SOPHOS

Security made simple.

Sophos Enterprise Console
quick startup guide

Product version: 5.5

Contents

1 About this guide

This guide tells you how to protect your network with Sophos security software.

The guide is for you if you are installing the software for the first time.

If you are upgrading, see the *Sophos Enterprise Console upgrade guide* instead.

Other documents you might need

If you have a very large network, you may want to consider the installation options in the *Sophos Enterprise Console advanced startup guide*.

Sophos documentation is published at http://www.sophos.com/en-us/support/documentation.aspx.

2 What do I install?

To protect your network, you install:

- **Sophos Enterprise Console** on your server. This enables you to install and manage Sophos security software.
- **Sophos security software** on your endpoint computers. This protects the computers against threats and sends alerts to Enterprise Console.
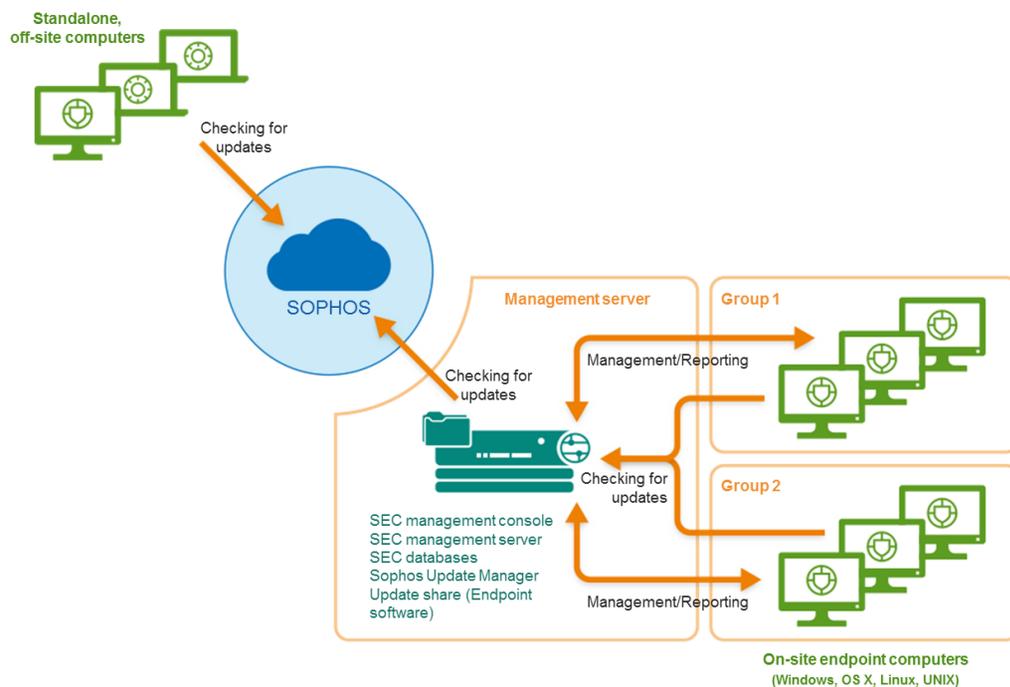
3 What are the key steps?

You carry out these key steps:

- Download the Enterprise Console installer.
- Check the system requirements.
- Create the accounts you need.
- Prepare for installation.
- Install Enterprise Console.
- Download security software.
- Create computer groups.
- Set up security policies.
- Search for computers.
- Prepare to protect computers.
- Protect computers.
- Check the health of your network.

4 Download the Enterprise Console installer

4.1 If you have a Sophos license

1. Log in to https://www.sophos.com/en-us/support/downloads.aspx with your Sophos ID.

   Note: If you need help with your Sophos ID, see Sophos knowledgebase article 111195.

2. If you have logged in for downloads before, you see the **Product Downloads and Updates** page.

   Note: If this is your first time, you see your profile. Click **Endpoint and Server Protection** and then **Downloads and Updates**.

3. Under **Console**, click the link for **Sophos Enterprise Console** and download the installer.

4.2 If you want to evaluate Enterprise Console

1. Go to http://www.sophos.com/en-us/products/free-trials/endpoint-protection.aspx.
2. Complete the registration form.

   After you submit the registration form, your evaluation credentials will be displayed. The credentials will also be sent to the email address you entered in the registration form. You will need them when setting up Enterprise Console.

