

# SOPHOS

## SMALL BUSINESS EDITION

### Sophos Control Center 4.0

### Guide de mise à niveau

Version du produit : 4.0

Date du document : septembre 2009



## Table des matières

1 A propos de ce guide.....	3
2 Nouveautés de Sophos Control Center 4.0.....	4
3 Configuration requise.....	5
4 Préparation à la mise à niveau.....	6
5 Mise à niveau du Sophos Control Center.....	8
6 Vérification de la protection des ordinateurs.....	9
7 Configuration du pare-feu.....	10
8 Paramétrage du contrôle des applications.....	11
9 Paramétrage du contrôle des périphériques.....	13
10 Support technique.....	16
11 Copyright.....	17

# 1 A propos de ce guide

Ce guide de mise à niveau de Sophos Control Center 4.0 décrit comment :

- Mettre à niveau depuis les versions 2.0 à 2.5 de Sophos Control Center vers la version 4.0 de Sophos Control Center.
- Mettre à niveau depuis Sophos Anti-Virus et Sophos Client Firewall (si votre licence inclut le pare-feu) vers Sophos Endpoint Security and Control.

Si vous utilisez une version précédente de Sophos PureMessage et si votre licence inclut une mise à niveau à la dernière version de Sophos PureMessage, consultez le *Guide de mise à niveau de Sophos PureMessage*. pour plus d'informations sur comment mettre à niveau.

- Paramétrer les nouvelles fonctionnalités de sécurité.

Vous pouvez trouver des détails sur toutes les autres options de configuration de Sophos Control Center non traitées dans ce guide dans l'*aide du Sophos Control Center*.

La documentation Sophos est publiée à la page suivante : <http://www.sophos.fr/support/docs/>.

## 2 Nouveautés de Sophos Control Center 4.0

Les fonctionnalités essentielles de la nouvelle version du Sophos Control Center sont les suivantes :

### **Prise en charge des derniers logiciels de sécurité pour postes d'extrémité**

La nouvelle version du Sophos Control Center vous permet d'utiliser Sophos Endpoint Security and Control pour les ordinateurs d'extrémité, lequel fournit la dernière version des logiciels antivirus et de pare-feu pour Windows 2000 et supérieur.

### **Tableau de bord**

L'interface de Sophos Control Center contient désormais un tableau de bord qui vous permet d'avoir un rapide aperçu du statut de sécurité du réseau. Vous pouvez configurer les valeurs seuil pour que le tableau de bord avertisse et envoie des messages d'alerte lorsqu'une valeur seuil est atteinte. Pour plus d'informations sur la configuration du tableau de bord, reportez-vous à l'Aide du Sophos Control Center.

### **Contrôle des applications**

Sophos Control Center vous permet de détecter et de bloquer les applications dont vous jugez l'utilisation inappropriée dans votre environnement de travail. Pour plus d'informations sur le contrôle des applications, reportez-vous à la section [Paramétrage du contrôle des applications](#) à la page 11.

### **Contrôle des périphériques**

Le contrôle des périphériques vous permet d'empêcher les utilisateurs d'utiliser sur leurs ordinateurs des périphériques de stockage externes, des supports de stockage amovibles et des technologies de connexion sans fil non autorisés. Pour plus d'informations sur le contrôle des périphériques, reportez-vous à la section [Paramétrage du contrôle des périphériques](#) à la page 13.

### **Lancement de Sophos PureMessage et de Sophos pour Microsoft SharePoint**

Si la console Sophos PureMessage ou Sophos pour Microsoft SharePoint est installée sur le même ordinateur que Sophos Control Center, vous pouvez les lancer depuis la console Sophos Control Center.

### 3 Configuration requise

Pour plus d'informations sur la configuration requise, consultez la page Configuration requise sur le site Web de Sophos (<http://www.sophos.fr/products/all-sysreqs.html>).

Par ailleurs, vous devez disposer d'un accès Internet pour télécharger le logiciel depuis le site Web de Sophos.

