

Installation de Trend OfficeScan XG (version 12)

Lionel FIS déc. 2017

Ce document récapitule les modalités d'installation de Trend OfficeScan XG, ainsi que le paramétrage conseillé. Il a été rédigé à partir des documents suivants :

- TRENDOfficeScan11ReseauPedagogiqueV1-0.pdf (DACE, mise à jour : 3 septembre 2015)
- OFFICESCAN_RANSOMWARE_TCh.pdf disponible sur le site MAGRET :
<http://pedagogie.ac-toulouse.fr/matrice/magret/gestion.htm>

Documentation Trend Micro :

- XG OfficeScan Manuel de l'administrateur :
http://docs.trendmicro.com/all/ent/officescan/v12.0/fr-fr/osce_12.0_ag.pdf
- Aide en ligne de l'agent OfficeScan XG :
http://docs.trendmicro.com/all/ent/officescan/v12.0/fr-fr/osce_12.0_agent_olh/About.html#GUID-401DC417-7463-4B1E-A888-D1FD74FD3B82

Champs d'application :

- Réseau pédagogique
- L'installation de la console Trend sur un serveur membre du domaine (serveur02) est vivement recommandée
- Système Windows serveur 2008 R2 ou supérieur
- IIS installé
- Installation initiale ou « par-dessus » une autre version d'OfficeScan (10.6 SP3 minimum)

Sommaire :

1-	Téléchargements pour OfficeScan :.....	2
2-	Installation de Trend OfficeScan XG sur un serveur membre (Serveur02) :	2
4-	Vérification de la présence de l'Agent Trend sur le serveur :	16
5-	Installation des Patches :.....	17
6-	Ouverture de la console Web OfficeScan :.....	18
7-	Paramétrage de Trend OfficeScan :.....	24
7-1	Menu Administration :	24
7-2	Menu « Mises à jour » :	28
7-3	Menu « Agents » :.....	31
7-4	Gestion des agents :	34
7-4.1	Gestion de l'arborescence des agents :	34
7-4.2	Menu Paramètres – Paramétrage par import d'un fichier .dat	37
7-4.3	Menu Paramètres - Paramétrage manuel :.....	41
8-	Installation et déploiement de l'agent Trend.....	51
8-1	Modification des fichiers et des droits, dans le répertoire d'installation de Trend OfficeScan :.....	51
8-2	Installation de l'agent Trend :.....	53
8-3	Installation automatique de l'agent Trend :.....	53
9-	Création d'un paquet pour les serveurs DMZ, ZMI et pour les postes isolés du réseau :.....	54
10-	Migration des agents vers le nouveau Serveur :	56
11-	Réinitialisation du mot de passe de la console Trend OfficeScan :	57

1- Téléchargements pour OfficeScan :

La version XG (version 12) et les Patchs sont disponibles sur le site Trend Micro ci-dessous :
http://downloadcenter.trendmicro.com/index.php?regs=fr&clk=latest&clkval=4973&lang_loc=2

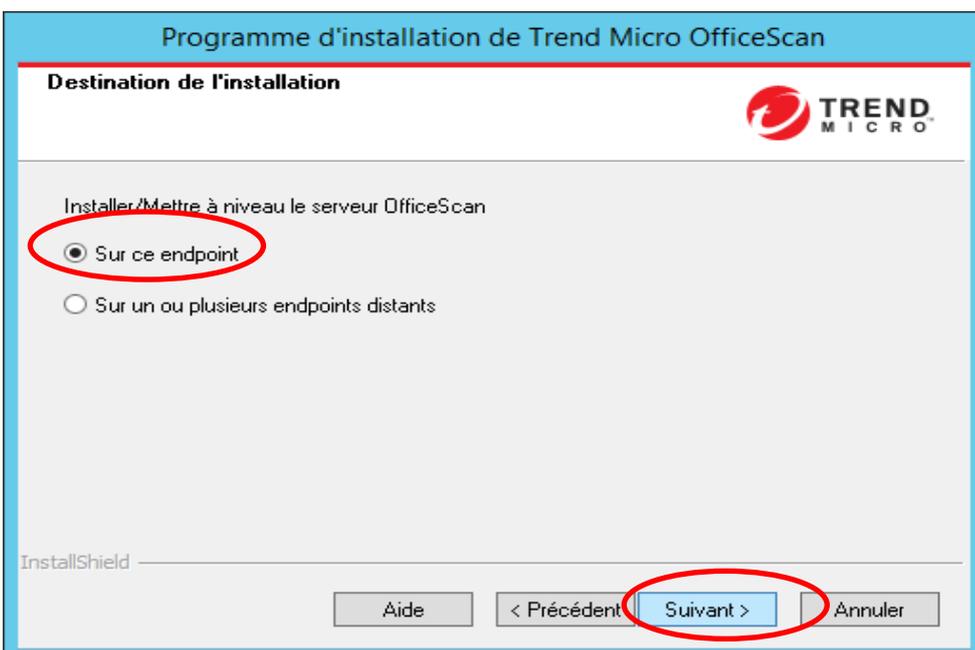
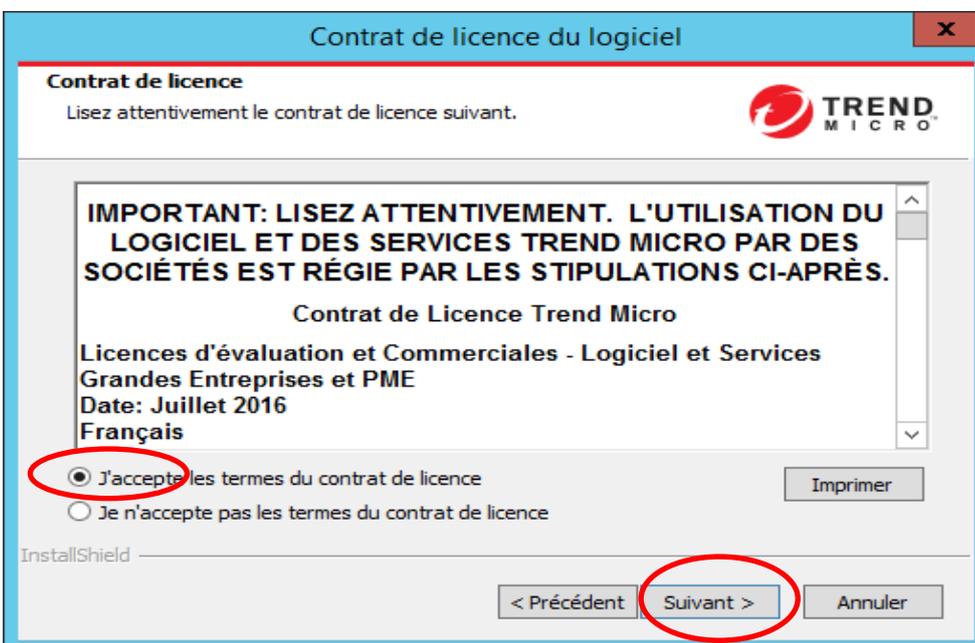
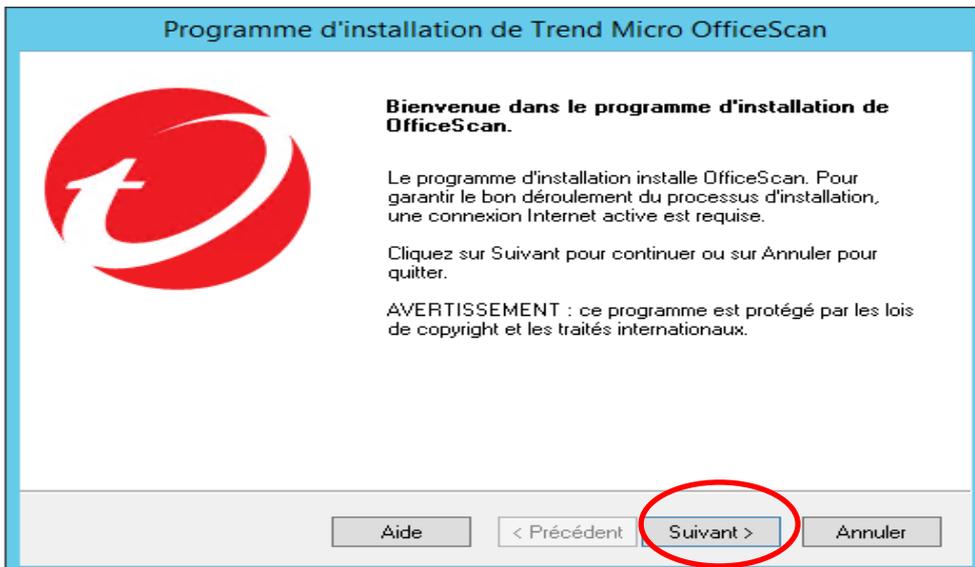
The screenshot shows the Trend Micro website's download center for OfficeScan XG. The page is in French and displays the 'OfficeScan XG Latest Version' section. It includes a navigation menu at the top, a sidebar with product categories, and a main content area with a table of download packages. The table has columns for Description, Date de publication, Nom de fichier, Taille en Mo, and Télécharger package. Two packages are listed: a French version (osce-xg-win-fr-b1406.exe) and an English version (osce-xg-win-en-gm-b1315.exe). There are also buttons for 'Patch produit' and 'Scan Engines'.

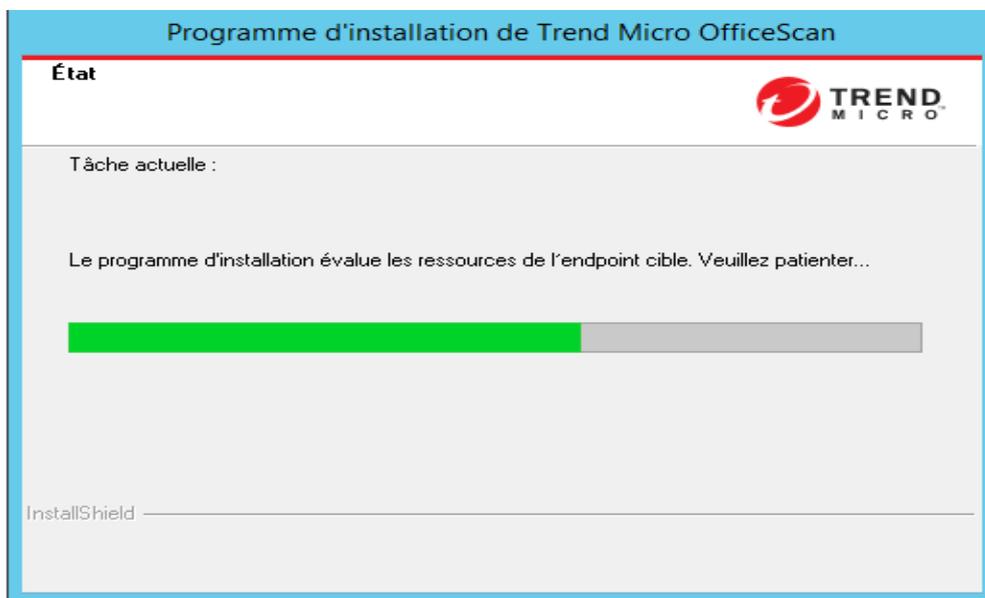
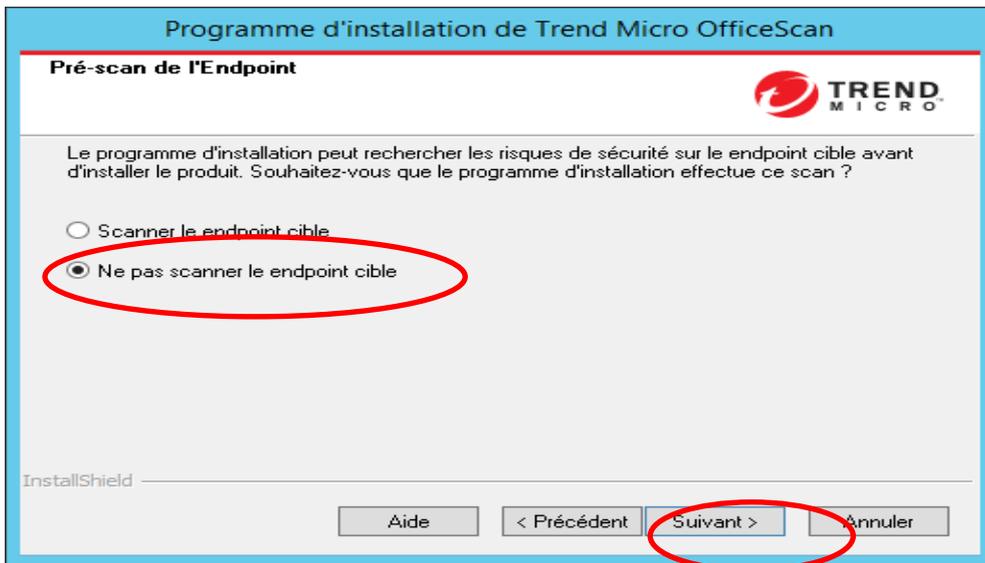
- Télécharger les versions françaises :
 - Full Installation Package (osce-xg-win-fr-b1406.exe)
 - Product Patch (osce_xg_win_fr_patch1_1576.exe)
 - Critical Patch (osce-xg-win-fr-criticalpatch-1775.exe)
- Débloquer les archives.

2- Installation de Trend OfficeScan XG sur un serveur membre (Serveur02) :

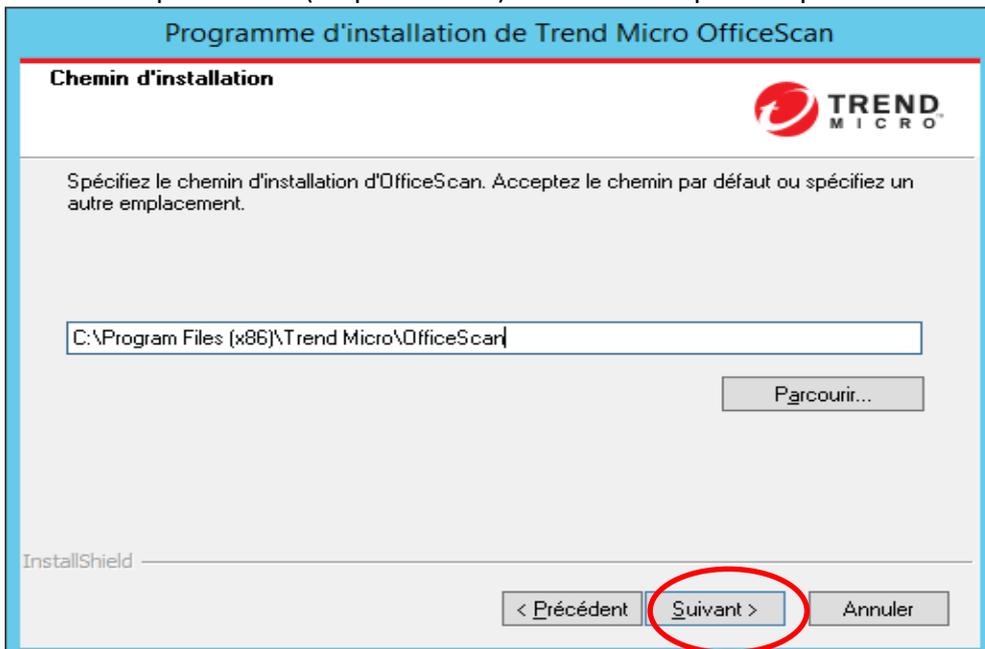
Exécuter OSCE.exe en tant qu'administrateur :

The screenshot shows a Windows File Explorer window titled 'Outils d'application' with the address bar set to 'C:\Pôle d'Appui'. The file list contains three files: OSCE.exe, osce_xg_win_fr_criticalp, and osce_xg_win_fr_patch1. A context menu is open over OSCE.exe, with the option 'Exécuter en tant qu'administrateur' selected. The window also shows a sidebar with 'Favoris' and 'Serveur02'.





Suivant l'espace disque disponible on pourra mettre le répertoire « Trend Micro » sur la partition C ou sur la partition D (de préférence). Prévoir un espace disponible de l'ordre de 30 Go :



Pas de serveur proxy, car on est sur un serveur pouvant accéder directement à Internet au travers du PFS.

L'adresse IP du serveur doit être dans la plage 10.255.X.Y+1 à 10.255.X.Y+11 (voir documentation Magret « MagretV16_Installation_serveur_V2012R2) :

Programme d'installation de Trend Micro OfficeScan

Serveur proxy

Si vous utilisez un serveur proxy pour accéder à Internet, spécifiez ci-dessous les paramètres proxy. OfficeScan utilise ces informations lors du téléchargement de mises à jour depuis le serveur de mise à jour de Trend Micro.

Paramètres proxy

Utiliser un serveur proxy

Type de proxy : HTTP SOCKS 4

Nom ou adresse IP du serveur :

Port :

Authentification (facultatif) :
Nom d'utilisateur :
Mot de passe :

InstallShield

Aide < Précédent **Suivant >** Annuler

Choisir une période de validité du certificat de 5 ans et garder le port SSL 4343 :

Programme d'installation de Trend Micro OfficeScan

Serveur Web

Configurez le serveur Web à utiliser pour le serveur OfficeScan. OfficeScan utilise le protocole de transfert SSL pour la console Web du serveur.

Serveur IIS : Site Web IIS virtuel

Port HTTP : 8080

Paramètres SSL

Période de validité du certificat : 5 an(s)

Port SSL : 4343

InstallShield

Aide < Précédent **Suivant >** Annuler

Indiquer le nom de domaine complet (FQDN) :

Programme d'installation de Trend Micro OfficeScan

Identification du serveur

Spécifiez si les agents OfficeScan doivent identifier le serveur selon son nom de domaine ou son adresse IP.

Trend Micro recommande d'utiliser une adresse IP si plusieurs cartes réseau sont installées sur le serveur et d'utiliser un nom de domaine complet (FQDN) ou un nom d'hôte si l'adresse IP est susceptible d'être modifiée.

Nom de domaine complet (FQDN) ou nom d'hôte :

Conseil : avant de continuer, vérifiez que le nom de domaine peut être résolu.

Adresse IP :

InstallShield

Aide < Précédent **Suivant >** Annuler

Ignorer l'enregistrement en ligne et faire suivant :

Programme d'installation de Trend Micro OfficeScan

Activation du produit

Étape 1. Enregistrement en ligne

L'activation comporte deux étapes :

1. Enregistrement en ligne.
Ignorez cette étape si vous possédez déjà un code d'activation.
2. Saisie du code d'activation.

Utilisez la clé d'enregistrement fournie avec votre produit et cliquez sur le bouton ci-dessous pour procéder à l'enregistrement en ligne. Un code d'activation vous sera alors envoyé par e-mail.

InstallShield

Aide < Précédent **Suivant >** Annuler

Copier les 37 caractères de la clé d'activation qui se trouve dans le fichier « cle d'activation.pdf » et les coller dans la fenêtre ci-dessous.

Cocher la case « Utiliser le même code d'activation pour Damage... »

The screenshot shows the 'Programme d'installation de Trend Micro OfficeScan' window. The title bar is blue with the text 'Programme d'installation de Trend Micro OfficeScan'. Below the title bar, there is a section titled 'Activation du produit' with the sub-header 'Étape 2. Saisie du ou des codes d'activation'. The Trend Micro logo is visible in the top right corner. The main area contains instructions: 'Saisissez les codes d'activation des services OfficeScan au format suivant : [XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX]'. There are three input fields, each containing the activation key 'OS-SBLL-D3PTF-DYTG-N-QHYMG-B3TQD-HQ9LK'. The first field is for 'Antivirus', the second for 'Damage Cleanup Services', and the third for 'Réputation de sites Web et anti-spyware'. A checkbox labeled 'Utilisez le même code d'activation pour Damage Cleanup Services, pour les services de réputation de sites Web et pour Anti-spyware' is checked. At the bottom, there are four buttons: 'Aide', '< Précédent', 'Suivant >', and 'Annuler'. The 'Suivant >' button is circled in red.

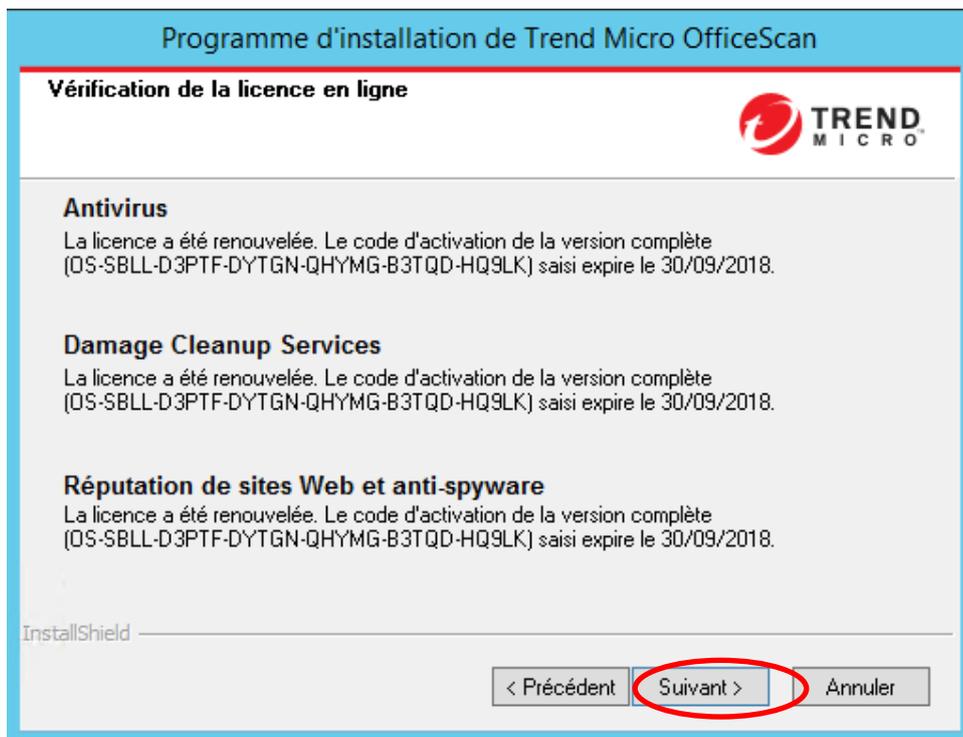
Le fichier de licence obtenu lors de la négociation initiale du contrat était valable pour une période de cinq ans (30/09/2010 au 30/09/2015).

Ce contrat a ensuite été reconduit pour trois ans, jusqu'au 30/09/2018. Bien qu'il soit obsolète le fichier de licence dont on dispose ici, permet l'activation en ligne de la licence :

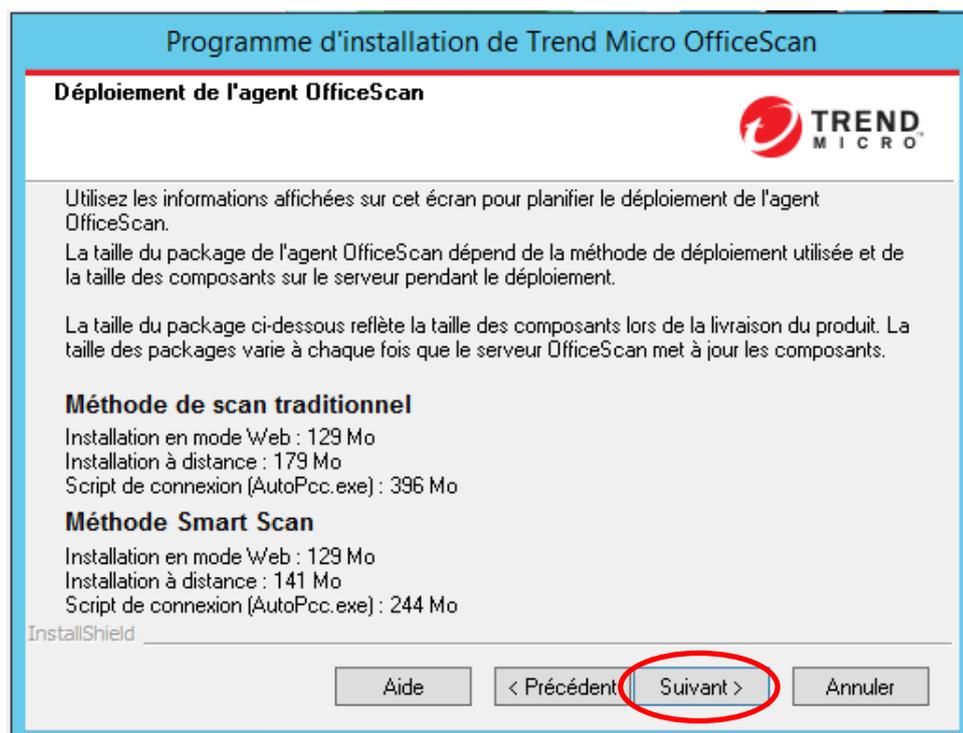
Répondre Oui, pour vérifier l'état de la licence en ligne :

The screenshot shows an error dialog box titled 'Programme d'installation de Trend Micro OfficeScan'. The text inside reads: 'Impossible de vérifier le code d'activation. Vérifiez l'état de votre licence en ligne ou contactez votre distributeur local pour obtenir un nouveau code d'activation.' At the bottom, there are two buttons: 'Oui' and 'Non'. The 'Oui' button is circled in red.