3. Click **Download** and download the Enterprise Console installer.

5 Check the system requirements

Check the hardware, operating system and system software requirements before you begin installation.

5.1 Hardware and operating system

For hardware and operating system requirements, see the system requirements page of the Sophos website (http://www.sophos.com/en-us/products/all-system-requirements.aspx).

5.2 Microsoft system software

Enterprise Console requires certain Microsoft system software (for example, database software).

The Enterprise Console installer attempts to install this system software if it is not already available on your server. However, in some cases, software is incompatible with your server or needs to be installed manually.

Note: After you install the required system software, you may need to restart your computers. For more information, go to https://www.sophos.com/en-us/support/knowledgebase/65190.aspx.

SQL Server installation

The installer attempts to install SQL Server 2012 Express Edition with Service Pack 2 (SP2), unless you choose to use an existing instance of SQL Server 2005 Express or later. Note that:

- We recommend that you do not install SQL Server on a domain controller.
- If you want to install the Enterprise Console databases on a separate server, ensure that the SQL Server instance can be accessed remotely. For more information, go to https://www.sophos.com/en-us/support/knowledgebase/118473.aspx.

.NET Framework installation

The installer installs .NET Framework 4.5.2, unless version 4.x is already installed.

Important: As part of the .NET Framework 4.5.2 installation some system services (such as IIS Admin Service) may restart.

After .NET Framework 4.5.2 is installed, you may receive a message asking you to restart your computer. If you do, we recommend that you restart the computer immediately or shortly after the installation.

Microsoft Message Queuing installation

The installer attempts to install Microsoft Message Queuing (MSMQ), unless it is already installed.

Important: During MSMQ installation, the following services are stopped: MSDTC, MSSQLServer, SQLSERVERAGENT. This interrupts access to the default SQL Server database. You should ensure that the services can safely be stopped during installation. You should also check that they have restarted afterwards.

5.3 Port requirements

Enterprise Console requires certain ports to be open. For more information, go to http://www.sophos.com/en-us/support/knowledgebase/38385.aspx.

6 The accounts you need

Before you install Sophos software, you should create the user accounts you need:

- **Database account.** This is a Windows user account that enables Enterprise Console's management service to connect to the database. It is also used by other Sophos services.

  We recommend that you name the database account **SophosManagement**.

- **Update Manager account.** This is a Windows user account that enables your endpoint computers to access the folders where Enterprise Console puts software updates.

  We recommend that you name the Update Manager account **SophosUpdateMgr**.

6.1 Database account

The database account should:

- Be able to log onto the computer where you are going to install the Sophos Management Server (a component of Enterprise Console).
- Be able to read and write to the system temporary directory e.g. "\windows\temp\". By default members of "Users" have this right.
- Have a UPN (User Principal Name) associated with the account if it is a domain account.

All other rights and group memberships that it needs are granted automatically during installation.

Sophos recommends that the account:

- Is not set to expire and does not have any other logon restriction.
- Is not an administrative account.
- Is not changed after installation.
- Is named **SophosManagement**.

For recommendations and step-by-step instructions, go to
https://www.sophos.com/en-us/support/knowledgebase/113954.aspx.

6.2 Update Manager account

The Update Manager account should have Read access to the folder where Enterprise Console puts software updates. By default this is: \\[servername]\SophosUpdate

Sophos recommends that the account:

- Is not set to expire and does not have any other logon restriction.
- Is not an administrative account.
- Has a UPN (User Principal Name) associated with the account if it is a domain account.

- Is named **SophosUpdateMgr**.

For recommendations and step-by-step instructions, go to
https://www.sophos.com/en-us/support/knowledgebase/113954.aspx.

7 Prepare for installation

Prepare for installation as follows:

- Ensure that you are connected to the internet.
- Ensure that you have the Windows operating system CD and Service Pack CDs. You may be prompted for them during installation.
- If User Account Control (UAC) is enabled on the server, turn off UAC and restart the server.

Note: You can turn UAC on again after you have completed the installation and downloaded your security software.

