

Solution pour les fonctions de sécurité affichant « Non disponible » lorsque des clés de fonction sont disponibles

Contenu

[Introduction](#)

[Conditions requises](#)

[Conditions préalables](#)

[Fond](#)

[Problème](#)

[Solution](#)

[Suppression du remplacement de machine pour revenir au niveau de cluster](#)

[Informations connexes](#)

Introduction

Ce document décrit comment dépanner et résoudre les problèmes sur l'appliance de sécurité de la messagerie électronique (ESA) et la sécurité de la messagerie électronique dans le cloud (CES) lorsque les fonctions de sécurité s'affichent comme « Non disponible » sur les politiques de messagerie entrante et sortante malgré la disponibilité des clés de fonction sur le périphérique.

Contribution d'Alan Macorra et de Mathew Huynh Ingénieurs Cisco CX.

Conditions requises

Conditions préalables

- Toute ESA/CES sur n'importe quelle version d'AsyncOS.
- Périphérique sous licence avec clés de fonction disponibles pour les services de sécurité.
- Compréhension des différents niveaux de configuration et de remplacement des clusters.

Fond

Le périphérique ESA/CES n'exécute aucune analyse de sécurité à partir de services tels que :

- Antispam
- Antivirus
- Protection avancée contre les programmes malveillants
- Graymail
- Filtres contre les attaques
- DLP (sortant uniquement)

Les touches de fonction sont disponibles et peuvent être vérifiées sur l'interface graphique ou l'interface de ligne de commande.

IUG: Administration système > Touches de fonction

CLI : touches de fonction

Dans les Stratégies de messages entrants et sortants, toutes les fonctionnalités de sécurité s'affichant comme "**Non disponible**", lors de la vérification du service de sécurité lui-même, il est configuré comme Activé.

Problème

Des clés de fonction sont disponibles sur le périphérique, mais les services sont « Non disponibles » et n'exécutent pas d'analyse.

En cliquant sur le lien « Non disponible » dans les stratégies de messagerie, vous redirige vers les paramètres globaux de ce service de sécurité spécifique, qui affiche activé et la modification de ce paramètre ne modifie pas l'état « Non disponible » dans les stratégies de messagerie elles-mêmes.

Exemple de résultat fourni :

Incoming Mail Policies

Mode —Cluster: Gear 1 Change Mode...

» Centralized Management Options

Find Policies

Email Address: Recipient Sender Find Policies

Any LDAP lookups will be made from the Login Host.

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
	Default Policy	Not Available	Not Available	Not Available	Not Available	Disabled	Not Available	

Outgoing Mail Policies

Mode —Cluster: Gear 1 Change Mode...

» Centralized Management Options

Find Policies

Email Address: Recipient Sender Find Policies

Any LDAP lookups will be made from the Login Host.

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	DLP	Delete
	Default Policy	Not Available	Not Available	Not Available	Not Available	Disabled	Not Available	Not Available	

Sophos

Mode — Machine: ESA_1.cisco.com Change Mode...

Centralized Management Options

Inheriting settings from Cluster: Gear 1:

- Override Settings

Settings for this feature are currently defined at:

- Cluster: Gear 1

Sophos Anti-Virus Overview

Anti-Virus Scanning by Sophos Anti-Virus:	Enabled
Virus Scanning Timeout (seconds):	60
Automatic Updates: (?)	Enabled

[Edit Global Settings...](#)

Current Sophos Anti-Virus files

File Type	Last Update	Current Version	New Update
Sophos Anti-Virus Engine	Never Updated	3.2.07.368.1_5.39	Available
Sophos IDE Rules	Never Updated	0	Available

Attention - Updates completed with error. [Update Now](#)

Applies to Login Host only.

Solution

Ce problème provient généralement de l'expiration des clés de fonction du périphérique avant le renouvellement et la réinstallation de la licence. Dans ce cas, le Contrat de licence de l'utilisateur final (CLUF) doit être accepté à nouveau. Étant donné que les périphériques étaient activés avant l'expiration, lorsque la réinstallation/le renouvellement de la clé initiale a été effectué, le CLUF n'est pas présenté à nouveau, car le périphérique est défini au niveau du cluster.

Pour résoudre ce problème, vous devez remplacer les paramètres de l'ESA/CES au **niveau machine** pour permettre au CLUF de se présenter pour acceptation. Ce faisant, le périphérique enregistre le renouvellement des clés et réactive les fonctionnalités.