The screenshot shows a progress bar window titled 'Vérification de l'état de la licence en ligne...'. The progress bar is partially filled with green, indicating the verification process is in progress.



Le choix de la méthode de scan s'effectuera plus tard (voir paragraphe 7-4-3) :



Installer le serveur Smart Protection Server intégré en l'absence de serveur Smart Protection autonome :

Programme d'installation de Trend Micro OfficeScan

Installer le serveur Smart Protection Server intégré

Le programme d'installation peut installer le serveur Smart Protection Server intégré sur le serveur OfficeScan cible, qui fournit des fonctionnalités de réputation de fichiers et de site Web, et une connexion à Deep Discovery Analyzer.

Trend Micro recommande d'installer un serveur Smart Protection Server autonome, qui fournit les mêmes fonctionnalités, mais peut prendre en charge un nombre supérieur d'agents.

Souhaitez-vous installer le serveur intégré ?

Non, j'ai déjà installé un serveur Smart Protection Server autonome ou j'envisage de le faire.

Oui, installer le serveur Smart Protection Server intégré. (OfficeScan utilisera le protocole SSL pour les services File Reputation)

Paramètres SSL

Période de validité du certificat : 5 an(s)

Port SSL : 4343

InstallShield

Aide < Précédent **Suivant >** Annuler

Installer l'agent OfficeScan sur le serveur :

Programme d'installation de Trend Micro OfficeScan

Installer l'agent OfficeScan

Choisissez d'installer l'agent OfficeScan sur le endpoint cible.

Installer l'agent OfficeScan

InstallShield

Aide < Précédent **Suivant >** Annuler

Pas de partage des informations :

Programme d'installation de Trend Micro OfficeScan

Smart Protection Network

TREND MICRO

TREND MICRO SMART PROTECTION NETWORK

Trend Micro Smart Protection Network est une infrastructure de sécurité en ligne de nouvelle génération conçue pour assurer une protection proactive contre les menaces les plus récentes.

Activer Trend Micro Smart Feedback (recommandé).

Lorsqu'il est activé, Smart Feedback partage des informations anonymes sur les menaces avec le réseau Smart Protection Network à des fins d'analyse. Vous pouvez désactiver Smart Feedback à tout moment via la console du produit.

Votre secteur d'activité (facultatif) : Non spécifié

InstallShield

Aide < Précédent **Suivant >** Annuler

Choisir un mot de passe pour l'accès à la console, et un autre mot de passe différent pour le téléchargement et la désinstallation de l'agent.

Une complexité minimale est requise (Exemple : première lettre en majuscule) :

Programme d'installation de Trend Micro OfficeScan

Mot de passe du compte administrateur

TREND MICRO

Spécifiez le mot de passe d'ouverture de la console Web ou de téléchargement/désinstallation de l'agent OfficeScan. Les mots de passe empêchent toute modification des paramètres de la console Web ou suppression de l'agent OfficeScan non autorisée.

Mot de passe de la console Web :

Compte : root

Mot de passe : [masqué]

Confirmer mot de passe : [masqué]

Mot de passe de téléchargement et de désinstallation de l'agent OfficeScan :

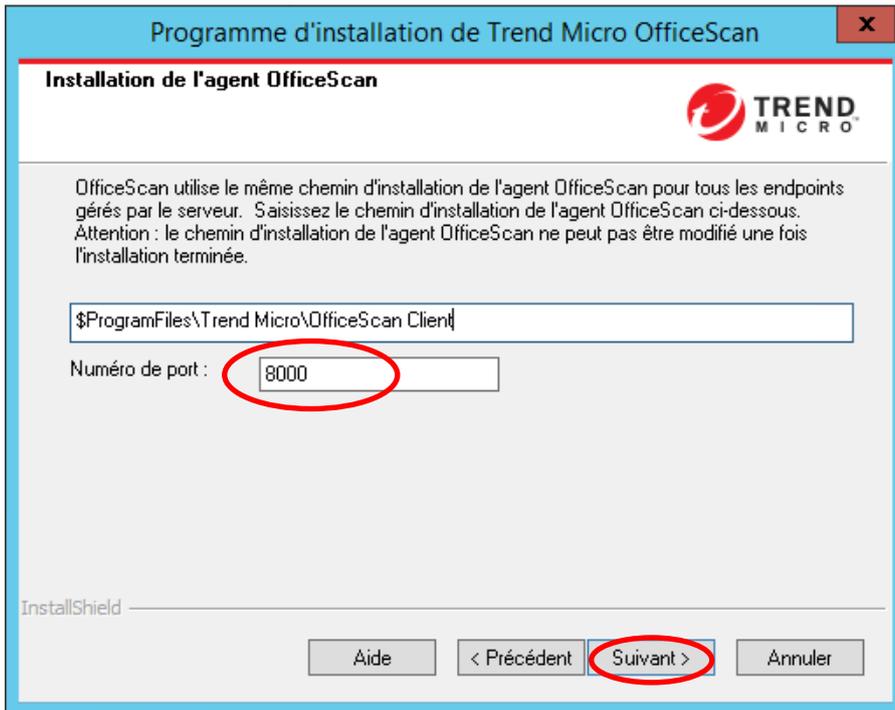
Mot de passe : [masqué]

Confirmer mot de passe : [masqué]

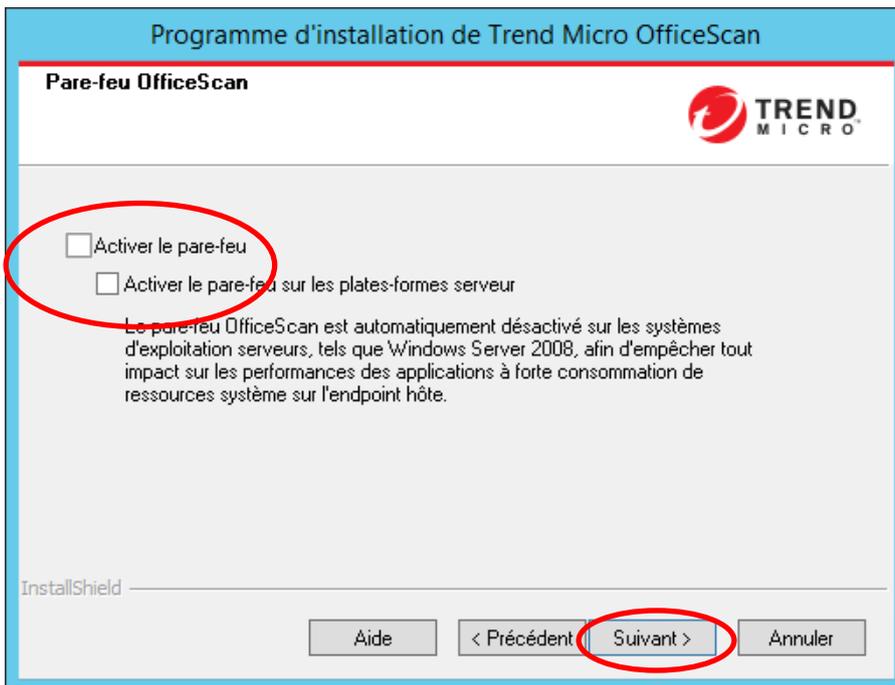
InstallShield

Aide < Précédent **Suivant >** Annuler

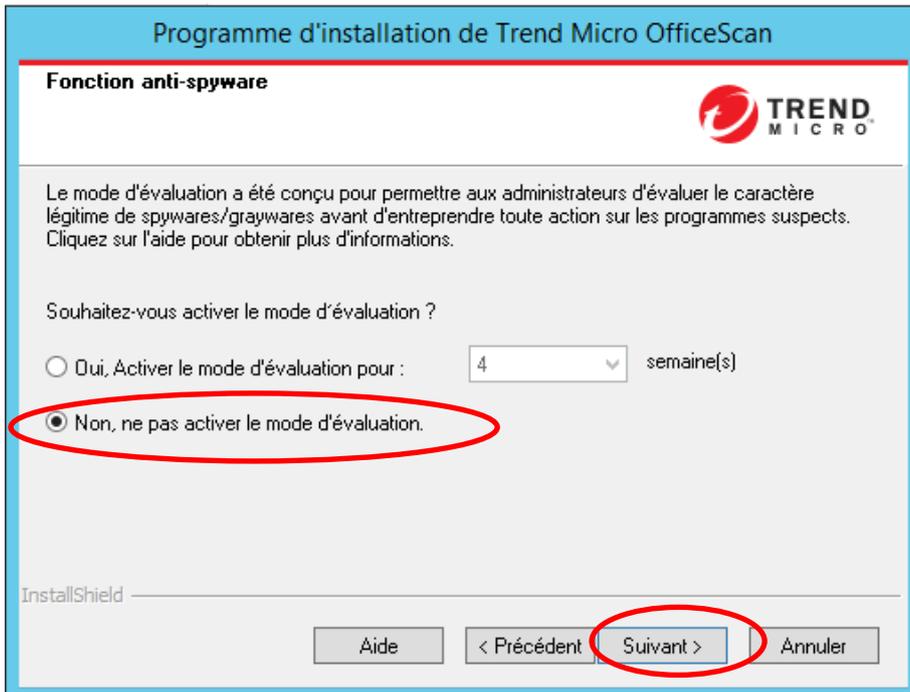
Installation de l'agent : conserver le chemin d'installation par défaut et fixer la valeur du port à 8000 :



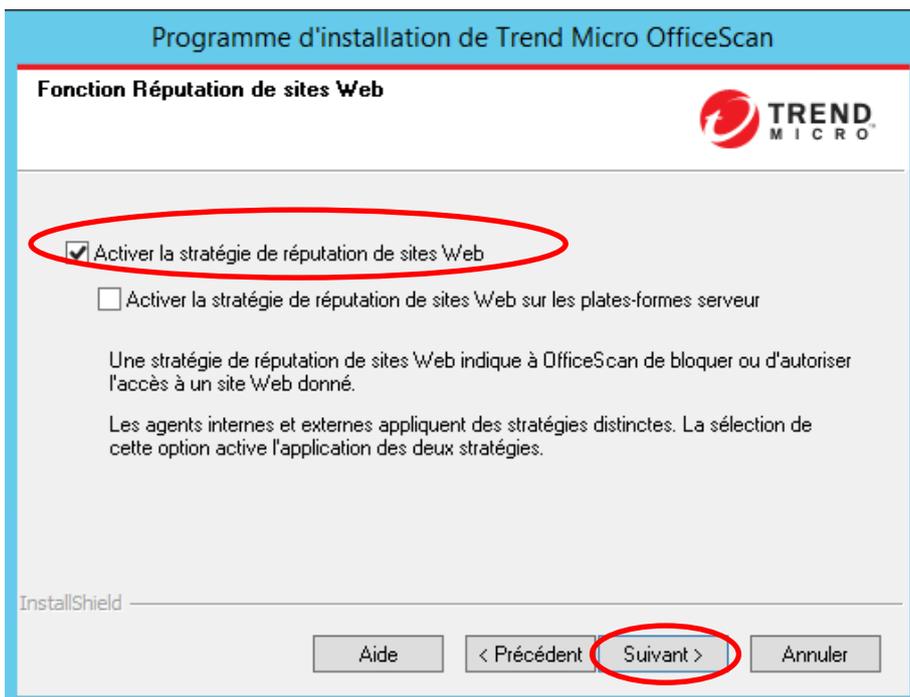
Ne pas activer le pare-feu OfficeScan :



Ne pas activer le mode d'évaluation, du caractère légitime des programmes suspects :



Activer la stratégie de réputation de sites Web :



Générer un certificat de sécurité et indiquer un mot de passe pour ce certificat (donner le même mot de passe que pour l'accès à la console Web) :

Programme d'installation de Trend Micro OfficeScan

Certificat d'authentification serveur



Autorisez OfficeScan à générer un certificat pour la communication avec les agents OfficeScan ou importez un certificat existant.
Remarque : OfficeScan crée une version de sauvegarde du certificat, qu'il soit nouvellement généré ou importé, dans le dossier <Dossier_installation_serveur>\AuthCertBackup\.

Générer un certificat d'authentification

Mot de passe de sauvegarde :

Confirmer le mot de passe :

Importer un certificat existant
Remarque : le certificat peut être un package au format ZIP généré par l'outil Gestionnaire de certificats d'authentification serveur ou un fichier PFX correctement formaté.

Mot de passe :

InstallShield

Raccourcis du menu Démarrer :

Programme d'installation de Trend Micro OfficeScan

Raccourcis programme OfficeScan



Le programme d'installation ajoute au menu Démarrer un dossier contenant les raccourcis du programme OfficeScan. Acceptez le nom par défaut ou spécifiez un nouveau nom. Il est possible d'ajouter les raccourcis à un dossier existant.

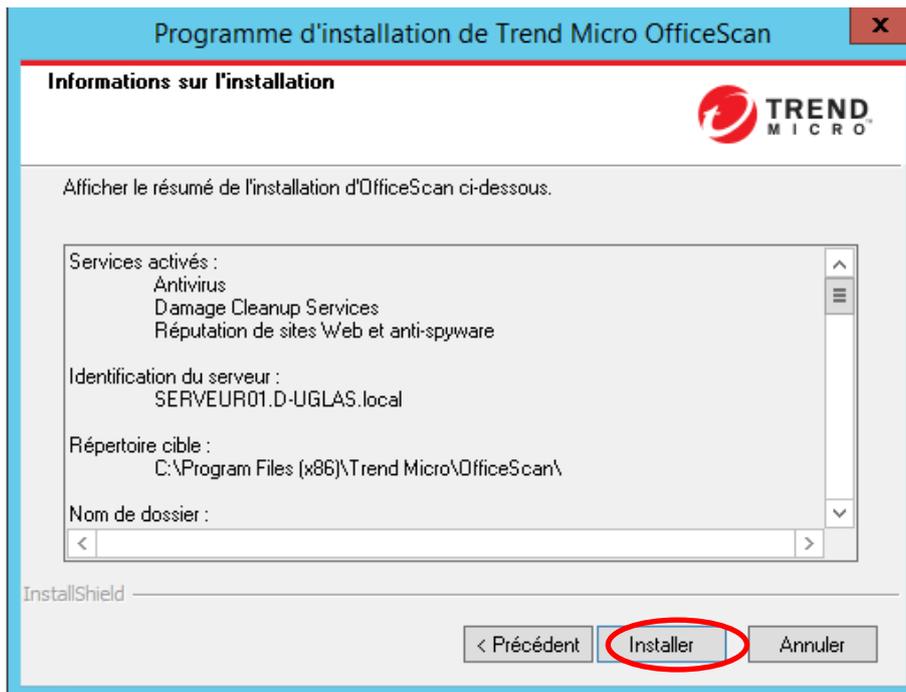
Nom de dossier :

Dossiers existants :

- Accessibility
- Accessories
- Administrative Tools
- Maintenance
- StartUp
- System Tools
- VMware

InstallShield

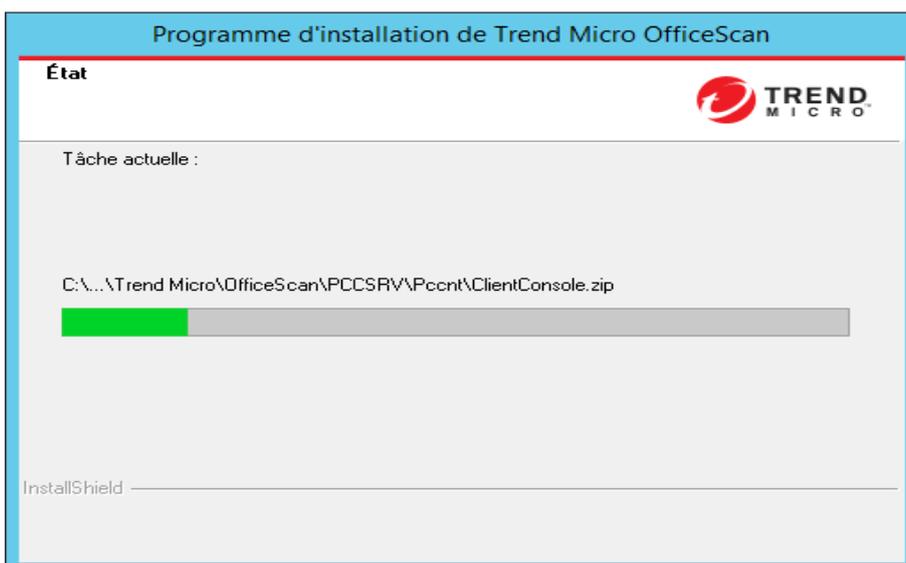
Récapitulatif avant le début de l'installation. Cliquer sur « Installer » :



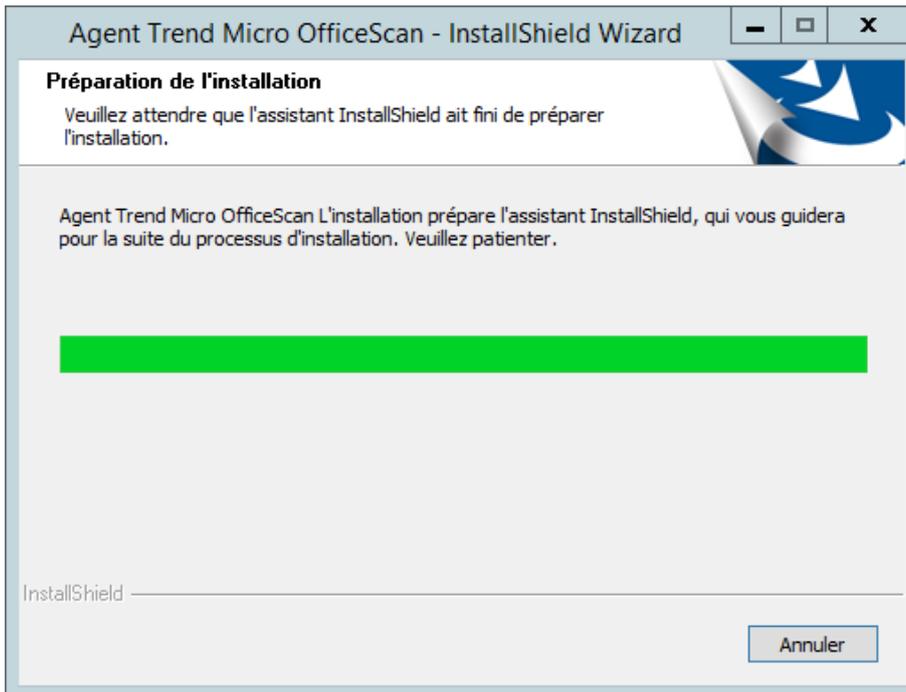
Remarque : IIS s'installera automatiquement dans le cas de Windows 2012R2, il pourra être nécessaire de l'installer préalablement sur des systèmes plus anciens.



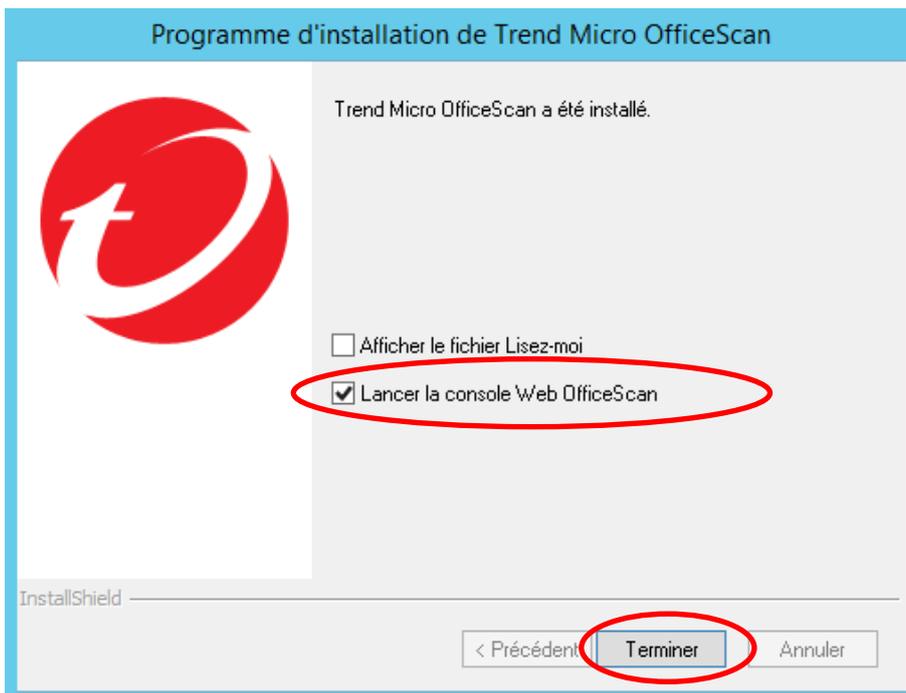
Début de l'installation : durée 10 à 15 mn environ suivant la configuration matérielle du serveur :



Installation de l'agent sur le serveur :

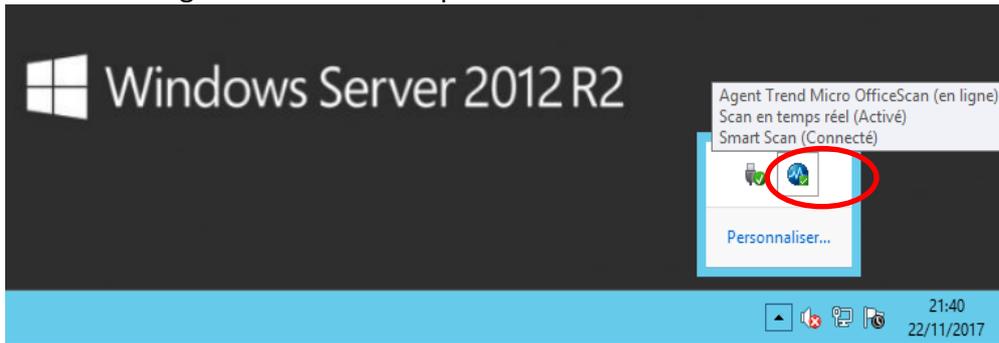


Installation terminée. Sélectionner « lancer la console Web OfficeScan » :

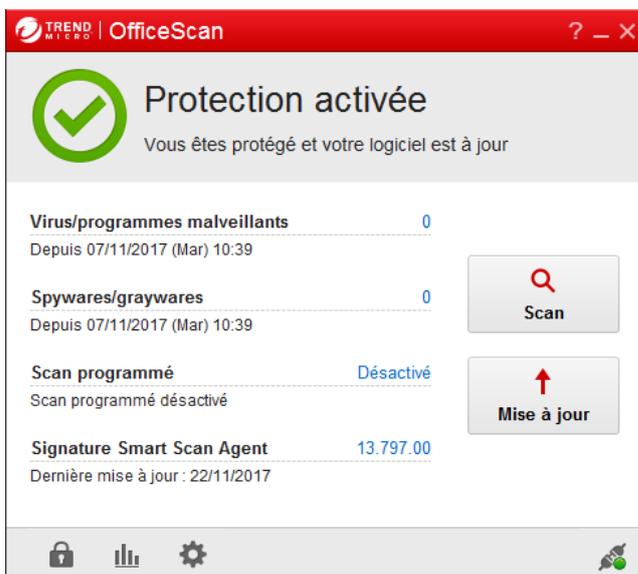


4- Vérification de la présence de l'Agent Trend sur le serveur :

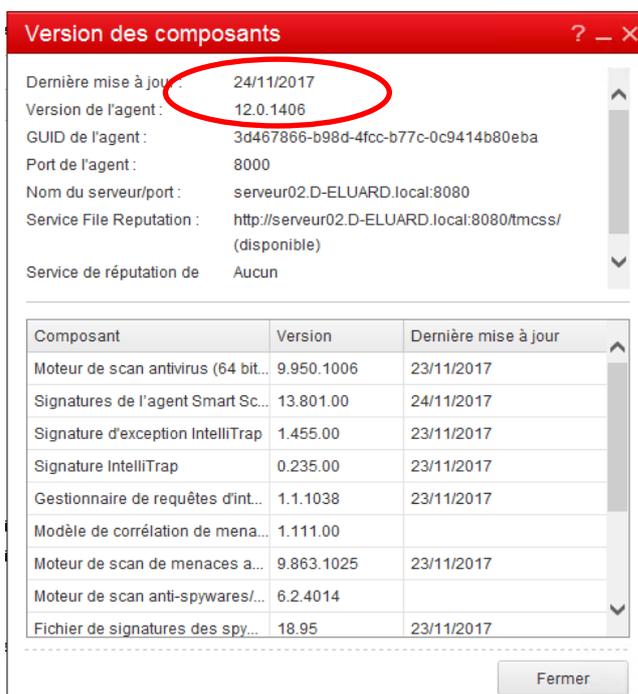
L'icône de l'Agent Trend est bien présente dans la zone de notification.



