

SOPHOS

Sophos Compliance Agent Guide de configuration

Version du produit : 3.3

Date du document : septembre 2009



Table des matières

1 A propos de ce guide.....	3
2 Agent de quarantaine.....	5
3 Agent temporaire.....	12
4 Langues de l'agent.....	16
5 Support technique.....	17
6 Copyright.....	18

1 A propos de ce guide

Ce guide vous décrit la configuration de l'agent de conformité (Sophos Compliance Agent) pour le logiciel Sophos Endpoint Security and Control.

Tout particulièrement, il vous fournit des informations sur :

- La conception, la configuration et la journalisation de l'agent de conformité et de l'agent de conformité temporaire (Dissolvable Compliance Agent).
- Les composants de l'interface de chaque agent, comme les boîtes de dialogue.
- Les langues prises en charge par les agents.

Ce guide s'adresse à vous si :

- Vous utilisez l'Enterprise Console.
- Vous utilisez Sophos NAC pour Endpoint Security and Control.
- Vous voulez obtenir des informations sur la conception de l'agent de conformité et sur l'agent de conformité temporaire.
- Vous voulez savoir quels composants de l'interface apparaissent sur le système d'extrémité.

Consultez le *Guide de démarrage rapide de Sophos Endpoint Security and Control* avant de lire ce guide.

Tous les documents Sophos Endpoint Security and Control sont disponibles sur : http://www.sophos.fr/support/docs/Endpoint_Security_Control-all.html.

1.1 Généralités

Sophos Compliance Agent est une application pour système d'extrémité configurable qui vérifie et applique la conformité aux stratégies NAC. L'agent récupère la stratégie NAC, vérifie l'état de conformité du système d'extrémité, corrige automatiquement les applications, envoie des messages à l'utilisateur et des rapports d'informations.

Sophos NAC prend en charge deux configurations d'agent. Les entreprises peuvent installer l'agent de quarantaine sur un système d'extrémité exécutant Microsoft Windows®. L'agent temporaire s'adresse aux utilisateurs invités exécutant Microsoft Windows.

- **Agent de quarantaine :** l'agent de quarantaine évalue les systèmes d'extrémité afin de déterminer s'ils sont en conformité avec la stratégie NAC. Ces évaluations sont effectuées avant l'autorisation d'accès au réseau puis régulièrement suite à l'autorisation d'accès au réseau. L'agent nécessite peu ou pas d'intervention de la part de l'utilisateur. L'agent de quarantaine dispose d'une fonction de quarantaine qui garantit son application et qui limite l'accès des systèmes d'extrémité à des zones spécifiques du réseau lorsque ceux-ci ne sont pas en conformité avec la stratégie NAC.
- **Agent temporaire :** l'agent temporaire évalue les systèmes d'extrémité pour déterminer s'ils sont en conformité avec la stratégie NAC avant d'autoriser l'accès au réseau. L'agent temporaire doit s'exécuter depuis un navigateur. L'agent temporaire s'adresse aux utilisateurs, comme les sous-traitants ou les invités, qui n'ont pas installé ou ne peuvent pas installer l'agent sur un système d'extrémité mais qui doivent quand même accéder à

des ressources réseau spécifiques. L'agent temporaire ne dispose pas de fonctionnalités d'application de la conformité, mais peut être utilisé avec l'application de DHCP.

Pour plus d'informations sur l'application de DHCP, reportez-vous au *Guide de configuration de DHCP de Sophos NAC*.

2 Agent de quarantaine

Cette section contient des informations sur la conception et la configuration de l'agent de quarantaine.

2.1 Conception

L'agent de quarantaine est une application de la zone de notification qui est installée sur le système d'extrémité et qui effectue régulièrement des opérations de traitement selon la stratégie NAC définie dans le NAC Manager. L'agent de quarantaine nécessite les droits administrateur local pour pouvoir être installé sur le système d'extrémité.

