

SOPHOS

SMALL BUSINESS EDITION

Sophos Control Center 4.0 Upgrade-Anleitung

Produktversion: 4.0
Stand: September 2009



Inhalt

1	Einleitung.....	3
2	Neuerungen in Sophos Control Center 4.0.....	4
3	Systemvoraussetzungen.....	5
4	Upgrade-Vorbereitung.....	6
5	Upgrade von Sophos Control Center.....	8
6	Prüfen, ob Computer geschützt sind.....	9
7	Einrichten der Firewall.....	10
8	Einrichten von Application Control.....	11
9	Einrichten von Device Control.....	13
10	Technischer Support.....	16
11	Copyright.....	17

1 Einleitung

In dieser Upgrade-Anleitung wird Folgendes beschrieben:

- Upgrade von Sophos Control Center 2.0 und 2.5 auf Sophos Control Center 4.0.
- Upgrade von Sophos Anti-Virus und Sophos Client Firewall (falls vorhanden) auf Sophos Endpoint Security and Control.

Wenn Sie über eine ältere Version von Sophos PureMessage verfügen und Ihre Lizenz ein Upgrade auf die neueste Version von Sophos PureMessage vorsieht, lesen Sie bitte die Upgrade-Anweisungen in der *Sophos PureMessage Upgrade-Anleitung*.

- Einrichten der neuen Sicherheitsfunktionen.

Konfigurationsoptionen von Sophos Control Center, die nicht in dieser Anleitung beschrieben werden, finden Sie in der *Hilfe zu Sophos Control Center*.

Sophos Begleitmaterial steht auf <http://www.sophos.de/support/docs/> zum Download bereit.

2 Neuerungen in Sophos Control Center 4.0

Die neue Version von Sophos Control Center weist folgende Merkmale auf:

Integration in neueste Endpoint Security-Software

Sie können die neue Version von Sophos Control Center gemeinsam mit Sophos Endpoint Security and Control, das aus den neuesten Versionen von Sophos Anti-Virus und Sophos Client Firewall besteht, auf Endpoints unter Windows 2000 und aufwärts einsetzen.

Dashboard

Die Benutzeroberfläche von Sophos Control Center kommt jetzt mit einem so genannten Dashboard daher, über das Sie den Sicherheitszustand Ihres Netzwerks stets im Blick haben. Sie können Grenzwerte festlegen, bei deren Erreichen auf dem Dashboard optische Warnungen angezeigt und Benachrichtigungen an die entsprechenden Computer gesendet werden. Die Konfiguration wird in der Hilfe zu Sophos Control Center beschrieben.

Application Control

Sophos Control Center kann Anwendungen erkennen und sperren, die Sie für den Einsatz im Unternehmen als unerwünscht betrachten. Weitere Informationen zu Application Control finden Sie unter [Einrichten von Application Control](#) (Seite 11).

Device Control

Anhand von Device Control können Sie das unerwünschte Anschließen unbekannter externer Hardwaregeräte, Wechselmedien und Wireless-Geräte verhindern. Weitere Informationen zu Device Control finden Sie unter [Einrichten von Device Control](#) (Seite 13).

Starten von Sophos PureMessage und Sophos für Microsoft SharePoint

Wenn Sophos PureMessage oder Sophos für Microsoft SharePoint auf demselben Computer installiert ist wie Sophos Control Center, können Sie diese Programme von Sophos Control Center aus starten.

3 Systemvoraussetzungen

Die Systemvoraussetzungen finden Sie auf der Sophos Website:

<http://www.sophos.de/products/all-sysreqs.html>.

Außerdem benötigen Sie Internetzugang, um die Software von der Sophos Website herunterladen zu können.

Für Sophos Control Center und Server-Komponenten gelten weitere Voraussetzungen:

- Es muss Zugriff auf und über die anderen Computer im Netzwerk bestehen.
- Es empfiehlt sich der Einsatz eines Serverbetriebssystems, z.B. Windows 2000 Server mit Service Pack 4 und aufwärts, Windows Server 2003 oder Windows Small Business Server 2003. Ansonsten könnte die Leistung von Sophos Control Center beeinträchtigt werden.

4 Upgrade-Vorbereitung

Hinweis:

- Es empfiehlt sich, von der vorhandenen Version von Sophos Control Center vor dem Upgrade ein Backup anzulegen.
- Nach Beendigung des Sophos Control Center Installationsassistenten ist auf dem Computer, auf dem das Upgrade durchgeführt wurde, entweder eine Neuansmeldung oder ein Neustart erforderlich.
- Wenn Sie auch Sophos Client Firewall installiert möchten, muss jeder Computer neu gestartet werden, auf dem die Firewall installiert wurde.