Dans le menu contextuel accessible avec un clic droit, on peut ouvrir la console de l'agent :



On peut aussi visualiser la version de l'agent, celle des différents moteurs de scan, la référence du fichier de signatures, les dates des dernières mises à jour, etc...



5- Installation des Patches :

D'une manière générale, il est important de procéder à l'installation du dernier patch de la version française en vigueur.

Si un autre patch plus ancien est requis, l'installation s'arrête. Un message indique alors la marche à suivre.

Ces patches sont disponibles sur le même site de téléchargement que la version complète :

http://downloadcenter.trendmicro.com/index.php?regs=fr&clk=latest&clkval=4973&lang_loc=2

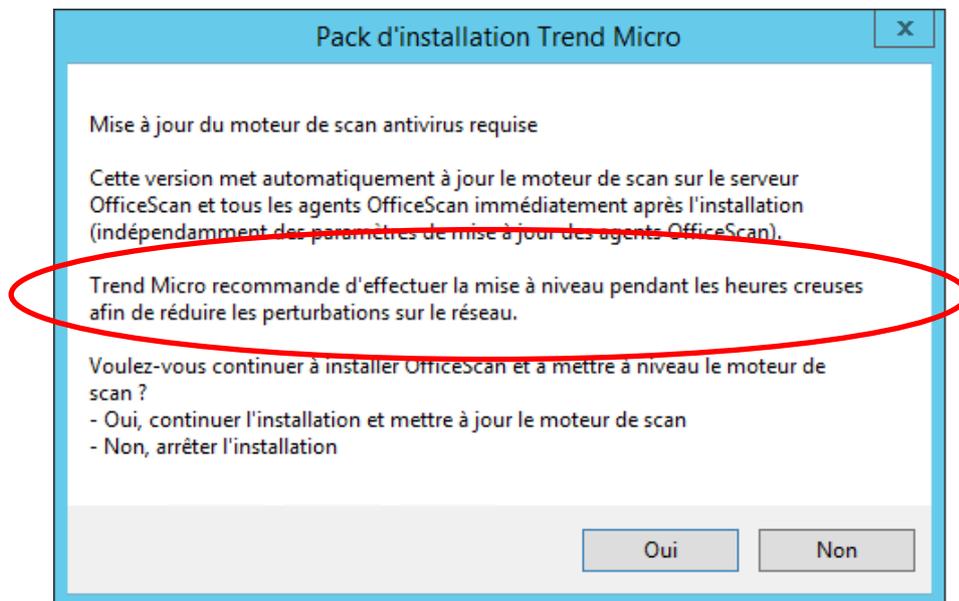
A ce jour, il faut installer dans cet ordre :

- Product Patch (osce-xg-win-fr-patch1-1576.exe)
- Critical Patch (osce-xg-win-fr-criticalpatch-1775.exe)

Ne pas oublier de débloquer les archives.

L'installation ne présente pas de difficulté particulière. Il suffit généralement, de valider les options proposées par défaut.

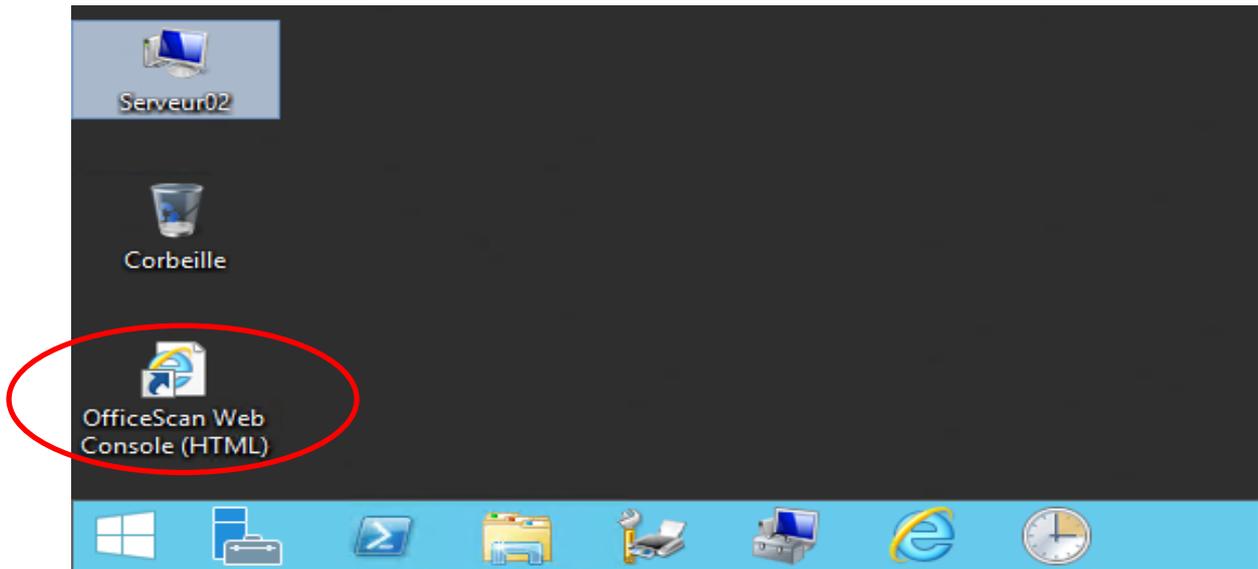
Attention toutefois aux avertissements, comme celui obtenu lors de l'installation du patch 1775 :



Des perturbations sur le réseau, sont à craindre. En cas de doute ne pas hésiter à reporter l'installation à une date à laquelle le réseau sera moins sollicité.

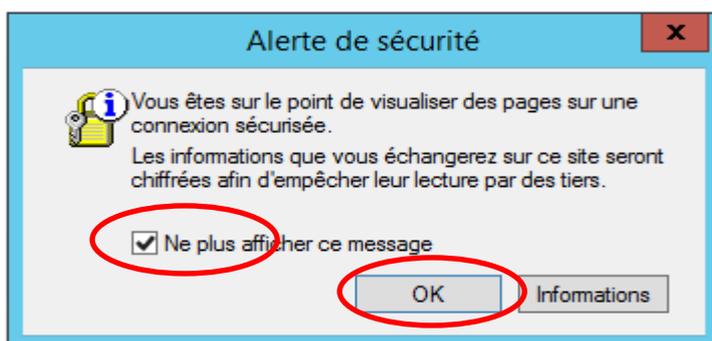
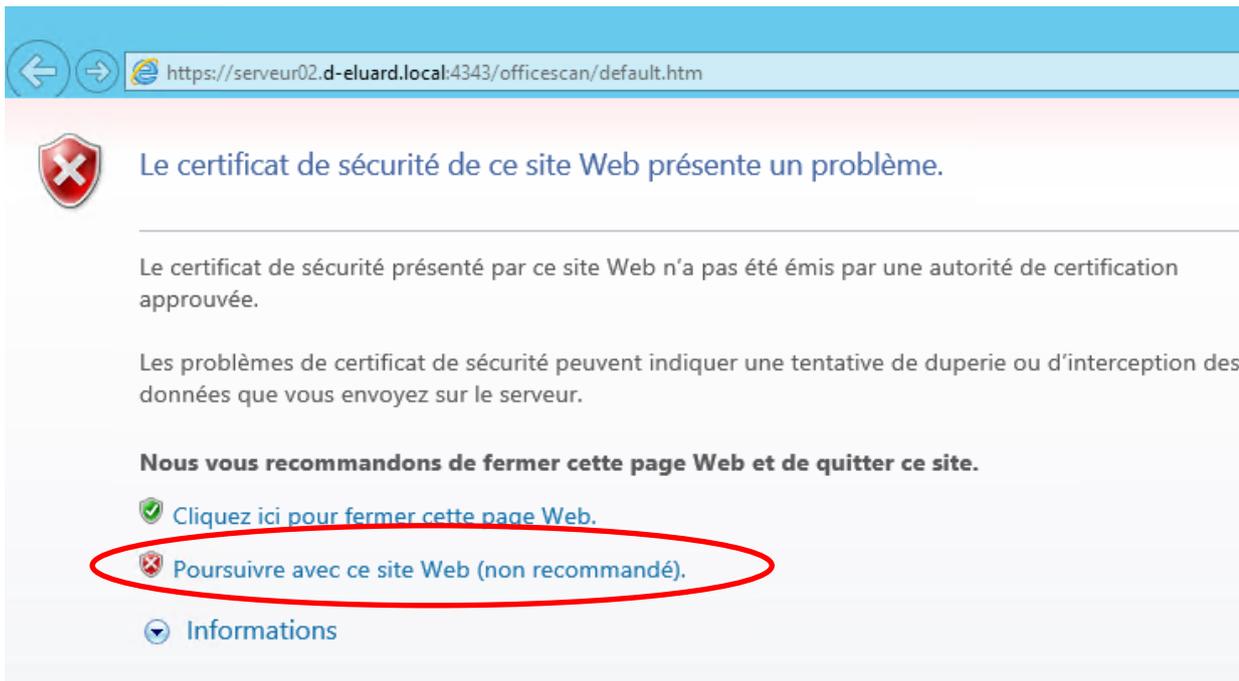
6- Ouverture de la console Web OfficeScan :

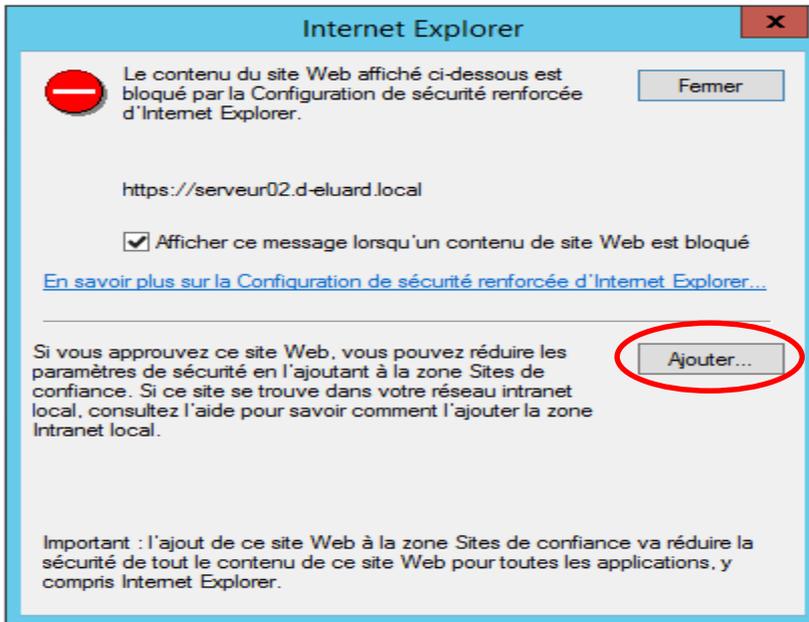
Une nouvelle icône est présente sur le bureau :



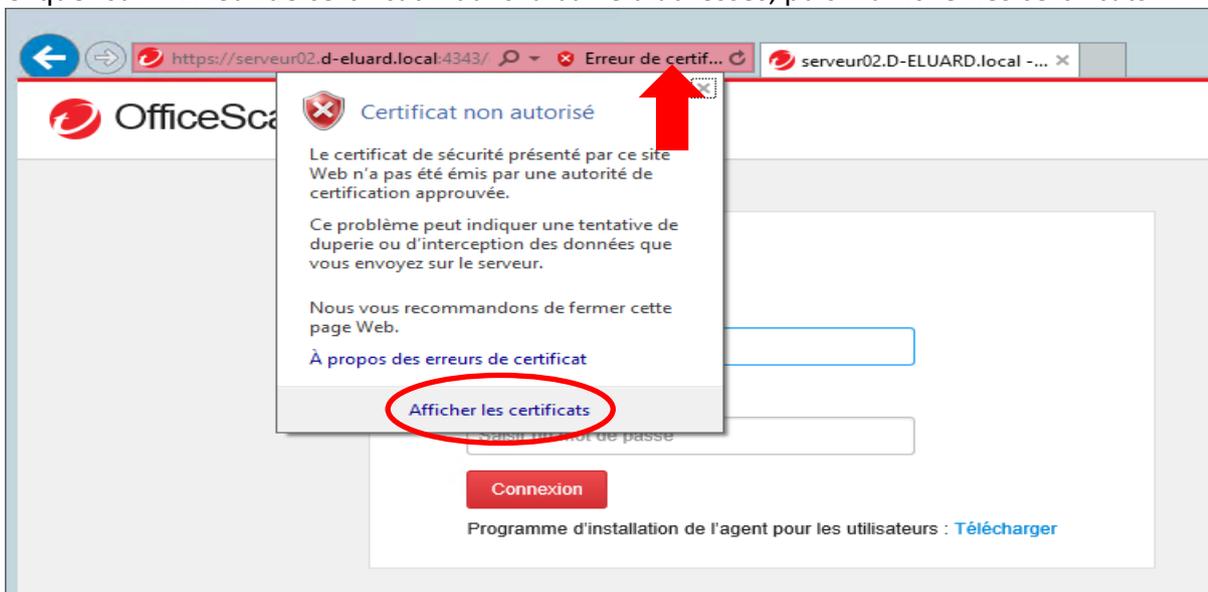
Au démarrage de la console : <https://serveurxx.d-xxxxx.local:4343/officescan/>

On obtient un avertissement de sécurité, faire « Poursuivre avec ce site Web » :

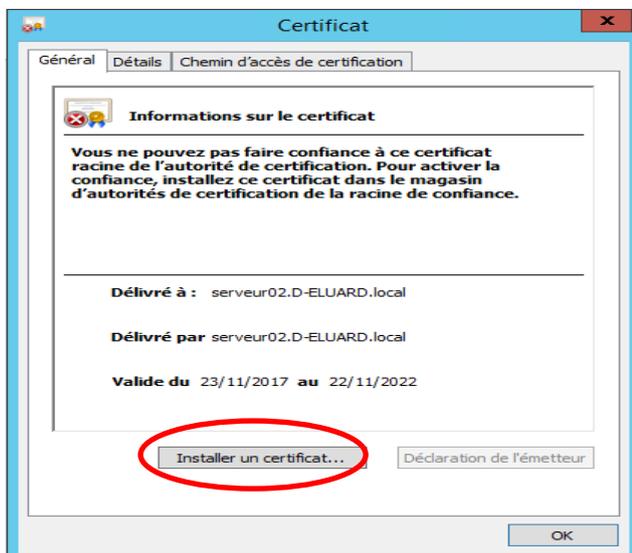


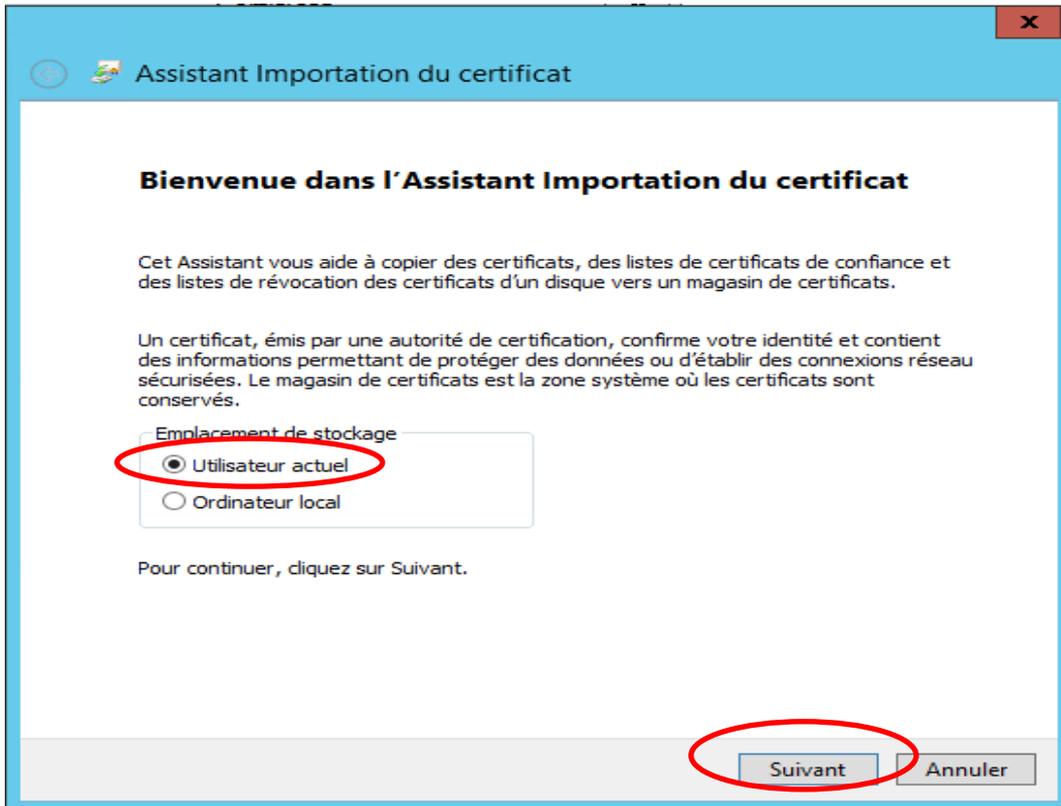


Cliquer sur « Erreur de certificat » dans la barre d'adresses, puis « afficher les certificats » :

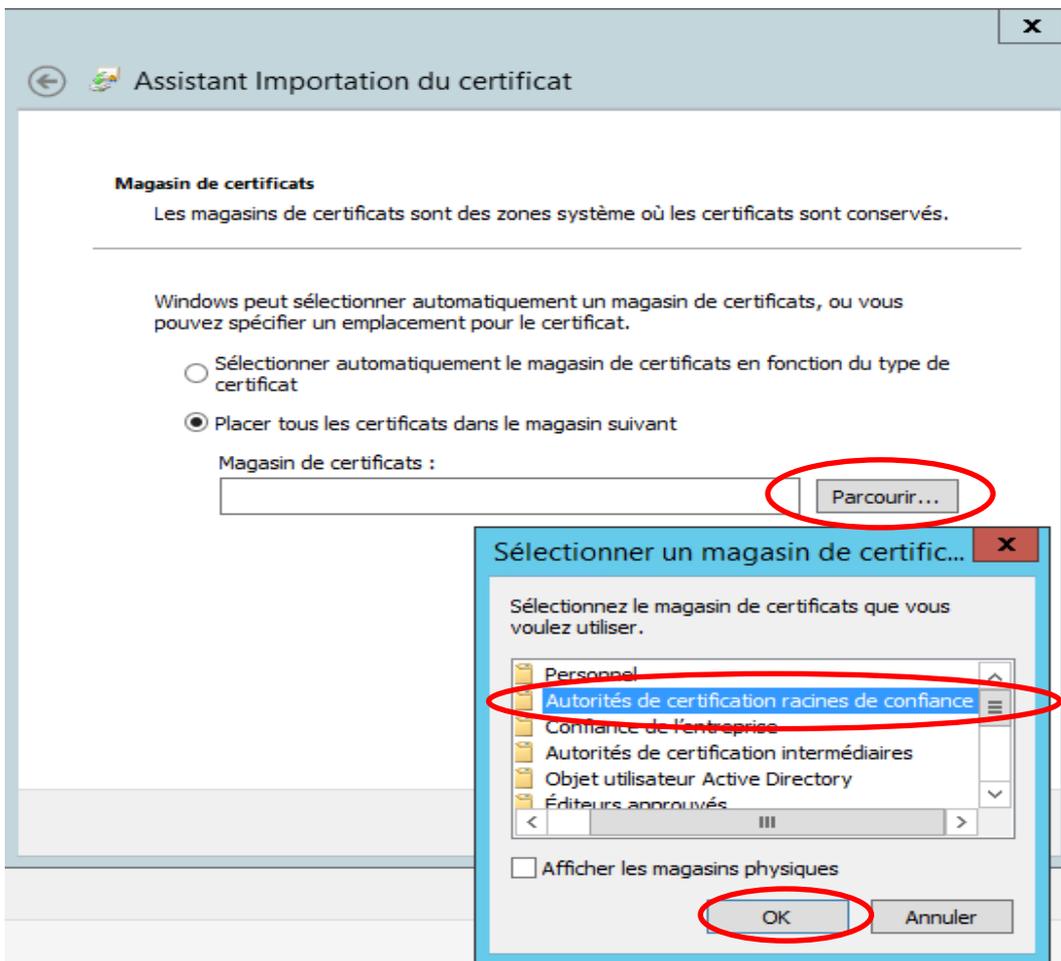


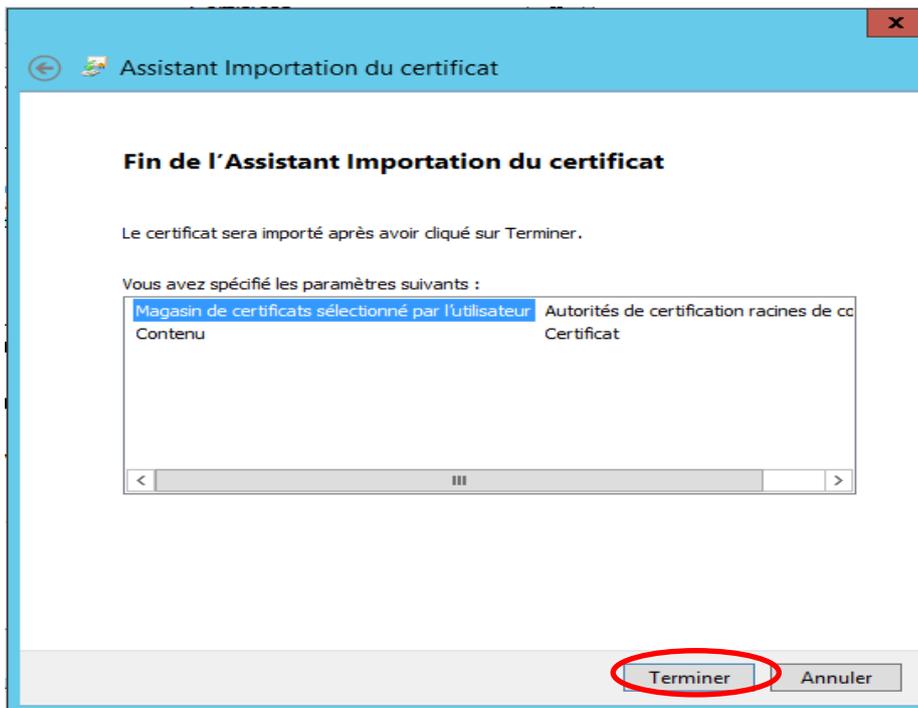
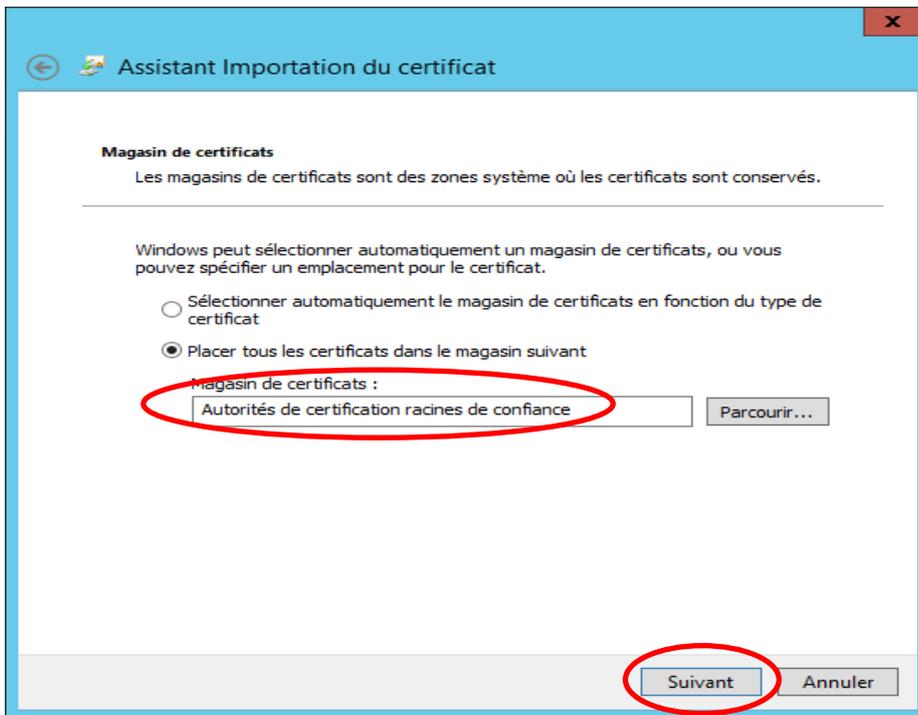
Faire : « Installer le certificat » :