Paramètres d'agent

L'agent de quarantaine apparaît sous la forme d'une icône dans la zone de notification et donne des informations sur l'état en cours de l'agent. L'icône de l'agent de quarantaine change pour indiquer quand le système d'extrémité est en quarantaine, quand il dispose d'un accès total au réseau, ou quand les résultats sont en attente. Les paramètres de l'agent, qui sont configurés dans les modèles de configuration de l'agent dans le NAC Manager peuvent être utilisés pour contrôler les options d'affichage et les fonctionnalités de l'interface. Une fois qu'un modèle de configuration d'agent est ajouté à une stratégie, les agents peuvent récupérer la stratégie et mettre en place les paramètres sur le système d'extrémité.

Opérations de traitement

L'agent de quarantaine lance une première évaluation de la conformité puis lance régulièrement des opérations d'évaluation de la conformité pour garantir que le système d'extrémité demeure conforme à la stratégie NAC. L'agent de quarantaine effectue toutes les opérations (récupération des stratégies, vérification des stratégies, application des stratégies, correction et édition de rapports) même en cas d'échec d'une de ces opérations. En cas d'échec d'une opération, celle-ci sera de nouveau effectuée à sa prochaine planification.

Accès réseau

L'utilisateur se voit ensuite attribué un accès réseau selon la conformité ou l'état d'accès du système d'extrémité et selon les modèles d'accès réseau associés qui ont également été définis dans la stratégie. Par exemple, si le système d'extrémité n'est pas conforme, l'agent peut mettre le système d'extrémité en quarantaine et restreindre son accès au réseau selon ce qui a été défini dans les modèles d'accès de non conformité associés. En cas d'accès restreint, l'agent doit permettre à l'utilisateur d'effectuer des actions correctives afin de récupérer un accès total au réseau et doit aussi permettre l'accès au serveur proxy s'il est utilisé.

Accès au serveur proxy

Si l'authentification de l'utilisateur via un serveur proxy est nécessaire pour que l'agent communique avec le serveur NAC, la boîte de dialogue Demande des codes d'accès apparaît sur le système d'extrémité et demande à l'utilisateur de saisir son nom utilisateur et son mot de passe avant la récupération de la stratégie. Si vous avez enregistré le nom utilisateur et le mot de passe proxy comme paramètres de l'agent dans le NAC Manager, l'agent gère automatiquement les prochaines requêtes d'authentification et ne nécessite aucune intervention de l'utilisateur.

Quarantaine et vérifications de la conformité

Un système d'extrémité demeure en quarantaine jusqu'à ce qu'il soit conforme à la stratégie établie. Toutefois, l'utilisateur peut annuler l'état de quarantaine au cours d'une session de l'agent si la stratégie NAC le lui permet. L'état de quarantaine est réinitialisé lorsque l'utilisateur désactive l'annulation de la quarantaine ou qu'il ferme la session sur la machine. En plus des vérifications permanentes de la conformité, l'utilisateur peut à tout moment procéder à une nouvelle vérification de l'état de conformité de son système d'extrémité en utilisant soit l'option du menu Vérifier la conformité disponible sur l'icône de la zone de notification de l'agent de quarantaine soit via le bouton Vérifier la conformité de la boîte de dialogue Résultats.

Edition de rapports et envoi de messages à l'utilisateur

Les données de rapport incluent des informations sur les applications logicielles installées ou non sur le système d'extrémité, sur l'état de conformité du système d'extrémité à la stratégie NAC lors de la vérification et sur les messages affichés à l'utilisateur ou sur les actions effectuées sur le système d'extrémité. Au cours de l'opération, l'agent de quarantaine affiche à l'utilisateur des messages définis dans les profils du NAC Manager ainsi que les erreurs de fonctionnement.