Jegliche ausstehenden Firewall-Alerts aus früheren Versionen von Sophos Control Center gehen beim Upgrade auf Sophos Control Center 4.0 verloren. Es empfiehlt sich daher, ausstehende Alerts vor dem Upgrade zu bereinigen.

4.1 Voraussetzungen

Vor dem Upgrade von Sophos Control Center und weiteren Upgrades auf allen von dieser Software zu verwaltenden Netzwerkcomputern müssen folgende Voraussetzungen erfüllt sein:

- Die [Systemvoraussetzungen](#) (Seite 5) werden erfüllt.
- Sie sind am Computer, auf dem Sophos Control Center upgegradet wird, als Administrator angemeldet.

Vorbereiten von Windows-Endpoints

Auf Endpoints, die unter Windows laufen, führen Sie bitte folgende Schritte durch:

- Deaktivieren Sie auf allen Windows XP-Systemen die einfache Dateifreigabe.
Nähere Anweisungen hierzu finden Sie unter <http://www.sophos.de/support/knowledgebase/article/12837.html>.
- Entfernen Sie auf Systemen mit Windows 2000- und höher, auf denen Sophos Client Firewall installiert werden soll, die Firewall-Software anderer Hersteller als Sophos (kurz: Fremdhersteller) – mit Ausnahme der Windows-Firewall.

Vorbereiten von Endpoints, auf denen Sophos Client Firewall nicht installiert werden soll

Wenn Sie über Windows XP-Systeme mit Service Pack 2 und aktivierter Windows-Firewall verfügen, auf denen Sophos Client Firewall **nicht** installiert werden soll, verfahren Sie wie folgt:

- Aktivieren Sie die Datei- und Druckerfreigabe für Microsoft-Netzwerke.
Nähere Anweisungen hierzu finden Sie unter <http://www.sophos.de/support/knowledgebase/article/11738.html>.
- TCP-Ports 8192, 8193 und 8194 müssen freigegeben sein.

- Fügen Sie folgende Programmausnahme hinzu: C:\Programme\Sophos\Remote Management System\RouterNT.exe.

Nähere Anweisungen hierzu finden Sie unter
<http://www.sophos.de/support/knowledgebase/article/11075.html>.

- Starten Sie die Computer neu, damit die Änderungen wirksam werden.

5 Upgrade von Sophos Control Center

Um Sophos Control Center unter Erhalt Ihrer Einstellung upzugraden, melden Sie sich am Computer, auf dem das Upgrade durchgeführt werden soll, als Administrator oder Domänenadministrator an, und verfahren Sie wie folgt:

1. Schließen Sie alle geöffneten Sophos Programme.
2. Rufen Sie die Seite mit den Sophos Produkt-Downloads auf (<http://www.sophos.de/support/updates/>) und geben Sie die Zugangsdaten ein, die Ihnen von Sophos übermittelt wurden.

Folgen Sie den Links zum Herunterladen des Sophos Control Center Installers und führen Sie ihn aus.

3. Klicken Sie im Eröffnungsfenster auf **Weiter**.

Der Sophos Control Center Installationsassistent leitet Sie durch die Installation. Übernehmen Sie die Voreinstellungen.

4. Wenn das Upgrade abgeschlossen ist, klicken Sie auf **Beenden**. Daraufhin werden Sie automatisch abgemeldet. Wenn Sie sich später abmelden möchten, deaktivieren Sie das Kontrollkästchen **Jetzt abmelden**, bevor Sie auf **Beenden** klicken.

In einigen Fällen reicht eine Abmeldung nicht aus und es ist ein Neustart des Systems erforderlich. In diesem Fall wird das Kontrollkästchen nicht angezeigt, sondern es öffnet sich ein Fenster mit einer Aufforderung zum Neustart des Systems, den Sie allerdings auch verschieben können.

5. Melden Sie sich bei der nächsten Anmeldung unter dem gleichen Namen an wie zuvor.

Nach der Installation von Sophos Control Center und dem Download der neuesten Endpoint-Softwareversion werden die Endpoints automatisch upgedatet.

Hinweis: Auf Endpoints unter Windows 98 und Mac OS X müssen Sie Sophos Anti-Virus manuell upgraden. Nähere Informationen zum manuellen Schutz von Computern finden Sie im Abschnitt *Sophos Control CenterStartup-Anleitung*.

