

# SOPHOS

## Sophos Control Center startup guide

Product version: 4.1

Document date: February 2011



# Contents

1 About this guide.....	3
2 System requirements.....	4
3 Installation.....	5
4 Protecting networked computers.....	8
5 Checking computers are protected.....	11
6 Setting up email alerts.....	12
7 Setting up scanning for potentially unwanted applications.....	13
8 Dealing with viruses.....	15
9 Setting up the firewall.....	16
10 Technical Support.....	18
11 Copyright.....	19

# 1 About this guide

This guide tells you how to protect your networked computers (both Windows computers and Macs) against viruses (including spyware), potentially unwanted applications, and other security threats.

If you have computers that never connect to your network, also refer to the *Sophos Endpoint Security and Control standalone startup guide*.

If you are upgrading from an earlier version of Sophos Control Center, refer to the *Sophos Control Center upgrade guide*.

For details of all the configuration options of Sophos Control Center, which are not covered in this guide, see Sophos Control Center Help.

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

## 2 System requirements

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

In addition, you must have internet access to download the software from the Sophos website.

Sophos Control Center and server components have the following other requirements:

- You must have access to and from the other computers on the network.
- It is recommended that a server operating system is used (such as, Windows Server 2003 or Windows Small Business Server 2011). Otherwise, the performance of Sophos Control Center is impacted.

**Important:** If you are installing Sophos Control Center on Windows 2008 Small Business Server (SBS), make sure you do not have Windows Live OneCare installed on the computer. To uninstall Windows Live OneCare, use the Add/Remove Programs utility from Windows Control Panel.

If you wish to use SQL Server, rather than SQL Server 2005 Express which is used by Sophos for their products, ensure it is installed and create a "SOPHOS" instance. For assistance on how to perform this please consult your SQL Server documentation or Microsoft Technical Support.

## 3 Installation

### 3.1 Preparing to install Sophos Control Center

Before you install Sophos Control Center, ensure:

- You have the username and password supplied by Sophos.
- You log on as an administrator or domain administrator, as appropriate, at the computer where you want to install Sophos Control Center.

**Note:** To protect computers that are in a workgroup, on any Windows platform, you must first perform the additional steps mentioned in the article:

<http://www.sophos.com/support/knowledgebase/article/29728.html>.

### 3.2 Preparing endpoint computers

Before you install the security software on the endpoint computers, ensure:

- Other vendor's anti-virus software is removed from all computers on which you want to install Sophos Anti-Virus.
- The operating system is configured, as required.

#### 3.2.1 Windows Vista and later

Sophos Anti-Virus has the following extra requirements on Windows Vista and later computers:

- Ensure the **Remote Registry** service is started and its startup type is set to **Automatic**. This service is not on by default in Windows Vista. This can be accessed via **Start, Control Panel, Administrative Tools, Services**. Scroll through the list of services and double-click **Remote Registry** service. In the **Remote Registry Properties** dialog box, on the **General** tab, in the **Startup type** field, click the drop-down arrow and select **Automatic**. Click **Apply**. Click **Start** and click **OK**.
- Turn off **User Account Control**. This can be accessed via **Start, Control Panel, User Accounts, Turn User Account Control on or off**. After installation is complete, you should turn it on.
- Open **Windows Firewall with Advanced Security**. This can be accessed via **Start, Control Panel, Administrative Tools**. Change the **Inbound rules** to enable the following:

Rule Name	Profile
Remote Administration (NP-In)	Domain
Remote Administration (NP-In)	Private

Rule Name	Profile
Remote Administration (RPC)	Domain
Remote Administration (RPC)	Private
Remote Administration (RPC-EPMAP)	Domain
Remote Administration (RPC-EPMAP)	Private

**Note:** When installation is complete, you should disable these again.

### 3.2.2 Windows XP

You must perform the following steps on any Windows XP computer with or without a service pack:

- Remove any other vendor's firewall software, except Windows Firewall, from all Windows XP computers on which you want to install Sophos Client Firewall.
- Disable Simple File Sharing.

To find out how to do this, see <http://www.sophos.com/support/knowledgebase/article/12837.html>.