2.2 Configuration

Pour configurer l'agent de quarantaine, effectuez les étapes suivantes :

- 1. Dans le NAC Manager, créez les ressources réseau et appliquez les aux modèles d'accès Agent Enforcer utilisés dans la stratégie pour les systèmes d'extrémité non conformes.**

Les ressources réseau sont des applications ou des périphériques nécessaires pour la correction des systèmes d'extrémité ou ceux dont l'accès par les systèmes d'extrémité placés en quarantaine doit être refusé. Les modèles d'accès Agent Enforcer sont utilisés avec la stratégie pour identifier les ressources réseau auxquelles les systèmes d'extrémité peuvent ou ne peuvent pas accéder lorsqu'ils utilisent l'agent de quarantaine pour la mise en application de la conformité. Les ressources réseau doivent être disponibles sur un système d'extrémité en quarantaine à des fins de correction et aussi pour fournir l'accès au serveur proxy si celui-ci est utilisé.

- 2. Déployez Sophos Compliance Agent sur les systèmes d'extrémité à l'aide de la Sophos Enterprise Console.**

Grâce à l'Assistant de protection des ordinateurs de la Sophos Enterprise Console, l'agent de quarantaine est déployé sur les systèmes d'extrémité. Une fois l'agent déployé, le système d'extrémité récupère la stratégie qui lui a été attribuée tandis que les paramètres définis dans la stratégie sont appliqués. La stratégie associée au groupe du système d'extrémité dans la Sophos Enterprise Console est récupérée par l'agent et utilisée pour la vérification de conformité du système d'extrémité.

Pour de plus amples informations sur les ressources réseau, sur les modèles d'accès Agent Enforcer, et sur les stratégies, reportez-vous à l'aide en ligne du NAC Manager.

2.3 Journalisation

Dans l'optique de la résolution des problèmes, l'agent de quarantaine prend en charge de nombreux types de fichiers journaux qui sont enregistrés sur le disque dur du système d'extrémité.

L'installation de Sophos Compliance Agent assure la journalisation automatiquement. Si l'agent rencontre une erreur au cours de l'installation ou en cas d'échec de l'installation, le journal fournit des informations sur la résolution des problèmes. Le journal d'installation de l'agent se trouve dans le répertoire %tmp%. A moins que vous ayez modifié l'emplacement du répertoire temp, vous pouvez accéder au répertoire en ouvrant l'Explorateur Windows et en saisissant %tmp% dans le champ d'adresse et en appuyant sur **Entrée**.

De plus, la journalisation peut être utilisée pour résoudre les problèmes d'activité de l'agent sur le système d'extrémité. La journalisation affecte les performances de l'agent de quarantaine ; par conséquent, elle doit uniquement être activée pour la résolution de problèmes et désactivée lorsque la résolution des problèmes est terminée. Les fichiers journaux excluent les données sensibles concernant l'utilisateur et contiennent des niveaux personnalisables d'informations. La journalisation est activée depuis la boîte de dialogue A propos de l'agent tandis que le niveau de journalisation est personnalisable en tant que paramètre d'agent.

Les trois fichiers journaux sont :

- **Session Log** : fournit des informations de haut niveau sur les erreurs.
 - **Trace Log** : fournit des informations détaillées sur les erreurs.
 - **Agent Log** : fournit des informations sur les erreurs concernant l'application de l'agent.
1. Dans le NAC Manager, rendez-vous sur la page **Create Agent Configuration Template**.
 2. Ajoutez le paramètre d'agent **Logging** au modèle de configuration de l'agent et sélectionnez ensuite le niveau de journalisation approprié.
Pour de plus amples informations sur les paramètres de l'agent, reportez-vous à l'aide du NAC Manager.
 3. Sur le système d'extrémité, ouvrez la boîte de dialogue **A propos de** de l'agent et sélectionnez la case **Activer la journalisation**.
Les fichiers journaux sont dans le dossier <lecteur>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Logs ou, pour Vista, dans le dossier <lecteur>:\ProgramData\Sophos\Sophos NAC\Logs.
 4. Lorsque la résolution des problèmes est terminée, sur le système d'extrémité, ouvrez la boîte de dialogue **A propos de** de l'agent et dessélectionnez la case **Activer la journalisation**.

2.4 Icônes, menus, infobulles et boîtes de dialogue

La section suivante contient des informations sur les icônes de la zone de notification, les astuces, les options de menu, les infobulles et les boîtes de dialogue disponibles dans l'agent de quarantaine.