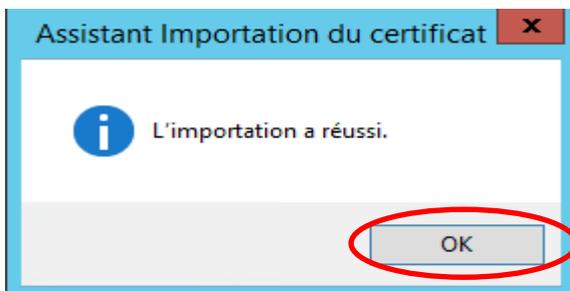
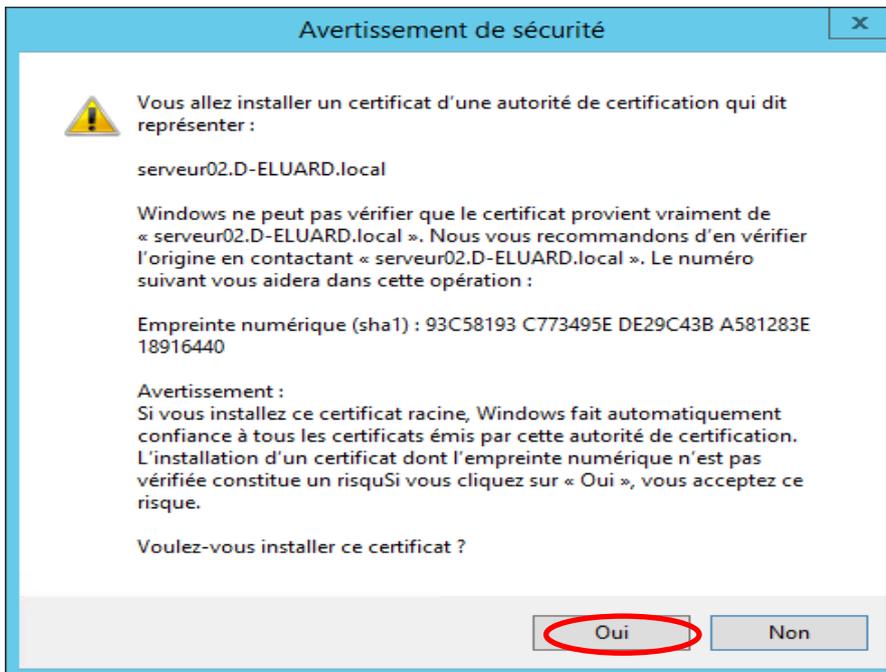




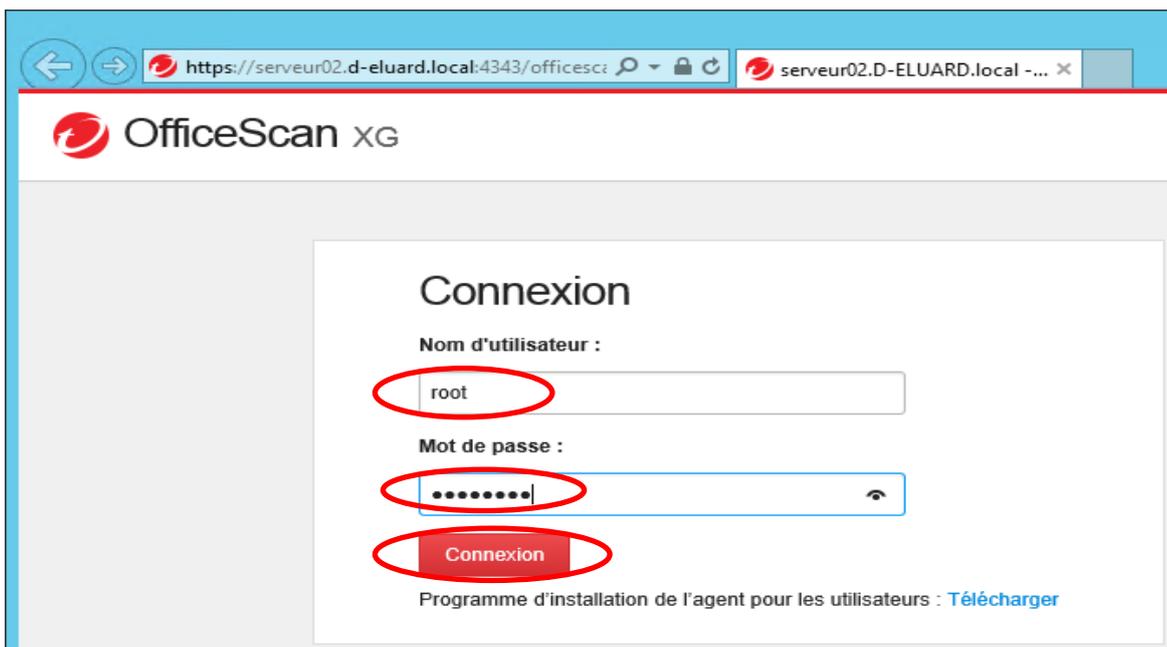
Choisir « Autorités de certification racine de confiance » :



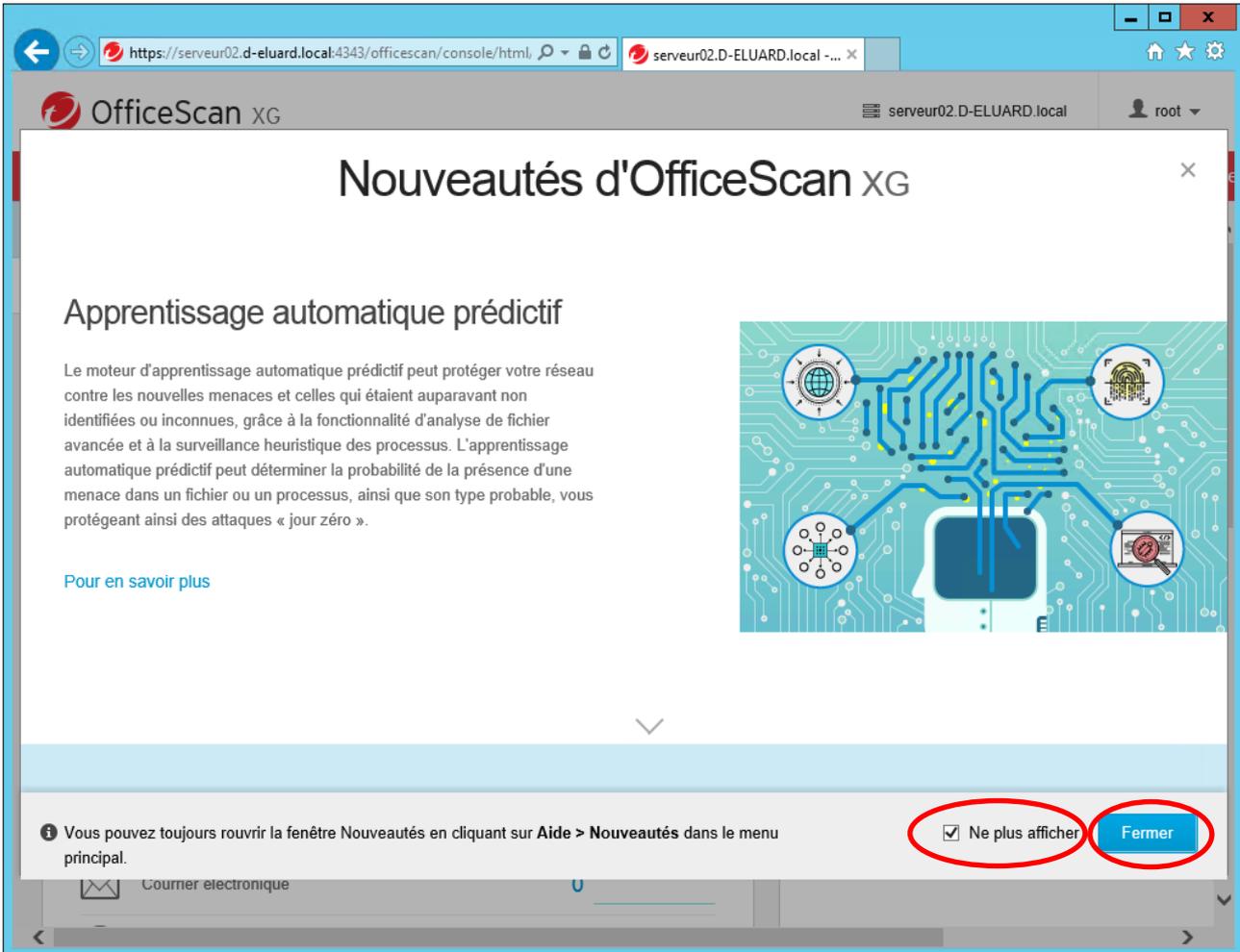




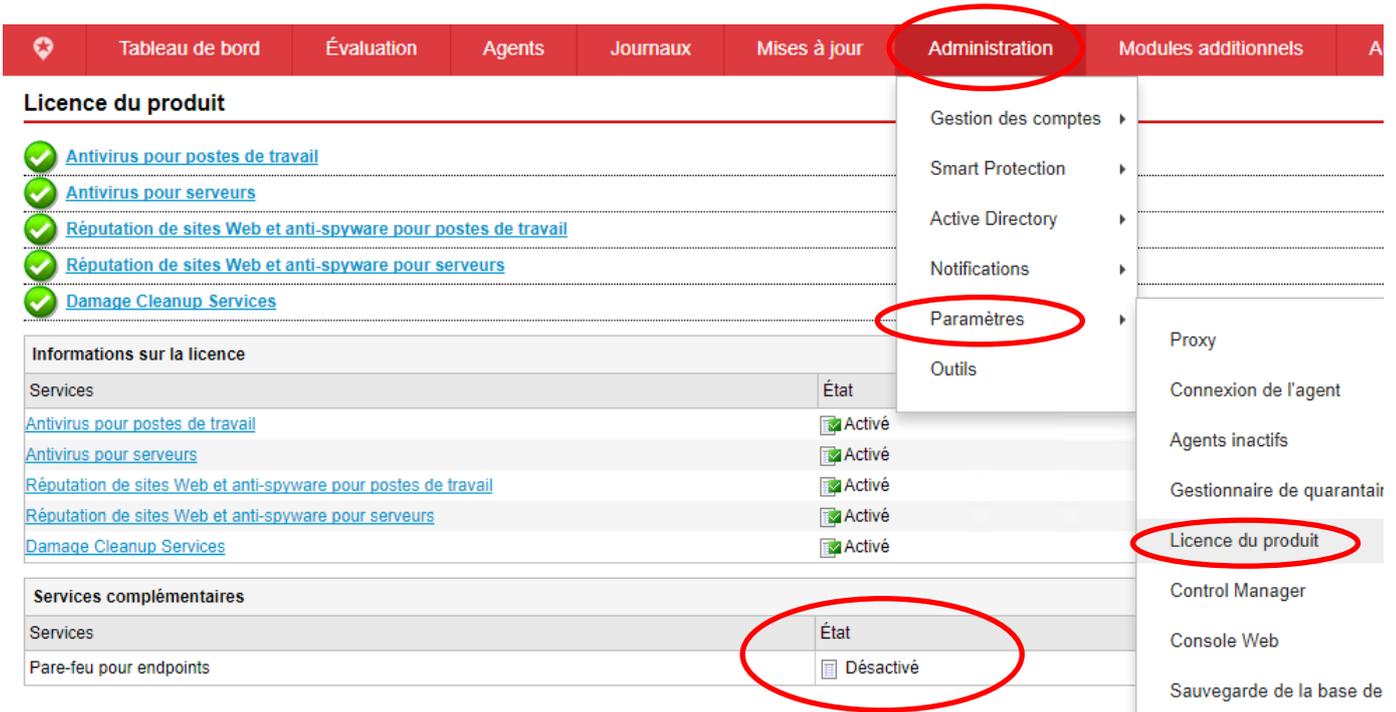
Au lancement suivant de la console le message d'erreur concernant le certificat a disparu. S'identifier avec le compte root :



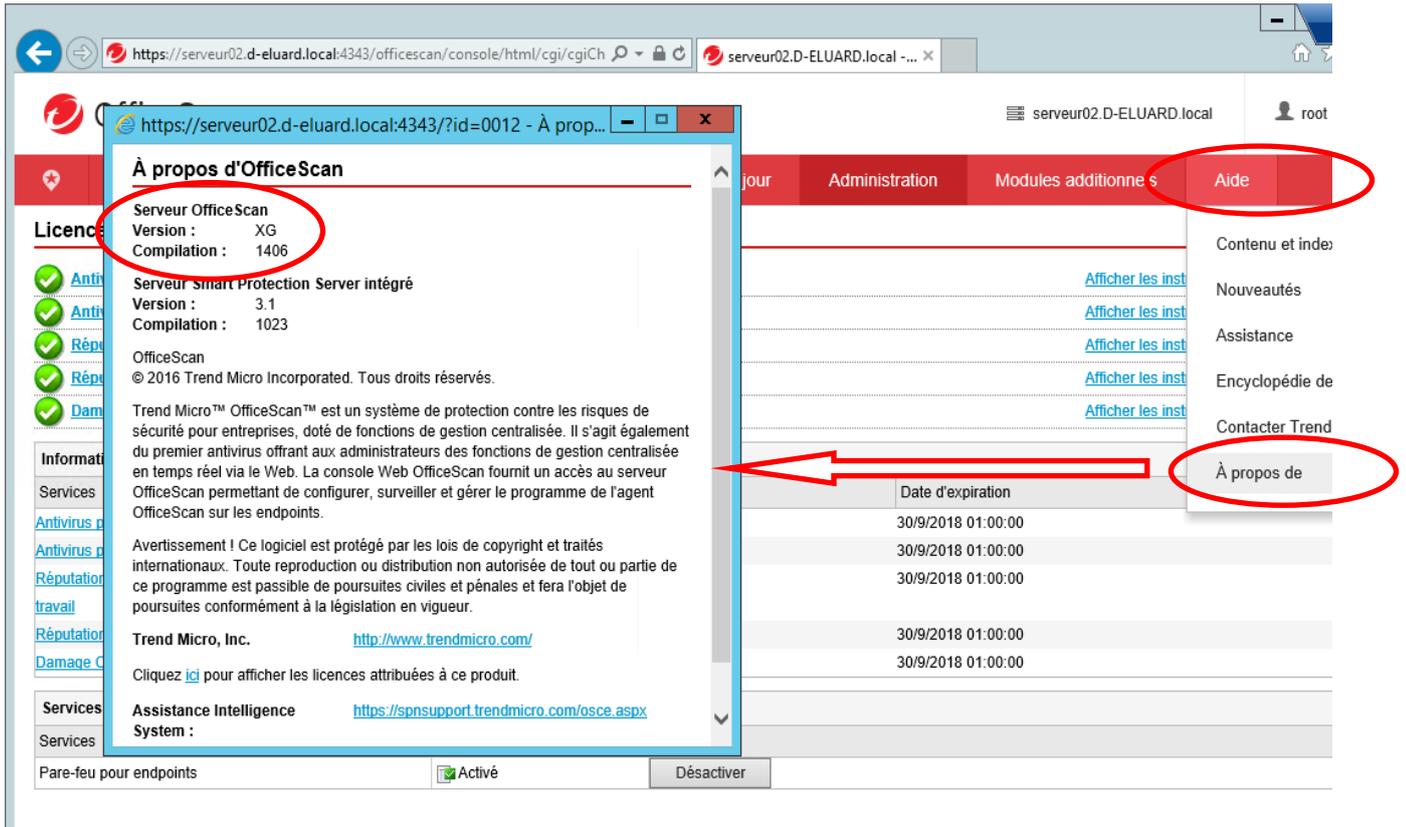
Une fenêtre présente les nouveautés d'OfficeScan XG. Cocher « Ne plus afficher » puis « Fermer » :



Dans le menu « Administration », « Paramètres », « Licence du produit » : tous les produits doivent être activés sauf le Parefeu :



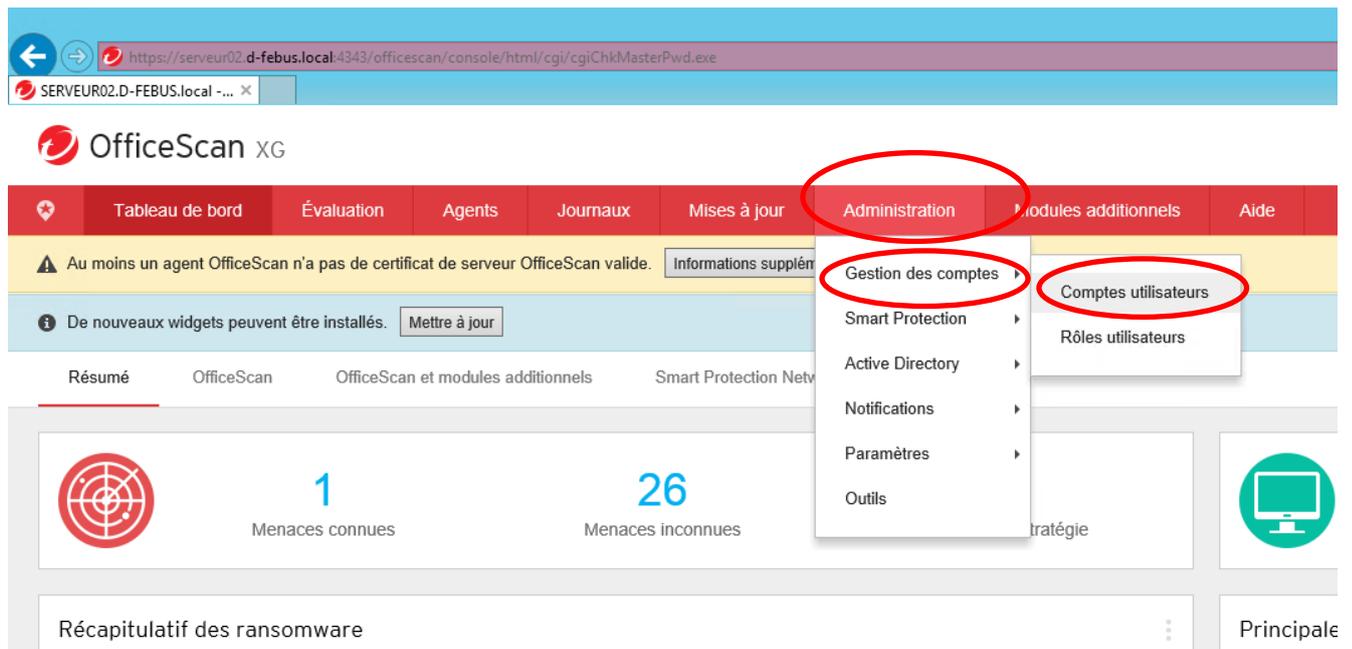
Dans le menu « Aide », « A propos de », on peut vérifier l'installation de la version XG :



7- Paramétrage de Trend OfficeScan :

7-1 Menu Administration :

Administration... Gestion des Comptes... Comptes utilisateurs...

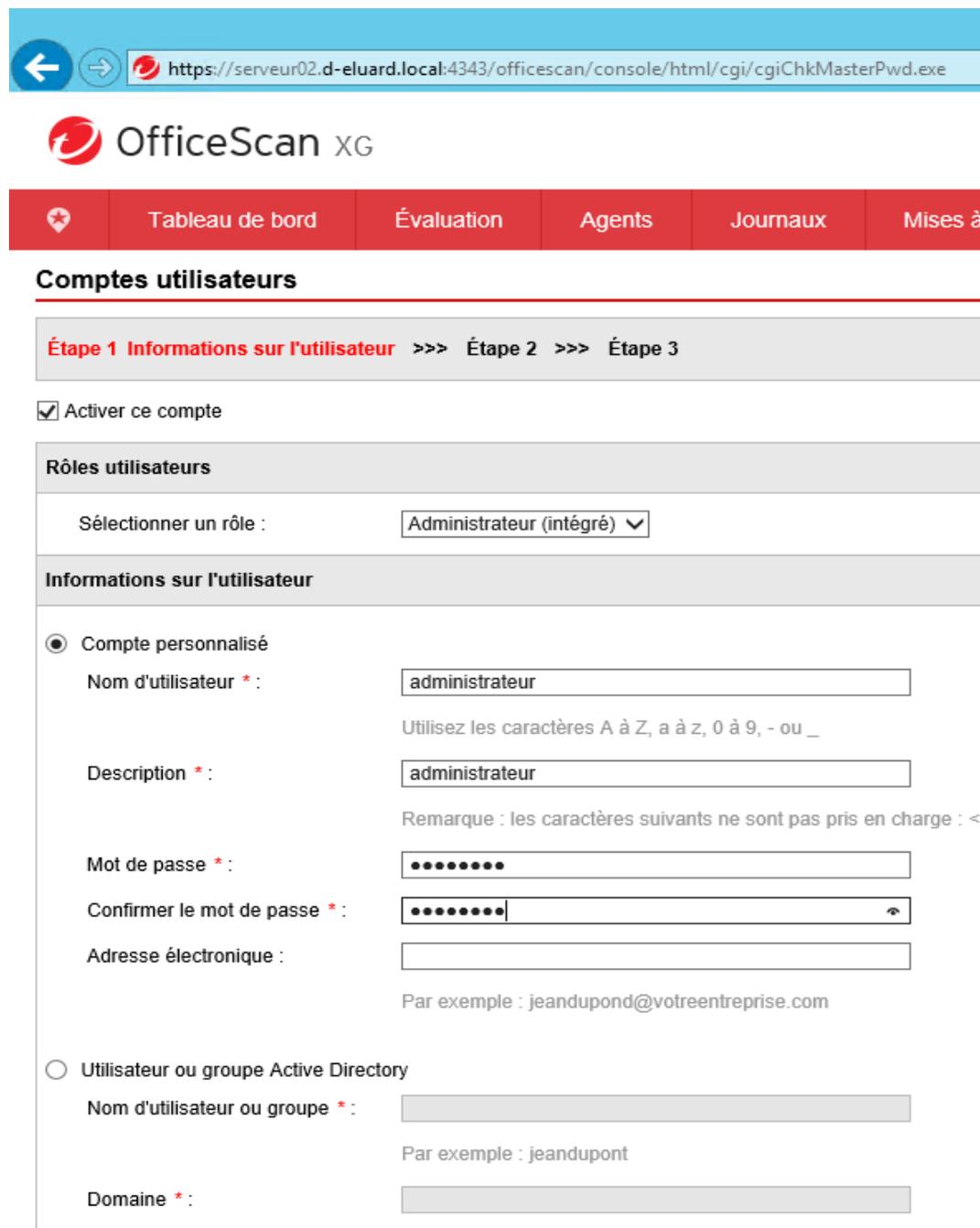


On pourra ici, changer le mot de passe du compte root, si cela s'avère nécessaire :



The screenshot shows the OfficeScan XG console interface. The browser address bar indicates the URL: <https://serveur02.d-eluard.local:4343/officescan/console/html/cgi/cgiChk>. The page title is "OfficeScan XG". The navigation menu includes "Tableau de bord", "Évaluation", "Agents", "Journaux", "Mises à jour", and "Administration". The main section is titled "Comptes utilisateurs". Below this, there are "Ajouter" and "Supprimer" buttons. A table lists users with columns for "Nom d'utilisateur", "Description", and "Domaine". The "root" user is highlighted with a red circle. Below the table, there are "Ajouter" and "Supprimer" buttons.