Sophos Control Center et les composants serveur ont les autres conditions requises suivantes :

- Vous devez avoir accès aux autres ordinateurs du réseau et depuis ces derniers.
- Il est conseillé d'utiliser un système d'exploitation de type serveur (comme Windows 2000 Server avec Service Pack 4 ou supérieur, Windows Server 2003 ou Windows Small Business Server 2003). Sinon, les performances du Sophos Control Center en subissent les conséquences.

## 4 Préparation à la mise à niveau

### Remarque :

- Nous vous recommandons vivement d'effectuer une copie de sauvegarde de votre version existante du Sophos Control Center avant de procéder à sa mise à niveau.
- Dès que l'Assistant d'installation du Sophos Control Center est terminée, fermez la session sur l'ordinateur sur lequel vous avez procédé à la mise à niveau du Sophos Control Center et rouvrez une session ou redémarrez l'ordinateur.
- Si vous choisissez d'installer Sophos Client Firewall (s'il est inclus dans votre licence), redémarrez chaque ordinateur sur lequel vous avez installé le logiciel de pare-feu pour l'activer.

Les alertes de pare-feu générées dans la version précédente du Sophos Control Center ne seront pas disponibles après la mise à niveau vers Sophos Control Center 4.0. Sophos vous recommande de solutionner toutes les alertes avant de procéder à la mise à niveau.

### 4.1 Conditions préalables

Avant de procéder à la mise à niveau du Sophos Control Center, et par conséquent de mettre à niveau les logiciels sur vos ordinateurs en réseau qu'il administre, les conditions préalables doivent être remplies :

- Toutes les configurations matérielles et systèmes requises dans la section [Configuration requise](#) à la page 5 sont satisfaites.
- Vous êtes administrateur de l'ordinateur sur lequel vous procédez à la mise à niveau du Sophos Control Center.

#### Préparation des ordinateurs d'extrémité sur lesquels est installé le système d'exploitation Windows

Pour les ordinateurs d'extrémité avec le système d'exploitation Windows, procédez ainsi :

- Désactivez le partage de fichiers simple sur tous les ordinateurs Windows XP.  
Pour savoir comment procéder, consultez l'article <http://www.sophos.fr/support/knowledgebase/article/12837.html>.
- Supprimez tout autre logiciel de pare-feu, à l'exception du pare-feu Windows, de tous les ordinateurs Windows 2000 et supérieur sur lesquels vous voulez installer le pare-feu.

#### Préparation des ordinateurs d'extrémité sur lesquels vous NE VOULEZ PAS installer Sophos Firewall

Si vous avez des postes de travail Windows XP Service Pack 2 sur lesquels vous *ne voulez pas* installer Sophos Firewall et si le pare-feu Windows est activé sur ces ordinateurs, procédez ainsi :

- Activez le Partage de fichiers et d'imprimantes pour les réseaux Microsoft.  
Pour savoir comment procéder, consultez l'article <http://www.sophos.fr/support/knowledgebase/article/11738.html>.

- Assurez-vous que les ports TCP 8192, 8193 et 8194 sont ouverts.
- Ajoutez l'exception suivante du programme : C:\Program Files\Sophos\Remote Management System\RouterNT.exe

Pour savoir comment procéder, consultez l'article  
<http://www.sophos.fr/support/knowledgebase/article/11075.html>.

- Redémarrez les ordinateurs pour que les modifications puissent être appliquées.

## 5 Mise à niveau du Sophos Control Center

Pour mettre à niveau le Sophos Control Center en conservant vos paramètres, ouvrez une session en tant qu'administrateur ou administrateur de domaine, selon le cas, sur l'ordinateur sur lequel la version précédente du Sophos Control Center est installée et procédez ainsi :

1. Fermez toutes les applications Sophos ouvertes, si elles le sont.
2. Visitez la page de téléchargement des produits Sophos sur <http://www.sophos.fr/support/updates/> et saisissez le nom utilisateur et le mot de passe qui vous ont été fournis par Sophos.