8 Install Enterprise Console

To install Enterprise Console:

1. At the computer where you want to install Enterprise Console, log on as an administrator:
   - If the server is in a domain, use a domain account that has local administrator rights.
   - If the server is in a workgroup, use a local account that has local administrator rights.

2. Find the Enterprise Console installer that you downloaded earlier.
3. Double-click the installer.
4. When you are prompted, click **Install**.

   The installation files are copied to the computer and a wizard starts.

5. The wizard guides you through installation. You should do as follows:

   a) Accept the defaults wherever possible.

   b) On the **Components Selection** page, ensure that all the components are selected.

   c) On the **System Property Checks** page, review the system check results and take action if necessary. For more information about the system check results, go to http://www.sophos.com/en-us/support/knowledgebase/113945.aspx.

   d) On the **Database Details** page, enter the details of the database account you created in Database account (page 10).

   e) On the **Sophos Update Manager Credentials** page, enter the details of the Update Manager account you created in Update Manager account (page 10).

6. When installation is complete, you may be prompted to restart. Click **Yes** or **Finish**.

Important: The Sophos Auditing database, **SophosSecurity**, must be present and running side by side with the other Enterprise Console databases, even if you don't intend to use the Sophos Auditing feature. This is because the database is used for enhanced access control as well as for logging audit events.

9 Enhance database security

Audit the database

In addition to the protection built into the Enterprise Console databases, we recommend setting additional protection at the SQL Server instance level (if not already in place) to audit user activities and changes on your SQL Server.

For example, if you are using an Enterprise edition of SQL Server 2008, you can use the SQL Server Audit feature. Earlier versions of SQL Server support login auditing, trigger-based auditing, and event auditing by using a built-in trace facility.

For more information about features that you can use for auditing activities and changes on your SQL Server system, see the documentation for your version of SQL Server. For example:

- SQL Server Audit (Database Engine)
- Auditing (Database Engine), SQL Server 2008 R2
- Auditing in SQL Server 2008
- Auditing (Database Engine), SQL Server 2008

Encrypt connections to the database

We strongly recommend that you encrypt connections between any clients and the Enterprise Console databases. For more information, see the SQL Server documentation:

- Enable Encrypted Connections to the Database Engine (SQL Server Configuration Manager)
- Encrypting Connections to SQL Server 2008 R2
- How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console

Control access to the database backups

Ensure proper, restrictive access control to any database backups or copies. This will ensure that unauthorized users cannot access the files, tamper with them, or accidentally delete them.

Note: The links in this section lead to information maintained by third parties and are provided for your convenience. Although we try to review the accuracy of the links periodically, the links may change without our knowledge.

10 Install an additional remote management console

You might want to install another instance of the Sophos Enterprise Console management console on another computer, so that you can manage networked computers conveniently. If you do not want to, skip this section.

Important: You must install the same version of Enterprise Console as is running on your management server.

Note: The new console will need to access the server on which you installed the Enterprise Console management server. If that server runs a firewall, you might need to configure the firewall to ensure that access is possible. For instructions on how to add a firewall rule to allow DCOM traffic from the remote console to the management server, see knowledgebase article 49028.

To install an additional management console:

If User Account Control (UAC) (on Windows Server 2008 or later and Windows Vista or later) is turned on, turn it off and restart the computer. You can turn UAC on again after you have installed the management console.

Log on as an administrator.

- If the computer is in a domain, use a domain account that has local administrator rights.

- If the computer is in a workgroup, use a local account that has local administrator rights.

1. Locate the Enterprise Console installer that you downloaded earlier and double-click it.

2. Extract the installation files to the suggested destination folder or another one of your choice. The folder must be on this computer.

   An installation wizard guides you through installation. Accept the default options, except as shown below:

   a) On the **Components Selection** page, make sure that **Management Console** is selected and **Management Server** and **Database** are not selected.

   b) On the **Management Server** page, enter the name of the server on which you installed the Enterprise Console management server.

      Note: If you changed the port during the management server installation, make sure that you specify the same port on this page.

   c) If you are in a domain environment, enter the user account that is used to access the Enterprise Console databases.