6 Prüfen, ob Computer geschützt sind

Über das Dashboard können Sie prüfen, ob Ihre Computer im Netzwerk geschützt sind.

Das Dashboard bietet einen Überblick über den Sicherheitsstatus des Netzwerks. Sie können Grenzwerte festlegen, bei deren Erreichen auf dem Dashboard optische Warnungen angezeigt und Benachrichtigungen an die entsprechenden Computer gesendet werden.

Zum Ein- oder Ausblenden des Dashboards klicken Sie in der Symbolleiste auf **Dashboard**.

Die Konfiguration des Dashboards und die Symbole werden ausführlich in der Hilfe zu Sophos Control Center beschrieben.

7 Einrichten der Firewall

Sophos Client Firewall lässt nach der Erstinstallation standardmäßig den gesamten Datenfluss zu. Sie können die Firewall jedoch auch so konfigurieren, dass sie nur erwünschten Datenverkehr im Netzwerk zulässt.

In der *Hilfe zu Sophos Control Center* wird die Konfiguration der Firewall ausführlich beschrieben.

Hinweis: Das IPv6-Protokoll wird von Sophos Firewall nicht unterstützt. Version 1 von Sophos Client Firewall lässt IPv6-Pakete durch. In den Versionen 1.5 und 2.0 von Sophos Client Firewall werden je nach Konfiguration alle IPv6-Pakete entweder blockiert oder zugelassen.

8 Einrichten von Application Control

Mit Sophos Control Center können Sie Controlled Applications erkennen und sperren, d.h. legitime Anwendungen, die zwar kein Sicherheitsrisiko darstellen, die aber für Ihre Unternehmensumgebung ungeeignet sind. Zu solchen Anwendungen gehören Instant Messaging (IM) Clients, Voice Over Internet Protocol (VoIP) Clients, Digital Imaging Software, Medienplayer, Browser Plug-Ins usw.

Hinweis: Die Option beschränkt sich auf Sophos Endpoint Security and Control für Windows 2000 und aufwärts.

Die Liste der Controlled Applications wird von Sophos zur Verfügung gestellt und regelmäßig aktualisiert. Sie können keine neuen Anwendungen in die Liste aufnehmen. Auf Wunsch können Sie jedoch bei Sophos die Aufnahme einer Anwendung, die im Netzwerk kontrolliert werden soll, in die Liste beantragen. Nähere Informationen finden Sie im Support-Artikel **35330** (<http://www.sophos.de/support/knowledgebase/article/35330.html>).

Die Hilfe zu Sophos Control Center enthält weitergehende Informationen zu Application Control.

8.1 Einrichten von Application Control

Sie können Sophos Control Center dazu konfigurieren, bei Zugriff auf Controlled Applications in Ihrem Netzwerk zu scannen.

1. Klicken Sie links unter **Konfiguration** auf **Application Control konfigurieren**.

Das Dialogfenster **Application Control konfigurieren** wird geöffnet.

2. Legen Sie auf der Registerkarte **Scans** folgende Optionen fest:

- Zur Aktivierung von On-Access-Scans markieren Sie die Option **On-Access-Scans aktivieren**. Wenn gestartete Anwendungen erkannt, aber nicht gesperrt werden sollen, markieren Sie die Option **Erkennen, aber laufen lassen**.
- Zur Aktivierung von On-Access-Scans und geplanten Scans markieren Sie die Option **On-Demand-Scans und geplante Scans aktivieren**.

Hinweis: Ihre Einstellungen für die Antivirus- und HIPS-Richtlinie bestimmen, welche Dateien überprüft werden (d.h. die Erweiterungen und Ausnahmen).

3. Klicken Sie auf die Registerkarte **Autorisierungen** und wählen Sie die zu überwachenden Anwendungen.

Unter *Auswählen von Control Applications* (Seite 11) wird das Auswählen von Anwendungen näher beschrieben.

8.2 Auswählen von Control Applications

Standardmäßig sind alle Anwendungen zugelassen. Sie können die Anwendungen, die Sie kontrollieren möchten, folgendermaßen wählen:

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Application Control konfigurieren**.

2. Klicken Sie im Dialogfeld **Application Control konfigurieren** auf die Registerkarte **Autorisierungen**.

3. Wählen Sie einen **Anwendungstyp**, z.B. **Dateifreigabe**.

Eine vollständige Liste der Anwendungen in dieser Gruppe wird in der Liste **Zugelassen** angezeigt.