Suivez les liens pour télécharger le programme d'installation du Sophos Control Center, puis exécutez-le.

3. Dans la page **Welcome**, cliquez sur **Next**.

L'Assistant d'installation du Sophos Control Center vous guide tout au long de l'installation. Acceptez les options par défaut.

4. Une fois la mise à niveau terminée, cliquez sur **Terminer** pour fermer la session automatiquement. Si vous voulez fermer la session ultérieurement, désélectionnez la case à cocher **Fermer la session maintenant** avant de cliquer sur **Terminer**.

Parfois, il est nécessaire de redémarrer Windows au lieu de simplement fermer la session. Dans ce cas, la case à cocher n'apparaît pas et un message vous demande si vous voulez redémarrer Windows maintenant ou ultérieurement.

5. Lorsque vous rouvrez une session, ouvrez-la avec le même nom d'utilisateur.

Une fois terminée l'installation du Sophos Control Center, les ordinateurs d'extrémité se mettront automatiquement à jour lorsque le téléchargement de la nouvelle version des logiciels pour postes d'extrémité sera terminée.

**Remarque :** sur les ordinateurs pour postes d'extrémité avec Windows 98 et Mac OS X, vous devrez mettre à niveau Sophos Anti-Virus manuellement. Pour plus d'informations sur la protection manuelle des ordinateurs, reportez-vous à la section *Sophos Control Center Guide de démarrage*.

## 6 Vérification de la protection des ordinateurs

Vous pouvez vérifier que vos ordinateurs en réseau sont protégés contre les menaces à l'aide du Tableau de bord.

Le tableau de bord donne un aperçu rapide de l'état de la sécurité du réseau. Vous pouvez configurer les valeurs seuil pour que le tableau de bord avertisse et envoie des messages d'alerte lorsqu'une valeur seuil est atteinte.

Pour afficher ou masquer le tableau de bord, cliquez sur le bouton **Tableau de bord** de la barre d'outils.

Pour plus d'informations sur la configuration du tableau de bord et une liste complète des icônes qui apparaissent ainsi que leur statut, reportez-vous à l'Aide du Sophos Control Center.

## 7 Configuration du pare-feu

Lorsque vous installez Sophos Firewall pour la première fois, il est configuré pour autoriser tout le trafic. Vous pouvez le configurer pour autoriser ou bloquer seulement le trafic requis.

Si vous paramétrez le pare-feu pour la première fois, reportez-vous l'*Aide du* Sophos Control Center pour configurer le pare-feu.

**Remarque :** Sophos Firewall ne prend pas en charge IPv6. La version 1 de Sophos Client Firewall laisse passer les paquets IPv6 ; en fonction de la configuration, les versions 1.5 et 2.0 de Sophos Client Firewall soit bloquent soit autorisent tous les paquets IPv6.

## 8 Paramétrage du contrôle des applications

Le Sophos Control Center vous permet de détecter et de bloquer les "applications contrôlées", c'est-à-dire des applications légitimes qui ne constituent pas une menace pour la sécurité, mais que vous considérez comme inappropriées dans votre environnement de bureau. Ces applications incluent des clients de messagerie instantanée (IM), des clients de voix sur IP (VoIP), des logiciels d'imagerie numérique, des lecteurs multimédia ou des plug-ins de navigateur.

**Remarque :** cette option s'applique seulement à Sophos Endpoint Security and Control pour Windows 2000 et supérieur.

La liste des applications contrôlées est fournie par Sophos et régulièrement mise à jour. Vous ne pouvez pas ajouter de nouvelles applications à la liste, mais vous pouvez soumettre une demande à Sophos pour inclure une nouvelle application légitime sur laquelle vous voulez avoir le contrôle sur votre réseau. Pour plus de détails, consultez l'article 35330 de la base de connaissances du support Sophos (<http://www.sophos.fr/support/knowledgebase/article/35330.html>).