#### Windows XP with Service Pack 2

On a computer with Windows XP Service Pack 2, if Windows Firewall is turned on, and you **do not** intend to install Sophos Client Firewall on this computer, you must do the following:

- Enable File and Printer Sharing for Microsoft Networks.
- Add the following program exception:

C:\Program Files\Sophos\Remote Management System\RouterNT.exe

To find out how to do this, see <http://www.sophos.com/support/knowledgebase/article/11075.html>.

### 3.2.3 Windows Server 2003 with Service Pack 1

If Windows Firewall is turned on, you must do the following:

- Enable File and Printer Sharing for Microsoft Networks.
- Add the following program exception:

C:\Program Files\Sophos\Remote Management System\RouterNT.exe

To find out how to do this, see <http://www.sophos.com/support/knowledgebase/article/11075.html>.

### 3.2.4 Windows 2000

- Remove any other vendor's firewall software, except Windows Firewall, from all Windows 2000 computers on which you want to install Sophos Client Firewall.

### 3.2.5 Windows 98 SE

- Remove any existing installation of Sophos Anti-Virus. To do this, use the Add/Remove Programs utility accessed via Windows Control Panel.

## 3.3 Installing Sophos Control Center

First install Sophos Control Center, which enables you to download, deploy, and manage anti-virus and firewall software.

1. Visit the Sophos product download page at <http://www.sophos.com/support/updates> and type the username and password supplied to you by Sophos.

Follow the links to download your Sophos Small Business Solutions product installer, then run it.

2. On the extractor (**Sophos Small Business Edition installer**) confirm the path for extraction of installation files (this must be on the same computer where you are installing Sophos Control Center) then click **Install**.
3. On the **Welcome** page, click **Next**.

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

4. On the **Setup Type** page, select **Complete** to install all the program features.

**Note:** If you want to manage security software from another computer, you can copy the installer to that computer, run it and select **Management Console only**.

Click **Next** and continue the wizard again with default options.

5. When installation is complete, click **Finish** to log off automatically. If you want to log off later, clear the **Log off now** check box before you click **Finish**.

Sometimes, it is necessary to restart Windows instead of simply logging off. In this case, the check box is not displayed, and a subsequent message asks you if you want to restart Windows now or later.

6. When you log on again, log on as the same user. The Sophos network protection wizard starts automatically.

For information on protecting networked computers, see [Protecting networked computers](#) (page 8).

## 4 Protecting networked computers

When you log on for the first time after installing, Sophos Control Center opens automatically and the Sophos network protection wizard starts. This wizard enables you to protect networked computers.

1. On the **Welcome** page, click **Next**.
2. On the **Sophos download account details** page, enter the username and password that were supplied to you by Sophos and click **Next**.

Sophos Control Center downloads the software to a folder on the computer that you are currently using and distributes it from there to other computers. The location differs based on the operating system:

- Windows 2000, XP, and 2003:  
C:\Documents and Settings\All Users\Application Data\Sophos\Update Manager\Update Manager\CIDs\
- Windows Vista and later:  
C:\ProgramData\Sophos\Update Manager\Update Manager\CIDs\

If you use a proxy server to connect to the Internet, select **Access Sophos via a proxy server** and enter the proxy details.

3. On the **Platform selection** page, select the software for the operating systems running on your computer.
  - The option **Windows 2000 and later** is selected by default.
  - If you have Mac OS X computers, select the Mac OS X check box. This will enable you to install anti-virus software on the computers later.
4. On the **Downloading software** page, a progress bar is displayed. Sophos Control Center downloads the software. When the download is complete, click **Next**.
5. On the **Windows user account details** page, enter details of an account that has administrative rights, that is valid on all networked computers, and can be used to install software on them. This is not the same as the Sophos account that you used earlier. In many cases, you can use the account that you logged on with before you began installation.
6. On the **Protect computers** page, the wizard searches for computers on which the software can be installed automatically.

Only Windows 2000 and later computers are listed on this page, as automatic installation is not possible on Windows 98 or Mac computers.

By default, all of the computers are selected for protection. You can clear the check box next to any computer on which you do not want to have protection. To select or clear all the check boxes in the list, select or clear the check box in the **Protect** column heading.

7. On the **Select features** page, select the features you want to install:

- Anti-virus protection (selected by default).
- Sophos Client Firewall protection (if your license includes it).

**Note:** You will have to restart each computer where you choose to install Sophos Client Firewall, to activate the firewall.

- Competitor removal tool.

Click **Next**.