      The account is the one that you entered when you installed the Enterprise Console databases. It is the same as that used by the Sophos Management Host service on the server on which you installed the Enterprise Console management server.

When the wizard has finished, log off or restart the computer (the final page in the wizard shows which). When you log on again, Enterprise Console opens automatically. If the **Download Security Software Wizard** runs, cancel it.

If you turned off User Account Control before installation, you can now turn it on again.

To enable other users to use the additional management console:

- Add them to the **Sophos Console Administrators** group and the **Distributed COM Users** group on the server on which you have installed the management server.

- Assign them to at least one Enterprise Console role and sub-estate.

11 Download security software

When you log back on (or restart) for the first time after installation, Enterprise Console opens automatically and a wizard runs.

Note: If you used Remote Desktop for installation, the console does not open automatically. Open it from the Start menu.

The wizard guides you through selecting and downloading the security software. You should do as follows:

1. On the **Sophos download account details** page, enter the username and password printed on your license schedule or your evaluation credentials. If you access the internet via a proxy server, select the **Access Sophos via a proxy server** check box and enter the proxy details.
2. On the **Platform selection** page, select only the platforms you need to protect now.

   When you click **Next**, Enterprise Console begins downloading your software.

3. On the **Downloading software** page, downloading progress is displayed. Click **Next** at any time.
4. On the **Import computers from Active Directory** page, select **Set up groups for your computers** if you want Enterprise Console to use your existing Active Directory computer groups.

Note: For information about protecting Windows 8 computers, go to http://www.sophos.com/en-us/support/knowledgebase/118261.aspx.

If you turned off User Account Control before installation, you can now turn it on again.

12 Create computer groups

If you used the **Download Security Software Wizard** to set up your computer groups (based on your Active Directory groups), skip this section. Go to Set up security policies (page 19).

Before you can protect and manage computers, you need to create groups for them.

1. If Enterprise Console is not already open, open it.
2. In the **Groups** pane (on the left-hand side of the console), ensure that the server name shown at the top is selected.
3. On the toolbar, click the **Create group** icon.

    A "New Group" is added to the list, with its name highlighted.

4. Type a name for the group.

To create further groups, go to the left-hand pane. Select the server shown at the top if you want another top-level group. Select a group if you want a sub-group within it. Then create and name the group as before.

13 Set up security policies

Enterprise Console applies "default" security policies to your computer groups. You do not have to change these policies unless you want to, with these exceptions:

- If you want to use Sophos Client Firewall, we recommend that you set up the firewall policy before deploying the firewall to computers.

- You must edit the application control, device control, patch or web control policies if you want to use these features. You can do this any time.

13.1 Set up a firewall policy

Note: During the installation of firewall, there will be a temporary disconnection of network adapters. The interruption may cause the disconnection of networked applications, such as Remote Desktop.

By default, the firewall blocks all non-essential connections. Therefore you must configure the firewall before you protect your computers.

1. In the **Policies** pane, right-click **Firewall**, and click **Create Policy**.

   A **New Policy** is added to the list, with its name highlighted. Type the name that you want to use for the policy.

2. Double-click the policy to edit it.

   A wizard is launched.

3. In the **Firewall Policy Wizard** we recommend that you make the following selections.

   a) On the **Configure firewall** page, select **Single location** unless you want the firewall to use different settings according to the location where you use it.

   b) On the **Operational Mode** page, select **Block inbound and allow outbound traffic**.

   c) On the **File and print sharing** page, select **Allow file and print sharing**.

14 Search for computers

If you used the **Download Security Software Wizard** to set up your computer groups (based on your Active Directory groups), skip this section. Go to Prepare to protect computers (page 21).

You must search for computers on the network before Enterprise Console can protect and manage them.

1. Click the **Discover computers** icon in the toolbar.
2. Select the method you want to use to search for computers.
3. Enter account details if necessary and specify where you want to search.

If you use one of the **Discover** options, the computers are placed in the **Unassigned** group.

15 Prepare to protect computers

Before you protect computers, you must prepare them as follows:

- Prepare for removal of third-party security software.
- Check that you have an account that can be used to install software.
- Prepare for installation of anti-virus software.