Pour plus d'informations sur les événements du contrôle des applications, reportez-vous à l'Aide du Sophos Control Center.

### 8.1 Paramétrage du contrôle des applications

Vous pouvez configurer le Sophos Control Center pour qu'il recherche les applications que vous souhaitez contrôler lors de leur accès sur votre réseau.

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle des applications**.

La boîte de dialogue **Configuration du contrôle des applications** apparaît.

2. Sur l'onglet **Contrôle**, définissez les options comme suit :

- Pour activer le contrôle sur accès, sélectionnez la case à cocher **Activer le contrôle sur accès**. Si vous voulez détecter des applications sans les bloquer sur accès, sélectionnez la case à cocher **Détecter mais autoriser l'exécution**.
- Pour activer le contrôle à la demande et le contrôle planifié, sélectionnez la case à cocher **Activer le contrôle à la demande et planifié**.

**Remarque :** vos paramètres de stratégie antivirus et HIPS déterminent quels fichiers vont être contrôlés (c'est-à-dire les extensions et les exclusions).

3. Cliquez sur l'onglet **Autorisation** et sélectionnez les applications que vous voulez contrôler.

Pour plus d'informations sur la sélection des applications, reportez-vous à la section [Sélection des applications à contrôler](#) à la page 12.

## 8.2 Sélection des applications à contrôler

Par défaut, toutes les applications sont autorisées. Vous pouvez sélectionner les applications que vous désirez contrôler de la manière suivante :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle des applications**.
2. Dans la boîte de dialogue **Configuration du contrôle des applications**, cliquez sur l'onglet **Autorisation**.
3. Sélectionnez le **Type d'application**, par exemple **Partage de fichiers**.

Une liste complète des applications incluses dans ce groupe apparaît dans la liste **Autorisées**.

- Pour bloquer une application, sélectionnez-la et déplacez-la dans la liste **Bloquées** en cliquant sur le bouton "Ajouter".



- Pour bloquer toutes les nouvelles applications que Sophos ajoutera à ce type à l'avenir, déplacez **Toutes ajoutées par Sophos à l'avenir** dans la liste **Bloquées**.

- Pour bloquer toutes les applications de ce type, déplacez toutes les applications de la liste **Autorisées** dans la liste **Bloquées** en cliquant sur le bouton "Ajouter tout".



Pour plus d'informations sur la désinstallation des applications contrôlées, reportez-vous à l'Aide du Sophos Control Center.

## 9 Paramétrage du contrôle des périphériques

**Important :** le contrôle des périphériques Sophos ne doit pas être déployé en parallèle à des logiciels de contrôle des périphériques d'autres éditeurs.

Le contrôle des périphériques vous permet d'empêcher les utilisateurs d'utiliser sur leurs ordinateurs des périphériques de stockage externes, des supports de stockage amovibles et des technologies de connexion sans fil non autorisés. Ceci peut aider à réduire considérablement votre exposition aux pertes accidentelles de données et limiter les possibilités pour les utilisateurs d'introduire des logiciels de l'extérieur de votre environnement réseau.

Les périphériques de stockage amovibles, les unités de disque optiques et les lecteurs de disquettes peuvent aussi être paramétrés pour fournir un accès en lecture seule.

Par défaut, le contrôle des périphériques est désactivé et tous les périphériques sont autorisés.

Si vous voulez activer le contrôle des périphériques pour la première fois, Sophos vous conseille de :

- Sélectionner des types de périphériques à contrôler.
- Détecter des périphériques sans les bloquer.
- Configurer les des alertes de contrôle des périphériques.
- Détecter et bloquer ou autoriser l'accès en lecture seule aux périphériques de stockage.

Pour plus d'informations sur les événements du contrôle des périphériques, reportez-vous à l'Aide du Sophos Control Center.