2.4.1 Icônes et astuces de la zone de notification

Les icônes de la zone de notification informent de l'état actuel de l'agent des manières suivantes :

- Les icônes de la zone de notification affichent les différents états de l'agent.
- Lorsque vous laissez le curseur en suspens au-dessus de l'icône de la zone de notification, une astuce d'utilisation associée à cette icône apparaît.

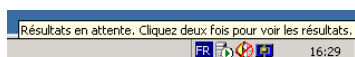





Schéma 1 : Exemple d'icône et d'astuce de la zone de notification

Le tableau suivant vous fournit des informations sur la signification des icônes.

Icône	Texte de l'astuce	Description
	Résultats en attente. Cliquez deux fois pour voir les résultats.	Icône qui apparaît lorsque les actions sont en attente et affichées dans la boîte de dialogue Résultats.
	Sophos Compliance Agent - Inactif. Machine en quarantaine.	Icône qui apparaît lorsque le système d'extrémité est en quarantaine.
	Sophos Compliance Agent - Inactif.	Icône qui apparaît lorsque l'agent est inactif.

2.4.2 Options de menu

Le menu de l'agent assure l'accès aux actions de l'agent en cliquant avec le bouton droit de la souris sur l'icône de la zone de notification. Un double clic de souris sur l'icône déclenche l'action du menu par défaut Afficher les résultats (en gras dans l'exemple).

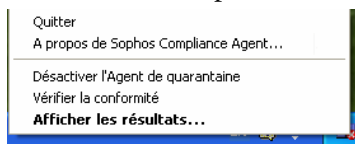


Schéma 2 : Exemple de menu

Le tableau suivant identifie le texte du menu et les descriptions.

Texte du menu	Description
Quitter	Quitte l'agent, supprime l'icône de la zone de notification et place le système d'extrémité en quarantaine, si applicable. Remarque : si le paramètre Show Exit Agent est Show, cette option du menu s'affiche. Si le paramètre Show Exit Agent est Hide (valeur par défaut), cette option du menu ne s'affiche pas. Pour de plus amples informations sur les paramètres de l'agent, reportez-vous à l'aide du NAC Manager.
A propose de Sophos Compliance Agent...	Affiche la boîte de dialogue A propos de.

Texte du menu	Description
Désactiver l'Agent de quarantaine	Annule la mise en quarantaine du système d'extrémité. Lorsque la quarantaine est désactivée, une marque s'affiche à côté du texte. Lorsque la quarantaine est activée, aucune marque ne s'affiche à côté du texte. Remarque : si l'option Quarantine Override dans la stratégie est paramétrée sur False (c'est-à-dire si le système d'extrémité n'est pas autorisé à annuler l'état de quarantaine), cette option du menu n'apparaît pas.
Vérifier la conformité	Commence une vérification de conformité lancée par l'utilisateur qui inclut des opérations de récupération de la stratégie, de vérification de la stratégie, d'application de la stratégie, de correction et d'édition de rapports.
Afficher les résultats...	Affiche la boîte de dialogue Résultats avec les messages provenant de la vérification de conformité la plus récente.

2.4.3 Infobulles

Les infobulles fournissent des informations textuelles supplémentaires concernant les actions effectuées ou requises par l'agent. L'infobulle affiche les actions requises de la part de l'utilisateur, comme les résultats sont en attente ou tout changement d'état de l'agent.

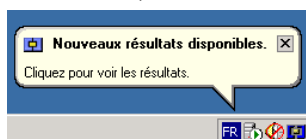





Schéma 3 : Exemple d'infobulle

Le tableau suivant identifie l'icône, le texte de l'infobulle et les descriptions.

Icône	Texte de l'infobulle	Description
	Légende : Nouveaux résultats disponibles. Texte : Cliquez pour voir les résultats.	Infobulle qui apparaît lorsque les actions sont en attente et affichées dans la boîte de dialogue Résultats.
	Légende : Votre machine a été mise en quarantaine. Pas de texte par défaut.	Infobulle qui apparaît lorsque le système d'extrémité est en quarantaine.
	Légende : Votre machine a été libérée de la quarantaine. Pas de texte par défaut.	Infobulle qui apparaît lorsque le système d'extrémité a été retiré de la quarantaine.