Note: Le mode de configuration avec lequel vous êtes actuellement connecté s'affiche dans l'angle supérieur gauche où il affiche **Mode — Cluster/Group/Machine**. Selon le mode, ce qui est affiché peut être différent de la même sortie initiale fournie qui est déjà en **mode machine**.

Avertissement : Lors de la création de remplacements pour cette solution, assurez-vous de **NE PAS** sélectionner Déplacer la configuration, car cela forcera la configuration au niveau du cluster dans un mode non configuré pour le service spécifique. Si cette option est sélectionnée, lors de la suppression des remplacements, la fonctionnalité repasse à l'état non configuré (non activé).

Sur chaque service de sécurité qui affiche "**Non disponible**" :

1. Cliquez sur le lien "**Non disponible**" de la page Stratégies de messages entrants ou sortants.
2. Cela redirige vers les paramètres globaux par moteur, sélectionnez **Change Mode...** puis dans le menu déroulant. Sélectionnez l'ordinateur actuellement connecté.
3. Cliquez sur **Override Settings**

4. Sélectionnez **Copier à partir de : Grappe** . (Les paramètres actuellement activés sont copiés du niveau du cluster vers l'ordinateur).
5. Cliquez sur Submit
6. La configuration indique maintenant qu'elle est **activée**, cliquez sur **Modifier les paramètres globaux...**
7. Le CLUF s'affiche, est lu et accepté.
8. **Validez les modifications** pour enregistrer ce paramètre.
9. Répétez les étapes pour les autres fonctionnalités qui doivent être réactivées.

Exemple de résultat fourni :

À l'aide de la liste déroulante de droite, changez-la pour la machine à laquelle vous êtes connecté.

Mode — **Cluster: Gear 1** Change Mode... ▾

▾ Centralized Management Options

Settings are defined:

[Delete Settings](#) for this feature at this mode.
You can also [Manage Settings](#).

Copie des paramètres d'un cluster à un remplacement de machine.

Mode — **Machine: ESA_1.cisco.com** Change Mode... ▾

▾ Centralized Management Options

Creating New Settings for Machine: ESA_1.cisco.com

Note: Creating new settings for this machine will override the settings currently inherited from Cluster: Gear 1.

Start with default settings
 Copy from: Cluster: Gear 1 ▾
Cluster: Gear 1

Cancel Submit

Sortie du paramètre de remplacement :

Mode — **Machine: ESA_2.cisco.com** Change Mode... ▾

▸ Centralized Management Options

Sophos Anti-Virus Overview	
Anti-Virus Scanning by Sophos Anti-Virus:	Enabled
Virus Scanning Timeout (seconds):	60
Automatic Updates: ?	Enabled

[Edit Global Settings...](#)

Après avoir cliqué sur **Edit Global Settings...** le CLUF s'affiche.

Mode —Machine: ESA_2.cisco.com

Change Mode...

▸ Centralized Management Options

(Sophos Anti-Virus) License Agreement

To enable Sophos Anti-Virus scanning, please review and accept the license agreement below.

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT OR AVAILABLE AT THE TIME OF YOUR ORDER (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE REPRESENTING THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND BINDING YOURSELF TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY

Decline

Accept

Accepter le CLUF et valider les modifications.

Les paramètres de Sophos sont désormais reflétés dans la stratégie de messagerie et ne sont plus affichés comme « Non disponible ».

Suppression du remplacement de machine pour revenir au niveau de cluster

Pour supprimer les paramètres de remplacement de la machine :

1. **Passez en mode Machine à partir de la liste déroulante, comme précédemment.**
2. Cliquez pour développer **Options de gestion centralisée**
3. Cliquez sur **Supprimer les paramètres**
4. Cliquez sur le bouton **Delete** et les paramètres reviendront au niveau supérieur (Group ou Cluster, selon la configuration).
5. Vérifiez que les paramètres sont correctement configurés au niveau supérieur choisi.
6. **Validez les modifications** pour enregistrer ce paramètre.

Exemple de sortie :

Mode —Machine: ESA_1.cisco.com

Change Mode...

▾ Centralized Management Options

Settings are defined:

To inherit settings from a higher level: [Delete Settings](#) for this feature at this mode.
You can also [Manage Settings](#).

Settings for this feature are also defined at:

- Cluster: Gear 1

Informations connexes

- [Appliance de sécurisation de la messagerie Cisco - Guides de l'utilisateur final](#)
- [Support et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.