- Um eine Anwendung zu sperren, wählen Sie sie und verschieben Sie sie in die Liste **Gesperrt**, indem Sie auf die Schaltfläche **Hinzufügen** klicken.



- Um neue Anwendungen zu sperren, die Sophos diesem Typ in Zukunft hinzufügt, verschieben Sie **Neue Anwendungen** in die Liste **Gesperrt**.

- Um alle Anwendungen dieses Typs zu blockieren, verschieben Sie alle Anwendungen aus der Liste **Zugelassen** in die Liste **Gesperrt**, indem Sie auf die Schaltfläche **Alle hinzufügen** klicken.



Unter Sophos Control Center wird Deinstallieren von Controlled Applications näher beschrieben.

9 Einrichten von Device Control

Wichtig: Es ist davon abzuraten, Sophos Device Control mit Gerätesteuersoftware anderer Anbieter zu kombinieren.

Mit **Device Control** können Sie verhindern, dass Benutzer nicht zugelassene externe Hardware, Wechselmedien und Wireless-Geräte auf dem Computer einsetzen. So wird das Risiko unerwünschter Datenverluste minimiert. Zudem wird die unzulässige Installation unternehmensfremder Software unterbunden.

Wechselmedien, optische Disk-Laufwerke und Diskettenlaufwerke können auch schreibgeschützt werden.

Device Control ist standardmäßig deaktiviert und alle Geräte sind zugelassen.

Für den ersten Einsatz von Device Control empfiehlt Sophos:

- Wählen Sie Gerätearten aus, die überwacht werden sollen.
- Lassen Sie Geräte zwar erkennen, jedoch nicht blockieren.
- Richten Sie Device Control-Alerts ein.
- Lassen Sie Device Control Speichermedien erkennen und blockieren oder schreibschützen Sie sie.

Die Hilfe zu Sophos Control Center enthält weitergehende Informationen zu Device Control.

9.1 Unterstützte Gerätetypen

Mit Device Control können Sie drei Gerätetypen sperren: *Speicher, Netzwerk und kurze Reichweite*.

Speichermedien

- Wechselmedien (z.B. USB-Flash-Laufwerke, PC-Kartenlesegeräte und externe Festplatten)
- Optische Laufwerke (CD-ROM/DVD-Laufwerke/Blu-ray-Laufwerke)
- Diskettenlaufwerke
- Sichere Wechselmedien (z.B. USB-Flash-Laufwerke mit Hardware-Verschlüsselung (SanDisk Cruzer Enterprise, SanDisk Cruzer Enterprise FIPS Edition, Kingston Data Traveler Vault – Privacy Edition, Kingston Data Traveler BlackBox und IronKey Enterprise Basic Edition))

Bei Bedarf können Sie auch unterstützte sichere Wechselmedien zulassen und andere Wechselmedien sperren. Auf der Sophos Website (www.sophos.de) finden Sie eine aktuelle Liste unterstützter sicherer Wechselmedien.

Netzwerkgeräte

- Modems
- Wireless-Geräte (Wi-Fi-Schnittstellen, 802.11-Standard)

Bei Netzwerkschnittstellen können Sie zudem die Zugangsstufe „Sperre umgangen“ einstellen. Hierdurch können Netzwerkgeräte (d.h. Wi-Fi-Adapter) aktiviert werden, wenn der Computer

physisch vom Netzwerk abgetrennt wird. Wählen Sie die Option **Sperre umgangen** aus, wenn Sie die Zugriffsstufen für Netzwerkgeräte festlegen.

Hinweis: Im Modus „Sperre umgangen“ sind Netzwerkbrücken nicht möglich (beispielsweise zwischen einem Unternehmensnetzwerk und einem unternehmensexternen Netzwerk). Der Modus „Sperre umgangen“ steht für Wireless-Geräte und Modems zur Verfügung. Hierbei werden Wireless- oder Modemnetzwerkadapter deaktiviert, wenn ein Endpoint an ein physisches Netzwerk angeschlossen wird (in der Regel per Ethernet-Verbindung). Wenn der Endpoint von dem physischen Netzwerk getrennt wird, wird der Wireless- oder Modemnetzwerkadapter wieder aktiviert.