2.4.4 Boîte de dialogue Demande des codes d'accès

La boîte de dialogue Demande des codes d'accès apparaît si l'authentification via un serveur proxy est nécessaire pour que l'agent communique avec le serveur NAC.

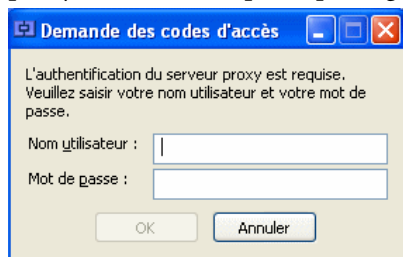


Schéma 4 : Exemple de boîte de dialogue Demande des codes d'accès

2.4.5 Boîte de dialogue Résultats

La boîte de dialogue Résultats affiche tous les messages utilisateur définis par les stratégies ou tous les messages d'erreur disponibles à l'utilisateur. La boîte de dialogue Résultats est disponible depuis l'option Afficher les résultats du menu et affiche les messages issus de la dernière vérification de conformité.

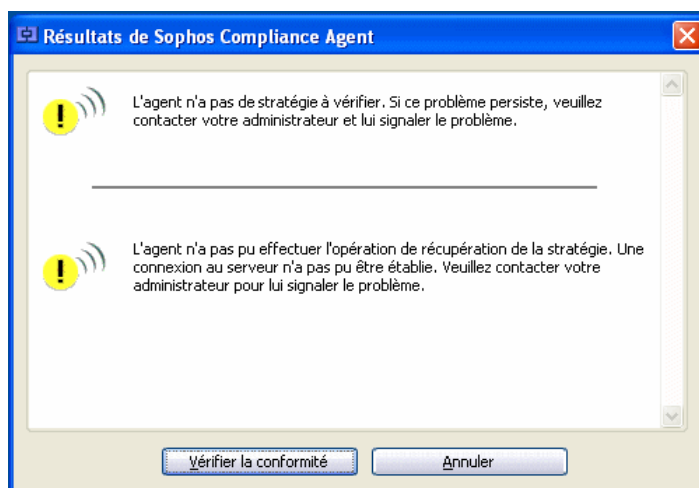


Schéma 5 : Exemple de boîte de dialogue Résultats

2.4.6 Boîte de dialogue A propos de

La boîte de dialogue A propos de affiche les informations sur l'agent, les informations de copyright et la case à cocher Activer la journalisation. La boîte de dialogue A propos de est disponible depuis l'option A propos de du menu.



Schéma 6 : Exemple de boîte de dialogue A propos de

3 Agent temporaire

Cette section contient des informations sur la conception et la configuration de l'agent temporaire.

3.1 Conception

L'agent temporaire peut être installé sur tout serveur Web Windows, y compris sur le serveur NAC et fournir l'accès à une page Web permettant aux utilisateurs invités d'exécuter l'agent temporaire. L'agent temporaire est une application autonome qui s'exécute localement sur le système d'extrémité et qui ne nécessite pas de disposer des droits administrateur ou de super utilisateur pour s'exécuter. Si l'authentification de l'utilisateur via un serveur proxy est nécessaire pour que l'agent temporaire puisse communiquer avec le serveur NAC, le navigateur Web invite l'utilisateur à saisir son nom utilisateur et son mot de passe.

Opérations de traitement

Dès qu'il est démarré, l'agent temporaire affiche une série de boîtes de dialogue indiquant la progression et les actions requises si nécessaire. L'agent temporaire effectue les opérations de traitement - récupération de la stratégie, vérification de la stratégie, application de la stratégie, correction et édition de rapports - à chaque fois qu'il est invoqué conformément à la stratégie NAC définie dans le NAC Manager. Lorsque les opérations de traitement sont terminées, l'agent temporaire se désinstalle du système d'extrémité. L'agent temporaire ne dispose pas de fonctionnalités d'application de la conformité, mais peut être utilisé avec l'application du protocole DHCP.