Ajouter un compte Administrateur (utile en cas de perte du mot de passe du compte root) :



The screenshot shows the OfficeScan XG console interface. The browser address bar indicates the URL: <https://serveur02.d-eluard.local:4343/officescan/console/html/cgi/cgiChkMasterPwd.exe>. The page title is "OfficeScan XG". The navigation menu includes "Tableau de bord", "Évaluation", "Agents", "Journaux", and "Mises à jour". The main section is titled "Comptes utilisateurs". Below this, there are "Étape 1 Informations sur l'utilisateur >>> Étape 2 >>> Étape 3". A checkbox "Activer ce compte" is checked. The "Rôles utilisateurs" section shows "Administrateur (intégré)" selected. The "Informations sur l'utilisateur" section has "Compte personnalisé" selected. The form fields are: "Nom d'utilisateur * : administrateur", "Description * : administrateur", "Mot de passe * : [masked]", "Confirmer le mot de passe * : [masked]", "Adresse électronique : [empty]", "Utilisateur ou groupe Active Directory" is unselected. The form fields are: "Nom d'utilisateur ou groupe * : [empty]", "Domaine * : [empty]".

Administration... Active Directory... Intégration Active Directory...

Faire « Enregistrer et synchroniser » :

The screenshot shows the OfficeScan XG Administration console. The 'Administration' menu is open, with 'Active Directory' and 'Intégration d'Active Directory' highlighted. The 'Intégration d'Active Directory' page is visible, showing fields for 'Domaines Active Directory', 'Paramètres de chiffrement pour les informations d'authentification du domaine', and buttons for 'Enregistrer', 'Annuler', and 'Enregistrer et synchroniser'.

The screenshot shows the OfficeScan XG Administration console after successful registration. A green message indicates 'Enregistrement des paramètres spécifiés effectué.' The 'Enregistrer et synchroniser' button is highlighted.

Administration... Active Directory... Synchronisation programmée...

The screenshot shows the OfficeScan XG Administration console. The 'Administration' menu is open, with 'Active Directory' and 'Synchronisation programmée' highlighted. The 'Synchronisation programmée' page is visible, showing options for 'Activer la synchronisation programmée d'Active Directory', 'Synchronisation programmée d'Active Directory', and frequency settings (Quotidienne, Hebdomadaire, Mensuelle). The 'Enregistrer' button is highlighted.

https://serveur02.d-eluard.local:4343/officescan/console/html/cgi/cgiChkMasterPwd.

OfficeScan XG

Tableau de bord Évaluation Agents Journaux Mises à jour

Synchronisation programmée

✓ Modification des paramètres de configuration effectuée.

Activer la synchronisation programmée d'Active Directory

Synchronisation programmée d'Active Directory

Quotidienne
 Hebdomadaire, tous les Lundi ▼
 Mensuelle, le 01 ▼

Heure de début: 00 ▼ : 00 ▼ (hh:mm)

Enregistrer Annuler

Administration... Paramètres... Agents inactifs...

Activer la Suppression automatique des agents, inactifs depuis plus de **90** jours :

Tableau de bord Évaluation Agents Journaux Mises à jour **Administration** Modules additionnels Aide

Agents inactifs

Suppression des agents inactifs

Activer la suppression automatique des agents inactifs
 Supprimer automatiquement les agents s'ils sont inactifs depuis 90 ▼ jours

Enregistrer Annuler

- Gestion des comptes
- Smart Protection
- Active Directory
- Notifications
- Paramètres**
 - Proxy
 - Connexion de l'agent
 - Agents inactifs**
 - Gestionnaire de quarantaine
 - Licence du produit
 - Control Manager
 - Console Web
 - Sauvegarde de la base de dor
- Outils

Tableau de bord Évaluation Agents Journaux

Agents inactifs

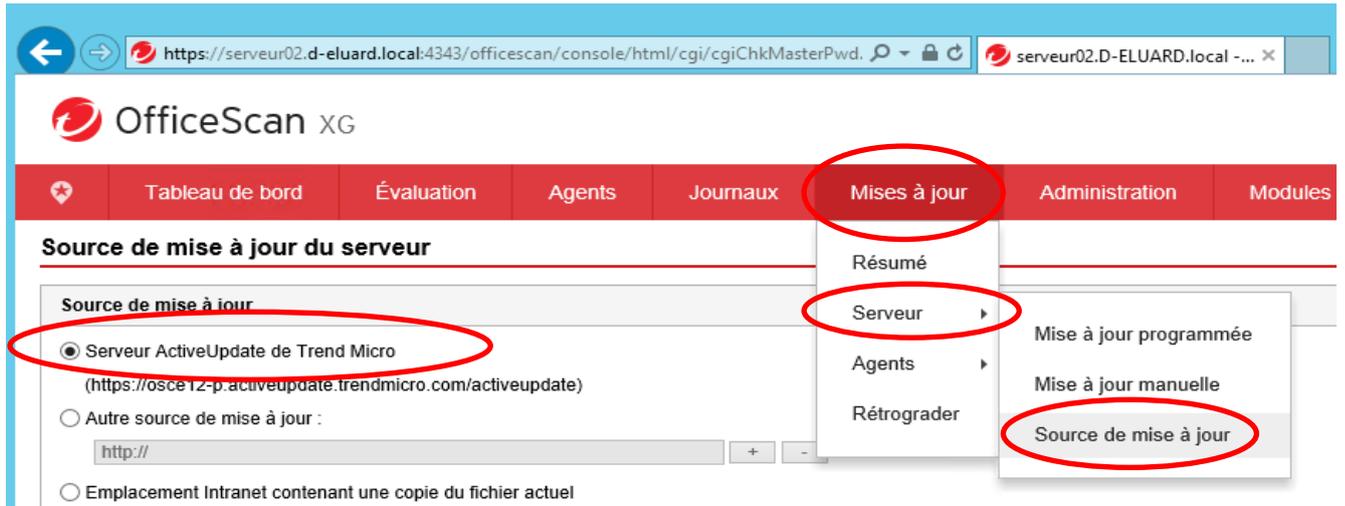
✓ Les paramètres de suppression des agents inactifs ont été mis à jour.

Suppression des agents inactifs

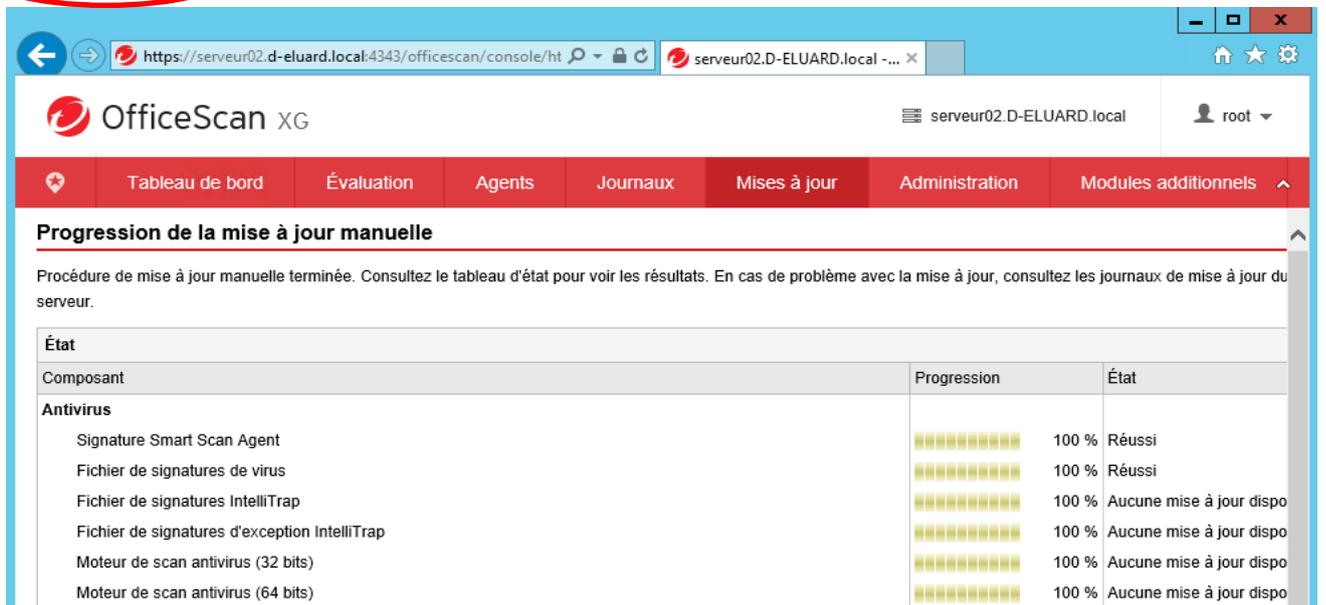
Activer la suppression automatique des agents inactifs
 Supprimer automatiquement les agents s'ils sont inactifs depuis 90 ▼ jours

Enregistrer Annuler

7-2 Menu « Mises à jour » : Mises à jour... Serveur... Source de mise à jour...



Mises à jour... Serveur... Mise à jour manuelle... cliquer sur « Mise à jour » :



Mises à jour... Serveur... Mise à jour programmée...

OfficeScan XG

Tableau de bord | Évaluation | Agents | Journaux | **Mises à jour** | Administration | Modules a

Mise à jour programmée du serveur

Activer la mise à jour programmée du serveur OfficeScan

Composants à mettre à jour

- Composants de l'Endpoint
- Antivirus
- Anti-spyware
- Damage Cleanup Services
- Pare-feu
- Composants de la surveillance des comportements
- Connexions suspectes
- Solution contre l'exploitation du navigateur

Programmation des mises à jour

Toutes les heures

Quotidienne

Hebdomadaire, tous les

Mensuelle, le

Heure de début : : (hh:mm)

Mettre à jour pour une période de heure(s)

OfficeScan XG

Tableau de bord | Évaluation | Agents | Journaux | **Mises à jour**

Mise à jour programmée du serveur

Modification des paramètres de configuration effectuée.

Activer la mise à jour programmée du serveur OfficeScan

Composants à mettre à jour

- Composants de l'Endpoint
- Antivirus
- Anti-spyware
- Damage Cleanup Services
- Pare-feu
- Composants de la surveillance des comportements
- Connexions suspectes
- Solution contre l'exploitation du navigateur

Programmation des mises à jour

Toutes les heures

Quotidienne

Hebdomadaire, tous les

Mensuelle, le

Heure de début : : (hh:mm)

Mettre à jour pour une période de heure(s)

Mises à jour... Agents... Source de mise à jour... simple vérification :

The screenshot shows the OfficeScan XG console interface. The top navigation bar includes 'Tableau de bord', 'Évaluation', 'Agents', 'Journaux', 'Mises à jour', 'Administration', and 'Mod'. The 'Mises à jour' menu is open, showing options: 'Résumé', 'Serveur', 'Agents', and 'Rétrograder'. The 'Agents' option is selected, leading to a sub-menu with 'Mise à jour automatique', 'Mise à jour manuelle', and 'Source de mise à jour'. The main content area is titled 'Source de mise à jour des agents'. It contains a section 'Sélectionnez des sources de mise à jour alternatives pour des agents spécifiques en indiquant' with two radio buttons: 'Source de mise à jour standard (mise à jour depuis le serveur OfficeScan)' (selected) and 'Source de mise à jour personnalisée'. Below this are several checkboxes: 'Les agents de mise à jour effectuent la mise à jour des composants, des paramètres du serveur OfficeScan', 'Les agents OfficeScan mettent à jour les éléments suivants à partir du serveur OfficeScan si toutes les sources pe...', 'Composants', 'Paramètres de domaine', and 'Programmes et correctifs de type hot fix des agents OfficeScan'. A table titled 'Liste des sources de mise à jour personnalisées' is empty. At the bottom, there is a 'Notifier tous les agents' button.

Mises à jour... Agents... Mise à jour automatique...

The screenshot shows the OfficeScan XG console interface. The top navigation bar includes 'Tableau de bord', 'Évaluation', 'Agents', 'Journaux', 'Mises à jour', 'Administration', and 'Modul'. The 'Mises à jour' menu is open, showing options: 'Résumé', 'Serveur', 'Agents', and 'Rétrograder'. The 'Agents' option is selected, leading to a sub-menu with 'Mise à jour automatique', 'Mise à jour manuelle', and 'Source de mise à jour'. The main content area is titled 'Mises à jour automatiques de l'agent'. It contains a section 'Déclencher les mises à jour des agents lorsque certains événements se produisent ou selon u...'. Below this is a section 'Mise à jour déclenchée par un événement' with three checkboxes: 'Lancer la mise à jour des composants sur les agents immédiatement après le téléchargement' (checked), 'Inclure ou les agents indépendants et hors ligne' (checked), and 'Permettre aux agents de lancer une mise à jour des composants lorsqu'ils redémarrent et se connectent au serveur' (checked). There is also an unchecked checkbox 'Exécuter un scan immédiat après la mise à jour (les agents indépendants sont exclus)'. Below this is a section 'Mise à jour programmée' with three radio buttons: 'Toutes les minutes', 'Toutes les heures' (selected), and 'Quotidienne'. There is also an option 'Hebdomadaire, tous les' with a dropdown set to 'Dimanche'. A dropdown menu is set to '04' heure(s) and a checkbox 'Mettre à jour les configurations des agents une seule fois par jour' is checked. At the bottom, there are 'Enregistrer' and 'Annuler' buttons.

OfficeScan XG

Tableau de bord Évaluation Agents Journaux Mises à jour Adm

Mises à jour automatiques de l'agent

✓ Les paramètres spécifiés ont été enregistrés.

Déclencher les mises à jour des agents lorsque certains événements se produisent ou selon une programmation.

Mise à jour déclenchée par un événement

Lancer la mise à jour des composants sur les agents immédiatement après le téléchargement d'un nouveau composant et

Inclure le ou les agents indépendants et hors ligne

Permettre aux agents de lancer une mise à jour des composants lorsqu'ils redémarrent et se connectent au serveur OfficeScan

Exécuter un scan immédiat après la mise à jour (les agents indépendants sont exclus)

Mise à jour programmée

Toutes les minutes

Toutes les heures

Quotidienne

Hebdomadaire, tous les

heure(s)

Mettre à jour les configurations des agents une seule fois par jour

Enregistrer Annuler

7-3 Menu « Agents » :

Agents... Regroupement des agents...

Regrouper les agents suivant leur appartenance au domaine :

OfficeScan XG

Tableau de bord Évaluation **Agents** Journaux Mises à jour

Regroupement des agents

Regrouper automatiquement les nouveaux agents OfficeScan à l'aide de :

Créer des groupes d'agents personnalisés pour les agents OfficeScan existants

Enregistrer Annuler

- Gestion des agents
- Regroupement des agents**
- Paramètres généraux de l'agent
- Emplacement de l'Endpoint
- Pare-feu
- Installation de l'agent
- Vérification de la connexion
- Prévention des épidémies

OfficeScan XG

Tableau de bord Évaluation Agents Journaux Mises à jour

Regroupement des agents

Regrouper automatiquement les nouveaux agents OfficeScan à l'aide de :

Créer des groupes d'agents personnalisés pour les agents OfficeScan existants

Enregistrer Annuler

https://serveur02.d-eluard.local:4343/officescan/console/html/cgi/cgiChkMasterPwd.exe

OfficeScan XG

Tableau de bord Évaluation **Agents** Journaux Mises à jour

Regroupement des agents

✓ Les paramètres ont été enregistrés.

Regroupement des agents

Regrouper automatiquement les nouveaux agents OfficeScan à l'aide de : Domaine Active Directory ▼

Créer des groupes d'agents personnalisés pour les agents OfficeScan existants

Enregistrer Annuler

Agents... Paramètres généraux de l'agent... Paramètres de sécurité...
 Pas de modifications dans cet onglet :

https://serveur02.d-eluard.local:4343/officescan/console/html/cgi/cgiChkMasterPwd.exe

OfficeScan XG

Tableau de bord Évaluation **Agents** Journaux Mises à jour Adm

Paramètres généraux de l'agent

Configurez des paramètres avancés qui s'appliqueront à t

Paramètres de sécurité Système Réseau **Paramètres généraux de l'agent**

Paramètres de scan

Exclure du scan en temps réel le dossier de la base

Exclure des scans les dossiers et les fichiers de ser

Activer le scan différé pour les opérations de fichier

Activer le démarrage anticipé de protection contre le

Paramètres de scan pour les fichiers compressés v

Scan en temps réel

Ne pas scanner les fichiers si la taille du fichier compressé dépasse Mo

Dans un fichier compressé, scanner uniquement les premiers fichiers

Scan manuel/Scan programmé/Scan immédiat

Ne pas scanner les fichiers si la taille du fichier compressé dépasse Mo

Dans un fichier compressé, scanner uniquement les premiers fichiers

Paramètres de scan antivirus/programme malveillant uniquement

Nettoyer/supprimer les fichiers infectés dans les fichiers compressés ⓘ

Paramètres de scan anti-spyware/grayware uniquement

Activer le mode d'évaluation ⓘ

Le mode d'évaluation se termine à 12:00:00 le

jj/mm/aaaa

Recherche de cookies ⓘ

Comptabiliser les cookies dans le journal de spywares

Paramètres de scan programmé

Rappeler aux utilisateurs le scan programmé minutes avant son exécution

Différer le scan programmé de heure(s) et minute(s) maximum

Arrêter automatiquement le scan programmé lorsque le scan dure depuis plus de heure(s) et minute(s)

Agents... Paramètres généraux de l'agent... Contrôle d'agent...

Ajouter le scan manuel pour les utilisateurs , et fixer le délais d'alerte à 20 jours.

https://serveur02.d-eluard.local:4343/officescan/console/html/cgi/cgiChkMasterPwd.exe

OfficeScan XG

Tableau de bord Évaluation **Agents** Journaux Mises à jour Administration

Paramètres généraux de l'agent

Configurez des paramètres avancés qui s'appliqueront à tous les agents OfficeScan du réseau.

Paramètres de sécurité Système Réseau **Contrôle d'agent**

Paramètres généraux

Ajouter le scan manuel au menu de raccourcis Windows sur les endpoints

Paramètres d'alerte

Afficher l'icône d'alerte dans la barre des tâches Windows si le fichier de signatures de virus n'a pas été mis à jour au bout de 20 jour(s)

Afficher un message de notification si le endpoint doit être redémarré pour charger un pilote en mode noyau ⓘ

Configuration de la langue de l'agent

Le programme de l'agent OfficeScan applique le paramètre de langue suivant :

Paramètres de langue locale sur l'endpoint

Langue du serveur OfficeScan

Enregistrer Annuler

https://serveur02.d-eluard.local:4343/officescan/console/html/cgi/cgiChkMasterPwd.exe

OfficeScan XG

Tableau de bord Évaluation Agents Journaux Mises à jour

Paramètres généraux de l'agent

Les changements de configuration ont été appliqués.

Une notification est actuellement envoyée aux agents OfficeScan. Veuillez noter que la propagation des nouveau:

<Précédent

7-4 Gestion des agents :

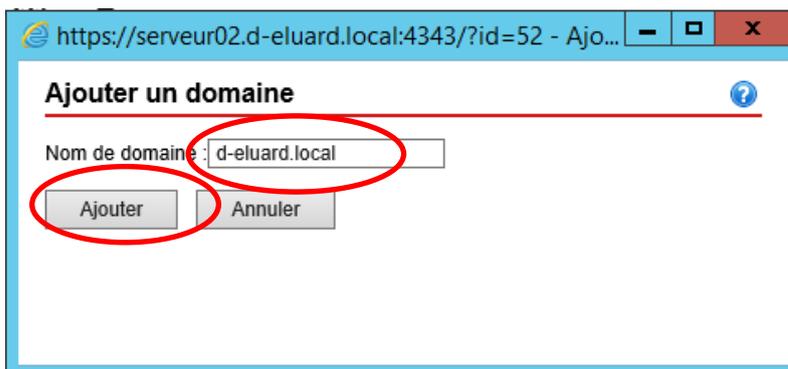
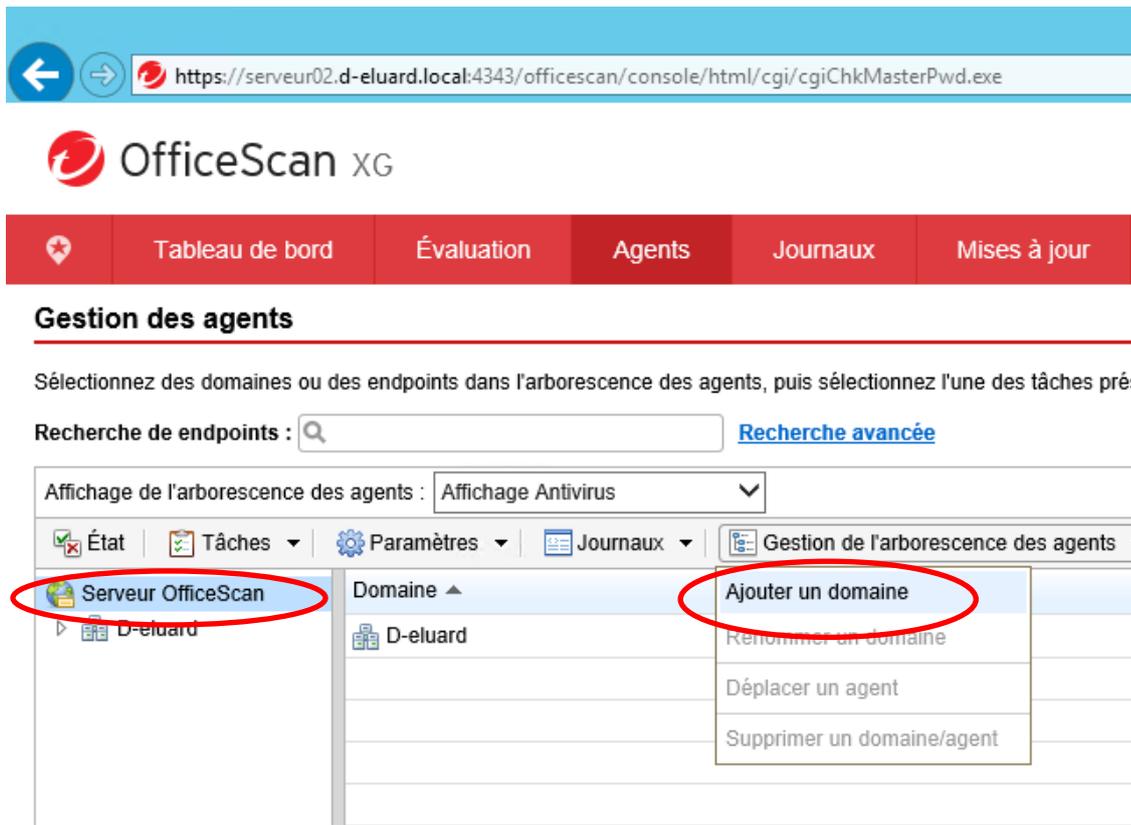
7-4.1 Gestion de l'arborescence des agents :

Nous allons regrouper les agents des stations et des serveurs dans un même domaine. Les serveurs pourront être regroupés dans un sous-ensemble « Serveurs ».