8. If there are computers listed on the **Computers you must protect manually** page, click **Print** to print out the list of these computers, click **Save As** to save a copy of the list, or make a note of them. Click **Next** and follow the wizard.

Sophos Control Center installs the software automatically on the computers that you selected.

As anti-virus and firewall protection is applied to each computer, a blue computer icon next to the computer name is displayed and the **Up to date** column displays the word **Yes**.

For information on how to protect computers manually, see [Protecting networked computers manually](#) (page 9).

## 4.1 Protecting networked computers manually

You can protect the computers manually.

1. Go to each of the computers on the list that you printed out or saved. Browse to the folder where the Sophos Control Center makes anti-virus and firewall software and updates available. By default, the folders are:

Operating System	Folder
Windows 2000 and later	\\[server name]\sophosUpdate\CIDs\Sxxx\EECSXP
Windows 98	\\[server name]\sophosUpdate\CIDs\Sxxx\ES9X
Mac OS X	smb://[server name]/sophosUpdate/CIDs/Sxxx/ESCOSX

Where:

[server name] is the name of the computer where you installed Sophos Control Center.

[Sxxx] is the number generated while downloading, for example, S000.

2. Double-click setup.exe (on Windows) or Sophos Anti-Virus.mpkg (on Mac OS X).

If you are installing on Mac OS X 10.2 or later, you must copy the Sophos Anti-Virus.mpkg to the Mac, and perform the installation there.

You can also now protect computers that are not always on the network ([Protecting computers that sometimes connect to your network](#) (page 10)).

## 4.2 Protecting computers that sometimes connect to your network

Computers that sometimes connect to your network (for example, laptops that are used away from the office, but are also brought into the office) can be protected even when they are not on the network.

All computers on which you have installed anti-virus and firewall software are already configured to get their anti-virus and firewall updates directly from Sophos when they are not connected to your network.

If there are computers that sometimes connect to your network, on which you have not yet installed anti-virus or firewall software, you should protect them the next time they are connected to your network. This is explained in the Sophos Control Center Help, in the section about protecting new computers.

## 5 Checking computers are protected

You can check that your networked computers are protected against threats by using the dashboard.

The dashboard provides an at-a-glance view of the network's security status. You can configure the threshold values for the dashboard to warn and send alert messages when a threshold value is reached.

To show or hide the dashboard, click the **Dashboard** button on the toolbar.

For information on how to configure dashboard and a complete list of icons that are displayed and their status, see Sophos Control Center Help.

## 6 Setting up email alerts

By default, desktop alerts are displayed only on the computer where the threat is found. You can configure Sophos Control Center so users you choose can also receive an email alert when a threat is found.

To configure email alerts for threats:

1. In the left pane, under **Configuration**, click **Configure scanning**.
2. In the **Configure scanning** dialog box, click **Messaging**.

The **Messaging** dialog box is displayed.

3. Click the **Email alerting** tab, select **Enable email alerting** to receive alerts by email.
4. In the **Messages to send** panel, select the events for which you want to send email alerts.

**Note:** The Suspicious behavior detection, Suspicious file detection, and Adware and PUA detection and cleanup settings apply only to Windows 2000 and later. The Other errors setting applies only to Windows.

5. In the **Recipients** panel, click **Add** or **Remove** to add or remove, respectively, email addresses to which email alerts should be sent. Click **Rename** to change an email address you have added.

**Note:** Mac OS X computers will send messages only to the first recipient in the list.

6. Click **Configure SMTP** to change the settings for the SMTP server and the language of the email alerts.
7. In the **Configure SMTP settings** dialog box, enter the details as described below.

- In the **SMTP server** text box, type the host name or IP address of the SMTP server. Click **Test** to send a test email alert.
- In the **SMTP sender address** text box, type an email address to which bounces and non-delivery reports can be sent.
- In the **SMTP reply-to address** text box, you can type in the text box an email address to which replies to email alerts can be sent. Email alerts are sent from an unattended mailbox.

**Note:** Linux and UNIX computers will ignore the SMTP sender and reply-to addresses and use the address root@<hostname>.

- In the **Language** panel, click the drop-down arrow, and select the language in which email alerts should be sent.

You can also configure Sophos Control Center to send email alerts about the network status based on the threshold level reached on the Dashboard, for information see the Manage notifications section in Sophos Control Center Help.