15.1 Prepare for removal of third-party security software

If you want the Sophos installer to remove any previously installed security software, do the following:

- If computers are running another vendor's anti-virus software, ensure that its user interface is closed.

  Note: HitmanPro.Alert may already be installed either as a standalone product or from Sophos Central. You should remove HitmanPro.Alert before applying on-premise management from Sophos Enterprise Console.

- If computers are running another vendor's firewall or HIPS product, ensure that it is turned off or configured to allow the Sophos installer to run.

If computers are running another vendor's update tool, you may want to remove it. See "Remove third-party security software" in the "Protecting computers" section of the Enterprise Console Help.

15.2 Check that you have an account that can be used to install software

You will be prompted to enter details of a Windows user account that can be used to install security software. It must:

- Have local administrator rights on computers you want to protect.
- Be able to log on to the computer where you installed Enterprise Console.
- Have Read permission to the location that computers will update from. To check this location, in the **Policies** pane, double-click **Updating**, and then double-click **Default**.

  Note: If the **Policies** pane (bottom left-hand side of the window) is not displayed, on the **View** menu, click **Endpoints**.

We recommend that the account:

- Is not a domain administrator account and is configured for constrained delegation.
- Has no administrative rights or any elevated privileges on the computer where Enterprise Console is installed.

- Has no Write or Modify permission to the location that computers will update from.

- Is used only for protecting computers and not used for general administrative tasks.

- Has its password changed frequently.

15.3 Prepare for installation of anti-virus software

You may need to prepare computers prior to installation of anti-virus software. For advice, see the Sophos endpoint deployment guide (https://docs.sophos.com/esg/enterprise-console/tools/deployment_guide/en-us/index.html), the section about preparing computers for deployment.

We recommend that the computers being protected have a firewall enabled.

Note: After the computers have been successfully protected and appear as managed in Enterprise Console, consider disabling any firewall exceptions created specifically to allow remote deployment on the computers.

16 Protect computers

This section tells you how to:

■ Protect Windows computers automatically.

■ Protect Windows computers or Macs manually.

■ Protect Linux computers (if your license includes this).

You can also use your own tools or scripts for installing protection on Windows computers. For details, go to https://www.sophos.com/en-us/support/knowledgebase/114191.aspx.

16.1 Protect Windows computers automatically

To protect computers:

1. Select the computers you want to protect.

2. Right-click and select **Protect computers**.

   Note: If computers are in the **Unassigned** group, simply drag them to your chosen groups.

3. A wizard guides you through the installation of Sophos security software. You should do as follows:

   a) On the **Welcome** page, click **Next**.

   b) On the **Installation Type** page, leave the option **Protection software** selected.

      "Protection" software is another term for the security software.

   c) On the **Select features** page, you can choose to install optional features.

      The current version of the firewall (included with Endpoint Security and Control 10.2 or earlier) cannot be installed on Windows 8 computers.

   d) On the **Protection summary** page, check for any installation problems. For help, see Troubleshooting (page 26).

   e) On the **Credentials** page, enter details of a Windows user account that can be used to install software on computers.

Installation is staggered, so that the process may not be complete on all the computers for some time.

When installation is complete, look at the list of computers again. In the **On-access** column, the word **Active** indicates that the computer is running on-access virus scanning.

16.2 Protect Windows computers or Macs manually

16.2.1 Locate the installers

If you have computers that you cannot protect from Enterprise Console, you can protect them by running an installer from the shared folder to which the security software has been downloaded. This folder is known as the bootstrap location.

To locate the installers:

1. In Enterprise Console, on the **View** menu, click **Bootstrap Locations**.

   A list of locations is displayed.

2. Make a note of the location for each operating system you want to protect.

16.2.2 Protect Windows computers manually

You must use an administrator account on the computers that you want to protect.

1. At each computer that you want to protect, browse to the bootstrap location, find `setup.exe` and double-click it.
2. In the **Sophos Setup** dialog box, in the **User account details**, enter details of the Update Manager account, **SophosUpdateMgr**, that you created to access the share where Enterprise Console puts software updates. You did this in Update Manager account (page 10).

   Tip: You can also use any low-privilege account that can access the bootstrap location. Enterprise Console will apply an updating policy that includes the right user account details later.