S'il n'existe pas déjà, créer le domaine : D-domaine.local :

Agents... Gestion des agents... Gestion de l'arborescence des agents...

Se placer au niveau « **Serveur OfficeScan** » et faire « **Ajouter un domaine** » :



Se placer au niveau « **D-domaine.local** » et Faire « Ajouter un domaine » :

The screenshot shows the OfficeScan XG web interface. At the top, the URL is <https://serveur02.d-eluard.local:4343/officescan/console/html/cgi/cgiChkMasterPwd.exe>. The page title is "OfficeScan XG". A navigation bar contains "Tableau de bord", "Évaluation", "Agents", "Journaux", and "Mises à jour". The main section is titled "Gestion des agents". Below this, there is a search bar for endpoints and a dropdown menu for "Affichage de l'arborescence des agents" set to "Affichage Antivirus". A toolbar includes "État", "Tâches", "Paramètres", "Journaux", and "Gestion de l'arborescence des agents". The left sidebar shows a tree view with "Serveur OfficeScan", "D-eluard", and "D-eluard.local" (highlighted with a red circle). A context menu is open over "D-eluard.local", with "Ajouter un domaine" (circled in red) selected. Other menu items include "Renommer un domaine", "Déplacer un agent", and "Supprimer un domaine/agent".

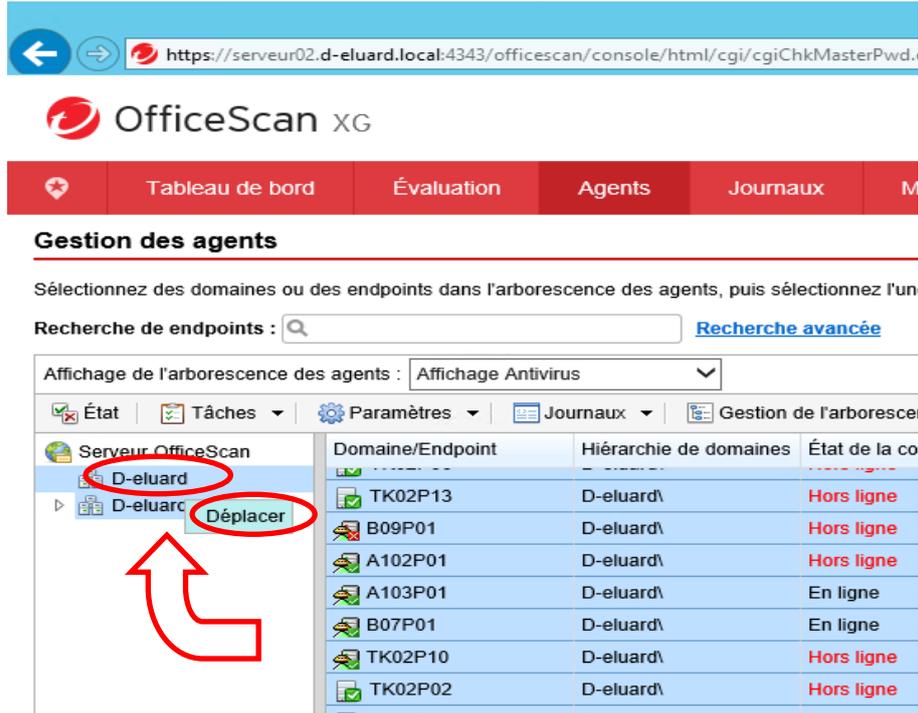
The screenshot shows a dialog box titled "Ajouter un domaine". It has a text input field for "Nom de domaine" containing "Serveurs" (circled in red). Below the input field are two buttons: "Ajouter" and "Annuler" (both circled in red).

On obtient :

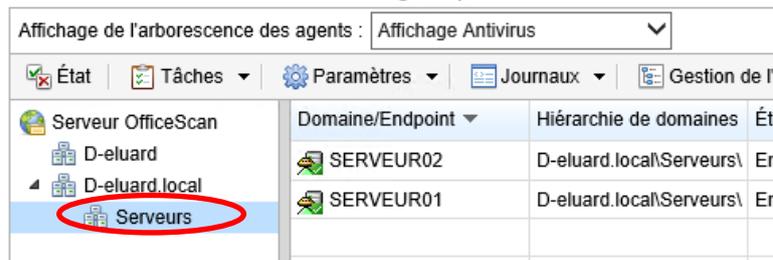
The screenshot shows the same OfficeScan XG interface as before, but the "Ajouter un domaine" dialog is closed. In the left sidebar, the tree view now includes "Serveurs" under "D-eluard.local". The main table area shows a new entry for "Serveurs" under the "Domaine/Endpoint" column.

Se placer au niveau « D-domaine ».

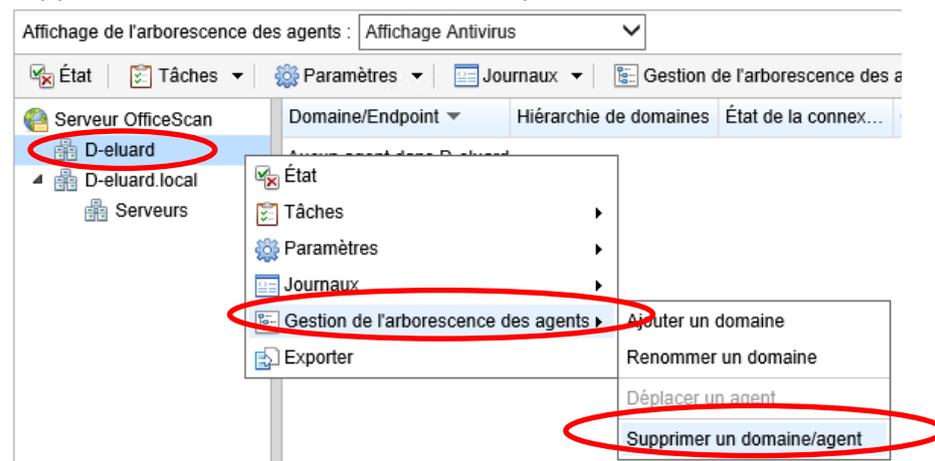
Sélectionner toutes les stations et les déplacer dans le domaine nouvellement créé :



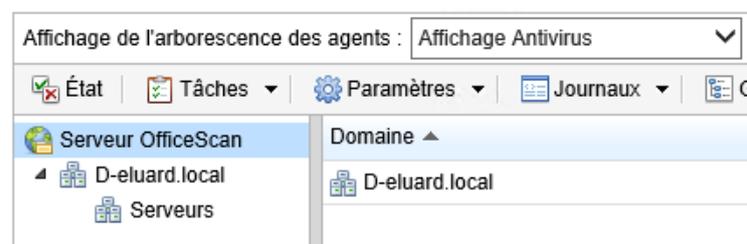
Procéder de même, afin de regrouper les serveurs dans le sous-domaine « Serveurs » :



Supprimer le domaine « D-domaine » qui est vide :



On obtient :



7-4.2 Menu Paramètres – Paramétrage par import d’un fichier .dat Agents... Gestion des agents... Paramètres...

https://serveur02.d-eluard.local:4343/officescan/console/html/cgi/cgiChkMasterPwd.exe

OfficeScan XG

Tableau de bord Évaluation **Agents** Journaux Mises à jour Administration Mod...

Gestion des agents

Sélectionnez des domaines ou des endpoints dans l'arborescence des agents, puis sélectionnez l'une des tâches présentées au-dessus de cette arbores

Recherche de endpoints : [Recherche avancée](#)

Affichage de l'arborescence des agents : Mise à jour

État Tâches **Paramètres** Journaux Gestion de l'arborescence des agents Exporter

Serveur OfficeScan

- D-eluard
 - Paramètres de scan
 - Paramètres de Web Reputation
 - Paramètres de l'apprentissage automatique prédictif
 - Paramètres de connexion suspecte
 - Paramètres de surveillance des comportements
 - Paramètres de contrôle des dispositifs
 - Soumission d'échantillons
 - Paramètres de l'agent de mise à jour
 - Privilèges et autres paramètres
 - Paramètres des services complémentaires
 - Liste des spywares/graywares approuvés
 - Liste des programmes approuvés
 - Exporter des paramètres
 - Importer des paramètres

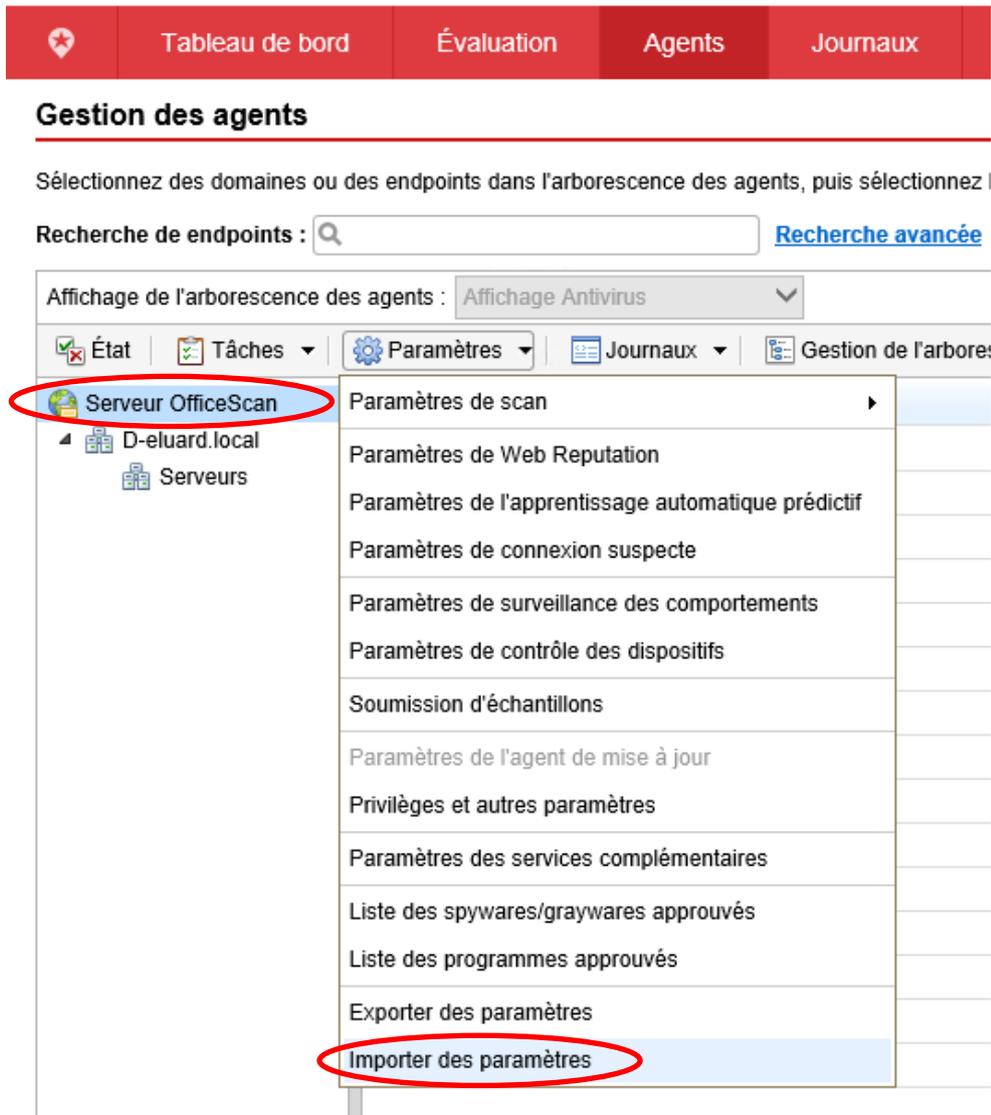
Remarques importantes :

- De nombreux paramètres (voir ci-dessus), concernant le serveur OfficeScan et son arborescence, doivent encore être configurés.
- Cette démarche pourra être simplifiée en effectuant l'import d'un fichier, comprenant l'ensemble de ce paramétrage (fichier .dat).
- Toutefois l'application de ce fichier, peut entrainer des perturbations importantes sur le réseau.
On évitera en particulier, le changement de la méthode de scan (passage de la méthode « Smart scan » à la méthode « Scan traditionnel » ou inversement), dans les périodes où le réseau est déjà fortement sollicité.
- L'import du fichier peut être réalisé à différents niveaux dans l'arborescence :
 - L'import au niveau « **Serveur OfficeScan** » concernera tous les domaines et sous-domaines.
 - L'import au niveau d'un domaine, ne s'appliquera qu'aux stations et serveurs du domaine.
- Les mots de passe permettant le téléchargement ou la désinstallation de l'agent, ne sont pas modifiés lors de l'import du fichier dat.

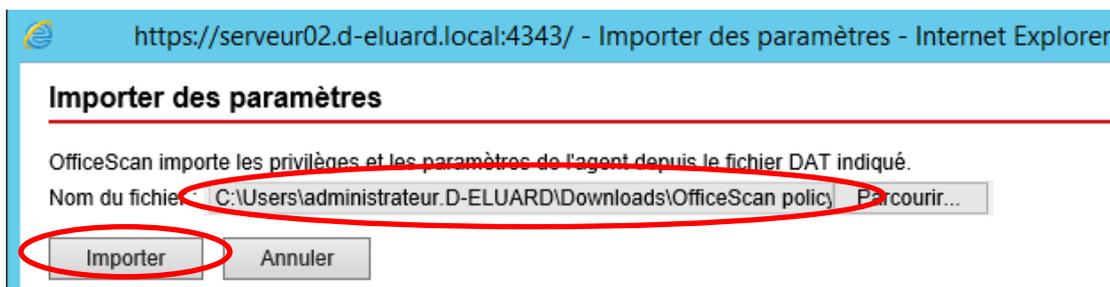
Import d'un fichier .dat : Le fichier **OfficeScan policy_L2.dat** n'est valable que si la console est installée sur Serveur02. Dans le cas contraire voir remarque page 40.

Se placer au niveau « Serveur OfficeScan » puis faire :

Agents... Gestion des agents... Paramètres... Importer des paramètres...



Indiquer le chemin du fichier .dat et faire Importer :



Le changement de méthode de scan peut entraîner quelques perturbations sur le réseau :

https://serveur02.d-eluard.local:4343/ - Importer des paramètres - Internet Explorer

Importer des paramètres

IMPORTANT : soyez prudents lors de l'importation de paramètres de méthode de scan. Le passage d'une méthode de scan à une autre requiert une planification et une exécution soigneuses. Avant de changer de méthode de scan, lisez les [directives](#) suivantes.

Importer des paramètres

Cliquez sur les liens ci-dessous pour afficher les détails des paramètres :

- [Méthodes de scan](#)
- [Paramètres de scan manuel](#)
- [Paramètres de scan en temps réel](#)
- [Paramètres de scan programmé](#)
- [Paramètres de scan immédiat](#)
- [Paramètres de Web Reputation](#)
- [Paramètres de l'apprentissage automatique prédictif](#)
- [Paramètres de connexion suspecte](#)
- [Paramètres de surveillance des comportements](#)
- [Paramètres de contrôle des dispositifs](#)
- [Soumission d'échantillons](#)
- [Privilèges et autres paramètres](#)
- [Paramètres des services complémentaires](#)
- [Liste des spywares/graywares approuvés](#)

Appliquer à tous les domaines

https://serveur02.d-eluard.local

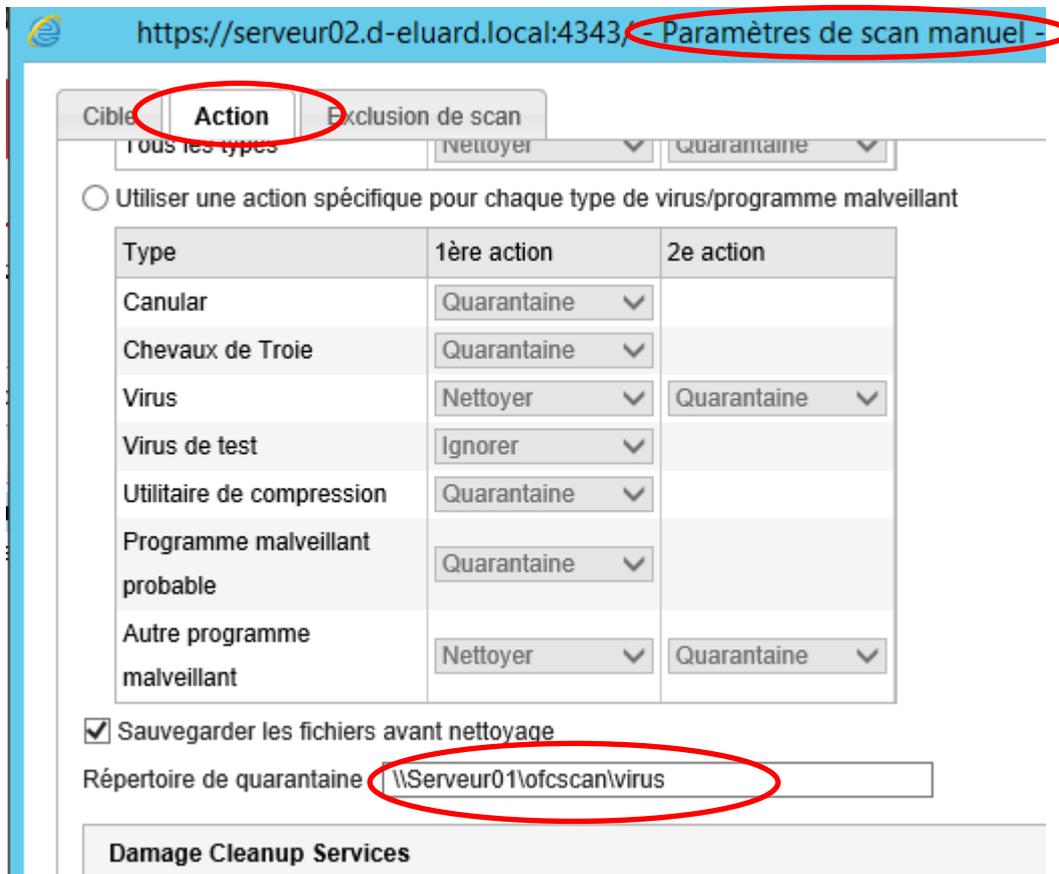
Importer paramètres

Le fichier de paramètres a été importé.

Remarque :

Si la console Trend est installée sur un Serveur01 et non sur un Serveur02, modifier les chemins de mise en quarantaine, après importation du fichier .dat.

Agents... Gestion des agents... Paramètres de scan... Paramètres de scan manuel... Onglet Action...



Procéder de même pour les menus :

- Paramètres de scan... Paramètres de scan en temps réel...
- Paramètres de scan... Paramètres de scan programmé...
- Paramètres de scan... Paramètres de scan immédiat...

7-4.3 Menu Paramètres - Paramétrage manuel :

Remarque : On est ici dans le cas où aucun fichier .dat n'a été importé, ou bien on souhaite vérifier le résultat de l'import.

Paramètres... Paramètres de scan... Méthodes de scan...

Le changement de méthode de scan peut entraîner quelques perturbations sur le réseau :

Décocher impérativement : « Scanner un lecteur réseau » :

https://serveur02.d-eluard.local:4343/ - Paramètres de scan en temps réel - Internet Explorer

Paramètres de scan en temps réel

Activer le scan antivirus/programme malveillant

Activer le scan antispyware/grayware

Cible | Action | Exclusion de scan

Action des utilisateurs sur les fichiers

Scanner les fichiers en cours de : création/modification et récupération ▼

Fichiers à scanner

Tous les fichiers scannables

Types de fichiers scannés par IntelliScan ⓘ

Fichiers possédant les extensions suivantes (séparer les différentes entrées par une virgule) :

."" ,.ACCDB,.ACE,.AMG,.ARJ,.BAT,.BIN,.BOO,.BOX,.BZ2,.CAB,.CDR,.CDT,.CHM,.CLA,.C LASS,.COM,.CPT,.CSC,.DLL,.DOC,.DOCM,.DOCX,.DOT,.DOTM,.DOTX,.DRV,.DVB,.DW G,.DWT,.EML,.EPOC,.EXE,.GMS,.GZ,.HLP,.HTA,.HTM,.HTML,.HTT,.INI,.JAR,.JPEG,.JP G,.JS,.JSE,.JTD,.JTT,.LNK,.LZH,.MDB,.MPD,.MPP,.MPT,.MSG,.MSI,.MSO,.MST,.NWS,. OBD,.OCX,.OFT,.OVL,.PDF,.PHP,.PIF,.PL,.PM,.POT,.POTM,.POTX,.PPAM,.PPS,.PPSM,

Paramètres de scan

Scanner les disquettes pendant l'arrêt

Scanner un lecteur réseau

Scanner le secteur d'amorçage du périphérique de stockage USB après sa connexion

Scanner tous les fichiers des périphériques de stockage amovibles lors de leur connexion

Des variantes de programmes malveillants en quarantaine sont détectées dans la mémoire ⓘ

Remarque : cette fonctionnalité requiert l'activation par les administrateurs du service de prévention des modifications non autorisées et du sei protection avancé.