### 9.1 Quels types de périphériques peuvent être contrôlés ?

Le contrôle des périphériques vous permet de bloquer trois types de périphériques : *stockage, réseau et courte portée*.

#### Stockage

- Périphériques de stockage amovibles (par exemple, les clés USB à mémoire flash, les lecteurs de cartes PC et les lecteurs de disques durs externes)
- Lecteurs de disques optiques (lecteurs de CD-ROM/DVD/Blu-ray)
- Lecteurs de disquettes
- Périphériques de stockage amovibles sécurisés (par exemple, lecteurs flash SanDisk Cruzer Enterprise, SanDisk Cruzer Enterprise FIPS Edition, Kingston Data Traveler Vault - Privacy Edition, Kingston Data Traveler BlackBox et IronKey Enterprise Basic Edition avec chiffrement matériel)

A l'aide de la catégorie de stockage amovible sécurisée, vous pouvez facilement autoriser l'utilisation de périphériques de stockage amovibles sécurisés pris en charge tout en bloquant d'autres. Pour obtenir une liste à jour des périphériques de stockage amovibles sécurisés pris en charge, visitez le site Web de Sophos ([www.sophos.fr](http://www.sophos.fr)).

## Réseau

- Modems
- Sans fil (interfaces Wi-Fi, norme 802.11)

Pour les interfaces réseau, vous pouvez définir un niveau d'accès supplémentaire du mode Bloquer le pont. Cela permet l'activation (c'est-à-dire les adaptateurs Wi-Fi) du périphérique réseau lorsque l'ordinateur est physiquement déconnecté du réseau. Sélectionnez l'option Bloquer le pont lors du choix des niveaux d'accès pour les périphériques réseau.

**Remarque :** le mode Bloquer le pont empêche tout pont de réseau, par exemple, entre un réseau professionnel et un réseau non professionnel. Ce mode est disponible pour les types de périphériques sans fil et modem. Ce mode fonctionne en désactivant les adaptateurs réseau sans fil ou modem lorsqu'un système d'extrémité est connecté à un réseau physique (généralement, via une connexion Ethernet). Une fois le poste déconnecté du réseau physique, les adaptateurs réseau sans fil ou modem sont réactivés de manière transparente.

## Courte portée

- Interfaces Bluetooth
- Infrarouge (interfaces infrarouge IrDA)

Le contrôle des périphériques bloque à la fois les périphériques et les interfaces internes et externes. Par exemple, le blocage des interfaces Bluetooth va bloquer :

- L'interface Bluetooth incorporée dans un ordinateur
- Tous les adaptateurs Bluetooth de type USB connectés à l'ordinateur.

## 9.2 Paramétrage du contrôle des périphériques

Vous pouvez configurer le Sophos Control Center pour qu'il recherche les périphériques que vous souhaitez contrôler lors de leur accès sur votre réseau.

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle des périphériques**.

La boîte de dialogue **Stratégie de contrôle des périphériques** apparaît.

2. Sur l'onglet **Configuration**, définissez les options comme suit :

- Pour activer le contrôle des périphériques, sélectionnez la case à cocher **Activer le contrôle des périphériques**. Si vous voulez détecter des périphériques mais ne voulez pas les bloquer, sélectionnez la case à cocher **Détecter mais ne pas bloquer les périphériques**.
- Pour définir le niveau d'accès de chaque type de périphérique, cliquez dans la colonne **Etat** située près du type de périphérique, puis cliquez sur la flèche de menu déroulant qui apparaît. Sélectionnez le type d'accès que vous voulez autoriser.

Par défaut, les périphériques ont un accès complet. Pour les périphériques de stockage amovibles, les unités de disque optiques et les lecteurs de disquettes, vous pouvez changer l'état de "Bloqué" ou en "Lecture seule". Pour les périphériques de stockage amovibles, vous pouvez changer cela en "Bloqué."

Pour plus d'informations sur le paramétrage des alertes de contrôle des périphériques, reportez-vous à l'Aide du Sophos Control Center.