## 7 Setting up scanning for potentially unwanted applications

By default, Sophos Anti-Virus detects viruses, Trojans, spyware, and worms. You can also configure it to detect potentially unwanted applications (PUAs).

**Note:** This option applies only to Sophos Anti-Virus running on Windows 2000 or later.

Sophos recommends that you begin by using a scheduled scan to detect potentially unwanted applications. This lets you deal safely with applications that are already running on your network. You can then enable on-access scanning for potentially unwanted applications to protect your computers in future.

### 7.1 Run a scheduled scan of the computers

1. In the left pane, under **Configuration**, click **Configure scanning**.
2. In the **Configure scanning** dialog box, in the **Scheduled scanning** panel, click **Add** to create a new scan, or select a scan in the list and click **Edit** to edit it.
3. In the **Scheduled scan** dialog box, click **Configure** (at the bottom of the page).
4. In the **Scanning and cleanup settings** dialog box, click the **Scanning** tab. In the **Scanning options** panel, select the **Scan for adware and PUA** check box and click **OK**.

When the scan is carried out, Sophos Anti-Virus may report some potentially unwanted applications. You can either authorize the applications or remove them from the computers.

### 7.2 Authorize applications that you want to use

You can choose to authorize applications that have been detected as adware/PUAs during a scheduled scan.

To authorize an application:

1. In the left pane, under **Configuration**, click **Configure scanning**.
2. In the **Configure scanning** dialog box, click **Authorization**.
3. In the **Authorization Manager** dialog box, do one of the following:
  - Select the application you want to authorize. Click **Add** to add it to the list of authorized applications.
  - If you cannot see the application, click **New entry**. In the dialog that opens, follow the link to Sophos's list of potentially unwanted applications. Find the application that you want to authorize and enter its name in the **Name** field.

### 7.3 Clean up applications that you do not want to use

You can cleanup applications that have been detected as an adware/PUA during a scheduled scan.

To clean up applications:

1. In the left pane, under **Action**, click **Resolve alerts and errors**.

The **Resolve alerts and errors** dialog box is displayed.

2. Select the check box for each application that you want to remove, or click **Select all**, and then click **Cleanup**.

This removes all known components of the selected applications from the selected computers. Cleanup might take some time.

**Note:** There are some applications that you cannot clean up using Sophos Control Center. In this case, go to the affected computer and clean up the application using Sophos Anti-Virus.

To fully clean up some applications consisting of several components from a computer, you may need to restart the computer. If this is the case, a message appears on the affected computer, giving an option to restart the computer immediately or later. The final cleanup steps are performed after the computer is restarted.

To find out more about a particular application on the Sophos website, in the **Resolve alerts and errors** dialog box, click the name of the application.

If you click **Acknowledge**, the selected applications are removed from the list. However, they are neither cleaned up nor authorized.

## 7.4 Enable on-access scanning for adware and potentially unwanted applications

1. In the left pane, under **Configuration**, click **Configure scanning**.

The **Configure scanning** dialog box is displayed.

2. Click **On-access scanning**.

The **On-access scan settings** dialog box is displayed.

3. In the **Scanning options** panel, select the **Scan for adware and PUA** check box. Click **OK**.

Some applications “monitor” files and attempt to access them frequently. If you have on-access scanning enabled, it detects each access and sends multiple alerts.

## 8 Dealing with viruses

You can clean up viruses as follows:

1. In Sophos Control Center, on the **Dashboard**, click the **Viruses/spyware** link.

In the **Resolve alerts and errors** dialog box, a list of infected computers, together with the virus details, is displayed.

2. Select the viruses that you want to clean up and click **Cleanup**.

This removes the virus from the file or boot sector that has been infected. However, cleanup of documents does not repair any changes that the virus has made in the document, and cleanup of programs should be used only as a temporary measure; you should subsequently replace cleaned programs from the original disks or a clean backup. Cleanup might take some time.

There are some viruses that you cannot clean up using Sophos Control Center. In this case, go to the affected computer and clean up the virus using Sophos Anti-Virus.

Sophos recommends that before you attempt to clean multi-component threats from the computers, you run a full scheduled scan of the computers to determine all components of multi-component threats.

To find out more about a particular virus on the Sophos website, in the **Resolve alerts and errors** dialog box, click the name of the virus.