Scanner les fichiers compressés

Nombre maximal de couches : 2 ▼ ⓘ

Scanner les objets OLE

Nombre maximal de couches : 3 ▼ ⓘ

Détecter le code d'exploitation dans les fichiers OLE ⓘ

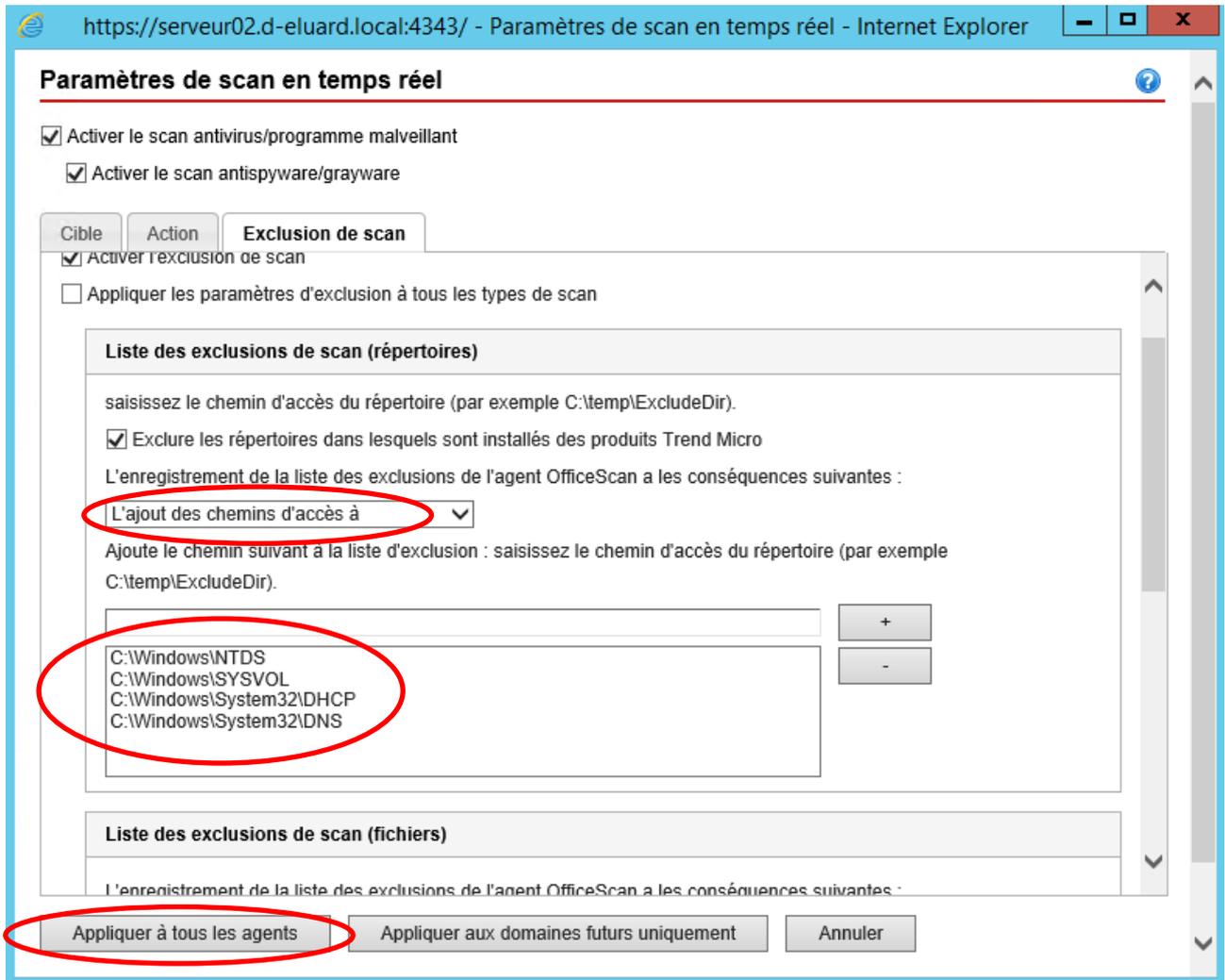
Paramètres de scan antivirus/programme malveillant uniquement

Activer IntelliTrap ⓘ

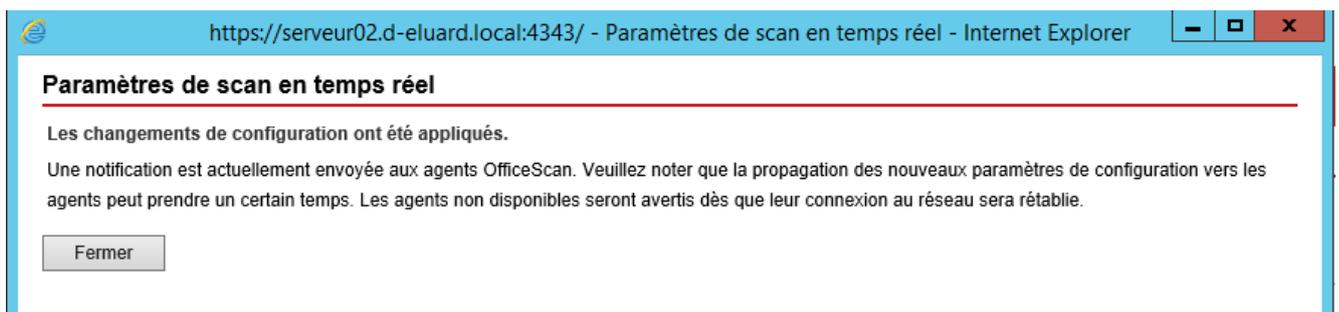
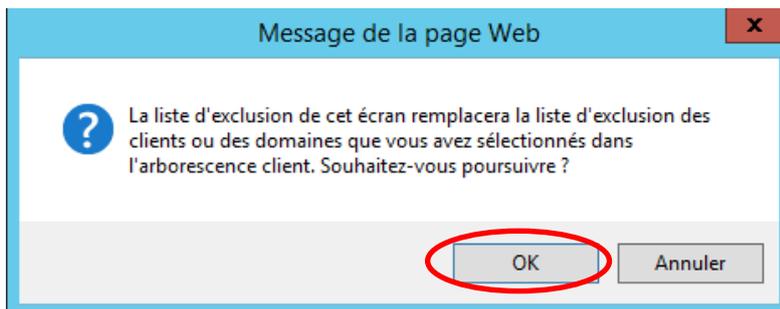
Activer le scan de la vulnérabilité CVE pour les fichiers téléchargés via Web et e-mail

Appliquer à tous les agents | Appliquer aux domaines futurs uniquement | Annuler

Paramètres... Paramètres de scan... Paramètres de scan en temps réel... Exclusion de scan...
Exclure du scan les dossiers systèmes sensibles :



Faire « Appliquer à tous les agents » :



Paramètres... Paramètres de scan... Paramètres de scan programmé... Exclusion de scan...
Faire un scan hebdomadaire, sans aucune exclusion :

Paramètres de scan programmé - Internet Explorer

Paramètres de scan programmé

Activer le scan antivirus/programme malveillant
 Activer le scan antispyware/grayware

Cible Action Exclusion de scan

Programmation

Quotidienne
 Hebdomadaire, tous les **Samedi**
 Mensuelle, le **01**
 Mensuelle, le **Premier** **Lundi**

Heure de début : **00** : **00** (hh:mm)

Fichiers à scanner

Tous les fichiers scannables
 Types de fichiers scannés par IntelliScan
 Fichiers possédant les extensions suivantes (séparer les différentes entrées par une virgule) :

.txt, .accdb, .arj, .bat, .bin, .boo, .cab, .chm, .cla, .class, .com, .csc, .dll, .doc, .docm, .docx, .dot, .dotm, .dotx, .drv, .eml, .exe, .gz, .hlp, .hta, .htm, .html, .htt, .ini, .jar, .jpeg, .jpg, .js, .jse, .lnk, .lzh, .mdb, .mpd, .mpp, .mpt, .msg, .msi, .msob, .msot, .mspx, .o, .ovl, .pdf, .php, .pif, .pl, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prc, .rar, .reg, .rtf, .scr, .shs, .sys, .tar, .vbe, .vbs, .vsd, .vss, .vst, .vx

Paramètres de scan

Scanner les fichiers compressés
Nombre maximal de couches : **2**

Scanner les objets OLE
Nombre maximal de couches : **3**

Détecer le code d'exploitation dans les fichiers OLE

Paramètres de scan antivirus/programme malveillant uniquement

Scanner la zone d'amorçage

Utilisation du processeur

Sur les endpoints des agents exécutant des applications consommant beaucoup de ressources de l'UC, OfficeScan peut s'interrompre entre les scans de fichiers afin de libérer des ressources de l'UC.

Élevé : scan des fichiers les uns après les autres (sans interruption entre les scans)
 Moyen : interruption entre les scans de fichiers si la consommation de l'UC est supérieure à 50 % ; pas d'interruption si elle est inférieure ou égale à 50 %

Appliquer à tous les agents Appliquer aux domaines futurs uniquement Annuler

Paramètres de scan programmé - Internet Explorer

Paramètres de scan programmé

Les changements de configuration ont été appliqués.
Une notification est actuellement envoyée aux agents OfficeScan. Veuillez noter que la propagation des nouveaux paramètres de configuration vers les agents peut prendre un certain temps. Les agents non disponibles seront avertis dès que leur connexion au réseau sera rétablie.

Fermer

Paramètres... Paramètres de surveillance des comportements...

Activer le blocage des processus de type Ransomware, et « Appliquer à tous les agents » :

https://serveur02.d-eluard.local:4343/ - Paramètres de surveillance des comportements - Internet Explorer

Paramètres de surveillance des comportements

ⓘ La surveillance des comportements ne prend pas en charge les plates-formes 64 bits Windows XP, Windows Server 2003 et Windows Vista (sans aucun Service Pack).

Règles Exceptions

Blocage du comportement des programmes malveillants

Activer le blocage du comportement des programmes malveillants
Menaces à bloquer

Protection contre les ransomware

Protéger des documents contre toute opération de chiffrement ou de modification non autorisée

Sauvegarder et restaurer automatiquement les fichiers modifiés par des programmes suspects ⓘ

Bloquer les processus généralement associés à des ransomware ⓘ

Activer l'inspection des programmes afin de détecter et de bloquer les fichiers exécutables compromis ⓘ

Remarque : l'inspection des programmes offre une sécurité accrue si vous sélectionnez « Menaces connues et potentielles » dans la liste déroulante Menaces à bloquer.

Protection contre les exploitations

Arrêter les programmes qui présentent un comportement anormal associé à des attaques par exploitation

Programmes récemment trouvés

Surveiller les programmes récemment trouvés téléchargés via HTTP ou des applications de messagerie ⓘ

Remarque : cette notification requiert l'activation par les administrateurs des fonctions Scan en temps réel et Web Reputation.

Surveillance des événements

Activer la surveillance des événements

► [Spécifier des paramètres détaillés](#)

Appliquer à tous les agents Appliquer aux domaines futurs uniquement Annuler

https://serveur02.d-eluard.local:4343/ - Surveillance des comportements - Internet Explorer

Surveillance des comportements

Les changements de configuration ont été appliqués.

Une notification est actuellement envoyée aux agents OfficeScan. Veuillez noter que la propagation du nouveau paramètre de configuration vers les agents peut prendre un certain temps. Les agents non disponibles seront avertis dès que leur connexion au réseau sera rétablie.

Fermer

https://serveur02.d-eluard.local:4343/ - Privilèges et autres paramètres - Internet Explorer

Privilèges et autres paramètres

Privilèges | Autres paramètres

Mode indépendant

Activer le mode indépendant

Scans

Autorisez les utilisateurs à exécuter les actions suivantes :

Configurer les paramètres de scan manuel

Configurer les paramètres de scan en temps réel

Configurer les paramètres de scan programmé

Scans programmés

Autorisez les utilisateurs à exécuter les actions suivantes :

Différer le scan programmé

Annuler et arrêter le scan programmé

Pare-feu

Afficher les paramètres du pare-feu sur la console de l'agent OfficeScan

Autoriser les utilisateurs à activer/désactiver le pare-feu, le système de détection d'intrusion et le message de notification de violation du pare-feu

Autoriser les agents OfficeScan à envoyer les journaux du pare-feu au serveur OfficeScan ⓘ

Surveillance des comportements

Afficher les paramètres de surveillance des comportements sur la console de l'agent OfficeScan

Liste des programmes approuvés

Afficher la liste des programmes approuvés sur la console de l'agent OfficeScan

Scan du courrier

Afficher les paramètres du scan du courrier sur la console de l'agent OfficeScan ⓘ

Paramètres proxy

Autoriser les utilisateurs à configurer des paramètres proxy ⓘ

Mises à jour des composants

Appliquer à tous les agents Appliquer aux domaines futurs uniquement Annuler

https://serveur02.d-eluard.local:4343/ - Privilèges et autres paramètres - Internet Explorer

Privilèges et autres paramètres

Privilèges **Autres paramètres**

Paramètres de mise à jour

- Les agents OfficeScan téléchargent des mises à jour depuis le serveur ActiveUpdate de Trend Micro
- Activer les mises à jour programmées sur les agents OfficeScan
- Les agents OfficeScan peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme de l'agent, ni déployer des correctifs de type hot fix

Paramètres de réputation de sites Web

- Afficher une notification lorsqu'un site Web est bloqué

Paramètres de surveillance des comportements

- Afficher une notification lorsqu'un programme est bloqué

Paramètres d'alerte de contact C&C

- Afficher une notification lorsqu'un rappel C&C est détecté

Paramètres d'alerte de restauration depuis la mise en quarantaine centrale

- Afficher une notification lorsqu'un fichier mis en quarantaine est restauré

Paramètres de l'apprentissage automatique prédictif

- Afficher une notification lorsqu'une menace est détectée

Autoprotection de l'agent OfficeScan

- Protéger les services de l'agent OfficeScan
- Protéger les fichiers du dossier d'installation de l'agent OfficeScan

Toujours dans :

Paramètres... Privilèges et autres paramètres... Autres Paramètres...

Désactiver le cache de Scan à la demande, puis « appliquer à tous les agents » :

https://serveur02.d-eluard.local:4343/ - Privilèges et autres paramètres - Internet Explorer

Privilèges et autres paramètres

Privilèges **Autres paramètres**

Afficher une notification lorsqu'une menace est détectée

Autoprotection de l'agent OfficeScan

Protéger les services de l'agent OfficeScan

Protéger les fichiers du dossier d'installation de l'agent OfficeScan

IMPORTANT : veuillez noter que les 2 fonctionnalités suivantes :

- Sont automatiquement désactivées sur les plates-formes Windows Server
- Ne sont pas prises en charge par les plates-formes 64 bits Windows XP, Windows Server 2003 et Windows Vista (sans aucun Service Pack)

Consultez l'aide en ligne pour plus d'informations.

Protéger les clés de Registre de l'agent OfficeScan

Protéger les processus de l'agent OfficeScan

Paramètres de scan programmé

Afficher un message de notification avant le début d'un scan programmé ⓘ

Paramètres du cache pour les scans

Activer le cache de la signature numérique ⓘ

Générer le cache tous les jours.

Activer le cache du Scan à la demande ⓘ

Ajouter le cache pour les fichiers légitimes qui n'ont pas été modifiés depuis jours.

Le cache de tous les fichiers légitimes expire dans jours.

Paramètres de scan de la messagerie POP3

Scanner la messagerie POP3

Restriction de l'accès à l'agent OfficeScan

Ne pas autoriser les utilisateurs à accéder à la console de l'agent OfficeScan depuis la barre d'état système ou le menu Démarrer de Windows ⓘ

Notification de redémarrage

Afficher une notification si le endpoint doit redémarrer pour terminer le nettoyage des fichiers infectés

Appliquer à tous les agents Appliquer aux domaines futurs uniquement Annuler

https://serveur02.d-eluard.local:4343/ - Privilèges et autres paramètres - Internet Explorer

Privilèges et autres paramètres

Les changements de configuration ont été appliqués.

Une notification est actuellement envoyée aux agents OfficeScan. Veuillez noter que la propagation des nouveaux paramètres de configuration vers les agents peut prendre un certain temps. Les agents non disponibles seront avertis dès que leur connexion au réseau sera rétablie.

Fermer

Paramètres... Paramètres des services complémentaires...

Pas de modifications sur cette page :

Paramètres des services complémentaires - Google Chrome

Non sécurisé | <https://serveur02.d-eluard.local:4343/officescan/console/html/clientmag/cl...>

Paramètres des services complémentaires

Service de prévention des modifications non autorisées ⓘ

Le service de prévention des modifications non autorisées ne prend pas en charge les plates-formes 64 bits Windows XP, Windows Server 2003 et Windows Vista (sans aucun Service Pack).

Activer le service sur les systèmes d'exploitation suivants :

- Windows XP
- Windows Vista
- Windows 7
- Windows 8/8.1
- Windows 10

Service de connexion suspect ⓘ

Activer le service sur les systèmes d'exploitation suivants :

- Windows XP
- Windows Vista
- Windows 7
- Windows 8/8.1
- Windows 10

Service de protection avancé ⓘ

Activer le service sur les systèmes d'exploitation suivants :

- Windows XP
- Windows Vista
- Windows 7
- Windows 8/8.1
- Windows 10

Appliquer à tous les agents Appliquer aux domaines futurs uniquement

Annuler

Se placer sur le domaine D-Domaine.local puis faire :

Paramètres... Paramètres de l'agent de mise à jour...

Affichage de l'arborescence des agents : Affichage Antivirus					
État	Tâches	Paramètres	Journaux	Gestion de l'arborescence des agents	Exporter
Serveur OfficeScan	Paramètres de scan	État de la connexion	GUID	Virus/	
D-eluard.local	Paramètres de Web Reputation	Hors ligne	793caba4-978c-4355-8b...	0	
Serveurs	Paramètres de l'apprentissage automatique prédictif	Hors ligne	3faee9a5-3b77-49cf-b4...	0	
	Paramètres de connexion suspecte	Hors ligne	8323b4c3-3599-42d8-8c...	0	
	Paramètres de surveillance des comportements	Hors ligne	ae115167-a47b-4e56-a...	0	
	Paramètres de contrôle des dispositifs	Hors ligne	d52c1652-8d2c-4995-b2...	0	
	Soumission d'échantillons	Hors ligne	32cb0ffb-7fef-4f33-8dee...	0	
	Paramètres de l'agent de mise à jour	Hors ligne	aac55685-7483-4029-a...	0	
	Privilèges et autres paramètres	Hors ligne	54757a8a-ab15-435c-b...	0	
	Paramètres des services complémentaires	Hors ligne	9aad7712-6a36-4ea2-a...	0	
		Hors ligne	2f44d222-6a02-4f15-a3...	0	

https://serveur02.d-eluard.local:4343/ - Paramètres de l'agent de mise à jour - Internet Explorer

Paramètres de l'agent de mise à jour

Pour répartir les tâches de déploiement des composants, des paramètres du domaine, des programmes agent et des correctifs de type hot fix sur les agents OfficeScan, définissez des agents OfficeScan en tant qu'agents de mise à jour ou mettez à jour les sources des autres agents. [En savoir plus...](#)

Les agents OfficeScan peuvent servir d'agents de mise à jour pour les éléments suivants :

- Mises à jour des composants
- Paramètres de domaine
- Programmes et correctifs de type hot fix des agents OfficeScan

Enregistrer Annuler

i La configuration de l'agent de mise à jour s'effectue en 2 étapes :

- Affectez l'agent OfficeScan en tant qu'agent de mise à jour de composants spécifiques (ci-dessus).
- Spécifiez les agents qui seront mis à jour dans Mettre à jour l'agent à partir des mises à jour > Agents > Sources de mises à jour.

Message de la page Web

Vous souhaitez définir tous les agents OfficeScan des domaines sélectionnés en tant qu'agents de mise à jour ?

Remarque : la définition d'un grand nombre d'agents OfficeScan en tant qu'agents de mise à jour peut affecter les performances réseau pendant l'installation initiale lorsque les agents de mise à jour téléchargent l'ensemble des composants à partir du serveur OfficeScan.

OK Annuler

https://serveur02.d-eluard.local:4343/ - Paramètres des agents de mise à jour - Internet Explorer

Paramètres des agents de mise à jour

Les changements de configuration ont été appliqués.

Une notification est actuellement envoyée aux agents OfficeScan. Veuillez noter que la propagation des nouveaux paramètres de configuration vers les agents peut prendre un certain temps. Les agents non disponibles seront avertis dès que leur connexion au réseau sera rétablie.

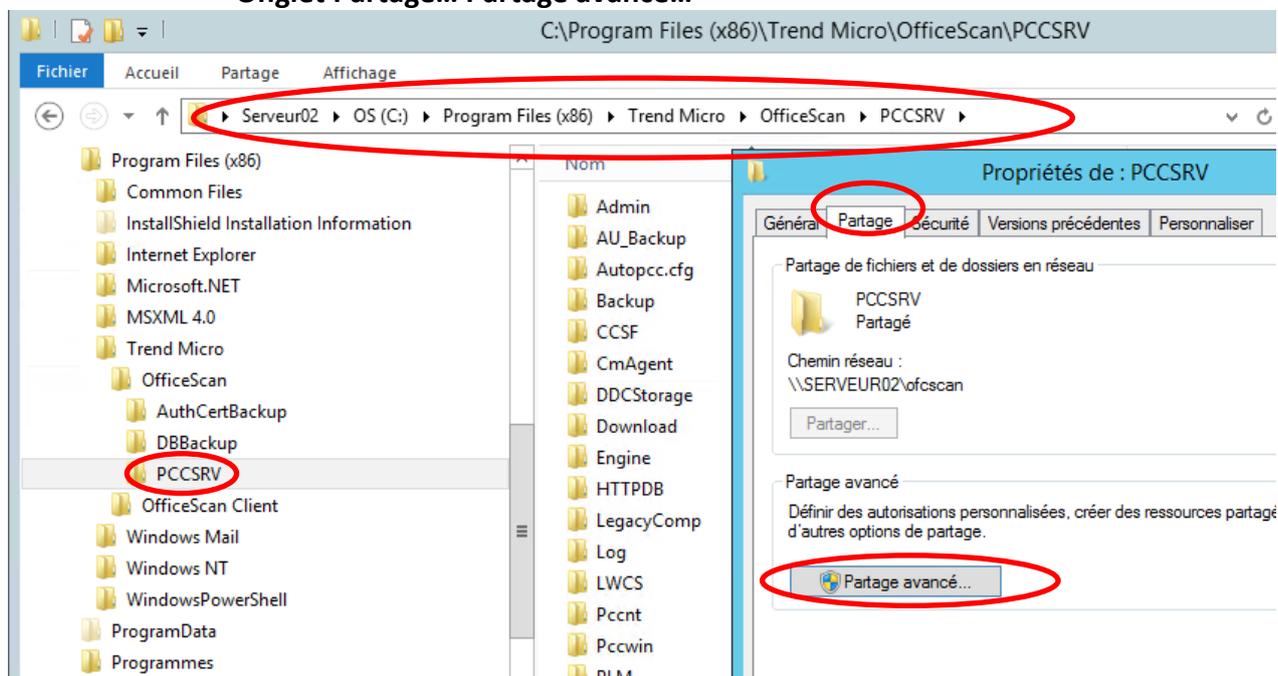
Fermer

8- Installation et déploiement de l'agent Trend

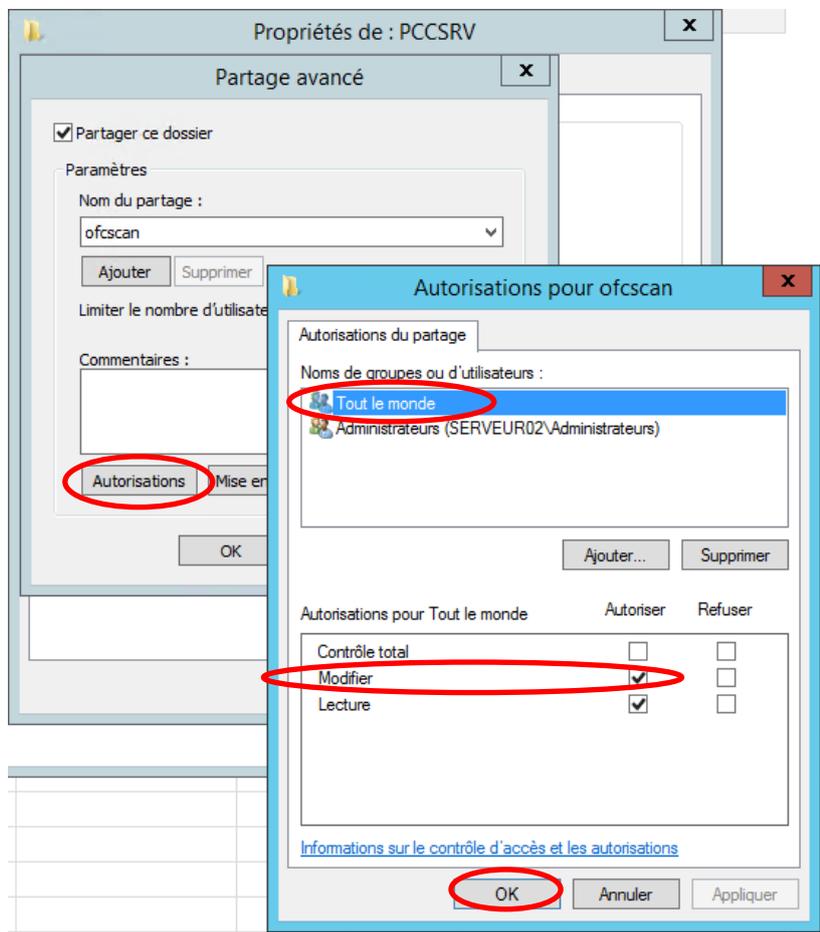
8-1 Modification des fichiers et des droits, dans le répertoire d'installation de Trend OfficeScan :

Ouvrir les propriétés du répertoire :

C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV :
Onglet Partage... Partage avancé...