Edition de rapports et envoi de messages à l'utilisateur

Les données de rapport incluent des informations sur les applications logicielles installées ou non sur le système d'extrémité, sur l'état de conformité du système d'extrémité à la stratégie NAC lors de la vérification et sur les messages affichés sur le système d'extrémité de l'utilisateur. Au cours de l'opération, l'agent de quarantaine affiche à l'utilisateur des messages définis dans les profils du NAC Manager ainsi que les erreurs de fonctionnement.

3.2 Configuration

Pour pouvoir utiliser l'agent temporaire, vous devez d'abord l'installer sur un serveur Web Windows accessible aux utilisateurs invités. L'agent temporaire peut être installé sur le même serveur que Sophos NAC.

1. Installez Sophos Compliance Dissolvable Agent sur un serveur Web Windows.

L'agent temporaire est disponible sur le site Web de Sophos. Autrement, vous pouvez installer l'agent temporaire depuis le CD-ROM Sophos Install CD. Tous les fichiers prenant en charge l'agent temporaire sont installés lors de l'installation de Sophos Compliance Dissolvable Agent. Pour plus d'informations, reportez-vous au *Guide de démarrage avancé de Sophos Endpoint Security and Control*.

2. **Communiquez l'URL de Sophos Compliance Dissolvable Agent aux utilisateurs invités si nécessaire.**

Le système d'extrémité récupère la stratégie qui lui a été affectée et évalue la conformité du système d'extrémité. Si vous installez l'agent temporaire dans le répertoire par défaut, les systèmes d'extrémité pourront accéder à l'agent temporaire en utilisant l'URL suivante : `http://<adresse ip/nom DNS>/dissolvableagent`. L'adresse IP ou le nom DNS correspond au serveur Web sur lequel vous avez installé l'agent temporaire.

3.3 Journalisation

Il n'y a aucun paramètre défini pour l'agent temporaire dans le NAC Manager. Le paramètre de journalisation est défini sur le système d'extrémité.

Dans l'optique de la résolution des problèmes, l'agent temporaire prend en charge plusieurs fichiers journaux qui, en cas d'utilisation, sont enregistrés sur le disque dur du système d'extrémité. La journalisation affecte les performances de l'agent temporaire ; par conséquent, la journalisation, qui est disponible depuis la boîte de dialogue **A propos de**, doit uniquement être activée dans le cadre de la résolution de problèmes et doit être désactivée lorsque la résolution des problèmes est terminée. Les fichiers journaux excluent les données sensibles concernant l'utilisateur et contiennent des niveaux personnalisables d'informations.

Les trois fichiers journaux sont :

- **Session Log** : fournit des informations de haut niveau sur les erreurs.
- **Trace Log** : fournit des informations détaillées sur les erreurs.
- **Agent Log** : fournit des informations sur les erreurs concernant l'application de l'agent.

1. Démarrez l'agent temporaire.
2. Cliquez avec le bouton droit de la souris sur l'icône Sophos NAC de la boîte de dialogue **Résultats** et sélectionnez **A propos de Sophos Compliance Agent**.
3. Dans la boîte de dialogue **A propos de**, sélectionnez la case **Activer la journalisation**.
4. Exécutez l'agent temporaire.
5. Retrouvez les fichiers journaux dans le répertoire `<lecteur>:\Sophos\SDA<numéro aléatoire>\Logs`.
6. Lorsque la résolution des problèmes est terminée, exécutez de nouveau l'agent temporaire, ouvrez la boîte de dialogue **A propos de** de l'agent temporaire et désélectionnez la case **Activer la journalisation**.

3.4 Boîtes de dialogue

La section suivante vous décrit en détails les boîtes de dialogue disponibles de l'agent temporaire.

3.4.1 Boîte de dialogue Demande des codes d'accès

La boîte de dialogue Demande des codes d'accès apparaît si l'authentification via un serveur proxy est nécessaire pour que l'agent puisse communiquer avec le serveur NAC.