## 9 Setting up the firewall

When you first install Sophos Client Firewall, it will be set to allow essential inbound and outbound traffic.

**Note:** Sophos Client Firewall does not support IPv6. Version 1 lets IPv6 packets through; versions 1.5 and 2.0 either block all or allow all IPv6 packets, depending on the configuration.

### 9.1 Configure the firewall

You can configure the firewall to allow or block the traffic as required. By default the firewall is set to allow essential inbound traffic and all outbound traffic.

To configure the firewall:

1. In the left pane, under **Configuration**, click **Configure firewall**.
2. On the Firewall configuration wizard, click **Next**.
3. On the **Configure firewall** page, choose any of the following options:

- **Single location**

Select for computers that are always on the network, for example, desktops.

- **Dual location**

Select if you want the firewall to use different settings according to the location where computers are used, for example, in the office (on the network) and out of the office. You may want to set up dual location for laptops.

- **Allow all traffic**

Select if you want to turn off the firewall and allow all traffic.

4. If you selected **Dual location** on the previous page, on the **Network identification** page, configure DNS or Gateway identification of your network.

**Note:** The **Network identification** page appears only if you select **Dual location**.

Sophos Control Center will then apply different firewall settings to the computers depending on whether they are on the network or not.

5. On the **Operational Mode** page, select a mode on how the firewall should handle inbound and outbound traffic.

- **Block inbound and allow outbound traffic**

This allows only essential traffic from your computers to access the network and internet but blocks any inbound traffic. Applications are not authenticated in this mode.

■ **Block inbound and outbound traffic**

If you select this mode, the firewall will block all outbound traffic, except for the applications you specify. Click **Trust** to the right of this option to add applications. For a "trusted" application, all network activity is allowed.

■ **Monitor**

This mode applies any specified rules to your computers, and also allows any unknown traffic to access the network and internet. The mode reports the information back to console. Use this mode to collect information about your network and create suitable rules.

■ **Custom**

This allows you to apply a custom configuration. Click **Advanced** to open advanced configuration for firewall.

**Note:** This is an advanced option, and you should only use it if you understand the effects of the changes you make.

For information on advanced firewall configuration, see the *Sophos Endpoint Security and Control Help*.

6. On the **File and print sharing** page, select **Allow file and print sharing** if you want to allow other computers on the local area network to access printers and shared folders on your computer.
7. If you selected **Dual location**, you will be prompted to the operational mode, and file and printer sharing (as mentioned in steps 5 and 6) for the secondary (off the network) location.

You can choose to run the wizard again, if you choose to modify any of the settings later.

After you have set up the firewall, you can view firewall events (for example, applications blocked by the firewall) in the **Firewall - Event Viewer**. For more information, see *Sophos Control Center Help*.

## 9.2 Dealing with items blocked by the firewall

Sophos Control Center may block applications or processes that you decide you want to run. If so, do as follows:

1. In Sophos Control Center, on the **Dashboard**, click the **Firewall** link.
2. In the **Firewall - Event viewer** dialog box, select the entry for the application you want to allow or create a rule for. Click **Create Rule**.
3. In the dialog box that appears, select whether to allow the application or create a rule for it using an existing preset.

## 10 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](mailto:support@sophos.com), including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

## 11 Copyright

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](mailto: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™**

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

Since DOC software is open-source, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn’t inform anyone that you’re using DOC software in your software, though we encourage you to let us<sup>10</sup> know so we can promote your project in the DOC software success stories<sup>11</sup>.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies<sup>12</sup> around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE<sup>13</sup>, TAO<sup>14</sup>, CIAO<sup>15</sup>, and CoSMIC<sup>16</sup> web sites are maintained by the DOC Group<sup>17</sup> at the Institute for Software Integrated Systems (ISIS)<sup>18</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>19</sup> for the development of open-source software as part of the open-source software community<sup>20</sup>. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me<sup>21</sup> know.

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

## **References**

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. [mailto:doc\\_group@cs.wustl.edu](mailto:doc_group@cs.wustl.edu)
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>

16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu/>
18. <http://www.isis.vanderbilt.edu/>
19. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
20. <http://www.opensource.org/>
21. <mailto:d.schmidt@vanderbilt.edu>
22. <http://www.dre.vanderbilt.edu/~schmidt/>

### **iMatix SFL**

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