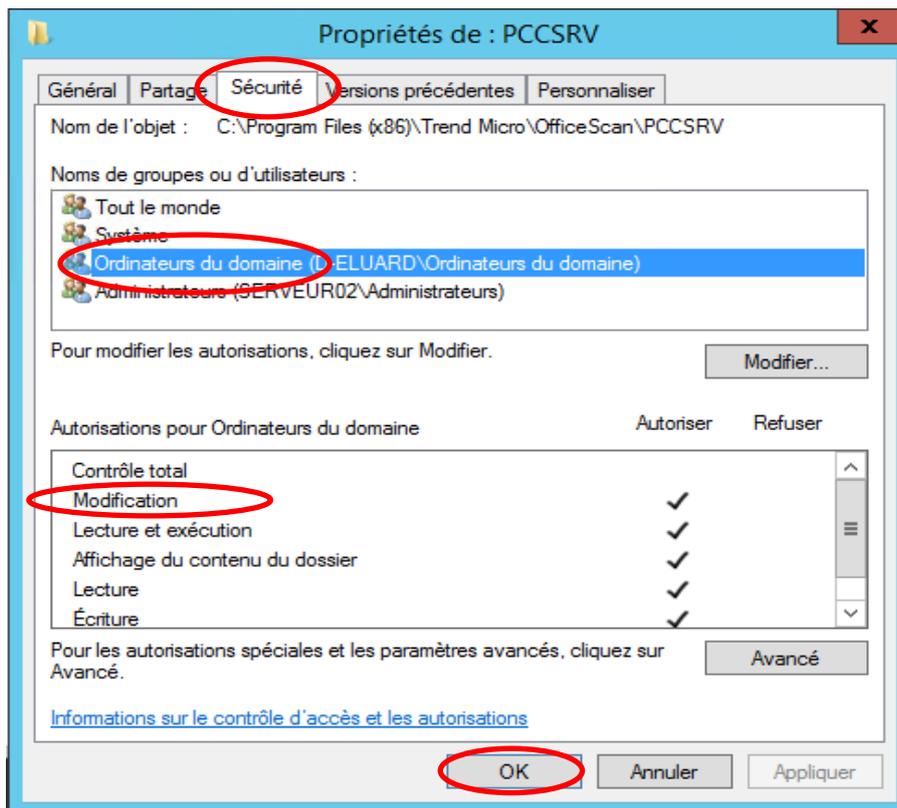


Dans les « autorisations du partage », donner les droits de « modification » à « Tout le monde » :



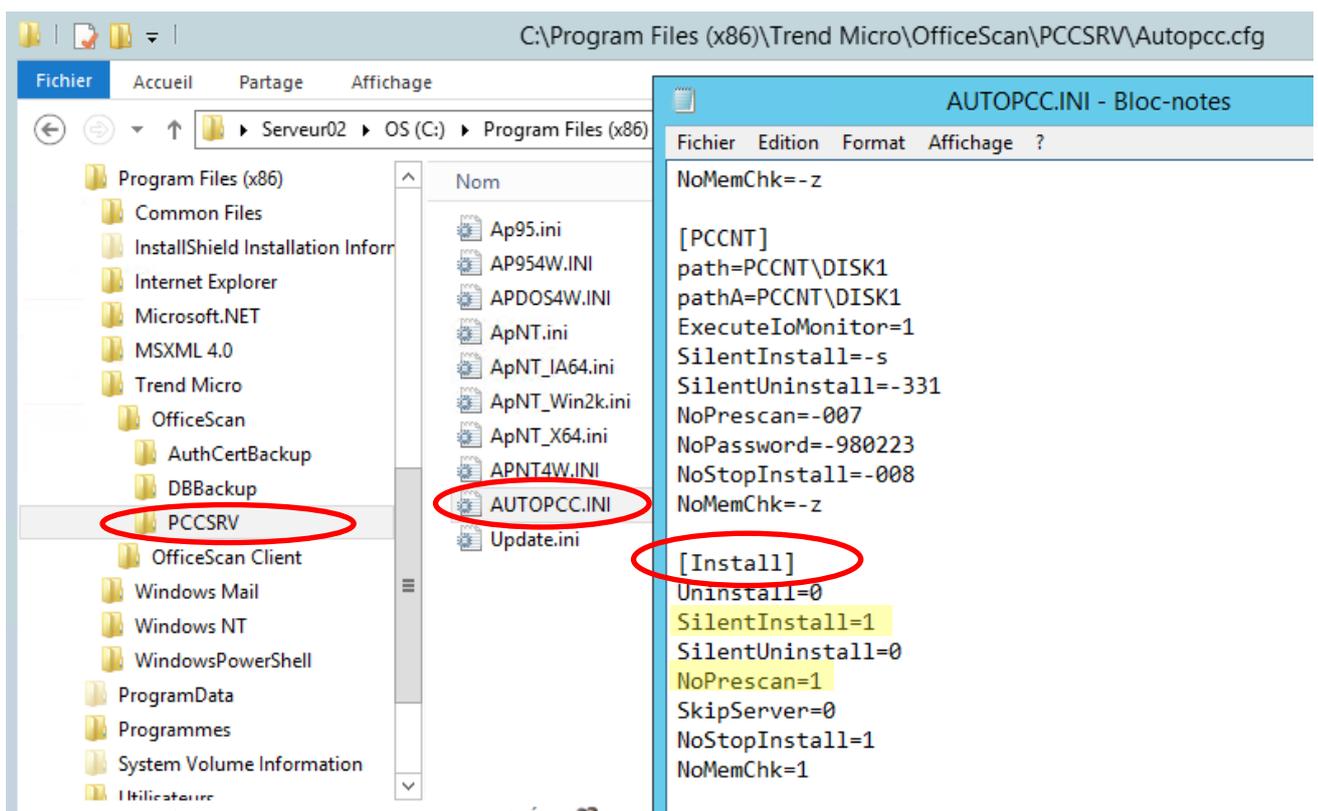
Onglet Sécurité...

Ajouter le groupe « **Ordinateurs du domaine** » avec les autorisations « **Modification** » :



Dans le répertoire : **C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV\Autopcc.cfg**
Editer le fichier **AUTOPCC.ini** et afin d'avoir une installation silencieuse de l'agent sans « préscan », apporter les modifications suivantes dans la section « Install » :

SilentInstall=1 NoPrescan=1

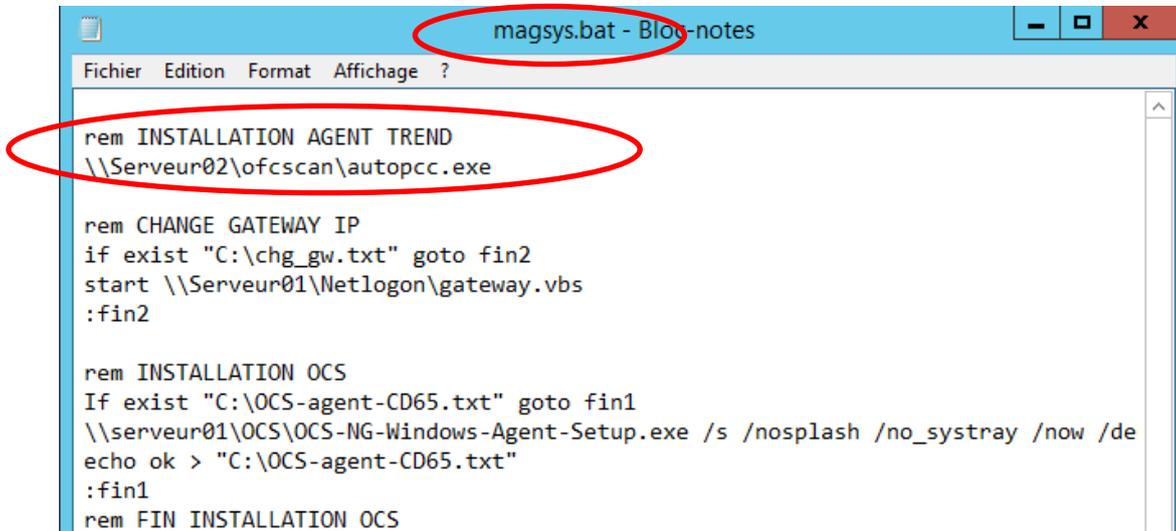


8-2 Installation de l'agent Trend :

La commande : `\\Serveur02\ofcscan\autopcc.exe` lancera l'installation de l'agent sur les stations ou les serveurs membres du domaine.

8-3 Installation automatique de l'agent Trend :

Ajouter la ligne `\\Serveur02\ofcscan\autopcc.exe` au fichier **Magsys.bat** dans **Netlogon** :



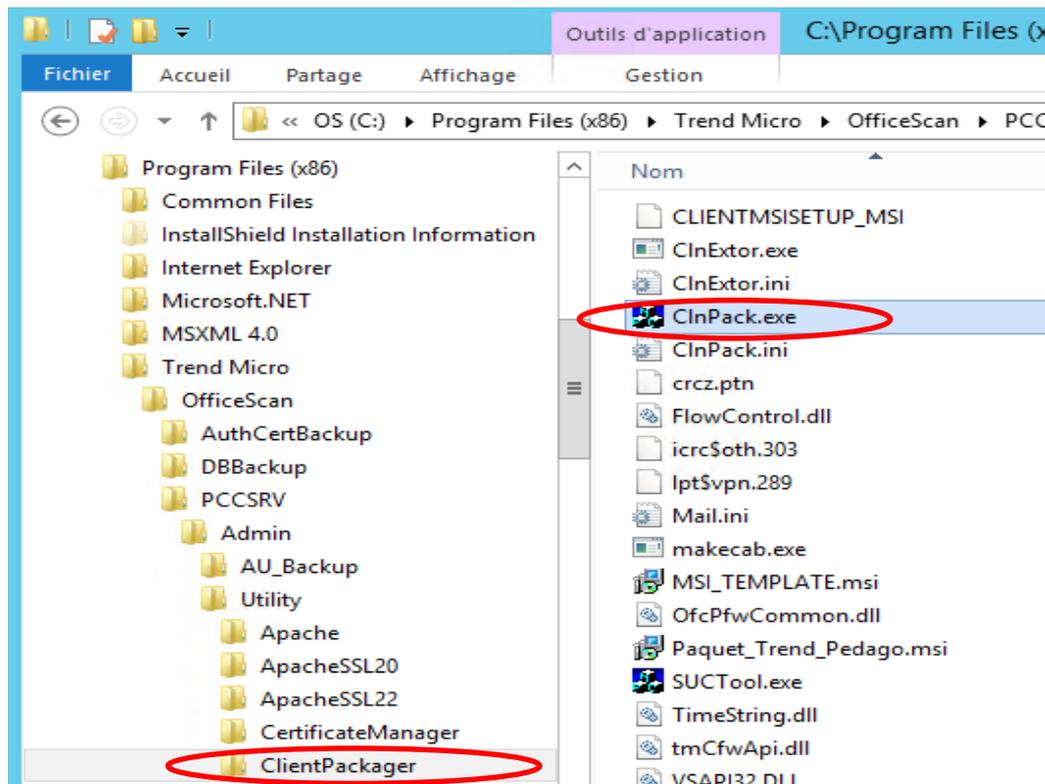
```
magsys.bat - Bloc-notes
Fichier Edition Format Affichage ?
rem INSTALLATION AGENT TREND
\\Serveur02\ofcscan\autopcc.exe

rem CHANGE GATEWAY IP
if exist "C:\chg_gw.txt" goto fin2
start \\Serveur01\Netlogon\gateway.vbs
:fin2

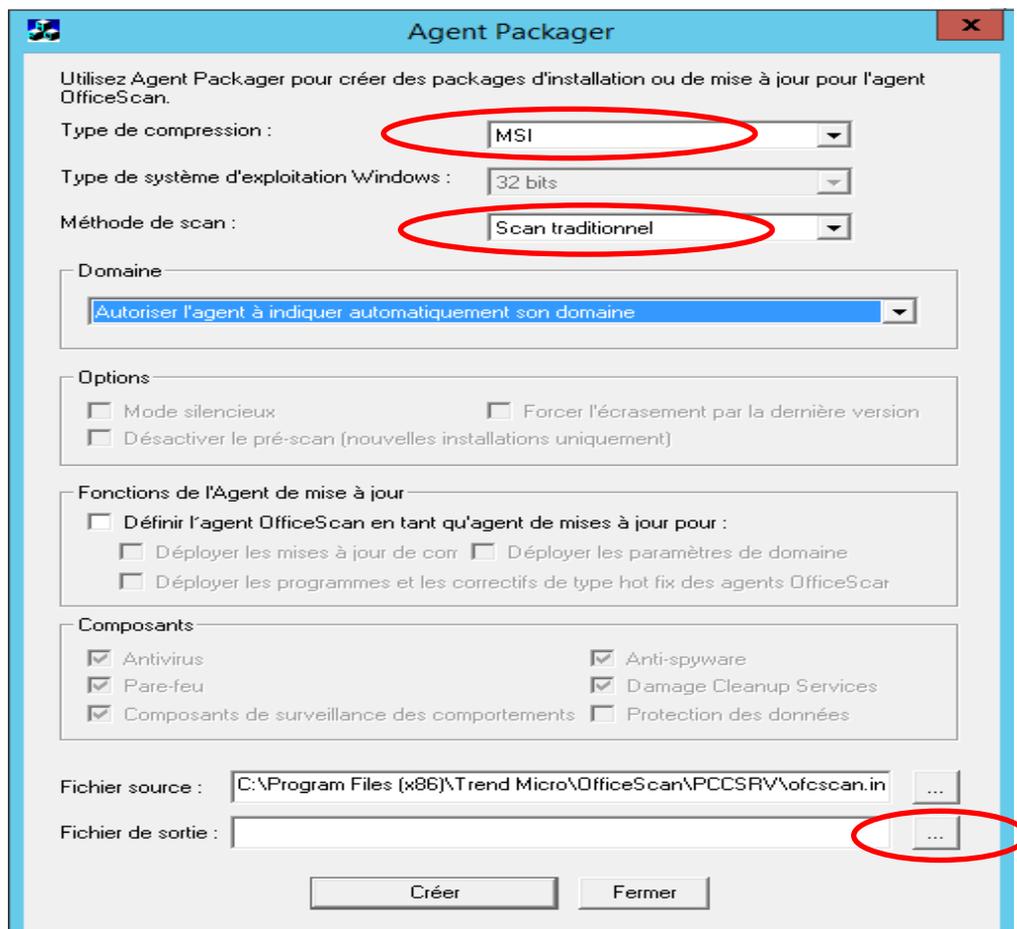
rem INSTALLATION OCS
If exist "C:\OCS-agent-CD65.txt" goto fin1
\\serveur01\OCS\OCS-NG-Windows-Agent-Setup.exe /s /nosplash /no_systray /now /de
echo ok > "C:\OCS-agent-CD65.txt"
:fin1
rem FIN INSTALLATION OCS
```

9- Création d'un paquet pour les serveurs DMZ, ZMI et pour les postes isolés du réseau :

Dans le répertoire : **C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV\Utility\ClientPackager**



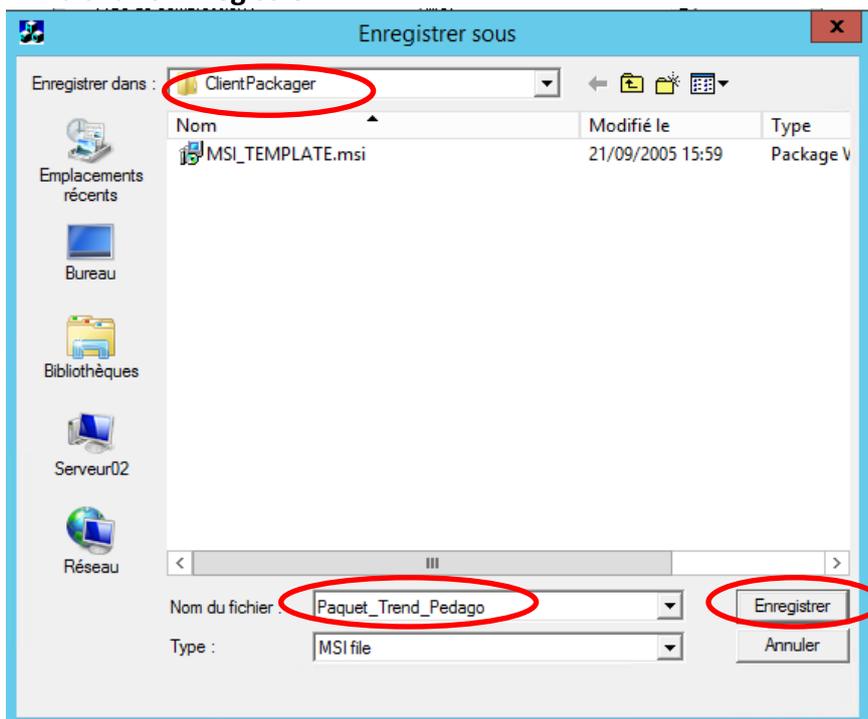
Exécuter **ClnPack.exe** fixer les paramètres du fichier de sortie (**MSI, Scan traditionnel**)



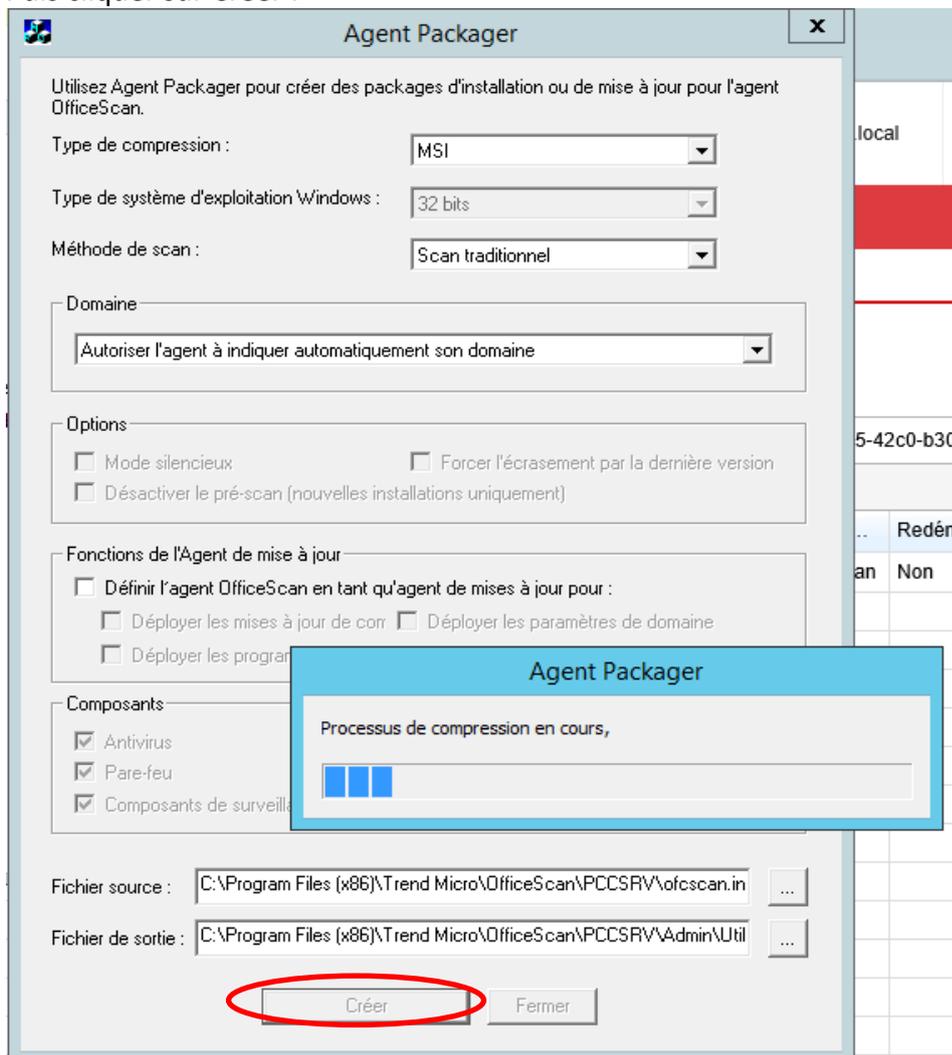
Indiquer le chemin et le nom du fichier de sortie :

C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV\Utility\ClientPackager\Paquet_trend_Pedago

Puis faire **Enregistrer** :



Puis cliquer sur **Créer** :



10- Migration des agents vers le nouveau Serveur :

Si la console Trend OfficeScan a été transférée d'un Serveur01 vers un Serveur02, il est nécessaire de connecter les agents Trend des stations à la nouvelle console.

On utilisera pour cela la commande IpXfer.

Dans Netlogon créer le fichier « **TrendMover.bat** » suivant :

```
Rem Migration des Agents Trend vers Serveur02 permettant le passage à la version Trend XG (12)
Rem Il est indispensable de connaître l'ancien mot de passe (ici "Aneto"), qui permettait, sur les stations, de
Rem télécharger l'agent Trend version 11
Rem 10.255.33.168 est l'adresse IP du Serveur02

if exist c:\cltmv.txt goto fin

Rem Stations 64 bits :
||serveur02\ofcscan\Admin\utility\ipxfer\IpXfer_x64.exe -s 10.255.33.168 -p 8080 -c 8000 -e
||serveur02\ofcscan\PCCNT\Common\OfcNTCer.dat -pwd Aneto

Rem Stations 32 bits :
||serveur02\ofcscan\Admin\utility\ipxfer\IpXfer.exe -s 10.255.33.168 -p 8080 -c 8000 -e
||serveur02\ofcscan\PCCNT\Common\OfcNTCer.dat -pwd Aneto

Rem Vérifier que "Ordinateurs du domaine" ont les droits de "Modification" sur le dossier "Packages"
echo %COMPUTERNAME% %DATE% %TIME% OK >> \\Serveur01\Packages\MigrationTrend.log
echo %COMPUTERNAME% OK >C:\cltmv.txt

:fin
```

Remarques :

- Mettre un espace, et pas de retour à la ligne après « -e ».
- A partir d'une station, lancer manuellement le script afin de vérifier, que le mot de passe est valide et que son exécution est correcte .
- Automatiser l'exécution du script en ajoutant la ligne :
\\Serveur01\Netlogon\TrendMover.bat
Aux « **Scripts** » « **Arrêt du système** » de la **Stratégie Ordinateurs**

11- Réinitialisation du mot de passe de la console Trend OfficeScan :

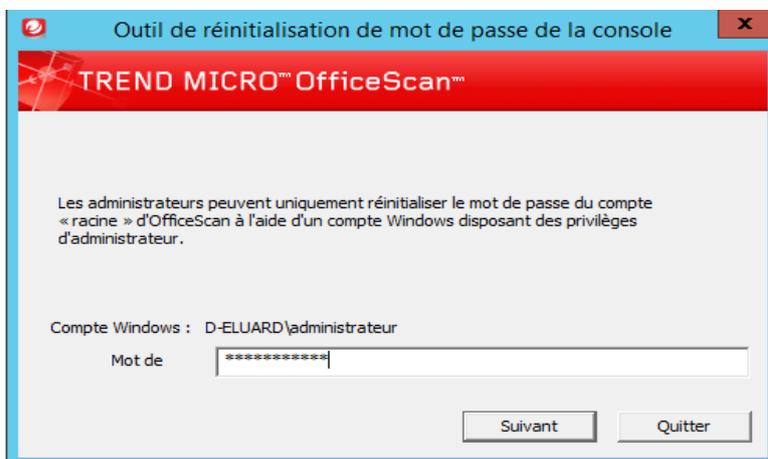
En cas de perte, le mot de passe du compte **root** de la console Web OfficeScan peut être réinitialisé.

Dans l'explorateur Windows, accéder au dossier :

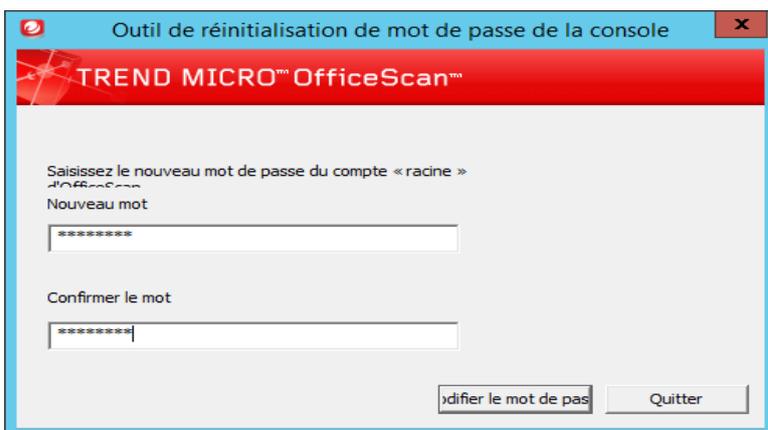
C:\Program Files (x86)\Trend Micro\OfficeScan\PCSRV\Admin\Utility\OSCEResetPW

Lancer l'exécutable : **OSCEResetPW.exe**

Le mot de passe de l'administrateur du domaine est nécessaire :



Indiquer le nouveau mot de passe du compte « root » :



Remarque : Les mots de passe nécessaires pour le téléchargement ou la désinstallation de l'agent sur les stations, peuvent être modifiés dans :

Paramètres... Privilèges et autres paramètres... Privilèges...