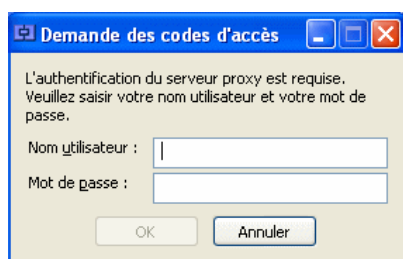


Schéma 7 : Exemple de boîte de dialogue Demande des codes d'accès

3.4.2 Boîte de dialogue Progression

La boîte de dialogue Progression apparaît lorsque l'agent effectue les opérations de traitement : récupération de la stratégie, vérification de la stratégie, application de la stratégie, correction et création de rapports. La boîte de dialogue Progression affiche l'état de l'opération en cours, la progression des opérations étape par étape et la progression générale des opérations.

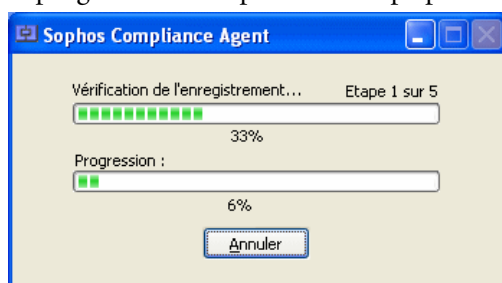


Schéma 8 : Exemple de boîte de dialogue Progression

3.4.3 Boîte de dialogue Résultats

La boîte de dialogue Résultats affiche tous les messages utilisateur définis par les stratégies ou tous les messages d'erreur disponibles à l'utilisateur.

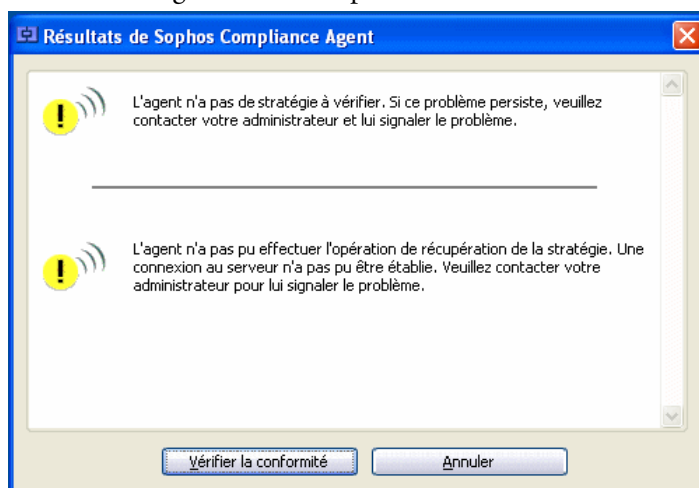


Schéma 9 : Exemple de boîte de dialogue Résultats

3.4.4 Boîte de dialogue A propos de

La boîte de dialogue A propos de affiche les informations sur l'agent, les informations de copyright et la case à cocher Activer la journalisation. La boîte de dialogue A propos de est disponible en cliquant sur l'icône Sophos de la boîte de dialogue Résultats.



Schéma 10 : Exemple de boîte de dialogue A propos de

4 Langues de l'agent

Par défaut, l'agent prend en charge les huit langues suivantes : anglais, français, espagnol, allemand, italien, japonais, chinois simplifié et chinois traditionnel.

Les messages utilisateur sont définis dans les profils du NAC Manager. L'agent affiche uniquement des messages utilisateur dans une langue spécifique si ceux-ci sont définis dans ce but.

Sophos vous recommande de créer un message pour un profil en anglais (langue par défaut) afin qu'en cas d'impossibilité d'afficher un message dans une autre langue, un message puisse toujours être affiché à l'utilisateur du système d'extrémité.

Pour de plus amples informations sur la création des messages utilisateur, reportez-vous à l'Aide du NAC Manager.

5 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, y compris :

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

6 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 licence conformément à ses termes ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.