder (as seen from the UNIX computers).

Now you are ready to install Sophos Anti-Virus using this deployment package.

7.1.3 Installing Sophos Anti-Virus using the deployment package

You use the package to install Sophos Anti-Virus in one of two ways:

- Manually on each computer.
- Automatically across the network.

7.1.3.1 Install Sophos Anti-Virus manually

1. Use your own tools to copy the deployment package to the computers where you want to install Sophos Anti-Virus.

2. Go to each computer and log in as root.
3. Place the deployment package in a temporary directory and change to that directory.
4. To install from the tar package, type:
tar -xvf savinstpkg.tar
./sophos-av/install.sh

The necessary files are copied from the server and Sophos Anti-Virus is installed. From now on, Sophos Anti-Virus will be updated automatically whenever the bootstrap location is updated.

7.1.3.2 Install Sophos Anti-Virus automatically

- To install Sophos Anti-Virus automatically from the deployment package, use one of the operating system administration tools that support remote deployment.
For more information, see the documentation for that tool.

Once Sophos Anti-Virus is installed, it will be started and will be updated automatically whenever the bootstrap location is updated.

7.2 Protecting UNIX computers using a tarball

7.2.1 Download the Sophos Anti-Virus tarball

1. Go to <http://www.sophos.com/support/updates/>.
2. Type your MySophos username and password.
3. Go to the web page for Sophos Anti-Virus for UNIX downloads, and download the Sophos Anti-Virus for UNIX tarball.
4. Ensure that the tarball is in a location that can be accessed from the UNIX computers that you want to protect.
Alternatively, copy it to a CD or DVD.

7.2.2 Install Sophos Anti-Virus using the tarball

As well as the tarball, this section assumes that you have downloaded Sophos Anti-Virus to a shared folder, as explained in the *Sophos Endpoint Security and Control advanced startup guide*.

If Sophos Anti-Virus version 4 is already installed on your UNIX computer, and you want to replace it with version 7, you must uninstall it first. For information about how to do this, see the *Sophos Anti-Virus UNIX startup guide* for version 4.

1. To find out the path of the shared folder to which Sophos Anti-Virus has been downloaded, known as the bootstrap location:
 - a) In Enterprise Console, on the **View** menu, click **Bootstrap Locations**.

In the **Bootstrap Locations** dialog box, the **Location** column displays the path of the bootstrap location for each platform.

b) Make a note of the relevant path.

2. Log on to your UNIX computer as root.
3. Locate the tarball that you downloaded earlier and untar it:

```
tar -xvf tarball
```

4. Run the install script:
./sophos-av/install.sh

When prompted for an update location, enter the address of the bootstrap location.

5. Trigger the first update:
/opt/sophos-av/bin/savupdate

When updating has finished, in Enterprise Console the UNIX computer appears in the **Unassigned** group.

6. If you have not done so already, in Enterprise Console create a new group where you want to put the UNIX computer.
7. Drag the computer from the **Unassigned** group to this group.
8. By default, this group already has a default updating policy applied to it. If you need to edit the policy, see the Enterprise Console Help.

You have protected this UNIX computer. From now on, Sophos Anti-Virus will be updated automatically whenever the bootstrap location is updated. Now repeat steps 2–8 for the other UNIX computers that you want to protect.

8 Check the health of your network

To check the health of your network from Enterprise Console:

- View the Dashboard.

If it is not already displayed, on the **View** menu, click **Dashboard**.

The Dashboard shows you how many computers:

- Have detected threats.
- Are out of date.
- Do not comply with policies.

9 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>.
- Download the product documentation at <http://www.sophos.com/support/docs/>.
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

10 Legal notices

Copyright © 2011 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.com or via the web at <http://www.sophos.com/support/queries/enterprise.html>. A copy of the license agreement for any such included software can be found at <http://opensource.org/licenses/cpl1.0.php>

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, 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 us¹⁰ know so we can promote your project in the DOC software success stories¹¹.

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 companies¹² 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 ACE¹³, TAO¹⁴, CIAO¹⁵, and CoSMIC¹⁶ web sites are maintained by the DOC Group¹⁷ at the Institute for Software Integrated Systems (ISIS)¹⁸ and the Center for Distributed Object Computing of Washington University, St. Louis¹⁹ for the development of open-source software as part of the open-source software community²⁰. 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 me²¹ know.

Douglas C. Schmidt²²

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
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/>

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.

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.

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

Original SSLeay license

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

This package is an SSL implementation written by Eric Young (ey@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>>.