Kurze Reichweite

- Bluetooth-Schnittstellen
- Infrarot-Schnittstellen (IrDA)

Device Control sperrt interne und externe Geräte und Schnittstellen. Wenn Bluetooth-Schnittstellen gesperrt werden, werden folgende Komponenten blockiert:

- Die integrierte Bluetooth-Schnittstelle im Computer
- USB-Bluetooth-Adapter, die an den Computer angeschlossen werden

9.2 Einrichten von Device Control

Sie können Sophos Control Center dazu konfigurieren, bei Zugriff auf Geräte in Ihrem Netzwerk, die überwacht werden sollen, zu scannen.

1. Klicken Sie auf der linken Seite unter **Konfiguration** auf **Device Control konfigurieren**.
Das Dialogfeld **Device Control-Richtlinie** wird angezeigt.
2. Nehmen Sie auf der Registerkarte **Konfiguration** die folgenden Einstellungen vor:
 - Aktivieren Sie zum Aktivieren von Device Control das Kontrollkästchen **Device Control-Scans aktivieren**. Wenn die Geräte bei Zugriff erkannt jedoch nicht blockiert werden sollen, wählen Sie das Kontrollkästchen **Geräte erkennen, aber nicht sperren**.
 - So können Sie die Zugriffsstufe für die einzelnen Gerätetypen festlegen: Klicken Sie in der Spalte **Status** neben den Gerätetyp und klicken Sie dann auf den Dropdown-Pfeil. Legen Sie eine Zugriffsart für die Geräte fest.

Standardmäßig besitzen die Geräte Vollzugriff. Wechselmedien, optische Laufwerke und Diskettenlaufwerke können gesperrt oder mit Lesezugriff ausgestattet werden. Sichere Wechselmedien können gesperrt werden.

Die Einrichtung von Device Control-Alerts wird in der Hilfe zu Sophos Control Center beschrieben.

9.3 Ausschließen eines Geräts

Sie können Geräte von Device Control-Richtlinien ausschließen.

Sie können ein einzelnes Gerät („nur dieses Gerät“) oder einen Gerätetyp („alle Geräte des Typs“) ausschließen. Schließen Sie nicht ein bestimmtes Gerät und den entsprechenden Gerätetyp gleichzeitig aus. Wenn Ausschlüsse für beides festgelegt werden, hat das Einzelgerät Vorrang.

So können Sie ein Gerät ausschließen:

1. Wählen Sie im Menü **Ansicht** die Option **Device Control-Ereignisse**.

Das Dialogfenster **Device Control – Ereignisanzeige** wird geöffnet.

2. Wenn nur bestimmte Ereignisse angezeigt werden sollen, spezifizieren Sie im Bereich **Suchkriterien** Ihre Suchanfrage und klicken anschließend auf **Suche**. Die gefilterten Ereignisse werden nun angezeigt.

3. Wählen Sie das von Device Control auszuschließende Gerät und klicken Sie auf **Gerät ausschließen**.

Das Dialogfenster **Gerät ausschließen** wird angezeigt. Im Bereich **Geräte-Details** werden Typ, Modell und Kennung des Geräts angezeigt.

10 Technischer Support

Technischen Support erhalten Sie auf <http://www.sophos.de/support/>.

Wenn Sie sich an den Technischen Support wenden, halten Sie möglichst folgende Informationen bereit:

- Die Versionsnummer(n) Ihrer Sophos Software
- Betriebssystem(e) und Patch Level
- Den genauen Wortlaut von Fehlermeldungen (falls zutreffend)

11 Copyright

Copyright © 2009 Sophos Group. Alle Rechte vorbehalten. Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Sophos und Sophos Anti-Virus sind eingetragene Marken von Sophos Plc und der Sophos Group. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.

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.de/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-source¹⁰, 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 us¹¹ know so we can promote your project in the DOC software success stories¹².

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 companies¹³ 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 ACE¹⁴, TAO¹⁵, CIAO¹⁶, and CoSMIC¹⁷ web sites are maintained by the DOC Group¹⁸ at the Institute for Software Integrated Systems (ISIS)¹⁹ and the Center for Distributed Object Computing of Washington University, St. Louis²⁰ for the development of open-source software as part of the open-source software community²¹. 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 me²² know.

Douglas C. Schmidt²³

The ACE home page is <http://www.cs.wustl.edu/ACE.html>

Quellen

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. <http://www.the-it-resource.com/Open-Source/Licenses.html>
11. mailto:doc_group@cs.wustl.edu
12. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
13. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
14. <http://www.cs.wustl.edu/~schmidt/ACE.html>
15. <http://www.cs.wustl.edu/~schmidt/TAO.html>
16. <http://www.dre.vanderbilt.edu/CIAO/>

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