### 9.3 Exemption d'un périphérique

Vous pouvez exempter un périphérique des stratégies de contrôle des périphériques.

Vous pouvez exempter une instance (“ce périphérique uniquement”) ou un modèle (“tous les périphériques de ce modèle”) de périphérique. Ne paramétrez pas d'exemptions à la fois au niveau du modèle et de l'instance du périphérique. Si les deux sont définis, le niveau de l'instance du périphérique aura priorité.

Pour exempter un périphérique :

1. Dans le menu **Affichage**, cliquez sur **Événements du contrôle des périphériques**.  
La boîte de dialogue **Contrôle des périphériques - Observateur d'événements** apparaît.
2. Si vous voulez afficher certains événements seulement, dans le volet **Critères de recherche**, définissez les filtres de façon appropriée et cliquez sur **Rechercher** pour afficher les événements.
3. Sélectionnez l'entrée du périphérique que vous voulez exempter, puis cliquez sur **Exempter un périphérique**.  
La boîte de dialogue **Exemption d'un périphérique** apparaît. Sous **Détails du périphérique**, le type, le modèle et l'identification du périphérique apparaissent.

## **10 Support technique**

Pour obtenir du support technique, visitez <http://www.sophos.fr/support>.

Si vous contactez le support technique, fournissez autant d'informations que possible, notamment :

- Le ou les numéro(s) de version des logiciels Sophos
- Le(s) système(s) d'exploitation et le(s) niveau(x) de correctif
- Le texte exact de tous les messages d'erreur

## 11 Copyright

Copyright © 2009 Sophos Group. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos et Sophos Anti-Virus sont des marques déposées de Sophos Plc et de Sophos Group. Sophos Group. Tous les autres noms de produits et d'entreprises cités dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

Les logiciels Sophos mentionnés dans le présent document incluent ou peuvent inclure des programmes logiciels concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence Common Public License (CPL), qui, entre autres droits, permettent à l'utilisateur d'avoir accès au code source. La licence CPL exige que pour tout logiciel concédé en licence sous les termes de la licence CPL, qui est distribuée sous un format de code objet, le code source soit aussi mis à disposition de ces utilisateurs sous un format de code objet. Pour chacun de ces logiciels couverts par la licence CPL, le code source est disponible sur commande par courrier postal envoyé à Sophos, par courrier électronique envoyé à [support@sophos.com](mailto:support@sophos.com) ou par Internet sur <http://www.sophos.fr/support/queries/enterprise.html>. Une copie du contrat de licence pour chacun des logiciels inclus est disponible sur <http://opensource.org/licenses/cpl1.0.php>

### **ACE™, TAO™, CIAO™, and CoSMIC™**

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

Since DOC software is open-source<sup>10</sup>, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us<sup>11</sup> know so we can promote your project in the DOC software success stories<sup>12</sup>.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies<sup>13</sup> around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

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

The ACE<sup>14</sup>, TAO<sup>15</sup>, CIAO<sup>16</sup>, and CoSMIC<sup>17</sup> web sites are maintained by the DOC Group<sup>18</sup> at the Institute for Software Integrated Systems (ISIS)<sup>19</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>20</sup> for the development of open-source software as part of the open-source software community<sup>21</sup>. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

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

If you have any suggestions, additions, comments, or questions, please let me<sup>22</sup> know.

Douglas C. Schmidt<sup>23</sup>

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

## **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. [://www.the-it-resource.com/Open-Source/Licenses.html](http://www.the-it-resource.com/Open-Source/Licenses.html)
11. [mailto:doc\\_group@cs.wustl.edu](mailto:doc_group@cs.wustl.edu)
12. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
13. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
14. <http://www.cs.wustl.edu/~schmidt/ACE.html>
15. <http://www.cs.wustl.edu/~schmidt/TAO.html>
16. <http://www.dre.vanderbilt.edu/CIAO/>

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