   Note: For information about command line parameters for the `setup.exe` file, see https://www.sophos.com/en-us/support/knowledgebase/12570.aspx.

16.2.3 Protect Macs manually

You must use an administrator account on the Macs that you want to protect.

1. At each Mac that you want to protect, browse to the bootstrap location. Copy the `Sophos Installer.app` installer file and the `Sophos Installer Components` directory to a preferred location (for example, the Desktop) and double-click it.

   A wizard guides you through installation.

2. Accept the default options. When prompted, enter the details of a user account that can install software on the Mac.

16.3 Protect Linux computers

For details of how to protect Linux computers (if your license permits this), see the *Enterprise Console startup guide for Linux and UNIX*.

17 Check the health of your network

To check the health of your network from Enterprise Console, do as follows.

1. On the menu bar, click the **Dashboard** icon (if the Dashboard is not already displayed).

   The Dashboard shows you how many computers:

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

18 Troubleshooting

When you run the **Protect computers wizard**, installation of security software can fail for a number of reasons:

- Automatic installation is not possible on that operating system. Perform a manual installation. See Protect Macs manually (page 24). For other operating systems (if your license permits you to protect them), see the *Sophos Enterprise Console startup guide for Linux and UNIX*.

- Operating system could not be determined. This may be because you did not enter your username in the format domain\username when finding computers.

- Firewall rules are blocking access needed to deploy the security software.

19 Get help with common tasks

This section tells you where you can find information on how to carry out common tasks.

Task	Document
Protect standalone computers	Enterprise Console advanced startup guide: *Protecting standalone computers* in Enterprise Console advanced startup guide
Configure Enterprise Console policies	Enterprise Console Help: Configuring policies
Deal with alerts	Enterprise Console Help: Dealing with alerts and errors
Clean up computers	Enterprise Console Help: Clean up computers now
Generate Enterprise Console reports	Enterprise Console Help: Generating reports

20 Technical support

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

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.

- Visit the Sophos support knowledgebase at www.sophos.com/en-us/support.aspx.

- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.

- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

21 Legal notices

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™ (henceforth referred to as "DOC software") are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University, Copyright (c) 1993-2014, all rights reserved. Since DOC software is open-source, freely available 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 any code built using DOC software that you release. No copyright statement needs to be provided if you just ship binary executables of your software products.

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 misappropriate the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, in a way 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 know so we can promote your project in the DOC software success stories.

The ACE, TAO, CIAO, DAnCE, and CoSMIC web sites are maintained by the DOC Group at the Institute for Software Integrated Systems (ISIS) and the Center for Distributed Object Computing of Washington University, St. Louis for the development of open-source software as part of the open-source software community. Submissions are provided by the submitter "as is" with no warranties whatsoever, including any warranty of merchantability, noninfringement of third party intellectual property, or fitness for any particular purpose. In no event shall the submitter be liable for any direct, indirect, special, exemplary, punitive, or consequential damages, including without limitation, lost profits, even if advised of the possibility of such damages. Likewise, 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. 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.

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 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. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, 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. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. 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

Boost Software License

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Common Public License

The Sophos software that is referenced 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 https://www.sophos.com/en-us/support/contact-support.aspx. A copy of the license agreement for any such included software can be found at 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.

Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Microsoft Public License (MS-PL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

   The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

   A "contribution" is the original software, or any additions or changes to the software.

   A "contributor" is any person that distributes its contribution under this license.

   "Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

   (A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

   (B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

   (A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

   (B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

   (C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

   (D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

   (E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

A copy of the MS-PL terms can be found at https://opensource.org/licenses/MS-PL.

OpenSSL Cryptography and SSL/TLS 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 © 1998–2016 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 (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 license 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.]

WilsonORMapper

Copyright © 2007, Paul Wilson

All rights reserved.

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

■ Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- 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.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT HOLDER 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.

Windows Template Library (WTL)

Copyright © Microsoft Corporation. All rights reserved.

The use and distribution terms for this software are covered by the Common Public License. Source code for this component is available here: https://sourceforge.net/projects/wtl/files/

zlib data compression library

Copyright © 1995–2013 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu